VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ
DEPARTMENT OF COMPUTER SYSTEMS

INTERAKTIVNÍ NAVIGAČNÍ BOD PRO GEOCACHING S ROZHRANÍM BLUETOOTH

INTERACTIVE BEACON FOR GEOCACHING BASED ON BLUETOOTH TECHNOLOGY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. MARTIN ZMITKO
AUTHOR

VEDOUCÍ PRÁCE — Ing. VÁCLAV ŠIMEK
SUPERVISOR

BRNO 2025

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Zadání diplomové práce

170546

Ústav:	Ústav počítačových systémů (UPSY)
Student:	**Zmitko Martin, Bc.**
Program:	Informační technologie a umělá inteligence
Specializace:	Inteligentní zařízení
Název:	**Interaktivní navigační bod pro geocaching s rozhraním Bluetooth**
Kategorie:	Vestavěné systémy
Akademický rok:	2024/25

Zadání:

1. Zabývejte se problematikou aktivity geocaching. Prostudujte aktuální pravidla s důrazem na techniky navigace k tzv. skrytým schránkám a podpůrné aplikace.
2. Prostudujte vlastnosti bezdrátového komunikačního rozhraní Bluetooth Low-Energy (BLE). Zaměřte se na možnosti jeho využití pro navigační účely a interakci s okolním prostředím.
3. S ohledem na poznatky z bodů 1) a 2) zadání definujte základní požadavky na tzv. navigační bod na bázi technologie BLE pro přenos zpráv a interakci s uživateli v rámci aktivity geocaching.
4. Prostudujte aktuální nabídku mikrokontrolerů společnosti NXP, které vynikají nízkou spotřebou, jsou vybaveny bezdrátovým rozhraním BLE a nabízejí podporu zabezpečení komunikace.
5. Navrhněte koncepci zařízení, které bude realizovat funkci navigačního bodu pro geocaching. Při návrhu dbejte na efektivitu, snadné použití a interakci s uživatelem.
6. Zvolte vhodné komponenty pro realizaci zařízení. Vytvořte schéma zapojení a následně i desku plošných spojů. Po osazení součástkami proveďte její oživení.
7. Implementujte obslužný firmware pro mikrokontroler, který zajistí potřebnou funkcionalitu dle koncepce z bodu 5) zadání a taktéž uživatelskou aplikaci pro mobilní zařízení.
8. Definujte sadu scénářů k ověření vlastností realizovaného řešení s důrazem na provozní výdrž zařízení, spolehlivost a splnění požadavků na uživatelskou interakci.
9. Zhodnoťte dosažené výsledky a diskutujte možnosti pokračování projektu či dalších vylepšení.

Literatura:

- Dle pokynů vedoucího.

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

Vedoucí práce:	**Šimek Václav, Ing.**
Vedoucí ústavu:	Sekanina Lukáš, prof. Ing., Ph.D.
Datum zadání:	1.11.2024
Termín pro odevzdání:	31.7.2025
Datum schválení:	10.7.2025

Abstrakt

Tato práce se zabývá návrhem a implementací bezdrátového navigačního bodu pro geocaching využívajícího technologii Bluetooth Low Energy (BLE). Jejím cílem je vytvořit zařízení, které obohatí zážitek z geocachingu o interaktivní prvek ve formě vysoce konfigurovatelného dialogu s uživatelem. Navržený systém umožňuje skrze mobilní aplikaci vedení hráče pomocí hádanek, úkolů nebo sběru informací z okolí, čímž rozšiřuje možnosti klasického hledání keší a zvyšuje jeho atraktivitu. Také přináší nový přístup k využití BLE v interaktivních venkovních hrách a může sloužit jako základ pro budoucí vývoj podobných technologií nejen v oblasti geocachingu.

Abstract

This thesis presents the design and implementation of a wireless beacon for geocaching, utilizing Bluetooth Low Energy (BLE) technology. The goal is to create a device that enhances the geocaching experience with an interactive element in the form of a highly configurable dialogue with its users. The proposed system guides players via a mobile application through riddles, tasks, or by gathering information from the surrounding environment, thus extending the possibilities of traditional geocache hunting and increasing its appeal. It also introduces a novel approach to the use of BLE in interactive outdoor games and may serve as a foundation for the future development of similar technologies beyond the scope of geocaching.

Klíčová slova

geocaching, Bluetooth Low Energy, vestavěné systémy, navigační bod, lokalizace, interakce, mobilní aplikace, NXP

Keywords

geocaching, Bluetooth Low Energy, embedded systems, beacon, localization, interaction, mobile application, NXP

Citace

ZMITKO, Martin. *Interaktivní navigační bod pro geocaching s rozhraním Bluetooth.* Brno, 2025. Diplomová práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Ing. Václav Šimek

Interaktivní navigační bod pro geocaching s rozhraním Bluetooth

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně pod vedením pana inženýra Šimka a externího konzultanta za firmu NXP pana Jana Valeše. Uvedl jsem všechny literární prameny, publikace a další zdroje, ze kterých jsem čerpal.

.....
Martin Zmitko
31. července 2025

Poděkování

Chtěl bych poděkovat panu inženýru Šimkovi za odborné vedení, zapůjčení potřebného vybavení a cennou pomoc při výrobě prototypů. Dále chci poděkovat své rodině a přátelům za podporu a trpělivost nejen během psaní této práce.

Obsah

1 Úvod **2**

2 Geocaching **3**
2.1 Portály pro geocaching 3
2.2 Pravidla hry 4
2.3 Pomocné technologie 5

3 Bluetooth Low Energy **8**
3.1 Srovnáni s Bluetooth Classic 8
3.2 Architektura 9
3.3 Využití BLE pro navigační účely a interakci s prostředím 13

4 Základní požadavky na interaktivní navigační bod pro geocaching **15**
4.1 Požadavky na hardwarové řešení 15
4.2 Požadavky na softwarové řešení 16
4.3 Mikrokontroléry NXP vyhovující požadavkům 16

5 Návrh řešení navigačního bodu **19**
5.1 Návrh hardwarového řešení 19
5.2 Návrh softwarového řešení 23

6 Implementace navrženého řešení **32**
6.1 Výroba prototypů 32
6.2 Implementace obslužného firmware mikrokontroléru 35
6.3 Implementace mobilní aplikace 38

7 Ověření řešení vůči stanoveným požadavkům **45**

8 Závěr **52**

Literatura **53**

A Schémata zapojení a seznamy použitých součástek **56**
A.1 Návrh s mikrokontrolérem QN9090 56
A.2 Návrh s modulem NINA-B506-00B 58

B Návrhové podklady pro desky plošných spojů **60**

C Unikátní identifikátory vlastní Bluetooth Low Energy služby **63**

Kapitola 1

Úvod

Geocaching je aktivita, která se dnes těší velké oblibě po celém světě. Jedná se o hru, která spočívá v hledání skrytých schránek (keší) pomocí polohového systému GPS. Lokaci keší často není snadné odhalit a její nalezení může obnášet řešení hádanek nebo plnění úkolů. S nástupem moderních technologií málokdo hledá keše bez pomoci chytrého telefonu, pročež se nabízí otázka: Jakými prostředky lze obohatit zážitek z geocachingu, učinit jej atraktivnějším a nabídnout jeho účastníkům inovativní a interaktivní podobu tohoto zážitku s využitím chytrých zařízení, která mají stále u sebe?

Navigační body pro geocaching nejsou novinkou – první zařízení tohoto typu, Garmin® Chirp™, se objevilo již před patnácti lety. V té době však byla technologie Bluetooth Low Energy (BLE) teprve v plenkách a uvedené zařízení bylo navrženo výhradně pro použití s proprietárními GPS přijímači stejné značky. Později se na trhu objevila i zařízení vybavená technologií BLE, což umožnilo jejich použití s chytrými telefony a zvýšilo jejich atraktivitu. Zmíněné navigační body nicméně slouží pouze jako pasivní prvky, které poskytují informace o keši (např. GPS souřadnice nebo odhad vzdálenosti), aniž by umožňovaly interakci ze strany uživatele. Ačkoli je některé keše stále využívají, nikdy se netěšily velké oblibě a jsou z důvodu ukončení jejich výroby v současné době prakticky nedostupné.

Cílem této práce, realizované ve spolupráci se společností NXP, je návrh a implementace bezdrátového navigačního bodu pro geocaching založeného na technologii BLE. Jedná se o malé, odolné zařízení s dlouhou výdrží na baterie, které vysílá bezdrátové signály detekovatelné chytrými telefony. Navigační bod je určen k umístění do keše nebo jejího blízkého okolí a po připojení prostřednictvím mobilní aplikace poskytne nálezci informace potřebné k jejímu objevení. Nejvýraznějším rozdílem oproti stávajícím řešením je jeho interaktivita – místo pouhého předání souřadnic či odhadované vzdálenosti vede zařízení nálezce k cíli prostřednictvím vysoce konfigurovatelného procesu ve formě dialogu, který může zahrnovat řešení hádanek nebo získávání informací z okolního prostředí.

Práce je členěna následovně: kapitola 2 pojednává o geocachingu, jeho pravidlech a technologiích, které jsou s ním spojeny. Kapitola 3 rozebírá technologii Bluetooth Low Energy, její architekturu a možnosti využití. Kapitola 4 na základě analýzy současného stavu formuluje základní požadavky na bezdrátový navigační bod a představuje vhodné mikrokontroléry společnosti NXP. V kapitole 5 je navrženo konkrétní řešení zařízení včetně návrhu desky plošných spojů a doplňkové uživatelské aplikace. Kapitola 6 přibližuje implementaci navrženého řešení. Kapitola 7 definuje sadu scénářů pro ověření implementace, popisuje průběh a výsledky testování a hodnotí splnění stanovených požadavků.

Kapitola 2

Geocaching

Tato kapitola pojednává o aktivitě geocaching [4, 9, 27] – globální hře, která spočívá v hledání skrytých schránek (anglicky *cache*, v češtině se ustálil a ve zbytku práce je využíván pojem *keš*, ale anglický pojem lze v českém textu najít často také) pomocí polohového systému GPS.

Keše jsou voděodolné schránky různých velikostí (od nejmenších *nano* keší s objemem do 20 ml po *velké* keše nad 20 litrů) a typů (popsaných v části 2.2). Musí obsahovat tzv. *logbook* – záznamovou knihu, do které se zapisují nálezy hledačů a instrukce pro nálezce – jasnou identifikaci, že se jedná o keš a informace ohledně přípustného nakládání s keší pro nezasvěcené. Pokud to velikost keše dovoluje, může obsahovat i různé předměty nízké (převážně sentimentální) hodnoty, které může nálezce vyměnit za jiné předměty stejné či vyšší hodnoty, případně přidat i vlastní [9]. Keše jsou umístěny na veřejně přístupných místech, nejčastěji v přírodě, a lokalita, ve které jsou umístěny, je většinou nějakým způsobem zajímavá nebo významná [27].

2.1 Portály pro geocaching

Klíčovou součástí hry jsou internetové portály fungující jako databáze keší [27]. Tyto portály obsahují jednak informace o keších – jejich přesné zeměpisné souřadnice a případně další informace a nápovědy využitelné k přesnější lokalizaci, ale také informace o samotných hráčích a jejich aktivitách – hráči zde zaznamenávají své nálezy a mohou si zobrazit statistiky svých i cizích aktivit a srovnat se s ostatními pomocí různých žebříčků [9].

Nejstarším a zdaleka nejrozšířenějším portálem je *Geocaching.com* provozovaný společností Groundspeak, který byl založen v roce 2000. V současné době obsahuje informace o více než 3 milionech keší ve 191 zemích světa a má 7 milionů aktivních uživatelů [10]. *Geocaching.com* funguje na freemium modelu – funkcionalita jako základní vyhledávání a přístup ke keším je zdarma, ale pro přístup k prémiovým keším, pokročilému filtrování na základě hodnocení, obtížnosti či atributů nebo statistikám je nutné zakoupení prémiového členství [9]. Také je dostupná mobilní aplikace (dále popsána v části 2.3.1), pro kterou platí další omezení.

Jako alternativa v reakci na uzavřenost platformy *Geocaching.com* později vznikla síť *Opencaching* [31], sdružení nezávislých lokálních portálů, které si klade za cíl poskytovat podobné služby jako *Geocaching.com*, ale s otevřeným přístupem k datům, provozovaným komunitou a bez nutnosti placení za prémiové členství. Oproti *Geocaching.com* je však *Opencaching* mnohem méně rozšířený, severoamerická verze *Opencaching.us* registruje

například pouze 3000 keší [31], zatímco *Geocaching.com* jich eviduje v této oblasti přes 1,3 milionu [10]. Další alternativou je např. *Terracaching* [30], který klade důraz na kvalitu a originalitu keší a vyšší míru zapojení komunity, taktéž však není příliš rozšířený.

2.2 Pravidla hry

Základní sada pokynů, kterými se účastníci hry dobrovolně řídí, se nazývá *Geocachers' Creed* (česky lze přeložit jako *Krédo geocachera*). Krédo bylo vytvořeno nezávislými členy geocaching komunity a není oficiálními pravidly hry, ale spíše souborem doporučení, jak se chovat při hledání a udržování keší [8].

2.2.1 Pravidla pro tvorbu keší

Závazná pravidla hry (týkající se převážně umístění keší, jejich obsahu, typu, způsobu záznamu nálezů apod.) stanovují tvůrci portálů, na kterých je keš umístěna. Protože je *Geocaching.com* dominantní platformou, tato práce se bude zabývat pravidly stanovenými tímto portálem. Kromě obecných pravidel existují i regionální pravidla[1], stanovená lokálními členy komunity, která upřesňují pokyny v lokálních oblastech (převážně zemích). Na dodržování pravidel dohlíží tzv. *Reviewer* – dobrovolník, který má za úkol kontrolovat nové keše a zajišťovat, aby byly v souladu s pravidly. Pokud keš neodpovídá pravidlům, je zamítnuta a tvůrci je poskytnuta zpětná vazba, jak keš upravit, aby byla přijata.
Následuje výběr relevantních pravidel pro tvorbu keší:

- Umístění keše musí být v souladu s lokálními zákony a povoleno vlastníkem či správcem pozemku.
- Keš a její fyzické trasové body musí být umístěny minimálně 161 m od jiné fyzické keše čí jejího fyzického trasového bodu.
- Keš musí být dlouhodobě udržitelná a volně přístupná, pro její nalezení nesmí být nutné kontaktovat jinou osobu (např. majitele keše či pozemku, na kterém je umístěna).
- Keš nesmí být zakopaná v zemi či připevněná ke stromu tak, aby byl omezen jeho růst nebo byl poškozen (je to ale možné s explicitním doloženým souhlasem majitele pozemku).
- Tvůrce keše se zavazuje sledovat stav keše a udržovat jí i její *listing* (stránku na portálu) v dobrém stavu.
- Obsah keše i jejího listingu musí být vhodný pro všechny věkové kategorie, nesmí obsahovat žádné nebezpečné nebo teplotně nestabilní předměty či jídlo a nesmí mít žádnou agendu (politickou, náboženskou apod.) nebo komerční charakter.
- Pro nalezení keše nesmí být nutné stažení, instalace nebo použití počítačového programu. Nutnost použití mobilní aplikace je povolena, ale pouze pro aplikace s obecnou funkcionalitou široce dostupnou napříč platformách (nelze vyžadovat použití specifické aplikace). Vynucení stažení textových, zvukových nebo obrazových souborů je povoleno.
- Keš může být (za předpokladu získání potřebných oprávnění) umístěna ve vesmíru.

[1] https://gcwiki.atlassian.net/wiki/spaces/GEO/overview

2.2.2 Typy keší

Kromě samotných pravidel *Geocaching.com* definuje i typy publikovatelných keší a požadavky na ně. Následující přehled shrnuje některé základní typy keší, jejich celkový počet je však vyšší. Nezmíněné typy keší jsou často zastaralé a již nejdou vytvářet, byly používány pouze ve vymezeném časovém období jako experimentální nebo nevyžadují fyzickou schránku.

- **Tradiční keš** – nejjednodušší typ keše, skládá se z jedné fyzické schránky s logbookem (*finálky*) umístěné na zadaných souřadnicích.
- **Multi keš** – kromě finálky (jejíž souřadnice jsou skryty) obsahuje alespoň jeden další trasovací bod (kde vstupní bod je daný známými souřadnicemi), který je nutné navštívit pro získání informací o lokaci dalšího trasovacího bodu nebo finálky (ve formě souřadnic nebo hádanky, která lze vyřešit pouze na základě informací obsažených v listingu nebo u trasovacích bodů). Trasovací body mohou být fyzické (kde zakladatel umístil nějaký předmět) nebo virtuální (informace lze získat z okolí).
- **Mystery keš** – nejvíce variabilní typ keše, může obsahovat trasovací body. Řadí se zde několik podtypů (které se ale v základním rozhraní nerozlišují):
  - **Puzzle keš** – souřadnice trasovacího bodu nebo finálky nemusí být pravdivé, pro jejich nalezení je nutné vyřešit nějakou hádanku. Hádanka může vyžadovat dodatečné informace dostupné z veřejných zdrojů nebo vybavení. *Geocaching.com* umožňuje přidat na listing i kontrolu správnosti řešení hádanky – souřadnic, aby měli hráči po vyřešení jistotu, že nebudou hledat na nesprávném místě.
  - **Bonus keš** – keš, jíž indície k nalezení jsou rozptýleny po vícero keších nejčastěji stejného tvůrce.
  - **Challenge keš** – keš, jíž nalezení je podmíněno splněním nějaké podmínky (např. nalezení keší všech států USA nebo nalezení keše každý den v roce).
- **Wherigo keš** – speciální typ keše, který k nalezení vyžaduje využití platformy Wherigo. Wherigo [11] je platforma pro tvorbu a hraní interaktivních her využívajících GPS k propojení reálného světa s virtuálním, vytvořená společností Groundspeak. Zahrnuje interakci jak s virtuálními předměty a postavami, tak s předměty a místy v reálném světě. Původně byla zamýšlena pro kompatibilní GPS zařízení značky Garmin, ale v současné době je dostupná jako mobilní aplikace pro Android a iOS.
- **Beacon keš** – není vlastním typem keše, ale používá se jako atribut keší, které obsahují bezdrátový vysílač (Wi-Fi, Bluetooth, NFC apod.) využitelný pro navigaci. Pokud je využití takového navigačního bodu pro nalezení keše nutné, její typ musí být označen jako *Mystery*.

2.3 Pomocné technologie

Podmínkou pro geocaching je použití GPS a jeho počátek je spojen se zpřesněním systému GPS pro civilní účely v roce 2000. V začátcích bylo toto podmíněno použitím ručních GPS přijímačů, které však oproti dnešku disponovaly omezenou funkcionalitou a pro běžného uživatele byly hůře přístupné a přívětivé. Hledání keší byl značně náročnější proces, kdy bylo nutné nejdříve stáhnout souřadnice keše z portálu, nahrát je do GPS přijímače, dobře

si prostudovat, případně vytisknout detaily o keši a následně se vydat na místo, kde se keš nachází, často s využitím papírové mapy, protože rané přijímače ukládat a zobrazovat mapy nedokázaly (s jejich vývojem se ale tato funkcionalita, nejen včetně funkcí mířených přímo na geocaching jako ukládání a správa keší, rychle objevila) [4].

2.3.1 Mobilní aplikace

S nástupem a vývojem chytrých telefonů se situace značně zjednodušila. Geocaching se stal snadno dostupnou aktivitou pro širokou veřejnost bez nutnosti hlubší technické a navigační znalosti nebo investice do navigačních zařízení. Objevilo se mnoho mobilních aplikací, které umožňují snadný přístup k informacím o keších, navigaci k nim a záznamu nálezů. Kromě stahování detailů keší pro offline použití díky mobilnímu připojení umožňují zjištění dostupných keší i v terénu, což kvůli sníženým nárokům na plánování dělá geocaching ještě dostupnějším.

Kvůli dominanci portálu *Geocaching.com* je pro aplikace jeho podpora téměř nutností. Groundspeak nabízí proprietární API pro přístup k datům o keších[2], které je ale dostupné pouze partnerským vývojářům, kteří se zavážou dodržovat podmínky užití a splňují kvantitativní minimální požadavky na počet aktivních uživatelů, poměr uživatelů s placeným členstvím apod. Z portálu je takto umožněn přístup ke všem keším, ale neplatící uživatelé jsou omezeni na stažení detailů o třech keších denně a nemají přístup k jiným než tradičním keším při vyhledávání.

Groundspeak nabízí oficiální bezplatnou mobilní aplikaci **Geocaching**®[3] pro platformy Android a iOS. Tato aplikace je využívána nejvyšším počtem uživatelů. Nepodléhá omezením pro partnerské vývojáře, ale zavádí vlastní omezení – neplatícím uživatelům neumožňuje vyhledávání keší jiných typů než tradičních, s vyšší obtížností nebo hodnocením, neumožňuje stahování detailů keší pro offline použití nebo tvorbu a synchronizaci seznamů keší.

Z partnerských aplikací stojí za zmínku **Cachly**[4], placená aplikace pro iOS, na této platformě se srovnatelnou popularitou s oficiální aplikací. Pro Android existuje populární bezplatná, otevřená aplikace **c:geo**[5] s podporou také pro *Opencaching*. Obě zmíněné aplikace umožňují všem uživatelům přístup k většině funkcí, které oficiální aplikace nabízí pouze platícím uživatelům (jako offline režim, pokročilé filtrování, notifikace o blízkých keších, tvorbu seznamů apod.), navíc přidávají některé vlastní funkce a rozšíření (jako poznámky, šablony pro záznamy nebo možnost offline záznamu nalezení keše s pozdější synchronizací). Také umožňují import *GPX* souborů obsahující informace o keších, stáhnutelných z webové verze *Geocaching.com* nebo jiných portálů všemi uživateli.

2.3.2 Bezdrátové navigační body

Pokusy o využití bezdrátových navigačních bodů pro navigaci ke keším již v minulosti proběhly. Jedná se o zařízení vysílající bezdrátové signály detekovatelné přenosnými zařízeními, umožňující lokalizaci podle síly signálu či přenášení zpráv v blízkosti keše nebo trasovacího bodu. Ač byly takové zařízení v nějaké míře využívány, nikdy se nestaly široce populárními.

[2] https://partnerships.geocaching.com/geocachingapi
[3] https://www.geocaching.com/play/mobile
[4] https://www.cachly.com/
[5] https://www.cgeo.org/

Chirp™[6] je specializovaný bezdrátový navigační bod vyvinutý v roce 2010 společností Garmin pro geocaching napájený knoflíkovou baterií s udávanou výdrží až 1 rok. Využívá ANT+ [7], bezdrátový protokol na pásmu 2,4 GHz vyvíjený společností Garmin pro účely komunikace převážně mezi sportovními sledovacími zařízeními s vysokými nároky na nízkou spotřebu energie. Výrobce udává pro Chirp dosah až 10 metrů. Chirp je schopen vysílat zprávy a souřadnice, které mohou být přijaty a zpracovány kompatibilními GPS přijímači stejné značky. Jedná se o zastaralý produkt, který se již neprodává a jeho podpora je omezená.

BlueGEO[7], představený českou firmou Waldi v roce 2015, je bezdrátový navigační bod pro geocaching využívající technologii Bluetooth Low Energy (popsanou v kapitole 3). Existují dva modely, větší je napájený tužkovými bateriemi s udávanou výdrží až 5 let, menší je napájený knoflíkovou baterií s udávanou výdrží až 2 roky. Je schopen vysílat zprávy, které mohou být přijaty mobilními telefony. K přijetí a zobrazení zpráv je dostupná aplikace pro Android specificky vyvinutá pro tento účel, zprávy je ale možné přečíst pomocí libovolné aplikace s podporou BLE terminálu. Jejich charakter je čistě informativní – poskytují souřadnice keše nebo informace potřebné k jejímu nalezení, ale neumožňují uživatelům kromě jejich přečtení s navigačním bodem jinak interagovat. Toto zařízení stále využívá několik keší převážně v České republice, ale již se také nevyrábí a byla ukončena jeho podpora[8].

[6] https://static.garmin.com/pumac/Chirp_OM_CS.pdf
[7] https://wiki.geocaching.cz/wiki/Bluegeo
[8] https://utiskare.cz/stranka/bluegeo-po-ukonceni-projektu-pripojeni-se-a-nastaveni

Kapitola 3

Bluetooth Low Energy

Bluetooth Low Energy (BLE) je technologie pro bezdrátovou komunikaci na krátké vzdálenosti vyvíjená a propagovaná konsorciem Bluetooth Special Interest Group (SIG) [1]. Byla představena v roce 2010 jako součást specifikace Bluetooth 4.0 a vyznačuje se především nízkou spotřebou energie, což ji dělá vhodnou k použití v malých zařízeních napájených bateriemi nebo s menšími nároky na datovou propustnost – např. v senzorech, osobních chytrých zařízeních nebo inteligentních navigačních bodech. Má hojné využití v uživatelském, průmyslovém i zdravotnickém sektoru a je důležitou součástí zařízení internetu věcí (IoT). Informace o této technologii v částech 3.1 a 3.2 jsou převzaté z knihy od autora Nareshe Gupty [12].

3.1 Srovnáni s Bluetooth Classic

V porovnání s původním Bluetooth (v dnešní době označovaným jako Bluetooth Classic nebo Bluetooth BR/EDR – Basic Rate/Enhanced Data Rate), ve starších verzích specifikace jedinou dostupnou variantou, se BLE vyznačuje hlavně zaměřením na jiný typ spojení a datových přenosů. Bluetooth Classic pro přenos dat vyžaduje udržení konstantního spojení, jehož navázání je pomalé, s protistranou. Toho je docíleno periodickou výměnou dotazovacích paketů, což je podmíněno vysokou spotřebou energie, ale umožňuje to vyšší datovou propustnost a spolehlivý přenos nepřetržitých datových toků jako je zvuk nebo video a přenos souborů.

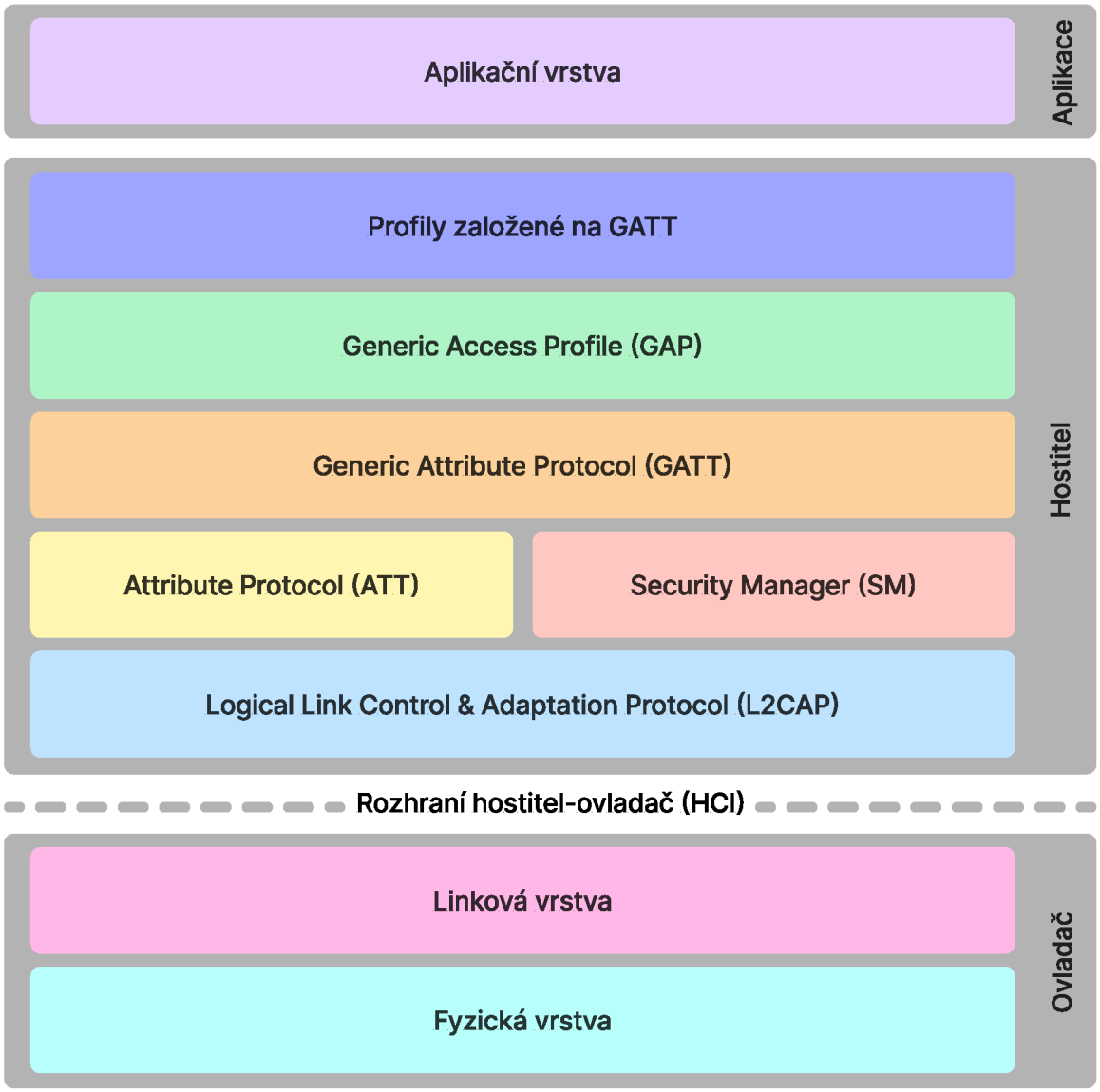
BLE je zaměřeno na krátké a periodické přenosy menšího množství dat, často s vysokými periodami nečinnosti. Spojení s protistranou nemusí být konstantní (proces párování, popsaný v sekci 3.2, je ale nutné provést při prvním spojením mezi zařízeními vždy) a přenos paketů probíhá pouze tehdy, když je nutné přenést nějaká data. To je umožněno změnami v architektuře protokolu se zaměřením na snížení spotřeby energie, především zvýšením rychlosti navázání spojení (snížením latence) redukcí velikosti paketů a počtu využívaných kanálů pro objevení protistran.

Od specifikace Bluetooth 4.0 probíhá vývoj obou technologií paralelně, přičemž se obě soustředí na odlišné případy užití. Kvůli zvýšení využitelnosti, míry adopce a interoperability jsou všechny verze specifikace zpětně kompatibilní s předchozími verzemi. Specifikace v novějších verzích zahrnuje požadavky na obě technologie současně a přináší různá vylepšení jako zvýšení datové propustnosti, nové standardizované profily pro zařízení, zlepšení bezpečnosti nebo podpora pro úplně nové síťové topologie (jako mesh pro BLE, umožňující vytváření velkých sítí s vysokou dostupností a redundancí ve verzi 5). BLE není z důvodu

přepracování architektury kompatibilní s původním Bluetooth BR/EDR, ale protože obě technologie sdílejí základní fyzickou vrstvu, je možné je implementovat v jednom zařízení a využívat konkurentně v tzv. duálním režimu.

3.2 Architektura

BLE je implementováno pomocí vrstvené architektury. Jednotlivé vrstvy jsou zodpovědné za různé aspekty komunikace a postupně abstrahují od nejnižších úrovní fyzické vrstvy (bezdrátového přijímače a vysílače) až po nejvyšší aplikační vrstvu zajišťující implementaci konkrétní funkcionality využívající BLE pro komunikaci na základě konkrétních profilů založených na GATT. Diagram architektury BLE je na obrázku 3.1.



Obrázek 3.1: Diagram vrstvené architektury protokolu Bluetooth Low Energy

3.2.1 Vrstvy ovladače

Spadají zde nejnižší vrstvy architektury implementované ovladačem – hardwarovým komponentem Bluetooth modulu.

Fyzická vrstva zajišťuje samotný přenos dat mezi zařízeními, tvoří ji bezdrátový přijímač a vysílač, anténa a další hardwarové komponenty pro tento účel. BLE využívá ISM pásmo (bezlicenční pásmo určené pro průmyslové, vědecké a zdravotnické použití) 2,4 GHz, které dělí do 40 kanálů s šířkou 2 MHz, z nichž jsou poslední tři vyhrazeny jako oznamovací – slouží k objevování a navazování spojení mezi zařízeními. Kvůli minimalizaci interference a zajištění spolehlivosti spojení je využíváno frekvenčního skákání, kdy se pravidelně mění kanál komunikace. Pro přenos dat je využívána modulace GFSK (Gaussian Frequency Shift Keying). Sílu vysílání lze dynamicky měnit v rozsahu 0,01 až 10 mW (-20 až 10 dBm), což umožňuje teoretický dosah až 100 m v otevřeném prostoru. BLE moduly mohou obsahovat pouze přijímač nebo vysílač, specifikace povoluje implementaci jen jednoho z nich.

Linková vrstva ovládá fyzickou vrstvu a zajišťuje správu spojení mezi zařízeními. Obsahuje protokoly pro objevování, navazování a udržování spojení, správu kanálů a přenosových parametrů. Také zajišťuje tvorbu odchozích a zpracování příchozích paketů, kontrolu chyb a zajištění integrity přenášených dat. Chování linkové vrstvy je definováno konečným automatem (viz obrázek 3.2) o pěti stavech:

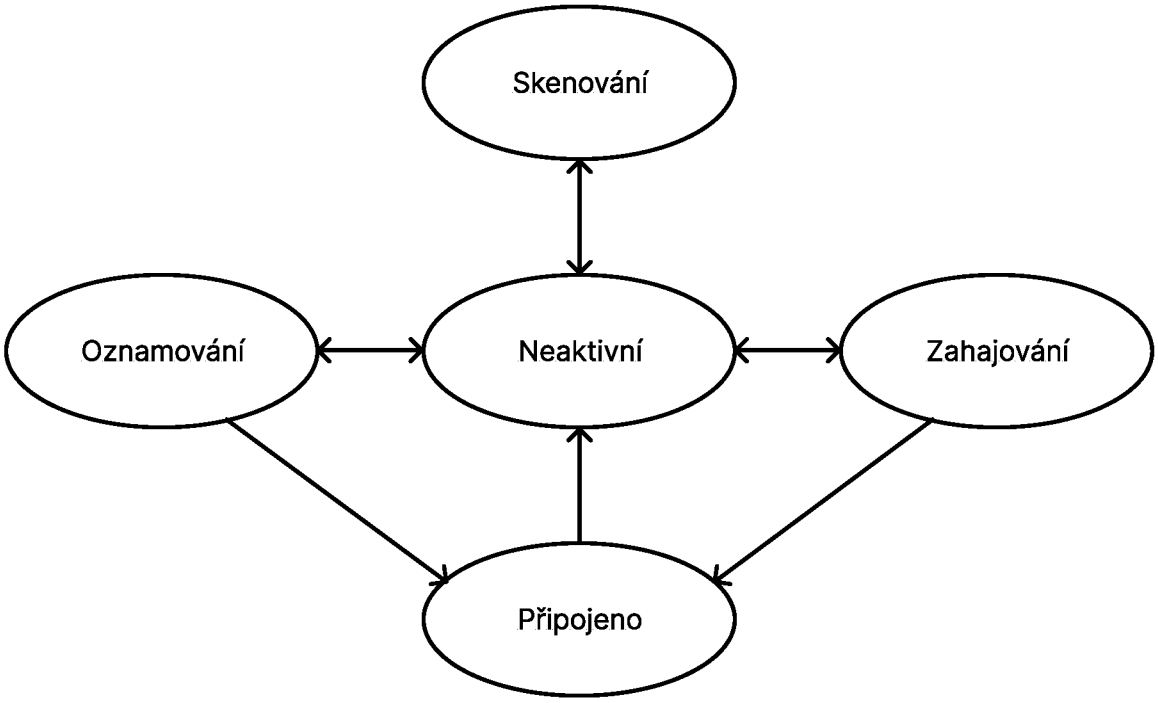
- **Neaktivní** – výchozí stav, zařízení nepřijímá ani neodesílá žádné zprávy.
- **Oznamování** – zařízení vysílá oznamovací zprávy, aby mohlo být objeveno jinými zařízeními.
- **Skenování** – zařízení naslouchá oznamovacím zprávám jiných zařízení a odpovídá požadavky na další informace.
- **Zahajování** – zařízení naslouchá oznamovacím zprávám jiných zařízení a odpovídá pokusem o připojení.
- **Připojeno** – spojení je navázáno a zařízení mohou přenášet data. Pokud zde zařízení přešlo ze stavu oznamování, je označeno jako *slave*, při přechodu ze stavu zahajování jako *master*.

Rozhraní hostitel-ovladač (*Host Controller Interface, HCI*) je standardizované rozhraní mezi ovladačem a hostitelem zajišťující komunikaci mezi nimi. Zahrnuje sadu definic příkazů, událostí a formátů zpráv, čímž umožňuje přenositelnost ovladačů mezi různými hostitelskými zařízeními. HCI pro BLE je mírně rozšířenou verzí HCI pro Bluetooth Classic, s nímž ale zachovává plnou kompatibilitu. HCI je jak pro ovladače, tak pro hostitele volitelnou součástí.

3.2.2 Vrstvy hostitele

Funkcionalita hostitele bývá často implementována zařízením resp. mikrokontrolérem, které využívá BLE modul pro komunikaci, může být ale implementována moduly samotnými, které tak poskytují kompletní řešení a snižují nároky (vývojové i výpočetní) na hostitele za cenu nižší flexibility.

L2CAP (*Logical Link Control and Adaptation Protocol*) je vrstva fungující jako rozhraní mezi linkovou vrstvou a vyššími vrstvami ATT a SMP. Zajišťuje transparentní abstrakci přenosu zpráv mezi vyššími vrstvami obou protistran multiplexací a demultiplexací napříč



Obrázek 3.2: Přechodový diagram konečného automatu představující stavy linkové vrstvy

kanály, segmentaci a spojování dat do paketů a poskytuje další kontroly integrity dat pro případy nezachycení chyby na linkové vrstvě. Také nahrazuje funkcionalitu HCI v případech, kdy jej BLE modul neimplementuje (převážně u modulů integrujících hostitelskou funkcionalitu), využitím vlastního rozhraní, jež může být implementováno libovolným způsobem. Jedná se o zjednodušení protokolu L2CAP z Bluetooth Classic, který byl přizpůsoben pro BLE.

Security Manager (SM) zajišťuje bezpečnost spojení mezi zařízeními. V architektuře se nachází nad L2CAP, pomocí něhož vykonává své funkce. Definuje procedury pro párování, autentizaci a šifrování spojení. Také zajišťuje správu klíčů a identifikátorů zařízení – obsahuje kryptografické algoritmy pro generování identifikátorů, klíčů a jejich výměnu, k čemuž využívá protokol SMP (*Security Manager Protocol*). SM má asymetrickou architekturu, kde je většina výpočetně náročných kryptografických operací prováděna na straně zařízení, které inicializuje spojení a má zpravidla nižší energetické nároky – např. centrála chytrého domova, jež inicializuje párování se senzory napájenými bateriemi. Specifikace definuje čtyři základní režimy zabezpečení:

1. Párování LE secure – nejbezpečnější režim představený ve specifikaci Bluetooth 4.2. Pro šifrování a výměnu klíču používá asymetrickou kryptografii ECDH (*Elliptic-curve Diffie-Hellman*), čímž chrání (ve spojení s metodami autentifikace představenými dále) proti pasivnímu i aktivnímu (MITM – *Man in the Middle*) odposlechu v průběhu celého spojení. Následující režimy představené ve specifikaci 4.0 a 4.1 se označují jako párování LE legacy a nechrání proti pasivnímu odposlechu v průběhu párování.

2. Autentifikováno s MITM ochranou – zajišťuje autentifikaci a šifrování spojení s ochranou proti MITM útoku. Je použita metoda autentifikace, která zahrnuje ověření totožnosti obou zařízení.

3. Neautentifikováno – zajišťuje šifrování spojení bez autentifikace, nechrání proti MITM útoku.

4. Bez zabezpečení – spojení není šifrováno ani autentifikováno, nejmenší nároky na výkon a energii.

Párování obnáší tři fáze:

1. Výměna informací o zařízeních, jejich podporovaných funkcích (především o možnostech uživatelského vstupu a výstupu pro zadání a zobrazení klíčů), velikosti a typech používaných klíčů pro autentizaci a šifrování a požadovaném typu zabezpečení.

2. Autentifikace a enkrypce – na základě informací z předchozí fáze zařízení použijí jednu z následujících metod pro vzájemnou autentifikaci využívající výměnu a porovnání šestimístného numerického kódu:

   - **Just Works** („prostě funguje“) – nejjednodušší metoda, kdy si zařízení vymění kód, na jehož základě se autentizují bez nutnosti uživatelského zásahu. Nechrání proti odposlechu v průběhu párování a je použitá v režimech 3 a 4.
   - **Numerické porovnání** – vyměněný kód je zobrazen na obrazovkách obou zařízení a uživatel musí ověřit, že se shoduje.
   - **Zadání kódu** – uživatel musí kód zobrazovaný na jednom zařízení zadat do druhého, což zajistí autentifikaci se zabezpečením proti MITM útoku.
   - **Out of Band** – kód je vyměněn mimo protokol BLE, např. přes NFC nebo QR kód, míra ochrany proti odposlechu závisí na konkrétní (volitelné) implementaci.

   Na základě výsledku autentifikace se zařízení dohodnou na klíčích pro šifrování a proběhne jejich výměna, další komunikace je již šifrovaná a chráněna proti odposlechu. Pro spojení LE legacy je v tomto kroku šifrování zabezpečeno krátkodobým klíčem, v případě LE secure může být vytvořen a použit dlouhodobý klíč (pro zabezpečení veškeré následující komunikace).

3. Výměna dalších specifických klíčů (volitelné) – po úspěšném párování a navázání šifrování mohou zařízení vyměnit další klíče používané při komunikaci, např. klíč pro rozlišení identity (v případě použití náhodných adres zařízení pro zamezení sledování na základě statické adresy) nebo klíč pro ověření podpisů zpráv. V případě spojení LE legacy proběhne tvorba a výměna dlouhodobého klíče pro šifrování v této fázi.

Attribute Protocol (ATT) je protokol poskytující mechanizmy pro objevení, čtení a zápis atributů. Při komunikaci používá model klient-server, kde server drží databázi atributů, které mohou být čteny nebo zapisovány klientem, jenž za tím účelem odesílá odpovídající požadavky. Atribut představuje jakoukoliv informaci, která může být přenesena mezi zařízeními, např. hodnotu senzoru, stav baterie nebo výrobce zařízení. Je složen z unikátního identifikátoru (pro adresování na serveru), typu (daného unikátním identifikátorem stanoveným buď BLE specifikací nebo vlastní implementací), oprávnění (povolení ke čtení či zápisu, požadavky na šifrování, autentifikaci nebo autorizaci) a hodnoty (fixní či variabilní velikosti ve formě pole oktetů). Kromě základních operací typu požadavek-odpověď iniciovaných klientem definuje také notifikace a indikace, kdy server může klienta informovat o změně hodnoty atributu bez nutnosti opakovaného dotazování. Jako odpověď na indikaci zasílá klient serveru potvrzení o příjmu, notifikace jsou jednosměrné.

Generic Attribute Profile (GATT) řadí atributy do hierarchické struktury a upřesňuje jejich vztahy a chování. Definuje koncept služeb, základních stavebních bloků pro tvorbu specifických, přenositelných profilů pro různé typy zařízení. Služba je pevně definovaná skupina charakteristik (standardně definovaných hodnot určených atributem upřesněných dodatečnými informacemi s volitelnou deklarací práv či požadovaných přístupových metod), které spolu souvisejí a poskytují určitou funkcionalitu, např. služba pro informace o zařízení (*Device Information Service*) nebo služba pro srdeční tep (*Heart Rate Service*). GATT přejímá model klient-server z ATT a definuje způsoby, jak mohou být atributy v rámci služeb čteny, zapisovány nebo sledovány.

Generic Access Profile (GAP) definuje základní pravidla a procedury pro objevování, párování a připojení společná pro veškerá BLE zařízení, čímž zajišťuje jejich interoperabilitu. Zahrnuje definice rolí zařízení optimalizované pro různé případy užití (centrála, periferie, pozorovatel, iniciátor), pojmenování a formátů základních atributů (např. název zařízení, identifikátor služby, identifikátor výrobce) pro zobrazení uživatelům nebo definice režimů, ve kterých se zařízení mohou nacházet včetně obsažených procedur (např. režimy spojení, viditelnosti, párování, *bonding* – trvalé pouto s důvěřovanou protistranou).

Profily založené na GATT jsou specifické sady služeb pro konkrétní typy zařízení s jasně danou funkcionalitou definované buď konsorciem SIG, nebo výrobci zařízení, závislé na profilech GATT a GAP, jež rozšiřují. Profil může pro zařízení definovat různé role s odlišným chováním a požadavky na komunikaci na základě jejich režimu definovaným GAP (např. profil pro teploměr může definovat roli zařízení v režimu periferie, která vystavuje charakteristiku obsahující naměřenou teplotu ke čtení, a roli zařízení v režimu centrály, která tuto charakteristiku pravidelně čte).

3.3 Využití BLE pro navigační účely a interakci s prostředím

Navigace pomocí BLE se řadí k jednomu z mnoha možných využití této technologie. Klíčovou roli v tomto případě hraje nízká spotřeba energie, díky čemuž je možné vytvořit malé zařízení napájené bateriemi s dlouhou výdrží a nízkou cenou – navigační body (anglicky označované jako *beacon*), které mohou být rozmístěny v oblasti zájmu a vysílat informace využitelné k lokalizaci, zejména ve vnitřních prostorách, kde signál GPS nemusí být dostupný nebo přesný. Výhodou BLE je jeho rozšířenost, je obsažený v téměř všech moderních chytrých telefonech a mnoha dalších zařízeních, což umožňuje jeho využití širokou veřejností [15].

3.3.1 Metody lokalizace

Přesná lokalizace zařízení pomocí technologie BLE je netriviální problém. Navigační body jsou ve většině případů nezávislé jednotky, schopné vysílat předem definované zprávy jako svůj identifikátor nebo polohu zařízení, které vyžaduje lokalizaci, ale nedokážou komunikovat mezi sebou nebo s centrálním serverem (výjimkou jsou např. mesh sítě, které jsou schopny pomocí vzájemného předávání zpráv s využitím záplavových algoritmů propagovat informace a být aktivní součástí lokalizace nebo předávat informace o uživatelích pro další zpracování centrálnímu serveru) a pomáhat s lokalizací jiným způsobem [17].

Nejjednodušším případem je situace, kdy stačí zjištění přibližné oblasti, ve které se zařízení nachází, pouhou detekcí signálu navigačního bodu. Na základě síly signálu (RSSI – *Received Signal Strength Indicator*) je možné určit přibližnou vzdálenost od navigačního bodu. Tato metoda je velmi nepřesná a závislá na mnoha faktorech – prostředí, překážkách,

interferenci nebo vlastnostech antén a vyžaduje kalibraci pro každé zařízení i prostředí zvlášť, jinak není velmi efektivní (síla signálu vysílaného navigačními body se může výrazně lišit i mezi jednotlivými kusy téhož modelu, každý přijímač může mít jinou citlivost) [15].

Přesnější lokalizace je možná pomocí využití sítě navigačních bodů a kombinace signálů z nich. Existuje několik metod, jak toho dosáhnout, z nichž je mnoho závislých na předchozí kalibraci pro dané prostředí a polohu navigačních bodů. Postupy založené na metodě *fingerprinting* využívají předem definovanou databázi známých RSSI jednotlivých navigačních bodů pro známé polohy přijímače, mezi nimiž je pro nalezení neznámé polohy na základě RSSI použita lineární interpolace [15]. Pro zpřesnění výsledků bylo využito i neuronových sítí přístupem využívajícím strojové učení nad kalibračními daty [14]. Existují i hybridní přístupy, kombinující lokalizaci na základě RSSI s daty z různých senzorů dostupných v běžných mobilních telefonech (jako akcelerometr, magnetometr či gyroskop) pro konstrukci přesné historie polohy zařízení s využitím metod dead reckoning [29], a to i bez nutnosti předchozí kalibrace na základě detekce význačných orientačních bodů [34].

Verze specifikace Bluetooth 5.1 přinesla nový způsob lokalizace na základě výpočtu úhlu dopadu (AoA – *Angle-of-Arrival*) signálu. AoA lze aproximovat pomocí rozdílu fází BLE signálů dopadajících na jednotlivé antény v anténovém poli. Na základě dat z několika takových polí se známou polohou je poté možné triangulovat polohu vysílače v prostoru [5]. Specifikace 6.0 definuje procedury pro tzv. *channel-sounding*, metody pro aproximaci vzdálenosti dvou zařízení pomocí rozdílů fází signálů vysílaných napříč kanály s různou frekvencí, umožňující přesnou lokalizaci bez nutnosti použití komplikovaných anténových polí [18].

3.3.2 Služby založené na poloze

Použití BLE pro lokalizaci umožňuje rozšíření poskytovaných služeb o interaktivní prvky založené na poloze zákazníka, také to dává provozovatelům možnost rozšířeného sledování chování zákazníků a získávání velkého množství cenných dat vhodných k analýze pro zlepšení služeb a maximalizaci zisku. Obchodníkům to umožňuje vytvářet zákazníkům personalizované nabídky, poskytovat informace o zboží v okolí, navigovat je k hledaným produktům nebo zobrazovat recenze a hodnocení. Restaurace mohou využít lokalizaci pomocí BLE ke zefektivnění obsluhy a procesu objednávání pomocí automatizace přiřazení zákazníků ke stolům detekcí jejich polohy [6]. V muzeích a galeriích může být využito k poskytování informací o exponátech, výstavách nebo umělcích a navigaci návštěvníků pro tvorbu interaktivních prohlídek [15].

Kapitola 4

Základní požadavky na interaktivní navigační bod pro geocaching

Na základě poznatků z kapitol 2 a 3 lze stanovit základní požadavky na navigační bod pro geocaching, který bude umístěn v terénu a interaktivním způsobem pomocí BLE poskytne uživatelům informace o blízké keši.

4.1 Požadavky na hardwarové řešení

Hardwarové řešení navigačního bodu by mělo splňovat následující kritéria:

- **Dlouhodobá funkčnost** – zařízení musí být spolehlivé a z důvodu umístění v terénu není žádoucí častá údržba. Musí být napájeno baterií a výdrž na jedno nabití by měla být alespoň v řádu měsíců.
- **Dostatečný dosah** – signál by měl být dostatečně silný, aby bylo možné jej zachytit alespoň v oblasti dané přesností běžných GPS přijímačů, a to i v prostředí s překážkami.
- **Podpora více uživatelů připojených současně** – zařízení by mělo být schopno obsloužit více uživatelů najednou, aby bylo možné využít jeho služeb i ve skupině.
- **Uživatelská přívětivost** – zařízení by mělo být jednoduché na použití. Jednak pro uživatele, kteří by jej měli dokázat využít i bez technických znalostí pouze na základě krátkého popisu v listingu keše, ale také pro majitele keší, kteří by měli schopni navigační bod implementovat s minimálním studiem dokumentace.
- **Odolnost** – zařízení by mělo být odolné vůči nepříznivým povětrnostním podmínkám.
- **Programovatelnost** – zařízení by mělo být programovatelné, aby bylo možné měnit jeho chování a obsažené informace. Programování by mělo být jednoduché a dostupné i pro uživatele bez technických znalostí, z důvodu zjednodušení údržby proveditelné i v terénu.
- **Bezpečnost** – přenášené informace nejsou citlivé a šifrování nebude nutné, ale zařízení musí být kvůli programovatelnosti chráněno proti neoprávněnému vniknutí nějakým mechanizmem pro autorizaci.

4.2 Požadavky na softwarové řešení

Jedním z hlavních cílů je rozšířit již existující řešení o interaktivitu, která byla dosud u podobných řešení omezená na jednosměrný přenos informací z navigačního bodu do přijímače. Oboustranná komunikace umožní tvorbu interaktivních a variabilních hádanek, což zvýší atraktivitu takových keší a bude mít pozitivní vliv na zážitek uživatelů. Proto bude součástí řešení i uživatelská mobilní aplikace s následujícími požadavky:

- **Podpora pro Android** – aplikace bude dostupná pro mobilní zařízení s operačním systémem Android, který je nejrozšířenější platformou pro chytré telefony u nás[1].
- **Uživatelská přívětivost** – aplikace bude dostatečně intuitivní a jednoduchá na použití, aby nebylo nutné studium manuálu.
- **Interaktivita** – aplikace bude podporovat obousměrnou komunikaci s navigačním bodem, umožní uživatelům zadávat odpovědi na hádanky a získávat zpětnou vazbu. Akce uživatele budou mít vliv na chování navigačního bodu a informace, které poskytuje.
- **Volitelnost** – aplikace nebude pro použití navigačního bodu nutná. Kvůli pravidlům portálu *Geocaching.com* nelze vynutit použití konkrétní aplikace, komunikační protokol s navigačním bodem musí být dostatečně jednoduchý a přehledný pro použití s libovolným BLE terminálem.

4.3 Mikrokontroléry NXP vyhovující požadavkům

NXP nabízí širokou škálu mikrokontrolérů založených na architektuře ARM. Podmínkou vhodného mikrokontroléru je integrace BLE modulu. Seznam vyhovujících mikrokontrolérů (získaných pomocí filtrování v nástroji pro výběr produktů na stránkách NXP[2], byly zahrnuty pouze aktivně podporované modely) je v tabulce 4.1. Následuje bližší popis vybraných modelů.

Mikrokontrolér	Jádro	Frekvence	BLE	Flash/RAM
KW45	Cortex-M0+ + Cortex-M3 + Cortex-M33	96 MHz	5.3	až 1 MB/128 kB
MKW39/38/37	Cortex-M0+	48 MHz	5.0	512 kB/64 kB
MKW36A/35A/34A	Cortex-M0+	48 MHz	5.0	až 512 kB/64 kB
MKW31Z	Cortex-M0+	48 MHz	4.2	až 512 kB/128 kB
QN908x	Cortex-M4	32 MHz	5.0	512 kB/128 kB
QN9090/30	Cortex-M4	48 MHz	5.0	až 640 kB/152 kB
MCX W71x	Cortex-M33 + Cortex-M3	96 MHz	5.3	až 1 MB/128 kB
NHS52S04	Cortex-M33F	32 MHz	5.3	1 MB/128 kB

Tabulka 4.1: Výběr mikrokontrolérů NXP s integrovaným BLE modulem

[1] https://gs.statcounter.com/os-market-share/mobile/czech-republic
[2] https://www.nxp.com/products/product-selector:PRODUCT-SELECTOR?category=c718_c978

- **KW45** – mikrokontrolér zaměřený na automotivní a industriální sektory. Kromě hlavního jádra obsahuje i specializované jádra vyhrazené pro rádiovou komunikaci a bezpečnostní funkce (rozšířená ochrana proti neoprávněnému přístupu, kryptografická akcelerace, zabezpečené uložiště a správa klíčů). Má volitelnou podporu sběrnice CAN.
- **MKW39/38/37** – velmi úsporné mikrokontroléry pro komunikaci na delší vzdálenosti v horších podmínkách. Také mají volitelnou podporu sběrnice CAN pro automotivní aplikace.
- **MKW36A/35A/34A** – starší verze předchozích modelů s podobnými vlastnostmi, ale s horšími parametry BLE modulu (nižší citlivost a datový průtok).
- **MKW31Z** – velmi úsporný mikrokontrolér se starší verzí BLE s volitelnou podporou komunikace ve standardu IEEE 802.15.4 (např. pro protokol Zigbee).
- **QN908x** – velmi úsporné mikrokontroléry s jádrem Cortex-M4 pro aplikace v uživatelském sektoru.
- **QN9090/30** – nahrazují starší modely QN908x a MKW31Z. Nabízí volitelný integrovaný NFC tag pro jednoduché OOB párování a konfiguraci. Ze všech zmíněných modelů v aktivním stádiu životního cyklu jsou nejlevnější.
- **MCX W71x** – mikrokontrolér zaměřený na automotivní a industriální aplikace. Obsahuje dedikovaný rádiový modul s vlastním jádrem a podporuje protokoly Thread a Zigbee, včetně sběrnice CAN. Je určen pro náročné aplikace s vysokými požadavky na bezpečnost.
- **NHS52S04** – nový mikrokontrolér s velmi nízkou spotřebou určený pro bezdrátové aplikace ve zdravotnickém průmyslu. Nahrazuje starší model QN908x.

Ze zmíněných mikroprocesorů by bylo na základě definovaných požadavků možné v navigačním bodu využít všechny – sdílí podporu zabezpečené komunikace pomocí BLE, jsou dostatečně energeticky úsporné a mají pro očekávané využití dostatečný rozsah přípustné operační teploty (všechny alespoň -40 až 105 °C). Avšak pro účely této práce se model **QN9090HN/30HN** jeví jako nejvhodnější. U použití v navigačním bodu se neočekávají vysoké nároky na výkon nebo paměť, proto je preferovaný model s nižšími parametry (pro QN9030HN 320 kB Flash a 88 kB ROM paměti), který je zároveň nejlevnější z nabízených. Pro odběr v malém množství při tvorbě prototypu je však cena obou variant totožná (přibližně 90 Kč za kus) a obě sdílí stejné pouzdro, proto bude při vývoji prototypu použita varianta QN9090HN, která může být v budoucí masové produkci nahrazena levnější variantou QN9030HN.

4.3.1 Moduly s integrovanou anténou

NXP nabízí primárně samotné čipy, které je nutné osadit na desku plošných spojů (DPS) vlastního návrhu obsahující alespoň základní pasivní komponenty (rezistory, kondenzátory atd.) nutné k provozu integrovaného napěťového regulátoru, oscilátory a další součástky s parametry a zapojením specifikovaným referenčním návrhem výrobce. Pro zajištění bezdrátové komunikace musí být přítomna i anténa s korektním impedančním profilem, propojená s mikrokontrolérem stopou s kontrolovanou impedancí, a ladící obvod pro zajištění správné funkce na požadované frekvenci (2,4 GHz) [19, 28].

Ačkoli NXP ke svým mikrokontrolérům nabízí referenční návrhy, které lze použít jako základ pro vlastní DPS včetně vhodných tištěných antén [19], je nutné je přizpůsobit konkrétním požadavkům a použitým materiálům, jež mají výrazný vliv především na impedanci signálových stop. Provedení takových úprav je časově náročné, nákladné (často je nutné pro dosažení požadovaných parametrů vyrobit mnoho iterací prototypu s úzkou spoluprací se zvoleným výrobcem DPS) a vyžaduje hluboké znalosti v oblasti návrhu radiofrekvenční elektroniky včetně specializovaných měřících nástrojů [28].

Kvůli zmíněným nárokům by bylo pro účely této práce vhodné použít hotový modul s integrovanou anténou, který by komplikace spojené s návrhem a výrobou DPS výrazně omezil. Takové moduly bývají taktéž vybaveny součástkami pro zajištění správné funkce mikrokontroléru, čímž dále zjednoduší návrh a výrobu. Jejich nevýhodou je vyšší cena oproti samotnému čipu včetně nutných pasivních součástek.

NXP má v nabídce několik modulů s integrovanou anténou, které by byly pro účely navigačního bodu použitelné. Avšak jde o vývojové moduly s vysokou cenou, které jsou určeny pro vývoj a testování prototypů, nikoli pro produkční nasazení. Příkladem je vývojový modul QN9090-001-T10[3] s mikrokontrolérem QN9090THN, malou velikostí a profrézovanými pokovenými okraji pro snadné osazení. Jeho cena je však v přepočtu přes 700 Kč za kus, což je pro produkční nasazení nepřijatelné.

Alternativou jsou moduly od třetích stran, které jsou dostupné za nižší cenu a splňují stanovené požadavky, avšak nejsou pro mikrokontroléry NXP velmi rozšířené. Jednou ze dvou nalezených možností je ISP5261-WX [13] od společnosti Insight SiP, založený na mikrokontroléru RW612. Kromě BLE 5.3 a dalších bezdrátových protokolů (Thread, Matter) podporuje i WiFi 6, což není pro účely navigačního bodu nutné a je podmíněno vyšší spotřebou energie při BLE operacích – pro vysílání o intenzitě 0 dBm je spotřeba 56 mA, což je výrazně více než u QN9090 (při stejné intenzitě je jeho spotřeba při vysílání 7,4 mA [21]). Také má užší rozsah přijatelného napájecího napětí a při připojení k baterii by návrh vyžadoval použití externího napěťového regulátoru.

Druhou alternativou jsou moduly série NINA-B506 [32] od společnosti u-blox. Ve verzi s integrovanou anténou existují dva modely – NINA-B506-00B založené na mikrokontroléru K32W148 a NINA-B506-10B založené na MCX W71. K32W148 je předchůdcem MCX W71 s plnou softwarovou i hardwarovou kompatibilitou, ale již není doporučený pro nové návrhy, pročež nebyl v části 4.3 zmíněn. Model NINA-B506-10B je v čase psaní této práce stále ve vývoji a není dostupný na trhu, proto je model **NINA-B506-00B** (který byl uveden na trh v roce 2024) pro použití v navigačním bodu jedinou možností. Jeho cena je přibližně 190 Kč za kus[4].

[3] https://www.nxp.com/part/QN9090-001-T10

[4] https://www.digikey.cz/cs/products/detail/u-blox/nina-b506-00b/21363316

Kapitola 5

Návrh řešení navigačního bodu

Tato kapitola se zabývá návrhem navigačního bodu pro geocaching na základě stanovených základních požadavků a poznatků z předchozích kapitol. Kapitola se dělí na dvě části – návrh hardwarového řešení (část 5.1) a návrh softwarového řešení (část 5.2) obsahující popis obslužného firmware mikrokontroléru, interaktivního dialogu s uživatelem včetně komunikačního protokolu a návrh uživatelské mobilní aplikace pro použití s navigačním bodem.

5.1 Návrh hardwarového řešení

Navigační bod je navržen jako samostatné zařízení s integrovaným mikrokontrolérem umožňujícím komunikaci pomocí BLE. Bude sestávat z desky plošných spojů (DPS) o malých rozměrech, jež by se měla vejít do keší o běžných velikostech. Návrh je zaměřen na nízkou výrobní cenu a koncipován tak, aby byl vhodný pro sériovou výrobu a následné uvedení na trh. Kvůli selhání pokusů o oživení prototypu s mikrokontrolérem QN9090 (viz část 6.1) byl proveden i návrh druhé verze zařízení s modulem NINA-B506-00B.

5.1.1 Obecný návrh

Zařízení je napájeno knoflíkovou baterií typu CR2032, umístěnou v držáku na DPS. Tento typ byl zvolen z důvodu dostupnosti a nízké ceny. Je běžně dostupný v obchodech s elektronikou a cena takových baterií se pohybuje v řádu nižších desítek korun. Zároveň má dostatečnou nominální kapacitu (přes 200 mAh) pro dlouhodobý provoz úsporných mikrokontrolérů včetně korektního provozního napětí pro jejich integrovaný regulátor (3 V).

Pro účely vytvoření prototypu může být navrženo a vyrobeno s využitím technologie 3D tisku plastové pouzdro, které bude chránit zařízení před nepříznivými povětrnostními podmínkami a umožní jeho snadné umístění v terénu. Návrh a výroba pouzdra však není pro funkční prototyp podmínkou a nebyla provedena. Deska obsahuje dva prokovené otvory o průměru 2,4 mm pro upevnění pomocí šroubů standardu M2 nebo jiných prostředků a může být umístěna přímo ve skryté schránce, která bude pro zařízení dostatečnou ochranou. V tom případě ale musí být případnému nálezci zamezen přístup ke tlačítku, buď fyzicky, nebo implementací softwarového mechanizmu pro uzamčení při ostrém provozu. Jeden otvor se nachází ve spodním rohu desky, druhý na horní části protilehlé strany tak, aby byl v dostatečné vzdálenosti od antény a nedošlo k degradaci kvality signálu, kterou může umístění kovového objektu v blízkosti antény způsobit.

Na DPS jsou umístěny tzv. fiduciály – kruhové značky o průměru 1 mm provedené jako pájecí plošky s 1 mm širokým okrajem v odmaskované mědi. Jsou rozloženy ve třech rozích

desky a tvoří vrcholy pravoúhlého trojúhelníku. Bývají využívány pro optickou detekci přesné polohy DPS při její výrobě, osazování povrchově montovanými součástkami (SMT, *Surface Mount Technology*) pomocí mechanických osazovacích strojů a testování [2].

Pro uživatelský vstup jsou na desce umístěna dvě tlačítka používaná při konfiguraci navigačního bodu – jedno pro reset mikrokontroléru a druhé pro vstup do režimu párování s mobilní aplikací a vrácení do továrního nastavení. Jedná se o běžné SMT mikrospínače o velikosti 4,6 mm x 2,8 mm a jsou pomocí pull-up rezistorů připojeny ke vstupům mikrokontroléru. Kvůli omezení zákmitů při jejich stisku je poblíž každého z nich mezi výstupem a zemí připojen kondenzátor o hodnotě 10 nF. Indikace stavu zařízení je zajištěna jednou červenou SMT LED s profilem 0603, která v režimu párování bliká.

Oba návrhy obsahují oscilátor s krystalem o frekvenci 32,768 kHz pro generování nízkofrekvenčního hodinového signálu pro časování a probouzení mikrokontroléru z režimu spánku. Pro jeho správnou funkci je nutné upravit jeho kapacitanci na hodnotu, jež mikrokontrolér vyžaduje. To je běžně zajištěno pomocí dvou kondenzátorů připojených mezi oba vývody krystalu a zem, v případě obou návrhů však mikrokontroléry obsahují interní konfigurovatelné kondenzátory, které umožňují nastavit kapacitanci krystalu bez nutnosti použití externích součástek, čehož bylo využito.

Programování a ladění mikrokontroléru je možné pomocí rozhraní *Serial Wire Debug* (SWD), pro nějž je připraven konektor 2x5 pinů s roztečí 1,27 mm zapojený dle standardního zapojení pro desetipinové ARM SWD konektory[1], které používají signály SWCLK (hodinový signál), SWDIO (datový signál), SWO (trasovací signál pro datový výstup, informace o běhu, nebo měření spotřeby) a RESET. SWD konektor lze použít i k napájení mikrokontroléru (pokud to programátor podporuje), v tom případě však nemůže být zapojena baterie, protože obvod neobsahuje žádný mechanizmus pro ochranu proti zpětnému proudu při odlišných napětích obou zdrojů (např. diodu).

5.1.2 Prototyp s mikrokontrolérem QN9090

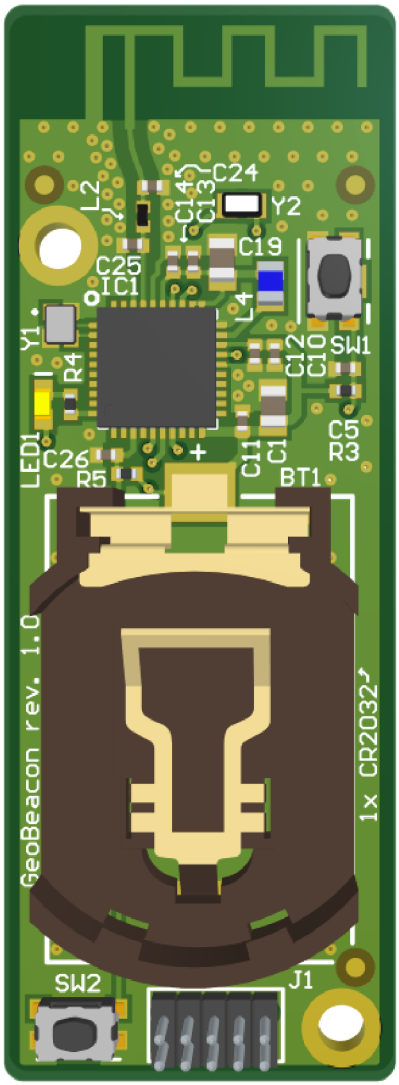
Prototyp je založen na mikrokontroléru QN9090HN v pouzdře HVQFN40 od společnosti NXP. Je osazen na DPS s rozměry 20 mm x 55 mm, jejíž 3D model je zobrazen na obrázku 5.1. Montážní otvory jsou umístěny v levém horním a pravém dolním rohu desky, vzdálené 15,5 mm horizontálně a 40 mm vertikálně od sebe.

Schéma zapojení a seznam použitých součástek je v příloze A.1. Zapojení a volba komponent nutných pro základní provoz mikrokontroléru (pasivní součástky zajišťující zpětnou vazbu pro interní regulátor napětí, oscilátory, kondenzátory filtrující záchvěvy v napájecím napětí a síť pro seřízení antény) následuje doporučení výrobce stanovené v datasheetu [21]. Kromě nízkofrekvenčního oscilátoru zapojení obsahuje i vysokofrekvenční oscilátor s krystalem o frekvenci 32 MHz, který je použit pro generování hodinového signálu pro integrované rádio. Jeho kapacitance je taktéž nastavena interně mikrokontrolérem.

Návrh DPS (podklady pro něj jsou zahrnuty v příloze B) byl proveden v programu Altium Designer a vychází z referenčních designů výrobce s označením JN-RD-6058[2], konkrétně návrhu OM15080 – zařízení vybaveného BLE modulem s USB konektorem typu A. Tento návrh byl upraven pro potřeby navigačního bodu. Byly odstraněny součástky nutné pro spojení USB, externí paměť Flash a jedna ze dvou LED. Místo zmíněných součástek bylo přidáno tlačítko pro účely vstupu do režimu párování, držák na knoflíkovou baterii,

[1] https://developer.arm.com/documentation/101416/0100/Hardware-Description/Target-Interfaces/Cortex-Debug--10-pin-

[2] https://www.nxp.com/webapp/Download?colCode=JN-RD-6058_QN9090_ReferenceDesign_1V0



Obrázek 5.1: 3D model desky plošných spojů prototypu s mikrokontrolérem QN9090

díry pro upevnění desky a konektor pro ladění a programování pomocí rozhraní *Serial Wire Debug* (SWD).

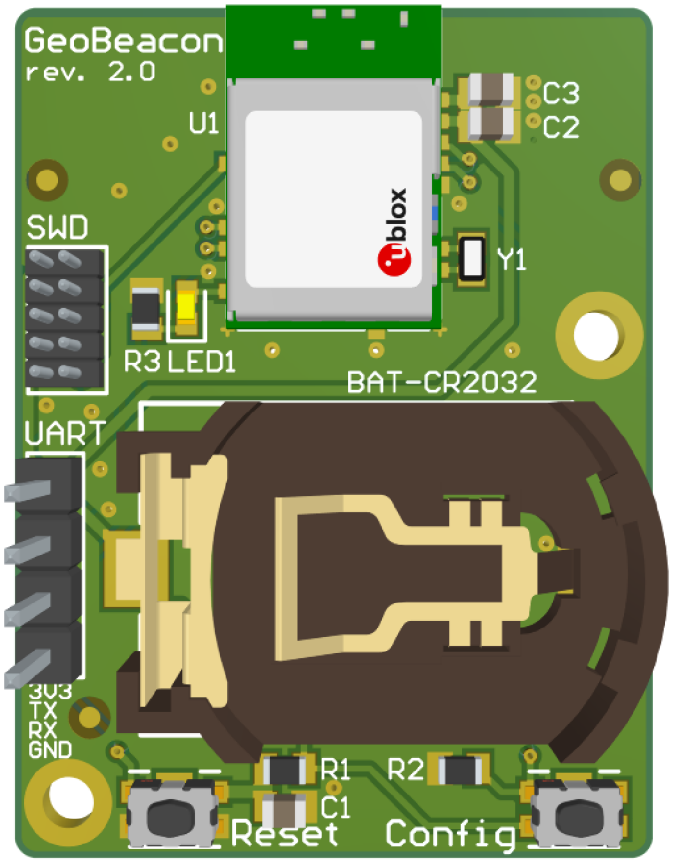
Složení vrstev DPS muselo být kvůli možnostem zvoleného výrobce prototypů DPS také upraveno. Původní návrh obsahoval dvouvrstvou DPS nejasné tloušťky a parametrů použitých materiálů, což bylo změněno na čtyřvrstvou DPS s celkovou tloušťkou 1,5 mm. Přesné složení vrstev se specifikací použitých materiálů je v příloze B. Vnější vrstvy jsou signálové s vylitou měděnou uzemněnou referenční plochou, vnitřní vrstvy slouží pouze jako uzemněná plocha. Oproti referenčnímu návrhu byl redukován počet prokovů pro uzemněné plochy, aby se snížily náklady na výrobu (výrobci DPS často účtují příplatky za vyšší hustotu otvorů), ale stále zůstal zachován dostatečný počet pro zajištění dobré vodivosti, propojení vrstev a stínění signálových stop.

Kvůli této změně bylo nutné upravit spoj mezi mikrokontrolérem a tištěnou anténou pro rádiovou komunikaci integrovanou přímo na DPS, přesně kopírující původní návrh výrobce. Jedná se o anténu typu *meandered inverted-F antenna* (MIFA) s impedancí 50 Ω. Stejnou

impedanci musí mít pro požadovanou frekvenci (2,4 GHz) i zmíněný spoj, jinak by mohlo dojít k degradaci kvality signálu. Impedance spoje je ovlivněna jeho šířkou, vzdáleností od uzemněné referenční plochy (zde při pohledu z vrchu druhé signálové vrstvy) a šířkou i dielektrickou konstantou použitých materiálů [28]. Vzhledem k provedeným změnám (zejména tloušťky DPS) bylo nutné provést simulaci impedančního profilu spoje a upravit jeho šířku. Simulace byla provedena v programu Altium Designer pomocí integrovaného nástroje pro analýzu impedance Simbeor a šířka byla snížena z původních 0,65 mm na 0,23 mm, přičemž vzdálenost od uzemněné plochy byla kvůli možnému vlivu na impedanční profil rozšířena na trojnásobek šírky spoje.

5.1.3 Prototyp s modulem NINA-B506-00B

Po selhání pokusů o oživení prototypu s mikrokontrolérem QN9090HN byl navržen druhý prototyp s modulem NINA-B506-00B od společnosti u-blox založeným na mikrokontroléru K32W148. Rozměry desky jsou 30 mm x 40 mm, zvoleny na základě doporučení výrobce modulu v integračním manuálu [33], jenž udává minimální přesah hostitelské DPS s vylitou měděnou plochou 10 mm na každé straně modulu. Montážní otvory jsou umístěny v levém dolním a pravém horním rohu desky, vzdálené 25 mm horizontálně a 22 mm vertikálně od sebe. 3D model návrhu je zobrazen na obrázku 5.2.



Obrázek 5.2: 3D model desky plošných spojů prototypu s modulem NINA-B506-00B

Zapojení bylo oproti předchozímu návrhu značně zjednodušeno, protože modul NINA-B506-00B obsahuje integrovanou anténu (včetně seřizovací sítě) a veškeré potřebné pasivní součástky pro jeho provoz. Pouze bylo nutné přidat kondenzátory pro stabilizaci napájecího napětí – jeden 100nF pro filtraci vysokofrekvenčních zákmitů způsobených rušením při vysílání a druhý 10µF, vyrovnávající poklesy napětí při vyšším odběru během BLE událostí – mezi napájecí vývody mikrokontroléru a zem. Problém dočasných poklesů napětí je způsoben vysokou interní rezistancí knoflíkové baterie, která může způsobovat poklesy napětí až v řádu desetin voltů při odběru v jednotkách mA. Schéma zapojení a seznam použitých součástek je v příloze A.2.

Tlačítko pro konfiguraci je narozdíl od minulé verze zapojeno k pinu BOOT_CONFIG mikrokontroléru pomocí pull-down rezistoru a vykonává navíc další funkci. Přivedení logické 1 na tento pin při resetu mikrokontroléru způsobí vstup do bootloaderu uloženém v paměti ROM, což umožní komunikaci s mikrokontrolérem pomocí periferních rozhraní – zejména nahrání nového firmware a vypálení pojistek [22]. K tomu účelu byl přidán čtyřpinový konektor s roztečí 2,54 mm pro připojení sériové linky UART. Využití tohoto konektoru je popsáno v části 6.1.2.

Pro usnadnění ručního osazení desky byly zapojené plošky modulu prodlouženy a přesahují jeho okraj o 0,3 mm, což zvýší pravděpodobnost správného kontaktu při zapájení. Taktéž byly pod spodní rohy modulu přidány centrovací křížky v odmaskované mědi, které usnadní jeho správné umístění při ručním osazení v případě nepřesné polohy potisku obrysu. Z důvodu usnadnění ručního osazení, menšího počtu součástek a větší desky byly použity SMT součástky s většími rozměry – typu 0805.

Navržená DPS je dvouvrstvá s celkovou tloušťkou 1,5 mm, tloušťka mědi je 35 µm a dielektrické jádro je z materiálu FR-4. Přesná specifikace složení a materiálových konstant vrstev není v tomto případě podstatná, deska neobsahuje žádné signálové stopy s kontrolovanou impedancí. Důležitá je dostatečná plocha, velikost a nepřerušenost uzemněné vylité měděné plochy pro zajištění silné referenční země pro rádiovou komunikaci. Tato plocha má (na obou vrstvách) obdelníkový výřez v oblasti přímo pod tištěnou anténou modulu, jenž je umístěn uprostřed hrany na horním okraji desky a je pro zajištění dobré kvality signálu nezbytný [33]. Podklady pro návrh DPS, vytvořené v programu Altium Designer, jsou v příloze B.

5.2 Návrh softwarového řešení

Softwarové řešení je členěno na dva hlavní pospolité celky – obslužný firmware mikrokontroléru a mobilní aplikaci pro interakci s uživateli a konfiguraci navigačního bodu pro majitele. Hlavním účelem obou částí je umožnit uživatelům interaktivní dialog s navigačním bodem, což bude zajištěno vhodně navrženým komunikačním protokolem založeným na předávání zpráv mezi mikrokontrolérem a mobilní aplikací.

5.2.1 Obslužný firmware mikrokontroléru

Firmware mikrokontroléru bude implementován v jazyce C s využitím vývojové sady MCUXpresso SDK[3], poskytující veškerou potřebnou funkcionalitu pro ovládání mikrokontrolérů společnosti NXP a jejich periferií. Jedná se o volně dostupnou modulární sadu knihoven a příkladů, jejíž součástí je i operační systém reálného času FreeRTOS, který bude využit pro správu úloh (včetně umožnění simulované konkurence) a komunikaci s BLE modulem.

[3] https://mcuxpresso.nxp.com/mcuxsdk/latest/html/index.html

V době, kdy neprobíhá žádná komunikace, bude navigační bod šetřit baterii přechodem do hlubokého spánku (*Deep sleep*), ze kterého bude probuzen při detekci pokusu o připojení nebo časovačem pro vysílání zpráv pro objevení. Hluboký spánek je pro tento účel vhodný, protože zachová obsah použité části paměti RAM, ale vypne většinu periferií a sníží spotřebu na minimum. NXP SDK k tomu poskytuje odpovídající funkcionalitu, která je schopná řídit přechody mezi režimy automaticky, a to ve všech stádiích BLE komunikace (objevení, připojení a přenos dat) [20, 22].

Správa BLE komunikace

Navigační bod bude zastávat roli periferie v objevitelném režimu – bude ve stanoveném intervalu vysílat zprávy pro objevení centrálami. Tento interval a síla vysílání budou stanoveny experimentálně v průběhu implementace na základě dosahu signálu a spotřeby energie. Při detekci pokusu o připojení od mobilního telefonu uživatele proběhne proces navázání spojení. Párování nebo *bonding* provedeno nebude, sice to znemožní šifrovanou komunikaci, ale pro účely navigačního bodu a vzhledem k charakteru přenášených informací šifrování není nutné. Protože je pro párování či *bonding* nutné v paměti mikrokontroléru uchovávat informace o spárovaných zařízeních a jedná se o nepřetržitě běžící aplikaci, ke které se připojuje velké množství zařízení, bylo by pro zabránění přeplnění paměti nutné implementovat mechanizmus pro automatické zapomínání protistran, což by částečně porazilo pointu párování. Taktéž to ulehčí proces spojení pro uživatele.

Po úspěšném připojení si navigační bod pro identifikátor připojeného zařízení bude pamatovat čas posledního připojení, momentální stav dialogu s uživatelem a vyšle mu úvodní zprávu. Stav dialogu bude následně využit pro rozhodování o platnosti odpovědí uživatele a případné obnovení konverzace při opětovném připojení v případě přerušení spojení (pak bude vždy znovu zaslána aktuální otázka). Pokud uběhne stanovený čas (nastavitelný při konfiguraci) od posledního připojení nebo je dosažena poslední otázka, navigační bod zapomene informace o daném uživateli a po jeho dalším připojení započne nový dialog.

Konfigurace

Protože dialog musí být konfigurovatelný, bude implementován proces pro jeho konfiguraci majitelem. Tento proces bude vyžadovat vyšší úroveň zabezpečení. Zde se nabízí využití párování, nějakého mechanizmu pro vzájemnou autentifikaci a následné šifrování komunikace, ale z důvodu výše zmíněných nevýhod párování použito nebude. Bude nutné implementovat nějaký mechanizmus pro autorizaci majitele, což bude bezpodmínečně vyžadovat přenos citlivých informací, ale pouze v rámci jednorázového procesu provedeném buď v kontrolovaném prostředí (např. doma) nebo v terénu, kde se přítomnost potenciálních útočníků nepředpokládá. Proto bylo vyhodnoceno, že autentizace a šifrování nejsou nutné.

Mechanizmem pro autorizaci majitele bude zadání hesla v aplikaci. Před první konfigurací bude z výroby nastaveno na výchozí hodnotu, v případě potenciální budoucí produkční výroby generované jako unikátní pro každý navigační bod a přiložené v balení. Po autorizaci jej bude, včetně dalších parametrů jako název keše, intervalu pro zapomenutí uživatele, síly vysílání nebo uloženého dialogu reprezentovaného stavovým automatem, možné změnit. V případě zapomenutí hesla půjde zařízení resetovat do továrního nastavení dlouhým stisknutím tlačítka.

Pro zvýšení bezpečnosti bude navigační bod akceptovat pokusy o autorizaci pouze v režimu konfigurace. Do něj se na omezenou dobu (byla zvolena jedna minuta) dostane krátkým stisknutím tlačítka, což bude signalizováno blikáním LED. Tímto způsobem se zamezí po-

kusům o útok na zařízení bez fyzického přístupu. V případě, kdy by útočník fyzický přístup měl, bude omezena možnost útoku na heslo hrubou silou implementací dočasné blokace protistrany po několika neúspěšných pokusech o autorizaci a ukončení režimu konfigurace po každém takovém pokusu.

GATT server

Navigační bod bude představovat GATT server a implementovat vlastní BLE profil založený na GATT, závislý na následujících službách:

- Device Information Service – poskytne informace o zařízení jako název, výrobce a verzi.
- Battery Service – poskytne informace o stavu baterie.
- Wireless UART Service – definovaná NXP, poskytne zapisovatelný atribut pro implementaci sériové komunikace.
- Nordic UART Service[4] – definovaná Nordic Semiconductor, poskytne atributy pro čtení a zápis sériové komunikace.
- Vlastní služba pro konfiguraci – poskytne následující zapisovatelné atributy pro autorizaci, konfiguraci dialogu a parametrů navigačního bodu. Unikátní identifikátory pro tuto službu a její atributy jsou uvedeny v příloze C.
  - Atribut pro autorizaci zápisem hesla majitele, z atributů pro konfiguraci jediný dostupný bez autorizace,
  - atribut pro zápis nového jména,
  - atribut pro zápis nového hesla,
  - atribut pro indikaci úmyslu nahrání nového dialogu zápisem jeho velikosti v bajtech a počtu přenesených paketů, po ukončení přenosu bude obsahovat kód indikující úspěch nebo chybu pro přečtení zařízením majitele,
  - atribut pro zápis dat dialogu, očekává přenos dat v několika paketech, kvůli kontrole integrity přenosu zahájených jejich sekvenčním číslem a
  - atribut pro čtení statistik o využití navigačního bodu.

Důvodem pro implementaci dvou odlišných služeb pro sériovou komunikaci je rozšíření kompatibility s různými terminály (odůvodnění je v části 5.2.2). Jedinou aplikací s podporou NXP Wireless UART Service je *IoT Toolbox*[5], ostatní aplikace (např. *nRF Connect*[6] nebo *Bluefruit Connect*[7]) nativně podporují pouze službu Nordic UART, jež je široce používána. Obě služby mají rozdílnou architekturu. NXP Wireless UART očekává u obou protistran vlastní GATT server, který poskytuje jedinou zapisovatelnou charakteristiku, zatímco Nordic UART dělí protistrany na GATT server a klient, přičemž server (zde navigační bod) poskytuje dvě charakteristiky – jednu zapisovatelnou (RX), přes kterou klient posílá data serveru, a jednu čtecí (TX), přes kterou server odesílá data klientovi ve formě notifikací.

[4] https://docs.nordicsemi.com/bundle/ncs-latest/page/nrf/libraries/bluetooth/services/nus.html
[5] https://play.google.com/store/apps/details?id=com.freescale.kinetisbletoolbox
[6] https://play.google.com/store/apps/details?id=no.nordicsemi.android.mcp
[7] https://play.google.com/store/apps/details?id=com.adafruit.bluefruit.le.connect

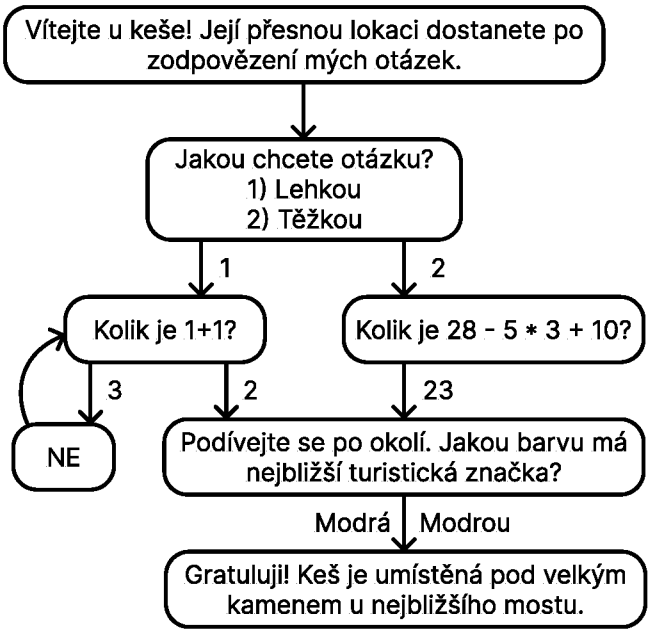
Navigační bod bude také sbírat statistiky o využívání, které budou po autorizaci správce dostupné pro čtení z atributu ve službě pro konfiguraci. Tento atribut bude mít velikost 25 bajtů, formát a význam dat je v tabulce 5.1. Přenášená data budou mít bajtové pořadí *little-endian*.

Bajt	Datový typ	Význam
0	`uint32_t`	Počet připojení k navigačnímu bodu
4	`uint32_t`	Počet unikátních uživatelů na základě BLE adresy
8	`uint32_t`	Počet úspěšných dokončení dialogu
12	`uint32_t`	Průměrné trvání dialogu (v milisekundách)
16	`uint32_t`	Nejdelší trvání dialogu (v milisekundách)
20	`uint8_t`	Počet nejvíce připojených uživatelů současně
21	`uint32_t`	Doba od posledního dokončení dialogu (v sekundách)

Tabulka 5.1: Formát a význam dat v atributu pro čtení statistik

5.2.2 Interaktivní dialog s uživatelem

Pro zajištění interaktivity bude komunikace probíhat pomocí větveného dialogu ve formě otázek a odpovědí. Proto bude reprezentován stavovým automatem, jehož stavy budou představovat aktuální otázku a přechody mezi stavy budou záviset na odpovědích uživatele. Při nesprávné odpovědi zůstane aktuální stav nezměněn. Pokud bude nějaký stav obsahovat pouze jeden odchozí přechod, pak tento přechod může být prázdný a provede se automaticky, což umožní použití tohoto stavu pro zobrazení libovolné zprávy nebo nápovědy. Bude možné vytvořit otázky s předem definovanou sadou odpovědí (uzavřené otázky), které se zobrazí uživateli v aplikaci jako tlačítka. Příklad dialogu reprezentovaného stavovým automatem je na obrázku 5.3.



Obrázek 5.3: Přechodový diagram konečného automatu představující interaktivní dialog s uživatelem

Protože dle pravidel portálu *Geocaching.com* není možné vynutit použití konkrétní aplikace, komunikační protokol musí být dostatečně jednoduchý a přehledný pro použití s libovolným BLE terminálem (aplikací umožňující připojení k zařízením a následnou komunikaci přes BLE v textové podobě), ale zároveň musí být zpracovatelný i uživatelskou aplikací pro zobrazení dialogu vlastním, přívětivým způsobem. Proto bude komunikační protokol založen na textových zprávách, kde zprávy vysílané navigačním bodem budou obsahovat otevřenou otázku zakončenou otazníkem a koncem řádku nebo zprávu bez požadované odpovědi zakončenou pouze koncem řádku (majitelem definovaný obsah zpráv pak kvůli jasné identifikaci typu a konce nesmí obsahovat konce řádků). V případě uzavřených otázek bude následovat seznam odpovědí, kde každá odpověď bude začínat číslem odpovědi a závorkou, následovanou textem odpovědi a koncem řádku. Uživatel bude odpovídat zasláním čísla odpovědi v případě uzavřených otázek nebo vlastní odpovědí v případě otázek otevřených. U špatných odpovědí následuje zpráva `Spatna odpoved. Zkuste to znovu.`, u správných odpovědí na otevřené otázky následuje zpráva `Spravne!` a přechod do následujícího stavu. Po dosažení posledního stavu a po přijetí jakékoliv zprávy po dosažení konce dialogu následuje zpráva `Jste na konci dialogu. Pro novy pruchod se odpojte a znovu pripojte.`

Navigační bod i mobilní aplikace budou pro dialog využívat kódování textu UTF-8, čímž bude zajištěna podpora pro české znaky a další znaky z různých jazyků. Pevně definované zprávy protokolu však obsahují pouze znaky ASCII, aby bylo zajištěno jejich správné zobrazení i v případech, kdy použitý BLE terminál toto kódování nepodporuje, jak je tomu např. u aplikace *IoT Toolbox* od výrobce NXP, na které byl protokol při vývoji testován.

Následující záznam komunikace přes terminál ukazuje možný průchod dialogem definovaným na obrázku 5.3 (řádky začínající znakem `>` představují zprávy z navigačního bodu, řádky začínající znakem `<` představují odpovědi uživatele):

```
> Vítejte u keše! Její přesnou lokaci dostanete po zodpovězení mých otázek.
> Jakou chcete otázku?
> 1) Lehkou
> 2) Těžkou
< 1
> Kolik je 1 + 1?
< 3
> NE
> Kolik je 1 + 1?
< 2
> Spravne!
> Podívejte se po okolí. Jakou barvu má nejbližší turistická značka?
< Červená
> Spatna odpoved. Zkuste to znovu.
< Modrá
> Spravne!
> Gratuluji! Keš je umístěná pod velkým kamenem u nejbližšího mostu.
> Jste na konci dialogu. Pro novy pruchod se odpojte a znovu pripojte.
```

5.2.3 Mobilní aplikace

Mobilní aplikace bude zajišťovat zpracování příchozí komunikace a poskytovat uživatelsky přívětivé rozhraní pro tvorbu a průchod interaktivním dialogem a konfiguraci navigačního bodu. Aplikace bude dostupná primárně pro operační systém Android, a to z důvodu jeho

dominance na českém trhu, komplikací spojených s vývojem pro iOS (nutnost registrace vývojáře, vlastnictví Apple zařízení a dodatečné náklady[8]) a faktu, že použití navigačního bodu uživateli nebude vynuceno touto aplikací. Podpora ostatních platforem je předmětem případného budoucího rozšíření.

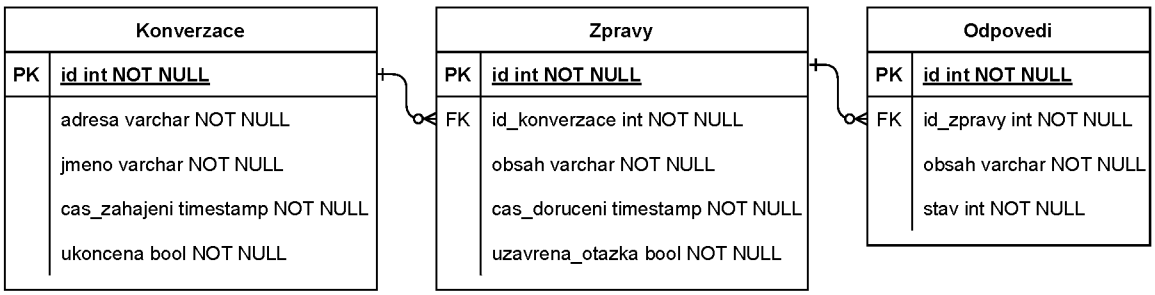
Aplikace bude mít dva oddělené režimy – režim pro uživatele umožňující interakci s navigačním bodem a režim pro majitele umožňující konfiguraci a správu navigačního bodu včetně tvorby, úpravy a nahrávání dialogu. Mezi oběma režimy bude možné volně přepínat, ve výchozím stavu ale bude dostupný pouze režim pro uživatele a přepínač se zobrazí pouze po jeho povolení v nastavení aplikace, přičemž bude zobrazeno varování informující uživatele, že tento režim je určen pouze pro majitele navigačních bodů a neposkytuje běžným uživatelům žádnou užitečnou funkcionalitu.

Uživatelský režim

Uživatelský režim se bude skládat ze dvou obrazovek. Hlavní obrazovka (na obrázku 5.5 vlevo) bude zabezpečovat interakci s navigačním bodem. Před připojením bude informovat uživatele, že probíhá vyhledávání. Po zachycení navigačního bodu proběhne notifikace uživatele (zvukem a vibracemi), pokus o připojení a po vzájemné výměně informací a dostupných služeb se jeho název (identifikační kód a název keše) zobrazí jako nadpis obrazovky. Poté bude aplikace čekat na přijetí zpráv, které budou zpracovány a zobrazeny v rámci dialogu.

Každá příchozí zpráva bude představena jako vizuálně odlišený blok, který bude obsahovat text zprávy, vstupní textové pole pro odpověď u otevřených otázek nebo tlačítka pro odpovědi v případě otázek uzavřených. Odeslané odpovědi se zobrazí pod sebou v rámci každého bloku (za otázkou, ale před uživatelským vstupem) a bude u nich barevná indikace správnosti. Po zobrazení poslední zprávy bude uživatel informován o úspěchu, zobrazí se tlačítko pro návrat na úvodní obrazovku (pro připojení k navigačnímu bodu) a proběhne automatické odpojení.

V případě náhodného odpojení (např. při ztrátě signálu) bude uživatel o této skutečnosti informován a vizuálně i funkčně se zmrazí části rozhraní pro uživatelský vstup, přičemž budou na pozadí probíhat pokusy o obnovení spojení. Historie dialogu bude v průběhu komunikace perzistentně ukládána na úložiště zařízení a bude možné se k ní kdykoliv vrátit. Při každém připojení proběhne prohledání interní databáze dialogů pro daný navigační bod a v případě shody poslední příchozí zprávy bude odpovídající dialog obnoven, jinak bude vytvořen nový. Schéma části databáze pro ukládání historie konverzací je na obrázku 5.4.



Obrázek 5.4: ER diagram části databáze pro ukládání historie konverzací

Druhou obrazovkou uživatelského režimu bude obrazovka s historií proběhlých dialogů zobrazených v podobě seznamu (na obrázku 5.5 vpravo), kde každý záznam bude iden-

[8] https://developer.apple.com/develop/

tifikován názvem navigačního bodu, datem a časem posledního připojení a indikátorem úspěšného zakončení. Po klepnutí na záznam bude zobrazena detailní historie dialogu ve stejné podobě jako v průběhu komunikace s možností procházení jednotlivých zpráv a odpovědí, ale bez možnosti interakce. V historii bude možné vyhledávat podle názvů navigačních bodů a filtrovat na základě data posledního připojení nebo úspěšnosti zakončení.

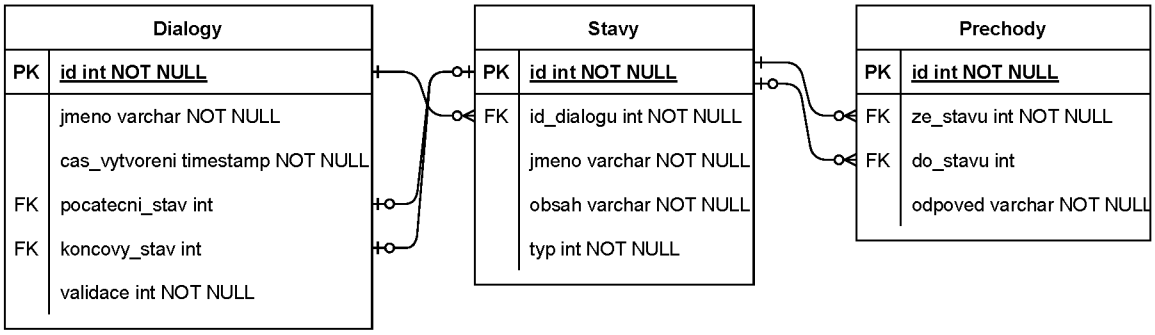
Obrázek 5.5: Návrh uživatelského rozhraní obrazovek pro interaktivní dialog s navigačním bodem (vlevo) a pro historii dialogů (vpravo)

Režim pro majitele

Režim pro majitele bude mít také dvě obrazovky. Hlavní obrazovka před připojením k navigačnímu bodu bude mít stejnou podobu jako v uživatelském režimu. Po připojení bude majitel vyzván k zadání hesla a v případě úspěšné autorizace se uloží pohled s dvěma pa-

nely. Prvním panel představuje konfiguraci navigačního bodu (jeho návrh je na obrázku 5.7 vlevo) a bude obsahovat stav baterie, formulář pro změnu parametrů jako název, interval pro zapomenutí uživatele, síla vysílání a přístupové heslo. Také zde budou tlačítka pro návrat do továrního nastavení a nahrání nového dialogu, po jehož stisknutí bude prezentován formulář pro volbu validního dialogu vytvořeného v aplikaci. Druhý panel bude sloužit ke zobrazení statistik o využívání navigačního bodu.

Druhá obrazovka režimu pro majitele bude sloužit ke tvorbě a úpravám dialogů. Bude zde seznam uložených dialogů, tlačítko pro vytvoření nového dialogu a tlačítko pro import dialogu ze souboru ve formátu JSON. Každý dialog bude mít upravitelný název a bude ho možné smazat, duplikovat nebo exportovat jako JSON. Po klepnutí na záznam nebo stisknutí tlačítka pro vytvoření nového dialogu bude zobrazen editor dialogu. Schéma části interní databáze pro editor je na obrázku 5.6.



Obrázek 5.6: ER diagram části databáze pro editor dialogu

Editor dialogu bude tvořen seznamem možných stavů, kde každý stav bude určen nastavitelným unikátním identifikátorem. Po klepnutí na stav nebo stisknutí tlačítka pro vytvoření nového bude zobrazen formulář pro jeho úpravu (na obrázku 5.7 vpravo), který bude obsahovat výběr typu (zpráva, otevřená otázka, uzavřená otázka), přepínač pro označení stavu za počáteční a pole pro text odesílaný uživateli, jenž bude vynucovat korektní formát pro zajištění funkčnosti komunikačního protokolu. Součástí formuláře bude také pole pro definici odpovědí a následujících stavů (určených jejich identifikátory zadanými ručně nebo vybranými ze seznamu uložených), jehož obsah bude záviset na typu stavu. Zprávy zde půjde označit jako koncové bez následujícího stavu, nebo jim půjde nastavit jeden následující stav. Otázkám zde bude možné nastavit seznam odpovědí a odpovídajících následujících stavů o libovolné délce.

Před nahráním dialogu do navigačního bodu bude vyžadována jeho validace. Ve výchozím stavu a po provedení jakýchkoliv změn bude dialog označen jako nezkontrolovaný a uživatel bude o této skutečnosti informován šedým indikátorem v seznamu dialogů a při zobrazení detailu dialogu. Po stisknutí indikátoru proběhne validace – zda jsou stavy korektně propojeny (všechny identifikátory následujících stavů existují), je definován právě jeden počáteční i koncový stav, který je dosažitelný ze všech ostatních stavů, a zda jsou všechny texty zpráv a odpovědí vynuceného formátu a pod limitem velikosti. Nabízí se i možnost automatické validace při každé změně, ale to by mohlo být pro uživatele rušivé (zejména při počátečním návrhu, kdy je dialog ještě neúplný), také by to mohlo vést k jisté míře nejasností, uživatel by byl od validace mírně odstíněn a nemusel by si vždy být plně vědom aktuálního stavu.

Všechny zjištěné nedostatky budou uživateli zobrazeny jako vyskakovací okno s jejich seznamem a popisem. V případě selhání kontroly bude uživatel informován o chybě, dialog bude označen jako nevalidní, indikátor se změní na červený a nebude jej možné nahrát do navigačního bodu. V případě zjištění méně závažných nedostatků napříč kterými bude dialog stále od začátku do konce průchozí (např. existence nedosažitelného stavu či chybějící text odpovědi) bude dialog stále možné nahrát, ale uživatel bude o této skutečnosti informován žlutým indikátorem s varováním.

Obrázek 5.7: Návrh uživatelského rozhraní obrazovek pro konfiguraci navigačního kodu (vlevo) a pro úpravu stavu dialogu (vpravo)

Kapitola 6

Implementace navrženého řešení

Předmětem následující kapitoly je popis implementace řešení na základě představeného návrhu. Část 6.1 přibližuje proces výroby prototypů a potíže, které se v průběhu vyskytly, část 6.2 popisuje implementaci obslužného firmware mikrokontroléru a část 6.3 se věnuje implementaci uživatelské mobilní aplikace.

6.1 Výroba prototypů

Desky plošných spojů byly vyrobeny na základě vytvořených podkladů firmou Gatema[1] v režimu Pool (se striktnějšími požadavky na formát dat, omezenými možnostmi úpravy parametrů výroby a horšími výrobními tolerancemi, ale s lepší cenou). Kvůli malé velikosti desek a relativně velké minimální účtované ploše bylo vyrobeno osm kusů od obou verzí návrhu. Desky byly následně s využitím vybavení laboratoře aplikovaných mikrokontrolérů osazeny součástkami objednanými u distributora DigiKey[2].

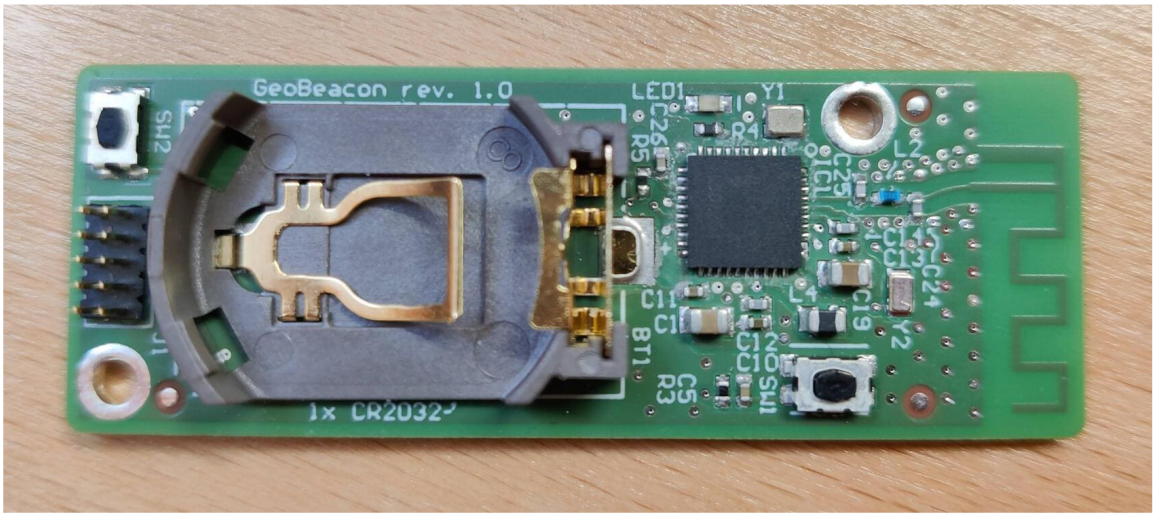
6.1.1 Prototyp s mikrokontrolérem QN9090

Po doručení desek a součástek byl osazen jeden kus prototypu s mikrokontrolérem QN9090 a vlastní anténou, jenž je na obrázku 6.1. Následné ověření funkčnosti odhalilo zásadní problém.

Pomocí ladící sondy PEMicro USB Multilink přes rozhraní SWD úspěšně proběhlo nahrání základního ukázkového programu obsaženého v SDK NXP a bylo zjištěno, že mikrokontrolér je včetně tlačítek, indikační LED i napájení z baterie funkční. Nahrání vlastního firmware či jakékoliv ukázky využívající BLE však ukázalo, že toto rozhraní nefunguje a prototyp nedokáže detekovat příchozí cizí signály, stejně tak žádné jiné zařízení nedetekuje jeho odchozí signál.

Na příčinu tohoto problému se ani po důkladném prozkoumání desky a úspěšné kontrole správného zapojení a funkčnosti komponent nepodařilo přijít. Pravděpodobnou příčinou je příliš velká odchylka impedance spoje antény od požadované hodnoty 50 Ω v důsledku změny tloušťky a materiálů DPS. Protože byl blízce následován referenční design včetně použití stejných komponent, bylo očekáváno, že drobné odchylky v návrhu povedou přinejhorším ke zhoršení kvality signálu. Tím ale byly výrazně podceněny nároky na správný návrh radiofrekvenční elektroniky, což je iterativní proces, který vyžaduje značnou míru znalostí, zkušeností a specializované vybavení.

[1] https://www.gatemapcb.cz/
[2] https://www.digikey.cz/



Obrázek 6.1: Fotografie vyrobeného prototypu navigačního bodu s mikrokontrolérem QN9090

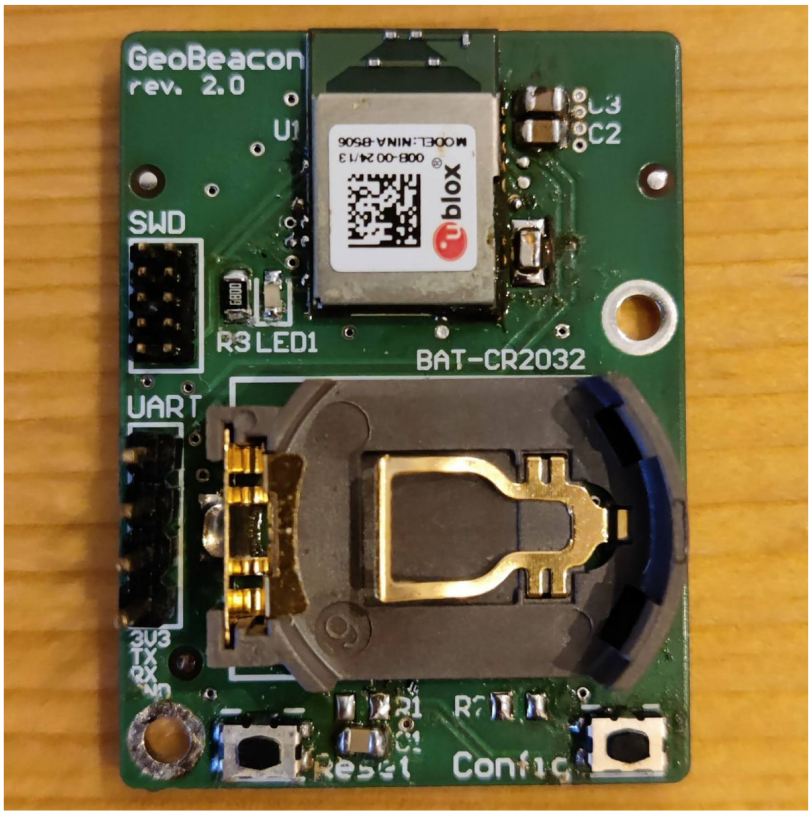
Z výše uvedených důvodů nebylo rozhodnuto o výrobě další iterace prototypu s vlastní anténou, návrh radiofrekvenční elektroniky není primární náplní této práce a úpravy bez úspěšné diagnostiky původního problému by byly bezpředmětné. Místo toho proběhl důkladný průzkum trhu a bylo zjištěno, že je dostupný modul NINA-B506 (popsaný v části 4.3.1), který naplní stanovené požadavky a jeho integrace je jednodušší. Ač byla dostupná pouze varianta s již zastaralým mikrokontrolérem, jeho použití bylo zvoleno jako nejvhodnější řešení a proběhl návrh nové revize prototypu s tímto modulem.

6.1.2 Prototyp s modulem NINA-B506

Po úspěšném návrhu a výrobě nové verze desky s modulem NINA-B506 byly osazeny další dva kusy prototypu, z nichž je jeden na obrázku 6.2. Kvůli nejasným chybám při pokusech o ladění přes SWD (týkajících se chybných pokusů o reset), kdy nebylo možné krokovat program, byly odpájeny rezistory R1 a R2, které napájejí spínače. Jejich použití není nutné, protože mikrokontrolér má na obou pinech interní. Bylo zjištěno, že tyto rezistory nejsou příčinou problému, přičinou byla chybná konfigurace interních kondenzátorů pro nízkofrekvenční krystal. Chybná kapacitance zabránila správnému fungování MCU a po jejím nastavení na nulu bylo možné firmware nahrát a ladit.

Mikrokontrolér K32W148 má oproti QN9090 odlišnou architekturu – rádiová jednotka představuje oddělené jádro s vlastní pamětí a firmwarem, který v jednotce není z výroby nahraný a kvůli bezpečnosti musí být podepsán a dodán vývojářem [22]. Tento firmware je v nepodepsané podobě dostupný v SDK NXP, ale MCU přijímá pouze podepsané verze obrazů ve formátu `SB3`, jež se dají vytvořit pomocí sady nástrojů SPSDK (*Secure Provisioning SDK*), knihovny pro Python 3 poskytující primárně kryptografickou funkcionalitu [25]. Proces tvorby a nahrání podepsaného obrazu pro rádiovou jednotku s využitím SPSDK byl následující:

1. Byl vygenerován nový asymetrický kryptografický pár pomocí křivky *secp384r1*.
2. Pomocí vytvořených klíčů byl vygenerován a podepsán kořenový x509 certifikát sloužící jako certifikační autorita.



Obrázek 6.2: Fotografie vyrobeného prototypu navigačního bodu s modulem NINA-B506

3. Byl vygenerován náhodný SB3 derivační klíč (SB3KDK) o velikosti 32 bajtů.
4. Na základě kořenového certifikátu a SB3KDK byl vytvořen jejich hash (RoTKTH, *Root of Trust Key Table Hash*).
5. Pomocí RoTKTH a SB3KDK byl vygenerován a podepsán obraz ve formátu SB3.
6. S využitím nástroje *blhost* (součást SPSDK, slouží ke komunikaci s mikrokontrolérem v režimu bootloader) byl prototyp přes převodník USB-UART připojen k počítači a proběhlo vypálení pojistek pro podepisování obrazů do paměti mikrokontroléru. K tomu bylo nutné nejprve příkazem zvýšit úroveň napájecího napětí hlavního jádra, poté byly zapsány klíče RoTKTH (pojistka `CUST_PROD_OEMFW_AUTH_PUK`) a SB3KDK (pojistka `CUST_PROD_OEMFW_AUTH_KDK`), které následně mikrokontrolér používá pro ověření validity a původu obrazů či pro autentifikaci vývojáře v případě vynucení zabezpečeného ladění. Vypálení pojistek je nevratnou operací.
7. Pomocí *blhost* byl úspěšně nahrán a ověřen podepsaný obraz SB3 do paměti rádiové jednotky.

Po úspěšném nahrání obrazu bylo možné nahrát vlastní firmware do hlavního jádra mikrokontroléru a ověřit funkčnost BLE komunikace, což bylo úspěšné. Při případné produkční výrobě by tento postup nebyl využit, protože není příliš efektivní. Použil by se postup, kdy jsou potřebné klíče a obrazy zkombinovány do jediného, který lze nahrát v jednom kroku pomocí SWD [23].

6.2 Implementace obslužného firmware mikrokontroléru

Obslužný firmware mikrokontroléru byl implementován v jazyce C s využitím MCUXpresso SDK a nástroje MCUXpresso IDE[3]. Jako základ posloužil ukázkový projekt *Wireless UART*[4], obsahující potřebný a „ověřený“ kód pro obsluhu BLE a implementaci této služby včetně služeb *Battery Service* a *Device Information Service*. Termín „ověřený“ je v tomto kontextu kvůli jeho zařazení v ukázkách myšlen jako „správně funkční“ a „paměťově bezpečný“, což je pro dlouhodobě běžící hůře dostupné zařízení kvůli riziku přetečení při nesprávném uvolňování paměti zásadní. Zmíněný projekt obsahuje kód pro implementaci těchto služeb i v režimu centrály a pro oboustrannou komunikaci využívá sériové linky UART s připojeným počítačem. Tyto součásti byly odstraněny a byla přidána funkcionalita nutná pro implementaci navigačního bodu, popsaná ve zbytku této části.

6.2.1 Interaktivní dialog

Implementace interaktivního dialogu se nachází v nově vytvořených souborech `game.c` a `game.h` ve složce `source`, kde jsou definice pro jeho datové struktury, funkce pro jeho inicializaci, reset do továrního nastavení (s jednou zprávou informující o této skutečnosti), rozhodnutí o následujícím stavu na základě přijaté zprávy, navrácení typu stavu a jeho textu a funkce pro zpracování příchozích dat nového dialogu a jeho korektní uložení.

V souboru `source/wireless_uart.c` byla funkcionalita pro čtení dat ze sériové linky s jejich přeposláním přes BLE a zpracování příchozích dat z BLE s jejich přeposláním na sériovou linku nahrazena zpracováním příchozích zpráv voláním odpovídajících funkcí z vlastní implementace a odesláním odpovědi na základě výsledku. Je taktéž ošetřen případný příjem zprávy ve více paketech, a to přidáním omezené vyrovnávací paměti pro každou připojenou protistranu, jejíž obsah je zpracován až po jejím naplnění či přijetí znaku pro konec řádku. Každému nově připojenému zařízení je přiřazen počáteční stav dialogu a s prodlevou (z důvodu ponechání času protistraně na přípravu před doručením první zprávy po připojení) dvou sekund odeslána odpovídající zpráva.

Aby se předešlo resetu dialogu při ztrátě napájení, musí být uložen perzistentně. K tomu je využit SDK modul NVM (*Non-volatile memory module*)[5], který zabezpečuje správu dat (ukládání, čtení) ve vyhrazeném bloku v paměti Flash. Ukazatel na datovou strukturu dialogu je pomocí makra `NVM_RegisterDataSet` registrován jako záznam v NVM tabulce, pro každou položku obsahující její unikátní identifikátor, datový typ a velikost včetně typu uložení (pouze ve Flash nebo se zrcadlením v paměti) a příznaku pro případné automatické obnovení položky při spuštění mikrokontroléru.

V tomto případě je dialog uložen pouze ve Flash (z důvodu jeho velikosti, v paměti RAM by mohl zabírat příliš mnoho místa) a je povolena jeho automatická obnova. Nevýhodou vypnutého zrcadlení je nutnost volání funkcí `NvMoveToRam` pro přenos dat do RAM před jejich modifikací a `NvSaveOnIdle` pro zpětné uložení do Flash. Jedná se o drahé operace, ale modifikace dialogu bude kromě prvotního nastavení navigačního bodu probíhat zřídka, tudíž je tento přístup přijatelný. Při inicializaci dialogu proběhne kontrola, zda byla z NVM načtena nějaká data (ukazatel má nenulovou hodnotu), a pokud ne, je inicializován na

[3] https://www.nxp.com/design/design-center/software/development-software/mcuxpresso-software-and-tools-/mcuxpresso-integrated-development-environment-ide:MCUXpresso-IDE

[4] https://mcuxpresso.nxp.com/mcuxsdk/latest/html/middleware/wireless/bluetooth/doc/Bluetooth%20Low%20Energy%20Demo%20Applications%20Users%20Guide/topics/wireless_uart.html

[5] https://mcuxpresso.nxp.com/mcuxsdk/latest/html/middleware/wireless/framework/services/NVM/README.html

výchozí hodnotu s následným uložením do Flash. Jméno navigačního bodu a přístupové heslo jsou uloženy a inicializovány stejným způsobem.

Protože je dialog uložen zmíněným způsobem, není možné, aby měl variabilní velikost – velikost každé datové struktury uložené pomocí NVM musí být známá při kompilaci. Proto byly stanoveny maximální počty a velikosti jednotlivých položek – maximální počet stavů je 16, maximální počet přechodů pro každý stav je 8, maximální velikost textu zprávy je 512 bajtů a maximální velikost odpovědi je 32 bajtů. Tyto hodnoty jsou použity jako fixní velikosti polí v datových strukturách dialogu, jeho velikost v paměti tedy odpovídá velikosti největšího možného dialogu.

Kvůli úspoře paměti, zjednodušení implementace a snížení nároků na výkon, potažmo energii, při vyhledávání v dialogu a porovnávání jeho stavů jsou pro jejich identifikaci použity unikátní identifikátory datového typu `uint8_t` počínaje nulou namísto řetězců použitých v uživatelské aplikaci. Pro reprezentaci neplatného či neexistujícího stavu je rezervován identifikátor `0xFF`.

6.2.2 Služba pro konfiguraci

Implementace vlastní služby pro konfiguraci byla (dle zvyklostí v MCUXpresso SDK) přidána do nově vytvořené složky `bluetooth/profiles/config`. Unikátní identifikátory služby a zahrnutých charakteristik (vypsané v příloze C) včetně počátečních (výchozích) hodnot a určení práv ke čtení/zápisu byly přidány do interní databáze GATT (soubory `gatt_db.c` a `gatt_uuid128.h` ve složce `source`). Kromě toho bylo nutné přidat všechny obsažené charakteristiky do seznamu sledovaných charakteristik u registrace obslužné funkce volané při pokusu o jejich zápis a tuto funkci upravit tak, aby při každém pokusu ověřila stav autorizace protistrany a případně volala příslušné funkce pro aktualizaci hodnot z vlastní implementace.

Jedinou výjimkou nevyžadující autorizaci před zápisem je charakteristika pro ověření hesla (uchovávaného pomocí NVM). Pokud je heslo při pokusu o zápis správné, dané protistraně je nastaven odpovídající příznak (uložený v poli struktur s informacemi o připojených protistranách indexovaném jejich unikátním identifikátorem generovaným automaticky počínaje nulou, mimo jiné obsahující i jejich aktuální stav dialogu), čímž jí je povolen zápis do ostatních charakteristik.

Z důvodu velké maximální velikosti dialogu bylo nutné místo běžného zápisu do charakteristik (velikostně omezeném velikostí přenosové jednotky BLE, řádově maximálně ve stovkách bajtů) zavést vlastní mechanizmus pro jeho přenos.

1. Protistrana indikuje úmysl přenést nový dialog zápisem velikosti přenášených dat (v nižších dvou bajtech) a počtu očekávaných paketů (ve vyšších dvou bajtech) do čtyřbajtové charakteristiky pro tuto indikaci. Pořadí bajtů všech přenášených dat je little endian.

2. Navigační bod alokuje paměť pro přenášená data a odpoví výsledkem této operace.

3. Protistrana v případě úspěchu postupně zapisuje jednotlivé pakety počínající jejich jednobajtovým číslem v sérii do charakteristiky pro přenos dat. Tato charakteristika nevyžaduje potvrzení zápisu, proto musí protistrana pakety kvůli jejich správnému zpracování vysílat s dostatečnými časovými intervaly (alespoň v rámci milisekund).

4. Navigační bod po přijetí každého paketu zkontroluje jeho číslo a data uloží do paměti.

5. Po obdržení posledního paketu proběhne deserializace dat a uložení pomocí NVM. V případě úspěchu je do charakteristiky pro indikaci uložena hodnota `0x0`. Při chybě v kterékoliv části procesu je do této charakteristiky uložena hodnota `0xFFFFFFFF`.

6. Protistrana s prodlevou od odeslání posledního paketu přečte hodnotu indikátoru a podle ní určí, zda byl přenos úspěšný a informuje uživatele o výsledku.

Kvůli strukturovanému charakteru dat dialogu a odlišným architekturám mikrokontroléru a mobilních zařízení bylo nutné zvolit formát pro serializaci dat, který by byl nezávislý na architektuře, byl by přenositelný mezi nimi a bylo by možné jej snadno deserializovat do odpovídajících datových struktur definovaných v jazyce C. Zvolený formát je v tabulce 6.1.

Deserializace dat probíhá kopírováním jednotlivých diskrétních přijatých hodnot do odpovídajících polí připravených datových struktur. Validita dat není (kromě kontroly celkové velikosti, správného pořadí a počtu přijatých paketů) ověřována. Validace dialogu probíhá v uživatelské aplikaci, tudíž by při přijetí dat mělo být zaručeno, že stanovené limity nebyly překročeny a že je dialog korektní. Pokud by nebyl dodržen formát pro serializaci, mohlo by dojít k přetečení paměti a k nepředvídatelnému chování, ale takovou kontrolu není možné implementovat jednoduchým způsobem pouze na základě přijatých dat. Jako mechanizmus pro komplexní validaci se nabízí např. použití kryptografických algoritmů, jako je HMAC (*Hash-based Message Authentication Code*) [16], což umožní ověřit integritu i autenticitu dat na základě hashování paketů s následným ověřením pomocí kryptografických klíčů vyměněných mezi aplikací a navigačním bodem. Vzhledem k tomu, že by takový přístup výrazně zvýšil složitost implementace, služba pro konfiguraci není určena pro použití širokou veřejností, validace dialogu včetně serializace do korektního formátu probíhá v mobilní aplikaci a kontrola integrity datových paketů probíhá již ve vrstvách ovladače BLE, nebyl takový přístup zvolen.

Název	**Datový typ**	**Velikost v bajtech**	**Popis**
`PocatecniId`	`uint8_t`	1	Id počátečního stavu
`KoncovyId`	`uint8_t`	1	Id koncového stavu
`PocetStavu`	`uint8_t`	1	Počet stavů dialogu
Opakovat následující blok `PocetStavu`-krát			
`Id`	`uint8_t`	1	Id stavu
`VelikostObsahu`	`uint16_t`	2	Velikost obsahu stavu
`Obsah`	`uint8_t[]`	`VelikostObsahu`	Obsah (text) stavu
`PrimyNaslednik`	`uint8_t`	1	Id přímého následníka
`UzavrenaOtazka`	`bool_t`	1	Indikace uzavřené otázky
`PocetPrechodu`	`uint8_t`	1	Počet přechodů ze stavu
Opakovat následující blok `PocetPrechodu`-krát			
`VelikostOdpovedi`	`uint8_t`	1	Velikost textu odpovědi
`Odpoved`	`uint8_t[]`	`VelikostOdpovedi`	Text odpovědi
`IdCile`	`uint8_t`	1	Id cíle přechodu

Tabulka 6.1: Popis formátu pro serializaci a přenos dialogu mezi aplikací a navigačním bodem

6.2.3 Služba pro statistiku

Implementace služby pro statistiku byla přidána do složky `bluetooth/profiles/stats`. Není to služba v pravém slova smyslu, nemá vlastní identifikátor a charakteristika, kterou poskytuje, je zařazena ve službě pro konfiguraci. Statisktiky (popsané v části 5.2.1) jsou ukládány jako datová struktura `statsData_t` pomocí NVM, v tomto případě se zrcadlením v RAM. Propis statistik do paměti flash kvůli jejich časté aktualizaci probíhá každý 16. pokus o zápis.

Služba si uchovává cyklickou vyrovnávací paměť s velikostí 32 záznamů, kam si ukládá adresy posledních připojených protistran, na základě kterých identifikuje uživatele, jejich aktuální stav spojení a čas prvního připojení. V případě, že je vyrovnávací paměť při připojení nového uživatele plná, je nejstarší záznam přepsán. Při dokončení dialogu je zjištěna doba trvání od prvního připojení a jsou aktualizovány relevantní statistiky. Do statistik se počítají pouze první úspěchy uživatelů, při opakovaném dokončení dialogu se statistiky neaktualizují.

Kvůli šetření energie je hodnota charakteristiky v databázi GATT aktualizována pouze při úspěšné autorizaci správce pomocí časovače s intervalem 1 minuta. Průběžná aktualizace je pro správný výpočet posledního času aktivity nutná, mikrokontrolér nemá žádný způsob, jak udržovat reálný čas (musel by být po každém resetu externě inicializován) a uběhlá doba musí být na základě rozdílu časových značek vypočítána před odesláním statistik. Moderní mobilní telefony často používají pro BLE komunikaci randomizované adresy, proto statistika o unikátních uživatelích nemusí být přesná.

6.3 Implementace mobilní aplikace

Uživatelská mobilní aplikace byla implementována jako nativní pro operační systém Android v programovacím jazyce Kotlin, zvoleném kvůli jeho moderní syntaxi oproti Javě a podpoře pro funkcionální programování. Minimální verze Android SDK, na kterou aplikace cílí, je 28 (Android 9), která pokryje přes 90 % zařízení na trhu[6], přičemž je stále dostatečně moderní pro poskytnutí kvalitního uživatelského zážitku a aktuální funkcionality při vývoji.

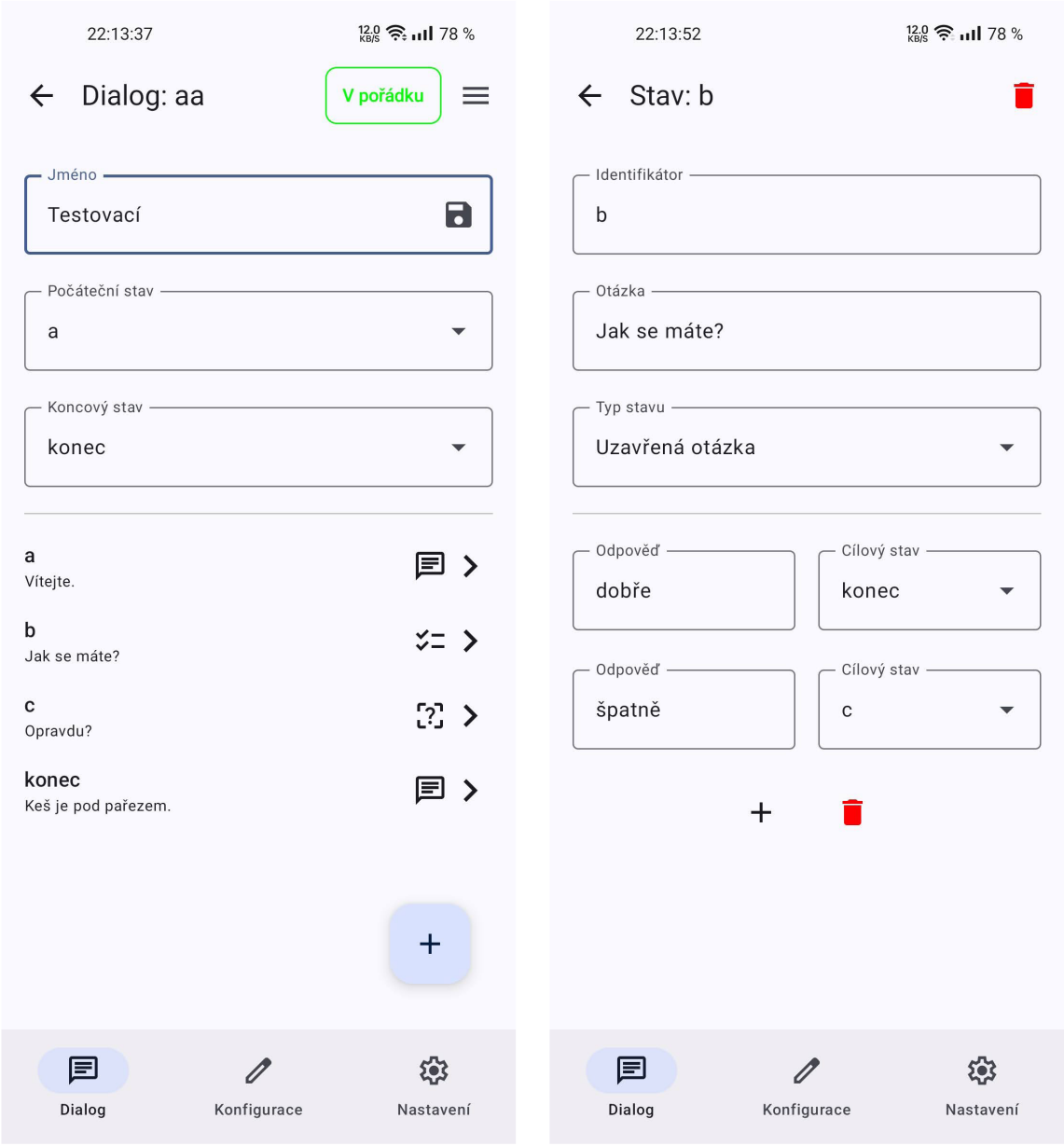
Aplikace využívá architektury MVVM (*Model-View-ViewModel*), kde *Model* je datová základna – interní databáze (viz část 6.3.2), nebo BLE protistrana (viz část 6.3.3). *View* je uživatelské rozhraní a *ViewModel* je mezivrstva zprostředkovávající prezentační logiku nad daty a propojující je s uživatelským rozhraním (viz část 6.3.1).

6.3.1 Uživatelské rozhraní

Uživatelské rozhraní bylo implementováno pomocí Jetpack Compose[7], což je moderní deklarativní způsob pro jeho tvorbu v Androidu, který umožňuje snadnou a rychlou implementaci a úpravy vzhledu aplikace včetně okamžitého náhledu na provedené změny. Taktéž poskytuje širokou sadu komponent a nástrojů pro návrh uživatelského rozhraní, zejména komponenty následující aktuální vizuální a funkční trendy obsažené v knihovně Material Design[8], jež byla při implementaci použita. Snímky obrazovek finální podoby editoru detailu dialogu a jeho stavu jsou na obrázku 6.3, na obrázku 6.4 jsou obrazovky pro interaktivní

[6] https://apilevels.com/
[7] https://developer.android.com/develop/ui/compose/documentation
[8] https://m3.material.io/

chat s uživatelem a jeho historii a obrázek 6.5 ukazuje obě záložky konfigurace navigačního bodu.

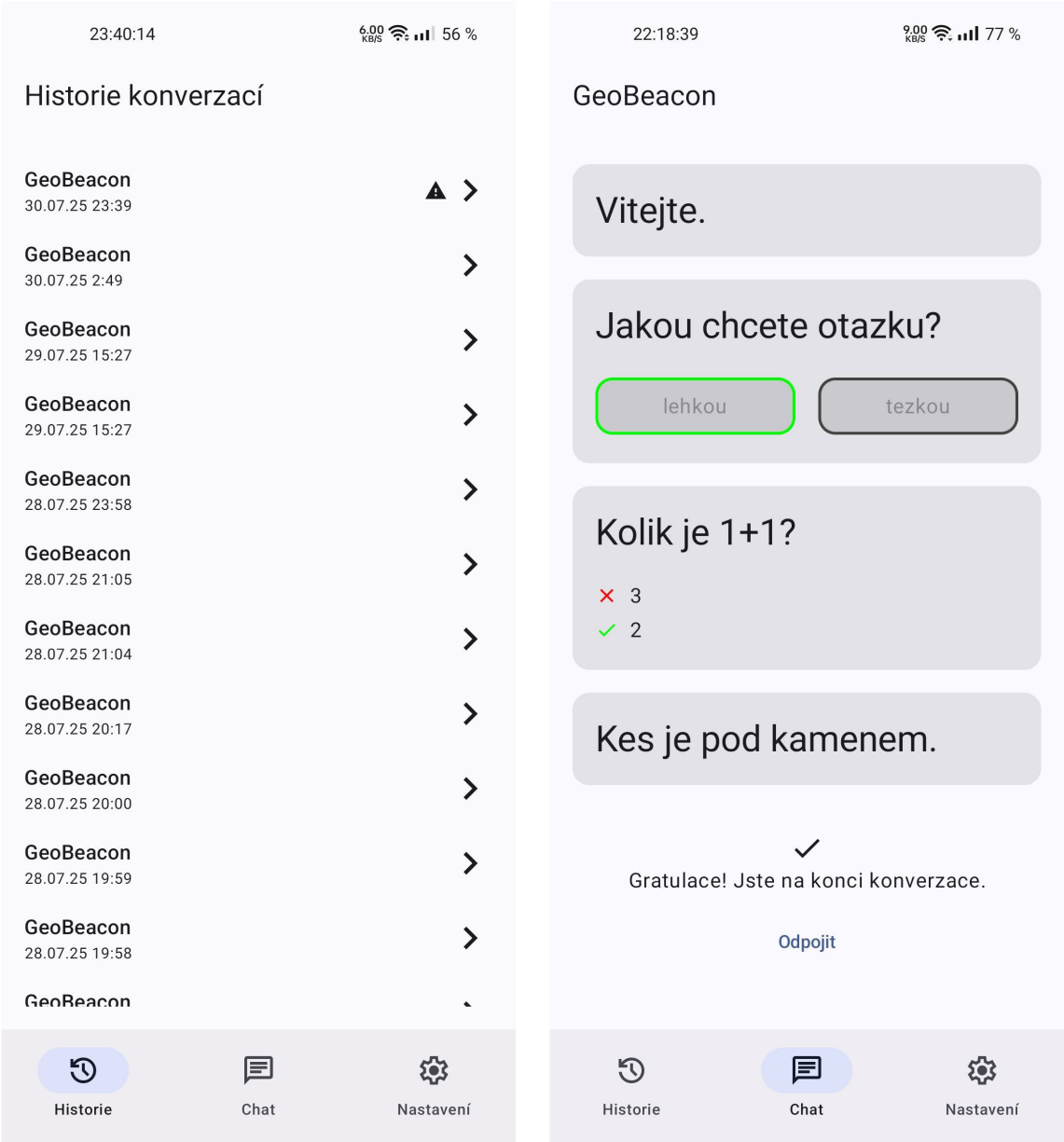


Obrázek 6.3: Snímek obrazovky finální podoby editoru detailu dialogu (vlevo) a jeho stavu (vpravo) v režimu pro majitele

Aplikace v novějších verzích Androidu (12+) následuje dynamické barevné schéma generované na základě pozadí plochy[9] (v nepodporovaných verzích je použito výchozí barevné schéma Material Design) a v nastavení je možné přestat respektovat systémové nastavení a přepínat mezi světlým a tmavým režimem. Pro veškerý text využívá *String Resources*[10],

[9] https://m3.material.io/styles/color/dynamic/user-generated-source
[10] https://developer.android.com/guide/topics/resources/string-resource

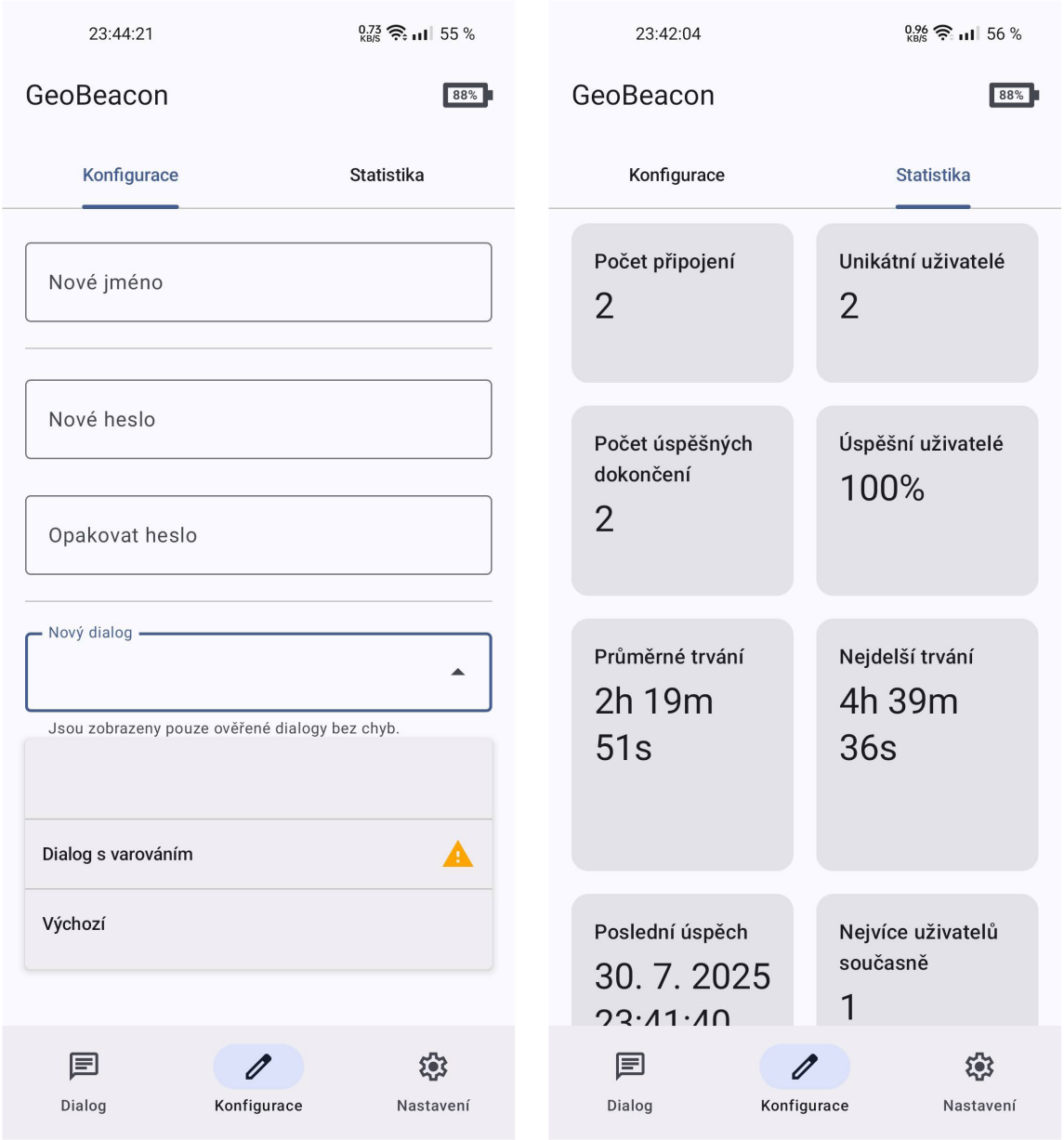
které umožňují snadnou lokalizaci řetězců, jenž byla provedena v češtině a angličtině. Jazyk je zvolen automaticky podle systémového nastavení.



Obrázek 6.4: Snímek finální podoby obrazovky s historií dialogu (vlevo) a interaktivní komunikace v uživatelském režimu (vpravo)

Uživatelské rozhraní využívá ke zobrazení aktuálních hodnot mechanizmu *Flow*[11], respektive *StateFlow* a *SharedFlow*, jenž jsou jednotlivým obrazovkám dostupné jako veřejné atributy ve třídách *ViewModel* jim příslušícím a uložené jako stav (*State*), při jehož změně dojde k rekompozici komponenty, která jej zobrazuje. Tímto způsobem je zajištěna reaktivita uživatelského rozhraní a jeho okamžitá a úsporná aktualizace při každé změně.

[11] https://developer.android.com/kotlin/flow



Obrázek 6.5: Snímek obrazovky finální podoby pohledu na konfiguraci navigačního bodu, záložka s konfiguračním formulářem (vlevo) a záložka s pohledem na statistiku (vpravo)

Jednotlivé obrazovky jsou zobrazeny pomocí komponenty `NavHost`, která zajišťuje přepínání mezi nimi pomocí spodní lišty s ikonami, jež je zobrazena na každé obrazovce. Její obsah závisí na aktuálně zvoleném režimu aplikace, pročež jsou definovány dvě sady obrazovek včetně jejich ikon, názvů a záznamů pro `NavHostController`, jehož metody, volané při klepnutí na ikonu v navigační liště nebo použití systémového tlačítka či gesta „zpět“, zajišťují samotnou navigaci.

`NavHostController` umožňuje i pokročilou správu historie navigace a předávání dat mezi obrazovkami, ale vzhledem k jednoduchosti navigačního schématu aplikace tyto funkce nebyly využity. Nabízelo by se to v případě obrazovky pro editor dialogů, kde je nutné pře-

cházet mezi pohledy na seznam dialogů, jejich úpravu a úpravu jednotlivých stavů, ale zaneslo by to zbytečnou složitost do jinak jednoduchého navigačního schématu a komplikovalo implementaci samotného editoru. Místo toho je pro zmíněné přechody použita komponenta `AnimatedContent`, která zajišťuje změnu zobrazeného obsahu na základě změny hodnoty proměnné (vybraného dialogu a jeho stavu, nulová hodnota, když není vybrán žádný) dle definované animace (bylo zvoleno horizontální přesunutí starého obsahu mimo obrazovku a přisunutí nového z druhé strany *slideInHorizontally*). Podpora pro návrat zpět gestem nebo systémovým tlačítkem funguje na základě detekce jeho použití (komponentou `BackHandler`) a vynulování proměnné pro výběr korespondující aktuálnímu pohledu.

6.3.2 Databáze

Databáze byla implementována pomocí knihovny Room[12], která poskytuje abstrakci nad SQLite databází uloženou v interním úložišti zařízení. Vývojáře odstiňuje od její správy a poskytuje snadno použitelné, ale výkonné rozhraní pro konfiguraci její struktury a práci s daty.

Struktura databáze je definovaná pomocí datových tříd pro každou tabulku označených anotací `@Entity` s názvy a specifikací jejich relací. Sloupce tabulek jsou definovány jako veřejné atributy těchto tříd s použitím anotací `@ColumnInfo` pro jejich názvy a další vlastnosti. Datové typy atributů jsou automaticky převáděny na odpovídající datové typy v SQLite databázi.

Přístup k datům zajišťují třídy *Data Access Object* (DAO), jenž definují metody pro manipulaci s daty a dotazování na ně. Tyto metody mají datový typ dle entit, na kterých mají pracovat, a jsou označeny anotacemi `@Insert`, `@Update`, `@Delete` a `@Query` označující příslušné operace. Díky tomu umožňují implementaci databázových operací s minimálním použitím SQL příkazů, které jsou nutné pouze v případě dotazů, ale zjednodušené využitím pomocných datových tříd, ve kterých jsou anotacemi vloženy entity, čímž je zajištěno automatické skládání tabulek a jejich sloupců v případě složitějších dotazů napříč více propojenými tabulkami. Také je využita možnost vracet data obalené v objektu Flow, který pro daný dotaz obsahuje vždy aktuální hodnoty a lze jej pozorovat na změny.

Operace poskytované DAO se následně používají v repozitářích (*Repository*), třídách, které odstiňují zbytek aplikace od konkrétní implementace databáze a její struktury převodem mezi datovými třídami entit a datovými třídami používanými ve zbytku aplikace. Metody repozitářů jsou následně volány z příslušných tříd *ViewModel*, jež zajišťují jejich volání na pozadí (operace s databází jsou blokující a nejdou vykonávat v hlavním vlákně) a předávají výsledky uživatelskému rozhraní.

Databáze obsahuje kromě tabulek pro ukládání historie komunikace a dat z editoru dialogů popsaných v části 5.2.3 i tabulku pro uložení uživatelského nastavení s jediným záznamem, jehož existence je zajištěna vložením výchozích hodnot během inicializace aplikace v případě jeho absence.

6.3.3 Správa Bluetooth Low Energy spojení

Pro správu BLE spojení byla vytvořena třída `BluetoothConnectionManager`, která odstiňuje zbytek aplikace od operací s Android Bluetooth API. Po ověření a případném vyžádání nutných oprávnění (které jsou odlišné pro různé verze systému Android) od uživatele je inicializována při spuštění aplikace a předána obrazovkám pro „chat“ a editor dialogů

[12] https://developer.android.com/training/data-storage/room

k následnému použití v jejich třídách ViewModel, inicializovaných kvůli jejich korektnímu vlastnictví až v kontextu obrazovek.

Tato třída zajišťuje inicializaci Bluetooth adaptéru, skenování dostupných zařízení, připojování k zařízením s udržením spojení, pokusy o znovupřipojení v případě jeho ztráty a odesílání i příjem dat včetně jejich zpřístupnění třídám ViewModel. Udržuje seznam identifikátorů používaných BLE služeb a charakteristik, na základě kterých filtruje nalezená zařízení (v případě objevení služby *Wireless UART* zastaví skenování a provede pokus o připojení), odesílá data a identifikuje přijatá data. Také spravuje vlastní GATT server se službou *Wireless UART*, který využívá k příjmu zpráv z navigačního bodu.

Bluetooth API je asynchronní a odpovědi od protistrany jsou zpracovávány pomocí obslužných funkcí, které jsou volány při událostech, jako je nalezení zařízení, objevení dostupných služeb a charakteristik nebo jejich čtení a potvrzení zápisu do nich. Z toho důvodu musel být pro přenos jednotlivých položek konfigurace implementován mechanizmus pro pozastavení těchto metod a čekání na potvrzení zápisu od protistrany nebo odpověď na pokus o čtení indikace úspěšnosti přenosu dialogu s předáním výsledku původní metodě. Byla použita `suspendCoroutine`, korutina, která uloží objekt `Continuation` do atributu třídy `BluetoothConnectionManager`, po dosažení jejího konce pozastaví své vykonávání a čeká na jeho obnovení pomocí volání metody uloženého objektu `resume` s výsledkem operace z obslužné funkce, čímž se zajistí jeho vrácení původní metodě a její ukončení. Kvůli zabránění situace, kdy by došlo k přepsání objektu `Continuation` před obnovením korutiny, je použit mechanizmus `Mutex` – vzájemné vyloučení s čekáním na jeho uvolnění, jímž je korutina obalena.

6.3.4 Dialog v režimu pro majitele

Dialog je reprezentován datovou třídou `DialogData`, obsahující seznam objektů `StateData` reprezentujících jeho stavy, které obsahují seznam objektů `TransitionData` reprezentujících přechody mezi stavy. Všechny tyto datové třídy implementují metody pro jejich validaci a serializaci do formátu pro přenos (specifikovaném v části 6.2.2).

Serializace dialogu probíhá s využitím třídy `ByteBuffer` obsažené v knihovnách Kotlinu, která po alokaci paměti pro přenášená data, jejichž celková velikost je vypočtena na základě velikosti jednotlivých položek dialogu předem, poskytuje metody pro přidání bajtů za poslední položku. Taktéž podporuje nastavení bajtového pořádku pro zápis datových typů větších než jeden bajt. Jeho metoda pro přidání jednoho bajtu `put` nepodporuje datový typ `UByte` (`uint8_t` v C), proto musel být kvůli zabránění možnému přetečení pro většinu položek zaveden mezikrok, kdy je jejich hodnota nejdříve převedena na `UByte` a poté na `Byte`, což zachová její bitovou reprezentaci, i když by hodnota bajtu se znaménkem byla po přečtení chybná. Unikátní identifikátory stavů jsou během serializace převedeny na sérii celých čísel počínaje nulou.

Validace dialogu probíhá následovně:

1. Je inicializován prázdný seznam, kam budou přidávány zjištěné problémy jako datové třídy, obsahující číslo řetězce je popisující, typ (varování/chyba) a příp. řetězec identifikující konkrétní stav nebo přechod, který bude v uživatelském rozhraní vložen do řetězce s popisem.

2. Proběhne kontrola, zda dialog není prázdný a má definován počáteční a koncový stav. Pokud ne, jedná se o chybu a validace nepokračuje dál.

3. Pro každý stav proběhnou kontroly, jeho obsah není prázdný (varování) a nemá nadlimitní velikost (chyba), pokud se jedná o koncový stav, zda jde o typ „zpráva“ (chyba), pokud není, zda mají všechny přechody z něj definovány cílové stavy (chyba) a zda mají definovány odpovědi (varování). Pokud jedna z kontrol skončí chybou, validace nepokračuje dál.

4. S využitím knihovny JGraphT[13] je vytvořen orientovaný graf, jehož vrcholy jsou stavy dialogu a hrany přechody mezi nimi.

5. Prohledáváním do šířky z počátečního stavu jsou zjištěny všechny dosažitelné stavy a všechny nedosažitelné stavy, které nejsou obsaženy v dosažitelných. Pokud koncový stav není dosažitelný z počátečního, jedná se o chybu a validace nepokračuje dál.

6. Pokud dialog obsahuje nedosažitelné stavy, je přidáno varování.

7. Směr hran orientovaného grafu je otočen a prohledáváním do šířky z koncového stavu jsou zjištěny všechny stavy, ze kterých je koncový stav dosažitelný. Pokud je zde některý ze stavů dosažitelných z počátečního obsažen, jedná se o chybu (po přechodu do takového stavu není možné průchod dialogem dokončit).

8. Seznam varování a chyb je vrácen jako výsledek validace, vzhledem k chybám nebo varováním proběhne aktualizace dialogu v databází a uživateli je zobrazen seznam zjištěných problémů ve vyskakovacím okně.

[13] https://jgrapht.org/

Kapitola 7

Ověření řešení vůči stanoveným požadavkům

V této kapitole je provedeno ověření navrženého řešení vůči požadavkům stanoveným v kapitole 4. Následuje seznam s požadavky, jejichž splnění lze ověřit triviálně a nevyžaduje delší popis či definici scénářů.

- **Podpora pro Android** – ověřeno, aplikace byla úspěšně nainstalována, spuštěna a použita na zařízeních s Androidem 9, 11 a 12, které byly využity při testování.
- **Interaktivita** – ověřeno, navržený formát dialogu byl úspěšně implementován jak v uživatelské aplikaci, tak v obslužném firmwaru pro mikrokontrolér, je dostatečně flexibilní pro podporu širokého spektra scénářů při hledání keší a dostatečně se odlišuje od stávajících řešení, čímž zvyšuje atraktivitu keše pro lovce.
- **Volitelnost uživatelské aplikace** – ověřeno, díky textovému formátu komunikace lze navigační bod použít kromě jeho konfigurace bez omezení i s BLE terminály s podporou *Wireless UART* nebo *Nordic UART*, např. s aplikací NXP IoT Toolbox.

Ve zbytku kapitoly je provedeno ověření požadavků, které vyžadují definici scénářů k ověření, podrobnější popis a testování. Každá část je věnována jednomu požadavku, kde odstavce psané kurzívou jsou scénáře pro jeho ověření, následované popisem průběhu a výsledků testování.

Podpora více uživatelů připojených současně

Navigační bod je schopen udržet spojení a komunikovat současně minimálně se třemi uživateli.

Ověřeno na základě testování s až (z důvodu jejich vlastnictví autorem či jeho blízkými a snadné dostupnosti tohoto počtu) čtyřmi zařízeními se systémem Android připojenými k navigačnímu bodu a komunikujícími současně alespoň v míře, v jaké by se to očekávalo od čtyř různých lidí využívající navigační bod zamýšleným způsobem. Více připojených uživatelů se v běžném provozu neočekává. Teoretický maximální počet protistran je 24, což je limit pro mikrokontrolér K32W148, ale je z důvodu šetření paměti implementačně omezen na 8.

Odolnost vůči povětrnostním podmínkám

Navigační bod je odolný proti mechanickému poškození, prachu a vlhkosti.

Částečně ověřeno. Z důvodu nefunkčního prototypu nebylo vyrobeno pouzdro, které by jej chránilo vůči stanoveným rizikům, což ale vzhledem k očekávanému umístění zařízení ve voděodolné a pevné schránce keše není naprosto nutné.

Navigační bod je schopen provozu v povětrnostních podmínkách ČR.

Ověřeno, zařízení je dostatečně tepelně odolné pro umístění do venkovního prostředí, maximální přípustný teplotní rozsah pro provoz všech použitých komponent je alespoň -20 až 60 °C, což je oboustranně omezeno hodnotami pro běžné baterie CR2032[1] a je dostatečné pro použití v povětrnostních podmínkách ČR.

Programovatelnost

Navigační bod je možné konfigurovat pomocí uživatelské aplikace změnou jeho jména, přístupového hesla a obsaženého dialogu.

Ověřeno, proběhla úspěšná implementace mechanizmu pro konfiguraci jak v uživatelské aplikaci, tak v obslužném firmwaru pro mikrokontrolér a jeho funkčnost byla ověřena na základě testování postupným nahráváním položek konfigurace v různých formátech (povolených i nepovolených a s méně běžnými speciálními znaky) a v celé škále povolených velikostí s následným ověřením jejich správnosti na základě zobrazení v uživatelské aplikaci, příp. průchodu dialogem.

Bezpečnost

Potenciální útočník nemá možnost provádět změny v konfiguraci navigačního bodu bez znalosti hesla, fyzického přístupu a bez přítomnosti správce s platným heslem.

Ověřeno, proběhla úspěšná implementace mechanizmu pro autorizaci heslem a bez jeho zadání není možné provádět změny v konfiguraci, také byla provedena dostatečná opatření proti útokům hrubou silou a byl implementován primitivní mechanizmus autentizace, vyžadující fyzický přístup k zařízení pro autorizaci.

Potenciální útočník nemá možnost provádět změny v konfiguraci navigačního bodu bez znalosti hesla za přítomnosti správce, který provádí konfiguraci.

Nebylo ověřeno, není použito šifrování bezdrátové komunikace, což navigační bod činí zranitelným vůči odposlechu a útokům typu MITM při konfiguraci. Z důvodu charakteru zařízení a jeho očekávaného umístění se ale pravděpodobnost takového útoku předpokládá jako velmi nízká. Přenášené informace nejsou citlivé a šifrování bylo vyhodnoceno jako zbytečné.

Potenciální útočník nemá možnost provádět změny v konfiguraci navigačního bodu bez znalosti přístupového hesla, ale s fyzickým přístupem.

Částečně ověřeno, heslo je uloženo bez šifrování v paměti Flash mikrokontroléru, což jej dělá snadno čitelným s připojením ladící sondy, jejíž vlastnictví útočníkem je ale nepravděpodobné a takový útok by vyžadoval konkrétní znalosti o zařízení a jeho architektuře. Díky možnostem správy životního cyklu mikrokontroléru je ale možné vypálením pojistky přejít

[1] https://www.duracell.com/wp-content/uploads/2021/06/CR2032CH_245mAh-CS.pdf

do stádia *OEM Closed* a zamezit přístupu k ladění bez ověření na základě vypálených klíčů vývojáře, což útočníkovi znemožní číst paměť [26]. Poté by bylo možné heslo získat pouze pomocí mikroarchitekturálních útoků, vzhledem k charakteru zařízení se ale takové útoky nepředpokládají.

Také je možné se znalostmi o navigačním bodu a fyzickým přístupem jej resetovat do továrního nastavení, ale v případě výroby pro použití veřejností by výchozí heslo bylo pro každé zařízení unikátní a pouhý reset by útočníkovi neumožnil přístup.

Dlouhodobá funkčnost

Navigační bod je schopen provozu po dobu minimálně 3 měsíců nezávisle na způsobu napájení.

Z důvodu nedostatku času při dopracování práce nebylo možné plně ověřit. V průběhu implementace byl využíván vývojový kit KW45B41Z-EVK napájený přes USB. Nejdelší doba, po kterou byl vývojový kit nepřetržitě zapnutý při testování, byly dva týdny, po jejichž skončení nebyla funkčnost nijak omezena.

Pro zajištění co největší spolehlivosti byla implementace založena na ověřené ukázce obsažené v SDK, byl kladen důraz na bezchybný kód jeho důkladnou kontrolou a průběžným laděním (neměly by se projevit žádné pády firmware mikrokontroléru v důsledku chyb) a mimo dynamických alokací paměti spravovaných knihovními funkcemi pro BLE a FreeRTOS nebyla použita téměř žádná vlastní alokace paměti, jejíž úniky by mohly být pro spolehlivost zařízení fatální. V případech, kdy použita z nevyhnutelných důvodů byla (pro alokaci místa před přenosem dialogu a jediný bajt identifikující protistranu k jeho předání úkolu pro zpožděné odeslání první zprávy po připojení), byl kladen důraz na její brzké, garantované uvolnění a minimalizaci jejího objemu.

Navigační bod je při napájení z baterie CR2032 o kapacitě 220 mAh schopen provozu po dobu minimálně 3 měsíců.

Ověřeno teoretickým výpočtem na základě odhadnutých parametrů. Kvůli nedostatku času při dopracování práce nebylo možné změřit spotřebu energie prototypu v dlouhodobém provozu a ověřit jeho skutečnou výdrž. Měření proběhlo alespoň v krátkodobém pětidenním provozu, kdy byl prototyp s modulem NINA-B506 nepřetržitě zapnutý a připojený k mobilnímu telefonu. Počáteční napětí nové baterie bylo 3,05 V a po pěti dnech provozu kleslo na 3 V.

Minimální napětí pro provoz mikrokontroléru je 1,81 V [32] a nominální kapacita baterie je 220 mAh, což znamená, že při konstantní zátěži (běžně se jedná maximálně o desetiny miliampéru) po spotřebování tohoto množství energie napětí klesne na spodní limit baterie (pro CR2032 je to běžně 2 V). Kvůli možným poklesům napětí při zátěži tedy lze napětí 2 V považovat za minimální možné. Při pulzní zátěži, kterou navigační bod vykazuje, se ale kapacita baterií CR2032 oproti nominální hodnotě snižuje, například při pulzech o velikosti 10 mA lze očekávat snížení kapacity na 180 mAh [3].

Pro standardní baterie tedy v tomto případu užití bude uvažována nominální kapacita 180 mAh. Pokles napětí o 0,05 V za pět dní znamená (při předpokladu lineárního poklesu na začátku životnosti baterie) 5% pokles v použitelném rozsahu napětí, což odpovídá spotřebované energii 9 mAh za pět dní, tedy 1,8 mAh denně. Při předpokladu, že spotřeba energie bude v průběhu životnosti baterie konstantní, je očekávaná výdrž 100 dní, což je více než 3 měsíce.

Následuje teoretický výpočet výdrže na základě odhadnutých parametrů a měření provedených NXP. Výpočet předpokládá použití oznamovacího intervalu 2 s a intervalu pro udržení spojení 1000 ms. Síla vysílání je nastavena na 0 dBm a frekvence jádra je 48 MHz. Očekávaná denní průměrná doba udržení spojení s uživatelem je 1 h s celkovým počtem $N_{zprava} = 200$ přenesených zpráv denně s velikostí 100 B, což odpovídá asi čtyřem nálezům s relativně komplikovaným dialogem. Jedná se o velmi pesimistický odhad, který by měl být v reálném provozu výrazně nižší, ale pro výpočet je použit k zajištění co nejhoršího scénáře a kompenzaci možných chyb v odhadech a dalších nezahrnutých faktorů. Na základě statistik získaných z webové aplikace *Project-GC*[2] je celkový počet aktivních keší v ČR při psaní práce 76054 a přibližný denní počet celkových nálezů odhadnutý z grafu pro jednotlivé dny je 15000, což dělá přibližný průměrný denní počet nálezů na keš 0,2.

Následující hodnoty byly převzaty z aplikační poznámky AN13230 [24], která obsahuje měření spotřeby mikrokontroléru při BLE událostech. V periodách mezi událostmi je mikrokontrolér v režimu *Deep sleep* s udržením obsahu RAM a potřebným proudem 2,8 μA [32]. Spotřeba energie při jednom oznámení s velikostí oznamovacího paketu 31 B je 4,78 nAh a při jednom spojení 1,86 nAh. Energie potřebná pro přenos paketu s jednou zprávou byla stanovena na základě času pro odeslání oznamovacího paketu $t_{31B} = 0,3$ ms, velikostí těchto paketů, proudu potřebného pro odesílání dat $I_{tx} = 4,6$ mA a odhadovaného času $t_{act} = 2$ ms a proudu $I_{act} = 4,6$ mA při zpracování v aktivním režimu následovně:

$$t_{tx} = \frac{t_{31B} \cdot 100 \text{ B}}{31 \text{ B}} = \frac{0,3 \cdot 100}{31} \approx 1 \text{ ms},$$

$$E_{zprava} = I_{tx} \cdot t_{tx} + I_{act} \cdot (t_{act} + t_{tx}) = 4,6 \cdot \frac{0,001}{3600} + 4,6 \cdot \frac{0,002 + 0,001}{3600} \approx 5,11\ \mu\text{Ah} = 5110\ \text{nAh},$$

celkový počet jednotlivých událostí za den je

$$N_{oznameni} = \frac{60 * 60 * 24}{2} = 43200 \text{ a}$$

$$N_{spojeni} = \frac{60 * 60}{1} = 3600,$$

energie potřebná pro režim „power-down“ na den (kvůli zjednodušení jsou periody probuzení při událostech zanedbány) je

$$E_{power-down} = I_{power-down} \cdot t_{power-down} = 2,8 \cdot 24 = 67,2 \mu\text{Ah} = 67200 \text{ nAh}$$

a celková spotřeba energie za den je

$$E_{den} = N_{oznameni} \cdot E_{oznameni} + N_{spojeni} \cdot E_{spojeni} + N_{zprava} \cdot E_{zprava} + E_{power-down},$$

$$E_{den} = 43200 \cdot 4,78 + 3600 \cdot 1,86 + 200 \cdot 5110 + 67200 \approx 1,3 \text{ mAh}.$$

Teoretická maximální výdrž na baterii CR2032 o kapacitě 180 mAh je tedy přibližně

$$\frac{E_{bat}}{E_{den}} = \frac{180}{1,3} \approx \boxed{138 \text{ dní}},$$

což je více než požadované 3 měsíce. Je to ale optimističtější výsledek než odhad po krátkodobém měření reálného prototypu, takže lze očekávat, že reálná výdrž bude nižší.

[2] https://project-gc.com/

Uživatelská přívětivost

Uživatelé jsou schopni použít aplikaci bez předchozího školení a úspěšně projít dialogem.

Ověřeno na základě uživatelského testování (N = 5). Z důvodu nefunkčního prototypu jej nebylo možné provést v terénu, ale bylo provedeno v prostorném obývacím pokoji, kde byl navigační bod umístěn. Pro účely testování byl vytvořen dialog, který od účastníků vyžadoval postupné nalezení tří skrytých předmětů, na kterých bylo napsáno heslo k postupu dál. Dialog byl uzavřenou otázkou na oblíbenou místnost před pokyny k nalezení druhého předmětu rozvětven na dva možné průchody, které vyžadovaly nalezení předmětu v místnosti, jež byla vybrána jako odpověď. Koncovým stavem byly pokyny k nalezení odměny za účast.

Účastníkům byl nejprve položen dotaz na jejich technické znalosti a zkušenosti s geocachingem, přičemž měli na výběr z možností „žádné“, „základní“, „střední“ a „pokročilé“. Poté jim byl předán mobilní telefon s nainstalovanou aplikací, krátce představen její účel a následně byli vyzváni k jejímu použití. Průchod dialogem byl stopován a po nalezení finální odměny byli účastníci dotázáni na jejich celkový dojem z této zkušenosti, přičemž měli na výběr z možností „velmi špatná“, „špatná“, „průměrná“, „dobrá“ a „velmi dobrá“.

Výsledky testování jsou shrnuty v tabulce 7.1. Všichni účastníci byli schopni úspěšně dokončit dialog bez jakýchkoliv problémů nebo žádostí o nápovědu, což ukazuje na intuitivnost uživatelského rozhraní a průchodu dialogem. Žádný z účastníků se nezasekl na žádném z předmětů a všechny celkové časy průchodů byly v očekávaném rozmezí.

Účastník	Zkušenosti	Technické znalosti	Čas (min)	Celkové hodnocení
1	žádné	základní	10	dobrá
2	základní	střední	12	velmi dobrá
3	střední	pokročilé	8	velmi dobrá
4	žádné	pokročilé	9	dobrá
5	žádné	základní	15	průměrná

Tabulka 7.1: Výsledky uživatelského testování navigačního bodu s využitím aplikace

Uživatelé jsou schopni použít navigační bod s využitím BLE terminálu bez popisu jeho fungování či formátu komunikačního protokolu a úspěšně projít dialogem.

Ověřeno na základě uživatelského testování na nových účastnících (N = 3), které proběhlo stejným způsobem jako testování s aplikací pro navigační bod, ale místo ní byl použit terminál obsažený v NXP IoT Toolbox a jediná instruktáž byla k účelu navigačního bodu a korektnímu spuštění správného modulu zmíněné aplikace, jenž byla nainstalována na mobilním telefonu, který byl účastníkům při testování vypůjčen.

Výsledky testování jsou shrnuty v tabulce 7.2. Ukázaly se jako horší než při testování s aplikací, což je nejspíš způsobeno horší uživatelskou přívětivostí terminálu a jeho ovládání. Všichni účastníci byli ale stále schopni dokončit dialog v přiměřeném čase a bez žádostí o nápovědu. Zvýšení průměrného času na dokončení bylo způsobeno delší počáteční dobou k orientaci ve způsobu použití terminálu a v případě účastníka 2 také opakovanými pokusy o zadání celé odpovědi na uzavřenou otázku místo jejího čísla.

Noví majitelé navigačního bodu jsou schopni vytvořit vlastní dialog pouze na základě předchozí zkušenosti s jeho použitím.

Částečně ověřeno na základě uživatelského testování (N = 2). Z důvodu očekávané zkušenosti majitelů keší s geocachingem bylo testování provedeno na účastníkovi 3 z testování

Účastník	Zkušenosti	Technické znalosti	Čas (min)	Celkové hodnocení
1	žádné	pokročilé	9	dobrá
2	základní	střední	16	průměrná
3	střední	základní	13	průměrná

Tabulka 7.2: Výsledky uživatelského testování navigačního bodu s využitím terminálu

s aplikací a účastníkovi 3 z testování s terminálem (jenž byl nejdřív proveden uživatelskou částí aplikace), kteří byli po předchozím testování vyzváni k vytvoření vlastního dialogu obdobného charakteru.

Zadání bylo oběma účastníky splněno a vytvořili lineární dialog o několika stavech, ale vyžadovalo to několik dotazů na podrobnosti ohledně fungování editoru a jeho možností. Jeden z účastníků také nechápal, proč se jeho dialog nezobrazuje v seznamu na obrazovce pro konfiguraci a musel být upozorněn na nutnost validace před nahráním. Oba účastníci ale ohodnotili zkušenost pozitivně a ač nejsou majitelé keší, prohlásili, že by použití navigačního bodu při založení zvažovali. Výsledky ukázaly, že noví majitelé navigačního bodu budou k jeho obsluze potřebovat manuál, ale do jisté míry se budou schopni orientovat i bez něj.

Dostatečný dosah

Navigační bod je schopen komunikovat s telefonem uživatele minimálně v oblasti přesnosti GPS přijímačů, a to i v přírodním prostředí s překážkami.

Ověřeno na základě měření RSSI s telefonem OnePlus 8T. Jako pesimistický odhad přesnosti GPS přijímačů byla zvolena oblast o poloměru 10 m kolem navigačního bodu. Ten byl umístěn do plastové schránky o objemu 2 l napodobující keš. Dle datasheetu modulu je nejsilnější signál vysílán kolmo k anténě, proto bylo měření provedeno v této poloze. Síla vysílání byla nastavena na 0 dBm.

Proběhly dvě měření. První měření zjišťovalo dosah v otevřeném prostoru, kdy byl navigační bod umístěn na zahradě a telefon byl umístěn v různých vzdálenostech od něj. Výsledky měření síly signálu jsou shrnuty v tabulce 7.3. Měření ukázalo, že navigační bod je schopen spolehlivě komunikovat s telefonem uživatele až do vzdálenosti 40 m, ve větší vzdálenosti již začalo docházet k výpadkům spojení, přenosy se zpomalily a od 50 m již nebylo možné navázat spojení vůbec.

Vzdálenost (m)	Síla signálu (dBm)	Spojení
1	-56	Spolehlivé
10	-74	Spolehlivé
20	-85	Spolehlivé
25	-88	Spolehlivé
30	-92	Spolehlivé
35	-96	Spolehlivé
40	-98	Mírně nespolehlivé
45	-102	Nespolehlivé
50	-105	Žádné

Tabulka 7.3: Výsledky měření dosahu navigačního bodu v otevřeném prostoru

Druhé měření proběhlo ve středně hustém listnatém lese, kdy byl navigační bod umístěn na strom ve výšce 1 m od země. Lokace měření je na obrázku 7.1. Kvůli stíženým

podmínkám nebyly při měření zaznamenávány přesné vzdálenosti. Měření bylo provedeno pohybem v přibližných kruzích kolem navigačního bodu a sledováním síly signálu. Při pohybu v okruhu ve vzdálenosti 10 m od navigačního bodu bylo možné navázat spojení a komunikovat s telefonem bez problémů. RSSI se pohybovalo v rozmezí -75 až -90 dBm. Při pohybu v okruhu 20 m od navigačního bodu bylo možné navázat spojení a komunikovat s telefonem, ale síla signálu se snížila na -90 až -100 dBm, spojení bylo místy nespolehlivé a docházelo ke zpomalování přenosů. Při pohybu v okruhu 30 m od navigačního bodu již spojení vypadávalo úplně, místy nebylo možné navázat spojení vůbec a síla signálu byla -105 dBm a nižší.

Bylo možné zřetelně pozorovat, že síla signálu je ovlivněna překážkami v podobě stromů a jejich listoví, které snižují dosah a kvalitu spojení. Při přechodu do hustější vegetace se RSSI viditelně snižovalo. Stále se ale potvrdilo, že navigační bod je v takovém prostředí použitelný.

Obrázek 7.1: Měření dosahu navigačního bodu v lese

Kapitola 8

Závěr

Cílem této práce bylo navrhnout a implementovat bezdrátový navigační bod pro geocaching využívající technologie Bluetooth Low Energy, založený na vysoce konfigurovatelném a interaktivním dialogu s uživateli obnášejícím řešení hádanek či získávání informací z okolního prostředí. Cíl byl dosažen zhodnocením současného stavu, stanovením základních požadavků na takové zařízení, výběrem vhodného mikrokontroléru společnosti NXP a vytvořením návrhu desky plošných spojů zařízení, jeho obslužného firmwaru a doplňkové mobilní aplikace pro uživatele, která umožňuje interakci s navigačním bodem a jeho konfiguraci majitelem. Navržené řešení bylo následně implementováno a ověřeno definicí sady testovacích scénářů, provedením testování a zhodnocením dosažených výsledků s ohledem na stanovené požadavky.

Z důvodu komplikací spojených s návrhem radiofrekvenční části zařízení se první prototyp s mikrokontrolérem QN9090 nepodařilo zprovoznit. Druhý prototyp s modulem NINA-B506, který byl navržen a vyroben, však je plně funkční a měřením bylo ověřeno, že je pro účel geocachingu použitelný. Práce přináší inovativní a plně funkční řešení navigačního bodu, které je dostatečně flexibilní pro použití v širokém spektru scénářů. Vzhledem k tomu, že se jedná o první návrh zařízení s takovými vlastnostmi, jej lze považovat za úspěšný a přínosný pro komunitu kolem geocachingu.

Navržený prototyp s vlastní anténou je až na jeho radiofrekvenční část plně funkční a se správným vybavením pro ladění takové elektroniky, dostatečným rozpočtem a časem pro iterativní vývoj s důrazem na použité materiály a jejich vlastnosti by jeho úspěšné dokončení bylo možné s minimálními úpravami. Umožnilo by to velmi levnou výrobu, nižší cenu pro uživatel a potenciální rozšíření uživatelské základny. Také se nabízí implementace šifrování komunikace, což by zvýšilo bezpečnost zařízení a snížilo riziko odposlechu a útoků typu Man-in-the-Middle. Další pokračování vývoje by mohlo obnášet například i implementaci vizuálního rozhraní pro editor dialogu, které by správcům navigačních bodů výrazně usnadnilo tvorbu a úpravy dialogu přehlednou vizualizací jeho struktury. Pro rozšíření uživatelské základny by aplikace mohla být implementována i pro operační systém iOS.

Přestože byl návrh navigačního bodu motivován specifickými potřebami geocachingu, principy, na nichž je založen, mají potenciál využití i v širším spektru interaktivních outdoorových her a edukačních aplikací. Kombinace bezdrátové komunikace a interaktivních scénářů řízených mobilní aplikací otevírá nové možnosti pro vytváření zábavných, poučných i soutěžních zážitků ve veřejném prostoru. Práce tak může sloužit nejen jako základ pro technický vývoj konkrétního zařízení, ale i jako inspirace pro návrh inovativních zážitkových systémů využívajících moderní vestavěné technologie.

Literatura

[1] Bluetooth SIG. *Bluetooth* online. 2025. Dostupné z: https://www.bluetooth.com/. [cit. 2025-01-21].

[2] Bose, C. a Amir, J. Design of fiducials for accurate registration using machine vision. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 1. vyd. IEEE, 1990, sv. 12, č. 12, s. 1196–1200. ISSN 0162-8828.

[3] Burdett, A. Ultra-Low-Power Wireless Systems: Energy-Efficient Radios for the Internet of Things. *IEEE Solid-State Circuits Magazine*. 1. vyd., 2015, sv. 7, č. 2, s. 18–28. ISSN 1943-0582.

[4] Cameron, L. *The Geocaching Handbook: The Guide for Family-Friendly, High-Tech Treasure Hunting*. 2. vyd. Morris Book Publishing, 2011. ISBN 978-0-7627-6383-2.

[5] Cominelli, M.; Patras, P. a Gringoli, F. Dead on Arrival: An Empirical Study of The Bluetooth 5.1 Positioning System. In: Pefkianakis, Y. a Lin, K. C.-J., ed. *Proceedings of the 13th International Workshop on Wireless Network Testbeds, Experimental Evaluation & Characterization*. New York, NY, USA: Association for Computing Machinery, 2019, s. 13–20. WiNTECH '19. ISBN 9781450369312.

[6] Dudhane, N. a Pitambare, S. Location Based and Contextual Services Using Bluetooth Beacons: New Way to Enhance Customer Experience. *Lecture Notes on Information Theory*. 1. vyd. LNIT, Červen 2015, sv. 3, č. 1, s. 31–34. ISSN 2301-3788.

[7] Garmin Canada Inc. *ANT* online. 2025. Dostupné z: https://www.thisisant.com/. [cit. 2025-01-10].

[8] Geocaching Community. *Geocachers' Creed* online. 2005. Dostupné z: http://www.geocreed.info/. [cit. 2025-01-10].

[9] Groundspeak Inc. *Geocaching.com* online. 2000-2025. Dostupné z: https://geocaching.com/. [cit. 2025-01-10].

[10] Groundspeak Inc. *Geocaching.com Newsroom* online. 2000-2025. Dostupné z: https://newsroom.geocaching.com/. [cit. 2025-01-10].

[11] Groundspeak Inc. *Wherigo®* online. 2000-2025. Dostupné z: https://www.wherigo.com/. [cit. 2025-01-10].

[12] Gupta, N. *Inside Bluetooth Low Energy*. 2. vyd. Artech House, 2016. ISBN 978-1-63081-089-4.

[13] Insight SiP. *ISP5261 Data Sheet* online. 2023. Dostupné z: https://www.insightsip.com/fichiers_insightsip/pdf/ble/ISP5261/isp_wifi_DS5261.pdf. [cit. 2025-07-28].

[14] Iqbal, Z.; Luo, D.; Henry, P.; Kazemifar, S.; Rozario, T. et al. Accurate real time localization tracking in a clinical environment using Bluetooth Low Energy and deep learning. *PLOS ONE* online. 1. vyd. PLOS, 2018, sv. 13, č. 10. ISSN 1932-6203. Dostupné z: https://doi.org/10.1371/journal.pone.0205392. [cit. 2025-05-09].

[15] Kaulich, T.; Heine, T. a Kirsch, A. Indoor Localisation with Beacons for a User-Friendly Mobile Tour Guide. *KI - Künstliche Intelligenz*. 1. vyd. Springer, 2017, sv. 31, č. 3, s. 239–248. ISSN 0933-1875.

[16] Krawczyk, H.; Bellare, M. a Canetti, R. *HMAC: Keyed-Hashing for Message Authentication* online. RFC 2104. RFC Editor, únor 1997. Dostupné z: https://www.rfc-editor.org/info/rfc2104. [cit. 2025-05-11].

[17] Lin, Y.-W. a Lin, C.-Y. An Interactive Real-Time Locating System Based on Bluetooth Low-Energy Beacon Network. *Sensors*. 1. vyd. MDPI, 2018, sv. 18, č. 5. ISSN 1424-8220.

[18] Nikodem, M.; Trajnowicz, G.; Blasio, G. Salvatore de a Alexis Quesada Arencibia, F. Experimental Evaluation of Multicarrier Phase Difference Localization in Bluetooth Low Energy. *IEEE Sensors Journal*. 1. vyd. IEEE, 2025, sv. 25, č. 1, s. 1548–1560. ISSN 1530-437X.

[19] NXP B.V. *AN2731: Compact Planar Antennas for 2.4 GHz Communication* online. 2020. Dostupné z: https://docs.nxp.com/bundle/AN2731. [cit. 2025-07-28].

[20] NXP B.V. *Bluetooth®Low Energy Application Developer's Guide* online. 2020. Dostupné z: https://community.nxp.com/pwmxy87654/attachments/pwmxy87654/wireless-connectivity/11469/1/Bluetooth%20Low%20Energy%20Application%20Developer%20Guide.pdf. [cit. 2025-07-28].

[21] NXP B.V. *QN9090(T)/QN9030(T) Product data sheet* online. 2020. Dostupné z: https://www.nxp.com/docs/en/nxp/data-sheets/QN9090(T)QN9030(T).pdf. [cit. 2025-07-28].

[22] NXP B.V. *K32W1480 Reference Manual* online. 2022. Dostupné z: https://www.nxp.com/webapp/Download?colCode=K32W1480RM. [cit. 2025-07-28].

[23] NXP B.V. *AN14003: Programming the KW45 flash for Application and Radio firmware via Serial Wire Debug during mass production* online. 2024. Dostupné z: https://docs.nxp.com/bundle/AN14003/. [cit. 2025-07-28].

[24] NXP B.V. *AN13230: Kinetis KW45 and K32W1 Bluetooth LE Power Consumption Analysis* online. 2025. Dostupné z: https://docs.nxp.com/bundle/AN13230/. [cit. 2025-07-28].

[25] NXP B.V. *AN13883: Updating KW45 Radio Firmware via ISP using SPSDK* online. 2025. Dostupné z: https://www.nxp.com/webapp/Download?colCode=AN13883. [cit. 2025-07-28].

[26] NXP B.V. *AN13931: Managing Lifecycles on KW45 and K32W148* online. 2025. Dostupné z: https://www.nxp.com/webapp/Download?colCode=AN13931. [cit. 2025-07-28].

[27] O'Hara, K. Understanding geocaching practices and motivations. In: Burnett, M. et al., ed. *CHI '08: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York, NY, USA: Association for Computing Machinery, Duben 2008, s. 1177–1186. ISBN 978-1-60558-011-1.

[28] Pattnayak, T. a Thanikachalam, G. *AN91445 - Antenna Design and RF Layout Guidelines* online. Cypress Semiconductor Corporation, 2018. Dostupné z: https://www.cypress.com/go/AN91445. [cit. 2025-04-23].

[29] Sheikh, H. S.; Abbas, A.; Abbasi, S. F.; Rustam, H. a Qasim, G. Enhanced Position Estimation Based on Hybrid Bluetooth and Pedestrian Dead Reckoning using Sensor Fusion Algorithm in Indoor Navigation. In: IEEE. *2023 IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology (ICES&T)*. Bahawalpur, Pákistán: IEEE, Leden 2023. ISBN 978-1-6654-5561-9.

[30] Terracaching. *Terracaching* online. 2004-2025. Dostupné z: https://www.terracaching.us/. [cit. 2025-01-10].

[31] The OCNA Team. *OpenCaching North America* online. 2010. Dostupné z: https://www.opencaching.us/. [cit. 2025-01-10].

[32] u-blox. *NINA-B50 series Data sheet* online. 2024. Dostupné z: https://content.u-blox.com/sites/default/files/documents/NINA-B50_DataSheet_UBX-22021114.pdf. [cit. 2025-07-28].

[33] u-blox. *NINA-B50 series System integration manual* online. 2024. Dostupné z: https://content.u-blox.com/sites/default/files/documents/NINA-B50_SIM_UBX-22021116.pdf. [cit. 2025-07-28].

[34] Wang, H.; Sen, S.; Elgohary, A.; Farid, M.; Youssef, M. et al. No need to war-drive: unsupervised indoor localization. In: Davies, N., ed. *Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services*. New York, NY, USA: Association for Computing Machinery, 2012, s. 197–210. MobiSys '12. ISBN 9781450313018.

Příloha A

Schémata zapojení a seznamy použitých součástek

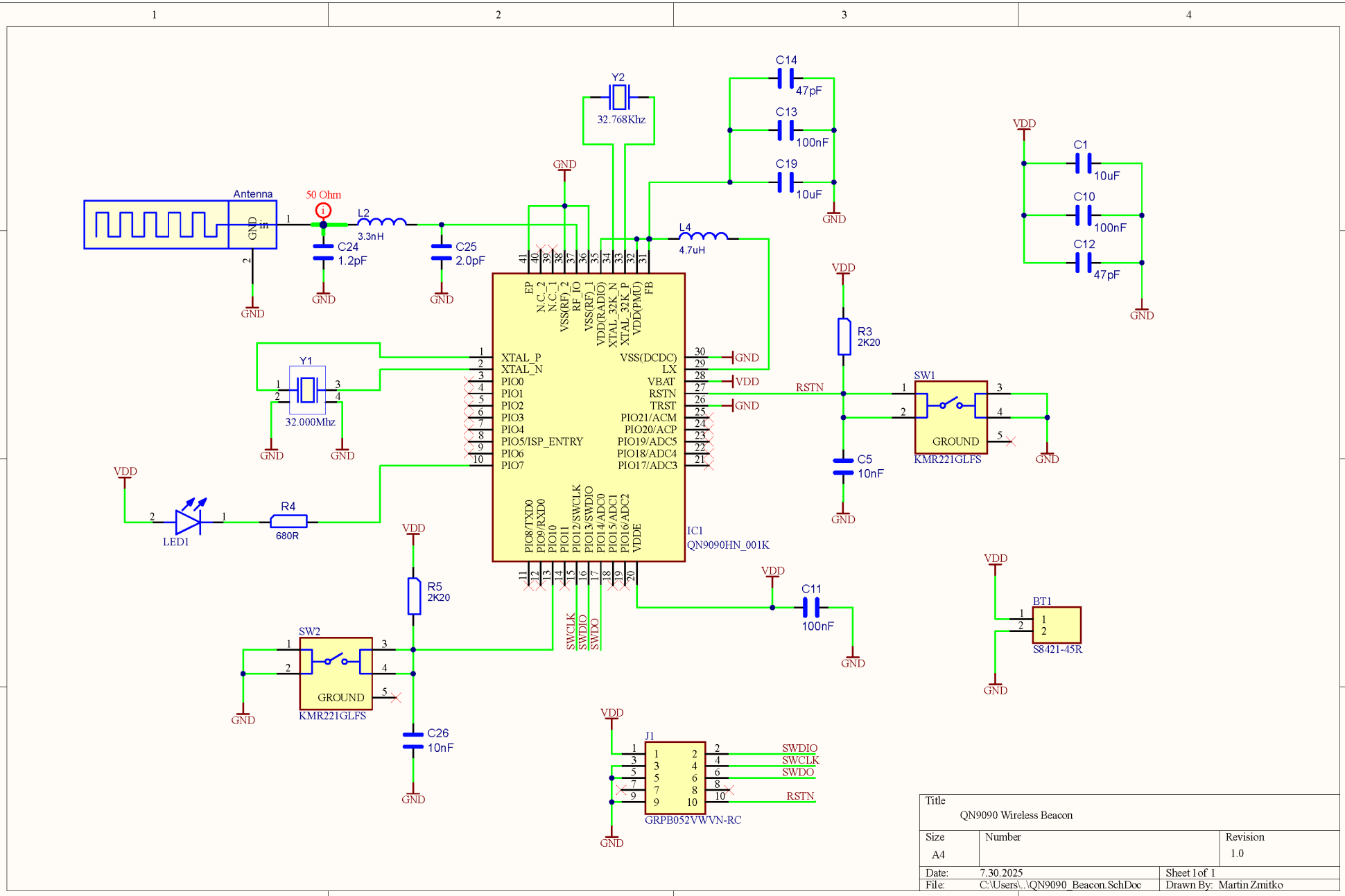
Tato příloha obsahuje schémata zapojení a seznamy použitých součástek pro oba návrhy prototypu navigačního bodu.

A.1 Návrh s mikrokontrolérem QN9090

Seznam použitých součástek je v tabulce A.1 a schéma zapojení je na další straně.

Designátor	**Hodnota**	**Výrobce**	**Číslo součástky**
BT1	držák baterie	Harwin	S8421-45R
C1, C19	10 uF	Murata	GRM21BR71A106KA73L
C5, C26	10 nF	Yageo	CC0402KRX7R7BB103
C10, C11, C13	100 nF	Murata	GRM155R71A104JA01D
C12, C14	47 pF	Murata	GRM1555C1E470JA01D
C24	1.2 pF	Murata	GRM1555C1H1R2BA01D
C25	2.0 pF	Murata	GJM1555C1H2R0BB01D
IC1	mikrokontrolér	NXP	QN9090HN/001K
J1	konektor	Sullins	GRPB052VWVN-RC
L2	3.3 nH	Murata	LQW15AN3N3B80D
L4	4.7 nH	TDK	MLZ2012M4R7HT000
LED1	červená LED	Rohm	SML-D12U8WT86
R3, R5	2.2 kOhm	Vishay	CRCW04022K20FKED
R4	680 Ohm	Panasonic	ERJ-2GEJ681X
SW1, SW2	mikrospínač	ITT C&K	KMR221GLFS
Y1	32 MHz	NDK	CS11213-32M
Y2	32.768 kHz	NDK	MU01089-32.768K

Tabulka A.1: Seznam použitých součástek



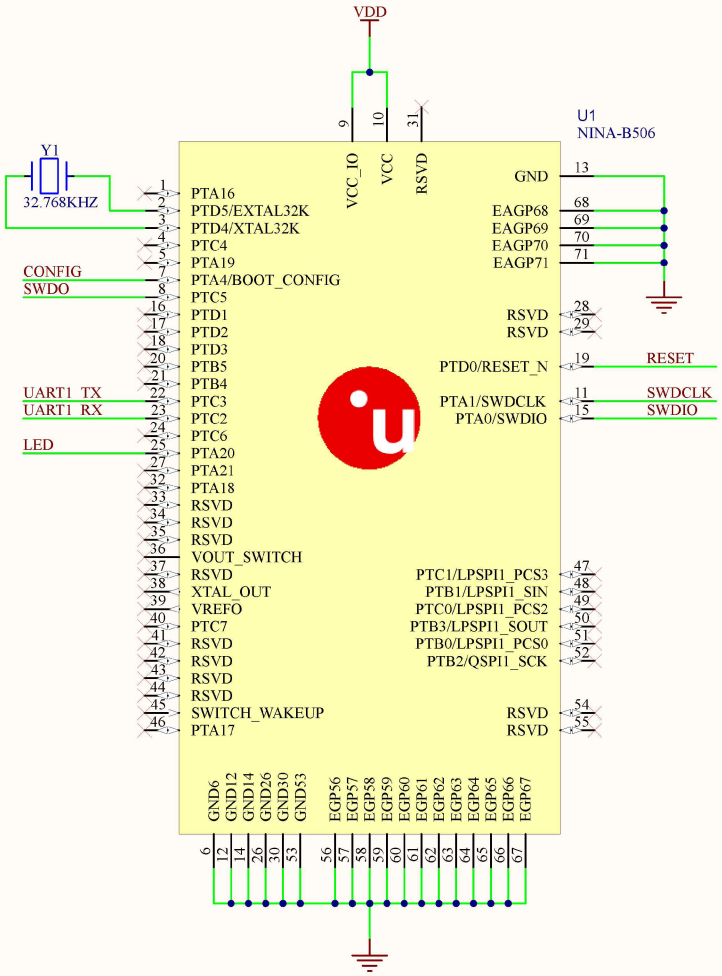
Title	QN9090 Wireless Beacon	
Size A4	Number	Revision 1.0
Date: 7.30.2025		Sheet 1 of 1
File: C:\Users\...\QN9090_Beacon.SchDoc		Drawn By: Martin Zmitko

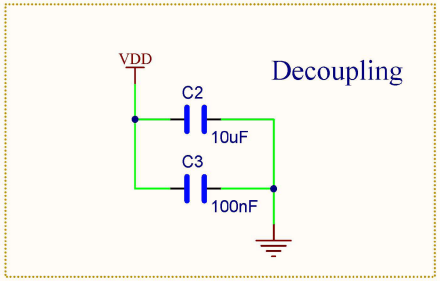
A.2 Návrh s modulem NINA-B506-00B

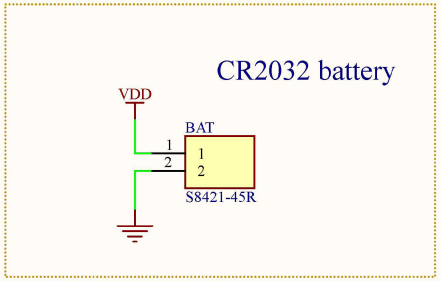
Seznam použitých součástek v tabulce A.2 a schéma zapojení je na následující straně.

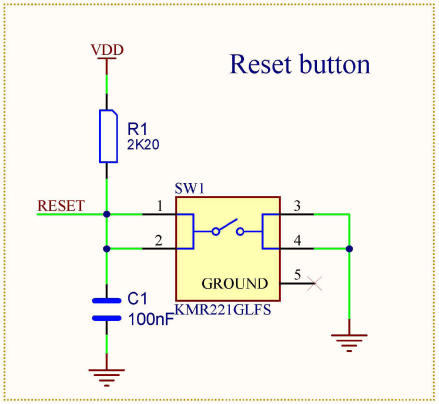
Designátor	**Hodnota**	**Výrobce**	**Číslo součástky**
BT1	držák baterie	Harwin	S8421-45R
C1, C3	100 nF	Yageo	CC0805KRX7R9BB104
C2	10 uF	Murata	GRM21BR71A106KA73L
U1	mikrokontrolér	u-blox	NINA-B506-00B
J1	konektor	Sullins	GRPB052VWVN-RC
J2	konektor	Würth Elektronik	61300411121
LED1	červená LED	Rohm	SML-D12U8WT86
R1, R2	2.2 kOhm	Yageo	RC0805FR-072K2L
R3	680 Ohm	Yageo	RC0805FR-07680RL
SW1, SW2	mikrospínač	ITT C&K	KMR221GLFS
Y1	32.768 kHz	NDK	MU01089-32.768K

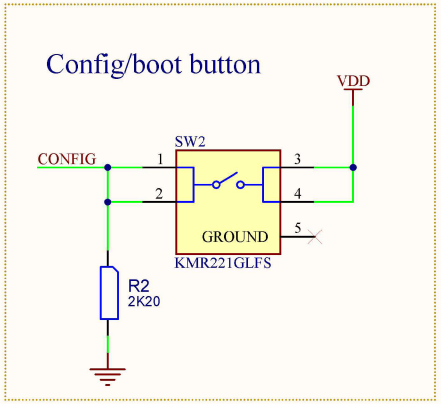
Tabulka A.2: Seznam použitých součástek pro návrh s modulem NINA-B506-00B

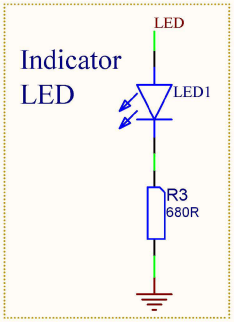


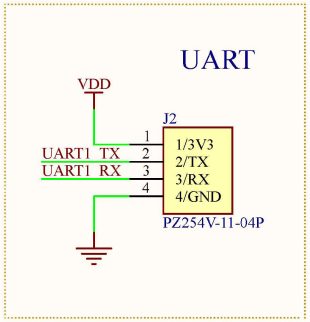


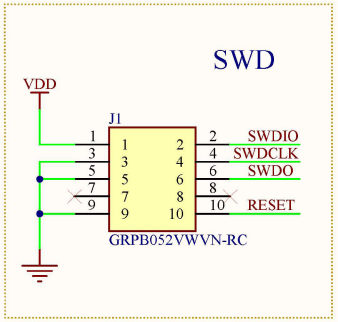












Title		
GeoBeacon		
Size: A4	Number	Revision: 2.0
Date: 7.30.2025		Sheet 1of 1
File: C:\Users\..\NINA-B506_Beacon.SchDoc		Drawn By: Martin Zmitko

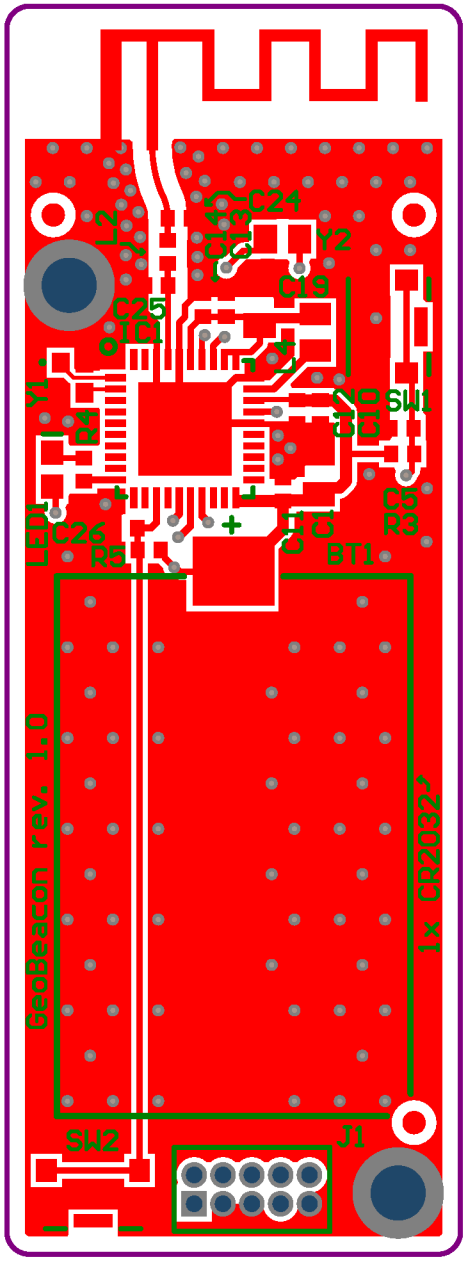
Příloha B

Návrhové podklady pro desky plošných spojů

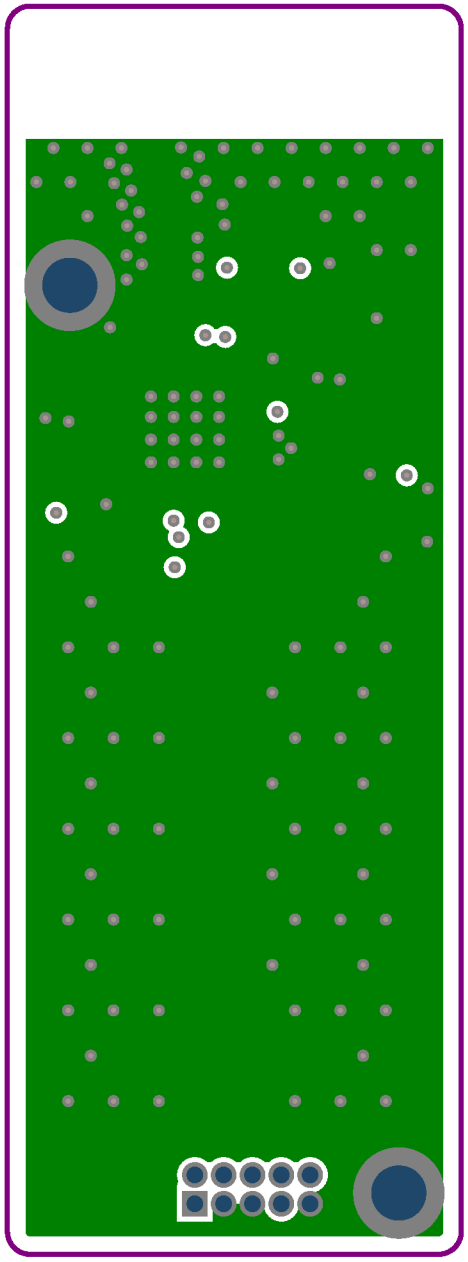
Tato příloha obsahuje návrhové podklady pro desky plošných spojů. Pro návrh s mikrokontrolérem QN9090 to jsou informace o složení jednotlivých vrstev desky (na obrázku B.1) a nákres jednotlivých vrstev nesoucích signály (na další straně). Nákres vrstev pro návrh s modulem NINA-B506-00B následuje stranu po nákresu pro návrh s QN9090.

Vrstva	Název	Materiál	Tloušťka	Dk (1 GHz)
1	Vrchní nepájivá maska	Elpemer 2467	0,015 mm	3,7
2	Vrchní vrstva (1)	Měď	0,0175 mm	
3	Dielektrikum	Prepreg IS400	0,13 mm	3,8
4	Vrstva 2	Měď	0,035 mm	
5	Dielektrikum (jádro)	Laminát IS400	1,2 mm	3,9
6	Vrstva 3	Měď	0,035 mm	
7	Dielektrikum	Prepreg IS400	0,13 mm	3,8
8	Spodní vrstva (4)	Měď	0,0175 mm	
9	Spodní nepájivá maska	Elpemer 2467	0,015 mm	3,7
		Celková tloušťka: 1,5 mm ± 10 %		

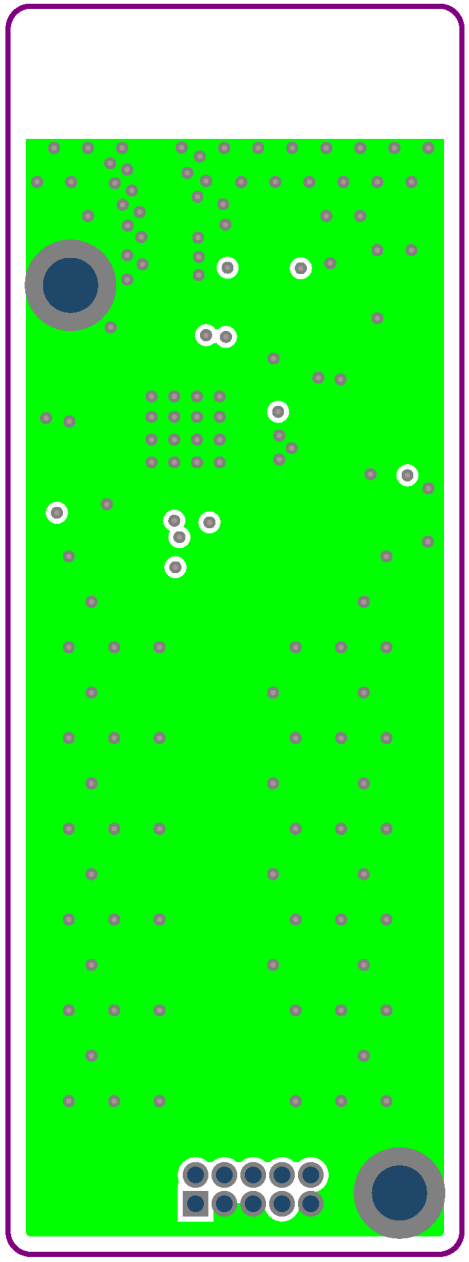
Obrázek B.1: Složení jednotlivých vrstev navržené desky plošných spojů s mikrokontrolérem QN9090



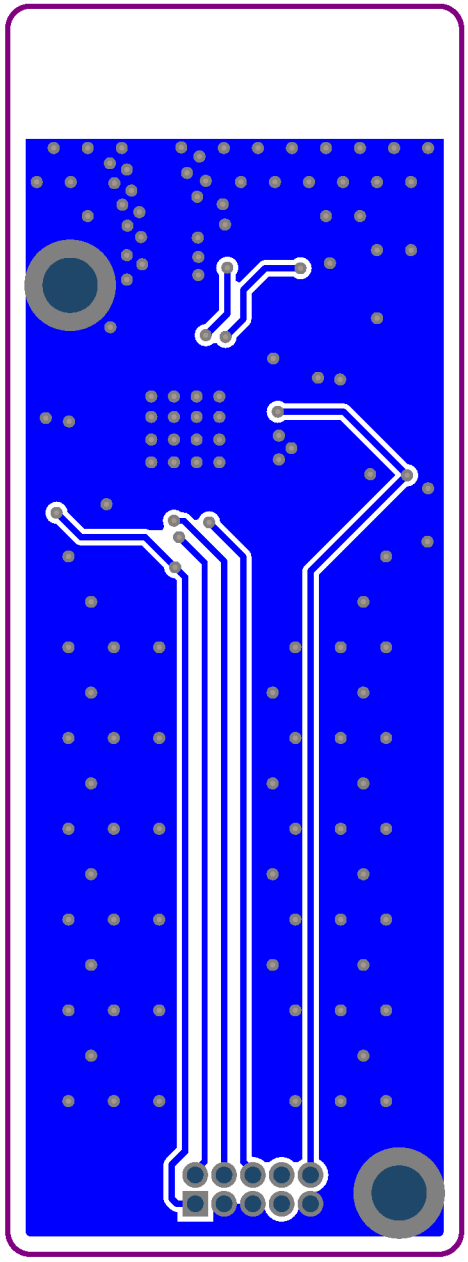
Vrchní vrstva (1)



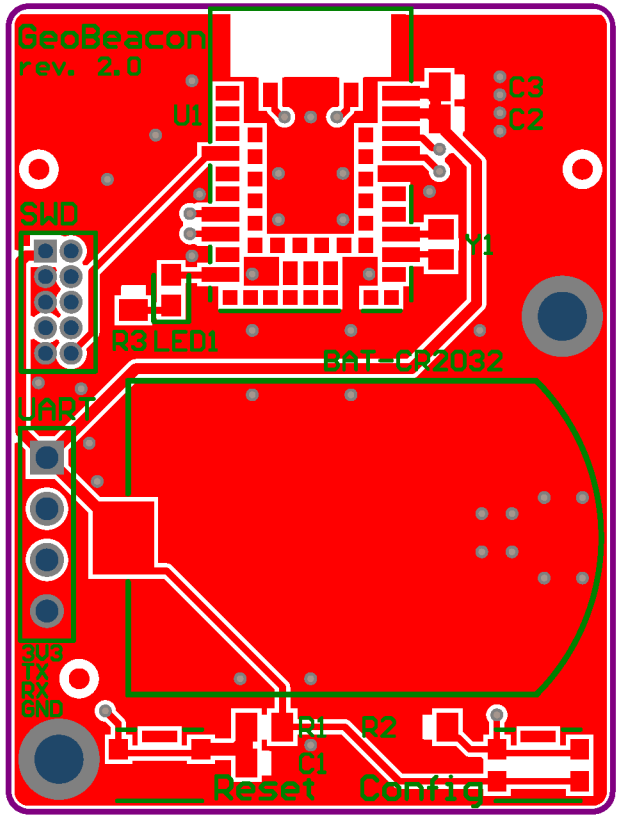
Vrstva 2



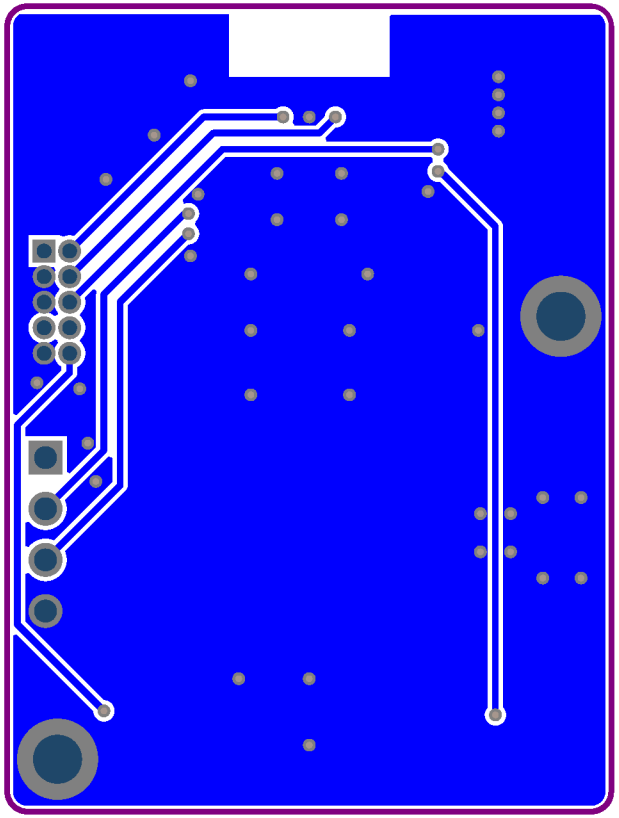
Vrstva 3



Spodní vrstva (4)



Vrchní vrstva



Spodní vrstva

Příloha C

Unikátní identifikátory vlastní Bluetooth Low Energy služby

Tato příloha obsahuje unikátní identifikátory vlastní Bluetooth Low Energy služby pro konfiguraci a jejích charakteristik. Všechny identifikátory jsou ve formátu UUID verze 4 o délce 128 bitů. Identifikátor služby byl generován náhodně, identifikátory charakteristik byly stanoveny jako nadcházející hodnotě identifikátoru služby. V tabulce C.1 jsou uvedeny názvy služeb i charakteristik (atributů) včetně jejich práv ke čtení (r), zápisu s potvrzením (w) a zápisu bez potvrzení (w-) protistranami a jejich unikátní identifikátory.

Název	**Práva**	**UUID**
Služba pro konfiguraci		d077defe-750a-fa81-724a-81ca3fe60900
Atribut pro autorizaci	w	d077defe-750a-fa81-724a-81ca3fe60901
Atribut pro změnu jména	w	d077defe-750a-fa81-724a-81ca3fe60902
Atribut pro změnu hesla	w	d077defe-750a-fa81-724a-81ca3fe60903
Atribut pro indikaci přenosu	r, w	d077defe-750a-fa81-724a-81ca3fe60904
Atribut pro přenos dat	w-	d077defe-750a-fa81-724a-81ca3fe60905
Atribut pro statistiku	r	d077defe-750a-fa81-724a-81ca3fe60906

Tabulka C.1: Unikátní identifikátory vlastní Bluetooth Low Energy služby pro konfiguraci