VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ
DEPARTMENT OF COMPUTER SYSTEMS

CHYTRÉ ZABEZPEČOVACÍ ZAŘÍZENÍ

SMART HOME SECURITY SYSTEM

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE **PETER DRAGÚŇ**
AUTHOR

VEDOUCÍ PRÁCE **Doc. Ing. ZDENĚK VAŠÍČEK, Ph.D.**
SUPERVISOR

BRNO 2020

Vysoké učení technické v Brně
Fakulta informačních technologií

Ústav počítačových systémů (UPSY) Akademický rok 2019/2020

Zadání bakalářské práce

Student: **Dragúň Peter**
Program: Informační technologie
Název: **Chytré zabezpečovací zařízení**
Smart Home Security System
Kategorie: Vestavěné systémy

Zadání:

1. Seznamte se s principem zabezpečení bytů a rodinných domů, senzory používanými v této oblasti a technologií Bluetooth Low Energy (BLE).
2. Navrhněte zabezpečovací zařízení, které bude umožňovat kromě běžných způsobů detekce vniknutí také detekci přítomnosti majitelů prostřednictvím BLE (např. přítomnost mobilního zařízení, chytrých hodinek, apod.).
3. Navržené zařízení implementujte formou prototypu (např. s využitím vývojových kitů) a ověřte jeho funkčnost. Implementujte alespoň dva bezdrátově komunikující senzory.
4. Diskutujte vlastnosti navrženého řešení a možnosti dalšího rozšíření.

Literatura:

- Dle pokynů vedoucího.

Pro udělení zápočtu za první semestr je požadováno:

- Splnění bodů 1 a 2 zadání.

Podrobné závazné pokyny pro vypracování práce viz https://www.fit.vut.cz/study/theses/

Vedoucí práce: **Vašíček Zdeněk, doc. Ing., Ph.D.**
Vedoucí ústavu: Sekanina Lukáš, prof. Ing., Ph.D.
Datum zadání: 1. listopadu 2019
Datum odevzdání: 28. května 2020
Datum schválení: 25. října 2019

Abstrakt

Práca sa zaoberá zabezpečovaním bytov a rodinných domov pomocou technológie Bluetooth Low Energy (BLE). Cieľom práce je vytvorenie a následná implementácia zabezpečovacieho zariadenia, ktoré pomocou Bluetooth dokáže detekovať prítomnosť majiteľa. V práci sú popísané zabezpečovacie systémy, technológia BLE a mikrokontrolér ESP32. Súčasťou práce je aj vytvorenie mobilnej aplikácie, ktorá slúži na nastavenie systému a jeho správu. V práci je ďalej popísaný návrh, zostrojenie prototypu a jeho implementácia. Poslednou časťou je overenie funkčnosti, testovanie a návrh možností ďalšieho rozšírenia vytvoreného prototypu.

Abstract

This thesis deals with the security of flats and houses using Bluetooth Low Energy (BLE) technology. The aim of the thesis is to develop an electronic security system for access and intrusion control exploiting the possibilities of Bluetooth Low Energy technology for improved user experience. The thesis describes security systems, BLE technology and ESP32 microcontroller. The creation of a mobile application that is used to set up the system and its management is included, as well. The thesis also describes the design, construction of a prototype and its implementation. The last part is the verification of functionality, testing and suggestions of possibilities for further improvement of the created prototype.

Kľúčové slová

zabezpečovacie zariadenie, elektronické zabezpečovacie systémy, EZS, Bluetooth Low Energy, BLE, WiFi, ESP32, pasívny infračervený senzor, PIR, magnetický kontakt

Keywords

security device, electronic security systems, ESS, Bluetooth Low Energy, BLE, WiFi, ESP32, passive infrared sensor, PIR, magnetic contact

Citácia

DRAGÚŇ, Peter. *Chytré zabezpečovací zařízení*. Brno, 2020. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Doc. Ing. Zdeněk Vašíček, Ph.D.

Chytré zabezpečovací zařízení

Prehlásenie

Prehlasujem, že som túto bakalársku prácu vypracoval samostatne pod vedením pána Doc. Ing. Zdeňka Vašíčka, Ph.D.. Uviedol som všetky literárne pramene, publikácie a ďalšie zdroje, z ktorých som čerpal.

.....
Peter Dragúň
27. mája 2020

Poďakovanie

Týmto by som chcel poďakovať hlavne vedúcemu práce, pánu doc. Ing. Zdeňku Vašíčkovi, Ph.D. za jeho odborné vedenie práce, cenné rady a zapožičanie vývojových modulov. Zároveň by som chcel poďakovať mojej rodine za podporu počas celého štúdia a počas písania práce.

Obsah

Zoznam obrázkov

Zoznam tabuliek

Kapitola 1

Úvod

V súčasnosti je čoraz častejšie zabezpečovať si svoj dom alebo byt aj inými technológiami ako je mechanické zabezpečenie. To je často jednoduché prekonať a odradí len časť potenciálnych zlodejov. Rozšírením pre tento systém môže byť napríklad domáce zabezpečovacie zariadenie alebo presnejšie elektronický zabezpečovací systém. Vďaka tomuto systému je možné identifikovať prítomnosť zlodeja aj po prekonaní mechanických systémov. Takéto zariadenia sú stále dostupnejšie a inteligentnejšie. Pri každom príchode a odchode z domu je však nutné tento systém zapnúť, respektíve vypnúť. To môže byť často otravné. Nutnosť stále zadávať kód a zároveň nezabudnúť toto zariadenie aktivovať je nevýhodou. Preto som sa rozhodol zamyslieť sa nad otázkou: Čo ak by zariadenie dokázalo detekovať prítomnosť majiteľa pri priblížení k objektu a detekovať jeho odchod?

Cieľom práce je vytvoriť zabezpečovacie zariadenie, ktoré pomocou Bluetooth dokáže detekovať prítomnosť majiteľa - jeho telefónu, hodiniek a podobne. Použitie Bluetooth je vhodné hlavne vďaka množstvu zariadení, ktoré ho podporujú. Ide hlavne o nositeľné zariadenia a zariadenia, ktoré majú ľudia stále pri sebe. Súčasťou práce bude zároveň aj vytvorenie mobilnej aplikácie, ktorá bude slúžiť na nastavenie systému a jeho správu. Podporovať by mala najrozšírenejšie mobilné operačné systémy ako Android a iOS.

Prvá časť práce sa venuje prieskumu a definovaniu rôznych technológií využívaných v navrhovanom prototype. V kapitole 2 sa zameriavam na definovanie rôznych typov zabezpečovania a využívaných prostriedkov. V ďalšej kapitole je opísaný Bluetooth Low Energy a spôsob komunikácie. Nasleduje popis mikrokontroléra použitého v systéme - ESP32.

V druhej časti práce sa venujem samotnému návrhu a implementácii zabezpečovacieho systému a spôsobu jeho nastavenia. Nasleduje zhrnutie vlastností navrhovaného systému a zamyslenie sa nad možnými rozšírenia tohoto systému.

Kapitola 2

Zabezpečovacie systémy

Vo všeobecnosti sa k zabezpečovacej technike radí viacero systémov zabezpečovania. Patria sem napríklad mechanické zábranné systémy (zámok, plot a pod.), elektronické zabezpečovacie systémy (EZS), elektronická požiarna signalizácia, systémy priemyselnej televízie (CCTV) a IP kamerové systémy. V tejto práci sa ďalej zameriam na elektronické zabezpečovacie systémy, ich využitie v domoch a bytoch. Ďalšie zabezpečovacie systémy sú spomenuté len stručne ako možné rozšírenia systému, keďže moderné zabezpečovacie systémy sa často spájajú do jedného systému, ktorý dokáže ochrániť domácnosť nie len pred zlodejmi ale aj prírodnými živlami.

2.1 Elektronické zabezpečovacie systémy

Elektronický zabezpečovací systém je poplachový systém pre detekciu a indikáciu prítomnosti, vstupu alebo pokusu o vstup narušiteľa do stráženého objektu. Rozdeľujeme ich podľa stupňa zabezpečenia do 4 kategórií, viď tabuľka 2.1.

Stupeň	**Miera rizika**	**Predpokladaný typ narušiteľa**
1	nízke	narušiteľ má malú znalosť EZS; obmedzený sortiment ľahko dostupných nástrojov
2	nízke až stredné	narušiteľ má určité znalosti o EZS; obmedzený sortiment základných prenosných prístrojov (napríklad multimeter)
3	stredné až vysoké	narušiteľ je oboznámený s EZS; úplný sortiment prenosných prístrojov a elektronických zariadení
4	vysoké	narušiteľ je schopný alebo má možnosť spracovať podrobný plán vniknutia; kompletný sortiment zariadení vrátane prostriedkov pre náhradu rozhodujúcich prvkov EZS

Tabuľka 2.1: Stupne zabezpečenia[13][6]

Klasické zabezpečovacie systémy používané v domácnostiach spadajú do stupňa zabezpečenia 1 až 2, teda nízke až stredné zabezpečenie. Existujú však systémy vyššieho stupňa aj pre domácnosti, ide však o nákladnejšie systémy.

Elektronické zabezpečovacie systémy sa vo všeobecnosti skladajú z rôznych prvkov. Sem patria prvky:[12]

- plášťovej ochrany
- tiesňovej ochrany - verejné alebo skryté
- ovládacie zariadenia
- ústredne EZS
- signalizačné (výstražné) zariadenia - siréna, maják
- priestorovej ochrany
- predmetovej ochrany - napríklad na ochranu zavesených predmetov ako obrazy
- vonkajšej obvodovej ochrany

Podľa normy ČSN EN 50131-1 musí EZS obsahovať:

- ústredňu,
- jeden alebo viac detektorov,
- jedno alebo viac signalizačných zariadení prípadne poplachových prenosných systémov,
- jedno alebo viac napájacích zariadení.

Všetky komponenty EZS musia podľa normy ČSN EN 50131-1 zaisťovať detekciu sabotáže. Teda musia obsahovať prostriedky k zamedzeniu prístupu k vnútorným súčiastkam, normálny prístup musí vyžadovať využitie vhodného nástroja. Prístup k prostriedkom určeným k orientácii zorného poľa detektoru nesmie byť prístupný neoprávneným osobám.[13]

2.1.1 Ústredňa EZS

Je zariadenie určené k príjmu a vyhodnocovaniu výstupných elektrických signálov čidiel alebo tiesňových hlásičov a k vytvoreniu signálu o narušení. V prípade drôtových ústrední slúži zároveň aj ako zdroj napájania pre senzory. Medzi jej ďalšie funkcie patrí diagnostika systému a uvedenie systému do stavu stráženia alebo do stavu pokoja. Vstupom do ústredne sú vstupné vyhodnocovacie obvody, ktoré vyhodnocujú prijaté informácie zo senzorov. Zároveň do vstupov môžeme zaradiť aj ovládacie prvky systému. Výstupom sú indikačné zariadenia pre optickú a akustickú signalizáciu. Ústredňa môže byť doplnená aj o výstup telefónneho voliča alebo pripojenie na internet. Tie slúžia pre identifikovanie poplachu aj v prípade poškodenia indikačných zariadení alebo použitia takzvaného tichého poplachu, teda bez spustenia optickej a zvukovej signalizácie.

Ústredne je možné rozdeliť do štyroch základných skupín:

- **slučkové** - pre každú poplachovú slučku má vlastný obvod, tie sú tvorené najčastejšie sériovým zapojením čidiel. Zmena odporu na slučke detekuje aktiváciu čidla alebo sabotáž na slučke. Systém má pomerne rozsiahlu káblovú sieť.

- **s priamou adresáciou čidiel** - fungujú na princípe komunikácie na dátovej zbernici. Ústredňa generuje adresy jednotlivých čidiel a prijíma odozvy. Káblová sieť je minimálna. Ústredňa dokáže identifikovať čidlo, ktoré spôsobilo poplach.
- **zmiešaného typu** - využívajú princíp dátovej komunikácie s koncentrátorom. Ten je pripojený na samotné čidlá pomocou slučiek.
- **s bezdrôtovým prenosom signálu od čidiel** - ide o najnovší typ ústrední. Najčastejšie pracujú v pásme 433 MHz s výkonom okolo 10 mW. Vlastný dosah vo voľnom prostredí je 100 - 200 m. Čidlá sú napájané z batérie. Podľa druhu komunikácie medzi ústredňou a čidlami môže tieto systémy ďalej rozdeliť na:
  - *s jednosmernou komunikáciou* - jednoduchšie systémy, v čidle sa nachádza vysielač a v ústredni prijímač. Najčastejšie pracujú pomocou systému pravidelnej kontroly vysielaním kontrolných telegramov. Vďaka tejto kontrole dokáže ústredňa zistiť poruchu či poškodenie čidla. Problémom týchto systémov je, že v prípade zaznamenania pohybu odosielajú poplachovú správu aj v prípade, že sa systém nachádza v stave odstrážené, to zbytočne vyčerpáva energiu zdroja. To je spôsobené tým, že čidlá nemajú informáciu o stave systému. Zároveň sú náchylnejšie na rušenie signálu, pretože kmitočet a modulácia sú nemenné.
  - *s obojsmernou komunikáciou* - každý prvok systému je vybavený vysielačom aj prijímačom. Výhodou oproti systémom s jednosmernou komunikáciou je, že systémy v stave pokoja nevysielajú, pri zapínaní systému si ústredňa overí stav prvkov, pri rušení je možné automatické preladenie na voľný kanál.

V súčasnosti medzi najpoužívanejšie patria bezdrôtové systémy. Výhodou je hlavne jednoduchá inštalácia, ľahké rozšírenie systému o ďalšie senzory, flexibilita systému, napríklad pri zmene rozostavenia nábytku a podobne. Tento spôsob komunikácie však prináša aj mnoho problémov, ktoré je potrebné riešiť. Jednou z nevýhod je napríklad nebezpečie rušenia komunikácie. To môže viesť k vzniku falošného poplachu, či strate spojenia. Samozrejmou požiadavkou je aj kódovanie komunikácie medzi prvkami systému. To znemožňuje skreslenie prenosu a zabraňuje neoprávnenému preniknutiu do systému.[6]

Napájanie ústredne

Keďže EZS musí fungovať aj v prípade výpadku elektrickej energie, musí byť napájací zdroj zálohovaný náhradným zdrojom napätia. Systém je teda okrem základného zdroja, ktorý slúži na trvalé napájanie EZS, vybavený aj náhradným napájacím zdrojom. Jeho kapacita sa líši podľa stupňa zabezpečenia (viď tabuľka 2.1) a je definovaná v norme ČSN EN 50131-1.

Zóny stráženia

Podľa reakcie ústredne na výstupný signál z detektoru rozlišujeme rôzne typy slučiek, resp. zón. Medzi základné radíme:

- **okamžitá slučka** - v pohotovostnom režime ústredňa nereaguje, v režime stráženia spôsobuje okamžite vyhlásenie poplachu. Do slučky sa pridávajú detektory, kde sa nepredpokladá pohyb užívateľov počas ochrany objektu.
- **oneskorená slučka** - v pohotovostnom režime ústredňa nereaguje, v režime stráženia ústredňa vyhlási poplach až po presne stanovenom čase. Do oneskorených slučiek sú

zapojené senzory, ktoré sa nachádzajú pri ovládacích prvkoch EZS (pri vstupe do objektu).

- **trvalá slučka** - ústredňa reaguje na narušenie okamžitým poplachom v stave strážení aj v pohotovostnom režime.

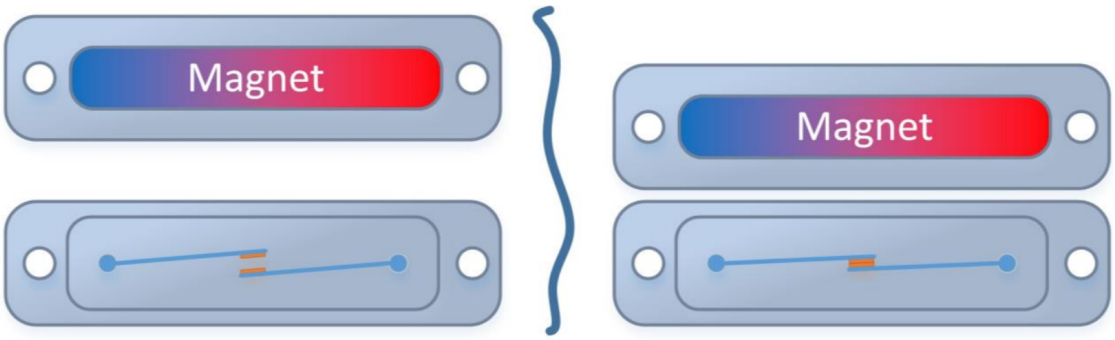
Tieto základné typy môžu byť prípadne modifikované a rozšírené o ďalšie.[12]

2.1.2 Detektory

Detektor alebo čidlo EZS je zariadenie reagujúce na narušenie stráženého objektu vytvorením určitého výstupného poplachového signálu. Časť detektoru, ktorá sníma zmenu stavu nazývame senzor. Poznáme rôzne druhy detektorov. Podľa typu napájania ich môžeme rozdeliť na nenapájané a napájané, podľa druhu zabezpečenia na priestorové a smerové.

Magnetický kontakt

Je určený na stráženie stavebných otvorov ako sú okná, dvere, rolety a podobne. Tvorí ho vždy dvojica dielov - jazýčkový kontakt a permanentný magnet. Jazýčkový kontakt je tvorený zatavenou sklenenou rúrkou, naplnenou ochrannou atmosférou. V nej sú umiestnené dva feromagnetické kontakty. Magnet sa montuje na pohyblivú časť okna (dverí) a jazýčkový kontakt na rám. V prípade, že sa magnet priblíži k jazýčkovému kontaktu, kontakty sa spoja viď obrázok 2.1. V prípade, že sa magnet vzdiali, kontakty sa znova rozopnú. Magnetický kontakt môže byť zabudovaný aj priamo do rámu dverí alebo okna, to umožňuje skrytú montáž.[12]



Obr. 2.1: Princíp činnosti magnetického kontaktu[5]

Detektory rozbitia skla

Keďže najjednoduchším spôsobom ako preniknúť do stráženého objektu je práve cez rozbité okno je dôležité myslieť na ich ochranu. Existuje hneď niekoľko spôsobov ako detekovať rozbitie skla:

- **poplachové fólie** - pracujú na princípe vodivých pásikov alebo plôch zaliatych vo vnútri fólie. Poplach je vyvolaný prerušením vodivého pásika. Nalepujú sa na sklenené výplne dverí, okien a výkladov.

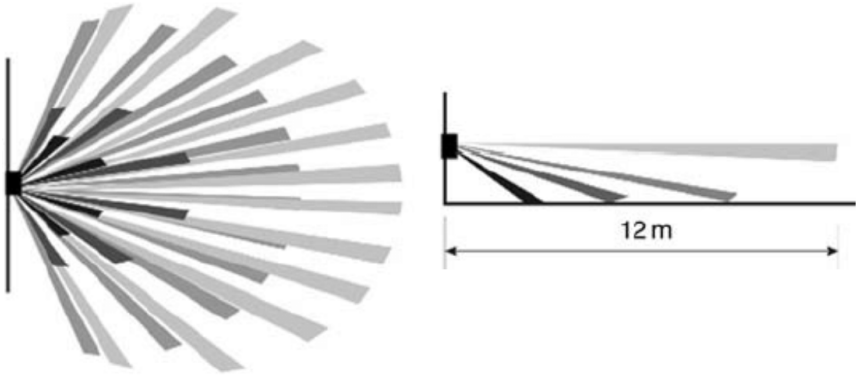
- **kontaktné snímače** - pracujú na princípe uzavretého elektrického obvodu. Rozbitím skla sa naruší a vyvolá tak poplach. Nedostatkom je nízka odolnosť voči vyrazeniu skla.
- **piezoelektrické snímače** - vyhodnocujú otrasy na skle, ktoré vznikajú pri rozbití, rezaní skla. Umiestňujú sa do rohu skla a majú dosah 1,5 až 3 m.
- **akustické detektory rozbitia skla** - detekujú zvuk rozbitia skla pomocou mikrofónu. Majú dosah až 10 m od stráženého skla. Sú náchylnejšie na falošné poplachy, ktoré môže vyvolať zvoniaci telefón, rozbitie skla vonku či brzdenie električky.

Pasívne infračervené detektory

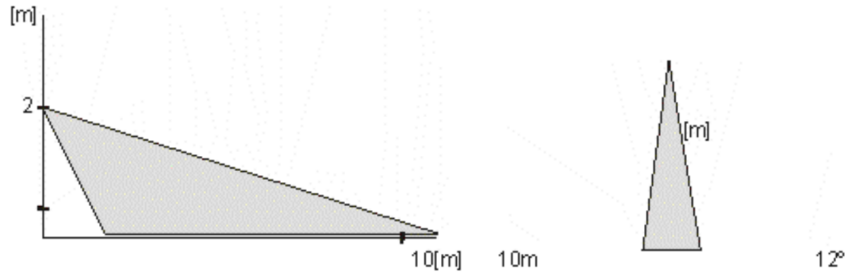
Pasívne infračervené detektory (PIR – Passive Infrared Receiver) snímajú zmeny v infračervenom pásme elektromagnetického vlnenia vo svojom okolí, na ich základe následne vyhodnocujú narušenie. Využíva sa pyroelektrický senzor, ktorý reaguje na pohybujúce sa teleso s teplotou odlišnou od teploty okolia. Ten je doplnený o optický systém, ktorý má funkciu zosilnenia signálu a zvýšenie citlivosti senzora. Využívajú sa Fresnelové šošovky alebo často sústava lomených zrkadiel napríklad tzv. čierne zrkadlo, ktoré neodráža viditeľne svetlo, ale naopak dobre odráža žiarenie vygenerované ľudským telom. PIR detektor je najcitlivejší na pohyb kolmý na optickú os detektora. Tieto detektory sú veľmi populárne najmä vďaka ich pomerne jednoduchej konštrukcii a nízkej cene. Ich výhodou je tiež, že dokážu detekovať prítomnosť človeka bez ožarovania elektromagnetickým vlnením, na ktoré môžu byť ľudia citlivý.[12]

V prípade EZS stupňa 3 a 4 (definované v tabuľke 2.1) musia byť detektory pohybu doplnené aj prostriedkami pre detekciu zakrytia (maskovania).[13]

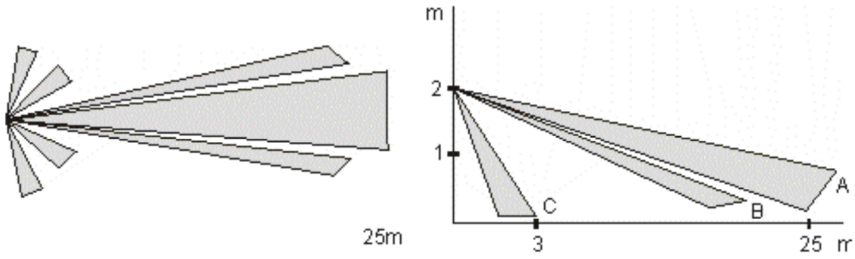
Na trhu sú dostupné detektory s rôznymi detekčnými charakteristikami (vejár, chodba, záves), ktorých typ závisí od použitia danej šošovky. Ich detekčné charakteristiky môžeme vidieť na obrázkoch 2.2, 2.3, 2.4 a 2.5. V ľavej časti môžeme vidieť pohľad zhora a v pravej časti pohľad zo strany.



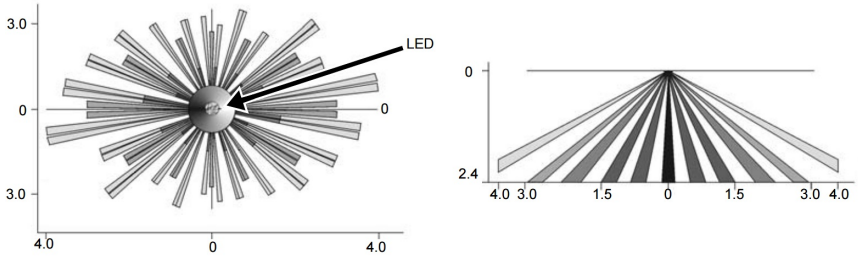
Obr. 2.2: Detekčná charakteristika PIR typu vejár[4]



Obr. 2.3: Detekčná charakteristika PIR typu záclona[12]



Obr. 2.4: Detekčná charakteristika PIR typu chodba[12]



Obr. 2.5: Detekčná charakteristika stropného PIR senzora[8]

Ultrazvukové detektory

Patria medzi aktívne prvky, teda do priestoru vysielajú energiu. Vysielač vysiela vlnenie konštantnej frekvencie nad pásmom počuteľného zvuku. Následne prijímač prijíma odrazený zvuk a vyhodnocuje fázy, ktoré vznikajú pri pohybe telesa v chránenom priestore. Jedná sa v podstate o aplikáciu Dopplerovho javu v pásme ultrazvuku. Na ultrazvuk môžu byť citlivé zvieratá (pes, netopier a pod.), ktoré tento zvuk môžu počuť. Dosah detektoru je približne 10 m. Ich citlivosť sa môže znížiť v prítomnosti materiálov, ktoré pohlcujú zvuk ako koberce, penové materiály a podobne.[6]

Mikrovlnné detektory

Vychádzajú z rovnakého princípu ako ultrazvukové detektory, pracujú však vo frekvenčnom pásme elektromagnetického vlnenia. Taktiež patria medzi aktívne prvky. Ich typický dosah je 15 až 30m. Na rozdiel od ultrazvukových a PIR senzorov sú citlivé na rušenie z okolia, preto je pravdepodobnosť vzniku falošného poplachu vyššia.[12]

Duálne detektory

Ide o spojenie PIR a ultrazvukového, prípadne mikrovlnného detektoru. Myšlienka za spojením je, že je malá pravdepodobnosť súčasného vzniku javov, ktoré by mohli vyvolať falošný poplach pri viacerých čidlách pracujúcich na rozdielnych fyzikálnych princípoch. Zároveň zvyšujú odolnosť voči poruchám. Detektory často umožňujú dve nastavenia - poplach sa spustí pri reakcii oboch čidiel alebo na vyvolanie poplachu stačí ľubovoľný detektor.[12]

2.1.3 Overovanie spojenia

Integrita spojenia senzorov s ústredňou musí byť pravidelne kontrolovaná v intervaloch špecifikovaných v tabuľke 2.2. Stupňom rozumieme stupeň zabezpečenia definovaný v tabuľke 2.1 a jednotlivé časy sú maximálne prípustné intervaly medzi signálmi alebo správami komunikácie. V prípade, že komunikácia nie je v tomto čase overená, systém by mal vyvolať oznámenie o poruche, prípadne o sabotáži. Zároveň systém nesmie byť prepnutý do stavu stráženia, ak nebola komunikácia overená v intervale podľa tabuľky 2.2.

	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Periodická komunikácia	240 min	120 min	100 s	10 s
Nastavovanie stavu stráženia	60 min	20 min	60 s	10 s

Tabuľka 2.2: Intervaly overovania[13]

2.1.4 Ovládacie a indikačné zariadenia

Ovládacie prvky slúžia na uvedenie systému do stavu stráženia alebo do stavu pokoja. Zároveň slúžia aj na zadávanie užívateľských kódov pre ovládanie systému, odstavenie poplachu, základnú správu systému.

- **blokovací zámok** - kombinuje mechanické zabezpečenie vstupných dverí s ovládaním EZS. Pri odomknutí dverí sa systém automaticky uvedie do stavu odstrážené. Zároveň pri zamykaní sa systém uvedie do stavu zabezpečené. Zámok je pritom možné uzamknúť len ak je EZS v normálnom stave. Použitie je prirodzené a jednoduché. Ide o jeden z najnákladnejších spôsobov ovládania systému.
- **spínací zámok** - podobný blokovaciemu zámku, neobsahuje systém blokovania uzamknutia dverí v prípade poruchy či chyby obsluhy (napríklad otvorené okno).
- **kódové klávesnice** - je nutné, aby elektronika klávesnice bola umiestnená v strážených priestoroch. Prináša nevýhodu, že užívateľ si musí zapamätať kód. Ten je však potrebné pravidelne meniť.
- **ovládanie kartou** - výhodou je multifunkčnosť karty, a teda možnosť využiť ju na ďalšie použitie ako obedy, dochádzkový systém, parkovanie a podobne. Nevýhodou je prenosnosť karty, prípadne možnosť jej skopírovania.
- **diaľkové ovládanie** - musí byť chránené vhodným kódom, aby sa nedal zachytiť jeho signál a vyrobiť kópia. Môže byť doplnené aj o ďalšie funkcie ako spustenie tiesňového hlásenia a pod.[12]

Indikačné prvky informujú o stave systému napríklad pomocou LED diódy, akustickej, vizuálnej signalizácie, prípadne ich kombináciou. Medzi najbežnejšie hlásenia patria:

- stav pokoja/stráženia
- uvádzanie do stavu stráženia
- hlásenie poruchy
- poplach

Akustické výstražné zariadenie musí byť v prevádzke aspoň 90 sekúnd pričom maximálna doba jeho činnosti nesmie prekročiť 15 minút.[13]

Systém môže byť doplnený o ďalšie doplnkové zariadenia, ktoré slúžia na komunikáciu s pultom centrálnej ochrany alebo na komunikáciu s majiteľom.[6]

Kapitola 3

Bluetooth Low Energy

Bluetooth je technológia na bezdrôtovú komunikáciu medzi dvoma a viacerými zariadeniami. Má široké využitie od rôznych ovládačov, cez prehrávanie hudby až po prenos súborov medzi zariadeniami. Operuje v rovnakom frekvenčnom pásme ako technológia Wi-Fi - 2,4 GHz. Vďaka tomu môžu menšie zariadenia využívajúce obe technológie súčasne používať spoločnú anténu, to však prináša aj nevýhodu v podobe rušenia.

Bluetooth Low Energy (BLE) je navrhované pre nízkoenergetickú operáciu. Od Bluetooth verzie 4.0 je súčasťou štandardu. Je primárne učené na výmenu kratších informácií nižšou rýchlosťou. Tento štandard je často využívaný pri zaradeniach napájaných z batérie, ako sú napríklad zariadenia Internetu vecí (IoT). Zariadenia s podporou tejto technológie sú označované často ako *Bluetooth Smart*, respektíve *Bluetooth Smart Ready* pre zariadenia spájajúce BLE a klasické Bluetooth.

3.1 Porovnanie s klasickým Bluetooth

Obe technológie využívajú rovnaké frekvenčné pásmo 2,402 - 2,480 GHz. Využívajú však rozdielny počet a rozostupy kanálov. BLE obsahuje 40 kanálov s rozostupom 2 MHz. Z toho sú 3 kanály určené na prenos informácií o zariadení tzv. *advertising*, zvyšných 37 kanálov je určených na prenos dát. V prípade klasického Bluetooth je týchto kanálov 79 a s rozostupom 1 MHz. V závislosti na použitej fyzickej vrstve protokol BLE dosahuje rýchlosť až 2 Mb/s (Bluetooth v5.0), oproti tomu klasické Bluetooth dosahuje rýchlosť až 3 Mb/s. BLE je v závislosti na použití 2 až 100 krát menej náročné na spotrebu energie. [1]

3.2 Topológia

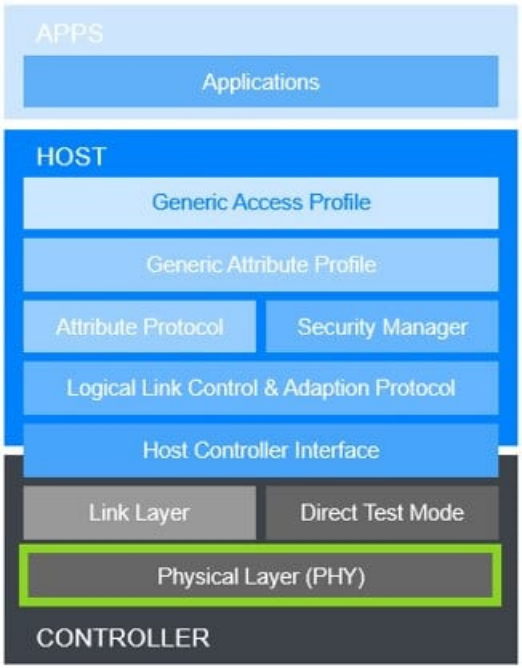
Bluetooth Low Energy dokáže pracovať s tromi rôznymi topológiami siete:

- **Point-to-point** - komunikácia medzi dvomi zariadeniami (1:1), je podporovaná ako pre BLE tak aj pre Bluetooth. Využíva sa napríklad na prehrávanie hudby. Táto topológia je vhodná pre rôzne typy zariadení. V prípade BLE sa táto topológia využíva napríklad pre fitnes zariadenia, merače tepu, periférie a príslušenstvo pre počítač.
- **Broadcast** - jedno zariadenie komunikuje s viacerými zariadeniami (1:M). Táto topológia je podporovaná len v BLE, využíva sa napríklad na lokalizáciu a navigáciu vo vnútri budovy.

- **Mesh** - komunikácia viacerých zariadení (M:N), je podporovaná len pre BLE. Vďaka tejto topológii je možné vytvoriť veľkú sieť zariadení. Táto topológia je vhodná ak je potrebné spojiť desiatky, stovky či tisícky zariadení, ktoré potrebujú medzi sebou spoľahlivo a bezpečne komunikovať. Využitie má napríklad v monitorovaní alebo automatizácii.[1]

3.3 Architektúra

Bluetooth implementuje kompletnú architektúru od fyzickej komunikácie medzi zariadeniami až po komunikáciu s vlastnými aplikáciami. Bluetooth je teda takzvaný *full protocol stack*. Kompletnú architektúru môžeme vidieť na obrázku 3.1.



Obr. 3.1: Architektúra BLE[1]

- **Physical Layer (PHY)** - fyzická vrstva, prenáša samotný analógový signál a transformuje ho na digitálny. Od Bluetooth v5.0 rozlišujeme 3 varianty PHY. Sú to:
  - LE 1M - rýchlosť prenosu dát 1 Mb/s, pôvodná PHY definovaná v Bluetooth v4.0, chyby dokáže detekovať, ale nie opraviť
  - LE 2M - rýchlosť 2 Mb/s, vzdialenosť prenosu je oproti LE 1M zmenšená na približne 80 %, chyby dokáže detekovať, ale nie opraviť
  - LE Coded - dokáže teoreticky zvýšiť vzdialenosť prenosu dvoj až štvornásobne, a to pomocou redundancie dát v odosielanom pakete. Vďaka tomu zariadenie na druhej strane dokáže detekovať a opraviť chyby v dátach. Existujú dva varianty v závislosti na úrovni redundancie - S=2 a S=8, kde S udáva počet redundantných dát v odosielanom pakete. To ma však nepriaznivý vplyv na rýchlosť odosielania, ktorá je znížená na 500 Kb/s, respektíve pre S=8 na 125 Kb/s.

- **Link Layer** - linková vrstva, jej úlohou je skenovanie, spravuje, vytvára spojenia
- **Direct Test Mode** - umožňuje testovanie fyzickej vrstvy
- **Host Controller Interface (HCI)** - sprostredkúva komunikáciu medzi vrstvami, môže využívať API alebo aj iné štandardné rozhrania ako USB, UART, SPI.
- **Logical Link Control and Adaption protocol (L2CAP)** - zapuzdruje dáta pre ďalšie vrstvy
- **Attribute Protocol** - samotné zdieľané dáta
- **Security Manager** - zabezpečuje párovanie a distribúciu kľúčov
- **Generic Attribute Profile (GATT)**
- **Generic Access Profile (GAP)** - priama komunikácia s aplikáciou, zabezpečuje pripojenia na služby pre BLE zariadenie [1][10]

Bližšie sa k GAP a GATT venujem v nasledujúcich podkapitolách 3.5 a 3.6.1.

3.4 Rozsah pokrytia

Rozsah pokrytia Bluetooth je závislý na viacerých faktoroch. Teoreticky je možné dosiahnuť vzdialenosť od metra až cez jeden kilometer. Bluetooth je navrhované na podporu rôznych rozsahov, konkrétna implementácia je ponechaná na vývojároch, aby si vybrali vhodné riešenie pre ich potreby. Jedným z faktorov je výber fyzickej vrstvy (PHY), kde rozdiely boli spomínané už v podkapitole 3.3. Ďalšími faktormi sú senzitivita prijímača, vysielací výkon, dosah antény alebo strata signálu po ceste, napríklad vďaka prekážkam a podobne.[1]

3.5 Generic Access Profile (GAP)

Ide o základný profil, ktorý implementujú všetky Bluetooth zariadenia. Definuje základné požiadavky zariadenia. Vyskytuje sa ako v klasickej (BR/EDR) verzii tak aj v Low Energy. Pre BLE definuje jednotlivé vrstvy architektúry, správanie a metódy pre vyhľadanie zariadenia, pripojenie k nemu, bezpečnosť a podobne. Zároveň definuje 4 špecifické roly, pričom zariadenie môže podporovať viacero rolí súčasne. Každá z rolí je optimalizovaná na špecifické použitie. Sú to:

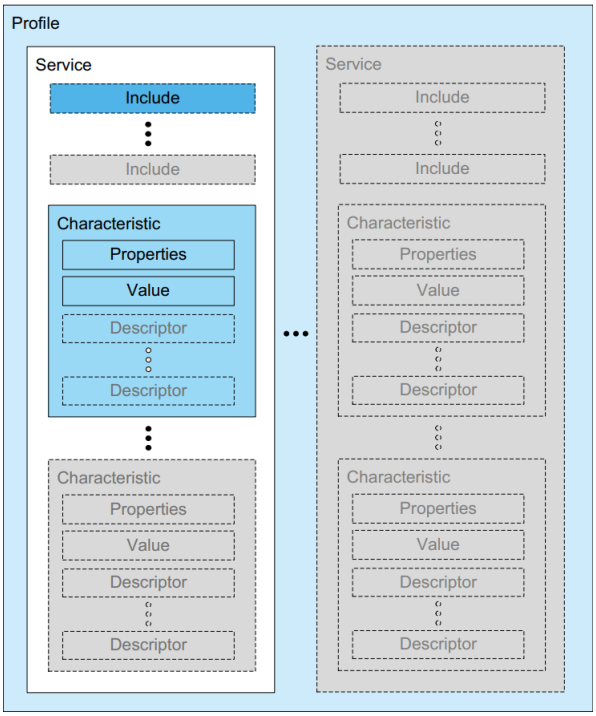
- **Broadcaster** - vysielanie dát, nepodporuje spojenia
- **Observer** - prijímanie dát, komplementárny k Broadcaster, nepodporuje spojenia
- **Peripheral** - podporuje jedno spojenie, menej komplexné ako Central
- **Central** - podporuje niekoľko spojení[1]

3.6 Attribute Protocol

Umožňuje čítať a zapisovať malé dáta na server. Každá hodnota, typicky pár bajtov, sa nazýva atribút (attribute). Tento protokol definuje pre každú hodnotu univerzálnu unikátnu identifikáciu - UUID. Tie môžu mať dĺžku 16, 32 alebo 128 bitov. Protokol definuje dve roly - klient a server. Zariadenie dokáže zároveň fungovať ako server aj ako klient. Server ukladá dáta a akceptuje požiadavky, príkazy a potvrdenia od klienta. Taktiež odosiela odpovede a upozornenia pri výskyte špecifikovanej udalosti na serveri.[1]

3.6.1 Generic Attribute Profile (GATT)

GATT definuje hierarchickú štruktúru dát. Je postavený na Attribute profile, definuje operácie nad dátami uloženými a zasielanými pomocou neho. Taktiež špecifikuje formát dát, ktoré sa nachádzajú na serveri. Dáta sú formátované ako služby (services) a charakteristiky (characteristics). Jedna služba môže obsahovať niekoľko charakteristík. Služby môžu byť aj zanorené, pričom zanorená služba existuje aj samostatne aj v rámci nadradenej služby. Charakteristiky obsahujú jednu hodnotu, jej vlastnosti a môžu obsahovať aj niekoľko deskriptorov, ktoré opisujú hodnotu. Na obrázku 3.2 je možné vidieť ako by napríklad mohla vyzerať hierarchia GATT.[1]



Obr. 3.2: Profilová hierarchia založená na GATT[1]

3.7 Párovanie zariadení

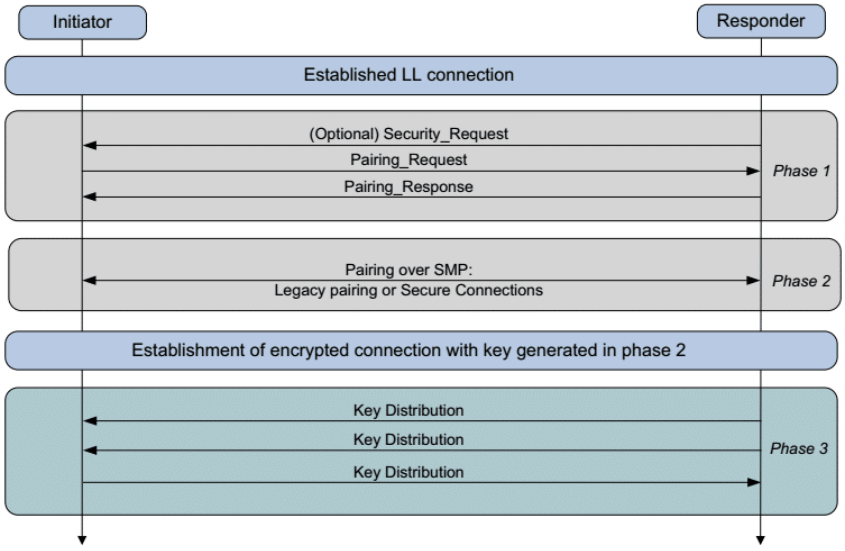
Pri BLE môžeme rozlišovať dva spôsoby spojenia zariadení a výmeny kľúčov. V prípade, že ide o dočasné kľúče a krátkodobé tzv. *párovanie*, je spojenie len dočasné a je nutné pri každom párovaní znova vymeniť nové dočasné kľúče. V prípade viazania alebo presnejšie

bonding si zariadenia uložia dlhodobé kľúče do internej pamäte. Vďaka tomu dokážu šifrovať komunikáciu, overovať podpísané dáta a rozšifrovať náhodne generované adresy. Proces viazania (bonding) zariadení môžeme rozdeliť na 3 fázy. Tento proces môžeme pre názornosť lepšie vidieť na obrázku 3.3. V prípade párovania je postup rovnaký, ale končí sa fázou 2. Tieto fázy sú:

- fáza 1 - výmena informácii o podporovaných vstupoch a výstupoch (napríklad obrazovka a klávesnica, tie sú využité pre zadanie alebo zobrazenie dočasného kľúča), možnostiach zabezpečenia ako ochrana proti odchytávaniu komunikácie alebo tzv. *Man-In-The-Middle* útoku. Nasleduje výmena párovacej informácie medzi zariadeniami. Okrem iného je v týchto paketoch znak definujúci, či sa jedná len o párovanie alebo následne aj bonding.

- fáza 2 - nasleduje výmena dočasných kľúčov pre šifrovanie komunikácie. Existuje niekoľko spôsobov výmeny týchto kľúčov. Časté je generovanie 6 miestneho kódu na jednej strane a prepísanie na druhej. Ďalšie spôsoby sú porovnávanie kódov, jednoduché potvrdenie tlačidlom alebo využitie inej technológie na distribúciu kľúča (napr. NFC). Pokračuje sa overením kľúčov. V prípade párovania nasleduje odosielanie samotných dát.

- fáza 3 - Táto časť komunikácie je už šifrovaná kľúčmi vygenerovanými vo fáze 2. Nasleduje generovanie a výmena dlhodobých kľúčov a výmena samotných dát. Pri ďalšom pripojení tento proces nie je potrebné opakovať.[1]



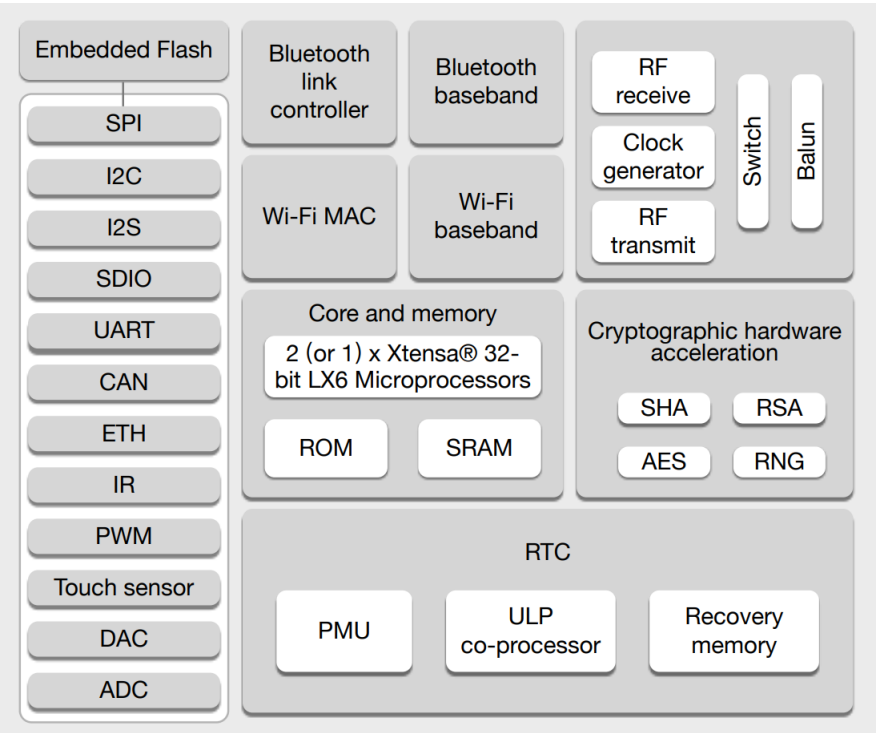
Obr. 3.3: Bonding diagram komunikácie[1]

Kapitola 4

ESP32

ESP32 je populárna séria systémov na čipe (SoC - System on chip) od spoločnosti Espressif Systems, ktorá vznikla v roku 2016. Je nasledovníkom známeho ESP2866. Ide o výkonnejší modul, ktorý má veľa ďalších vlastností ako podporu Bluetooth, viac univerzálnych vstupno-výstupných (GPIO) pinov a podobne. V závislosti na variante existujú rôzne výkonné modely s rôznymi vlastnosťami. Vďaka jeho pomerne nízkej cene a nízkej spotrebe je vhodný na automatizáciu domácnosti, v IoT zariadeniach, v medicíne, priemysle a podobne. Bol navrhnutý ako samostatne fungujúci mikrokontrolér s ohľadom na maximálny výkon s minimálnou spotrebou energie.

4.1 Architektúra



Obr. 4.1: Funkčný blokový diagram ESP32[2]

Jadrom ESP32 je 32-bitový procesor Xtensa s jedným alebo dvomi jadrami a frekvenciou až 240Mhz, ten je doplnený o 520 KB SRAM a 448 KB ROM. Zároveň na čipe môžeme nájsť podporu aj pre Wi-Fi 2,4 Ghz (802.11 b/g/n), Bluetooth v4.2 BR/EDR aj BLE (podľa aktuálnych informácií bol certifikovaný aj na v5.0[1]). Čip má podporu aj pre hardvérovú akceleráciu šifrovania, množstvo rôznych periférií a 34 vstupno-výstupných portov (GPIO). Celý blokový diagram je znázornený na obrázku 4.1.[2]

4.2 Varianty

ESP32 je dostupné v niekoľkých verziách. Tie môžeme v základe rozdeliť na SoC, moduly a vývojové dosky, viď obrázok 4.2. Tie sa ďalej rozdeľujú napríklad podľa špecifikácií a dostupných súčastí. Súčasťou modulov a vývojových dosiek býva často aj anténa vytlačená priamo na doske, prípadne je možnosť pripojenia externej antény, ktorou sa dokáže zväčšiť dosah zariadenia. Existujú rôzne varianty vývojových modulov, často môžme nájsť varianty s pridanou funkcionalitou ako je napríklad kamera, čítačka microSD kariet a podobne.

(a) SoC[2] (b) Modul[3] (c) Vývojová doska[4]

Obr. 4.2: Varianty ESP32

4.3 Programovanie

Existuje viacero možností programovania ESP32. Asi najznámejším a najpoužívanejším je Arduino IDE, prípadne editor s rozšírením PlatformIO. Obe možnosti využívajú pre programovanie jazyk C++. Ide o riešenie s jednoduchou inštaláciou, ktoré ponúka menej možností a väčšie výsledné programy. Na základné aplikácie je často postačujúce. Knižnica je aktualizovaná menej často, čo môže priniesť niekoľko problémov.

Ďalšou z možností je využite frameworku ESP-IDF, ktorý v podstate rieši všetky problémy spomínané v knižnici pre Arduino IDE. Prináša však malú nevýhodu programovania v C a zložitejšiu inštaláciu. Tento nástroj je vyvíjaný samotnou spoločnosťou Espressif Systems a je označovaný za preferovanú formu programovania mikrokontroléru. Je založený na operačnom systéme reálneho času (RTOS), konkrétne na FreeRTOS s otvoreným kódom.

Jednou z možností je aj použitie MicroPython, ktorý je založený na Pythone 3.4 a prináša teda výhody vyššieho programovacieho jazyka. Ide o menej bežný spôsob, a teda

[1] `https://www.espressif.com/en/news/BLE_5.0_Certification`

[2] prevzaté z: `https://www.gridconnect.com/products/esp32-d0wdq6-2-4-ghz-wi-fi-bluetooth-combo-chip`

[3] prevzaté z: `https://www.blueberrye.me/compute-boards/esp-wroom-32-esp32-wifi-bt-ble-mcu-module/a-1690130`

[4] prevzaté z: `https://navody.arduino-shop.cz/navody-k-produktum/vyvojova-deska-esp32.html`

existuje na neho menej príkladov a návodov. Zostavenie je založené na frameworku ESP-IDF. Oproti predchádzajúcemu spôsobu ponúka menšie možnosti konfigurácie a menej časté aktualizácie knižnice.

4.4 Režim spánku

ESP32 podporuje niekoľko režimov spánku čo pomáha ešte viac zmenšovať jeho spotrebu. V tabuľke 4.1 je možné vidieť porovnanie jednotlivých módov šetrenia energie. V poslednom stĺpci tabuľky sú uvedené len pridané časti, takže pre aktuálny riadok platí to isté čo pre predchádzajúci plus naviac informácie v tomto riadku.

Ako prvý je pre porovnanie uvedený aktívny mód, a teda základný mód so všetkými aktívnymi časťami. V prípade súčasného využitia Wi-Fi a Bluetooth môže spotreba dosahovať v špičke až 790 mAh. Pri móde s uspatým modemom (modem sleep) sú neaktívne Wi-Fi, Bluetooth, rádio vysielač a periférie. Je možné nastaviť frekvenciu procesora a upraviť tak spotrebu. V ľahkom spánku (light sleep) je naviac pozastavený procesor, dochádza k uloženiu obsahu RAM. Pri prebudení sa systém vráti do predchádzajúceho stavu. V hlbokom spánku (deep sleep) je procesor úplne vypnutý, koprocesor stále sleduje zmeny na senzoroch a prebúdza procesor. Narozdiel od ľahkého spánku nedochádza k automatickej obnove pamäti RAM. Stále je však možné využiť RTC pamäť na uloženie a znovu načítanie dát pri prebudení. Pri hibernácii (hibernation) je naviac odstavený aj koprocesor a RTC pamäť. Všetko okrem jedného časovača a niektorých vstupných RTC je vypnuté. Tie sú zodpovedné za prebudenie systému.[7]

Mód	Spotreba	Pridané neaktívne časti
Active	80 - 260 mA[5]	-
Modem sleep	3 - 20 mA	Wi-Fi, Bluetooth, periférie, vysielač
Light sleep	0,8 mA	pozastavený procesor
Deep sleep	10 μA	procesor
Hibernation	2.5 μA	koprocesor

Tabuľka 4.1: Porovnanie spotreby v jednotlivých módoch[7]

[5]V prípade zasielania dát pomocou Wi-Fi alebo Bluetooth je spotreba vyššia ako pri prijímaní

Kapitola 5

Mobilné aplikácie

Existuje niekoľko spôsobov ako vytvoriť aplikácie pre mobilné zariadenia. Základným spôsobom je vývoj natívnych aplikácií. V súčasnosti je však čoraz častejšie využitie webových technológií ako je HTML, CSS a Javascript. Každá varianta prináša určité výhody a nevýhody, je nutné vybrať technológiu vhodnú pre aktuálne potreby. V texte sa ďalej primárne zameriam na dva najpopulárnejšie mobilné operačné systémy - Android a iOS.

5.1 Natívne aplikácie

Natívne aplikácie sú aplikácie vyvíjané pre konkrétnu platformu natívnym programovacím jazykom. V prípade Androidu je to teda Java alebo Kotlin, pre iOS to sú Swift alebo Objective-C. Aplikácie môžu mať prístup k všetkým senzorom telefónu, ku kontaktom a podobne. Takéto aplikácie sú často plynulejšie a rýchlejšie. Prinášajú však aj nevýhody v podobe zložitejšieho programovania užívateľského rozhrania. Ďalšou nevýhodou natívnych aplikácií je, že sú určené len pre jednu platformu. Aplikácia vytvorená pre iOS nie je podporovaná na zariadeniach s Androidom a naopak.[3]

Existujú však aj frameworky, vďaka ktorým je možné vytvárať multiplatformové natívne aplikácie. Sem patrí napríklad Xamarin, Titanium alebo React Native. Medzi platformami sú minimálne rozdiely a je možné zdieľať až 90 % kódu. Prispieva to tak k šetreniu času a tým aj nákladov pri vývoji aplikácie pre obe platformy.[11]

5.2 Webové aplikácie

Ide o tradičné webové aplikácie, ktoré sú zobrazované pomocou užívateľom zvoleného prehliadača. Majú pomerne obmedzený prístup k zdrojom zariadenia ako sú senzory a podobne. Aplikácie sa vytvárajú pomocou webových technológií HTML, CSS a Javascript. Tieto technológie môžu byť rozšírené o ďalšie knižnice a frameworky ako sú Angular, React, Vue a ďalšie. Na funkčnosť aplikácie je pri tom nevyhnutné pripojenie na internet. Vďaka konceptu progresívnych webových aplikácií (Progressive Web Applications) dokážu tieto aplikácie využívať niektoré funkcie známe z natívnych aplikácií ako napríklad zasielanie upozornení a ďalšie. Výhodou je, že aplikácia nie je uložená priamo v zariadení a teda nezaberá užívateľovi miesto v pamäti. Zároveň tento spôsob ponúka okamžité aktualizácie.[3]

5.3 Hybridné aplikácie

Ide o spojenie natívnych a webových aplikácií. Takto vytvorené aplikácie sú priamo nainštalované v zariadení, nevyžadujú teda pripojenie na internet. Ide v podstate o natívnu aplikáciu s webovým oknom, v ktorom je zobrazený samotný obsah. Pre koncového užívateľa je toto webové okno v podstate neviditeľné a nevidí rozdiel oproti natívnej aplikácii. Ide o prenosný spôsob programovania aplikácií, jedným kódom je možné vytvoriť multiplatformovú aplikáciu. Výsledná aplikácia môže byť pomalšia oproti natívnej práve vďaka ďalšej vrstve v aplikácii. Tieto aplikácie sa však stále zlepšujú a rýchlosť oproti natívnym aplikáciam prestáva byť citeľná. Táto technológia je primárne používaná na jednoduchšie aplikácie.[3]

Existuje množstvo frameworkov, ktoré umožňujú takto zabaliť webovú aplikáciu do natívnej. Tie často definujú vlastné prvky užívateľského rozhrania a urýchľujú tak prácu vývojárom. Zároveň to umožňuje zdieľať dizajn jednotlivých prvkov s užívateľským rozhraním celého systému. Viacero frameworkov je založených na Apache Cordova. Ten poskytuje otvorený kód a vďaka tomu aj možnosť pridávania rozšírení na podporu napríklad Bluetooth, ale aj ďalších senzorov v zariadení. Samotná aplikácia je vyvíjaná v HTML, CSS a Javascript. Z tohto frameworku vychádzajú ďalšie ako je napríklad PhoneGap, Ionic alebo Framework7, ktoré umožňujú využívať ďalšie knižnice. Rozdiely medzi týmito frameworkami sú však pre užívateľa minimálne a výber je často na preferenciách podporovaných knižníc a podobne.[11]

Kapitola 6

Návrh prototypu

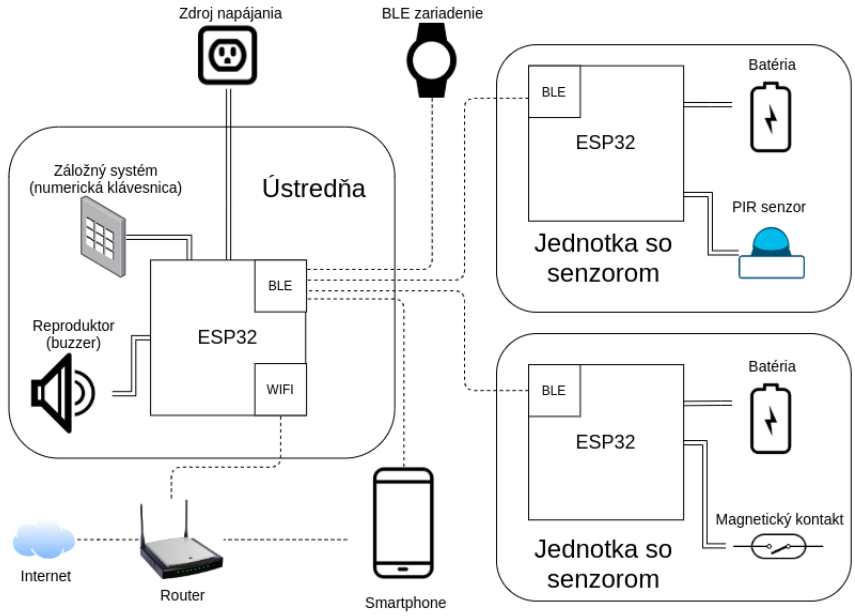
Cieľom práce je navrhnúť zabezpečovacie zariadenie, ktoré bude schopné detekovať prítomnosť majiteľa pomocou BLE. Toto elektronické zabezpečovacie zariadenie bude primárne určené pre bežné domácnosti. Pôjde teda o systéme so stupňom zabezpečenia 2, podľa tabuľky 2.1. Výsledné zariadenie musí obsahovať BLE modul, pomocou ktorého bude pravidelne skenovať okolie pre prítomnosť známych zariadení. O skenovanie sa pritom bude starať samotná ústredňa zabezpečovacieho zariadenia, ktorá zároveň vyhodnocuje informácie zo senzorov. Na základe toho sa systém dokáže prepínať medzi rôznymi stavmi (odstrážené, zabezpečené, alarm a podobne).

Existuje niekoľko spôsobov ako takýto systém vytvoriť. Jedným zo spôsobov je napríklad využite topológie *Mesh*. Pomocou nej je možné spojiť zariadenia do jednej veľkej siete. Takýto systém disponuje pomerne veľkým dosahom vďaka spôsobu komunikácie. Jeho nevýhodou je, že zariadenia nie je možné uviesť do hlbokého spánku. Tento spôsob by teda vyžadoval napájanie jednotlivých senzorov z elektrickej siete, prípadne by znamenal pomerne časté vymieňanie batérií. V prípade zabezpečovacieho systému by to vytvorilo nepohodlnú údržbu, respektíve inštaláciu systému. Senzory sú totiž často umiestňované na miesta, kde nie je v dosahu elektrická zásuvka.

Druhým navrhovaným spôsobom je využitie topológie *Point-to-point*. V tomto prípade ústredňa funguje ako server a senzory sa na ústredňu pripájajú ako klienti. Keďže klient (senzor) iniciuje spojenie, udržiava sa v aktívnom stave čo najkratší čas. Tým sa šetrí spotrebovaná energia a senzor dokáže fungovať aj z batérie. Po skončení komunikácie je možné senzor uspať na zvolenú dobu. V prípade zaznamenania narušenia je senzor prebudený zo spánku a odošle hlásenie na hlavnú jednotku. Tento spôsob komunikácie sa ukázal ako vhodnejší pre navrhovaný systém, a teda celá nasledujúca kapitola popisuje detailnejšie túto variantu.

Pre začiatok je nutné definovať pojmy. V systéme sa vyskytujú dva druhy BLE zariadení - senzory a užívateľom definované zariadenia. V nasledujúcom texte budú BLE zariadeniami myslené len zariadenia, ktoré užívateľ definoval ako zariadenia prepínajúce systém do stavu odstrážené. Pre senzory je často využívaný aj presnejší pojem jednotka so senzorom.

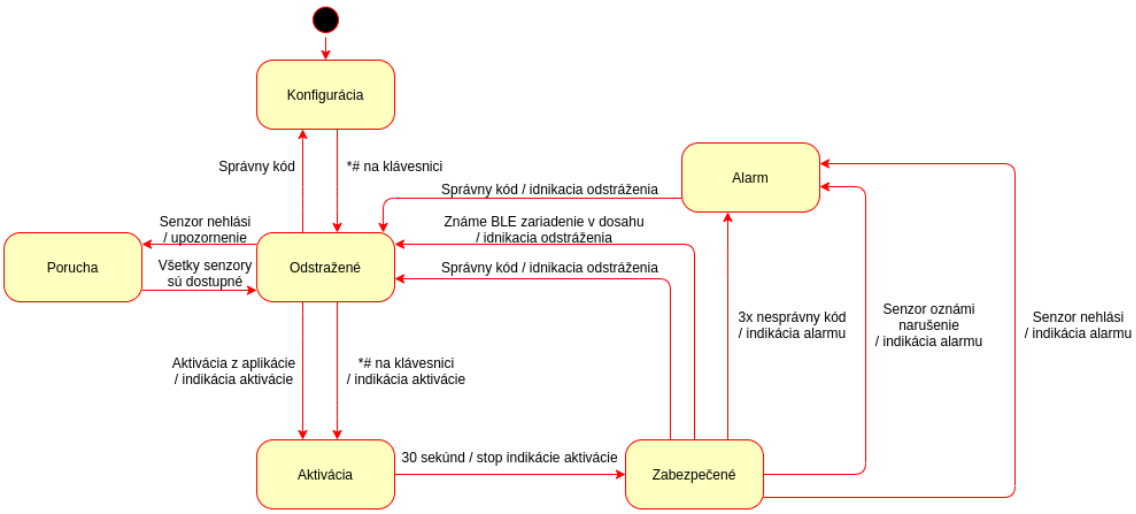
Celý navrhovaný systém môžeme vidieť ako blokový diagram na obrázku 6.1. Súčasťou diagramu sú obe časti systému - ústredňa aj samotné senzory. Podrobnejšie sa k jednotlivým častiam venujem v nasledujúcich kapitolách.



Obr. 6.1: Blokový diagram prototypu

6.1 Stavy systému

Zariadenie musí byť schopné rozlišovať rôzne stavy stráženia a prepínať medzi nimi. Na obrázku 6.2 je zobrazený stavový diagram, ktorý ukazuje jednotlivé stavy a prechody medzi nimi.



Obr. 6.2: Stavový diagram prototypu

Navrhované stavy zahrňujú:

- **konfigurácia** - stav určený pre konfiguráciu samotného systému. V tomto stave je možné zmeniť kód, ktorým sa zariadenia dokáže prepnúť zo stavu *zabezpečené* naspäť do stavu *odstrážené*. Zároveň je možné zmeniť známe zariadenia, nastavenia Wi-Fi

siete a podobne. Okrem tohto stavu nie je možné meniť nastavenia systému. Systém je v tomto stave možné meniť z akéhokoľvek zariadenia v lokálnej sieti. Na to aby sa systém do tohto stavu dostal je potrebné zadať správny kód na číselnej klávesnici.

- **odstrážené** - režim, v ktorom je systém pripravený kedykoľvek na prepnutie do stavu aktivácie systému. V tomto režime sa kontrolujú pripojené senzory, nie však ich výstup, ale len ich dostupnosť. Zadaním správneho kódu je možné prepnúť ústredňu do stavu *konfigurácie*.

- **porucha** - nastane v prípade nedostupnosti aspoň jedného senzoru. Systém v tomto stave nie je možné aktivovať. Ústredňa spustí indikáciu tohto stavu upozornením, teda rozsvietením diódy. Pri opätovnej dostupnosti všetkých senzorov je stav systému automaticky zmenený na *odstrážene*.

- **aktivácia** - prechodný stav trvajúci približne 30 sekúnd. Počas aktivácie systému ústredňa vydáva signalizáciu o tom, že je čo najskôr nutné opustiť strážené priestory. Zároveň ústredňa oznámi senzorom tento stav a tie sa presunú do stavu *zabezpečené*.

- **zabezpečené** - po aktivácii sa systém automaticky prepne do stavu *zabezpečené*. V tomto stave sa vyhodnocujú prijaté informácie z jednotlivých senzorov a v prípade, že je zaznamenané narušenie zmení sa stav na *alarm*. Zároveň v tomto režime opakovane prebieha aktívny sken okolia pre známe BLE zariadenia. V prípade, že sa takéto zariadenia nájde a ústredňa je schopná sa k nemu pripojiť, vykoná sa deaktivácia systému, a teda zmena stavu na *odstrážené*. Druhým spôsobom prechodu do stavu *odstrážené* je zadaním správneho kódu na číselnej klávesnici. V prípade opakovaného zadania nesprávneho kódu prejde systém do stavu *alarm*.

- **alarm** - nastane v prípade zaznamenania neoprávneného vstupu do objektu, opakovaným zadaním nesprávneho kódu či opakovanou nedostupnosťou senzoru. Ústredňa spustí indikáciu alarmu. Z tohto stavu sa dá dostať jedine zadaním správneho kódu na číselnej klávesnici, teda skenovanie okolitých zariadení je pozastavené. Následne je systém uvedený do stavu *odstrážené* a je pripravený na ďalšie použitie.

Všetky spomínané stavy platia pre ústredňu systému. Pre jednotky so senzormi stačí pre jednoduchosť uvažovať len nad stavom stráženia a pohotovostných režimom. Tento režim môže chápať aj ako stav *odstrážené*, kedy senzory ústredni len oznamujú, že nedošlo k žiadnej chybe, sú stále dostupné, teda overujeme integritu spojenia.

6.2 Ústredňa

Ústredňu v tomto prípade tvorí vývojový modul s mikrokontrolérom ESP32. Ten je vhodný hlavne vďaka jeho dostupnosti a podpore všetkých potrebných technológií. Na modul sú následne pripojené jednotlivé signalizačné zariadenia ako je reproduktor (bzučiak) alebo ďalšie LED diódy a podobne. Tieto zariadenia informujú prevažne o zmenách stavu systému ako je napríklad prepínanie do módu stráženia. To je dôležité ako upozornenie pre majiteľa, že systém sa aktivuje, a teda by mal opustiť strážený priestor. V navrhovanom systéme je to hlavne dôležité, aby sa majiteľ dostal z dosahu hlavnej jednotky so svojím Bluetooth zariadením, inak by systém mohol nechcene prepnúť do stavu *odstrážené*.

Ústredňa bude pripojená na Wi-Fi sieť. Pomocou nej následne na internet, odkiaľ bude možné aktualizovať čas systému pre zaznamenanie času alarmu, poslednej komunikácie

senzorov a podobne. Zároveň v lokálnej sieti bude pomocou HTTP požiadaviek komunikovať s mobilnou aplikáciou.

Pre napájanie systému je navrhnuté priame napájanie z elektrickej siete. To je potrebné hlavne z dôvodu súčasného využívania Wi-Fi a Bluetooth technológií, ktoré sú najviac náročné na spotrebu, ako bolo spomenuté v kapitole 4.4. Napájanie je taktiež vhodné realizovať pomocou kombinácie napájania z elektrickej siete a batérie. V tomto prípade by sa primárne preferovala elektrická sieť, pri jej prípadnom výpadku by sa plynulo prešlo na záložnú batériu. Pri výpadku energie by tak ústredňa dokázala naďalej vyhodnocovať informácie zo senzorov.

6.2.1 Periférne zariadenia

Ústredňa sa okrem ESP32 skladá aj z ďalších periférnych zariadení, ktoré pomáhajú indikovať stavy systému, záložný systém v prípade vybitia BLE zariadenia, strata, odcudzenie a podobne. Týmto záložným systémom môže byť napríklad kódová klávesnica. Tá je vhodná hlavne vďaka jednoduchosti na použitie, zároveň so sebou nie je nutné nič nosiť, stačí si zapamätať kód.

K indikačným zariadeniam môžme zaradiť LED diódy, reproduktor alebo bzučiak. Tieto zariadenia indikujú stav systému, prípadne zmenu stavu. Ústredňa by mala obsahovať minimálne dve LED diódy, jednu na indikáciu upozornenia a druhá dióda by mala slúžiť ako indikácia narušenia. V prípade aktivácie zabezpečenia systém opakovane bliká diódou určenou na upozornenie a vydáva tón, aby oznámil majiteľovi, že má opustiť priestor. V prípade alarmu sa aktivuje indikácia narušenia spolu so zvukový oznámením. Pri deaktivácii systému sa rozsvieti indikácia upozornenia a zároveň sa krátkym tónom ohlási zmena stavu na *odstrážené*.

6.2.2 Komunikácia so zariadeniami

Okrem iného sa ústredňa stará o komunikáciu s uloženými zariadeniami. Pre nastavenie nového zariadenia sa ústredňa pokúsi na takéto zariadenia pripojiť pomocou tzv. *bondingu*. Je vyžadované, aby zariadenie podporovalo šifrovanú komunikáciu pomocou BLE. V prípade, že to zariadenie nepodporuje nie je možné ho pridať na zoznam známych zariadení, a teda deaktivovať EZS pomocou neho. Šifrovanie je vyžadované hlavne kvôli bezpečnosti, keďže je pomerne jednoduché skopírovať zariadenie. Zároveň sa očakáva, že zariadenie bude plniť úlohu servera v komunikácii. Ústredňa tak dokáže identifikovať aj mobilný telefón v prípade, že sa nachádza v stave BLE servera.

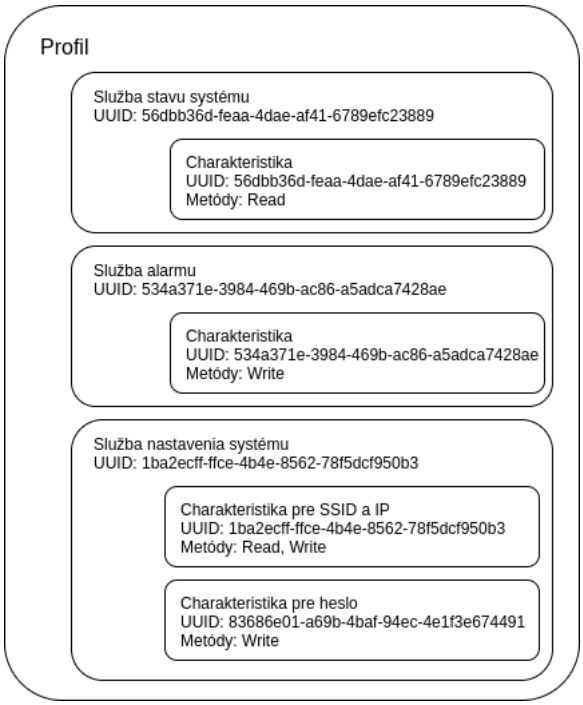
6.2.3 Štruktúra BLE služieb

Ústredňa obsahuje tri BLE služby. Tie sú rozdelené podľa ich funkcie na:

- **služba stavu systému** - pomocou tejto služby senzory zisťujú stav systému a podľa neho upravujú svoje nastavenie. Zároveň slúži aj ako overenie, že senzor je dostupný, a teda prečítal charakteristiku. Ide o jednoduchú číselnú hodnotu z rozsahu 0 - 2. Stavom systému sa v tomto prípade rozumie stav stráženia (1) alebo stav pokoja (0). Ostatné stavy nie sú pre senzory dôležité. Vďaka tomu je možné aktualizovať program pre ústredňu pridaním nového stavu bez potreby zmeny programu pre senzory. V prípade neznámeho senzoru ústredňa odpovedá hodnotou 2.

- **služba alarmu** - slúži na zápis oznámenia o narušení. Senzor zapíše nenulovú hodnotu v prípade, že zaznamenal narušenie. V prípade, že ide o neznámy senzor zápis tejto hodnoty slúži na definovanie typu senzoru. Typ senzoru pri tom definuje samotný senzor zápisom príslušnej hodnoty. Neznámym senzorom teda nie je možné spustiť alarm, čo slúži aj ako zabezpečenie proti neoprávnenému zápisu od narušiteľa.
- **služba nastavenia systému** - využíva sa na počiatočné nastavenie systému. Slúži na komunikáciu s mobilným zariadením. Aplikácia odošle meno a heslo pre Wi-Fi sieť. Pri prečítaní systém vráti IP adresu ústredne.

Každá služba obsahuje vlastné unikátne identifikačné číslo a minimálne jednu charakteristiku. Konkrétny prehľad usporiadania služieb spolu s povolenými metódami je graficky znázornený na obrázku 6.3. Zároveň sú v obrázku zobrazené konkrétne použité identifikátory, ktoré môžu byť využité pre vytvorenie nových senzorov. Pre jednoduchosť služba a charakteristika zdieľajú rovnaké identifikačné číslo.



Obr. 6.3: Štruktúra BLE služieb

6.3 Jednotka so senzorom

Hlavnou časťou jednotky so senzorom je ESP32. Pre túto jednotku bola zvolená vývojová doska s konektorom na batériu s napätím až 3,7 voltov. ESP pomocou BLE komunikuje s ústredňou. Konkrétny spôsob komunikácie je popísaný v kapitole 6.4. Okrem ESP je súčasťou jednotky aj samotný senzor a indikačná LED dióda. Tá sa rozsvieti v prípade, že bolo zaznamenané narušenie priestoru. Táto jednotka musí podporovať minimálne PIR senzor a magnetický senzor. Všeobecne by však zariadenie malo podporovať akýkoľvek senzor, ktorý pri zistení narušenia dá na výstup napätie na úrovni logickej 1 prípadne 0.

Táto časť nebola v zadaní bližšie špecifikovaná, preto bola zvolená varianta, ktorou je možné zachytiť čo najväčšie spektrum senzorov.

6.3.1 Použité senzory

Medzi použité senzory boli zaradené najdostupnejšie senzory. Zároveň bol kladený dôraz aj na ich spotrebu. Senzory by pri tom mali byť schopné pri narušení oznámiť túto skutočnosť jednoduchým zmenením svojho výstupu na opačnú hodnotu.

PIR senzor

Pre PIR senzor bol vybraný senzor AM312, konkrétne modul zobrazený na obrázku 6.4. Je primárne navrhovaný na prácu pri izbových teplotách, s napätím do 3,6 V a prúdom do 100 μA. Dokáže pritom detekovať zmenu v infračervenom poli až na vzdialenosť 3 - 5 metrov s uhlom 100 až 130 stupňov v závislosti na osi. Vďaka tomu je senzor použiteľný v dvoch najbežnejších typoch - vejár a strop, viď rozdelenie typov PIR senzorov v kapitole 2.1.2.[9] Tento senzor bol zvolený len v prototype ako demonštrácia funkčnosti zariadenia, v reálnom nasadení by mal byť použitý senzor s nižším odberom energie. Existujú senzory so spotrebou len 1 - 6 μA v pokojnom stave.[1]

Obr. 6.4: PIR senzor[2]

Obr. 6.5: Magnetický senzor[3]

[1]Napríklad senzory od spoločnosti Panasonic, špecifikácia dostupná na `https://b2b-api.panasonic.eu/file_stream/pids/fileversion/4541`

[2]prevzaté z: `https://www.laskarduino.cz/arduino-micro-pir-detektor-pohybu-am312`

[3]prevzaté z: `https://www.amazon.co.uk/Gikfun-Sensor-Magnetic-Switch-Arduino/dp/B0154PTDFI`

Magnetický kontakt

Pre magnetický senzor bol vybraný senzor MC-38, zobrazený na obrázku 6.5. Ten bol zvolený vďaka jeho dostupnosti, cene a jednoduchosti inštalácie. Jeho operačná vzdialenosť je 15 až 25 mm. Ide o normálne uzavretý senzor, teda v prítomnosti magnetu je jazýčkový kontakt zopnutý.

6.3.2 Napájanie

Napájanie jednotky so senzorom bude realizované pomocou batérie. Tým sa systém stane jednoduchším na inštaláciu a prípadne zmeny umiestnenia jednotlivých senzorov. Je však nutné, aby takéto napájanie vydržalo v priemere aspoň rok. Pri výpočte vhodnej kapacity musíme počítať so spotrebou ESP32, ako aj so spotrebou samotného senzoru. Môžme pritom uvažovať niekoľko stavov:

- systém je stále v stave *odstrážené*. Zariadenie je v stave hlbokého spánku dlhšiu dobu.
- systém pravidelne strieda stavy. Ide o očakávané zaobchádzanie so systémom. Počíta s tým, že s tým že systém je rovnaký čas v oboch stavoch.
- systém je stále v stave *zabezpečené*. Ide o extrém, kde je systém stále aktivovaný, teda hlboký spánok je obmedzený na kratšiu dobu. V tomto prípade je spotreba energie najvyššia.

Týmto rozdelením môžme získať minimálnu, priemernú a maximálnu spotrebu systému. Podľa tabuľky 4.1 môžeme určiť, že spotreba modulu počas hlbokého spánku je 10 μA. Následne sa zariadenie prebudí a začne odosielať dáta pomocou BLE, je teda v aktívnom stave. Keďže ide o odosielanie dát počítame s hornou hranicou 260 mA. Experimentami bolo zistené, že zariadenie ostane v aktívnom stave maximálne po dobu 3,2 sekúnd. Odber zariadenia pri prebúdzaní pri tom zanedbáme nakoľko ide o krátkodobú spotrebu a na výsledné meranie by nemala veľký vplyv.

Pri výpočte najprv zistíme koľko z hodiny strávil senzor vo vybranom stave podľa nasledujúceho vzťahu:

$$(\text{počet cyklov za hodinu} * \text{čas strávený v stave})/3600$$

Tento čas vynásobíme spotrebou vo vybranom stave. Následne jednotlivé stavy spočítame a dostaneme spotrebu ESP32 za hodinu. K tejto spotrebe je potrebné pripočítať spotrebu senzora. Túto celkovú spotrebu vynásobíme počtom hodín v roku a dostaneme minimálnu kapacitu batérie potrebnú pre jednotku so senzorom.

V nasledujúcom výpočte uvažujeme čas spánku 20 minút pri zabezpečenom systéme a 120 minút pri odstráženom stave. Kombinovanou hodnotou pri tom rozumieme spánok v priemere 70 minút. Takto dostaneme nasledujúce hodnoty:

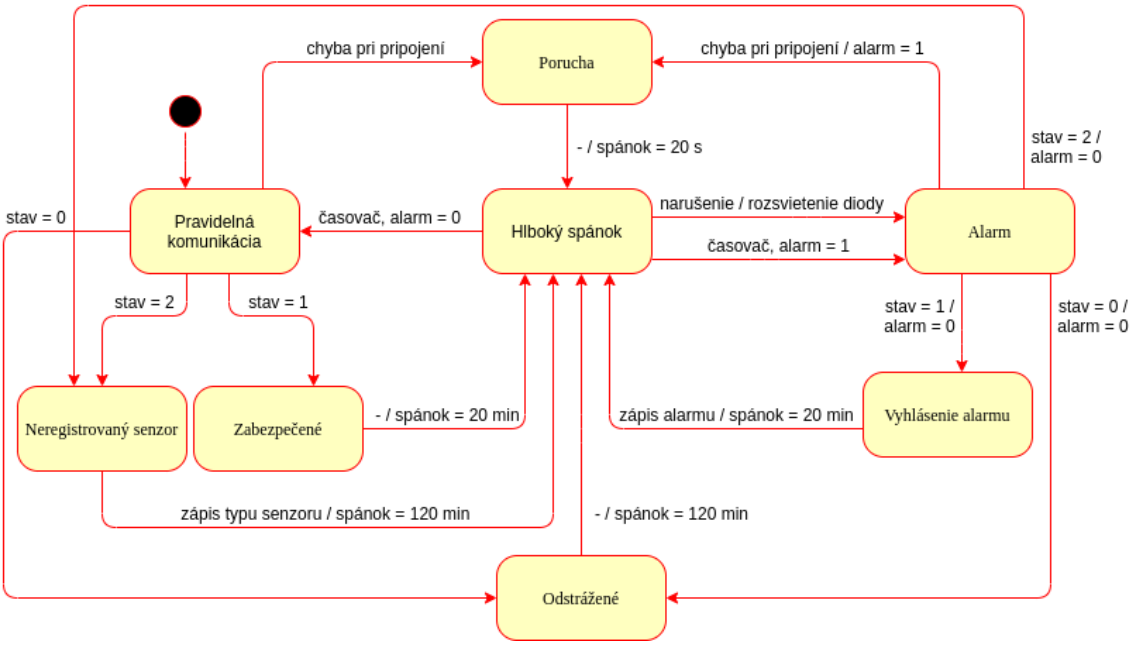
Celková kombinovaná spotreba systému je teda približne 207,936 μAh, v prípade, že započítame aj nami využitý senzor dostaneme sa na hodnotu 307,936 μAh. Za rok tak systém spotrebuje 2697,519 mAh. V prípade využitia úspornejšieho senzora by táto hodnota mohla byť podstatne nižšia. Ideálnym napájaním pre systém bude teda batéria s kapacitou približne 2700 mAh a napätím 3,3 - 3,7 V. Tieto teoreticky zistené výpočty však nebolo možné potvrdiť meraním, preto predstavujú len odhad spotreby.

Stav systému	mód ESP	spotreba za hodinu
zabezpečené	aktívny	691,489 μAh
	hlboký spánok	9,973 μAh
odstrážené	aktívny	115.504 μAh
	hlboký spánok	9,996 μAh
kombinované	aktívny	197,944 μAh
	hlboký spánok	9,992 μAh

Tabuľka 6.1: Výpočet spotreby

6.4 Komunikácia ústredne so senzormi

Pri komunikácií so senzormi sa využíva technológia BLE. Ústredňa vystupuje ako server, na ktorý sa pripájajú senzory ako klienti. Pri komunikácii sa využíva bonding, senzory sú teda trvalo spárované so základnou jednotkou a komunikácia prebieha v šifrovanej podobe. V kapitole 6.2.3 je opísaná štruktúra serveru. Rozhodovanie senzoru je graficky znázornené na stavovom diagrame 6.6. *Stav* je hodnota prečítaná z charakteristiky ústredne, *alarm* je premenná uložená v RTC pamäti mikrokontroléru, *spánok* je čas, na ktorý je systém uvedený do hlbokého spánku.



Obr. 6.6: Stavový diagram senzoru

Klient sa najprv pripojí na server a zistí stav ústredne prečítaním hodnoty služby. Následne podľa zisteného stavu urobí jedno z nasledujúcich:

- v prípade, že senzor ešte nebol registrovaný, ústredňa odpovedá hodnotou 2. Informuje to tak senzor o to, že ešte nebol konfigurovaný. Následne senzor odošle informáciu

o svojom type na ústredňu. Jeho registráciu je potrebné potvrdiť v mobilnej aplikácii. Zároveň sa takýmto spôsobom zamedzuje zistenie stavu systému prípadnému narušiteľovi, ktorý by poznal spôsob komunikácie.

- ak je systém v stave *konfigurácie* alebo *odstrážené* (ústredňa vrátila hodnotu 0), jednotka so senzorom sa uspí na 120 minút. Senzor je v tomto prípade deaktivovaný. Tento spôsob je vhodný hlavne pre šetrenie batérie jednotky.

- v ostatných stavoch sa jednotka so senzorom uspí na 20 minút. Zároveň sa aktivuje prebudenie jednotky pomocou senzora. V prípade prebudenia zo senzora sa na príslušnú službu serveru zapíše oznámenie o narušení.

Po všetkých variantách sa jednotka so senzorom uspí na stanovený čas. Pri uspávaní sa využije mód hlbokého spánku, ktorý patrí medzi najúspornejšie pričom dokáže stále prebudiť systém z externého zdroja. Týmto externým zdrojom je v tomto prípade čidlo, ktoré pri zaznamenaní narušenia automaticky jednotku prebudí. Po prebudení senzor znova oznámi svoju funkčnosť ústredni a zistí stav systému. Rozhodovanie sa opakuje.

Jednotlivé rozostupy medzi overeniami dostupnosti senzorov boli zvolené na základe tabuľky 2.2. Je dôležité zvoliť správne rozostupy pre zabezpečenie čo najčastejšej komunikácie a zároveň udržanie čo najnižšej spotreby jednotiek so senzormi. Spomínané rozostupy platia len pre pravidelnú komunikáciu, ktorou sa overuje dostupnosť senzorov. V prípade, že senzor zaznamená narušenie, jednotka je okamžite prebudená.

V prípade, že sa senzoru nepodarí kontaktovať ústredňu uspí sa na 20 sekúnd, po ktorých toto odosielanie znova opakuje. Ústredňa pravidelne kontroluje dostupnosť senzorov. Ak sa senzor neohlási po očakávanej dobe podľa aktuálneho stavu, dostane ďalšie 2 možnosti na nadviazanie komunikácie. V prípade že sa ani po tejto dobe nepodarí senzoru pripojiť, je vyhlásený za nedostupný a systém je prepnutý do stavu poruchy, respektíve je vyvolaný poplach kvôli sabotáži senzoru.

6.5 Správa systému

Celý systém je potrebné spravovať. Keďže samotný systém neobsahuje žiadnu zobrazovaciu jednotku, ako je displej, nie je možné túto správu vykonávať priamo z ústredne. Túto funkciu v navrhovanom systéme bude zastrešovať mobilná aplikácia. Tá by sa mala postarať o nasledovné funkcie:

- **počiatočné nastavenie systému** - slúži na nastavenie názvu a hesla Wi-Fi siete, na ktorú sa má zariadenie pripojiť. Následne sa odošle odpoveď z ústredne v podobe IP adresy ústredne.

- **zmena číselného kódu** - zmena aktuálneho kódu, ktorý slúži na deaktiváciu systému a prepnutie do stavu konfigurácie.

- **správa senzorov** - zobrazenie základných informácií o senzore, pridávanie nových senzorov, prípadne ich odoberanie.

- **správa spárovaných zariadení** - pridávanie nových zariadení, odstraňovanie zariadení. Slúžia na automatickú deaktiváciu systému. Zároveň by aplikácia mala podporovať nastavenie vzdialenosti, na ktorú bude ústredňa tieto zariadenia registrovať.

- **aktivácia systému** - aktivácia systému pomocou aplikácie, teda prepnutie do stavu aktivácie a následne do stavu zabezpečené.

Odosielanie takmer všetkých požiadaviek na ústredňu bude prebiehať pomocou HTTP požiadaviek na lokálnej sieti. Je teda nutné, aby obe zariadenia boli pripojené na rovnakú Wi-Fi sieť. Výnimkou budú počiatočné nastavenia, ktoré slúžia práve na nastavenie komunikácie pomocou Wi-Fi. Tieto počiatočné nastavenia budú prebiehať pomocou technológie BLE. Pri všetkých nastaveniach musí byť systém v stave konfigurácie. Jedinou výnimkou je aktivácia systému, ktorá okrem stavu konfigurácie podporuje aj stav odstrážené.

Využitie HTTP oproti BLE ponúka jednoduchšiu komunikáciu, nevyžaduje od užívateľa zapnutie dvoch technológií - služby polohy a Bluetooth. Služby polohy sú pre novšie operačné systémy nutné pre skenovanie okolitých Bluetooth zariadení. Zároveň využitie HTTP môže byť v budúcnosti rozšírené pre komunikácie aj mimo lokálnu sieť, napríklad zaslanie notifikácie o alarme a podobne.

Pre čo najväčšiu kompatibilitu medzi platformami je najvhodnejšie využiť štandardné webové technológie ako sú HTML, CSS a Javascript. Pre jednoduchší prístup k zariadeniu a zároveň ušetrenie pamäti na ESP bola zvolená varianta s hybridnou aplikáciou. Vďaka tomu funguje ESP len ako aplikačný server a nie je nutné na ňom uchovávať ďalšie informácie v pomerne malej pamäti. Očakáva sa, že aplikácia bude pravidelne používaná na kontrolu systému, prípadne občasné zmeny v nastaveniach zabezpečovacieho systému. Konkrétne bol pre aplikáciu zvolený Framework7, ktorý je postavený na Apache Cordova. Ide o pravidelné aktualizovaný a stále vyvíjaný nástroj. Do aplikácie je pri tom stále možné pridávať ďalšie moduly vyvinuté pre Apache Cordoba.

Kapitola 7

Implementácia

Samotná implementácia prototypu sa skladá z dvoch na seba nadväzujúcich častí. Prvou sú programy pre vstavaný systém, teda pre mikrokontrolér ESP32. Ide o program pre ústredňu a program pre jednotku so senzorom. Druhou časťou je mobilná aplikácia pre správu systému a zobrazenie aktuálnych informácií o zabezpečovacom systéme. V kapitole je následne popísaná aj konkrétna komunikácia medzi zariadeniami v systéme.

7.1 ESP32

Z dostupných možností pre implementáciu bol vybraný framework ESP IDF ako najvhodnejší. Ten sa ukázal ako najlepší pre komunikáciu pomocou BLE, komunikácia je pomerne jednoduchá s veľkou mierou konfigurácie. Framework poskytuje zároveň veľké množstvo príkladov, ktoré demonštrujú jednotlivé funkcie a možnosti použitia. Dostupná je tiež pomerne obsiahla dokumentácia[1], ktorá pomôže najmä s inštaláciou a nastavením systému. Zároveň obsahuje aj popis jednotlivých funkcií a ich parametrov. Tá bola spolu s príkladmi zároveň využitá na oboznámenie sa so spôsobom programovania jednotlivých súčastí systému. Niektoré časti kódu boli s malými úpravami priamo prevzaté z týchto príkladov. Išlo napríklad o základnú kostru komunikácie pomocou Wi-Fi a Bluetooth Low Energy.

7.1.1 Ústredňa

Ústredňa systému sa stará o niekoľko rôznych činnosti, tie sú samostatne rozdelené na úlohy (task). To umožňuje systému pravidelne opakovať činnosti ako je čítanie hodnôt z klávesnice, indikácia alarmu a podobne. Pri spustení ústredne sa najprv načíta konfigurácia systému uložená v stálej pamäti (non-volatile memory). Tá obsahuje kód pre odstráženie systému, počet senzorov, adresy jednotlivých senzorov, meno a heslo Wi-Fi siete. Okrem týchto informácii systém automaticky ukladá aj adresy spárovaných zariadení a k nim patriace kľúče. Po načítaní celej konfigurácie nasleduje prípadné pripojenie k Wi-Fi sieti, inicializácia aplikačného rozhrania systému, synchronizácia aktuálneho času pomocou protokolu SNTP (Simple Network Time Protocol) a inicializácia jednotlivých štruktúr potrebných pre komunikáciu pomocou BLE.

Samotný program pre ústredňu sa skladá z niekoľkých častí rozdelených do logických celkov podľa funkcie. Jednou z hlavných častí je komunikácia pomocou BLE. Ústredňa sa pri tom správa ako server pri komunikácii so senzormi, ale zároveň ako klient pri komunikácii so

[1] Dostupná z: `https://docs.espressif.com/projects/esp-idf/en/latest/esp32/`

známymi zariadeniami. Väčšina BLE nositeľných zariadení totiž funguje ako server pre zníženie spotreby energie. Pri oboch typoch komunikácie ústredňa stále nadväzuje šifrované spojenie. Po aktivácii systému ústredňa pravidelne skenuje okolie pre dostupné zariadenia. Najprv prebieha selekcia na základe vzdialenosti od ústredne pomocou hodnoty sily signálu – RSSI (received signal strength indicator). Následne prebieha hľadanie známych zariadení. Ak sa takéto zariadenie nájde, ústredňa sa pokúsi k nemu pripojiť. V prípade úspešného pripojenia následne mení svoj stav na deaktivované.

Hodnota RSSI je nastaviteľná z mobilnej aplikácie. Užívateľ v aplikácii zadá desatinným číslom maximálny počet metrov, na ktorý má systém zaznamenávať zariadenia. Táto hodnota je zaslaná na ústredňu kde je prepočítaná na hodnotu RSSI a následne uložená v pamäti. Prepočet prebieha pomocou vzorca:

$$\text{RSSI} = \text{faktor prostredia} * (-10) * \log_{10}(\text{vzdialenosť}) + \text{RSSI jedného metra}$$

Faktor prostredia označuje konštantu podľa prostredia. V našom prípade je prostredie vo vnútri domu alebo bytu, kde je pomerne dosť prekážok, preto je táto konštanta zvolená na maximum – 4. *RSSI jedného metra* je hodnota RSSI na vzdialenosť jedného metra. Táto hodnota je vypočítaná z vysielacieho výkonu zariadenia. V systéme sa táto hodnota nemení, na začiatku inicializácie ústredne sa nastaví na maximálnu podporovanú úroveň +9 dbm. Ide o približný výpočet a výsledná hodnota sa mení v závislosti na umiestnení zariadení a podobne. Vzorec je možné označiť ako tradičný výpočet RSSI zo vzdialenosti.[2]

Ústredňa očakáva v pravidelných intervaloch pripojenie senzora. Ak toto spojenie nie je opakovane nadviazané, systém túto skutočnosť indikuje rozsvietením diódy, ktorá okrem poruchy oznamuje, že systém nie je možné prepnúť do stavu stráženia. V prípade pokusu o aktiváciu systému je užívateľ upozornený ako vizuálne tak aj akusticky. Senzor je zaznamenaný pri pripojení a následnom prečítaní charakteristiky definujúcej stav systému. Zaznamená sa čas v podobe časovej známky a vynuluje sa počítadlo označujúce koľkokrát sa jednotka neozvala. Ďalej môže nasledovať zápis do služby alarmu, ten je zaznamenaný, uchovávajú sa pri tom informácie o tom, ktorý senzor a kedy tento alarm spustil. Následne sú spustené indikácie alarmu.

Pre záložný spôsob deaktivácie alarmu a základnú interakciu priamo s ústredňou bola zvolená maticová číselná klávesnica o veľkosti 4x3. Využíva sa známy princíp striedania výstupu po stĺpcoch a načítavanie hodnôt po riadkoch. Pri opakovanom zadaní nesprávneho kódu na deaktiváciu systému je spustený alarm. Toto počítadlo je vynulované pri zadaní správneho kódu. Maximálna podporovaná dĺžka kódu je 18 znakov. Pri presiahnutí tohto rozsahu sa kód vyčistí a nový znak je pridaný do prázdneho kódu.

Ústredňa implementuje aj vlastné aplikačné rozhranie, pomocou ktorého sú odosielané a prijímané požiadavky z aplikácie. V prípade, že systém nie je v stave konfigurácie, ústredňa odpovie chybovým kódom a nevykoná sa žiadna zmena. Samotný obsah požiadaviek a odpovedí je odosielaný vo formáte JSON.

7.1.2 Jednotka so senzorom

Hlavnou časťou programu pre senzor je komunikácia pomocou Bluetooth Low Energy. Jednotka po prebudení inicializuje štruktúry potrebné pre samotnú komunikáciu. Nasleduje vyhľadávanie hlavnej jednotky. Senzor sa snaží o pripojenie k ústredni a zistenie jej stavu.

[2]Dostupné napríklad z: `https://forums.estimote.com/t/determine-accurate-distance-of-signal/2858/5`

V prípade, že sa pripojenie nepodarilo, jednotka sa uspí na niekoľko sekúnd a pokúsi sa znova pripojiť. Ak bolo zároveň zaznamenané narušenie, jednotka si túto informáciu uloží do RTC pamäte. Ako bolo opísané v kapitole 4.4, táto pamäť nie je zmazaná ani počas hlbokého spánku. Pri ďalšom prebudení sa pokúsi znova toto narušenie nahlásiť.

V prípade úspešného pripojenia, jednotka prečíta aktuálny stav systému. Ak bola jednotka prebudená narušením zo senzora a systém je v stave *zabezpečené*, zapíše túto informáciu do príslušnej BLE charakteristiky. Pri tejto komunikácií sa vymieňajú číselné hodnoty, ktoré reprezentujú jednotlivé stavy. V prípade, že išlo o prebudenie časovačom, jednotka ohlási svoju prítomnosť ústredni spárovaním a prečítaním BLE charakteristiky. Podľa stavu systému sa nastaví čas, po ktorom bude jednotka znova prebudená.

Program pre jednotku so senzorom je zdieľaný pre oba typy senzorov. Pri programovaní mikrokontroléru je potrebné v konfigurácii vybrať typ senzoru. Tým sa zmení spôsob prebudenia mikrokontroléru. Podľa tohto nastavenia zároveň senzor oznamuje svoj typ ústredni pri prvom pripojení. Konfiguráciu je možné meniť pomocou príkazu *idf.py menuconfig*. Samotné nastavenie je v kategórii s názvom *Sensor configuration*.

V prototype je senzor napájaný jednou batériou typu 18650 s kapacitou 2600 mAh, čo by podľa teoretických výpočtov malo vystačiť na takmer rok prevádzky jednotky so senzorom bez potreby výmeny batérie.

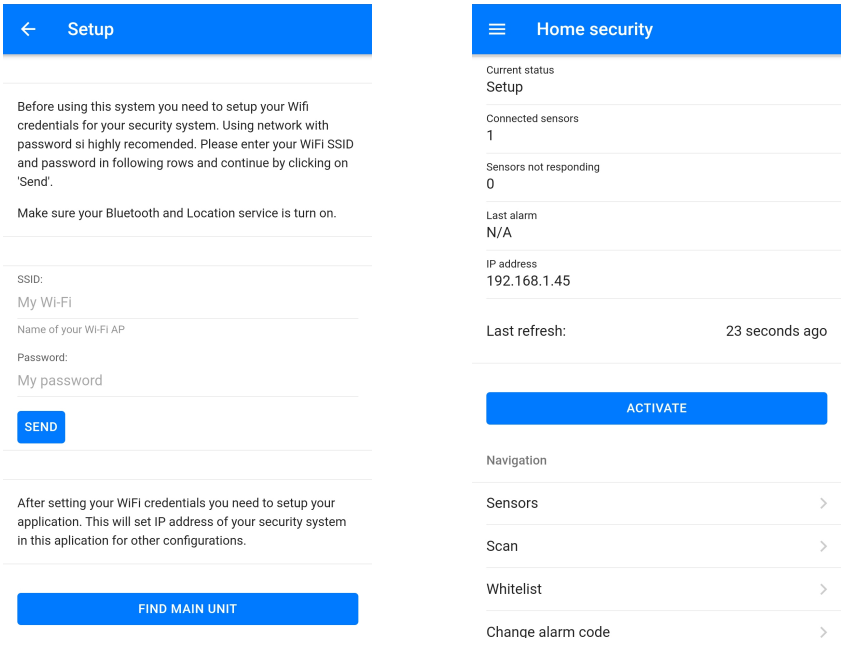
7.2 Mobilná aplikácia

Pre implementáciu aplikácie bol využitý Framework7 vo verzi 5.5 a React. Na programovanie bol teda z väčšej časti využitý jazyk Typescript. Aplikácia pre komunikáciu pomocou BLE využíva prídavný modul *bluetoothle*[3]. Podporuje pri tom Android od verzie 6.0, Windows 10 a iOS od verzie 8. Tento modul je využívaný na skenovanie okolitých zariadení. Hľadá sa pri tom zariadenie podľa názvu, unikátneho identifikačného čísla služby a charakteristiky. Následne sa využíva aj na samotné pripojenie, zápis a prečítanie údajov z charakteristiky.

Samotná aplikácia je rozdelená na niekoľko obrazoviek podľa ich funkcie. Na hlavnej obrazovke sú zobrazené základne informácie o systéme spolu s tlačidlom pre aktiváciu systému. V dolnej časti stránky sa nachádza aj navigácia na ďalšie stránky, prípadne tá je dostupná aj v ľavom menu aplikácie.

Pri prvom spustení mobilnej aplikácie je užívateľ presunutý na obrazovku s nastavením aplikácie, kde je potrebné vyplniť názov a heslo Wi-Fi siete. Toto nastavenie je dostupné len ak je ústredňa v stave *konfigurácie*. Pri prvom spustení je ústredňa automatický do tohto stavu prepnutá. Následne pri nastavení ďalšej aplikácie je však nutné znova prepnúť ústredňu do tohto stavu. Zamedzuje sa tak nepovolenému prístupu k systému. Snímok obrazovky z tohto nastavenia je zobrazený na obrázku 7.1a. Pri úspešnom odoslaní údajov je nutné počkať na reštart systému. Skončenie nastavovania je oznámené krátkym pípnutím, po ktorom je ešte nutné získať IP adresu ústredne pre následnú komunikáciu pomocou HTTP. Po získaní adresy je užívateľ automaticky presunutý na domovskú stránku aplikácie odkiaľ sa môže prepnúť na ďalšie nastavenia. V hornej časti obrazovky sú zobrazené aktuálne informácie o systéme. Tie sú automaticky aktualizované v intervale 30 sekúnd. V prípade neúspešnej aktualizácie údajov je užívateľ informovaný o nedostupnosti ústredne. V spodnej časti stránky sa nachádzajú skratky pre rýchlu navigáciu medzi obrazovkami aplikácie. Tá

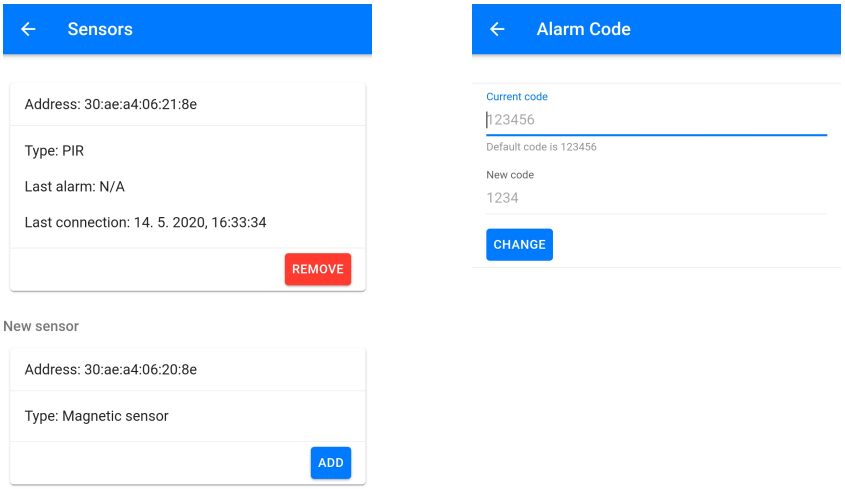
[3]Dostupný z: `https://github.com/randdusing/cordova-plugin-bluetoothle`



(a) Setup (b) Home

Obr. 7.1: Nastavenie aplikácie

je tiež prítomná v menu aplikácie dostupnom v ľavom hornom rohu obrazovky. Ukážku domovskej obrazovky je možné vidieť na obrázku 7.1b.

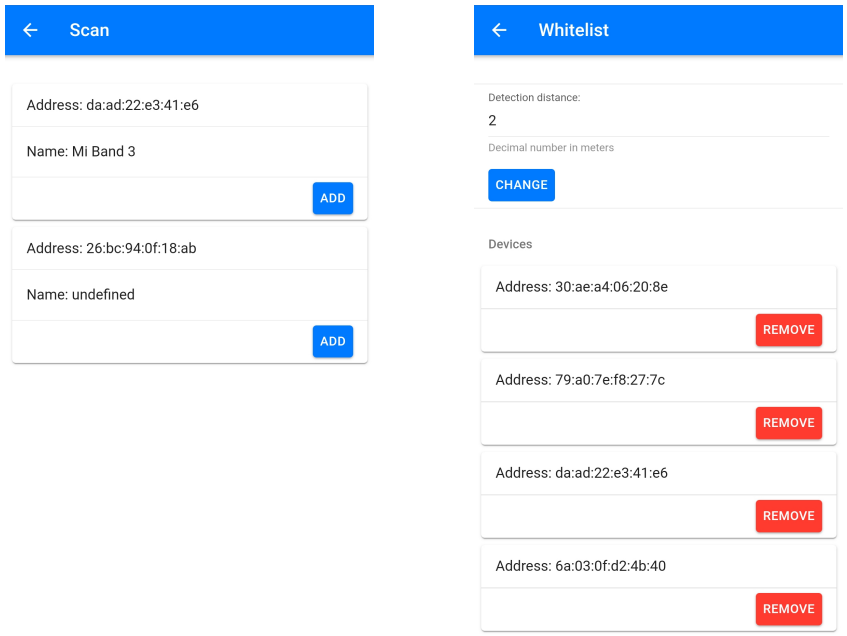


(a) Senzory (b) Zmena kódu zabezpečenia

Obr. 7.2: Nastavenia zabezpečenia

Následne je potrebné definovať jednotlivé senzory systému. Tie sa pri prvom pripojení registrujú do aplikácie. Registrácia prebieha po jednom senzore. V aplikácii je možné vidieť

aktuálne senzory plus prípadne jeden nový, ktorý naposledy žiadal o spárovanie. Pre registráciu nového senzoru musí byť systém v stave konfigurácie. Príklad s jedným registrovaným a jedným novým senzorom je zobrazený na obrázku 7.2a. Tu je možné vidieť typ senzora, pri už registrovaných senzoroch aj ich poslednú komunikáciu a naposledy spustený alarm. Následne sa odporúča zmena číselného kódu, ktorým sa systém deaktivuje, jeho nastavenie je zobrazené na obrázku 7.2b. Aplikácia obsahuje aj nápovedu pre prvotný kód.



(a) Vyhľadávanie nových zariadení (b) Definované zariadenia

Obr. 7.3: Nastavenia detekcie zariadení

Ďalším krokom by malo byť definovanie BLE zariadení, ktoré automaticky deaktivujú systém. Pri pridávaní nových zariadení prebieha sken pre okolité zariadenia. Príklad výsledku skenovania zariadení je zobrazený na obrázku 7.3a. Zariadenia, ktoré sú spárované so systémom je následne možné prehliadať a vymazávať na stránke zobrazenej na obrázku 7.3b. Na tejto stránke je zároveň možné zmeniť vzdialenosť, na ktorú sú zariadenia detekované.

7.3 Vyhodnotenie korektnej funkčnosti

Systém bol testovaný vo vnútri v domácom prostredí pre simulovanie podmienok, do ktorých je primárne navrhovaný. Pre účely testovania systému bolo nutné upraviť rozostupy medzi komunikáciou ústredne so senzormi. Tie boli podstatne skrátené na niekoľko desiatok sekúnd, aby bolo možné sledovať správanie systému v prípade výpadku senzora. Nedostupnosť senzora bola testovaná priamo odpojením jeho napájania a následného sledovania reakcie ústredne. Test prebehol úspešne a ústredňa dokázala zistiť chýbajúci senzor a zároveň v aplikácii oznámiť túto skutočnosť. Pri opätovnom zapojení senzora sa ústredňa dokázala vrátiť do pôvodného stavu. Dosah ústredne na senzory sa pri testovaní ukázal ako priemerný, ale stále postačujúci na menší byt alebo dom.

Systém bol testovaný aj na prijímanie falošného oznámenia o narušení. Na to bol využitý mobilný telefón, ktorý odosielal na službu alarmu nenulové hodnoty. Systém tieto

oznámenia ignoroval a alarm nebol spustený. Takto bolo overené, že systém prijíma len údaje z registrovaných senzorov a ostatné zapísané hodnoty ignoruje.

Automatická deaktivácia systému bola testovaná pomocou inteligentného náramku od spoločnosti Xiaomi, konkrétne model Mi band 3. Ide o jeden z veľmi populárnych náramkov. Systém bol pri správnom nastavení schopný detekovať prítomnosť zariadenia na niekoľko metrov aj cez zatvorené dvere, prípadne stenu. Systém je teda schopný zistiť prítomnosť majiteľa ešte pred vstupom do domu. Detekcia zariadenia bola bezchybná a ústredňa bola schopná identifikovať zariadenie opakovane bez problémov, a to aj v prostredí s vyšším výskytom BLE a Wi-Fi zariadení.

Mobilná aplikácia bola primárne testovaná len pre operačný systém Android. Všetky používané súčasti aplikácie sú však dostupné aj pre ďalšie platformy ako je iOS či Windows. Ich funkcionalita však nebola overená a je možné, že aplikácia by si pre tieto platformy mohla vyžadovať drobné úpravy. Bohužiaľ pri testovaní neboli dostupné ďalšie platformy, keďže komunikáciu pomocou BLE nie je možné simulovať. Keďže aplikácia bola primárne testovaná na počítači a až následne na mobilnom zariadení, všetko okrem komunikácie pomocou BLE bolo otestované aj na tejto platforme.

Kapitola 8

Záver

Cieľom práce bolo vytvoriť prototyp inteligentného zabezpečovacieho zariadenia, ktorý pomocou Bluetooth Low Energy dokáže zistiť prítomnosť známeho zariadenia. Na základe prítomnosti takého zariadenia je systém následne deaktivovaný.

Na začiatku práce bol vykonaný prieskum zabezpečovacích systémov, ich použitie v domoch a bytoch. Zároveň boli zhodnotené používané technológie, ich pozitíva ale aj nedostatky. Nasledovalo oboznámenie sa s princípom komunikácie pomocou Bluetooth Low Energy. Zároveň boli spomenuté rôzne prístupy k vytváraniu mobilných aplikácii. Všetky tieto poznatky boli využité pri návrhu výsledného zabezpečovacieho systému a mobilnej aplikácie určenej na jeho správu. V návrhu boli využité najbežnejšie typy senzorov používané v domácnostiach. Pri návrhu systému bolo zároveň potrebné myslieť aj na spotrebu senzorov a vytvoriť tak systém čo najlepšie udržiavateľný.

Navrhovaný zabezpečovací systém bol následne implementovaný ako prototyp s využitím vývojových modulov ESP32. Tie boli zvolené vďaka integrácii BLE a WiFi komunikácie. Pre zníženie spotreby senzorov bol využitý mód hlbokého spánku. Výsledný systém sa ukázal ako funkčný. Na správu a nastavenia systému bola zvolená mobilná aplikácia. Tá poskytuje jednoduché ovládanie systému a základné informácie o ňom. Zvolená bola varianta hybridnej aplikácie, ktorá poskytuje najväčšiu kompatibilitu medzi platformami. Pri testovaní prototypu sa zistilo, že dokáže pokryť len menšie objekty vďaka obmedzenému dosahu ústredne.

Vytvorený prototyp spĺňa cieľ práce a v budúcnosti by bolo možné ho rozšíriť o podporu ďalších senzorov a funkcií. Zabezpečovací systém by mohol obsahovať aj kamerový systém. Prípadne by bolo možné rozšíriť systém aj o ďalšie senzory zabezpečujúce požiarnu ochranu domu alebo celkovú domácu automatizáciu ako napojenie systému na osvetlenie domu, vykurovanie a podobne.

Vďaka napojeniu systému na internet by bolo možné odosielať upozornenia užívateľovi o nedostupnosti senzorov, upozornenia o alarme, prípadne kontaktovať políciu alebo bezpečnostnú službu.

Literatúra

[1] Bluetooth SIG. *LEARN ABOUT BLUETOOTH* [online]. 2020 [cit. 2020-04-13]. Dostupné z: https://www.bluetooth.com/learn-about-bluetooth/bluetooth-technology/.

[2] Espressif Systems. *IESP32 Series Datasheet* [online]. V3.3. 2020 [cit. 2020-04-22]. Dostupné z: https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf.

[3] Griffith, C. *What is Hybrid App Development?* [online]. 2019 [cit. 2020-05-13]. Dostupné z: https://ionicframework.com/resources/articles/what-is-hybrid-app-development.

[4] Jin, Y., Yan, D. a Sun, H. Lighting System Control in Office Building Using Occupancy Prediction Based on Historical Occupied Ratio. *IOP Conference Series: Earth and Environmental Science* [online]. 1. vyd. Marec 2019, č. 238, s. 9, [cit. 2020-02-23]. DOI: 10.1088/1755-1315/238/1/012009. Dostupné z: https://doi.org/10.1088/1755-1315/238/1/012009.

[5] Kutaj, M. a Velas, A. Magnetické kontakty - testovanie spoľahlivosti. *Riešenie krízových situácií v špecifickom prostredí* [online]. 20. vyd. Žilina: [b.n.]. 2015, s. 8, [cit. 2020-02-23]. Dostupné z: http://fbiw.uniza.sk/rks/2015/articles/Kutaj_Velas.pdf.

[6] Křeček, S. *Příručka zabezpečovací techniky.* 3. vyd. Blatná: Blatenská tiskárna s.r.o., 2006. 313 s. ISBN 80-902938-2-4.

[7] Last Minute Engineers. *Insight Into ESP32 Sleep Modes & Their Power Consumption* [online]. 2020 [cit. 2020-04-21]. Dostupné z: https://lastminuteengineers.com/esp32-sleep-modes-power-consumption/.

[8] Lelong. *Lelong* [online]. 2020 [cit. 2020-02-23]. Dostupné z: https://www.lelong.com.my/paradox-360-u00b0-ceiling-mounted-digital-motion-detector-paradome-dg467-skytechpro-F785655-2007-01-Sale-I.htm.

[9] NANYANG SENBA OPTICAL AND ELECTRONIC CO.,LTD.. *Pyroelectric Infrared Radial Sensor* [online]. 1. vyd. 2018 [cit. 2020-05-01]. Dostupné z: https://drive.google.com/file/d/1z-Ni9ebEjoxDKRnMG1l4lpxKL1xhjP20/view.

[10] RF Wireless World. *Home of RF and Wireless Vendors and Resources* [online]. 2012 [cit. 2020-04-13]. Dostupné z: https://www.rfwireless-world.com/Terminology/BLE-Protocol-Stack-Architecture.html.

[11] Saccomani, P. *Native Apps, Web Apps or Hybrid Apps? What's the Difference?* [online]. 2019 [cit. 2020-05-13]. Dostupné z: https://www.mobiloud.com/blog/native-web-or-hybrid-apps/.

[12] Velas, A. *Elektrické zabezpečovacie systémy* [online]. 1. vyd. Žilina: EDIS – vydavateľstvo ŽU, 2010 [cit. 2020-02-21]. 104 s. ISBN 978-80-554-0224-6. Dostupné z: http://fsi.uniza.sk/kbm/wp-content/uploads/2013/12/Velas_EZS.pdf.

[13] ČESKÝ NORMALIZAČNÍ INSTITUT. *ČSN EN 50131-1: Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 1: Systémové požadavky.* 2. vyd. 2007.

Príloha A

Mapovanie GPIO pinov

ESP32	**Periférie**
GPIO18	Bzučiak
GPIO19	Alarm LED
GPIO5	Upozorňovacia LED
GPIO12	Klávesnica stĺpec 0
GPIO13	Klávesnica stĺpec 1
GPIO14	Klávesnica stĺpec 2
GPIO27	Klávesnica rad 0
GPIO26	Klávesnica rad 1
GPIO25	Klávesnica rad 2
GPIO33	Klávesnica rad 3

Tabuľka A.1: Mapovanie GPIO pinov ústredne

ESP32	**Periférie**
GPIO32	Výstup zo senzoru
GPIO33	Alarm LED

Tabuľka A.2: Mapovanie GPIO pinov jednotky so senzorom