Obsah

1. Automatizace domácnosti a technologie dálkového přenosu

Následující část má bezprostřední vztah k bakalářské práci. Neobsahuje tedy všechny informace o daných tématech, ale pouze ty, které jsou potřebné. Nejprve je zde popsaná automatizace domácnosti, co to znamená a jaké jsou dnes možnosti jejího využití. Následuje část zabývající se technologiemi bezdrátového přenosu informací. Nejprve je pojednáno o tom, co tento typ komunikace obnáší, jaké má výhody a nevýhody. Dále je uveden popis některých principů tří často používaných standardů bezdrátové komunikace (WiFi, Bluetooth a ZigBee).

1.1 Automatizace domácnosti

Automatizace domácnosti spočívá v automatizování činností, které řídí domácnost, normálně vykonávané člověkem. V souvislosti s tím někdy hovoříme o inteligentní domácnosti. Může se jednat v nejjednodušším případě o prostý časovač, vypínající světlo [S, str.1], nebo i o komplexnější řešení, jako je ovládání domácnosti na dálku (ideálně mobilním telefonem, nebo tabletem), inteligentní řízení spotřebičů domácnosti (jako světla, větrák, žaluzie…) na základě nejrůznějších senzorů a podobně.

Automatizace v mnohém usnadňuje život a umožňuje provádění akcí, které by jinak byli prakticky nemožné (například zabezpečení domu). Jedním z cílů inteligentních domů je úspora energií, díky využití automatizace. Mezi typické aplikace automatizace domácnosti patří:

- Zmíněné zabezpečení
- Systém pro inteligentní vytápění a ventilaci (HVAC)
- Ovládání spotřebičů [T]
- Samo zavlažovací systémy [U]

Ovladače a časovače

Nejjednodušším prvkem automatizace domácnosti mohou být různé časovače. Na českém trhu jsou k dispozici především zásuvky a relé (na DIN lištu) s časovým spínačem. Jejich cena se pohybuje okolo 100–300 kč.

Další volbou jsou pak různé WiFi spínače, jako například [V] či spínače/relé, ovládané RF ovládači pracující na některé z nelicencovaných frekvencích, například [G]. Cena je podobná.

Inteligentní ovládací prvky

Pro ještě komfortnější ovládání a automatizaci domácnosti je možné využít některé inteligentní systémy, jako jsou Amazon Alexa, nebo Google Assistant.

1.2 Technologie bezdrátového přenosu

Pro přenos dat či řídících signálů je vždy potřeba zvolit vhodné médium, přes které se budou tyto informace přenášet. V některých situacích není pro přenos vhodné (a někdy dokonce ani možné) používat kabely (ať už metalické nebo optické). V těchto případech je potřeba přenášet informace bezdrátově, tj. za využití jiných médií, jako je vzduch.

Podobně jako je nutné u kabelového spojení využít vhodný způsob komunikace (například zvolit vhodnou sběrnici a nastavit ji správné parametry) je potřeba se způsobem komunikace zabývat rovněž u bezdrátového přenosu. Zde je nutné zejména zvolit vhodnou technologii (jako je Wifi, Bluetooth či ZigBee) a její parametry [A].

Výhody bezdrátového přenosu

Bezdrátová komunikace má oproti kabelové řadu výhod. Zejména se jedná o následující:

- Jednodušší připojení – zařízení není potřeba připojovat kabelem, a dokonce nemusí být ani vybaveno konektorem pro toto připojení (pozn. pro dálkový přenos prostřednictvím světla je však stále potřeba mít nějaký přijímající port). Z toho rovněž plyne, že není potřeba měnit strukturu sítě kvůli změnám v místnosti a rovněž není potřeba myslet na konkrétní strukturu sítě ještě před budováním.
- Větší spolehlivost – Častým zdrojem problémů s kabelovým připojením jsou chyby na straně kabelů – jejich poškození. Použitím bezdrátových technologií se lze vyhnout tomuto typu chyb.
- Snadná rozšiřitelnost sítě – U kabelového připojení je potřeba řešit způsob rozšíření sítě a v případě, že stávající struktura sítě rozšíření nepodporuje, tak je potřeba ji celou pozměnit. Bezdrátové sítě tento problém eliminují.
- Nižší cena – Použitím bezdrátových technologií se značně sníží pořizovací cena sítě – není potřeba kupovat drahou kabeláž. Rovněž instalace kabelů do starých budov může být velmi nákladná a problémová.

Nevýhody bezdrátového přenosu

Kromě množství výhod, které bezdrátová komunikace představuje jsou zde rovněž některé nevýhody tohoto typu komunikace:

- Rušení signálu – zařízení, využívající bezdrátové technologie může způsobovat rušení ostatních zařízení a rovněž opačně – dané zařízení může být rušeno od ostatních zařízení, pracujících na podobném principu
- Bezpečnost – bezdrátová komunikace často vysílá (a přijímá) signály do relativně rozsáhlého otevřeného prostoru, tudíž jsou takto vysílaná data často daleko méně chráněná než u kabelového přenosu (kde je k získávání dat potřeba mít fyzické připojení k síti, ve které se data přenáší) [A] [Q, str. 5-6] [R, str. 406]. Je tedy nutné zabezpečit přenos dat.

Modulace

Signál, který je potřeba přenášet v bezdrátových sítích reprezentuje přenášená data. Ty jsou však třeba nějakým způsobem upravit, protože z dat vytvořený signál (obvykle reprezentovaný dvěma úrovněmi napětí na vodiči) není pro bezdrátový přenos příliš vhodný. Tato modifikace signálu se nazývá modulace. Jedná se o proces, při kterém signál v základním pásmu (např. video) moduluje tzv. nosný signál, který data přenáší a informace je zakódovaná právě tím, jak je původním signálem modulovaný.

Modulace přináší do bezdrátového přenosu mnoho výhod:

- Menší velikost antén
- Větší dosah
- Kvalitnější přenos informací [AI, str.1-2]

Způsob komunikace

V případě bezdrátových technologií se využívá některého pásma elektromagnetického vlnění. Rychlost šíření tohoto záření je ve vakuu rovno konstantě c (přibližně 3×10^8), v médiu jako je vzduch se pak šíří rychlostí c, podělenou indexem lomu (konkrétně pro vzduch je tento index blízký 1, takže můžeme uvažovat prakticky stejnou rychlost jako pro vakuum) [M] [N, str 2-3] [O, str.24] [P, kap 8.2].

V současnosti se na trhu s elektronikou zařízení, využívající především dva různé principy dálkového přenosu informací, první je založen na využití světla, druhý pak využívá rádiové vlny. [A]

Přenos informací pomocí světelného signálu

V případě světelného signálu se většinou využívá infračerveného záření, jelikož není lidským okem viditelné, avšak je možné vyrobit přijímač, která tento signál detekuje (a to je

vlastnost, která se zde vyžaduje).

Kromě těchto definovaných protokolů je pro komunikaci pomocí IR záření možno použít standardů IEEE 802.11 (Tyto standardy to tak definují). V praxi se však nikdy nic takového nedočkalo rozšíření.

První princip, který je možný použít je využití infračerveného záření. Jelikož není obvykle v domácnosti mnoho zařízení, pracujících s IR, nebývají většinou zařízení navzájem příliš rušeny. Stále zde však existuje rušení od jiných zdrojů infračerveného záření, například ze slunečního záření, nebo fluorescenčního světla. Rušení od těchto zdrojů je však možné potlačit jistými principy. Prvním je vyhrazení určité vlnové délky, která se bude pro přenos informací používat a následným použitím filtru na přijímací diodě, který odfiltruje ostatní vlnové délky. Nepotlačené rušení (od zdrojů, které vyzařují v oné vyhrazené vlnové délce (problémem je tedy zejména Slunce) je možné dále potlačit tím, že bude přijímač reagovat pouze na nějakou modulovanou frekvenci, nepřítomnou v daném zdroji (tedy například ve slunečním záření). Systémy využívající IR záření se vyznačují tím, že je musejí splňovat podmínku přímé viditelnosti vysílače a přijímače. Není tedy možné (bez případných dodatečných, opakovacích zařízení) ovládat zařízení za rohem, pokud není přímo viditelné. Právě díky této vlastnosti je možné volně využívat zařízení, využívající tohoto principu, protože nedochází k žádnému rušení a není tak potřeba regulovat směrnicemi používaní IR vysílání. Dosah IR vysílačů se obvykle udává v jednotkách, případně desítkách metrů.

Přenos informací pomocí rádiových vln

Kromě IR záření mohou zařízení k dálkovému přenosu informací využívat také rádiových vln na různých frekvencích. Zde však již existují jistá omezení. Rádiové vlny se totiž (na rozdíl od IR světla) šíří i skrze předměty. To je příčinou toho, že se mohou i relativně vzdálená zařízení komunikující na stejných vlnách vzájemně rušit. Aby se předešlo naprostému zarušení prostoru, je potřeba mít k vysílání na určitých frekvencích licenci. Je zřejmé, že si běžní uživatelé zařízení v domácnosti nemohou dovolit kupovat drahé licence kvůli každému bezdrátově ovládanému zařízení, které si koupí. Z tohoto důvodu bylo navrženo tzv. pásmo ISM.

V pásmu ISM jsou definovány frekvenční rozsahy, které je možné volně použít pro schválená zařízení bez licence. To ovšem také znamená, že zařízení pracující v těchto rozsazích musejí

tolerovat rušení od ostatních zařízeních pracujících na stejných frekvencích. [C, s.66]. Dokument „ITU Radio Regulations“ toto pásmo vyhrazuje pro „Provoz vybavení nebo zařízení určených ke generování a využívání lokální vysokofrekvenční energie pro průmyslové, vědecké, lékařské, domácí nebo podobné účely, s výjimkou aplikací v oblasti telekomunikací“.

Nejčastěji se pro komunikaci v pásmu ISM používá frekvenční pásmo 2,4 GHz. To je dané historickým vývojem. Zejména u mikrovlnných trub bylo potřeba zvolit vhodné pásmo [X]. Zvolené pásmo 2,4 Ghz bylo vybráno z několika důvodů, zejména však na základě empirického měření průniku a šíření tepla pro různé potraviny (při použití frekvencí tohoto pásma) a s ohledem na rozměry použitého magnetronu (součástky, která generuje mikrovlnné záření [W, kap. 6-20]).

IOT protokoly:

https://www.postscapes.com/internet-of-things-protocols/

https://www.ubuntupit.com/top-15-standard-iot-protocols-that-you-must-know-about/

sniffing:

https://www.youtube.com/watch?v=pfG8uEDZj5g

MQTT:

https://www.youtube.com/watch?v=EIxdz-2rhLs

https://www.youtube.com/watch?v=iNWsW_q4Fu0

PŘEDNÁŠKA!!!!:

https://www.youtube.com/watch?v=s6ZtfLmvQMU

1.3 WiFi

Wifi je technologie, využívající standardů z rodiny IEEE 802.11. První verze tohoto standardu byla organizací IEEE schválena v roce 1977 [A, s.6]. Od té doby vyšlo mnoho dalších verzí standardů. Jednotlivé verze se od sebe mohou odlišovat různými parametry, například frekvenčním pásmem, šířkou pásma jednotlivých kanálů, maximální rychlostí přenosu atd. Organizace Wi-Fi Alliance rozlišuje některé standardy IEEE 802.11 číslem generace WiFi, nejnovější je prozatím zatím 6. generace (založená na standardu 802.11ax).

IEEE 802.11 PHY Standards							
Release date	Standard	Frequency Band	Bandwidth	Transmission Scheme	Max Modulation	MIMO	Max Data Rate
1997	802.11	2.4 GHz	20 MHz	DSSS, FHSS	QPSK	N/A	2 Mb/s
1999	802.11b	2.4 GHz	20 MHz	DSSS	QPSK	N/A	11 Mb/s
1999	802.11a	5 GHz	20 MHz	OFDM	64QAM	N/A	54 Mb/s
2003	802.11g	2.4 GHz	20 MHz	DSSS, OFDM	64QAM	N/A	54 Mb/s
2009	802.11n	2.4 GHz 5 GHz	20 MHz 40 MHz	OFDM	64QAM	4x4	600 Mb/s
2013	802.11ac	5 GHz	20 MHz 40 MHz 80 MHz 160 MHz	OFDM	256QAM	8x8	6.93 Gb/s
2018	802.11ad	60 GHz	2160 MHz	SC, OFDM	256QAM	Beamforming	6.93 Gb/s

GRANDMETRIC WATCH!

Tabulka 1 – některé důležité verze standardu IEEE 802.11 a jejich parametry[1]

Wifi funguje na principu vysílání a přijímání rádiových vln. Organizace IEEE rozhodla využít pro technologii Wi-Fi frekvence z pásma ISM [B, str.2]. Wifi standardně využívá frekvencí 2,4Ghz a 5Ghz. Nejprve byla zařízení Wi-Fi schopná pracovat pouze v jednom z těchto dvou frekvenčních pásem, ale 4. generace (IEEE 802.11n) přidává možnost práce v obou zmíněných pásmech. Moderní zařízení s wifi si tak mohou vybrat (a dokonce během své činnosti měnit) frekvenci, na které budou spolu komunikovat.

Obě pásma mají svá pro i proti. Mezi výhody pásma 2.4Ghz patří zejména větší pokrytí signálu a rovněž větší kompatibilita (platí spíše pro starší zařízení). Na druhou stranu pásmo 5Ghz nabízí podstatně vyšší přenosové rychlosti a dále větší množství komunikačních kanálů [D].

Režim sítě

Wifi nachází uplatnění v (bezdrátových) lokálních sítích. V nich pak rozlišujeme 3 režimy na základě toho, jak se Wifi zařízení v síti mezi sebou navzájem spojují (jakou plní roli):

- Režim infrastruktury
- Ad hoc režim
- Smíšený režim

V režimu infrastruktury je v sítí přítomen minimálně jeden centrální prvek (tzv. přístupový

[1] https://www.grandmetric.com/2018/05/29/wi-fi-standards-evolution/

bod), který zprostředkovává komunikaci mezi jednotlivými prvky (klienty) sítě, případně poskytuje připojení do jiné sítě přes distribuční systém (DS). V tomto režimu sítě je výhoda, že je snadné připojit do stávající infrastruktury nový prvek.

Ad hoc je režim bezdrátové sítě, ve které není přítomen žádný centrální prvek (přístupový bod) se kterým by prvky sítě komunikovali, ani zde není žádné spojení se pevnou sítí přes distribuční systém. Jedná se tedy o decentralizovanou síť. Jednotlivé prvky tedy mezi sebou navzájem komunikují přímo (toto spojení se někdy označuje jako tzv. peer-to-peer). V tomto režimu má síť rovněž SSID identifikátor, kterým je možné síť identifikovat. [A][B]

Bezpečnost wifi sítě

1.4 Bluetooth

Bluetooth je standard, definovaný v IEEE 802.15.1. Vytvořila jej firma Ericsson v roce 1994 a od té doby vyšlo několik nových verzí [A]. Podobně jako WiFi pracuje v ISM pásmu 2,4 GHz. Na rozdíl od Wi-Fi však není definován pouze na prvních dvou vrstvách ISO/OSI, ale definuje protokoly na všech sedmi vrstvách tohoto modelu. Na nejnižší úrovni, kde definuje způsob přenosu jednotlivých bitů využívá metodu FHSS, která zajišťuje, že při přenosu bitů vysílač přeskakuje mezi několika frekvencemi [AD].

Zařízením, které jej využívají, umožňuje vytvořit tzv. PAN (osobní síť). V těchto sítích má každé zařízení přiřazeno unikátní 48bitovou adresu BD_ADDR (BlueTooth Device Address) – jedná se o obdobu MAC adresy u ethernetu. Tu používá pro komunikaci s ostatními zařízeními. Jedno zařízení může být v roli master (řídící), slave (podřízená) nebo obojího [AB, str.4]. K jedné řídící stanici se připojuje jedno a více podřízených zařízení (používá se pouze adhoc komunikace mezi master a slave stanicí). Zde hovoříme o tzv. piconetu (pikosíti). Maximální počet zařízení v jedné pikosíti je 8 (jedna řídící stanice a až 7 podřízených). Stanice náležící do jedné pikosítě může zároveň patřit do jiné pikosítě. Jedná se tedy o rozšíření sítě mezi zařízeními. Takto vytvořenou síť nazýváme tzv. scatternet (rozprostřená síť). V každé rozprostřené síti má každá pikosíť unikátní identifikátor – je jím BD_ADDR její řídící stanice. Díky rozlišení jednotlivých pikosítí pak může každá tato síť využívat jiné skokové sekvence (frekvenčních kanálů na kterých se vysílají/přijímají data) [AC, str. 20].

1.5 ZigBee

Zigbee je bezdrátová technologie, založená na standardu IEEE 802.15.4. Je určená pro

vytváření sítě PAN (osobní síť) a pracuje v pásmu ISM 868 MHz, 902-928 MHz a 2,4 GHz [A].

Zařízení v ZigBee síti

ZigBee standard specifikuje 2 typy zařízení – FFL (Full Function Device) a RFD (Reduced Function Device). FFL zařízení je obvykle schopné mnoha funkcí a je stále aktivní, zatímco RFD se nachází většinu času v režimu spánku, ze kterého se občas probudí, například aby odeslalo hodnoty neměřené na nějakém senzoru.

V síti pak každé ze zařízení plní některou ze 3 funkcí:

- Koordinátor
- Koncové zařízení
- Směrovač

Topologie sítě

Na základě definovaných zařízení pak existují 3 možné topologie ZigBee sítě:

- Hvězda
- Strom
- Mesh síť [AG, str.5]

ZigBee Model

ZigBee podobně jako Bluetooth definuje komunikaci na všech úrovních modelu ISO/OSI, nekopíruje však přesně jednotlivé vrstvy. První 3 vrstvy modelů ISO/OSI a ZigBee si odpovídají, ale vrstvy L4-L7 jsou spojené do vrstev APS (Application Support) a ZDO (ZigBee Device Object). [AH, str. 42]

2. Vestavné systémy a vývojové prostředky

Vestavný systém můžeme definovat jako software spolu s počítačem, zabudovaným do nějakého zařízení takovým způsobem, že jej uživatel nevidí jako počítač [E, str.3]. Tento počítač je většinou jednoúčelový, určený pro předem navržené použití. Tím se liší od univerzálních počítačů, které mohou poskytovat různé funkce a jejichž uplatnění se může měnit (například osobní počítač) [F, str. 3].

Historie

Po objevení polovodičů a zejména po vynálezu tranzistoru a integrovaného obvodu se začali

vedle mechanických systémů objevovat systémy elektronické. Ty přinesli mnohá vylepšení. Oproti mechanickým systémům byli znatelně jednodušší na návrh, lehčí, menší a rovněž bylo odstraněno mechanické opotřebení, které bylo u mechanických systémů problémem. I přes výhody, které číslicové systémy přinášeli zde však byli některé vážné nedostatky. Například podobně jako u mechanických systémů, i zde je často nutné při přidání nějaké funkcionality navrhnout znovu celý systém (zejména celý návrh desky plošných spojů).

Velké změny v návrhu systémů způsobil rozvoj integrovaných obvodů, zejména mikroprocesorů. Dosud bylo totiž potřeba pro každou aplikaci vytvořit vlastní systém „na míru“. S programovatelnými paměťmi, které bylo možné připojit k mikroprocesorům, případně které byli součásti mikrokontrolerů však tento problém odpadl a samotný návrh systému se přesunul do jeho popisu. Systém totiž vzniká jeho programováním, což je svým způsobem samotný popis systému. Zde jde konečně mluvit o vestavěném systému, protože zde máme hardware (počítač) i software, které společně vytváří nějaký celek, který se navenek uživateli jeví jako jednoúčelové zařízení. Vestavěné systémy mají oproti číslicovým a mechanickým systémům mnoho výhod. Kromě již zmíněného usnadnění návrhu jsou tyto systémy rovněž snadno rozšiřitelné – stačí do systému pouze nahrát nový kód a není potřeba vytvářet úplně nový návrh systému, jako tomu bylo dříve. Hromadná výroba a rozsah použití těchto systémů také způsobil značný pokles ceny oproti dříve zmíněným systémům.

Základním prvkem vestavěných systémů je jedno, či více číslicové zařízení, které se chová jako mozek celého systému a řídí jeho činnost. Typicky se jedná o mikroprocesor, mikrokontroler nebo digitální signálový procesor [H, str. 1].

Architektura řídícího zařízení

Při návrhu systému se využívá jedna ze dvou architektur:

- Von Neumannova architektura
- Harvardská architektura

Hlavním rozdílem je způsob práce s pamětí. Ve Von Neumannově architektuře je paměť pro program i data spojená do jedné paměti, v Harvardské architektuře je pak rozdělena.

Mikroprocesor (CPU) je programovatelné elektronické výpočetní zařízení, určené pro všestranné použití. Jedná se o čip, obsahující 3 základní součásti:

- Aritmeticko-logickou jednotku

- Řídící jednotku
- Registry [I, str. 18 – 19]

Mikroprocesor sám o sobě je z hlediska vestavěných systémů relativně jednoduché zařízení, které pro funkci systému potřebuje připojit některé další součásti, jako jsou paměti (RAM a ROM), čítače, časovač a podobně. Návrhář tedy musí tyto součásti přidat externě, aby zařízení fungovalo správně. Systémy, zahrnující mikroprocesory jsou obvykle založeny na Von Neumannově architektuře [J].

Mikrokontrolér je zařízení, které na rozdíl od mikroprocesoru má již všechny součásti, potřebné pro svoji činnost v sobě. Obvykle využívá Harvardské architektury [J].

2.1 Raspberry Pi

Zařízení Raspberry Pi je levný univerzální počítač malých rozměrů. Poskytuje široké možnosti v oblasti multimédií a 3D grafiky, předpokládá se že bude časem využíván i jako herní platforma.

Název Raspberry Pi vytvořila komise dozorčí rady. Slovo Raspberry je vzato jako název ovoce (malina), jak už je u počítačových systémů zvykem nazývat podle ovoce. Slovo “Pi” označuje zkráceně “Python” - programovací jazyk, který měl být původně jediným programovacím jazykem dostupným na platformě Raspberry Pi [AA].

Historie

Raspberry Pi vzniklo v r. 2006 za přispění studijního ředitele pro informatiku na Cambridgeské univerzitě za účelem lokálních potřeb. Měl to být nástroj, který by poskytl prvotní impuls studentů k nějakému z univerzitních kurzů.

2.2 ESP8266 a ESP32

Jedná se o levný mikročip, disponující Wi-Fi stackem, schopný provozu RTOS (realtime operačního systému). Je založen na 32bitovém procesoru s architekturou RISC [AE].

ESP32 je nástupce ESP8266. Kromě komunikace přes Wi-Fi umožňuje rovněž komunikaci pomocí Bluetooth, díky hybridnímu Wi-Fi/Bluetooth čipu [AF].

2.3 Python

Python je objektově orientovaný skriptovací jazyk, s velkou oblastí využití. Mezi jeho přednosti patří jednoduchost, přehlednost, objektově orientovaný přístup. Jelikož je Python

open-source, je možné jeho interpret stáhnout a používat zdarma [Z ,str 3]. Často se využívá k programování GUI aplikací, aplikací využívající síťovou komunikaci a rovněž pro různé matematické programy či programy, využívající umělou inteligenci.

Python se rovněž často používá k programování Raspberry Pi. Právě druhá část jména vychází z názvu Python [AA, str 165].

// TODO: Knihovna kiwy

3. Zhodnocení současného stavu a plán práce

Stanovení cílů

Cílem práce bude vytvořit systém pro automatizaci domácnosti. Tento systém bude sestávat z několika částí.

Základním prvkem bude centrální jednotka (tzv. hub), která bude řídit jednotlivé spotřebiče. Kromě přímého ovládání bude rovněž umožňovat tvorbu podmínek (na základě snímači naměřených hodnot), za kterých se provede jistá akce a rovněž uchovávat případné časovače nejrůznějších událostí. Centrální prvek bude moci být řízen buďto prostřednictvím připojeného displeje, ale pro pohodlnější přístup rovněž z jiných zařízení, jako je mobilní telefon, notebook a podobně. Pro větší dostupnost a multiplatformní přístup bude přístup k centrálnímu prvku řešen pomocí webové stránky.

Dalším prvkem navrhovaného systému budou moduly, připojené ke koncovým (ovládaným) zařízením, případně k nejrůznějším senzorům. Půjde o jednoduše konfigurovatelná zařízení, s několika piny. Jednotlivé piny bude možné nastavit jako:

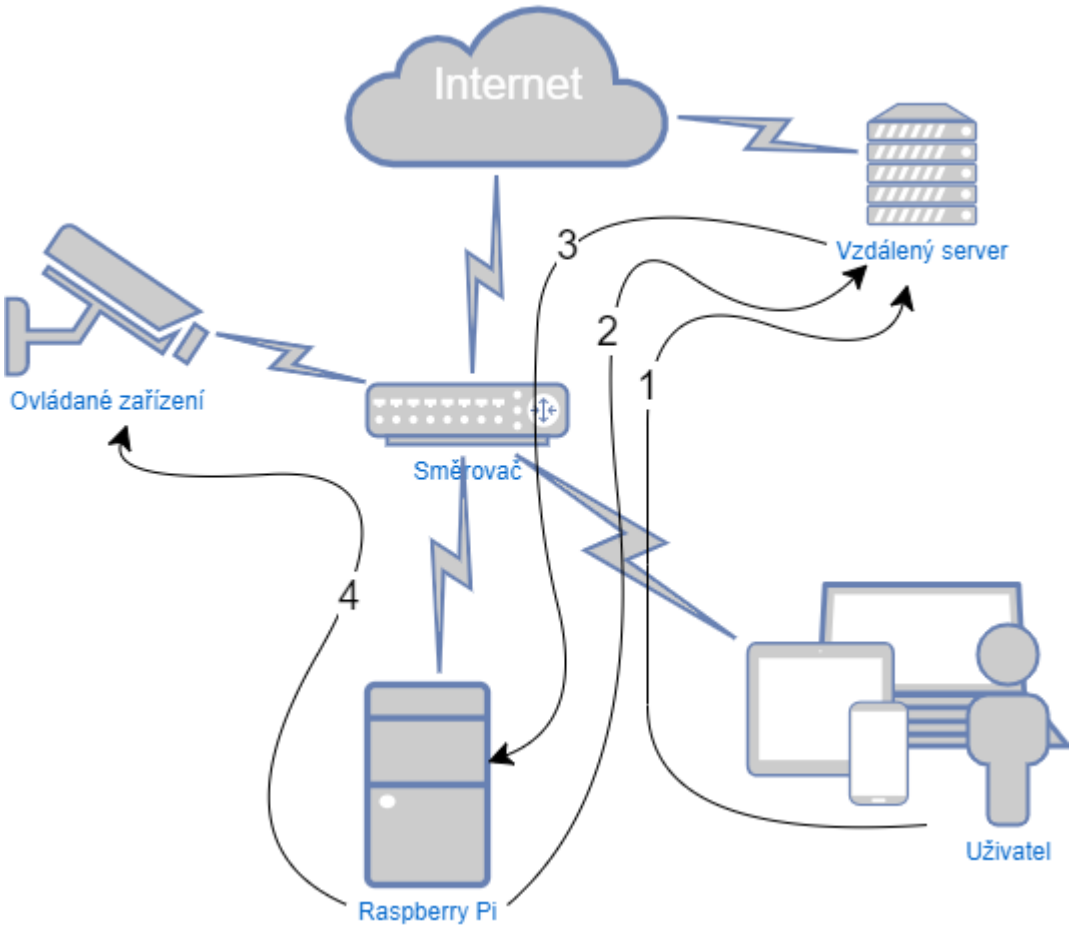
- Vstupní – pro snímání hodnoty senzoru
- Výstupní – pro spínání připojených zařízení, ať již půjde o prosté zapnutí/vypnutí zařízení, nebo ovládání výstupu pulzně šířkovou modulací (stmívání světel, nastavení úhlu natočení servo motorů…)

Samotnou konfiguraci pinů bude provádět centrální prvek a bude ji možno provádět buď z připojeného displeje, nebo z různých zařízení ovládajících domácnost (mobilních zařízení a podobně, jak již bylo zmíněno výše).

Posledním prvkem systému bude server, přijímající požadavky od zařízení ovládajících domácnost. Tento server bude určen k řízení domácnosti v globálním měřítku, to znamená, aby ji bylo možné ovládat i mimo lokální síť. Za tímto účelem bude obsahovat databázi,

obsahující informace o všech uživatelích, o všech jejich připojených zařízeních, o jejich stavu a případné instrukce pro tato zařízení (jako časované spouštění). Každý uživatel se při přístupu k tomuto veřejnému serveru bude muset autentizovat pro zajištění bezpečnosti komunikace po síti (zejména jako ochrana neautorizovaného přístupu k nějakému zařízení a k informacím o domácnosti vůbec).

Celá architektura systému je zobrazena na obr. 3.



Obr.3 – Architektura systému pro automatizaci domácnosti[2]

Jako technologii bezdrátového přenosu jsem zvolil Wi-Fi. V rámci globálního přístupu k systému nepřipadá Bluetooth, ani ZigBee v úvahu. V rámci lokální sítě je možné je sice již použít, ale protože rozšíření stávající infrastruktury sítě WLAN je snadné, a navíc centrální jednotka (Raspberry Pi) stejně musí komunikovat se směrovačem (bránou do sítě internet)

[2] Vlastní obrázek

přes WiFi, rozhodl jsem se rozhodl i při komunikaci centrální jednotky s moduly využít Wi-Fi. Další výhodou je rovněž to, že pro komunikaci prostřednictvím Wi-Fi sítě existuje větší podpora (existující knihovny pro komunikaci touto bezdrátovou technologií a množství modulů, které ji využívají…).

Volba vybavení

Na základě porovnání různých technologií, které je možné využít při budování systému pro automatizaci domácnosti, a které jsem shrnul v předchozích částech jsem se rozhodl pro následující technologické vybavení:

- Jako centrální prvek jsem zvolil využít Raspberry Pi verze 3. Tento počítač má dostatečný výkon na obsluhu dipleje, již v sobě (ve zvolené verzi) obsahuje Wi-Fi modul a díky operačnímu Raspbian, který je z rodiny UNIX systémů, podporuje mnoho nástrojů – nebude tedy problém použít přímo toto zařízení k naprogramování modulů připojených ke koncovým zařízením
- K Raspberry Pi bude připojen displej o velikosti 3.5 palce. Je to dostatečná velikost pro základní přehledné uživatelské rozhraní a zároveň se relativně malou velikostí zamezí velkým nákladům na pořízení budovaného systému. Větší velikost displeje by rovněž mohla způsobit, že by zařízení svými rozměry „překáželo“ a nedalo se použít jako malý, nenápadný prvek řídící domácnost
- Koncové modulu budou využívat čipu ESP8266. K tomu jsem se rozhodl z toho důvodu, že jejich cena je oproti výkonnějším a novějším ESP32 asi o třetinu nižší. ESP8266 svým výkonec bohatě postačují na jejich účelu v systému. Konkrétně využiji moduly „ESP-01 ESP8266 WIFI“ a „RobotDyn ESP8266-PRO"

Jak již bylo shrnuto v části „Automatizace domácnosti“, existuje mnoho různých systémů ovládání domácnosti, ať již se jedná o ta komerční, která obvykle zahrnují nějaký „chytrý“ centrální prvek, který je možné zakoupit jako plně funkční, prakticky nakonfigurované zařízení, nebo různé programové řešení (obvykle zdarma ke stažení s licencí open source) pro některou platformu jako je Raspberry Pi či BeagleBone. Přestože je některá z těchto řešení možné rozšiřovat, obvykle jsou spíše určeny pro ovládání různých komerčních zařízení, ovládaných přes Wi-Fi, jako jsou zásuvky, žárovky, rychlovarné konvice, ústřední vytápění a podobně. Záměrem mé práce bude se spíše zaměřit na ovládání a přidání inteligence různým prvkům, které ji postrádají a jsou tedy z hlediska dálkového ovládání (a potažmo automatizace domácnosti) nepoužitelné. Za tímto účelem navrhnu několik typů koncových zařízení, doplněných o dálkové ovládání. Tato koncová zařízení se budou skládat z již zmíněných koncových modulů ESP8266 a dalších modulů/součástek, rozšiřujících jejich funkčnost.

Především půjde o tyto rozšiřující prvky:

- Relé

- Stmívač
- MOSFET tranzistor pro PWM modulaci (jednak pro ovládání intenzity LED osvětlení, ale rovněž pro řízení servo motorů)

Rovněž koncové moduly osadím několika různými senzory, aby tak bylo ovládání domácnosti flexibilnější a uživatel mohl stanovit podmínky provedené různých akcí (jako například sepni topný ventilátor, pokud teplota klesne pod 15 °C, natoč žaluzie při dostatečném venkovním světle a podobně). Za účelem těchto a dalších akcí jsem se rozhodl využít těchto typů senzorů:

- Senzor vlhkosti ovzduší a teploty
- Senzor vlhkosti půdy (pro samo-zavlažování)
- Senzor intenzity osvětlení
- Detektor pohybu (PIR senzor a mikrovlnný senzor doppler)
- Hallův senzor (pro detekci otevření dveří / oken)
- Senzor přítomnosti vody (pro detekci záplavy a podobně)
- Senzor pro detekci hořlavých plynů

Je zřejmé, že konkrétní aplikace senzorů (a jejich kombinace) pak již bude záviset pouze na požadavcích uživatele, jelikož jednotlivé senzory mohou mít různé využití. Například pohybové čidlo může sloužit jako plnohodnotný zabezpečovací systém, stejně dobře, jako spínač osvětlení v místnosti – případně může plnit funkci obojího současně. Ve chvíli, kdy bude místnost zakódovaná tak bude senzor sloužit pro ochranu před vloupáním, zatímco v době odkódování bude (v případě přítmí v místnosti) spínat světlo.

***Programové vybavení**

Celá komunikace tedy bude probíhat následujícím způsobem:

Nejprve je potřeba se pomocí zařízení, schopného komunikace po síti (tablet, telefon, PC…) připojit ke vzdálenému serveru, poskytujícímu nějaké grafické uživatelské rozhraní, ve kterém bude možné nastavovat požadované akce (jako zapnutí/vypnutí nějakého ovládání zařízení, nastavení času zapnutí zařízení a podobně). Požadavek se odešle na server, kde se uloží. Raspberry pi bude posílat v pravidelných časových intervalech dotazy na vzdálený server, zda došlo ke změně stavu, a pokud ano, tak server pošle Raspberry Pi nový stav. Následně se Raspberry Pi připojí k lokálním serverům (ESP8266 modulů) a odešle jim příslušný požadavek. Celá architektura systému je zobrazena na následujícím obrázku:

4. Realizace a testování

4.1 Raspberry Pi

Aplikace

4.2 Veřejný server

Konfigurace serveru

Pro účely správy uživatelů je potřeba v databázi uchovávat relaci uživatelů. Tato relace bude mít jedinečný identifikátor, název uživatele (login) a heslo. Z důvodu ochrany před neautorizovaným přístupem však nebude heslo v databázi uloženo přímo. Při prolomení přístupu do databáze ze strany potencionálního útočníka by takový systém měl velké bezpečnostní riziko – všechna hesla v databázi by byla odhalena. Pro účely ochrany uživatelů, potažmo jejich domácnosti využiji funkci hashování. Ta převede uživatelské heslo (různé délky) na výstupní řetězec znaků fixní délky. Při přístupu k uživatelskému účtu se pak vždy porovná hash uložený v databázi s tím, který se v okamžiku přihlašování vytvoří hashovací funkcí ze zadaného hesla. Bude-li hash souhlasit, dojde k úspěšné autorizaci uživatele a ten bude přihlášen do svého účtu.

Pro samotné hashování se používají různé algoritmy. Mezi často používané patří MDA a algoritmy ze skupiny SHA. Já použiji SHA256, jelikož MDA je často označováno jako již nevyhovující pro hashování citlivých údajů, kvůli malé složitosti algoritmu. Hrozí totiž odhalení díky dnešním relativně výkonným výpočetním strojům.

MDA SHA: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=7029

https://auth0.com/blog/hashing-passwords-one-way-road-to-security/ - PYTHON!!!

https://security.blogoverflow.com/2013/09/about-secure-password-hashing/

Aplikace na zpracování požadavků

4.3 Koncové moduly

Aplikace

5. Seznam použité literatury

[A] Wi-Fi, Bluetooth, ZigBee and WiMax

[B] Bezdrátové sítě WiFi (Zandl Patrick)

[C] ITU Radio Regulations (https://www.itu.int/pub/R-REG-RR/en)

[D] https://www.minim.co/blog/wifi-frequency-bands-2.4-ghz-and-5-ghz

[E] Designing Embedded Systems with PIC Microcontrollers: Principles and Applications (Tim Wilmshurst)

[F] Embedded Systems: Architecture, Programming and Design (Raj Kamal)

[G] https://tfe.cz/ctyrkanalovy-prijimac-rfc4-rx.htm

[H] Embedded Systems Circuits and Programming (Julio Sanchez, Maria P. Canton)

[I] Microprocessor and Interfaces (A.P.Godse, D.A.Godse)

[J] https://circuitdigest.com/article/what-is-the-difference-between-microprocessor-and-microcontroller

[K] https://www.arduino.cc/en/guide/introduction

[L] Arduino Programming with .NET and Sketch (Agus Kurniawan)

[M] http://coolcosmos.ipac.caltech.edu/cosmic_classroom/cosmic_reference/whatisir.html

[N] Clinical Optics and Refraction (Andrew Keirl)

[O] The World of Physics (John Avison)

[P] Electronic, Magnetic, and Optical Materials, Second Edition (Pradeep Fulay, Jung-Kun Lee)

[Q] Wireless Communications (T. L. Singal)

[R] Guide to Computer Network Security (Joseph Migga Kizza)

[S] Home Automation Made Easy: Do It Yourself Know How Using UPB, Insteon, X10 and Z-Wave (Dennis C Brewer)

[T] https://www-sciencedirect-com.ezproxy.lib.vutbr.cz/science/article/pii/S1084804517303533

[U] https://www-sciencedirect-com.ezproxy.lib.vutbr.cz/science/article/pii/S0045790615000257

[V] https://www.chytrevypinace.cz/Sonoff-Basic-d1.htm

[W] Microwave Engineering (V.S.Bagad)

[X] https://www.indiegogo.com/projects/why-2-4ghz-chasing-wireless-history#/

[Y] Síťové aplikace a jejich architektura (Petr Matoušek)

[Z] Naučte se Python - pohotová příručka (David Ascher)

[AA] Raspberry Pi - uživatelská příručka (Eben Upton)

[AB] Bluetooth Application Deeloper's Guide (David Kammer, Gordon McNutt, Brian Senese,

Jennifer Bray)

[AC] Wireless Personal Communications: Simulation and Complexity (Mohsen A. M. El-Bendary)

[AD] Getting started with Bluetooth (Madhushree Ganguli)

[AE] https://www.espressif.com/en/products/hardware/esp8266ex/overview

[AF] https://www.espressif.com/en/products/hardware/esp32/overview

[AG] Hands-On ZigBee: Implementing 802.15.4 with Microcontrollers (Fred Eady)

[AH] Zigbee Wireless Networking (Drew Gislason)

[AI] Analog Communication (A.P.Godse U.A.Bakshi)