Zabezpečovací systém s autentizací pomocí mobilního telefonu

Martin Velecký

Bakalářská práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2017/2018

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Martin Velecký**
Osobní číslo:	**A14065**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Zabezpečovací systém s autentizací pomocí mobilního telefonu**
Téma anglicky:	**A Security System with Mobile Phone Authentication**

Zásady pro vypracování:

1. **Vypracujte literární rešerši na dané téma.**
2. **Vyberte vhodnou metodu autentizace uživatelů prostřednictvím bezdrátové komunikace s mobilním telefonem.**
3. **Navrhněte jednoduchý zabezpečovací systém na bázi platformy Arduino.**
4. **Uvedený návrh hardwarově realizujte.**
5. **Vytvořte programové vybavení pro řídicí mikropočítač.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **CATSOULIS, John. Designing embedded hardware. 2nd ed. Sebastopol, CA: O'Reilly, 2005, xvi, 377 p. ISBN 0596007558.**
2. **LADMAN, Josef. Elektronické konstrukce pro začátečníky. Praha: BEN – technická literatura, 2001. ISBN 80-730-0015-6.**
3. **MARGOLIS, Michael. Arduino cookbook. 2nd ed. Sebastopol, Calif.: O'Reilly, 2012, xx, 699 p. ISBN 1449313876.**
4. **MASSIMO BANZI. Getting started with Arduino. 2nd ed. Farnham: O'Reilly, 2011. ISBN 9781449309879.BARR, Michael a Anthony J. MASSA.**
5. **PINKER, Jiří. Mikroprocesory a mikropočítače. Praha: BEN – technická literatura, 2004. ISBN 80-7300-110-1.**

Vedoucí bakalářské práce: **Ing. Jan Dolinay, Ph.D.**
Ústav automatizace a řídicí techniky

Datum zadání bakalářské práce: **12. prosince 2017**

Termín odevzdání bakalářské práce: **24. května 2018**

Ve Zlíně dne 12. prosince 2017

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne …….

podpis diplomanta

ABSTRAKT

Cílem práce je vytvořit zabezpečovací systém s autentizací uživatelů prostřednictvím mobilního telefonu. Teoretická část se zabývá poplachovými zabezpečovacími a tísňovými systémy, technologií Bluetooth a platformou Arduino. V praktické části se zabývám návrhem zabezpečovacího systému, jeho konstrukcí, vytvoření programového vybavení pro mikropočítač a vytvořením mobilní aplikace.

Klíčová slova: Poplachový zabezpečovací a tísňoví systém, PZTS, Arduino, Bluetooth

ABSTRACT

The aim of the thesis is to create a intruder alarm system with user authentication via mobile phone. The theoretical part deals with intruder alarm system, Bluetooth technology and the Arduino platform. In the practical part we deal with the design of the security system, its construction, software development for microcomputers and the creation of mobile applications.

Keywords:

intruder and hold-up alarm system, I&HAS, Arduino, Bluetooth

PODĚKOVÁNÍ

Tímto bych rád poděkoval vedoucímu práce Ing. Janu Dolinayovi, Ph.D. za cenné rady a pozitivní přístup.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD **8**
I TEORETICKÁ ČÁST **9**
1 POPLACHOVÝ A TÍSŇOVÝ ZABEZPEČOVACÍ SYSTÉM **10**
1.1 ÚSTŘEDNA 10
1.1.1 Analogové ústředny 11
1.1.2 Sběrnicové ústředny 12
1.1.3 Bezdrátové ústředny 12
1.2 DETEKTORY 13
1.3 VSTUPNÍ A VÝSTUPNÍ ZAŘÍZENÍ 13
2 BLUETHOOT **14**
2.1 SPECIFIKACE 14
2.2 NAVÁZÁNÍ KOMUNIKACE 15
2.3 PÁROVÁNÍ 16
2.3.1 Legacy pairing 16
2.3.2 Secure Simple Pairing (SSP) a Secured conections 16
2.3.2.1 Out of Band 16
2.3.2.2 Numeric Comparison 16
2.3.2.3 Passkey Entry 17
2.3.2.4 Just works 17
3 ARDUINO **18**
3.1 ARDUINO UNO 18
II PRAKTICKÁ ČÁST **19**
4 HARDWARE ÚSTŘEDNY **20**
4.1 DCCDUINO UNO 20
4.2 DFROBOT LCD KEYPAD SHIELD V1.0 20
4.3 BLUETOOTH MODUL MLT-BT05 21
5 SOFTWARE ÚSTŘEDNY **22**
5.1 KOMUNIKACE 22
5.2 OVLÁDÁNÍ 22
5.3 REŽIMY 22
6 MOBILNÍ APLIKACE **24**
6.1 PÁROVÁNÍ 25
ZÁVĚR **26**
SEZNAM POUŽITÉ LITERATURY **27**
SEZNAM OBRÁZKŮ **29**
SEZNAM TABULEK **30**

ÚVOD

Poplachové zabezpečovací a tísňové systémy se stávají běžným zabezpečovacím prostředkem k ochraně majetku nejen v podnikatelské sféře, ale i v soukromém sektoru. Důležitou roli hraje v dnešní době bezdrátový přenos, který se stále více modernizuje a specializuje. Stejně tak tomu je i u bezpečnostních systémů.

Cílem práce je navrhnout ústřednu, a její ovládání skrze bezdrátovou komunikaci.

I. TEORETICKÁ ČÁST

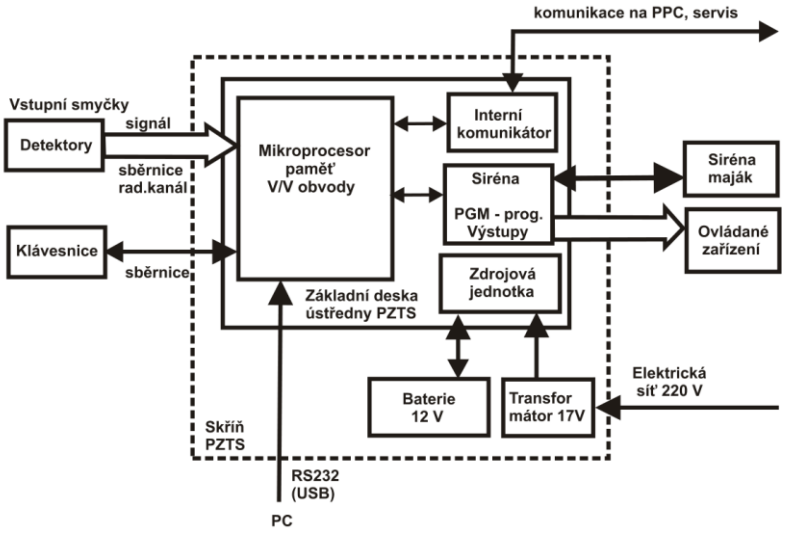
1 POPLACHOVÝ A TÍSŇOVÝ ZABEZPEČOVACÍ SYSTÉM

Poplachový zabezpečovací a tísňový systém má za úkol detekci a signalizaci narušení, pokusu o narušení objektu nebo krádeže předmětu.[1] Jelikož samotné PZTS není schopno zasáhnout proti narušiteli, je potřeba PZTS navázat na složky fyzické ochrany nebo upozornit majitele objektu. [2]

Poplachový zabezpečovací a tísňový systém se skládá z ústředny, detektorů, ovládacích a signalizačních prvků a prvku pro přenos poplachové informace. [1]

1.1 Ústředna

Ústředna je hlavní rozhodovací jednotka, která se stará o obsluhu všech ostatních prvků.[1]

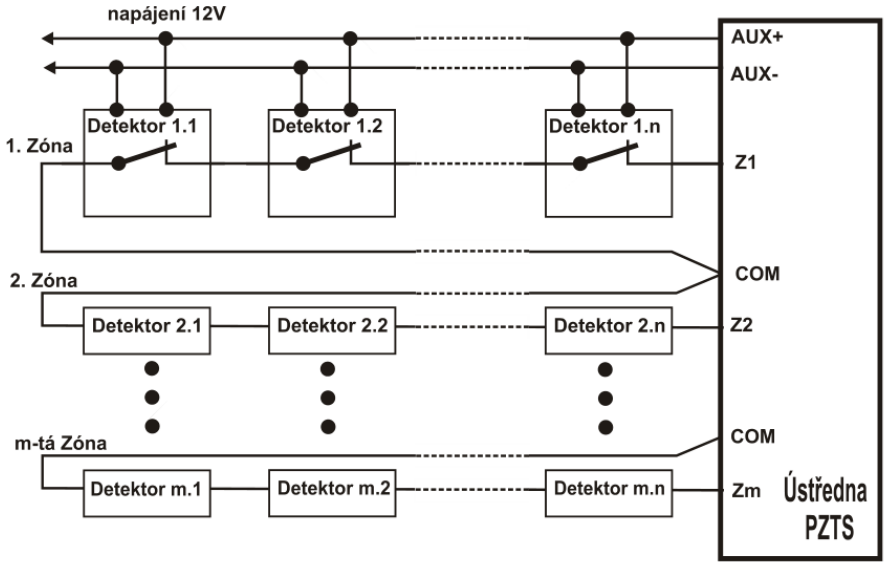


Obr. 1 Schéma ústředny PZTS[3]

Získává informace o narušení z detektorů a rozhoduje o tom, jestli vyhlásit poplach pomocí signalizačních prvků. Ústředna je napájena ze sítě pomocí 230 V a pro případ výpadku obsahuje záložní zdroj. Pro ostatní prvky zajišťuje správné napětí a umožňuje diagnostiku celého systému.[1]

1.1.1 Analogové ústředny

Analogové ústředny používají dva dráty k napájení a další drát pro každou rozhodovací smyčku, na kterou je přivedeno konstantní napětí. V případě detekce narušitele smyčka pomocí spínacích nebo rozpínacích kontaktů změní odpor a ústředna dle toho pozná narušení. [3]

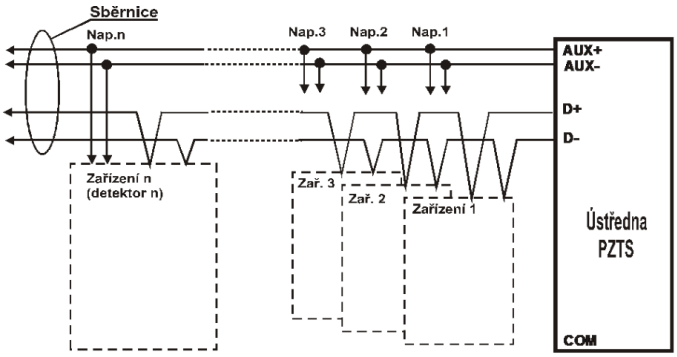


Obr. 2 Schéma zapojení analogové ústředny[3]

Podle zapojení smyček dokáže ústředna poznat v jakém stavu se smyčka nachází. Zatímco ty nejjednodušší zapojení jako jednoduše vyvážená smyčka, nedokáží rozeznat, který detektor spustil poplach oproti složitějším smyčkám jako ATZ.[3]

1.1.2 Sběrnicové ústředny

Sběrnicová ústředna používá ke komunikaci sběrnici. Sběrnice si určuje každý výrobce sám, ale nejčastěji používané sběrnice jsou RS 485 a RS 232. Sběrnice se se skládá ze dvou vodičů a ke každému detektoru musí navíc vést dva vodiče s napájením. [3] [1]

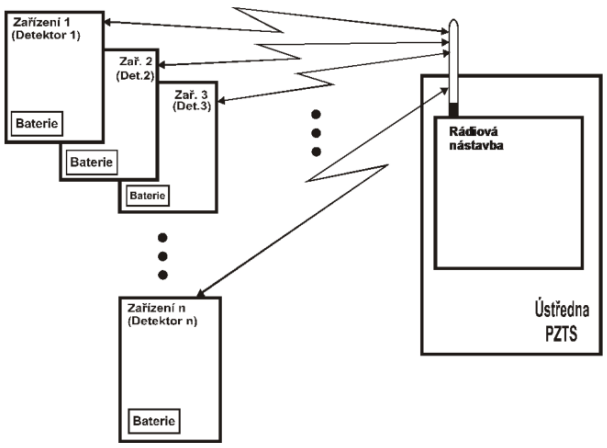


Obr. 3 Schéma zapojení sběrnicové ústředny[3]

Sběrnicová ústředna používá detektory s přímou adresací. Každá adresa je jedinečná, takže nemůže dojít k záměně detektoru a ústředna pozná, který detektor spustil poplach. Komunikace probíhá tak, že ústředna generuje adresy detektorů a přijímá odezvy o stavu.[3]

1.1.3 Bezdrátové ústředny

Bezdrátové ústředny využívají elektromagnetické vlnění. V ČR pracují nejčastěji v pásmu 433 MHz a 868MHz, které jsou v ČR k volnému použití. Komunikace ústředny s detektory probíhá jedno směrně (tzv. simplex) nebo obousměrně (tzv. duplex). [1]



Obr. 4 Schéma zapojení bezdrátové ústředny [3]

Bezdrátové ústředny se snadno a rychle instalují a je jednoduché přidat detektor do už existující instalace to vše s minimálním zásahem do interiéru. Nevýhodou je potřeba pravidelná výměny baterek. [3]

1.2 Detektory

Detektor je prvek, který zajišťuje generování signálu o vstupu do střežené oblasti. Detekci provádí převodem fyzikální veličiny na elektrický signál, a proto se dají detektory dělit na:[1]

- Mikrovlnné detektory
- PIR detektory
- Magnetické čidla
- Akustické detektory
- Kapacitní čidla

1.3 Vstupní a výstupní zařízení

Nejběžnějším způsobem signalizace narušení objektu je siréna se zabudovanou světelnou signalizací, připojuje se na programovatelný výstup nebo na sběrnici.[3]

V případě komerčních objektů bývá objekt napojen na DPPC, které monitoruje stav ústředny. Připojení probíhá prostřednictvím GSM sítě a to buď pomocí SMS nebo datového připojení. Dále je možné připojit ústřednu pomocí internetu anebo pomocí radiového spojení, které je nejnákladnější variantou, protože DPPC potřebuje vlastní radiové pásmo.[2]

Pro obsluhu ústředny se nejčastěji používají numerické klávesnice se zobrazovací jednotkou, kterou tvoří buď LED jednotka nebo LCD displej. V dnešní době se kromě klávesnice začaly rozšiřovat i RFID čipy nebo mobilní telefony. [3]

2 BLUETHOOT

Bluetooth je bezdrátová technologie používaná k připojování zařízení na krátkou vzdálenost využívající pásmo 2,4 GHz, která byla vytvořená jako náhrada za sběrnici RS-232. [4] [5]

V roce 1996 několik firem začalo vyvíjet vlastní bezdrátovou technologii na krátkou vzdálenost. Intel vyvíjel Biz-RF. Ericsson vyvíjel MC-Link. A Nokia vyvíjela Low Power-RF. Tyhle společnosti spolu s Toshibou, a IBM vytvořily "Bluetooth Special Interest Group", která má na starosti dohled nad vytvářením jednotlivých specifikací a udělovaní licence k používání loga, pro jejíž udělení musí žadatel být členem Bluetooth Special Interest Group a dokázat shodu jejich výrobku se specifikací. [5]

2.1 Specifikace

Specifikace Bluetooth ve verzi 1.0 byla vydána v roce 1999, první verze, kterou Bluetooth SIG vydalo. Tahle verze nebyla úplně spolehlivá a spoustu výrobců mělo problém s připojováním k zařízením cizích výrobců. Proto byla vydána BT specifikace verze 1.1, která odstraňovala chyby předchozí verze a navíc byl přidána indikace síly signálu. BT ve verzi 1.1 byla v roce 2002 ratifikováná jako standard IEEE Standard 802.15.1–2002. [6]

V roce 2003 byla vydána BT specifikace 1.2, která mimo jiné přinesla rychlejší připojování vyhledávání zařízení, zrychlení přenosu až na 721 Kbit/s a využitím Adaptive frequency-hopping spread spectrum se snížila interference různých zařízení. Tato verze byla v roce 2005 ratifikována jako standard IEEE Standard 802.15.1–2005.[6]

V roce 2004 byla vydána specifikace BT 2.0 + EDR (enhanced data rate), která představila volitelný část EDR, který zvyšuje rychlost přenosu na 2,1 Mbit/s a snižuje spotřebu elektřiny. EDR plouživá k dosažení vyšší rychlosti kombinaci Gaussian frequency-shift keying a Klíčování frekvenčním posuvem.[6]

EDR je volitelnou částí specifikace a tedy záleží jen na výrobci zařízení, jestli ji použijí. Proto vznikla situace, kdy výrobci začaly vyrábět zařízení, ještě předtím než byla specifikace vydána. Některé firmy ještě v roce 2017 ERD nepoužívají, protože je to pro ně finančně nevýhodné pořizovat licence pro výrobky jako jsou čtečka čárových kódů, která nepotřebuje vyšší přenosové rychlosti. [6]

V roce byla vydána verze Bluetooth 2.1 + ERD, která zlepšuje bezpečnost párování tím, že přidává Secure Simple Pairing. Verze 2.1 přidala další řadu vylepšení, které vedly ke snížení spotřeby.[6]

V roce 2009 byla vydána specifikace BT 3.0 + HS (high speed) jako u předchozí verze. Verze 3.0 přivedla volitelnou součást HS, která umožňovala zvýšit rychlost až na 24 Mbit/s tím, že BT provedlo propojení zařízení a přenos dat probíhal přes wi-fi. Stejně jako ERD i HS je volitelná část a proto někteří výrobci ho ve svých zařízeních nepoužívali. [6]

V roce 2010 je vydána specifikace Bluetooth 4.0 + LE (low energy). Jejím hlavním rozšířením je volitelná část, která snižuje energetickou náročnost BT tím, že některé protokoly nahradila novými, které jsou úspornější. Na rozdíl od ostatních částí není LE zpětně kompatibilní, proto se začalo BT dělit na BT classic a BT LE. Aby mohla zařízení, jako například mobil, pracovat s oběma druhy BT, vytváří se BT čipy s podporou všech potřebných protokolů.[7]

V roce 2013 byla vydána BT specifikace 4.1. Byla to první specifikace, která umožňovala upgrade z BT 4.0 na 4.1 pomocí upgradu firmwaru. Přidala možnost, aby se jedno zařízení mohlo chovat jako hub i peripheral zároveň, což umožňuje například chytrým hodinkám přijímat data od monitoru srdečního tepu a zároveň poslat notifikaci na mobil. Další novinky jsou podpora koexistence pro zařízení s LTE a omezení času hledání okolních zařízení.[7]

V prosinci roku 2014 vychází BT specifikace 4.2, která přidala podporu pro Internet Protocol Support Profile (IPSP), který umožňuje komunikaci mezi prvky s BT za použití IPv6 paketů, což zjednodušilo adaptaci už existujících zařízení (např. Wifi router) pro jejich použití jako přístupové brány pro BT zařízení. Další novinky byly zvýšení výkonu pro zařízení třídy 1 z 10 dB na 20 dB, zvýšení velikosti paketu z 27 na 251 bytes. Byla vylepšena bezpečnost, tím že se Simple pairing vyměnilo za novou sadu šifer pod názvem Secure conections.[7]

2.2 Navázání komunikace

Každé zařízení má 48-bit jedinečnou adresu, která identifikuje zařízení. I když v praxi se uživatelovi ukazuje jméno, které si uživatel může změnit.

Kterékoliv zařízení ve viditelném modu vysílá na požádání jméno zařízení, třída zařízení, seznam služeb, technické informace a každé zařízení, může vyhledávat zařízení a poslat žádost o tyto informace. Každé zařízení může být nakonfigurováno jak má odpovídat na tyto dotazy.

2.3 Párování

BT používá tři verze zabezpečování komunikace do verze 2.0 používá to co se dnes označuje jako “Legacy paring”, od verze 2.1 do verze 4.1 se používá “Simple paring” a od verze 4.2 se používá “Secured conections” [8]

2.3.1 Legacy pairing

Legacy pairing má na výběr pouze jednu možnost a to je zadání stejného hesla na obou zařízení. Jako heslo se může použít jakýkoliv řetězec z kódování UTF-16, ale jenom některá zařízení dokážou zadat opravdu všechny znaky. To vedlo k tomu, že i zařízením jako je například handsfree měla nastavena čtyřmístný kód, který nešel měnit například “1234”. Další problém je že Legacy pairing nemá žádný mechanizmus jak rozpoznat omezení jednotlivých zařízení, proto je na uživateli, aby si toho byl vědom možností jednotlivých zařízení.[8]

2.3.2 Secure Simple Pairing (SSP) a Secured conections

2.3.2.1 Out of Band

Tato metoda používá externí způsob komunikace k předání šifrovacích klíčů. Používá se například NFC. Párovací proces probíhá přes BT, a zařízení si jenom pomocí této komunikace předávají klíče.[8]

2.3.2.2 Numeric Comparison

Pokud obě dvě zařízení mají displej a aspoň jedno má tlačítka Ano/Ne jde použít Numeric Comparision při této metodě se zobrazuje na displeji 6 místný kód, a pokud se shoduje na obou zařízeních lze stisknutím tlačítka potvrdit. Tenhle způsob poskytuje ochranu proti aktivnímu odposloucháváni za předpokladu, že obě zařízení mají tlačítka a porovnání je uděláno pořádně,

2.3.2.3 Passkey Entry

Tato metoda se používá, pokud mají obě dvě zařízení displej a aspoň jedno má numerickou klávesnici. V případě že obě zařízení mají klávesnice, zadávají se u obou zařízení a pokud je jenom u jednoho zařízení tak se zadává jenom u něho.[8]

2.3.2.4 Just works

Tahle metoda nevyžaduje žádnou interakci a poskytuje nejmenší způsob zabezpečení a neposkytuje žádný způsob autentizace.[8]

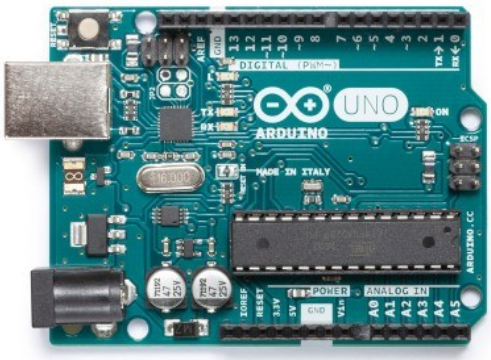
3 ARDUINO

Arduino je otevřená platforma, kterou tvoří specializovaný hardware, jazyk Wiring, softwarové knihovny pro jednotlivé součástky a arduino IDE. Hardware se dá rozdělit na dvě části desky s mikroprocesory a přídavné moduly, které se nasazují na desky a rozšiřují ho o další senzory. Samotné mikropočítače vyrábí výrobci licencovaní firmou Arduino, ale moduly už licenci nepotřebují. Jelikož je platforma otevřená, jsou k dispozici plány jednotlivých mikropočitačů a další výrobci je můžou vyrábět, ale nesmí používat jméno arduino proto vzniklo mnoho klonů s různými jmény, které jsou plně kompatibilní s oficiálními mikropočítači.[8]

Software se skládá z Arduino IDE, které spravuje firma arduino ale do samotného projektu přispívá mnoho dobrovolníků. Arduino IDE spravuje jenom knihovny, které jsou součástí Git repositáři a ostatní vyvíjejí dobrovolníci nebo jiné firmy.

3.1 Arduino UNO

Arduino Uno je mikropočítač založený na čipu ATmega328P o frekvenci 16 MHz. Obsahuje 32 kB flash paměti Má 20 pinů vstup/výstup z toho je 14 digitálních a 6 analogových. Programování probíhá přes USB rozhraní, které v mikropočítači je konvertováno pomocí čipu ATmega8U2 na TTL signál a na počítači je použita virtuální sériová linka.[10]

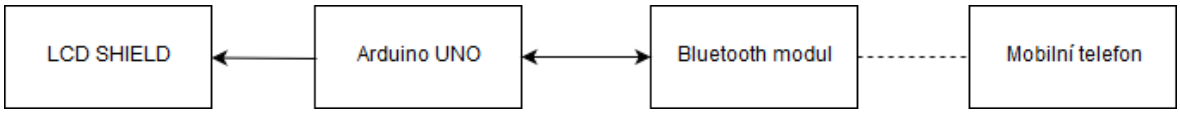


Obr. 5 Arduino UNO

II. PRAKTICKÁ ČÁST

4 HARDWARE ÚSTŘEDNY

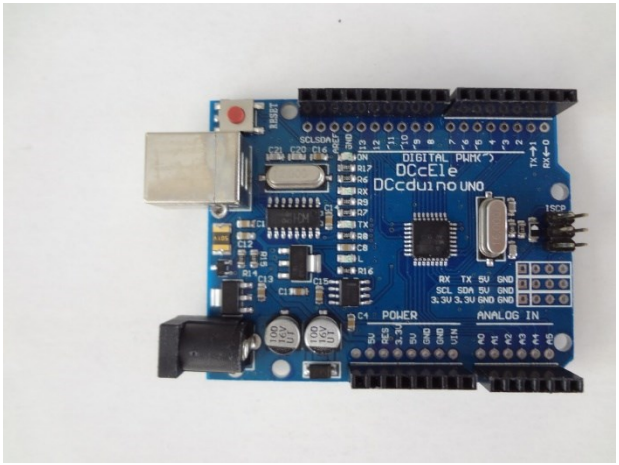
Navrh je řešen z dvou modulů pro arduino a Arduina UNO. Pro komunikaci přes Bluetooth používám modul MLT-BT05, který jako jediný potřebuje pro přenos dat převod napětí na 3V. Proto je součástí prototypu dělič napětí, který poskytuje potřebné napětí pro přenos dat k modulu.



Obr. 6 Blokové schéma zapojení [vlastní]

4.1 Dccduino UNO

Dccduino je klon Arduina Uno, který je plně kompatibilní s Arduino UNO, jediné úpravy provedené na desce je nahrazeny čip ATMEGA16U2, který slouží pro konverzi USB signálu na signál UART za čip CH340G a přidání vývodů pinů navíc. Jako všechny klony jeho hlavní výhodou je jeho pořizovací cena nevýhodu je potřeba na starších PC (Windows 7 a starší) nainstalovat driver, který je k dostání na čínských stránkách.[11]

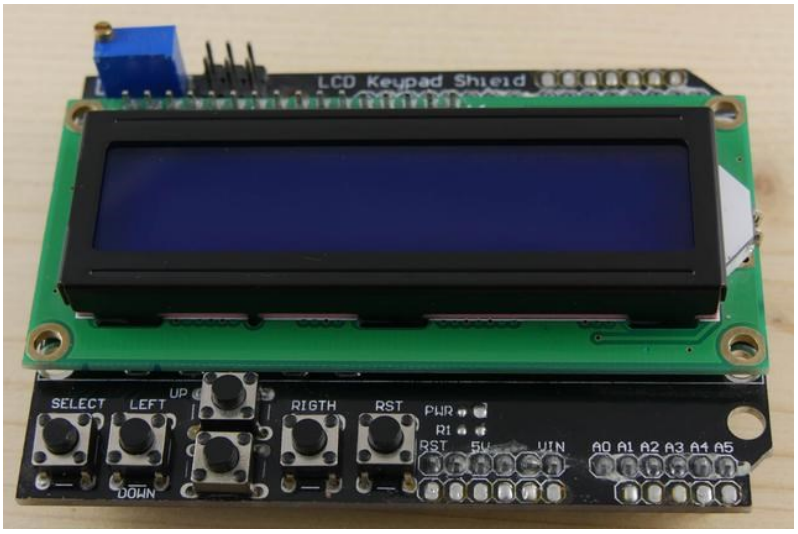


Obr. 7 Fotografie Dccduino UNO[11]

4.2 DFROBOT LCD keypad shield v1.0

Je to modul, který kombinuje LCD displej a klávesnici. Má 6 tlačítek 4 jsou používány jako šipky a dvě mají název select a reset. Výhodou modulu je, že využívá pro všechny tlačítka

jenom jeden analogový pin a nevýhodou je že součástí modulu není čip, který by převáděl komunikaci na sériovou a proto je potřeba 7 pinů pro ovládání. [12]



Obr. 8 Fotografie DFROBOT LCD keypad shield v1.0[12]

4.3 Bluetooth modul MLT-BT05

Je BT modul používají čip CC2541s vlastním firmwarem ovládaný pomocí AT příkazů. Má dva mody, pokud k němu není připojený je v režimu Modul MLT-BT05 je klonem modulu, který klonem modulu HC-11, který jako jediný má dohledatelného čínského výrobce a tedy i softwarovou podporu. MLT-BT05 se liší od HC-11, tím že nemá regulátor pro datové piny, chybí na desce jeden ze dvou oscilátor, který deska nepotřebuje a mají rozdílný firmware, takže MLT-BT05 chybí některé příkazy nebo jsou rozdílné, které má HC-11.

Tab. 1 Seznam součástek

Název součástky	**Hodnota**	**Množství**
Dccduino UNO	-	1x
DFROBOT LCD keypad shield v1.0	-	1x
Bluetooth modul MLT-BT05	-	1x
Rezistor	20000 Ω	1x
Rezistor	10000 Ω	1x

5 SOFTWARE ÚSTŘEDNY

Ústředna byla naprogramována v jazyce Wiring a k programování jsem použil Arduino IDE.

Program ústředny využívá knihovnu SoftwareSerial pro komunikaci s modulem Bluetooth a knihovnu LiquidCrystal pro komunikaci s LCD displejem.

Pro šifrování se používá knihovna libHydrogen, která se používá k šifrování komunikace a párování. Její hlavní výhodou je velikost a přívětivé API .

Ústřednu jsem programoval v Arduino IDE.

5.1 Komunikace

Modul MLT-BT05 simuluje sériovou linku, proto jsou použity příkazy tvořené ASCII řetězci. Komunikace probíhá obousměrně.

Tab. 2 Komunikační příkazy [vlastní]

Příkazy	
MZAS	Mobil pošle příkaz ústředně k zastřežení
MODS	Mobil pošle příkaz ústředně k dostřežení
MALM	Mobil pošle příkaz ústředně k okamžitému spuštění alarmu
MCO	Mobil pošle dotaz na to, v jakém stavu se ústředna nachází
UZAS	Ústředna zasílá informaci o zahájení odpočítávání
UODS	Ústředna zasílá informaci o dostřežení
UALM	Ústředna zasílá informaci o zahájení odpočítávání

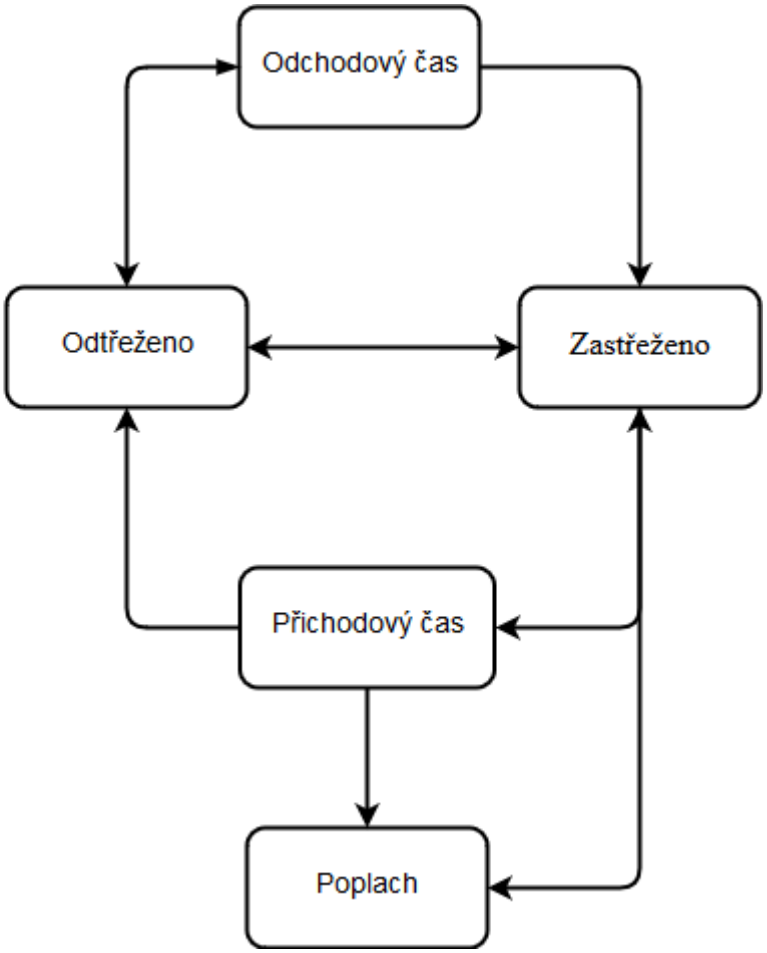
5.2 Ovládání

Ústředna se nedá ovládat pomocí tlačítek, diplej a tlatčítka slouží pouze k párování.

5.3 Režimy

Ústředna má pět stavů, ve kterých se může nacházet. Nejdůležitější jsou stavy zastřeženo, odstřeženo, které mezi sebou přechází. Při spuštění poplachu detektorem se nejdřív přepnou do stavu odpočítávání, v diagramu jsou označeni jako příchodový a odchodový stav, které

umožňují odejít nebo odblokovat ústřednu než se přepnou do požadovaného stavu. Pokud by se ve stanovené lhůtě ve stavu příchodový čas ústředna neodblokovala, přechází do stavu poplach.

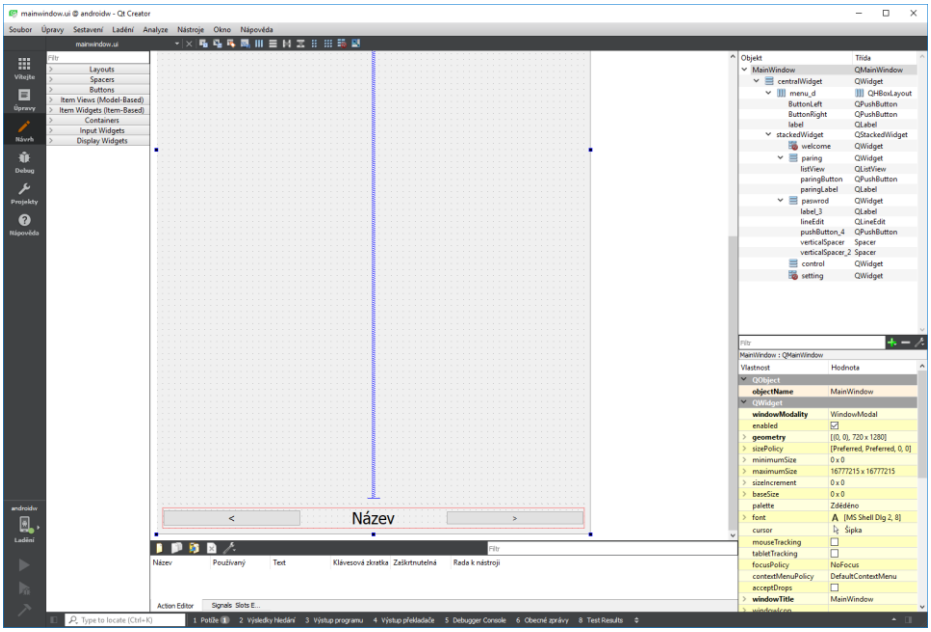


Obr. 9 Schéma stavového automatu [vlastní]

6 MOBILNÍ APLIKACE

K vytvoření mobilní aplikace je použit framework Qt, který umožňuje vytvářet v C++ aplikace pro PC a mobilní telefony. K šifrování je použita knihovna libHydrogen.

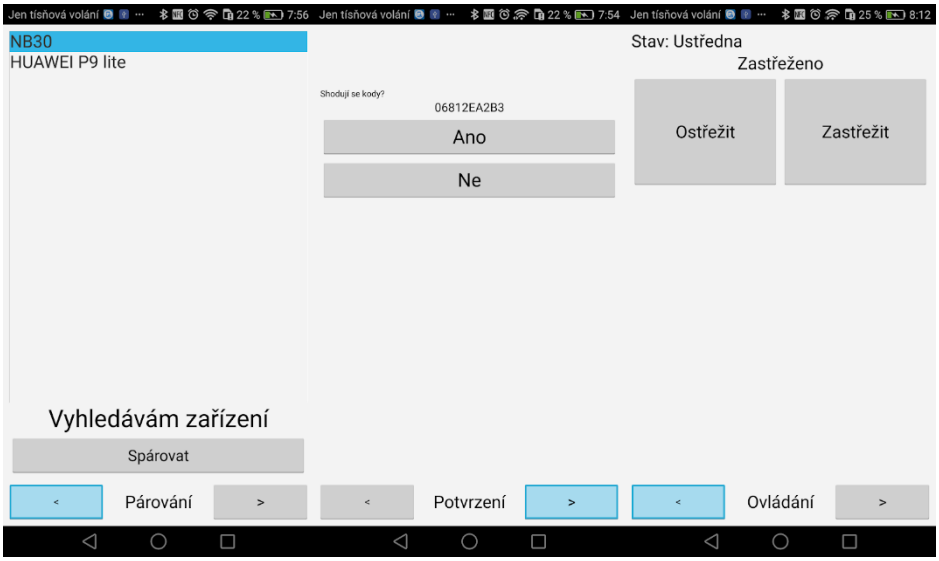
K programování jsem použil Qt Creator, který má integrovaný editor oken.



Obr. 10 Okno Qt creator IDE [vlastní]

Ovládání a funkce

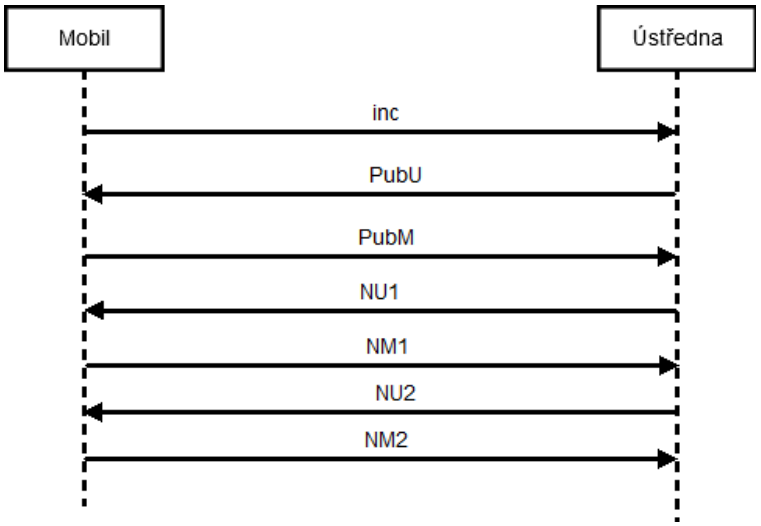
Mobilní aplikace má tři okna jedno ve kterém se vybírá zařízení k párování, druhé k potvrzení, párování a třetí k ovládání ústředny.



Obr. 11 Okna aplikace [vlastní]

6.1 Párování

Párování začíná tím, že mobil pošle požadavek inc o párování na ústřednu. Ta odpoví zasláním svého veřejného klíče PubU a mobil jako odpověď pošle svůj veřejný klíč PubM. Po výměně klíčů vygeneruje ústředna náhodný řetězec, zašifruje ho veřejným klíčem mobilu PubM a rozdělí na dvě poloviny, NU1 a NU2 . Dále mobil znovu vygeneruje náhodný řetězec, zašifruje ho veřejným klíčem ústředny PubU a rozdělí na dvě poloviny, NM1 a NM2. V dalším kroku ústředna pošle první část NU1, a potom mobil pošle svoji první část NM1. To se opakuje a ústředna pošle NU2 a mobil NM2. Následně obě zařízení spočítají hash ze sloučených dat NM1, NM2, NU1 a NU2, které se ořežou a zobrazí se na displeji.



Obr. 12 Schéma komunikace při párování [vlastní]

Tenhle postup zabraňuje tomu, aby došlo ke kompromitaci přenosového kanálu při aktivním odposlouchávání tím, že první data NU1 a NM1 jsou vyměněna předtím, než je může útočník dešifrovat. Proto pokud se útočník pokusí o aktivní odposlech, skončí mobil a ústředna s rozdílným hashem na displeji.

ZÁVĚR

V této práci jsem se zabýval návrhem ústředny a jejím zapojením s mobilní telefonem, navrhl jsem párování, které je odolné vůči odposlouchávání.

SEZNAM POUŽITÉ LITERATURY

[1] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. Vyd. 2. [S.l.: s.n.], 2003. ISBN 80-902-9382-4.

[2] Moderní dohledová poplachová a přijímací centra reprezentují víc než jen terminologickou změnu. *Tzbinfo* [online]. 27.11.2017 [cit. 2018-05-24]. Dostupné z: https://www.tzb-info.cz/poplachove-a-zabezpecovaci-systemy/16607-moderni-dohledova-poplachova-a-prijimaci-centra-reprezentuji-vic-nez-jen-terminologickou-zmenu

[3] DRGA, Rudolf. Elektronické bezpečnostní systémy: Poplachové zabezpečovací a tísňové systémy. Studijní výukový materiál. Zlín, 2013.

[4] A short history of Bluetooth. *Nordic Semiconductor* [online]. 14.7.2014 [cit. 2018-05-24]. Dostupné z: www.nordicsemi.com/eng/News/ULP-Wireless-Update/A-short-history-of-Bluetooth

[5] Tech History: How Bluetooth got its name. *EE Times* [online]. 3.5.2008 [cit. 2018-05-24]. Dostupné z: www.eetimes.com/document.asp?doc_id=1269737

[6] Archived Core Specifications. *Bluetooth* [online]. [cit. 2018-05-24]. Dostupné z: www.bluetooth.com/specifications/bluetooth-core-specification/archived-specifications

[7] Bluetooth 4.1, 4.2 and 5 Compatible Bluetooth Low Energy SoCs and Tools Meet IoT Challenges (Part 1). *DigiKey electronics* [online]. 6 .4.2017 [cit. 2018-05-24]. Dostupné z: https://www.digikey.com/en/articles/techzone/2017/apr/bluetooth-41-42-5-low-energy-socs-meet-iot-challenges-part-1

[8] Bluetooth pairing machanism. *Silabs* [online]. 8.6.2015 [cit. 2018-05-24]. Dostupné z: www.silabs.com/community/wireless/bluetooth/knowledge-base.entry.html/2015/08/06/bluetooth_pairingma-Fe61

[9] *Arduino: Introduction* [online]. [cit. 2018-05-24]. Dostupné z: www.arduino.cc/en/guide/introduction

[10] *Arduino: Arduino Uno Rev3* [online]. [cit. 2018-05-24]. Dostupné z: https://store.arduino.cc/arduino-uno-rev3

[11] *Dccele dccduino uno clone do arduino r3 uno* [online]. [cit. 2018-05-24]. Dostupné z: https://produto.mercadolivre.com.br/MLB-751088656-dccele-dccduino-uno-clone-do-arduino-r3-uno-pronta-entrega-_JM

[12] *Arduino LCD KeyPad Shield* [online]. [cit. 2018-05-24]. Dostupné z: https://www.dfrobot.com/wiki/index.php/Arduino_LCD_KeyPad_Shield_(SKU:_DFR0009)

SEZNAM OBRÁZKŮ

Obr. 1 Schéma ústředny PZTS[3] 10
Obr. 2 Schéma zapojení analogové ústředny[3] 11
Obr. 3 Schéma zapojení sběrnicové ústředny[3] 12
Obr. 4 Schéma zapojení bezdrátové ústředny [3] 12
Obr. 5 Arduino UNO 18
Obr. 6 Blokové schéma zapojení [vlastní] 20
Obr. 7 Fotografie Dccduino UNO[11] 20
Obr. 8 Fotografie DFROBOT LCD keypad shield v1.0[12] 21
Obr. 9 Schéma stavového automatu [vlastní] 23
Obr. 10 Okno Qt creator IDE [vlastní] 24
Obr. 11 Okna aplikace [vlastní] 24
Obr. 12 Schéma komunikace při párování [vlastní] 25

SEZNAM TABULEK

Tab. 1 Seznam součástek 21

Tab. 2 Komunikační příkazy 22