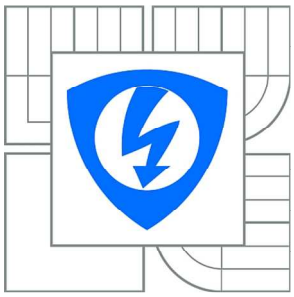
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

KOMUNIKAČNÍ ROZHRANÍ V MOBILNÍCH TELEFONECH

COMMUNICATION INTERFACES IN MOBILE PHONES

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

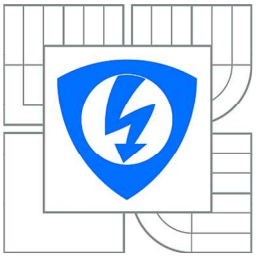
AUTOR PRÁCE — JIŘÍ PARDUBA

AUTHOR

VEDOUCÍ PRÁCE — Ing. ONDŘEJ MORSKÝ

SUPERVISOR

BRNO 2010



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student:	Jiří Parduba	***ID:***	106693
Ročník:	3	***Akademický rok:***	2009/2010

NÁZEV TÉMATU:

Komunikační rozhraní v mobilních telefonech

POKYNY PRO VYPRACOVÁNÍ:

Práce se věnuje problematice komunikačních rozhraní moderních mobilních telefonů a smartphonů. Úkolem studenta je popsat veškerá dostupná i v současné době vyvíjená rozhraní pro spojení mobilního telefonu s okolím, s GSM sítí, ale i se SIM kartou. Práce by měla být zaměřena na bezpečnost přenášených dat a také na možnost využití těchto rozhraní programátorem mobilních aplikací. Praktickým výstupem práce bude aplikace, která zjistí polohu telefonu z okolních sítí (Bluetooth, NFC, …) a podle ní vykoná požadovanou akci.

DOPORUČENÁ LITERATURA:

[1] RISCHPATER, Ray. Beginning Java ME Platform: APRESS, c2008. 569 s. ISBN 1-4302-1062-1.
[2] YANG, Baijian, ZHENG, Pei, NI, Lionel M. Professional Microsoft Smartphone Programming: WROX, c2008. 569 s. ISBN 978-0-471-76293-5.

Termín zadání:	29.1.2010	***Termín odevzdání:***	2.6.2010

Vedoucí práce: Ing. Ondřej Morský

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

ABSTRAKT

Tato práce se zabývá popsáním možností připojení mobilního telefonu do okolních sítí pomocí technologií, které jsou dostupné na dnešních mobilních telefonech, je to Bluetooth, IrDA Data, NFC, kabelové spojení a GPS. Dále popsáním mobilních sítí, zde jsou popsány technologie, se kterými se mobilní telefon propojuje se sítí na úrovni mobilního operátora, těmi jsou GSM, GPRS, EDGE a UMTS. Poté je uvedeno propojení telefonu se SIM kartou, zde jsou popsány funkce SIM karty a jak je používaná. Všechny tyto kapitoly jsou zaměřeny z pohledu bezpečnosti a programátora. Na základě nastudovaných možností se vybrala technologie, která byla použita při realizaci praktické části bakalářské práce. Nejlépe použitelnou se ukázala technologie Bluetooth. Dále jsou popsány tři nejpoužívanější operační systémy pro mobilní telefony, těmi jsou Windows Mobile (Phone), Symbian OS a Android, z toho vyplynulo, jaké jsou možnosti jejich využití. V praktické části jsou aplikovány znalosti z teoretické části a programovacím jazykem Java je realizována aplikace, které komunikuje pomocí technologie Bluetooth. Tato aplikace je vytvořena na platformě JavaME a z uživatelského hlediska je použitelná například k informačním sdělením o historických památkách, konkrétně je demonstrována na památce v Brně.

KLÍČOVÁ SLOVA

Bluetooth, mobilní telefon, programování, zabezpečení, Java.

ABSTRACT

The Bachelor thesis is focused on technologies, which are used for connection of mobile phone to other networks, which are available for current mobile phones - Bluetooth, IrDA Data, NFC, Cable connection and GPS, mobile networks, there are described technologies, which are used for connection to networks on the level of mobile operator - GSM, GPRS, EDGE and UMTS. In Bachelor thesis is also described connection of mobile phone and SIM card, there are shown functions of SIM card and how is the card used. These chapters are focused on security and programming properties of technologies. The appropriate technology, which was used in practiced part of Bachelor thesis, was chosen on basis of its properties with compare to other technologies. The most useful technology, which was chosen, is Bluetooth. There are also described three the most used operating systems for mobile phones – Windows Mobile (Phone), Symbian OS and Android, in this chapter is shown how these systems can be used. In practiced part of bachelor thesis are used data from theoretical part and by programming language JAVA is programmed the application, which communicates by Bluetooth. This application is programmed on the platform JavaME and users can use this application for example information announcements about historical monuments. This is concretely demonstrated on the historical monument in Brno.

KEYWORDS

Bluetooth, cellular phone, programming, security, Java.

PARDUBA, J. *Komunikační rozhraní v mobilních telefonech.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2010. 41 s. Vedoucí bakalářské práce Ing. Ondřej Morský.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma Komunikační rozhraní v mobilních telefonech jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a~jsem si plně vědom následků porušení ustanovení § 11 a následujících zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne ....

(podpis autora)

PODĚKOVÁNÍ

Děkuji vedoucímu bakalářské práce ing. Ondřeji Morskému za účinnou metodickou, pedagogickou a odbornou pomoc a další cenné rady při zpracování mé bakalářské práce.

V Brně dne ....

(podpis autora)

OBSAH

SEZNAM OBRÁZKŮ

ÚVOD

Tato práce je zaměřena na popis možností připojení telefonu do okolních sítí, jako je například Bluetooth, do mobilních sítí například GSM, ale také na propojení mobilního telefonu se SIM kartou, dále na operační systémy pro mobilní telefony a na praktickou část, kterou je aplikace pro mobilní telefon komunikující přes Bluetooth. Každá kapitola je zaměřena na jednu globální oblast a ta je soustředěna na konkrétní problémy. V těchto kategoriích se řeší bezpečnost dané technologie a využití z programátorského hlediska. Na závěr každé kapitoly jsou zhodnoceny výhody a nevýhody. Ty by měly ujasnit, proč je technologie, kterou si na závěr zvolím pro další rozšíření, nejlepší.

V první kapitole jsou podrobně rozebrány čtyři technologie, které využívá mobilní telefon pro komunikaci s okolními zařízeními. První technologií je bluetooth, u té jsou popsány dvě aktuální verze a jedna, která by měla být využívaná od roku 2010. Další částí je bezpečnost, u které jsou uvedeny a popsány tři základní bezpečnostní prvky. V části programování jsou uvedeny možnosti využití bluetooth v programech. Druhou technologií je IrDA Data, tato technologie je okrajově popsána. Třetí popsanou technologií je NFC, která u nás zatím není často využívaná. Poslední technologií je GPS, která je podrobně popsána i s jejím zabezpečením.

Druhá kapitola zachycuje dvě technologie a jejich variace. První je GSM a s ním související GPRS a EDGE, zaměřené na obecné popsání jejich principu a bezpečnost. Druhou je W-CDMA a UMTS, které jsou zaměřeny stejně jako GSM, přidány jsou také obrázky vystihující strukturu GSM sítě, princip autentizace a základní architekturu UMTS sítě.

Třetí kapitola popisuje SIM kartu, zaměřil jsem se především na princip karty a její bezpečnost, dále je popsána technologie SIM Toolkit a GSM banking, který tuto technologii využívá. Informace jsou uvedeny také o technologii SWP, avšak tato technologie je momentálně vyvíjená a tak je popsána jen okrajově.

Ve čtvrté kapitole jsou popsány tři operační systémy pro mobilní telefony, využívané na více než jedné značce mobilního telefonu. Zmíněn je vývoj a také jaké platformy podporují z pohledu programátora

Pátá kapitola je zaměřena na popis praktické části, kterou je aplikace komunikující přes technologii Bluetooth. Popsána je z uživatelského a programátorského hlediska, závěrem je shrnuta, na jakých zařízeních byla aplikace odzkoušena.

1 MOBILNÍ TELEFON V OKOLNÍCH SÍTÍCH

V následujícím textu jsou představeny technologie používané v mobilních telefonech, se kterými je možné připojit se k počítači.

1.1 Bluetooth

1.1.1 Obecné informace

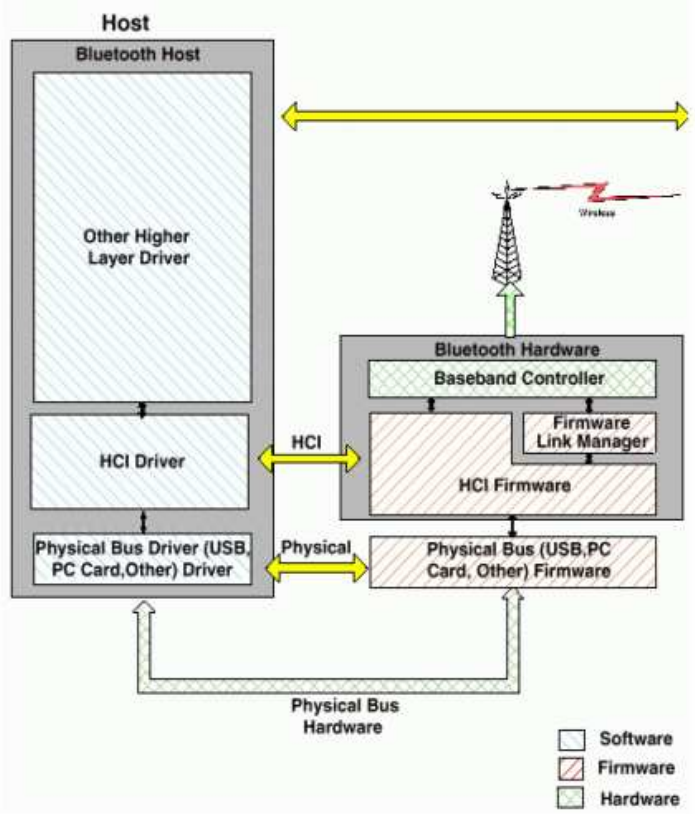
Technologie Bluetooth je využívaná k bezdrátovému přenosu s krátkým dosahem, mezi elektronickými zařízeními. Ve většině případů je nutné, aby byla zařízení ve vizuálním kontaktu. Maximální vzdálenost mezi jednotlivými zařízeními je 30m v prostranství bez překážek, ale v praxi se největší vzdálenost pohybuje do 10m, aby nedošlo ke ztrátě signálu. Původně sloužila tato technologie jako náhrada kabelů při připojování zařízení k počítači.

Technologie je definovaná standardem IEEE 802.15.1 a je zařazena do kategorie osobních počítačových sítí PAN. Přenos probíhá v bezlicenčním pásmu 2,4GHz, konkrétně bluetooth využívá 2,402 – 2,48GHz, to je rozděleno na 79 kanálů s odstupem 1MHz. Přenosová rychlost se liší u jednotlivých standardů.

V současné době se v mobilních telefonech nejvíce využívá **Bluetooth v2.0 EDR** (Enhaced Data-Rate), které má přenosovou rychlost až 2,1Mb/s a používá modulační technologii pi/4 DQPSK.

Bluetooth v2.1 + EDR je vylepšená verze Bluetooth v2.0 EDR. Vylepšení spočívá v jednodušším párování zařízení, u něj je snížený počet kroků potřebných ke spárování, takže by měl být uživatelsky méně náročný a přístupnější méně zdatným uživatelům. Dále je snížena energetická náročnost, oproti předchozí verzi by měla být spotřeba Bluetooth modulu 5x menší. Posledním vylepšením je vybavení této verze o technologii NFC (Near Field Communication), při jejím použití dojde k párování automaticky těsným přiblížením obou zařízení a následným potvrzením spojení.

Bluetooth v3.0, tato verze vychází z v2.1, avšak rychlost se zvyšuje až na 24Mb/s. Je založena na protokolu 802.11 PAL (Protocol Adaptation Layer), který vychází ze standardu Wi-Fi. V praxi díky blízkým vlastnostem technologií bude fungovat tak, že pokud bude přístroj s touto technologií a zařízení s podporou Wi-Fi využije se technologie s rychlejším přenosem. Tato verze zatím není používaná, za standard byla přijata v dubnu 2009 a v prvních zařízeních by se měla objevovat začátkem roku 2010.



Obr. 1.1: Znázornění principu bluetooth (převzato z [2]).

1.1.2 Bezpečnost

Bluetooth využívá tři základní bezpečnostní služby, těmi jsou autentizace (ověření totožnosti komunikujících stran), důvěrnost (ochrana před odposloucháváním) a autorizace (povolení přístupu k službám). Může pracovat v jednom ze tří bezpečnostních režimů: bez zabezpečení (režim umožňující navázat komunikaci jakémukoliv jinému zařízení), bezpečnost na úrovni služeb (autorizuje přístup k jednotlivým službám na zařízení) a bezpečnost na úrovni spoje (zabezpečuje přístup před navázáním spojení).

Při párování zařízení se vygeneruje inicializační klíč – ze zadaného PIN, z unikátní adresy zařízení (BD_ADDR), které spojení vytvořilo a náhodně vygenerovaného čísla, které vytvoří zařízení přijímající připojení, to je pro každé připojení odlišné.

Délka PIN je 8 – 128b, adresa zařízení je 48b, stejně jako u síťové karty a náhodně vygenerované číslo má 128b.

Nejnebezpečnější fáze přenosu dat je při výměně těchto údajů mezi zařízeními, protože není nijak chráněna, proto se nedoporučuje při přenosu citlivých dat provádět párování na veřejném místě, kde by mohlo dojít k odposlechu. Jakmile proběhnou všechny tyto kroky, vytvoří se v zařízeních klíč spoje (link key). Tento klíč je tajný

a zařízení ho nikdy nevysílají. Autentizace a generování klíčů využívá algoritmy $E_0, E_1, E_3, E_{21}, E_{22}$ vytvořené na bázi symetrického blokového algoritmu SAFER+.

Za bezpečnostní prvek se dá považovat i krátká vzdálenost, ve které lze mezi zařízeními data přenášet. Díky tomu se na veřejném prostranství dá odhalit místo, ze kterého by bylo odposlouchávání dat možné.

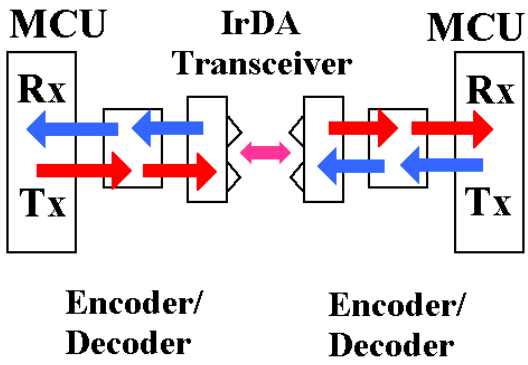
1.1.3 Využití v programování

K této technologii je možné vymyslet jakákoliv aplikace do mobilního telefonu, komunikující s okolními zařízeními. Například by se dala využít k ovládání počítače, nebo jako jednoduchý messenger mezi dvěma zařízeními. Já mám v plánu Bluetooth využít k lokalizaci zařízení. V praxi by mělo zařízení přečíst určité ID jiného zařízení a přehrát zvukovou stopu.

1.2 IrDA Data

1.2.1 Obecné informace

Technologie IrDA Data (Infrared Data Association Data) přenáší data v infračervené oblasti spektra na velmi krátké vzdálenosti řádově desítky cm, vzdálenost je závislá na vysílacím výkonu. Vlnová délka světla je 850 – 900nm. Nevýhodou přenosu dat je přímá viditelnost zařízení. Rychlost přenosu dat je dána standardem, IrDA **1.0** podporuje rychlost 2,4 – 115,2kb/s, IrDA **1.1**, ten podporuje rychlosti 576,1152 a 4Mb/s a **VFIR** (Very Fast IrDA), který zvládne přenosovou rychlost až 16MB/s.



Obr. 1.2: Způsob přenosu dat mezi zařízeními využívající IrDA (převzato z [6]).

1.2.2 Bezpečnost

Protože IrDA funguje na krátké vzdálenosti a potřebuje přímou viditelnost, není potřeba žádné zabezpečení. V praxi funguje přenos dat tak, že se na zařízení aktivuje příjem

IrDA signálu a na druhém poté spustí, jakmile jsou na sebe zařízení namířena, zahájí se přenos dat.

1.2.3 Programování

Jelikož IrDA u mobilních telefonů nemá vysokou rychlost, je možné vymyslet aplikace na synchronizaci dat mezi zařízeními. Také by své využití našla aplikace, která by pracovala jako univerzální dálkový ovladač na různá zařízení využívající IrDA, těmi jsou televize, radia a jiné.

1.3 NFC

1.3.1 Obecné informace

NFC (Near Field Communication) je vysokofrekvenční bezdrátová komunikační technologie, která umožňuje výměnu dat mezi zařízeními ve vzdálenosti do 10cm. Technologie je rozšíření ISO/IEC 14443 (bezkontaktní karty, RFID), která kombinuje rozhraní a čtečku čipových karet v jednom zařízení. NFC je zaměřen především na použití v mobilních telefonech. Technologie komunikuje pomocí magnetického pole v nelicencovaném pásmu 13,56MHz. Rychlost přenosu dat je 106, 212, 424 nebo 848kb/s. V České republice není zatím tato technologie téměř využívaná, ale do budoucna se počítá s bezkontaktním placením, např. jízdenek v hromadné dopravě, k párování zařízení podporující Bluetooth 2.1. Výhodou technologie je nízká energetická náročnost.

1.3.2 Bezpečnost

Protože komunikace technologie je omezena na řádově centimetry, není odposlouchávání přenosu téměř možné bez fyzického kontaktu se zařízením, NFC sám o sobě neposkytuje žádnou ochranu, takže hrozí čtení dat při zcizení zařízení. To může být problém provozování služby, při které dochází k finančním transakcím.

1.3.3 Programování

U této technologie by se dala naprogramovat aplikace pro synchronizace dat.

1.4 Kabelové spojení

1.4.1 Obecné informace

Dnes nejpoužívanějším přenosem dat mezi mobilním telefonem a počítačem je sériově přes USB (Universal Serial Bus) rozhraní. To má výhodu, že využívá možnost

Plug & Play, díky kterému se nemusí po připojení zařízení k počítači restartovat počítač. V praxi funguje tento přenos tak, že se zařízení připojí k počítači a na mobilním telefonu se aktivuje přenos, buď jen čtením z paměti telefonu, takže se nemusí instalovat žádné ovladače a přenos funguje stejně jako při použití běžného flash disku. Telefon musí podporovat master storage, aby byl takový přenos umožněn. Je možné zvolit variantu, která telefon spáruje s příslušným softwarem daného výrobce. V ní je možnost, u většiny dnešních telefonů, přistupovat prostřednictvím počítače do kalendáře, SMS zpráv a podobných aplikací použitých v mobilním telefonu. To je pohodlnější při rozsáhlejších úpravách na telefonu.

1.4.2 Bezpečnost

Protože tato technologie pracuje pomocí kabelového spojení, není odposlouchávání samotného přenosu dat možné.

1.4.3 Programování

Pro přípojení přes USB by bylo možné naprogramovat aplikaci využívající komponenty mobilního telefonu, protože má na zařízení nejmenší energetickou náročnost. Například by se telefon s lepším rozlišení fotoaparátu dal využít jako web kamera.

1.5 GPS

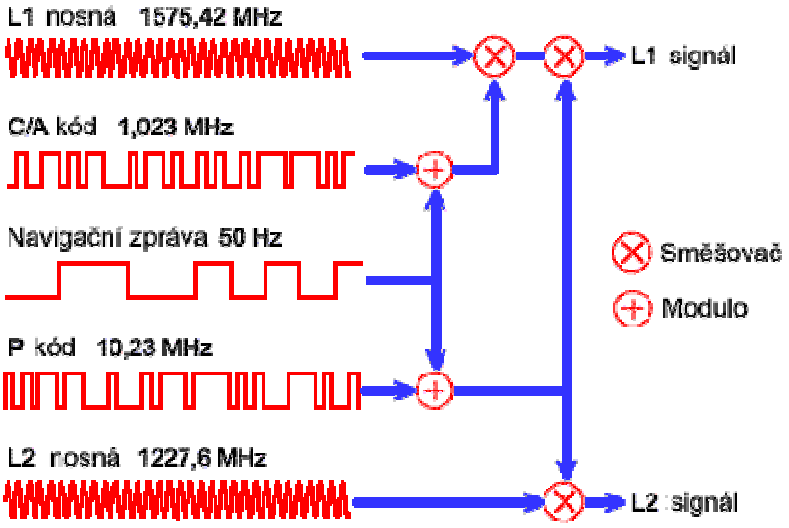
1.5.1 Obecné informace

GPS (Global Positioning System) je původně vojenský navigační systém provozovaný Ministerstvem obrany Spojených států amerických. Dokáže s několika centimetrovou přesností určit polohu kdekoliv na Zemi. K určení polohy se využívá jednosměrný přenos mezi družicí a zařízením. Družice signál vysílá a zařízení na Zemi signál přijímá. Družice jsou umístěny na šesti oběžných drahách, je jich 30, ale ve skutečnosti se používá 24 družic. Zbylé družice jsou záložní v případě poruchy. Jedna družice objede oběžnou dráhu za 12 hodin, z toho vyplývá, že se poloha družice mění, současně však bývá z jednoho místa na Zemi viditelných 6 – 12 družic.

Pro přenos signálu jsou vyhrazeny dva kmitočty, první s označením L1 má 1575,42MHz a s označením L2 o kmitočtu 1227,60MHz. Každá družice vysílá současně na obou kanálech, ale pro běžné přijímače se používá pouze kanál L1. Kanál L2 se používá pro velmi přesná měření. Princip výpočtu vzdálenosti je jednoduchý. Přijímač si nejprve vypočte vzdálenost, která jej dělí od několika okolních družic, a to z doby cesty signálu a z rychlosti světla včetně započítání vlivu atmosféry. Pokud tedy zná přijímač zatím jen vzdálenost k jedné z družic, předpokládá dle pravidel geometrie, že sám leží někde na plášti koule s poloměrem rovným dané vzdálenosti, jejíž střed

tvoří daná družice. Pokud ale zná vzdálenost i k jinému satelitu, může vypočíst průnik povrchu koule, což je už jen kružnice. Se třetí koulí se možnost polohy zúží pouze na dva body, přičemž jeden z nich leží buď vysoko v prostoru, nebo hluboko v Zemi a může se škrtnout. Tím je základní výpočet polohy hotov.

Signál GPS je velice slabý. Jeho úroveň se v blízkosti Země pohybuje v řádech 10 wattů. Jen pro přibližnou představu, v literatuře se taková energie přirovnává k úrovni světelného záření žárovky 25W pozorovaného ze vzdálenosti 17,7 tisíc km. Takový slabý signál je utopen hluboko v lokálním elektromagnetickém rušení, což ale není na závadu díky systému rozprostřeného spektra (CDMA), jež dovoluje restaurovat i podobně zarušený signál. Tato koncepce má svůj původ v období studené války, kdy se USA snažily systém skrýt před tehdejším ruským protivníkem. Další důvod je také omezený přísun elektrické energie, kterou družice čerpají ze solárních panelů. Nevýhodou pro uživatele je však to, že GPS si žádá nejlépe přímou viditelnost na oblohu. Slabý signál je špatně dostupný v budovách a podléhá atmosférickým vlivům.



Obr. 1.3: Vznik signálu GPS (převzato z [7]).

1.5.2 Bezpečnost

Signál je modulován kódovou posloupností, podle které dokáže přijímač rozpoznat satelit. Kanál L1 používá kód C/A (Coarse Acquisition) a současně kód P. Kódová posloupnost se využívá pro vojenské účely, taktéž je použit pro kanál L2.

1.5.3 Programování

Rozhraní GPS je nejvhodnější k použití s navigačním programem, který přímo na

displej ukazuje polohu v určité ulici, k tomu je však potřeba využití map, které dnes aktualizují dvě společnosti. Dále by se dala využít ke stejnému programu, který mám v plánu programovat, avšak je zapotřebí přímá viditelnost na družici, proto by bylo použití omezeno na venkovní použití.

1.6 Shrnutí

Jediní realizovatelní „kandidáti“ na zjišťování polohy v programu jsou Bluetooth a GPS. Jako nejlepší z těchto technologií bylo vybráno Bluetooth, protože jako jediná funguje na větší vzdálenost a je to nejrozšířenější technologie mezi mobilními telefony, která pracuje s okolními sítěmi. K aplikaci, která bude naprogramována, je vhodné i GPS a jelikož by stačila jednosměrná komunikace, byla by i nejméně náročná. Do programu by stačilo vložit souřadnici, na které se má zvukový záznam přehrát a problém by byl vyřešen, avšak nevýhodou je přímá viditelnost nutná k zjištění polohy mobilního zařízení a tudíž nemožné využití v uzavřených prostorech.

2 MOBILNÍ TELEFON V MOBILNÍ SÍTI

V této kapitole jsou představeny technologie používané při přenosu hovorů a dat v síti mobilních operátorů.

2.1 GSM

2.1.1 Obecné informace

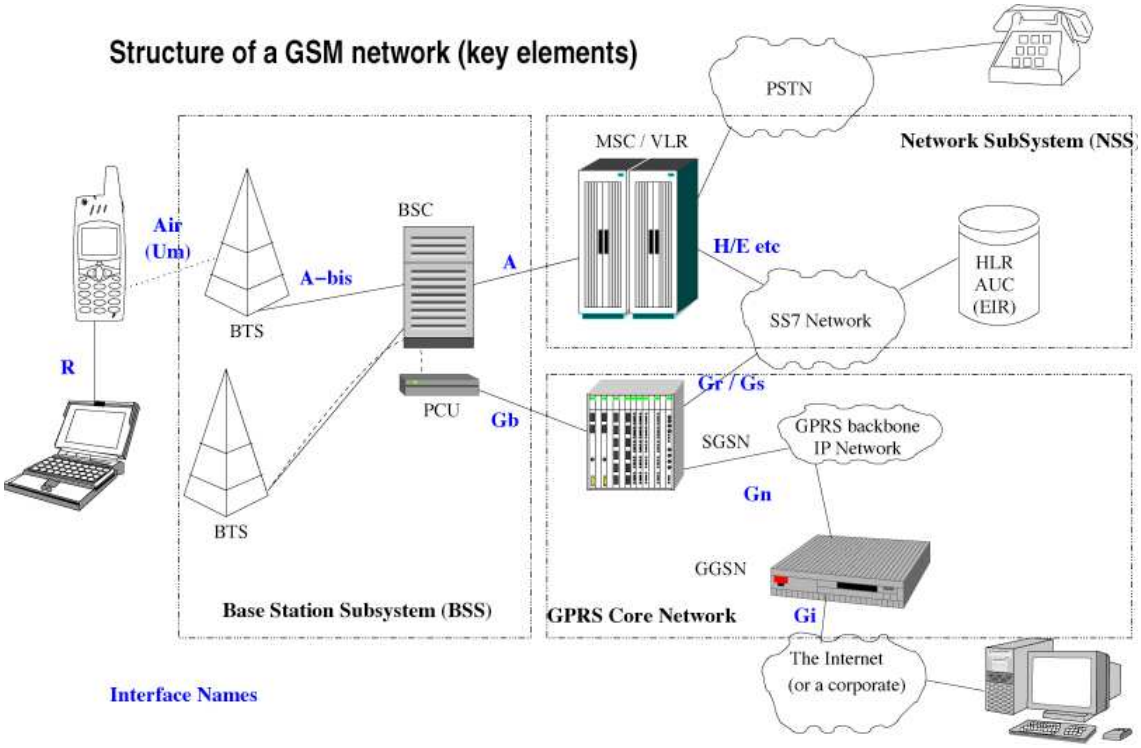
Systém **GSM** (Global Systém for Mobile Communication, Group Speciál Mobile) je využíván pro komunikaci mobilních zařízení po celém světě, základními službami je hlasová služba, posílání zpráv a datová služba. Patří mezi systémy druhé generace, které jsou plně digitální. Systém efektivně využívá přidělená kmitočtová pásma. Kmitočtové pásmo je rozděleno na PGSM a EGSM, GSM 1800 a GSM 1900. Technologie je založena na přepínání okruhů.

PGSM (Primary GSM) nebo GSM 900 pracuje v přiděleném kmitočtovém pásmu 890 – 960MHz. Pro uplink je vyhrazeno pásmo 890 – 915MHz a pro downlink 935 – 960Mhz. Uvnitř každého pásma je vytvořeno 124 rádiových kanálů a každý má šířku 200kHz. Systém PGSM používá 124 duplexních kanálů. V každém kanálů je vytvořeno 8 TS (Time Slot – časový interval) a do každého TS je přiřazen jeden účastnický kanál.

EGSM (Extended GSM) je rozšířený PGSM. Pásma, které PGSM využívá, jsou na krajích rozšířena o 10MHz, tím se kapacita zvýšila o 50 duplexních kanálů. Systém je dnes běžně využíván.

GSM 1800 pracuje v kmitočtovém pásmu 1710 – 1880MHz. Pro uplink je použito 1710 – 1785MHz a 1805 – 1880MHz pro downlink. Tyto pásma jsou rozdělena na 374 radiových kanálů a každý má šířku pásma 200kHz. Opět má každé pásmo 8 TS, takže celkový počet účastnických kanálů je 2992.

GSM 1900 využívá kmitočtové pásma v rozsahu 1850MHz – 1990MHz. Pro uplink 1850 – 1910MHz a 1930 – 1990 pro downlink. Pásma jsou rozdělena na 299 radiových kanálů s šířkou 200kHz. Celkový počet účastnických kanálů je 2392, protože je počet TS opět 8. Dnešní telefony běžně zvládají všechny tři pásma, je to tzv. triband.



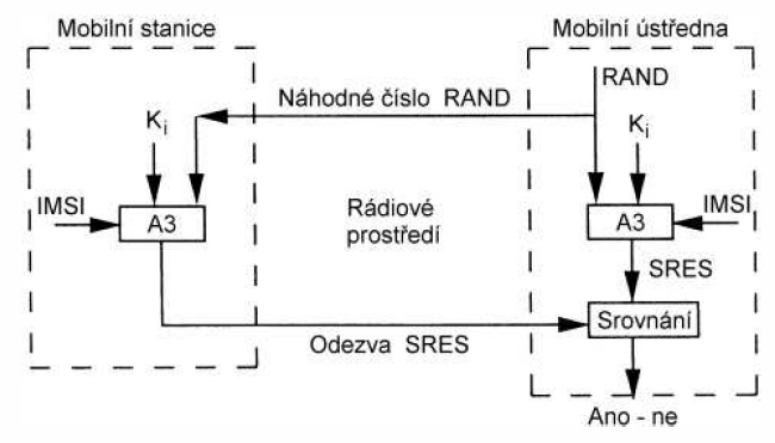
Obr. 2.1: Struktura GSM sítě (převzato z [4]).

2.1.2 Bezpečnost

Každý uživatel mobilního telefonu má přidělen jedinečný identifikátor IMSI (International Mobile Subscruber Identity), který se skládá z trojmístného kódu země MCC (Mobile Country Code), dvoumístného kódu mobilní sítě MNC (Mobile Network Code) a desetimístného identifikačního čísla uživatele mobilního telefonu. IMSI je uloženo do SIM mobilního telefonu. Informace o zákazníkovi včetně IMSI je uložena v síti mobilního operátora, kterého uživatel využívá primárně, v registru HLR (Home Location Register). Při každém přístupu do GSM sítě se musí uživatel autentizovat. Před navázáním jakéhokoliv připojení musí zařízení provést registraci, během ní je SGSN (Serving GPRS Support Node) informováno o požadavku přístupu do sítě. Na základě požadavku o připojení je zařízení do sítě připojeno.

Autentizace je založena na principu *výzva – odpověď*. Autentizaci provádí SGSN, který náhodně vygeneruje 128bitové číslo. U uživatele se autentizace provádí na SIM kartě. Na této kartě běží algoritmy specifické pro provozovatele sítě, které pro vstupní algoritmus použijí náhodné číslo a privátní klíč uložený na SIM. Vytvoří 32bitovou odpověď a 64bitový klíč, který je použit pro šifrování provozu. Privátní klíč se nikdy nepřenáší sítí.

V GSM síti je zachována anonymita uživatelů, díky použití TMSI (Temporary Mobile Subscriber Identity) dočasné identitě. Ta nahrazuje IMSI, které se při provozu posílá jen jednou, při prvním připojení do sítě.



Obr. 2.2: Způsob autentizace v GSM síti (převzato z [3]).

2.1.3 Programování

Pro využití GSM by byla vhodná aplikace, jako je například interní záznamník hovorů, nebo aplikace, která by odesílala sms zprávy v případě nedostupnosti uživatele, například při konferenci, kdy nemůže účastník hovor přijmout

2.2 GPRS

2.2.1 Obecné informace

GPRS (General Packet Radio Service), je to mobilní datová služba pracující v GSM síti. Patří do 2,5 generace, neboli 2,5G. GPRS je paketově přepínaná. Rychlost přenosu se určuje v závislosti na použité třídě, na které jsou mobilní zařízení rozdělena. Třída určuje kolik TS (Time Slot) umí zařízení využít. Nejběžnější využívanou třídou je třída 10, která maximálně využije 5 TS najednou a to v konfiguraci 4 + 1 nebo 3 + 2 (4 TS pro downlink + 1 TS pro uplink nebo 3 TS pro downlink a 2 TS pro uplink). GPRS je kódováno čtyřmi různými schématy CS-1 až CS-4 a aktuální schéma se vybírá podle aktuálního odstupu signál / rušení. Nejvyšší rychlost 80kb/s GPRS dosáhne při využití schématu CS-4 a konfigurace 4 + 1. Pokud zařízení využívá třídu 32 a zároveň ji podporuje i provozovatel sítě, dokáže zařízení využít 6 TS. Rychlost se pak zvýší na 100kb/s. GSM/GPRS využívá modulaci GMSK, která umožňuje přenést jeden informační bit na jeden symbol na radiové vrstvě.

2.2.2 Bezpečnost

Jelikož GPRS využívá k přenosu systém GSM, odpovídají tomu i jeho bezpečnostní prvky.

2.3 EDGE

2.3.1 Obecné informace

EDGE (Enhanced Data rates for GSM Evolution) je další technologií GSM pro přenos dat. Řadí se do 2,75 generace, neboli 2,75G [1]. Oproti GPRS nabízí tato technologie několik vylepšení. To spočívá ve zvýšení efektivity přenosu. Toho se dosahuje použitím modulace 8-PSK (osmistavová fázová modulace), která umožňuje přenést tři informační bity pomocí jednoho symbolu na radiové vrstvě. Nejvyšší rychlost přenášena technologií EDGE je maximálně 236,8kb/s při konfiguraci telefonu 4 + 1 (4 TS pro downlink + 1 TS pro uplink) a kódovaného schématu MCS-9, avšak je potřeba zařízení podporující tuto technologii

2.3.2 Programování

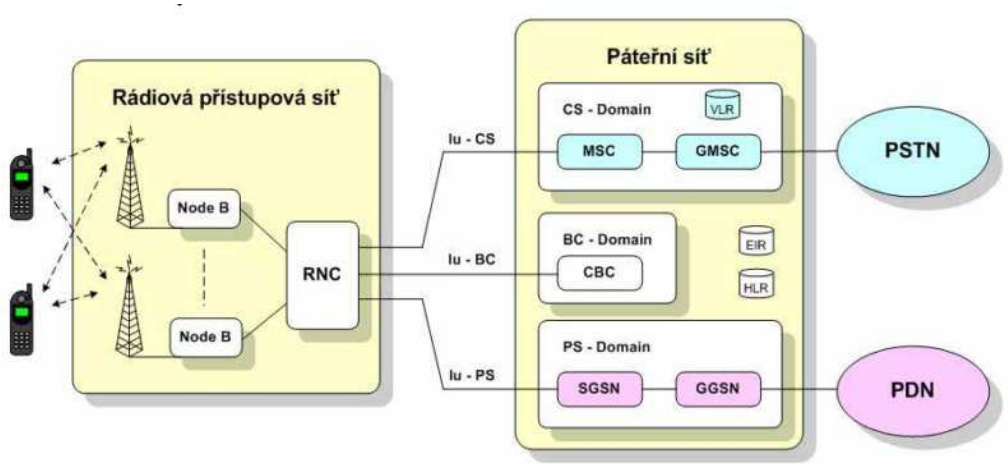
Pro GPRS a EDGE by byla nejvhodnější aplikace, která využívá přenos dat, tou by například mohl být messenger komunikující prostřednictvím sítě internet, ale také by se dalo využít zasílání stavu telefonu, které by se využívalo ve firmě ke kontrole zaměstnanců.

2.4 UMTS, W-CDMA

2.4.1 Obecné informace

W-CDMA (Wideband Code Division Multiple Access) je technologií patřící mezi systémy 3G a je součástí standardů ITU-2000. Je to evropsko-japonský standard sítě mobilních telefonů. V mobilních telefonech je využita terestrická služba, té se říká UTRA (UMTS Terrestrial Radio Access). Standard W-CDMA se také často označuje jako UMTS. Zatímco W-CDMA je technický název naznačující, že jde o širokopásmové CDMA, tedy WideBand CDMA, označení UMTS je název ekonomicko – politický.

UMTS (Universal Mobile Telecommunication System) je technologie, která se řadí do systému třetí generace, neboli 3G. Tato technologie byla vyvíjená jako nástupce GSM. Pro komunikaci využívá W-CDMA (Wideband Code Division Multiple Access), je evropským standardem pro sítě třetí generace. Pro UMTS jsou vyhrazena kmitočtová pásma v okolí 2GHz.



Obr. 2.3: Základní architektura sítě UMTS (převzato z [3]).

2.4.2 Bezpečnost

Zabezpečovací úroveň UMTS je vyšší než u výše uvedených technologií, díky šířce pásma, které UMTS využívá je šifrování využito bez dopadu na rychlost přenosu a snižování kvality služeb.

Bezpečnost má dvě úrovně: bezpečnost 3GPP, která zajišťuje přístup k UMTS a bezpečnou komunikaci mezi prvky GPP, které se týkají vzdušného rozhraní a přístupové sítě UTRAN a bezpečnost na aplikační vrstvě, která chrání komunikaci mezi koncovými body.

Bezpečnost, kterou využívá UMTS, byla použita i GSM, avšak některé prvky byly vylepšené a některé nové. Vylepšena byla autentizace, protože ta která byla použita u GSM využívala jednostrannou komunikaci na straně uživatele před přístupem do sítě pomocí SIM. Normy 3GPP se zaměřily na slabší místa GSM a zesílily jejich řešení. Šifrování bylo zesíleno, délka klíčů se tak prodloužila z 64bitů na 128bitů, zvýšila se kvalita kontroly integrity dat, bezpečnost mezi sítěmi, oproti GSM u kterého je za bezpečnost zodpovědná základnová stanice jsou u UMTS zodpovědné ústředny (přepínače). Dále mechanismus identity terminálu je přímo integrován do protokolu, oproti GSM, které jej má jen jako doplněk.

Autentizace mezi mobilními přístroji a sítí UMTS je založena na USIM (Universal Subscriber Identity Module), je to modul obdobný jako SIM u GSM. USIM má kapacitu dat 64kB a kromě bezpečnosti slouží pro personalizaci mobilního terminálu. Pro zajištění integrity a utajení musí projít fází AKA (Authentication and Key Agreement), v té se uživatelský terminál a síť dohodnou na souboru klíčů. AKA je systém založený na výzvě a odpovědi, využívá symetrické šifrování a dovoluje autentizaci uživatele i sítě. 3G síť je tak chráněna proti útokům ze strany falešné stanice, díky identifikaci sítě vůči uživateli.

Bezpečnostními slabinami 3G sítí je, že jsou postaveny na IP, proto se na ně

vztahují všechny bezpečnostní problémy IP komunikace, vhodné je proto používat IPSec VPN tunely mezi základnovými stanicemi a RNC.

2.4.3 Programování

Jelikož technologie UMTS dokáže přenést velký objem dat za krátký časový úsek, byla by vhodná aplikace pro streamování videa přes fotoaparát moderního telefonu.

2.5 Shrnutí

Hlavní rozdíly mezi GSM a UMTS jsou ve využití rozdílného kmitočtového pásma a struktuře jejich sítí. UMTS využívá důkladnější bezpečnost přenášených dat a tak pro využití je daleko příznivější. Přenos dat je u této technologie daleko rychlejší, avšak GSM pro běžné hovory a nenáročné přenosy dat vystačuje a není tak technicky náročné jako UMTS.

3 MOBILNÍ TELEFON A SIM KARTA

Tato kapitola popisuje, jak využívá telefon pro práci s různými systémy SIM kartu.

3.1 SIM karta

3.1.1 Obecné informace

SIM (Subscriber Identity module) je čipová karta o velikosti 15 x 25mm a je používaná ve všech dnešních GSM telefonech. Karta má velikost paměti od 16 do 64kB, je důležitá k autentizaci uživatele do sítě, proto sebou nese informace IMSI, to je číslo, které jednoznačně identifikuje účastníka na celém světě.

SIM karta umožňuje uživatelům měnit telefony pouhým vyjmutím této karty a vložením do jiného mobilního telefonu, přitom telefonní číslo zůstane zachováno.

Číslo IMSI je jedinečné sériové číslo na mezinárodní úrovni, které zabezpečuje bezpečnostní autentizaci a šifrování informací. První tři číslice představují MCC (Mobile Country Code), další dvě číslice představují MNC (Mobile Network Code). Dalších deset čísel představuje identifikaci mobilní stanice.

SIM karta je čipová karta, ale má také ICC-ID číslo na základě mezinárodní normy ISO/IEC 7812. Maximální délka viditelného čísla karty je 20 znaků, číslo se skládá z následujících pododdílů.

- Issuer identification number (max. 7 čísel)
- Individual account identification

Používání SIM karet je povinné v zařízeních GSM. Ekvivalent pro sítě UMTS se nazývá UICC (Universal Integrated Circuit Card), která provozuje aplikaci USIM. U CDMA je populární R-UIM (Removable User Identity Module). Mnoho CDMA zařízení však nepoužívá žádné vyjímatelné karty a služba je tak vázána přímo na zařízení.

K_i je 128 bitová hodnota, která je použita v autentizaci SIM do mobilní sítě. Každá SIM má unikátní K_i a ten je zložen do databáze domovské sítě.

Do této karty se přistupuje pomocí dvou kódů, tím je PIN kód, které lze libovolně měnit a kód PUK, který slouží pro odblokování karty po zapomenutí PIN kódu, ten však měnit nelze a je nutné si jej uschovat.

3.1.2 Bezpečnost

Postup ověřování je následující:

Když se mobilní zařízení nastartuje, získá ze SIM karty číslo IMSI a předá ho mobilnímu operátorovi, kterého žádá o autentizaci.

Provozovatel sítě hledá příchozí IMSI v databázi a číslo K_i, na jejich základě vygeneruje SRES_1.

Provozovatel sítě vygeneruje náhodné číslo (RAND) a podepisuje K_i spojené s IMSI.

Provozovatel sítě odešle RAND na mobilní zařízení, které ho dále předává na SIM kartu. SIM karta s K_i generuje SRES_2, které se pošle provozovateli sítě.

Provozovatel sítě poté porovná vygenerovaný SRES_1 a SRES_2 a pošle odpověď do mobilního zařízení. Pokud tyto čísla odpovídají je přístup do sítě umožněn. K_i se používá pro šifrování veškeré další komunikace.

3.2 SIM Toolkit

SIM Toolkit (běžně označováno jako STK) je standardní systém GSM, umožňující využít malé programy na SIM kartě. Skládá se ze sady příkazů, které jsou na kartě naprogramovány a definují, jak by měla karta komunikovat s okolním světem. Provádí příkazy nezávisle na telefonu a připojení k síti, avšak telefon musí tuto funkci podporovat, dnešní telefony tuto službu zvládají. SIM Toolkit umožňuje SIM kartě interaktivní výměnu mezi síťovou aplikací a konečným uživatelem a přístup nebo kontrolu přístupu k síti. Karta také dává příkazy telefonu, například zobrazení menu.

STK využívá mnoho mobilních operátorů po celém světě, pro různé druhy aplikací, většinou si operátor do SIM karty zavede své interní aplikace. Nejpoužívanější aplikací je mobilní bankovnictví. STK je vhodné pro použití na SIM kartě hlavně z toho důvodu, že se z karty přímo napájí a aplikace má nízkou paměťovou náročnost a jednoduché uživatelské rozhraní.

3.2.1 GSM Banking

GSM Banking, neboli mobilní bankovnictví umožňuje spravovat bankovní účet přímo v mobilním telefonu, stačí jen pokrytí GSM signálem, to však záleží na bance. Některé banky nabízí pouze informace o zůstatku na účtu, ale v dnešní době, je u většiny bank možné přes mobilní telefon plně spravovat bankovní účet.

Tato služba se dá využívat různými způsoby: přes SMS, aplikaci v Javě, pomocí wapu, nebo mobilního prohlížeče. V praxi je však nejvíce využívaná a oblíbená technologie SMS, zabezpečená pomocí SIM Toolkit. Samotný přenos SMS zpráv je šifrovaný a pro její přenos je potřeba speciální SIM karty, označenou jako bankovní SIM, nebo SIM s bankovní aplikací. Tato SIM karta má speciální bakovní PIN a PUK

a když má být určitá bankovní služba využívaná, je potřeba sdělit informace o kartě bance, ta tak může službu nakonfigurovat.

Mezi novější formy mobilního bankovnictví patří Javové aplikace. Jsou zmenšenou podobou internetového bankovnictví a lze je nainstalovat pouze do vybraných typů mobilních telefonů. Nabídnou hezčí grafiku a orientaci při procházení účtem, je však nutné počítat cenou za datové přenosy, které javová aplikace vyžaduje.

3.2.2 Programování

Pro SIM Toolkit by byla vhodná aplikace, zabírající co nejméně místa na paměti karty, proto by byla nejvhodnější aplikace, pracující ve formě jednoduchých příkazů, například na vyvolání určitého požadavku u operátora.

3.3 SWP

SWP (Single Wire Protocol) je specifikace pro jedno-vodičové připojení mezi SIM kartou a NFC. V praxi by tato technologie měla být využívaná k placení telefonem, neboli by telefon měl fungovat jako čipová karta s bezdotykovým přístupem, např. k placení jízdenek MHD v menších městech.

4 SYSTÉMY MOBILNÍCH TELEFONŮ

V této kapitole se nachází popis tří nejvyužívanějších (figuruje minimálně na dvou značkách mobilních telefonů) OS pro mobilní telefony.

4.1 Windows Mobile (Phone)

Tento OS přišel na trh v roce 2000, pod názvem Pocket PC 2000 a byl založen na Windows CE 3.0, později se systém přejmenoval na Windows Mobile. K dnešnímu dnu prošel OS spoustou obměn a na trh bylo vpuštěno asi 9 verzí i s nejnovější Windows Phone 7. V této kapitole se budu věnovat verzi WM 6, WM 6.5 a WP 7.

Verze **Windows Mobile 6.0** byla vydána v únoru 2007 a byla dodávána ve třech různých verzích. Windows Mobile 6 Standard (pro smartphony, telefony bez dotykového displeje), Windows Mobile 6 Professional (pro Pocket PC s funkcí mobilního telefonu) a Windows Mobile 6 Classic (pro Pocket PC funkce mobilního telefonu).

Windows Mobile 6 je poháněn systémem Windows CE 5.0 (verze 5,2) a je silně vázán na produkty Windows Live a Exchange 2007. Esteticky byl Windows Mobile 6 pojat jako tehdy nově vydané Windows Vista. Oproti předchozím verzím, nabídla WM 6 lepší stabilitu, podporu pro display o rozlišení 320×320 a 800×480 (WVGA), Operační systém Live Update, Microsoft Bluetooth Stack, AJAX, JavaScript, XMLDOM, .Net Compact Framework v2 SP2 před instalován v ROM, Microsoft SQL Server 2005 Compact Edition předinstalovám v ROM, Office Mobile s podporou formátů pptx, docx, xlsx.

Windows Mobile 6.5, byla vydána v květnu 2009 a do prvního mobilního telefonu byla aplikována v říjnu 2009. Jedná se o vylepšenou verzi 6.1, která byla přechodem mezi verzí 6 a 6.5, avšak měla jen drobné vylepšení. WM 6.5 obsahuje zdokonalené GUI, internetový prohlížeč Internet Explorer Mobile 6 s vylepšeným rozhraním. Zdokonaleno bylo také ovládání dotykem (uživatelsky přístupnější ovládání prsty), přidána podpora A-GPS, což je podpora datových komunikací k GPS. V dalším upgradu bylo opět zdokonaleno ovládání dotykem, přidáním multitouch.

Windows Phone 7 byl představen v únoru 2010, jedná se o revoluci mezi operačními systémy pro mobilní telefony od Microsoftu. Tuto verzi výhradně využívají zařízení s kapacitními displeji ovládanými prsty, dotykový display rozezná šest druhů gest. OS je propojen se sociálními sítěmi a webovými službami, navíc podporuje i xBox Live. GUI bylo oproti předchozím produktům Microsoftu pro mobilní telefony od základů změněno, nyní v něm není použito tlačítka „Start“ nebo křížků v pravých horních rozích oken, ukončující aplikace. Nevýhodou nového OS je, že

nepodporuje multitasking jako takový, ale fungují push notifikace nebo aktivní aplikační rozhraní skrze widgety na úvodní obrazovce, ale samotná aplikace plnohodnotně na pozadí nepoběží. Další novinkou je instalace aplikací, ta je oficiálně možná jen pomocí speciálního systému od Microsoftu, tzv. Windows Marketplace for Mobile.

Pro vývojáře je nejdůležitější informací, že Microsoft vydal plnohodnotné vývojové prostředí, které je dostupné zdarma, obsahuje čtyři nástroje Visual Studio 2010 Express for Windows Phone, Windows Phone Emulator, Silverlight for Windows Phone a XNA 4.0 Game Studio, dostupné na webu Microsoftu, avšak instalaci programu je zatím možné provést pouze přes výše uvedený systém. OS nebude podporovat zpětnou kompatibilitu s předchozími verzemi.

4.2 Symbian OS

Prvopočátky tohoto OS se datují již od 80. let, kdy firma Psion začala vyvíjet grafický OS EPOC, ten byl určen pro přenosná zařízení, jako jsou PDA. Tento OS prošel řadou obměn až do řady EPOC Release 5, kdy bylo poprvé zmíněno označení Symbian OS, avšak tehdy ještě tento název nebyl příliš používán. V červnu roku 2001 byla uvolněna první oficiální verze pod názvem Symbian OS verze 6.0., hlavní novinkou byla podpora Bluetooth a otevřenost, tzn. že umožňoval instalaci aplikací. Jako první byl využíván v mobilním komunikátoru Nokia 9210 Series 80, prvním smartphonem využívající **Symbian OS ve verzi 6.1** byl mobilní telefon Nokia 7650 Series 60, ten byl unikátní tím, že jako první měl fotoaparát.

Další verze uvedena v roce 2003 byl **Symbian OS 7.0**, používám byl v zařízeních UIQ, Series 80, 90 a 60. Byla přidána podpora EDGE, IPv6. Podpora Java byla sjednocena z pJava a JavaPhone ve standard Java ME, výhodou byla také zpětná kompatibilita s verzí 6.x.

Verze **Symbian OS 8.0** byla ohlášena v roce 2004, výhodou byl výběr mezi dvěma jádry (EKA1 a EKA2). Jádra byly uživatelsky totožné, ale jejich architektura byla odlišná. EKA2 využíval oproti EKA1 real-time jádro. Zahrnuty byly také API pro podporu CDMA, 3G, duplexní data streaming, DVB-H, OpenGL ES s vektorovou grafikou a přímý přístup k obrazovce.

Symbian OS 9.1, který byl uvolněn počátkem roku 2005 obsahovala nové funkce z hlediska bezpečnosti, k usnadnění zabezpečení přispěl modul mandatory code signing. Dále přibyl ARM EABI binární model a podpora Bluetooth 2.0. Pro přístup k některým API je nutné využít digitální podpis. Základní možností je user-grantable a vývojáři si jej mohou samostatně podepsat, pokročilé funkce již vyžadují certifikaci s podpisem přes Symbian Signed program a je nutné jeho schválení výrobcem telefonu. Například program pro psaní je user-grantable, zatímco program využívající multimediální ovladače vyžaduje schválení výrobcem telefonu. TC TrustCenter ACS Publisher ID

certificate potřebuje vývojář pro podepsání aplikace.

Verze 9.3 představena v červenci 2006 podporuje lepší správu paměti a nativní podporu WiFi 802.11, HSDPA. V březnu 2007 byla představena verze **9.4**, která by měla být o 75% rychlejší, podporuje SQL, známá je také pod označením S60 5th Edition. OS 9.5 oznámena v březnu 2007 obsahuje podporu digitální televize v DVB-H a ISDB-T formátech.

V únoru 2010 se Symbian stal Open Source projektem, to by mělo přispět k rychlejšímu vývoji a rozšíření.

Na rok 2011 je ohlášen Symbian[4], který stejně jako Windows Phone 7 series pravděpodobně nebude kompatibilní s předchozími verzemi a bude přizpůsoben většímu a variabilnímu rozlišení displeje.

Z hlediska bezpečnosti je na tom Symbian OS velice dobře, průměrný uživatel by neměl mít strach z napadení telefonu virem, většinou, když u těchto operačních systému vyskytl nějaký útok, byl způsoben chybou uživatele, který i přes varování o nedůvěryhodnosti produktu aplikaci nainstalovat a tím si problémy způsobil. O bezpečnosti jsem se také zmiňoval v odstavci o verzi Symbian OS 9.1, podrobněji bych ještě zmínil, že uživatel si nemůže podepsat aplikaci sám k přístupu pro Bluetooth, IrDA, GSM CellID, hlasové hovory, GPS a několik dalších.

Z programátorského hlediska je základem OS rodný jazyk Symbian C++, uvolněno bylo více platforem založených na OS Symbian, pro vybraný systém si musí vývojář zvolit vhodné SDK, z nejdůležitějších jsou to UIQ a S60. V roce 2010 se výrobce snažil Symbian sjednotit, aby mezi SDK byly menší rozdíly. Symbian C++ bohužel vyžaduje použití speciálních technik a to může i z poměrně jednoduchého problému udělat složitost. Od roku 2006 byl Nokií vyvinut Carbide.c++, které je nabízené ve čtyřech verzích: Express, Developer, Professional a OEM, podle rostoucí úrovně schopností programátora. Pro vyladění je používán program Microsoft Visual Studio. Tento programovací jazyk je ale jen jednou z možností. Aplikace pro Symbian OS je možné programovat pomocí jazyka Python, Java ME, Flash Lite, Ruby, .Net, Web Runtime. K dispozici také byl Borland IDE pro Symbian OS.

Java ME aplikace pro Symbian OS, se vyvíjí použitím standardních technik a nástrojů, jako je Sun Java Wireless Toolkit. Jsou zabaleny v JAR souborech. Obě CLDC a CDC aplikace mohou být vytvořeny v programu NetBeans.

4.3 Android

Tento operační systém pro mobilní zařízení zahrnuje middleware a klíčové aplikace a používá upravenou verzi linuxového jádra. To bylo původně vytvořeno firmou Android Inc, kterou později koupil Google. Po vývoji systému celou platformu i se zdrojovými kódy předal sdružení firem Open Handset Alliance, které je také členem.

Platforma Android byla ohlášena 5. listopadu 2007 zároveň se založením Open Handset Alliance, která sdružuje 65 hardware, software a telekomunikačních společností, aby prosazovali otevřené standardy pro mobilní zařízení. Google Android kódu uvolnil nejvíce pod Apache Licence, free software a open source licence.

V následujícím textu jsou postupně popsány verze operačního systému a zmíněny nejdůležitější vylepšení a změny.

Verze **1.5 (Cupcake)** na Linux Kernel 2.6.27 byla vydaná 30. Dubna 2009, obsahovala možnost nahrávat a sledovat videa prostřednictvím režimu videokamera. Zahrnuta byla podpora Bluetooth A2DP a AVRCP, možnost automaticky se připojit k headsetu Bluetooth v určité vzdálenosti.

1.6 (Donut) na Linux Kernel 2.6.29 byla ohlášena 15. Září 2009, přidána podpora integrovaného fotoaparátu a videokamery, podpora CDMA/EVDO, 802.1x, VPN, gesta a WVGA rozlišení obrazovky.

2.0/2.1 (Eclair) na Linux Kernel 2.6.29 byla uvolněna 26. Října 2009. V ní byla optimalizovaná rychlost hardwaru, podpora více velikostí a rozlišení displeje, podpora přisvětlovací diody, digitální zoom fotoaparátu, podpora Bluetooth 2.1.

2.2 (Froyo) na Linux Kernel 2.6.32 byla představena 20. Května 2010 na konferenci Google I/O. Hlavními vylepšeními je možnost instalovat aplikace na paměťovou kartu, pomocí kompilátoru JIT (Jist-in-time) se podařilo zvýšit rychlost systému, vylepšena správa paměti RAM, vytváření **WiFi hotspotu** z mobilního zařízení**,** nebo sdílení internetové připojení přes USB kabel, podpora Open GL ES 2.0, přidána další vrstva vývojářského API.

Android SDK umožňuje vývojářům psát aplikace v jazyce Java s využitím knihoven vyvinutých společností Google, ten zahrnuje vývojové prostředí, emulátor, debugger, sadu knihoven, dokumentaci, ukázkové programy, tutoriály, odpovědi na často kladné otázky a další. Vývojové prostředí běží na desktopových OS Windows XP/Vista/7, Mac OS X (10.4.8 a novější), Linux (Ubuntu 6.06) kompatibilní na platformě x86. Mezi potřebné nástroje patří Java Development Kit, Apache Ant a Python. Eclipse 3.2 nebo novější je oficiálně podporované vývojové prostředí. Díky Android Development Tools Plugin získává toto prostředí všechny potřebné doplňky pro vývoj aplikací v OS Android. Samozřejmostí pro vývoj, kompilování a ladění aplikací je možnost použití nástroje příkazového řádku. Jednou z podstatných nevýhod tohoto operačního systému je nepodporování JavaME.

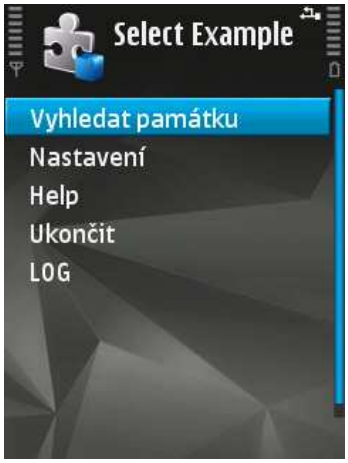
5 APLIKACE

Tato kapitola bakalářské práce je věnována praktické části, která spočívala v návrhu a realizaci aplikace komunikující přes Bluetooth mobilního telefonu a touto technologií zjišťuje polohu přístroje v síti.

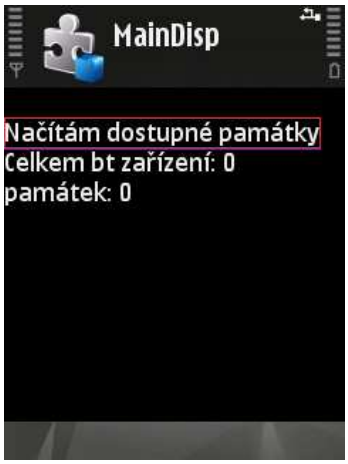
5.1 Popis a princip

Díky první části práce bylo nastudováno, která technologie bude použita pro komunikaci mobilního telefonu s okolními zařízeními. Po veškerém uvážení byla vybrána technologii Bluetooth. V potaz navíc připadala technologie GPS, která by však nebyla přístupná v uzavřených prostorech a technologie NFC, která momentálně není podporována téměř žádným mobilním telefonem na českém trhu. Aplikace tedy komunikuje přes technologii Bluetooh, avšak po změně API Bluetooth za API NFC (tento název pravděpodobně neexistuje, je použit pro lepší představivost) a následném přizpůsobení aplikace na danou technologii, by měla aplikace přes NFC komunikovat.

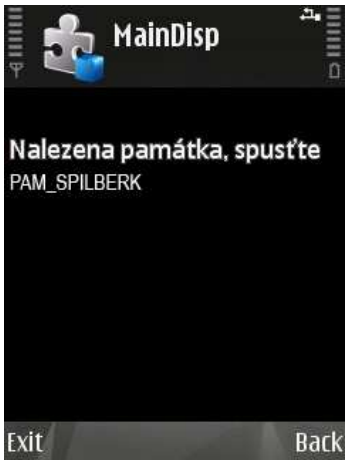
Jak funguje aplikace a co je jejím principem z **uživatelského** hlediska? V principu má aplikace informativní charakter pro návštěvníky památek v Brně. Návštěvník přijde k památce, která je vybavena Bluetooth vysílačem, zapne již nainstalovanou aplikaci viz. obr. 5.1 a po spuštění položky „Vyhledat památku“ viz. obr. 5.2 se mu vyhledá zařízení. Po kliknutí na položku „Nalezena památka, spusťte“ viz. obr. 5.3 se spustí zvukový soubor, který informace o památce sdělí uživateli aplikace, dále se na displeji zařízení zobrazí obrázek, s mapou centra Brna a zaznačenou polohou viz. obr 5.4, kde se zájemce o informaci nachází. Po přehrání zvukového souboru se uživatel může vrátit zpět do základního menu a poté opět vyhledávat památky a přehrávat další informace. V základním menu aplikace se dále nachází položka „Nastavení“ viz. obr. 5.5, ve které je možné přepnout jazyk na angličtinu, vybrat si paměťový prostor, ze kterého se budou hudební soubory načítat, barvu pozadí, barvu písma a poslední položkou je možnost mít zapnuté testování, jestli je Bluetooth aktivované. Pokud bude tato položka aktivována, bude uživatel, pokud má Bluetooth vypnuté, o tomto stavu informován. Třetí a zároveň poslední položkou v základním menu je „Help“ ve které se nachází základní informace o aplikaci.



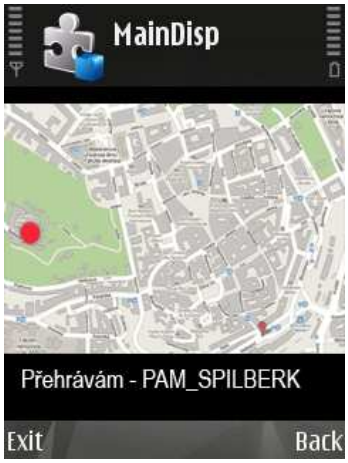
Obr. 5.1: Hlavní menu programu.



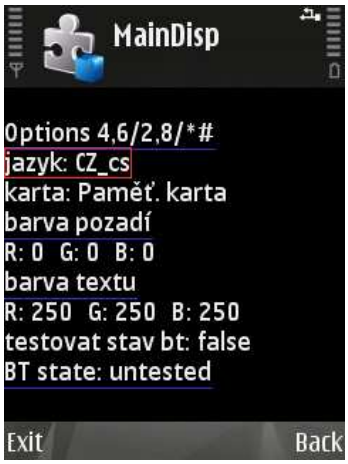
Obr. 5.2: Položka „Vyhledat památku“.



Obr. 5.3: Zobrazení nalezené památky.



Obr. 5.4: Přehrávání zvukového záznamu.



Obr. 5.5: Položka „Nastavení“.

5.2 Minimální požadavky

Mobilní zařízení, které bude tuto aplikaci využívat, má minimální požadavky, těmi jsou podpora:

- Technologie Bluetooth
- Platforma JavaME
- Zařízení, které má alespoň vnitřní flash paměť, s dostatečným místem pro uložení souborů aplikace, cca 50MB
- Doporučuji zařízení s RAM pamětí s minimální velikostí 5MB

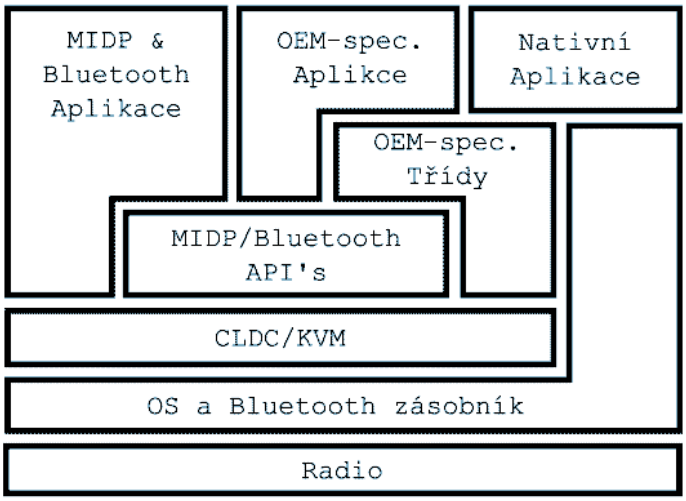
5.3 Programování

Jak funguje aplikace z **programátorského** hlediska? Tato aplikace je naprogramována v jazyce Java na platformě Java ME, připojení aplikace k Bluetooth zařízení pracuje přes JSR-82 a o přehrávání hudebních záznamů se stará implementovaný hudební přehrávač JSR-135, podrobnosti o těchto specifikacích jsou uvedeny níže. Principielně: Po stisknutí tlačítka „Vyhledat památku“ se aktivuje vyhledávání Bluetooth zařízení v dosahu mobilního přístroje, pokud bude zařízení pojmenováno tak jak je definováno v apList.txt, bude název památky zobrazen na displeji telefonu, zařízení je pojmenováno vždy prvními písmeny PAM a poté za podtržítkem následuje název památky, např. PAM_SPILBERK. To je první druh filtrace, který je do aplikace implementován, další je filtrace podle MAC adresy přístroje umístěného na místě památky, proto nemůže dojít k tomu, aby někdo narušil funkčnost tohoto systému. Samozřejmě je možné, aby někdo své zařízení pojmenoval stejně a MAC adresu si změnil za adresu vysílacího zařízení, to však není legální. Poté co zařízení vyhledá památku, nabídne se možnost přehrání informací o památce pod odkazem „Nalezena památka, spusťte“ to aktivuje hudební přehrávač a vyhledá hudební soubor, který je umístěn v paměti telefonu, nebo na paměťové kartě. Možností jak tento problém řešit bylo více, jako například stažení hudebního souboru z přístupového bodu, to by však mohlo způsobovat problémy se zatížeností při vyšším počtu připojených účastníků a při rozsáhlé informaci by přenos souboru trval delší dobu. Protože bylo zadáno využívat moderní mobilní telefony a smartphone přístroje, byla použita metoda umístění hudebních souborů přímo na zařízení. Dále se na displeji zobrazí obrázek, který je rovněž umístěn na jedné z pamětí v přístroji.

Bluetooth (JSR-82)

Než byla specifikace JSR-82 vytvořena neexistovala žádná otevřená standardizovaná cesta vývoje aplikací využívající Bluetooth, ta skrývá složitosti zásobníku za množinu několika aplikačních rozhraní jazyka Java. Tato specifikace popisuje dvě základní možnosti přístupu k Bluetooth., těmi jsou Bluetooth API a Object Exchange API. Rozhraní vytvořené podle uvedené specifikace zprostředkuje následující možnosti:

- Registrování služeb
- Hledání okolních zařízení a detekci služeb nabízených těmito zařízeními
- Vytvoření RFCOMM, L2CAP a OBEX spojení mezi zařízeními
- Použití vytvořených spojení k zasílání a přijímání dat (bez podpory přenosu řeči)
- Ovládat a kontrolovat komunikační spojení
- Upravovat zabezpečení těchto spojení



Obr. 5.6: Architektura J2ME CLDC/MIDP a Bluetooth.

Aplikační rozhraní JSR-82 dokáže pracovat s nativním Bluetooth zásobníkem a zároveň také s Bluetooth zásobníky Javy, standardizuje programovací rozhraní a jeho dva volitelné balíky mohou být použity s jakýmkoli J2ME profilem. Základní kroky Bluetooth – J2ME:

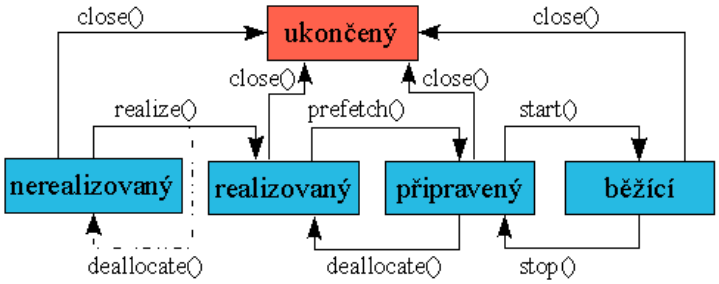
- Inicializace zásobníku – Bluetooth specifikace nechává implementaci tohoto kroku na výrobci zařízení, proto se také u jednotlivých zařízení může lišit
- Správce zařízení – Bluetooth API obsahuje třídy LocalDevice a RemoteDevice umožňující správu zařízení
- Hledání zařízení pro spojení – Na základě objektu třídy DiscoveryAgent je možné hledat zařízení pro spojení třemi možnými způsoby
- Hledání služeb na zařízení – Po nalezení zařízení je možno na tomto zařízení pomocí objektu DiscoverAgent hledat registrované služby
- Komunikace – Komunikující zařízení musí sdílet komunikační protokol (RFCOMM, L2CAP, OBEX). V případě použití jiného protokolu je nutné, aby aplikace tento protokol implementovala použitím obecného CLDC frameworku.

Mobile Media API (JSR-135)

Tato specifikace rozšiřuje J2ME o práci s multimédii. Například audiem a videem. V této práci byla použita třída `javax.microedition.media.Player`, pro přehrání zvukových dat. Během svého životního cyklu se může ocitnout v několika stavech:

- Nerealizovaný stav – V tomto stavu se `Player` nachází po svém vytvoření, protože nemá ještě dostatek informací o zvukových datech.

- Realizovaný stav – Zvuková zařízení se ještě nealokují, aby zbytečně nebyla blokována.
- Připravený stav – Přechod z připraveného do běžícího stavu by měl trvat minimum času, proto v připraveném stavu jsou už alokována zvuková zařízení a zásobníky naplněny zvukovými daty, je-li to potřeba.
- Běžící stav – V běžícím stavu `Player` přehrává zvuková data. V tomto stavu není možné nastavovat počet opakování zvuku metodou `setLoopCount()`.
- Ukončený stav – Do ukončeného stavu přejde `Player` z jakéhokoliv stavu voláním metody `close()`. V tomto stavu uvolní všechny zdroje a nedá se dále použít.



Obr. 5.7: Životní cyklus třídy player (převzato z [19]).

Obrázek ukazuje celý životní cyklus objektu typu `Player`. Pro lepší přehlednost z něj byly vypuštěny některé šipky. Je-li `Player` v nerealizovaném stavu a zavolá se metoda `prefetch()` nebo `start()`, automaticky je zavolána jako jejich součást metoda `realize()`. Je-li `Player` v realizovaném stavu a zavolá se na něm metoda `start()`, automaticky je zavolána jako její součást metoda `prefetch()`.

Paměťové karty

Tato aplikace podporuje následující druhy paměťových karet:

- SDCard
- CFCard
- MemoryStick

5.4 Shrnutí

Program je konstruován tak, že lze do apListu (je umísteň jako textový soubor v programu, ten je přiložen v práci na CD) přidat neomezený počet zařízení podporující tuto aplikaci, stačí vytvořit na daném zdrojovém zařízení určitý název, zjistit jeho MAC adresu a to pak zakomponovat do programu. Při testování programu byly použity mobilní telefony Evolve Zion, Nokia 5300 a Nokia N95 jako zdrojová zařízení, pro cílová zařízení byly odzkoušeny mobilní telefony Nokia N95, Nokia 5300 a Samsung U600. Jak potvrdila teorie o Symbian OS, který je použit na mobilním telefonu Nokia N95, neumožnil OS aplikaci přístup k paměťové kartě, ani paměti telefonu, proto na něm nebylo možné přehrání zvukového souboru uskutečnit. Vyhledání zařízení přes Bluetooth proběhlo bez problémů. Pro plnohodnotné zprovoznění aplikace by se musela nechat aplikace certifikovat výrobcem OS, což by znamenalo vynaložit značné finanční prostředky. Na dalších dvou zařízeních proběhlo odzkoušení aplikace bez problémů.

6 ZÁVĚR

Tato bakalářská práce byla zaměřena na prostudování technologií, které jsou používány v moderních mobilních telefonech a smartphonech. Cílem bylo popsat jejich principy, bezpečnost přenášených dat a využití v programování. Důvodem tohoto studia byl výběr nejvhodnější technologie, která byla využita v praktické části této práce.

Největší důraz při studiu a následném popisu technologií používaných v komunikaci mobilního telefonu s okolními sítěmi, byl kladen na Bluetooth, protože při zjišťování informací o telefonech byla tato technologie nejpoužívanější a i v počítačovém světě je z uvedených technologií nejčastěji používaná.

Při popisu technologií používaných v mobilních sítích je nejpodrobněji popsána GSM, taktéž ji dnes využívá každý mobilní telefon. Jelikož by k programu musela být využita i služba operátora, která je zpoplatněna, není využití technologie v programu z praktického hlediska nejvhodnější. Využití UMTS není vhodné ze stejného důvodu, navíc není pokrytí signálu UMTS v ČR tak plošně rozšířené jako GSM.

V kapitole „Mobilní telefon a SIM karta“ byl podrobně popsán princip SIM karty a k ní přidružená technologie a využívaná služba, avšak pro praktickou část bakalářské práce není tento způsob vhodný z důvodu malé paměti a téměř nemožného rozšíření z důvodu složitého, nebo téměř nemožného programování SIM karet operátorů.

Ve čtvrté kapitole byly popsány tři operační systémy pro mobilní zařízení, díky podrobnému nastudování jednotlivých systémů bylo zjištěno, že na Androidu není možné aplikaci, která byla v praktické části práce vytvořena, zprovoznit. Důvodem je, že nepodporuje JavaMe, ale jen modifikovanou Javu a aplikace by musela být programována ve vývojovém prostředí Android SDK. U Symbian OS bylo pro změnu zjištěno, že aby aplikace mohla být zprovozněna, respektive, aby mohla využívat čtení z paměťové karty, nebo telefonu, bylo by nutné aplikaci nechat certifikovat výrobcem, což je finančně náročné. Přístup na paměťové prostory není možný z důvodu bezpečnosti operačního systému. Jako jediný bezproblémový se jeví operační systém Windows Mobile (Phone), který takovým zabezpečením nedisponuje a zároveň umí využívat platformu JavaME, proto ho jako jediný z těchto tří považuji za multiplatformní.

Poslední kapitola byla věnovaná samotné aplikaci. Po vybírání technologie, přes kterou aplikace komunikuje, byla kvůli univerzálnosti zvolena jako nejlepší technologie Bluetooth, kterou podporuje téměř každé mobilní zařízení. Dalším krokem bylo vybrání programovacího jazyka. Kvůli multiplatformosti byl zvolen jazyk Java. Aplikace je programována na platformě JavaME a díky API, které podporuje tato platforma a mobilní zařízení, bylo programování jednoduché a aplikace kompatibilní s mnoha druhy mobilních zařízení. Po určení těchto základních požadavků vznikla

naprogramováním aplikace s pracovním názvem „Památkovník“. Zadáním práce bylo, aby program zjistil polohu telefonu z okolních sítí a podle ní vykonal požadovanou akci. Tou požadovanou akcí je vzniklá aplikace, která pracuje jako průvodce po památkách v centru Brna a zjištěním polohy se projevuje tak, že při přehrávání informace o památce se zobrazuje obrázek s mapou centra a vyznačeným bodem, kde se zařízení nachází. Celá aplikace je pojata demonstračně a není tedy nutné, aby pracovala pouze v centru Brna. Jednoduchými zásahy do programu se dá přizpůsobit jakékoliv lokalitě.

LITERATURA

[1] PUŽMANOVÁ, R., Bezpečnost bezdrátové komunikace, 2005

[2] HANUS, S. Rádiové a mobilní komunikace. Rádiové a mobilní komunikace II. Brno: FEKT VUT v Brně, 2005. s. (52 s.)

[3] NOVOTNÝ, Vít. Bezšňůrová koncová zařízení, koncová zařízení GSM. Účastnická koncová zařízení [online]. 2003 [cit. 2009-12-02], s. 60-71.

[4] SANDBOX [online]. 2009 [cit. 2009-12-06]. ENG. Dostupný z WWW: <www.sandbox.com>.

[5] WIKIMEDIA [online]. 2009 [cit. 2009-12-06]. ENG. Dostupný z WWW: <commons.wikimedia.org>

[6] SOCIETY OF ROBOT [online]. 2009 [cit. 2009-12-06]. ENG. Dostupný z WWW: www.societyofrobot.com

[7] DVOŘÁK, Jan. GPS. Referát [online]. 2006 [cit. 2009-12-05] Dostupný z WWW: <http://radio.feld.cvut.cz>

[8] NOVÁK, Adam. Nové Bluetooth 3.0 schváleno. Zvládá rychlost až 24 megabitů za sekundu. Mobil.idnes.cz [online]. 2009 [cit. 2009-10-28]. Dostupný z WWW: <http://mobil.idnes.cz/>.

[9] Bluetooth Core Specification v3.0 + HS. Bluetooth SIG [online]. 2009 [cit. 2009-10-22]. Dostupný z WWW: <http://www.bluetooth.com>.

[10] SIM Toolkit. Cellular [online]. 2006 [cit. 2009-10-27]. Dostupný z WWW: <http://www.cellular.co.za/sim_toolkit.htm>.

[11] GSM. GSM World [online]. 2009 [cit. 2009-12-01]. Dostupný z WWW: <http://www.gsmworld.com/>.

[12] ŘEZNÍČEK, Martin. Přenosové formáty (modulace, mnohonásobný přístup) mobilních systémů 2. a 2,5. generace. Semestrální práce [online]. 2007 [cit. 2009-12-03], s. 1-4. Dostupný z WWW: <http://radio.feld.cvut.cz/personal/mikulak/MK/MK07_semestralky/prenosove_formaty_2G_a_2_5G.pdf>.

[13] *Microsoft.com* [online]. 2010 [cit. 2010-05-30]. Microsoft. Dostupné z WWW: <http://www.microsoft.com/presspass/events/mix/VideoGallery.asp>.

[14] *Allaboutsymbian.com* [online]. 2010 [cit. 2010-04-02]. All about Symbian. Dostupné z WWW: <http://www.allaboutsymbian.com/>.

[15] *Developer.symbian.org/* [online]. 2010 [cit. 2010-04-02]. Symbian developer. Dostupné z WWW: <http://developer.symbian.org/>.

[16] *Android.com* [online]. 2010 [cit. 2010-05-30]. Android. Dostupné z WWW: <http://www.android.com/>.

[17] *Google Android cz* [online]. 2010 [cit. 2010-05-30]. Svět Androidu. Dostupné z WWW: <http://www.android-google.cz/>.

[18] ZUZAŇÁK, Ing. Jiří. *Osobní stránky Ing. Jiří Zuzaňák* [online]. 2010 [cit. 2010-02-11]. Prezentace JavaME. Dostupné z WWW:<www.fit.vutbr.cz/~izuzanak/www/tam/ slides. pdf>.

[19] BITTNEROVÁ, Lucie Rút. *Interval.cz* [online]. 2004 [cit. 2010-03-30]. J2ME v kostce - Jak na zvuk. Dostupné z WWW: <http://interval.cz/clanky/j2me-v-kostce-jak-na-zvuk-1/>.

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

EDR	Enhaced Data-Rate
NFC	Near Field Communication
PAL	Protocol Adaptation Layer
Wi-Fi	Wireless Fidelity
PIN	Personal Identification Numer
IrDA	Infrared Data Association
VFIR	Very Fast IrDA
USB	Universal Serial Bus
SMS	Short Message Service
GPS	Global Positioning Systém
CDMA	Code Division Multiple Access
C/A	Coarse Acquisition
GSM	Global Systém for Mobile Communication, Group Speciál Mobile
PGSM	Primary GSM
EGSM	Extended GSM
TS	Time Slot
IMSI	International Mobile Subscruber Identity
MCC	Mobile Country Code
MNC	Mobile Network Code
HLR	Home Location Register
SGSN	Serving GPRS Support Node
TMSI	Temporary Mobile Subscriber Identity
GPRS	General Packet Radio Service
GMSK	Gaussian Minimum-Shift Keying
EDGE	Enhanced Data rates for GSM Evolution
W-CDMA	Wideband Code Division Multiple Access
UTRA	UMTS Terrestrial Radio Access

UMTS	Universal Mobile Telecommunication Systém
USIM	Universal Subscriber Identity Module
AKA	Authentication and Key Agreement
IP	Internet Protocol
IPSec	IP Security
VPN	Virtual Private Network
RNC	Radio Network Controller
SIM	Subscriber Identity Module
ICC-ID	International Criminal Court – ID
ISO/IEC	International Organization for Standardization / IEC
UICC	Universal Integrated Circuit Card
R-UIM	Removable User Identity Module
PUK	PIN Unlock Key
STK	SIM Toolkit
SWP	Single Wire Protocol
OS	Operační systém