ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA ELEKTROTECHNICKÁ, Katedra řídící techniky

DIPLOMOVÁ PRÁCE

Návrh a realizace bezdrátového přenosu dat

2007 Jiří Chvojan

ČVUT FEL Praha

České vysoké učení technické v Praze - Fakulta elektrotechnická

Katedra řídicí techniky *Školní rok:* 2003/2004

ZADÁNÍ DIPLOMOVÉ PRÁCE

Student: Jiří Chvojan

Obor: Technická kybernetika

Název tématu: Bezdrátové řízení technologie

Zásady pro vypracování:

1. Porovnejte možné způsoby realizace bezdrátového přenosu dat.
2. Vyberte vhodný typ a navrhněte model pro ověření komunikace.
3. Na vybraném modelu demonstrujte jednoduchý řídicí program.

Seznam odborné literatury: Dodá vedoucí práce.

Vedoucí diplomové práce: doc. Ing. Jan Bílek, CSc.

Datum zadání diplomové práce: prosinec 2003

Termín odevzdání diplomové práce: květen 2005

doc. Ing. Michael Šebek, DrSc.
vedoucí katedry

L.S.

v zast.
prof. Ing. Vladimír Kučera, DrSc.
děkan

V Praze dne 25.03.2004

Prohlášení

Prohlašuji, že jsem svou diplomovou práci vypracoval samostatně a použil jsem pouze podklady (literaturu, projekty, SW atd.) uvedené v přiloženém seznamu.

V Praze dne 19. 1. 2007

podpis

Poděkování

Rád bych poděkoval vedoucímu diplomové práce Doc.Ing. Janu Bílkovi, CSc.

Abstrakt

Bezdrátové technologie jsou v dnešní době jedním z nejperspektivnějších odvětví informačních technologií. Tato práce se zabývá hlavními rysy a problematiku spojenou s návrhem bezdrátového spojení pomocí standardu 802.11. Jejím cílem je popsat principy a fungování sítí založených na tomto standardu a návrh realizace tohoto spojení pro účely řízení modelu v reálném čase. V první části jsou rozebrány teoretické základy ohledně fungování a provozu bezdrátových sítí a ve druhé části je praktický návrh řešení pomocí vývojové desky s procesorem PIC18F452.

Abstract

Presently, wireless technologies are the most perspecrive branche of information technologies. This work is devoted to a propsal of a wireless network based on 802.11 standard. Main principles and realization propsal for the model controling purposes are described. First a theoretical introduction to the wireless network is analyzed. Finaly a practical realization based on development board with PIC18F452 processor outlined.

Obsah

Úvod

Úkolem diplomové práce je návrh bezdrátového řízení modelu. Po důkladném průzkumu bezdrátových technologií jsem se rozhodl pro standard 802.11. Je pravda, že jsem měl vícero kandidátů, ale nakonec jsem dal přednost právě této technologii.

Revize 802.11b je v dnešní době asi nejrozšířenější bezdrátová specifikace standardu 802.11 která se používá pro přenos dat. V dnešní době se začínají prosazovat různé jiné alternativy s vyššími přenosovými rychlostmi pracujícími ve vyšších frekvenčních pásmech a používajícími odlišné protokoly. Pro naše účely ovšem bohatě postačí přenosová rychlost která se u této specifikace pohybuje v teoretické rovině okolo 10 Mbps. Pro řešení jsem vybral vývojovou desku osazenou mikrořadičem firmy Microchip s označením PIC18F452. Toto řešení se mi přišlo zajímavé pro jeho nízkou spotřebu což je jedním z hlavních důvodů mého výběru. Toto zařízení by mělo pracovat v mobilním zařízení a proto otázka spotřeby je jedním z hlavních kritérií. Dalším důvodem byla rošířenost standardu a tudíž i dostupnost hardwaru pro PC.

V závěru byla komunikace testována na modelu pračky, který jsem pro tyto účely vyrobil.

1 Diskuse použité technologie bezdrátového připojení

1.1 Infračervená technologie

Infračervené záření (také IR, z anglického infrared) je elektromagnetické záření s vlnovou délkou větší než viditelné světlo, ale menší než mikrovlnné záření. Název značí "pod červenou" (z latiny infra = "pod"). Infračervené záření zabírá ve spektru 3 dekády a má vlnovou délku mezi 760 nm a 1 mm, resp. energii fotonů mezi 0,0012 a 1,63 eV.

Infračervené záření se dále dělí na jednotlivá pásma. Toto dělení ovšem není jednoznačně dané. Jedno schéma je například toto:

- blízké (near) infračervené záření neboli NIR
- IR-A podle normy DIN, vlnová délka $0,76 - 1,4\mu m$, definováno podle vodní absorpce; často používané v telekomunikacích optických vláken
- IR krátké vlnové délky (short wave) neboli SWIR
- IR-B podle DIN, vlnová délka $1,4 - 3\mu m$, při $1450nm$ značně roste vodní absorpce
- IR střední vlnové délky (medium wave) neboli MWIR
- IR-C podle DIN, též prostřední (intermediate-IR neboli IIR), $3 - 8\mu m$
- IR dlouhé vlnové délky (long wave) neboli LWIR
- IR-C podle DIN, $8 - 15\mu m$
- dlouhé (far) infračervené záření neboli FIR $15 - 1000\mu m$

Další často používané rozdělení je toto:

- blízké $(0,7 - 5\mu m)$
- střední $(5 - 30\mu m)$
- dlouhé $(30 - 1000\mu m)$

Aplikace

Infračervené záření se používá pro přenos informací na krátkou vzdálenost, nejčastěji podle standardu IrDA. Příkladem mohou být mobilní telefony či dálkové ovladače. Infračervené záření v nich vysílají LED diody.

Telekomunikační pásma

Pro účely optické komunikace se IR záření dělí takto:

- O-pásmo 1260-1360 nm, f = 238-220 THz
- E-pásmo 1360-1460 nm, f = 220-206 THz
- S-pásmo 1460-1530 nm, f = 206-196 THz
- C-pásmo 1530-1565 nm, f = 196-191 THz
- L-pásmo 1565-1625 nm, f = 191-185 THz
- U-pásmo 1625-1675 nm, f = 185-179 THz

1.1.1 IrDA

IrDA je standard vytvořený IrDA konzorciem (Infrared Data Association), který definuje jak bezdrátově přenášet digitální data pomocí infračerveného záření. IrDA ve svých specifikacích definuje standardy jak fyzických koncových zařízení tak protokolu jimiž komunikuji IrDA zařízení. IrDA standard vznikl z potřeby mobilně propojit různé zařízení mezi sebou (hlavní využití IrDA je pro spojení notebooku či různých personálních komunikátorů, ale IrDA rozhraním jsou vybavovány například i videokamery).

IrDA zařízení komunikují pomocí infračervených LED diod a přijímačem jsou PIN fotodiody. IrDA zařízení dle normy IrDA 1.0 a 1.1 pracují do vzdálenosti 1.0 m při bitové chybovosti BER (bit error ratio, poměr chybné přenesených bitů ke správně přeneseným) 10-9 a maximální úrovni okolního osvětlení 10klux (denní svit slunce). Rychlosti jsou pro IrDA v. 1.0 od 2400 do 115200 kbps, používá se pulsní modulace 3/16 délky původní doby trvání bitu. Formát dat je stejný jako na sériovém portu, tedy asynchronně vysílané slovo uvozené startbitem.

IrDA v. 1.1 definuje navíc rychlosti 0.576 a 1.152 Mbps s pulsním kódováním 1/4 délky doby trvání původního bitu (střída 1/4). Při těchto rychlostech je již základní jednotka (paket) vysílán synchronně uvozen startovní sekvencí.

Pro rychlost 4 Mbps se používá takzvaná 4PPM modulace se střídou 1/4, v níž se 2 bity informace zakódují do pulsu v jednom ze čtyř možných časových pozic, nositelem informace je zde tedy pozice pulsu v čase namísto existence pulsu jako u předchozích modulací.

Důvodem použití 4PPM modulace je to, že je potřeba polovina bliknutí LED diody než v předcházejících modulacích - lze tedy přenášet data dvakrát rychleji. Kromě toho se přijímači lépe udržuje úroveň ostatního osvětlení - při 4PPM modulaci dopadá na přijímač konstantní počet pulsů za danou dobu.

IrDA definuje ještě tzv. low-power IrDA zařízení s dosahem do 20 cm a maximální rychlostí 115kbps

Požívané protokoly

IrDA Infrared Link Access Protocol (IrLAP)

Jedná se o úpravu protokolu HDLC pozměněného pro potřeby IrDA komunikace. V podstatě se stará o to, aby při komunikaci více zařízení najednou tato zařízení nerušila a určuje pravidla pro vzájemnou komunikaci. V praxi to vypadá tak, že jedno zařízení je primární a ostatní jsou sekundární. IrLAP popisuje jak spolu naváží zařízení komunikaci, ukončí či jak se budou interně číslovat. Navázání spojení začíná na rychlosti 9600 Bd a po výměně informací o rychlostech jednotlivých koncových účastníků komunikace se vytvoří logické kanály řízené vždy jen jedním primárním zařízením.

IrDA Infrared Link Management Protocol (IrLMP)

IrLMP má za úkol detekovat přítomnost zařízení která nabízejí nějakou službu, kontrolovat tok dat a dělat multiplexor pro konfigurace kde se účastní více stanic s různými schopnostmi Aplikace potom využívají vrstvy IrLMP k dotazům zda je v dosahu požadované zařízení apod. V této vrstvě však není definován spolehlivý způsob vytvoření kanálu, ten je definován až v IrDA

Transport Protocols (Tiny TP).

IrDA Transport Protocols (Tiny TP) je vrstva která udržuje virtuální kanál mezi zařízeními a sama opravuje chyby na lince (ztráta paketu apod.), provádí rozdělení dat do paketů a jejich znovusestavení.

IrDA Object Exchange Protocol (IrOBEX)

Jedná se o jednoduchý protokol s příkazy PUT a GET který dovoluje přenášet binární data mezi zařízeními. Je postaven na TinyTP a norma definuje co napsat do paketu aby se zařízení poznala a komunikovala.

Extensions to IrOBEX for Ir Mobile Communications

Je to rozšíření IrOBEX pro mobilní zařízení (handheldy, PDA, mobily) Definuje jak přenášet informace vztahující se k GSM síti (adresáře, SMS, kalendář, ovládání vytáčení čísel, digitální přenos voice pres Ir ...)

IrTran-P (Infrared Transfer Picture) Specification

Jedná se o definici kterou vyvynuly velké firmy vyrábějící digitální fotoaparáty k přenosu obrázků přes infra rozhraní. Je postaven také nad TinyTP.

1.1.2 Laserová pojítka

Optickým bezdrátovým spojem (FSO) se obvykle rozumí digitální plně duplexní spoj umožňující širokopásmové komunikační přenosy vzduchem při použití neviditelných paprsků světla. Vedle datových spojů lze tyto spoje s výhodou použít i pro přenos hlasu či obrazu.

Přenosová rychlost

Jelikož je rychlost šíření světla vzduchem vyšší něž přes vláknovou infrastrukturu, je možné bezdrátové optické spoje nazvat optickou komunikací rychlostí světla. Musíme však brát v úvahu návazné prvky, které přece jenom určité snížení přenosové rychlosti způsobí. Ale i tak lze realizovat obrovské datové toky v řádech Gigabitů (v případě produktů LightPointe se jedná až o 2,5 Gbit/s). Každá jednotka je tvořena kombinovaným optickým vysílačem a přijímačem, takže se navíc jedná o obousměrné plně duplexní spojení.

Spolehlivost a dostupnost

Realizovat spolehlivé spoje na delší vzdálenosti znemožňuje útlum světla v atmosféře, který se razantně zvyšuje smogem, deštěm, sněžením a především mlhou. Jelikož je závislost na povětrnostních podmínkách podstatnou nevýhodou těchto spojů, snaží se výrobci aplikovat do svých produktů stále nové a nové metody pro zvýšení spolehlivosti. Jednou z nich je např. vícesvazkové šíření signálu, které je odolnější jak vůči atmosférickým vlivům tak i vůči zaclonění paprsku. Zpravidla se používají 4 svazky. Významný je také přechod na délku nosné vlny v pásmu 1550nm (drtivá většina současných spojů používá vlnovou délku 850nm) Díky výhodnějším podmínkám pro bezpečnou práci v pásmu 1550nm lze podstatně zvýšit výkon laserového vysílače Pro přijímače se vedle běžně používaných křemíkových PIN diod, které jsou dostatečně rychlé, začínají používat tzv APD diody. Tyto mají až stonásobnou citlivost oproti PIN diodám, avšak musí být stabilizována jejich teplota, musí pracovat při větším napětí, atd. U profesionálních systémů jsou však čím dál častěji používané, neboť - jak udávají samotní výrobci - výsledek stojí za investice. Spolehlivost s ohledem na vlivy počasí je pak dokonce lepší než 99,995 procenta. Dalšího zvýšení spolehlivosti výrobci dosahují také použitím velkých apertur vysílacích soustav. Dochází tak ke snížení optické intenzity na výstupu, což dále zvyšuje odolnost svazku vůči zaclonění. Velmi důležitým hlediskem je zajištění směrové stability spoje. Je třeba si uvědomit, že na vzdálenost kilometru znamená i nepatrné chvění vysílače metrové odchylky paprsku. Proto bývají držáky velice robustní a předimenzované, aby se tomuto vlivu zamezilo. Někdy však ani nejpevnější uchycení nemusí stačit, neboť budova, na kterou je zařízení instalováno se může pohybovat. Na střechách výškových budov mohou výkyvy dosáhnout i několika centimetrů. Někteří přední výrobci začínají do svých zařízení aplikovat další prostředek pro zvýšení spolehlivosti, tzv. Autotracking systém, což je systém aktivního zaměřování, který automaticky upravuje směr paprsku dle potřeby.

Přestože výrobci udávají garantované dosahy v některých případech až 5 km, realizovat lze pouze spoje na relativně krátké vzdálenosti (kolem 500m). Tak lze zajistit dostupnost

99,99 procenta. Neoddiskutovatelnou podmínkou spolehlivého spoje je snad ještě více než u mikrovlnných systémů naprostá přímá viditelnost.

Výhody oproti mikrovlnným spojům

- vysoké přenosové rychlosti (až 2.5 Gbit/s) - vysoká přenosová rychlost umožňuje plnohodnotné nasazení těchto systémů ve všech typech přenosových sítí
- žádné vzájemné rušení - vysoce směrový paprsek zaručuje vysokou prostorovou selektivitu přenosového signálu, proto nehrozí interference s jinými spoji
- žádná potřeba kmitočtového přídělu - pásmo optické nosné vlny leží mimo oblast působnosti ČTÚ, proto při instalaci a provozu spoje nevznikají legislativní překážky a optická síť je tak naprosto nezávislá na omezeném a regulovaném spektru a kmitočtové licenci
- Transparentnost pro používané protokoly a navazující sítě - Ethernet, Fast Ethernet, Gigabit Ethernet, SONET/SDH, ATM, FDDI atd.
- přenositelnost a flexibilita řešení - frekvenční nezávislot umožňuje případné přesunutí spoje na jiné lokality bez přeladění
- interní i externí umístění - některá zařízení lze umístit jak vně budov, tak i uvnitř např. za okno a chránit tak samotné jednotky před atmosférickými vlivy
- bezpečnost přenášených dat - lze používat výše zmiňované kryptografické protokoly
- příznivý poměr cena/výkon - tato pojítka jsou zvláště u vysokých přenosových kapacit podstatně cenově přístupnější než kapacitou srovnatelná rádiová pojítka

1.2 Technologie založené na šíření radiových vln

1.2.1 PacketRadio

Packet Radio je v radioamatérská obdoba internetu. Síť PR je sítí uzlových stanic (nódů) a BBS (Bulletin Board Service - serverů umožňujících ukládání a čtení soukromé i veřejné pošty - bulletinů). Od počátku byla síť PR budována tak, že pro spojení jednotlivých prvků sítě byly použity bezdrátové linky v radioamatérských pásmech. Jednotliví uživatelé (radioamatéři) se do sítě PR připojovali též bezdrátově pomocí svých radioamatérských zařízení. Dnes se v některých případech pro zvýšení přenosových rychlostí využívá pro přenos dat mezi páteřními body též sítě internet. Některé BBS umožňují vstup do systému kromě přístupu bezdrátového též vstupu přes internet.

PR umožňuje posílání zpráv či souborů buď konkrétnímu adresátovi, nebo do veřejně přístupných diskusních skupin apod. Podoba s internetem a elektronickou poštou není náhodná, packet radio však spatřilo světlo světa o něco dříve než komercionalizovaná podoba e-mailu a i jeho rychlost je nepoměrně nižší. Radioamatérům však slouží pro šíření informací v rámci regionu, státu či celého světa dostatečně. O síť PR se ale musí neustále starat, dozorovat ji a rozvíjet množství nadšených radioamatérů. Systémovým operátorům jednotlivých uzlů sítě se říká sysopové (SYStem-OPerátor). Právě díky jejich času může síť šlapat tak, jak má. Provoz sítě je financován z příspěvků uživatelů.

Kromě privátních zpráv jsou pomocí PR šířeny nejčastěji radioamatérské informace (např. rady, žádosti o rady, schemata zapojení, informace o podmínkách šíření radiových vln, obecná sdělení o konání radioamatérských setkání, podmínky radioamatérských diplomů... atd.) Síť PR je přístupná výhradně radioamatérům.

Jako přenosový protokol je používán AX.25, který vznikl ze známějšího X.25 Hardwarové požadavky na straně uživatele předpokládají kromě PC a speciálního zdarma přístupného software i speciální modem. Modem lze nahradit zvukovou kartou.

Výhodou využívání sítě PR vůči využívání internetu jsou nulové náklady na připojení k síti a též i okamžitá dostupnost připojení k síti PR pomocí jednotné technologie prakticky na celém území nejen České republiky, ale i všech vyspělých zemí světa. Pro připojení uživatelů se používají kmitočty v pásmech VKV 145 MHz a 432 MHz.

Nevýhodou je relativně pomalý přenos dat - nejrozšířenějšími přenosovými rychlostmi pro připojení uživatelů jsou 1,2 kbit/s (1200 bitů za sekundu) a 9,6 kbit/s. V místech, kde není možné připojení v pásmech VKV (typicky na moři) se využívají KV kmitočty, kde je však přenosová rychlost pouhých 300 bit/s. (Pro porovnání - rychlost telefonního modemu používaného pro připojení k síti Internet je 56 kbit/s, tedy asi 50x vyšší než běžné připojení do PR a skoro 200x vyšší než připojení do PR přes pásma KV.)

1.2.2 Wireless USB

V roce 2001 si společnost Cypress Semiconductor (CS) nechala registrovat ochrannou známku na označení WirelessUSB a od stejného roku vyrábí a nabízí integrované obvody pro bezdrátovou komunikaci.

WirelessUSB je vlastní protokol vyvinutý společností CS, který umožňuje levněji řešit

bezdrátové připojení periferních zařízení ovládaných člověkem (HID = Human Interface Devices), jako jsou například bezdrátové klávesnice a myši. V podstatě jde o náhradu klasického kabelového USB spojení periferního zařízení bezdrátovým připojením, přičemž osobní počítač nemusí toto bezdrátové připojení obsluhovat. To znamená, že není třeba žádný speciální software pro dané zařízení.

CS volil pro svůj nový protokol bezlicenční pásmo 2,4 GHz které rozděluje na 79 nezávislých kanálů. To umožňuje zařízením vysílat v jednotlivých kanálech vzájemně nezávislé signály. Navíc protokol WirelessUSB podporuje "frequency hopping" (stejně jako BlueTooth) s výše uvedeným počtem kanálů. To znamená, že by neměl být problém používat protokol WirelessUSB zároveň s dalšími protokoly v daném frekvenčním pásmu.

Zařízení s integrovanými obvody určenými pro práci s protokolem WirelessUSB společnosti CS jsou schopny komunikovat na vzdálenost 10 metrů, což je srovnatelné s technologií BlueTooth (pokud se dají oba způsoby komunikace srovnávat). Vzdálenost mezi zařízeními je možné zvýšit až na 100 metrů přidáním externích zesilovačů. Přenosová rychlost protokolu WirelessUSB je pouhých 64 kbit/s (u jednosměrných sítí), ale jak bylo uvedeno, je plně dostačující pro zařízení, jako jsou například myši a klávesnice.

Protokol WirelessUSB byl navržen tak, aby komunikace mezi zařízeními dosahovala malého zpoždění (CS udává až 30 milisekund) při minimálním odběru elektrické energie (1 μ A ve "sleep modu"). V této souvislosti se nabízí srovnání s technologií BlueTooth a ZigBee. Základní rozdíl mezi WirelessUSB a technologií BlueTooth je ten, že zařízení pracující s protokolem WirelessUSB nevyžadují přenos synchronizačních údajů během nevyužívané doby (stejně jako je tomu u technologie ZigBee). Protokol WirelessUSB je charakteristický jednoduchými a krátkými procedurami výměny zpráv v případě nutnosti komunikace. V opačném případě jsou zařízení podporující protokol WirelessUSB v tzv. "sleep modu" až do okamžiku, kdy je detekován signál od uživatele. To vše má za následek úsporu elektrické energie a dlouhou provozní dobu baterií.

CS udává, že v laboratorních podmínkách byla naměřena doba šest až osm měsíců u klávesnice napájené třemi tužkovými bateriemi typu AA (CS ovšem podrobněji neuvádí, jak test probíhal, zda se jednalo o nepřetržitý provoz zařízení atd.). Pro srovnání: u technologie ZigBee je garantována životnost baterií až na několik let.

1.2.3 HomeRF

HomeRF využívá protokol SWAP (Shared Wireless Access Protocol). Umožňuje datový přenos rychlostí do 2 Mbit/s s dosahem do 100 metrů a je používán v pásmu 2,4 GHz. Z uvedených faktů by mohlo vyplývat, že HomeRF má velký potenciál stát se konkurentem Bluetooth, ovšem proti těmto skutečnostem působí fakt, že jedná o centralistickou koncepci a opírá se o domácí počítač. Významným faktorem může být i to, že HomeRF je prodávána za cenu 500 USD).

1.2.4 Wi-Fi - IEEE 802.11

Jedná se asi o nejrozšířenější standard v oblasti bezdrátových technologiích navržený speciálně pro aplikace bezdrátových sítí. Vývoj tohoto standardu byl podporován asociací firem zvanou Wireless Ethernet Compatibility Alliance (WECA).

Pro komunikaci se v dnešní době používají dvě přenosová pásma. Jsou to:

2,4 GHz - toto pásmo je nelicencované a tudíž nolně přístupné široké veřejnosti. Hlavní nevýhodou je silný provoz a tím pádem i veliké zarušení což může mít za následek omezení přenosové rychlosti.

5 GHz - v tomto případě se jedná o pásmo licencované. Je zde povolen vyšší vysílací výkon a je rozděleno na více kanálů. Z toho plyne větší dosah i přenosové rychlosti.

V jednotlivých frekvenčních pásmech se ještě standard dělí na různé revize označované písmeny. Důvodem proč se tak stalo a stále děje je především požadavek na co nejvyšší přenosovou rychlost. Nejznámější a nejpoužívanější jsou 802.11a která pracuje ve frekvenčním pásmu 5 GHz dále 802.11b a 802.11g pracující v pásmu 2.4 GHz. Jednotlivé revize se od sebe liší kódováním přenosu, takže je zcela běžné, že jeden adaptér podporuje více revizí.

Tento standard je založen na sedmivrstvém modelu OSI a definuje jeho dvě spodní vrstvy. Jsou to Fyzické, která se stará o komunikaci na nejnižší úrovni a v podstatě se stará o řešení vlastního připojení a dále definuje vrstvu spojovou která se zabývá kódováním a přenosem informace. Všechny ostatní vrstvy nechává standard nespecifikované.

Protože se jedná o bezdrátovou technologii kde nemůžeme přesně vymezit pokrytí je standard 802.11 vybaven mechanismy které chrání síť před nepovolaným přístupem a případným zneužitím. Proto jsou zde postupy, které by měly tento problém ošetřit. Jsou v zásadě dvě:

Šifrování jedná se o zašifrování komunikace předem daným klíčem a tím se znemožní případné odposlechnutí původní zprávy

Autentizace je určena k tomu, aby mohl k síti přistupovat jen určitý předem daný okruh stanic

WLAN sítě podle 802.11 mohou pracovat ve dvou základních režimech. Prvním z nich je **"ad hoc"** mod, určený zejména pro běžné peer-to-peer sítě pro zhruba 2-5 počítačů spojených bezdrátovou sítí. Je možné si jej představit jako klasickou malou LAN síť, kdy všechny stroje komunikují se všemi ostatními jako rovný s rovnými.

výhody: není potřeba instalovat metalickou kabeláž při dočasném propojení dvou nebo více počítačů, nízká cena, nutné pouze síťové adaptéry

nevýhody: nutnost přímého spojení mezi jednotlivými počítači

Druhým režimem je mod **"infrastructure"**, tedy implementace klasického vztahu klient server. "Serverem" je v tomto případě tzv. Access Point (AP), tedy zařízení schopné zajišťovat komunikaci všech připojených klientů. Zde probíhá komunikace výhradně s Access Pointem, tzn. jednotliví klienti se na vzájem nemusí vůbec vidět. AP jsou vybaveny také zásuvkou pro připojení k vnitřní metalické síti LAN, takže fungují jako přemostění mezi LAN a WLAN.

výhody: není potřeba instalovat složitou infrastrukturu metalické kabeláže ve velkých firmách a stačí propojit pouze přístupové body, v dnešní době už nízká cena

nevýhody: nutnost na každý uzel pořídit přístupový bod a zabezpečit jej proti neoprávněnému přístupu

Nejčastěji se můžeme s tímto standardem setkat v oblasti bezdrátových počítačových sítí a to jak při propojování počítačů mezi sebou tak i pro připojení různých periferií jako jsou například tiskárny. Můžeme ho však také nalézt v mobilních telefonech či PDA.

Velikou výhodou tohoto standardu kromě jeho zajisté zajímavých parametrů je jeho veliká rozšířenost. S ní ruku v ruce jde i nízká cena koncových zařízení a tím i zajímavost pro uživatele. Tato dobrá dostupnost jak hardwaru tak i dokumentace a různé další literatury měla velkou váhu při mém rozhodování o volbě komunikační technologie.

1.2.5 ZigBee - 802.15.4

Komunikační technologie popsaná standardem IEEE 802.15.4 - ZigBee patří do skupiny bezdrátových sítí PAN (Personal Area Networks). Do této skupiny sítí patří i velmi rozšířený IEEE 802.15.1 - Bluetooth, jež nalézá hlavní uplatnění převážně ve spotřební elektronice. Existuje však celá škála průmyslových aplikací, pro které Bluetooth není vhodný. Z tohoto důvodu byla založena ZigBee aliance za účelem vytvoření nového bezdrátového komunikačního standardu vhodného i pro účely průmyslové automatizace. V současné době se na vývoji a rozvoji tohoto standardu podílí více než šedesát firem a mezi nimi jsou i přední světové firmy z oboru automatizace (Honeywell, Motorola, Philips, Samsung, Omron, ABB, Siemens). ZigBee je navržen jako jednoduchá a flexibilní technologie pro tvoru i rozsáhlejších bezdrátových sítí u nichž není požadován přenos velkého objemu dat. K jejím hlavním přednostem patří spolehlivost, jednoduchá a nenáročná implementace, velmi nízká spotřeba energie a v neposlední řadě též příznivá cena. Díky těmto vlastnostem nalezne uplatnění v celé škále aplikací, jež leze zařadit do několika skupin:

- automatizace budov (zabezpečení, ovládání světel, kontrola přístupu)
- spotřební elektronika (dálkové ovládání elektrospotřebičů)
- počítačové periferie (bezdrátové myši, klávesnice)
- průmyslová automatizace
- zdravotnictví (pacientské monitory)

Díky různorodosti předpokládaných aplikací standard definuje tři základní režimy přenosu dat:

- periodicky se opakující (přenos dat z čidel)
- nepravidelné přenosy (externí události, např. stisknutí tlačítka uživatelem)

- opakující se přenosy u nichž je požadavek na malé zpoždění (bezdrátové počítačové periferie - klávesnice a myši)

Struktura komunikačního standardu

Kvůli nutnosti implementovat standard ZigBee i do málo výkonných 8 bitových mikrokontrolérů (HC08, x51) bylo dbáno na maximální jednoduchost implementace protokolů. Díky tomu struktura protokolů nezabere více než 30kB programové paměti. Protokol se skládá z třech základních vrstev. Vrstvy standardu IEEE 802.15.4, nad nimi je definována síťová vrstva (NWK) a aplikační vrstva (APL). Fyzická vrstva specifikuje přístup k přenosovému médiu. Síťová vrstva realizuje připojení k síti, zabezpečení a směrování paketů. Aplikační vrstva (APL) zajišťuje potřebné služby. Skládá se z aplikační podvrstvy (APS), ZigBee objektů a uživatelských aplikačních objektů.

Fyzická a MAC vrstva standardu IEEE 802.15.4

Standard IEEE 802.15.4 definuje několik základních radiových pásem, aby mohl být využit v různých zemích, kde jsou rozdílné národní předpisy a normy. Hlavním problémem u většiny bezdrátových technologii jsou rozdílné definice radiových pásem v Americe a v Evropě. Z tohoto důvodu byli definovány tři základní frekvenční pásma: globální, Amerika a Austrálie, Evropa.

Dosah ZigBee je přibližně 10 až 50 metrů v závislosti na lokálních podmínkách šíření signálu. Pro přenos se datový signál moduluje metodou O-QPSK (BPSK) a přenášejí prostřednictvím DSSS (Direct Sequence Spread Spectrum). Pro přístup k fyzickému médiu je použita metoda CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance and optional time slotting).

MAC vrstva (linková) definuje samotný komunikační protokol, jež je založen na přenosu datových rámců. Jsou definovány čtyři typy komunikačních rámců, jež jsou vyžínány pro přenos dat, řízení či správu sítě:

Data Frame rámec využívaný pro všechny přenosy užitečných dat

Acknowledgement Frame rámec pro přenos potvrzovací informace využíván na úrovni MAC pro potvrzování komunikace

Beacon Frame rámec používaný koordinátorem k vysílání tzv. beacons (používané pro uvádění klientských zařízení do spánkového režimu)

MAC Command Frame rámec k nastavování a řízení klientských zařízení v síti ZigBee

Z důvodů minimalizace spotřeby koncových zařízení může být na základě synchronizace mezi koordinátorem sítě a koncovou stanicí uspávána jednotlivá koncová zařízení. K jejich probouzení dochází v předem definovanou dobu, a poté jsou přeneseny veškeré užitečné informace. Interval synchronizačních sekvencí může být v rozmezí 15ms až přibližně 15 minut. Synchronizace je realizována pomocí tzv. rámce beacon. Koncová zařízení jsou periodicky

problouzena a přenáší data ke koordinátoru sítě. Ten tato data uloží a následně přepošle při probuzení zařízení pro nějž jsou tata data určena. Tento přístup umožňuje extrémně snížit spotřebu koncových zařízení. Tato zařízení mohou tak být napájena bateriově. Při využití všech úsporných opatření je možné dosáhnout výdrže koncového zařízení na jednu alkalickou baterii 6 měsíců až 2 roky. Pokud síť funguje bez použití beacon sekvencí, jednotlivá zařízení periodicky dotazují koordinátora.

Topologie sítě, zabezpečení

Technologie ZigBee postavená na fyzické linkové vrstvě IEEE 802.15.4 definuje tři různé síťové topologie. Základní topologii je topologie hvězdicová s centrálním řídícím uzlem (koordinátorem sítě). Druhým typem je stromová struktura jež umožňuje zvětšit vzdálenost mezi koordinátorem a koncovým zařízením. Protokol též umožňuje vytvoření redundancích spojení a vyniká tak topologie typu sítě - mesh. S její pomocí je možné vytvořit síť prakticky libovolného uspořádání.

Standard ZigBee dělí zařízení na zařízení FFD (Full Functional Device) a RFD (Reduced Functionality Device). FFD zařízení implementují kompletní protokolový rámec a zajišťují veškeré služby, které standard ZigBee stanovuje. RFD zařízení implementují pouze nezbytné protokolové knihovny z důvodu maximálního omezení hardwarové náročnosti. Tyto zařízení mohou pracovat pouze jako koncová. Mohou komunikovat pouze s koordinátorem sítě a jsou omezeny na hvězdicové uspořádání topologie (koncové větve). Koordinátor sítě a směrovače jsou realizovány FFD zařízeními.

Jednotlivá zařízení sítě jsou adresována pomocí binárního adresného kódu o délce 64 bitů či ve zkrácené podobě 16 bitů. Lokální zkrácená adresa umožňuje v jedné síti adresovat maximálně 65535 zařízení. Každá sestavená síť je ještě dále identifikována 16 bitovým PAN ID, jež slouží pro rozlišení překrývajících se sítí postavených na standardu IEEE 802.15.4. Každou síť zakládá a spravuje koordinátor, který též přiděluje PAN ID. Ostatní stanice pracují jako směrovače a koncová zařízení.

Síťová vrstva (NWK) zajišťuje připojení k sítí, zabezpečení, směrování a synchronizaci. V případě koordinátora sítě je ještě zodpovědná za start sítě a přiřazování adres nově nalezeným zařízením.

Jako základní zabezpečení ZigBee se používá AES (Advanced Encryption Standard) s klíčem o délce 128 bitů jež je implementován v síťové vrstvě. Pokud je požadováno i zabezpečení MAC Command Frame, Beacon Frame a Acknowledgement Frame je realizováno již v MAC vrstvě pomocí AES. Díky tomu je možné ověřit autenticitu a integritu MAC rámce a zajistit jeho důvěrnost. Při požadavku na ověření integrity je vytvořen MIC (Message Integrity Code) o délce 4, 8 či 16 oktetů a je vyslán společně s MAC rámcem. V tomto případě je použit AES algoritmus v CTR (Counter) módu. Pokud je nutné zajistit důvěrnost MAC rámce je k němu přidána informace o pořadí rámce a klíče (Frame Count, Key Sequence Count). Na vysílací a přijímací straně je udržována aktuální informace o čísle rámce. Pokud obdrží přijímací zařízení rámec s neplatným číslem je detekováno narušení bezpečnosti. AES je použit v CBC-MAC (Cipher Block Chaining) módu. Při implementaci jak ověřování integrity tak šifrování je použit AES v módu jež je nazýván CCM.

Síťová vrstva používá k zabezpečení SSP (Security Services Provider). Tato vrstva zajišťuje zabezpečení ochozích rámců, dekódování a ověřování pravosti příchozích rámců. Jako zabezpečovací algoritmus je použit AES v mírně modifikovaném módu CCM jež nese označení CCM . Síťová vrstva je zodpovědná za realizaci zabezpečení. Vyšší vrstvy se starají o nastavení SSP (nastavení klíčů a udávají jakým způsobem bude použit CCM pro jednotlivé rámce).

Aplikační vrstva

Aplikační vrstva protokolu (APL) se skládá z pomocné aplikační APS podvrstvy, ZigBee objektů (ZDO) a uživatelem definovaných aplikačních objektů. Pomocná aplikační podvrstva je zodpovědná za párování zařízení podle poskytovaných služeb a požadavků. To je realizováno pomocí tzv. párovací (binding) tabulky. ZigBee objekt definuje roli jednotlivých zařízení v rámci sítě (koordinátor, směrovač, koncové zařízení). Dále zajišťuje vyhledávání nových zařízení a jimi poskytovaných služeb. V neposlední řadě zodpovídá za zabezpečení (volí jeho způsob, jako např. veřejné klíče, symetrické klíče). Uživatelské aplikační objekty implementují konkrétní požadavky aplikace dle definovaného ZigBee profilu. ZigBee profil zastřešuje definice možných zařízení, formátů a typů zpráv. Každý profil je určen unikátním 16 bitovým identifikátorem podle specifikace ZigBee Alliance

Tato nová technologie mi také přišla velmi zajímavá především z hlediska spotřeby, ale v současné době je jen málo zařízení které dokážou komunikovat pomocí tohoto standardu a navíc jsou zatím příliš drahá. Myslím si, že tento standard má velikou budoucnost a proto jsem mu při popisu věnoval větší pozornost.

1.2.6 Bluetooth - IEEE 802.15.1

Jde o otevřený protokol pro bezdrátový přenos dat a hlasu. Je založen na vysílaní radiových vln s krátkým dosahem, zajištujících rychlé navázání chráněné komunikace s ostatními zařízeními. Bluetooth se synchronizuje s výchozím časovacím mechanismem, definovaným řídící funkcí piconet.

Historicky byl první návrh předložen společností Ericsson v roce 1994. Poté v roce 1998 vznikla skupina SIG (Special Interest Group), do které postupně vstupovaly spolecnosti: Ericsson , Nokia, Toshiba, IBM, Intel, Sony a další výrobci. Skupina SIG má pres 2.000 členů z různých oblastí a počet členů se stále rozrůstá.

Jde o univerzalní radiový systém, skládající se z malých základních struktur, označovaných pojmem pikonet (miniaturní sít). V každé z těchto struktur se může pohybovat až 8 miniaturních modulů (terminálů), z nichž každý obsahuje radiový vysílač s přijímačem. Pracuje na průmyslové frekvenci 2.4 GHz, označované jako pásmo Industrial Scientific Medical (ISM), které není prakticky celosvětově licencováno. Podobně jako u klasických počítačových sítí mohou být zařízení propojena jako rovný s rovným (peer-to-peer), nebo s jedním nadřízeným zařízením systémem master-slave, přenos se přitom může odehrávat mezi dvěma zařízeními (point-to-point) nebo od jednoho zařízení ostatním (point-to-multipoint). Bluetooth nevylučuje ani propojení dvou a více piconetů stejným protokolem, potom ale klesá přenosová rychlost.

Zařízení navzájem komunikují technikou přeskoku kmitočtů (Frequency Hopping). Jedná se o sekvenci až 78 možných frekvencí. Datová zpráva je tak vysílána pomocí mnoha nosných frekvencí tzv. hops.

Vysoké spolehlivosti je dosaženo díky tomu, že nepotvrzené tj. chybně přenesené rámce jsou znovu přenášeny s jinou nosnou frekvencí tj. v dalším hopu. Umístění více systémů v jednom místě je umožněno použitím různých sekvencí v každém systému.

Tyto moduly potom spolu mohou vzájemně bezdrátově komunikovat, tedy vysílat nebo přijímat nejrůznější digitální data, a to až na vzdálenost 12 metrů přičemž přenosová rychlost se pohybuje okolo 1Mb/s. Současná specifikace umožňuje symetrické přenosy 432.6Kb/s, asymetrický přenos 721/57.6Kb/s či synchronní hlasové kanály 65Kb/s. Cílem do budoucna je dosáhnout přenosových rychlostí až 2Mb/s.

V jedné samostatně se řídící pikosíti, využívající určitý radiový kanál, musí jeden z u účastníků jako první (master) iniciovat sestavení sítě a plní tedy pro tuto chvíli řídící (master) funkci. Tato funkce spočívá především v identifikaci účastníků a zajištění jejich vzájemné synchronizace. Ostatní účastníci představují podřízené jednotky (slave).

Tyto funkce jsou však dočasné a zanikají po zrušení dané pikonet sítě. V příštím cyklu může funkci řídící jednotky plnit libovolný jiný účastník. V dané lokalitě mohou být ve stejný okamžik další pikosítě. Přičemž libovolný účastník může být zapojen současně do několika z nich. Tak vzniká rozptýlená síť Bluetooth. Všechny potřebné kroky pro navázání a udržování vzájemného spojení si provádí systém Bluetooth zcela automaticky sám.

Bluetooth systém se skládá:

- Bluetooth^{TM} radio - vysílač, přijímač, analogová radio elektronika.

- Bluetooth^{TM} Link Controller - řídí navázání spojení a komunikaci, identifikaci, přístup.
- Bluetooth^{TM} Link Manager - připravuje data a zaručuje komunikaci se zařízením, kde je Bluetooth modul umístěn.

Vyzářený výkon je automaticky zesílen/zeslaben tak, aby komunikace probíhala při co nejmenším odběru. Je-li např. připojený spotřebič vzdálen pouze pár metrů, je signál utlumen na nejnižší možnou mez. Navíc při nízkém nebo nulovém přenosu dat přechází zařízení do low-energy módu, který je přerušován pouze krátkými pulzy nezbytnými pro ověření, zda druhé zařízení je stále připojeno. Pro porovnání: Bluetooth radio spotřebuje 3% energie, které by spotřeboval moderní modem. Bluetooth radio je navrženo pro práci i ve velmi rušném prostředí (myšleno plném rádiových signálů). Ochrana dat uživatele je zajištěna korekčními mechanismy, interním kódováním a bohatou škálou autentifikačních rutin.

Bezpečnost technologie Bluetooth

Na jednu stranu spočívá nebezpečí ve využívání nelicencovaného pásna 2.4GHz, ale na druhou stranu jsou data chráněna samotnou podstatou technologie Bluetooth. Tento standard byl původně navržen jako náhrada kabelu pro dvě zařízení, to znamená na krátkou vzdálenost. V tomto případě není nějak těžké zabezpečit, aby se vaše data nedostala do neoprávněných rukou. Nicméně při expanzi možností využití Bluetooth, zejména v oblasti tzv. Access pointů, kdy se propojuje více uživatelů najednou, získává další zabezpečení posílaných dat na důležitosti. Mnohem zásadnější ochrana by měla přijít také se standardem verze 2, kdy se počítá i se zvýšením dosahu signálu. Rozlišujeme dva typy zabezpečení:

Hardwarová ochrana

Nejnižší úroveň ochrany posílaných dat prostřednictvím technologie Bluetooth je její hardwarová specifikace. Z hlediska frekvence jí bezpečnost dostatečně zajišťuje technika rozprostření signálu metodou FHSS - "frequency hopping" s rychlostí 1600 skoků za sekundu a s prodlevou 625 s, přičemž počet kanálů je 79. Již z tohoto hlediska je velice těžké tento signál odposlouchávat. Bluetooth zařízení mají navíc zabudovanou vnitřní bezpečnostní ochranu proti odposlechu a falsifikaci originálních dat. Svou roli také hraje udělený rozsah frekvenčního pásma, který je ve většině Evropy (kromě Francie) 2,4 - 2,2475 GHz.

Aplikační ochrana

Aplikační neboli softwarovou ochranu dat je nutno rozdělit podle důležitosti těchto paketů. Podle toho pak rozlišujeme různé úrovně softwarového zabezpečení. Specifikace Bluetooth definuje 3 takové úrovně:

- **nedůležitá data - non-secure** Pro data, jako jsou například elektronické vizitky posílané z mobilního telefonu se používá (v návaznosti na definované profily) nechráněná komunikace. Přitom nechráněná by se slušelo dáti do uvozovek, každá komunikace mezi dvěma zařízeními je, jak už bylo řečeno, zabezpečena hardwarově a principielně.

- **vyšší bezpečnost - autentizace** Pro data s visačkou vyššího zabezpečení se využívá klasického způsobu ochrany dat a tím je takzvaná komunikace na vyžádání. Běžný způsob autentizace výzva-odezva (challenge-response) zajišťuje, že každá uskutečněná komunikace je přesně adresována. Každý Bluetooth chipset má totiž v sobě zakódovanou 48-bitovou informaci - adresu, na základě které komunikuje s jinými přístroji. Jakmile dojde k nesrovnalosti adresy či jakémukoliv přerušení toku dat, komunikační kanál se neotevře a komunikace se přeruší. Veškerá zařízení spolu komunikují peer to peer, při autentizaci se rozdělí na Master (zařízení, které vyslalo požadavek na spojení) a Slavě (přijímá požadavek a odesílá zpět svou 48-bitovou adresu). Jednotlivá zařízení se mohou spojovat individuálně, ale i hromadně.

- **důležitá data - autentizace + kryptování** U dat, která chceme uchovat v tajnosti za každou cenu, což může být například i přenos hlasu (head set - mobilní telefon), je bezpečnost navíc zaručena vestavěnou podporou 128-bitového šifrovacího kódu. Tento šifrovací kód můžeme dále dělit podle dvou klíčů: a) Private user key - tajná entita, získává se během inicializace a není nikdy prozrazen b) Random number - je rozdílný pro každou novou transakci, získává se ze pseudo-náhodného procesu v Bluetooth jednotce,

Celkově je tedy aplikační systém odolný proti vícenásobným cestám šíření a obsahuje korekci chyb a již zmiňovanou enkrypci. Nutno podotknout, že s každou zašifrovanou informací se snižuje i přenosová rychlost.

Tento standard nevyniká ani nízkou spotřebou a ani přenosovou rychlostí. Myslím, že na svou dobu to byla dobrá technologie, ale se vzrůstajícími nároky uživatelů na objem přenesených dat se výrobci začnou poohlížet po něčem jiném. Problematické je to i s výstavbou rozsáhlejších sítí kdy při větším počtu komunikujících účastníků dramaticky klesá přenosová rychlost.

2 Popis standardu 802.11

Na základě předchozí analýzy a zvážení všech výhod a nevýhod jsem vybral standard IEEE 802.11. Hlavním důvodem byla jeho vysoká rozšířenost, dostupnost a výsledná cena koncových zařízení.

2.1 Komponenty sítě

Každá 802.11 síť obsahuje čtyři hlavní druhy fyzických komponent:

- Distribuční systém
- Přístupový bod (access point)
- Bezdrátové médium
- Stanice

Distribuční systém v okamžiku kdy síť tvoří více přístupových bodů musí spolu komunikovat a předávat si informace o poloze jednotlivých stanic. Distribuční systém je vlastně logická komponenta sloužící k přesměrování datového toku k příslušné stanici v závislosti na její poloze. Standard 802.11 ovšem žádnou takovou komponentu blíže nespecifikuje a ve většině případů je distribuční systém tvořen mostem (bridge) a distribučním médiem. To dosti často bývá Ethernet.

Přístupový bod (Access point) ten právě představuje ono přemostění (bridge) mezi bezdrátovou a drátovou sítí. Dosti často obsahuje i další doplňkové funkce, ale přemostění je jeho základní a nejdůležitější funkcí.

Bezdrátové médium jedná se o nosič dat při přenosu dat od jedné stanice k druhé. Dalo by se říci že je to vzduch, ale není tomu tak. Jedná se spíše o dvě rádiové frekvence (2.4 a 5 GHz) a velmi zřídka používanou infračervenou fyzickou vrstvu.

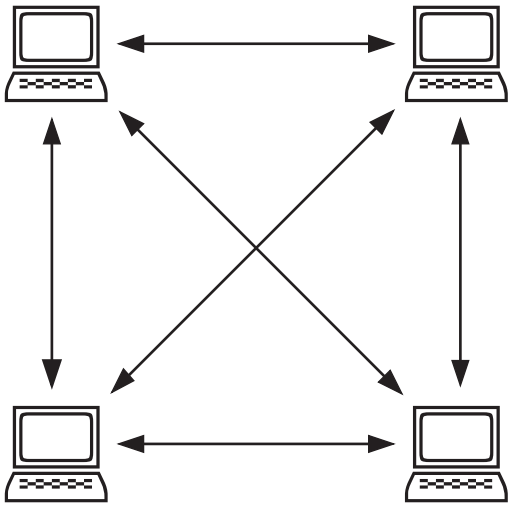
Stanice je to jakékoliv zařízení kromě přístupového bodu, které se účastní komunikace v bezdrátové síti. Stanice může být jak mobilní (notebook, PDA, mobilní telefon ...) tak se může jednat i o zařízení prakticky nepřenosné (stolní počítač, tiskárna ...)

2.2 Typy sítí

Základní blok 802.11 se označuje jako Basic Service Set (BSS). Jde o skupinu stanic, která spolu navzájem komunikují na území vymezeném průnikem dosahů jednotlivých stanic a nazývaném Basic Service Area (BSA). Rozlišujeme dva typy sítí podle toho jakým způsobem probíhá komunikace mezi jednotlivými členy BSS.

2.2.1 Ad-hoc sítě

Ad-hoc sítě často nazýváme jako peer-to-peer, nezávislé nebo jako Independent Basic Service Set (IBSS). Jedná se v podstatě o soubor bezdrátových stanic které komunikují přímo mezi sebou bez použití jakéhokoliv prostředníka. Z toho vyplívá, že pokud spolu chtějí stanice komunikovat musí být navzájem v rádiovém dosahu.



Obrázek 1: Ad-hoc síť

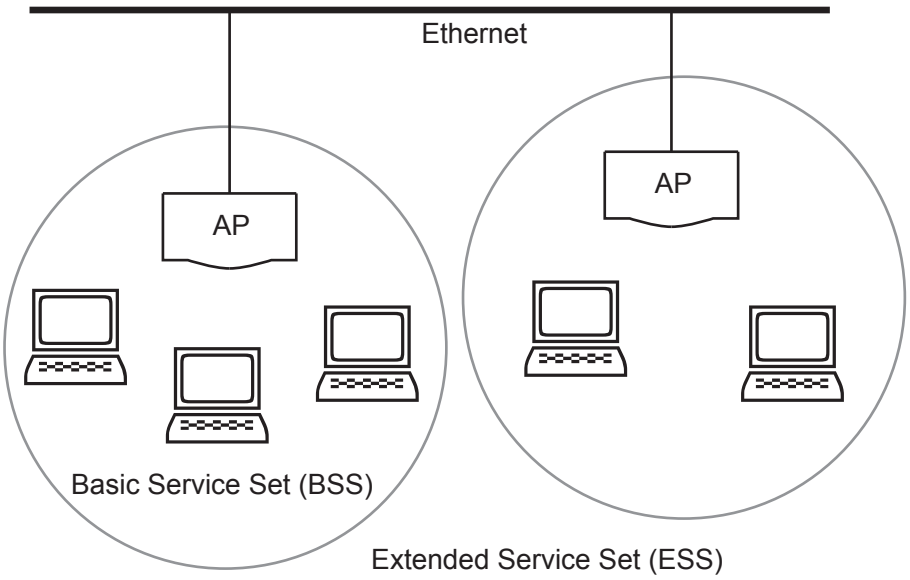
Tento režim je vhodný pro snadno uskutečnitelné bezdrátové spojení mezi stanicemi vzdálenými několik metrů. Nejčastěji se používá pro jednorázové spojení několika počítačů na omezený čas. Pro rozlehlejší sítě o větším počtu uživatelů, nebo v případě rozlehlého a členitého prostředí je tento model nevhodný a nepoužitelný. Vzhledem ke složitosti nastavování sítě se tento systém v praxi moc neujal.

2.2.2 Infrastrukturní sítě

Tento typ sítě se nazývá infrastrukturní proto, protože má přesně vymezenou infrastrukturu. Stanice zde nekomunikují přímo mezi sebou, ale prostřednictvím síťové komponenty zvané přístupový bod (access point, AP)

Jak již bylo řečeno, přístupový bod kromě toho, že komunikuje se stanicemi zajišťuje i připojení na páteřní síť (Ethernet). Protože však může komunikovat s více stanicemi najednou slouží i k bezdrátové komunikaci mezi jednotlivými stanicemi aniž by chtěly přistupovat na páteřní síť.

Komunikace tedy probíhá ve dvou krocích. Nejdříve ze stanice na přístupový bod a poté z přístupového bodu k cílové stanici. Může se zdát, že infrastrukturní typ sítě má větší nároky na přenosovou kapacitu, ale není tomu tak. Zatímco v případě Ad-hoc sítě musí stanice



Obrázek 2: Infrastrukturní síť

udržovat spojení s každou stanicí se kterou komunikuje tak u infrastrukturní sítě udržuje spojení pouze s přístupovým bodem. Navíc pokud je stanice v úsporném režimu, může pro ni přístupový bod data ukládat a vyslat je až se probudí.

V infrastrukturní síti se musí stanice asociovat s přístupovým bodem a bez toho vytvoření sítě není možné. Asociační proces vždy iniciuje mobilní stanice a přístupový bod jí to buď umožní a nebo zamítne. Takto se může asociovat pouze s jedním přístupovým bodem.

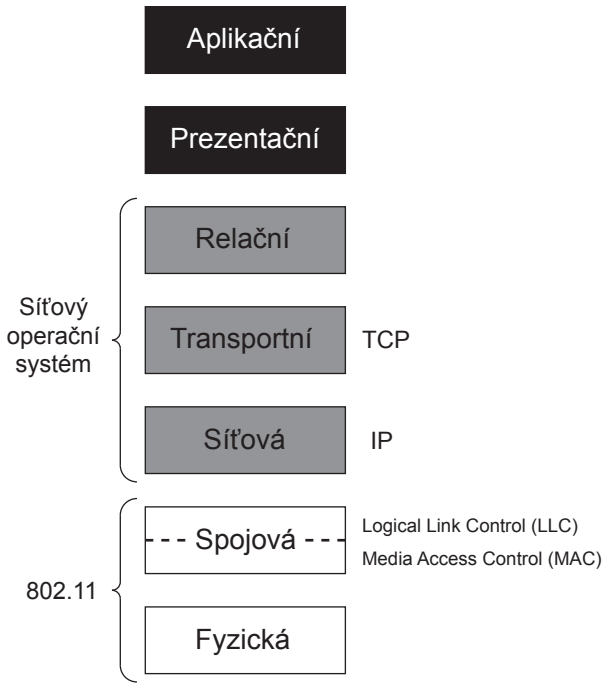
Rozšířená oblast služeb (Extended Service Set)

BSS může vytvořit síť v domácnost nebo menší kanceláři, ale ve větších a členitých prostorách jako jsou např. celé budovy ním pokrytí nabídnout nemůže. Standard 802.11 dovoluje vytvořit větší sítě propojením BSS do takzvaných Rozšířených Souborů Služeb, Extended Service Set (ESS). ESS vytvoříme propojením jednotlivých BSS přes páteřní síť. Stanice mohou uvnitř ESS mezi sebou komunikovat ačkoliv jsou v rozdílných BSS a mohou i mezi jednotlivými BSS pohybovat.

2.3 OSI model

Standard 802.11 se stejně jako jiné standardy v síťové komunikační technice je popsán sedmivrstvým modelem s názvem OSI (Open System Interconnection).

1. physical layer (fyzická vrstva) Komunikace na nejnižší hardwarové úrovni.
2. data-link layer (spojová vrstva) Vrstva zabývající se kódováním a přenosem informací



Obrázek 3: OSI model

3. network layer (síťová vrstva) Obsluha přenosových tras a zpráv
4. transport layer (transportní vrstva) Řízení doručování informací a kvality přenosu
5. session layer (relační vrstva) Udržování a koordinace komunikace
6. presentation layer (prezentační vrstva) Formátování, konverze a zobrazení přenesených dat
7. application layer (aplikační vrstva) Přenos informací mezi programy

Každý produkt na síti je možné popsat pomocí těchto vrstev. Specifikace 802.11 však definuje pouze dvě nejnižší vrstvy a to fyzickou a spojovou.

2.4 Fyzická vrstva

Fyzická vrstva je fyzickým rozhraním mezi zařízeními v síti. A protože hovoříme o bezdrátových sítích jedná se o vrstvu bezdrátovou.

Původně (při vydání standardu v roce 1997) byly ve standardu 802.11 definovány tři fyzické vrstvy.

- Frequency-hooping (FH) spread-spectrum radio

- Direct-sequence (DS) spread-spectrum radio
- Infračervené světlo

V roce 1999 při revizi standardu byly tyto tři vrstvy doplněny ještě o další dvě

- Orthogonal Frequency Division Multiplexing (OFDM)
- High-Rate Direct Sequence (HR/DS nebo HR/DSSS)

2.4.1 Rozprostřené spektrum (spread spectrum)

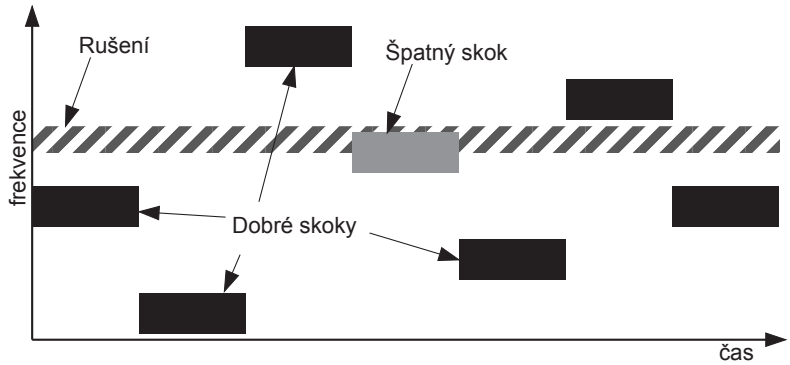
Technologie rozprostřeného spektra se používá pro dosažení rychlých datových přenosů v pásmu ISM. Na rozdíl od tradičních rádiových technologií, které se snaží do co nejužšího pásma vměstnat co největší datový tok tak u rozprostřeného spektra se používá matematické funkce pro rozprostření celé síly signálu do relativně Širokého frekvenčního bloku. Přijímač poté provede opačnou matematickou funkci a převede rozprostřený signál do klasického úzkopásmového signálu se kterým potom pracuje.

2.4.2 Typy rozprostřeného spektra

Fyzická rádiová vrstva 802.11 předepisuje tři různé techniky rozprostřeného spektra.

Frekvenční skoky (Frequency hopping, FHSS)

Použitím metody FHSS je pásmo rozděleno na 75 dílčích kanálů o šířce 1MHz. Zbylých cca 4,5 MHz slouží jako ochranné pásmo proti interferencím z vedlejších frekvenčních pásem. Vysílač a přijímač se shodnou na přenosovém vzorci a data jsou poslána přes tuto sekvenci dílčích kanálů. Každá konverzace uvnitř sítě se provádí pomocí jiné sekvence dílčích kanálů která je navržena tak, aby se minimalizovala pravděpodobnost, že dva odesílatelé použijí stejný kanál.

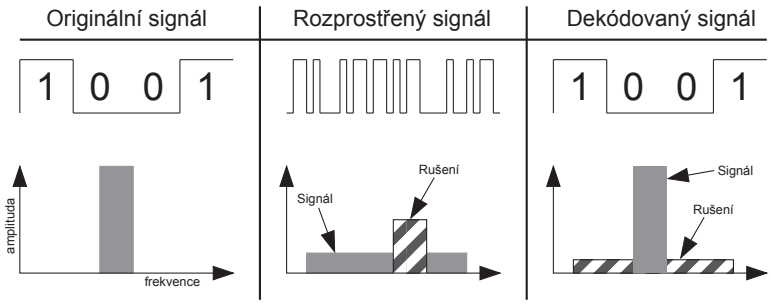


Obrázek 4: Princip FHSS

Jednou z hlavních výhod FHSS je větší počet systémů pracujících najednou v pásmu 2,4GHz. Teoreticky je to až 26 přístupových bodů najednou.

Přímá sekvence (Direct Sequence, DSSS)

Narozdíl od FHSS, DSSS dělí pásmo na 3 kanály po 22Mhz. Data jsou poslána pouze přes jeden z kanálů. Pro kompenzaci šumu v daném kanálu se používá technika "chipping". Každý datový bit je převeden na redundantní sérii bitů zvaných "chips". Po přijetí této série přijímač inverzním postupem příslušná data dekóduje a dále pak zpracovává. Nadbytečnost dat spolu s šířkou kanálu 22Mhz umožňuje kontrolu chyb a jejich korekci což minimalizuje potřebu opětovných přenosů a tím se zvýší i propustnost sítě.



Obrázek 5: Princip DSSS

Ortogonální frekvenční multiplex (Orthogonal Frequency Division Multiplex, OFDM)

Systémy s ortogonálním frekvenčním multiplexem rozdělí přenosové pásmo na velké množství úzkých kanálů. Data se po těchto kanálech přenášejí paralelně a relativně malou rychlostí. Výsledná přenosová rychlost je pak dána součtem rychlostí jednotlivých kanálů. Vzhledem k malé přenosové rychlosti kanálem je signál mnohem robustnější. Tohoto systému využívá v pásmu 2.4GHz například specifikace IEEE 802.11g a v pásmu 5GHz IEEE 802.11a.

2.4.3 Vylepšení fyzické vrstvy specifikací 802.11b

Klíčový přínos specifikace 802.11b je standardizace fyzické vrstvy pro podporu dvou nových přenosových rychlostí 5.5Mbps a 11 Mbps. Pro tyto rychlosti musela být vybrána technika DSSS protože jak bylo uvedeno výše FHSS nepodporuje rychlosti vyšší než 2 Mbps. Důsledkem toho je problém s nekompatibilitou zařízení se specifikací 802.11b a zařízení podle standardu 802.11 pracující se systémem FHSS.

DSSS standard specifikuje 11ti bitový chipping nazývaný Baker sekvence pro kódování posílaných dat. Každá tato sekvence reprezentuje jeden datový bit, který je převeden na časový průběh signálu nazývaný "symbol" který může být poslán bezdrátovou cestou. Tyto symboly jsou přenášeny rychlostí 1 MSps (1 milion symbolů za sekundu) dvoustavovým

klíčováním fázovým posuvem (BPSK). V případě přenosové rychlosti 2Mbps je klíčování důmyslnější a je prováděno čtyřstavově (QPSK).

Pro zvětšení přenosové rychlosti specifikace 802.11b se používají zdokonalené šifrovací techniky. Spíše než dvě Baker sekvence specifikuje 802.11b doplňkový šifrovací klíč (CCK) který se skládá ze souboru 64 osmibitových kódových slov. Tyto kódová slova mají takové matematické vlastnosti, že je přijímač dokáže od sebe bezpečně odlišit a to i v přítomnosti značného šumu. Pro přenosovou rychlost 5.5 Mbps používá CCK 4 bitové kódování a v případě 11 Mbps potom kódování 8 bitové. Pro obě rychlosti se používá technika QPSK a přenosová rychlost 1.375 MSps.

Pro prostředí s velkým rušením a pro větší dosah používají sítě 802.11b dynamic rate shifting, což je automatické přizpůsobení přenosové rychlosti ke kompenzaci rušivých vlivů na kanál. V ideálním případě se stanice spojí plnou rychlostí 11Mbps. Nicméně, když se zařízení pohybuje mimo ideální dosah nebo se ocitne v prostředí s větším rušením sníží se přenosová rychlost na 5.5, 2 nebo 1 Mbps. V opačném případě pokud se podmínky pro přenos zlepší přenosová rychlost se opět zvýší na maximální možnou mez. Rate shifting je mechanizmus fyzické vrstvy a je transparentní vzhledem k uživateli i k vyšším vrstvám.

2.4.4 Radiové frekvence

V dnešní době jsou ve standardu 802.11 definovány dvě frekvenční pásma a to 2.4GHz a 5GHz. Zatímco pásmo okolo frekvence 5GHz není celosvětově sjednoceno a vedou se spory mezi americkým a evropským regulátorem, pásmo okolo frekvence 2.4GHz nebo alespoň jeho části jsou globální a až na různé specifika použitelné na celém světě. Jak to vypadá konkrétně ukazuje následující tabulka:

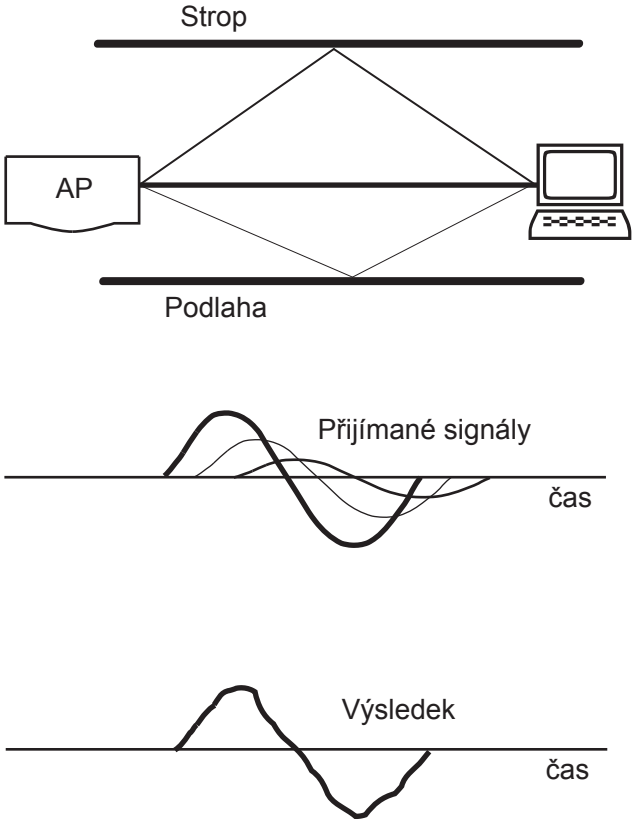
Země	**Kanály (frekvence)**
USA a Kanada	1 - 11 (2.412 - 2.462)
Evropa mimo Francie a Španělska	1 - 13 (2.412 - 2.472)
Francie	10 - 13 (2.457 - 2.472)
Španělsko	10 - 11 (2.457 - 2.462)
Japonsko	14 (2.484)

Jak již bylo řečeno, technologie rozprostřeného spektra vysílá do frekvenčního rozsahu 22MHz zatímco odstup mezi kanály je pouhých 5MHz. Z toho plyne, že vysílání na jednom kanálu se překrývá s vysíláním na sousedních čtyřech kanálech. To znamená, že pokud chceme provozovat dva přístupové body najednou, musíme je nastavit, aby pracovaly minimálně pět kanálů od sebe. Z tohoto zjištění plyne, že ani oněch 13 kanálů, které jsou vyhrazeny pro provoz v České republice není zase tak mnoho jak by se mohlo zdát.

2.4.5 Interference signálu

Problémem u rádiového signálu a to zejména v uzavřených prostorách je ten, že se odráží od různých překážek jako jsou zdi, nábytek atd. Protože stanice v rámci BSS používají téměř výhradně všesměrové antény signál od vysílače k přijímači může a téměř vždy putuje po

více přenosových cestách. Takové cesty jsou různě dlouhé a vzhledem ke konečné rychlosti šíření signálu ke svému cíli putují různě dlouhou dobu. Celý princip znázorňuje následující obrázek:



Obrázek 6: Interference signálu v uzavřené místnosti

Jelikož přenosový signál zde představuje elektromagnetické vlnění a to má tu vlastnost, že se skládá, je výsledný signál vlastně složením všech signálových cest včetně jejich zpoždění.

Časový rozdíl mezi přijetím prvního a posledního signálu z vysílací stanice se nazývá rozprostřené zpoždění (spread delay). Takovýto časový rozdíl nabývá hodnot řádově nanosekund. Zařízení pracující podle standardu 802.11 se dokáží vypořádat se zpožděním cca 500ns. To je krajní hodnota a nemůžeme zde očekávat žádné závratné rychlosti. Pokud je zpoždění větší, nelze takovou síť realizovat. Pro plnou rychlost (11 Mb/s) se udává zpoždění maximálně okolo 65ns. Se vzrůstající dobou pak klesá přenosová rychlost.

2.4.6 Podvrstvy PLCP a PMD

Pokud se podíváme ještě podrobněji na fyzickou vrstvu, zjistíme, že se skládá ze dvou podvrstev

- protokol konvergence fyzické vrstvy (Physical Layer Convergence Procedure, PLCP)
- podvrstva závislá na volbě fyzického média (Physical Medium Depend, PMD)

PMD se stará o přenos bitů od vrstvy PLCP pomocí antény do etheru. Podstatě se stará o kódování přenášení dat výše zmíněnými principy

PLCP tato vrstva představuje spojení mezi přenášenými rámci MAC vrstvy a přenosovým médiem. Vzhledem k tomu, že právě ona určuje jak se tato data budou přenášet (jaká se použije modulace ...) umožňuje tak MAC vrstvě být nezávislou na druhu přenosu. Kromě toho také informuje MAC vrstvu o tom, zdali je přenosové médium k dispozici a tím páde zdali se mohou připravená data vyslat

Struktura PLCP podvrstvy

Standard 802.11 definuje dvě přípustné struktury podvrstvy PLCP. A to dlouhou a krátkou preambuli. Dlouhou preambuli musí podporovat všechny systémy, zatímco krátká slouží ke zvětšení propustnosti sítě zejména při hlasových a videopřenosech. Formát PLCP rámce se skládá z již zmíněné preambule a hlavičky.

1.PLCP preambule

- synchronizační pole obsahující u dloulé preambule 128 bitů a u krátké 56 bitů
- oddělovač začátku rámce (Start Frame Delimiter, SFD) Používá se pro označení počátku každého rámce

2.PLCP hlavička

- 8 bitů pro určení datové rychlosti (Data Rate, DR) Informuje jak rychle jsou data přenášena
- 8 bitů vyhrazeno pro další použití
- 16 bitů informuje o délce přenášených dat, tedy o délce MAC rámce
- 16 bitů CRC kód, jedná se o kontrolní součet pro vyloučení chyb. Jeho úlohou je vyloučit chybu v PLCP hlavičce

Aby se předešlo problémům se zpětmou kompatibilitou, přenáší se celý PLCP rámec rychlostí 1 Mb/s. Proto 802.11b dosahuje v nejlepším případě 85% fyfické vrstvy

2.5 Spojová vrstva a MAC vrstva

Spojová vrstva u standardu 802.11 sestává ze dvou částí. Logical Link Control (LLC) a Media Access Control (MAC). Vrstva LLC je shodná se standardem 802.2, má 48 bitové adresování stejně jako další sítě standardu 802. Tato skutečnost umožňuje velmi jednoduché přemostění do ostatních klasických sítí. Vrstva MAC je ovšem odlišná a specifická pro tento typ sítě. Pro robustnost MAC podvrstvy jsou důležité dvě hlavní vlastnosti.

- kontrolní součet CRC
- fragmentace paketů

Každý přenášený paket je opatřen CRC součtem aby se zamezilo poškození při přenosu resp. aby se toto poškození bezpečně odhalilo.

Fragmentace paketů slouží k rozdělení velkých paketů na menší části a to z důvodu poruchy během přenosu kde by opakované přenášení celého paketu zbytečně síť zatěžovalo. Vzhledem k tomu, že náchylnost oproti metalickému přenosovému médiu je podstatně větší, ušetří se tím mnoho kapacity sítě. A v neposlední řadě pravděpodobnost vzniku poruchy narůstá s velikostí přenášeného paketu.

2.5.1 Mezirámcové mezery

Podobně jako u Ethernetu hrají i zde mezirámcové mezery velikou roli. Slouží totiž ke koordinaci přístupu k přenosovému médiu. Standard 802.11 definuje čtyři typy mezirámcových mezer.

Short interframe space (SIFS) nejkratší mezirámcová mezera sloužící pro bezprostřední odpovědi (ACK,CTS,...)

Point coordination function IFS (PIFS) mezirámcová mezera střední délky používaná pro výzvy. Ta má přednost před normálním provozem a když chce stanice poslat něco urgentně může to učinit po PIFS a předběhnout tak ostatní.

DCF interframe space (DIFS) nejdelší mezirámcová mezera zaručuje minimální prostoj při soupeření anonymních rámců

Extended interframe space (EIFS) nejedná se fixní interval a používá se pouze tehdy pokud nastala chyba v přenosu rámce

Koordinace přístupu k médiu

Aby bezdrátové sítě mohly vůbec fungovat, musí se vyřešit jeden základní problém. A to jakým způsobem bude probíhat provoz na přenosovém médiu v případě pokud bude chtít vysílat několik stanic najednou. Pokud by toto nebylo nijak ošetřeno docházelo by k častým kolizím a znemožňovalo by to provoz sítě. Standard 802.11 definuje dvě funkce pro koordinaci přístupu k médiu.

- Funkce distribuované koordinace DFC (Distributed Coordination Function) je základem standardního přístupového mechanismu CSMA/CA a je u bezdrátových sítí široce používána
- Funkce koordinace jedním bodem PFC (Point Coordination Function) je pro aplikace blízké reálnému času jako je např. přenášení videa. Během doby kdy je systém v PCF módu přístupový bod vyzívá každou stanici jestli nemá připravená data a po daném čase přistupuje k další. Žádná stanice v tomto případě nemá právo vysílat dokud na ní nepřijde řada a není k tomu vyzvaná. Výhodou tohoto způsobu komunikace je skutečnost, že pokud přístupový bod přistupuje k jednotlivým stanicím popořadě a jen po určitý přesně definovaný čas je zaručena maximální latence. Naopak pokud stanice potřebuje okamžitě komunikovat tak nemůže a musí čekat až na ni přijde řada ikdyž ostatní stanice zrovna komunikovat nechtějí. Toto zpoždění může být zejména u rozsáhlých sítí značné. V současné době je velmi málo rozšířen.

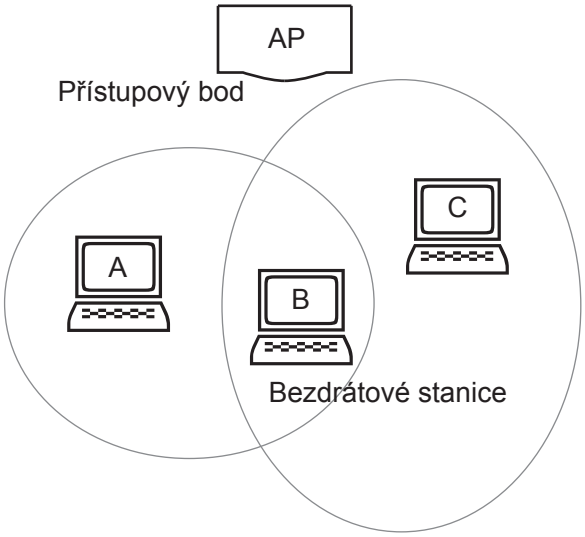
2.5.2 CSMA/CA a problém skrytého uzlu

Vrstva MAC je v zásadě velmi podobná s 802.3 v tom, že je navržená pro více uživatelů na jednom sdíleném přenosovém médiu kdy zařízení které vysílá před zahájením přenosu poslechne zda na médium nevysílá už někdo jiný. U Ethernetové sítě (802.3) protokol CSMA/CD (Carrier Sense Multiple Access with Collision Detection) řídí jak stanice přistupují k přenosovému médiu a jak řešit kolize které se vyskytnou při současném pokusu o komunikaci dvou nebo více stanic. V bezdrátových sítích 802.11 není detekce kolizí možná kvůli jevu zvanému "blízký / vzdálený" problém. Pro detekci kolize musí stanice v jednom okamžiku vysílat a přijímat, ale rádiová část pokud vysílá tak ztrácí schopnost přijímat a tím odhalit kolizi.

Pro vyřešení tohoto nedostatku používá 802.11 mírně upravený protokol známý jako Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) nebo Distributed Coordination Function (DCF). CSMA/CA se pokusí vyvarovat kolizím použitím jednoznačného paketového potvrzení (ACK) což znamená, že přijímací stanice vyšle ACK paket jako potvrzení, že datový paket došel v pořádku.

CSMA/CA funguje následovně. Pokud stanice chtějí vysílat a není detekovaná žádná aktivita stanice čekají ještě další náhodný časový úsek a pokud po jeho uplynutí stále není žádná aktivita stanice začne vysílat. Jestliže je paket přenesen v pořádku, stanice která ho přijme vyšle zpět ACK rámec. Stanice, která vysílá ho přijme a dokončí přenos. Jestliže ovšem ACK rám není přijat buď z důvodu, že datový paket nedorazil v pořádku nebo je poškozen důsledkem kolize stanice počká opět náhodnou dobu a pokusí se vyslat data znovu.CSMA/CA tak poskytuje způsob vzduchu jako sdíleného média. Nicméně tento způsob poskytuje nižší výkon, než ekvivalentní síť Ethernet.

Další problém v bezdrátové sítí je takzvaný "hidden node" problém ve kterém stanice na opačné straně AP můžou registrovat aktivitu z tohoto AP, ale už ne od sebe navzájem díky vzájemné vzdálenosti. Proto 802.11 specifikuje v MAC vrstvě nepovinný protokol Request to Send / Clear to Send (RTS / CTS). Pokud je protokol povolen stanice vyšle RTS a čeká na AP až jí odpoví CTS. Protože AP poslouchají všechny stanice v síti tak jim CTS řekne že někdo komunikuje a ony odloží přenos do té doby než bude AP schopen s nimi komunikovat.

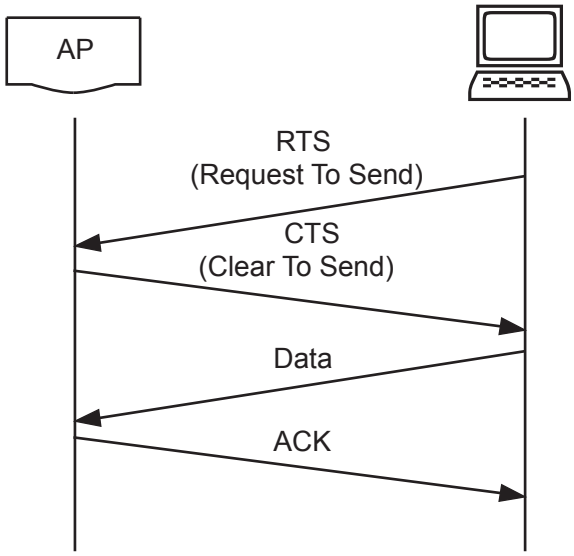


Obrázek 7: Princip vyniku hidden node

MAC vrstva poskytuje ještě další dvě vlastnosti, které mají za účel zvýšit odolnost proti poruchám. Kontrolní součet CRC a paketová segmentace. Každý paket obsahuje vypočítaný CRC součet, který zajišťuje že data nebyla během přenosu poškozena. Paketová segmentace umožňuje veliké pakety rozdělit a přenášet po částech což je velmi užitečné zejména v prostředí kde je veliký provoz a dlouhé pakety by tak byly náchylnější na poruchy a kolize. Tato technika výrazně snižuje potřebu opakovaných přenosů a tím zvyšuje propustnost sítě. Vrstva MAC je také zodpovědná za opětovné poskládání paketu a dělá to transparentně vůči protokolům vyšší úrovně.

2.6 Řízení spotřeby

Kromě řízení přístupu k médiu obsahuje MAC vrstva i systém řízení spotřeby který se používá hlavně u přenosných zařízení. Standard podporuje dva napájecí módy a to Continuous Aware a Power Save Polling mód. V prvním případě je vysílač vždy zapnutý zatímco ve druhém je ve stavu spánku do té doby dokud pro ni nemá přístupový bod připravena data. Stanice rádiovou část pravidelně zapíná po přijetí signálu z přístupového bodu. Tento signál obsahuje informaci o tom, pro kterou ze stanic má připraveny data. Ta se následně probudí, přijme tato data a pak se opět vrátí do sleep módu.



Obrázek 8: Předcházení kolizím

2.7 Formát MAC rámce

Rámec sestává z MAC hlavičky, která obsahuje informace o přenášených datech a těla rámce obsahujícího samotná přenášená data spolu s kontrolním součtem CRC.

Hlavička rámce obsahuje:

Frame control (FC) informace o verzi protokolu a typu rámce (řídící, datový nebo kontrolní)

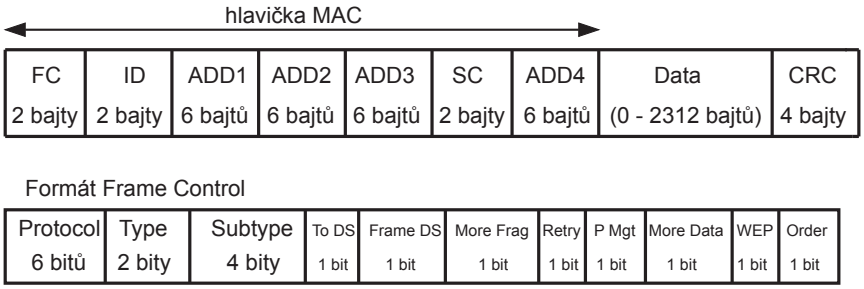
Duration/ID (ID) Station ID je identifikátor stanice používaný pro funkci úspory energie a Duration Value je délka trvání rámce používaná pro výpočet rezervace přenosového média pomocí Network Allocation Vector (NAV)

Adress field 1-4 jsou čtyři adresní pole obsahující adresy zdroje, cíle, přenašeče a přijímače v závislosti na poli Frame Control

Sequence Control používá se pro defragmentaci a likvidaci duplikátních rámců

Jednotlivá políčka MAC rámce jsou zřejmá a popsaná výše. Zajímavá je ovšem struktura políčka Frame Control, které obsahuje důležité informace o vlastnostech rámce.

- Protocol indikuje verzi standardu 802.11
- Type a Subtype indikuje obsah rámce. Jednotlivé typy jsou Řídící (management), Ovládací (control) a Datový (Data), Subtypy pak mohou být RTS, CTS, ACK atd.



Obrázek 9: Formát MAC rámce

- To DS je nastaveno na 1, pokud je rámec posílán do distribučního systému
- From DS je nastaveno na 1, pokud je rámec přijímán od distribučního systému
- More Fragment je nastaveno na 1 pokud byl přenášený rámec rozdělen na více částí přenášených samostatně
- Retry oznamuje, že jde znovuvysílání již vysílané části rámce. Přijímač tak pozná duplicitu rámce.
- Power Management je režim úspory energie v němž se bude stanice nacházet po přenesení rámce.
- More Data oznamuje, že je ve vyrovnávací paměti pro tuto stanici uloženo více dat
- WEP indikuje, že tělo rámce je kódováno algoritmem WEP
- Order indikuje, že rámec je odesílán službou Strict-Ordering, tedy nebude dále zpracováván.

2.8 Bezpečnost

Bezdrátová síť má oproti klasické drátové síti jednu podstatnou nevýhodu, která vychází přímo z jejího principu. Zatímco u drátové sítě je její odposlouchávání dosti komplikované neboť bychom se museli dostat přímo ke kabelu u bezdrátové sítě nelze přesně vymezit prostor ve kterém lze signál přijímat. Proto je zde otázka bezpečnosti velice důležitá a můžeme ji rozdělit do dvou hlavních skupin.

šifrování tedy zabespečení přenášených dat před odposlechnutím

autorizace tedy řízení přístupu oprávněných uživatelů

2.8.1 Šifrování přenášených dat

Aby byly WiFi sítě důvěryhodné a mohlo dojít k jejich masovému rozšíření byla už přímo do standardu 802.11 zahrnuta možnost šifrovat provoz.

WEP-Wired Equivalent Privacy

Ve WiFi sítích se o zabezpečení stará WEP což je standard pro zabezpečení rádiové části sítě. To znamená, že zabezpečuje přenos jen na mezi stanicí a přístupovým bodem. Pokud je přístupový bos připojen na nějakou lokální síť, nebo dokonce na internet musí se dále bezpečnost řešit dalším způsobem. Standard WEP používá jako šifru symetrickou streamovou šifru RC4, tedy šifru s tajným klíčem. Pro šifrování a dešifrování klíč expanduje podle určitých pravidel na délku jakou má samotná zpráva a pak je pomocí operace XOR zpráva zašifrována resp. rozšifrována. Obě zařízení mezi nimiž komunikace probíhá musejí pak znát jednak klíč a jednak ona pravidla podle kterých klíč expanduje. Standard ovšem neřeší distribuci takového klíče a je na výrobci jak to ošetří. WEP definuje délku klíče na 40 bitů což není mnoho. Někteří výrobci používají vlastní šifry dlouhé 128 bitů a nebo i 256 bitů. Problém je v tom, že takto Dlouhé klíče nejsou standardizovány a může tedy nastat problém se vzájemnou kompatibilitou.

2.8.2 Autentizace

Druhou důležitou součástí bezpečnostní strategie je řízení přístupu do sítě, tedy autentizace uživatele. U kabelových sítí je situace opět podstatně jednodušší. Pokud nechceme aby se někdo připojoval do sítě tak jednoduše omezíme přístup do určitých prostor.

Protože jak je výše zmíněno nemůžeme u bezdrátových sítí vymezit jejich přesný rozsah musíme řešit otázku kdo k ní přistupovat může a kdo nikoliv. Autentizace ve standardu 802.11 je obecně jednosměrný proces. To znamená, že zatímco stanice se při přístupu k přístupovému bodu musí autentizovat opačně to neplatí. Přístupový bod se při pokusu o spojení se stanicí autentizovat nemusí což působí občas problémy s bezpečností.

Standard 802.11 definuje dvě metody autentizace

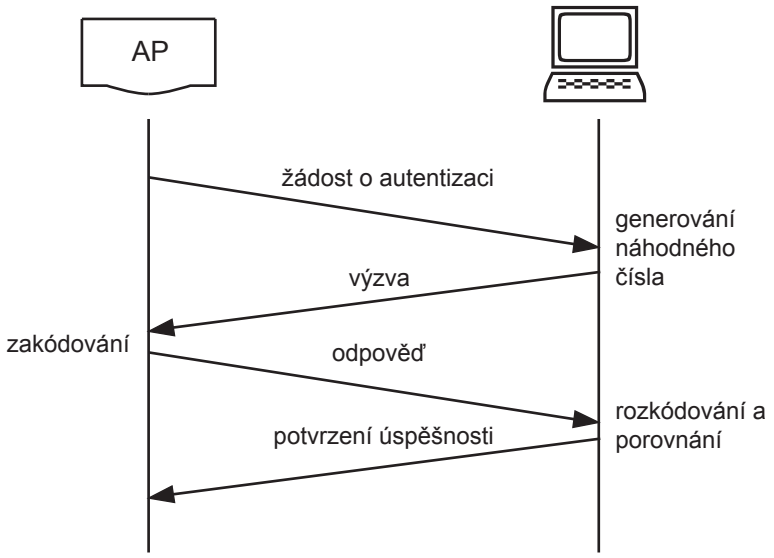
- open system autentizace
- shared-key autentizace

Open-system autentizace

Tato metoda spočívá v tom, že přístupový bod přijme stanici na základě informací, které mu sama poskytne. Taková stanice se identifikuje prostřednictvím SSID (Service Set Identifier). Pokud ale přístupový bod své SSID vysílá, tak není problém ho odchytit a vzápětí se s ním autentizovat pro přístup k síti. Z výše uvedeného je zřejmé, že tato metoda není zrovna nejbezpečnější a proto se v praxi moc nepoužívá.

Shared-key autentizace

V případě této autentizace je nutné použít také WEP. Standard 802.11 vyžaduje, aby každé zařízení s implementovaným WEP bylo také schopno užívat autentizaci sdíleným klíčem.



Obrázek 10: Shared-key autentizace

Jak je zřejmé z názvu, autentizace se zde provádí pomocí klíče. Tento klíč musí být známý každému zařízení, které chce přistupovat do sítě. Samotné ověřování probíhá následovně. Přístupový bod odešle náhodné číslo zakódované pomocí daného klíče stanici, ta ho opět použitím klíče dekóduje a pošle zpět pokud se obě čísla shodují, umožní přístupový bod stanici přístup do sítě.

3 Hardwarové řešení ovládací jednotky

Diskuse hardware ovládací jednotky
Hardware musí splňovat následující požadavky:

- Dostatečný výpočetní výkon pro ovládání WiFi rozhraní
- Dostatečný počet I/O pro ovládání funkčních částí pračky

Další hlediska:

- Snadnost vývoje SW (Dostupnost IDE a kompilátoru pro vyšší programovací jazyky)
- Snadnost vývoje HW

Po zvážení všech hledisek jsem se rozhodl pro jednočipový mikrokontroler PIC 18F452 a jeho implementaci ve vývojové desce Chipweb ER25. Mikrokontroler je pro tuto aplikaci dostatečně rychlý a ve vývojové desce je již zapojen s konektorem pro osazení WiFi PCMCIA karty.

3.1 Popis hardware ovládací jednotky

3.2 Vývojová deska ER25

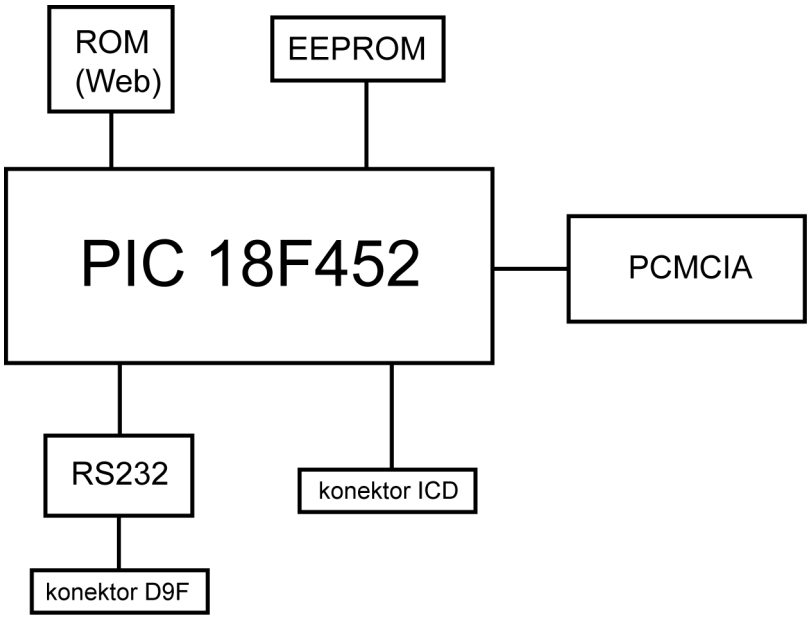
Pro hardwarovou realizaci jsem použil vývojový kit, který je osazen procesorem od firmy Microchip. Jedná se o modelovou řadu PIC18Fxxx, která svým výkonem dostačuje pro použití se standardem 802.11b. Zároveň se jedná o velmi úsporný mikroprocesor a proto je vhodný zejména pro mobilní bateriově napájená zařízení což podtrhuje i funkce automatické kontroly napájecího napětí. O pracovní frekvenci se stará externí oscilátor, který má frekvenci 20MHz a mikroprocesor s ním dosahuje výkonu 5 MIPs.

Na desce se kromě bezdrátového rozhraní nachází také rozhraní sériové a celý obvod je navržen tak, aby bylo možné Mikroprocesor pomocí něj programovat přímo v zapojení.

Jak jsem se zmínil hlavní a podstatnou částí celé vývojové desky je rozhraní podle standardu 802.11b, které je zajišťováno prostřednictvím běžné PCMCIA karty.

Celé zařízení je napájeno napětím 9 voltů s maximální spotřebou 500mA. Vzhledem k tomu, že dnes není problém sehnat akumulátory velikosti AA o kapacitě převyšující 2500mAh potom si myslím, že deska napájená z článku složeného z těchto baterií vydrží poměrně dlouho a pro řízení modelu v laboratorních podmínkách. Pro ještě větší výdrž a dobu provozu může mikroprocesor pokud není využívána vypínat PCMCIA kartu pomocí rozhraní 802.11b.

K vývojové desce je přiložen i obslužný open source software psaný v jazyce C který obsahuje předem napsané a odladěné knihovny. Jsou zde přeprogramovány kódy s nimiž může deska pracovat v obou typech sítí a to jak Ad-hoc tak i Infrastructure, což nám dává široké možnosti použití např. ovládání modelu ze vzdáleného počítače přes internet. Dále jsou zde knihovny pro podporu WEP zabezpečení 64-bitovým a nebo dokonce 128-bitovým klíčem. Dále je zde možnost spustit na mikroprocesoru aplikaci WebServer, která nám umožní konfigurovat zařízení přes bezdrátové rozhraní. Samozřejmě nechybí zde ani podpora běžných síťových protokolů jako jsou IP, UDP, TCP, HTTP a DHCP.



Obrázek 11: Blokové schema vývojové desky

3.3 Popis napojení na jednotlivé prvky

Na vývojové desce jsou vyvedeny následující piny procesoru:

Konektor	Piny
J4	RB6 - RB7
J6	RA0, RB0 - RB7, RC0 - RC1, RE0 - RE1
J7	RC3 - RC5, Vdd, GND
J4	je využit pro In - Circuit Debugging/Programming

Piny jsem jednotlivým funkčním částem pračky přidělil takto:

Vstupy

RC0 Termostat

RC3 Start programu

RC4 Kontakt dveří bubnu

Výstupy

RB0 Spínač motoru

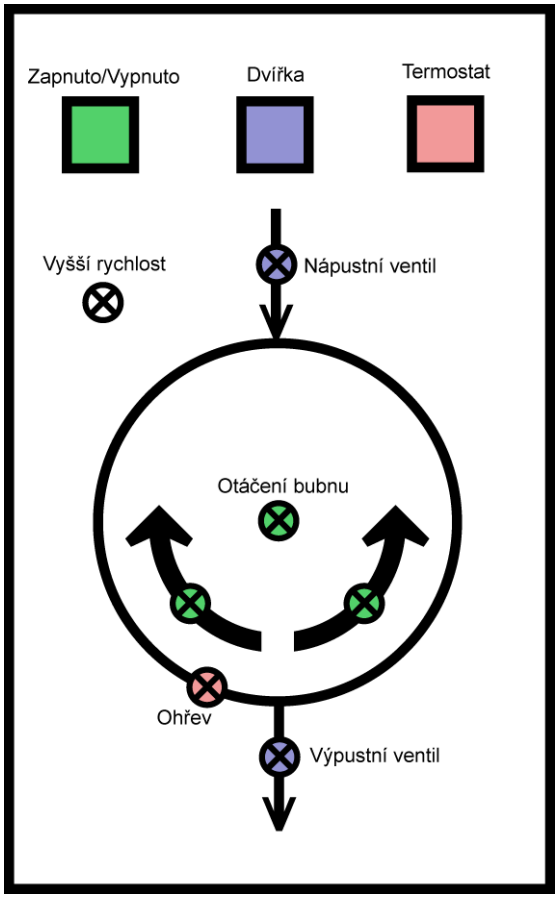
RB1 Směr rotace motoru

RB2 Rychlost rotace motoru

RB3 Topné těleso

RB4 Nápustní ventil

RB5 Výpustní ventil

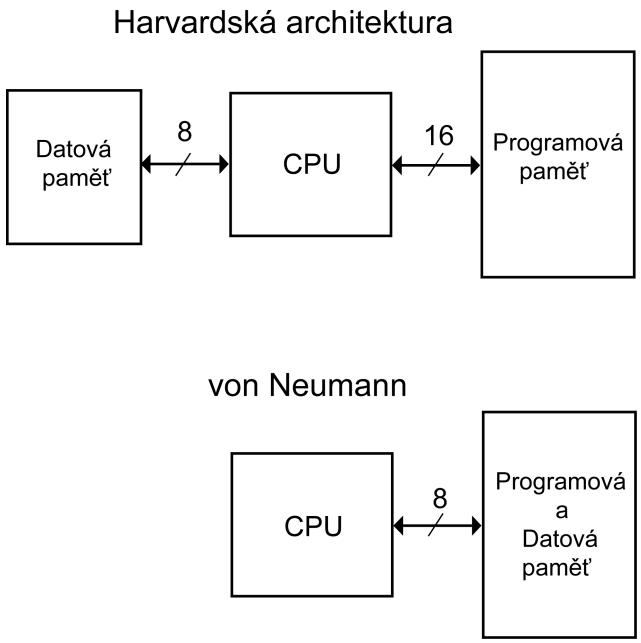


Obrázek 12: Schematické znázornění reálného modelu pračky

Hardwarová realizace na skutečné pračce by tedy vypadala takto: Čtyř-žilový kabel vede z konektoru J7 na panel pračky ke dveřím bubnu a spínači Start. Uvnitř pračky je konektor J6 (resp. výše zmíněné piny) připojen na reléové pole, přes které jsou ovládány příslušné funkční části pračky.

3.4 Architektura PIC18F452

Tento obvod je postaven na Harvardské architektuře, což znamená, že má pro datovou a programovou paměť dvě oddělené a nezávislé sběrnice. Tento fakt mu dovoluje daleko rychleji připravovat data a tím i vykonávat instrukce oproti standardní von Neumannově architektuře kde paměťová i datová sběrnice používají stejnou sběrnici. To znamená, že pro provedení jedné instrukce musí v případě von Neumanna několikrát přistupovat na sběrnici, aby dostal požadovaná data. To může mít za následek velikou vytíženost sběrnice a pokles na výkonu. U Harvardské architektury se vše odehrává v jednom cyklu, protože paměťová i datová paměť mohou být zpřístupněny v jeden okamžik. Protože jsou sběrnice oddělené a navzájem na sobě



Obrázek 13: Harvardska architektura

nezávislé, mohou mít také rozdílnou datovou šířku. Zatímco datová sběrnice má standardní šířku 8 bitů programová je rozšířena na 16 bitů, což jí dovoluje přenášet dlouhé dvoubajtové instrukce v jednom hodinovém cyklu.

3.4.1 CPU a ALU

Central Processing Unit (CPU) je odpovědná za zpracování instrukcí v programové paměti. Avšak mnoho instrukcí operuje i s datovou pamětí. Pro takovéto operace je zde Arithmetic Logical Unit (ALU). Kromě toho, že vykonává aritmetické a logické operace stará se také o práci se STATUS registrem kde nastavuje různé příznaky v závislosti na výsledku prováděných instrukcí.

Central Processing Unit (CPU)

CPU může být považováno za mozek celého mikrořadiče. Je zodpovědný za přísun odpovídajících instrukcí pro zpracování, jejich dekódování a následné zpracování. Někdy, zejména u aritmetických a logických operací úzce spolupracuje s ALU. Ovládá také programovou i datovou sběrnici a přistupuje na stack.

Arithmetic Logical Unit (ALU)

Mikrořadič obsahuje také 8 bitovou ALU a 8 bitový pracovní registr (WREG). ALU je univerzální aritmeticko-logická jednotka vykonávající booleovské operace mezi pracovním registrem a libovolným datovým registrem.

3.4.2 Organizace paměti

Mikroprocesor obsahuje tři různé druhy pamětí.

- Programová paměť
- Datová paměť
- Datová EEPROM

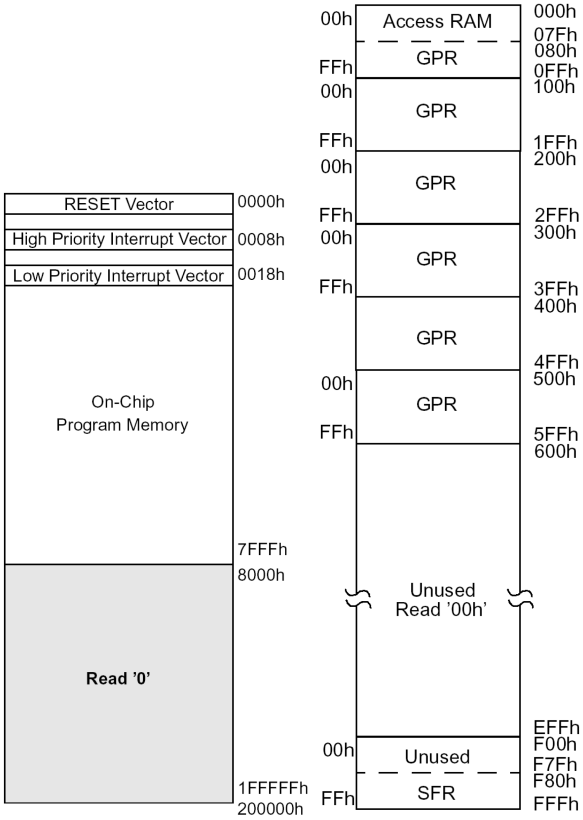
Organizace programové paměti

21-bitový program counter který určuje pořadí vykonávaných instrukcí je schopen adresovat až 2 MB paměti. Data na adresách jež převyšují fyzickou kapacitu paměti jsou čtena jako 0. PIC18F452 má 32 KB a ta dokáže pojmout až 16K jednoduchých instrukcí. Na začátku bloku programové paměti jsou umístěny postupně Reset vektor (0000h) pak následují vektory přerušení podle priority (0008h - 0018h) a potom už jen vlastní program.

Organizace datové paměti

Datová paměť je implementovaná jako statická z důvodu rychlosti, neboť jsou zde umístěny registry. Každý registr má 12-bitovou adresu která dovoluje adresovat až 4096 bytů paměti. Tato paměť je rozdělena na 16 "bank" a každá obsahuje 256 bytů. Dolní 4 bity adresy jsou pro výběr banky, horní 4bity nejsou implementovány a zbylé slouží k adresování registrů.

Ty se podle funkce dělí na dvě základní skupiny Speciál Function Registers (SFR) a General Purpose Registers (GPR). SFR registry začínají na adrese 0xFFF a slouží k nastavování a sledování činnosti mikroprocesoru a periferií kdežto GPR jsou volné blíže nespecifikované registry sloužící k odkládání dat uživatelského programu a začínají na začátku banky 0. Datová paměť může být adresována buď přímo a nebo nepřímo. Přímé adresování se děle za použití BSR (Bank Select Register)



Obrázek 14: Organizace paměti

Datová paměť EEPROM

Tato paměť slouží pro ukládání různých konstant nebo výsledků měření a má tu výhodu, že v ní zůstanou data uchována i při odpojeném napájecím napětí. Ukládání a čtení dat je odlišné od předchozích typů pamětí neboť není přímo mapovaná jako registry, ale přistupuje se k ní pomocí SFR (speciálních funkčních registrů). Ty jsou dohromady čtyři:

- EECON1
- EECON2
- EEDATA
- EEADR

EEPROM dovoluje číst i zapisovat po celých bytech. Pokud přistupuji k paměti v registru EEDATA jsou přečtená nebo zapisovaná data a do registru EEADR uložím adresu ke které chci přistupovat. Tento mikroprocesor obsahuje celkem 256 bytů datové EEPROM v rozsahu adres 0h až FFh. Zapisovaný byte napřed automaticky smaže původní data a zapíše nová. Čas zápisu je řízen automaticky prostřednictvím vnitřního časovače.

3.4.3 Vstupně - výstupní porty

I/O piny jsou vlastně nejjednodušší periferní zařízení pomocí něhož mikroprocesor ovládá ostatní zařízení. V závislosti na zvoleném nastavení může mít mikroprocesor 3 nebo 5 vstupně výstupních portů. Navíc mohou být některé I/O piny podle nastavení využívány k různým účelům (I/O, A/D, PWM . . .). Vlastnosti a nastavení portů se řídí nastavením následujících registrů:

TRIS registr určuje zda je příslušný pin jako vstup nebo výstup

PORT registr zde se podle konfigurace čtou nebo zapisují data z nebo na vstupní piny

LAT registr slouží k jednorázovému zastavení rychle se měnících dat, aby byl čas je pořádku přečíst jako celek

Registry PORTA, TRISA a LATA

PORTA je 7-pinový I/O port. Pokud se v jemu odpovídajícím registru TRISA nastaví příslušný bit na 1, změní se nastavení příslušného pinu na vstup, jde do vysoké impedance a čeká na vstupní úroveň. Pokud se zde ovšem nastaví hodnota 0, pak se bude jednat o výstup a jeho úroveň se bude řídit podle hodnoty v registru PORTA.

Funkce pinu RA4 je zdvojena a může být použit jako vstup hodinového signálu. Na desce ovšem není vyveden a proto se s ním dále nebudeme zabývat.

Dalším několikaúčelovým pinem je RA5, který se mimo jiné dá použít jako analogový vstup s A/D převodníkem a jeho nastavení se řídí registrem ADCON1. Ale protože ani tento není na desce vyveden, nebudeme se jím také zabývat, což je veliká škoda.

Registry PORTB, TRISB a LATB

PORTB je 8-pinový I/O port. Základní nastavení je podobné jako u PORTA a je vysvětleno výše. Oproti předchozímu portu jsou zde oslabeny vnitřní pull-up rezistory

Piny RB7-RB4 pokud jsou nastaveny jako vstupní mohou být použity jako vstupy pro vnější přerušení při změně hodnoty. Tyto vstupy jsou porovnávány se starou hodnotou a pokud je zjištěna nějaká změna nastaví se příznak přerušení RBIF v registru INTCON0.

Toto přerušení může vzbudit zařízení ze stavu SLEEP, nebo provézt příslušnou proceduru k jeho ošetření. Nakonec se nastaví RBIF bit na hodnotu 0 aby mohl program pokračovat dál. Toto přerušení se používá zejména pro klíčové operace kde je potřeba okamžitě zareagovat na nastalou situaci nebo k probuzení mikroprocesoru.

Dále ještě stojí za zmínku piny RB0, RB1 a RB2. Ty mohou být použity jako vstupy vnějšího přerušení spouštěné náběžnou nebo sestupnou hranou signálu. To na jakou hranu budou reagovat záleží na hodnotě bitu INTEDGx obsaženého v registru INTCON2. Pokud je zde nastavena hodnota 1 reagují na náběžnou hranu a pokud je zde 0 tak na sestupnou. Pokud se na RBx / INTx objeví odpovídající hrana nastaví se odpovídající bit INTxF. Toto přerušení může být zrušeno nastavením odpovídajícího bitu INTxE. Příznakový bit

INTxF zůstane nastaven i po odeznění přerušení a musí být nastaven na 0 pomocí procedury, která ošetřuje příslušné přerušení. Tyto vstupy mohou být také použity pro probuzení mikroprocesoru ze stavu SLEEP.

Priorita přerušení INT1 a INT2 se nastavuje pomocí bitů INT1IP a INT2IP v registru INTCON3. Pro INT0 se žádná priorita nenastavuje, ta je vždy nejvyšší.

3.4.4 Přerušení

O přerušeních zde již při různých příležitostech psáno bylo, ale myslím si, že jde o velmi důležitou funkci mikroprocesoru a proto si myslím, že stojí za shrnutí ve zvláštní sekci. Přerušení se dosti často používají v real-time řízení a proto

Přerušení může vzejít z mnoha zdrojů:

- přerušení z vnějších zdrojů jako jsou vstupy INT, INT1 a INT2
- přerušení při změně signálu na vstupech RB7 - RB4
- přetečení časovačů TMR0 - TMR3
- přerušení od rozhraní USART a to buď v případě že je vstupní buffer plný a nebo naopak výstupní prázdný
- přerušení od synchronního sériového portu (SSP)
- dokončený převod na A/D převodníku
- přerušení od vstupu Compare/Capture/PWM (CCP) v závislosti na funkci
- přerušení od LVD pokud dojde k poklesu napájecího napětí
- od paralelního rozhraní
- od rozhraní CAN

Ostatní zdroje přerušení se mapují do deseti paměťových registrů, které slouží k nastavování a zjišťování stavu přerušení. Jsou to:

- INTCON
- INTCON1
- INTCON2
- INTCON3
- PIR1
- PIR2

- PIE1
- PIE2
- IPR1
- IPR2

Za zmínku stojí registr INTCON a v něm bit GIE/GIEH. Jedná se o Global Interupt Enable bit a slouží ke globálnímu povolení všech přerušení. Pokud bychom chtěli povolit pouze některá uděláme to ve zbytku INTCON, PIR, PIE a IPR registrech. Kde do PIR se ukládají jednotlivé příznaky přerušení, v PIE se přerušení povolují a nakonec v IPR se volí jejich priorita.

Bohužel na vývojové desce ER25 jsou téměř všechna přerušení blokována pro obsluhu PCMCIA karty. Musíme si tedz vystačit s cyklickým čtením vstupů mikrořadiče. Vzhledem k frekvenci na které běží (20MHz) by to pro většinu reálných systémů mělo bohatě stačit.

3.4.5 Časovače

Mikroprocesor PIC18F452 obsahuje čtyři programovatelné na sobě nezávislé časovače. Mezi jejich hlavní rysy patří

- vysoká univerzálnost, mohou se tvářit jako 8-bitové nebo 16-bitové a chováním jako čítače či časovače
- nejen, že je u nich umožněno data číst, ale i do nich zapisovat
- pro volitelnou rychlost čítání jsou vybaveny 8-bitovou předděličkou
- možnost výběru mezi interním, nebo externím signálem
- při přetečení nastaví přerušení
- pro externí signály umožňují volit typ spouštěcí hrany

Podobně jako ostatní moduly mají i časovače své registry pro nastavení výše uvedených vlastností. Zde se o konfiguraci starají bity v registru T0CON

Standardně jsou časovače nastaveny jako 8-bitové čítače. V podstatě ale pořád fungují jako 16-bitové s tím rozdílem, že v 8-bitovém režimu je MSB nastaven vždy na 0. Tuto vlastnost určuje jediný bit v T0CON a to T08BIT. Z toho vyplívá, že snadno za běhu můžeme zdvojnásobit jeho velikost a naopak.

Pokud časovač pracuje v 16-bitovém režimu je potřeba při čtení uložit najednou dva bajty TMRxH a TMRxL. To může být obtížný úkol, neboť když přečteme jeden a přejdeme k druhému, může se stát, že se změní jeho hodnota. Tato záležitost je zde ošetřena tím, že v TMRxH není aktuální hodnota horního bajtu časovače, ale její obraz v době čtení bajtu spodního. To mám umožňuje přečíst celou hodnotu v jednom okamžiku.

U zápisu je to obdobné. Napřed se musí do registru TMRxH zapsat hodnota a následně zapsáním dat do registru TMRxL se do časovače uloží celých 16-bitů.

Režim časovače dostaneme nastavením TxCS na hodnotu 0. V tomto režimu se Timerx inkrementuje každý takt hodinového signálu. Pokud ovšem do registru TMRx zapíšeme nějakou hodnotu inkrementování počká dva hodinové cykly, aby uživatel s tou hodnotou mohl ještě pracovat. V módu čítače se Timetx inkrementuje s náběžnou nebo sestupnou hranou na vstupu TxCLK.

Capture mód

Capture mód úzce souvisí s problematikou časovačů a vzhledem k tomu, že vývojová deska má tento výstup vyveden tak ho zde zmiňuji. Využívá se k přesnému měření časových úseků. V tomto módu se do registrů CCPR1H a CCPR1L zaznamená 16-bitová hodnota jednoho ze dvou čítačů TMR1 nebo TMR2 a to s každou spádovou hranou nebo s každou náběžnou hranou nebo s každou čtvrtou či šestnáctou náběžnou hranou na pinu RC1/CCP2. To na kterou událost se bude hodnota zaznamenávat určí nastavení v registrech CCP2M3 až CCP2M0 v registru CCP2CON. Pokud dojde k zachycení hodnoty, nastaví se příznakový bit CCP2IF v registru PIR2. Tento příznak se po přečtení a zpracování hodnoty musí vymazat. Nová hodnota při dalším zachycení samozřejmě přepíše hodnotu předchozí.

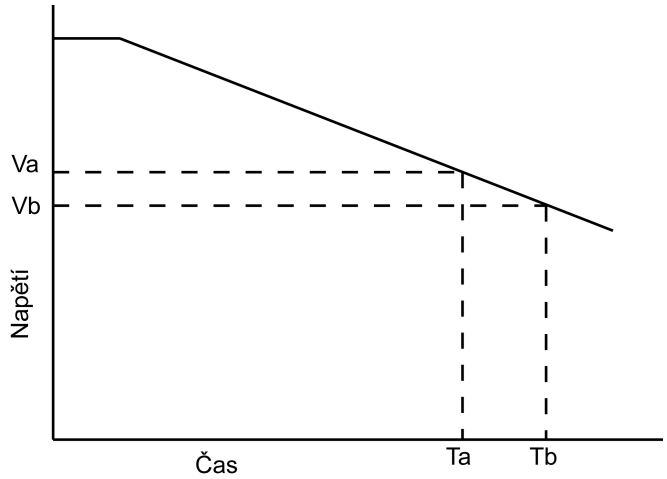
3.4.6 Low Voltage Detect

V případě, kdy je aplikace, pro který je tato deska určena, mobilní a tudíž napájena z baterie, je nutné pro jeho správnou funkci hlídat napájecí napětí. Pro tyto případy je mikroprocesor vybaven modulem zvaným "low voltage detect". Tento modul je softwarově programovatelný a nastavuje se zde mezní hodnota po kterou je zařízení schopno bezchybného provozu. Nemusí to být spodní hranice kde je schopen pracovat mikroprocesor, ale nastaví se hranice nejcitlivější části celého zařízení. Pokud napětí klesne pod určenou hodnotu nastaví se příznak přerušení a mikroprocesor může začít vykonávat příslušnou proceduru vedoucí například k celkovému bezpečnému odstavení systému. Protože se napětí baterie snižuje relativně pomalu vzhledem k rychlosti procesoru není nutné aby byl tento modul stále v provozu. Už pro jeho vlastní spotřebu je optimální, aby se spouštěl v delších intervalech vždy na krátkou dobu jen aby změřil aktuální hodnotu. Tato doba ovšem nesmí být moc krátká a to z toho důvodu aby se obvod stačil stabilizovat.

Na obrázku je vykreslena napěťová charakteristika která se podobá charakteristice reálné baterie. Vlivem zátěže klesá napětí až klesne na hodnotu VA a to způsobí, že se v čase TA generuje přerušení. Toto přerušení způsobí, že se začne vykonávat procedura mající za následek vypnutí celého systému. Napětí VB na obrázku ukazuje minimální provozní napětí celého systému. Rozdíl časů TB-TA je čas potřebný na vypnutí systému.

3.4.7 Watchdog časovač a funkce Sleep

Dalšími velmi užitečnými funkcemi pro práci v mobilním zařízení jsou funkce Watchdog a Sleep . Pokud se mikroprocesor chová tak jak nemá, Watchdog je schopen ho restartovat a tím



Obrázek 15: Průběhy napětí při detekci nízkého napětí

ho vrátit do normálního režimu vykonávání programu. Tato vlastnost samozřejmě přispívá k celkové bezporuchovosti a výkonnosti celého systému. Obzvláště u mobilních zařízení se tato vlastnost zdá být praktická, neboť nemusíme mít zařízení vždy po ruce. Watchdog je nezávislý vnitřní RC oscilátor který běží bez nutnosti jiných externích komponent nebo hlavního oscilátoru. Běží dokonce i když je mikroprocesor ve stavu Sleep.

Pokud mikroprocesor pracuje způsobí přetečení Watchdog časovače reset celého mikroprocesoru a program poběží od začátku. Pokud se ovšem nachází ve stavu Sleep mikroprocesor se vzbudí a pokračuje v normálním režimu dál. WDT může být stále zapnut pomocí konfiguračního bitu WDTEN. Pokud ovšem tento bit nastavíme na nulu, můžeme WDT spouštět a vypínat softwarově bitem SWDTEN.

Funkce Sleep zastaví téměř všechnu aktivitu v mikrokontroleru a sníží jeho spotřebu na minimum. Do tohoto režimu se dostane spuštěním instrukce Sleep a v tomto režimu je spotřeba opravdu hodně malá a výrazně prodlužuje životnost případných napájecích baterií. Vypnou se všechny oscilátory až na oscilátor WDT. Ten se sice vynuluje, ale poběží dál. Co se týče I/O portů, ty se zachovají ve stejném stavu jako před funkcí SLEEP. Pro maximální úsporu energie by však měly být buď na úrovni VDD nebo VSS. Celkové spotřebě ve SLEEP režimu také neprospívá když na výstupech je zařízení, které trvale (i během spánku) odebírá proud. Takové obvody je nutno také vypínat. Co se týče vstupů, které jsou ve stavu vysoké impedance tak ty by měly být buď uzemněny nebo na úrovni napájecího napětí, aby se zabránilo střídajícím se proudům zapříčiněných plovoucími vstupy. Do normálního stavu se pak dostane pokud nastane přerušení (od Watchdog časovače a nebo prostý Reset)

4 Software pro ovládací jednotku a připojené PC

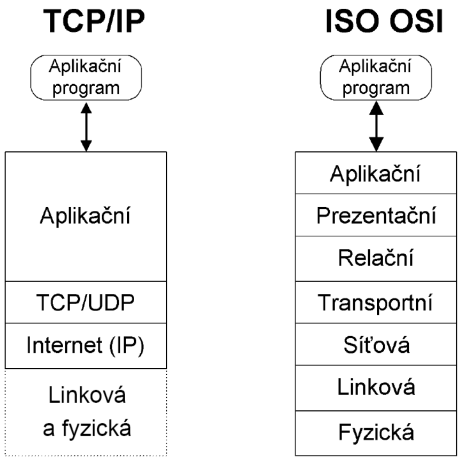
Analýza softwarového řešení Software se skládá ze dvou částí

- Program pro mikrokontroler
- Ovládací program pro PC

Vývojová deska podporuje jak TCP/IP tak i UDP protokol. Rozdíl mezi nimi je z aplikačního hlediska zásadní. Protokol TCP je tzv. spojovanou službou což znamená, že příjemce potvrzuje že obdržel data a jestli jsou v pořádku. V případě ztráty nebo poškození si příjemce vyžádá opětovný přenos chybějící části. Na druhou stranu UDP protokol přenáší data pomocí datagramů a pokud ho vyšle tak už ho nezajímá jestli byl doručen.

Z toho vyplívá, že každý protokol je určen pro jinou aplikaci. TCP/IP se používá pro přenos obrázků či programů, neboť je požadavek aby celý obsah byl doručen v pořádku a je jedno, jak dlouho to bude trvat. V opačném případě např. při poslechu streamů jako jsou např. internetová rádia nebo televize je důležitější včasné doručení dat než je to jestli jsou všechna.

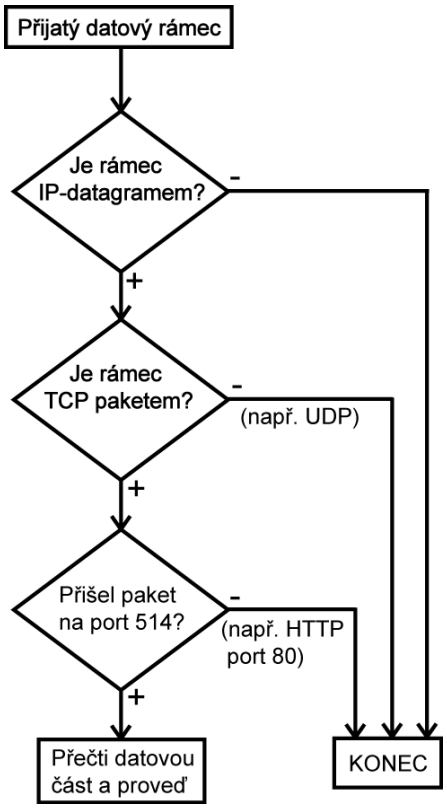
Vzhledem k tomu, že mám požadavek aby model dělal to co se od něj požaduje a nezáleží na tom, jestli se jeho reakce nepatrně zpozdí volil jsem protokol TCP/IP. Protokol TCP/IP



Obrázek 16: Porovnání modelů TCP/IP a OSI

využívá čtyři vrstvy na rozdíl od klasického sedmivrstvého OSI modelu. Na obrázku je vidět jejich vzájemné porovnání. Z těchto čtyř protokol definuje prostřední dvě (Internet(IP) a TCP). Z hierarchického hlediska je pod nimi fyzická a linková (spojovací) vrstva které jsou definovány standardem příslušného přenosového média.

Výhodou protokolu TCP/IP je, že v případě použití jiné technologie řešení spoje, například klasického Ethernetu po kabeláži není nutné vlastní programy přepisovat, upraví se pouze několik direktiv pro překladač. Portfolio produktů Chipweb ER2x zahrnuje například desku



Obrázek 17: Průběh zpracovávání TCP/IP paketu

ER22 která disponuje jak PCMCIA/WiFi rozhraním tak i obvodem RTL8139 a konektorem pro připojení UTP kabelu (Ethernet 10/100Mbps). Aplikace dále popisovaná je proto nasaditelná nejen v prostředí bezdrátových sítí ale lze i s minimálními náklady na vývoj vytvořit aplikaci plně provozovatelnou např. po internetu.

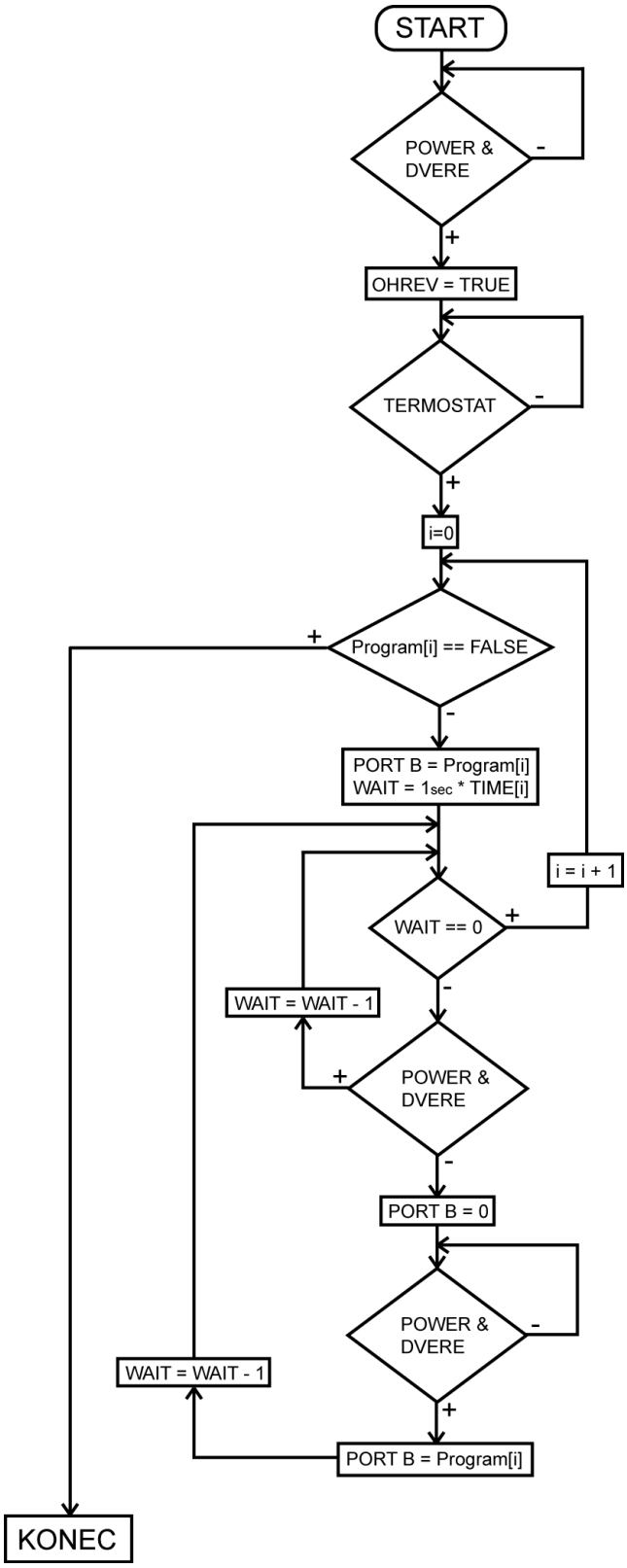
4.1 Program pro mikrokontroler

Program pro mikrokontroler vychází z SDK dodávaného s vývojovou deskou ER25.

Aplikace nahraná v procesoru obsahuje jednoduchý webserver, který zobrazuje stránky uložené v paměti EEPROM, driver pro PCMCIA rozhraní driver pro WiFi rozhraní a jednoduchý IP stack s implementací TCP, UDP a ICMP protokolů. SDK obsahuje zdrojové kódy k těmto komponentům a pár vzorových aplikací.

Algoritmus řízení pračky

Na obrázku je znázorněn vývojový diagram řídícího algoritmu. Jedná se o jednoduchý algoritmus pro ovládání jednoduché pračky který testuje vstupy kterými jsou tlačítko power, kontakt dvířek bubnu a poslední vstup je kontakt termostatu který dává signál správné



Obrázek 18: Vývojový diagram řídícího algoritmu

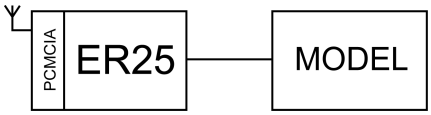
teploty vody. Ty pak vyhodnocuje a nastavuje odpovídající výstupy podle řídícího programu. V poli *Program* jsou jednotlivé činnosti které pračka může provádět a v poli *Time* se nachází hodnota určující čas po který za dodržení vstupních signálů se činnost provádí. Jelikož jsou výstupy na modelu přímo spojeny s jednotlivými bity výstupní brány PORT B hodnoty z pole Program po překopírování na PORT B vytváří bitový obraz určující nastavení výstupů. Rozhodl jsem se navrhnout dvě verze obslužných programů a to:

- přímo řízenou
- autonomní

Ačkoliv jsem je navrhl pro stejný model a to model pračky každá z nich se hodí pro jinou oblast použití.

Autonomní model

Autonomní model je charakteristický tím, že ke svému provozu nepotřebuje spojení s řídícím počítačem. Ten mu pouze zašle řídící paket ve kterém jsou v datové části uloženy parametry prováděného programu (v našem případě program praní). Mikrokontrolér tuto informaci zpracuje a začne provádět příslušný program aniž by vyžadoval jakýkoliv řídící zásah z okolí.



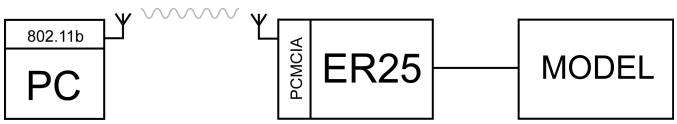
Obrázek 19: Princip autonomního modelu

Tento způsob práce je vhodný pro jednoduché a bezpečné procesy kde může mikrokontrolér automaticky zasahovat. Klíčové hodnoty z řídícího procesu se mohou ukládat v jeho interní paměti EEPROM a následně jednou za určitý čas se připojit a poslat nashromážděná data ke kontrole a případnému zpracování Vzhledem k tomu, že systém pracuje zcela autonomně, není zde zavedena zpětná vazba k řídícímu počítači. Protože mikrokontrolér nepotřebuje komunikovat s okolím, může mít po většinu času vypnutou komunikační PCMCIA kartu a tím výrazně snížit spotřebu a šetřit tím baterie ze kterých by mohl být napájen. Zadání parametrů potřebných pro běh programu se v našem případě děje zasláním paketu v jehož datové části je uložen datagram se strukturou která je zobrazena na obrázku. Datagram je na začátku a na konci ohraničen hodnotami 0x80h což znamená, že jde o řídící datagram a data jsou platná. Ostatní datagramy nejsou zpracovávány a jsou zahozeny hned po jejich přijetí.

Obrázek 20: Datagram s obsahem celé sekvence

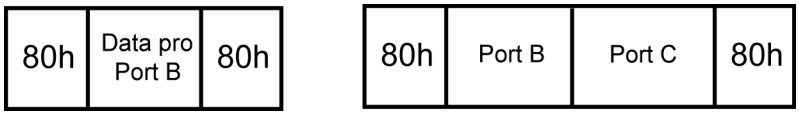
Přímo řízený model

Zcela opačný případ je druhá verze řízení pračky, která je přímo řízená z ovládacího počítače. Zde mikrokontrolér zastává roli jakéhosi prostředníka mezi řídícím počítačem a samotným procesem. Jeho jediným úkolem je přijímat pakety a následně jednorázově provádět co se po něm žádá.



Obrázek 21: Princip řízeného modelu

Nemá žádnou řídící ani rozhodovací úlohu. Mikrokontrolér může obdržet dva různé druhy paketů. Buď řídící, kde je obsažen příkaz co má provézt a nebo tzv. pollovací, kterým se řídící počítač dotazuje na jeho aktuální stav aby měl zpětnou vazbu od procesu. V řídícím datagramu je v našem případě obsažen pouze jeden byte který reprezentuje stav na portu B a mikrokontrolér ho jen na tento port zapíše. Nezjišťuje žádné okolnosti a jen ho tam zkopíruje. Pollovací datagram obsahuje jeden jediný byte s hodnotou 0xFFh. Po jeho přijetí mikrokontroler obratem pošle paket jenž obsahuje datagram se dvěma byty. Ty reprezentují Port B což jsou výstupy a Port C který představuje vstupy od řídícího procesu. Oba typy datagramů jsou zobrazeny na obrázku.



Obrázek 22: Datagramy pro řízený model. Vlevo datagram s příkazem a vpravo odpověď se stavem procesoru

Takovýto systém řízení se uplatní zejména u složitějších procesů a technologií které vyžadují komplexnější a složitější řízení případně lidský dohled za použití nějakého druhu vizualizace.

Jelikož jsem navrhoval oba dva způsoby mohu říci, že ačkoliv je Chipweb programován v jazyce C a tudíž psaní a úpravy různých funkcí či procedur jsou oproti assembleru podstatně

snazší je z hlediska vývoje výhodnější druhý způsob.

Pro úspěšné naprogramování a následné odladění byly použité následující prostředky

- MPLAB IDE v 7.42
- Kompilátor HI-TECH PICC18 v 3.02
- In-Circuit debugger SCPD2
- In-Circuit programátor Presto

4.1.1 Popis SDK Chipweb

Zdrojové kódy SDK jsou organizovány tak, aby šel celý projekt zkompilovat z příkazové řádky kompilací jednoho souboru (*p18web.c*) tj. všechny další soubory jsou do tohoto souboru vloženy pomocí direktivy *#include*.

Následuje výpis souborů SDK a popis funkcí souborů.

ht_make.bat skript pro kompilaci z příkazové řádky

p18web.c hlavní soubor do kterého jsou ostatní zdrojové soubory vkládány

ccs_p18.h direktivy a definice pro překladač CCS

ht_p18.h direktivy a definice pro překladač HI-TECH

ht_utils.c zdrojové kódy některých funkcí implementovaných v kompilátoru HI-TECH přímo

p18_defs.c definice datových typů a některých maker používaných v SDK

p18_drv.c funkce používané nízkoúrovňovými drivery *p18_eth.c* a *p18_wlan.c*

p18_eth.c ovladač ethernet rozhraní (nevyužit)

p18_wlan.c ovladač WiFi rozhraní

wlan.h konstanty a struktury pro *p18_wlan.c*

p18_net.c síťový driver

p18_ip.c funkce IP protokolu

p18_dhcp.c DHCP protokol

p18_udp.c funkce UDP protokolu (nevyužit)

p18_tcp.c funkce TCP protokolu (modifikován, přidán handler portu 514)

p18_tcpc.c TCP klient (nevyužit)

p18_http.c jednoduchý http server, zobrazuje stránky z ROM paměti

4*p18_lcd.c* ovladač pro LED (nevyužit)

p18_mail.c SMTP/POP3 klient (nevyužit)

p18_ser.c ovladač sériového rozhraní

p18_time.c NTP klient (nevyužit)

p18_usr.c funkce pro uživatelskou konfiguraci

webrom.h definice pro souborový systém ROM kde jsou uloženy webstránky

WEBPAGE.ROM obsah paměti ROM

4.1.2 Zpracování příchozího paketu v ChipWebu

Příchozí data jsou zpracována podle OSI modelu. Po přijetí je 802.11 rámec uložen do RAM WiFi karty a následně funkcí *getwc_rxbuff*() (soubor *p18_wlan.c*) načten do vstupního bufferu. V průběhu hlavní smyčky je na data mimo jiné zavolána funkce *load_rxbuff*() (soubor *p18_net.c*) která rámec zpracuje do podoby paketu, vyčistí buffer a připraví ho na příjem dalších dat.

Je li paket IP paketem je na něj zavolána funkce *ip_recv*() (soubor *p18_ip.c*) ve které je rozhodnuto o jaký podprotokol (TCP, UDP, ICMP) se jedná a je volán příslušný handler (*tcp_recv*(), *udp_recv*(), *icmp_recv*())

Při příchodu TCP paketu se během funkce *tcp_recv*() rozhoduje o portu na který paket přijde a podle toho je opět volán příslušný handler. Aplikace v současné době podporuje tyto porty: HTTP (80) , DAYTIME (13) a RCMD (514). Na port RCMD reaguje voláním funkce *cmd_recv*() (soubor *pracka.c*) která paket přijme rozhodne jestli paket obsahuje dotaz na stav (hodnota FFh) nebo příkaz pro pračku (jakákoliv jiná hodnota) a podle toho volá buď funkci *state_report*(), která odpoví aktuálním stavem, nebo paket zpracuje jako příkaz-program pro pračku.

4.1.3 Úpravy SDK pro potřeby aplikace

Soubor *p18web.c* jsem zkopíroval do *p18pracka.c* a přidal soubory *pracka.c* a *pracka.h*, které jsem pomocí direktivy *#include* vložil. Výchozím souborem pro kompilaci se tak stal tento soubor.

Do části, která zpracovává TCP (soubor $p18_tcp.c$) pakety jsem zařadil rutinu která reaguje na port 514:tcp a volá funkci která obsahuje vlastní kód programu řízení pračky. Tato funkce je v souboru *pracka.c*. Další úpravy se týkaly odstranění zbytečných komponent jako například NTP server a SMTP-POP3 klient.

4.1.4 MPLAB IDE v 7.42

Tento program, který se používá pro vývoj programu pro mikroprocesory PIC, je volně dostupný na stránkách společnosti Microchip. Verze programu 7.42 byla poslední verzí dostupnou v době psaní této práce a byla zde použita. Vývojové prostředí obsahuje nástroje pro psaní programu, včetně zvýraznění syntaxe, následné kompilaci a vytváření zdrojových souboru pro programátor a debugger. Umožňuje také program krokovat v reálném prostředí mikroprocesoru, nastavovat breakpointy a měnit hodnoty v registrech a paměti. Pro základní nastavení konfiguračních registrů mikroprocesoru lze použít nástroj Visual Initializer, pomocí něhož lze komfortně nastavit a vybrat funkce jednotlivých periferních obvodu a který následně vygeneruje podprogram, který provede inicializaci obvodu po restartu. S programem se instalují všechny potřebné knihovny, hlavičkové soubory, kompilátory a skripty linkeru. Program též disponuje poměrně rozsáhlou nápovědou.

Popis rozhraní programu

V levém horním okně je vidět seznam souborů projektu organizovaný podle typu souboru. Pravé horní okno je editor zdrojového kódu programu. Do levého spodního okna IDE vypisuje výstupy během kompilace programu, ladění a programování procesoru. Pravé spodní okno slouží ke sledovaní hodnot registrů procesoru a proměnných programu. Okno vprostřed je Stimulus workbook který sdružuje stimuly zasílané programu během simulovaného pomocí prostředku MPLAB SIM.

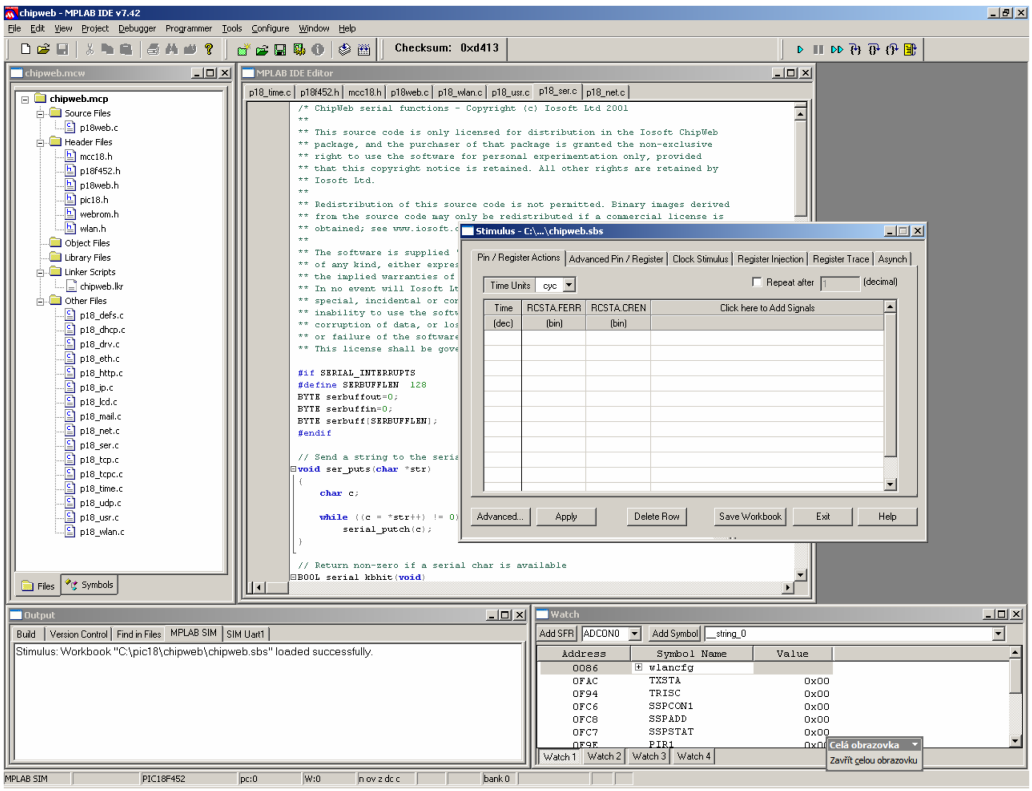
IDE je možno provozovat s různými kompilátory, tato volba je součástí parametrů projektu, jinými slovy je možno mít vývojové prostředí nainstalováno s několika kompilátory najednou a vhodný kompilátor volit nejen při vytvoření projektu ale i před každou kompilací.

Debugger/Simulátor MPLAB SIM

Tento nástroj slouží pro ladění programů mimo procesor, simulací jejich běhu v počítači. Je možné jak měnit přímo hodnoty SFR registrů tak i hodnoty proměnných programu. Pomocí Stimulus Workbook lze vyvolávat v procesoru asynchronní i synchronní události a stimulovat vstupy diskrétními i analogovými hodnotami.

Ostatní nástroje MPLAB IDE

Vývojové prostředí dále obsahuje prostředek pro práci s obsahem procesoru jako je mazání, čtení, zápis a to jak programové paměti, paměti EEPROM, tak i konfiguračních a ochranných bitů procesoru. K použití tohoto nástroje je třeba mít k počítači připojený hardwarový programátor nebo debugger, které popíšu ve zvláštních kapitolách. Pro vývoj ve skupinách MPLAB IDE obsahuje rozhraní pro CVS server.



Obrázek 23: Prostředí MPLAB

4.1.5 Kompilátor HI-TECH PICC18

Výběr kompilátoru je mnohem důležitější než by se na první pohled mohlo zdát. Záleží právě na něm jak výsledný program bude fungovat. Nemám teď na mysli jeho funkčnost, ta by měla být zaručena bez ohledu na kompilátor, ale záleží právě na něm jak bude výsledný program veliký a jak rychle se bude vykonávat.
Nejpoužívanějšími C kompilátory pro procesor PIC18F452 jsou:

- Microchip C18
- CCS C Compiler
- HI-TECH PICC18

Jak z názvu vyplývá, první uvedený je vyvinut výrobcem procesorů PIC. Bohužel tento kompilátor není výrobcem Chipwebu podporován a tak bylo nutno použít některý jiný. CCS kompilátor bohužel není dostupný vzhledem ke své vysoké ceně, čili volba padla na poslední, HI-TECH PICC18, který je nabízen v limitované verzi ke stažení na firemních webových stránkách.

Výrobce uvádí následující vlastnosti:

- Plná podpora standardu ANSI C
- Výkonnost výsledného kódu srovnatelná s programem psaným přímo v asembleru
- Modularita (organizováno ve zdokumentovaných knihovnách)
- Kompatibilita (Integrace s MPLAB IDE)
- Komplexnost prostředí (makroasembler,preprocesor)

Během své práce na programu jsem vyzkoušel jak kompilátor od Microchipu tak i HI-TECH takže jsem měl možnost srovnání. Podle mého názoru je HI-TECH opravdu lepší kompilátor, nicméně proklamovaná kompatibilita s MPLAB IDE je přinejmenším sporná, protože po instalaci kompilátoru a plug-inů se mi nepodařilo z MPLABu zkompilovat program, který z příkazové řádky bez problémů zkompilovat šel.

Kompilátor podporuje datový typ "bit" což je v případě práce s jednotlivými I/O piny kontroléru velmi užitečná vlastnost. Ačkoliv u jednočipových mikrokontrolérů přistupujeme na vstupně výstupní porty často bit po bitu, ne všechny kompilátory si poradí s takovouto proměnnou. Dále disponuje velmi dobrou optimalizací kódu z čehož plyne, že binární soubor pro upload do procesoru vychází velmi malý.

4.1.6 Debugger SCPD2

Debugger SCPD2 je zařízení určené k ladění aplikací procesorů PIC osazených v obvodech, tzv. In-Circuit Debugging. Je signálově, a softwarově kompatibilní s ICD2 od firmy Microchip a je li připojen k MPLAB IDE, zachází se s ním stejně. Od svého vzoru se liší pouze absencí USB rozhraní z čehož vyplývá i nižší rychlost komunikace s mikrokontrolerem, což se projevilo hlavně během ladění síťových funkcí.

4.1.7 Programátor PRESTO a aplikace Up!

Programátor podporuje programování osazených součástek - ISP (In-System Programming) a ICP (In-Circuit Programming). S počítačem je propojen rozhraním USB ze které je i napájen. Komunikuje v režimu Full speed a pracuje na počítačích s portem USB 1.1 i 2.0. K připojení aplikace slouží 8-pinový konektor ISP, který je shora kompatibilní s 6-pinovým konektorem ICSP pro mikrokontroléry PIC, který obsahují všechny programátory firmy ASIX. Funkce vývodu VPP je rozšířena o obousměrnou datovou komunikaci, přidány jsou vývody MISO (vstup) a LVP (vstup/výstup). Vývod VDD připojený k vývodům napájecího napětí programované součástky může volitelně buď poskytovat napětí z USB o nominální hodnotě 5 V nebo využívat napětí přiváděné z programované aplikace v rozsahu 3 až 5 V s tolerancí ±10%. Toto napětí je pak použito i pro digitální signály. Lze detekovat přítomnost externího napájení pro tři úrovně - 3 V, 5 V a přepětí. Je implementována i nadproudová ochrana programovacího a napájecího napětí.

Stav programátoru je přehledně indikován pomocí dvou LED. ON-LINE (zelená LED) informuje o připojení k USB, ACTIVE (žlutá LED) signalizuje aktivitu na programovacím rozhraní, např. programování či verifikaci. Vlastní programováni se spouští pomocí tlačítka Go.

Software

Základním softwarovým prostředkem pro práci s programátorem PRESTO je program UP. Kromě běžných příkazů poskytuje řadu nadstandardních funkcí. Jde např. o možnost definování projektů, parametry při spouštění z příkazového řádku umožňující bezobslužné použití programátoru při rutinním programování, nastavení prostředí včetně klávesových zkratek, automatické generování sériového čísla apod. Program UP je určen pro Windows verze 95, 98, ME, 2000 a XP. Podpora USB je k dispozici od verze W98SE, pro komunikaci se zařízeními se sběrnicí USB se používají modifikované ovladače D2XX firmy FTDI. Software UP podporuje mikrokontroléry Microchip PIC a Atmel AVR a 8051. Bohužel tento prostředek není podporován MPLAB IDE, takže z hlediska vývoje aplikace sloužil spíše k finálnímu naprogramování mikrokontroleru a přehledné orientaci v obsahu paměti EEPROM.

PRESTO kromě samotného programování poskytuje i základní podporu při ladění aplikací. U mikrokontrolérů PIC lze s jeho pomocí řídit i stav součástky - režimy Reset a Run.

4.2 Program pro PC

Ovládací program pro PC musí splňovat následující požadavky:

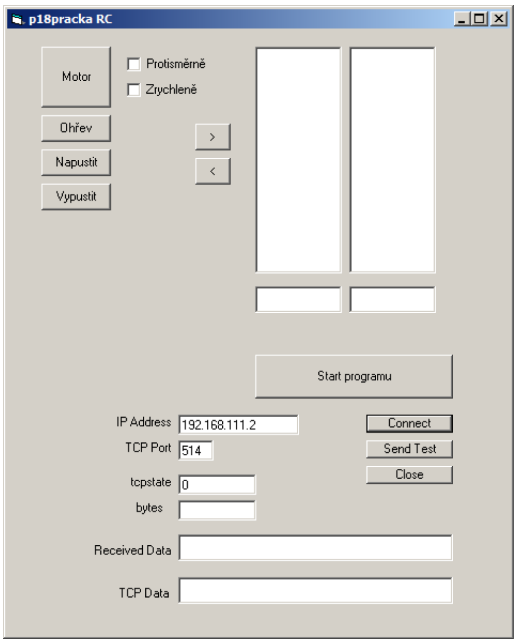
- Vytvoření ovládacího datagramu pro program v mikrokontroleru
- Odeslání datagramu pomocí TCP protokolu
- Zpětná vazba z mikrokontroleru, zobrazení stavu/činnosti mikrokontroleru

Program jsem napsal ve vývojovém prostředí Microsoft VisualBasic 5.0 z čehož i vyplývá platforma běhu, MS Windows 95 - XP.

Srdcem celého programu je OCX komponent MS Windows Socket komponent (winsock.dll) který v podstatě funguje jako datová pumpa. Vytvoří TCP spojení na portu 514 k serveru, v tomto případě mikrokontroleru, a do spojení odešle datagram.

4.2.1 Autonomní model

Mikrokontroler po obdržení datagramu uzavře TCP spojení a začne vykonávat program na základě dat která obdržel. Pokud je s vykonáváním hotov, čeká na další datagram. Ten může mít dvě různé funkce. Pokud je uvozen hodnotou 0x80h mikrokontroler začne s vykonáváním nového programu s ohledem na svoje vstupy a výstupy a nebo začíná hodnotou 0xFFh a v tom případě odpoví paketem v němž je uložen jeho momentální stav (hodnoty na portech B a C)

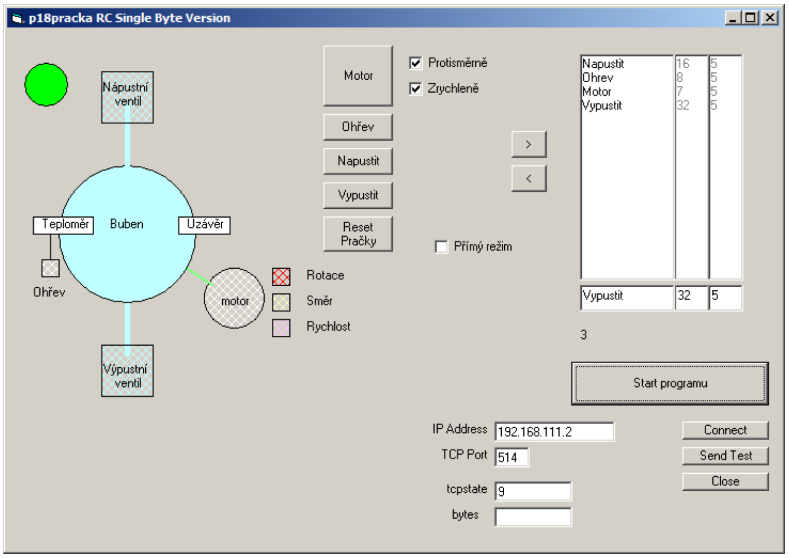


Obrázek 24: Rozhraní pro autonomní model

4.2.2 Přímo řízený model

Stejně jako v případě autonomního modelu komunikace probíhá pomocí datagramů jež řídí činnost mikrokontroleru. Rozdíl je v tom, že veškerou řídící funkci zde přebírá ovládací program běžící v PC. Tento program neustale vysílá pakety, které obsahují datagramy o délce jednoho bytu a hodnotě 0xFFh. Na ně mikrokontroler odpovídá datagramem jenž obsahuje 2 byty s jeho stavem jak bylo popsáno výše. Zvolil jsem interval 500ms neboť tento proces má dlouhé časové konstanty a pro jeho sledování to bohatě stačí.

Pokud mikrokontroler obdrží datagram jenž začíná a končí hodnotou 0x80h detekuje ho jako řídící. Tento datagram má pevnou délku jednoho bytu a obsahuje nastavení výstupů. Tento stav je ověřen prvním pollovacím paketem a jeho stav zpět poslán do řídícího programu kde se nastaví příslušné výstupní indikátory.



Obrázek 25: Rozhraní pro přímo řízený model

Popis rozhraní

Vlevo je schematicky znázorněna pračka respektive, její funkční části. Prostřední část jsou programovací tlačítka která upravují hodnotu v textovém poli označeném "Povel". Hodnota je zobrazována dekadicky a lze ji upravovat. Do textového pole "# vteřin" se zapisuje doba ve vteřinách po kterou má povel běžet. Ovládací datagram se pomocí tlačítka [>] shromažduje v seznamu v pravé části okna programu odkud lze jednotlivé povely odstranit pomocí tlačítka [<]. Tlačítkem [Start Programu] se začnou vysílat datagramy s jednotlivými povely. Schematické znázornění vlevo téměř okamžitě reaguje na jakékoliv změny stavu vstupů a výstupů které mu na jeho periodické žádosti mikrokontrolér posílá. Nepatrné zpoždění je zapříčiněno tím, že pollovací paket chodí jednou za 100ms.

5 Závěr

V zadání diplomové práce bylo navrhnout a realizovat bezdrátové spojení a aplikovat ho na jednoduchý model. Pro prostudování možností jsem vybral spojení na základě standardu 802.11b (WiFi). Pro tento účel jsem si poměrně zdlouhavým procesem opatřil od firmy IOSOFT vývojovou desku ER25. Výběr padl na tuto ne příliš dostupnou desku z toho důvodu, protože jejím srdcem je mikrokontroler od firmy Microchip. S výrobky této firmy mám dobré zkušenosti a i dostupnost programátorů a debuggerů je poměrně dobrá.

Po té co jsem vývojovou desku obdržel a měl možnost si jí prohlédnout zarazilo mě její poněkud nešťastné hardwarové zpracování. Ocelový plášť PCMCIA karty se nacházel přímo pod deskou s plošnými spoji a v některých místech se jí dokonce dotýkal. Podle mého názoru kdybych připojil napájecí napětí mohlo by přinejmenším dojít k její špatné funkčnosti a nebo dokonce ke zničení.

Při práci mi nejvíce vadila absence možnosti debuggování přímo v procesoru jelikož některé vstupy a výstupy k tomu určené byly využity pro obsluhu PCMCIA karty. I přes tuto překážku šel program docela dobře odladit pomocí informací vypisovaných na sériové rozhraní RS232.

V celé práci jsem se snažil postupovat způsobem, co nejvíce podobným návrhu komerčního zařízení se zřetelem na flexibilitu, cenovou dostupnost, odolnost vůči chybám a variabilitu použití. Popsaným způsobem, za minimálního úsilí, lze ovládat prakticky libovolný jednoduchý technologický proces založený na diskrétních hodnotách vstupu a výstupu. Po doplnění příslušným hardwarem jako jsou posuvné registry případně A/D nebo D/A převodníky by bylo možné použít vývojovou desku ER25 téměř na jakýkoliv technologický proces.

Reference

[1] Rita Pužmanová: *Bezpečnost bezdrátové komunikace*, Vydalo CP Books 2005

[2] Patrick Zandl: *Bezdrátové sítě WiFi Praktický průvodce* Vydalo CP Books 2003

[3] Libor Dostálek, Alena Kabelová: *Velký průvodce protokoly TCP/IP a systémem DNS* Vydalo CP Books 2000

[4] Miroslav Virius: *Jazyk C a C++: kompletní kapesní průvodce* Vydalo Grada 2005

[5] *Microchip DataSheet "39564c.pdf"*
http://ww1.microchip.com/downloads/en/DeviceDoc/39564c.pdf

[6] Wi-Fi Alliance http://wi-fi.org/

Přílohy:

Schéma vývojové desky ER25