VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

BEZPEČNÁ KOMUNIKAČNÍ INFRASTRUKTURA PRO NOSITELNÉ MEDICÍNSKÉ APLIKACE

SECURE COMMUNICATION INFRASTRUCTURE FOR WEARABLE MEDICAL APPLICATIONS

DISERTAČNÍ PRÁCE
DOCTORAL THESIS

AUTOR PRÁCE Ing. Jakub Frolka
AUTHOR

VEDOUCÍ PRÁCE doc. Mgr. Karel Slavíček, Ph.D.
ADVISOR

BRNO 2024

ABSTRAKT

Disertační práce se zabývá návrhem a optimalizací nového dedikovaného bezdrátového komunikačního protokolu pro nositelné externí kardiostimulátory s ohledem na energetickou úspornost a spolehlivost přenosu dat. V rámci práce byly analyzovány současné komunikační potřeby a technická omezení těchto zařízení, přičemž důraz byl kladen na minimalizaci energetické spotřeby. Pro optimalizaci komunikačního protokolu byl vytvořen simulační model, který umožnil testování různých konfigurací protokolu. Klíčovým přínosem tohoto modelu je jeho schopnost optimalizovat parametry přenosu, jako jsou délka datového rámce, použité BCH kódy a přenosové rychlosti. Navržený protokol je jednosměrný, což umožňuje kardiostimulátorům pouze vysílat data, čímž se minimalizuje spotřeba energie a zajišťuje ochrana proti kybernetickým hrozbám. Výsledky simulace ukázaly, že navržený komunikační protokol je schopný zajistit bezpečný přenos dat až pro 10 uživatelů současně v dosahu jedné přijímací stanice při přenosové rychlosti 100 kb/s a vyšší. Pro zabezpečení přenosu byly využity BCH kódy, které zajišťují ochranu před chybami při přenosu. Tato práce představuje ucelený koncept dedikovaného komunikačního protokolu, který lze využít nejen pro externí kardiostimulátory, ale i pro další aplikace vyžadující nízkoenergetické bezdrátové přenosy. Simulační model může sloužit jako základ pro další vývoj a přizpůsobení protokolu konkrétním potřebám.

KLÍČOVÁ SLOVA

nositelný kardiostimulátor, bezdrátová komunikace, telemedicína, komunikační protokol, BCH kódování, simulační model, optimalizace

ABSTRACT

This doctoral thesis deals with the design and optimization of a new dedicated wireless communication protocol for wearable external pacemakers with respect to energy efficiency and data transmission reliability. The current communication needs and technical limitations of these devices were analyzed, with emphasis on minimizing energy consumption. To optimize the communication protocol, a simulation model was developed to test different protocol configurations. The main contribution of this model is its ability to optimize transmission parameters such as data frame length, BCH codes used and transmission rates. The proposed protocol is unidirectional, allowing pacemakers to only transmit data, minimizing power consumption and providing protection against cyber threats. Simulation results showed that the proposed communication protocol is capable of providing secure data transmission for up to 10 users simultaneously within the range of a single receiving base station at a data rate of 100 kb/s or higher. BCH codes were used to secure the transmission to provide protection against transmission errors. This work presents a comprehensive concept of a dedicated communication protocol that can be used not only for external pacemakers but also for other applications requiring low-power wireless transmissions. The simulation model can serve as a basis for further development and adaptation of the protocol to specific needs.

KEYWORDS

wearable pacemaker, wireless communication, telemedicine, communication protocol, BCH coding, simulation model, optimization

Vysázeno pomocí balíčku `thesis` verze 4.11; `https://latex.fekt.vut.cz/`

FROLKA, Jakub. *Bezpečná komunikační infrastruktura pro nositelné medicínské aplikace*. Disertační práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2024. Vedoucí práce: doc. Mgr. Karel Slavíček, Ph.D.

Prohlášení autora o původnosti díla

Jméno a příjmení autora:	Ing. Jakub Frolka
VUT ID autora:	110408
Typ práce:	Disertační práce
Akademický rok:	2024/25
Téma závěrečné práce:	Bezpečná komunikační infrastruktura pro nositelné medicínské aplikace

Prohlašuji, že svou závěrečnou práci jsem vypracoval samostatně pod vedením vedoucího závěrečné práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce. Při vypracovávání práce byly použity nástroje Grammarly, GPT-4 a DeepL, a to za účelem práce s odbornou literaturou a pro zlepšení čitelnosti textu. Po použití těchto nástrojů jsem obsah zkontroloval a upravil a za obsah práce přebírám plnou odpovědnost. Uvedené nástroje jsou použity v souladu s pravidly VUT v Brně platnými v době psaní této práce a jsou dostupné na adrese `https://www.vut.cz/uredni-deska/ai/vzdelavani`.

Jako autor uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autora*

*Autor podepisuje pouze v tištěné verzi.

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu mé disertační práce, doc. Mgr. Karlovi Slavíčkovi, Ph.D., za jeho neocenitelné odborné vedení, trpělivý přístup a ochotu věnovat čas konzultacím, které mi poskytly cenné rady a podněty k dalšímu směřování mé práce. Jeho odborné znalosti a konstruktivní zpětná vazba byly pro mě neocenitelným přínosem a pomohly mi překonat klíčové výzvy, které s touto prací souvisely. Vedení Ústavu telekomunikací FEKT VUT v Brně pak děkuji za možnost absolvovat doktorské studium souběžně s mými běžnými pracovními povinnostmi.

Velké poděkování patří také mé rodině, která mě během celého studia a přípravy této práce podporovala. Jejich trpělivost, povzbuzení a porozumění byly pro mě stálým zdrojem motivace a pomáhaly mi soustředit se na dosažení svých cílů. Bez jejich podpory by tato práce nebyla možná.

Zvláštní díky chci vyjádřit také svým kolegům, kteří mě během mé práce doprovázeli a svými cennými radami, sdílenými zkušenostmi a ochotou pomoci přispěli k řešení mnoha dílčích problémů. Jejich podpora byla pro mě nejen praktickým přínosem, ale také cenným zdrojem inspirace a spolupráce. Mezi nimi bych chtěl zvlášť poděkovat následujícím osobnostem, jejichž podpora a povzbuzení pro mě byly klíčové:

Ing. Vlastimil Člupek, Ph.D., Ing. Jan Dvořák, Ph.D., Ing. David Grenár, Ph.D.,
doc. Ing. Jan Jeřábek, Ph.D., Ing. Tomáš Lieskovan, Ph.D., Ing. Vojtěch Myška, Ph.D.,
Ing. Pavel Sikora, RNDr. Ing. Pavel Šeda, Ph.D.

Na závěr bych rád poděkoval všem, kteří se jakýmkoliv způsobem podíleli na této práci, ať už svými odbornými názory, podporou či povzbuzením. Vaše pomoc a důvěra ve mě mi umožnily tuto práci dokončit a dosáhnout svých cílů.

Obsah

Úvod **19**

1 Současný stav poznání **21**

1.1 Komplexní metodologický přístup k evaluaci bezpečnostních hrozeb v komunikačních lékařských infrastrukturách 21

1.2 DDoS útoky a jejich klasifikace 22

1.2.1 Záplavové útoky na síťovou a transportní vrstvu 22

1.2.2 Záplavové útoky na aplikační vrstvu 22

1.2.3 Obrana proti DDoS útokům 23

1.3 Zhodnocení možných bezpečnostních dopadů 25

1.4 Bezdrátové komunikační protokoly 26

1.4.1 Radiová přenosová pásma 27

1.4.2 Bluetooth a Bluetooth Low Enery (BLE) 28

1.4.3 Wi-Fi 29

1.4.4 LoRa a LoRaWAN 29

1.4.5 Zigbee 29

1.4.6 Mobilní sítě 30

1.4.7 Z-Wave 30

1.4.8 IQRF 30

1.4.9 Výběr vhodné bezdrátové technologie 30

1.5 Modelování a simulace datového provozu 32

1.5.1 Matematické nástroje použité pro simulace 33

2 Kódy pro bezpečný přenos a ukládání dat **39**

2.1 Algebraické základy samoopravných kódů 39

2.2 Bose–Chaudhuri–Hocquenghem kódy 42

2.3 Použití BCH kódů v komunikačních a datových systémech 43

2.3.1 Využití BCH kódů pro zlepšení poměru signálu a šumu a bitové chybovosti 44

2.4 Systémové začlenění BCH kódů a význam jednotlivých pojmů 44

2.4.1 Binární BCH kódy 45

2.4.2 Kódování BCH kódů 47

2.4.3 Dekódování BCH kódů 49

3 Cíle disertační práce **57**

4 Koncepce komunikačního protokolu **59**
4.1 Analýza technických prostředků 61
4.1.1 Radiofrekvenční moduly 61
4.1.2 Výběr radiofrekvenčního řešení 64
4.2 Analýza anténního systému 64
4.2.1 Kvalitativní hodnocení anténních systémů 66
4.3 Parametry fyzické vrstvy přenosu 68
4.4 Koncepce struktury rámce pro bezdrátovou technologii 68
4.5 Návrh BCH kódů na základě specifických vstupních parametrů 75
4.5.1 Varianta nejkratšího rámce 76
4.5.2 Varianta delšího rámce 77
4.5.3 Shrnutí délky navržených rámců připravených pro simulace . . 78
4.5.4 Generující polynomy pro navrhované BCH kódy 79
4.6 Simulační model 80
4.6.1 Konstrukce simulačního modelu 80
4.6.2 Implementace systému pro vyhledávání a vyhodnocení kolizí . 83
4.7 Simulace a zhodnocení získaných výsledků 87
4.7.1 Přenosová rychlost a celková délka datového rámce 87
4.7.2 Počet opakování kritických dat 89
4.7.3 Počet opravitelných bitových chyb 90
4.7.4 Počet současně komunikujících uživatelů 90

5 Zásady pro implementaci vlastního řešení **95**
5.1 Radiofrekveční modul pro kardiostimulátor 95
5.2 Koncepce základnové stanice 96

Závěr **99**

Autorova literatura **103**

Literatura **105**

Seznam symbolů a zkratek **115**

Seznam příloh **119**

A Přehled vlastností BCH kódů **121**

B Analýza vlastností radiofrekvenčních modulů **123**
B.1 Srovnání klíčových parametrů RF modulů založených na architektuře Intel 8051 123

B.2 Srovnání klíčových parametrů RF modulů založených na architektuře ARM Cortex-M4 124
B.3 Srovnání klíčových parametrů RF modulů založených na architektuře ARM Cortex-M33. 125
B.4 Srovnání klíčových parametrů RF modulů s proprietární architekturou 126

C Průzkum výrobců antén a jejich srovnání parametrů 127

D Výsledky simulací dedikovaného komunikačního protokolu pro různé doby vysílání 129

Curriculum Vitæ 137

Seznam obrázků

1.1 Schéma datového provozu při útoku. 24
1.2 Obranné mechanismy a jejich umístění v jednoduché síti autonomních systémů (AS). 25
2.1 Zapojení děličky mod $g(x)$. 49
2.2 Vývojový diagram Berlekamp-Massey algoritmu. 52
4.1 Příklady externích kardiostimulátorů: a) Mediatrade model EPG10, b) St. Jude Medical model 3085. 59
4.2 Znázornění možných nároků na přenos dat od pacientů při rehabilitaci. 60
4.3 Znázornění základních bloků bezdrátového rámce dané typem radiového modulu. 69
4.4 Znázornění bloků navrženého bezdrátového rámce. 69
4.5 Blokové znázornění oddělovačů začátku (SFD) a konce (EFD) obecného multirámce. 70
4.6 Blokové znázornění struktury multirámce pro kardiostimulátor. 71
4.7 Znázornění vztahu multirámců a sekvenčních čísel. 73
4.8 Znázornění funkce kruhového bufferu pro zpracování STD rámců. . . 74
4.9 Rámec a jejich zabezpečené bloky pro variantu bez zabezpečení bloku NODE ID. 76
4.10 Rámec a jejich zabezpečené bloky se zabezpečení bloku NODE ID. . . 77
4.11 Rámec a jejich zabezpečené bloky pro variantu bez zabezpečení bloku NODE ID. 78
4.12 Rámec a jejich zabezpečené bloky se zabezpečení bloku NODE ID. . . 78
4.13 Znázornění časových intervalů úderů srdce několika pacientů. 81
4.14 Závislost počtu pacientů na nutném počtu opakování pro délku rámce 40 B pro různé přenosové rychlosti. 91
4.15 Závislost počtu pacientů na nutném počtu opakování pro délku rámce 24 B pro různé přenosové rychlosti. 92
4.16 Optimalizovaný rámec délky 40 B a velikosti jednotlivých bloků. . . . 93
5.1 Znázornění scénáře přenosu informací z kardiostimulátoru. 95
5.2 Blokové řešení kardiostimulátoru a RF modulu. 96
5.3 Blokové řešení základnové stanice. 96

Seznam tabulek

1.1 Doporučené rádiové kmitočty dle ČTÚ pro zařízení s krátkým dosahem [110, 112]. 28
1.2 Porovnání bezdrátových komunikačních technologií. 31
4.1 Vybrané antény pro 434MHz 67
4.2 Vybrané antény pro 868MHz 67
4.3 Přehled vhodných formátů fyzického rozhraní. 68
4.4 Podrobná struktura multirámce. 72
4.5 Význam jednotlivých bitů pole STD datového rámce. 75
4.6 Délky datových rámců a jejich vysílací doby v závislosti na bitové rychlosti 88
4.7 Tabulka přenosových rychlosti pro různý počet pacientů a opakování pro délku rámce 40 B 91
4.8 Tabulka přenosových rychlosti pro různý počet pacientů a opakování pro délku rámce 24 B 92
B.1 Přehled klíčových RF modulů založených na architektuře Intel 8051. . 123
B.2 Srovnání klíčových parametrů RF modulů založených na architektuře ARM Cortex-M4. 124
B.3 Srovnání klíčových parametrů RF modulů založených na architektuře ARM Cortex-M33. 125
B.4 Přehled klíčových RF modulů s proprietární architekturou. 126
C.1 Výběr antén na trhu pro frekvenční pásma 434MHz a 868MHz. 128
D.1 Tabulka výsledků simulací pro dobu vysílání 9,583 ms. 129
D.2 Tabulka výsledků simulací pro dobu vysílání 8,333 ms. 130
D.3 Tabulka výsledků simulací pro dobu vysílání 6,4 ms. 131
D.4 Tabulka výsledků simulací pro dobu vysílání 6,25 ms. 131
D.5 Tabulka výsledků simulací pro dobu vysílání 5 ms. 132
D.6 Tabulka výsledků simulací pro dobu vysílání 3,84 ms. 132
D.7 Tabulka výsledků simulací pro dobu vysílání 3,2 ms. 133
D.8 Tabulka výsledků simulací pro dobu vysílání 1,92 ms. 133
D.9 Tabulka výsledků simulací pro dobu vysílání 1,6 ms. 134
D.10 Tabulka výsledků simulací pro dobu vysílání 0,96 ms. 134
D.11 Tabulka výsledků simulací pro dobu vysílání 0,64 ms. 135
D.12 Tabulka výsledků simulací pro dobu vysílání 0,384 ms. 135
D.13 Tabulka výsledků simulací pro dobu vysílání 0,16 ms. 136
D.14 Tabulka výsledků simulací pro dobu vysílání 0,096 ms. 136

Úvod

Rozvoj datových sítí a internetových technologií v 90. letech 20. století významně ovlivnil způsob komunikace napříč mnoha obory, včetně zdravotnictví. Díky možnosti univerzálního přenosu dat bylo možné integrovat různé typy komunikace (hlas, obraz, text) do jediného systému, což se promítlo do efektivnější spolupráce mezi lékařskými týmy a urychlilo diagnostické procesy. Ve zdravotnických zařízeních byla v této době široce rozšířena technologie ATM (Asynchronous Transfer Mode), jež se vyznačuje vysokou propustností a nízkou latencí. V České republice byl na přelomu století implementován například projekt MEDIMED [34], který s využitím centrálního archivu [33, 35] umožňoval přenos a sdílení velkých multimediálních souborů (rentgenové snímky, ultrazvukové záznamy aj.) mezi nemocnicemi. Tato řešení přispěla k všestrannějšímu a rychlejšímu využití sítí v rámci sdílení medicínských dat.

S pokračujícím rozvojem moderních informačních technologií získala na významu tzv. telemedicína, jež označuje spojení lékařské informatiky a telekomunikací s cílem poskytovat zdravotnické služby na dálku. Telemedicína umožňuje nejen přenos velkoobjemových dat, ale i dat nízkých objemů, která mohou být klíčová pro průběžné monitorování pacienta. V rámci telemedicínských aplikací se využívá např. vzdálený přístup k laboratorním výsledkům, odborné konzultace či kontinuální sledování chronicky nemocných pacientů. Tím jsou zajištěny lepší podmínky pro rychlou diagnostiku, dostupnost péče i v odlehlých oblastech a snížení přetížení zdravotnických pracovišť.

Současně roste význam nositelné elektroniky, která se uplatňuje v celé řadě zdravotnických zařízení a senzorů. Tato elektronika dokáže průběžně sbírat data o zdravotním stavu uživatele a poskytovat je v reálném čase lékařským systémům. Nositelná zařízení (např. chytré hodinky, senzory pro měření tepu nebo tzv. wearables pro rehabilitační účely) však kladou specifické nároky na bezdrátový přenos dat. Přestože jsou v praxi využívány standardní technologie jako Bluetooth, ZigBee či Wi-Fi, není jejich nasazení pro externí kardiostimulátory vždy vhodné. Důvodem je zejména požadavek na velmi nízkou spotřebu energie, vysokou spolehlivost přenosu a minimalizaci kybernetických rizik.

Jádrem problému je tedy skutečnost, že dosud neexistuje dedikovaný bezdrátový komunikační protokol pro nositelné externí kardiostimulátory, jenž by splňoval veškeré požadavky na energetickou úspornost a spolehlivost přenosu. Tato disertační práce si proto klade za cíl vyplnit mezeru ve výzkumu a navrhnout nový komunikační protokol se zaměřením na nízkou energetickou náročnost a robustní přenos dat. Vytvořený návrh umožní zlepšit úroveň péče o pacienty, neboť lékaři budou mít k dispozici včasné a spolehlivé informace o srdeční aktivitě uživatelů externích nositelných kardiostimulátorů.

Disertační práce je rozdělena do pěti hlavních částí. Sekce 1.1 až 1.3 zahrnují popis komplexního metodologického přístupu k evaluaci bezpečnostních hrozeb v komunikačních lékařských infrastrukturách a zhodnocení možných bezpečnostních dopadů. V sekci 1.4 je provedena analýza existujících bezdrátových komunikačních protokolů a rádiových přenosových pásem. Sekce 1.5 se zabývá nástroji pro modelování a simulace datového provozu. Kapitola 2 je zaměřena na kódy pro bezpečný přenos a ukládání dat, s bližším zaměřením na skupinu detekčních a samoopravných kódů, které jsou využity v návrhu nového komunikačního protokolu. Cíle disertační práce jsou uvedeny v kap. 3. Hlavnímu cíli návrhu komunikačního protokolu je věnována kap. 4, která obsahuje analýzu komunikačních potřeb nositelných kardiostimulátorů, analýzu technických prostředků, popis parametrů fyzické vrstvy, koncepci struktury rámce pro bezdrátovou technologii, simulační model pro ověření a optimalizaci návrhu komunikačního protokolu. Kapitola 5 je zaměřena na zásady pro vlastní implementaci řešení navrženého komunikačního protokolu a infrastruktury.

1 Současný stav poznání

Se současným technickým pokrokem v oblasti mikroelektroniky se otevírá řada možností využití nových technických prostředků pro zlepšení životních či pracovních podmínek člověka. Jednou ze zajímavých aplikačních oblastí je i nositelná elektronika ve zdravotnictví.

Nositelná zařízení v lékařství musí splňovat řadu klíčových technických požadavků, aby zajistila bezpečné, přesné a spolehlivé používání. Splnění většiny těchto požadavků, jako např. odolnost vůči prachu a vlhkosti, hygienická nezávadnost, dlouhá životnost, elektrická bezpečnost a pod., je na zodpovědnosti výrobce příslušného zařízení.

Tato práce je soustředěna na bezdrátovou komunikaci, zejména na kompatibilitu se zdravotnickým prostředkem (v případě kardiostimulátoru vysílání jen po dobu klidové fáze srdce), spolehlivost přenosu dat a energetickou náročnost. Ochrana osobních a zdravotních údajů je přitom klíčová.

1.1 Komplexní metodologický přístup k evaluaci bezpečnostních hrozeb v komunikačních lékařských infrastrukturách

S rozvojem telemedicíny a vývojem nových zdravotnických řešení je nezbytné klást důraz na analýzu a minimalizaci bezpečnostních rizik. Nedávné útoky na nemocniční zařízení, které vedly k omezení jejich provozu, zdůrazňují význam ochrany proti kybernetickým hrozbám. Jedním z možných typů útoků, které mohou ohrozit funkčnost zdravotnických systémů, je odepření služby (DoS – Denial of Service). Tento typ útoku slouží k zamezení přístupu uživatelů k síťovým službám cílového systému.

První distribuovaný DoS (DDoS) útok byl oznámen v roce 1999 [31], přičemž od té doby se DDoS útoky staly jedním z nejčastějších typů kybernetických hrozeb.

Pro realizaci DDoS útoků jsou často využívány sítě vzdáleně ovládaných zařízení, známých jako boti (nebo zombie), které společně tvoří tzv. botnet. Tato zařízení simultánně generují velký objem datového provozu nebo požadavků na služby cílového systému. Výsledkem je buď výrazné zpomalení odezvy systému, nebo jeho úplné zhroucení [68]. Boti bývají obvykle infikované počítače nebo jiná síťová zařízení, a přestože mají jednotlivě omezené prostředky, jejich velký počet umožňuje útočníkům provést útoky s rozsáhlými a ničivými dopady. Tyto útoky jsou často označovány jako "záplavové útoky".

1.2 DDoS útoky a jejich klasifikace

Distribuovaná povaha DDoS útoků činí obranu proti těmto útokům mimořádně složitou. Útočníci často využívají podvržené IP (Internet Protokol) adresy (tzv. IP spoofing), aby skryli svou pravou identitu, což ztěžuje identifikaci původce útoku. Vzhledem k bezpečnostním slabinám mnoha zařízení připojených k Internetu je snadné tato zařízení zneužít, což přispívá k rychlému nárůstu útoků, zejména těch zaměřených na protokoly aplikační vrstvy. Jedním z klíčových kroků při návrhu účinné obrany proti záplavovým útokům je hluboké porozumění všem aspektům DDoS útoků, což v odborné literatuře vedlo k návrhům různých klasifikací.

Záplavové útoky lze rozdělit do dvou hlavních kategorií podle cílené protokolové vrstvy:

1.2.1 Záplavové útoky na síťovou a transportní vrstvu

Tyto útoky se zaměřují na protokoly TCP (Transmission Control Protocol), UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol) a DNS (Domain Name System). Podle [68, 74] mohou být dále rozděleny do čtyř typů:

- Záplavové útoky: Cílem je vyčerpání šířky pásma konektivity oběti. Mezi nejznámější příklady patří UDP flood, ICMP flood nebo DNS flood.
- Záplavové útoky zneužívající chyby protokolů: Útočník využívá specifickou vlastnost nebo implementační chybu protokolu. Typickými příklady jsou TCP SYN flood, TCP SYN-ACK flood a RST/FIN flood.
- Reflektivní záplavové útoky: Útočník posílá podvržené žádosti (např. ICMP žádost) tzv. reflektorům, které následně odpověďmi vyčerpávají zdroje oběti (např. útoky Smurf a Fraggle).
- Amplifikační záplavové útoky: Útočník využívá služeb, které generují větší objem odpovědí než původní dotazy. Kombinace reflektivní a amplifikační techniky je běžná u botnetů. Například Smurf útok využívá broadcastové adresy pro amplifikaci.

1.2.2 Záplavové útoky na aplikační vrstvu

Útoky na aplikační vrstvě jsou zaměřeny na vyčerpání serverových zdrojů (např. CPU, paměť, šířka pásma, databáze nebo HDD) [77]. Tyto útoky bývají nenápadnější než útoky na síťové vrstvě, protože napodobují běžný provoz, ale jejich důsledky jsou stejně závažné. Mezi typické příklady patří:

1. Reflektivní a amplifikační záplavové útoky: Využívají stejného principu jako útoky na nižší vrstvy. Například DNS amplifikační útok generuje velké odpovědi na malé dotazy s podvrženou zdrojovou IP adresou [68].

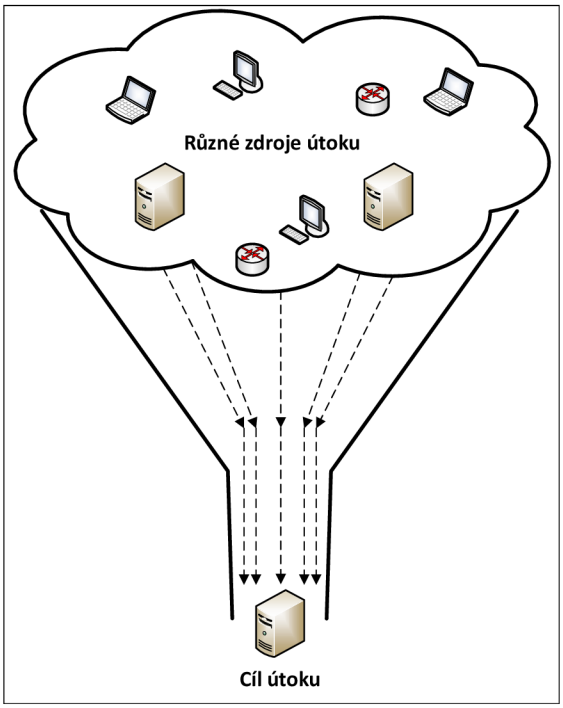
2. HTTP (HyperText Transfer Protocol) záplavové útoky [78, 107]:
   - Relační záplavové útoky: Generují velký počet relačních spojení, jako je HTTP GET/POST Excessive Verb.
   - Útoky žádostí: Využívají jedné relace k odeslání více požadavků (např. HTTP GET/POST Excessive Verb single session).
   - Útoky pomalých žádostí/odpovědí:
     - Slowloris: Odesílá HTTP hlavičky po malých částech, což server nutí čekat na dokončení.
     - HTTP fragmentace: Fragmentuje HTTP pakety a odesílá je pomalu, aby udržela spojení otevřená.
     - Slowpost: Pomalu odesílá obsah těla HTTP POST zprávy po definovaných malých částech.
     - Slowread: Pomalu přijímá odpovědi, čímž udržuje spojení aktivní [57].

1.2.3 Obrana proti DDoS útokům

DDoS záplavové útoky vyčerpávají značné množství systémových zdrojů po cestě k oběti. Hlavním cílem obrany je proto tyto útoky co nejdříve detekovat a zastavit co nejblíže jejich zdrojům. Schéma datového provozu při DDoS útoku, znázorněné na Obr. 1.1, ilustruje, jak záplavový útok probíhá. Internet jako rozsáhlá síť umožňuje vedení útoků z více míst současně. Tento proces lze přirovnat k nálevce, kde na vstupu velké množství napadených zařízení tvoří síť botnet. Každý bot přispívá do útoku svým dílem datového provozu. Na výstupu nálevky, kde je umístěna oběť, prochází síťový provoz několika společnými zařízeními, která přenášejí jak legitimní (žádoucí), tak nežádoucí provoz. Právě v tomto místě lze s největší přesností rozlišit legitimní provoz od útoků. Nicméně přístupová zařízení připojená k oběti často nemají dostatek prostředků na filtrování velkého množství provozu, což vede ke ztrátě legitimního provozu. Proto je ideální filtrování nežádoucího provozu realizovat co nejblíže zdrojům útoku, aby se minimalizovalo zatížení zařízení na cestě k oběti. V praxi je však často nezbytné nalézt kompromis mezi místem detekce a filtrování, aby byla zachována vysoká přesnost detekce a zároveň byla zařízení schopna efektivně reagovat na útok spuštěním filtrace.

V odborných publikacích [28, 68, 74] bylo navrženo několik mechanismů pro obranu proti záplavovým útokům. Tyto mechanismy byly následně klasifikovány dle jejich místa nasazení, jak je uvedeno v kapitole 1.2. Na základě této klasifikace lze obranné mechanismy rozdělit do několika kategorií podle cílové vrstvy a jejich umístění v síti.

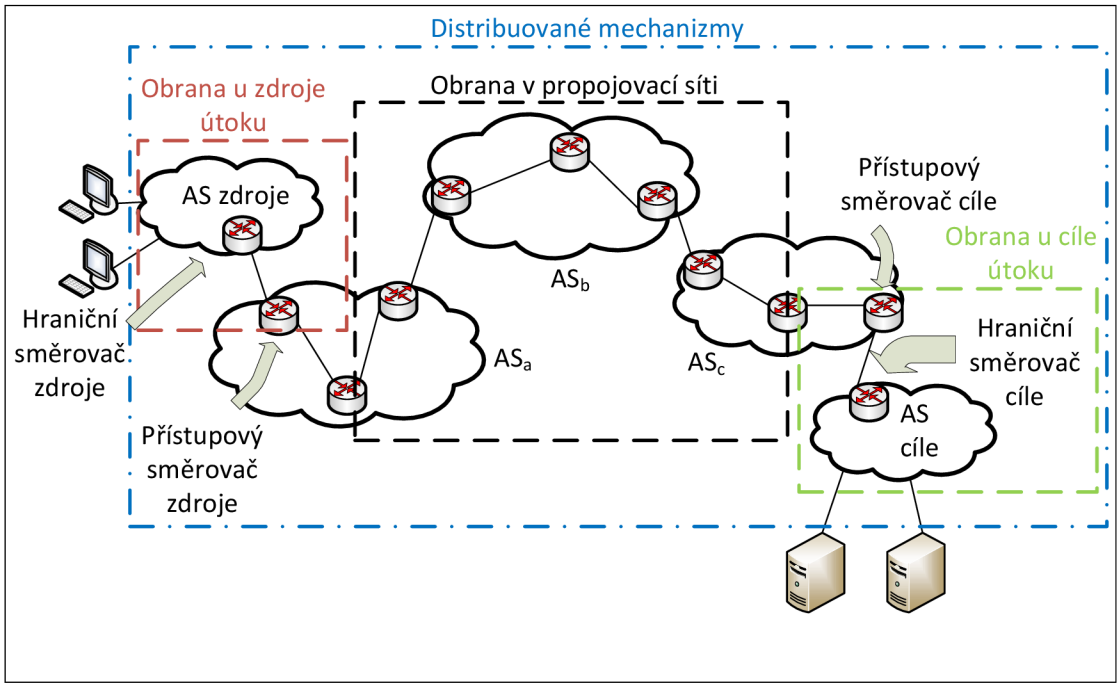
Rozdělení obranných mechanismů dle jejich umístění bylo poprvé představeno



Obr. 1.1: Schéma datového provozu při útoku.

v článku [31]. Později bylo toto rozdělení rozšířeno o kategorii distribuovaných mechanismů v článku [107]. Obr. 1.2 znázorňuje jednoduchou síť autonomních systémů (AS) a možnosti umístění jednotlivých typů obranných mechanismů v síti.

1. Mechanismy pro obranu proti záplavovým útokům zaměřeným na síťovou a transportní vrstvu:
   - Umístěné u zdroje: Mechanismy lokalizované co nejblíže zdroji útoku. Jejich cílem je zabránit šíření škodlivého provozu do dalších částí sítě.
   - Umístěné u cíle: Mechanismy nasazené v blízkosti cílového systému, kde je možné s největší přesností detekovat a filtrovat škodlivý provoz.
   - Umístěné v propojovací síti: Mechanismy implementované na úrovni páteřní nebo propojovací infrastruktury. Tyto systémy umožňují filtrovat škodlivý provoz v mezilehlých částech sítě.
   - Distribuované mechanismy: Kombinace výše uvedených přístupů. Distribuované mechanismy umožňují detekci a zmírňování útoků na více úrovních sítě, čímž zvyšují účinnost ochrany.
2. Mechanismy pro obranu proti záplavovým útokům zaměřeným na aplikační vrstvu:
   - Umístěné u cíle: Mechanismy zaměřené na ochranu aplikačních serverů před útoky, které vyčerpávají zdroje serveru.
   - Distribuované mechanismy: Mechanismy kombinující detekci a zmírňování na více úrovních sítě, přičemž se zaměřují na aplikační provoz.



Obr. 1.2: Obranné mechanismy a jejich umístění v jednoduché síti autonomních systémů (AS).

Důležitost obrany proti DDoS útokům

Existuje mnoho typů DDoS útoků, které představují závažné bezpečnostní riziko. Obranné mechanismy musí být schopny detekovat a efektivně čelit různým druhům záplavových útoků, a to jak objemným síťovým, tak nenápadným aplikačním útokům. Vzhledem k distribuované povaze těchto útoků a využití botnetů je identifikace původců a zmírnění dopadů stále výzvou pro moderní bezpečnostní systémy.

1.3 Zhodnocení možných bezpečnostních dopadů

V předchozích částech byly popsány DDoS útoky jako jedno z klíčových rizik v kontextu kybernetické bezpečnosti. Při návrhu nového systému je nezbytné důkladně zhodnotit potenciální rizika a jejich dopady. Vzhledem k tomu, že se jedná o systém pro lékařské aplikace, mohou mít jakékoli DDoS útoky kritické důsledky na zdraví a bezpečnost pacientů. Z tohoto důvodu je zásadní, aby navrhovaný systém byl chráněn proti externí hrozbě.

Práce [48] se zabývá návrhem bezpečného komunikačního modelu pro implantovaný kardiostimulátor, který se pohybuje v domácím prostředí pacienta, jenž se zaměřuje na rovnováhu mezi bezpečnostními mechanismy a možností nouzového přístupu lékaře. Byly analyzovány různé přístupy k šifrování, autentizaci a řízení

přístupu, přičemž zvláštní pozornost byla věnována nízkoenergetickým protokolům a jejich dopadu na výdrž baterie zařízení. V práci byly identifikovány hlavní bezpečnostní hrozby, jako jsou odposlech komunikace, neoprávněný přístup a přetížení systému.

Po operaci srdce, např. po provedení bypassů je nyní pacient dočasně připojen na nepřenosný kardiostimulátor. Pro pacienty vyžadující dlouhodobější rekonvalescenci nově vznikl požadavek na vývoj nositelného externího kardiostimulátoru s bateriovým napájením. Při návrhu komunikačního systému pro externí nositelné kardiostimulátory, které jsou napájeny z baterie, je uvažována varianta, kdy bude systém z bezpečnostních důvodů izolován od externích přístupů mimo nemocniční prostředí. Aby byla minimalizována energetická náročnost bezdrátové komunikace mezi externím kardiostimulátorem a základnovou stanicí, bude uvažován komunikační protokol, který umožňuje pouze vysílání dat směrem od kardiostimulátoru, bez možnosti jejich příjmu kardiostimulátorem. Tímto způsobem bude zajištěna ochrana externího kardiostimulátoru jako koncového zařízení před přímými kybernetickými útoky.

Pro zajištění bezpečnosti systému jako celku je proto nutné zaměřit ochranu na vnitřní přenosovou infrastrukturu nemocničního zařízení a obslužný server, který zpracovává data přenesená z externích kardiostimulátorů.

V dalších částech práce budou popsány informace potřebné k navržení bezpečného a spolehlivého bezdrátového komunikačního systému pro externí nositelné kardiostimulátory.

1.4 Bezdrátové komunikační protokoly

V dnešní době existuje mnoho norem a protokolů určených pro bezdrátové aplikace, od jednoduchých po složité. Mezi nejznámější patří Bluetooth a Wi-Fi. Bluetooth je široce používán pro nízkoenergetické aplikace, zejména v lékařství a fitness pro sledování fyzického stavu. Na druhou stranu Wi-Fi se využívá pro lokální datové sítě a vysokorychlostní připojení k internetu. V novějších verzích je efektivnější a energeticky méně náročná, což umožňuje její využití v chytrých zařízeních, včetně aplikací pro sběr dat.

Další protokoly pro bezdrátovou komunikaci, například z rodiny IEEE 802.15 [49], jsou využívány v Personal Area Networks (PAN) pro komunikaci senzorů na osobě a v blízkém okolí. Časté jsou i proprietární protokoly, které využívají ISM (Industrial, Scientific, and Medical) pásma pod 1 GHz, například pro vzdálený monitoring teploty nebo pro ovládání garážových vrat.

Bezdrátové systémy používají různé přístupové body nebo uzly k vytvoření adhoc sítí, jako jsou například Wireless Sensor Networks (WSN). Tyto sítě se skládají

z tisíců uzlů, které komunikují mezi sebou. Technologie ZigBee je vhodná pro sítě s nízkou spotřebou energie, zatímco UWB nabízí výhody v rychlosti přenosu dat, ale má omezenou vzdálenost mezi uzly. Wi-Fi je rozšířenou technologií i v náročných prostředích, jako jsou doly, ale trpí vysokou spotřebou energie a nutností dodatečné infrastruktury.

V lékařské nositelné elektronice se používají protokoly, které zajišťují spolehlivý a bezpečný přenos dat mezi zařízeními a centrálními systémy. Tyto protokoly umožňují efektivní integraci zdravotnických údajů do širších systémů péče o pacienty.

1.4.1 Radiová přenosová pásma

Radiová přenosová pásma hrají klíčovou roli v moderních implantovatelných kardiostimulátorech, což jsou zařízení používaná k individuální regulaci srdečního rytmu u pacientů s různými srdečními poruchami. Využití RF (Radiofrekvenční) technologie v těchto zařízeních nabízí několik výhod, zejména v oblasti komunikace a řízení zařízení.

Pro lékařská elektronická zařízení, která se používají k diagnostice, monitorování a léčebným účelům, jsou vyhrazena specifická rádiová frekvenční pásma. Tato pásma jsou regulována s cílem minimalizovat rušení a zajistit bezpečnost pacientů i ochranu citlivých dat.

MedRadio (Medical Device Radiocommunications Service)

MedRadio (Medical Device Radiocommunications Service) je služba vyhrazená pro bezdrátovou komunikaci mezi lékařskými zařízeními. Tento systém byl navržen tak, aby umožňoval bezpečné a efektivní používání rádiových frekvencí pro zdravotnické aplikace [38, 111].

Frekvenční pásma:

- Pásmo 401-406 MHz je určeno pro komunikaci s lékařskými implantáty a nositelnými zařízeními. Toto pásmo zahrnuje například kardiostimulátory, inzulinové pumpy a další zařízení, která slouží k monitorování nebo regulaci zdravotního stavu pacienta.
- Pásmo 413-457 MHz je další frekvenční rozsah určen v rámci MedRadio, který určen je pro různé lékařské aplikace.

MBAN (Medical Body Area Network)

MBAN (Medical Body Area Network) je typ bezdrátové sítě pracují v pásmu 2360-2400 MHz určené pro zdravotnické aplikace, kde jsou senzory a zařízení umístěny na těle pacienta nebo v jeho blízkosti. Tato síť umožňuje sběr a přenos zdravotních

dat v reálném čase, což je klíčové pro monitorování zdravotního stavu a zajištění péče[29].

ISM pásma (Industrial, Scientific, and Medical)

ISM pásma (Industrial, Scientific, and Medical) jsou frekvenční rozsahy určené pro bezdrátové aplikace v průmyslovém, vědeckém a medicínském sektoru. Tato pásma byla určena Mezinárodní telekomunikační unií (ITU) a jsou navržena pro použití s nízkou intenzitou elektromagnetického záření, což znamená, že zařízení pracující v těchto pásmech by neměla významně rušit ostatní komunikační služby[51, 52].

Použití ISM pásma je regulováno s cílem minimalizovat rušení s ostatními rádiovými službami. Zařízení pracující v těchto pásmech musí vyhovět specifickým technickým normám, které omezují jejich výkon a šířku pásma, aby se předešlo vzájemnému rušení. Také Český telekomunikační úřad (ČTU) uvádí všeobecné oprávnění k využívání rádiových kmitočtů a k provozování zařízení krátkého dosahu [110, 112], které je potřeba zohlednit při návrhu bezdrátového zařízení, naše zájmové kmitočty jsou uvedeny v Tab.1.1.

Tab. 1.1: Doporučené rádiové kmitočty dle ČTÚ pro zařízení s krátkým dosahem [110, 112].

Kmitočtové pásmo	**Maximální výkon**
433 MHz	10 mW e.r.p
863–876 MHz	25 mW e.r.p
915–921 MHz	25 mW e.r.p
2,4 GHz	25 mW e.i.r.p

Tabulka uvádí maximýlní výkonové hodnoty pro jednotlivá kmitočtová pásma, kde e.r.p. značí efektivní vyzářený výkon a e.i.r.p je pak ekvivalentní izotropně vyzářený výkon.

V Tab. 1.1 vymezených rádiových kmitočtů dle českého národního regulátora jsou zvažovány a charakterizovány následující bezdrátové technologie a to Bluetooth, Bluetooth Low Energy (BLE), Wi-Fi, Mobilní sítě, LoRa, Z-Wave, Zigbee a IQRF [22].

1.4.2 Bluetooth a Bluetooth Low Enery (BLE)

Bluetooth technologie je v současnosti rozdělena do dvou variant, které fungují ve stejném bezlicenčním ISM pásmu 2,4 GHz, ale tyto varianty nejsou vzájemně kompatibilní. Bluetooth Classic je původní standard, zaměřený hlavně na přenosy audia

a dat mezi zařízeními. Bluetooth Low Energy (BLE) je modernější verze navržená pro aplikace s velmi nízkou spotřebou energie, což je ideální pro tzv. Internet věcí (IoT - Internet of Things) a senzorové sítě. BLE podporuje i Mesh topologii a je vhodná pro lokalizační aplikace, jako je detekce vzdálenosti a směru zařízení [23].

1.4.3 Wi-Fi

Největší rozšíření doznala skupina bezdrátových protokolů Wi-Fi (Wireless Fidelity). Běžné standardy bezdrátových lokálních sítí, jako jsou 802.11b až 802.11ax, jsou široce používané v domácnostech, kancelářích a venkovních prostorech, ale nejsou ideální pro IoT zařízení kvůli vyšší spotřebě energie a omezené podpoře nízkých datových rychlostí. Proto byl vyvinut standard 802.11ah, který se zaměřuje na energeticky úspornou komunikaci potřebnou pro IoT a zařízení s nízkou přenosovou rychlostí a delší životností baterie. Na rozdíl od předchozích standardů využívá 802.11ah jiné frekvenční pásmo, specificky v oblasti pod 1 GHz, což zvyšuje jeho dosah a efektivitu pro IoT aplikace [22, 101].

1.4.4 LoRa a LoRaWAN

LoRa (Long Range) je bezdrátová technologie vyvinutá společností Semtech pro LPWAN (Low Power Wide Area Network) a řeší potřeby IoT sítí, jako je velký dosah, nízká spotřeba energie a bezpečný přenos dat. Funguje v pásmech pod 1 GHz (169 MHz, 433 MHz, 866 MHz a 915 MHz) s modulací chirp spread spectrum, což umožňuje dlouhý dosah a různé datové rychlosti. LoRa pracuje společně s protokolem LoRaWAN, který je open-source a zajišťuje správu kapacity sítě, spotřeby energie a zabezpečení. LoRaWAN využívá topologii „hvězdy hvězd“ a skládá se ze čtyř podsystémů: aplikační server, síťový server, brány a "smart"(inteligentní) objekty [22, 65].

1.4.5 Zigbee

Zigbee je bezdrátová technologie určená pro nízkoenergetické sítě s nízkou datovou propustností, vhodná pro zařízení IoT v domácnostech, průmyslu a automatizaci budov. Zigbee standardizuje protokol pro komunikaci mezi senzory a dalšími zařízeními na krátké vzdálenosti s nízkým výkonem, což umožňuje dlouhou životnost baterie. Funguje v pásmech 868 MHz, 915 MHz a 2,4 GHz, poskytuje flexibilní a škálovatelnou síť typu mesh a je ideální pro aplikace, kde je prioritou nízká spotřeba energie [30].

1.4.6 Mobilní sítě

Nejznámější technologie pro IoT využívající licencovaná pásma mobilních sítí jsou NB-IoT (Narrowband IoT) a LTE-M (LTE for Machines), obě vyvinuté v rámci standardu 3GPP. NB-IoT je navržena pro statické aplikace, jako jsou senzory a měřicí zařízení, a vyniká nízkou spotřebou energie, velkým dosahem a schopností podporovat vysokou hustotu zařízení. Naopak LTE-M je optimalizováno pro mobilní aplikace, nabízí vyšší přenosové rychlosti, nízkou latenci a podporu mobility, což jej činí ideálním pro scénáře v reálném čase, jako je sledování polohy a hlasová komunikace. Obě technologie se navzájem doplňují a pokrývají širokou škálu IoT aplikací od jednoduchých statických až po komplexní mobilní scénáře [92].

1.4.7 Z-Wave

Protokol Z-Wave představuje interoperabilní bezdrátovou komunikační technologii. Tento protokol byl navržen primárně pro řízení, monitorování a snímání stavu zařízení v obytných a komerčních prostředích. Díky svým vlastnostem je Z-Wave široce využíván v aplikacích inteligentního bydlení a systémů automatizace budov. Z-Wave operuje v pásmu pod 1 GHz, což zajišťuje jeho vysokou odolnost vůči rušení způsobenému jinými technologiemi využívajícími pásmo 2,4 GHz, jako jsou Wi-Fi, Bluetooth nebo ZigBee [105].

1.4.8 IQRF

Technologie IQRF je bezdrátová komunikační platforma, která je navržena pro nízkoenergetické a robustní přenosy dat v pásmu ISM na frekvencích 868 MHz a 916 MHz. Tato technologie je primárně určena pro aplikace v oblasti IoT, průmyslové automatizace a inteligentních měst. IQRF umožňuje obousměrnou komunikaci s nízkou latencí a podporuje topologie sítí typu Mesh [53].

Srovnání jednotlivých technologií v závislosti na jejich dosahu použitelnosti a dalších parametrů je přehledně uvedeno v Tab. 1.2. Hodnoty pro dosah a maximální přenosovou rychlost jsou uvedeny pro přímou viditelnost, v reálných podmínkách může být významně nižší.

1.4.9 Výběr vhodné bezdrátové technologie

Byla provedena analýza přenosových pásem a analýza existujících komunikačních protokolů, které tyto pásma využívají. Přenosové pásmo 2,4 GHz je aktuálně velmi využíváno a bylo by proto relativně velké riziko rušení komunikace kardiostimulátoru jiným typem provozu.

Tab. 1.2: Porovnání bezdrátových komunikačních technologií.

Typ	**Dosah**	**Frekvence**	**Přenosová rychlost**	**Spotřeba energie**	**Typické použití**	**Síťová topologie**
Bluetooth	10–100 m	2,4 GHz	1–3 Mbit/s	Střední	Audio zařízení, periferie	Point-to-point, point-to-multipoint
BLE	10–100 m	2,4 GHz	125 kbit/s – 2 Mbit/s	Nízká	IoT zařízení, senzory, chytré hodinky	Point-to-point, broadcast
Wi-Fi	až 100 m	2,4/5/6 GHz	až 46 Gb/s	Vysoká	Domácí sítě, internet, streamování	Star (hvězda)
LoRa	2–15 km	868 MHz (EU)	0,3-50 kbit/s	Velmi nízká	IoT, senzorové sítě, smart city	Star-of-stars
Mobilní sítě	Globální	Různé	100 kbit/s – 20 Gb/s	Vysoká	Mobilní telefony, data	Cellular
Z-Wave	až 30 m	868,42 MHz (EU)	100 kbit/s	Nízká	Domácí automatizace	Mesh
Zigbee	10–100 m	2,4 GHz	250 kbit/s	Nízká	Domácí automatizace, chytré osvětlení	Mesh
IQRF	až 500 m	868 MHz (EU)	19,2 kbit/s	Velmi nízká	Průmyslové aplikace, smart city	Mesh

Po důkladném zvážení vlastností jednotlivých pásem a protokolů bylo rozhodnuto použít subgigahertzové ISM pásmo s generálním povolením k provozu. Existující protokoly pracující v tomto pásmu, jako např. IQRF, Z-Wave či LoRaWAN, se ukázaly jako nepříliš vhodné zejména z důvodu velké spotřeby energie.

Na trhu existuje široká škála radiofrekvenčních transponderů, které zajišťují základní vysílání a příjem datových rámců bez nutnosti používat konkrétní komunikační protokol. Jako nejvhodnější řešení se tak jeví vývoj dedikovaného komunikačního protokolu v subgigahertzovém ISM pásmu.

1.5 Modelování a simulace datového provozu

Modelování a simulace datového provozu je důležitý proces pro analýzu a optimalizaci přenosu dat v sítích. Tento proces zahrnuje vytvoření modelu sítě, který simuluje chování datového provozu a pomáhá predikovat zatížení sítě, identifikovat možné problémy a optimalizovat její výkon. Modelování a simulace datového provozu umožňuje navrhnout efektivnější a spolehlivější sítě, což je klíčové pro moderní digitální infrastrukturu.

Matematické základy

Pro modelování datového provozu lze využít matematické metody, jako je pravděpodobnostní modelování, teorie front, analytické modely propustnosti a diferenciální rovnice.

- **Pravděpodobnost a statistika:** Pravděpodobnostní modely (např. Poissonův proces) odhadují náhodný příchod paketů a ztrátovost, což pomáhá předpovídat zátěž sítě.
- **Teorie front:** Modely M/M/1 nebo M/M/c určují pravděpodobnost zpoždění a ztrát paketů při různém zatížení sítě.
- **Propustnost sítě:** Výpočet propustnosti a maximální kapacity kanálu (např. Shannonův teorém) odhaduje maximální přenosovou rychlost a efektivitu.
- **Diferenciální rovnice:** Modelují dynamiku toku dat a jsou využívány při řízení přenosové kapacity (např. v TCP).

Tyto postupy pomáhají navrhnout efektivnější síťové topologie, optimalizovat zátěž a simulovat krizové scénáře, což zlepšuje stabilitu a výkon sítě.

Simulační nástroje

Níže jsou uvedeny komerčně dostupné simulační nástroje, které mohou být využity pro modelování jednoduchých i složitých síťových topologií.

- **GNS3**
  Nástroj GNS3 představuje platformu pro simulaci složitých sítí, která se používá jak pro výuku, tak pro testování síťové architektury a konfigurací v prostředí, které emuluje reálné nasazení. S GNS3 lze modelovat provoz, testovat směrovací protokoly a přenosy a provádět různé síťové konfigurace, a to bez rizika narušení produkční sítě. Nástroj využívá skutečné obrazy síťových operačních systémů (např. Cisco IOS, Juniper JunOS), což umožňuje přesné modelování chování síťových zařízení [40].

- **NS-3 (Network Simulator 3)**
  NS-3 je moderní simulační nástroj pro analýzy a simulace datového provozu nejen v IP sítích. NS-3 podporuje tvorbu simulačních modelů dostatečně realistických pro použití jako reálný síťový emulátor, propojitelný s reálnými sítěmi a využívající existující protokolové implementace. Podporuje simulace komplexních síťových topologií, protokolů a technologií, včetně bezdrátových sítí, mobilních sítí, senzorových sítí a IoT [72].

- **Castalia**
  Castalia je simulátor pro bezdrátové senzorové sítě (WSN), sítě v oblasti těla a sítě embedded zařízeních s nízkou spotřebou. Je založen na platformě OMNeT++ a mohou jej používat výzkumní pracovníci a vývojáři, kteří chtějí testovat své distribuované algoritmy a/nebo protokoly v realistických modelech bezdrátových kanálů s realistickým chováním uzlů, zejména pokud jde o přístup k rádiové síti[25].

- **Matlab**
  MATLAB je výkonný nástroj pro simulace a analýzy, který je často využíván i pro modelování datového provozu v sítích. MATLAB nabízí širokou škálu funkcí a knihoven, které podporují výpočetní a analytické metody vhodné pro různé scénáře v síťovém provozu, včetně statistického modelování, teorie front a simulace přenosu dat [106].

- **R Studio**
  R Studio je oblíbený nástroj pro statistické výpočty a analýzy dat, který lze využít také pro simulace a modelování datového provozu. R studio nabízí širokou škálu balíčků a funkcí, které usnadňují práci s pravděpodobnostními modely, teorií front a simulací přenosu dat [76].

Přestože uvedené nástroje pokrývají většinu běžných potřeb a scénářů využití, objevují se nové nástroje v souvislosti s vývojem nových technologií, které reagují na měnící se potřeby aplikací, ale i uživatelů. Pro konkrétní aplikace je důležité důkladně analyzovat požadavky a zvážit dostupné alternativy, přičemž je vhodné kombinovat různé nástroje dle potřeby, současně sledovat nové trendy a možnosti optimalizace řešení.

1.5.1 Matematické nástroje použité pro simulace

V této kapitole připomeneme a definujeme matematický a statistický aparát používaný pro konstrukci simulačních modelů.

Při řešení práce byly vytvářeny modely vysílání dat z nositelných externích kardiostimulátorů na základě statistických vlastností chování lidského srdce, zejména nominální tepové frekvence a její variability, tzv. HRV.

Nominální tepovou frekvenci člověka (když odmyslíme závislost na aktuální fyzické zátěži) je možné popsat pomocí rozdělení pravděpodobnosti spojitého typu. Hodnota tepové frekvence má biologické omezení jak z pohledu minimální, tak i maximální hodnoty.

Nominální tepovou frekvenci je možné popsat pomocí tzv. useknutého logaritmicko-normálního nebo useknutého exponenciálního rozdělení pravděpodobnosti. HRV má přibližně normální rozdělení pravděpodobnosti. Vůči okamžiku prvního měření je okamžik úderu lidského srdce posunut o náhodnou hodnotu z intervalu 0 - čas mezi údery srdce v klidovém stavu. Tento časový interval je možné vyjádřit pomocí rovnoměrného rozdělení pravděpodobnosti. Použité rozdělení pravděpodobnosti jsou připomenuta v následující podkapitole.

Zde připomeneme nejdůležitější pojmy a vztahy z teorie pravděpodobnosti a matematické statistiky. Základním pojmem teorie pravděpodobnosti je náhodná veličina. Náhodná veličina je náhodná proměnná, např. X, která nabývá číselných hodnot a má proto smysl se ptát na pravděpodobnost vzniku náhodného jevu $X = a$, případně náhodného jevu $X \leq b$.

Pravděpodobnostní chování náhodné veličiny X můžeme popsat pomocí její distribuční funkce. Distribuční funkci náhodné veličiny X nazýváme reálnou funkci

$$F(x) = P(X \leq x)$$

definovanou na intervalu $(-\infty, \infty)$, která vyjadřuje pravděpodobnost, že náhodná veličina X nabývá hodnotu menší nebo rovnou x.

Distribuční funkce $F(x)$ náhodné veličiny X má následující vlastnosti:

1. $F(x)$ je neklesající,
2. $F(x)$ je zleva spojitá,
3. $\lim_{x\to-\infty} F(x) = 0$, $\lim_{x\to\infty} F(x) = 1$,
4. $0 \leq F(x) \leq 1$ pro všechna $x \in (-\infty, \infty)$,

viz např. [62].

Řekneme, že náhodná veličina X má diskrétní rozdělení pravděpodobnosti, jestliže nabývá pouze konečného nebo spočetného počtu hodnot $x_1, x_2, \ldots$ tak, že

$$\sum_{i=1}^{\infty} P(X = x_i) = 1.$$

Chování diskrétní náhodné veličiny X můžeme popsat pomocí její pravděpodobnostní funkce p, která vyjadřuje pravděpodobnost, že náhodná veličina X nabývá hodnoty x :

$$p(x) = P(X = x).$$

Řekneme, že náhodná veličina X má spojité rozdělení pravděpodobnosti, jestliže existuje nezáporná integrovatelná funkce $f(x)$ definovaná na množině $\mathbb{R}$, taková, že pro všechna x platí

$$P(X \leq x) = F(x) = \int_{-\infty}^{x} f(t)\,dt.$$

Funkci $f(x)$ nazýváme hustota pravděpodobnosti náhodné veličiny X.

Pro popis vlastností náhodné veličiny potřebujeme charakterizovat její polohu a variabilitu. Pro popis polohy používáme nejčastěji střední hodnotu, případně medián a dále kvantilové charakteristiky. Pro popis variability náhodné veličiny používáme rozptyl, případně směrodatnou odchylku.

Střední hodnotou náhodné veličiny X definujeme vztahem

$$E(X) = \sum_{i=1}^{\infty} x_i p(x_i),$$

pro diskrétní náhodné veličiny a

$$E(X) = \int_{-\infty}^{\infty} x f(x)\,dx$$

pro spojité náhodné veličiny.

Mediánem náhodné veličiny X rozumíme takové číslo m, pro které platí

$$P(X \leq m) \geq \frac{1}{2} \quad \text{a} \quad P(X \geq m) \geq \frac{1}{2},$$

tj. náhodná veličina X nabývá zhruba stejně často hodnot nižších i vyšších než m.

Kvantilem p% náhodné veličiny X rozumíme nejmenší takové číslo x_p, pro které platí

$$F(x_p) \geq p/100.$$

Rozptyl náhodné veličiny X definujeme vztahem

$$D(X) = E[(X - E(X))^2].$$

Odmocninu rozptylu nazýváme směrodatnou odchylkou náhodné veličiny X a značíme

$$\sigma(X) = \sqrt{D(X)}.$$

Definice těchto základních pojmů jsou převzaty z [108].

Použitá rozdělení pravděpodobností

V této kapitole připomeneme vlastnosti použitých rozdělení pravděpodobnosti. Nejedná se o nové výsledky, ale o drobné modifikace stávajících postupů u modelů, které potřebujeme k modelování chování reálných uživatelů. Každé z použitých rozdělení pravděpodobnosti je možné charakterizovat pomocí distribuční funkce, hustoty rozdělení pravděpodobnosti a tzv. momentových číselných charakteristik.

Pro konstrukci modelů potřebujeme pracovat s několika typy rozdělení pravděpodobnosti:

- Logaritmicko-normální rozdělení. Toto rozdělení pravděpodobnosti nejlépe popisuje základní tepovou frekvenci pacientů.
- Normální (Gaussovo) rozdělení. Tímto rozdělením modelujeme variabilitu tepové frekvence pacienta.
- Rovnoměrné rozdělení. Pomocí tohoto rozdělení pravděpodobnosti modelujeme dobu od začátku měření do prvního pulzu srdce nebo stimulačního impulzu kardiostimulátoru.
- Poissonovo rozdělení. Toto rozdělení pravděpodobnosti použijeme pro popis počtu kolizí ve vysílání.
- Exponenciální rozdělení. Tímto rozdělením pravděpodobnosti budeme modelovat čas mezi výskytem kolizí.

Většina zde připomínaných pojmů a vlastností je převzata z [109].

Logaritmicko-normální rozdělení pravděpodobnosti

Logaritmicko-normální rozdělení pravděpodobnosti je rozdělení náhodné proměnné, jejíž logaritmus má normální (Gaussovo) rozdělení. Pokud tedy náhodná proměnná X má logaritmicko-normální rozdělení, pak proměnná $Y = \ln(X)$ bude mít normální rozdělení.

Toto rozdělení je užitečné pro modelování náhodných proměnných, které jsou vždy kladné a mohou nabývat velmi širokého spektra hodnot. Je typické pro situace, kde jsou hodnoty dat asymetrické a existují výrazné extrémní hodnoty.

Hustota pravděpodobnosti $f(x)$ logaritmicko-normálního rozdělení je dána vztahem:

$$f(x) = \frac{1}{x\sigma\sqrt{2\pi}} \exp\left(-\frac{(\ln(x) - \mu)^2}{2\sigma^2}\right),$$

kde:

- $x > 0$ je hodnota náhodné proměnné,
- μ je střední hodnota logaritmu náhodné proměnné,
- σ je směrodatná odchylka logaritmu náhodné proměnné.

Logaritmicko-normální rozdělení je asymetrické a má delší "ocas" na pravé straně, což naznačuje možnost výskytu extrémně velkých hodnot. Proměnná X je vždy kladná, což odpovídá základní tepové frekvenci [36, 54]. Číselné charakteristiky:

$$E(X) = e^{(\mu+\sigma^2/2)},$$

$$D(X) = (e^{\sigma^2} - 1)e^{2\mu+\sigma^2},$$

$$\text{medián } x_{0.5} = e^{\mu}.$$

Normální (Gaussovo) rozdělení pravděpodobnosti

Normální rozdělení pravděpodobnosti je asi nejčastěji používané rozdělení. Má řadu praktických aplikací a stejně mnoho významných charakteristických vlastností.

Hustota pravděpodobnosti $f(x)$ normálního rozdělení je dána vztahem:

$$f(x) = \frac{1}{x\sigma\sqrt{2\pi}} \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right),$$

kde:

- $x > 0$ je hodnota náhodné proměnné,
- μ je střední hodnota náhodné proměnné,
- σ je směrodatná odchylka náhodné proměnné.

Číselné charakteristiky:

$$E(X) = \mu,$$

$$D(X) = \sigma^2.$$

Rovnoměrné rozdělení pravděpodobnosti

Náhodná veličina s rovnoměrným rozdělením $R(a, b)$, kde a, b jsou reálná čísla a $a < b$, má hustotu pravděpodobnosti

$$f(x) = \begin{cases} \frac{1}{b-a} & \text{pro } x \in \langle a, b\rangle, \\ 0 & \text{pro } x \notin \langle a, b\rangle. \end{cases}$$

Číselné charakteristiky:

$$E(X) = x_{0.5} = \frac{a+b}{2},$$

$$D(X) = \frac{(b-a)^2}{12}.$$

Poissonovo rozdělení pravděpodobnosti

Náhodná veličina s Poissonovým rozdělením $Po(\lambda)$, kde λ je reálné číslo, $\lambda > 0$, má pravděpodobnostní funkci

$$p(x) = \frac{\lambda^x}{x!} e^{-\lambda}, \quad x = 0, 1, 2, \ldots$$

Náhodná veličina s Poissonovým rozdělením má následující číselné charakteristiky:

$$E(X) = \lambda,$$
$$D(X) = \lambda.$$

Exponenciální rozdělení pravděpodobnosti

Exponenciální rozdělení pravděpodobnosti zpravidla vyjadřuje čas mezi řídkými událostmi, např. výskytem kolizí ve vysílání [26], [27]. Náhodná veličina s exponenciálním rozdělením $Exp(\lambda)$, kde λ je reálné číslo, $\lambda > 0$, má hustotu pravděpodobnosti

$$f(x) = \begin{cases} \lambda e^{-\lambda x} & \text{pro } x \geq 0, \\ 0 & \text{pro } x < 0. \end{cases}$$

Číselné charakteristiky:

$$E(X) = \frac{1}{\lambda},$$
$$D(X) = \frac{1}{\lambda^2}.$$

Shrnutí

Všechny výše popsané rozdělení pravděpodobnosti budou použity pro konstrukci simulačního modelu, kde jednotlivé aspekty datových přenosů mají různá rozdělení pravděpodobnosti, např.:

- Nominální tepovou frekvenci pacientů modelujeme pomocí logaritmicko-normálního rozdělení pravděpodobnosti,
- časový posun prvního tepu srdce pacienta od počátečního času simulace modelujeme pomocí rovnoměrného rozdělení pravděpodobnosti,
- variability tepové frekvence člověka modelujeme pomocí normálního rozdělení pravděpodobnosti.

Zde připomenuté vlastnosti a číselné charakteristiky klíčových rozdělení pravděpodobností budou dále využity pro konstrukci simulačního modelu komunikačního protokolu pro nositelné externí kardiostimulátory.

2 Kódy pro bezpečný přenos a ukládání dat

V oblasti zabezpečení dat při jejich přenosu a ukládání představují klíčový nástroj detekční a samoopravné kódy. Tyto kódy slouží k detekci a opravě chyb, které vznikají vlivem rušení, šumu nebo jiných poruch v komunikačních kanálech či úložných médiích. Jejich implementace umožňuje zvýšit spolehlivost systémů pracujících s daty, a to při zachování vysoké efektivity přenosu [113].

- **Detekční kódy** jsou navrženy tak, aby umožnily identifikaci chyb vzniklých během přenosu nebo ukládání dat. Tyto kódy sice neumožňují automatickou opravu chyb, ale poskytují informaci o tom, že došlo k jejich výskytu. Jsou proto využívány tam, kde je klíčová detekce poruch a případná oprava chyb se řeší opakováním přenosu. Nejznámějším příkladem detekčních kódů, které jsou využívány v přenosových systémech je CRC (Cyclic Redundancy Check).
- **Samoopravné kódy** jsou rozšířením detekčních kódů, které umožňují nejen detekovat, ale také opravit chyby vzniklé během přenosu či ukládání dat. Tímto způsobem zvyšují spolehlivost přenosových systémů a umožňují minimalizovat nutnost opakování přenosu. Příkladem samoopravných kódů mohou být Bose–Chaudhuri–Hocquenghem kódy (BCH) kódy, Reed-Solomonovy kódy a Turbo kódy.

2.1 Algebraické základy samoopravných kódů

Pro konstrukci detekčních i samoopravných kódů využíváme řadu poznatků z algebry. Matematický aparát algebry definuje řadu algebraických struktur složených z množiny prvků a jedné či více operací nad těmito prvky od grupoidu po těleso. Algebra jako matematická disciplína obecně zkoumá závislosti významných vlastností matematických operací a definuje řadu algebraických struktur, které jsou z pohledu vlastností operací nad prvky příslušné množiny významné. Na tomto místě připomeneme několik klíčových algebraických struktur:

- Grupoid
- Pologrupa
- Grupa
- Okruh
- Obor integrity
- Těleso

Grupoid

Grupoid je nejjednodušší algebraická struktura, jejíž význam je především teoretický. Pologrupa je nejjednodušší algebraická struktura. Skládá se z množiny prvků M a binární operace $\oplus$ definované nad prvky této množiny. Na vlastnosti množiny M nejsou kladeny žádné specifické požadavky vyjma uzavřenosti vůči operaci $\oplus$, tj. výsledek operace $\oplus$ provedené nad prvky množiny M musí být prvkem množiny M.

Pologrupa

Nejjednodušší vlastnost, kterou můžeme požadovat od operace $\oplus$ je tzv. asociativita. Říkáme, že operace $\oplus$ na množině M je asociativní, jestliže pro každé tři prvky $x, y, z \in M$ platí $(x \oplus y) \oplus z = x \oplus (y \oplus z)$. Tj. nezáleží na pořadí provádění operací. Grupoid s touto vlastností se nazývá pologrupa. Pologrupa, ve které existuje tzv. neutrální prvek, tj. prvek $e \in M$ takový, že pro každý prvek $x \in M$ platí $e \oplus x = x \oplus e = x$, se nazývá monoid.

Grupa

Pologrupa $(M, \oplus)$ s neutrálním prvkem e, ve které pro každý prvek $x \in M$ existuje tzv. inverzní prvek, tj. prvek $x^{-1} \in M$ takový, že $x \oplus x^{-1} = x^{-1} \oplus x = e$, se nazývá grupa. Je-li navíc operace $\oplus$ komutativní, tj. pro každé dva prvky $x, y \in M$ platí $x \oplus y = y \oplus x$, nazývá se grupa $(M, \oplus)$ komutativní, nebo též Abelovská grupa.

Okruh

O něco složitější jsou algebraické struktury se dvěma operacemi. Původně byly rozvíjeny zejména pro popis vlastností číselných množin a pro zkoumání vlastností polynomů, zejména z pohledu možnosti nalezení kořenů polynomu pomocí běžných algebraických operací.

Nejjednodušší algebraická struktura se dvěma binárními operacemi je okruh. Okruh je množina prvků spolu se dvěma operacemi $(M, \oplus, \otimes)$ těchto vlastností:

- $(M, \oplus)$ je komutativní grupa
- $(M, \otimes)$ je pologrupa s neutrálním prvkem
- platí distributivní zákony: pro každé tři prvky $x, y, z \in M$ platí $x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$

Operaci $\oplus$ obvykle nazýváme sčítání a neutrální prvek grupy $(M, \oplus)$ značíme 0. Operaci $\otimes$ obvykle nazýváme násobení a neutrální prvek pologrupy $(M, \times)$ značíme 1.

Okruh $(M, \oplus, \otimes)$ se nazývá triviální, pokud množina M obsahuje pouze jeden prvek. Dá se ukázat, že okruh $(M, \oplus, \otimes)$ je triviální právě tehdy, když v něm pro neutrální prvky 0 a 1 platí $0 = 1$.

Obor integrity

Okruh se nazývá komutativní, je-li pologrupa $(M, \otimes)$ komutativní. Prvky $a, b \in M$ takové, že $a \neq 0, b \neq 0$ a zároveň $a \otimes b = 0$ se nazývají dělitelné nuly.

Netriviální komutativní okruh $(M, \oplus, \otimes)$, který nemá dělitele nuly, se nazývá obor integrity.

Důležitou vlastností oboru integrity je možnost definovat dělitelnost. Říkáme, že prvek $a \in M$ oboru integrity M dělí prvek $b \in M$, jestliže existuje prvek $c \in M$ takový, že $a \otimes c = b$.

Množina celých čísel $\mathbb{Z}$ s obvyklým sčítáním a násobením je oborem integrity.

Těleso

Těleso je komutativní okruh s alespoň dvěma prvky, ve kterém pro každý prvek $x \in M$ existuje prvek $x^{-1} \in M$ takový, že platí $x \otimes x^{-1} = 1$. Každé komutativní těleso je oborem integrity.

Těleso nad nekonečnou množinou M může sloužit pro porozumění vlastnostem množiny reálných a komplexních čísel, které tvoří těleso vzhledem k obvyklým operacím sčítání a násobení.

Pro potřeby konstrukce detekčních a samoopravných kódů využíváme tělesa s konečnou množinou prvků. Lze dokázat, že pokud je těleso $(T, \oplus, \otimes)$ konečné, je počet prvků množiny T roven mocnině prvočísla ($|T| = p^n$, kde p je prvočíslo a n je přirozené číslo) [41].

Konečné těleso bývá na počet francouzského matematika Évarista Galoise obvykle nazýváno Galoisovo těleso. Galoisovo těleso o p^n prvcích značíme $GF(p^n)$.

Nechť $(T, +, \cdot, 0, 1)$ je konečné těleso. Nejmenší přirozené $r > 0$ takové, že

$$\underbrace{1 + 1 + \cdots + 1}_{r\text{-krát}} = 0,$$

se nazývá charakteristika tělesa T ($\mathrm{char}(T)$).

$$\mathrm{char}(GF(p^k)) = p$$

Každé konečné těleso T má $\mathrm{char}(T) = p$ pro nějaké prvočíslo p.

Okruh zbytkových tříd

Zbytková třída modulo n je množina všech celých čísel, které po dělení n dávají stejný zbytek.

Množina zbytkových tříd modulo n tvoří okruch vzhledem k obvyklým operacím sčítání a násobení. Tento oktuh značíme $(\mathbb{Z}_n)$. Lze dokázat, že $(\mathbb{Z}_n)$ je obor integrity, právě když n je prvočíslo.

Polynomy nad $\mathbb{Z}_p$

Okruh polynomů nad oborem integrity je zase oborem integrity [42].

Polynom nad $\mathbb{Z}_p$ v proměnné x je výraz tvaru:

$$a(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0$$

kde koeficienty $a_0, a_1, \ldots, a_k$ jsou ze $\mathbb{Z}_p$.
Množinu všech polynomů nad $\mathbb{Z}_p$ v proměnné x značíme $\mathbb{Z}_p[x]$.

Stupeň polynomu $a(x)$ je největší k takové, že $a_k \neq 0$. Značí se $\mathrm{st}(a(x))$.

Polynom $q(x)$ stupně $k \geq 1$ se nazývá ireducibilní nad $\mathbb{Z}_p$, jestliže se nedá napsat jako součin dvou polynomů nižšího stupně než k.

Prvek $c \in \mathbb{Z}_p$ je kořen polynomu $q(x) \in \mathbb{Z}_p[x]$, jestliže platí $q(c) = 0$ v $\mathbb{Z}_p$.

Prvek $c \in \mathbb{Z}_p$ je kořen polynomu $q(x)$ právě, když polynom $(x - c)$ dělí polynom $q(x)$.

Polynom $q(x)$ stupně $\mathrm{st}(q) \leq 3$ je ireducibilní nad $\mathbb{Z}_p$ právě tehdy, když nemá kořen v $\mathbb{Z}_p$.

Polynomy nad $\mathbb{Z}_p$ jsou základem konstrukce mnohých detekčních a samoopravných kódů. Další kapitola bude zaměřena na BCH kódy, které budou využity pro zabezpečení dat navrženého komunikačního protokolu.

2.2 Bose–Chaudhuri–Hocquenghem kódy

Tato kapitola se zaměřuje na popis BCH kódů, jejich vlastnosti a využití v současných komunikačních zařízeních.

Bose–Chaudhuri–Hocquenghemovy kódy, známé pod zkratkou BCH kódy, jsou pojmenovány podle svých objevitelů. Jedná se o lineární blokové cyklické kódy, které rozšiřují možnosti Hammingových kódů tím, že umožňují opravovat více chyb. BCH kódy byly nezávisle objeveny A. Hocquenghemem v roce 1959 a R. C. Bosem a D. K. Chaudhurim v roce 1960 [63]. Cyklická struktura těchto kódů byla následně dokázána W. W. Petersonem v roce 1960.

Nejjednodušší formou těchto kódů jsou binární BCH kódy, které lze snadno implementovat v digitálních zařízeních. Jednou z jejich hlavních výhod je velká flexibilita v nastavení parametrů, což umožňuje dobrý kompromis mezi délkou informačního slova, počtem opravovaných chyb a složitostí dekódovacích metod [18]. První dekódovací algoritmus navrhl W. W. Peterson v roce 1960. Následně byly vyvinuty další efektivní dekódovací algoritmy, například od Berlekampa, Chiena, Forneyho a Masseyho [63].

Speciálním případem BCH kódů jsou Reed–Solomonovy (RS) kódy. Ty jsou obzvláště významné, protože umožňují konstrukci velmi účinných kódů pracujících nad binárními poli [18].

2.3 Použití BCH kódů v komunikačních a datových systémech

BCH kódy jsou korekční kódy široce používané k zajištění spolehlivosti a bezpečnosti dat během jejich přenosu nebo ukládání. Tyto kódy umožňují detekci a opravu chyb, které vznikají při přenosu dat přes komunikační kanály nebo při ukládání na paměťová média, čímž se stávají klíčovým prvkem v systémech vyžadujících vysokou spolehlivost přenosu.

BCH kódy zahrnují i Reed–Solomonovy kódy, které chrání data na úrovni celých symbolů (například bajtů), což je činí velmi efektivními v případech, kdy je třeba chránit data před sekvenčními chybami. Typické aplikace BCH kódů zahrnují:

- **Optická média**: CD, DVD a Blu-ray disky, kde BCH kódy zajišťují integritu uložených dat a umožňují jejich načtení i při drobném poškození média.
- **Disková pole RAID 6**: BCH kódy se zde používají ke zvýšení spolehlivosti ukládání dat a k ochraně proti selhání více disků současně.
- **Telekomunikační zařízení**: V zařízeních, jako jsou xDSL modemy, BCH kódy pomáhají zajistit spolehlivý přenos dat i v podmínkách šumu a dalších forem rušení.
- **Satelitní komunikace a digitální televize**: BCH kódy jsou součástí standardu DVB-S2 a chrání data přenášená satelitním signálem, což zajišťuje vysokou kvalitu obrazu a zvuku i za nepříznivých podmínek.
- **Mobilní komunikace**: BCH kódy chrání data při přenosu mezi mobilními zařízeními a zajišťují jejich bezchybné doručení i přes možné rušení a odrazy signálu.
- **Videokonference a streaming**: Kódy jsou součástí doporučení ITU-T H.261 pro kódování videa a chrání data přenášená při videokonferencích nebo online streamování.

BCH kódy tak hrají klíčovou roli v moderních technologiích, kde je kritická spolehlivost přenosu a uchování informací.

2.3.1 Využití BCH kódů pro zlepšení poměru signálu a šumu a bitové chybovosti

V moderních komunikačních systémech jsou BCH kódy široce využívány pro zlepšení výkonnosti přenosu dat, zejména v prostředích s proměnlivým signálem a šumem. Využití BCH kódů může výrazně zlepšit poměr signálu k šumu (SNR) a snížit bitovou chybovost (BER), což umožňuje snížit požadovaný vysílací výkon při zachování požadované kvality přenosu. Studie [37] analyzuje vliv BCH kódů na BER v prostředích s různými hodnotami SNR a ukazuje, že BCH kódy dokážou účinně opravovat chyby způsobené šumem, což vede ke zlepšení efektivního SNR. Podobné závěry jsou uvedeny v článku [64], který srovnává BCH a Reed-Solomon kódy a dochází k závěru, že BCH kódy dosahují výrazně nižší hodnoty BER než RS kódy, což je činí vhodnějšími pro bezdrátové systémy vystavené šumu. Oba články naznačují, že zlepšení BER dosažené BCH kódy umožňuje efektivně snížit požadavky na vysílací výkon, bez zhoršení kvality přenosu. V článku [75] autoři zkoumají adaptivní nastavení BCH kódů pro WBAN sítě dle standardu IEEE 802.15.6, kde adaptivní kódování umožňuje optimalizaci přenosu podle úrovně SNR každého uzlu, čímž se zajišťuje spolehlivý přenos dat i v prostředích s proměnlivým šumem.

Celkově lze tedy konstatovat, že využití BCH kódů pro zlepšení SNR a BER umožňuje optimalizovat výkonnost přenosu při nižším vysílacím výkonu, což je výhodné v bezdrátových systémech a aplikacích s omezenou dostupností energie. Proto se v další části zaměříme na tento typ kódování.

2.4 Systémové začlenění BCH kódů a význam jednotlivých pojmů

BCH kódy jsou zařazeny do skupiny lineárních blokových cyklických kódů, které pracují s binárními daty a slouží jako účinné zabezpečovací mechanismy v komunikačních systémech. Pro snazší pochopení jejich vlastností jsou proto dále uvedeny základní charakteristiky lineárních blokových cyklických kódů. Informace vycházejí zejména z odborných publikací [39, 73].

Blokové kódy

Blokové kódy jsou definovány přesným rozdělením informačních a zabezpečovacích bitů v kódové kombinaci, jak je uvedeno v [73]. Každá kódová kombinace systema-

tického kódu délky n obsahuje k informačních bitů a $r = n - k$ zabezpečovacích bitů. Tento typ kódu je označován jako (n, k) kód, přičemž vždy platí nerovnost $n > k$. Zabezpečovací bity jsou přidávány za účelem detekce a případné opravy chyb, ke kterým může dojít během přenosu dat. Blokové kódy nacházejí uplatnění zejména tam, *kde je požadována pevná délka přenášených datových rámců.*

Lineární kódy

Kódové kombinace v případě lineárních kódů mohou být generovány jako lineární kombinace jiných kódových slov, což vyplývá z aplikace principů lineární algebry. Tyto kódy jsou specifikovány generující maticí G, která má k řádků a n sloupců. Každý řádek matice G představuje lineárně nezávislou kombinaci, která umožňuje efektivní generování kódových kombinací. Lineární struktura těchto kódů přispívá k jednoduchosti algoritmů pro jejich dekódování a analýzu. Využití lineárních kódů je běžné v systémech, *kde je důležitá výpočetní efektivita.*

Cyklické kódy

Cyklické kódy představují specifický podtyp lineárních (n, k) kódů, u nichž je generující matice g tvořena řádky, které vznikají cyklickým posunutím jednoho základního řádku. Tento druh kódů je definován generujícím polynomem $g(x)$, jehož řád určuje schopnost detekce a opravy chyb. Počet zabezpečovacích bitů $r = n - k$ je přímo závislý na stupni tohoto polynomu. V případě cyklických kódů délky n je prvních k bitů určeno pro nezabezpečená data, zatímco zbývajících r bitů představuje zabezpečovací informace.

Výhodou cyklických kódů je jejich snadná implementace pomocí posuvných registrů s lineární zpětnou vazbou, což zjednodušuje proces kódování i dekódování. Díky těmto vlastnostem jsou cyklické kódy hojně využívány v aplikacích, *kde je požadována robustní detekce a oprava chyb*, například v oblasti bezdrátových komunikací nebo ukládání dat.

2.4.1 Binární BCH kódy

V této kapitole jsou popsány základní vlastnosti binárních BCH kódů. Při jejich návrhu je třeba sestavit vytvářecí polynom $g(x)$, jehož konstrukce vychází z Bose-Chaudhuriho teorému, jak uvádí [63].

Návrh vytvářecího polynomu začíná volbou primitivního polynomu a sestavením Galoisova tělesa $GF(q^m)$. Na základě tohoto tělesa jsou určeny minimální polynomy

$m_j(x)$ pro kořeny α^j, kde $j = 1, 2, \ldots, 2t$ a α značí symbol Galoisova tělesa. Vytvářecí polynom je následně definován jako nejmenší společný násobek (LCM) těchto minimálních polynomů, což je vyjádřeno následující rovnicí:

$$g(x) = LCM[m_1(x) + m_2(x) + \cdots + m_{2t-1}(x)]. \tag{2.1}$$

Binární BCH kódy jsou dále charakterizovány třemi základními parametry, které jsou uvedeny níže [63]:

Bloková délka n je dána rovnicí:

$$n = 2^m - 1, \tag{2.2}$$

kde m představuje stupeň použitého primitivního polynomu. Bloková délka určuje celkový počet bitů v jednom kódovém slově.

Počet informačních bitů v kódovém slově:

$$k \geq n - mt, \tag{2.3}$$

kde t označuje počet chyb, které mohou být detekovány a opraveny. Hodnota k udává délku nezabezpečené části kódového slova.

Minimální vzdálenost d_{min} je stanovena vztahem:

$$d_{min} \geq 2t + 1. \tag{2.4}$$

Tento parametr udává schopnost kódu detekovat a opravovat chyby – větší minimální vzdálenost znamená vyšší odolnost proti chybám.

Důležitým parametrem každého kódu je také informační rychlost kódu, která je definována jako poměr počtu informačních bitů k k celkové délce kódového slova n. Tento parametr je vyjádřen následující rovnicí:

$$R = \frac{k}{n}. \tag{2.5}$$

Informační rychlost kódu R udává efektivitu využití přenosového kanálu, přičemž vyšší hodnota R značí menší režii zabezpečení, ale zároveň i nižší schopnost detekce a opravy chyb.

V příloze A jsou uvedeny existující binární BCH kódy pro vybrané blokové délky $n = 2^m - 1$, konkrétně $n = 63, 127, 255$. Tyto hodnoty představují standardní parametry často používané při návrhu komunikačních systémů.

Pro využití BCH kódů při návrhu komunikačního systému je nutné určit počet informačních bitů k, které je potřeba zabezpečit, což lze vypočítat pomocí rovnice (2.3). Na základě tohoto výpočtu je třeba vybrat vhodné parametry n a odpovídající korekční schopnost t z tabulek existujících BCH kódů, které jsou uvedeny v příloze A. Tento postup zajistí, že zvolený kód bude splňovat požadavky na spolehlivost přenosu dat.

V následujících částech je popsán proces zabezpečení zpráv pomocí vybraných BCH kódů, a to včetně kroků potřebných pro jejich zakódování a následného dekódování. Zakódování je realizováno přidáním zabezpečovacích bitů ke vstupním datům, zatímco dekódování zahrnuje detekci a opravu chyb na základě analýzy kódového slova. Tímto způsobem je zajištěna ochrana přenášených dat proti chybám způsobeným šumem nebo rušením v přenosovém kanálu.

2.4.2 Kódování BCH kódů

Proces kódování BCH kódů vyžaduje definování základních polynomů, které se používají při matematickém popisu zabezpečení dat:

- $p(x)$ – polynom nezabezpečené zprávy,
- $g(x)$ – vytvářecí (generující) polynom,
- $m(x)$ – polynom podílu,
- $d(x)$ – polynom zbytku po dělení,
- $c(x)$ – polynom zabezpečené zprávy (kódové slovo),
- $r(x)$ – polynom přijaté zprávy,
- $e(x)$ – chybový polynom.

Podle [18, 39, 73] je způsob zabezpečení zpráv pomocí BCH kódů popsán následující rovnicí:

$$\frac{p(x) \cdot x^{n-k}}{g(x)} = m(x) + \frac{d(x)}{g(x)}, \tag{2.6}$$

kde $p(x) \cdot x^{n-k}$ reprezentuje polynom nezabezpečené zprávy rozšířený o $n-k$ nulových bitů. Tato rovnice ukazuje rozdělení vstupního polynomu na podíl $m(x)$ a zbytek $d(x)$ při dělení generujícím polynomem $g(x)$. Rovnice (2.6) lze přepsat do tvaru:

$$p(x) \cdot x^{n-k} = m(x) \cdot g(x) + d(x). \tag{2.7}$$

Tato rovnice vyjadřuje, že nezabezpečená zpráva $p(x) \cdot x^{n-k}$ je rozdělena na část, která je dělitelná $g(x)$, a na část reprezentovanou zbytkem $d(x)$.

Použitím operací modulu 2 je možné upravit tuto rovnici na výsledný vztah pro kódové slovo $c(x)$:

$$c(x) = p(x) \cdot x^{n-k} + d(x) = m(x) \cdot g(x), \tag{2.8}$$

kde $c(x)$ je polynom zabezpečené zprávy, který obsahuje původní informační část $p(x) \cdot x^{n-k}$ doplněnou o zabezpečovací bity reprezentované $d(x)$. Tento postup zajišťuje, že kódové slovo $c(x)$ splňuje následující podmínku: je dělitelné generujícím polynomem $g(x)$ beze zbytku. Tato skutečnost je využita pro kontrolu správnosti přijatého polynomu $r(x)$ v procesu dekódování. BCH kódy jsou zařazeny do skupiny cyklických kódů, což umožňuje jejich kódování realizovat standardním způsobem používaným pro cyklické kódy. Kódování je proto prováděno s využitím děličky mod $g(x)$ která je klíčovou součástí kodéru. Tento přístup umožňuje vytvoření polynomu zabezpečené zprávy $c(x)$ přímo během procesu dělení [100].

Postup kódování může být shrnut do tří kroků:

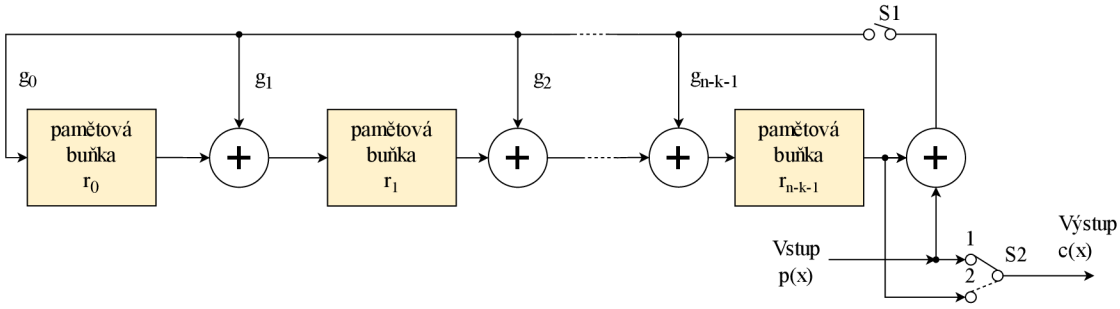
1. Rozšíření polynomu nezabezpečené zprávy: Polynom nezabezpečené zprávy $p(x)$ je vynásoben členem $x^{(n-k)}$. Tímto krokem je nezabezpečená zpráva rozšířena o $(n-k)$ nulových bitů, což odpovídá zvýšení jejího řádu.
2. Dělení vytvářecím polynomem: Rozšířený polynom $p(x) \cdot x^{n-k}$ je vydělen vytvářecím polynomem $g(x)$. Výsledkem tohoto dělení je zbytek $d(x)$, který obsahuje zabezpečovací bity.
3. Generování kódového slova: Zbytek po dělení $d(x)$ je přičten k rozšířenému polynomu $p(x) \cdot x^{n-k}$, který byl získán v bodě 1, což dává výsledný polynom zabezpečené zprávy $c(x)$. Tento polynom je kódovým slovem BCH kódu.

Kodér BCH kódu realizovaný děličkou g(x)

Postup zabezpečení popsaný výše je založen na dělení rozšířeného polynomu vytvářecím polynomem $g(x)$ a je realizován pomocí děličky mod $g(x)$. Dělička je implementována jako kruhový posuvný registr, jehož architektura je tvořena zpětnými vazbami a sčítačkami mod 2. Umístění sčítaček mod 2 je určeno vytvářecím polynomem $g(x)$, přičemž jsou umístěny před ty členy, které mají v polynomu $g(x)$ znaménko součtu.

Zapojení děličky mod $g(x)$ je znázorněno na Obr. 2.1, přičemž základní podoba byla převzata z [63].

Kruhový posuvný registr je tvořen $(n-k)$ paměťovými buňkami $(r_0 \dots r_{n-k-1})$. Počet těchto buněk odpovídá řádu vytvářecího polynomu $g(x)$. Pro nejvyšší řád polynomu $g(x)$ není nutné v registru použít paměťovou buňku, a příslušná sčítačka mod 2 je umístěna před buňkou r_0.



Obr. 2.1: Zapojení děličky mod $g(x)$.

Popis funkce kodéru BCH kódu realizovaného děličkou mod $g(x)$

Funkci kodéru na Obr. 2.1 lze rozdělit do dvou hlavních fází:

1. Načítání vstupní zprávy do registru: Vstup kodéru $p(x)$ je tvořen posloupností k informačních bitů. Spínač $S2$ je nastaven do polohy 1, což umožňuje přímý přenos vstupních bitů na výstup kodéru. Zároveň jsou tyto bity postupně načítány do paměťových buněk posuvného registru, a to během prvních k cyklů. Spínač $S1$ je v této fázi sepnut.
2. Po načtení k informačních bitů je spínač $S1$ rozepnut a spínač $S2$ přepnut do polohy 2. V následujících $n - k$ cyklech dochází k posouvání obsahu registru, přičemž na výstupu kodéru jsou generovány zabezpečovací bity. Po dokončení n cyklů je na výstupu vytvořeno kódové slovo $c(x)$, které obsahuje původní informační bity i zabezpečovací bity.

Tento postup se poté opakuje pro každou další vstupní posloupnost. Implementace tohoto procesu pomocí kruhového registru s minimálním počtem operací zajišťuje vysokou efektivitu a spolehlivost kódování.

2.4.3 Dekódování BCH kódů

Dekódování BCH kódů je proces, při kterém je analyzováno přijaté kódové slovo $r(x)$, které mohlo být během přenosu narušeno chybami. Vztah mezi přijatým polynomem $r(x)$, původním kódovým slovem $c(x)$ a chybovým polynomem $e(x)$ je podle [73] vyjádřen rovnicí:

$$r(x) = c(x) + e(x) \tag{2.9}$$

Pokud přijatý polynom $r(x)$ obsahuje t nebo méně chyb, lze určit chybový polynom $e(x)$ a následně opravit chyby. Pokud však počet chyb přesáhne zabezpečovací schopnost kódu t, proces dekódování skončí neúspěšně.

Vlastní postup dekódování může být shrnut do následujících kroků[55]:

1. výpočet syndromů S_j pro $j = 1, 2, \ldots, 2t$,
2. nalezení chybového lokalizačního polynomu $\Lambda(x)$,
3. nalezení kořenů chybového lokalizačního polynomu,
4. opravení chyb na určitých pozicích.

Výpočet syndromů

Prvním krokem dekódování je výpočet syndromů (příznaků), které slouží k detekci chyb v přijatém polynomu $r(x)$. Syndromy jsou získány dosazováním kořenů vytvářecího polynomu $g(x)$ do polynomu přijaté zprávy $r(x)$. Výsledkem jsou hodnoty S_j, které splňují následující syndromové rovnice:

$$S_j = r(\alpha^j) = e(\alpha^j) = \sum_{k=0}^{n-1} e_k \alpha^{jk}, \qquad j = 1, 2, \ldots, 2t, \tag{2.10}$$

kde α je kořen primitivního polynomu vytvářejícího Galoisova tělesa $GF(2^m)$. Pokud $r(x)$ obsahuje chyby, syndromy S_j, nabývají nenulových hodnot. Hodnoty $S_1, S_2, \ldots, S_{2t}$ se nazývají syndromy přijatých dat a jsou klíčové pro další kroky dekódování.

Pokud je v přijatém polynomu $r(x)$ přítomno v chyb na pozicích $i_1, i_2, \cdots, i_v$ s odpovídajícími chybovými hodnotami $e_{i_j} \neq 0$, lze Syndromy S_j, podle [70] vyjádřit jako:

$$S_j = \sum_{l=1}^{v} e_{i_l} (\alpha^j)^{i_l} = \sum_{l=1}^{v} e_{i_l} (\alpha^{i_l})^j. \tag{2.11}$$

Zavedeme-li substituci $X_l = \alpha^{i_l}$, rovnice přechází na tvar:

$$S_j = \sum_{l=1}^{v} e_{i_l} X_l^j, \qquad j = 1, 2, \ldots, 2t. \tag{2.12}$$

Hodnoty X_l se nazývají lokátory chyb. Pokud je například $X_l = \alpha^3$, znamená to, že chyba se nachází na třetí pozici, tedy $i_1 = 3$. Tím je určena pozice chyby v přijatém polynomu.

Nalezení chybového lokalizačního polynomu

Z rovnice (2.12) lze sestavit soustavu rovnic, která je vyjádřena ve tvaru:

$$\begin{aligned} S_1 &= \quad e_{i_1} X_1^j + e_{i_2} X_2^j + \cdots + e_{i_v} X_v^j \\ S_2 &= e_{i_1} X_1^{2j} + e_{i_2} X_2^{2j} + \cdots + e_{i_v} X_v^{2j} \\ &\vdots \\ S_{2t} &= e_{i_1} X_1^{2tj} + e_{i_2} X_2^{2tj} + \cdots + e_{i_v} X_v^{2tj} \end{aligned} \tag{2.13}$$

kde S_j představují syndromy, $X_l = \alpha^{il}$ jsou lokátory chyb a e_{il} odpovídají hodnotám chyb. Tato soustava obsahuje $2t$ rovnic s v neznámými lokacemi chyb. Přímé řešení této soustavy je však výpočetně náročné, neboť se jedná o nelineární rovnice vyššího řádu. Pro zjednodušení výpočtu je zaveden chybový lokalizační polynom, který je definován jako:

$$\Lambda(x) = \prod_{l=1}^{v}(1 - X_l x) = \Lambda_v x^v + \Lambda_{v-1} x^{v-1} + \cdots + \Lambda_1 x + \Lambda_0, \tag{2.14}$$

kde platí, že $\Lambda_0 = 1$. Tento polynom umožňuje transformovat problém lokalizace chyb na úlohu nalezení kořenů tohoto polynomu, které odpovídají lokátorům chyb X_l. V následující části bude představen algoritmus pro nalezení lokalizačního polynomu $\Lambda(x)$.

Berlekamp-Massey algoritmus

Berlekamp-Massey algoritmus (dále jen BM algoritmus) je standardní metoda pro stanovení chybového lokalizačního polynomu $\Lambda(x)$. Tento algoritmus je založen na iterativním hledání co nejkratšího posuvného registru (LFSR) schopného generovat všechny syndromy S, jak je popsáno v [61, 102].

V průběhu iterací se počítají syndromy a upravují parametry LFSR, dokud není dosaženo správného lokalizačního polynomu $\Lambda(x)$. Každá iterace zahrnuje výpočet odchylky (angl. discrepancy), což je klíčový parametr pro úpravu polynomu.

Po výpočtu prvního syndromu S_1 se další syndromy počítají podle vztahu:

$$S_{i+1} = -\sum_{n=1}^{l^i} \Lambda_n^i S_{i+1-n}. \tag{2.15}$$

Následně je počítána odchylka $d^{(i)}$, která je definována podle [43] jako:

$$d^{(i)} = S_{i+1} + \sum_{n=1}^{l^i} \Lambda_n^i S_{i+1-n} = \sum_{n=0}^{l^i} \Lambda_n^i S_{i+1-n}. \tag{2.16}$$

Pokud je odchylka $d^{(i)} = 0$, pak současný LFSR správně vytváří následující syndrom S_2. Následující úpravou je pak:

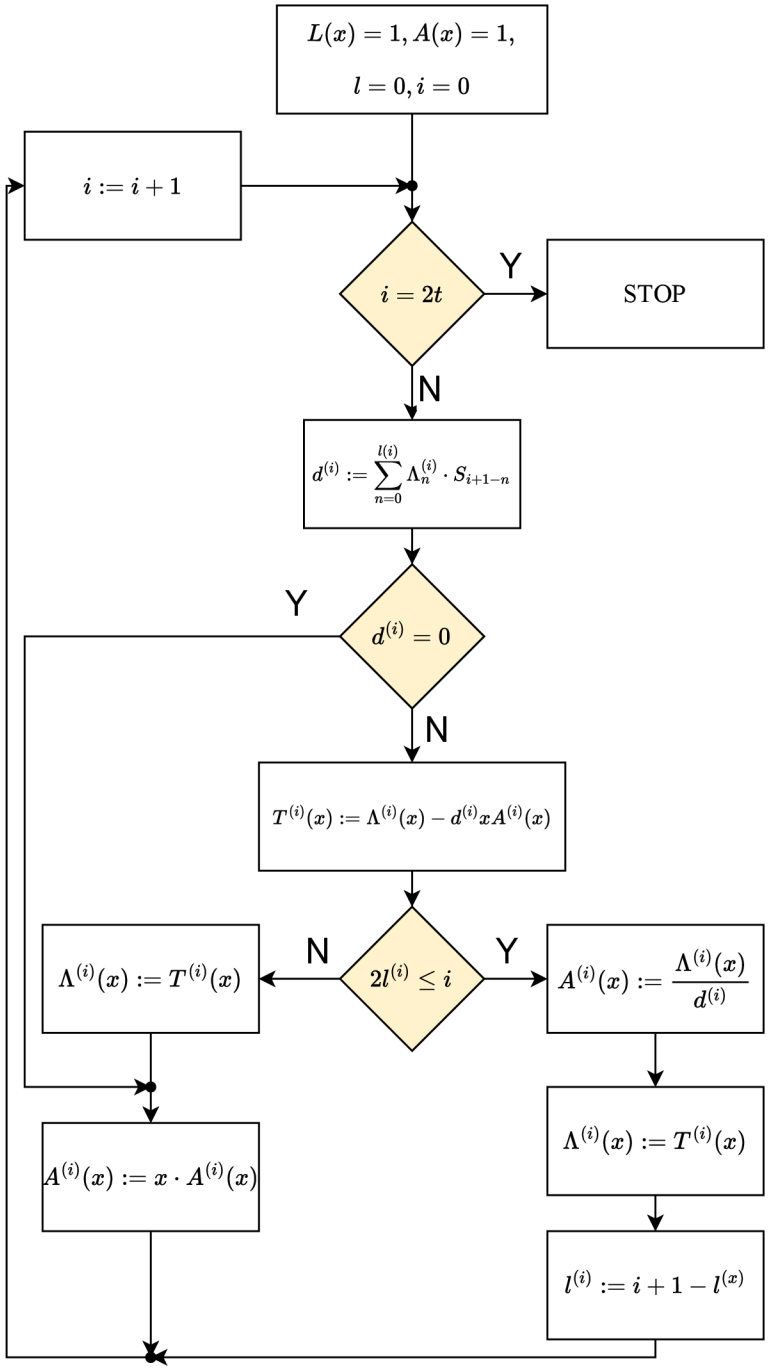
$$\begin{aligned} l^{(i+1)} &:= l^i \\ \Lambda^{(i+1)}(x) &:= \Lambda^i(x) \\ i &:= i + 1. \end{aligned}$$

Pokud $d^{(i)} \neq 0$, musí být LFSR upraven, dokud není $d^{(i)} = 0$. Tím je prodloužen o polynom

$$\Lambda^{i+1}(x) = \Lambda^i(x) - x^{i-m} \frac{d^{(i)}}{d^{(m)}} \Lambda^{(m)}(x), \tag{2.17}$$

kde m a d_m jsou z m-té iterace, která vytvořila chybný syndrom S_m, a x^{i-m} posouvá na požadovanou pozici LFSR.

Tyto kroky BM algoritmu mohou být formálně shrnuty tzv. Blahutovou interpretací a jsou znázorněny na Obr.2.2. Podle znázorněného algoritmu jsou jednotlivé fáze popsány takto:



Obr. 2.2: Vývojový diagram Berlekamp-Massey algoritmu.

1. **Základní nastavení**
   Iterační index: $i = 0$
   Délka LFSR: $l^{(1)} = 0$
   Chybový lokalizační polynom: $\Lambda^{(1)}(x) = 1$
   Pomocný polynom: $A^{(1)}(x) = 1$
2. **Kontrola, zda platí** $i = 2t$. Pokud ano, iterace končí.
3. **Výpočet odchylky nebo chyby**, která souvisí s vytvořením dalšího syndromu podle rovnice (2.16)

$$d^{(i)} = \sum_{n=0}^{l^i} \Lambda_n^i S_{i+1-n}.$$

4. **Kontrola, zda je odchylka rovna nule** $d^{(i)} = 0$. Pokud ano, aktuální LFSR o délce $l^{(i)}$ a chybový polynom $\Lambda^{(i)}(x)$ vytváří další syndrom S_{i+1}. V tom případě se přejde ke kroku 5, jinak se pokračuje ke kroku 6.
5. **Posunutí pomocného polynomu LFSR o jednu pozici**

$$A^i(x) = xA^{(i)}(x) \tag{2.18}$$

   a dále se pokračuje krokem 12.
6. **Upravení dočasného chybového polynomu** $T^{(i)}(x)$ přidáním posunutého pomocného chybového polynomu $A^{(i)}(x)$ k současnému chybovému polynomu $\Lambda^{(i)}(x)$ podle vztahu:

$$T^{(i)}(x) = \Lambda^{(i)}(x) - d^{(i)}xA^{(i)}(x). \tag{2.19}$$

7. **Kontrola, zda je potřeba zvětšit LFSR**. Pokud platí $2l^{(i)} \leq i$, pokračuje se krokem 8, jinak krokem 9.
8. **Aktualizace chybového polynomu podle vztahu:**

$$\Lambda^{(i)}(x) := T^{(i)}(x) \tag{2.20}$$

   a provede se opět krok 5.
9. **Normalizace chybového polynomu** $\Lambda(x)$ jeho dělením výrazem $d^{(i)} \neq 0$ a uložení výsledku do pomocného LFSR $A^{(i)}(x)$:

$$A^{(i)}(x) := \frac{\Lambda^{(i)}(x)}{d^{(i)}} \tag{2.21}$$

   a pokračuje se krokem 10.
10. **Aktualizace polynomu** $\Lambda^{(i)}(x)$, jelikož byl v předchozím kroku uložen do $A^{(i)}(x)$, může být aktualizován podle vztahu:

$$\Lambda^{(i)}(x) := T^{(i)}(x) \tag{2.22}$$

   a pokračuje se krokem 11.

11. **Prodloužení LFSR** podle následujícího vztahu:

$$l^{(i+1)} = i + 1 - l^{(x)} \tag{2.23}$$

a pokračuje se krokem 12.

12. **Inkrementace iteračního indexu** i a návrat ke kroku 2.

Po provedení všech výše uvedených kroků je nalezen chybový lokalizační polynom. Dalším krokem je použití Chienova vyhledávání k nalezení jeho kořenů, jak je popsáno dále.

Tento algoritmus je popsán v mnoha publikacích zabývajících se kódováním a opravou chyb. Pro podrobnější informace viz [43, 63, 70, 91].

Nalezení kořenů chybového lokalizačního polynomu

Dalším krokem po nalezení lokalizačního polynomu $\Lambda(x)$ je nutné určit jeho kořeny. Tento krok se provádí pomocí Chienova vyhledávání [70]. Princip spočívá v postupném dosazování všech prvků z Galoisova tělesa $\mathrm{GF}(q^m)$ (které bylo použito pro tvorbu vytvářecího polynomu) do rovnice lokalizačního polynomu (2.14).

Například, předpokládejme, že $v = 2$. Lokalizační polynom je pak podle vztahu (2.14) získán ve tvaru:

$$\Lambda(x) = \Lambda_0 + \Lambda_1 x + \Lambda_2 x^2 = 1 + \Lambda_1 x + \Lambda_2 x^2. \tag{2.24}$$

Pro každý nenulový prvek Galoisova tělesa dosadíme za $x = 1, x = \alpha, x = \alpha^2, \ldots, x = \alpha^{q^m-2}$. Dostaneme:

$$\begin{aligned}
\Lambda(1) &= 1 + \Lambda_1(1) + \Lambda_2(1)^2, \\
\Lambda(\alpha) &= 1 + \Lambda_1(\alpha) + \Lambda_2(\alpha)^2, \\
&\vdots \\
\Lambda(\alpha^{q^m-2}) &= 1 + \Lambda_1(\alpha^{q^m-2}) + \Lambda_2(\alpha^{q^m-2})^2.
\end{aligned}$$

Prvky Galoisova tělesa, pro které vyjde $\Lambda = 0$, označují svým exponentem pozici chyby.

Opravení chyb

Jakmile jsou určeny všechny pozice chyb $i_1, i_2, \ldots, i_v$, je vytvořen chybový polynom $e(x)$, který má nenulové koeficienty pouze na těchto pozicích. Následně je tento polynom přičten k polynomu přijaté zprávy $r(x)$, podle vztahu:

$$c(x) = r(x) + e(x). \tag{2.25}$$

Tím je získáno původní kódové slovo $c(x)$, čímž je dekódovací proces úspěšně ukončen.

Shrnutí analýzy BCH kódů

BCH kódy představují relativně jednoduchý, avšak velmi účinný nástroj pro opravu bitových chyb, které mohou vznikat například vlivem rušení nebo nízké hodnoty signálového poměru (SNR). Výpočetní náročnost BCH kódů je nesymetricky rozdělena mezi vysílač a přijímač. Na straně vysílače (kodéru BCH kódu) je konstrukce kódu algoritmicky jednodušší a méně náročná na výpočetní výkon než na straně přijímače (dekodéru BCH kódu).

Tato vlastnost činí BCH kódy velmi vhodnými pro zamýšlenou aplikaci, v níž na straně vysílače pracujeme s nositelným zařízením napájeným z baterie. Úspora výpočetního výkonu na straně vysílače tedy přímo přispívá ke snížení energetické náročnosti zařízení, což je v tomto kontextu klíčový požadavek. Na straně přijímače, kde je k dispozici stabilní zdroj napájení, není vyšší výpočetní náročnost dekódování překážkou.

BCH kódy pracují s fixní délkou kódového slova, která je určena předem. Pro každou délku kódového slova existuje několik možností, jak kódové slovo rozdělit mezi užitečná data a zabezpečovací bity. Tato vlastnost poskytuje určitou míru variability v počtu opravitelných bitových chyb, což umožňuje optimalizaci vysílacího výkonu, a tím i spotřeby energie komunikačního modulu. Zabezpečení přenosu pomocí BCH kódů tak zvyšuje spolehlivost bezdrátové komunikace, aniž by došlo k výraznému zvýšení energetické náročnosti nositelného zařízení. Toto řešení je proto klíčové pro návrh dedikovaného komunikačního protokolu, který zajišťuje dlouhou výdrž baterie a robustnost přenosu dat.

3 Cíle disertační práce

Předkládaná disertační práce vychází z analýzy potenciálu moderních komunikačních technologií v kontextu nositelné zdravotnické techniky a klade si za cíl využít pokrok ve vývoji elektrotechniky pro aplikace v oblasti zdravotní péče.

Záměrem práce je zkoumat přístupy, které umožní efektivní využití technologických inovací pro odesílání dat z nositelné zdravotnické techniky, kde dosud možnost on-line přenosu dat chybí. Práce má ambici přispět ke zlepšení zdravotní péče i zlepšení uživatelského komfortu pacientů.

Hlavním cílem práce je navrhnout koncepci bezpečného komunikačního protokolu pro přenos alarmových stavů nositelných externích kardiostimulátorů, tento protokol vyvinout a otestovat na simulačním modelu a připravit doporučení pro pilotní implementaci na reálném hardwaru. Protokol bude provozován v ISM pásmu a má za úkol mimo jiné optimalizovat spotřebu energie, neboť bude provozován na nositelných zařízeních napájených z mobilních zdrojů (baterie).

Z hlavního cíle disertační práce jsou odvozeny cíle dílčí:

- Analýza komunikačních potřeb a možností nositelných externích kardiostimulátorů
- Návrh koncepce komunikačního protokolu
- Vytvoření simulačního modelu a optimalizace navrženého protokolu

Pozornost bude soustředěna zejména na vlastní koncepci a návrh komunikačního protokolu a konstrukci simulačního modelu. Splnění cílů bude demonstrováno prostřednictvím ucelené koncepce dedikovaného komunikačního protokolu pro nositelné kardiostimulátory.

4 Koncepce komunikačního protokolu

Externí kardiostimulátory jsou využívány pacienty v rekonvalescenční fázi po operaci srdce, pro dočasnou stimulaci a kontrolu před implantováním trvalého kardiostimulátoru, nebo pro sledování pacienta po defibrilaci srdce. Externí dočasné kardiostimulátory nabízí několik výrobců. Jako příklad je možné uvést nositelný externí kardiostimulátor firmy Mediatrade (Obr. 4.1a) [21] nebo firmy St. Jude Medical (Obr. 4.1b)[50]. Tyto kardiostimulátory během svého provozu generují několik klíčových informací. Mezi kritické stavové údaje patří:

- stav výstrahy v případě odpojení elektrod,
- změna přednastavených parametrů,
- nedostatečná úroveň nabití baterie.

Vedle těchto zásadních informací jsou k dispozici další užitečné údaje, například aktuální srdeční frekvence a historie stimulovaných nebo spontánních srdečních tepů, které byly zaznamenány v předchozích časových úsecích.

(a) (b)

Obr. 4.1: Příklady externích kardiostimulátorů: a) Mediatrade model EPG10, b) St. Jude Medical model 3085.

Stávající řešení externích kardiostimulátorů jsou zcela autonomní. Pokud tedy zdravotnický personál chce zjistit diagnostické údaje, nebo nastavit terapeutické údaje, je nutné tyto úkony provádět přímo na zařízení instalovaném na pacientovi. Zejména tak je nutné pravidelně sledovat stav baterií, protože nelze spolehlivě odhadnout rychlost jejich vybíjení. Životnost baterií výrobci uvádějí jen 3 dny. Navíc je nutné baterie vyměnit včas, protože jsou zdrojem energie pro záložní zdroj, který udrží zařízení při výměně baterie v chodu pouze 30 sekund.

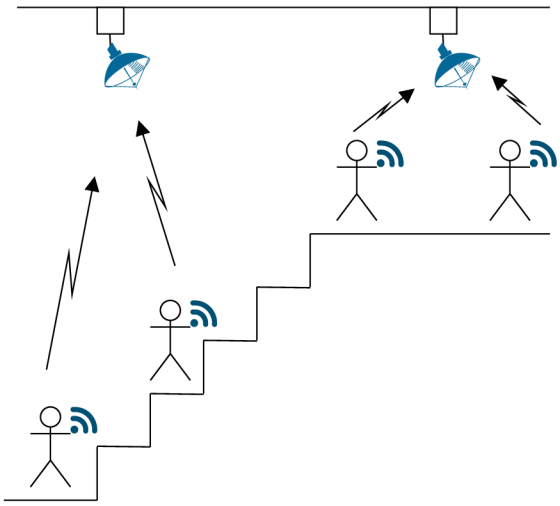
I když o bezdrátový přenos dat z těchto zařízení se výrobci pokoušeli, vždy od něj upustili právě kvůli nárokům na velký odběr z baterií při přenosu dat.

Záměrem práce je proto poskytnout výrobcům nový energeticky nenáročný způsob řešení protokolu pro přenos dat z nositelných kardiostimulátorů. Nová generace externích nositelných kardiostimulátorů by měla navíc umožnit bezdrátový přenos údajů od několika pacientů do sesterny tak, aby nebylo nutné zjišťovat kritické údaje přímo na externím kardiostimulátoru. Koncepce řešení komunikačního protokolu pro bezdrátový přenos musí být energeticky nenáročná a zejména nesmí ohrozit vlastní činnost kardiostimulátoru při stimulaci srdce.

Kardiostimulátor je napájen baterií, jejíž výměna je, jak už bylo řečeno, pro pacienta riziková a často náročná procedura. Z tohoto důvodu je nezbytné optimalizovat komunikační protokol tak, aby minimalizoval energetickou spotřebu a zároveň maximalizoval pravděpodobnost úspěšného přenosu dat.

Vzhledem k fyziologickým omezením kardiostimulátoru je datový přenos možný pouze v tzv. refrakterním časovém úseku, což je krátký interval následující bezprostředně po stimulaci nebo spontánním srdečním tepu. Tento omezený časový úsek vyžaduje velmi efektivní návrh protokolu, který umožní přenos dat bez nutnosti potvrzení o přijetí základnovou stanicí.

Hlavním cílem návrhu komunikačního protokolu je umožnit kardiostimulátoru pouze odesílat data, přičemž příjem potvrzení není vyžadován. Za účelem optimalizace protokolu bylo proto nutné simulovat chování pacientů v reálných podmínkách, zejména v situacích, kdy více pacientů na oddělení provádí rehabilitační cvičení v dosahu jedné základnové stanice. Tato situace je znázorněna na Obr. 4.2. Přenášený datový rámec je navržen tak, aby byl dostatečně krátký a přenosy byly časově rozptýlené. I tyto vlastnosti potvrzují možnost uvažovat o implementaci dedikovaného komunikačního protokolu založeného pouze na vysílání, což dále přispívá k minimalizaci energetické spotřeby zařízení.



Obr. 4.2: Znázornění možných nároků na přenos dat od pacientů při rehabilitaci.

4.1 Analýza technických prostředků

Při návrhu vlastní koncepce protokolu je potřeba vzít v potaz i možnosti technických prostředků. V následující části práce budou proto analyzovány dostupné rádiové frekvenční moduly, jednotlivé čipové architektury a anténní komponenty vhodné pro návrh koncepce vlastního řešení.

4.1.1 Radiofrekvenční moduly

Na trhu existuje řada výrobců radiofrekvenčních (RF) modulů pracujících v subgigahertzovém ISM pásmu, které bylo definováno v sek. 1.4.1. Tyto čipy jsou v převážné většině založeny na jedné z těchto hardwarových architektur:

- proprietární řešení,
- Intel 8051,
- ARM Cortex-M4,
- ARM Cortex-M33.

U starších architektur a zejména proprietárních řešení existují tři varianty RF modulů:

- vysílač
- přijímač
- transceiver, t.j. přijímač i vysílač v jednom RF modulu, který se softwarově přepíná do režimu příjmu nebo vysílání, pracující pouze v jednom kmitočtovém pásmu.

Pro praktické použití je nejvhodnější použít RF moduly typu transceiver, neboť hrozí výrazně nižší riziko, že s aktualizací firmware nebo software dojde k nesouladu nastavení parametrů komunikace mezi vysílačem a přijímačem.

Prakticky všechny soudobé RF moduly podporují více kmitočtových pásem a to minimálně pásmo 433 MHz a pásmo 868 MHz. Proto v následujícím přehledu uvádíme pouze RF moduly typu transceiver, které podporují obě kmitočtová pásma. Řada výrobců nabízí celou škálu podobných RF modulů stejné architektury, které se liší pouze ve velikosti programové paměti, paměti RAM, případně počtu GPIO (General-purpose input/output) pinů použitelných jako vstupní či výstupní rozhraní.

V následujících odstavcích je uveden přehled běžných RF modulů, které jsou v současné době na trhu. Přehled si neklade za cíl přinést vyčerpávající seznam všech dostupných RF modulů, ale slouží jako orientační pomůcka pro výběr vhodného typu pro implementace v reálném kardiostimulátoru.

Moduly založené na architektuře Intel 8051

Intel 8051 (Intelem označovaný jako MCS-51) je jednočipový osmibitový mikrokontrolér Harvardské architektury vyvinutý společností Intel v roce 1980 pro použití v embedded systémech. Původní verze od společnosti Intel byly populární v 80. a na počátku 90. let a vylepšené binárně kompatibilní deriváty jsou populární dodnes. Jedná se o mikro počítač s komplexní instrukční sadou s oddělenými paměťovými prostory pro programové instrukce a data. Intel již rodinu MCS-51 a jeho nástupce nevyrábí, vylepšené binárně kompatibilní deriváty vyráběné mnoha výrobci, jako např. Atmel, Infineon Technologies, NXP nebo Texas Instruments, se používají dodnes. Jedním z těchto derivátů doplněných o digitální signálový procesor (DSP) jsou např. RF moduly Nordic Semiconductor nRF9E5 [71], nebo moduly Texas Instruments řady CC1110 a CC1111 [98].

Přehled klíčových RF modulů založených na architektuře Intel 8051 je k nalezení v příloze B.1.

RF moduly Texas Instruments řady CC1111 se od řady CC1110 liší v zásadě jen podporou USB rozhraní, obě varianty existují ve třech verzích - s programovou pamětí velikosti 8 kB, 16 kB, resp. 32 kB.

Moduly založené na architektuře ARM Cortex-M4

Architektura ARM Cortex-M4 je založena na instrukční sadě ARMv7E-M. Koncepčně se jedná o jádro ARM Cortex-M3 doplněné o DSP instrukční sadu a volitelně i o jednotku zpracování reálných čísel v pohyblivé řádové čárce (FPU), které jsou známé jako ARM Cortex-M4F. DSP činí tuto architekturu vhodnou pro použití v RF modulech a dalo tak vzniknout první generaci RF modulů s univerzální architekturou, které nepotřebují další mikrokontrolér pro napojení aplikačních rozhraní.

Klíčovým výrobcem RF modulů postavených na architektuře ARM Cortex-M4 je firma Silicon Labs. Přehled klíčových RF modulů založených na architektuře ARM Cortex-M4 je k nalezení v příloze B.2.

Moduly založené na architektuře ARM Cortex-M33

Architektura ARM Cortex-M33 vznikla v roce 2016 a je založena na instrukční sadě ARMv8-M. Volitelně může být doplněna o bezpečnostní instrukce známé pod označením TrustZone. V jistém smyslu jde o nástupce architektur ARM Cortex-M3 a ARM Cortex-M4 a používá se nejen v moderních mikrokontrolerech, ale i RF modulech. Tato architektura tak v případě použití v RF modulech zachovává všechny dobré vlastnosti modulů založených na architektuře ARM Cortex M-4 avšak má perspektivu dlouhodobější komerční dostupnosti.

Architektura ARM Cortex-M33 je stále relativně nová a jedny z prvních RF modulů postavených nad touto architekturou jsou moduly Silicon Labs řady EFR32FG23 [89] a EFR32FG28 [90], která je oproti řadě EFR32FG23 vybavena navíc i podporou protokolu Bluetooth. Obě typové řady RF modulů EFR32FG23 a EFR32FG28 existují v celé řadě variant, které se liší v implementaci bezpečnostních aspektů architektury ARM Cortex-M33, tzv. Secure Vault [20], počtu GPIO pinů, velikosti programové paměti a paměti RAM a v případě řady EFR32FG28 i implementací protokolu Bluetooth. Pro účely implementace navržené koncepce komunikačního protokolu v reálných kardiostimulátorech je samozřejmě vhodnější varianta s vyšším stupněm zabezpečení a naopak protokol Bluetooth nebude využit. V tabulce, která je umístěna v příloze B.3 jsou proto uvedeny jen moduly těchto vlastností.

Další používané architektury

Jedná se o nejstarší avšak dosud používané RF moduly. Jejich hlavní nevýhodou je velmi úzké spektrum nabízených rozhraní, zpravidla SPI nebo UART, a nemožnost programování vlastního komunikačního protokolu přímo na RF modulu. Pro implementaci vlastního komunikačního protokolu je tak nutné použít externí mikrokontrolér, což zvyšuje spotřebu, komplexnost a zástavbovou plochu vyvíjené elektroniky.

Nejrozšířenějšími RF moduly této kategorie jsou čipy SiliconLabs řady Si44xx. Přehled nejvýznamnějších modulů této řady je v tabulce v příloze B.4.

V současné době stále existuje na trhu široká škála hotových RF modulů postavených na těchto čipech. Nejběžnějšími moduly jsou:

- Moduly firmy RFSolutions, ZETA-433 a ZETA-868 postavené na čipech SiliconLabs Si4455 [79],
- Obdobné moduly ZETAPLUS-433 a ZETAPLUS-868 téhož výrobce doplněné o lokální mikrokontroler a ovládání pomocí tzv. AT příkazů [80],
- Transceiver modul výrobce Microchip Technologies v pásmu 868 MHz [67],
- Vysílací modul RFM68W [46] a přijímací modul RFM69HW [47] výrobce HOPE Microelectronics pracující v pásmu 868 MHz,
- Obdobné moduly téhož výrobce pro pásmo 433 MHz RFM42, resp RFM43 [45] a RFM31B [44]

Na bázi modulů ZETA-868 a ZETA-433 byl již v rámci přípravného řešení sestaven testovací komunikační modul pro zamýšlený typ kardiostimulátoru. Tento komunikační modul používal mikrokontroler Arduino Nano a k stávajícímu externímu kardiostimulátoru byl připojen kabelem. V rámci zmíněného řešení nebyla řešena problematika komunikačního protokolu a komunikace tak byla možná jen pro jeden kardiostimulátor v daném čase. Tento testovací modul tak posloužil především pro stanovení výchozích cílů této práce.

4.1.2 Výběr radiofrekvenčního řešení

Byla provedena analýza dostupných hotových RF modulů. Jako perspektivní se z hlediska dlouhodobé udržitelnosti nového řešení jeví architektura ARM Cortex-M33. Tato architektura je nejmodernější a zdá se, že klíčoví výrobci mají snahu tuto architekturu preferovat.

Čipy jednotlivých typů architektury se liší především počtem a strukturou rozhraní, velikostí operační paměti a paměti pro uložení mikrokódu, podporovanými frekvenčními pásmy a typem pouzdra.

Pro reálnou implementaci v kardiostimulátoru však není vhodné používat již hotové RF moduly a to zejména z důvodu jejich rozměrů a spotřeby. Jako technicky nejschůdnější řešení se jeví použití RF čipu architektury ARM s dostatečným prostorem pro vlastní softwarový kód, do kterého bude možné implementovat navržený komunikační protokol.

Z důvodu dlouhodobější perspektivy dostupnosti technických prostředků je vhodnější použití architektury ARM Cortex-M33. Tato architektura navíc podporuje moderní prvky kybernetické bezpečnosti.

Na základě podrobného porovnání vlastností jednotlivých komponent byl jako nejvhodnější vytipován pro ověření čip SiliconLabs EFR32FG23B020F512IM40 [89]. Tento čip používá moderní architekturu ARM Cortex-M33 a u modelů čipové řady EFR32FG23 patří k čipům s nejvyšší podporou bezpečnostních funkcí a větší programovou pamětí i pamětí RAM. Z modelů těchto vlastností byl zvolen čip s nejmenším pouzdrem (a tím i nejmenším počtem externích rozhraní typu GPIO, které se ovšem pro očekávanou reálnou implementaci uplatní jen v malém počtu).

4.2 Analýza anténního systému

Bezdrátové moduly vyžadují pro spolehlivý přenos dat vhodnou anténu, která zajistí optimální příjem a vysílání signálu. Antény mohou být externí mono-pólové antény (prutové), interní vyleptané na desce plošných spojů (DPS), nebo keramické. Externí prutové antény se vyznačují vyšší účinností, ale jejich rozměry jsou nepraktické pro nositelné zařízení. Interní antény vytvořené na DPS poskytují integraci bez nutnosti dalších součástí, avšak jejich výkon často závisí na kvalitním návrhu desky. Keramické antény představují kompromis mezi velikostí a výkonem. Jsou kompaktní, snadno se integrují do malých zařízení a díky své směrové charakteristice a odolnosti vůči okolnímu rušení poskytují spolehlivý signál i v náročných podmínkách. Pro jejich vybuzení stačí jen malý výkon. Při výběru keramické antény je důležité zvolit i správné provedení pouzdra, které může být s pájecími ploškami přímo pod pouzdrem (LGA/QFN), kdy se počítá s automatizovaným strojovým osazením,

nebo s vývody na okrajích pouzdra pro snadnější ruční pájení při vývoji bezdrátového modulu. Pro užití v nositelném kardiostimulátoru bude zřejmě příhodné užít keramickou anténu.

V dnešní době jsou na trhu dvě nejčastěji využívané technologie výroby keramických antén: IMD (Isolated Magnetic Dipole) a PIFA (Planar Inverted-F Antenna). Tyto technologie představují odlišné přístupy k návrhu kompaktních antén, které se běžně používají v moderních bezdrátových zařízeních, jako jsou mobilní telefony, IoT zařízení, nositelná elektronika a další.

Srovnání kompaktních keramických antén:

- IMD (Isolated Magnetic Dipole) Hlavním inovativním aspektem IMD antén je schopnost izolovat magnetický dipól, čímž se minimalizují vzájemné interference mezi anténou a okolními elektronickými součástkami. Tato vlastnost výrazně zlepšuje kvalitu přenosu a stabilitu signálu, což je obzvláště důležité v zařízeních, kde jsou antény umístěny v těsné blízkosti jiných komponent [32].
- PIFA (Planar Inverted-F Antenna) PIFA antény jsou kompaktní a relativně jednoduché na výrobu, což přispívá k jejich popularitě zejména v mobilních zařízeních, jako jsou telefony a tablety. Poskytují dobrý výkon při malých rozměrech a lze je snadno přizpůsobit pro různé frekvenční pásma, což umožňuje podporu různých komunikačních standardů. Jedním z klíčových omezení PIFA antén je jejich vysoká závislost na zemní rovině antény (ground plane). Aby bylo dosaženo maximálního výkonu antény, musí být ground plane správně navržena a dostatečně velká, což může být v některých zařízeních limitujícím faktorem[24].

Při návrhu bezdrátových zařízení je klíčové správné umístění antény tak, aby bylo dosaženo optimálního výkonu. Výrobci antén často poskytují doporučení pro jejich efektivní integraci. Základní zásady pro umístění antény jsou [59]:

- Umístění podél hrany zemní roviny: Dlouhá strana antény by měla být zarovnána podél hrany zemní roviny.
- Odebrání zemní roviny pod anténou: Zemní rovina by měla být odstraněna ze všech vrstev DPS přímo pod anténou, aby nedocházelo k nežádoucímu ovlivnění signálu. Tento prostor je označován jako Ground clearance.
- Vzdálenost od krytu zařízení: Vzdálenost mezi anténou a krytem nebo plastovým obalem by měla být větší než 1,5 mm.
- Vzdálenost od velkých prvků a stínění: Vzdálenost mezi anténou a většími okolními prvky, by měla být přizpůsobena výšce těchto součástek, ale neměla by být menší než 1,5 mm.

- Vzdálenost od okraje DPS: Minimální vzdálenost mezi koncem antény a koncem desky plošných spojů by měla být alespoň 10 mm, ačkoli u vysoce výkonných IMD antén mohou některé návrhy umožnit i kratší vzdálenosti.

4.2.1 Kvalitativní hodnocení anténních systémů

Pro hodnocení kvality antén je v praxi potřeba srovnat nejen jejich fyzické rozměry, ale také klíčové parametry, mezi něž patří return loss (ztráty odrazem), peak gain (maximální zisk) a VSWR (poměr stojatých vln).

- Return loss je parametr, který popisuje ztrátu energie vracející se zpět do zdroje místo toho, aby byla přenesena do antény nebo zátěže. Vyjadřuje, jak dobře je anténa nebo přenosová linka přizpůsobena dané impedanci (obvykle 50 ohmů v RF systémech). Vyšší hodnota return loss signalizuje lepší přizpůsobení, zatímco nižší hodnota znamená horší přizpůsobení, což vede k většímu odrazu signálu zpět ke zdroji.
- Peak gain označuje maximální zisk antény ve směru jejího vyzařovacího vzoru. Tento parametr udává nejvyšší úroveň zesílení signálu, kterou anténa může dosáhnout v určitém směru, a je měřen v decibelech (dB) vůči izotropnímu zářiči (dBi). Vysoký peak gain je výhodný, pokud je cílem směrovat signál efektivně do jednoho směru.
- VSWR (Voltage Standing Wave Ratio), neboli poměr stojatých vln napětí, měří, jak dobře je anténa přizpůsobena impedanci zdroje, typicky 50 ohmů. VSWR se vypočítá porovnáním napěťové vlny směřující k zátěži s napěťovou vlnou odráženou se zpět. Ideální přizpůsobení by mělo VSWR 1:1, což znamená, že veškerá energie je přenesena do zátěže bez odrazů. V praxi je běžně akceptovatelné přizpůsobení s VSWR 2:1, které poskytuje dostatečně efektivní přenos energie. Čím vyšší je první číslo ve VSWR poměru, tím horší je přizpůsobení a tím méně efektivní je systém.

Srovnání těchto parametrů pomáhá určit, která anténa dosahuje nejlepšího výkonu a je nejvhodnější pro danou aplikaci. V Tab. 4.1 a Tab. 4.2 jsou uvedena srovnání parametrů antén pro frekvence 434 MHz a 868 MHz (blíže viz příloha C). Uvedené antény podporující frekvenci 868 MHz, umožňují využití i frekvenčního pásma 915 MHz, které bylo také diskutováno jako jedno z uvažovaných volných ISM pásem.

Při výběru vhodné antény pro vlastní RF modul, který bude umístěn v kardiostimulátoru, hrají klíčovou roli (vedle co nejpřesnějšího ladění na požadovanou přenosovou frekvenci) následující parametry:

- Fyzické rozměry antény - pro umístění celého řešení je uvnitř kardiostimulátoru prostor velikosti přibližně 14x45 mm a do tohoto prostotu je třeba umístit

Tab. 4.1: Vybrané antény pro 434MHz

Parametr	**ACAG1204-433-T** [15]	**ANT1204LL20R0433A** [96]
Výrobce	ABRACON	Pulse Electronics
Frekvence [MHz]	433	433
VSWR [-]	2	-
Peak gain [dBi]	-1,72	0,83
Return loss [dB]	-6,5	<-6,5
Výška [mm]	1,6	1,5
Délka [mm]	12	12,3
Šířka [mm]	4	4

Tab. 4.2: Vybrané antény pro 868MHz

Parametr	**M620720** [60]	**SRC1024** [19]
Výrobce	KYOCERA AVX	Antenova
Frekvence [MHz]	868 – 870, 902 – 928	863 – 870, 902 – 928
VSWR [-]	2	1,7
Peak gain [dBi]	1,54	0,3
Return loss [dB]	-	<-10
Výška [mm]	1,08	0,5
Délka [mm]	6	1
Šířka [mm]	2	0,5

desku plošných spojů, na které bude instalován vlastní RF čip, anténa a veškeré pasivní prvky impedančního přizpůsobení propojení antény s RF čipem.

- Požadavky na prostorové umístění antény na DPS. Některé typy antén vyžadují pro správnou funkci velmi přesné umístění na DPS, které může přesahovat fyzické možnosti umístění DPS potřebné velikosti dovnitř kardiostimulátoru.
- Odolnost proti "rozladění", tj. narušení impedančního přizpůsobení vlivem přiblížení části těla uživatele ke kardiostimulátoru a tím i k anténě. Nositelné kardiostimulátory můžou být umístěny buďto v kapse oděvu uživatele, nebo přímo připevněny na ruku člověka. Je proto žádoucí, aby anténa nebyla příliš citlivá na podobné změny umístění.

Z důvodu malých rozměrů se jako jediná možnost ukázalo použití kompaktních keramických antén. Byla provedena řada měření s výše popsanými typy antén. U všech typů antén se podařilo najít vhodné rozvržení DPS a impedanční přizpůsobení, které minimalizuje ztráty výkonu způsobené zpětným odrazem signálu.

Jako nejvhodnější typ antény byla v rámci této práce vytipována a ověřena anténa typu IMD a to konkrétně model KYOCERA M620720 pracující v pásmu 868 MHz. Obecně je pro pásmo 868 MHz k dispozici širší nabídka součástkové základny, zejména antén.

4.3 Parametry fyzické vrstvy přenosu

Na základě porovnání uvedeném v sek. 4.1.1, byl vybrán rádiový modul firmy Silicon Labs řady EFR32FG23, tento modul nám určuje parametry fyzického rozhraní. Parametry byly vybírány v ISM pásmu a jsou uvedeny v Tab. 4.3. Nejdůležitějším parametrem je bitová rychlost, která je důležitá pro návrh komunikačního protokolu a následné simulace. Pro různé bitové rychlosti následně proto bude nutné provést simulace pro konkrétní délky rámců tak, aby byla zjištěna maximální možná délka přenášeného rámce a zároveň i maximální potřebná rychlost, která je k tomu zapotřebí, aby nedocházelo ke kolizím z jiných vysílačů.

Tab. 4.3: Přehled vhodných formátů fyzického rozhraní.

Číslo	Kmitočtové pásmo	Modulační formát	Bitová rychlost
1	434 MHz	2GFSK	100 kb/s
2	434 MHz	2GFSK	50 kb/s
3	434 MHz	4GFSK	50 kb/s
4	868 MHz	2GFSK	38,4 kb/s
5	868 MHz	2GFSK	50 kb/s
6	868 MHz	GMSK	500 kb/s
7	915 MHz	2GFSK	50 kb/s
8	915 MHz	2GFSK	500 kb/s
9	915 MHz	2GFSK	2000 kb/s
10	915 MHz	OOK	120 kb/s
11	915 MHz	4GFSK	200 kb/s

4.4 Koncepce struktury rámce pro bezdrátovou technologii

U návrhu struktury rámce jsem vycházel z obecné struktury, jak je znázorněno na Obr. 4.3, definované rádiovým modulem vybraným pro návrh simulačního modelu

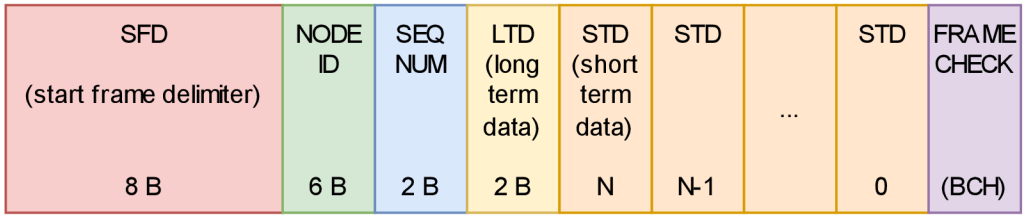
a také pro možnou budoucí implementaci v rámci ověření a optimalizace navrženého komunikačního protokolu.

Obr. 4.3: Znázornění základních bloků bezdrátového rámce dané typem radiového modulu.

Obecný rámec obsahuje několik povinných i nepovinných možností, které je potřeba nastavit. K tomu, jak všechny potřebné možnosti nastavit, může být využit návod uvedený [81]. Parametry potřebné k nastavení jsou:

- **Preamble** - je úvodní část rámce, která je použita k synchronizaci mezi vysílačem a přijímačem. Preambule se skládá ze sekvence opakujících se bitů, což je pomáhá přijímači detekovat a bezchybně přijímat data.
- **Syncword** - Synchronizační slovo slouží jako oddělovač v rádiovém rámci, po kterém se odmodulované bity uloží do Rx FIFO. Synchronizační slovo ze své podstaty také implementuje funkci filtrování/adresování paketů, protože rádiové pakety s jinými než očekávanými synchronizačními slovy jsou automaticky zahozeny.
- **Frame Header** - Záhlaví obsahuje logicky oddělené pole od pole Payload s možnými různými konfiguracemi. To znamená, že pole záhlaví může být vyloučeno z výpočtu CRC a rozkládání. Pole záhlaví může obsahovat nastavení délky (Lenght).
- **Payload** - Vlastní přenášená data.
- **CRC** - je počítáno na vysílací straně na dosud nekódovaném (ani FEC, ani symbolově kódovaném, ani rozkládaném (Whitening)) toku bajtů. Na přijímací straně se CRC vypočítá znovu na plně dekódovaném toku bajtů, a pokud se výsledek shoduje s přijatou hodnotou CRC, je příjem paketu považován za úspěšný.

Ze zmíněné obecné struktury byla navržena struktura rámce pro nový komunikační protokol, který je znázorněn na Obr. 4.4.



Obr. 4.4: Znázornění bloků navrženého bezdrátového rámce.

Povinná pole Preamble, Syncword a Header byla zahrnuta do bloku označeného jako SFD (start frame delimiter), délka tohoto bloku je 8 B.

Vedle dat, která jsou potřeba přenášet v co nejkratším čase, jako jsou např. informace o tom, že došlo ke změně konfigurace kardiostimulátoru, nebo došlo k přerušení spojení s elektrodami existují i informace, které se mění jen v delším časovém horizontu, např. konkrétní hodnoty nastavení šířky a amplitudy stimulačního impulzu.

Informace dlouhodobého charakteru tak není potřeba přenášet v každém datovém rámci. Jednou z možností je používat dva typy rámců - jeden pro data, která se mohou měnit rychle a často, a druhý pro data dlouhodobého charakteru. Použití dvou typů datových rámců by však vedlo ke zbytečně složitější rozhodovací logice jak na straně vysílače, tak i na straně přijímače.

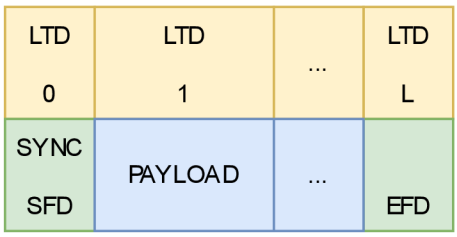
Proto bylo přistoupeno k návrhu unifikovaných datových rámců, které se budou přenášet:

- **NODE ID** a **SEQ NUM** - Identifikace přístroje a rámce,
- **LTD** - Long Term Data - Část dat dlouhodobého charakteru (nastavení přístroje, napětí baterie),
- **STD** - Short Term Data - Několik po sobě jdoucích hodnot dat krátkodobého charakteru (alarmové stavy).

Popis datového rámce pro dlouhodobá data - LTD

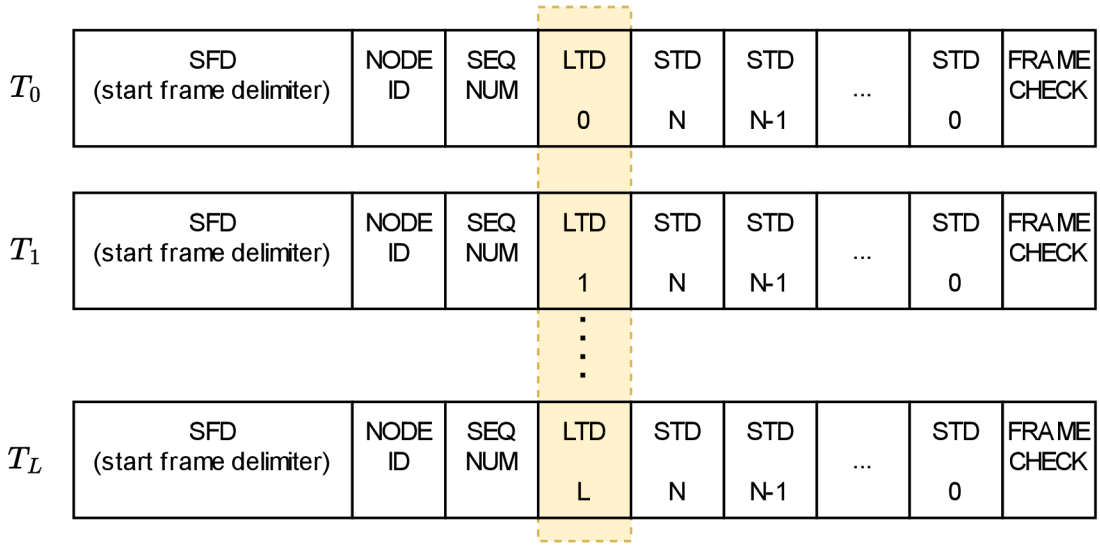
Tento model je částečně inspirovaný používáním multirámců v tradičním telekomunikačním provozu pro přenos signalizace informací mezi telefonními ústřednami na rozhraní typu E1 [99].

Multirámec pro přenos dlouhodobých dat je tak přenášen v několika po sobě jdoucích datových rámcích. Vzhledem k tomu, že počítáme i s případnými ztrátami při přenosu jednotlivých dílčích datových rámců, je třeba zajistit vhodné zabezpečení multirámce, který se obecně skládá z oddělovačů začátku a konce multirámce (SFD, EFD) a vlastních dat, jak je znázorněno na Obr. 4.5.



Obr. 4.5: Blokové znázornění oddělovačů začátku (SFD) a konce (EFD) obecného multirámce.

Struktura přenášených dat z kardiostimulátoru v multirámci T_0 až T_L je uvedena na Obr. 4.6.



Obr. 4.6: Blokové znázornění struktury multirámce pro kardiostimulátor.

Obsahem multirámce budou zejména následující data (jedná se o 16-ti bitová čísla):

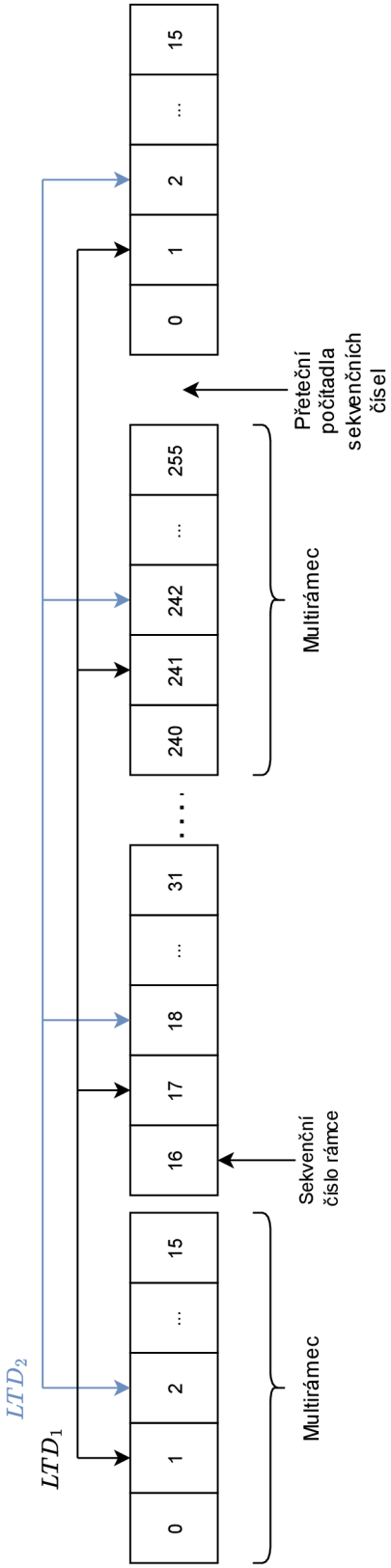
- Napětí baterie,
- Citlivost snímání QRS komplexu (kmitů stahu srdce),
- Frekvence stimulace,
- Amplituda stimulačního impulzu,
- Šířka stimulačního impulzu.

Pro přenos klíčových dat tedy potřebujeme celkem 5x2 B + 2 B pro identifikaci začátku a konce multirámce, tj. celkem 12 B. Zde můžeme s výhodou využít skutečnosti, že pro identifikaci dílčího datového rámce používáme 8-mi bitové sekvenční číslo. Multirámec je proto rozšířen na 16 B, tak aby se do jednoho cyklu číslování dílčích datových rámců vešel celistvý počet multirámců. Výsledkem je dvojí kontrola konzistence dat v multirámci a případná možnost kombinovat data z více po sobě jdoucích multirámců. Pro doplnění multirámce na 16 B jsou zopakovány klíčové hodnoty - frekvence stimulace a amplituda stimulačního impulzu. Podrobná struktura multirámce je zřejmá z Tab. 4.4.

Tab. 4.4: Podrobná struktura multirámce.

Označení	**Popis**
LTD_0	SFD - označení začátku rámce
LTD_1	Frekvence stimulace bity 8-15
LTD_2	Frekvence stimulace bity 0-7
LTD_3	Amplituda stimulačního impulzu bity 8-15
LTD_4	Amplituda stimulačního impulzu bity 0-7
LTD_5	Citlivost snímání QRS komplexu bity 8-15
LTD_6	Citlivost snímání QRS komplexu bity 0-7
LTD_7	Frekvence stimulace bity 8-15
LTD_8	Frekvence stimulace bity 0-7
LTD_9	Šířka stimulačního impulzu bity 8-15
LTD_{10}	Šířka stimulačního impulzu bity 0-7
LTD_{11}	Amplituda stimulačního impulzu bity 8-15
LTD_{12}	Amplituda stimulačního impulzu bity 0-7
LTD_{13}	Napětí baterie bity 8-15
LTD_{14}	Napětí baterie bity 0-7
LTD_{15}	EFD - označení konce rámce

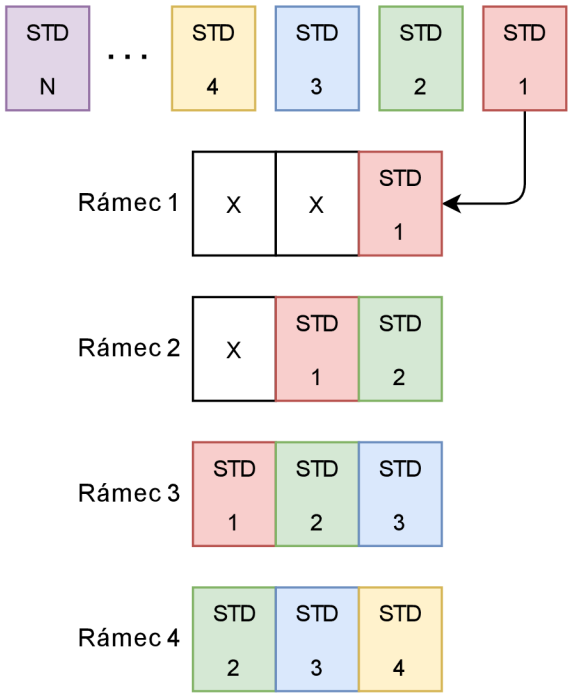
Zarovnání velikosti multirámce na dělitele rozsahu sekvenčních čísel přináší jednak možnost dodatečné kontroly integrity multirámce a případně i možnost doplňovat či kombinovat údaje z několika po sobě jdoucích multirámců, pokud nedošlo ke změně, což by bylo indikováno bitovým příznakem v poli STD některého z dílčích rámců. Vztah multirámců, poloh jednotlivých významových polí a sekvenčních čísel dílčích datových rámců je ilustrován na Obr. 4.7.



Obr. 4.7: Znázornění vztahu multirámců a sekvenčních čísel.

Popis datového rámce pro krátkodobá data - STD

Aby byla zajištěna největší pravděpodobnost doručení důležitých informací včas, tak již při návrhu struktury rámce je počítáno i s daty z předchozích časových úseků. Počet nutně opakovaných dat z předchozích časových úseků je analyzován v následující sek. 4.7. V poli krátkodobých dat $(STD_0, ..., STD_N)$, ve kterém se budou přenášet alarmové stavy ve formátu jejich příznaků, má jedna buňka délku 1 B. Toto pole tvoří tzv. kruhový buffer (vyrovnávací paměť), kdy do buňky pole STD_0 přichází aktuální data, a data z předchozích časových úseků se postupně posouvají v poli do dalších buněk STD_1 a tak dále, jak je znázorněno na Obr. 4.8. Tím je zajištěno, že pokud dojde k výpadku několika rámců, tak důležitá krátkodobá data budou doručena v následujících rámcích.



Obr. 4.8: Znázornění funkce kruhového bufferu pro zpracování STD rámců.

V poli krátkodobých dat označovaném jako STD, se přenáší převážně jednobitové stavové případně alarmové informace. Popis významu jednotlivých bitů tohoto pole je v Tab. 4.5.

Tab. 4.5: Význam jednotlivých bitů pole STD datového rámce.

Bit	Význam	
1	Režim činnosti	1 = stimulace jen v případě nečinnost srdce, 0 = stimulace nezávisle na činnosti srdce.
2	Režim činnosti	1 = stimulace v srdeční síni, 0 = stimulace v srdeční komoře.
3	Rezerva	pro budoucí použití
4	Srdeční aktivita	1 = vlastní aktivita srdce.
5	Stav elektrod	1 = elektrody připojeny, 0 = elektrody odpojeny. **Toto je jeden z klíčových alarmových stavů.**
6	Změna konfigurace	1 = konfigurace nezměněna, 0 = konfigurace změněna. **Toto je další z klíčových alarmových stavů.**
7	Baterie	1 = baterie je v pořádku, 0 = napětí baterie je kriticky nízké.
8	Rezerva	pro budoucí použití.

Vzhledem ke skutečnosti, že je navrhována koncepce komunikačního protokolu pouze pro vysílání, bez možnosti požadavku na opakování přenosu byly místo dostupného detekčního kódu CRC pro kontrolu rámců, navrženy BCH kódy, které zvládají nejen detekovat chyby, ale také je opravit. Úmysl využití BCH kódů nám také potvrzují informace uvedené v sek. 2.3.1, kdy díky možnosti snížení vysílacího výkonu, z důvodu úspor energie, by měl být rámec úspěšně doručen i za předpokladu zhoršení bitové chybovosti. Využití BCH kódů nám určuje přesnou délku rámce. V následující kapitole 4.5 je proto navrženo několik možných variant BCH kódů, které nám určují délky jednotlivých rámců.

4.5 Návrh BCH kódů na základě specifických vstupních parametrů

Pro návrhy BCH kódů se vychází z informací uvedených v sek. 2.4.1 a sek. 2.4.2. Pokud vycházet z obecného rámce, který je uveden na Obr. 4.4 a známe délku přenesených jednotlivých bloků, je možné pro něj navrhnout dvě hlavní varianty řešení, kdy první variantou je uvažována co nejkratší délka rámce a druhou variantou je rámec delší. Tyto dvě varianty budou popsány v následujících podkapitolách. Obě uvažované varianty obsahují povinné pole rámce, které nám určuje vybraný

bezdrátový modul a jsou obsahem pole SFD, které má pevnou délku 8 B.

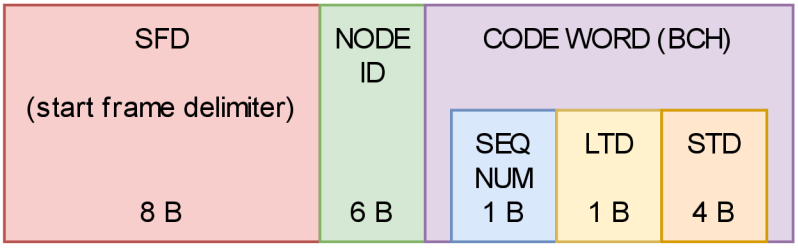
Také pole NODE ID, které nám identifikuje jednotlivé kardiostimulátory, nám může návrh použitého BCH kódu ovlivnit, jelikož NODE ID je dostatečně jedinečný, tak může být vyloučen z kódového slova, které bude chráněno proti chybám. I kdyby došlo v době vysílání NODE ID k jeho malému pozměnění vlivem rušení, vyhodnocovací systém by měl být schopen určit, o který kardiostimulátor se jedná. Pro ověření v rámci simulace, jakou váhu bude mít i výsledná délka rámce, na počet kolizí, byla také uvažována varianta zabezpečení veškerých bloků.

4.5.1 Varianta nejkratšího rámce

Pro první uvažovanou nejkratší možnou variantu byl uvažován rámec délky 22 B a nejdelší možnou variantou nejkratšího rámce, rámec délky 46 B. Tyto varianty jsou popsány níže.

Varianta bez zabezpečením NODE ID

V tomto případě bloky SEQ NUM, LTD, STD jsou zabezpečeny BCH kódem a podle jejich délky 6 B se vybírá použitý BCH kód, který nám ovlivní celkovou délku rámce. Při návrhu této nejkratší varianty je pro blok STD zvažována délka 4 B, kdy je obsahem aktuální informace a tři informace z předchozích časových úseků. Zabezpečený blok BCH kódem je označen jako kódové slovo (CODE WORD (BCH)) jak lze vidět na obrázku 4.9.



Obr. 4.9: Rámec a jejich zabezpečené bloky pro variantu bez zabezpečení bloku NODE ID.

Pokud chceme zabezpečit 6 B tj. 48 bitů, pro vybrání správného BCH kódu může být použita tabulka existujících BCH kódů uvedená v příloze A, kdy hledáme BCH kód, který dokáže zabezpečit minimálně k informačních bitů (48). Použitelné jsou tedy BCH kódy:

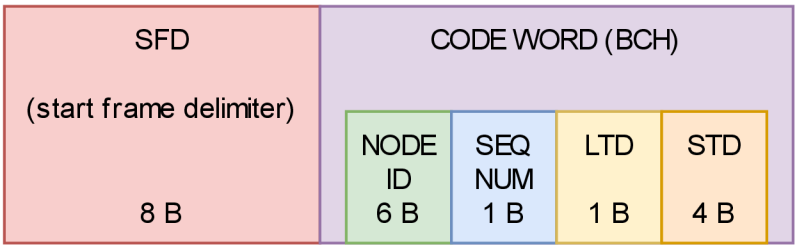
- BCH(63,51; t=2), odpovídající délce 8 B,
- BCH(127,50; t=13), odpovídající délce 16 B,
- BCH(255,55; t=31), odpovídající délce 32 B.

Z těchto možností BCH kódu je patrné, že pokud sečteme délky SFD + NODE ID a kódového slova BCH kódu, vidíme, že možné délky přenášeného rámce jsou:

- 22 B,
- 30 B,
- 46 B.

Varianta se zabezpečením NODE ID

Pokud zabezpečíme BCH kódem i blok NODE ID, jak můžeme vidět na Obr. 4.10, tak se dostaneme na délku dat 12 B.



Obr. 4.10: Rámec a jejich zabezpečené bloky se zabezpečení bloku NODE ID.

Vhodné BCH kódy, které umožňují zabezpečit 96 bitů jsou:

- BCH(127,99; t=4), odpovídající délce 16 B,
- BCH(255,99; t=23), odpovídající délce 32 B.

Z těchto možností BCH kódu patrné, že pokud sečteme délky SFD a kódového slova BCH kódu, vidíme, že jsou možné délky přenášeného rámce:

- 24 B,
- 40 B.

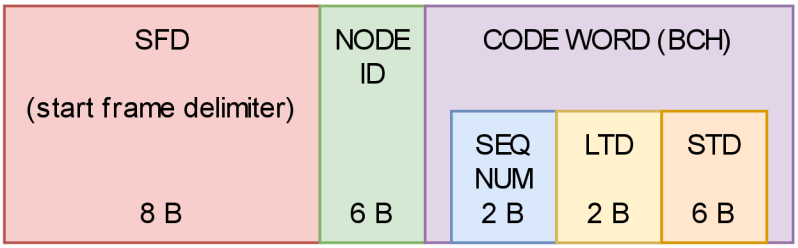
4.5.2 Varianta delšího rámce

Jako druhou variantu byl zvažován rámec, kdy bloky SEQ NUM, LTD, STD byly požadovány delší. Řešení můžeme opět rozdělit do dvou možností, kdy v jedné variantě nebudeme zabezpečovat blok NODE ID, abychom dostali co možná nejkratší možný rámec.

Varianta bez zabezpečením NODE ID

Na Obr. 4.11, můžeme opět vidět koncepci varianty, kdy počítáme se zabezpečením bloků SEQ NUM, LTD, STD.

Vidíme, že je potřeba zabezpečit 10 B tj. 80 bitů, pro vybrání správného BCH kódu nám opět poslouží tabulka existujících BCH kódů uvedená v příloze. Použitelné jsou tedy BCH kódy:



Obr. 4.11: Rámec a jejich zabezpečené bloky pro variantu bez zabezpečení bloku NODE ID.

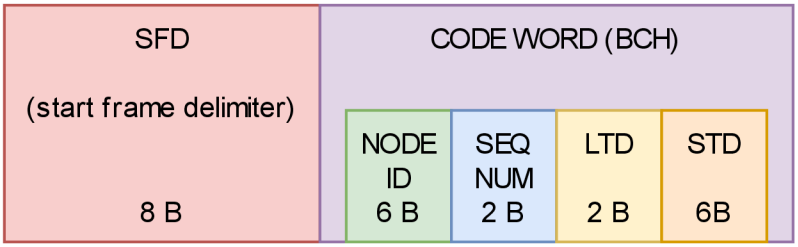
- BCH(127,85; t=6), odpovídající délce 16 B,
- BCH(255,87; t=26), odpovídající délce 32 B.

Z těchto možností BCH kódu je patrné, že pokud sečteme délky SFD + NODE ID a kódového slova BCH kódu, vidíme, že možné délky přenášeného rámce jsou:

- 30 B,
- 46 B.

Varianta se zabezpečením NODE ID

Pokud zabezpečíme BCH kódem i blok NODE ID, jak můžeme vidět na Obr. 4.12 tak se dostaneme na délku dat 16 B.



Obr. 4.12: Rámec a jejich zabezpečené bloky se zabezpečení bloku NODE ID.

Vhodné BCH kódy, které umožňují zabezpečit 128 bitů jsou:

- BCH(255,131; t=18), odpovídající délce 32 B.

U této navržené varianty BCH kódu je patrné, že pokud sečteme délky SFD a kódového slova BCH kódu, vidíme, že možná délka přenášeného rámce je:

- 40 B.

4.5.3 Shrnutí délky navržených rámců připravených pro simulace

V předchozích kapitolách bylo popsáno několik délek možných rámců, kdy k povinné části rámce byly navrženy možné délky BCH kódů a tím byly určeny možné délky rámce. Pro zopakování jsou délky zde znovu uvedeny: 22 B, 24 B, 30 B, 40 B, 46 B.

Tyto délky rámce poslouží jako vstupní data pro následné simulace, kdy přepočtem s bitovou rychlostí tvoří dobu přenosu jednoho rámce.

4.5.4 Generující polynomy pro navrhované BCH kódy

V předchozích částech byly navrženy čtyři možné varianty, jak může vypadat přenášený rámec. U těchto variant bylo zmíněno 7 možností BCH kódů. Pro jejich možnou implementaci a pro zakódování informačních bitů je potřeba znát i jejich generující polynomy. Jelikož budou uvažovány tři různé délky BCH kódů, budou využívány tři délky Galoisových těles $GF(2^6), GF(2^7), GF(2^8)$, jejichž prvky, spolu s jejich nerozložitelnými polynomy, jsou uvedeny např. v [63]. Následně je využito tolik nerozložitelných polynomů, aby bylo dle Bose-Chaudhuriho teorému $2t$ po sobě jdoucích kořenů. Zapsáním těchto nerozložitelných polynomů dle rovnice (2.1) a jejich vynásobením dostaneme generující polynom $g(x)$.

Pro zvažované BCH kódy jsou uvedeny jejich parametry n, k, t a jejich generující polynomy $g(x)$ v zápisu pomocí osmičkové soustavy.

1. BCH(63,51; t=2), 12471.
2. BCH(127,50; t=13), 5444651252331401242150142 1.
3. BCH(255,55; t=31), 7315425203501100133015275306032054325414.
4. BCH(127,99; t=4), 3447023271.
5. BCH(255,99; t=23), 1065666725347317422274141620157433225241107643230 3431
6. BCH(127,85; t=6), 130704476322273
7. BCH(255,87; t=26), 1101367634147432364352316343071720462067225452733 11721317
8. BCH(255,131; t=18), 2157133314715101512612502774421420241654 71.

Například pro první variantu BCH(63,51; t=2) přepíšeme generující polynom $g(x)$ zapsaný jako 12471 do binární podoby 001010100111001 a z ní následně může být převeden do polynomiálního tvaru $g(x) = x^{12} + x^{10} + x^8 + x^5 + x^4 + x^3 + 1$.

Takto navržené BCH kódy však jsou primárně určeny jako vstup pro simulaci délky doby přenášeného rámce, ale pro výslednou implementaci mohou být použity i jiné varianty BCH kódu, které budou mít pouze rozdílný poměr mezi informačními a zabezpečovacími bity. Tím nebudou ovlivněny výsledky simulací, založené na délce rámce a odpovídající době vysílání. Možné další varianty BCH kódů jsou uvedeny v příloze A.

4.6 Simulační model

Dostupné RF moduly podporují jen některé přenosové (bitové) rychlosti. Přenosovou rychlostí a délkou rámce je dána doba přenosu dat a tedy i doba, kdy může docházet ke kolizi s vysíláním dat jiného pacienta. Podobně BCH kódy podporují jen některé délky zprávy, která se skládá z informačních a zabezpečovacích bitů. Podle poměru velikosti vlastních dat k velikosti celé zprávy zabezpečení BCH kódem je určen počet případně chybných bitů, které je možné opravit. Proto je snaha optimalizovat dva parametry velikosti zprávy:

- celková délka zprávy,
- počet opravitelných chybných bitů.

S narůstající celkovou délkou zprávy roste počet pravděpodobnosti kolize s vysíláním od více pacientů. S počtem opravitelných bitových chyb roste odolnost protokolu vůči externím RF vlivům, která efektivně způsobují zhoršení SNR.

Kolize ve vysílání principiálně není možné vyloučit. U dat, která se mění rychle, je řešením tato data opakovat v několika po sobě jdoucích rámcích. Počet opakování zvyšuje délku rámce nebo snižuje kódový zisk BCH kódu a tím zvyšuje buďto pravděpodobnost kolize, nebo snižuje počet opravitelných bitů.

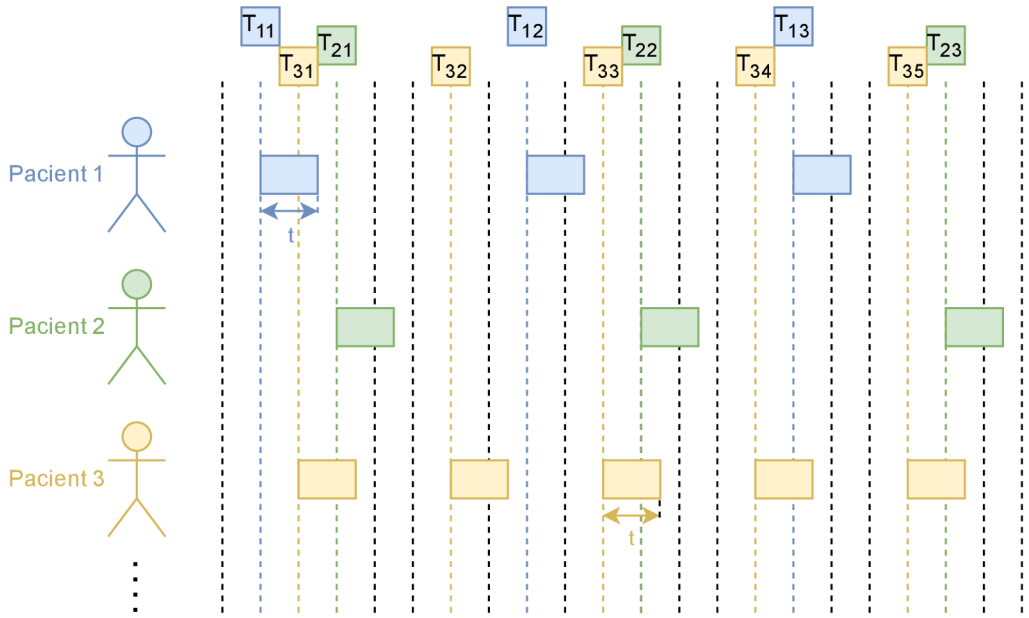
Simulační model má za úkol optimalizovat parametry obecného návrhu protokolu a to zejména:

- Stanovit optimální počet opakování časově rychle proměnných hodnot v datovém rámci.
- Stanovit maximální počet pacientů, kteří budou "viditelní" jednou základnovou stanicí tak, aby nedocházelo k významným ztrátám dat.

4.6.1 Konstrukce simulačního modelu

Na Obr.4.13 je uvedeno grafické znázornění situace, kdy Pacient1 který má na sobě aktivovaný nositelný externí kardiostimulátor periodicky na základě své tepové frekvence a variability srdce, v časových intervalech T_{11}, T_{12}, T_{13} odesílá datový rámec o časové délce t. S určitým časovým posunem začíná na základě své tepové frekvence vysílat i Pacient2 v časových intervalech T_{21}, T_{22}, T_{23} a také Pacient3 v časových intervalech T_{31}, T_{32}, T_{33}. Jak je ze znázorněné situace patrné, tak došlo ke kolizi rámců Pacienta1 a Pacient3 v intervalu T_{11} a T_{31} a také i Pacienta2 s Pacient3 v intervalu T_{31} a T_{21}, a podobně také v pozdějších intervalech.

Dle výše popsané situace bylo potřeba vytvořit simulační model, který by sloužil k vytvoření časových intervalů pro jednotlivé pacienty, které by reflektovaly vlastnosti základní tepové frekvence spolu s její variabilitou (HRV). Jako matematický



Obr. 4.13: Znázornění časových intervalů úderů srdce několika pacientů.

základ pro zkonstruování simulačního modelu byly využity informace z sek. 1.5.1, jehož algoritmus vytvoření v R Studiu je dále v textu popsán formou pseudokódu.

Algoritmus 1 pro simulaci tepové frekvence pacientů simuluje časové intervaly mezi údery srdce vybraných pacientů během rehabilitace. Jeho účelem je vytvořit časové série dat, které reprezentují nepravidelnosti v tepové frekvenci pacientů. Tyto série jsou generovány na základě náhodného výběru pacientů z populace s logaritmicko-normálním rozložením tepové frekvence. Simulace má za cíl modelovat a minimalizovat kolize při přenosu dat, což je důležité pro optimalizaci návrhu přenosového protokolu. Nejprve jsou uvedeny vstupy a výstupy a následně celý algoritmus

Vstupy algoritmu:

- M: celkový počet pacientů (např. 350), reprezentující celkový počet pacientů v nemocnici.
- N: počet pacientů, který se náhodně vybere z celkového počtu pacientů.
- REP: počet opakování simulace nad stejnou populací (např. 1000) pro statistickou významnost výsledků.
- T: délka časového intervalu, po který probíhá sledování (např. 1200 sekund).

Struktura simulačního algoritmu:

- Pro hodnoty velikosti vzorku N v rozsahu 4 až 10 se opakovaně vybírá náhodný vzorek N pacientů.

- Pro každého pacienta se určuje náhodný počáteční posun a simulují se časové intervaly mezi údery srdce na základě průměrné tepové frekvence a její variability.
- Vygenerované časové série (obsahující jednotlivé časy úderů srdce) jsou uloženy do samostatných souborů pro každého pacienta a opakování.

Algoritmus 1 Simulace tepové frekvence pacientů

Vstup: $M \leftarrow 350$ (počet pacientů), $REP \leftarrow 1000$ (počet opakování), $T \leftarrow 1200$ (délka intervalu rehabilitace)
for $N = 4$ **to** 10 **do**
  $Y \leftarrow$ logaritmicko-normální rozložení tepové frekvence pro M pacientů
  $P \leftarrow$ transformace Y na intervaly mezi údery srdce omezena na $[40, 180]$ úderů za minutu
  for $j = 1$ **to** REP **do**
    $Base \leftarrow$ náhodný výběr N pacientů z P
    $Tick \leftarrow$ prázdný seznam délky N
    for $i = 1$ **to** N **do**
      $\phi \leftarrow$ náhodný posun od 0 po $Base[i]$
      $t \leftarrow \{\phi\}$
      $n \leftarrow T/Base[i] + 1$
      $HRV \leftarrow$ normální rozložení s odchylkou $0.2 \times Base[i]$
      for $k = 1$ **to** n **do**
        $t \leftarrow t \cup \{t[k] + Base[i] + HRV[k]\}$
      end for
      $Tick[i] \leftarrow t$
    end for
    for $i = 1$ **to** N **do**
      Ulož data $Tick[i]$ do souboru `Serie_j_Person_i.csv`
    end for
  end for
end for

Výstupy: Algoritmus 1 ukládá výsledky pro každého pacienta a každé opakování simulace do samostatného CSV (Comma Separated Values) souboru. Tyto soubory lze využít k následné analýze kolizí při přenosu dat a k optimalizaci rehabilitačních procesů.

Pro zpracování výsledků navrženého simulačního modelu byl vytvořen systém pro vyhledávání a vyhodnocení kolizí v prostředí Matlab, který je popsán v následující části.

4.6.2 Implementace systému pro vyhledávání a vyhodnocení kolizí

Vzhledem ke kritické povaze přenosu dat v reálném čase v lékařských systémech, jako jsou externí kardiostimulátory, je minimalizace kolizí zásadní pro zajištění spolehlivé komunikace. Navržený systém se zaměřuje na detekci a řízení kolizí v signálních rámcích vytvářených zařízeními, což je nezbytné pro optimalizaci komunikačních protokolů s nízkou spotřebou energie.

Systém zpracovává vstupní data, která se skládají ze seznamu zařízení a signálových rámců (nebo impulzních rámců), které produkují. Tyto signální rámce jsou analyzovány za účelem identifikace kolizí, které mohou narušit spolehlivou komunikaci v systémech reálného času, jako jsou kardiostimulátory. Systém pro vyhledávání a vyhodnocování kolizí je systém sérií algoritmů, které byly navrženy v prostředí Matlab a jsou popsány několika pseudokódy uvedenými níže.

Navržené algoritmy jsou klíčové pro odhalení potenciálních kolizí v datových rámcích přenášených více zařízeními pracujícími ve stejném prostředí. Včasnou identifikací takových kolizí můžeme optimalizovat komunikační protokol tak, aby data z jednotlivých zařízení byla přenášena spolehlivě a bez chyb.

Algoritmus 2 Kontrola kolizí v matici

```
Vstup: F (pole buněk), rowSize, columnSize
Výstup: C (pole buněk s informacemi o kolizích)
Inicializace C jako pole buněk o velikosti (rowSize × columnSize)
for row = 1 to rowSize do
    for column = 1 to columnSize do
        intervalToCheckCell ← F[row, column]
        if intervalToCheckCell ≠ empty then
            if intervalToCheckCell = 0 then
                continue
            end if
            hasCollision ← findCollision(F,
                    intervalToCheckCell, row,
                    rowSize, columnSize)
            C[row, column] ← hasCollision
        end if
    end for
end for
```

V Algoritmu 2 pro kontrolu kolizí v matici se inicializuje pole buněk C, do kterého se ukládají informace o kolizích pro každou buňku v matici F. Algoritmus prochází

každou buňku v matici pomocí vnořených smyček nad řádky a sloupci. Pro každou buňku načte interval z matice F a zkontroluje, zda není prázdný a nenulový. Pokud jsou tyto podmínky splněny, zavolá algoritmus funkci *findCollision*, aby zjistil, zda interval nekoliduje s jinými intervaly v matici. Výsledek kontroly kolize je pak uložen do pole C. Tento proces zajišťuje, že každá buňka v poli C odpovídá tomu, zda existuje kolize s jinými intervaly v matici, což umožňuje komplexní analýzu překryvů.

Algoritmus 3 Vyhledání kolize v matici

```
Vstup: F (cell array), intervalToCheckCellInput (interval pro kontrolu),
rowToSkip, rowSize, columnSize
Výstup: hasCollision (boolean určující, zda byla nalezena kolize.)
hasCollision ← false
for row = 1 to rowSize do
    if row = rowToSkip then
        continue
    end if
    for column = 1 to columnSize do
        intervalToCheckCell ← F[row, column]
        if intervalToCheckCell ≠ empty then
            if intervalToCheckCell = 0 then
                continue
            end if
            isOverlap ← isIntervalOverlapping(
                    intervalToCheckCellInput[1],
                    intervalToCheckCellInput[2],
                    intervalToCheckCell[1],
                    intervalToCheckCell[2])
            if isOverlap then
                hasCollision ← true
                return
            end if
        end if
    end for
end for
```

Algoritmus 3 pro vyhledávání kolizí v matici je navržen tak, aby určil, zda interval z určité buňky koliduje s jinými intervaly v matici F. Jako vstupy přijímá matici F, interval, který má být kontrolován, a index řádku, který má být vynechán. Funkce prochází všechny řádky a sloupce matice s výjimkou řádku obsahujícího interval,

který má být kontrolován. Pro každou buňku načte interval, přeskočí prázdné nebo nulové intervaly a pomocí funkce *isIntervalOverlapping* ověří, zda se aktuální interval překrývá se zadaným intervalem. Pokud je zjištěn jakýkoli překryv, funkce nastaví příznak kolize na hodnotu true a okamžitě se vrátí. V opačném případě ukončí prohledávání a vrátí hodnotu false.

Algoritmus 4 Kontrola překrývání intervalů

Vstup: $x1$, $x2$ (interval 1), $y1$, $y2$ (interval 2)
Výstup: $isOverlap$ (boolean určující, zda se intervaly překrývají.)
$isOverlap \leftarrow (x1 \leq y2 \wedge y1 \leq x2)$

Algoritmus 4 pro kontrolu překrývání intervalů určuje, zda se dva intervaly překrývají. Přijímá čtyři parametry představující počáteční a koncové body dvou intervalů. Funkce vyhodnotí, zda se intervaly protínají a to tak, že zkontroluje, zda konec prvního intervalu není menší než začátek druhého intervalu a zda konec druhého intervalu není menší než začátek prvního intervalu. Pokud jsou tyto podmínky splněny, považují se intervaly za překrývající se a funkce vrátí hodnotu true; v opačném případě vrátí hodnotu false. Tato funkce je klíčová pro zjišťování překryvů ve funkci *findCollision*.

Jednou z důležitých metrik, která je z matice kolizí získána, je řada po sobě jdoucích kolizí. Pro zjištění takové řady slouží Algoritmus 5, který představuje funkci, která počítá posloupnosti po sobě jdoucích kolizí ve vstupním poli (obsahuje jedničky a nuly; jednička je kolize a nula nikoli). Funkce hledá po sobě jdoucí kolize v rozsahu od dvou do nejdelší po sobě jdoucí řady kolizí v daném poli. Funkce inicializuje pole, které uchovává počty pro každou délku posloupnosti, a poté iteruje přes každou možnou délku od 2 do N. Pro každou délku prohledá vstupní pole a spočítá, kolikrát se v něm objeví posloupnost po sobě jdoucích jedniček dané délky. Pokud se počet po sobě jdoucích jedniček rovná aktuální délce, funkce zkontroluje, zda posloupnost končí nulou nebo na konci pole, a pokud ano, zvýší počet platných posloupností. Pokud počet překročí požadovanou délku, vynuluje se. Nakonec funkce uloží počet platných sekvencí pro každou délku a vrátí pole obsahující tyto počty.

Dalšími důležitými ukazateli, které shromažďujeme, jsou celkový počet impulzů, celkový počet kolizí, nejdelší po sobě jdoucí série kolizí a procento kolizí. Ty jsou důležité pro další zkoumání a statistickou analýzu.

Úkolem simulačního modelu je analýza pravděpodobnosti vzniku kolizí ve vysílání jednotlivých uživatelů nositelných externích kardiostimulátorů v závislosti na počtu uživatelů, kteří jsou v dosahu dané přijímací stanice, délky přenášené datové zprávy a přenosové rychlosti.

Pravděpodobnost vzniku kolizí je třeba analyzovat zejména z pohledu počtu po

Algoritmus 5 Počítání po sobě jdoucích kolizí v sériích o délce 2 až N

```
function countConsecutiveCollisionsInSeries(array, N)
    Vstup:
        array (pole celých čísel, kde 1 označuje část zájmové sekvence.)
        N (maximální délka kontrolované řady)
    Výstup:
        numSeriesArray (pole celých čísel, kde každá položka na indexu k−1 označuje počet nalezených po sobě jdoucích sekvencí délky k.)
    numSeriesArray ← zero array of length N − 1
    for k = 2 to N do
        count ← 0
        numSeries ← 0
        for i = 1 to length(array) do
            if array[i] = 1 then
                count ← count + 1
                if count = k then
                    if (i + 1 ≤ length(array) ∧ array[i+1] ≠ 1) ∨ (i = length(array)) then
                        numSeries ← numSeries + 1
                        count ← 0
                    end if
                else if count > k then
                    count ← 0
                end if
            else
                count ← 0
            end if
        end for
        numSeriesArray[k-1] ← numSeries
    end for
    return numSeriesArray
end function
```

sobě jdoucích kolizí, neboť podle maximální velikosti bloku po sobě jdoucích kolizí je třeba nastavit počet opakování kritických dat, případně upravit velikost datového bloku nebo přenosovou rychlost.

Zjištění nejdelšího souvislého bloku kolizí a analýza počtu po sobě jdoucích kolizí se sice slovně snadno popíše, ale provedení podrobné analýzy, tj. zjištění počtu dvojic, trojic, případně delších sekvencí po sobě jdoucích kolizí není algoritmicky snadné. Pro tuto analýzu bylo vyvinuto několik algoritmů popsaných v kapitole 4.6, které postupně vytvoří matici kolizí pro přenosy jednotlivých datových rámců a následně v této matici vyhledávají souvislé bloky kolizí zadané délky.

4.7 Simulace a zhodnocení získaných výsledků

Model dedikované bezdrátové komunikace externích kardiostimulátorů má řadu parametrů:

- přenosová rychlost a celková velikost datového rámce,
- počet opakování kritických dat,
- počet opravitelných bitových chyb,
- počet současně komunikujících uživatelů.

Tyto parametry jsou určitým způsobem provázané. Vzájemná závislost těchto parametrů a tím určené omezení jsou diskutovány v následujícím textu.

Cílem simulací není najít to jediné správné řešení, ale stanovit hranice použitelnosti komunikačního protokolu pro očekávané scénáře použití. V praxi je proto možné použít více variant protokolu (nastavení parametrů) pro různé scénáře použití kardiostimulátoru.

První scénář použití, který byl podnětem k této analýze, je použití nositelného externího kardiostimulátoru u pacientů, kteří rehabilitují např. po chirurgickém zákroku nebo po aplikaci defibrilátoru. Tito pacienti se pohybují po chodbách a schodištích nemocnice obvykle v počtu 1 až 3 pacientů.

Druhý známý scénář použití je klidový režim pacientů, kdy pacienti odpočívají na lůžku a může tak být v dosahu jednoho přijímače více pacientů, t.j. vysílačů. Zde se dá očekávat 4 až 10 pacientů v dosahu jednoho přijímače. Není přímo nutné použít pro oba scénáře zcela stejný komunikační protokol, je to však výhodné z pohledu jednoduchosti konstrukce a ovládání kardiostimulátorů.

4.7.1 Přenosová rychlost a celková délka datového rámce

Dostupné RF čipy podporují pouze některé modulační formáty a přenosové rychlosti. Přenosová rychlost a celková velikost datového rámce určují společně dobu přenosu rámce a tím pro daný počet uživatelů určují i pravděpodobnost kolize či

více po sobě jdoucích kolizí ve vysílání. Na druhou stranu s vyšší rychlostí rostou nároky na kvalitu RF signálu a tím i vysílaný výkon. Vysílaný výkon má samozřejmě bezprostřední vliv na spotřebu energie.

Do celkové velikosti datového rámce se promítá několik vlivů:

- Délka preambule - tato délka je konstantní a je určena typem a konfigurací použitého RF čipu.
- Délka bloku dat zabezpečeného pomocí BCH kódu. Zde je na výběr několik možností popsaných v sek. 4.5. Tento blok obsahuje vlastní přenášená data a zabezpečovací kód, který slouží pro případné opravy bitových chyb.
- Délka bloku bez zabezpečení BCH kódem, pokud je takový blok použit.

Pro přehlednost jsou vstupní parametry pro simulace uvedeny v Tab. 4.6, kdy jsou uvedeny délky možných rámců jako Data v bytech, možné bitové rychlosti a následně délka doby vysílání.

Tab. 4.6: Délky datových rámců a jejich vysílací doby v závislosti na bitové rychlosti

Data [B]	**22**	**24**	**30**	**40**	**46**
Bitová rychlost [kb/s]	**doba vysílání [ms]**				
38,4	4,583	5,000	6,250	8,333	9,583
50	3,520	3,840	4,800	6,400	7,360
100	1,760	1,920	2,400	3,200	3,680
120	1,466	1,600	2,000	2,667	3,067
200	0,880	0,960	1,200	1,600	1,840
500	0,352	0,384	0,480	0,640	0,736
2000	0,088	0,096	0,120	0,160	0,184

Na základě uvedené tabulky byly provedeny simulace pro vybrané doby vysílání, které jsou uvedeny v příloze D.

Jako příklad uvažujme nejdelší navrženou variantu přenášeného rámce tedy 46 B a pro nejmenší bitovou rychlost 38,4 kb/s, jsou výsledky simulací uvedeny v příloze v Tab. D.1, tato tabulka nám dává pohled na závislost počtu po sobě jdoucích kolizí a počtu jejich výskytů na počet osob, které mají vysílací kardiostimulátor při rehabilitaci. Tato varianta rámce má svou délkou navrženého BCH kódu největší potenciál pro jeho optimalizaci z hlediska počtu opakování dat. Ale zároveň, jak je zřejmé, s rostoucím počtem uživatelů se úměrně zvyšuje počet po sobě jdoucích kolizí, které mají za důsledek potřebu zvyšování opakování dat z předchozích intervalů. Pokud by byla vyžadována stoprocentní jistota přenesených dat, tak by bylo potřeba pro 10 sledovaných pacientů vložit do rámce třináct datových informací z předchozích rámců. Pokud k tomu připomeneme informaci, že data musí být vysílána v závislosti

na tepové frekvenci, tak pro nejjednodušší příklad, kdy je tepová frekvence 60 tepů za minutu, tak by mohla vzniknout situace, kdy data jsou úspěšně přenesena až po třinácti vysílacích intervalech tj. za 13 s. Za předpokladu, že by byla akceptovatelná ztráta dat do 10-ti promile, tak by stačilo vložit deset datových informací z předchozích rámců. Pokud budeme zvažovat scénář, kdy budou rehabilitovat maximálně 4 pacienti, tak je potřeba vložit 8 datových informací z předchozích intervalů, respektive 5 pokud bychom akceptovali pravděpodobnost ztráty dat do 25-ti promile.

Některé kombinace přenosové rychlosti a velikosti datového rámce vedou bohužel k relativně dlouhé době přenosu a tím pádem i k vyšší pravděpodobnosti výskytu kolizí a kolizí s vícenásobným opakováním a nejsou proto v praxi použitelné. Provedená simulace pomohla identifikovat takové kombinace. Jako použitelné pro praktickou implementaci tak byly vytipovány přenosové rychlosti 100 – 500 kb/s a délky rámců 24 B a 40 B.

4.7.2 Počet opakování kritických dat

Pokud dojde ke ztrátě kriticky důležitých dat, je třeba jejich vysílání co nejdříve zopakovat. Proto jsou kritická data vysílána v několika po sobě jdoucích datových rámcích. Pokud je počet opakování těchto dat větší, než maximální počet po sobě jdoucích kolizí, budou tato data nakonec úspěšně doručena k cíli (byť se zpožděním několika datových rámců).

Počet po sobě jdoucích kolizí roste s délkou datového rámce (respektive dobou jeho přenosu) a s počtem současně vysílajících stanic (uživatelů v dosahu daného přijímače).

Kritická data můžou obsahovat i alarmové stavy (např. odpojení elektrod kardiostimulátoru nebo vybití baterií) a proto není možné počet opakování zvyšovat nad jistou obecně přijatelnou hranici. Zvýšení počtu opakování kritických dat sice přispěje ke zvýšení pravděpodobnosti doručení těchto dat, data doručená po určité době ale přestávají mít smysl. Např. informaci o odpojení elektrod od kardiostimulátoru je nutné doručit co nejdříve.

Doba doručení kritických dat je obvykle vyjádřena v běžných časových jednotkách, t.j. v sekundách. Okamžik vysílání kardiostimulátoru je však určen tepovou frekvencí uživatele a dobu doručení proto potřebujeme stanovit v počtu úderů srdce uživatele. Na druhou stranu i maximální přípustná doba doručení zprávy, t.j. doba od kdy je ohroženo zdraví a život uživatele, není jednoznačně definovaná konstanta a může souviset m.j. i s tepovou frekvencí.

Po diskusi s lékaři byla maximální přípustná doba doručení zprávy stanovena jako 8 úderů srdce, t.j. maximální počet opakování kritických dat je stanoven jako 8 opakování.

Nižší počet opakování samozřejmě vede ke kratší době přenosu rámce a tím i nižší pravděpodobnosti vzniku kolizí. Vzhledem ke způsobu konstrukce datových rámců navrhovaného protokolu a tím daným omezením na velikost rámce a počet opakování kritických zpráv není možné optimální hodnoty stanovit analytickým způsobem a bylo proto nutné provést simulaci.

4.7.3 Počet opravitelných bitových chyb

S růstem počtu opravitelných bitových chyb se snižují nároky na poměr SNR a tím i vysílací výkon a tím pádem spotřebu energie. I tato hodnota má své pragmatické omezení. Počet opravitelných bitových chyb je dán velikostí BCH bloku a velikostí přenášených dat.

Podporované velikosti přenášených datových bloků a jim odpovídající počty opravitelných bitových chyb byly diskutovány v sek. 4.5 a přehledně uvedeny v tabulce v příloze A. Pro navrhovaný komunikační protokol jsou vhodné velikosti BCH bloků 63, 127 a 255 bitů. Delší BCH bloky by z pohledu počtu opravitelných bitových chyb již nepřinesly užitek a naopak by vedly ke zvýšení pravděpodobnosti kolizí a opakovaných kolizí.

V případě kratších BCH bloků je možné nechat některé datové pole nezabezpečené. Vhodným kandidátem je NODE ID. V případě opravitelných bitových chyb lze předpokládat, že bitové chyby jsou rozmístěny napříč datovým rámcem přibližně rovnoměrně (jsou způsobeny především šumem). V případě vyššího počtu opravitelných bitových chyb (pokud by bylo skutečně nutné takový počet chyb opravovat) lze očekávat, že se adekvátní počet bitových chyb vyskytne i v nezabezpečené preambuli datového rámce, případně nezabezpečeném datovém poli. Pokud tyto datová pole nebudou mít specifické vlastnosti (dostatečná Hammingova vzdálenost mezi použitelnými hodnotami) BCH zabezpečení zbytku datového rámce nepřinese kýžený efekt.

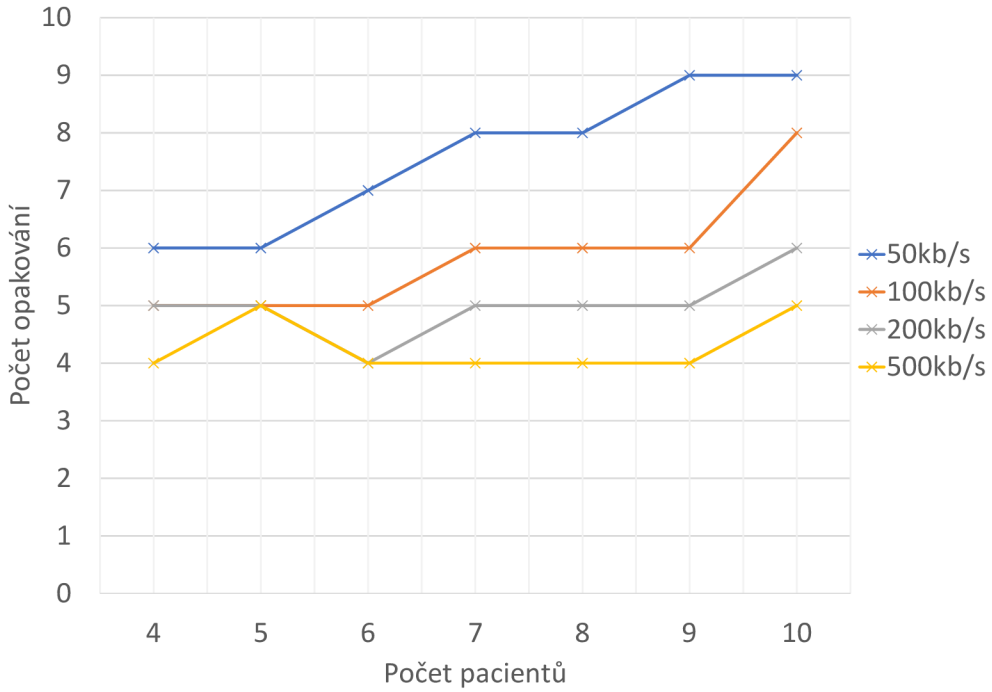
4.7.4 Počet současně komunikujících uživatelů

Snahou pro nastavení optimálních parametrů navrženého datového protokolu je maximalizovat možný počet současně komunikujících uživatelů. Minimální požadovaný počet současně komunikujících uživatelů je 4. Maximální počet není z principu omezen, je třeba jej však odhadnout pomocí simulace.

Vyšší počet současně komunikujících uživatelů vede k vyšší pravděpodobnosti vzniku kolizí při vysílání. V Tab. 4.7 jsou uvedeny výsledky simulací pro různé počty současně komunikujících uživatelů pro jednotlivé přenosové rychlosti a nutný počet opakování kritických dat pro variantu navrženého bezdrátového rámce o délce 40 B. Tato závislost je také názorně vynesena v grafu na Obr. 4.14.

Tab. 4.7: Tabulka přenosových rychlosti pro různý počet pacientů a opakování pro délku rámce 40 B

Bitová rychlost [kb/s]	**38,4**	**50**	**100**	**200**	**500**	**2000**
Doba vysílání [ms]	**8,333**	**6,400**	**3,200**	**1,600**	**0,640**	**0,160**
Počet pacientů	**Počet opakování**					
4	8	6	5	5	4	3
5	6	6	5	5	5	3
6	8	7	5	4	4	3
7	8	8	6	5	4	3
8	10	8	6	5	4	4
9	11	9	6	5	4	3
10	13	9	8	6	5	4



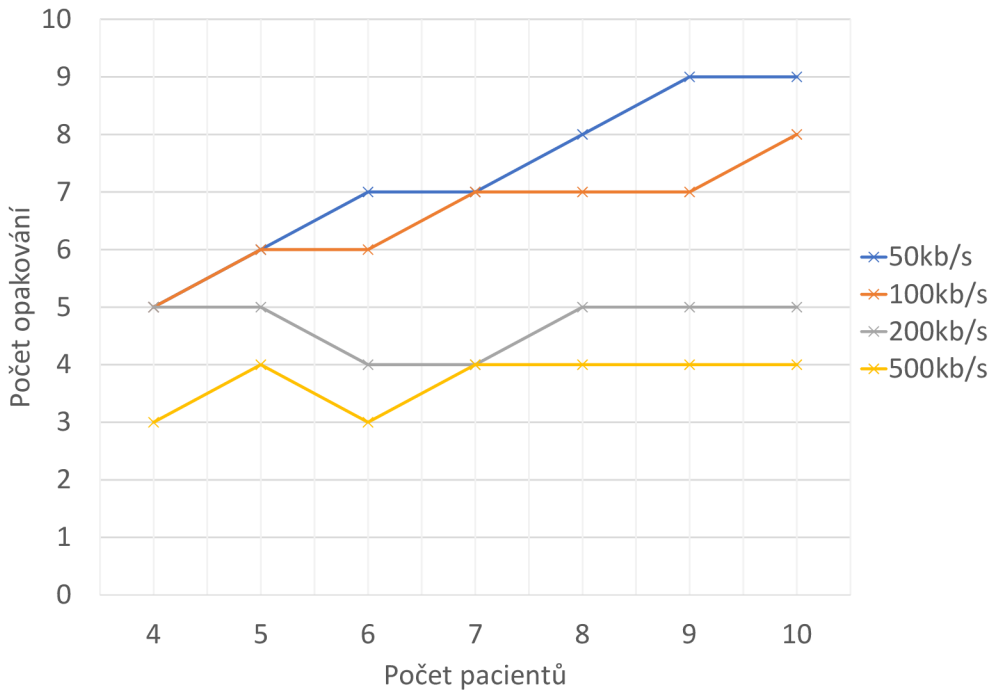
Obr. 4.14: Závislost počtu pacientů na nutném počtu opakování pro délku rámce 40 B pro různé přenosové rychlosti.

Tyto výsledky vycházejí z možných variantních simulací, které jsou uvedeny v příloze D, kdy bylo provedeno shrnutí pro jednotlivé přenosové rychlosti a nutný počet vložených opakování dat předchozích intervalů tak, aby byla zajištěna stoprocentní pravděpodobnost doručení dat.

V Tab. 4.8 jsou pak uvedeny výsledky pro různé počty současně komunikujících uživatelů pro jednotlivé přenosové rychlosti a nutný počet opakování kritických dat pro variantu navrženého bezdrátového rámce o délce 24 B, tato závislost je také vynesena v grafu na Obr. 4.15.

Tab. 4.8: Tabulka přenosových rychlosti pro různý počet pacientů a opakování pro délku rámce 24 B

Bitová rychlost [kb/s]	**38,4**	**50**	**100**	**200**	**500**	**2000**
Doba vysílání [ms]	**5,000**	**3,840**	**1,920**	**0,960**	**0,384**	**0,096**
Počet pacientů	**Počet opakování**					
4	5	5	5	5	3	3
5	6	6	5	5	4	3
6	7	6	5	4	3	3
7	7	7	6	4	4	3
8	8	7	5	5	4	4
9	9	7	5	5	4	3
10	9	8	6	5	4	3



Obr. 4.15: Závislost počtu pacientů na nutném počtu opakování pro délku rámce 24 B pro různé přenosové rychlosti.

Z těchto tabulek a grafů je patrné, že pro 10 pacientů a při dodržení maximálního počtu opakování, které bylo po diskusi s lékaři odhadnuto jako 8, jsou pro velikosti přenášených rámců ideální tyto přenosové rychlosti:

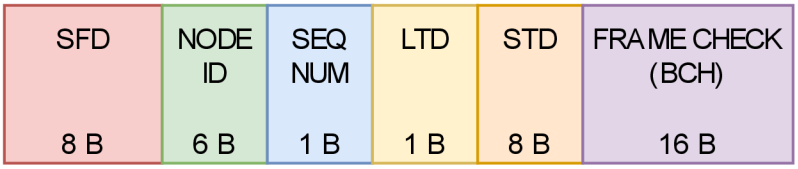
- pro 40B – 100 kb/s,
- pro 24B – 50 kb/s.

Je však třeba zdůraznit, že u navrženého rámce o délce 24 B jsme limitováni vybraným BCH kódem BCH(127,99), který zvládne opravit až 4 bitové chyby a počítá se u něj v poli STD o délce 4 B s počtem opakování 4, kdy rozšíření pole STD na 8 B není možné. Pro vyřešení této situace jsou tři možnosti:

- **Zvýšení přenosové rychlosti:** neupravovat BCH kód, ale zvýšit přenosovou rychlost na 500 kb/s.
- **Snížení počtu současně komunikujících uživatelů**.
- **Úprava BCH kódu se snížením současně komunikujících uživatelů**.

Optimalizace koncepce bezdrátového rámce

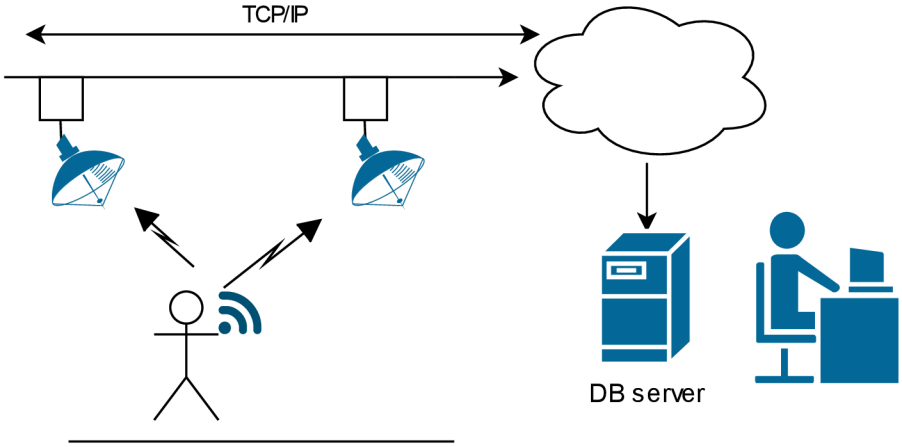
Na základě výsledků simulací, které jsou uvedeny v předchozích podkapitolách lze konstatovat, že jako nejvhodnější se jeví rámec s délkou 40 B. Tento rámec se vyznačuje použitelností až pro 10 současně komunikujících pacientů, při zaručené minimální přenosové rychlosti 100 kb/s. Délka navrženého rámce je vyhovující, ale bylo potřeba upravit strukturu, konkrétně délky jednotlivých bloků, kdy v sek. 4.5, bylo počítáno s delším sekvenčním číslem (SEQ NUM) a delším blokem pro pomaleji se měnící data (LTD). Struktura původně navrženého konceptu rámce, je upravena a jeho optimalizované rozložení jednotlivých bloků je na Obr. 4.16.



Obr. 4.16: Optimalizovaný rámec délky 40 B a velikosti jednotlivých bloků.

5 Zásady pro implementaci vlastního řešení

Tato kapitola se zabývá koncepcí rádiového modulu a základnové stanice. Na Obr. 5.1 je znázorněný uvažovaný scénář, kdy pacient s kardiostimulátorem se může pohybovat blízko jedné nebo více základnových stanic. Základnové stanice přijmou pomocí navrženého bezdrátového protokolu datový rámec, ten je následně obalen do hlaviček TCP/IP protokolu a následně je odeslán na databázový server, který může být umístěný kdekoli v infrastruktuře nemocničního zařízení. V databázovém serveru jsou zpracována přijatá data, která mohou být zobrazena ošetřujícím lékařem pro kontrolu stavu pacienta.



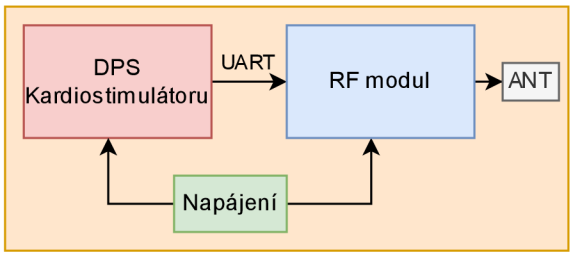
Obr. 5.1: Znázornění scénáře přenosu informací z kardiostimulátoru.

5.1 Radiofrekveční modul pro kardiostimulátor

Radiofrekvenční modul pro kardiostimulátor musí akceptovat navržený koncept komunikačního protokolu. Pro fyzické umístění modulu je v šasi kardiostimulátoru relativně malý prostor o rozměrech přibližně 14x45 mm. Do tohoto prostoru je třeba umístit vlastní RF čip, anténu a nezbytné pasivní součástky pro impedanční přizpůsobení spoje RF modul - anténa. Přitom umístění antény, jak bylo již řečeno, má klíčový význam pro dosažení dobré kvality signálu. Blokové schéma radiofrekvenčního modulu a jeho napojení na kardiostimulátor je znázorněno na Obr. 5.2.

Radiofrekvenční modul bude s vlastním kardiostimulátorem komunikovat na rozhraní UART rychlostí 19 kb/s. Přenos dat bude synchronizován příchodem dat, komunikační protokol bude implementován v radiofrekvenčním modulu. Z důvodu minimalizace nároků na prostor i spotřebu energie bude použit RF čip na bázi architektury ARM Cortex-M33, který poskytuje dostatečný výpočetní výkon i možnosti

programování a umožní tak přímou implementaci navrženého komunikačního protokolu.

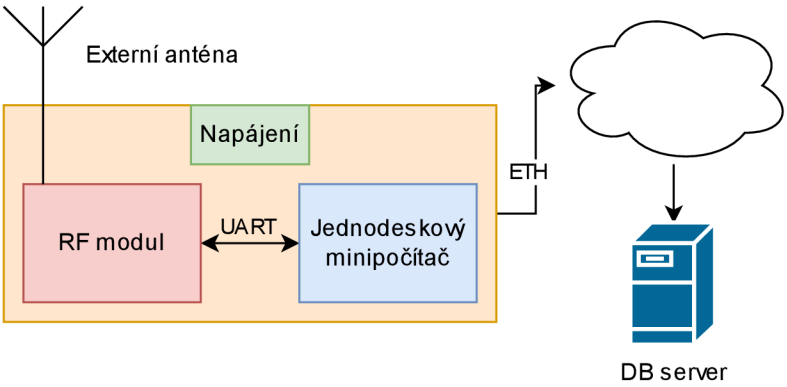


Obr. 5.2: Blokové řešení kardiostimulátoru a RF modulu.

V základnové stanici bude použit shodný RF čip nakonfigurovaný pro příjem. To usnadní zajištění kompatibility vysílače a přijímače na nejnižších úrovních komunikace.

5.2 Koncepce základnové stanice

Oproti řešení RF modulu pro kardiostimulátor, kdy je dbáno na co nejmenší velikost a největší úsporu energie odebírané z baterie, je řešení základnové stanice méně náročné. V případě základnové stanice je plánována pevná instalace s externím napájením, ať už pomocí externího zdroje, nebo pomocí PoE (Power over Ethernet) a větší externí anténou. Je tedy možné základnovou stanici plánovat větší a zároveň s vyšším výpočetním výkonem pro zpracování dat. Navržená základnová stanice je tvořena ze základních bloků, které jsou znázorněny na Obr. 5.3. RF modul je stejný jako u modulu pro kardiostimulátor.



Obr. 5.3: Blokové řešení základnové stanice.

Proces příjmu rámců a následné zpracování můžeme shrnout do těchto bodů:

- **Příjem rámce** - rámec je přijat na vstup rádiového modulu a je uložen do paměti.
- **Kontrola BCH** - po příjmu celého rámce následuje proces dekódování BCH kódu. Vzhledem k vyšší výpočetní náročnosti dekódovacího procesu, je přijatý rámec předán pomocí UART rozhraní z RF modulu do malého výkonnějšího jednodeskového minipočítače, jakým může být např. Raspberry Pi. Zde je možné implementovat algoritmus pro dekódování rámce, který je popsán v sek. 2.4.3.
- **Zapouzdření do TCP/IP** - pokud dle předchozího kroku, byl rámec dekódován a vyhodnocen jako bezchybný, popřípadě byly chyby opraveny, je rámec obalen do TCP/IP hlavičky a předán na ethernetové rozhraní.
- **Odeslání** do databázového serveru umístěného v infrastruktuře nemocničního zařízení.

Jakmile budou data přijata databázovým serverem, je provedena jejich kontrola z hlediska duplicity (příjmu z více základnových stanic) a následně jsou dále zpracována a mohou být zobrazena ošetřujícím lékařem.

Závěr

Hlavním cílem předkládané disertační práce byla analýza komunikačních potřeb a možností nositelných externích kardiostimulátorů a návrh koncepce dedikovaného komunikačního protokolu pro tento typ kardiostimulátorů.

Navržená koncepce komunikačního protokolu přitom respektuje komunikační potřeby a technická omezení dostupných prostředků a je tak připravena pro reálné nasazení.

Provedená analýza komunikačních potřeb a omezení nositelných externích kardiostimulátorů byla základem pro sestavení simulačního modelu. Simulační model pak posloužil pro optimalizaci parametrů navrženého konceptu komunikačního protokolu a stanovení hraničních počtů uživatelů a minimálních požadavků na přenosovou rychlost.

Úsporná koncepce nového komunikačního protokolu pro nositelný kardiostimulátor vychází z potřeb datových přenosů a omezeními danými rozměry technického řešení a energetickou spotřebou při vlastní implementaci tohoto protokolu. Použití bezdrátové technologie umožňuje vytvořit komunikační kanál sdílený více účastníky - uživateli externích kardiostimulátorů a je proto třeba vhodným způsobem zajistit dostatečně vysokou pravděpodobnost doručení zprávy.

Z důvodu optimalizace spotřeby energie a zajištění bezpečnosti proti kybernetickým hrozbám nositelného kardiostimulátoru jako koncového zařízení je komunikační protokol navržen jako jednosměrný, kdy externí kardiostimulátor pouze vysílá a prostor možného výskytu uživatelů je pokryt dostatečným počtem přijímacích základnových stanic. Data daného uživatele můžou být přijímána i více stanicemi a centrální server pak řeší případné vícenásobné doručení datového rámce od několika přijímacích stanic. Datový rámec proto musí obsahovat jednoznačný identifikátor uživatele (kardiostimulátoru). Tímto identifikátorem je jednak sériové číslo kardiostimulátoru a dále sekvenční číslo datového rámce.

Jedna přijímací stanice může být v dosahu více uživatelů. Vzhledem k jednosměrnému způsobu přenosu nebude doručení zprávy potvrzováno. Proto je třeba minimalizovat pravděpodobnost výskytu vzájemných kolizí. Výskyt kolize nelze jednoznačně vyloučit. Počet současně komunikujících uživatelů není příliš velký, čas mezi jednotlivými datovými přenosy jednoho uživatele je dán jeho aktuální tepovou frekvencí a délka přenášené zprávy není příliš velká. Z těchto důvodů je velmi pravděpodobné, že při opakovaném vysílání zprávy nebudou všechna opakování kolidovat s vysíláním jiných uživatelů.

Při konstantní délce datového rámce je přenosovou rychlostí určen maximální počet současně komunikujících uživatelů. Externí nositelné kardiostimulátory odesílají data v časových intervalech určených tepovou frekvencí uživatele. Tato frekvence

se mění se zdravotním stavem a fyzickou a psychickou zátěží člověka. Jako jediná vhodná metoda studia vlivu počtu současně komunikujících uživatelů na počet kolizí ve vysílání je proto simulace.

Pokud jsou kritická data zopakována ve čtyřech po sobě jdoucích datových rámcích, musely by nastat čtyři kolize ve vysílání v řadě, aby došlo k úplné ztrátě dat. Pokud bude maximální blok souvislých kolizí kratší, všechna data se přenesou, byť v některých případech s drobným zpožděním. Proto kritická data jsou opakována v osmi po sobě jdoucích datových rámcích. Na základě výsledků simulace bylo zjištěno, že tento model je použitelný až pro 10 uživatelů v dosahu jedné přijímací stanice a pro přenosové rychlosti 100 kb/s a vyšší. Při této konfiguraci je možné přenos dat zabezpečit BCH kódem BCH(255,131), který umožňuje opravu až 18 bitových chyb, což odpovídá zhruba 0.5 chybným bitům na 1 B přenášených dat.

BCH kód vyžaduje použití bloku dat určité délky. Tento blok pak můžeme využít buďto pro přenos většího objemu užitečných dat s menším prostorem pro zabezpečovací bity a tedy s nižším počtem opravitelných vadných bitů, nebo naopak pro přenos menšího objemu dat, kdy více prostoru zůstane pro zabezpečovací bity a tudíž je získána schopnost opravit vyšší počet případně chybných bitů.

Při simulaci bylo dále ověřováno několik variant formátu datového rámce od minimalistické varianty, kdy část datového rámce je zabezpečena BCH kódem velikosti 63 bitů až po variantu s BCH blokem velikosti 255 bitů.

V případě minimalistické varianty 63-bitového BCH bloku je k dispozici pouze 32 bitů pro přenos krátkodobých dat, které tak mohou být opakována v maximálně čtyřech po sobě jdoucích datových rámcích. Větší prostor pro vlastní data by znamenal snížení opravných schopností BCH kódu a tím i odolnosti protokolu proti rušení. Počtem opakování krátkodobých dat je omezen maximální počet uživatelů, kteří můžou být současně v dosahu jednoho přijímače a takové omezení je zapotřebí řešit organizačně-technickým způsobem, např. zvýšením počtu přijímacích stanic a snížením citlivosti přijímače, nebo snížením vysílacího výkonu vysílače tak, aby nedocházelo k vyššímu počtu po sobě jdoucích kolizí ve vysílání.

Největší délka bloku BCH kódu, který je vhodný pro navrženou koncepci komunikačního protokolu je 255 bitů. Blok této velikosti poskytuje prostor pro 8 opakování krátkodobých dat, což je maximální vhodný počet z pohledu aplikace navrženého komunikačního protokolu. V BCH bloku délky 255 bitů je k dispozici dostatek zabezpečovacích bitů pro opravu až 23 chybných bitů, což v případě navrženého protokolu odpovídá schopnosti opravit 0,5 bitu z každého bytu přenášených dat.

Dostupné RF moduly nabízí jen omezené kombinace modulačního formátu a přenosové rychlosti. Z této nabídky jsou pro přenos dat nositelných kardiostimulátorů použitelné přenosové rychlosti 100 kb/s a vyšší, u rychlostí nad 500 kb/s se však dají očekávat vyšší nároky na kvalitu signálu a tím i vysílaný výkon a spotřebu energie.

Klíčový výsledek této práce je proto komplexní simulační model komunikace nositelných externích kardiostimulátorů. Simulační model posloužil pro optimalizaci parametrů koncepčního návrhu komunikačního protokolu pro nositelné kardiostimulátory a může sloužit i v budoucnu pro modifikaci těchto parametrů v případě potřeby použití jiného typu RF čipu, který může podporovat odlišné přenosové rychlosti, pro případné další scénáře využití nositelných kardiostimulátorů, případně pro další obdobné aplikace.

Vlastní implementace dedikovaného komunikačního protokolu do nositelného externího kardiostimulátoru je závislá na jeho vnitřní struktuře, rozhraní, které je možné použít pro napojení komunikačního modulu, možnostech fyzického umístění desky plošných spojů, směrové orientaci antény a dalších technických detailech, které jsou závislé na konkrétním typu kardiostimulátoru.

Reálná implementace je proto úkolem výrobců kardiostimulátorů a naše pracoviště nabízí pomoc a součinnost jak při případných modifikacích navržené koncepce komunikačního protokolu tak i při vývoji vlastní implementace.

Zájem o spolupráci již projevil konkrétní výrobce nositelných externích kardiostimulátorů.

Autorova literatura

[1] Blažek, P.; Gerlich, T.; Martinásek, Z.; aj.: Comparison of Linux Filtering Tools for Mitigation of DDoS Attacks. In *41st International Conference on Telecommunications and Signal Processing (TSP)*, ročník 41, Athens: Institute of Electrical and Electronics Engineers Inc., 2018, ISBN 978-1-5386-4695-3, ISSN 1805-5435, s. 145–149, doi:10.1109/TSP.2018.8441309.

[2] Frolka, J.; Hajný, J.; Smékal, D.: Generátor kybernetických útoků. *Elektrorevue - Internetový časopis (http://www.elektrorevue.cz)*, ročník 19, č. 2, 2017: s. 53–57, ISSN 1213-1539.

[3] Frolka, J.; Mlýnek, P.: Měření a testování optické trasy a aktivních prvků. *Elektrorevue - Internetový časopis (http://www.elektrorevue.cz)*, ročník 20, č. 4, 2018: s. 112–117, ISSN 1213-1539.

[4] Frolka, J.; Slavíček, K.; Šeda, P.: Optimizing Low-Power Communication Protocols for External Pacemakers: Collision Prevention and Reliability in Multi-Patient Scenarios. In *ICUMT 2024 – The 16th International Congress on Ultra Modern Telecommunications and Control Systems (ICUMT)*, Meloneras, Gran Canaria, Spain, 2024, str. 6.

[5] Grenar, D.; Frolka, J.; Slavíček, K.; aj.: NETWORK PHYSICAL LAYER ATTACK IN THE VERY HIGH CAPACITY NETWORKS. *Advances in Electrical and Electronic Engineering*, ročník 21, č. 1, 2023: s. 37–47, ISSN 1336-1376, doi:10.15598/aeee.v21i1.4973.

[6] Kováč, D.; Mašek, P.; Hošek, J.; aj.: Usability Study of ITU-T P.1201 Amd.2 Standard for Video Quality Estimation in HTTP-based Online Streaming Services. In *40th Anniversary of International Conference on Telecommunications and Signal Processing (TSP)*, Barcelona, Španělsko, 2017, ISBN 978-1-5090-3981-4, s. 20–25, doi:10.1109/TSP.2017.8075929.

[7] Lieskovan, T.; Kohout, D.; Frolka, J.: Cyber range scenario for smart grid security training. *Elektrotechnik und Informationstechnik*, ročník 140, č. 5, 2023: s. 1–8, ISSN 1613-7620, doi:10.1007/s00502-023-01146-0.

[8] Myška, V.; Mezina, A.; Vaněk, P.; aj.: CovidStopHospital: e-Health Service for X-Ray-Based COVID-19 Classification and Radiologist-Assisted Dataset Creation. In *15th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, Ghent, 2023, ISBN 979-8-3503-9328-6, s. 62–67.

[9] Pokorný, J.; Ma, K.; Saafi, S.; aj.: Prototype Design and Experimental Evaluation of Autonomous Collaborative Communication System for Emerging Maritime Use Cases. *SENSORS*, ročník 21, č. 11, 2021: s. 1–20, ISSN 1424-8220, doi:10.3390/s21113871.

[10] Sharma, S.; Tiwari, D.; Garg, A.; aj.: Enhancing Plant Disease Detection with CNNs and LLMs: A Comprehensive Approach to Diagnosis and Mitigation. In *ICUMT 2024 – The 16th International Congress on Ultra Modern Telecommunications and Control Systems (ICUMT)*, Meloneras, 2024, str. 6.

[11] Smékal, D.; Frolka, J.; Hajný, J.: Acceleration of AES Encryption Algorithm Using Field Programmable Gate Arrays. *IFAC-PapersOnLine (ELSEVIER)*, ročník 49, č. 25, 2016: s. 384–389, ISSN 2405-8963, doi:10.1016/j.ifacol.2016.12.075.

[12] Smékal, D.; Frolka, J.; Hajný, J.: Akcelerace šifry AES pomocí programovatelných hradlových polí. *Elektrorevue - Internetový časopis (http://www.elektrorevue.cz)*, ročník 18, č. 3, 2016: s. 76–82, ISSN 1213-1539.

[13] Člupek, V.; Frolka, J.: Autentizace na hardwarově omezených zařízeních. *Elektrorevue - Internetový časopis (http://www.elektrorevue.cz)*, ročník 17, č. 6, 2015: s. 185–192, ISSN 1213-1539.

[14] Čučka, M.; Grenar, D.; Frolka, J.; aj.: Simulation and Measurement of Optical Networks 10 and 100 Gb/s. In *New Trends in Signal Processing 2022*, 2022, Hotel Chopok, Demanovska dolina, Slovakia: NTSP, 2022, ISBN 978-80-8040-610-3, s. 1–4, doi:10.23919/NTSP54843.2022.9920378.

Literatura

[15] Abracon: ACAG1204-433-T Datasheet. https://cz.mouser.com/datasheet/2/3/ACAG1204-433-T-1609117.pdf, cit. 2024-11-10.

[16] Abracon: ACR1504I3 Datasheet. https://cz.mouser.com/datasheet/2/3/ACR1504I3-2584395.pdf, cit. 2024-11-10.

[17] Abracon: ACR2005I4 Datasheet. https://cz.mouser.com/datasheet/2/3/ACR2005I4-2584419.pdf, cit. 2024-11-10.

[18] Adámek, J.: *Kódování a teorie informace*. Praha: Ediční středisko ČVUT, vyd. 1 vydání, 1991, ISBN 80-01-00661-1.

[19] Antenova: SRCI024 Datasheet. https://cz.mouser.com/datasheet/2/23/Silvai_SRC1024_PS_1_01-3304015.pdf, cit. 2024-11-10.

[20] Arm Community: Security Scenarios Addressed by Arm Cortex-M23 and Cortex-M33. https://community.arm.com/arm-community-blogs/b/internet-of-things-blog/posts/security-scenarios-addressed-by-arm-cortex-m23-and-cortex-m33, 2017, cit. 2024-11-16.

[21] AVDZP: Pacemaker Information EPG10. https://www.avdzp.cz/katalog/en/mediatrade.html, cit. 2024-09-10.

[22] Bembe, M.; Abu-Mahfouz, A.; Masonta, M.; aj.: A survey on low-power wide area networks for IoT applications. *Telecommunication Systems*, ročník 71, č. 2, 2019: s. 249–274, ISSN 1572-9451, doi:10.1007/s11235-019-00557-9.
URL https://doi.org/10.1007/s11235-019-00557-9

[23] Bluetooth Special Interest Group: Bluetooth Technology Overview. https://www.bluetooth.com/learn-about-bluetooth/tech-overview/, cit. 2024-10-22.

[24] Bonefaccic, D.; Bartolicc, J.: Small Antennas: Miniaturization Techniques and Applications. *Automatika*, ročník 53, č. 1, 2012: s. 49–60, doi:10.7305/automatika.53-1.164.

[25] Boulis, T.: Castalia: A Simulator for Wireless Sensor Networks and Body Area Networks. 2013, accessed: 2024-11-16.
URL https://github.com/boulis/Castalia

[26] Budíková, M.; Kroupová, M.; Šályová, J.; aj.: *Statistika a pravděpodobnost.* Brno: Masarykova univerzita, 2016, ISBN 978-80-210-8206-9.
URL `https://www.muni.cz/vyzkum/publikace/1342297`

[27] Bílková, D.; Budinský, P.; Vohánka, V.: *Pravděpodobnost a statistika.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2009, ISBN 978-80-7380-224-0.

[28] Chen, L.-C.; Longstaff, T. A.; Carley, K. M.: Characterization of defense mechanisms against distributed denial of service attacks. *Computers & Security*, ročník 23, č. 8, 2004: s. 665–678.

[29] Commission, F. C.: Amendment of the Commission's Rules to Provide Spectrum for the Operation of Medical Body Area Networks. `https://www.fcc.gov/document/medical-body-area-networks-first-report-and-order`, 2012, cit. 2024-10-22.

[30] Connectivity Standards Alliance: Zigbee. `https://csa-iot.org/all-solutions/zigbee/`, cit. 2024-10-22.

[31] Criscuolo, P. J.: Distributed denial of service: Trin00, tribe flood network, tribe flood network 2000, and stacheldraht ciac-2319. Technická zpráva, DTIC Document, 2000.

[32] Desclos, L.: Advances in High-Performance Ceramic Antennas for Small-Form-Factor, Multi-Technology Devices. *Microwave Journal*, 2008, cit. 2024-11-10.

[33] Dostál, O.; Javorník, M.: Metropolitní archív medicínských obrazových informací. *Zpravodaj ÚVT MU*, ročník XII, č. 5, 2002: s. 14–17, ISSN 1212-0901, cit. 2023-09-01.
URL `http://ics.muni.cz/zpravodaj/articles/255.html`

[34] Dostál, O.; Javorník, M.: Projekt MeDiMed. *Zpravodaj ÚVT MU*, ročník XVI, č. 2, 2005: s. 8–11, ISSN 1212-0901, cit. 2023-09-01.
URL `http://ics.muni.cz/zpravodaj/articles/345.html`

[35] Dostál, O.; Javorník, M.; Slavíček, K.; aj.: MEDIMED-Regional Centre for Archiving and Interhospital Exchange of Medicine Multimedia Data. In *Proceedings of the Second IASTED International Conference on Communications, Internet, and Information Technology*, International Association of Science and Technology for Development - IASTED, 2003, ISBN 0-88986-398-9, s. 609–614.

[36] Dupač, V.; Hušková, M.: *Pravděpodobnost a matematická statistika.* Praha: Karolinum, druhé vydání, 2013, ISBN 978-80-246-2208-8.

[37] Elghayyaty, M.; Hadjoudja, A.; Mouhib, O.; aj.: Performance Study of BCH Error Correcting Codes Using the Bit Error Rate Term BER. *International Journal of Engineering Research and Applications*, ročník 7, č. 2, Part-2, 2017: s. 52–54, ISSN 2248-9622, cit. 2024-10-22.
URL `https://www.ijera.com/papers/Vol7_issue2/Part-2/J0702025254.pdf`

[38] Federal Communications Commission: Medical Device Radiocommunications Service (MedRadio). `https://www.fcc.gov/medical-device-radiocommunications-service-medradio`, cit. 2023-09-01.

[39] Frolka, J.: *BCH kódy*. Diplomová práce, Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, Brno, 2012.

[40] GNS3: GNS3 Network Simulation Software. https://www.gns3.com/, cit. 2023-09-10.

[41] Gollová, A.: Algebraické kódování, Konečná tělesa. `https://math.fel.cvut.cz/en/people/gollova/tik/tik_h4a.pdf`, 2018, cit. 2023-09-01.

[42] Gollová, A.: Algebraické kódování, Počítání modulo polynom. `https://math.fel.cvut.cz/en/people/gollova/tik/tik_h3a.pdf`, 2018, cit. 2023-09-01.

[43] Hanzo, L.; Liew, T. H.; Yeap, B. L.: *Turbo coding, turbo equalisation and space-time coding for transmission over fading channels*. Chichester: Wiley, 2002, ISBN 0-470-84726-3.

[44] HopeRF: RFM31B Datasheet. `https://docs.rs-online.com/255c/0900766b80f44156.pdf`, cit. 2024-11-16.

[45] HopeRF: RFM42 Datasheet. `https://www.tme.eu/Document/68c8b83d55e84eece2d6ad064e838e39/RFM42.pdf`, cit. 2024-11-16.

[46] HopeRF: RFM68W Datasheet. `https://docs.rs-online.com/5c2c/0900766b8127e027.pdf`, cit. 2024-11-16.

[47] HopeRF: RFM69HW Datasheet. `https://docs.rs-online.com/d64e/0900766b8127e052.pdf`, cit. 2024-11-16.

[48] Ibrahimi, S.: *A Secure Communication Model for the Pacemaker: A Balance Between Security Mechanisms and Emergency Access*. Diplomová práce, Eindhoven University of Technology, 2014, cit. 2024-11-07.
URL `https://research.tue.nl/files/46987826/782901-1.pdf`

[49] IEEE 802.15 Working Group: IEEE 802.15: Wireless Specialty Networks. https://www.ieee802.org/15/, cit. 2024-11-16.

[50] International, S.: External Pulse Generator 3085 Specification Sheet. https://sante.ro/wp-content/uploads/2016/04/External_Pulse_Generator_3085_Spec_Sheet_RD3_FINAL_RGB_ID-2001433AEN.pdf, 2016, cit. 2024-09-10.

[51] International Telecommunication Union: SM.1056-1: Protection of radio services in the LF, MF and HF bands from power line telecommunication systems. https://www.itu.int/dms_pubrec/itu-r/rec/sm/R-REC-SM.1056-1-200704-I!!PDF-E.pdf, cit. 2023-09-01.

[52] International Telecommunication Union: Impact of industrial, scientific and medical (ISM) equipment on radiocommunication services. https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-SM.2180-2010-PDF-E.pdf, 2010, cit. 2023-09-01.

[53] IQRF Tech s.r.o.: What is IQRF. https://www.iqrf.org/what-is-iqrf, 2024, cit. 2024-11-16.

[54] Jarušková, D.: *Pravděpodobnost a matematická statistika*. České vysoké učení technické v Praze, 2015, cit. 2023-09-01.

[55] Jiang, Y.: *A practical guide to error-control coding using MATLAB*. Norwood: Artech House, c2010, ISBN 978-1-60807-088-6.

[56] Johnson: 0433AT62A0020E Datasheet. https://cz.mouser.com/datasheet/2/611/0433AT62A0020E_AEC_7hvqEo4-2585919.pdf, cit. 2024-11-10.

[57] Kenig, R.; Manor, D.; Gadot, Z.; aj.: DDoS Survival Handbook. 2013, [cit. 2023-04-15].

[58] KYOCERA-AVX: 1004796 Datasheet. https://cz.mouser.com/datasheet/2/40/AVX_E_1004795_1004796-2936341.pdf, cit. 2024-11-10.

[59] KYOCERA-AVX: M-Series Antenna Application Note. https://www.kyocera-avx.com/docs/techinfo/ApplicationNotes/Antenna-AppNotes/AVX-E_AppNote-M-Series.pdf, cit. 2024-11-11.

[60] KYOCERA-AVX: M620720 Datasheet. https://cz.mouser.com/datasheet/2/40/AVX_E_M620720-3312995.pdf, cit. 2024-11-10.

[61] Lee, L. H. C.: *Error-control block codes for communications engineers*. Boston: Artech House, 2000, ISBN 1-58053-032-X.

[62] Libor Žák: Popisná statistika - zavedení pojmu. https://mathonline.fme.vutbr.cz/download.aspx?id_file=475, cit. 2023-09-01.

[63] Lin, S.; Costello, D. J.: *Error control coding /*. Upper Saddle River: Prentice-Hall, druhé vydání, c2004, ISBN 0-13-042672-5.

[64] Lone, F. R.; Puri, A.; Kumar, S.: Performance Comparison of Reed Solomon Code and BCH Code over Rayleigh Fading Channel. *International Journal of Computer Applications*, ročník 71, č. 20, 2013: s. 23–26, ISSN 0975-8887, cit. 2024-10-22.
URL https://arxiv.org/abs/1307.6930

[65] LoRa Alliance: About LoRaWAN. https://lora-alliance.org/about-lorawan/, cit. 2024-10-22.

[66] LPRS: LPRS-CCA-868 Datasheet. https://docs.rs-online.com/2aa9/A700000007241016.pdf, cit. 2024-11-07.

[67] Microchip: MRF89XAM8A Datasheet. https://docs.rs-online.com/d1e1/0900766b81422d0f.pdf, cit. 2024-11-16.

[68] Mirkovic, J.; Reiher, P.: A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, ročník 34, č. 2, 2004: s. 39–53.

[69] Molex: 206649-0001 Datasheet. https://docs.rs-online.com/5789/A700000007613004.pdf, cit. 2024-11-07.

[70] Moon, T. K.: *Error correction coding*. Hoboken: Wiley-Interscience, 2005, ISBN 0-471-64800-0.

[71] Nordic Semiconductor : nRF9E5 Datasheet. https://cz.mouser.com/datasheet/2/297/NRSAS00034_1-2559940.pdf, 2023, cit. 2024-11-16.

[72] Ns-3 Project: Ns-3: A Discrete-Event Network Simulator for Internet Systems. https://www.nsnam.org, cit. 2024-10-22.

[73] Němec, K.: *Datová komunikace*. Brno: Vutium, vyd. 3 vydání, 2007, ISBN 80-214-1652-1.

[74] Peng, T.; Leckie, C.; Ramamohanarao, K.: Survey of network-based defense mechanisms countering the DoS and DDoS problems. *ACM Computing Surveys (CSUR)*, ročník 39, č. 1, 2007: str. 3.

[75] Quan, D. T.; Hiep, P. T.; Kohno, R.: Performance Analysis Method for IEEE 802.15.6 Based WBANs with Adaptive BCH Code Rates. *Wireless Personal Communications*, ročník 94, č. 3, 2017: s. 605–619, ISSN 1572-834X, doi:10.1007/s11277-016-3639-4.
URL https://doi.org/10.1007/s11277-016-3639-4

[76] R Development Core Team: R: A Language and Environment for Statistical Computing. Cit. 2024-09-10.
URL https://www.r-project.org/

[77] Ranjan, S.; Swaminathan, R.; Uysal, M.; aj.: DDoS-Resilient Scheduling to Counter Application Layer Attacks Under Imperfect Detection. In *INFOCOM*, 2006, s. 1–13.

[78] Ranjan, S.; Swaminathan, R.; Uysal, M.; aj.: DDoS-shield: DDoS-resilient scheduling to counter application layer attacks. *IEEE/ACM Transactions on Networking (TON)*, ročník 17, č. 1, 2009: s. 26–39.

[79] RFSolutions: ZETA Datasheet. https://cz.mouser.com/datasheet/2/975/RFSO_S_A0009835375_1-2576210.pdf, cit. 2024-11-16.

[80] RFSolutions: ZETAPLUS Datasheet. https://cz.mouser.com/datasheet/2/975/RFSO_S_A0009835147_1-2576128.pdf, cit. 2024-11-16.

[81] Silicon Labs: AN1253: EFR32 Radio Configurator Guide for SSv5. https://www.silabs.com/documents/public/application-notes/an1253-efr32-radio-configurator-guide-for-ssv5.pdf, cit. 2024-11-11.

[82] Silicon Labs: Si4430/31/32 Datasheet. https://cz.mouser.com/datasheet/2/368/Si4430_31_32-1397927.pdf, cit. 2024-11-16.

[83] Silicon Labs: Si4455 Datasheet. https://cz.mouser.com/datasheet/2/368/Si4455-1397974.pdf, cit. 2024-11-16.

[84] Silicon Labs: Si4464/63/61/60 Datasheet. https://cz.mouser.com/datasheet/2/368/Si4464_63_61_60-1397874.pdf, cit. 2024-11-16.

[85] Silicon Labs: Si4468/7 Datasheet. https://cz.mouser.com/datasheet/2/368/Si4468_7-1397993.pdf, cit. 2024-11-16.

[86] Silicon Labs: EFR32FG12 Datasheet. https://cz.mouser.com/datasheet/2/368/efr32fg12_datasheet-1800085.pdf, 2023, cit. 2024-11-16.

[87] Silicon Labs: EFR32FG13 Datasheet. https://cz.mouser.com/datasheet/2/368/efr32fg13_datasheet-1666242.pdf, 2023, cit. 2024-11-16.

[88] Silicon Labs: EFR32FG14 Datasheet. https://cz.mouser.com/datasheet/2/368/efr32fg14_datasheet-1487141.pdf, 2023, cit. 2024-11-16.

[89] Silicon Labs: EFR32FG23 Datasheet. https://cz.mouser.com/datasheet/2/368/efr32fg23_datasheet-3010260.pdf, 2023, cit. 2024-11-16.

[90] Silicon Labs: EFR32FG28 Datasheet. https://cz.mouser.com/datasheet/2/368/efr32fg28_datasheet-3412435.pdf, 2023, cit. 2024-11-16.

[91] Sweeney, P.: *Error control coding*. Chichester: Wiley, c2002, ISBN 0-470-84356-X.

[92] Tabbane, S.: IoT Standards Part II. https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2018/IoT-BDG/7.%20IoT%20Standards%20Part%20II%20-%20Sami%20Tabbane.pdf, 2018, cit. 2024-11-16.

[93] TE Connectivity: ANT-433-SP Datasheet. https://cz.mouser.com/datasheet/2/418/9/ENG_DS_ANT_433_SP_A-3238491.pdf, cit. 2024-11-10.

[94] TE Connectivity: ANT-433-uSP410 Datasheet. https://cz.mouser.com/datasheet/2/418/9/ENG_DS_ant_433_usp410_ds_A-3238211.pdf, cit. 2024-11-10.

[95] TE Connectivity: ANT-868-CHP-T Datasheet. https://docs.rs-online.com/68d6/A700000006946672.pdf, cit. 2024-11-07.

[96] TE Connectivity: ANT1204LL20R0433A Datasheet. https://cz.mouser.com/datasheet/2/447/datasheet_ant1204ll20r0433a_v1_1617827477-2903031.pdf, cit. 2024-11-10.

[97] TE Connectivity: L9000122-01 Datasheet. https://www.te.com/commerce/DocumentDelivery/DDEController?Action=srchrtrv&DocNm=L9000122-01&DocType=Data%20Sheet&DocLang=English&DocFormat=pdf&PartCntxt=L9000122-01, cit. 2024-11-10.

[98] Texas Instruments: CC1110Fx / CC1111Fx Datasheet. https://www.ti.com/lit/ds/symlink/cc1110-cc1111.pdf, 2023, cit. 2024-11-16.

[99] Union, I. T.: ITU-T Recommendation G.704: Synchronous Frame Structures Used at 1544, 6312, 2048, 8448 and 44 736 kbit/s Hierarchical Levels. https://www.itu.int/rec/T-REC-G.704-199810-I/en, 1998, cit. 2024-11-16.

[100] Wallace, H.: Error Detection and Correction Using the BCH Code. Technická zpráva, Atlantic Quality Design, Inc., 2001.
URL https://aqdi.com/wordpress/wp-content/uploads/2015/12/bch.pdf

[101] Wi-Fi Alliance: Wi-Fi CERTIFIED HaLow. https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-halow, cit. 2024-10-22.

[102] Wicker, S. B.; Bhargava, V. K.: *Reed-Solomon codes and their applications*. New York: IEEE, c1999, ISBN 0-7803-5391-9.

[103] Würth Elektronik: 7488910043 Datasheet. https://www.we-online.com/components/products/datasheet/7488910043.pdf, cit. 2024-11-10.

[104] Würth Elektronik: 7488918022 Datasheet. https://docs.rs-online.com/fce8/A700000009413167.pdf, cit. 2024-11-07.

[105] Z-Wave Alliance: Technology Overview. https://z-wavealliance.org/technology-overview/, 2024, cit. 2024-11-16.

[106] Zaplatílek, K.; Doňar, B.: *MATLAB*. Praha: BEN - technická literatura, první vydání, 2004, ISBN 80-7300-133-0.
URL http://www.digitalniknihovna.cz/mzk/uuid/uuid:d393a6e0-7b52-11e2-b212-005056827e52

[107] Zargar, S. T.; Joshi, J.; Tipper, D.: A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE communications surveys & tutorials*, ročník 15, č. 4, 2013: s. 2046–2069.

[108] Zuzana Hrdličková: Náhodná veličina a její charakteristiky. https://mathonline.fme.vutbr.cz/download.aspx?id_file=502, cit. 2023-09-01.

[109] Zuzana Hrdličková: Základní rozdělení pravděpodobnosti. https://mathonline.fme.vutbr.cz/download.aspx?id_file=628, cit. 2023-09-01.

[110] Český telekomunikační úřad: Všeobecné oprávnění č. VO-R/10/07.2021-8. https://ctu.gov.cz/sites/default/files/obsah/vo-r10-072021-8.pdf, 2021, cit. 2024-10-22.

[111] Český telekomunikační úřad: Kmitočtové spektrum. https://spektrum.ctu.gov.cz/kmitocty, cit. 2023-09-01.

[112] Český telekomunikační úřad: Využívání vymezených rádiových kmitočtů. https://ctu.gov.cz/vyuzivani-vymezenych-radiovych-kmitoctu, cit. 2023-09-01.

[113] Šilhavý, P.: *Datová komunikace.* 1, Vysoké učení technické v Brně, první vydání, 2012, ISBN 978-80-214-4455-3, 1–211 s.

Seznam symbolů a zkratek

3GPP (3rd Generation Partnership Project)

ATM (Asynchronous Transfer Mode)

B/s (Byte per second)

b/s (bit per second)

BAN Body Area Network

BER (Bit Error Rata) bitová chybovost

BCH (Bose–Chaudhuri–Hocquenghem)

BLE (Bluetooth Low Energy)

CPU (Central Processing Unit)

CRC Cyclic Redundancy Check

CSV (Comma Separated Values)

ČTU (Český telekomunikační úřad)

dB (decibel)

DoS (Denial of Service)

DDoS (Distributed Denial of Service)

DNS (Domain Name System)

DSL (Digital Subscriber Line)

DSP (Digital Signal Procesor)

DVB (Digital Video Broadcasting)

FEC (Forward error correction)

FPU (Floating-Point Unit)

GF (Galois field) Galoisovo těleso

GFSK (Gaussian Frequency Shift Keying)

GMSK (Gaussian Minimum Shift Keying)

GPIO (General-purpose input/output)

HDD (Hard Disk Drive)

HRV (Heart Rate Variability) variabilita tepové frekvence

HTTP (HyperText Transfer Protocol)

Hz (Hertz)

ICMP (Internet Control Message Protocol)

IoT (Internet of Things) Internet věcí

IP (Internet Protocol)

ISM (Industrial, Scientific, and Medical)

LCM (Least Common Multiple)

LFSR (Linear-feedback shift register)

LoRa (Long Range)

LPWAN (Low Power Wide Area Network)

LTD (Long Term Data)

LTE (Long Term Evolution)

LTE-M (LTE for Machines)

MBAN (Medical Body Area Network)

MedRadio (Medical Device Radiocommunications Service)

ITU (The International Telecommunication Union)

NASA (National Aeronautics and Space Administration)

NB-IoT (Narrowband IoT)

OOK (On/Off Keying)

PAN (Personal Area Networks)

PoE (Power over Ethernet)

RAM (Random Access Memory)

RF (Radio Frequency) Radiofrekvenční

SEQ NUM (Sequence Number) Sekvenční číslo

SFD (Start Frame Delimiter)

SNR (Signal To Noise Ratio)

STD (Short Term Data)

TCP (Transmission Control Protocol)

UDP (User Datagram Protocol)

UWB (Ultra-Wideband)

WBAN (Wireless Body Area Networks)

Wi-Fi (Wireless Fidelity)

WSN (Wireless Sensor Networks)

Seznam příloh

A Přehled vlastností BCH kódů **121**

B Analýza vlastností radiofrekvenčních modulů **123**

B.1 Srovnání klíčových parametrů RF modulů založených na architektuře Intel 8051 123

B.2 Srovnání klíčových parametrů RF modulů založených na architektuře ARM Cortex-M4 124

B.3 Srovnání klíčových parametrů RF modulů založených na architektuře ARM Cortex-M33. 125

B.4 Srovnání klíčových parametrů RF modulů s proprietární architekturou 126

C Průzkum výrobců antén a jejich srovnání parametrů **127**

D Výsledky simulací dedikovaného komunikačního protokolu pro různé doby vysílání **129**

A Přehled vlastností BCH kódů

Délka n; Informační znaky k; Korekční schopnost t

n	k	t		n	k	t
63	57	1		255	247	1
	51	2			239	2
	45	3			231	3
	39	4			223	4
	36	5			215	5
	30	6			207	6
	24	7			199	7
	18	10			191	8
	16	11			187	9
	10	13			179	10
	7	15			171	11
127	120	1			163	12
	113	2			155	13
	106	3			147	14
	99	4			139	15
	92	5			131	18
	85	6			123	19
	78	7			115	21
	71	9			107	22
	64	10			99	23
	57	11			91	25
	50	13			87	26
	43	14			79	27
	36	15			71	29
	29	21			63	30
	22	23			55	31
	15	27			47	42
	8	31			45	43
					37	45
					29	47
					21	55
					13	59
					9	63

B Analýza vlastností radiofrekvenčních modulů

B.1 Srovnání klíčových parametrů RF modulů založených na architektuře Intel 8051

1. Nordic Semiconductor nRF9E5 [71]
2. Texas Instruments CC1110F8 [98]
3. Texas Instruments CC1110F16 [98]
4. Texas Instruments CC1110F32 [98]
5. Texas Instruments CC1111F8 [98]
6. Texas Instruments CC1111F16 [98]
7. Texas Instruments CC1111F32 [98]

Tab. B.1: Přehled klíčových RF modulů založených na architektuře Intel 8051.

Číslo	**Bitová rychlost [kb/s]**	**Vysílací výkon [dBm]**	**Velikost paměti Flash [KB]**	**Velikost paměti RAM [kB]**	**Počet GPIO pinů**	**Pouzdro**
1	50	10	4 kB	256 B	8 + SPI	QFN-32
2	500	10	8kB	1kB	19	QFN-36
3	500	10	16kB	2kB	19	QFN-36
4	500	10	32kB	4kB	19	QFN-36
5	500	10	8kB	1kB	19	QFN-36
6	500	10	16kB	2kB	19	QFN-36
7	500	10	32kB	4kB	19	QFN-36

B.2 Srovnání klíčových parametrů RF modulů založených na architektuře ARM Cortex-M4

1. Silicon Labs EFR32FG14P231F256GM48-B [88]
2. Silicon Labs EFR32FG14P231F256IM48-B [88]
3. Silicon Labs EFR32FG14P231F128GM48-B [88]
4. Silicon Labs EFR32FG14P231F256GM32-B [88]
5. Silicon Labs EFR32FG14P231F256IM32-B [88]
6. Silicon Labs EFR32FG14P231F128GM32-B [88]
7. Silicon Labs EFR32FG13P231F512GM48-D [87]
8. Silicon Labs EFR32FG13P231F512GM32-D [87]
9. Silicon Labs EFR32FG12P231F512GM68-C [86]

Všechny uvedené moduly mají stejný parametr maximální bitové rychlosti:

- pro kmitočtové pásmo 434 MHz: 100 kb/s,
- pro kmitočtové pásmo 868 MHz: 500 kb/s,
- pro kmitočtové pásmo 915 MHz: 2000 kb/s.

Tab. B.2: Srovnání klíčových parametrů RF modulů založených na architektuře ARM Cortex-M4.

Číslo	**Vysílací výkon [dBm]**	**Velikost paměti Flash [KB]**	**Velikost paměti RAM [kB]**	**Počet GPIO pinů**	**Pouzdro**
1	20	256	32	32	QFN48
2	20	256	32	32	QFN48
3	20	128	16	32	QFN48
4	20	256	32	16	QFN32
5	20	256	32	16	QFN32
6	20	128	16	16	QFN32
7	20	512	64	32	QFN48
8	20	512	64	16	QFN32
9	20	512	64	46	QFN68

B.3 Srovnání klíčových parametrů RF modulů založených na architektuře ARM Cortex-M33.

1. Silicon Labs EFR32FG23B020F512IM48-C [89]
2. Silicon Labs EFR32FG23B020F512IM40-C [89]
3. Silicon Labs EFR32FG23B020F128GM40-C [89]
4. Silicon Labs EFR32FG23B010F512IM48-C [89]
5. Silicon Labs EFR32FG23B010F512IM40-C [89]
6. Silicon Labs EFR32FG23B010F128GM40-C [89]
7. Silicon Labs EFR32FG28B320F1024IM68-A [90]
8. Silicon Labs EFR32FG28B320F1024IM48-A [90]
9. Silicon Labs EFR32FG28B310F1024IM68-A [90]
10. Silicon Labs EFR32FG28B310F1024IM48-A [90]

Všechny uvedené moduly mají stejný parametr maximální bitové rychlosti:

- pro kmitočtové pásmo 434 MHz: 100 kb/s,
- pro kmitočtové pásmo 868 MHz: 500 kb/s,
- pro kmitočtové pásmo 915 MHz: 2000 kb/s.

Tab. B.3: Srovnání klíčových parametrů RF modulů založených na architektuře ARM Cortex-M33.

Číslo	**Vysílací výkon [dBm]**	**Velikost paměti Flash [KB]**	**Velikost paměti RAM [kB]**	**Počet GPIO pinů**	**Pouzdro**
1	20	512	64	31	QFN48
2	20	512	64	23	QFN40
3	20	128	32	23	QFN40
4	14	512	64	31	QFN48
5	14	512	64	23	QFN40
6	14	128	32	23	QFN40
7	20	1024	256	49	QFN68
8	20	1024	256	31	QFN48
9	14	1024	256	49	QFN68
10	14	1024	256	31	QFN48

B.4 Srovnání klíčových parametrů RF modulů s proprietární architekturou

1. Silicon Labs Si4431 [82]
2. Silicon Labs Si4432 [82]
3. Silicon Labs Si4455 [83]
4. Silicon Labs Si4460 [84]
5. Silicon Labs Si4461 [84]
6. Silicon Labs Si4463 [84]
7. Silicon Labs Si4464 [84]
8. Silicon Labs Si4467 [85]
9. Silicon Labs Si4468 [85]

Tab. B.4: Přehled klíčových RF modulů s proprietární architekturou.

Číslo	**Bitová rychlost [kb/s]**	**Vysílací výkon [dBm]**	**Pouzdro**
1	256	13	QFN20
2	256	20	QFN20
3	500	13	QFN20
4	1000	13	QFN20
5	1000	16	QFN20
6	1000	20	QFN20
7	1000	20	QFN20
8	1000	13	QFN20
9	1000	20	QFN20

C Průzkum výrobců antén a jejich srovnání parametrů

Pro zmenšení polí v tabulce jsou typ antény a výrobce označeny čísly následovně

1. ABRACON ACAG1204-433-T [15]
2. ABRACONACR1504I3 [16]
3. ABRACON ACR2005I4 [17]
4. Linx Technologies ANT-433-USP410 [94]
5. Wurth Elektronik 7488910043 [103]
6. Linx Technologies ANT-433-SP [93]
7. Linx Technologies ANT-433-USP-T [97]
8. Pulse Electronics ANT1204LL20R0433A [96]
9. Johanson Technology 0433AT62A0020E [56]
10. Linx Technologies ANT-868-CHP-T [95]
11. Molex 206649-0001 [69]
12. Wurth Elektronik 7488918022 [104]
13. LPRS LPRS-CCA-868 [66]
14. KYOCERA AVX 1004796 [58]
15. KYOCERA AVX M620720 [60]
16. Antenova SRCI024 [19]

Tab. C.1: Výběr antén na trhu pro frekvenční pásma 434MHz a 868MHz.

Číslo	**Frekvence [MHz]**	**VSWR [-]**	**Peak gain [dBi]**	**Return loss [dB]**	**Výška [mm]**	**Délka [mm]**	**Šířka [mm]**
1	433	2	-1,72	-6,5	1,6	12	4
2	433, 868, 915	-	1,75	<-20	1,2	15	4
3	433 – 470	-	0,3	-23,26	1,6	20	5
4	430 – 435	2,2	-8	<-10	2,9	13,2	9,1
5	423 – 443	2	-4	<-15	1,2	22,5	5,5
6	429 – 437	1,9	-6,4	-	1,5	27,95	13,7
7	429,5 – 436,5	2	-9,8	-	2,62	12,7	9,14
8	433	-	0,83	<-6,5	1,5	12,3	4
9	423 – 443	-	-4	<-9,5	1,2	25	5
10	868	≤2	0,5	-	1,7	16	3
11	698 – 960	-	1,1	<-7	1,2	20	10
12	700 – 960	4	2,1	<-15	6	40	5
13	863 – 870	2	0	-	0,5	5	3
14	315 – 2700	2,5	1,6	-	3,2	36	9
15	868 – 870, 902 – 928	2	1,54	-	1,08	6	2
16	863 – 870, 902 – 928	1,7	0,3	<-10	0,5	1	0,5

D Výsledky simulací dedikovaného komunikačního protokolu pro různé doby vysílání

V této příloze jsou uvedeny tabulky výsledků simulací pro různé doby vysílání, které jsou výstupem systému pro vyhledávání kolizí. Znázorňují závislost počtu právě rehabilitujících pacientů a počtu výskytů po sobě jdoucích kolizí. Pro statistickou významnost byla pro každý počet pacientů provedena simulace v počtu 1000 opakování (výběru náhodných pacientů a tím i jejich různých tepových frekvencí). Z těchto důvodů je např. ve sloupci pro 4 osoby součet počtu výskytů 4000.

Tab. D.1: Tabulka výsledků simulací pro dobu vysílání 9,583 ms.

Počet osob	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Počet po sobě jdoucích kolizí	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**
0	0	0	0	0	0	0	0
1	32	3	0	0	0	0	0
2	2142	1380	754	350	132	30	17
3	1601	2784	3471	3369	3031	1900	1443
4	199	724	1494	2525	3518	4407	4689
5	25	101	250	610	1060	1998	2740
6	0	8	26	126	205	509	827
7	1	0	5	17	44	110	226
8	0	0	0	3	9	34	47
9	0	0	0	0	1	10	7
10	0	0	0	0	0	2	2
11	0	0	0	0	0	0	0
12	0	0	0	0	0	0	2

Tab. D.2: Tabulka výsledků simulací pro dobu vysílání 8,333 ms.

Počet osob	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Počet po sobě jdoucích kolizí	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**
0	0	0	0	0	0	0	0
1	68	10	0	0	0	0	0
2	2513	1964	1301	724	354	116	61
3	1286	2509	3549	3952	4007	3091	2677
4	122	462	1003	1891	2862	4150	4850
5	10	52	135	360	642	1295	1850
6	0	3	11	66	108	272	432
7	1	0	1	7	20	56	104
8	0	0	0	0	6	17	20
9	0	0	0	0	1	2	4
10	0	0	0	0	0	1	0
11	0	0	0	0	0	0	0
12	0	0	0	0	0	0	2

Tab. D.3: Tabulka výsledků simulací pro dobu vysílání 6,4 ms.

Počet osob	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Počet po sobě jdoucích kolizí	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**
0	0	0	0	0	0	0	0
1	260	63	16	3	1	0	0
2	2943	3009	2627	1925	1387	648	511
3	745	1737	2907	4024	4816	5107	5170
4	51	179	403	925	1562	2719	3461
5	1	12	44	108	202	455	706
6	0	0	3	14	29	54	124
7	0	0	0	1	3	15	22
8	0	0	0	0	0	2	6

Tab. D.4: Tabulka výsledků simulací pro dobu vysílání 6,25 ms.

Počet osob	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Počet po sobě jdoucích kolizí	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**
0	0	0	0	4	0	0	0
1	284	70	17	2083	1	0	0
2	2959	3098	2744	3961	1529	731	582
3	708	1655	2827	844	4777	5229	5339
4	48	166	368	96	1483	2568	3292
5	1	11	41	11	182	408	651
6	0	0	3	1	27	50	111
7	0	0	0	1	1	12	20
8	0	0	0	0	0	2	5

Tab. D.5: Tabulka výsledků simulací pro dobu vysílání 5 ms.

Počet osob	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Počet po sobě jdoucích kolizí	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**
0	0	0	0	0	0	0	0
1	587	216	74	22	4	1	0
2	2989	3695	3808	3457	3065	2008	1708
3	399	1011	1934	3060	4091	5490	6103
4	25	74	171	418	766	1353	1890
5	0	4	12	38	67	132	250
6	0	0	1	5	6	14	43
7	0	0	0	0	1	1	4
8	0	0	0	0	0	1	2

Tab. D.6: Tabulka výsledků simulací pro dobu vysílání 3,84 ms.

Počet osob	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Počet po sobě jdoucích kolizí	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**
0	0	0	0	0	0	0	0
1	1140	637	303	149	48	16	9
2	2635	3834	4554	4785	4912	4119	3850
3	216	500	1081	1869	2724	4245	5201
4	9	28	61	162	299	588	854
5	0	1	1	14	16	30	78
6	0	0	0	1	1	2	6
7	0	0	0	0	0	0	2

Tab. D.7: Tabulka výsledků simulací pro dobu vysílání 3,2 ms.

Počet osob	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Počet po sobě jdoucích kolizí	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**
0	0	0	0	0	0	0	0
1	1609	1044	628	356	168	68	37
2	2248	3646	4653	5288	5776	5515	5467
3	138	300	692	1264	1904	3101	4001
4	5	10	27	85	148	305	454
5	0	0	0	7	4	11	37
6	0	0	0	0	0	0	3
7	0	0	0	0	0	0	1

Tab. D.8: Tabulka výsledků simulací pro dobu vysílání 1,92 ms.

Počet osob	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Počet po sobě jdoucích kolizí	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**
0	0	0	0	0	0	0	0
1	2778	2590	2277	1891	1487	976	786
2	1185	2333	3545	4791	5983	7058	7866
3	36	75	174	311	511	921	1275
4	1	2	4	6	19	45	70
5	0	0	0	1	0	0	3

Tab. D.9: Tabulka výsledků simulací pro dobu vysílání 1,6 ms.

Počet osob	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Počet po sobě jdoucích kolizí	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**
0	0	0	0	0	0	0	0
1	3136	3107	2957	2698	2351	1712	1507
2	845	1846	2930	4119	5342	6710	7662
3	18	45	113	180	299	555	787
4	1	2	0	3	8	23	43
5	0	0	0	0	0	0	1

Tab. D.10: Tabulka výsledků simulací pro dobu vysílání 0,96 ms.

Počet osob	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Počet po sobě jdoucích kolizí	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**
0	3	0	0	0	0	0	0
1	3665	4166	4527	4836	4990	4583	4599
2	329	824	1453	2129	2933	4277	5207
3	2	9	20	35	75	139	189
4	1	1	0	0	2	1	5

Tab. D.11: Tabulka výsledků simulací pro dobu vysílání 0,64 ms.

Počet osob	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Počet po sobě jdoucích kolizí	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**
0	20	5	1	1	0	0	0
1	3831	4587	5270	5902	6448	6570	7026
2	149	405	724	1089	1522	2382	2915
3	0	2	5	8	30	48	57
4	0	1	0	0	0	0	2

Tab. D.12: Tabulka výsledků simulací pro dobu vysílání 0,384 ms.

Počet osob	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Počet po sobě jdoucích kolizí	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**
0	97	42	18	11	3	1	0
1	3847	4812	5689	6578	7369	8043	8802
2	56	145	292	411	625	944	1190
3	0	1	1	0	3	12	8

Tab. D.13: Tabulka výsledků simulací pro dobu vysílání 0,16 ms.

Počet osob	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Počet po sobě jdoucích kolizí	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**
0	684	484	312	236	191	111	99
1	3307	4487	5634	6682	7690	8697	9662
2	9	29	54	82	117	192	268
3	0	0	0	0	2	0	1

Tab. D.14: Tabulka výsledků simulací pro dobu vysílání 0,096 ms.

Počet osob	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Počet po sobě jdoucích kolizí	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**	**Počet výskytů**
0	1274	1153	961	762	691	500	540
1	2723	3843	5021	6207	7258	8437	9380
2	3	4	18	31	50	63	80
3	0	0	0	0	1	0	0

Curriculum Vitæ

Jakub Frolka

Affiliation

E-mail:	frolka@vut.cz
Tel:	+420 541 146 993
WWW:	`https://www.vut.cz/lide/jakub-frolka-110408`

KVALIFIKACE A PROFESNÍ KARIÉRA

Kvalifikace

2015 – dosud	student doktorského studia oboru Teleinformatika,Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií.
2009 – 2012	Ing. obor Telekomunikační a informační technika, Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Diplomová práce: *BCH kódy*
2007 – 2009	Bc. obor Teleinformatika, Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Bakalářská práce: *Zabezpečení přenosu dat BCH kódy*

Profesní kariéra

2015 – dosud	Vědecko-výzkumný pracovník – Vysoké učení technické v Brně
2012 – dosud	Správce výpočetní techniky a interních počítačových sítí – Vysoké učení technické v Brně

VÝZKUMNÉ PROJEKTY

2022 – 2024	Transformace formy a obsahu vzdělávání na Vysokém učení technickém v Brně, MŠMT
2022 – 2023	VB01000036 Technologie pro testování kyberbezpečnosti ICT, MVČR
2017 – 2020	FEKT-S-17-4184 Výzkum informačních a komunikačních systémů a jejich bezpečnost
2018	OBJB170796 Implementace Linuxu a komunikačních funkcí (IP Sec) do PQ monitorů

ODBORNÉ ČINNOSTI

Pedagogická činnost

2018 – 2022	Architektura sítí
2016 – 2019	CCNA Cisco akademie

DALŠÍ KVALIFIKACE A ZNALOSTI

Jazykové znalosti	Český jazyk (rodilý mluvčí)
	Anglický jazyk (úroveň B2)

Specializační certifikace

2018	Mikrotik MTCNA, MTCNW, Academy trainer
2017	Palo Alto Networks Accredited Configuration Engineer (ACE)
2016	CCNA Instructor Fast Track
2016	200-125 Cisco Certified Network Associate

SHRNUTÍ PUBLIKAČNÍ ČINNOSTI

- Vědecké časopisy s impakt faktorem podle Web of Science: 3
- Mezinárodní konference indexované ve Web of Science nebo Scopus: 7
- Celkový počet citací podle Web of Science: 15
- Celkový počet citací podle Scopusu: 29
- H-index podle Web of Science: 2
- H-index podle Scopusu: 3