Energy efficient wireless network for long term continuous acquisition and monitoring of physiological parameters.

Celić, Luka

University of Zagreb
FACULTY OF ELECTRICAL ENGINEERING AND COMPUTING

Luka Celić

Energy efficient wireless sensor network for long term continuous acquisition and monitoring of physiological parameters

DOCTORAL THESIS

Zagreb, 2020.

University of Zagreb
FACULTY OF ELECTRICAL ENGINEERING AND COMPUTING

Luka Celić

Energy efficient wireless sensor network for long term continuous acquisition and monitoring of physiological parameters

DOCTORAL THESIS

Supervisor: Professor Ratko Magjarević, PhD.

Zagreb, 2020.

Sveučilište u Zagrebu
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

LUKA CELIĆ

Energetski učinkovita bežična senzorska mreža za dugotrajno kontinuirano prikupljanje i nadzor fizioloških parametara

DOKTORSKI RAD

Mentor: Prof. dr. sc. Ratko Magjarević

Zagreb, 2020.

Doctoral thesis was written at the University of Zagreb, Faculty of Electrical Engineering and Computing, Department of Electronic Systems and Information Processing.

Supervisor: Professor Ratko Magjarević, PhD.

Thesis consists 148 pages.

Thesis no. _____

About the Supervisor

Ratko Magjarević was born in 1959. in Zagreb. He graduated Electrical Engineering in 1982 and in 1988 he received his Master Degree. In 1994. he received his Ph.D. in the field of Electrical Engineering from the University of Zagreb. He spent his Academic career at the University of Zagreb, where he was elected to the position of full professor with tenure in the field of Electrical Engineering in 2011.

Apart from Zagreb, he has been teaching at the universities of Trieste, Ljubljana and Bogota, Colombia for many years. During 2005-06 Resides at the Institute for Biomedical Engineering, University of Stuttgart, Germany. Already in 2002-04 he was one of the experts on the European Commission project "Chartography of Medical and Biological Engineering in Europe" and later on the European projects FP6, FP7, Horizon 2020, TEMPUS and COST projects. He has been the leader of bilateral scientific projects with partners in Slovenia, Italy, the United Kingdom, Macedonia, Hungary, France and Colombia. He has led an R&D project under IRI1 and a number of other research and professional projects. He has published more than 80 papers in journals and conference proceedings, several editorial books, several book chapters and encyclopedia citations, and has delivered more than twenty invited lectures at major international conferences.

Professor Magjarević is an official and a member of several international and national scientific and professional organizations. In the International Federation of Medical and Biological Engineering (IFMBE), he was elected for two three-year terms of office as President: 2012-15 term and 2021 - 24. In 2014, he received the FER Golden Plaque "Josip Loncar" for his contribution to the teaching and development of biomedical engineering, as well as the recognition of the Senate of the Republic of Colombia for his global contribution to the development of biomedical engineering. In 2013, he was elected Honorary Senator of the University of Ljubljana.

O mentoru

Ratko Magjarević rođen je u Zagrebu 1959. godine. Diplomirao je elektrotehniku, smjer Industrijska elektronika, 1982., magistrirao 1988. i doktorirao 1994. godine u polju elektrotehnike na Sveučilištu u Zagrebu Fakultetu elektrotehnike i računarstva. Akademsku karijeru proveo je na Sveučilištu u Zagrebu gdje je 2011.g. izabran u zvanje redoviti profesor u trajnom zvanju u polju elektrotehnike.

Osim u Zagrebu, predaje već niz godina na sveučilištima u Trstu, Ljubljani i Bogoti, Kolumbija. Tijekom 2005.-06. boravi na Institute for Biomedical Engineering Sveučilišta u Stuttgartu, Njemačka. Već 2002.- 04. g. jedan od eksperata na projektu Europske komisije „Chartography of Medical and Biological Engineering in Europe“ a kasnije na europskim projektima FP6, FP7, Obzor 2020, te TEMPUS i COST projektima. Bio je voditelj bilateralnih znanstvenih projekata sklopljenih s partnerima u Sloveniji, Italiji, Ujedinjenom kraljevstvu, Makedoniji, Mađarskoj, Francuskoj i Kolumbiji. Vodio je istraživačko razvojni projekt u okviru IRI1 i niz drugih znanstvenoistraživačkih i stručnih projekata. Objavio je više od 80 radova u časopisima i zbornicima konferencija, nekoliko uredničkih knjiga, više poglavlja u knjigama i navoda u enciklopedijama te održao je više od dvadeset pozvanih predavanja na značajnim međunarodnim konferencijama.

Dr. sc. Magjarević je aktivan dužnosnik i član više međunarodnih i nacionalnih znanstvenih te strukovnih organizacija. U Međunarodnoj federaciji medicinskog i biološkog inženjerstva (International Federation for Medical and Biological Engineering – IFMBE), izabran je u dva trogodišnja mandata za Predsjednika u mandatnom razdoblju 2012.-15. g. i 2021. – 24. Godine 2014. primio je zlatnu plaketu "Josip Lončar" FER-a za doprinos nastavi i razvoju biomedicinskog inženjerstva kao i priznanja Senata Republike Kolumbije za globalni doprinos razvoju biomedicinskog inženjerstva. 2013.g. izabran je za počasnog Senatora Sveučilišta u Ljubljani.

Acknowledgments

Finishing PhD thesis across 2 continents and 3 countries is almost impossible without wide support. Firstly, I would like to express my deepest gratitude to my mentor prof. dr. sc. Ratko Magjarević. Over the 15 years we known each other and worked together on various projects, he showed only the highest professional work ethics and care for its students and colleagues. As students and colleagues, we knew he would protect our best interest which gave us great working motivation and positive atmosphere for contributing in the best of our abilities. While continuing my career and working for other employers, working with prof. Magjarević is still one off the most positive and rewarding work experience.

Secondly, I wish to express my deepest gratitude to my wife and my family. Changing several countries and employers while continuing to work on the theses would not be possible if my wife didn't take some of the burden on itself. My family and friends were always here to support me directly or indirectly and being able to share this achievement with them makes me a rich person.

I would also like to express my gratitude to the thesis's comity and my University department, ZESOI (Zavod za elektroničke sustave i obradu informacija). It was my home for many years and the university gave me full support since early undergraduate student days.

Lastly, I wish to express my gratitude to all professors and teachers. In a time when education and it's role is relativized, I would like to acknowledge the noble work they are doing and time they give to us un/grateful students coming and leaving through generation changes.

Abstract

Science and technology advancements in the past decade provide new means of support in medicine and healthcare, for patients and for the ageing population. One of the main challenges is the efficiency of healthcare services where much is expected from biomedical engineering solutions such as wireless sensor networks. Still perceived usefulness of the wearable devices and adoption rate is limited due to existing barriers, such as reliability and power efficiency of the portable devices. The motivation of the research in this thesis was to apply best practices in energy efficiency and wireless communication to lower adoption barriers, implement non-invasive devices for long-term continuous acquisition and monitoring of physiological parameters and extended cycles between device charging. Foundation for these changes are developments in connectivity and transfer of data towards the concentrator, gateway, smartphone or cloud. As wireless communication accounts for largest part of the sensor node consumption, it is crucial to use energy efficient wireless sensor networks.

An overview is given of technologies used in wireless sensors network for healthcare and different role which they fulfil. Approaches on how devices in healthcare are operating is changing with the rise of smartphones, broadband connectivity, cloud and IoT best practices. Later in the thesis, the absence of the comprehensive energy efficient wireless sensor network solution capable to guaranty consistent low power consumption across full bandwidth range, consistent bandwidth regardless of number of connected nodes and automatically adaptable bandwidth and latency based on changing requirements when device is in use are discussed.

The theses presents an architecture and methods for energy efficient wireless sensor networks, optimisations chosen to be embedded in the proposed solutions have none or limited dependency outside the architecture itself to provide consistent results on different platforms or environments not used in the theses. The research resulted in defining of two architectures of energy efficient wireless sensors network in healthcare. The first architecture is based on novel wireless and packet distribution protocols, while the second was designed to provide interoperability and seamless connectivity exploiting existing standards, technologies and best practices.

Successful validation and implementation of custom developed platform and protocols was made and showed fulfilling of the research and design goals.

Keywords: WSN, energy efficiency, low power consumption, seamless connectivity

Sažetak

Energetski učinkovita bežična senzorska mreža za dugotrajno kontinuirano prikupljanje i nadzor fizioloških parametara

Napredak znanosti i tehnologije u proteklom desetljeću u području poluvodičkih tehnologija, bežične tehnologije i povezivanja, minijaturizacije i integracije komponenti, umjetne inteligencije, pa čak i u području građe i sastava baterija za nosive i ugrađene uređaje, poboljšali su značajke i mogućnosti medicinskih uređaja. Smatra se da su takvi uređaji prikladni za pružanje podrške oboljelim osobama kao i starijem stanovništvu i da mogu značajno doprinijeti pružanju učinkovitih zdravstvenih usluga pojedincima koji se liječe, na rehabilitaciji ili žele nastaviti živjeti neovisno uz zadržanu kvalitetu života. Još uvijek nije u potpunosti prihvaćena korisnost nosivih uređaja od strane korisnika i njihovo usvajanje je ograničeno nizom prepreka. Projektiranje uređaja i sustava koji uvažavaju korisnika, njegove interese i ograničenja, moglo bi dovesti do povećanja prihvaćanja njihove korisnosti i stope usvajanja. Primjena najboljih praksi u energetskoj učinkovitosti i bežičnoj komunikaciji mogu smanjiti prepreke koje korisnik ima pri usvajanju nosivog uređaja budući da nisu invazivni i imaju produžene cikluse između punjenja uređaja. Temelj ovih promjena je razvoj u povezivanju i prijenosu podataka prema koncentratoru, usmjerivaču podataka, pametnom telefonu ili servisu u oblaku. Kako bežična komunikacija najčešće čini najveći dio potrošnje senzorskih čvorova, presudno je korištenje energetski učinkovite bežične mreže senzora. To se dodatno naglašava ako postoji namjera dugoročnog kontinuiranog prikupljanja i praćenja fizioloških parametara.

Područje istraživanja ove disertacije je optimiranje potrošnje elektroničkih sustava, u ovom slučaju bežične senzorske mreže za dugotrajno kontinuirano prikupljanje i nadzor više fizioloških parametara (višeparametarsko praćenje). Neposredna primjena istraživanja je u praćenju kardiovaskularnih pacijenata tijekom rehabilitacije, s mogućnošću prilagodbe sustava za praćenje pacijenata oboljelih i od drugih nezaraznih kroničnih bolesti.

U radu je izložen pregled područja istraživanja, tehnologija koje se koriste u bežičnim senzorskim mrežama za zdravstvo i različite uloge koje one izvršavaju. Porastom broja i uporabe pametnih telefona, širokopojasne povezanosti, servisa u oblaku i razvojem najboljih praksi u IoT-u pristupi funkcioniranja uređaja u zdravstvu se mijenjaju. Iako široko korišteni komunikacijski protokoli omogućavaju isporuku novih funkcionalnosti krajnjem korisniku, njihova ograničenja motivirala su na ovo istraživanje. Uočen je nedostatak sveobuhvatnog

energetski učinkovitog bežičnog senzorskog rješenja sposobnog: jamčiti nisku potrošnju energije u cijelom rasponu korištenja kapaciteta komunikacijskog kanal, konzistentnu propusnost bez obzira na broj spojenih čvorova, automatski prilagodljivu propusnost i latenciju na temelju promjena potreba spojenih uređaja. Rad opisuje i analizira elemente potrošnje energije bežične senzorske mreže, zajedno s analizom primjenjivih optimizacija. Cilj teze je predložiti arhitekturu i metode za postizanje energetski učinkovite bežične senzorske mreže, stoga odabrane optimizacije i predložena rješenja nemaju (ili imaju minimalnu) ovisnost izvan same arhitekture. Opisani pristup je odabran kako bi se dobili konzistentni rezultati korištenja predložene arhitekture na platformama ili okruženjima različitim od opisanih u disertaciji. Istraživački rad rezultirao je razvojem dviju arhitektura energetski učinkovitih bežičnih senzorskih mreža u zdravstvu. Prva arhitektura se temelji na novo razvijenim protokolima za bežičnu i paketnu distribuciju, dok je cilj druge arhitekture osiguranje interoperabilnosti i bešavne povezanosti koristeći postojeće standarde, tehnologije i najbolje prakse.

U kontekstu bežične komunikacije između dva nosiva uređaja, komunikacija se često odvija u ograničenom neposrednom području tijela (Wireless Body Area Network - WBAN) ili u području lokalne bežične mreže (Wireless Local Area Network - WLAN). Bežična komunikacija može se odvijati u licenciranim dijelovima radio spektra poput onog namijenjenog ostvarivanju komunikacijskih usluga za ugrađene medicinske uređaje (engl. Medical Implant Communications Services, MICS) ili u dijelu spektra otvorenim za javnu upotrebu u industriji, znanosti i medicini (engl. Industrial, Scientific and Medical, ISM). Minimalni uvjet za ostvarenje uspješne komunikacije između odašiljačkog i prijamnog čvora je prijam signala na prijamniku koji je veći od minimalne osjetljivosti prijamnika. Na osjetljivost i jačinu prijamnog signala utječe radio frekvencija nosioca signala, modulacija signala, izračena snaga odašiljača, gubici u prijenosnom kanalu, te dobici ili gubici prijamne i odašiljačke antene. Niže radio frekvencije nosioca obilježava i niže prigušenje u prostoru, veća prodornost kroz prepreke, te u konačnici rezultira povećanim dometom komunikacije. Međutim niže frekvencije nosioca nameću i nižu brzinu prijenosa podataka radi ograničene širine dostupnog radnog radio spektra te time ograničava količinu informacija koju je moguće razmijeniti između dva bežična čvora. Osjetljivost radio prijamnika za određenu frekvenciju nosioca moguće je povećati korištenjem modulacije s manjom brzinom prijenosa znakova. Navedena opcija poput korištenja manje radiofrekvencije nosioca značajno će limitirati mogućnost razmjene podataka između dva bežična čvora.

Model povezivanja otvorenih sustava (engl. Open System Interconnection model, OSI) dijeli ukupnu funkcionalnost protokola na slojeve poput definicije fizikalnih specifikacija za korišteni medij, protokol za uspostavljanje i održavanje pristupa mediju i slično. Većina protokola namijenjena za komunikaciju bežičnih senzorskih čvorova definirana je ili u prvom i drugom sloju OSI modela ili u petom, šestom i sedmom sloju. Navedeni pristup rezultira protokolima koji su najčešće bazirani na TCP/IP protokolima, stoga i efikasnost cjelokupnog protokola uvelike je definirana njihovim značajkama. Protokoli koji primjenjuju OSI model, definiraju namjensko zaglavlje u svakom sloju kako bi se osigurala mogućnost neovisne zamjene pojedinog sloja bez utjecaja na ostale slojeve. Takav pristup rezultira povećanim zaglavljem u nižim slojevima OSI modela što rezultira povećanim brojem podataka koji se trebaju razmijeniti između dva bežična čvora. Dodatno, pojedini slojevi mogu imati redundantne podatke. Budući da razmjena podataka značajno doprinosi ukupnoj potrošnji, minimiziranjem količine razmijenjenih i redundantnih podataka minimizira se i potrošnja.

Energetska učinkovitost bežične senzorske mreže rezultat je energetske učinkovitosti svih pojedinih komponenti. Analizu potrošnje pojedinih komponenti i pronalaženja istovjetnosti moguće je olakšati grupiranjem komponenti prema području djelovanja: individualno, lokalno i globalno. Komponente na koje sustav može utjecati odabirom ili dizajnom s ciljem ostvarivanja energetski učinkovitog bežičnog sustava su radio primopredajnik, komunikacijski protokol, procesorska jedinica i vremenska sinkronizacija. Česte metode optimizacije energetske učinkovitosti uključuje optimizaciju radio protokola, redukciju razmjene podatka, optimiziranu budnost čvorova te energetski učinkovito usmjeravanje.

Prva predložena i razvijena arhitektura temeljena na novo razvijenim protokolima sačinjena je od dvije temeljne komponente bežičnih senzorskih mreža: i) energetski učinkoviti bežični protokol za razmjenu podataka u bežičnim senzorskim mrežama u zdravstvu i ii) protokol razmjene paketa visoke propusnosti namijenjen prijenosu biomedicinskih podataka u stvarnom vremenu.

Energetski učinkovit bežični protokol za razmjenu podataka u bežičnim senzorskim mrežama u zdravstvu temeljen je na sveobuhvatnom pristupu optimiziranja potrošnje: optimiran pristup mediju, minimiziranje negativnih učinaka gubitka paketa, adaptivna raspodjela propusnosti unutar okvira, prilagodljiva latencija, kompenzacija pogreške i stabilnosti oscilatora, optimirane metode za izračunavanje preciznog stvarnog vremena i smanjenje podataka zaglavlja.

Pristup mediju optimira i raspodjeljuje teret potrošnje između pristupne točke i spojenih senzorskih čvorova te smanjuje utjecaj povišene potrošnje uslijed gubitka paketa. Povišena potrošnja pristupne točke je posljedica aktivnog vremena komunikacije s višestrukim senzorskim čvorovima, dok je povišena potrošnja senzorskog čvora posljedica potrebe ranijeg buđenja iz stanja mirovanja i dužeg vremena u kojem je prijamnik aktivan. Kompenzacija pogreške računanja vremena i oscilatora omogućuje vremensku točnost koja minimizira vrijeme koje prijamnik i odašiljač moraju provesti u aktivnom stanju te smanjenje utjecaja rasta potrošnje uslijed gubitka paketa. Ukoliko se zaglavlje paketa ne primi unutar određenog vremena, čvor odlazi u stanje mirovanja kako bi se smanjila potrošnja. Dostupnost visoke vremenske točnosti omogućava računski i energetski učinkovite zamjene dijeljenja s množenjem i logaritamskim dijeljenjem. Zahvaljujući logaritamskim svojstvima moguće je korištenje logaritamskog dijeljenja s bazom koja se realizira primjenom pomičnog registra. Dodatno smanjenje potrošnje ostvareno je uparivanjem optimiranog zaglavlja, primjenom adaptivne latencije i adaptivne raspodjele širine kanala (engl. *bandwidth*). Optimirano i reducirano zaglavlje u svakom paketu prema pristupnoj točki ubacuje i broj paketa koji čekaju na razmjenu. Time pristupna točka ima uvid u stvarnom vremenu potrebe svih povezanih čvorova. Ukoliko pojedini čvor ima i povećane potrebe za izmjenu paketa, pristupna točka može koristiti manju latenciju i dodijeliti veću širinu kanalu unutar pojedinog okvira. Ukoliko pojedini čvor nema potrebe za izmjenom podataka, pristupna točka povećava latenciju kako bi se ostvarila smanjena potrošnja.

Protokol razmjene paketa visoke propusnosti namijenjen prijenosu biomedicinskih podataka u stvarnom vremenu ostvaren je višeslojnim pristupom optimizacije, primjenom konteksta komunikacije, adaptivnom veličinom adresnog prostora i metoda ravnomjerne raspodjele propusnosti kanala.

Višeslojni pristup sagledava istovremeno funkcionalnost svih slojeva u komunikaciji između dva uređaja. Takav pristup zajedno s primjenom konteksta komunikacije omogućio je drastično smanjenje zaglavlja u odnosu na druge protokole uz gotovo potpuno zadržanu funkcionalnost. Definirana su četiri konteksta komunikacije: komunikacija susjeda, dostava paketa čvora centralnom serveru, dostava paketa čvoru s naznačenom adresom i dostava paketa svim čvorovima u mreži. Dostava paketa susjednom čvoru garantira redukciju zaglavlja od 8 bajta, dostava paketa centralnom serveru i dostava paketa svim čvorovima garantira najmanju uštedu od 4 bajta. Posebno značajna ušteda u kontekstu senzorskih čvorova s limitiranim izvorom energije je garantirana ušteda od 8 bajta između rubnog čvora, koji je najčešće

senzorski čvor i sljedećeg čvora. S obzirom na postignutu redukciju podataka, moguće je optimirati i ograničiti maksimalnu duljinu paketa kako bi se postigla ravnomjernija raspodjela propusnosti kanala. To je posebice važno za podatke u stvarnom vremenu koji su generirani od strane senzorskih čvorova s ograničenom radnom memorijom.

Iako novo razvijeni protokol razmjene paketa visoke propusnosti namijenjen prijenosu biomedicinskih podataka u stvarnom vremenu pruža poboljšanu učinkovitost, pojedine implementacije mogu zahtijevati upotrebu standardnih protokola. U sklopu rada, provedeno je istraživanje i modeliranje mogućnosti optimiranja standardnog protokola. MQTT protokol je odabran s obzirom na sve veću upotrebu u modelu komunikacije objave/pretplate (engl. *publish/subscribe*) u komunikaciji bežičnim mrežama Internet stvari (engl. *Internet of Things*) te za bazne protokole notifikacija za servise u oblaku. Optimizacija je fokusirana na reduciranje podataka potrebnih za prijenos u MQTT protokolu, zaglavlju i temi poruke. Predstavljena optimizacija donosi dvije razine optimizacije ovisno o potpunom ili djelomičnom pridržavanju standarda, uz zadržavanje deskriptivnosti teme MQTT protokola. Budući da je pretpostavka kako primarni protok informacija teče u smjeru nosivog čvora, preko pristupne točke prema brokeru poruka, optimizacija zamjenjuje ponavljajući prijenos teme za jedan zamjenski bajt (engl. *Wildcard)*.

Validacijom optimizacije i implementacije novo razvijenih protokola potvrđeno je ispunjavanje postavljenih ciljeva dizajna novo razvijenih protokola, međutim potrebno je zapaziti poteškoće pri korištenju razvijenih platformi temeljenim na istim. Potrebni su značajni resursi za istraživanje i razvoj, dokumentaciju, edukaciju i održavanje platforme operativnom. Dodatno, ove tehnologije nisu dostupne u svakodnevnom okruženju korisnika stoga se njihova korisnost može ostvariti u specijalno razvijenim platformama i sustavima. Logičan slijed nastavka istraživanja je proveden u smjeru istraživanja mogućnosti optimiranja tehnologije dostupne u svakodnevnom okruženju korisnika s ciljem ostvarenja arhitekture energetski učinkovite bežične senzorske mreže.

Upotreba sve više prisutne bežične tehnologije rezultirat će i većom izloženošću korisnika drugim uređajima u blizini. Stoga je potrebno dodatno zaštiti sigurnost i anonimnost korisnika. Istovremeno povezivanje se želi dozvoliti samo čvorovima koji su dokazali svoj identitet. Postojeće tehnologije poput Bluetooth IRK, Edystone ephemeral ID i Microsoft CDP nisu u mogućnosti ponuditi metode identifikacije uz zadržanu anonimnost za sve predviđene uvjete rada: Internet veza dostupna, Internet veza nedostupna, lokalna i globalno distribuirana lokacija potvrde identiteta. Dodatno, želja je omogućiti korisniku bešavnu oportunističku

povezanost. Bešavna povezivost bez korisničke potrebe za uspostavljanjem/održavanjem veze može pružiti korisniku, a posebno starijoj populaciji i pacijentima, jednostavnost upotrebe i poboljšano korisničko iskustvo. Jednostavnost upotrebe i eliminacija potrebe za sučeljem prema korisniku otvara mogućnost manjih i ergonomičnijih senzorskih uređaja pogodnih za primjenu u zdravstvu. S obzirom da je Bluetooth tehnologija sveprisutna u okruženju korisnika, primarno radi nazočnosti u mobilnim uređajima korisnika, Bluetooth je odabran kao tehnologija kojom će se pokušati optimirati funkcionalnosti protokola i po potrebni razvoj dodataka protokolu kako bi se ostvarili navedeni ciljevi.

Druga novo razvijena arhitektura razvijena upotrebom tehnologije prisutne u okruženju korisnika, definira energetski učinkovitu arhitekturu i metode za pružanje anonimne bešavne povezanosti za dugotrajno kontinuirano prikupljanje i nadzor fizioloških parametara nosivih uređaja preko poznatih i nepoznatih roaming mreža. Razvijena arhitektura koristi Bluetooth LE standard uz dodatne optimizacije koje osiguravaju nisku potrošnju prilikom učestale promjene pristupnih točki. Predloženo rješenje pruža mrežno-agnostičko usmjeravanje paketa prema aplikaciji bez obzira je li čvor u kućnoj ili roaming mreži. Upravljanje povezivanjem je autonomno, bez korisničkog unosa ili upravljanja. Kako bi se motivirale nepoznate pristupne točke za pružanje oportunističke Internetske povezanosti, predloženi su načini certificiranja i opseg certificiranja. Predstavljen certifikat potvrđuje da uređaj koji traži povezivanje služi za dozvoljene certificirane aktivnosti bez pokušaja nepotrebnog crpljenja resursa pristupne točke. Omogućavanje bešavne povezanosti zahtjeva prevladavanje oprečnih zahtjeva: i) odašiljanje radio fara s ciljem označavanja prisutnosti uređaja radi pokretanja postupka povezivanja uz sprječavanje profiliranja i održavanje privatnosti uređaja, ii) sigurno povezivanje s nepoznatim anonimnim uređajima i iii) osiguranje povezanosti u matičnoj/kućnoj ili u nepoznatoj/roaming mreži uz zadržanu uniformnost komunikacije. Opisane metode otkrivanja i certifikacije uređaja razvijene u ovom dokumentu zadržavaju anonimnost korisnika dok istovremeno podržavaju funkcionalnosti brzog međusobnog povezivanja sa ili bez pristupa Internetu. Uspostava komunikacijske veze između dva bežična čvora koja su članovi iste matične mreže ostvaruje se direktno bez posrednika. Uspostava komunikacijske veze između dva međusobno nepoznata čvora u roamingu uspostavlja se putem pristupne točke i davatelja certifikacijske usluge u oblaku. S obzirom da je svrha povezivanja u roamingu pristup Internetu kako bi se došlo do matične mreže, pristupna točka i davatelj certifikacijskih usluga moraju dokazati senzorskom čvoru da uistinu i posjeduju povezanost prema Internetu. Senzorski čvor dostavlja pristupnoj točki zahtjev na koji može ispravno odgovoriti jedino matični davatelj usluge. Stoga pristupna

točka mora proslijediti zahtjev svojem matičnom davatelju usluga koji taj zahtjev prosljeđuje davatelju usluge senzorskog čvora. Adresa davatelja usluge nalazi se u radio far paketu odašiljanog od strane senzorskog čvora. Razvijeno rješenje podržava decentraliziranu funkcionalnost više ponuđača usluga, izbjegavajući zaključavanje dobavljača i ograničavajući eksploataciju širom svijeta. Opisana je optimizacija implementacije BLE radio-signala koji je u skladu sa BLE standardom koji može podržati postupak uspostavljanja veze. Novo razvijena arhitektura energetski učinkovitog bežičnog sustava za dugotrajno kontinuirano prikupljanje i nadzor fizioloških parametara putem oportunističke povezanosti nazvana je Se-Co (*Seamless Connectivity*).

Verifikacija rezultata istraživanja provedena je na modelu sustava, a validacija protokola napravljena je mjerenjima u različitim uvjetima primjerenim zdravstvu, za najpovoljniji i najnepovoljniji scenarij. Ostvareni izvorni znanstveni doprinosi doktorskog rada su:

1. Protokol za raspodjelu paketa u senzorskoj mreži namijenjenim prijenosu biomedicinskih podataka, temeljen na optimizaciji strukture zaglavlja paketa.
2. Energetski učinkovit komunikacijski protokol za primjenu u senzorskim mrežama namijenjenim prijenosu biomedicinskih podataka, temeljen na optimizaciji vremena pristupa mediju te optimizaciji korisnog dijela poruke
3. Arhitektura energetski učinkovitog bežičnog sustava za dugotrajno kontinuirano prikupljanje i nadzor fizioloških parametara.

Istraživanje bi bilo dobro nastaviti u području potvrđivanja sigurnosnih zahtjeva i jačanja modela povjerenja i provjere valjanosti certifikata. Vrijedno je napomenuti da u trenutnom Se-Co rješenju dva pružatelja usluga moraju jedni drugima vjerovati. Domaći davatelj izdaje roaming pružatelju anonimnu potvrdu za uređaj u roaming mreži. Omogućavanje paradigme nultog povjerenja, gdje dva pružatelja usluga ne moraju vjerovati jedni drugima može značajno unaprijediti predloženu metodu.

Contents

1 Introduction

Healthcare, diagnostic treatments and therapy are becoming more accessible in a world where the global population is getting older. Eurostat projects that the share of those aged 80 years or above in the EU-28's population will increase by two and a half times between 2018 and 2100, from 5.6 % to 14.6 %, as shown in Figure 1-1. The effects of this group shift is projected to increase overall healthcare costs, as shown in Figure 1-2. Greater pressure is now being brought to bear on reducing wasteful treatments [1] or improving efficiency using new technologies. One of these new technologies is wearable device technology.

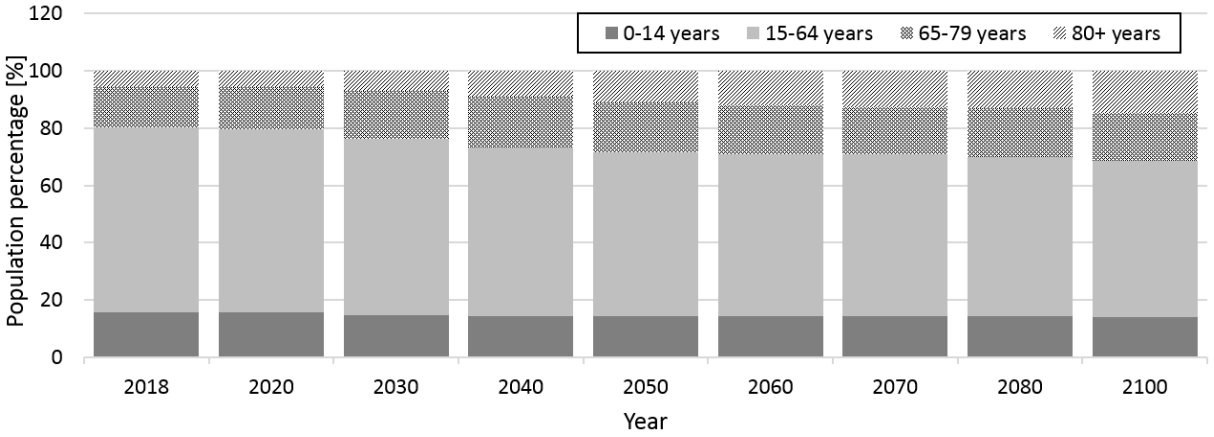


Figure 1-1 Population structure by major age groups, EU-28, 2018-2100 (% of total population) [2].

Traditionally telemonitoring equipment was used only during patient stays in the hospital as the system and unit costs were too high for the users and communication technologies were limited and cumbersome. Over the past two decades multiple technologies have undergone substantial improvements. Advancements in semiconductor technologies have enabled the capability to deliver faster, smaller and cheaper integrated circuits. The rise of wireless technology and connectivity have created the concept of connectivity everywhere, with mobile Internet at the core of the concept. Further, developments in battery chemistry have delivered greater power densities which have resulted in reduced size of batteries.

As a consequence of all of these combined advancements, new solutions and systems are becoming feasible and coming within reach of end users. In particular, these advancements have enabled delivery of improved performance wearable devices for healthcare. Such newly delivered devices are enabling long term patient monitoring and the integration of their data

into healthcare systems aimed at supporting medical decision making. Wearable devices are capable of providing new functionalities to healthcare such as personalisation, supporting the ageing population and increased efficiency of healthcare services. This is especially true for individuals who are under medical treatment, rehabilitation and/or who are currently living independently and wish to continue to do so (Figure 1-3).

However, the perceived usefulness of such wearable devices and their adoption rate has been limited due to existing barriers in design, especially those related to the power consumption of wearables, i.e. the need for frequent recharging of wearable devices or their bulky construction due to the dimensions and/or weight of batteries. Promotion and adoption of those designs which are tailored to the user in terms of his specific health and wellness issues, and his interest in some specific functionalities, could lead to an increase of perceived usefulness of the wearable devices and to a higher adoption rate. Applying best practices in energy efficiency and wireless communication may lower adoption barriers through less obtrusive devices and extended cycles between device charging. The foundation for these changes is improvements in connectivity and transfer of data towards the concentrator, gateway, smartphone or cloud.

As wireless communication accounts for the largest part of the sensor node consumption, it is crucial to use energy efficient wireless sensor networks. This is further accentuated if there is the intent for long term continuous acquisition and monitoring of physiological parameters. Therefore, improvement in power consumption optimisation and reduction may increase user acceptance and contribute to individuals' health or wellness improvement. The research conducted and the results described in this thesis is focused towards presenting the impact of communication protocol structure and architecture on the energy efficiency of a wireless system.

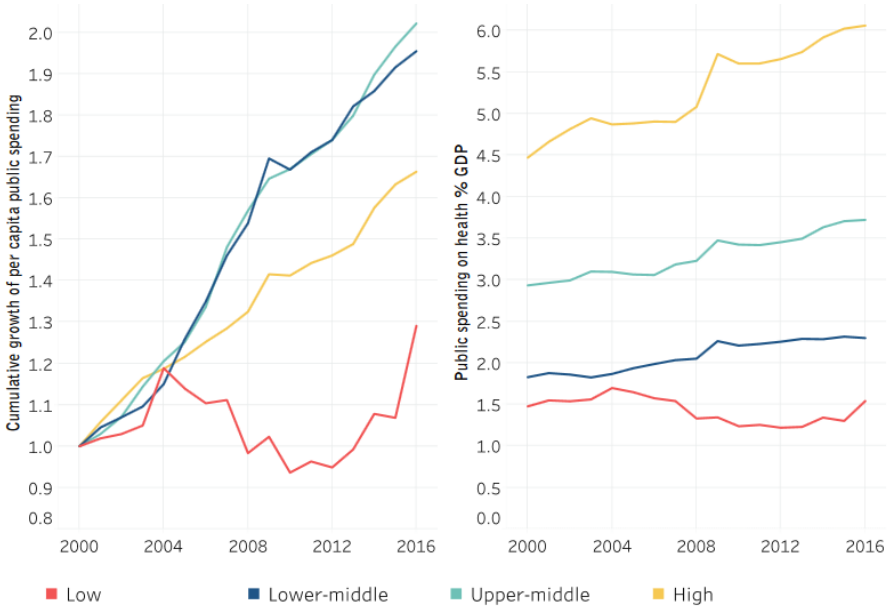


Figure 1-2 Public per capita spending on health is increasing, with the exception of low-income countries (from [3]).

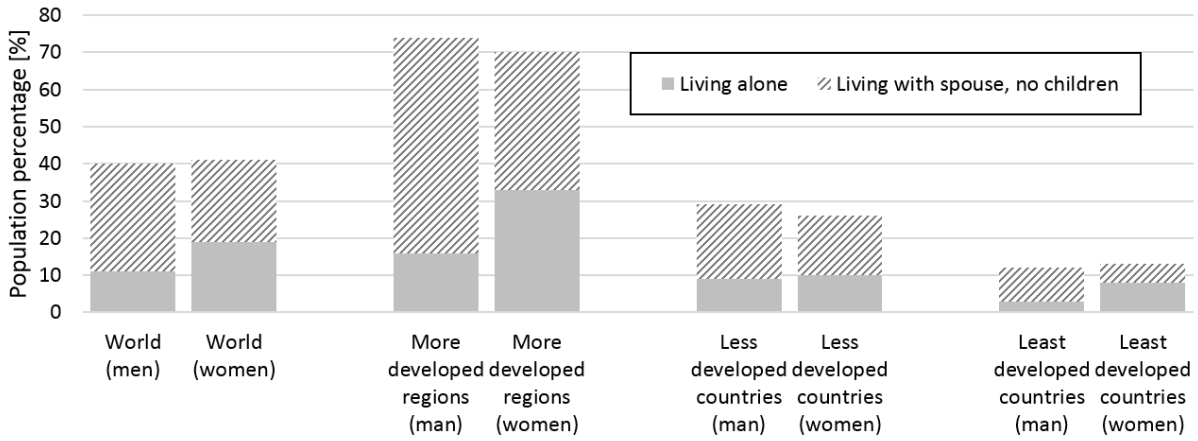


Figure 1-3 Percentage of people over 60 years of age living independently in a) the world, b) more developed regions, c) less developed regions, and d) least developed countries [4].

An overview is given of technologies used in wireless sensor networks for healthcare and the different roles which they fulfil. Approaches to how devices in healthcare are operating are changing with the rise of smartphones, broadband connectivity, cloud and IoT best practices. Although widely used communication protocols are enabling delivery of new functionalities to the end user, they possess limitations. It is these limitations which have motivated this research. As needs change during the course of the day, transmission requirements change from state transmission (in normal conditions) to full telemetry

transmission (in case of emergency or full data gathering). As most wireless protocols have fixed frame rates, should additional data arrive in the transmitting buffer, the protocols can transmit data by extending transmission until the end of the frame. This results in a constant minimal latency which data will experience before they are transmitted, and possible medium collision. Should the application require low latency for transmission of real time data, it is required to set a higher frame rate during the connection stage. A higher frame rate will result in higher minimal consumption, decreasing the intervals between which the device needs to be charged.

Designed optimisation methods applied in standard wireless communication protocols encompass limitations which have motivated this research activity. A particular motivation was to propose solutions for bridging the absence of a comprehensive energy efficient wireless sensor network. This solution has to be capable of guaranteeing: consistent low power consumption from the minimal to maximal bandwidth used; consistent bandwidth regardless of number of connected nodes; automatically adaptable bandwidth and latency based on changing requirements when device is in use; low overhead across all Open System Interconnection (OSI) layers; modern routing optimisations and a seamless experience for the end user.

The thesis is divided into 5 chapters: i) Introduction, ii) Wireless sensor networks and protocols in healthcare, iii) Optimization of energy efficiency in communication protocols for long term data acquisition and monitoring in wireless networks, iv) Architecture of an energy efficient wireless system for long term continuous data acquisition and monitoring and its validation and v) Discussion and conclusion.

The second chapter starts with an overview of wireless sensor networks in healthcare and associated technologies and protocols. An overview of existing protocol footprints across multiple Open System Interconnection layers is presented. Also, an overview is given of challenges in maintaining reliable and continuous connectivity required for acquisition and monitoring of physiological parameters from a wireless sensor network. Further, the limitations of existing protocols are highlighted.

The second part of the chapter focuses on analysing the energy efficiency of wireless sensor networks. A description and analysis of energy consumption constituents is given together with available power saving mechanisms. As the goal is to deliver an architecture and methods for an energy efficient wireless sensor network, the discussion concentrates on tools and methods for which no, or limited, dependency are present outside the architecture itself, to provide consistent results on different platforms or environments not addressed in this thesis.

These tools and methods encompass radio modulation, medium access control, mitigating clock error and timing source stability.

The third and last part of the chapter analyses wearable device barriers, privacy, security and seamless connectivity. A comprehensive approach was taken to determine the main wearable device adoption rate barriers and what is perceived device usefulness. Guidelines are given, to which non-functional requirements of wearable devices and underlining technology should adhere, for a successful adoption rate. Since a wearable device transmits data over the air, nearby observers can intercept packets or detect activity, therefore an overview of privacy and security threats is given. Analysis of vulnerability, and techniques to preserve privacy of a Bluetooth low energy technology, is presented. This part of the chapter concludes with an analysis and overview of researchers approaches to achieve seamless connectivity.

The third chapter outlines a novel architecture for an energy efficient wireless system for long term continuous data acquisition and monitoring of physiological parameters. Two main components of the architecture are outlined; i) an energy efficient wireless protocol for exchange of data in wireless sensor networks in health care, and ii) a high throughput packet exchange protocol for real time data in wireless sensor networks in healthcare.

The first part of the chapter concentrates on the notion of energy efficient wireless protocols for the exchange of data in wireless sensor networks in health care. A comprehensive optimisation approach is developed based on research of the following characteristics of the protocol: optimised medium access control, adaptive bandwidth allocation, adaptive latency, compensation of clock inaccuracy and stability, power optimised methods to calculate precise time using fixed point arithmetic, data reduction and minimising negative effects of packet loss. The specificity and commonalities of healthcare use cases outlined both impose challenges and present optimisation opportunities when trying to achieve energy efficiency. Combined multi-layer protocol optimisation in the context of exploiting healthcare device operation resulted in reduction of protocol overhead and improved energy efficiency. Novel methods for adaptive bandwidth allocation, adaptive latency and adaptive energy saving methods are shown and behaviour modelled. Embedded methods in the protocol seamlessly switch from low throughput high latency to low latency high throughput mode and maximise energy efficiency for changing operation requirements. Developed methods for automatic bandwidth allocation and energy saving are shown and modelling of their performance is carried out. In wireless communication and protocols, packet loss is a “normal” occurrence, therefore analysis of packet loss impact is made. Conclusions from the analysis on how to minimise packet loss impacts are

embedded into the method to minimise negative impacts when packet loss occurs. Clock synchronisation underpins energy efficient wireless communication so methods to maintain the required clock synchronisation between two communicating nodes are developed. Modelling of the developed method is carried out to establish the appropriate trade-off between absolute clock synchronisation error and power consumption to maintain a selected level of error. This part of the chapter concludes with modelling of the expected power consumption envelope.

The second part of the chapter presents a novel high throughput packet exchange protocol for real time data in wireless sensor networks in healthcare. Through the multi-layer approach, it is possible to greatly reduce requirements on the distribution layer. Additionally, it is shown that by exploiting context information when routing and introducing a publish-subscribe model, it is possible to greatly reduce the size of the packet header without compromising packet delivery and achieve high throughput. The developed novel protocol with reduced header size and resulting small overhead allows the selection of a smaller maximum size of the packet. This small packet size facilitates equal distribution of bandwidth to multiple services in memory-constrained wearable devices. This novel protocol with low overhead achieves the same packet efficiency when sending small packets like most standard protocols using larger packets.

Certain projects may have limitations in using custom developed protocols, thus a requirement may be to use existing protocols and standards. In the last section of the chapter, a novel method to achieve high efficiency while using a standard MQ Telemetry Transport (MQTT) packet/message protocol employed in wearables and IoT is presented. The presented optimisation delivers two levels of optimisation depending on the total or partial adherence to the standard. As the assumption is that flow of information is primarily from the wearable node upstream, across a gateway towards a message broker, optimisation exchanges repetitive transmission of the topic for a single wildcard byte. Optimisations retain topic descriptiveness of the MQTT protocol while being capable of providing great data reduction.

Chapter four is dedicated to validation of the developed architecture of an energy efficient wireless system for long term continuous data acquisition and monitoring. Test platform and platform components are described. All platform components are custom developed, from the wearable device itself up to software programme support. Validation of the novel protocols developed confirmed the previously defined models, matching observed behaviour and measured parameters. Although successful validation and implementation of the novel custom developed platform and protocols was carried out and they fulfilled design goals,

there is a need to acknowledge difficulties when using proprietary developed tools and materials. Substantial research and development resources and expertise needs to be available in order to build the platform. This can limit scalability and increase operational cost. Additionally, these technologies are not available in a user's everyday environment, requiring costly investment. Research was conducted on how to exploit technologies available to the user to provide an architecture for energy efficient seamless connectivity by means of a neutral impact connecting/sharing approach and guaranteeing to the user security and anonymity. Providing seamless connectivity requires overcoming contradictory requirements: i) broadcasting device presence to initiate the connection process while preventing device profiling and maintaining device privacy, ii) connecting to unknown anonymous devices while maintaining security, and iii) ensuring connectivity in home and roaming networks while maintaining communication uniformity. Research of available technology and solutions to fulfil these requirements showed a lack of suitable candidates, with most solutions supporting only a single vendor provider.

The novel architecture presented in this thesis defines an energy efficient architecture and methods for providing anonymous seamless connectivity for wearable and IoT devices across known and unknown networks. The device discovery and certification methods developed herein retain user anonymity while supporting efficient fast offline and online functionality. The proposed solution provides network-agnostic routing to the application, irrespective of whether the node is in a home or roaming network. Management of the connectivity is autonomous, without user input or management. Certification methods and nodes certification scope was proposed to incentivise unknown networks to provide Internet connectivity, as certified devices do not pose a security threat for those network. The developed solution supports decentralised multivendor functionality, avoiding vendor lock in and limiting worldwide exploitation. Implementation optimisation of the Bluetooth Low Energy (BLE) broadcast beacon, which is compliant with the BLE standard capable of supporting the Seamless Connectivity (Se-Co) connection setup process, is described.

In the fifth chapter, a broad discussion on architecture is presented and conclusions are given. Research work resulted in the development of two novel architectures of energy efficient wireless sensor networks in healthcare. The first architecture is based on novel wireless and packet distribution protocols, while the second was designed to provide interoperability and seamless connectivity exploiting existing standards, technologies and best practices. Taking into account the research work and the results achieved, the following contribution may be

declared as being achieved: i) Energy efficient communication protocol for application in sensor networks aimed at transfer of biomedical data based on optimisation of media access time and optimisation of payload, ii) Packet distribution protocol in sensor networks aimed at transfer of biomedical data based on optimisation of packet header structure, and iii) Architecture for an energy efficient wireless system for long term continuous data acquisition and monitoring of physiological parameters.

2 Wireless sensor networks and protocols in healthcare

2.1 Wireless sensor networks overview

This section starts with an outline of wireless sensor networks in healthcare and related technologies and protocols. Upon providing an overview of the existing technology, challenges in accomplishing reliable and continuous acquisition and monitoring of physiological parameters from a wireless sensor network are presented.

2.1.1 Wireless communication technologies and protocols in health care

Technology advancements over the past decade in the fields of semiconductor technology, wireless technology and connectivity, components miniaturisation and integration, artificial intelligence and the chemistry of batteries are redefining healthcare. Healthcare device communication range and scope can be a short-range (across the body area only): Wireless Body Area Network (WBAN), or part of a Wireless Local Area Network (WLAN), where it communicates with nearby devices. The basis of WBAN devices is wireless communication, where communication without the need for human interaction is preferable. This method of communication encompasses the operating principle of Internet of Things (IoT) devices. Examples of shared principles are security, privacy, connection establishment, power management and many others. Many publications [5-7] combine the two terms together. WBAN could be defined as a special purpose sensor network designed to operate autonomously to connect various medical sensors and appliances located inside and outside a human body. The IEEE802.15.6 standard [8] defines WBANs as a single hub with several sensor nodes. IoT could be defined as system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction [9]. Since WBAN and IoT devices span across multiple technologies, research on technology state of art and best practices was carried out in the fields of healthcare, WBAN, wearable devices and IoT [10-23] as well as network and security.

Wireless networks operate in both, licensed and unlicensed radio bands [11]. Licensed bands are Medical Implant Communications Services (MICSs) which is reserved for implant

communications and Medical Telemetry Services (WMTSs). Devices operating on these bands generally offer low data rates. Devices operating on Industrial, Scientific and Medical (ISM) and Ultra-wideband (UWB) bands offer higher data rates. Table 2-1 outlines frequency bands and their usage. Protocols operating on the 2.4 GHz ISM band are Ant, ZigBee, Bluetooth Low Energy (BLE), Thread, 6LoPAN. Since the band is open, it is prone to interference in populated areas. Wireless networks can operate in star network topology, mesh network topology [24] or in a hybrid start-mesh topology configuration [25]. Mesh networks are resilient to a single node outage, but the routing of data can consume additional power and node's resources. A star network is more efficient and resource conservative, but it is susceptible to a single node outage.

Table 2-1 Frequency bands and usage

Frequency band	*Use*
402 to 405 MHz	Medical Implant Communications Service (MICS) band, Narrowband (NB)
420to 450 MHz	WMTS Band (used in Japan), Narrowband (NB)
433.05 - 434.79 MHz	ISM Europe
605 to 614 MHz	WMS Band (used in USA), Narrowband (NB)
1395 to 1400 MHZ	
863 to 870 MHz	WMTS Band in Europe, Narrowband (NB)
902 to 928 MHz	Narrowband (NB)
2400 to 2450 MHz	ISM Global
3100 to 1600 MHz	UWB Band

2.1.2 Communication protocols and OSI layer

The OSI – Open System Interconnection [26], [27] conceptual model is used in order to better understand communications technologies and where different solutions and protocols are implemented. This model defines seven abstract layers in order to facilitate interoperability of diverse communication systems with standard protocols. The method to enable protocol interoperability and consistency is protocol encapsulation outlined in Figure 2-1. The method ensures logical separation between layers since every layer is independent. The result is a modular approach where protocols can be replaced without impacting on one another. OSI layers are: Application, Presentation, Data Flow, Transmission, Path Control, Data link and Physical.

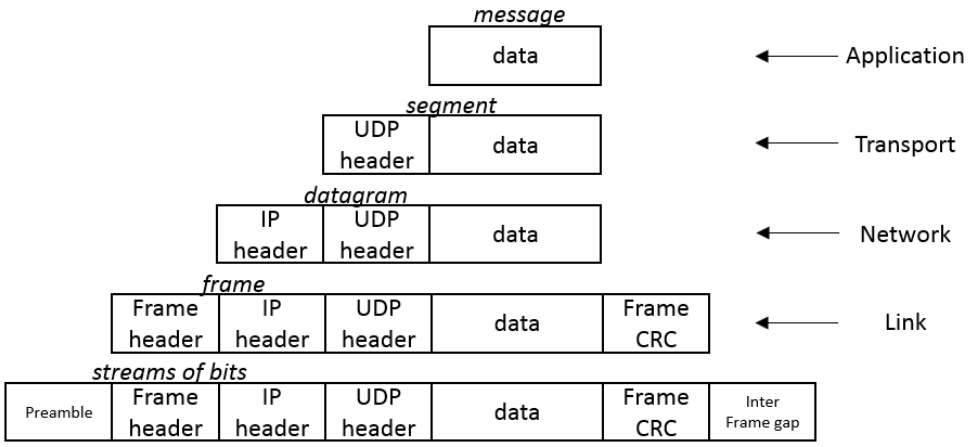


Figure 2-1 Protocol encapsulation method for application data sent over UDP and Ethernet.

According to [26], "The Physical Layer provides the mechanical, electrical, functional and procedural means to activate, maintain, and de-activate physical-connections for bit transmission between data-link-entities." It is responsible for defining encoding, layout, impedance, wireless frequency etc. This layer will encode digital symbols into a signal required for the carrying medium (optical, radio, electrical).

According to [26], "The Data Link Layer provides functional and procedural means for connectionless-mode among network-entities, and for connection-mode for the establishment, maintenance, and release data-link-connections among network-entities and for the transfer of data-link-service-data-units." The data link layer encompasses a protocol to control access to the medium and detect errors which may occur during transmission through the physical medium. Data are exchanged in frames.

According to [26], "The Network Layer provides the means to establish, maintain, and terminate network-connections between open systems containing communicating application-entities and the functional and procedural means to exchange network-service-data-units between transport-entities over network-connections". The network layer, through methods of addressing, routing and traffic control, successfully exchanges data units over network connections between communicating nodes.

According to [26], "The transport-service provides transparent transfer of data between session-entities and relieves them from any concern with the detailed way in which reliable and cost-effective transfer of data is achieved." The transport layer provides a means for reliable and effective data transfer. Some of the activities of this layer may include segmenting data into packets small enough to be transported across the network layer.

The session layer, presentation layer and application layer are often grouped together and collectively named the application layer. It defines application interactions with the underlying protocols and how data are transferred.

Figure 2-2 shows commonly used protocols in healthcare and IoT in the appropriate OSI layer. The proliferation of protocols in use can be seen on the Link/Physical layer, shown in Figure 2-2. This can be correlated with three factors: number of constraints per layer, relative resource cost of operation for that layer and suitability of standards in use.

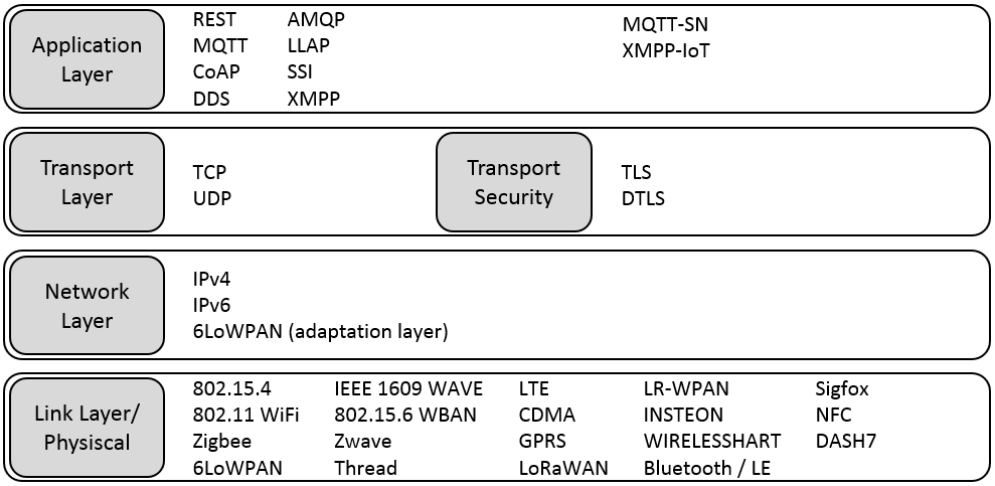


Figure 2-2 Protocols across OSI layers [28].

In addition to the protocols listed above, a comprehensive list of protocols used in IoT together with specific protocol placement on the OSI layer model is shown in Figure 2-3.

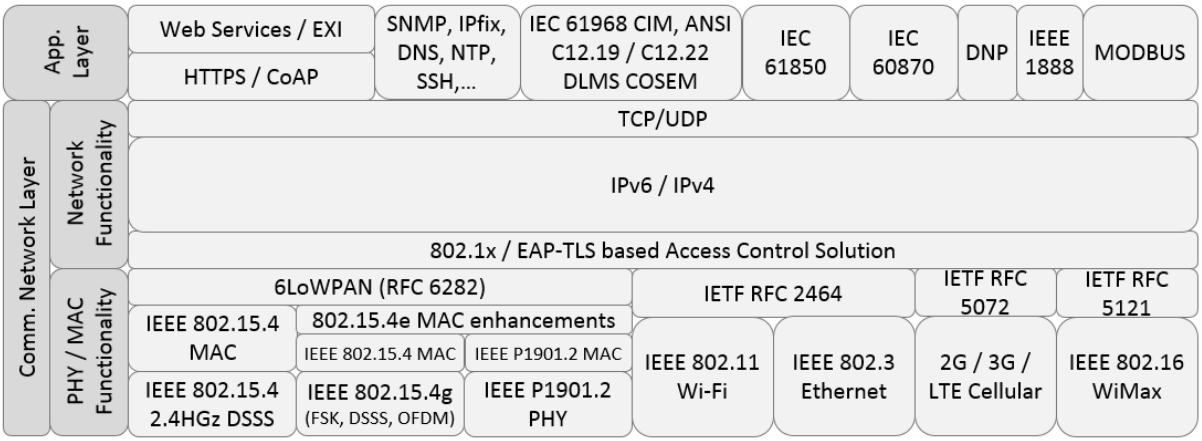


Figure 2-3 Protocols used in IoT [29].

2.1.3 Packet error detection

In order to provide reliable communication, a communication protocol needs to be able to detect errors in the communication path. Detection is achieved by appending an error detection code to the original packet. A longer linear arithmetic error detection code provides better probability of detecting the error at the extra expense of larger overhead. More elaborate coding can offer the same error detection probability as longer code, but with usage of shorter code, resulting in small packet data overhead. This elaborate coding error detection performance comes at the expense of higher computational cost. Therefore, it is crucial to find the balance between error code length or computational efficiency and the required probability of error detection. Performance of common error detection such as first complement, second complement, XOR and Cyclic Redundancy Check (CRC) was analysed by Maxino [30] and results wherefrom are shown in Figure 2-4.

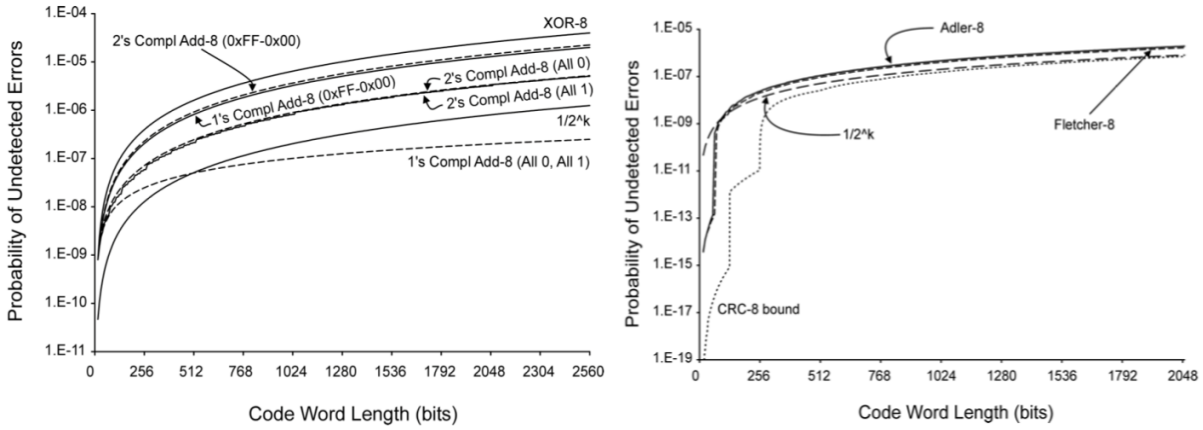


Figure 2-4 Error detection performances of various error detection codes for data and random independent bit errors (BER of 10−5) (from [30]).

It is worth highlighting that each of the Link, Network and Transport layers have their own error detection checksum. On the Link layer CRC error detection is calculated across the whole frame. For the Internet Protocol (IP) and the User Datagram Protocol (UDP) only the sum of words in their header is used in the checksum calculations. Link layer ensures integrity of the whole frame and its constituent data including IP and UDP headers. These encapsulations of layers and headers minimise processor consumption. For example, for IP header, the checksum calculation is carried out on a very small number of header bytes instead of a calculation on the entire larger payload. Optimisation to save processor resources comes at the expense of increasing the overall packet overhead. Additionally, concatenating headers from various layers can result in a header that is several times larger than the payload.

2.1.4 Protocol overhead and efficiency

Protocol encapsulation used in communication protocols enables the ability to interchange seamlessly individual layers in the OSI model. Every layer contains all the data needed for that layer, which reduces the computation requirements when assembling or disassembling the packets. A negative effect of this approach is that increased overhead packet transmitted through the communication medium contains multiple headers and checksums from all layers. This was a motivation for extensive optimisation research work [31] and numerous publications. An example can be found in the 6LoWPAN protocol, which was created with the goal of extending IP support to low-power wireless sensor networks with minimal interventions on the IP headers. The standard for 6LoWPAN header optimisation was developed by the Internet Engineering Task Force (IETF) [32]. 6LoWPAN uses IEEE 802.15.4 as the data link layer protocol. In a worst-case scenario, out of a maximum frame size of 127 bytes in IEEE 802.15.4, only 33 bytes are the useful payload making the overhead 248 % of the data payload as shown in Figure 2-5. For the IEEE 802.15.4 packet header 46 bytes are used and for the IPv6/UDP header 48 bytes are used in the worst-case scenario. Looking in greater detail at the IEEE 802.15.4 header we can see that 12 bytes are used only for the definition of the source and destination link layer MAC address.

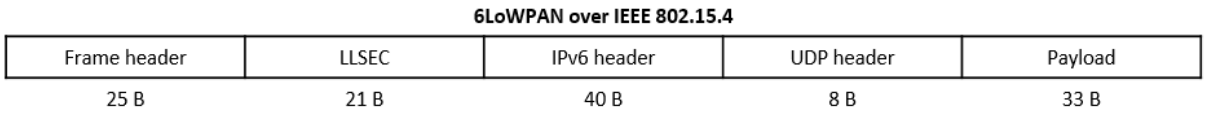


Figure 2-5 Packet overhead in worst case scenario for 6LoWPAN over IEEE802.15.4.

Optimisation of the large header size is addressed in the compression format RFC6282 [33]. Optimisation is provided for Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMP). Optimisation methods will reduce the header size when common attributes are used, and source and destination addresses can be deducted from the link-layer. Three optimisation examples are shown in Figure 2-6. It is possible to see that compression will be achievable only under specific scenarios. Compression will be possible to be achieved when the source or destination address is possible to be derived from the Link layer. The gateway node interconnects the IEEE 802.15.4 protocol with the IP protocol. If a network address translation approach is used, which exchanges longer MAC address in the connection stage, it would be possible to reduce the overhead for a short local network address [34].

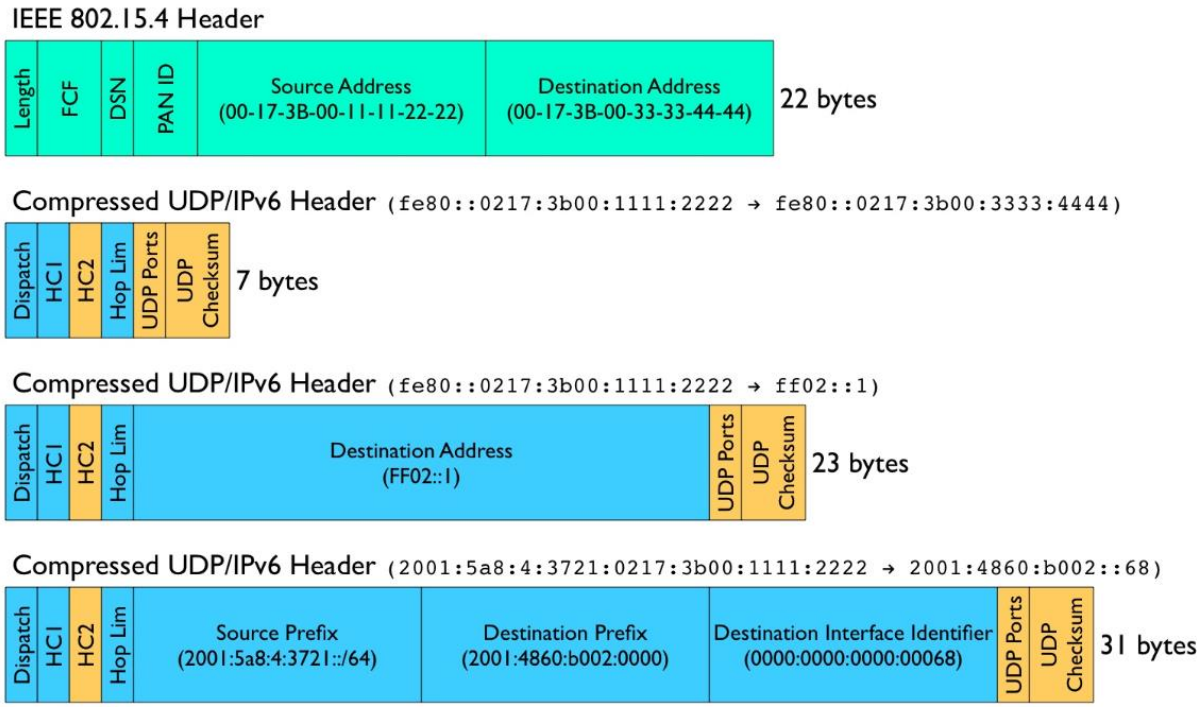


Figure 2-6 6LoWPAN header compression examples (from [33]).

In the case of BLE, after a connection is established and when the data channel is used, the initial Maximum Transfer Unit (MTU) is 27 bytes [35]. Total payload data is only 20 bytes and the total network and link protocol minimal overhead, as shown in Figure 2-7, is 19 bytes resulting in an overhead of 47%. As a result, substantial overhead support for larger MTU was added in BLE 4.2 If both connected devices support higher MTU, they can request to change MTU to up to 251 bytes. In the case where a smaller amount of data is transmitted, the protocol overhead is several times the size of the payload thus reducing the overall efficiency of the protocol. A BLE connection packet contains an access address after the initial preamble. This address is used in the receiver as a sync word which signals the start of the packet assembly. Connection packets use a link unique access address to interact and wake up the processor core only when packets sent to the node are received. This method contributes to the overall energy efficiency. In the BLE broadcast packet, all broadcasting devices use the same access address. To prevent excess power consumption caused by waking up the main CPU core on receipt of every broadcasting packet, it is important to have hardware support to also filter incoming packets at the device address.

<table>
<tr><th>Preamble</th><th>Access Address</th><th colspan="6">PDU (2 -257)</th><th>CRC</th></tr>
<tr><td rowspan="4">1 byte
(1M PHY)

2 bytes
(2M PHY)</td><td rowspan="4">4 bytes</td><td>LL Header</td><td colspan="4">Payload (0-251 bytes)</td><td rowspan="2">MIC (Optional)</td><td rowspan="4">3 bytes</td></tr>
<tr><td rowspan="3">2 bytes</td><td>L2CAP Header</td><td colspan="3">ATT Data (0-247 bytes)</td></tr>
<tr><td rowspan="3">4 bytes</td><td colspan="2">ATT Header</td><td>ATT Payload</td><td rowspan="3">4 bytes</td></tr>
<tr><td>Op Code</td><td>Attr. handle</td><td rowspan="2">Up to 244 bytes</td></tr>
<tr><td>1 byte</td><td>2 bytes</td></tr>
</table>

Figure 2-7 BLE connection data packet structure [36].

2.1.5 Limitations of existing protocols

LoRa [37] and Sigfox [38] protocols operate in a sub-gigahertz band and they can have an operating range from a few kilometres in urban areas to several tens of kilometres in suburban areas. A long operation range comes at the expense of limited communication speed. Further limitations are placed by operators by limiting data upload. In the case of Sigfox, the upload is limited up to 12 bytes per upload, and to 140 bytes daily, which is impractical for wearable and IoT use cases.

Although it may seem that there are a great number of available protocols to choose from, as shown in Figure 2-2, many of them use the same Link layer protocol. ZigBee, Thread and 6LoWPAN all are based on the IEEE 802.15.4 link layer protocol, which has limited capability to adapt to changes in traffic.

Bluetooth Low Energy was created as a state transmission protocol capable of long operation from a single CR2032 battery. However, this is possible only if the transmission rate is kept low. BLE's Medium Access Control (MAC) operates in Frequency Division Multiple Access (FDMA) and Time Division Multiple Access (TDMA).

For both IEEE 802.15.4 and Bluetooth, the frame rate is constant. This results in a constant latency which data will experience before they are transmitted. When a surge of data occurs and arrives in the transmitting buffer, the two protocols can transmit additional data only by extending transmission until the end of the frame. Applications such as motion tracking, which display to the user motion captured from the sensor on the user's body, require low latency for transmission of real time data. Higher latency would create jittering and delays between user's movement and movement shown on the screen. These types of applications will set higher frame rates during the connection stage. A higher frame rate will result in higher minimal consumption, shortening the interval between which the device needs to be charged. Should the developer select a lower frame rate with higher latency, it will have a lower minimal power consumption, although some applications which require lower latencies will not be supported. There is a need to implement a wireless protocol with adaptive frame rate capable

of delivering low power consumption when the wearable device is in the transmitting state and low latency when there are real-time data waiting to be transmitted. Researchers have concluded that variable rate transmission optimisation is more efficient than variable transmission power optimisation [39].

According to [40-46], the user would receive one set of devices to be used for both long-term monitoring and real-time data streaming. In real-time streaming of motion captured data, a protocol needed to provide low latency transmission in order to support functionalities like assisted exercise [40-46] to the user should be used.

A review of wireless low power protocols suggests that existing protocols have many more aspects in which they may be optimised [47-51].

2.2 Energy efficiency of a wireless sensor network

To achieve energy efficiency in a wireless sensor network, all building components of the wireless communication network must be optimised. A single non–optimised component can downgrade the overall energy efficiency. This section will explore critical components and methods to improve overall energy efficiency.

2.2.1 Energy consumption and saving mechanisms

A wireless sensor network is a collection of devices which needs to achieve delivery of data from data source network endpoint nodes to predefined data sink nodes using predefined actions and methods. Some of these methods handle radio modulation/demodulation, medium access control, routing protocol, baseband radio and battery management. In order to achieve appropriate energy optimisation, categories of energy consumption in wireless sensor networks must first be defined.

Various authors define consumption elements and optimisation from various aspects related to their research. Some authors define consumption elements related to the MAC protocol [52] while other authors approach this from a routing protocol perspective [53].

A comprehensive and more encompassing definition of the approach of energy consumption elements/constituents is offered by Najmeh [54] and Kamyabpour et al. [55] where they present an Energy Defined Architecture (EDA), as shown in Figure 2-8. The total consumption of a node is the sum of all consumption constituents. EDA groups power consumption into five categories: individual, local, global, sink and environment, as shown in Figure 2-8.

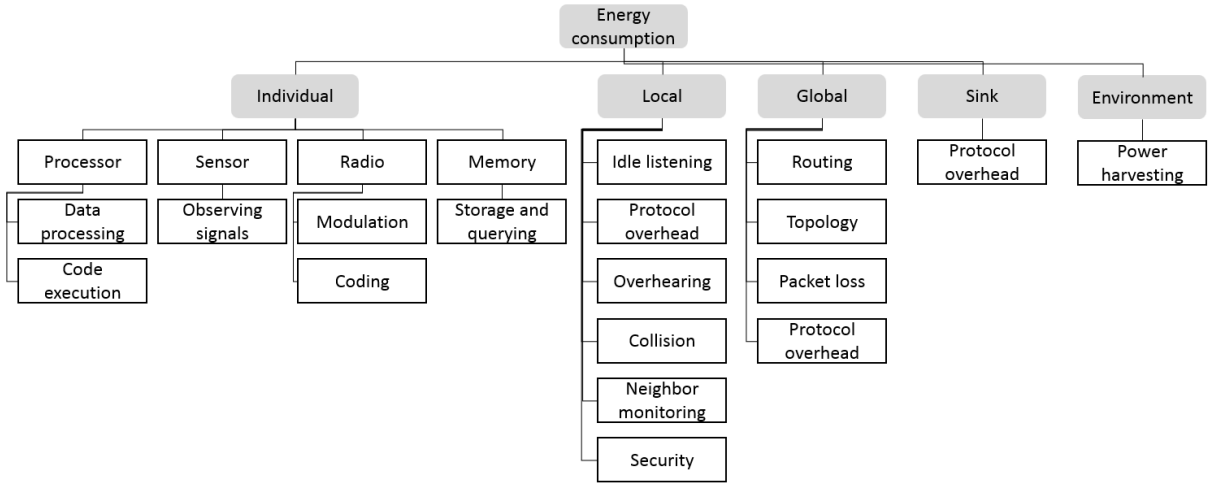


Figure 2-8 Energy consuming constituents [54].

Although the proposed EDA summarises well the individual consumption contributors, segregation of individual consumption could obscure cross-constituent opportunities for energy optimisation. Communication protocols can directly control radio, local and global energy consumption elements/constituents. Wireless communication protocol timing and computing requirements can influence either, positively or negatively, processor and memory energy consumption elements/constituents. Therefore, cross-constituent optimisation methods can complement an individual consumption constituent view and optimisation method. A well-defined classification of energy efficient mechanisms is described by Ridha et al. [56] and Tifenn [57], as shown in Figure 2-9. Five optimisation mechanisms are proposed: radio optimisation, data reduction, sleep/wakeup scheme, energy efficient routing and battery repletion. Both approaches define energy consumption constituents and classification optimisation methods but provide a biased view deriving from the authors research work. Taking a cross-section of both is necessary to provide a complete non-biased overview.

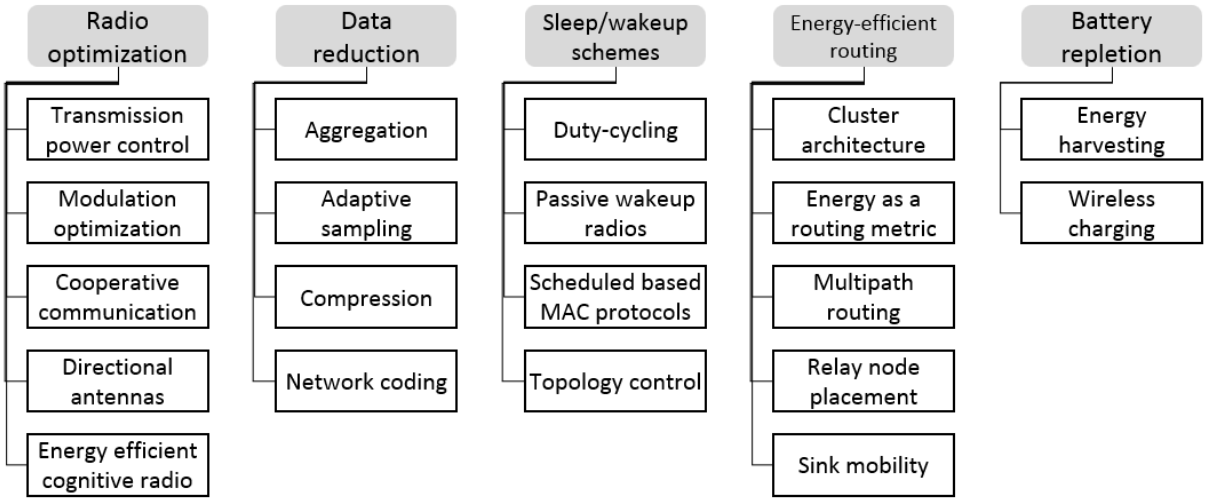


Figure 2-9 Classification of energy-efficient mechanisms [56].

2.2.2 Processor consumption

An individual consumption category encompasses elements and parameters related to the sensor node itself such as consumption arising from the processor, sensors, radio and memory. At the processor level available optimisation components are state (idle, sleep, deep sleep), frequency and voltage.

Wireless protocol requirements can influence the ability to change the state, e.g. switching power on and off, of various System on Chip (SoC)/discrete subcomponents. A wireless protocol uses shared subcomponents such as a high frequency clock or timers. Careful design of the protocol to minimise sharing of the subcomponents could also result in minimising power consumption. A shared resource is able to enter power off mode only if all related subcomponents do not need the resource output. For example, MAC could group requirements for the high frequency clock only during active communication. This can result in a higher chance that both processor and radio do not require the high frequency clock at the same time and allow the device to power off the high frequency clock and save power. This entanglement between user code, wireless protocol and subcomponents may indicate to developers to separate nodes' critical actions running on the internal clock and intermittent activity such as sampling, processing etc.

The ability to change the processor or main clock, the bus frequency and voltage is determined by the architecture of the system on the chip used. Comparing, for example, microcontrollers nRF51822 [58] and ATmega168 [59], the difference in internal architecture presents different power consumption models. nRF51822 power consumption $P_{nRF51822}$ (excluding other peripherals and subcomponents) is

$$P_{nRF51822} = 810\ \mu A\ +\ f_{CLK}[\mathrm{MHz}] \cdot 275\ \mu A/\mathrm{MHz} \quad (2\text{-}1)$$

where f_{CLK} processor clock frequency in MHz. Power consumption is dominated by a static current of 810 µA for powering the 16 MHz clock and a dynamic current of 275 µA multiplied by the MHz f_{CLK} processor clock frequency. The internal architecture of ATmega168 results in an almost linear relation between power consumption ($P_{ATmega168}$) and processor clock frequency f_{CLK}

$$P_{ATmega168} = 100\ \mu A\ +\ f_{CLK}[\mathrm{MHz}] \cdot 400\ \mu A/\mathrm{MHz} \quad (2\text{-}2)$$

as the static clock drive and distribution current is 4 times smaller than the processor current. Figure 2-10 clearly shows how nRF51822 has a larger power consumption of 1.1 mA at low MHz clock frequency compared to ATmega168 with the consumption of 0.5 mA. This suggests that lowering the clock frequency of nRF51822 can reduce power consumption but not as effectively as in case of ATmega168. For nRF51822 the priority is to enter into a sleep state as soon as possible. Figure 2-11 further outlines power consumption normalised to 1 million processor operations, highlighting that nRF51822 should always operate at the highest clock speed possible when executing code.

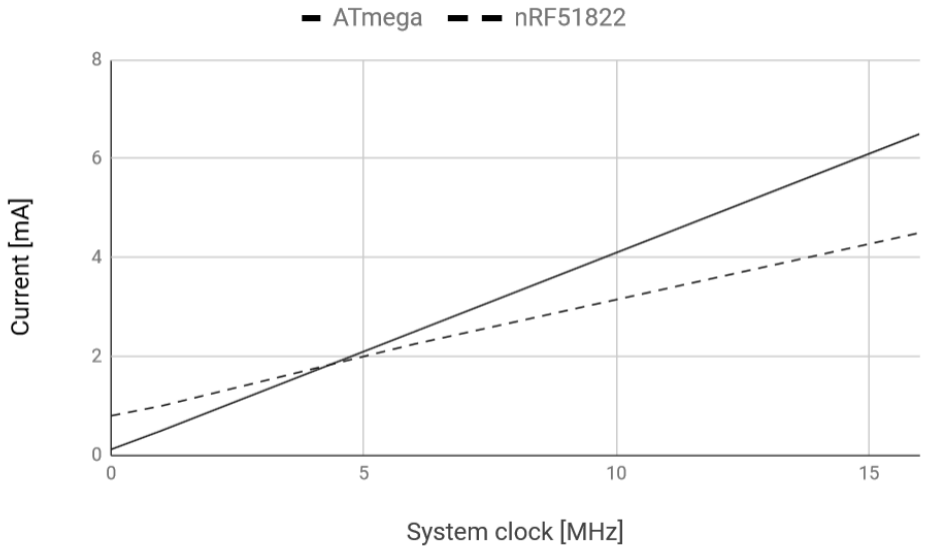


Figure 2-10 Relation between processor current consumption and clock frequency.

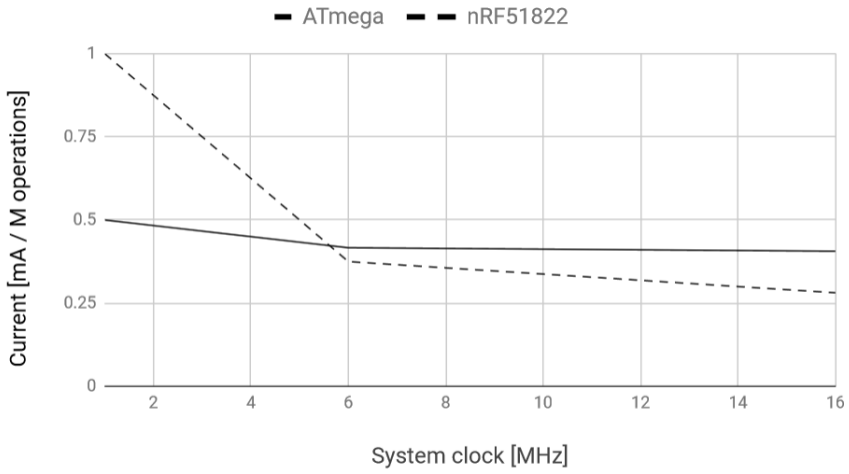


Figure 2-11 Relation between current consumption for 1 million processor operations and clock frequency.

When optimising the design of protocols to be used in wireless sensor networks, it is not possible to control underlying hardware and internal components. Nevertheless, an optimised protocol needs to be designed with an understanding of common underlying hardware limitations and provide best practices to facilitate underlying hardware to use power saving techniques.

2.2.3 Radio modulation and coding consumption

This research will not consider the efficiency of all different modulation schemes and their power efficiency, but rather will analyse the impact of modulation on an existing system on chip (SoC), nRF51422, operating in the radio spectrum range of 2.400 GHz to 2.4835 GHz using Gaussian Frequency Shift Keying (GFSK) modulation.

Communication using 2.4 GHz offers the advantages of small footprint antenna due to short wavelength and the availability of high data rates. This can result in making communication more energy efficient, but it is also susceptible to higher signal propagation losses compared to a lower frequency spectrum. Free-space path loss is calculated as

$$FSPL[\text{dB}] = 20\log_{10}(d) + 20\log_{10}(f_{carrier}) + 20\log_{10}\left(\frac{4\pi}{\text{c}}\right) \quad (2\text{-}3)$$

where d is the distance of the receiver from the transmitter, $f_{carrier}$ is the carrier frequency used and c is the speed of light. The higher the frequency $f_{carrier}$, the higher the free-space path loss is. From Figure 2-12 the exponential nature of the free-space path loss, reaching 70 dB in just 30 meters (both antennas are isotropic antennas any losses, reflection, noise or

obstacles existing in the environment are ignored), may be observed. In addition to the free-space path loss, higher frequencies are also more susceptible to signal attenuation in travelling through different materials. There are extensive reports on propagation losses in the 2.4 GHz radio spectrum [60][61][62]. In the indoor environment the human body can introduce an additional shadowing body effect which can contribute to signal attenuation losses [63] and the usable range is greatly affected by the type of the antenna used [62].

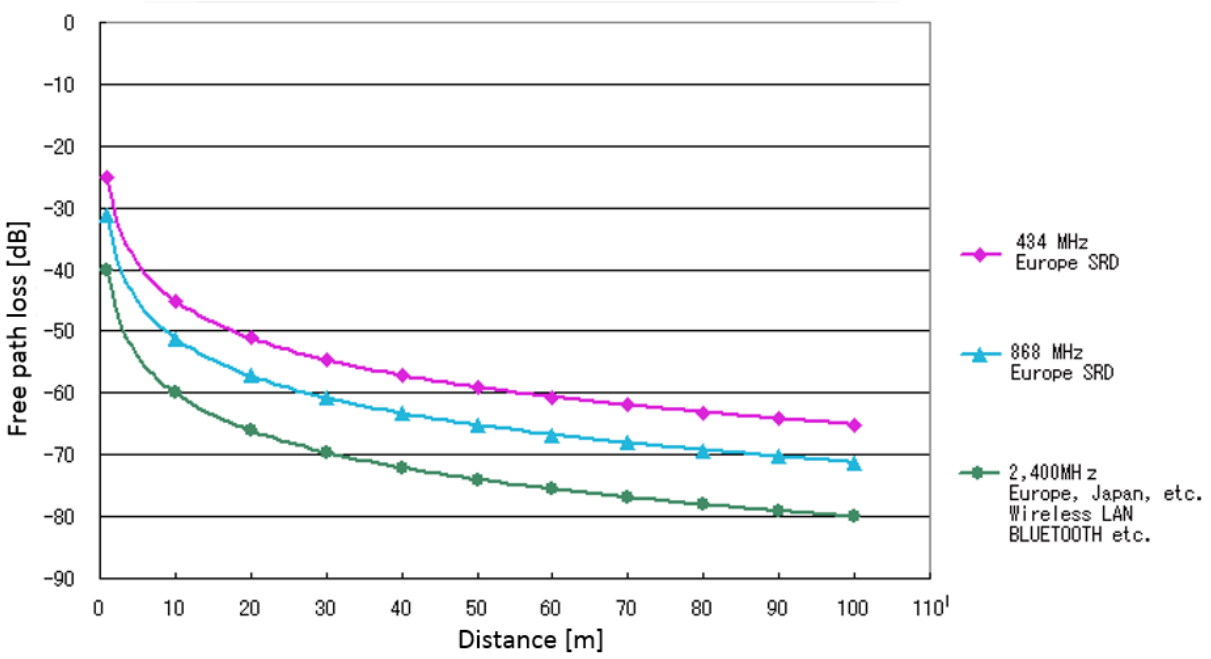


Figure 2-12 Free-space path loss for 2.4 GHz radio spectrum (from [46]).

Summing all signal gains and losses from the transmitter through a medium until reaching the receiver defines the link budget as:

$$Received\ power[\text{dB}] = Transmitted\ power[\text{dB}] + Gains[\text{dB}] - Losses[\text{dB}] \qquad (2\text{-}4)$$

Gains could come from transmitter and/or receiver directional antenna gain. Losses could arise from anisotropic antenna radiation, signal path loss and transmitter/receiver losses. The received power must be greater than the selected receiving sensitivity which offers acceptable bit error rates (BER).

The integrated SoC nRF51822 and integrated radio transceiver offer three data rates using two over the air modulations: 2 Mbit/s using 2 M symbols/s modulation, 1 Mbit/s using 1 M symbols/s and 250 kbit/s using 1 M symbols/s with encoding one bit in four symbols. The declared radio sensitivity (0.1% BER) of nRF51822 using 2 Mbit/s over the air encoding is -85 dBm. The transmission current does not change if a different data rate is selected. Radio

receiving current variation between the highest and lowest data rate is 12%. From the energy consumption perspective, the ideal scenario would be to always transmit data using the highest possible data rate that the radio can offer. The cost in energy per bit transmitted for nRF51822 using 0.25 Mbit/s is 7.5 times higher than using 2 Mbit/s, at the expense of 11 dBm lower receiver sensitivity than using 0.25 Mbit/s. This reduces the operational range in which two nodes can establish a reliable connection.

In cases where there is a need to extended the range of what an energy efficient 2 Mbit/s radio link can achieve, e.g. due to increased losses in the signal path or to increased distance between two operational devices, three options are available: to increase transmitted power, to increase radio receiver sensitivity or to focus the transmitting/receiving radio beam using a directional antenna. Power output can be increased to an integrated component operational maximum. Beyond that, external power amplifiers must be added which increase the device size and bring additional cost. Using directional antennas without Multiple Input Multiple Output (MIMO) would result in the radio beam changing direction as the node moves. This points to the conclusion that without changing the physical aspects of the node, only a change of sensitivity and increasing the transmitting power (to integrated circuit operational maximum) are available as options.

In the case of nRF24L01/nRF51822, receiver sensitivity may be increased by reducing the data rate to 1 Mbit/s or 0.25 Mbit/s. This effectively reduces the required link budget and increases the achievable communication range. Alternatively, or in a conjunction, the transmitting output power can be increased by up to 4 dBm. As the transmitted power increases, BER decreases and more packets are successfully transmitted. An interesting analysis and empirical measurement to determine the cost to successfully transmit a byte was carried out by Xenofon et al. [64]. Transmitted power was changed, and numbers of successfully and un-successfully transmitted packets where recorded. The resulting curves in Figure 2-13 outline an almost constant energy cost when BER is small as the chances of not receiving a packet are very small. As the receiving signal strength index (RSSI) decreases, BER increases and retransmission of packets increases the overall energy per correct transmitted byte cost. Although the graph shows that there is a range of almost 6 dB where the packet will be transmitted at increased cost, high retransmit numbers would result in impractically long latency.

Even with an additional link budget gain using the described methods, in some scenarios this may not be enough to cover all rooms in a house [65].

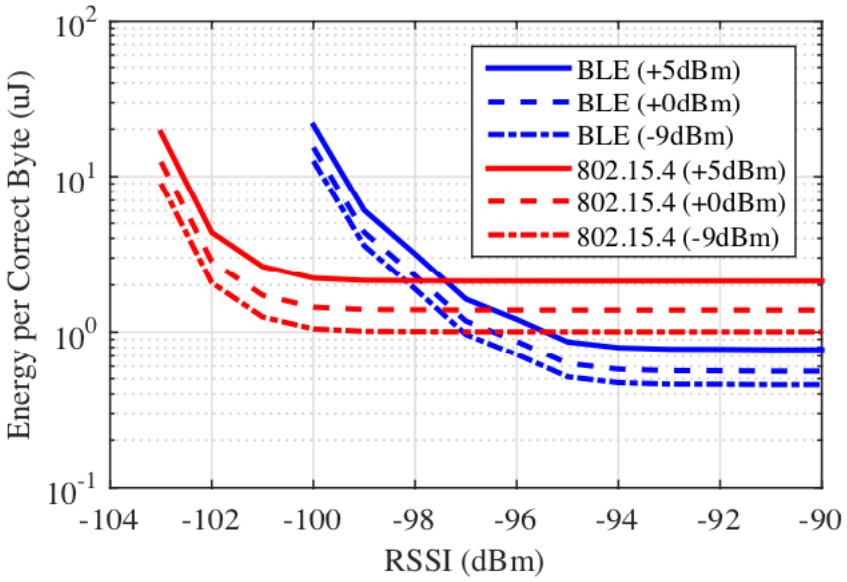


Figure 2-13 Energy cost to transmit correct byte depends on RSSI and transmitted power (from [64]).

2.2.4 Medium Access Control and energy efficiency optimisation

An optimisation method for MAC can be based on using a variant of TDMA, FDMA, Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) algorithm or wake-up radio (WuR).

A wake-up radio requires additional space on the printed circuit board which is not suitable for healthcare devices where minimised device size is desired to provide better comfort to the user/patient. Additionally, a wake-up radio band could have different propagation attenuation. This can result in waking the device by the wake-up call received on a low attenuation path, with the main radio still out of reach, or vice versa. A review (Rajeev et al [66]) of 75 wake-up radio prototypes concluded with the statement, "Keeping a dual radio mechanism using separate components is expensive for IoT device production. This also includes the RF front-end circuits whose WuR performance mostly depends on the chip design." An additional increase in the cost of the device is noted, "With the inclusion of WuR, the overall cost is expected to rise and can become one of the hurdles of this method. Further, the cost of designing ultra-low power WuR is still challenging. Current WuR have a shorter communication range than the traditional radios, making it difficult to align coverage of these two radios." Taking the availability of a system on a chip with wake-up radio into consideration,

the previously stated challenges and the nature of healthcare data exchange as a long predictable connection, a wake-up radio is not currently seen as a suitable method for energy efficient and cost-effective solutions.

The second method researched in the optimisation of MAC is Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA). An advantage of a wireless protocol using CSMA-CA can be found in possible lower latency in the network and the lack of a need for a scheduling beacon to be transmitted. However, a wireless protocol using this MAC must listen if the radio medium is free before transmission (ZigBee beaconless configuration). Radio listening consumes a substantial amount of energy, lowering the throughput and adding delays. In a network configuration where two peripheral nodes are on the opposite edges of the network and at a distance of 2/3 of the maximal communication range from a concentrator node between them, collision will still occur. The two nodes are distanced more than the maximum communication range, therefore they will both detect that the medium is free and start to communicate at the same time. Signals from both nodes will collide with equal strength at the concentrator node. To overcome these limitations, protocols like ZigBee use a hybrid method where they first broadcast a scheduling beacon defining a TDMA slot (ZigBee contention access period - CAP) followed by a CSMA-CA slot (ZigBee contention-free period - CFP). This allows having a minimum guaranteed bandwidth (ZigBee GTS) and an on-demand broadcasting spike of pending data without the need for waiting for additional beacon slots.

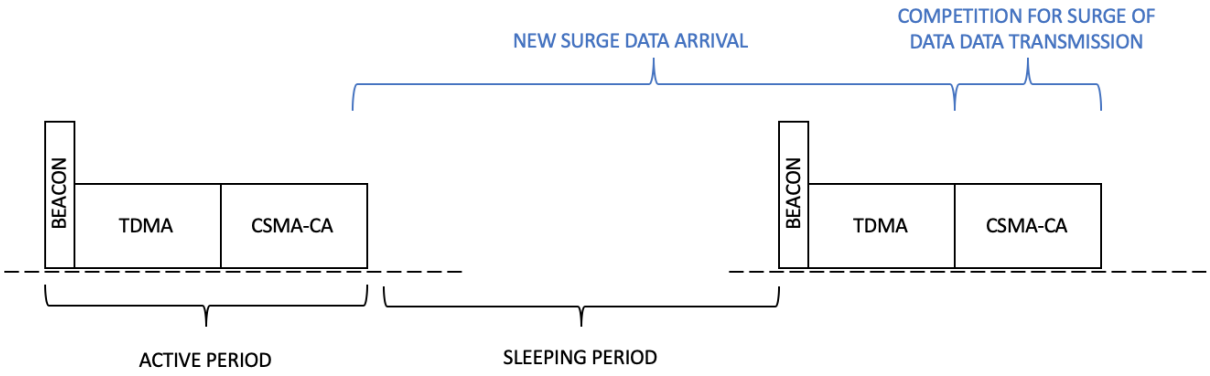


Figure 2-14 Waiting interval from new data generation until possible additional bandwidth transmission.

The worst-case scenario arises when a surge of data arrives after the CSMA-CA slot shown in Figure 2-14. In this scenario waiting time will be for the entire duration of the radio sleeping period. Effective data transmission latency $t_{latency}$ for CSMA-CA MAC will be

$$t_{CSMA-CA\ latency} \in [0\ ,\ t_{frame}\ ] \tag{2-5}$$

where t_{frame} is frame duration. Zero latency will occur if data arrive just before the start of transmission, and t_{frame} could occur if data arrive just as the packet is starting to be transmitted. Therefore, the ability to transmit a spike of newly arrived data is limited and available only until the end of the CFP slot. This approach introduces complexity in the protocol and results in higher power consumption compared to a TDMA protocol like BLE [67] in cycling applications and overall greater consumption in constant data transmission [64].

One of the reasons for ZigBee's increased power consumption compared to BLE comes from the radio requirement to listen and compete for a slot in a frame in superframe contention-free periods (CFP). Should a surge of data occur, the ZigBee node can compete in CFP and to try to send additional packets of data in the same frame. Since healthcare use cases are strongly influenced by generation of data in regular intervals, and in predictable quantities such as in the use case of ECG monitoring or heart rate value transmission, it is possible to add one additional frame of latency and remove the CSMA-CA period. Use of only TMDA will improve energy efficiency and overall throughput of data as shown in Figure 2-15.

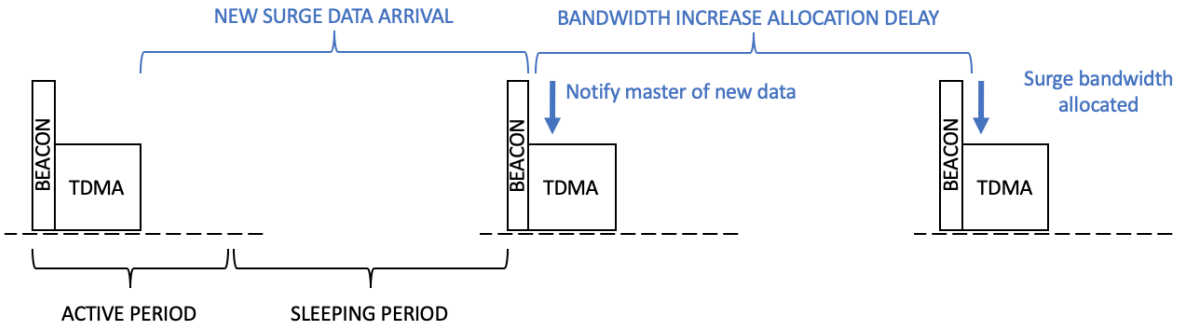


Figure 2-15 Time required to increase node's bandwidth allocation on surge of data.

The energy efficiency of TDMA/FDMA is higher than CSMA-CA as with TDMA/FDMA, radio is only active when it receives or transmits data. A drawback of this MAC method is the pulse response latency increase on a surge of data. The data transmission latency $t_{TDMA\ latency}$ is

$$t_{TDMA\ latency} \in [t_{frame}\ ,\ 2\ t_{frame}\ ] \tag{2-6}$$

where t_{frame} is the frame period. Single frame data transmission latency is present when data arrives from the end of a sleep period to start of communication with the master node. Dual frame latency is present when the data arrives straight after communication with the master.

In a wireless network a master node usually communicates with multiple slave nodes. Therefore, synchronisation between master and multiple slaves must exist. Two methods of synchronisation with slave nodes can be adopted; beacon and beaconless.

In a beaconless mode (not CSMA-CA) slaves are not aware of their neighbours as the scheduling is done on a communication channel shared only between the master and a single slave node. In this scenario the master assigns individual time synchronisation points for every slave node that is connected. A similar approach can be observed in BLE when a single master node connects to multiple slave nodes, as shown in Figure 2-16.

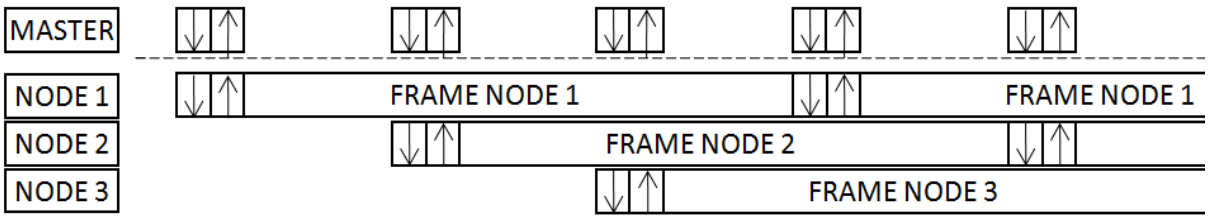


Figure 2-16 Beaconless frame allocation when the master is connected to multiple slave nodes.

As may be observed in Figure 2-16, the master can align the start of individual communication channel frames (connection interval), with a sufficient time between them to ensure the ability to execute one bidirectional communication and prevent reaching connection timeout. Additional bidirectional communication slots can be added until the start of the subsequent channel frame without impacting other nodes. For the case when NODE 1 requires additional bandwidth, the master could intermittently skip communication with NODE 2 to allow NODE 1 to transit all of the necessary data, overlapping with the frame start of NODE 2. The impact on NODE 2 is increased latency and power consumption, as the node is turning on the radio and listening for a packet expected from the master. The packet is not coming since the master is communicating with NODE 1. This points to the conclusion that this approach is optimal when nodes are transmitting small amounts of data, with a node bandwidth B_{node} smaller than

$$B_{node} \leq B_{channel} \,/\, N_{connected\ nodes} \tag{2-7}$$

where $B_{channel}$ is channel bandwidth and $N_{connected\ nodes}$ is the total number of connected nodes to a single master. When a single slave node requires more bandwidth than the B_{node} at any given point in time, the latency and power consumption of other slave nodes will be impacted and increased. Additionally, since communication with slave nodes is distributed over

time, this could prevent the master node from entering deep sleep mode and only halt the processor core, resulting in increased power consumption for the master. Therefore, managing connections with a large numbers of slave nodes is not suitable using this method.

Improvements of the beaconless approach to minimise the master's energy consumption could be carried out by keeping single frame time synchronisation for all slave nodes and grouping allocated slots at the beginning of the frame, as shown in Figure 2-17. As the slots are grouped at the beginning of the frame, it is more likely that the master node will be able to enter deep sleep mode. Limitations of this optimisation arise from the fact that the master needs to communicate in advance with the slave node to determine where in the frame is the next allocation. This introduces additional latency on a data surge. In addition, fragmentation of individual slave's slots allocation could result in the inability to enter deep sleep or the ability to combine multiple slots to use a longer and more efficient packet length. As the packets could be lost, the master must keep both current and future slots empty for a single slave node as, until the next successful communication, it cannot be sure if the slot received the data.

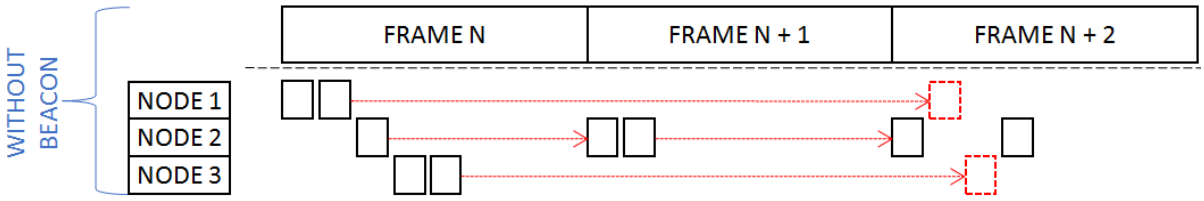


Figure 2-17 Improved beaconless frame allocation communication of master slave nodes.

In a TDMA MAC using beacon frame allocation, the master transmits an allocation packet to all nodes at the start of the frame, as given in Figure 2-18. The allocation packet holds data regarding individual slot allocations for individual connected nodes. It provides efficient grouping of individual slave nodes at the beginning of the frame. This ensures the ability of the master node to enter deep sleep when a fraction of the total channel bandwidth is used, which minimises the master's node power consumption. Additional grouping of all slots allocated to an individual slave node ensures the ability of the slave node to enter deep sleep mode in a continuous block, minimising power consumption. The master node can distribute channel bandwidth as per individual slave node's needs. Contrary to beaconless frame allocation, a surge of data from one slave node does not negatively impact latency and power consumption of other slave nodes.

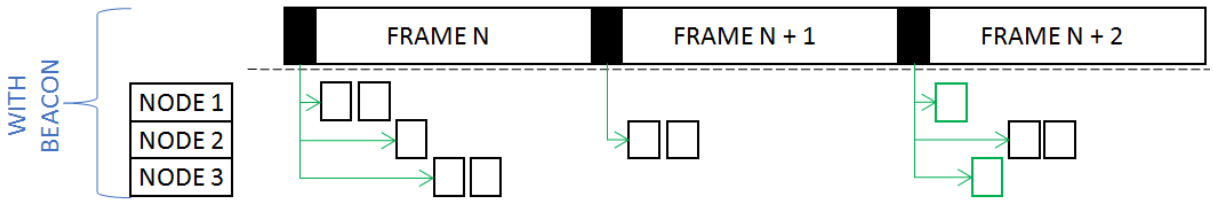


Figure 2-18 Master's beacon frame allocation of slots.

Frame allocation using a beacon introduces constant allocation packet overhead resulting in increased baseline power consumption and, as mentioned above, while the latency response to a surge of data is increased by one additional frame. Should the master node be able to promptly enter deep sleep mode or poses a greater power reserve, it is possible to remove negative additional frame latency by distributing slots across the frame, keeping free slots between allocated slots. When a surge of data occurs, master and slave node can continue data exchange as long as they have free slots available. This optimisation method is illustrated in Figure 2-19. The method combines TDMA's energy efficiency and the low latency of CSMA-CA.

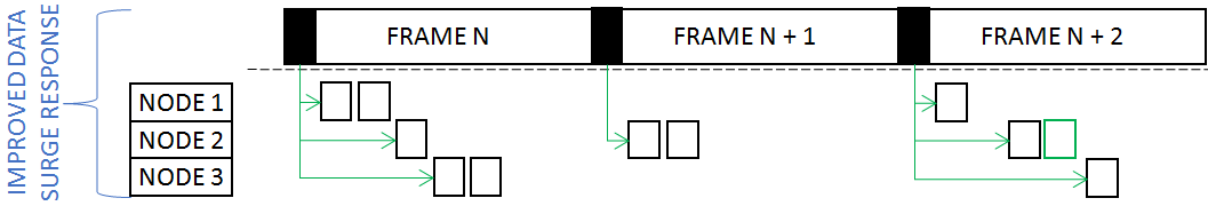


Figure 2-19 Improving data surge latency by spreading slots allocation in frame.

Table 2-2 shows a summary of MAC models. TDMA MAC models provide power efficiency without increased cost or increase in the size of the device from fitting additional components. From TDMA models, only beacon-based frame allocation MAC models are suitable for supporting a large number of connected devices and variable loads.

Table 2-2 Summary of MAC models

MAC Model	Additional Bandwidth Allocation Latency	Power efficiency	Considerations
Wake-up radio	0 [frame]	High	Additional size and cost
CSMA-CA	1 [frame]	Low	Low efficiency
TDMA (beaconless)	1 [frame]	High	Limited to small number of connected nodes
TDMA (beacon)	2 [frame]	High	Increased latency
TDMA (slot spread allocation)	1 [frame]	High	Master impact depending on deep sleep capabilities

2.2.5 TDMA communication and clock synchronisation

TDMA MAC communication is characterised by dividing of time slots for different devices to access the medium. To preserve device power, the device should keep all internal components in sleep mode for as long as possible. Only a low frequency low power oscillator (LF OSC) is always kept on, providing wake-up capabilities. A wake-up sequence powers up a high frequency oscillator (HF OSC) and turns on the processor core to execute application tasks or perform wireless communication. Therefore, the node is constantly changing state between power on and sleep.

Figure 2-20 shows the events sequence required for a successful wireless communication using nRF51422. Only internal components required for wireless communication are shown. As the low power low frequency clock (LF_CLK) tick interval is relatively large, the node needs to calculate the wake-up value of the LF_CLK to start the high frequency clock (HF_CLK) and processor before entering sleep mode. On LF_CLK the value match of master and slave events (M1, S1) interrupt is raised and HF_CLK is ramped up to allow the processing unit to prepare (M2, S2) for the incoming communication event. The precise HF_CLK will calculate the match value (M3, S3) on which an interrupt will be caused, and the radio will be powered on and ramp up until reaching a phased-locked loop lock. It is worth highlighting that an S3 event is happening before an M3 event, as the slave node must enter into a receiving state (S4) before the master starts to transmit (M4). As soon as the master has completed transmitting the packet (M5), it transits to ramp up state and enters a receiving state (M6). Similar to an S3 event happening ahead of the M3 when the master transmits the

packet, an M6 event occurs before the S7. Since the slave node, by receiving the master's packet, is now synchronised to the master's clock, it is safe to set the time gap between M6 and S7 to only a few µs.

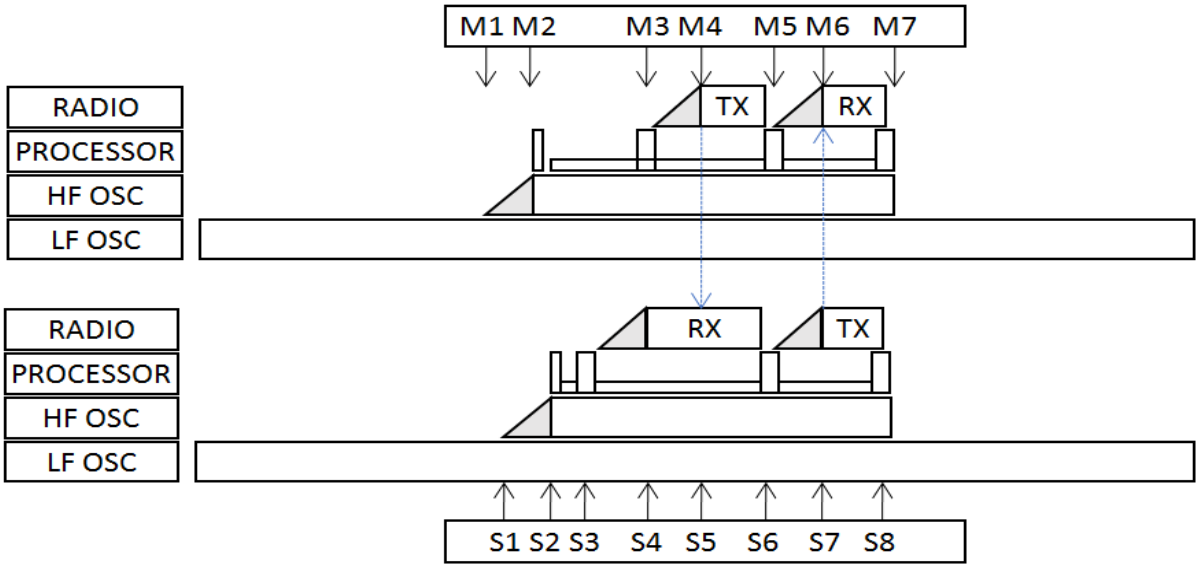


Figure 2-20 Internal events in TDMA communication.

The slave node, following the transmission of the packet (S8), calculates the next LF_CLK match value and enters deep sleep mode by disabling both the main processor and HF_OSC. On receiving the packet from the slave node (M7), the master calculates the next LF_CLK match value and enters deep sleep mode, ending a communication slot.

In conclusion, the clock synchronisation between master and slave node will determine the delay between S3/S4 and M3/M4. The greater the clock frequency error and instability, the greater the delay between S3/S4 and M3/M4 needs to be, hence resulting in increased power consumption.

To maximise power efficiency and lower power consumption, the device needs to wake up just prior to the radio activity ($t_{SLOT\ START}$) designated by the protocol. The device must wake up sufficiently in advance to be able to complete activities ($t_{SLEEP\ TO\ RADIO\ READY}$) before the protocol radio activity designated time occurs: powering on the high frequency clock ($t_{HF\ CLK\ POWER\ ON}$), powering on the processor ($t_{PROC\ POWER\ ON}$), executing code to initialise and turn on the radio module ($t_{RADIO\ INIT}$) and completing the radio clock settling time ($t_{RADIO\ SETTL.}$).

In order to achieve successful communication between two wearable nodes, the transmitting node must start the transmission slightly after the receiving node enters a reception state $t_{TX\ DELAY}$. This implies that the internal time of the two nodes must be synchronised.

Should the transmitting clock run 15 µs ahead of the receiving clock and the $t_{TX\ DELAY}$ is equal to 10 µs, the transmitting node would start transmitting 5 µs before the receiving node would enter into a receiving state. This would result in the inability of the receiving node to ever receive a valid radio packet and in a communication failure. Therefore, the clock synchronisation mechanism is an indispensable part of the communication protocol. That issue was a motivation for researching various clock synchronisation options [68].

2.2.6 Frequency error impact on wireless communication

In the previous section, TDMA communication and clock synchronisation, two nodes internal clock synchronisation is considered crucial for successful communication and it is an integral part of the wireless communication protocol. After initial internal synchronisation of the clocks, without oscillator frequency error compensation, the clock periods of the devices will diverge causing insecurity ($t_{insecurity}$) at a maximum rate of double the single oscillator frequency inaccuracy (ppm) in a worst-case scenario

$$t_{insecurity} = t_{period} \cdot 2 \text{ ppm} \tag{2-8}$$

$$t_{insecurity} = t_{frame} \cdot 2 \text{ ppm} \tag{2-9}$$

where t_{period} is period between a two packet exchange, which is equal to t_{frame} when packets are exchanged in every frame. Considering a crystal oscillator tolerance across the working temperature range of 60 ppm for a 16 MHz crystal and 500 ppm for a 32 kHz crystal, their respective worst-case time divergences are shown in Figure 2-21. For example, without a synchronisation mechanism and oscillator frequency error compensation, after 5 frames and communicating every 8th frame, the cumulative error would be 462 µs if the node uses a 16 MHz oscillator as a reference. The error increases to almost 2 ms if a 32 kHz oscillator was used as the time reference clock.

From a clock error perspective, a particularly vulnerable state impacting nodes connectivity is that of receiving successfully a packet in the first frame after the master's allocation of connectivity to the slave node. When the slave node enters into the receiving mode and responds to the master's ping, the internal clock frequencies difference/error between master and slave device is unknown. Therefore, the internal time of the master and slave will diverge in a worst-case error scenario as shown in Figure 2-21. This vulnerability will be even more accentuated when signal path loss between the master and slave is at the limit of reliable

connection resulting in a high probability bit error rate (BER). In that scenario the node needs to increase the pre- and post-listening period for each frame for $t_{insecurity}$.

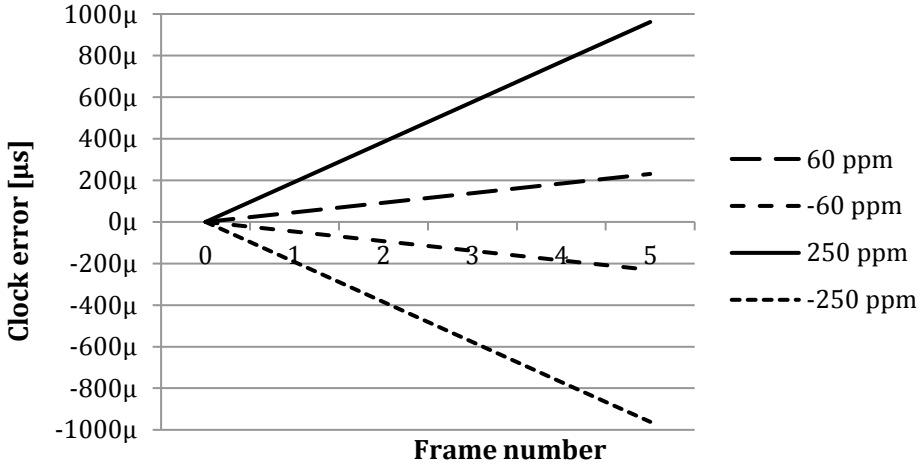


Figure 2-21 Worst case internal time divergence for two wireless nodes.

2.2.7 Crystal oscillator and clock stability

Relative clock frequency error between master node and slave node can be measured and compensated for, but another important aspect of synchronisation is how stable will this relative difference be over time. Therefore, it is worth analysing what can impact the clock source stability which is derived from crystal oscillator characteristics. As a crystal oscillator uses physical properties of the material to exercise highly selective resonance most of the impacts of the frequency stability are related to the physical aspect of the oscillator as described by Vig [69] and Filler [70]. Differences in crystal oscillator properties can be influenced by crystal cut, crystal connection method and even deposition of atoms on the crystal from contaminants present inside the crystal oscillator housing.

Three terms need to be distinguished to understand crystal oscillators as a frequency source: accuracy, precision and stability, as shown in Figure 2-22. A system that possesses the property of precision will experience small divergence between results from the mean value of all results. In system which is accurate, the mean value will be close to the value definition. Stability describes the amount of change as a function of parameters such as time, temperature, shock, and similar.

For the purpose of wireless communication and time synchronisation, a crystal oscillator does not need to be precise (inside the radio limits) as the relative clock error compensation mechanism can eliminate absolute time inaccuracy. Stability on the other hand

will define what is the shortest safe time for which a slave node needs to enter receiving mode ahead of a master node entering transmitting mode. As the error compensation mechanism constantly calculates the time difference between two communication events, only short-term influences on the clock stability can impact in determining what the minimum guard time set is. Figure 2-22 (left panel) visualises possible influencers of the crystal frequency stability. Temperature changes and power on/off cycle will not generate significant crystal resonating frequency changes between communication events as either they are happening too slowly during this short period of time, or they are not occurring at all. The other factors such as vibration, shock and orientation changes relative to the Earth's gravity are all associated with the acceleration at the crystal plane. Table 2-3 outlines acceleration levels and effects on the deviation in crystal frequency. Although Table 2-3 suggests that vibration arising due to various activities during which the wearable device would be worn will not impact clock stability, validation with empirical measurements must be carried out.

Table 2-3 Acceleration levels and effects on the deviation in crystal frequency (from [69]).

Acceleration Levels and Effects

Environment	Acceleration typical levels*, in g's	Δf x10^{-11}, for 1x10^{-9}/g oscillator
Buildings**, quiesent	0.02 rms	2
Tractor-trailer (3-80 Hz)	0.2 peak	20
Armored personnel carrier	0.5 to 3 rms	50 to 300
Ship - calm seas	0.02 to 0.1 peak	2 to 10
Ship - rough seas	0.8 peak	80
Propeller aircraft	0.3 to 5 rms	30 to 500
Helicopter	0.1 to 7 rms	10 to 700
Jet aircraft	0.02 to 2 rms	2 to 200
Missile - boost phase	15 peak	1,500
Railroads	0.1 to 1 peak	10 to 100

* Levels at the oscillator depend on how and where the oscillator is mounted
Platform resonances can greatly amplify the acceleration levels.
** Building vibrations can have significant effects on noise measurements

4-65

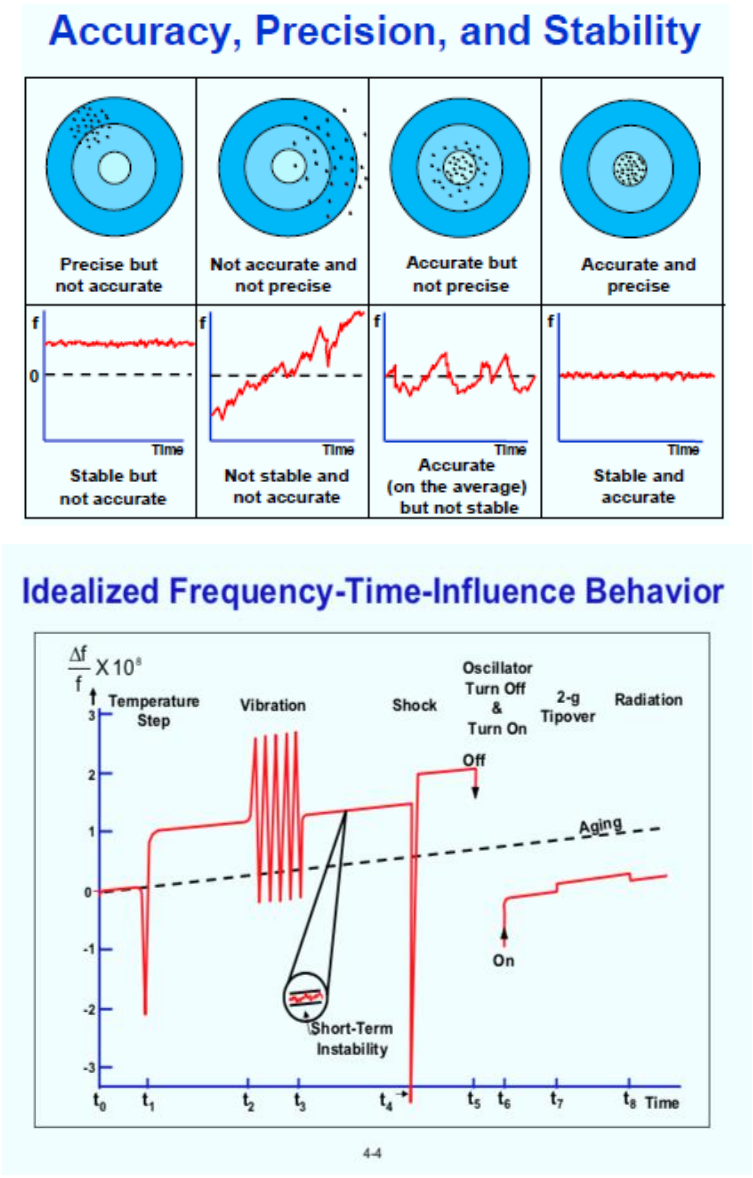


Figure 2-22 Crystal oscillator definition and frequency influences (from [69]).

2.2.8 Internal clock precision and power consumption considerations

The power consumption of any digital gate is proportional to its switching frequency. This results in a higher power consumption of the driving and distributing current for the 16 MHz clock compared to the 32 kHz clock. The driving and distribution current ($I_{RUN\ XOSC}$) of the core in nRF51822 for 16 MHz is 250-470 µA. This current decreases to 1 µA for 32 kHz. Since the basic power consumption reduction technique is to keep the node in sleep mode as long as possible, the current for driving the oscillator could be higher than the average consumption of the processor. Therefore, it is preferable to use a lower frequency clock and oscillators during sleep mode. As the processor and some peripherals need a high frequency

clock to execute operations, theoretically a high frequency clock should be turned on whenever needed, and turned off when not needed, and as often and fast as possible.

In practice, the start-up current for turning on a high frequency clock can be high and a minimal time is required to ramp up the crystal oscillator and stabilise the output. In the case of nRF51822 the total start-up time $t_{START\ X16M}$ is 800 µs. This interval has a high consumption interval $t_{START\ XOSC}$ of 500 µs during which the start-up consumption current $I_{START\ XOSC}$ is 1.1 mA. The crystal oscillator average wake-up current is

$$I_{XOSC\ WAKEUP} = \frac{(I_{START\ XOSC} \cdot t_{START\ XOSC}) + (I_{RUN\ XOSC} \cdot (t_{START\ X16M} - t_{START\ XOSC}))}{1\ [\mathrm{s}]}. \quad (2\text{-}10)$$

Figure 2-23 shows average start up current as a function of the sleep interval. It may be noted that for nRF51822 it is not worth while turning off the high frequency clock if the sleep duration is shorter than 1.5 ms or 49 intervals of the 32 kHz clock.

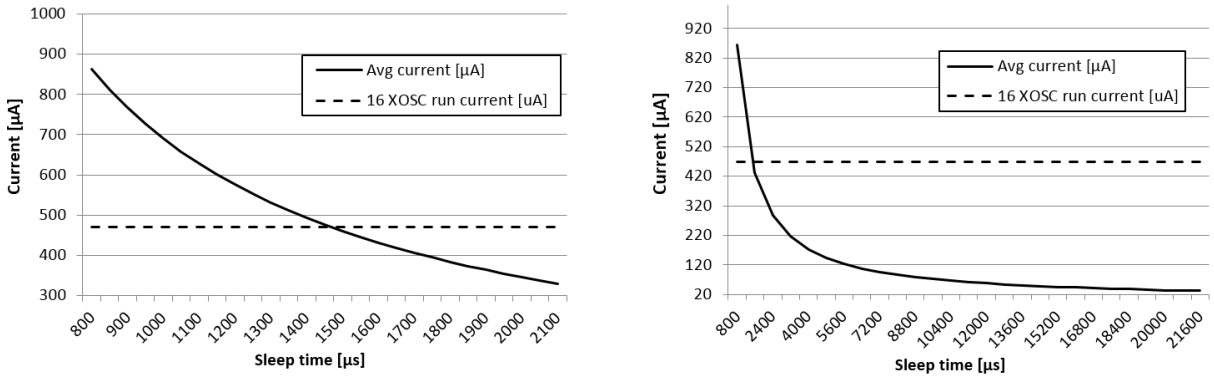


Figure 2-23 Average start up current as a function of the sleep interval; left up to 2100 µs, right up to 21600 µs.

Use of the 32 kHz clock as the node's internal time reference, as it is the only one always active, would also mean adopting the 32 kHz crystal's oscillator frequency error. This error is usually higher than the error in high frequency crystal oscillators. In the case of BLE, a maximal error of 250 ppm is allowed across the operating range. As explained in section 2.2.6 [Frequency error impact on wireless communication], accurate internal timing is critical for achieving successful and energy efficient wireless communication. If the 32 kHz frequency oscillator provides sufficient short-term stability, a node can measure the actual frequency of the 32 kHz clock using a higher precision clock. Measured clock error can then be used for compensation when time is calculated from the 32 kHz frequency oscillator. Figure 2-24 outlines the measurement accuracy of a low frequency 32 kHz clock relative to error measured with a 16 MHz clock. A reasonably long period should be chosen to provide required

measurement accuracy of clock error. For a short measurement period of less than 20 µs, measuring inaccuracy is higher than drift of the 32 kHz clock. A measuring period of 102 ms provides an accuracy of 0.6 ppm. This accuracy would guarantee that if the high frequency clock is calibrated, the low frequency clock could be calibrated as well.

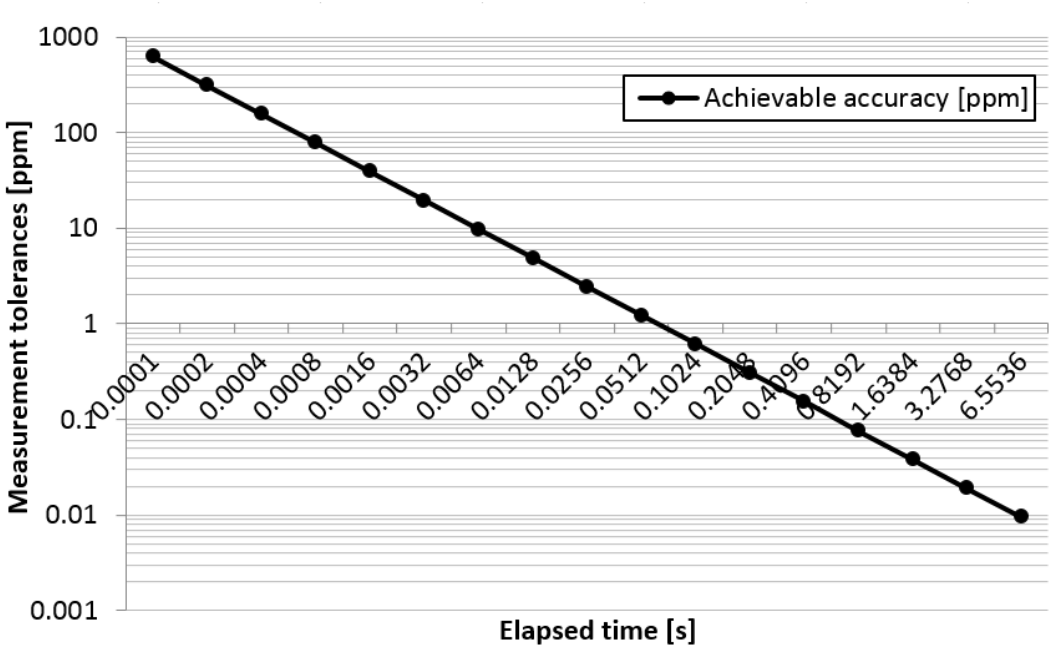


Figure 2-24 Measured clock accuracy of a 32 kHz clock oscillator frequency when measured with a clock frequency of 16 MHz.

2.2.9 Publish subscription data distribution

In healthcare, in most cases, there is one or multiple nodes which might be interested to in collecting and processing data from multiple nodes. For the case where a wearable device is the source of data, it would be impractical and energy expensive to send multiple packets to all interested nodes. Additionally, the wearable device would need to maintain the list of all nodes which notified the wearable node of their interest in the wearable device's data. Should a subscribed node disconnect without previously notifying the wearable device, the wearable device would still send packets to the non-existing node in the network and consume precious power. Another approach could be where the wearable device broadcasts messages in the network. If the messages are distributed throughout the whole network, it may increase battery consumption for other wearable nodes as well, as they will receive messages produced from all other wearable nodes in the network. In addition to increased power consumption, if the number of contents producing nodes is large, it can cause exhaustion of the available bandwidth in the direction from the network towards the wearable node. Should the broadcasting be filtered

towards wearable nodes, to overcome the outlined negative effects of broadcasting, it may impede functionalities such as device/service discovery.

A publish-subscribe model can provide a one-to-many distribution model. In contrast to a packet/message delivery based on delivery address, in a publish-subscribe model categorisation of the packet/message, which is usually called a topic, is used to deliver the packet/message to a subscriber for that topic. A node interested in receiving data generated from a specific node can express its interest by subscribing to the publish-subscribe distribution node. Often this node is a central server in the network, as for a successful distribution of the data, the node needs to know if the subscribed node is still connected to prevent exhausting of the network bandwidth. Figure 2-25 outlines the distribution difference of a single packet for broadcast-based distribution and subscription-based distribution. In the publish-subscribe model (Figure 2-25 on the right) wearable devices are not expending their limited available energy and limited communication bandwidth on incoming packets which are not of interest to them (Figure 2-25, left panel).

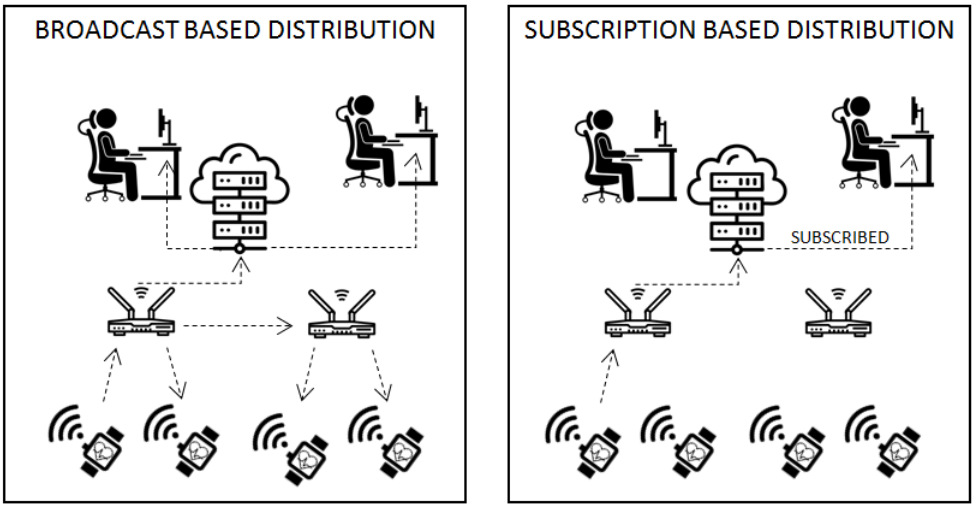


Figure 2-25 Difference between broadcast-based and subscription-based packet distribution.

Additionally, in many situations, the publish-subscribe model allows removing service discovery mechanisms. Consumer nodes can subscribe to a topic. When a node joins the network and publishes message with a topic for which another node previously subscribed, published messages will be forwarded to the consumer node as shown in Figure 2-25 (right panel).

The MQTT protocol experienced adoption growth in the IoT community and has started to be used as a backbone for cloud services such as Amazon Web Services AppSync

notifications due to its simplicity, versatility and human readable topics. Due to wide support from different cloud providers and platforms, it has been chosen as the messaging protocol for the presented solution. The MQTT message packet structure is shown in Figure 2-26. For packets like acknowledgments without payload data, the minimal packet size is 6 bytes.

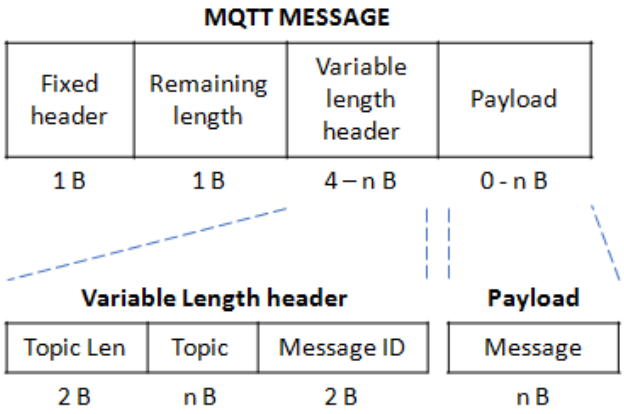


Figure 2-26 MQTT packet and header structure.

2.3 Increasing connectivity coverage and automatic link management as power optimisation method

Section 2.2.3 outlines the relation between extending communication range and power consumption. This section will look at reducing power consumption by reducing the required communication range through providing higher network coverage of energy efficient connectivity. Higher network coverage is envisioned to be available by removing obstacles that are preventing higher adoption rates for wearable devices.

2.3.1 Holistic approach to the wearable device barriers, adoption rate and evolution

Wearable devices are delivering an increasing number of benefits to their users and promise larger healthcare personalisation by gathering trends, however there remains a number of barriers preventing their wider adoption [71-76]. In a typical user's wearable-smartphone scenario, the user is required to manage several actions: i) pairing and establishing connectivity between two devices, ii) ensuring connectivity of the smartphone to the Internet (mobile plan or credit), and iii) managing charging level of both devices. Failure of any of those three actions may cause service failure as a whole and all its linked services. Successful use of wearable devices presumes that the user has a certain level of technical knowledge and dexterity to

interact with wearable devices and smartphones for establishing, maintaining and troubleshooting their connectivity. Although a younger healthy population may have such skills, the latter may pose a significant barrier for the elderly, children, and populations with disabilities or insufficient technical skills. Moreover, service failure can require troubleshooting the problem remotely and/or sending a technician onsite, both resulting in increased service costs. Therefore, ensuring seamless connectivity and management without user interaction are potential prerequisites for lowering user adoption barriers and service provision operational costs. The adoption of a human-centred design approach can facilitate in maintaining high utility value due to the interdisciplinary nature of problems and at the same time help to reduce adoption barriers and certain inconveniences [77]. Products without user interfaces and hermetically enclosed electronics have additional useful features such as allowing more carefree use due to a water resistant design and longer lasting operability since there is no display to consume power. The capability of the product to self-maintaining connectivity and enrolling in the user base without user interactions would allow designing and production of devices without any user interface. Further improvements may be achieved by providing usability beyond simple informative data towards more actionable data [78].

As wearable devices start to be more powerful and focused towards mobile and Cloud solutions, IoT and wearables start to overlap and share patterns. For example, IoT devices are designed to be deployed for a long period of time with a communication management preferable without the need for human interaction. Using same design approach for wearables may be beneficiary and improve user expirience. Understanding the history and forces driving the evolution of IoT can help to better understand possible directions in which wearable and IoT devices will evolve and how to make them more user centric. An analysis carried out by Ibarra-Esquer et al. [79] on tracking the evolution of the IoT concept across different application domains identifies two trends in the description what IoT is; extension to the existing Internet and evolution of the Internet. Although definitions may appear as diverging, authors conclude that they usually encompass the same five elements: networking, services, communications, data and things. Data and things could be bonded to the node at one end of the system, services to the data consumer at the other end and communications and networking as the underpinning link between them. Therefore, a priority should be placed on maintaining connectivity whenever possible.

Constant connectivity and the increasing number of smart devices which broadcast their presence to nearby listeners have exposed users' privacy and security vulnerabilities [80-81].

Acknowledged to be one of the crucial technology factors, trust [82-83], as well as social related factors, need to be properly addressed. As users' privacy and data-trail awareness starts to rise, a balance between user/device identifiability and privacy is needed. Information which is not needed for certain processes should not be exposed.

2.3.2 Privacy and security vs. device discovery and authorization

Two important stages are present when providing connectivity; device discovery and authorisation to join to a network. Both stages challenge the state of maintaining anonymity and privacy while providing reasonable security.

Device discovery can be found in smart devices which broadcast their presence to nearby listeners, such as in Bluetooth Low Energy (BLE) devices. As devices broadcasting their presence to nearby listeners have exposed users' privacy and security vulnerabilities [80-81][84][85], several new features and methods have been designed to overcome those recognised vulnerabilities. Device anonymity may be achieved by hiding all identifiable data from non-authorised paired devices/services. For example, the device could expose a pseudo-random medium access control (MAC) identity (ID), allowing only authorised paired devices/services to resolve the pseudo-random number to a valid device MAC/ID. Resolving a pseudo-random number into a valid device MAC/ID is carried out using a previously shared secret in the authorisation or pairing stage.

Bluetooth natively provides an IRK (Identity Resolution Key) [86] service where the detected pseudo-random MAC is decrypted using keys from all previously paired devices, although it is suitable only for identifying a limited number of known devices offline. The scalability of this approach would be impractical, time-consuming and expensive when trying to resolve the identity for a large number of devices and searching online through the database of stored keys.

The inclusion of both offline and centralised identification capability is offered by Edystone Ephemeral ID (EID) [87] which has based its solution around a combination of nonce and time state-defined encryption. Similar to pseudo-random MAC, EID has limitations in cases where there is a need to centrally pre-compute cryptographic states for a large number of devices [87]. The provided solution requires 6.75 GB for storing four hours of Ephemeral IDs for 30 million devices. As per Gartner [88], 318 million wearable devices were shipped worldwide in 2017 and 2018. The prediction for shipment in 2022 alone is 453 million wearable devices which suggests more than a billion shipped devices worldwide in the period from 2019

to 2022. The Edystone solution would require the computing of 225 GB of data every 4 hours without counting a 60 day time drift. Moreover, it does not provide options to support multiple service providers and distributed identity resolving. Device power failure is another limitation in EID. Since the time variable is used as an encryption secret, it will be lost in the event of a power failure and the device will not compute a valid EID resulting in the device's inability to establish a valid connection.

Another service for device discovery using Bluetooth low energy (BLE) is the Microsoft Connected Device Platform (CDP) where, in addition to the discovery service, the platform also provides a message exchange service between devices: "provides a discovery system to authenticate and verify users and devices, as well as providing a message exchange between devices" [89]. It uses the cryptographic one-way SHA-256 hash function to generate a 20 B hash from 4 B salt and device thumbprint which is sent to the centralised Web server. Similar to EID, the high likelihood for pre-computing limitations may result from the use of a one-way hash function. A CDP BLE broadcast message also contains device type bytes which, in an environment of only a few CDP devices, can enable active tracking of device activity. Additionally, offline use capability is a limitation in this design since it requires communication with a CDP web service to obtain information on other devices signed with the same Microsoft Account.

In the "node joining network" stage, reasonable security needs to be provided in order for a gateway to accept a connection request from the node. Additional interoperability needs to be provided when nodes want to connect outside of their home network. Granlund et al. [90] proposed the use of two mechanisms for enabling secure sensor mobility between different administrative domains. Authors have drawn parallels with EduRoam where academic institutions all over the world are interconnected using the RADIUS [91] Authentication, Authorisation and Accounting (AAA) protocol in a tree-like structure. Users are identified using a Network Access Identifier (NAI) with route to the home AAA server. This method provides a complete guarantee of the user joining the network, but it also exposes his identity.

The concept of Global Mobility network (GLOMONET), with mutual (anonymous) authenticated and key agreement (MAKA) protocols, was originally proposed by Zhu et al. [92] and followed by others [93-100]. These proposed protocols are evolving and are able to provide user anonymity although they rely on a pre-existing relation between the connectivity provider and user where Temporary Identity (TID) is generated. Lee et al. [96] proposed the delivery of a smartcard and password to the user for successful authentication. Ruhul et al. [100] suggested

a protocol requiring a user setup phase where user ID and hashed password are shared with a gateway node to create a shared secret. After a shared password is generated, it needs to be propagated to gateway nodes. Additionally, users are required to execute actions in order to connect and enter passwords. This action imposes the existence of a user interface on the node itself and would prevent connection to a new node. In [100], the gateway node knows the identity of both users and mobile user. Temporary identity is changed only by the gateway node after a successful login phase which makes tracking possible when the mobile user tries to connect. Kai et al. [93] proposed additional anonymity improvements in which a mobile node can chose when to generate a new random number to hide its temporary identity. Messages are encrypted using a foreign agent public key to prevent a denial of service attack on the home agent.

Even if anonymity is preserved in the discovery and authentication stage, normal communication of the node can be used for detection of activity, as noted by Das [84]. A similar de-anonymisation fingerprint attack on Tor hidden services is described by Albert [101]. For example, in the everyday home environment, a simple smartphone can be used to profile neighbour's daily activities. Through a simple and free smartphone app it is possible to detect when the neighbour's laptop is on, as shown in Figure 2-27 (left panel). From Figure 2-27 it is shown possible to read device manufacturer, device type and receiver strength signal without possessing specific field knowledge. A person with bad intentions could exploit this information and build an activity profile of a target person or apartment. This profile can be used to give information when it is safe to execute malicious activities.

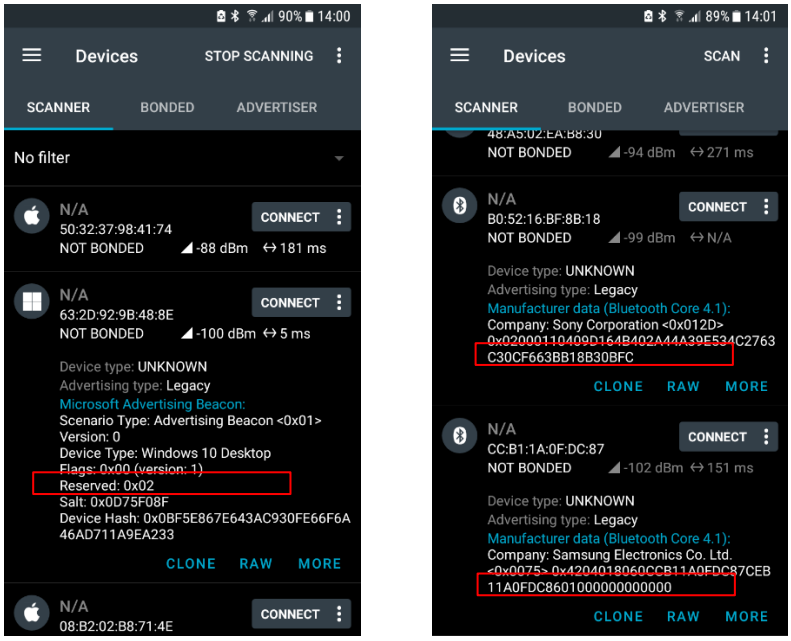


Figure 2-27 Scanning for nearby devices using a smartphone.

2.3.3 Seamless connectivity

The connectivity of a wireless sensor network (WSN) can be improved either by extending the working range of wireless communication or by improving coverage/availability of interoperable/compliant infrastructure to which the node can connect.

Extending the working range of wireless communication can either be achieved by increased transmitting power or by increased receiver sensitivity. Maintaining the low-power attribute of wearable and IoT devices prevents increasing the transmitted output power. Therefore, only sensitivity can be increased which is the case for a low-power wide-area network (LPWAN). As outlined in section 2.1.5, increasing sensitivity may be achieved at the expense of lowering the effective communication data rate. This could be impractical for wearable and IoT use cases.

Improving wireless connectivity by improving coverage/availability of interoperable/compliant infrastructure can be achieved using several approaches; using devices with multichannel capability, deploying new infrastructure or reuse of technology already present/deployed. In [102], hyper connectivity is seen as a way to ensure evolution towards distributed IoT architectures with better efficiency, scalability, end-to-end security, privacy and resilience. Pramanik et al. [22] concluded that wireless body area networks (WBAN) are autonomous and capable of opportunistically finding a suitable communication network. Jamil et al. [23] proposed a WBAN solution to overcome connectivity limitations by using nodes

capable of communicating over multiple channels and opportunistically connecting. This approach increases size and cost since there is a need to add active and passive components for multiple communication channels. Lei et al. proposed the creation of community networks [18]. In this scenario a service provider such as a hospital is responsible for providing a service in a specific region. This approach requires the setting up of a suitable infrastructure. Examples of interoperable wireless neighbourhood area networks like Wi-SUN or JupiterMesh are highlighted in [102]. Rohokale et al. [19] proposed a cooperative IoT model where a mobile device would act as a gateway. Consideration of the same approach can be found in Dutta [103] where firstly leveraging smartphones as a temporary gateway used as a router, or secondly as a Bluetooth profile proxy when interacting with a Bluetooth device, are envisaged. The router option offers better flexibility while the BLE profile proxy is better suited to the power and processing constraints of the device.

In conclusion, seamless connectivity approach can extend connectivity beyond the home network by means of autonomous connection management which is achieved without increased transmitting power or changes to device hardware properties.

3 Optimization of energy efficiency in communication protocols for long term data acquisition and monitoring in wireless networks

3.1 Energy efficient wireless protocol for exchange of data in wireless sensor networks in health care

3.1.1 Healthcare use case

Certain patterns and commonalities may be observed in wireless communication in the healthcare environment [11]. These patterns mainly come from fact that nodes have primarily data source or data sink role. Data generated at primarily data source devices such as sensor devices are forwarded directly or through an intermediary towards data consumer nodes. Examples of data consumers on the network are monitoring services which process data from groups of sensors. Another example could be a local display and/or monitoring device as shown in Figure 3-1. From a wireless communication perspective three main use cases can be found:

- wireless device communicating with an infrastructure wireless gateway
- wireless device communicating with a mobile device as part of a Personal Area Network/Body Sensor Area Network
- wireless device communicating with display equipment.

These use cases can be translated into a star network or point to point network topology. Since the basic power optimisation method is data reduction, wireless healthcare devices should exploit it and transmit a minimal set of data when the state of the measuring subject or parameter is within the boundaries considered normal. In the case of suspicions conditions, a device should transmit the maximum set of data in real time to help determine current status. Therefore, energy efficient wireless communication protocols used in healthcare must be optimised for two end of operation modes:

- Low data rate data transfer
- High data rate real-time data transfer

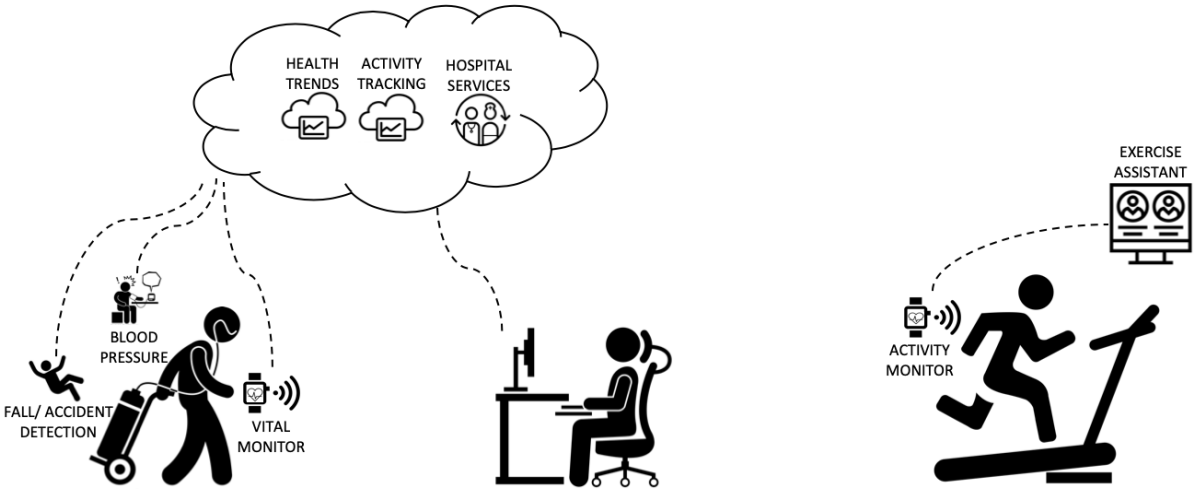


Figure 3-1 Healthcare wireless use cases.

3.1.2 Efficient multi-layer protocol

As presented in the previous section, multi-layer optimised protocols have a better chance of achieving energy efficiency in real life use. A novel wireless communication protocol named Wireless Of Low Complexity (WOLC) is developed with multi-layer optimisation approach for the purpose of this research. The following energy savings and optimisations methods are chosen for energy efficient wireless protocol: data reduction, sleep/wake-up schemes. Data reduction focuses on minimising protocol overheads and enabling efficient sleep/wake-up schemes.

An energy efficient protocol should provide optimal performance in the connection base scenario where there would be a change in wireless communication mode from low throughput to high throughput data rate.

The first objective of the wireless protocol is to minimise protocol overhead. Protocol efficiency is relatively low in the case of small data payloads such as transmitting heart rate readings consisting of three bytes of data - two for the type and one for heart rate value, as shown in 2.1.4.

The second objective is to allow efficient time division multiple access (TDMA) scheduling by ensuring the radio being in sleep mode whenever it is not transmitting or receiving data. A scheduling algorithm is needed to compensate for clock mismatch resulting from the clock drifts of the two communicating devices. A factor limiting the theoretical maximum sleep time is the radio ramp up time, i.e. the time required to start and achieve a phase locked loop of the radio modulation clock. In most low power transceivers this may be around 130 μs – 500 μs [58], [104].

The developed MAC model uses a continuously linked frame model without guaranteed sleep time, shown in Figure 3-2 (panel A). Absence of guaranteed sleep time enables high data rate when required. In case of a low data rate, low power is achieved since nodes communicate for only the minimal required time to transmit all of the data. This model correlates power consumption with the required data rate. Each frame has a fixed length of 41 ms which results in a frame frequency of 24.39 Hz. Data transfer latency required to transfer data from one node to another is the time from the moment when the surge of data occurs to the transmit buffer, until the start of transmission of the data. Frame frequency of 24.39 Hz results in a best-case scenario a latency of 41 ms and in a worst case latency of 82 ms.

Inside of each frame there are 2 possible slot formats, as shown in Figure 3-2 (panel B), bidirectional and unidirectional. Bidirectional slot is used when exchanging data both ways between master and slave node, while a unidirectional slot is broadcast only in the direction from master towards multiple slave nodes on a shared master node address.

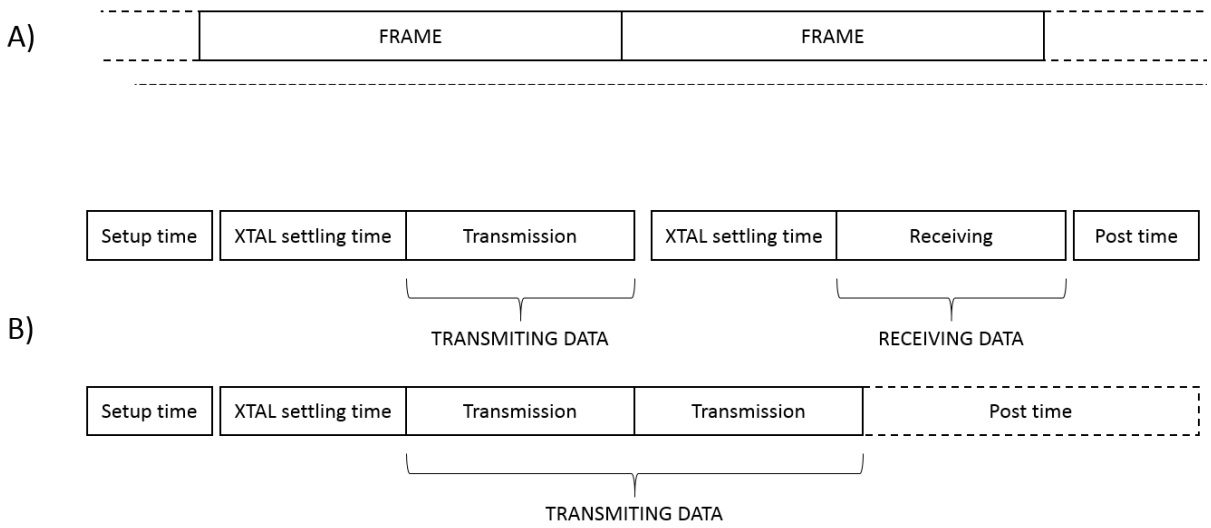


Figure 3-2 A) Frame distribution across time, B) Slot inter-stages.

An unidirectional slot executes the radio clock settling only once, compared to twice in bidirectional slot. This enables the remaining time to be used to transmit additional data. For the case where the radio is communicating using a 1 Mbit/s or 0.25 Mbit/s slot components setup time and oscillator settling duration have fixed execution time. Only transmit/receive slot component has variable duration execution time. The resulting slot duration and effective speed is shown in Figure 3-3. The total length of the slot is 750 μs when using a 2 Mbit/s data rate, 75 μs for setup and post wireless transmission time, 130 μs for settling time and 168 μs for data transmission and receival. The effective data exchange time in the slot is 44%, achieving an

896 kbit/s throughput. The substantial difference between over the air speed of 2 Mbit/s and effective speed of 896 kbit/s is a result of the radio to initiate settling after every radio mode change, sleep to transmission and transmission to receiving. Radio settling time is comparable in length to the transmission time, which implies that almost half of the energy spent in wireless communication is due to waiting for the settling of the clock. Settling of the clock requires a smaller percentage of the total time for the 1 Mbit/s and 0.25 Mbit/s data rate, due to lower over the air speed. Achieved effective radio transmission times of 61 % for 1 Mbit/s and 81 % for 0.25 Mbit/s.

Due to a settling time comparable to the transmission time at 2 Mbit/s, transmitting at two times slower speed (1 Mbit/s) increases transmission time by only 60 % with a resulting power consumption increase close to 60 %.

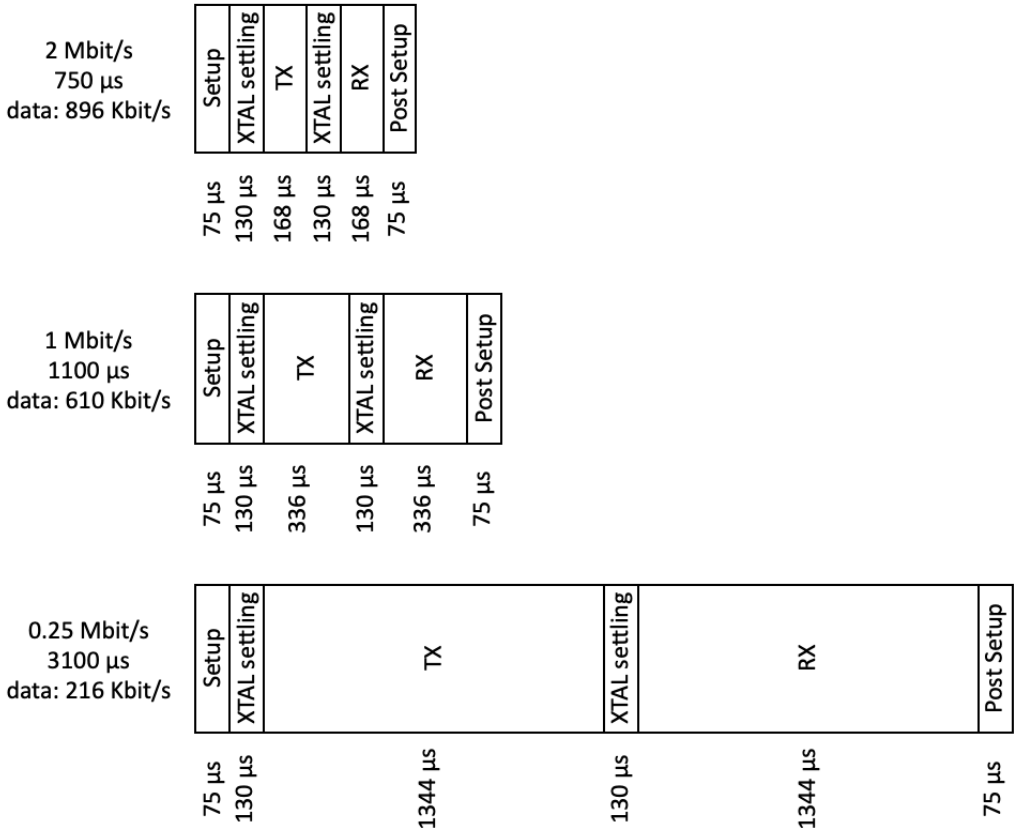


Figure 3-3 Slot duration and effective speed.

Each frame has a fixed slots distribution, as shown in Figure 3-4. Each frame starts with bidirectional connection/ping slots whose function is to advertise the master's node presence and thus enable discoverability. Connection slots are transmitted using three over the air speeds; 2 Mbit/s, 1 Mbit/s and 0.25 Mbit/s, to provide either range or reduced power consumption. A

slave node with the intent of joining the master's node network will respond to the received ping/connection request with a connection response packet. Connection response packet contains slave's node address and description. The master node, based on the received data, will decide whether to join the slave node to the network or not.

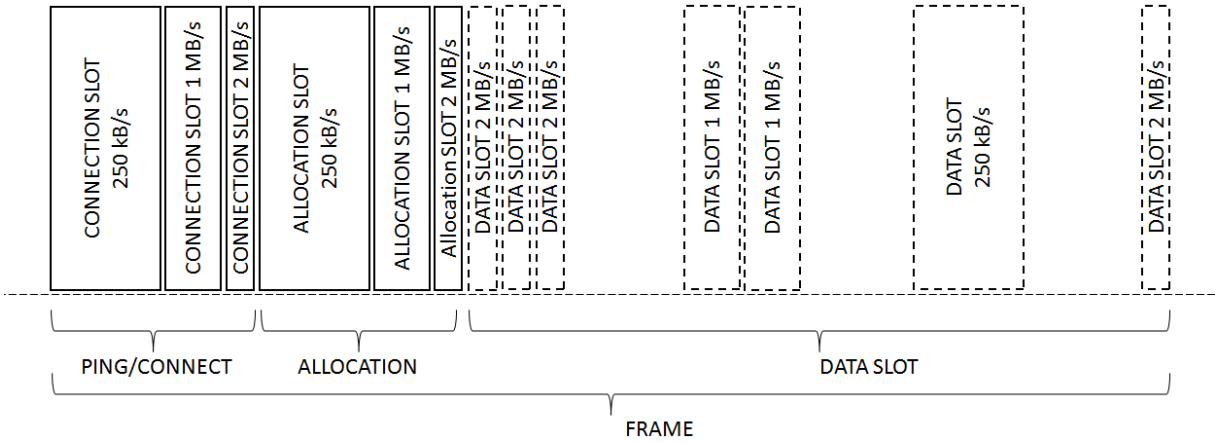


Figure 3-4 Inter frame slot distribution.

To preserve power, the slave node will always try to listen for the master node at the highest encoding speed of 2 Mbit/s. If no message is received at the highest encoding speed, the receiver will retry and listen at 1 Mbit/s. The same switch to 0.25 Mbit/s procedure is adopted if listening on 1 Mbit/s fails.

Since multiple slave nodes will try to respond to the same ping/connection packet, a collision of multiple connection request may occur. Master rejects connection request by not posting the slave's address in the allocation slot. The master's absence of broadcasting the slave's address is treated as a collision occurrence. When collision occurs, a random back off period is used prior to the retry of the slave node to connect again.

A connection slot is a bidirectional slot type where the first ping/connection request packet is transmitted from the master node to the slave followed by the slave node responding with transmission of the connection response packet. The connection slot packets content is shown in Figure 3-5. Ping/connection request packet type is a single byte defined as 0x10 HEX followed by a description of the master node. Next is the master ping flag 0x03HEX followed by the display name and clock parameters. A connection response packet is transmitted by the slave and contains the packet definition set to 0x20 HEX followed by the six-byte access address. The access address is unique per slave node. On access address the slave node will listen for packets from master node during the data slot. The last part of the connection response

packet is the slave node description which is used to determine node type and whether to grant access.

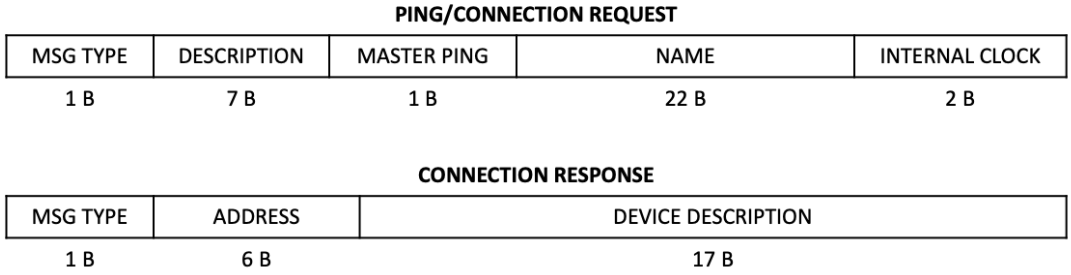


Figure 3-5 Connection slot packets definition.

The connection slot is followed by an unidirectional allocation slot shown in Figure 3-6. The allocation slot is transmitted using the master node address. Inside the allocation slot there are two packets with message type 0x30 HEX for the first allocation packet and 0x40 HEX for the second allocation packet. The frame data slot section can be divided into a maximum of 44 individual data slots if a 2 Mbit/s speed is used. Allocating data slot section with a lower over the air speed data slot will result in a lower maximal number of slots that can be served in a specific frame.

The first packet in the allocation slot contains new node connection data and data slot allocation mapping to a specific connected slave node. If the master node decides to accept the incoming slave node connection request, the first allocation packet will encompass a connection grant response. Connection grant response contains the slave's node address and designated shortened address to be used as an identifier in the data slot assignments list. The newly connected node is prioritised in the data slots allocation and receives allocation in the first data slot. The remaining time is divided equally among all other nodes scheduled to communicate in the current frame. Following the node connection grant response, data in the first allocation packet are the first 14 bytes of the slots allocation data. Data reduction method is used to decrease energy consumption where the slave's long 5 byte node address is exchanged for a single byte address for the duration of the connection session. Address byte contains shortened slave node address in the lower 6 bits and slot speed in the upper 2 bits. This results in a maximum number of 64 slave nodes which can be served by a single master.

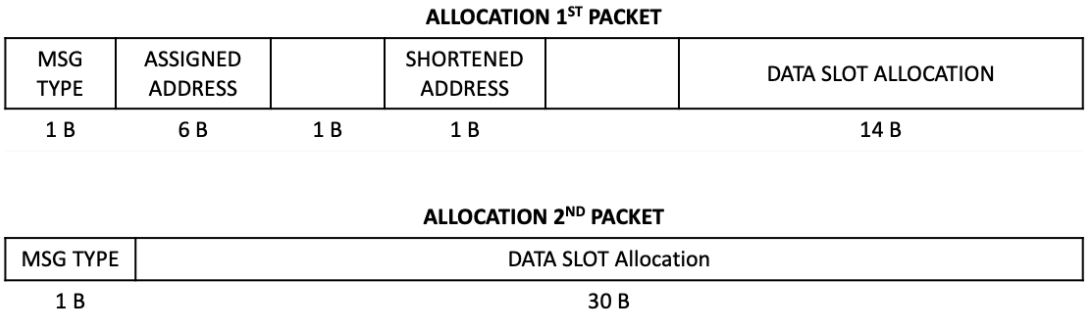


Figure 3-6 Allocation slot packets definition.

The final slots in the frame are a bidirectional data slot. This slot contains a link management byte, data length byte and up to 30 bytes of data as shown in Figure 3-7. The packet structure allows efficient link management while minimising packet overhead by using only two bytes. The lower four bits contains identifier of the last transmitted and received packet. By using a rolling incremental counter of two bits for each direction, there is a constant distance of three which is used to prevent double processing of retransmitted packets. Although two bits would be sufficient to prevent double processing of retransmitted packets, using four bits will enable future protocol expansion using multiple unidirectional frames. The top four bits inside the link byte sent from master to slave node represent the coded with number of the frame which will be skipped before listening again for the frame.

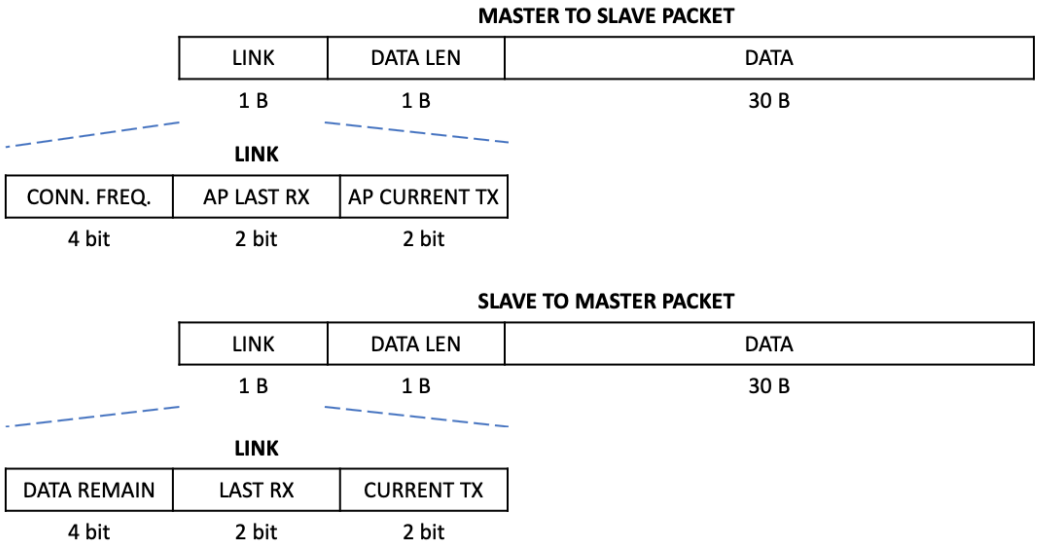


Figure 3-7 Data slot packets definition.

3.1.3 Automatic bandwidth allocation and pulse response

Top four bits in the packet sent from the slave to the master node shown in Figure 3-7 contain the amount of data left to be transmitted from the slave node divided by 32. This results in the slave node's ability to notify the master node of the data length pending to be transmitted in the transmitting buffer. The slave node can notify the master node its readiness to transmit from zero to 16 data slots (increments of 32 bytes, from 0 to 512 bytes). Slot allocation is determined based on the master node list of slave's last transmitted data remain value. When the surge of data occurs in the slave's node transmit buffer, the master node will receive information about the surge only after the successful receipt of slave's packet in data slot. In the next frame master will be informed that the slave node needs more assignments of data slots. In the example shown in Figure 3-8 surge of 512 bytes occurs, the master node assigns 18 data slots to enable the slave node to transmit the required data. This results in a delay of one frame from the surge of data event until transmission of all the data as shown in Figure 3-8.

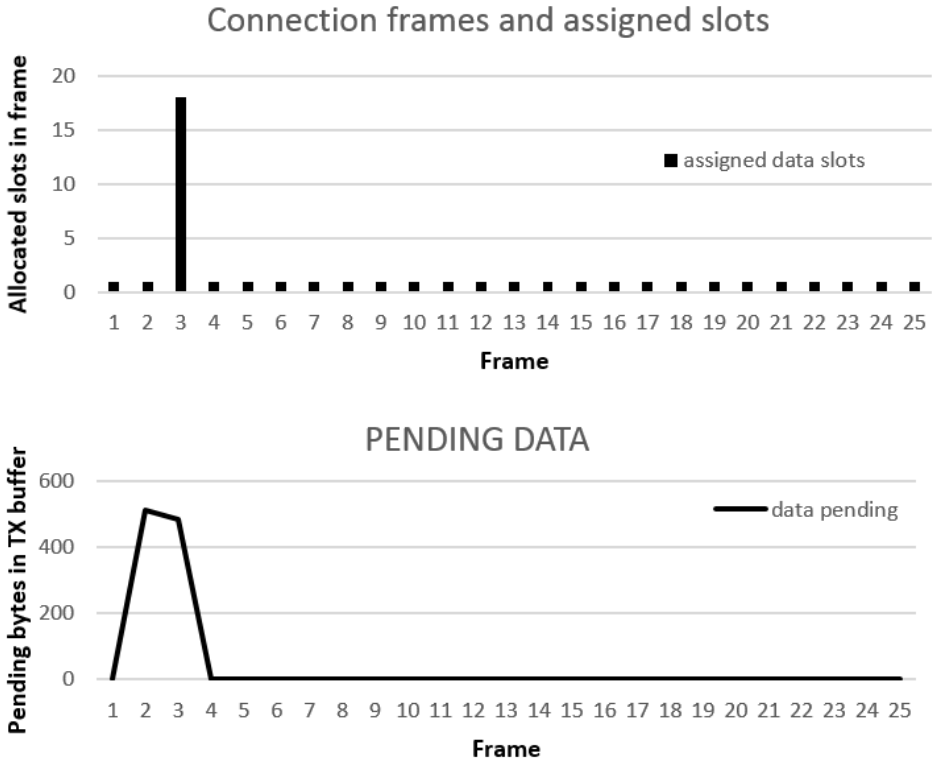


Figure 3-8 Dynamic data slot allocation pulse response to surge of 512 bytes of data in the slave's node transmit buffer.

3.1.4 Automatic energy saving and pulse response

Transmission of slave's pending data to transmit buffer gives the master node full awareness of its own pending data and pending data for every individual connected node. This allows successful management of connected nodes. Master node has full management of data slots allocation and power management. Power management is achieved by assigning *N* amount of skipping frames before next communication with an individual slave node if power saving is enabled. The master node will try to allocate to every individual node a combination of frame skipping and data slot numbers. The algorithm to determine number of skipped frames ($N_{skipped\ frame}$) for the slave node number of ready to be transmitted data slots in transmit buffer ($N_{tx\ buff\ slot}$) is

If ($N_{tx\ buff\ slot} > 4$) then

$N_{skipped\ frame} = 2^0 - 1 = 0$ (every frame)

If ($4 > N_{tx\ buff\ slot} > 1$) then

$N_{skipped\ frame} = 2^1 - 1 = 1$ (every 2nd)

If ($N_{tx\ buff\ slot} = 1$) then

$N_{skipped\ frame} = 2^2 - 1 = 3$ (every 4th)

If ($N_{tx\ buff\ slot} = 0$) then

increase from $N_{skipped\ frame} = 2^0 - 1$

until $N_{skipped\ frame} = 2^4 - 1 = 7$ (every 8th or frame rate of 3.048 Hz)

When surge of data event occurs, the algorithm is designed to have a step response by terminating power saving method of frame skipping. This behaviour is in place to prevent overflow in slave node transmitting buffer when services with high data rate are initiated. These services could require live sensor data transmission or voice data transmission. If the number of pending slots to be transmitted drops to 0, with less than 32 bytes in the output buffer, the frame rate will experience an exponential decay settling to one-eighth of the nominal frame rate corresponding to 3.048 Hz or every 328 ms.

Two example use cases are chosen to present impulse and step response of wireless communication when slave node is communicating at 1/8th of the nominal frame rate. Case one simulates requirement to transmit once 512 bytes length message. Case two simulates start of real-time ECG data transfer.

In the first use case 512 bytes length message is loaded in to the transmit buffer and pending to be transmitted (frame 2 in Figure 3-9). In the next scheduled frame (frame 3), the slave node will notify the master node (in data connection slot) that more than 16 slots of data are pending for transmission. Since the frame frequency can be updated only with a packet coming from the master node to the slave node, the slave node must skip and wait for another 7 periods before the master node increases the connection to the full frame rate, as shown in Figure 3-9 (frame time 10). In the next frame, the master node has enough free bandwidth to allocate all 17 data slots to the slave node (frame time 10 in Figure 3-9). In this frame the frame rate is set to nominal, resulting in a slave node communicating in the next frame 11. In the same frame slave node communicates to the master node that there are no more data to be transmitted. The master node in the next frame 12, starts to decrease the frame rate speed. Used power saving method prevent slave node from listening to every frame which achieves power saving. Skipping frame listening introduce additional latency equal to the number of skipped frames. The node is active in 7 frames compared to 21 without power saving enabled at the expense of an additional 287 ms delay if no packet error occurs.

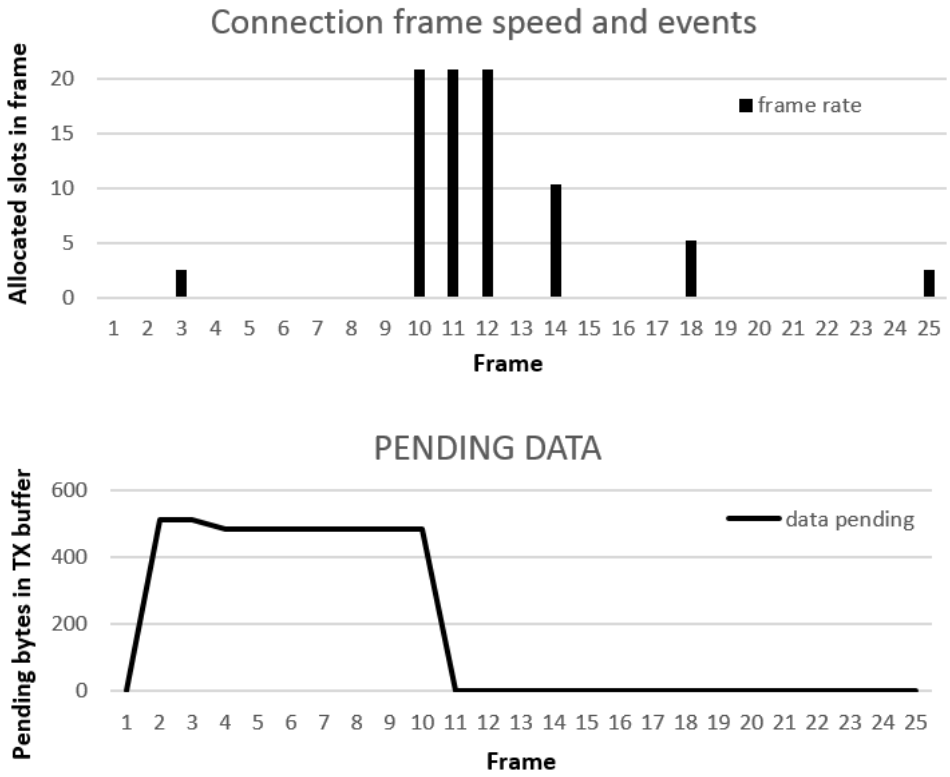


Figure 3-9 Power saving method impact of frame skipping on latency when surge of data occurs.

In power saving mode extended latency requires larger transmitting buffers if overflow or data loss is to be prevented when transmitting real-time data with high data rate. In the second use case node starts to generate 64,000 bits/s. Figure 3-10 shows the pulse response characteristics when automatic power saving is used. By the time the master node changes communication frame rate with the slave to the nominal frame rate, the slave node already has 2634 bytes queued in transmission buffer. Master node can allocate half of the 2 Mbit/s data slots (22) to serve the slave node. In order to arrive at a settled number in the transmitting buffer, 7 frame periods must pass with 22 data slots allocated equivalent to 127 kbit/s transfer speed. After 7 frames the master node can reduce the allocation of data slots to a 11-12 equivalent to 63 kbit/s – 69 kbit/s. The pulse response does not take into the account packet error. For the case where the slave node does not have a transmitting buffer capable of storing newly generated real-time data between the change from power saving mode to full frame rate, the user code should ensure that the slave node informs the master node of low latency connection requirement.

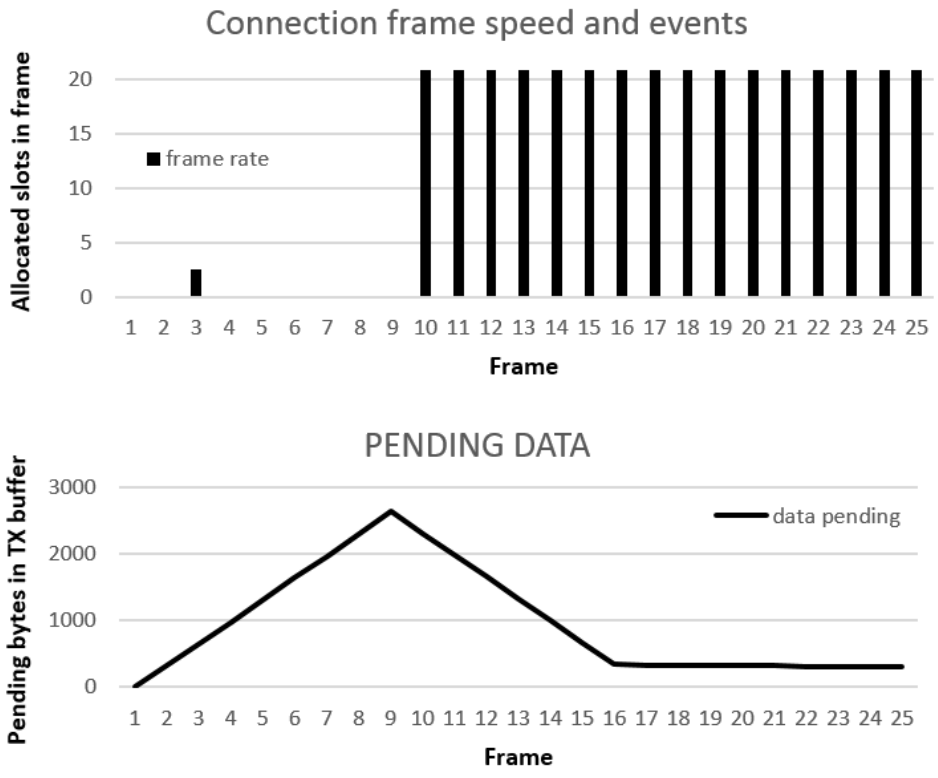


Figure 3-10 Power saving method impact of frame skipping on slave transmit buffer when real-time data starts to be generated at high data rate.

3.1.5 Protocol minimisation impact of packet loss

In the case where the distance between the master node and the slave node increases, BER will increase as well. Some packets may not be received or the integrity check may fail. This can decrease the overall achieved throughput and increase effective power consumption. The presented protocol and MAC define a bidirectional data slot as a base method to exchange data between master and slave node. Master node firstly transmits data to the slave node, followed by slave node transmission to the master node. Failure may occur in both directions.

To minimise throughput degradation as a result of packet loss in any direction, the protocol treats every direction as a separate channel. The link byte shown on Figure 3-7, encompasses the value of two rolling counters. The first rolling counter is the last received counter from the direction of master to slave, The second rolling counter is the last transmitted counter in the direction master to slave. After establishment of a new slave connection the master node transmit packet with a counter value of 0. On each occasion when slave node receives packet from the mater node, it will update last received counter value for the direction master to slave. On each occasion when master node receives packet from the slave, it will update counter value for direction slave to node. The protocol exploits the required radio ramp up (PLL lock) time ($t_{RAMP\ UP}$) between the slave node's change of state from receiving into transmitting. The available time of 130 μs is sufficient for the slave node to update the packet being transmitted to the master by adding last received counter value from the master. On a successful receival of packet from slave node, master node determines whether the slave node received the last sent packet. Should the underlying hardware fail to support an update of the packet during radio ramp up time, the slave node would not be able to transmit the last received counter state from the master node. This would introduce a delay of one bidirectional slot before the master is able to determine the value of the slave's last received packet.

The size of the rolling counter is 2 bits, allowing 4 states. If only bidirectional slots would be used 1 bit with 2 states would be sufficient. The MAC and protocol must be expandable for future improved efficiency applications where unidirectional slots would be required. Should that be the case, one slot could transmit up to three packets requiring a four-state counter.

3.1.6 Frequency error compensation, time synchronisation and MAC

Clock synchronisation is tightly coupled with the medium access control method. Medium access control predefines interaction events in which nodes transmit and receive data.

Two possible implementations were analysed when designing MAC. In the first MAC approach the master node is the first to transmit, followed by slave transmission. In the second MAC approach the slave firstly transmits in the designated slot followed by the master's transmission. Two MAC approaches are shown in Figure 3-11. Both options include benefits and trade-offs for the master and slave node from the power consumption, synchronisation and timed division multiplexing (TDM) perspective.

The first option (Figure 3-11 panel A) minimise power consumption for the master since the master radio is active and powered only for the required transmission and receiving time. The slave node needs to be in receiving mode sufficiently in advance to compensate for clock drift between the master and the slave node. When the master transmits its packet the slave node will reply immediately. Since only one clock is used as the reference time keeping clock, the inter-slot security window only needs to account for the master node clock instability and the slave's response jitter time. This results in better TDM efficiency and higher throughput.

In the second option (Figure 3-11 panel B), the slave needs first to transmit packet in the bidirectional slot. This option benefits the slave node's power consumption since the slave node would be able to turn on the radio only for the required transmission and receiving time. The master node would be responsible for extending its receiving state to compensate for clock drift between the slave and master nodes. For the 2 Mbit/s slot which is 750 µs wide, this results in a minimal 75 µs reduction of active time for slave node and increase of power efficiency by at least 10 % . Although this second MAC approach can save the slave node's power consumption, it introduces the possibility for slot drifting and possible collision between two slots in proximity, which require increase of guard time between the bidirectional slots. The result of guard time increase is a decrease of overall throughput and TDM efficiency. Since the start of transmission is dependent on the slave's clock, an internal clock error of two slave nodes may have the opposite sign resulting in two slots coming closer and closer. Eventually the slots will overlap, and collision will occur resulting in communication failure. Frame synchronisation would be possible to achieve by using allocation slot as slave node realignment time. This method works only when slave node is communicating frequently with master node. In case of low frame rate or packet loss, increased time between communication of master and slave will result in slave clock drift and collision will occur.

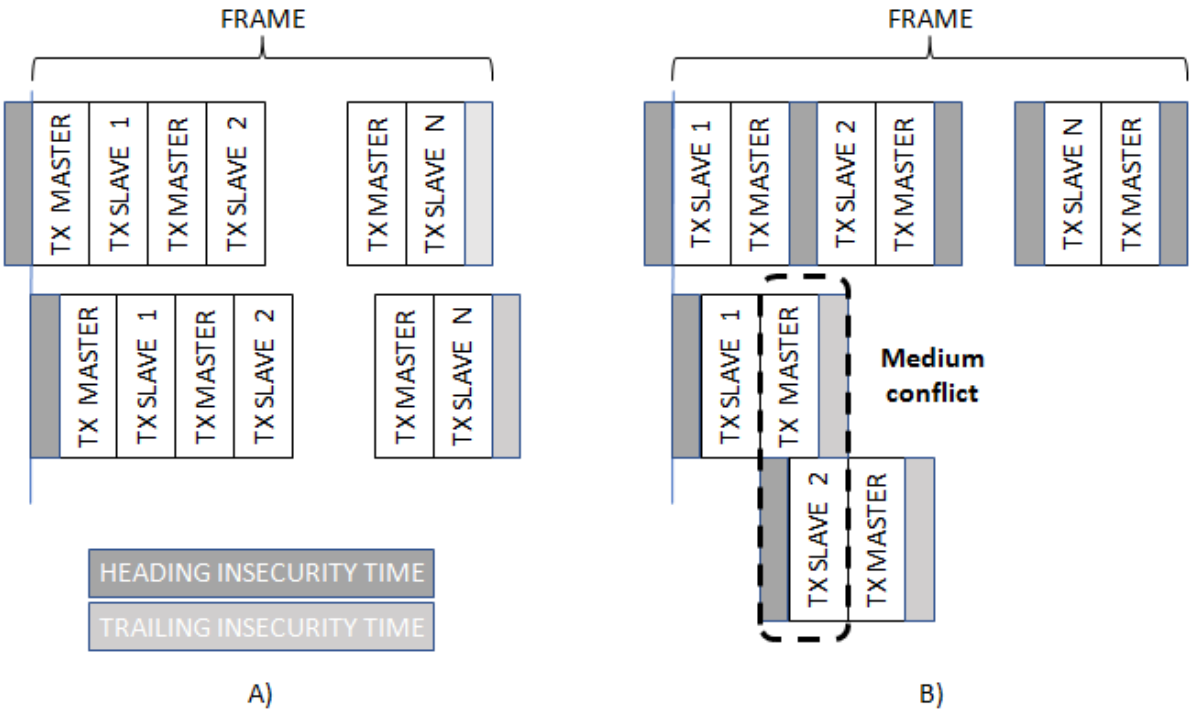


Figure 3-11 Internal clock error impact for A) Master led medium access, B) Slave led medium access.

When the radio is in receiver mode, the receiver circuit will try to detect a predefined synchronisation symbol or address. When the symbol or address is detected, it will start to assemble the receiving packet with demodulated data. In case where the distance between the master node and the slave node increases, BER will also increase and some packets may be lost, or the integrity check may fail. Since the slot has a fixed length, if the address match is not detected by $t_{ADDR\ MATCH\ DEADLINE}$ the node must enter a disabled state as an address match beyond the deadline will lack a receiving time limited by slot boundaries. The representation of the late address match scenario is shown in Figure 3-12, from which it is clearly visible that keeping the radio active after the $t_{ADDR\ MATCH\ DEADLINE}$ will only consume power without the time to receive a full packet.

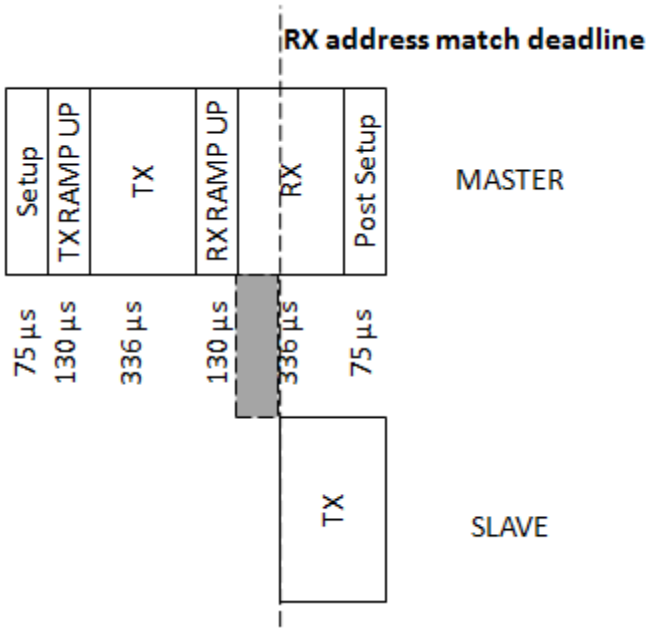


Figure 3-12 Address match deadline time.

The selected underlying hardware supports detection of the receivers address match. If the address match does not occur by the expiration of a predefined time, it will switch the radio into disabled mode to reduce energy consumption. The power saving for the master node ($P_{MASTER\ SAVING}$) from turning off the radio in the case where a packet is not received is

$$P_{MASTER\ SAVING} = \frac{t_{MAX\ PACKET}}{t_{SLOT}} = \frac{t_{1\ Mbit/s\ MAX\ PACKET}}{t_{1\ Mbit/s\ SLOT}} = \frac{336\ \mu s}{1100\ \mu s} = 30{,}5\% \qquad (3\text{-}1)$$

where $t_{MAX\ PACKET}$ is the maximum length of the packet and t_{SLOT} is the slot length.

The slave node will have higher power saving for this method as the slave node always starts in receiving state at the start of the slot. Therefore failure to receive a packet will be detected much sooner in the slot compared to the master node resulting in slave node radio turning off sooner. The power saving for the slave node ($P_{SLAVE\ SAVING}$) using the described method and data rate of 1 Mbit/s is

$$P_{SLAVE\ SAVING} = \frac{t_{SLOT} - (t_{SETUP} + t_{RAMP\ UP} + t_{POST\ SETUP})}{t_{SLOT}} = \frac{820\ \mu s}{1100\ \mu s} = 74{,}5\% \qquad (3\text{-}2)$$

where t_{SETUP} is 75 µs setup time, $t_{RAMP\ UP}$ is 130 µs of radio ramp up and $t_{POST\ SETUP}$ 75 µs of post slot preparing time.

Presented protocol MAC is a trade-off between efficiency and time synchronisation described in 2.2.4. The designed MAC also impacts slave's probability of successful transmission of data to the master node. For the case where the channel conditions are identical

in both directions, if the probability of successful transmission from master's node to slave node $P(master\ to\ slave)$ is

$$P(master\ to\ slave) = X \tag{3-3}$$

the probability of the slave's successful transmission to the master $P(slave\ to\ master)$ is

$$\begin{aligned} P(slave\ to\ master) &= P(master\ to\ slave) \cdot X \\ P(master\ to\ slave) &= X^2 \end{aligned} \tag{3-4}$$

as the slave node only replies to a successfully received master's packet. This results in exponential growth of the failure probability of successful transmission from the slave to master. Motivation to limit slave's node transmission only upon receiving successfully master's node packet, is to minimise the opportunity for wireless medium collision. Collision may occur if the master's and slave's clocks are out of synchronisation due to long periods of unsuccessful packet exchange.

As a result of the preceding analysis, the protocol will use the following synchronisation and error compensation methods and properties:

1. all connected slave nodes will use the master node internal time as a reference time and compensate for time and frequency difference between them and the master,
2. slave nodes will use the master's ping slot transmission as a clock resynchronisation event and calculate the time difference and compensate the internal clock frequency error,
3. after the slave establishes a connection with the master node, for each frame from the first ping packet ($N_{FRAME\ FROM\ INITIAL\ PING}$), the slave node will increase the heading and trailing insecurity window ($t_{\ INSECURITY}$)

$$t_{\ INSECURITY} = t_{JITTER} + t_{FRAME} \cdot ppm_{OSC} \cdot N_{FRAME\ FROM\ INITIAL\ PING} \tag{3-5}$$

   where t_{JITTER} is receival insecurity and ppm_{OSC} is maximum crystal oscillator frequency error defined by the protocol (16 MHz – 60 ppm, 32 kHz – 250 ppm) until receiving the second ping slot from master node,
4. if a node is in receiving state and the address match does not happen by $t_{\ ADDR\ MATCH\ DEADLINE}$ the radio will switch to disabled state.

3.1.7 Bit error rate impact

Since the channel loss in different environments will have different values, it is not possible to use distance as attribute when describing protocol performance. A more accurate attribute is the bit error rate (BER) since it defines channel properties with a single number.. The longer the packet transmitted, the more byte/bits it holds, which in turn, increases the overall error probability of packet error rate (PER). For a packet with a length of n bits the resulting packet error rate (PER_n) will be

$$PER_n = 1 - (1 - BER)^n \tag{3-6}$$

Exponential relation between PER and the length of the packet may be noted in Figure 3-13. Minimal packet length defined by WOLC protocol is 12 bytes and maximal length is 41 bytes. For a maximum packet length of 41 bytes at the receiver sensitivity edge (declared by the nRF51422 manufacturer), the probability for packet error is 27 %. This is substantially higher than to 9 % for packet error minimal packet size of 12 bytes is transmitted.

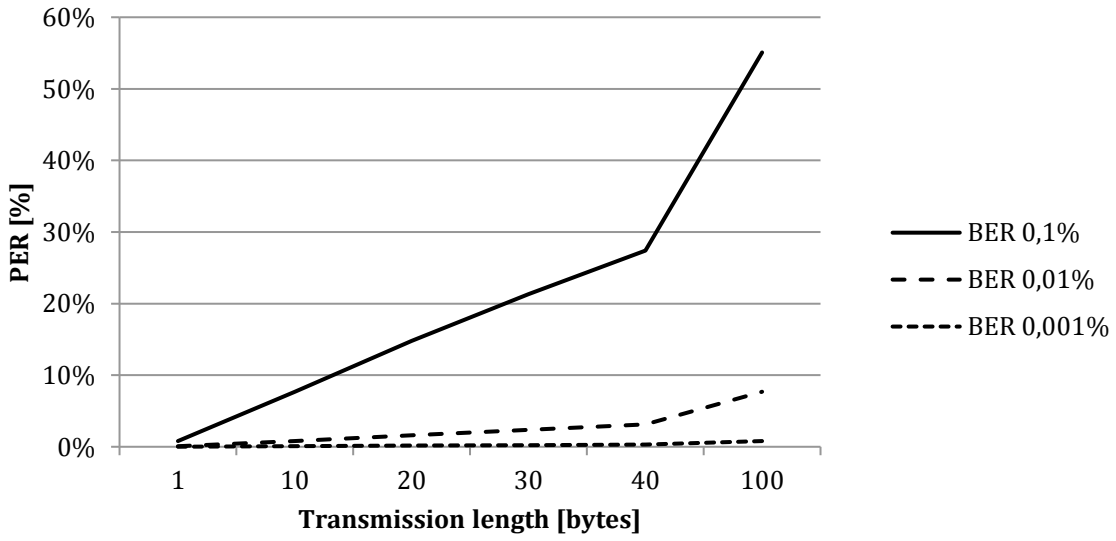


Figure 3-13 Packet error for different packet length for a given bit error rate.

For a slave's node packet to reach the master, the slave node must receive three packets, two allocation packets from the allocation slot and one packet from the bidirectional data slot followed by a successful transmission to the master node. This results in a combined probability of slave packet not reaching master ($P(slave\ data\ upload)$) of

$$P(slave\ data\ upload) = 1 - (1 - PER)^4 \tag{3-7}$$

which result in an exponentially increased probability of failure. For BER of 0.1% and packet length of 40 bytes, probability of failure will reach 72 % as shown in Figure 3-14. Therefore, when channel is approaching to the edge of the receiver's sensitivity, the communication will exponentially deteriorate.

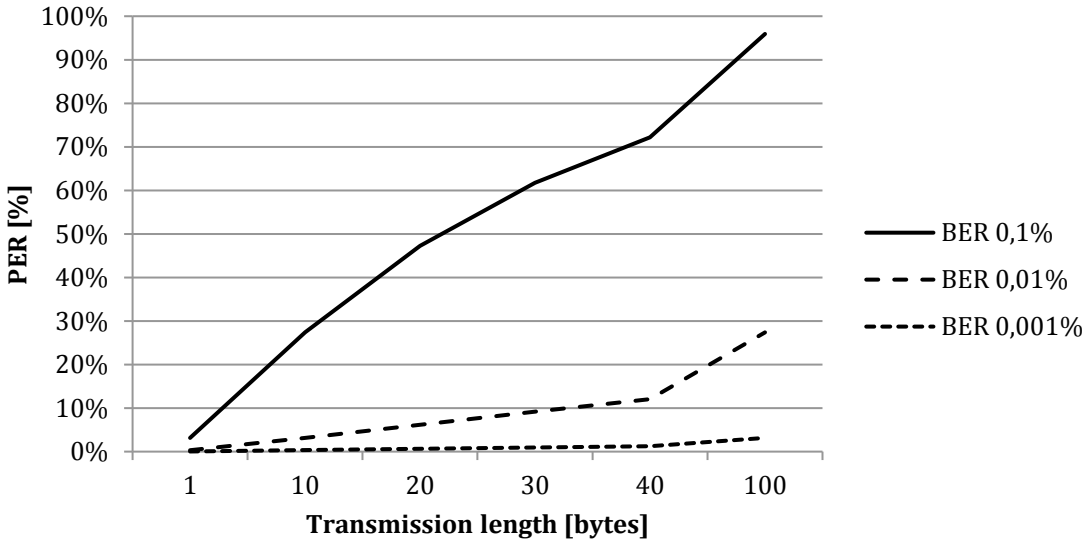


Figure 3-14 Probability of slave transmission failure for different packet length for a given BER .

The model shows that at a sensitivity where BER is 0.02% the slave's packet would need to be half the size of the allocation packets to have the same probability for a packet failure, as shown in Figure 3-15. In case where a large number of time allocation slots and master's node packet are received at the same time, and the slave node is unable to execute a successful transmission to the master node, the slave could limit the packet length to increase the probability of a successful transmission.

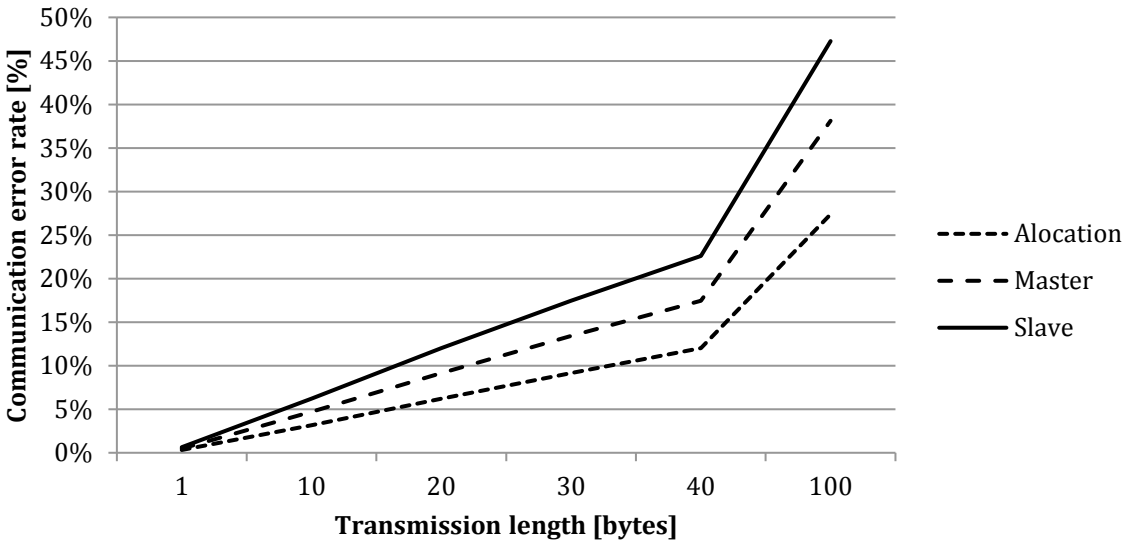


Figure 3-15 Error probability for allocation slot, master's node packet transmission to slave node and slave's node packet transmission to master node.

3.1.8 Synchronisation and error measuring precision

As described in 2.2.5 [TDMA communication and clock synchronisation] section, the prerequisite for successful wireless communication using TDMA MAC is that the receiver enters in the receiving state before the transmitter starts to transmit. The slave node must compensate for its own and for the master's clock error to guarantee that it would enter in receiving state before the master node. The slave node has to compensate by adding twice the maximal timing error in every frame (start and end) if it is unable to measure the frequency difference Δf between the master node's clock and its own clock frequency. The slave will observe the drift of $t_{SLOT\ START}$ relative to the its internal clock due to error between the two clocks as shown in Figure 3-16.

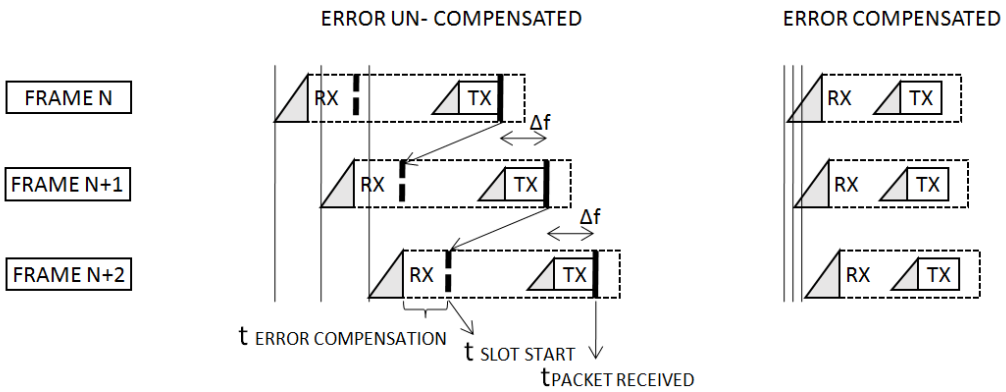


Figure 3-16 Drift of slot start from slave's perspective due to clock difference.

In the previously described method, the slave node synchronised internal time reference after it successfully received a packet from the master node. When a frame occurs without the slave node receiving a packet from the master node, it is not possible to re-synchronise the slave's clock and compensate the clock differential error. Packets may not be received from the master in three cases: if the slave node enters sleep mode and skips *N* frames, if the slave is out of range or due to noise in the communication channel. In such a case the slave node must add additional time slot ($t_{FRAME\ ERROR\ COMPENSATION}$), before and after time scheduled for packet receipt, for every frame in which the slave node did not receive a packet from the master, as shown in Figure 3-17.

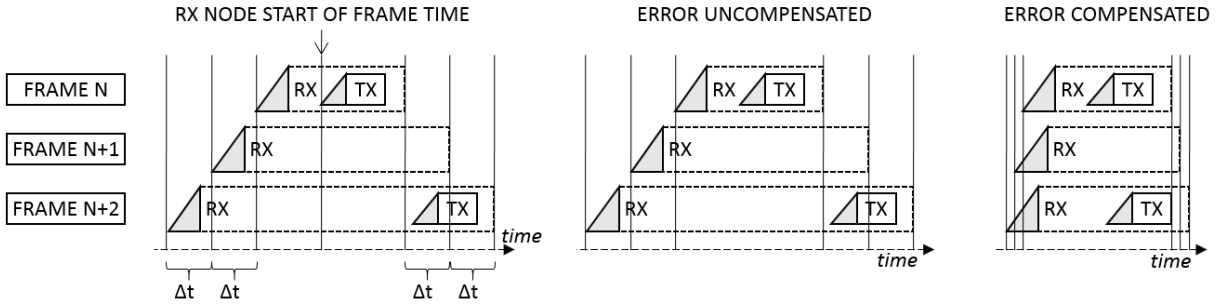


Figure 3-17 Effects of lack of synchronisation on the slave radio receive time.

As described in 2.2.6, Frequency error impact on wireless communication, with a frame length of 41 ms, the worst case scenario error after the first frame is 3.28 µs for a 16 MHz clock with 40 ppm clock frequency instability and 20.5 µs for a 32 kHz clock with 250 ppm clock frequency instability. After the 8th frame, this time error will increase to 26.2 µs for a 16 MHz clock and 164 µs for a 32 kHz clock. This increases the duration of slave node in receive state and consequently it increases its average power consumption. In terms of power consumption, the worst-case scenario is in case when the slave node tries to connect to the master node and does not receive a valid packet from the master node in the frames following the connection grant and before timeout is reached. The slave node cannot calculate the frequency difference and save power by reducing $t_{FRAME\ ERROR\ COMPENSATION}$. Since the slave node did not enter power save mode, it will continue listening for an allocation packet in every frame. The power consumption impact of the slave node's inability to compensate time error is shown in Figure 3-18. By the 128th frame (3 s) the error with clock frequency of 32 kHz is 3072 µs resulting in an increase of the slave node's average power consumption for an additional 768 µA. There is a possibility to reduce average power consumption of the slave node by listening only every fourth to 192 µA or every eight allocation frame to 96 µA.

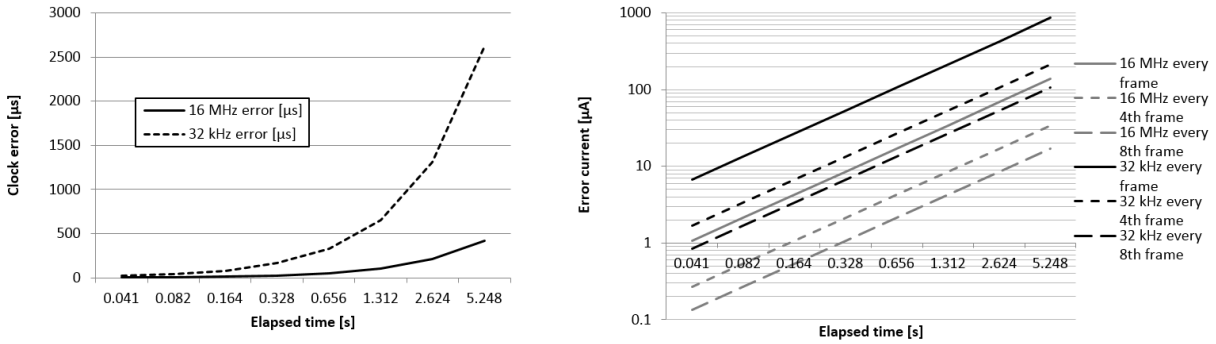


Figure 3-18 Cumulative time error impact on power consumption.

In order to minimise the aforementioned effects, it is desirable to measure the clock difference as soon as possible and compensate for the slave's clock difference relative to the master's clock. Continued measuring of short time intervals will not provide enough clock difference accuracy ($\Delta f_{accuracy}$) for the clock frequency difference as the accuracy is determined by elapsed time ($t_{elapsed\ time}$) and time of one clock cycle ($t_{measuring\ unit}$):

$$\Delta f_{accuracy} = \frac{t_{measuring\ unit}}{t_{elapsed\ time}} = \frac{t_{16\ MHz\ CLK\ tick}}{t_{elapsed}} = \frac{62.5\ \text{ns}}{t_{elapsed}} \tag{3-8}$$

Successful connection to the master node by the slave node implies that the slave node received 2 packets from the master node - ping and allocation packets. The time between receiving 2 packets is 750 µs (0.0156 frame time) which results in a theoretical accuracy of 83 ppm. Since there is jitter in the measurement process, in 4 clock cycles it results in an effective error of 333 ppm which is larger than the 32 kHz clock instability over the full operating range. Figure 3-19 shows the achievable relative clock accuracy between master and slave node depending on the time between two received packets. It may be noted in Figure 3-19 that it is possible to observe a relative clock accuracy of 5 ppm after the slave node successfully receives two allocation slots.

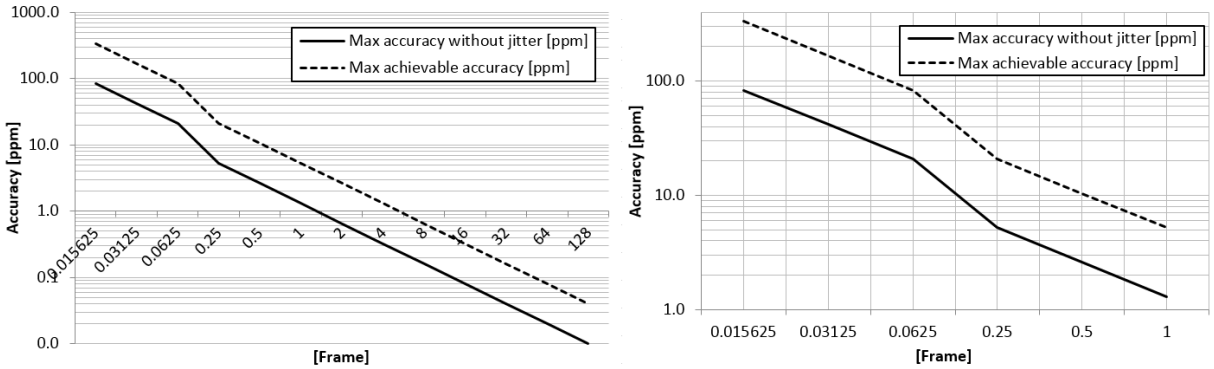


Figure 3-19 Accuracy of measurement of the difference between master and slave node clock frequency as a function of time (in frame fraction/number).

Improved relative clock accuracy between the master node and the slave node, results in reduced accumulated relative clock error when the two nodes do not exchange packets for a extended number of frames. This reduces power consumption since the additional time for which the slave node needs to be in the receiving state is reduced. By achieving a relative clock accuracy of 5 ppm in one frame using a crystal oscillator with 40 ppm absolute frequency accuracy, it is possible to reduce average power consumption due to clock error from 122 µA to 15 µA (before connection timeout occurs) as shown in Figure 3-20. Although it is possible to achieve even greater relative accuracy between the master's and slave's clock, it may be possible that the clock instability is greater than the achieved relative measurement accuracy. Therefore, measurement accuracy of clock difference should be in range of clock instability.

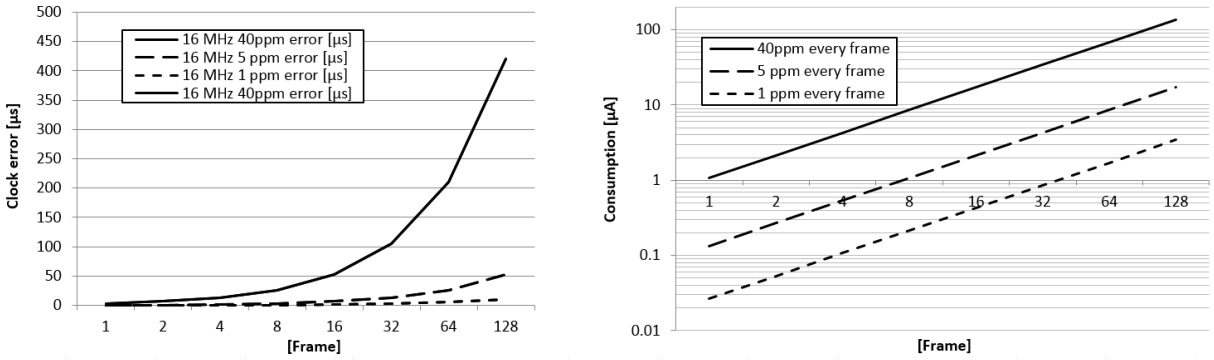


Figure 3-20 Cumulative time error impact on power consumption depending on relative clock accuracy.

Upon slave node successfully receipt of two consecutive allocation packets from the master node, the difference in clock frequency between the two nodes and their stability determine the increase of a slave node receiving state power consumption beyond theoretical values.

3.1.9 Expected power consumption envelope

To simplify power consumption model, currents in power consumption model will be normalized to an average current of that component as it would happen once in a second. This simplifies calculation for different operating scenarios. Average normalized current is multiplied by the number of occurrences of that component in one second.

Based on the WOLC protocol MAC, power consumption changes during a send-receive cycle has a specific pattern. For the master node, the pattern consists of pre-slot radio and data preparation, radio ramp up, transmit packet, preparation for the response packet, ramp up to the opposite radio functionality, receive packet and process packet. The current consumption (I_{WOLC}) is defined by

$$I_{WOLC} = I_{radio} + I_{time\ \&\ clock} + I_{processor} \tag{3-9}$$

where $I_{processor}$ is the processor core current, $I_{time\ \&\ clock}$ is processor time keeping and clock current and I_{radio} is radio current. The radio average current component is the sum of all the radio currents flowing in periods when radio is active, i.e. during allocation slots, bidirectional slots, slot guard time before (before and after) and time due to clock error. The radio total current consumption during a cycle is equal to

$$I_{radio} = I_{alloc\ slot} + I_{bi-slots} + I_{guard\ time} + I_{time\ error} \tag{3-10}$$

where $I_{alloc\ slot}$ is average current of allocation slot, $I_{bi-slots}$ is average current of bidirectional slot, $I_{guard\ time}$ is average current during guard time and $I_{time\ error}$ average current because of timing error. When there are multiple bidirectional slots ($N_{bi\ slot}$) frame consumption envelope will be defined as

$$\begin{aligned} I_{radio} &= I_{alloc\ slot} + (N_{bi-slot} \cdot I_{bi-slot}) + \left(N_{slots} \cdot I_{guard\ time}\right) + I_{time\ error} \\ I_{radio} &= I_{alloc\ slot} + I_{guard\ time} + N_{bi-slot} \cdot \left(I_{bi-slot} + I_{guard\ time}\right) + I_{time\ error}. \end{aligned} \tag{3-11}$$

where N_{slots} is number of allocated slots in the frame.

The time tracking and clock source current component encompass four components

$$I_{time\ \&\ clock} = I_{32\ kHz} + I_{XOSC\ wakeup} + I_{16\ MHz} + I_{timer} \tag{3-12}$$

where I_{32kHz} is 32 kHz clock current, $I_{XOSC\ wakeup}$ is 16 MHz clock current during wake-up, I_{16MHz} is 16 MHz oscillator driving current (HFCLK) and I_{Timer} is 1 MHz timer. The 32 kHz clock oscillator running current is 1 µA and the 1 MHz timer running current is 4 µA. Since the

1 MHz timer running current is 100-10,000 smaller than other currents, it will be not included in the model. As per previous analysis, 16 MHz clock source will stop if there is more than 1.5 ms between periods where clock is required. If the time difference between the end of the allocation slot and start of the allocated slot is greater than 1.5ms, additional 16 MHz wake-up current will occur. If this is not the case only one occurrence of the 16MHz wake-up current will occur. The current consumption of the 16 MHz clock is proportional to the number of slots in frame. The total time and clock current ($I_{time\ \&\ clock}$) is

$$I_{time\ \&\ clock} = I_{32\ kHz} + \left(N_{wakeup} \cdot I_{XOSC\ wakeup}\right) + (1 + N_{slots}) \cdot (I_{16\ MHz} + I_{16\ MHz\ guard\ time}) \quad (3\text{-}13)$$

where N_{wakeup} is total number of 16 MHz clock oscillator wakeup times, $I_{16\ MHz\ guard\ time}$ is guard time current, $I_{16\ MHz}$ is 16 MHz clock running current and $I_{32\ kHz}$ is 32 kHz clock running current. Wake-up current of 16 MHz oscillator $I_{XOSC\ wakeup}$

$$I_{XOSC\ wakeup} = \frac{(I_{start\ XOSC} \cdot t_{start\ XOSC}) + (I_{run\ XOSC} \cdot (t_{start\ X16M} - t_{start\ XOSC}))}{t_{frame}} \quad (3\text{-}14)$$

is composed of $I_{start\ XOSC}$ initial spike current during start of the 16 MHz oscillator, $I_{run\ XOSC}$ is run 16 MHz oscillator average current during oscillator start debouncing, $t_{start\ XOSC}$ is spike duration, $I_{run\ XOSC}$ is oscillator debounce period and t_{frame} is the duration of the frame.

During bi-directional slot the processor is not entering the sleep mode as the inactivity period is shorter than 1.5 ms. This results in a processor current ($I_{processor}$)

$$I_{processor} = (1 + N_{slots}) \cdot I_{core\ active} \quad (3\text{-}15)$$

proportional with number of slots N_{slots} where $I_{core\ active}$ is microcontroller processor core active current.

Summing of all power consumption elements will result in a current consumption

$$I_{total} = I_{XOSC\ wakeup} + (1 + N_{slots}) \cdot \left(I_{radio\ guard\ time} + I_{16\ MHz\ guard\ time} + I_{processor}\right) + I_{alloc\ slot} + N_{slots} \cdot (I_{bi-slot} + I_{16\ MHz}) + I_{time\ error} \quad (3\text{-}16)$$

where $I_{alloc\ slot}$ is the average current for an allocation slot. Power consumption components are shown in Figure 3-21 with a resulting current consumption pattern. The slave node will have a similar pattern, as only transmit and receive will change positions. Additional to

master/slave pattern, slave node will have additional guard period before the bidirectional slot start time.

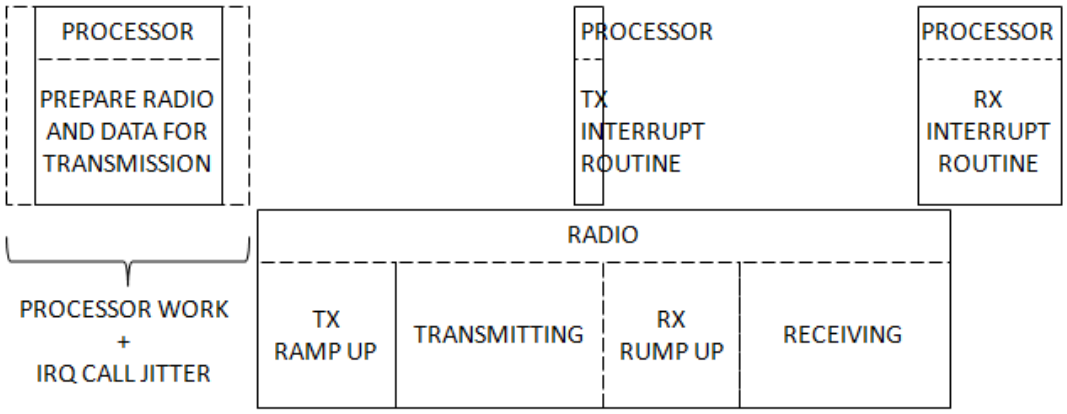


Figure 3-21 Power consumption components in bidirectional master slot.

In order to simplify the analysis and comparison of the power consumption model for different configurations such as speed and transmitted data, the power consumption model is transformed. From the model, defined as the sum of all current components,

$$I_{WOLC} = I_{XOSC\ wakeup} + (1 + N_{slots}) \cdot \left(I_{radio\ guard\ time} + I_{16\ MHz\ guard\ time} + I_{processor}\right) + I_{alloc\ slot} + N_{slots} \cdot (I_{bi-slot} + I_{16\ MHz}) + I_{time\ error} \quad (3\text{-}17)$$

the constant per frame power consumption component $I_{slot\ const}$ will be defined for a set data rate

$$I_{slot\ const} = I_{XOSC\ wakeup} + 2\left(I_{radio\ guard\ time} + I_{16\ MHz\ guard\ time} + I_{processor}\right) + I_{alloc\ slot} \quad (3\text{-}18)$$

where $I_{alloc\ slot}$ is the average current consumption for an allocation slot. With the replacement of current elements with a single constant average frame current ($I_{slot\ const}$), the total average current per frame $I_{WOLC\ frame}$ is

$$I_{WOLC\ frame} = I_{slot\ const} + I_{bi-slots} + I_{16\ MHz} + I_{time\ error} \quad (3\text{-}19)$$

where $I_{bi-slots}$ is the average current during a bidirectional slot. Equation highlights the nature of the protocol with a constant consumption from allocation slot regardless of the number of bidirectional data slots. From Table 3-1, a 1.4 µA difference between the slot transmitting 31 bytes of user data and the slot only maintaining the link is visible. The difference is minimal as

the radio is in ramp-up for 260 µs and transmitting and receiving for only 48 µs each, resulting in a total duration of 506 µs. The transmission of 31 bytes adds just additional 124 µs. Additionally there is a constant power consumption of $I_{XOSC\ wakeup}$, $I_{processor}$, $I_{alloc\ slot}$, $I_{radio\ guard\ time}$ and $I_{16\ MHz\ guard\ time}$ as described in the equation above.

Table 3-1 Power consumption components for frame using 2Mbps communication for slave upload slot and empty slot.

	Qty	*Upload slot*		*Empty slot*	
$I_{ALLOC\ SLOT}$	1	5.63 µA	38.4%	5.63 µA	42.7%
$I_{BI-SLOT}$	1	4.63 µA	31.6%	3.16 µA	24.0%
$I_{CORE\ ACTIVE}$	2	1.26 µA	8.6%	1.26 µA	9.5%
I_{16MHz}	2	0.71 µA	4.8%	0.71 µA	5.3%
$I_{XOSC\ WAKEUP}$	2	1.38 µA	9.4%	1.38 µA	10.5%
$I_{16\ MHz\ GUARD\ TIME}$	2	0.06 µA	0.4%	0.06 µA	0.4%
$I_{RADIO\ GUARD\ TIME}$	1	1.01 µA	6.8%	1.01 µA	7.6%
I_{TOTAL} **[µA]**		14,6		13,2	
$I_{TOTAL\ (POWER\ SAVE)}$ **[µA]**		44,7		40,2	
$I_{TOTAL\ 20\ FRAME/s}$ **[µA]**		357,9		322,0	

When a slower symbol rate is selected, transmission/receiving times increase and differences in power consumption between upload and empty packet become noticeable, as shown in Figure 3-22. In order to increase power efficiency, the node should maintain the connection at least possible incidence acceptable for the application and avoiding communication timeout. The trade-off of the increased power efficiency is increased latency, as data will queue for longer in the transmit buffer waiting for the communication frame. This is in line with the WOLC protocol and developed MAC, as it self-balances power efficiency and latency based on application requirements.

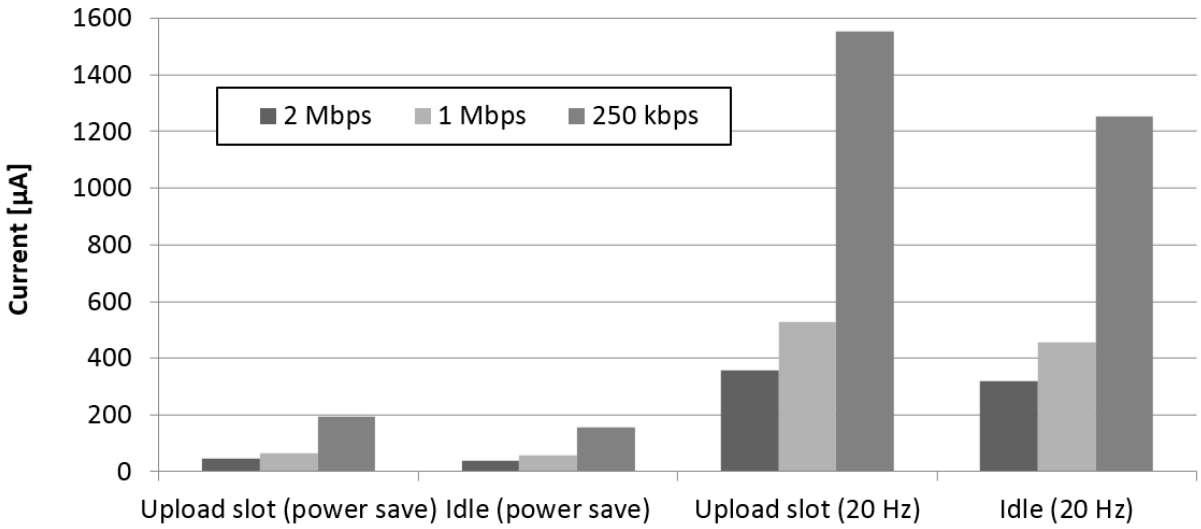
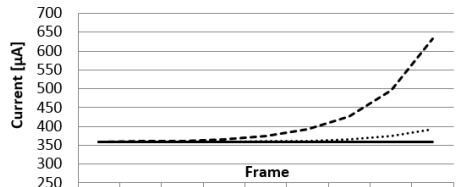
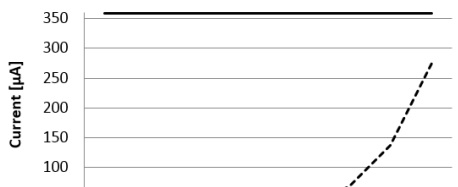


Figure 3-22 Power consumption using different symbol rate and frame rates.

Based on the described power consumption model and the previously outlined power consumption increase due to timing error, it is possible to predict how power consumption increases during connection establishment or communication in noisy environments. Should the node be unable to receive a packet after the first connection and allocation frame, the power consumption approaching timeout will almost double, as shown in Figure 3-23. This could drain the battery more quickly than expected. A possible optimisation for this scenario could be to decrease the frequency of attempting to communicate with the master node. Instead of trying to communicate every frame, the node could try to communicate e.g. in every 8 frames.



	1	2	4	8	16	32	64	128	256
Theoretical min consumption	358	358	358	358	358	358	358	358	358
Consumption 40 ppm error	359	360	362	366	375	392	427	495	632
Consumption 5 ppm error	358	358	358	359	360	362	366	375	392



	1	2	4	8	16	32	64	128	256
Theoretical min consumption	358	358	358	358	358	358	358	358	358
40ppm every frame	1.1	2.1	4.3	8.6	17.2	34.3	68.6	137.	274.
5 ppm every frame	0.1	0.3	0.5	1.1	2.1	4.3	8.6	17.2	34.3

Figure 3-23 Impact of absence of time synchronisation on power consumption.

3.2 High throughput packet exchange protocol for real time data in wireless sensor network in healthcare

3.2.1 Packet distribution in healthcare use case

As stated in chapter 3.1.1 Healthcare use cases, packet and messages distribution in healthcare environment implies some commonalities similar to wireless communication commonalities and implies either transmission of states or continuous stream of data. Custom protocol named flexyNET is developed during this research in order to support high throughput in wireless sensor networks. Optimizations of the protocol to achieve high throughput and facilitate transmission of continuous stream of data may be achieved by minimising protocol overhead and providing efficient routing. Minimising protocol overhead allows maximising usage of available bandwidth to transmit useful data. The method used to achieve minimisation of the protocol overhead is data reduction which may be achieved by exploiting context under which device is operating or creating group of related services for which data reduction can be put in place. From Figure 3-24 it is possible to group a few packets/messages routing services:

1. Packet needs to be distributed to specified address node,
2. Packet needs to be distributed to central routing/distributing/processing service,
3. Packet needs to be distributed to neighbouring node with a single hop,
4. Packet needs to be broadcasted through the network.

The first possible routing and delivery is comparable to standard IP routing protocol where packet/message needs to be routed through the network and delivered to a specified address node.

The second scenario is common scenario where packet/message of a certain type needs to be sent to dedicated central router/server/processor. A common example is an attempt to centrally collect electrocardiograms from all patients' telemonitoring devices. The full address length of four bytes for IPv4 and up to 16 bytes for IPv6 is exchanged by a single bit which flags that packet destination is intended for central network router. This change results in overhead reduction by 32 to 128 times. In a hospital network, all electrocardiograms with specific port may be routed to designated central node. This node may be responsible to deliver incoming messages to all interested network nodes or to a designated data processor. The

scenario avoids the necessity to include electrocardiogram control room address in the packet header. Only the source address is required to be included into the header of the packet.

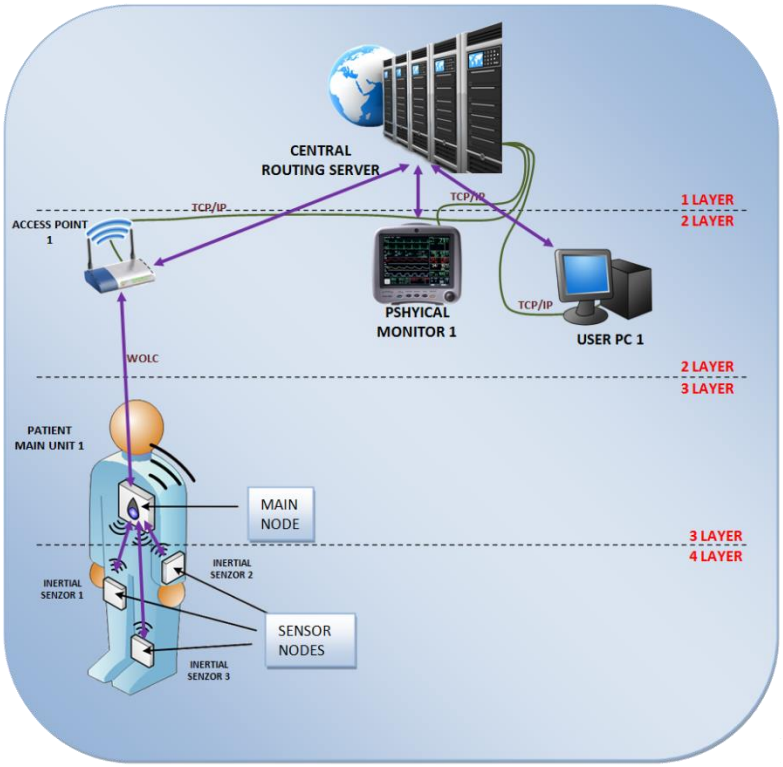


Figure 3-24 Healthcare environment with packet routing and delivery path.

In the third scenario, two neighbouring nodes are exchanging packets/messages. An example of this use case is a star network like a body sensors area network. In this case, every slave node is exchanging data with the master node. In both wireless and wired connection, two nodes are aware of each others addresses. When they are exchanging data, adding definition which describes this packet as single hop neighbour packets enables omitting both source and destination address from packet header. Packet routing protocol which is able to support the proposed method reduces header overhead from 8 bytes, for 4 byte address universe, up to 32 bytes for 16 bytes IPv6 address universe.

In the last mentioned scenario, a node in the network wants to broadcast the packet across the network. Examples of that scenario may be found in the device/service discovery or when a device is broadcasting its state in the network. In this scenario, since the intended destinations are nodes in the network, omitting of the destination address would reduce data needed to be added in the header of the packet by four to 16 bytes while keeping successful packet delivery.

3.2.2 Embedded resource constraints, trade-offs and optimisation

Small and inexpensive wearable devices usually have greater constrains on available RAM memory for a particular SoC used. As this SoC may have a total of 32k bytes of available RAM, support for receiving full TCP/IP packet often is not possible. Additional impact of having large packets over limited bandwidth communication channels is the effect of "traffic jam". Large and therefore slow to transmit packet on the top of the queue is slowing down all other smaller packets behind him. When wireless connectivity experiences packet loss and retransmission, available throughput will be temporarily reduced resulting in transmission delays for all packets in the transmit buffer. To minimise delivery delays for other smaller packets, protocol can either cancel the transmission of the bigger packet. Still the service which originally added packet in to the buffer can re-send it again. Protocol with low overhead allows packet size to be decreased. For a steady stream of data, shorter packets will be generated which take short time to transmit and will generate time multiplexing effect. Figure 3-25 illustrates comparison of packet size impact on the transmit schedule of packets inside transmission buffer. Although data to transmit is the same, delay seen by service A & B will be lower when shorter packets are being used. Effective delay for service C will increase. Presented method ensures sharing of the communication bandwidth across multiple services in real-time stream scenario. The required minimal supported packet size for flexyNET is chosen to be 256 bytes, as it will help to distribute bandwidth across services in a more uniform manner.

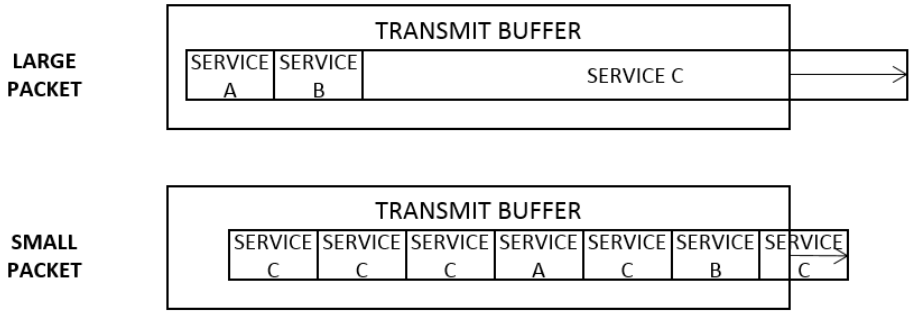


Figure 3-25 Packet size impact on the transmit schedule of packets inside transmission buffer.

3.2.3 Network layer header optimisations

Optimization requires scale down from general use cases to well defined scope. Clear scope definition offers opportunity for data reduction. Further data reduction opportunities can be found removing duplicate data or optimizing protocol components like error detection.

Developed network layer header optimization encompasses multiple optimization methods to achieve smaller header overhead and greater protocol efficiency; variable size network address universe, port/type data reduction, context aware address data reduction, multilayer optimisation approach for error detection and security encryption. Optimizations are focused for frequent real-time small to mid size packets/messages in a star topology use case.

3.2.4 Address and port universe optimisations

Not all applications require address space universe with 4.2 billion unique addresses as presented in previous sections. Developed protocol allows choosing network address universe in one byte increment up to a total of four bytes. When deploying new networks it is possible to choose from 256, 65,536 , 16 million up to 4.2 billion unique node addresses respectively. Even if four address byte universe is selected, protocol may optimise in some cases the length of addresses in the header. Protocol will allways setup source/destination address width to the lowest possible number of bytes capable to send the packet without loss of data. If a source/destination address value is less than 256, protocol will set source/destination address length of 1 byte. Careful address assignment which assigns addresses up to 255 to nodes which receive or send often data, can decrease header size and header overhead.

Similar to address space reduction, data reduction optimisation is applied to reduce port number from 65,536 totally possible ports down to 256, as it is unlikely that memory constrained embedded device will have code implementation to process more than 256 different calls.

3.2.5 Context based data reduction routing optimisations

The developed protocol supports context aware data reduction for four routing scenarios; packet delivery to neighbouring node, packet delivery to central node, packet delivery to exact address and broadcast packet distribution. Depending on the use case scenario it is possible to completely omit source and destination address from the packet header. Reduction on Network OSI layer does not impact functionality of higher layers and can achieve data reduction up to 8 bytes shown in Figure 3-26.

Address data size in header depending on use case

Routing	Source address length	Destination address length	Total bytes	Worst case scenario data reduction
Packet delivery to neighboring node	0	0	0	8
Packet delivery to central	1 - 4	0	1-4	4
Broadcast packet delivery	1 - 4	0	1-4	4
Packet delivery to exact address	1 - 4	1 - 4	2-8	0

Figure 3-26 Address data size reduction in packet header for IPv4.

Upon establishing of connectivity between the two devices on physical layer, they firstly exchange devices details on port 0x05 including their address and names ([0-2] MyAdress, [3] my NodeType, [4] myNodeName). This allows all following data exchange between neighbours to use reduced header.

In the case of sending packet to neighbouring node, protocol will omit source and destination address as it is not needed for a successful packet delivery. When the packet is received in the receiving node, network layer can automatically reconstruct both source and destination address for seamless usage by the upper layers. If upper layer support check and use of source and destination size as parameter, it is possible to omit the need to reconstruct the full packet and achieve additional computation and power consumption reduction.

As the neighbouring nodes know each other's addresses, sending node can always safely omit adding sender address in the packet header. When the neighbouring node receives packet without source address, it will attach sender's node address and forward to other connections in the network shown in Figure 3-27. This ensures data reduction for the first hop is always applicable and it is particularly beneficiary for power constrained wearable devices as they can omit most of the header data when transmitting data.

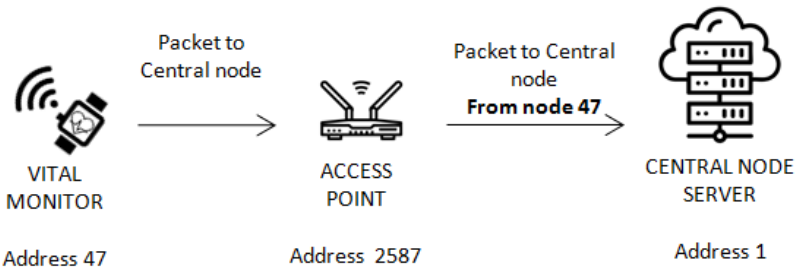


Figure 3-27 Always applicable data reduction of sender omitting packet source address.

3.2.6 Multilayer packet integrity & security optimisations

Multilayer optimisation of packet error detection takes in to the account communication methods described in section 2.1.3. Most protocols on layer two in OSI model like Wi-Fi, BLE and Ethernet use CRC as error detecting method, or protocols like Universal Asynchronous Receiver/Transmitter (UART) use reliable connections, enabling upper layers to reduce error detection. There is a notion that underlying protocol has error detection mechanisms adequate for the used medium and connection on which it operates, therefore the networking layer needs to detect only occasional errors.

As the aim of the protocol is to have low impact on available processor and memory resources, first complement 8-bit checksum is chosen as a default error detection method since it provides required error detection performance (Figure 2-4). In the scenarios where underlying layers do not provide substantial integrity check like Infrared Data Association (IrDA), optional CRC-16 error detection method is available to ensure data integrity. Two bit-s will be used to encode error detection method; 1st complement checksum or CRC-16.

Every packet will start with 0xAA hexadecimal value. This will trigger start of packet decoding with integrity check or enable resynchronisation on the receiver side upon communication interruption or packet corruption. Synchronization byte will be followed by variable header, port, data and error detection block shown in Figure 3-28. The smallest achievable packet size is 6 bytes for a packet which contains one byte for sync, 3 bytes for header, one byte for data and one for error detection.

Similar to error detection in which network layer is exploiting error detection from the link layer, developed protocol provides two security options which leverage security from underlying layers; no encryption when the whole network is using secure connection on link layer and secure channel encryption when there is need to strengthen the security. Cryptographic algorithm used in the protocol when security is enabled will be RC4. RC4 is chosen as encryption or decryption since it can be executed fast even when used platform does not have cryptographic engine using lookup table.

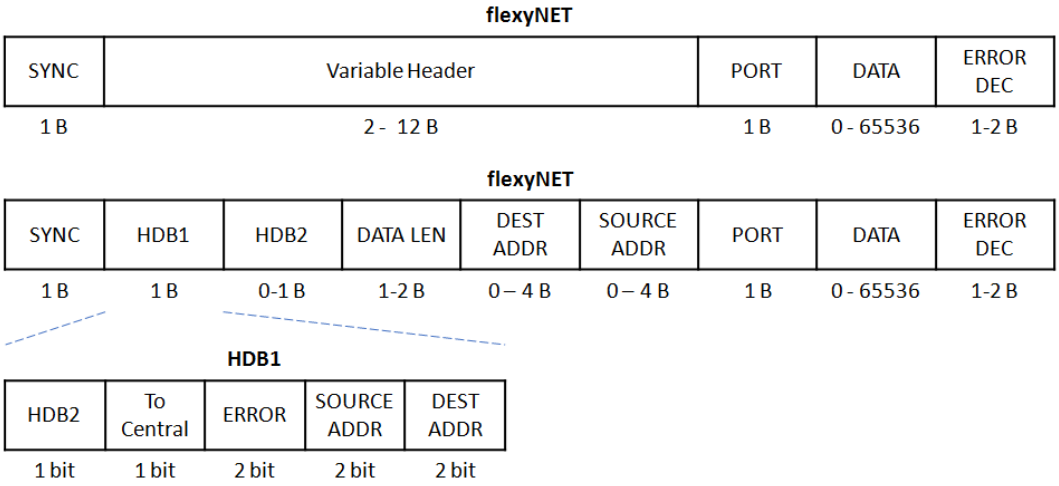


Figure 3-28 flexyNET protocol packet structure.

3.2.7 Data distribution optimisation

As nodes in the network may generate data which may be of interest to a bigger number of nodes, publish-subscription method is designed to minimise header size required to be sent for a successful distribution form the generating node.

Publish-subscription model is designed to work through the help of the central server node. As the central server is receiving updates from all nodes, when a new node joins the network, or disconnects, it can update distribution list. Upon establishing connection and exchanging node details, nodes interested in the content from other nodes may send subscription request packet to the central server node. Protocol support data reduction optimisation with one bit which marks central node as packet destination in the optimised flexyNET header. Packet delivered to central node is handed to central node's router. Router checks if the packet is for central server node. If so, it is forwarded to the routing layer which forwards to all subscribed nodes based on subscription to an address and port type. To minimise packet traffic in the network and especially towards resource constrained peripherals sensors, every subscription needs to provide source address, additionally to the port. This approach creates distinction between broadcasting packets which primarily should be used for device or service discovery across the network and subscription which is persistent one-to-many distribution mechanism from known devices or services.

As presented in 3.1.1, it is common in a healthcare network to have three or more layers resulting in two more packet hops until reaching the central node as shown in Figure 3-29. In a wireless network, it is reasonable to assume that a node which generates data and a node which consumes data could change their location in the network. As a node can reconnect in a different

part of the network, delivery of packets based on routing tables may suffer from slow update of tables due to registration packets increased latency due to channel congestion. Distribution of real-time content may have better chances of not suffering from packet being delivered to wrong part of the network when publish-subscription model is used. This is primarily the case since central server has central place in the network from which it is possible to distribute to any connected part of the network because all nodes report to it.

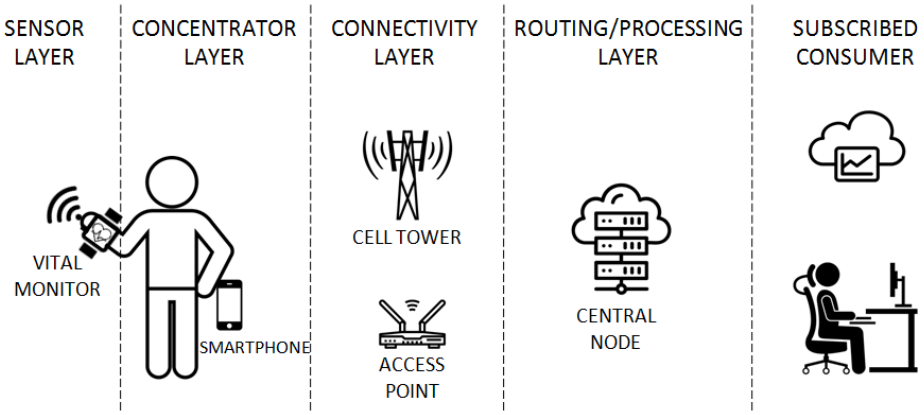


Figure 3-29 Multi layer nature of connectivity in healthcare network.

3.3 Publish-subscribe messaging protocol

Although the presented novel protocol will achieve smaller overhead and greater efficiency in many scenarios, often commercial implementations will impose use of well-known standards. This motivated research of a possible optimisation methods for standard publish-subscribe protocols with the aim to achieve level of efficiency as close as possible to the flexyNET protocol. Due to widespread support from different cloud providers [105] and platforms, our research was concentrated to MQTT protocol.

Since the overhead of the MQTT header and the topic can easily be several times larger than the useful payload, research on header optimization was focused in two directions: compatibility with existing protocols and maximal achievable optimization. Optimization is crucial to the link between the wearable node and the gateway since there are constrains in available bandwidth and power. The higher the amount of data which needs to be transmitted the higher power consumption is.

Common wearable devices are repetitive and post data of the same type. This means that certain topics will be used repeatedly when data are broadcasted/published. Since topics are human readable text, which from the development and maintenance perspective is better to

be longer and descriptive, their representation is not optimized. For example, in the case of a wearable topic:

"net_8a56bc72/user_723bf8ac/left_arm/heart_rate" and the payload "HeartRate:67",

the header is 8 times larger than the actual data payload.

3.3.1 First level optimisation

To overcome inefficiency presented in the previous section and to maintain a descriptive character of the topic, first level optimization focus on compliance with existing protocol by replacing text sections for an escape byte value. Escape byte value is character commonly not used. After establishing the connection, the device needs to send a packet of a type "publish" with the text to be replaced between two wildcards 0x81, as in

MESSAGE TYPE 0x30 (PUBLISH, Topic "optimisation/")
DATA: 0x81, "net_8a56bc72/user_723bf8ac/left_arm/heart_rate", 0x81

MESSAGE TYPE 0x30 (PUBLISH, Topic: 0x81)
DATA [16 Byte]: "HeartRate:67"

Wildcards are characters with a starting value of 0×81 and, for the example above, the topic may be replaced with a single character 0×81. In the development stage, the developer can determine which sections of text are repetitive and notify this to the MQTT gateway. The node can concatenate a list of text replacements with wildcards in the optimization packet. The receiver node, based on storage capacity, will confirm which wildcards are accepted. Whenever a packet is received and a wildcard is present in the topic, the wildcard will be replaced by a full text hence maintaining standard message processing.

3.3.2 Second level optimisation

As implementations of MQTT broker are also available as open source [106], if minor changes to the protocol are acceptable, it is possible to take stable source code implementation and add minor optimisations to the protocol. This enables deeper second level optimization which strips out completely the topic content from the header, thus removing the current

requirement of minimal 3 B (2 B length + topic "/"). This is achieved by introducing the 0×0A (new line) character as a delimiter between the topic and the payload. In order to allow further optimization and combining of wildcards between topics and payloads, the 0×03 (end of text) character is placed at the end of the text. To prevent packet misinterpretation, a new publish message type 0×00 is selected to be introduced for the second level optimized publish packet. For the above example, overhead is reduced from 62 B to a total data (topic + payload) length of 5 B with a use of a single wild card, as for example

MESSAGE TYPE 0x30 (PUBLISH, Topic "optimisation/")

DATA [Byte]: 0x81 + "net_8a56bc72/user_723bf8ac/left_arm/heart_rate" + 0x0A "HeartRate:" + 0x81

MESSAGE TYPE 0x00 (PUBLISH)

DATA [3 Byte]: 0x81+ "67"

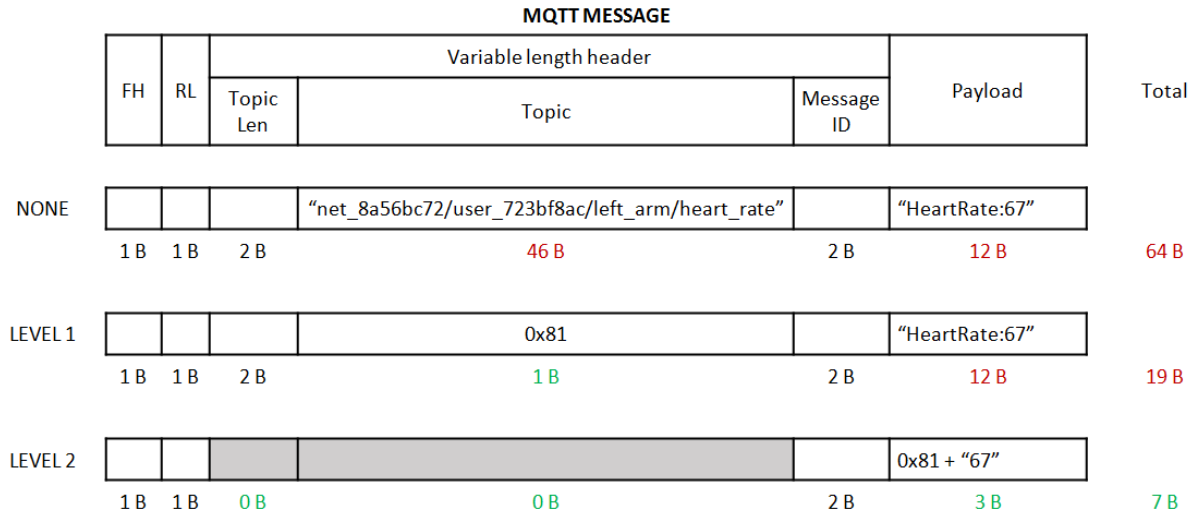


Figure 3-30 MQTT publish message with no optimization, level 1 and level 2 optimization.

An overview of packet content difference for different levels of optimization is illustrated in Figure 3-30. The proposed optimization of the MQTT variable header results in a protocol efficiency comparable to flexyNET or others strict byte-oriented protocols like BLE which uses profiles. Introducing a single message, with descriptions provided by wildcards, after the connection is established, removes the need to transmit full topic for all subsequent messages while maintaining complete descriptiveness, packet processing and human

readability of MQTT. The provided example resulted in a reduction of overall packet size by more than six times. Improved efficiency directly reflects on either extending battery life or increasing the quantity of application data which is possible to be sent through a communication channel.

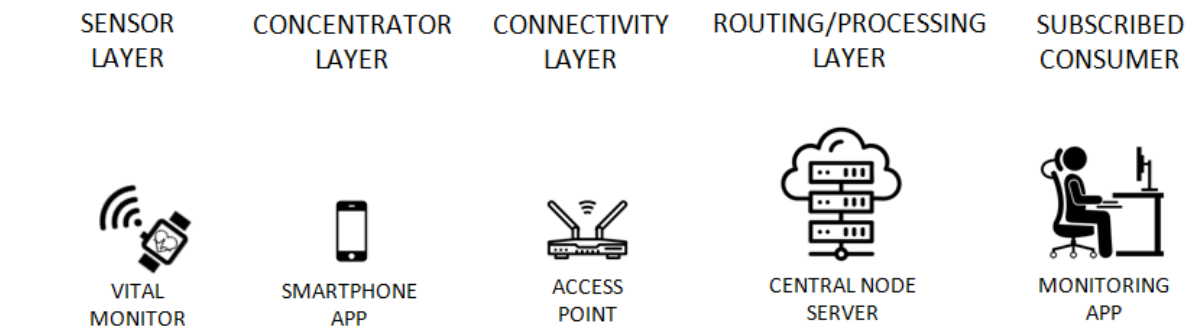
4 Architecture of an energy efficient wireless system for long term continuous data acquisition and monitoring and its validation

Two test environment setups were prepared for validation purposes. The first test environment is based on custom developed hardware and software. The second test environment is based on off the shelf devices and uses standard wireless protocol.

4.1 Proprietary platform

The first test environment consists of custom developed platform with custom developed embedded devices and custom developed software applications as shown in Figure 4-1. Embedded devices are; peripheral wearable node, central wearable node and WOLC access point. Software applications are access point management application, central server application, monitoring application and signal generator application.

The environment uses presented flexyNET as packet distribution protocol across all link layer protocols: WOLC, UART, USB and TCP/IP. WOLC is used as wireless communication protocol.



RTOS	ANDROID	RTOS, WINDOWS	WINDOWS	WINDOWS
C	JAVA	C, .NET, C#	.NET, C#	.NET, C#
flexyNET, WOLC	flexyNET, WiFi, TCP/IP	flexyNET, WOLC, USB, TCP/IP	flexyNET, TCP/IP, WiFi	flexyNET, TCP/IP
nRF51822,nRF51422 LPC1347, nRF24L01		LPC1347, nRF24L01		
2.4 GHz ISM radio, ECG/EMG, QRS detector, 3-axis inertial sensors, microSD storage, Audio codec, ADC, GPIO, UART...		2.4 GHz ISM radio USB 2.0		

Figure 4-1 Custom developed research platform.

The platform backbone is based on TCP/IP communication through usage of central server shown in Figure 4-2. Central server is acting as a central node in the star configuration network responsible for: incoming TCP/IP socket connection authentication, authorisation, routing all flexyNET packets and provide book keeping of subscription list. All other peripheral nodes in the network connect via TCP/IP to allow usage of standard network infrastructure like Internet or local networks. A common communication layer across the whole network is flexyNET protocol. flexyNET packets are encapsulated inside TCP/IP packets. Central server is written in C# language using .NET framework.

Figure 4-2 Central server application with a list of connected nodes, access points list and subscription list.

Connectivity layer acts as a bridge between platform's network and wearable devices. Custom developed access point hardware provides connectivity to the wearable device using WOLC protocol. Access point hardware is custom developed board based on LPC1347 microcontroller and nRF24L01 radio transceiver. Through USB connection it communicates to the access point application. The access point application runs on windows machine. One side of access point application is connected to access point hardware through USB and on the other side to the platform network using TCP/IP. Figure 4-3 outlines developed access point hardware and windows application. As per Figure 4-1 access point application is written in C# language using .NET framework. Access point hardware is written in C and runs on top of real-time operating system CMSIS-RTOS.

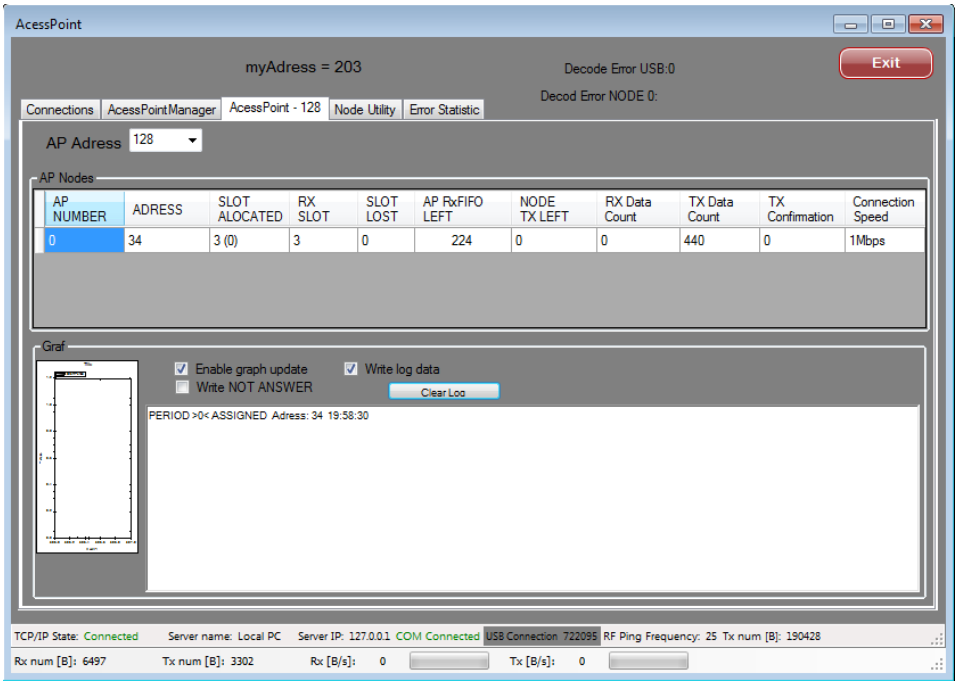


Figure 4-3 Connectivity layer, access point application.

At the sensor layer, two wearable devices where used to test the developed wireless and packet protocol. The research started on device with LPC13xx microcontroller paired to nRF24L01 wireless chip. Nordic family fronted chips were selected since they offer data rate of 2Mbit/s to 250kbit/s over the air. Later in the research device with nRF51822 and nRF51422 were developed due to small form QFN package with integrated 2.4 GHz wireless frontend and ARM Cortex-M0. The nRF51 family provides also software package support for BLE and ANT protocol. The nRF51 family offers an advanced programmable internal logic which facilitates implementation of custom wireless protocol and minimise power consumption. Figure 4-4 shows developed sensor layer devices.

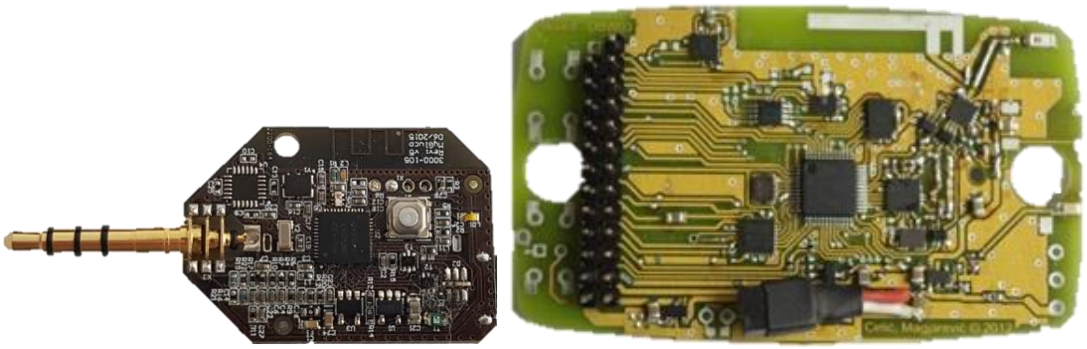


Figure 4-4 Sensor layer devices.

Monitoring application is used to process and visualize ECG data coming from the wearable node. Upon connecting to the central server/node, monitoring application send subscription request to the central node to receive stream of real-time ECG measurements from the wearable device. The received data is processed in QRS detector and RR peak filer. QRS detector provides patients heart rate, while RR peak filter is used for breathing detection. Application is written in C# language using .NET framework and communicates with central server thorough flexyNET protocol encapsulated in TCP/IP. Figure 4-5 shows the application connected to the server and receiving and analysing ECG sensor data.

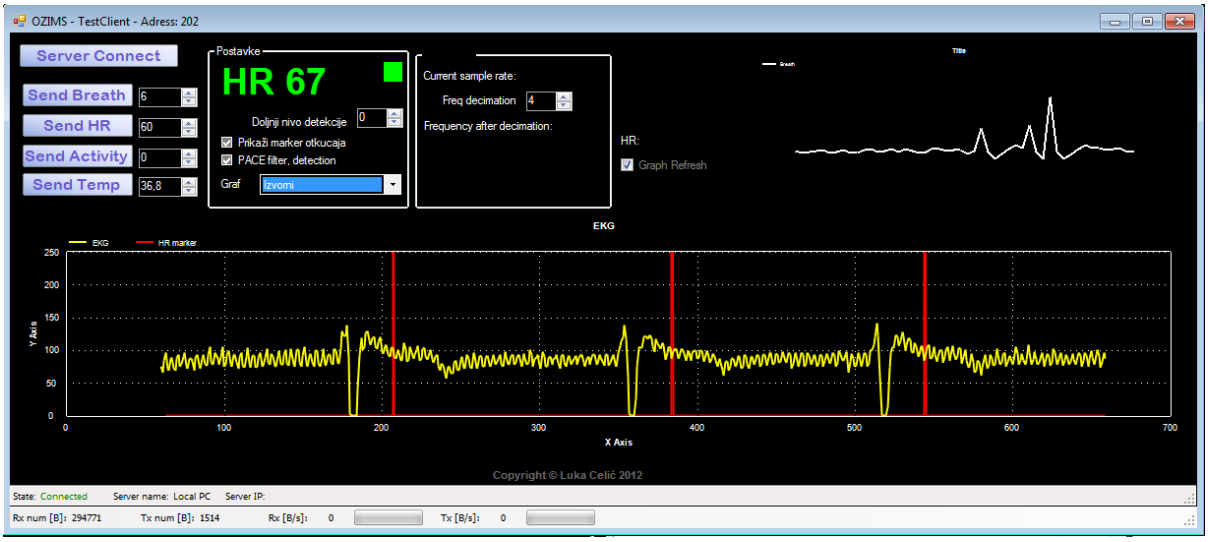


Figure 4-5 Real time ECG monitoring application.

In order to have testing repeatability, feature is developed on wearable node which may on demand store all outgoing packet towards the network to a local microSD drive. Using developed signal generator application, it is possible to reply in a controlled environment packets previously stored on wireless node microSD card. This application feature ensures consistency of results when testing flexyNET protocol or other application or network

component performance. The application is written in C# language using .NET framework and communicates with central server thorough flexyNET protocol encapsulated in TCP/IP. Figure 4-6 shows application connected to the server and receiving and analysing the ECG sensor data.

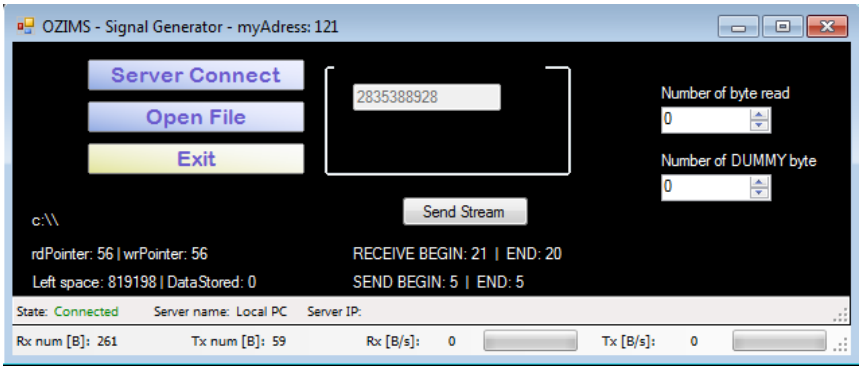


Figure 4-6 Signal generator application.

4.2 Validation of energy efficient wireless communication protocol

4.2.1 Achieving satisfactory time accuracy with available compute resources

In previous sections we outlined the importance of time and frequency accuracy to achieve reliable wireless communication. Since 32 kHz clock (LFCLK) consume only 1 µA when active, it is suitable to be used as always active clock. The 16 MHz clock will be powered on demand. One clock cycle of LFCLK is exactly 30.517,578,125 µs which is to coarse to measure relative error of 16 MHz clock frequency between master and slave node. The 16 MHz clock is regularly halted for *N* number of LFCLK cycles, absolute time needs to be kept without introducing errors. Counting round value of 30 µs for every LFCLK introduces 1696 ppm error in time keeping. Since it is not possible to avoid errors, acceptable error level should be chosen. Total error introduced by the arithmetic operations is set to be lower than 1 ppm. This means that 7 significant digits or greater precision needs to be maintained across arithmetic operations.

Accurate time counting is achievable using either floating point arithmetic or fixed point arithmetic. Floating point arithmetic operation may take up to 40 times longer comparing to equivalent fixed point arithmetic operation. As protocol events may shift states in hundred of µs at 2 Mbit/s, floating point arithmetic operations would not be calculated in required time. Therefore, fixed point arithmetic will be used.

Whenever there is more than 1500 µs pause before the next radio activity, high frequency clock will be stopped. Conversion of sleep time (t_{sleep}) in to the number of sleep

cycles ($N_{LFCLK\ sleep\ cycles}$) of LFCLK frequency (f_{LFCLK}) is needed. High frequency clock will be stopped for a time slot

$$N_{LFCLK\ sleep\ cycles} = \frac{t_{sleep} \cdot f_{LFCLK}}{f_{timer\ CLK}} = \frac{t_{sleep} \cdot 32{,}768}{1{,}000{,}000} \tag{4-1}$$

where $f_{timer\ CLK}$ is timer clock frequency of 1 MHz. Interim multiplication of t_{sleep} and f_{LFCLK} would exceed 32-bit integer value, as the sleep time can be up to 656,000 µs since base unit is one µs. Therefore a 64-bit integer needs to be used. The implementation code using C language is

```
uint64_t lfclk_sleep_clock =  (   (  ((uint64_t)(sleep_time)) *  RTC1_CLK_FREQ ) / TIMER0_CLK_FREQ );
```

The equation (4-1) calculates for how many low frequency clock a high frequency clock will be inactive. Since the node internal time reference unit is one µs and it is not divisible with a low frequency clock period, remainder error will always exist in range from zero up to one µs. This division error is greater than the clock accuracy. Therefore, the actual sleep time has to be tracked with picoseconds precision

$$t_{sleep}\,[\text{ps}] = \frac{N_{LFCLK\ sleep\ cycles} \cdot 10^{12}}{f_{LFCLK}} \tag{4-2}$$

To simplify time tracking and computing, low frequency clock sleep interval is divided in to whole number, microsecond sleep component ($t_{\mu s\_sleep}$)

$$t_{\mu s\_sleep}\,[\text{us}] = t_{sleep}\,[\text{ps}] \,/\, 10^6 \tag{4-3}$$

and a division reminder error ($t_{reiminder\ error}$)

$$t_{reiminder\ error}[\text{ps}] = t_{reiminder\ error}[\text{ps}] + t_{sleep}[\text{ps}]\ \%\ 10^6 \tag{4-4}$$

kept in picosecond precision. Division reminder error is incremented with the result of the modulo operation. The above equation results in implementation code

```
uint64_t sleep_time_ps
        = (rtc_sleep_clock * SECONDS_TO_USECONDS * USECONDS_TO_PSECONDS) / RTC1_CLK_FREQ;
uint64_t sleep_time_us
        = sleep_time_ps / USECONDS_TO_PSECONDS;
uint64_t sleep_time_remaining_ps
        = sleep_time_ps - (sleep_time_us * USECONDS_TO_PSECONDS);
sleepTotalError_ps
        += sleep_time_remaining_ps;
```

for which measurement showed excess processor core active time of 500 µs. The analysis of the excess processor core active time was conducted by measuring individual software subcomponent execution time. It was determined that individual 64 bit integer divisions, in the code above, could take from 224 up to 264 µs as shown in Figure 4-7. This resulted in 57 µA of excessive average power consumption or 11% of total power consumption in 1 Mbit/s full frame speed communication due to additional 700 µs in which processor calculates sleep time. Computation optimisation was necessary to improve power efficiency.

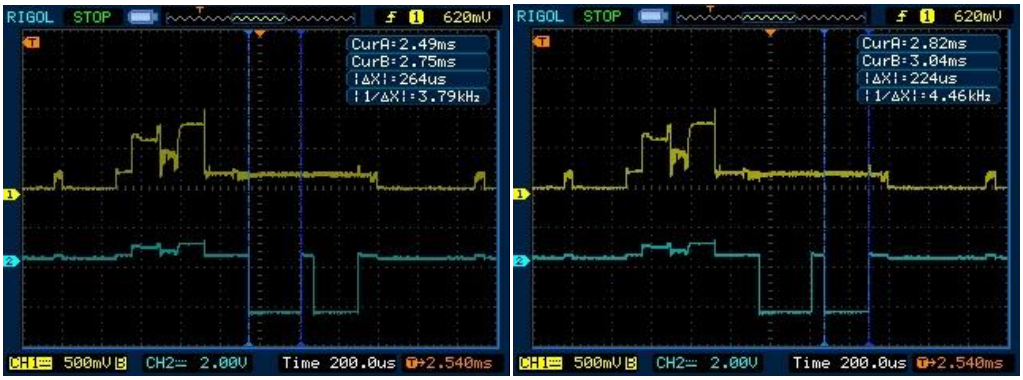


Figure 4-7 Time necessary to execute 64 bit division on nRF51 family microcontroller.

Analysis of available Cortex M0 processor commands [107] and execution time was conducted. Logical right shift is equivalent to division by a power of the radix 2 and is executed in a single cycle. Therefore, division of number X with number Y can be exchanged for X multiplied by a constant value and the result is shifted logically right by N constant number of bits. This is possible as previous equation has only one multiplication variable. Resulting replacement equation is

$$N_{LFCLK\ sleep\ cycles} = \frac{t_{sleep} \cdot f_{LFCLK}}{f_{timer\ CLK}} = t_{sleep} \cdot \frac{f_{LFCLK}}{f_{timer\ CLK}} \cdot \frac{2^x}{2^x} \tag{4-5}$$

$$N_{LFCLK\ sleep\ cycles} = \frac{t_{sleep} \cdot \frac{32{,}768}{1{,}000{,}000} \cdot 2^X}{2^X} = \frac{t_{sleep} \cdot CONST}{2^{N_{BIT\ SHIFT\ CONST}}}$$

where $2^{BIT\ SHIFT\ CONST}$ is a constant defined at compile time. The resulting equation using logical shift right operation is

$$N_{LFCLK\ sleep\ cycles} = \left(t_{sleep} \cdot CONST\right) \gg X_{BIT\ SHIFT\ CONST} \tag{4-6}$$

and it has only one fixed point multiplication and one logical shift right operation. Code changes using new equation resulted in decreased time per single calculation. Calculation execution time decreased from initial 224 µs - 264 µs, down to 3.4 µs. Disassembly analysis of the code showed no substantial processor instructions dropping from original 41 down to 33 instructions. The main execution difference is due to avoiding looping which is present in the division subroutine.

The secondary problem was choosing adequate shift right constant to keep introduced computing error below set level. The total computation error was set to be less than 0.1 ppm. There are two time computations, therefore maximal individual allowed computation error is 0.05 ppm. Minimal number of significant digits ($N_{significant\ digits}$) required to have computation error below maximal allowed ($Error_{max}$) of 0.05 ppm is

$$\begin{aligned} N_{significant\ digits} &\geq \log_{10}\left(\frac{1}{Error_{max}}\right) \\ N_{significant\ bits} &\geq \log_2\left(\frac{1}{Error_{max}}\right) \geq 24.25 \end{aligned} \tag{4-7}$$

The bigger the constant value ($CONST$), the lower number of bits (N_{bits}) is required

$$N_{bits} \geq \log_2\left(\frac{1}{Error_{max}}\right) - \log_2(CONST) \tag{4-8}$$

Further by exploiting properties of logarithmic operations, the equation can be divided in to

$$\begin{aligned} 24.25 &\geq \log_2\left(\frac{multiplier}{divider}\right) + \log_2(2^{N_{BIT\ SHIFT\ CONST}}) \\ N_{BIT\ SHIFT\ CONST} &\geq 24.25 - \log_2\left(\frac{multiplier}{divider}\right) \end{aligned} \tag{4-9}$$

where $multiplier_{CONST}$ is multiplier constant and $divider_{CONST}$ is divider constant. The above equation exactly specifies constant value ($N_{BIT\ SHIFT\ CONST}$) for power of two multiplications and shift right required for a given multiplier and divider. In the case of the LFCLK sleep cycles formula, logarithmic value of divider is 1,000,000 and multiplier is 32,768 which results in -

4.93 bits. Since error is set to 0.05 ppm, resulting in to 24.25 bits, the required number of bits for multiplication and later logical shift right is 29.18. Precision is true for worst case scenario when the variable value is 1. As the variable in the LFCLK sleep cycles formula will be greater than 1500, it will further reduce computation error.

4.2.2 Clock stability measurements

As relative time accuracy between master and slave node is imperative for energy efficient communication, it was necessary to determine the achievable accuracy level in real life. Implementation of maintenance of the node's internal time reference provided satisfactory levels of error minimization, the remaining main source of error is clock stability.

Testing of slave node in motion clock stability relative to a static master node was carried out for various use case and acceleration loads. Relative clock stability between the master node clock and the slave node clock was measured to be on average 3 when nodes were not subjected to external acceleration. In the following test, slave node was mounted on wrist. The relative clock stability was recorded during subject running with the slave node. There were no changes observed in relative clock stability. In the second test scenario, the node was placed on the belt while the subject was walking. No changes in average relative clock stability was observed. In the third scenario, the slave node was shaken separately in all 3 axis with the hand. No change in average stability was observed. In the last test scenario, node was dropped from 1 m height several times to the floor while the node is active. Relative clock stability was decreased to 4 ppm with occasional maximal error of 15 ppm. Achieved relative clock stability due to vibration is shown on Table 4-1.

Table 4-1 Measured clock source stability for across activities.

Static node	**3 ppm**
Wrist mounted walk	3 ppm
Belt mounted	3 ppm
Hand shake in all 3 axis	3 ppm
1 m drop shock test	4 ppm ± 6 ppm
2 g tip over test	3 ppm
Power off/on cycle	3 ppm (absolute relative error change)

4.2.3 Processor core active time

Slave's processor core active time measurements was carried out to validate power consumption model and improve it if needed. Total processor active time for allocation slot was measured to be 72 µs, consisting of 32 µs after receiving first allocation packet and 40 µs after the second one, as shown in Figure 4-8. Additional 8 µs is spent on calculating next radio wakeup time. During data slot processor is active for 133 µs, 32 µs after receiving packet and 101 µs after packet transmission where preparation for next frame and sleep is carried out. Additional 32 µs is required to calculate wakeup values before HFCLK is turned off and nodes enters in to minimal power consumption state. Allocation outperforms estimation of 180 µs as optimization work was carried out. Optimization decreased initial total processor active time from 200 µs down to 72 µs by reducing the number of times data are copied in internal buffers. Coping of 32 bytes of data was measured to take 7.8 µs or 125 clock cycles. Data slot has increased processor active times compared to allocation slot as looping through 44 allocation slots results in frequent dump of instructions prepared in three stages pipeline processor core architecture.

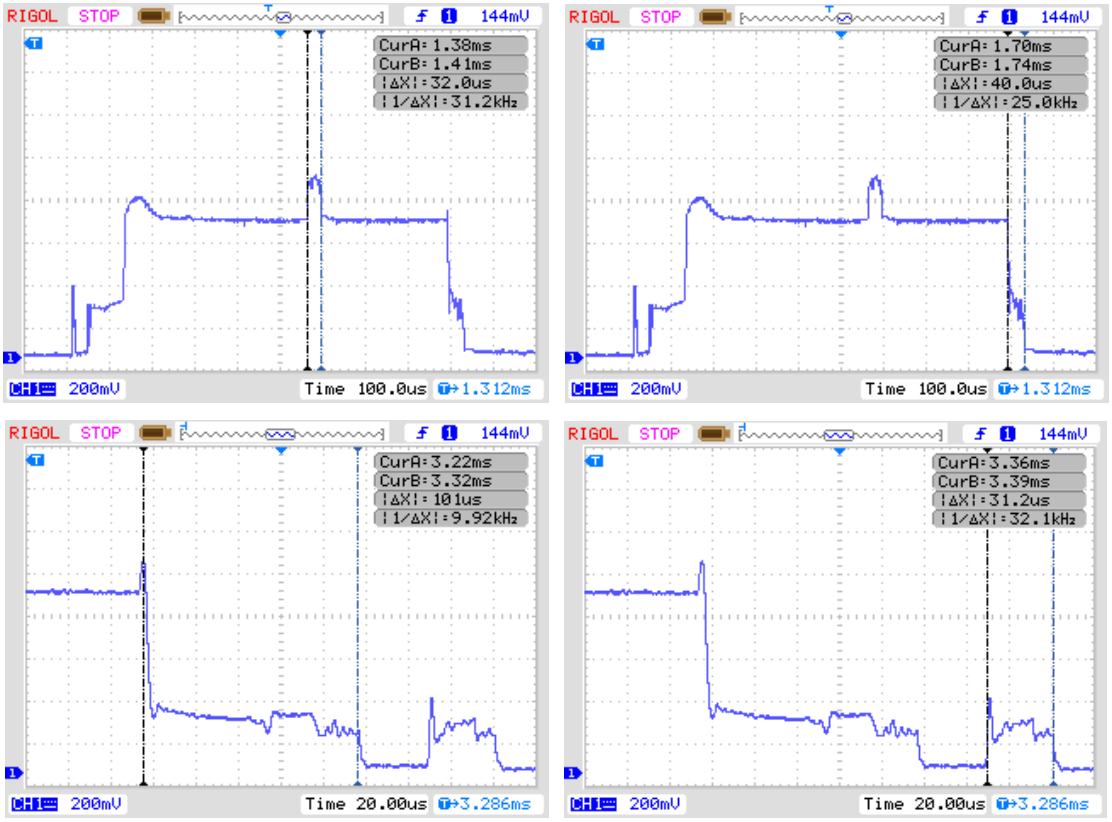


Figure 4-8 Processor active time; top allocation slot, bottom sleep prepare.

4.2.4 Automatic protocol power optimisation and pulse response

Measurements was carried out to validate wireless protocol theoretical latency and pulse response. A test function is written and enabled on the slave node to enable control of test scenarios. In the first test scenario, the wireless connection between master and slave node was in normal operational mode with communication on every frame. Figure 4-9 (left panel) shows captured pulse response to surge of 64 bytes of data. The connection was idle and 30 out of 64 bytes where transmitted in the first coming frame. In the following frame master node increased slot allocation number for the slave node. The remaining 42 bytes where transmitted in the following frame as three data slots were allocated to the slave node. For the first 30 bytes latency will be up to one frame length, or 41 ms. For the remaining bytes the latency will be from one up to two frames or from 41 to 82 ms.

In the second test scenario, the wireless connection was in power saving mode when the surge of data occurred. Similarly to the first test scenario, latency for the first 30 bytes in the transmit buffer is up to one frame, now 328 ms, and between one and two for the rest, 328 to 656 ms. Carried out measurements validated correct behaviour of power saving algorithm. Shown in Figure 4-9 on the left is one frame latency when number of allocation slots are increased. Shown in Figure 4-9 on the right is latency of eight frames when slave node changes communication state from power save mode to a normal full frame communication.

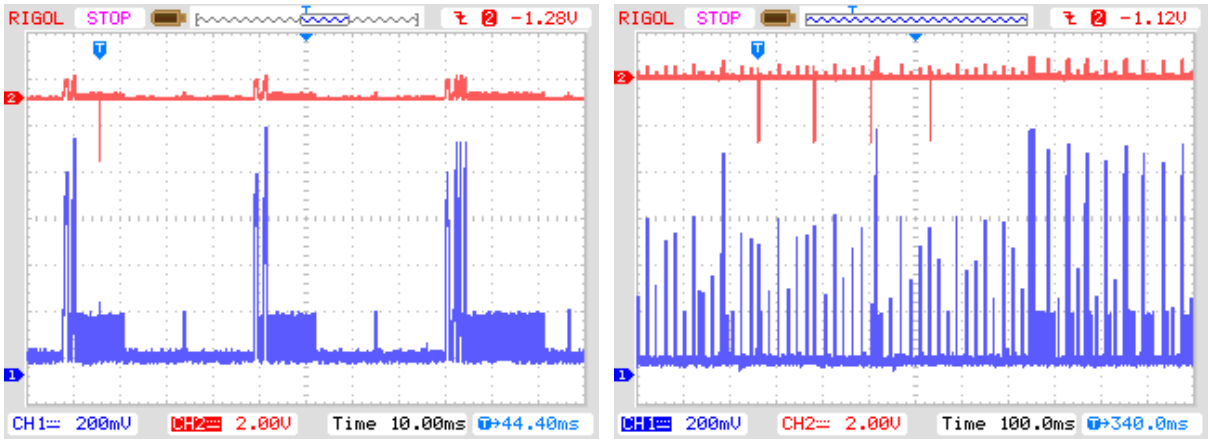


Figure 4-9 Wireless protocol latency and pulse response.

Further optimisation of the slot allocation algorithm minimised chances of data from the slave node to experience latency of two frames. If the total required bandwidth from all nodes is below channel bandwidth, the master node can allocate more sequential data slots to the slave nodes. Instead of the master node allocating minimally required one data slot to a single slave node, when the connection is idle, it can allocate additional unused data slots. For

example, instead of one allocated data slot, the slave node received allocation of five data slots. The slave node always transmit the amount of pending data in transmit buffer to the master node. In the event of the master node receiving packet from the slave with reported no additional data to be transmitted, even if there are more slot allocated to the slave node, master will not engage in next data slot for this node as there is no data to be transmitted. This effectively ensures the slave node can experience maximum of one frame latency for 5 data slots or 150 bytes of data.

4.2.5 Achieved time synchronization

Time synchronization Measurements started with measuring baseline clock stability. Relative clock stability was measured to be on average 3 ppm which translates to maximal 1 µs error when slave node communicates in power save mode. Measurement of the difference between the slave's node internal reference for start of receive time and the master's node start of transmit was carried out for allocation slot and data slot. Allocation slot has a 63 µs difference between starting of receiving and actual receive time shown in Figure 4-10 (left). Data slot difference is 20 µs, shown in Figure 4-10 (right), which is equal to the guard period. Upon the receipt of the allocation slot, the internal time reference of the slave node is re-synchronized with the mater's node. Presented method compensates relative clock difference and aligns data slot to the right point in time. The difference between slave's node expected start of master transmit time and actual master start of transmit is 43 µs. This results in clock error between the master node and the slave node of 131 ppm without clock error compensation. The communication was successful since a total of 75 µs guard time used in the testing. If the clock deviation was opposite in sign, communication would fail as transmitter would start to transmit before receiver starts to receive.

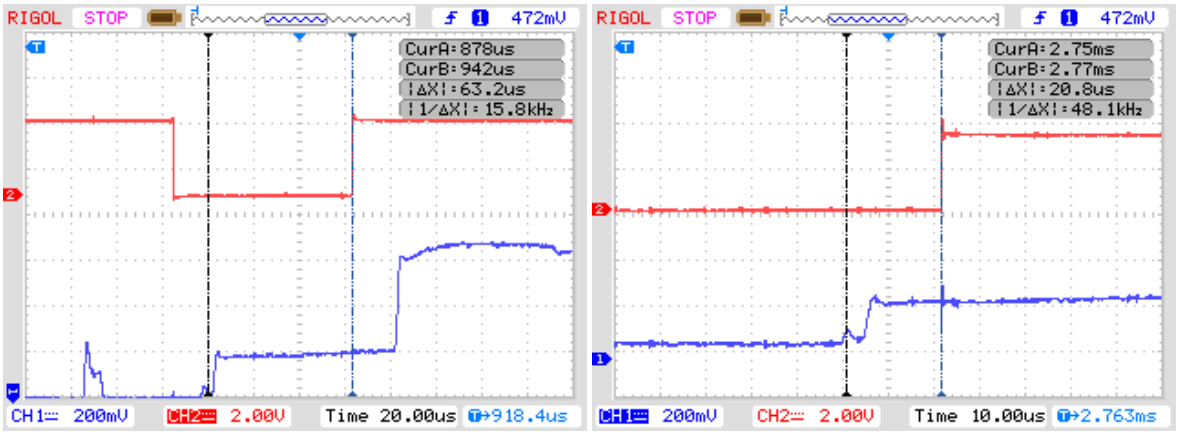


Figure 4-10 Relative time error resulting in drift of allocation slot (left) vs. data slot (right).

Upon enabling clock error compensation method, measurements confirmed start of transmit happening within 3 ppm of slave's expected time as show in Figure 4-11. To achieve higher clock error compensation beyond minimal timer interval of 1 µs, error compensation mechanism averages clock error from more than 20 last frames.

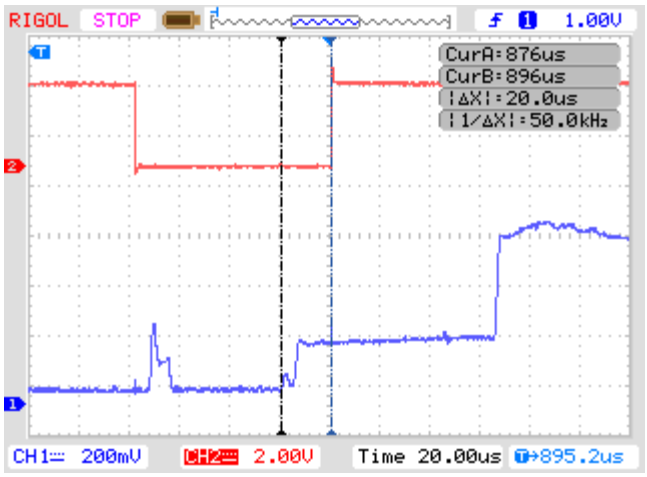


Figure 4-11 Transmitting start time matching receiving expected time after relative time error compensation functionality enabled.

4.2.6 Wireless protocol current measurements

Protocol power consumption validation needs to isolate external power consumption constituents such as low drop voltage regulators. The measurement of current was carried out by adding 0.5 ohm shunt resistance in series on an isolated power supply line powering the nRF51 through its supply pins as shown in Figure 4-12. Resistance is added by replacing inductor L3 in series (CIM05U102NC) shown in the schematic. The voltage drop over the 0.5

resistor is amplified using a voltage amplifier with resulting sensitivity of 0.05 mV/µA. Operating current of the slave node using WOLC protocol has a large dynamic range, form few µA up to 17,000 µA. Measuring the current consumption using oscilloscope and a shunt resistor has limited accuracy and is used to validate power consumption model based on observed pattern duration and values. Absolute average current is measured using LC filter with low cut off frequency.

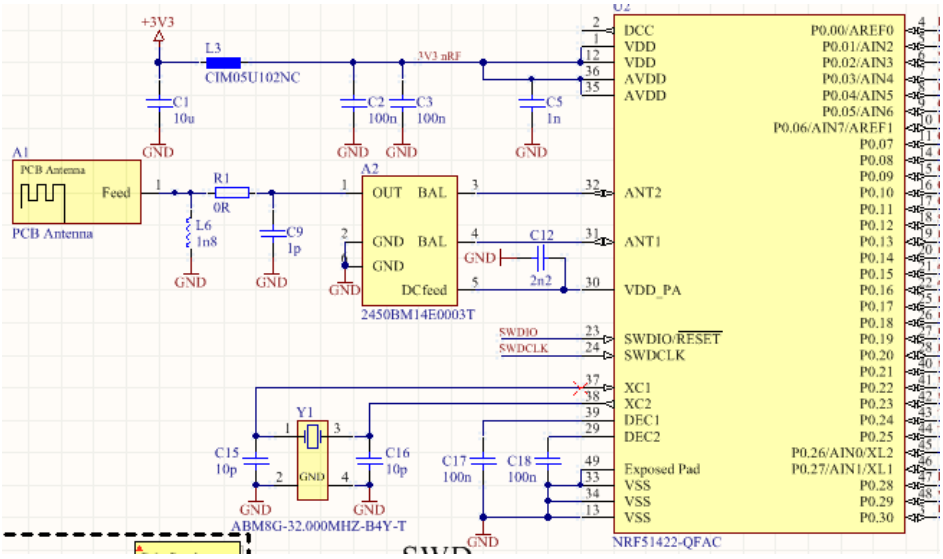


Figure 4-12 Power supply of nRF51.

Power consumption measurements were carried out across all power and wireless communication stages; power on, establishing connection, full frame connectivity and power save mode as shown in Figure 4-13.

After transition from the slave node power off state (Figure 4-13 label A) to slave node power on state, wearable device's firmware is programmed to execute initial software and hardware setup routines (Figure 4-13 label B). During that period, the device's power consumption is constant and caused by the processor core and clock subcomponents. Radio frontend is disabled and does not contribute to the consumption current. The power up routine lasts 334 ms as the running program is waiting HFCLK to be available. The average consumption of this state is 3.84 mA. Following the setup routines, the slave node device initialises radio and enters in to scanning stage, waiting to receive ping from a white listed access point device (Figure 4-13 label C). Scanning stage varies between zero ms and 41 ms (one frame) since every 41 ms master node transmits connection ping. The average consumption current during this stage is 14.2 mA. Upon successful received ping (end of label C) the device replies to the master ping and enters short sleep before waking again to listen

allocation slot. If the master node grants connectivity and assign an address to the slave node, the slave node enters connected state and it will only listen allocation slots from this point forward (label D). After 8 consecutive empty slots, wireless communication is switched form full frame to power saving state (label E) where the slave node communicates with master on every 8th frame.

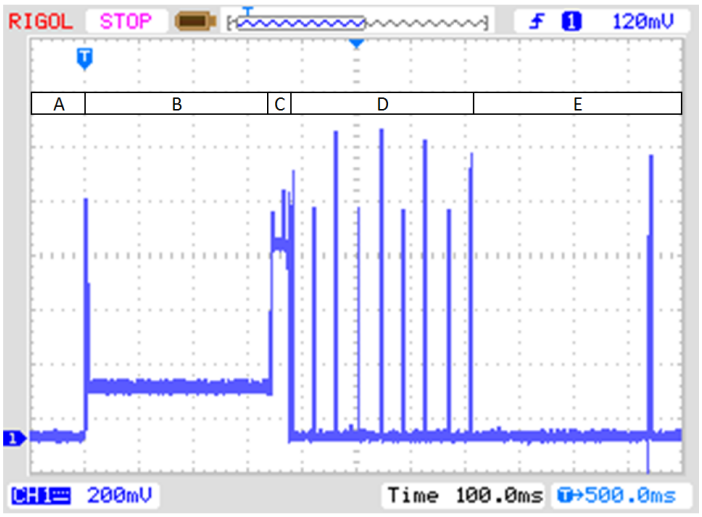


Figure 4-13 Power consumption states; power off (A), node initialization (B), scanning mode (C), connected with empty slots (D) and connected power save (E).

Figure 4-14 show a more detail relation between master's protocol states and slave node power consumption. Visible are the three distinctive power consumption patterns; HFCLK startup spike, allocation slot and data slot. In the connected mode, the slave node is active only to receive the master node allocation packet and execute bidirectional communication in allocated data slot.

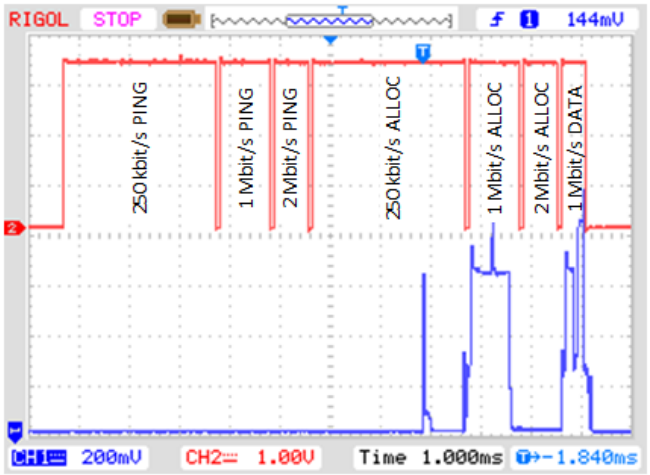


Figure 4-14 The slave node power consumption compared to master node active time.

The slave node is in low power sleep state with processor core, radio and HFCLK turned off most of the time. Slave's HFCLK is started up 800 µs before the required time to start ramp up of radio receiver as shown in Figure 4-15. First current peak has an average current of 1.44 mA lasting 160 µs. It is followed by a 460 µs of clock debouncing period with average current of 160 µA. A sudden drop of the post start-up current is due to transition of HFCLK to standby mode, where the crystal oscillator is kept active but the output is disconnected from the clock distribution to achieve low current of 30 µA. This is possible due to programmable triggers and events architecture which the nRF51 family offers. Using this architecture, after entering into the sleep mode, the slave node enters into the receiving mode without wakening up processor core. Firstly, LFCLK triggers start up of the HFCLK. Upon elapsing the time required for HFCLK to be available, LFCLK again triggers precise start of timer used to keep track of the absolute radio time. This timer has preset counter match values which trigger power on of the radio and transition in to receive mode.

The allocation slot current consumption pattern is shown in Figure 4-15 (right). The first visible rise in current consumption after radio enters receive ramp up state is equivalent to 4.64 mA and lasting 76 µs. It is followed by peak of 14.5 mA for next 76 µs during which the PLL locks and the current consumption decreases to constant 12.6 mA in receive state. A short peak of 16 mA is observed after the first allocation packet is received and radio, clock source and processor core are active at the same time. A post allocation slot current of 4.4 mA is observed during processing of the second received allocation packet.

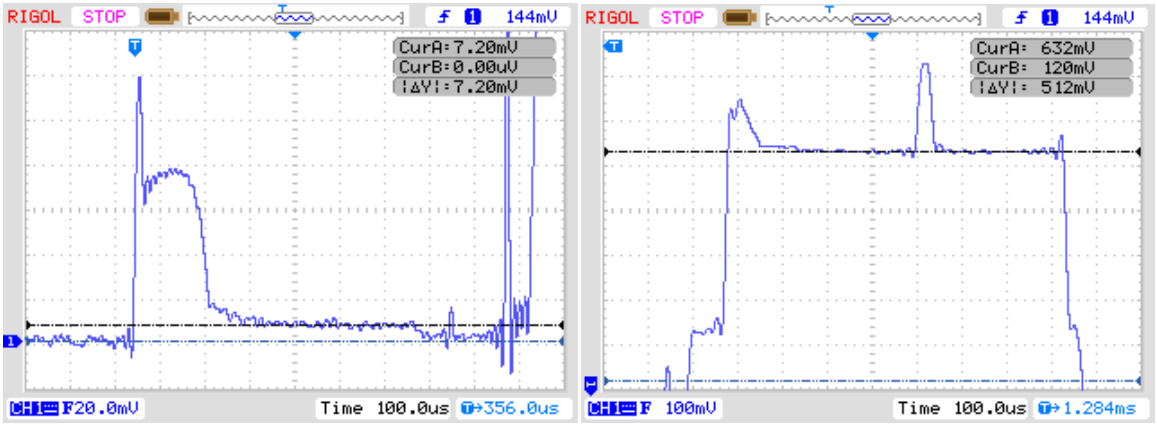


Figure 4-15 HFCLK power up after sleep (left) and allocation slot (right) current.

Data slot current consumption pattern is shown in Figure 4-16 (left). Five key elements are distinguishable: radio ramp up, receiving state, transmit ramp up, transmit and post slot processing. The measured radio ramp up current is equal as to the allocation slot radio ramp up.

The measured current for transmit radio ramp up and processor current for handling received packet is 10 mA, followed with only transmit radio ramp up current of 6.4 mA. The radio transmit current is measured to be 16.9 mA at 4 dBm transmitted power. The post slot current in which processor is preparing for the next slot is 4.5 mA.

After the protocol determines that there are no more data slots left to receive in current frame, it enables interrupt on the next LFCLK and enters in to the sleep mode as shown in Figure 4-16 (right). During this state, the measured current is only 360 µA coming from HFCLK drive. In the next interval of LFCLK, the interrupt is triggered and the processor computes next wakeup time. In the calculation of next wakeup time, accumulated error of time tracking is added to the total sleep time. The average current measured during that state is 4.5 mA After the processor disables HFCLK and enters sleep, current consumption falls to 24 µA. Carried out measurements validate wireless protocol consumption model proposed in Chapter 3.

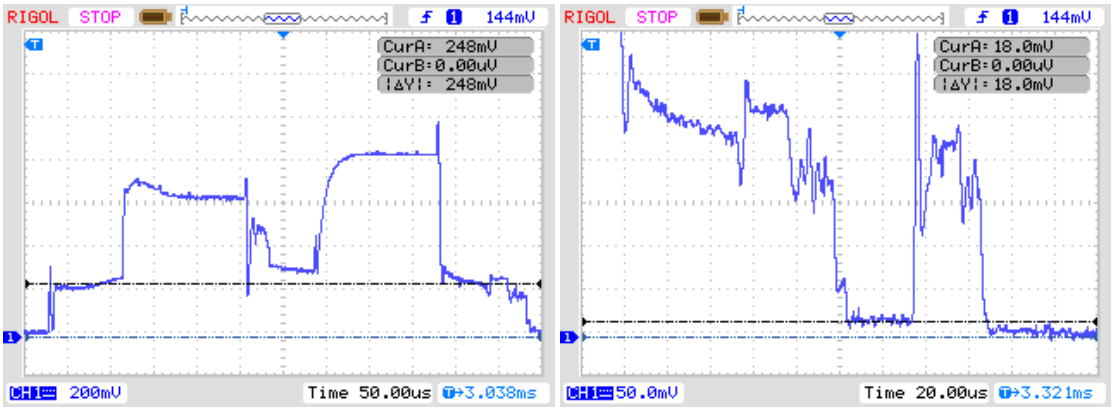


Figure 4-16 Data slot (left) and sleep prepare (right) current .

To put a real perspective of achieved power consumption results, the same printed circuit board was used to measure consumed power for transferring single frame data with BLE and WOLC. For BLE power consumption measurements, program code was loaded from Nordic Semiconductors example project. WOLC achieved overall lower consumption and lower power consumption per transmitted byte as shown in Table 4-2. Optimisation achieved low overhead and low computational complexity which allows main processor core to exit active state faster and return to sleep state.

Table 4-2 Measured avarage current consumption for BLE and WOLC.

	Frame rate	B/frame	Current	µA/Byte
BLE	2 Hz	28	110 µA	**1.96**
WOLC	3 Hz	30	87 µA	**0.96**

4.3 Validation of high throughput packet exchange protocol

4.3.1 Developed software support

In order to support the use of flexyNET protocol three software libraries where created for three language implementations; C, C# and Java. The first C language implementation is limited to link management, encoding and decoding due to platform limitations. Implementation for high level programming languages C# and Java where developed as add on library, .dll file for C# and .jar library for Java.

The structure of the C# and Java library is shown in Figure 4-17. The figure outlines modular component implementation together with a flexible number of connections. Two main components of flexyNET library are flexyNET connection and flexyNET Routing class. The first class is responsible of decoding packets from incoming stream of bytes, handle errors, decrypt/encrypt packet data and translate transmitting packet in to byte stream. Packet encoding and decoding is a part of the connection class, as it needs to preserve link and decoding states for the connection. The second class, flexyNET Routing is responsible of interacting with one or multiple flexyNET connections, request packet decoding, maintain routing tables and forward packets which are for this node to the application through call-back functions. As the implementation is modular, it is possible to connect any application or communication handlers at either end.

Implementation of flexyNET Connection is multi-thread safe and use locks to guaranty data consistency. External transport handlers for USB or TCP/IP can safely access and write or read to the connection buffer. On the other side flexyNET Routing's packet decoding thread will register its semaphore to be notified when incoming data are written to the connection

receive buffer. This removes the needs for constant pooling of new data and removes the latency between receiving the packet, decoding and invoking call-back function.

Routing data reduction optimization methods are applied in the routing class for examples like direct communication between neighbouring nodes. Routing class holds routing tables and information of neighbouring nodes through individual connections. In case a node has two connections, like an access point, it can receive packet with optimised header in which sender's address is omitted. If the packet is intended for a different address in the network, flexyNET Routing will update the packet and add neighbouring node address before forwarding packet to the network through second flexyNET connection. Context data reduction optimisation method such as sending packet to the central server or broadcasting, is applied on the application side since application has the context knowledge.

As the library is developed and written in C# and Java, it is possible to integrate flexyNET in Windows, Mac and Android devices as a client-side application or run it as a server side application.

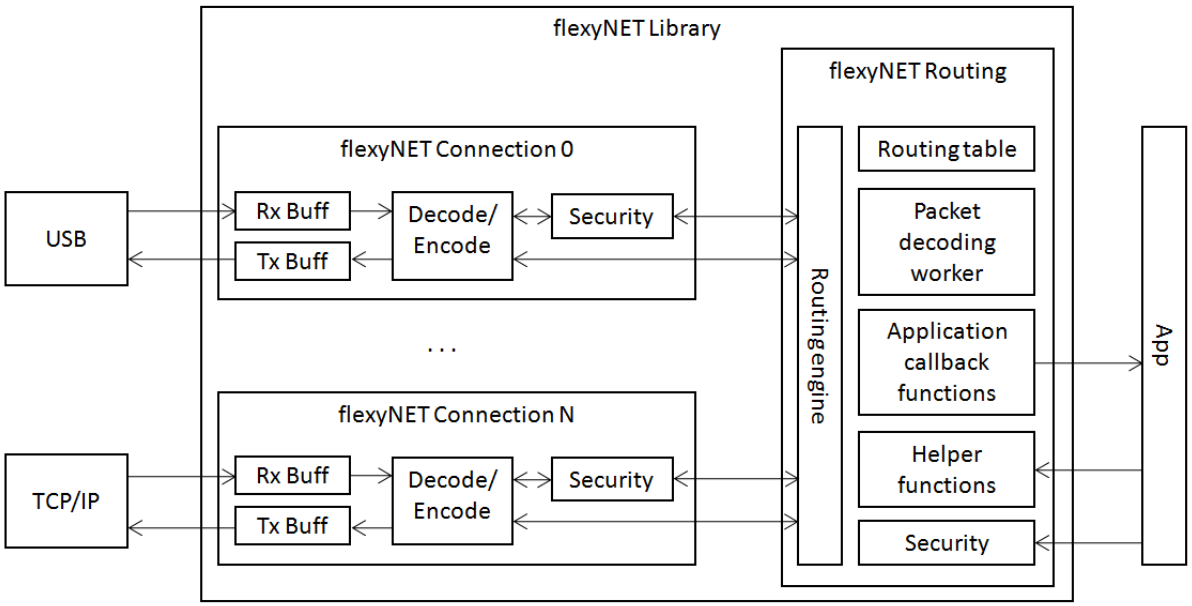


Figure 4-17 Internal architecture of flexyNET library for C# and Java.

4.3.2 Test environment and protocol encapsulation

The test environment is set as shown in Figure 4-18. Across the network, flexyNET is used as consistent packet distribution protocol which is encapsulated depending on the application into one or more other protocols. From data source up to the data sink, the network

has different connectivity speeds, 515 kbit/s over WOLC (combined duplex speed), 1 Mbit/s using a USB connection and 1 Gbit/s when using Ethernet connection.

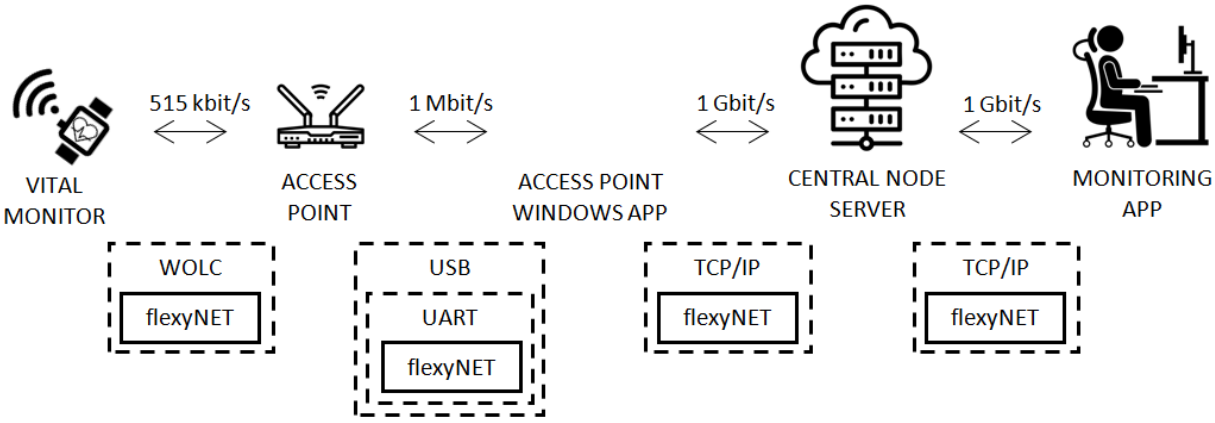


Figure 4-18 Test environment and protocol encapsulation across the network.

4.3.3 Addressability and upfront content challenges

The developed protocol achieves small overhead using context data reduction methods and with optimization of available set of functionalities. Small overhead results in improved efficiency. Packet port/type with only 1 byte length contributes in achieving these results. As each service was mapped to one port number changes in service type, version or adding new services resulted in requiring bookkeeping functionality of the specific port assignment to a specific function. Maintaining backward compatibility limits re-usage of the ports/types number which could lead to exhaustion of available ports/types out of total 256 available, even if not all ports are being used. An approach without using port/type can be found in higher layer messaging protocols like MQTT. It provides flexibility and human readable description. Still the overhead can be several times greater than the actual payload. Merging the two approaches together as described in this theses, combines best aspects of both: minimal overhead and human readable topics.

4.3.4 Performances validation

Test environment presented in 4.1 is used for validation of individual and a group one protocol performances. The first test was designed to measure the maximal and sustainable throughput between the generator node and central server. The generator app is used to emulate node packets at very high bandwidth. To remove any performance deterioration due to the network latency, both the central server and the node where on the same local machine. During

the test, sustainable central server processing speed and of 140 Mbit/s was recorded with peaks up to 160 Mbits/s, when one node was connected. With two nodes connected, a total combined connection/routing speed of 160 Mbit/s - 176 Mbit/s was achieved.

In the second test scenario, access point and ECG analyser were connected to the network. The access point was providing connectivity for 4 nodes, each set to generate constantly 64 kbit/s, summing to a total of 256 kbit/s. During the tests all components where able to sustain a constant feed from the nodes and route packets accordingly.

The third carried out test scenario test all context optimised routing. Packets were prepared for different scenario and pushed into the network. By using developed packet capturing feature, all packets where analysed. A successful validation of all header data reduction optimisation method is confirmed:

- Omitting sender's address on the first hop,
- Omitting receiver's address when packet destination is neighbouring node,
- Omitting receiver's address when packet destination is central server,
- Omitting receiver's address when packet is broadcast type,
- Setting minimal byte length able to store receiver's address.

The fourth carried out test scenario test if delay caused by drop in bandwidth will be equally distributed to all services. For the test execution, a wearable node with ECG and inertial sensors was chosen. The two services have a different bandwidth, ECG has 1.6 kbit/s and 3-axis inertial sensors has 7.2 kbit/s. Distance from the access point and wearable node was slowly increased towards the range limit. At the same time monitoring application was running to monitor arrival delay from the 2 services. Both services were equally impacted by the delay from the available bandwidth reduction.

4.3.5 Software libraries validation

In order to support long term reliable and continuous acquisition and monitoring of physiological parameters from a wireless sensor network, developed software packages C# and Java were tested for memory leaks, recovery after drop of connectivity and stable work over multiple weeks. Tests validated the developed software support without issues spotted.

4.3.6 Overall achieved protocol efficiency

Although flexyNET has 256 times smaller maximal packet size than UDP/IP, achieved protocol efficiency of flexyNET is 98.5 %, slightly higher that 98 % of UDP/IP over Ethernet.

This result in smaller memory requirements on the nodes and facilitating even bandwidth distribution across services.

4.4 Seamless connectivity

Although successful validation and implementation of custom developed platform and protocols is confirmed therefore fulfilling design goals, there is a need to acknowledge difficulties when using proprietary developed tools and materials. A substantial research and development resources and expertise needs to be available in order to build the platform. Upon successful initial platform deployment and start of use, if additional scaling of components is required, securing additional resource is needed. These resources will be consumed either in producing units of developed proprietary hardware and/or execute required software changes. Additional obstacles may arise as the knowledge transfer and upskilling of new resources will take higher effort in comparison to the usage of widely adopted standards and practice. These challenges were experienced during our previous research [108, 41]. This motivated research activities to analyse technology availability and standards in use around the user which could be used as building blocks for energy efficient wireless sensor network for long term continuous acquisition and monitoring of physiological parameters. As of-the-shelf devices and technology will be used, there are limitations in number of optimisations which could be used. Primary optimisation method was chosen to be increased network coverage, as the aim was to remove necessity to supporting long range communication. Architecture and methods need to ensure seamless experience across a user's multiple environments present during the day as shown in Figure 4-19.

Research work concluded with seamless connectivity (Se-Co) [109] architecture and methods proposal. Proposed architecture aims to ensure seamless connectivity by connecting either to home or to previously unknown roaming networks without a need for user intervention and without taking over the tasks of establishing and maintaining connection. Chain of trust guarantees that gateways share resources only with genuine devices without degrading gateway's or peripheral device's privacy. They are both secure and motivated to share a part of their Internet bandwidth with nearby devices holding anonymous certification of ethical usage and no harm for the network.

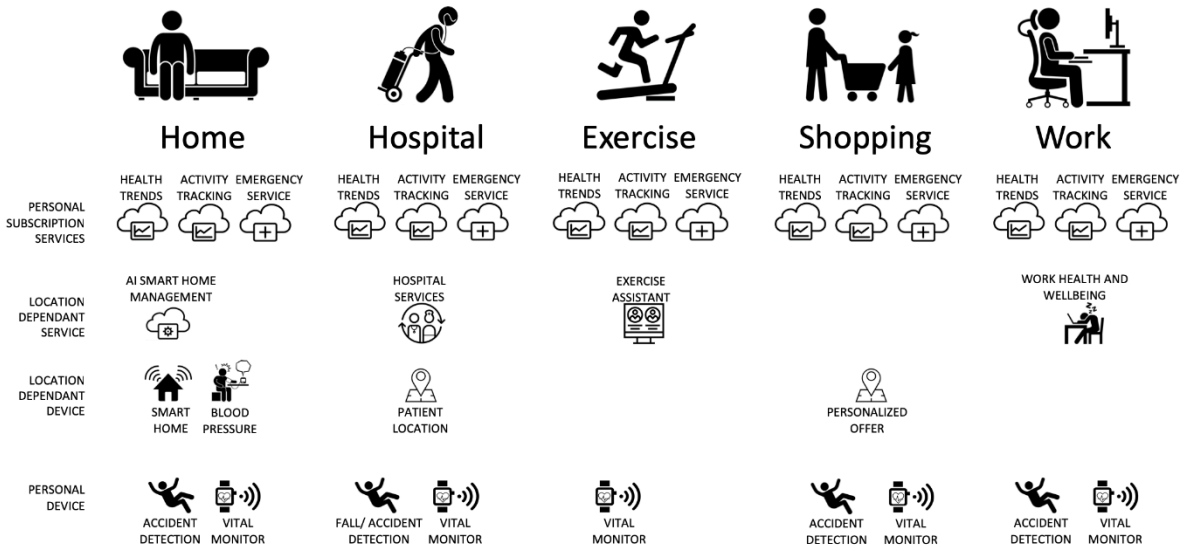


Figure 4-19 Services across user's daily activities.

Providing seamless connectivity requires overcoming contradictory requirements:

- broadcasting device presence to initiate the connection process while preventing device profiling and maintaining of device privacy,
- connecting to unknown anonymous devices while maintaining security, and
- ensuring connectivity in home and roaming networks while maintaining communication uniformity.

The Se-Co architecture, methods and procedures support programmatically (without user intervention) establishing connectivity of IoT and wearable devices with gateways both in home (known) networks and in roaming networks (unknown private phone or infrastructure gateways). Se-Co methods are used to maintain the privacy and security of peripheral devices and gateways, with options to disclose a granular layer of identification and certification. Outline of Se-Co implementation using a BLE wireless protocol is presented due to availability of BLE devices round the user, although another wireless protocol may also be used. Attributes defining Se-Co are:

1. seamless anonymous connectivity based on opportunistic Internet connectivity from known and unknown networks while keeping both privacy and security intact,
2. autonomous connectivity management without user input,
3. flash anonymous device discovery methods to determine if the device is a part of the same home network without a call to the home provider,

4. incentivize provision of Se-Co services through ethical use and no harm certification of device's hardware, firmware and application scope,
5. adaptation of Bluetooth LE broadcasting packets to support Se-Co methods for advertising and resolving pseudo-random ID to device ID by the home on-premises/cloud provider at the predicted scale of a billion active devices,
6. home and roaming network application agnostic messages routing

4.4.1 Seamless connectivity architecture and methods

The architecture of the proposed Se-Co solution consists of: certification authorities, providers, gateways and nodes. Providers and gateways can have attributes of home or roaming. If gateways and providers are part of the same network relative to the node, they have a home attribute and if not, they have a roaming attribute. The solution architecture is shown in Figure 4-20.

Se-Co certification authority provides certificates to devices/nodes which are hardware, firmware and application scope compliant. The provider is a central body which can create a virtual private network (VPN) and associate gateways and nodes with it. In a provisioning stage, the home provider and nodes exchange certificates and public keys. Once the device provisioning is completed, connectivity between devices associated with the same home network can be established, with or without Internet connectivity. Connection between the node and the gateway is established autonomously without user actions when the node is a part of the same VPN as a gateway or when a roaming gateway receives certification from the home gateway that the node is Se-Co certified. Certification is given upon successful pseudo-random identity resolution which the anonymous node broadcasts. The cloud providers are able to resolve device pseudo-random identity efficiently 'on the fly' and cost-efficiently for any large number of associated devices. In a home network, all devices are interconnected and capable of exchanging data across that VPN using all available bandwidth.

When a node is out of reach of the home network, a connection to a roaming network can be achieved only if the roaming provider has Internet connectivity to the node's home provider. This is aligned with the scope of the node connectivity aim through roaming network communication with the home network. In the roaming network, all traffic coming from roaming providers outside of the VPN is forwarded to the home provider. Through roaming provider, the devices have the ability to send to, and receive from, the home network provider bandwidth-limited encrypted packets. The home provider is responsible for decrypting and

ingesting packets into the home network and also to encrypt packets from the home network being sent to the devices currently in a roaming network. Roaming network gateways provide a bandwidth-limited access (at their discretion). Gateways connected to broadband Internet and having constant power supply may be willing to provide higher bandwidth to a larger number of devices. In contrast, a smartphone gateway has a limited bandwidth and a limited energy supply with the aim of preventing degradation of usable smartphone time of use. Therefore, the smartphone acting as a gateway is willing to provide access to only a few devices providing very limited bandwidth.

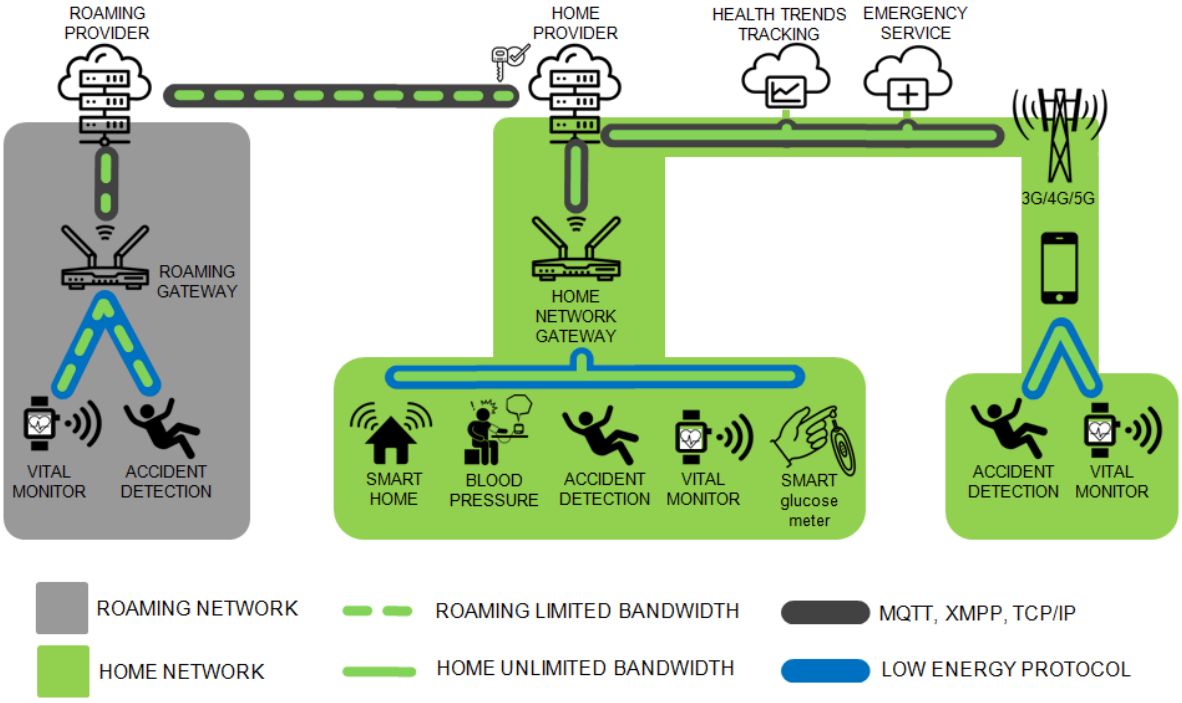


Figure 4-20 Solution architecture.

4.4.2 Se-Co chain of trust and privacy

Chain of trust is the basis for the GLOBONET concept and MAKA protocol. Proposals from [92-100] provide device identity confirmation through a home agent. This identity does not provide device scope, therefore identity of a device which is a BLE sniffer and profiler can be validated. Adding a specific scope attribute to the certification could enable device profiling. As an example, where 20 devices are near a gateway, adding a scope attribute would potentially isolate single nodes by their specific scope and enable device tracing and profiling.

Se-Co compliant devices do not disclose their scope to the roaming gateway/provider, but provide certification that the device does not pose a threat to the roaming network. Both the device and firmware are certified. If the device is programmable or customizable, certification

will be extended to prevent post-sale harmful modification. Chain of trust across different device stages is shown in Figure 4-21. Communication between providers uses standard WEB secure channels and X.509 certificates.

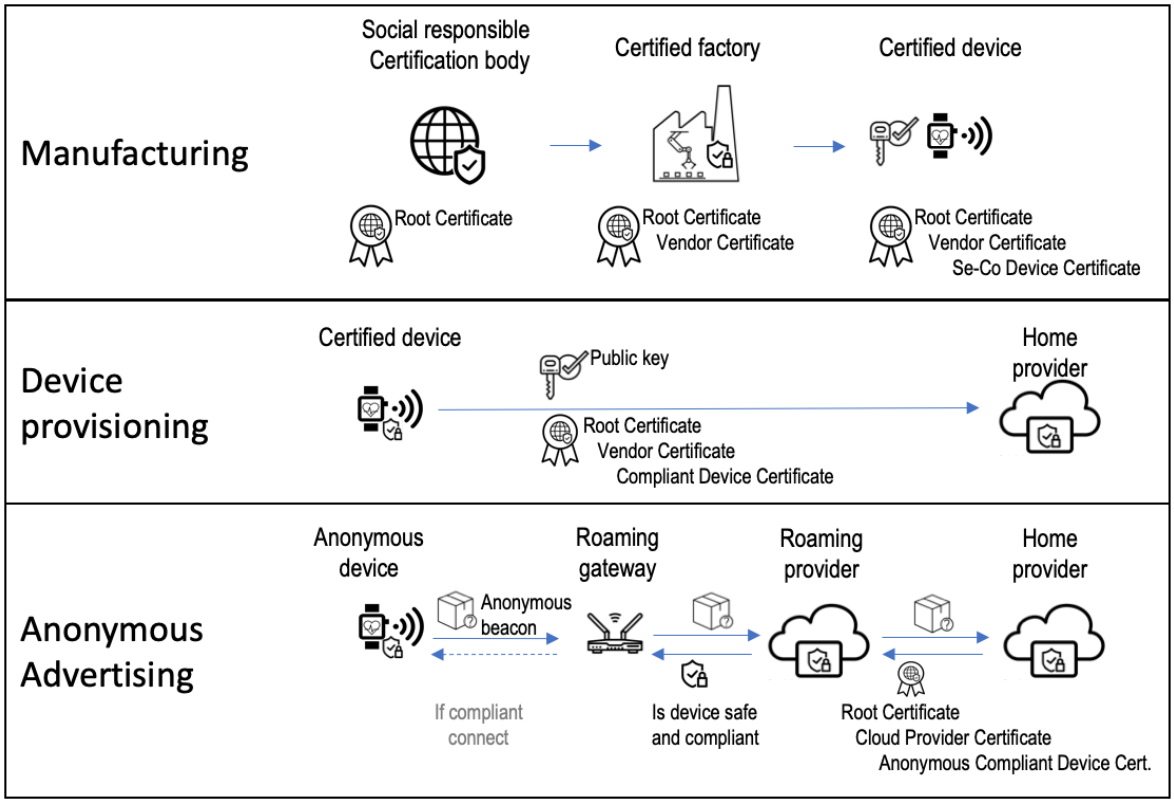


Figure 4-21 Chain of trust across different device stages.

4.4.3 User privacy and device identifiability

The developed architecture supports two identification methods based on modern cryptography functions. The node broadcasts a pseudo-random advertisement to nearby listeners which carry out the following identity resolution methods:

- resolving an advertised pseudo-random ID to a device ID efficiently and 'on the fly' for any number of devices using public-key cryptography,
- high probability determination of whether the observed peripheral device is a part of the same home network to support fast connection regardless of online or offline status.

The solution maintains device privacy and anonymity against nearby listening devices, gateways or providers which are not a part of the same home network by frequently generating new pseudo-random IDs. At the same time generation of new pseudo-random IDs does not

impact on the method to identify devices which are a part of the same network or cloud providers. Disabling of reverse IP address tracking and profiling of the gateway by the node is achieved by hiding the gateway's address behind the cloud provider. All traffic between two different networks is routed and exchanged centrally between the two cloud providers. To an external observer, the cloud provider is a single visible address/entity entry point for multiple associated networks. A node trying to profile and track the gateway's physical location and IP address will always receive a response from a single cloud provider when connecting/connected to different roaming networks, thus preventing effective profiling.

4.4.4 Resolving pseudo-random advertisement into ID at scale

Se-Co provides improvements from solutions presented in section 2.3.2 [Privacy and security] which have either scalability or offline constraints. Se-Co provides a pseudo-random architecture and methods which ensure device privacy and anonymity while retaining efficient 'on the fly' decoding of a device's pseudo-random ID using an integrated cryptography model: Elliptic Curve Diffie-Hellman key exchange, Advanced Encryption Standard (AES) symmetric encryption and one way hash cryptographic functions. Cryptography used in BLE 4.2 relies on ECC and AES with 256 and 128 bit key sizes, respectively [110]. Security reports [111-112] estimate that the ECC with a 256 bit key size is secure to use for another few decades, along with projections of a RSA key becoming impractically large and consuming more power [113].

In order to resolve pseudo-random identity, decision was made to use the public-private key pair method. Since an AES key is derived from a shared secret between the provider and the peripheral devices using Elliptic Curve Diffie-Hellman key exchange (Figure 4-22), only the provider can decode the device's ID using its private key. The same principle is used in Transport Layer Security (TLS) and sequentially in Hyper Text Transport Protocol Secure (HTTPS), both used today worldwide. Although using AES 256 and ECC 512 bit keys would provide longer lifespan of the security, we decided to use 256 bit ECC key size because of the payload limitation in broadcasting packets. The public compressed key for 256 bit ECC is a 257 bit key which may be divided between two broadcast packets. Larger ECC keys would not be possible to broadcast with BLE specification 4.2. The major future adoption of devices with BLE revision 5 will allow the use of ECC with a 512 bit key size.

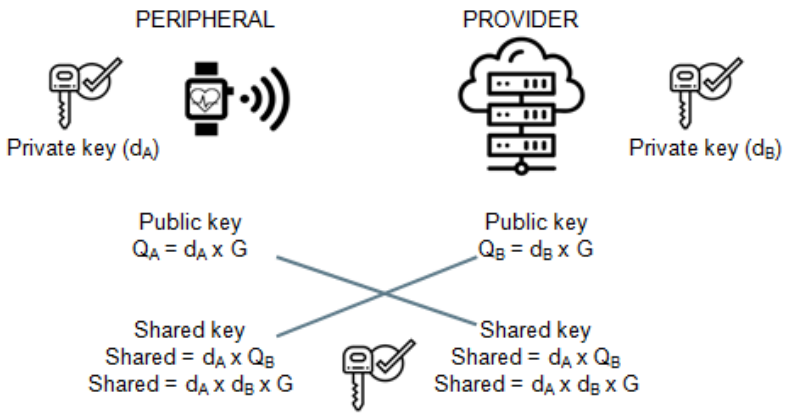


Figure 4-22 Elliptic Curve Diffie-Hellman key exchange.

In the device provisioning stage, peripheral devices store the provider's public key and IP address. For every session, the peripheral device generates a random public/private key pair. Using the provider's public key, the device computes a shared key which is used to derive the symmetric AES key. The AES symmetric key is used to encrypt the device's ID into a 16 B block. By broadcasting a random peripheral device's public key and AES block, the provider and only him, is able to decrypt the AES block and access the device ID. EID operational model resulted in a problem space and required computations ($N_{total\ computation}$)

$$N_{total\ computation} = N_{device\ number} \cdot N_{window\ size} \tag{4-10}$$

where $N_{device\ number}$ is all device for which a single provider provides service, $N_{window\ size}$ is number of the parallel time window required to have due to device time error. Propose novel approach allows use of standard server-side public-key cryptography found in TLS to retrieve the device ID. Due to use of public-key cryptography, problem space is reduced to

$$N_{total\ computation} = 1\ (Single\ packet\ decryption) \tag{4-11}$$

eliminating long running and expensive (pre)computation. This makes solution viable for resolving requests for any number of devices and providing support for billions of predicted active devices.

BLE 4.2 advertisement packet limits user defined bytes to a size of 29 B which is not sufficient to transmit a compressed ECC public key (33 B) and AES block (16 B). To overcome this limitation, an ECC public key is split between a BLE scan and response packet, as shown in Figure 4-23.

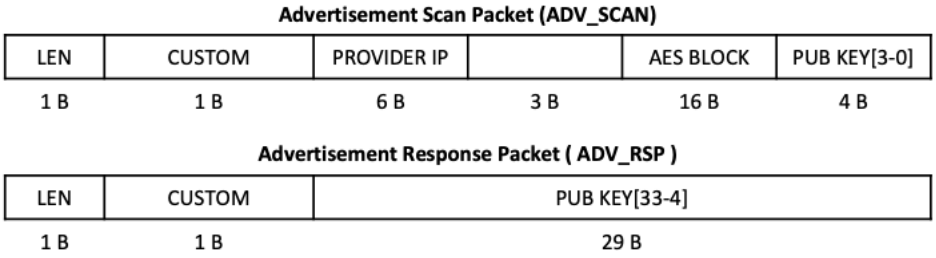


Figure 4-23 Advertising and request response packets.

A summarised comparison between different identification method used for low power devices on Table 4-3 outlines how Se-Co fulfils shortcomings of existing methods in use.

Table 4-3 Comparison of different identification method used in low power devices.

	Offline resolution	*Online resolution*	*Scaling impact*	*Multi provider*
Bluetooth IRK	Supported	Not supported	Resource intensive	Not supported
EID	Supported	Supported	Resource intensive	Not supported
Microsoft CDP	Not supported	Supported	Unknown	Not supported
Se-Co	Supported	Supported	No impact	Supported

4.4.5 Determining peripheral devices belonging to a home network

In a worst case scenario, the roaming networks may provide only a restricted bandwidth connectivity service. Therefore, in terms of power consumption and communication channel congestion, it is crucial to efficiently detect the probability that the observed peripheral device and the gateway are a part of the same network. This detection is achieved using a highly efficient method capable of resolving in real time and in congested areas where thousands of peripherals advertise their presence.

In section 2.3.2. (Privacy and Security), Microsoft's CDP service approach was outlined. The service uses a one-way hash function which meets the requirements for privacy and network identification. The Se-Co architecture and methods use the same one-way model, where hash is generated from nonce (advertised payload) and home network key. Our design challenge was to find space for the hash result since the advertisement packet payload is already full as it contains the peripheral device's public key and AES block. Since the output of the hash is pseudo-random, it is suitable for use as a replacement for the dummy advertised device random access address. This approach provides the same device tracking protection but with an added functionality to detect the device belonging to a home network. For that purpose, the 32 B result of the hash function will be trimmed to 9 B of which 6 B is used as a random address

and the remaining 3 B in the advertisement packet. Final assembly of the advertisement packet is shown in Figure 4-24.

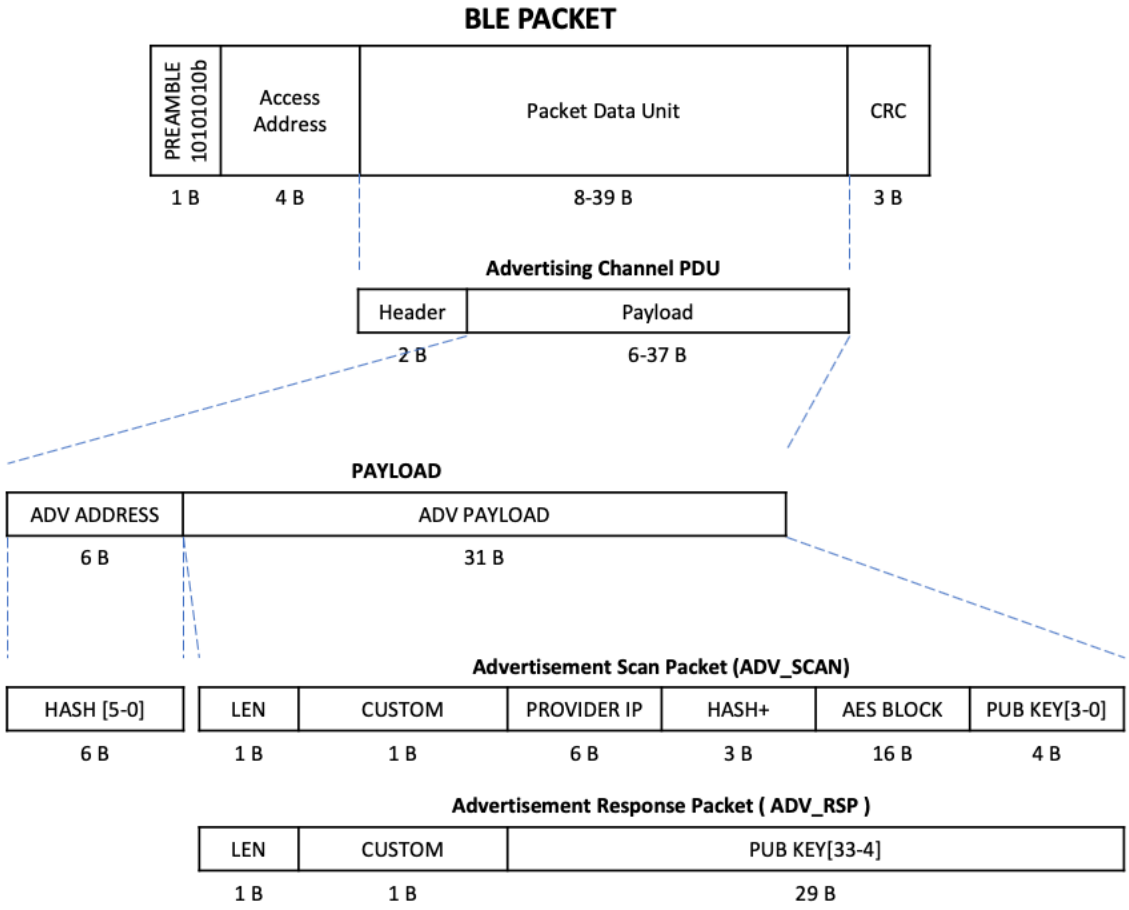


Figure 4-24 Complete Bluetooth LE packet including advertising packet with address.

As the nonce and hash result is available in the advertisement packet, the proposed method saves the peripheral's power and prevents communication channel congestion since the gateway can act as a passive observer and does not need to actively ping peripheral devices for response packet information.

4.4.6 Connection establishment and certifications

As noted in the Introduction, the goal of this solution and methods is to provide the required uninterrupted connectivity service to peripheral devices, both in home and roaming network environments. The designed solution provides power efficient and anonymous methods for establishing a connection between any two anonymous devices. Power efficiency is achieved by minimizing events with data exchange and by pushing computation to devices

with higher energy availability. Minimizing data exchange events is achieved by using cryptography models. This connection process is shown in Figure 4-25.

The connection establishment process was designed to remove delays, allow caching and preserve the peripheral device's power, the latter of which is achieved by pushing power extensive pre-computation towards the gateway and providers.

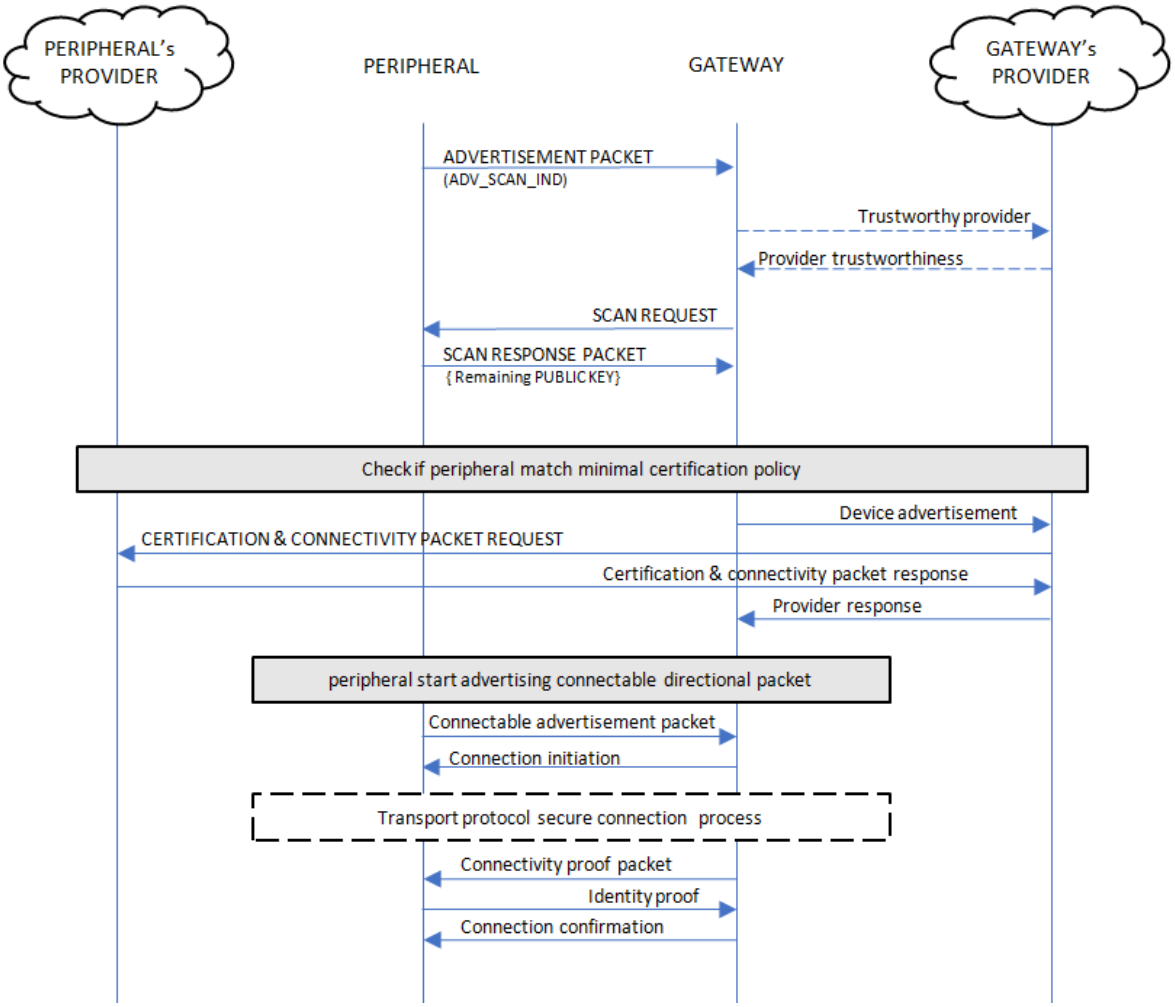


Figure 4-25 Connection process using Bluetooth LE 4-transport layer.

4.4.7 Connection establishment - roaming

The connection process starts with the gateway (home/roaming) receiving the peripheral device's non-connectable advertisement. As described in 4.4.4 and 4.4.5, from the initial advertisement packet, the gateway can determine:

- whether the observed peripheral device is a part of a home network (either real-time or offline), and
- which is the provider's IP address.

After determining the provider's trustworthiness, certificate or confirmation of whitelisted status, the gateway sends a scan request to the peripheral device (a scan request is interpreted by the peripheral device as a connectivity offer and it adds the offer to a list for subsequently making a choice on connection).

Upon receiving the scan response, the gateway forwards the received packets to its provider. The gateway's provider makes a request to the device's provider requesting a connection token/packet, which is further used when the connection with the peripheral device is established. The response is then returned back to the gateway's provider and if the preset policy is met, it forwards a positive reply and connection token/packet to the gateway. We chose that method to maintain the gateway's anonymity and privacy by hiding the gateway's local IP or other traceable information behind the gateway's provider.

Regarding the peripheral device's decision to connect with the selected gateway, the device will start to broadcast a connectable advertisement with the selected gateway's address (ADV_DIRECT_IND). If the security policy of the peripheral device matches the predefined policy, the gateway will respond with a connection request and the Bluetooth LE connection process will start, thus establishing the transport layer. In the response from the peripheral device's provider, data to instruct the gateway to connect using a "Just Works" or OOB (Out Of Bound) method with provided passcode are included.

Upon establishing the Bluetooth LE transport layer, the gateway will forward an Internet connectivity proof packet to the peripheral device. The peripheral device replies with an identity proof packet to which the gateway replies with an acknowledgment.

4.4.8 Internet connectivity and identity proof

Since the peripheral device seeks connection to a roaming gateway to establish Internet connectivity, it needs to be able to determine whether that roaming gateway is a genuine provider. This is achieved by sending a connectivity proof packet upon establishing a connection on the transport layer and with periodical pings as shown in Figure 4-26. The connectivity proof was designed to be consistent for both connection scenarios to minimize code footprint:

- connecting to a roaming network, and
- connecting to a home network (offline capable).

In the roaming scenario, Internet connectivity and access to the peripheral device's provider is verified. The proof packet is encrypted using an AES key derived from a shared

secret between the peripheral device and its provider. Since a valid packet can be generated only by the provider, providing a valid packet with a full calculated hash is sufficient proof to a peripheral device that the gateway has access to the peripheral device's provider. Since the public key is randomly generated per session, false gateway reply attacks are not possible outside the current key pair session.

In the second scenario, connectivity to a valid home network is verified. Since connectivity between the peripheral device and the gateway needs to support the capability to connect between, for example, a user's smartwatch and smartphone in an offline environment, the home network AES key is used for packet encryption.

In both scenarios, master keys are used only once to limit the exposure of static keys and to prevent attacks. The proof packet contains the AES key to be used in all subsequent communication.

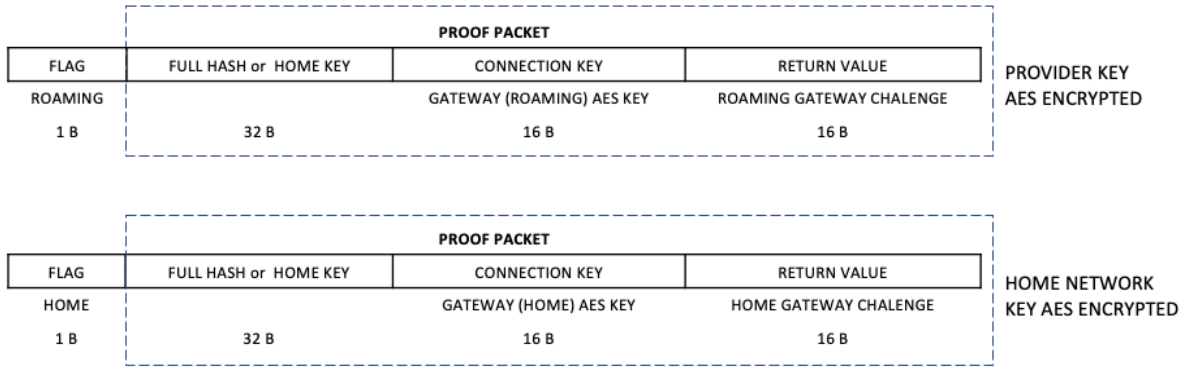


Figure 4-26 Connection establishment packet.

The peripheral device proves its identity to the gateway by replying with a packet containing the previously sent gateway's challenge encrypted with the gateway provided AES key. False peripheral reply attacks are prevented since the gateway is using a new random key in each proof packet sent.

4.4.9 Anonymous chain of trust and ID certifications

Since Se-Co aims to provide connectivity access to genuine peripherals and non-harmful devices while devices want to protect their anonymity, there may be a need to efficiently establish a chain of trust between anonymous devices. Three levels of identification are designed to offer balance between full anonymous certification and use case where domain or ID need to be exposed:

- anonymous – Se-Co/ethical compliant consumer device (W/o category certification),
- domain certification and
- ID certification.

A cloud provider, depending on manufacturer's certification, will issue the certificate to a roaming network provider proving that the device, as observed by the roaming gateway, is not harmful and can be offered connectivity.

Combination of Internet connectivity proof and the device anonymous certification provides enough information for roaming and for the peripheral device's cloud provider to programmatically decide, based on previously set rules, whether they want to exchange connection information, thereby allowing connection between the gateway and peripheral.

4.4.10 Fast offline home network connection

An important solution design feature is the supporting of fast offline connection capability, currently found in examples of connecting wearables to smartphones, or IoT sensors to local networks (Figure 4-27). Upon receiving an advertisement packet from the peripheral device, the gateway can determine whether there is a high probability that two devices belong to the same home network. If that is the case, the gateway can skip all calls to the device provider, offer connectivity and try to connect using the home key. If the connection attempt is unsuccessful, the gateway may repeat the process using the roaming connection process.

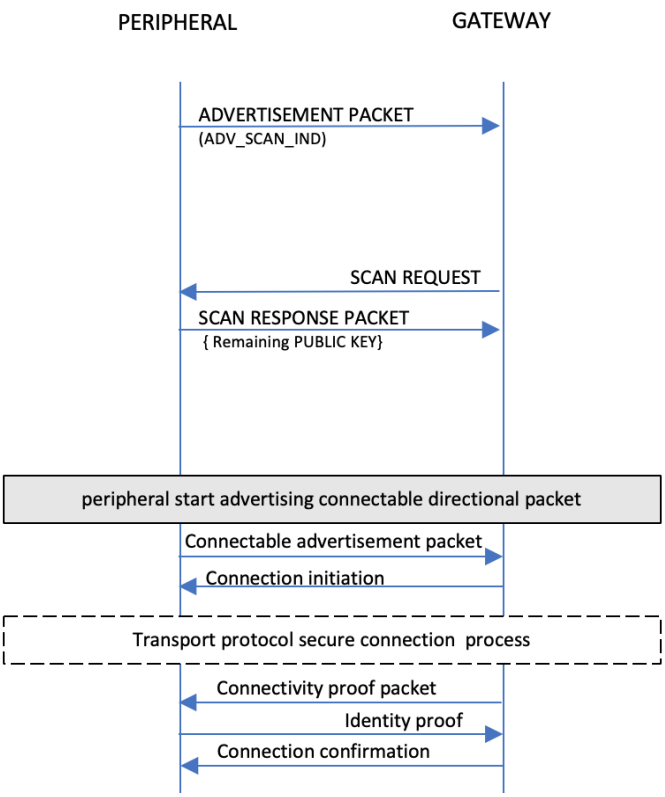


Figure 4-27 Fast offline connection process.

4.4.11 Switching to a home network in a multi-network environment

A particularly interesting scenario happens when a peripheral device is within range of multiple gateways and randomly chooses a roaming gateway. Since a peripheral device is broadcasting only its presence and not listening to the radio in order to conserve power, it cannot detect whether there is a home network in range. To overcome that obstacle, Se-Co uses providers as proxies.

After the home gateway receives an advertisement packet where the hash result matches the gateway's computation using the home network key, it sends a message to the provider to request the peripheral device to disconnect from the current roaming gateway, compute a new random session key (and address) and reconnect to a specific address of the home network gateway. Since the peripheral device has a new pseudo-random address, the privacy is protected from nearby listening devices.

4.4.12 Easy key revocation and access management

Since the proposed solution provides connectivity to anonymous certified devices, the provider can single-snidely revoke a home network key. That simplifies key/access

management/distribution. As an example, when there is a need to revoke access to devices which previously were a part of the home network, the provider can invalidate the current home network key and trigger reissuing of new keys to all remaining devices in the network. Roaming will be approved by the provider since the provider has insight into which devices are a part of the same network.

4.4.13 Results and validation

Although general Se-Co paradigm is applicable to range of protocols like BLE, Wi-Fi, ZigBee, Thread etc., validation using BLE wireless protocol was tested. Validation of Se-Co architecture and methods started with validation of individual sub components. In the BLE Se-Co implementation shown in Figure 4-20, it is crucial to validate wireless low power layer as is the layer with the biggest number of constrains. Expressify ESP32 based boards were chosen to simulate smart device. Gateway was simulated by both ESP32 based board and application running on Android phone. Two platforms were chosen as they are inexpensive and available featuring large community support suitable for students and researchers should they want to validate results themselves. Available Arduino libraries where used to perform ECDH key exchange, compute hash, perform AES encryption/decryption and setup required BLE and Wi-Fi functionality.

Connection activities from Figure 4-25 and Figure 4-27 where successfully tested with implementing custom payload and address within boundaries of BLE, as per Se-Co specification. Behaviour of underpinning key methods where validate to be equal to the theoretical described; generating of the pseudorandom ID, resolving of pseudorandom ID using public-private model and determining if a observed device is part of same home network. Cryptographic SHA-256 hash calculation required on average 153 µs to execute. Elliptic curve calculation, required for ECHD where executed on average in 36 ms. Achieved performance allowed smart device to efficiently compute and change it's advertisement pseudorandom ID signature and perform required cryptographic functions during connection establishment. Performance ensured gateway's ability to determine in µs if observed devices are part of same home network. Empirical test were conducted to determine impact of trimming hash function digest from 32 bytes to 9 bytes. Particular attention was given to determine false positive occurrence where lower trimmed 9 bytes are equal to computed hash with different upper 23 bytes. In the empirical test computing 4 millions hashes there were no false positive and no true

positive occurrence. This is in line with expectations as 9 bytes provide still large combination universe.

Positive validation of ability to create Se-Co gateways on existing consumer devices like smartphones was confirmed. Although peripheral's advertisement packet payload content is completely customized, it is still within BLE standard and therefore visible to BLE compliant devices. Both Android application and ESP32 based gateway connected to Node.Js servers acting as home or roaming provider. Home provider's ability to resolve pseudorandom ID using its private key was successfully confirmed.

During testing BLE advertised device address using ESP32 supported setting up of user provided pseudorandom ID address except for the last 4 bits, therefore lower 8 bytes where used instead of 9 bytes to compare hash digest output when determining if two devices are part of same home network.

4.4.14 Proposed solution limitations acknowledgments

It should be noted that Se-Co aims primarily to provide opportunistic connectivity to smart devices like wearable and IoT. Seamless connectivity is primarily focused on granting connectivity and connection management across known and unknown networks while preserving both parties' privacy and security. In order for a user to experience seamless connectivity, sufficient number of Se-Co gateways should be around the user. This implies that sufficient adoption rate is required. A key design feature to achieve high adoption rate was to maintain neutral impact for the connectivity donor, in form of power consumption, security, privacy, additional broadband cost or required user management. It is not envisioned for Se-Co to guaranty connectivity and provide telemetry for life threat detection devices.

5 Discussion and conclusion

The end of the 20th century and the beginning of the 21st century were marked by a significant increase in the population of elderly and an increase in the incidence of chronic diseases. In that period, significant progress had been made in the research and development of all kinds of new technologies, in particular not only development of technologies dedicated directly to health but also other technologies which became enabling technologies in medicine and healthcare, e.g. connectivity, artificial intelligence, semiconductor technology and chemistry of batteries. Wearable devices and wireless body sensor networks play an important role in such developments, especially for individuals who are under medical treatment, rehabilitation or live independently in their later years and wish to maintain their quality of life. However, the perceived usefulness of wearable devices and their adoption rate will not increase without careful design which acknowledges the user with his interests and limitations. As a foundation for such changes, improvements in connectivity and transfer of data to smartphones, dedicated servers or the cloud are the key technologies. Wireless communication accounts for the largest part of the sensor node consumption, it is crucial to use energy efficient wireless sensor networks. This is further accentuated if there is intent for long-term continuous acquisition and monitoring of physiological parameters and vital signals.

This thesis analyses and describes technologies used in wireless sensor networks for healthcare and the different roles they fulfil. With the rise of smartphones technologies, the cloud, IoT best practices and access to different connectivity options, devices in healthcare and approaches to how devices operate are changing. Widely used communication protocols are enabling the delivery of new functionalities to the end user. Optimisation methods designed and chosen for those wireless communication protocols possess limitations which motivated the research reported herein. The main motivation for this research was to propose solutions for bridging the absence of a comprehensive energy-efficient wireless sensor network solution capable of guaranteeing: consistent low power consumption from minimal to maximal used bandwidth; consistent bandwidth regardless of number of connected nodes; automatically adaptable bandwidth and latency based on changing requirements when the device is in use; low overhead across all OSI layers; modern routing optimisations; and seamless experience for the end user.

C1. Energy efficient communication protocol for application in sensors networks aimed for transfer of biomedical data, based on optimization of media access time and optimization of payload

The research started with the hypothesis that in order to achieve an energy efficient wireless system architecture for long term continuous data acquisition and monitoring of physiological parameters, all components of the system need to be optimized and energy efficient. If one component of the wireless system is not optimal it will reduce overall efficiency. In the research different models which describe wireless sensor network power consumption elements were analysed. Multiple definitions of wireless power consumption elements were merged together to achieve a more comprehensive view on individual impact, cross layer dependencies and analysis of possible optimisations. As the aim of the research was to deliver an architecture for an energy efficient wireless system for long term continuous data acquisition and monitoring of physiological parameters, optimisations chosen to be embedded in the proposed solutions have no, or limited, dependency outside the architecture itself. This will allow the providing of consistent results on different platforms or environments not covered in this research thesis.

Wireless protocol consumption constituents are analysed, and research on existing and novel optimisations is presented. A comprehensive optimisation approach was taken in order to achieve an energy efficient wireless protocol for the exchange of data in wireless sensor networks: optimised medium access control with adaptive bandwidth allocation, optimisation of latency, compensation of clock inaccuracy and stability, data reduction and minimising effects of packet loss. The impact of medium access control and clock synchronisation on wireless protocol energy efficiency is clearly outlined in the research. Various medium access control models are analysed across existing protocols and with respect to the literature. As analysed protocols had either an energy efficient predictive medium access or more energy demanding reactive reduced latency medium access control, a novel protocol is designed to combine positive aspects from both. Analysis of power efficiency deterioration due to packet loss and medium access control model is carried out which resulted in newly designed optimisations to minimise power efficiency deterioration. The presented novel medium access control with adaptive frame rate and bandwidth allocation combines positive aspects of ultra-low power wireless protocols when transmitting states, and low power adaptive low latency when transmitting real-time data. As clock synchronisation between master and slave node in

crucial for achieving wireless energy efficiency, research on clock synchronisation methods and models is carried out. A trade-off between clock accuracy, energy efficiency and energy required to maintain clock accuracy is researched. The developed power efficient optimisation method of maintaining high clock precision using fixed point arithmetic is achieved by exploiting the properties of logarithmic calculation and processor commands. Models are designed to provide guidance on how to achieve the required precision. Wireless medium access control and link layer data reduction optimisation is designed to enable achieving of high efficiency while transmitting smaller packets. As smaller packets have lower probability of packet collision and lower bit error rate probability when the receiver is close to its sensitivity threshold, a smaller number of re-transmissions will contribute to the overall energy efficiency of the protocol.

Optimisation of the energy efficient wireless protocols for exchange of data in wireless sensor networks in health care are validated to maintain low power performance across bandwidth requirements. Positive validation of clock synchronisation, adaptive bandwidth and latency allocation and preserving efficiency while connecting a large number of slave nodes to a single master were achieved. Validation was carried out by measuring the degree to which the following were achieved: clock synchronisation, clock stability, dynamic bandwidth and latency allocation and power consumption across designed operating range.

Taking into account the research work and results in Chapter 3 and Section 4.2, contribution C1 may be declared as accomplished.

C2. Packet distribution protocol in sensor networks aimed for transfer of biomedical data, based on optimization of packet header structure

The previous contribution focussed on the physical and data link layer. As the above mentioned research found that all layers need to be energy efficient for the sensor network as a whole to be efficient, further research concentrated on the optimisation of the upper layers in the OSI model. An evaluation of existing research work and optimisations are presented through the lens of a multi-layer optimisation approach and based on the hypothesis that by exploiting context information it is possible to greatly reduce overhead data. Protocol encapsulation typically used in common protocols achieves the ability to interchange seamlessly individual layers in the OSI model. Every layer contains all the data needed for that

layer, which reduces the computation requirements when assembling or disassembling the packets. A negative effect of this approach is increased overhead. A single protocol may span across several layers, or the layer underneath may already enforce strict packet integrity check or encryption. Through the multi-layer approach, it is possible to greatly reduce requirements on the network and transport layer. Data used for packet routing holds a substantial part of the total overhead data. Research of optimisation methods present in commonly used protocols resulted in a proposed novel routing data reduction method where context is exploited, and strict scopes are defined. Context routing optimisation replaces universal routing data, with only required data needed to execute the routing between two nodes. The proposed method always guarantees data reduction on the first hop which is particularly important for a wireless sensor network. In a wireless sensor network, communication between the sensor node and the gateway/concentrator is subject to the limited power supplies of the sensor node. Reducing power consumption by reducing the total amount of data needed to be transmitted will conserve sensor node power supplies. Additionally to the context optimisation, strict scope is introduced by flagging the packet destination of the central server. This attribute delivers the capability of publish/subscribe delivery model and routing data reduction. The combined optimisations achieved greatly reduce the size of the packet header without compromising packet delivery. The achieved reduction in overhead results in high efficiency when short status is transmitted. It also allows lowering the maximum size of the packet while retaining the same protocol efficiency as if a larger packet size would be used. Smaller packet sizes facilitate transmission of real-time data as there are no big delays in packet transmission. This contributes to the even distribution of the available bandwidth across different services and a better user experience.

Protocol design methods are validated across libraries written using three programming languages and a mixed transportation network. The protocol was tested using a combination of live healthcare connected devices, data generator virtual nodes, routing analysers/loggers and healthcare data consumer nodes. The protocol is validated as being suitable for real time high throughput packet exchange in wireless sensor networks in healthcare. Low overhead enables transmission of small packet sizes without performance deterioration and balancing of latency across multiple services using the same communication channel.

As some projects will have limitations in the use of existing protocols and standards, research was carried out on widely used protocols suitable for achieving the same goals as proprietary developed protocols. Research work concluded with the proposed novel optimisation method to achieve high efficiency while retaining topic descriptiveness using a

messaging MQTT protocol. Two levels of optimisation are presented based on the capabilities of either adding support for a custom message to the MQQT broker or not. The optimisation achieved greatly facilitates evolution and versioning of provided services while minimising overheads.

Taking into account the research work and results in Chapter 3 and Section 4.3, contribution C2 may be declared as accomplished.

C3. Architecture for energy efficient wireless system for long term continuous data acquisition and monitoring of physiological parameters

Although successful validation and implementation of a custom developed platform and protocols is carried out in this thesis, and design goals are fulfilled, there is a need to acknowledge difficulties when using proprietary developed tools and materials. Substantial research and development resources and expertise needs to be available in order to build the platform. Additionally, these technologies are not available in a user's everyday environment. Therefore, research was conducted on how to exploit technologies available to the user to provide energy efficient seamless connectivity by means of a neutral impact connecting/sharing approach, and guarantee the security and anonymity of users. The presented Se-Co solution in the thesis defines the energy efficient architecture and methods for providing anonymous seamless connectivity for wearable and IoT devices across known and unknown networks. The proposed solution provides network-agnostic routing to the application irrespective of whether the node is in a home or roaming network. Management of the connectivity is autonomous, without user input or management. Certification methods and nodes certification scope was proposed to incentivise unknown networks to provide Internet connectivity as certified devices do not pose a security threat for the network. The device discovery and certification methods developed herein retain user anonymity while supporting efficient fast offline and online functionality. Implementation optimisation of the BLE broadcast beacon, which is compliant with the BLE standard capable of supporting the Se-Co connection setup process, is described.

Positive validation of the ability to create Se-Co gateways on existing consumer devices like smartphones was carried out. Although a peripheral's advertisement packet payload content is completely customised, it is still within the BLE standard and therefore visible to BLE compliant devices. Both Android application and an ESP32 based gateway connected to

Node.Js servers acting as a home or roaming provider. The home provider's ability to resolve a pseudorandom ID using its private key was successfully confirmed.

The overall research work delivered an architecture where it is possible to use proprietary developed protocols presented in C1 and C2 across layers 1-7 of the OSI model or use optimised versions of two standard protocols. The developed energy efficient wireless protocol for exchange of data in wireless sensor networks in healthcare can be used with a high throughput packet exchange protocol for real time data in wireless sensor networks in healthcare or with a MQTT protocol. The developed Se-Co architecture with secure energy efficient connectivity management is applicable for both BLE and the energy efficient wireless protocol for exchange of data in wireless sensor networks in healthcare. Combining the whole research work, it possible to state that the goal of proposing a valid architecture for an energy efficient wireless system for long term continuous data acquisition and monitoring of physiological parameters is achieved.

Taking into account the research work and the results in Chapter 3 and Chapter 4, contribution C3 may be declared as accomplished.

Further work should be carried out in the area of validating security claims and strengthening the trust and validation model. It is worth mentioning that in the current Se-Co solution two providers need to trust each other. The home provider is issuing to the roaming provider an anonymous certificate for a device in the roaming network. Future work should be conducted to enable zero trust paradigms, where two providers do not need to trust each other. A method where the home provider can issue a certificate to the roaming provider, which only the device can confirm without disclosing any privacy data to the roaming provider, would be desired.

Summary

Technology advancements in past decade in the fields of semiconductor technology, wireless technology and connectivity, components miniaturisation and integration, artificial intelligence and chemistry of batteries are delivering healthcare and wearable devices with improved capabilities. These devices are seen as capable of providing new means of support for the ageing population and increased pressure to deliver efficient healthcare services. This will be especially true for individuals who are under medical treatment, rehabilitation or they are living, and wish to continue to live, independently. However, the perceived usefulness of the wearable devices and adoption rate is limited due to existing barriers. Adoption of designs which acknowledges the user with his interests and limitations could lead to an increase in the perceived usefulness of the wearable devices and their adoption rate. Applying best practices in energy efficiency and wireless communication could lower adoption barriers through less invasive devices and extended cycles between device charging. The foundation for these changes are developments in connectivity and transfer of data towards the concentrator, gateway, smartphone or cloud. As wireless communication accounts for the largest part of the sensor node consumption, it is crucial to use energy efficient wireless sensor networks. This is further accentuated if there is the intent for long term continuous acquisition and monitoring of physiological parameters.

An overview is given of technologies used in wireless sensor networks for healthcare and the different role which they fulfil. Approaches to how devices in healthcare may operate are changing with the rise of smartphones, broadband connectivity, cloud and IoT best practices. Although widely used communication protocols are enabling delivery of new functionalities to the end user, they possess limitations which have motivated the research herein. One of the main motivations was the absence of a comprehensive energy efficient wireless sensor network solution capable of: guaranteeing consistent low power consumption across the full bandwidth range, consistent bandwidth regardless of number of connected nodes and an automatically adaptable bandwidth and latency based on changing requirements when the device is in use.

The thesis describes wireless sensor network power consumption elements together with an analysis of applicable optimisations. As the aim of the thesis is to deliver an architecture and methods for an energy efficient wireless sensor network, optimisations chosen to be embedded in the proposed solutions have no, or limited, dependency outside the architecture

itself so as to provide consistent results on different platforms or environments not used in the thesis.

Research work resulted in the development of two architectures for energy efficient wireless sensor networks in healthcare. The first architecture is based on novel wireless and packet distribution protocols, while the second was designed to provide interoperability and seamless connectivity by exploiting existing standards, technologies and best practices.

In the research for the first developed architecture, development and validation of two novel components of wireless sensor networks: i) an energy efficient wireless protocol for the exchange of data in wireless sensor networks in health care, and ii) a high throughput packet exchange protocol for real time data in a wireless sensor network in healthcare, was carried out. An energy efficient wireless protocol for the exchange of data in wireless sensor networks in healthcare is validated in terms of maintaining low power performance across bandwidth requirements. Performance does not deteriorate with connection of a large number of slave nodes to a single master. This is possible due to a comprehensive optimisation approach; optimised medium access control with adaptive bandwidth allocation, adaptive latency, compensation of clock inaccuracy and stability, optimised methods to calculate precise time using fixed point arithmetic, data reduction and minimising the negative effects of packet loss. In the thesis a novel high throughput packet exchange protocol for real time data in wireless sensor networks in healthcare is presented. Evaluation of optimisations is presented through the lens of a multi-layer optimisation approach. Through this multi-layer approach, it is possible to greatly reduce requirements on the distribution layer. Additionally, it is shown that by exploiting context information when routing and introducing a publish-subscribe model, it is possible to greatly reduce the size of the packet header without compromising packet delivery, and achieve a high throughput. The achieved reduced header size with resulting small overhead allows the selection of a smaller maximum size of the packet to facilitate equal distribution of bandwidth in memory-constrained wearable devices without reducing the packet efficiency as had been found when larger packets have been used.

As some projects will have limitations on using existing protocols and standards, a novel method to achieve high MQTT packet/message efficiency used in Wearables and IoT is presented. The presented optimisation delivers two levels of optimisation depending on total or partial adherence to the standard, while retaining the topic descriptiveness of MQTT protocol. As the assumption is that the primary flow of information is from the wearable node upstream,

across the gateway towards the message broker, optimisation replaces repetitive transmission of the topic for a single wildcard byte.

Although successful validation and implementation of the custom developed platform and protocols is achieved in the thesis with the fulfilling of design goals, there is a need to acknowledge difficulties when using proprietary developed tools and materials. Substantial research and development resources and expertise needs to be available in order to build the platform. Additionally, these technologies are not available in a user's everyday environment. Therefore, research was carried out on how to exploit technologies available to the user to provide an architecture for energy efficient seamless connectivity by means of a neutral impact connecting/sharing approach and guarantee of user security and anonymity. The presented architecture in the thesis defines the energy efficient architecture and methods for providing anonymous seamless connectivity for wearable and IoT devices across known and unknown networks. The proposed solution provides network-agnostic routing to the application irrespective of whether the node is in a home or roaming network. Management of the connectivity is autonomous, without user input or management. Certification methods and nodes certification scope were proposed to incentivise unknown networks to provide Internet connectivity as certified devices do not pose a security threat for the network. Providing seamless connectivity requires overcoming contradictory requirements: i) broadcasting device presence to initiate the connection process while preventing device profiling and maintaining of device privacy, ii) connecting to unknown anonymous devices while maintaining security, and iii) ensuring connectivity in home and roaming networks while maintaining communication uniformity. Research on available technology and solutions to fulfil the above requirements showed a lack of suitable candidates with most solutions supporting only a single vendor. The device discovery and certification methods developed herein retain user anonymity while supporting efficient fast offline and online functionality. The developed solution supports decentralised multivendor functionality, avoiding vendor lock in and limiting worldwide exploitation. Implementation optimisation of the BLE broadcast beacon, which is compliant with the BLE standard capable of supporting the Se-Co connection setup process, is described.

References

1. "Health at a Glance: Europe 2018 STATE OF HEALTH IN THE EU CYCLE", available at: https://ec.europa.eu/health/sites/health/files/state/docs/2018_healthatglance_rep_en.pdf (17 Mar 2019.)

2. Eurostat Statistics Explained, "Population structure and ageing", available at: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Population_structure_and_ageing#Past_and_future_population_ageing_trends_in_the_EU

3. WHO, Public spending on health: a closer look at global trends, https://www.who.int/health_financing/documents/health-expenditure-report-2018/en/

4. United Nations Department of Economic and Social Affairs, Population Division, Population Ageing and Development 2012, New York, September 2012.

5. Baloch, Z., Shaikh, F. K., & Unar, M. A. (2018). A context-aware data fusion approach for health-IoT. International Journal of Information Technology, 10(3), 241–245, DOI:10.1007/s41870-018-0116-1

6. Shaji, J. E., Varghese, B., Varghese, R., "A Health Care Monitoring Systemwith Wireless Body Area Network using IoT", International Journal of Recent Trends in Engineering & Research, Vol.3, No. 11, November 2017, pp. 112-117, DOI: 10.23883/IJRTER.2017.3499.EDO9R

7. Annapoorani, G., Inja, P., Medhi, P., Thapliyal, V., Kaushik, M. S., "Healthcare Monitoring in IOT using WBAN", International Journal of Recent Research Aspects, Vol. 5, No.1, March 2018, pp. 280-283.

8. Xu, N., "A survey of sensor network applications", IEEE communications magazine, Vol. 40, November 2001; pp. 102-114.

9. Internet of things, available at: https://en.wikipedia.org/wiki/Internet_of_things (21 Apr 2019.)

10. Nikoukar, A., Raza, S., Poole, A., Günes, M., Dezfouli, B., "Low-Power Wireless for the Internet of Things Standards and Applications", IEEE Access, Vol. 6, November 2018, pp. 1-1., DOI: 10.1109/ACCESS.2018.2879189.

11. Filipe, L., Fdez-Riverola, F., Costa, N. and Pereira, A., "Wireless Body Area Networks for Healthcare Applications - Protocol Stack Review", International Journal of Distributed Sensor Networks, Vol. 2015, October 2015, pp. 1-23.

12. Riazul Islam, S. M., Kwak, D., Kabir, H., Hossain, M., Kwak, K. S., "The Internet of Things for Health Care- A Comprehensive Survey", The Journal for rapid open access publishing, 2015.

13. Mdhaffar, A., Chaari, T., Larbi, K., Jmaiel, M., Freisleben, B., "IoT-based health monitoring via LoRaWAN", IEEE EUROCON 2017 -17th International Conference on Smart Technologies, Ohrid, Macedonia, 2017, DOI: 10.1109/eurocon.2017.8011165

14. Datta, S. K., Bonnet, C., Gyrard, A., Ferreira da Costa, R. P., Boudaoud, K., "Applying Internet of Things for personalized healthcare in smart homes", 24th Wireless and Optical Communication Conference (WOCC), Taipei, Taiwan, 2015, DOI:10.1109/wocc.2015.7346198

15. Majumder, S., Aghayi, E., Noferesti, M., Memarzadeh-Tehran, H., Mondal, T., Pang, Z., Deen, M, J., "Smart Homes for Elderly Healthcare-Recent Advances and Research Challenges", Sensors, Vol. 17, No. 11, October 2017, DOI: 10.3390/s17112496

16. Bellagente, P., Depari, A., Ferrari, P., Flammini, A., Sisinni, E., Rinaldi, S., "M3IoT — Message-oriented middleware for M-health Internet of Things: Design and validation", 2018 IEEE International Instrumentation and Measurement Technology Conference, Houston, TX, USA, 2018, DOI:10.1109/i2mtc.2018.8409656

17. Zhang, X.M., Zhang, N., "An Open, Secure and Flexible Platform Based on Internet of Things and Cloud Computing for Ambient Aiding Living and Telemedicine", 2011 International Conference on Computer and Management (CAMAN), Wuhan, China, 2011, DOI: 10.1109/CAMAN.2011.5778905

18. You, L., Liu, C., Tong, S., "Community Medical Network (CMN): Architecture and implementation," 2011 Global Mobile Congress, Shanghai, China, 2011, DOI: 10.1109/GMC.2011.6103930

19. Rohokale, V. M., Prasad, N. R., Prasad, R., "A cooperative Internet of Things (IoT) for rural healthcare monitoring and control", 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), Chennai, India, 2011, DOI:10.1109/wirelessvitae.2011.5940920

20. Jara, A. J., Zamora-Izquierdo, M. A., Skarmeta, A. F., "Interconnection Framework for mHealth and Remote Monitoring Based on the Internet of Things", IEEE Journal on Selected Areas in Communications, Vol. 31, No. 9, 2013, pp. 47–65, DOI:10.1109/jsac.2013.sup.0513005

21. Chen, M., Ma, Y., Li, Y., Wu, D., Zhang, Y., Youn, C.-H., "Wearable 2.0: Enabling Human-Cloud Integration in Next Generation Healthcare Systems", IEEE Communications Magazine, Vol. 55, No. 1, January 2017, pp. 54–61, DOI: 10.1109/mcom.2017.1600410cm

22. Pramanik, P. K. D., Nayyar, A., Pareek, G., "WBAN: Driving e-healthcare Beyond Telemedicine to Remote Health Monitoring. Telemedicine Technologies", January 2019, pp. 89–119, DOI: 10.1016/b978-0-12-816948-3.00007-6

23. Khan, J. Y., Yuce, M. R., "Wireless Body Area Network (WBAN) for Medical Applications. New Developments in Biomedical Engineering", in New Developments in Biomedical Engineering, IntechOpen, Domenico Campolo, 2010, DOI: 10.5772/7598

24. Touati, F., Tabish, R., "U-Healthcare System: State-of-the-Art Review and Challenges. Journal of Medical Systems", Journal of Medical Systems, Vol. 37, No. 3, 2013, pp. 1-20, DOI:10.1007/s10916-013-9949-0

25. Zhang, Y., Sun, L., Song, H., Cao, X., "Ubiquitous WSN for Healthcare: Recent Advances and Future Prospects", IEEE Internet of Things Journal, Vol. 1, No.4, June 2014., pp. 311–318, DOI:10.1109/jiot.2014.2329462

26. X.200 : Reference Model of Open Systems Interconnection for CCITT applications, November 1988.

27. X.800 : Security architecture for Open Systems Interconnection for CCITT applications, ITU, March 1991.

28. Russell, B., Duren, D. V., "Practical Internet of Things Security", available at: https://www.researchgate.net/profile/Ali_Al-Qurabat2/post/Can_any_one_share_me_a_Book_of_Practical_Internet_of_Things_Security/attachment/5a415ea84cde266d587da2a7/AS%3A575551220207619%401514233512763/download/Brian+Russell%2C+Drew+Van+Duren-Practical+Internet+of+Things+Security-Packt+Publishing+%282016%29.pdf (20 Apr 2019.)

29. Culler, D. E., "The Internet of Every Thing - steps toward sustainability CWSN Keynote" available at: https://www.cs.berkeley.edu/~culler/talks/Culler-CWSN.pptx (20 Mar 2019.)

30. Maxino, T. C., "The Effectiveness of Checksums for Embedded Networks", master thesis, Carnegie Mellon University, Pittsburgh, Pennsylvania, USA, 2006.

31. Jonathan Hu, 6LoWPAN: Incorporating IEEE 802.15.4 into the IP architecture, available at: https://pdfs.semanticscholar.org/ab4a/681523f427a03aa1adbd3b8c6b01103ef969.pdf

32. Compression Format for IPv6 Datagrams in Low Power and Lossy Networks(6LoWPAN), Network Working Group, available at: https://tools.ietf.org/html/draft-ietf-6lowpan-hc-15

33. Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks, Internet Engineering Task Force, available at: https://tools.ietf.org/html/rfc6282

34. Garg, R., & Sharma, S. (2018). Modified and Improved IPv6 Header Compression (MIHC) Scheme for 6LoWPAN. Wireless Personal Communications, DOI:10.1007/s11277-018-5894-z

35. Bluetooth core specification, Bluetooth SIG, available at: https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=457080

36. Bluetooth 5 speed: How to achieve maximum throughput for your BLE application, available at: https://www.novelbits.io/bluetooth-5-speed-maximum-throughput/

37. LoRaWAN™ 1.1 Specification, available at: https://lora-alliance.org/sites/default/files/2018-04/lorawantm_specification_-v1.1.pdf (18 Mar 2019.)

38. Sigfox connected objects: Radio specifications, available at https://build.sigfox.com/sigfox-device-radio-specifications (18 Mar 2019.)

39. Sodhro, A. H., Chen, L., Sekhari, A., Ouzrout, Y., and Wu, W., "Energy efficiency comparison between data rate control and transmission power control algorithms for wireless body sensor networks", International Journal of Distributed Sensor Networks, Vol 14, No.1, 2018, https://doi.org/10.1177/1550147717750030

40. Šeketa, G., Ortiz, G., Wilches, C., Perdomo, O., Celić, L., Lacković, I., Zequera, M., Magjarević, R., "Simultaneous Measurement of Trunk Orientation and Centre of Pressure for Postural Stability Evaluation", IFMBE Proceedings, January 2015., pp. 363-366.

41. Džaja, D., Varga, M., Šeketa, G., Žulj, S., Celić, L., Lacković, I., Magjarević, R., "System for Assisted Exercising and Qualitative Exercise Assessment", IFMBE Proceedings, 2015,. pp. 682-686.

42. Žulj, S., Šeketa, G., Džaja, D., Celić, L., Magjarević, R., "Virtual reality system for assisted exercising using WBAN", IFMBE Proceeding, 2015., pp. 719-722.

43. Šeketa, G., Džaja, D., Žulj, S., Celić, L., Lacković, I., Magjarević, R., "Real-Time Evaluation of Repetitive Physical Exercise Using Orientation Estimation from Inertial and Magnetic Sensors", IFMBE Proceedings, Budapest, Hungary, 2015., pp. 11-15.

44. Zanesco, A., Sacerdoti, F., Esteve, A. B., Magjarević, R., Celić, L., "Wearable Sensor for Real-Time Monitoring of Exercise Routines", IFMBE Proceedings, 2014., pp. 355-359.

45. Pozaić, T., Džaja, D., Varga, M., Matec, I., Celić, L., Lacković, I., Magjarević, R., "Quantitative and Qualitative Assessment of Assisted Strength Exercising", IFMBE Proceedings, 2014., pp. 71-75.

46. "Propagation loss in free space/over flat terrain", avaialble at: https://www.cdt21.com/resources/siryo1.asp (12 May 2019.)

47. Yadav, S., Yadav, R.S., "A review on energy efficient protocols in wireless sensor networks", Wireless Networks, Vol.22, No.1, January 2016, pp. 335-350.

48. Tosi, J., Taffoni, F., Santacatterina, M., Sannino, R., Formica, D., "Performance Evaluation of Bluetooth Low Energy: A Systematic Review", Sensors, Vol. 17, December 2017.

49. Gomez, C., Oller, J., Paradells, J., "Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology", Sensors, Vol.12, No.9, 2012, pp. 11734-11753.

50. Adamu, M. Z., Ang, L. M., Seng, K. P., "Performance Evaluation of Ant-Based Routing Protocols for Wireless Sensor Networks", International Journal of Computer Science Issue, Vol. 9, June 2012.

51. Mikhaylov, K., Plevritakis, N., Tervonen, J., "Performance Analysis and Comparison of Bluetooth Low Energy with IEEE 802.15.4 and SimpliciTI", Journal of Sensor and Actuator Networks, Vol. 2, September 2013, pp. 589-613.

52. Al Ameen, M., Islam, S. M. R., Kwak, K., "Energy Saving Mechanisms for MAC Protocols in Wireless Sensor Networks", International Journal of Distributed Sensor Networks, Vol. 6, No. 1, October 2010, https://doi.org/10.1155/2010/163413

53. Pramanick, M., Basak, P., Chowdhury, C., Neogy, S., "Analysis of Energy Efficient Wireless Sensor Networks Routing Schemes," Fourth International Conference of Emerging Applications of Information Technology, Kolkata, 2014, pp. 379-384, DOI: 10.1109/EAIT.2014.69

54. Pour, N. K., "Energy Efficiency in Wireless Sensor Networks", doctoral thesis, Faculty of Engineering and InformationTechnology atThe University of Technology Sydney, Australia, 2015.

55. Kamyabpour, N., Hoang, D. B., "A Hierarchy Energy Driven Architecture for Wireless Sensor Networks", IEEE 24th International Conference on Advanced Information Networking and Applications Workshops, Perth, WA, 2010, pp. 668-673, DOI: 10.1109/WAINA.2010.46

56. Soua, R., Minet, P., "A survey on energy efficient techniques in wireless sensor networks", WNNC 2011 - 4th Joint IFIP Wireless and Mobile Networking Conference, Oct 2011, Toulouse, France, pp.1 – 9.

57. Rault, T., "Energy-efficiency in Wireless Sensor Networks", doctoral thesis, Université de Technologie de Compiègne, France, 2015.

58. Nordic Semiconductor, "nRF51 Series Reference Manual, version 3", available at: https://infocenter.nordicsemi.com/pdf/nRF51_RM_v3.0.pdf (10 Apr 2019.)

59. ATmega168 datasheet, "High Temperature Automotive Microcontroller", available at: http://ww1.microchip.com/downloads/en/DeviceDoc/Atmel-9365-Automotive-Microcontrollers-ATmega88-ATmega168_Datasheet.pdf (10 Apr 2019.)

60. Propagation Losses Through Common Building Materials, Magis Networks, Inc. Available at: https://www.am1.us/wpcontent/uploads/Documents/E10589_Propagation_Losses_2_and_5GHz.pdf, (10 June 2019.)

61. Indoor Path Loss, Digi, Available at: http://ftp1.digi.com/support/images/XST-AN005a-IndoorPathLoss.pdf, (10 June 2019.)

62. Abdullah, M. W., Fafoutis, X., Mellios, E., Klemm, M., Hilton, G. S., " Investigation into off-body links for wrist mounted antennas in bluetooth systems", 2015 Loughborough Antennas & Propagation Conference (LAPC), Loughborough, UK, 2015, DOI:10.1109/lapc.2015.7366050

63. Januszkiewicz, L., "Article Analysis of Human Body Shadowing Effect on Wireless Sensor Networks Operating in the 2.4 GHz Band", Sensors, Vol. 18, October 2018, pp. 3412.

64. Fafoutis, X., Tsimbalo, E., Zhao, W., Chen, H., Mellios, E., Harwin, W., Piechocki, R., Craddock, I., " BLE or IEEE 802.15.4: Which Home IoT Communication Solution is more Energy-Efficient", EAI Endorsed Transactions on Internet of Things, Vol. 2, No. 5, December 2016.

65. Fafoutis, X., Tsimbalo, E., Mellios, E., Hilton, G., Piechocki, R., Craddock, I., "A residential maintenance-free long-term activity monitoring system for healthcare applications", EURASIP Journal on Wireless Communications and Networking, Vol. 31, December 2016., DOI: 0.1186/s13638-016-0534-3

66. Piyare, R., Murphy, A. L., Kiraly, C., Tosato, P., Brunelli, D., "Ultra Low Power Wake-Up Radios: A Hardware and Networking Survey", IEEE communications surveys & tutorials, Vol. 19, No. 4, 2017, pp. 2117 - 2157.

67. Dementyev, A., Hodges, S., Taylor, S., Smith, J., "Power Consumption Analysis of Bluetooth Low Energy, ZigBee and ANT Sensor Nodes in a Cyclic Sleep Scenario", IEEE International Wireless Symposium (IWS), Beijing, China, 2013.

68. Wu, Y., Chaudhari, Q., Serpedin, E., "Clock Synchronization of Wireless Sensor Networks," IEEE Signal Processing Magazine, Vol. 28, No. 1, January 2011, pp. 124-138, DOI:10.1109/MSP.2010.938757

69. Vig, J. R., (2019). Quartz Crystal Resonators and Oscillators for Frequency Control and Timing Applications - A Tutorial, January 2007.

70. Filler, R. L., "The Acceleration Sensitivity of Quartz Crystal Oscillators: A Review", IEEE Transactions on Ultrasonics, Ferroelectrics and Frequency Control, Vol. 35, No. 3, May 1988, pp. 297-305.

71. Piwek, L., Ellis, D. A., Andrews, S., Joinson, A., "The rise of consumer health wearables: promises and barriers", Plos Medicine, Vol. 12, No.2, February 2016, https://doi.org/10.1371/journal.pmed.1001953

72. Mercer, K., Giangregorio, L., Schneider, E., "Acceptance of Commercially available wearable activity trackers among adults aged over 50 and with chronic illness: a mixed-methods evaluation", JMIR Mhealth Uhealth, Vol.4, No.1, January 2016, DOI:10.2196/mhealth.4225

73. Salifu, Y., Jeffrey, S., Abdul, H. B., "Older people, assistive technologies, and the barriers to adoption: A systematic review", International Journal of Medical Informatics, Vol. 94, October 2016, pp. 112–116, DOI: 10.1016/j.ijmedinf.2016.07.004

74. Lee, C., Coughlin, J. F., "Older adults'adoption of technology: An Integrated Approachto Identifying Determinants and Barriers ", Journal of Product Innovation Management, Vol.32, 2014, pp.747–759, DOI:10.1111/jpim.12176

75. Baig, M. M., GholamHosseini, H., Moqeem, A. A., Mirza, F., Lindén, M., "A systematic review of wearable patient monitoring systems– Current challenges and opportunities for clinical adoption", Journal of Medical Systems, Vol.41, No.7, July 2017, DOI:10.1007/s10916-017-0760-1

76. Peek, S. T. M., Aarts, S., Wouters, E. J. M., "Can smart home technology deliver on the promise of independent living? A Critical Reflection Based on the Perspectives of Older Adults", in Handbook of Smart Homes, Health Care and Well-Being, van Hoof, J., Demiris, G., Wouters, E. J. M. (eds.), Springer International Publishing Switzerland, January 2015, DOI:10.1007/978-3-319-01583-5_41

77. Matt, J., "The wearable revolution that has arrived...sort of", available at: http://designinteractive.net/6790/ (05 Jun 2019.)

78. Al Hogail, A., "Improving IoT technologyadoption through improving consumer trust", Technologies, Vol. 6, July 2018, DOI: 10.3390/technologies6030064

79. Ibarra-Esquer, J., González-Navarro, F., Flores-Rios, B., Burtseva, L., and Astorga-Vargas, M., "Tracking the Evolution of the Internet of Things Concept Across Different Application Domains", Sensors, Vol. 17, No.6, June 2017, pp. 1379, DOI: 10.3390/s17061379

80. Pham, V., Hagen, J., "Bluetooth security and threats", Norwegian Defence Research Establishment, available at: https://pdfs.semanticscholar.org/a41b/3c341fb6ddd16528eb2e558532258a35ea90.pdf (14 May 2019.)

81. Stephen, A. W., Sarma, S. E. , Rivest, R. L., Engels, D. W., "Security and privacy aspects of low-cost radio frequency identification systems", In Security in Pervasive Computing, Hutter D., Müller G., Stephan W., Ullmann M. (eds). Vol. 2802, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 2004, DOI:10.1007/978-3-540-39881-3_18

82. Schall, M. C., Sesek, R. F., Cavuoto, L. A., "Barriers to the adoption of wearable sensors in the workplace: a survey of occupational safety and health professionals", HumFactors, Vol. 60, No. 3., 2018, pp. 351–362, DOI:10.1177/0018720817753907

83. Kalantari, M., "Consumers' adoption of wearable tech-nologies: literature review, synthesis, and future research agenda", Int J Technol Market, Vol. 12, 2017, pp. 274–307, DOI:10.1504/IJTMKT.2017.10008634

84. Das, A. K., Pathak, P. H., Chuah, C. N. and Mohapatra, P., "Uncovering privacy leakage in ble network traffic of wearable fitness trackers", In Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications (HotMobile), New York, NY, USA, 2016, pp. 99–104.

85. Guide to BluetoothSecurity, NIST Special Publication 800-121, Revision 2, 2017, available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf (05 May 2019.)

86. Bluetooth SIG, "Specification of the Bluetooth system", February 2014.

87. Hassidim, A., Yossi, M., Moti, Y., Ziv, A., "Ephemeral identifiers: Mitigating tracking & spoofing threats to BLE beacons", available at: https://pdfs.semanticscholar.org/338c/de818bdeff25c4d1f4894bfcf8f60805248d.pdf (13 May 2019.)

88. Costello, K., "Gartner Says Worldwide Wearable Device Sales to Grow 26 Percent in 2019", available at: https://www.gartner.com/en/newsroom/press-releases/2018-11-29-gartner-says-worldwide-wearable-device-sales-to-grow- (13 May 2019)

89. Microsoft open specifications, "Bluetooth: advertising Beacon" February 2019.

90. Granlund, D., Holmlund, P., and Åhlund, C., "Opportunistic Mobility Support for Resource Constrained Sensor Devices in Smart Cities", Sensors, Vol. 15, No.3, March 2015, pp. 5112–5135, DOI: 10.3390/s150305112

91. Rigney, C., Livingston, S.W., Merit, A. R., Daydreamer, W. S., "Ed. Remote Authentication Dial in User Service (RADIUS)", IETF, RFC2865: Pleasanton, CA, USA, June 2000.

92. Jianming Zhu, and Jianfeng Ma., "A new authentication scheme with anonymity for wireless environments", IEEE Transactions on Consumer Electronics, Vol. 50, No.1, February 2004, pp. 231–235, DOI:10.1109/tce.2004.1277867

93. Chain, K., Kuo, W.C., Cheng, J. C., "A Novel Mobile Communications Authentication Scheme with Roaming Service and User Anonymity", Applied Sciences, Vol. 6, 2016, pp. 393, DOI: 10.3390/app6120393

94. Xu, G., Liu, J., Lu, Y., Zeng, X., Zhang, Y. and Li, X., "A novel efficient MAKA protocol with desynchronization for anonymous roaming service in Global Mobility Networks", Journal of Network and Computer Applications, Vol. 107, 2018, pp. 83–92. doi:10.1016/j.jnca.2018.02.003

95. Gope, P., Hwang, T., "An efficient mutual authentication and key agreement scheme preserving strong anonymity of the mobile user in global mobility networks", Journal of Network and Computer Applications, Vol 62., February 2016, pp. 1-8.

96. Lee, C. C., Hwang, M. S., Liao, I. E., "Security enhancement on a new authentication scheme with anonymity for wireless environments", IEEE Trans. Ind. Electron., Vol. 53, No. 5, October 2006, pp. 1683-16870.

97. Mun, H., Han, K., Yan, S. L., Chan, Y. Y., Choi, H. H., "Enhanced secure anonymous authentication scheme for roaming service in global mobility networks", Mathematical and Computer Modelling, Vol. 55, No.1, 2012, pp. 214-222.

98. Yoon, E. J., Yoo, K. Y., Ha, K. S., "A user friendly authentication scheme with anonymity for wireless communications", Computers & Electrical Engineering, Vol. 37, No. 3, May 2011, pp. 356-364.

99. Zhou, T., Xu, J., "Provable secure authentication protocol with anonymity for roaming service in global mobility networks", Computer Networks, Vol. 55, No. 1, January 2011, pp. 205-213.

100. Amin, R., Islam, S. H., Biswas, G. P., Khan, M. K., and Kumar, N., "A robust and anonymous patient monitoring system using wireless medical sensor networks", Future Generation Computer Systems, Vol. 80, March 2018, pp. 483–495, DOI:10.1016/j.future.2016.05.032

101. Kwon, A., AlSabah, M., Lazar, D., Dacier, M., Devadas, S., "Circuit Fingerprinting Attacks: Passive Deanonymization of Tor Hidden Services", available at: https://www.usenix.org/node/190967 (19 Mar 2019.)

102. Vermesan, O. et al., "The Next Generation Internet of Things – Hyperconnectivity and Embedded Intelligence at the Edge", available at: http://www.internet-of-things-research.eu/pdf/The_Next_Generation_IoT_Hyperconnectivity_and_Embedded_Intelligence_at_the_Edge_Research_Trends_IERC_2018_Cluster_eBook_978-87-7022-007-1_P_Web.pdf (21 May 2019)

103. P. Dutta, "The internet of things has a gateway problem", In Proceedings of the 16th International Workshop on Mobile Computing Systems and Applications (HotMobile), New York, NY, USA, 2015, pp. 27– 32, DOI: 10.1145/2699343.2699344

104. CC2541 datasheet, "2.4-GHzBluetooth™lowenergyandProprietarySystem-on-Chip", January 2012.

105. Agarwal, P., Alam, M., Islamia, J. M., "Investigating IoT Middleware Platforms for SmartApplication Development", New Delhi, India, October 2018, https://arxiv.org/ftp/arxiv/papers/1810/1810.12292.pdf

106. "Mosquitto Github repository", available at: https://github.com/eclipse/mosquitto

107. Cortex-M0 Technical Reference Manual, "Instruction Set Sumary", 2009.

108. Celić, Luka; Varga, Matija; Pozaić, Tomislav; Žulj, Sara; Džaja, Dominik; Magjarević, Ratko WBAN for Physical Activity Monitoring in Health Care and Wellness. // IFMBE Proceedings Volume 39, 2013 / Mian Long (ur.). Heidelberg: Springer Berlin Heidelberg, 2013. pp. 2228-2231

109. Celic, L., Magjarevic, R., "Seamless Connectivity Architecture and Methods for IoT and Wearable Devices", Automatika, DOI: 10.1080/00051144.2019.1660036

110. Padgette, J. et al. "Guide to Bluetooth security", NIST Special Publication 800-121, revision 2, available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf (15 May 2019)

111. Smart, N., "ECRYPT II yearly report on algorithms and keysizes (2011-2012)", available at: https://cordis.europa.eu/docs/projects/cnect/6/216676/080/deliverables/002-DSPA20.pdf (15 May 2019)

112. Smart, N. P., "Algorithms, key size and protocols report, ECRYPT 2018", available at: http://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf (15 May 2019)

113. Suárez-Albela, M., Fraga-Lamas, P., Fernández-Caramés, T. M. A., "Practical evaluation on RSA and ECC-based cipher suites for IoT high-security energy-efficient fog and mist computing devices", Sensors, Vol. 18, No. 11, November 2018, DOI: 10.3390/s18113868.

Figure list

Table list

Biography

Born in Pula, Luka Celić graduated from the University of Zagreb, Faculty of Electrical Engineering and Computing in 2011. As a proactive student and technology enthusiast, he won five different student awards during his studies, including the prestigious Rector's Award of the University of Zagreb. His bachelor's degree and master degree was completed under the mentorship of Professor Ratko Magjarević, Ph.D. After completing his studies, he was employed at the University of Zagreb, Faculty of Electrical Engineering and Computing as a research assistant on the FP7 project *Advanced solution for Supporting Cardiac Patients in Rehabilitation* - HeartWays under the leadership of Professor Ratko Magjarević. In the next three and a half years, the HeartWays project was successfully completed. Luka joined the team of Professor Magjarević which just received the project Technology Platform for New ICT Strategies in diabetes Therapy and Control - DiabICT. In early 2016, he moved to Dublin, Ireland, and was employed by a consulting firm specializing in integration and development of customer service software. In late 2016 he moved position to Accenture, a global corporation with nearly half a million employees at the Global Centre for Innovation, dedicated to providing innovation guidance and services to corporate clients. At the end of 2018, he was hired as the Head of Innovation and Solution at Web Summit, which organises one of the world's largest start-up conferences. In mid-2019, he took up the position of Assistant Vice President for a finance company in Dubai.

Throughout his career, he published as author or co-author, articles in journals and conferences where he has equally represented papers at scientific and health conferences. Throughout his career, his guiding principles of action and learning have been to respect others' knowledge, skills and experience. Knowledge gained through scientific work helped him to adapt to technologies with which he had no previous contact. Equally, the knowledge and principles of the economy assisted him in scientific research with a view to applicable research and development.

Bibliography

1. Celić, Luka; Magjarević, Ratko Seamless Connectivity Architecture and Methods for IoT and Wearable Devices. Automatika – Journal for Control, Measurement, Electronics, Computing and Communications (2019) doi:10.1080/00051144.2019.1660036

2. Žulj, Sara; Celić, Luka; Grgurević, Mladen; Prašek, Manja; Magjarević, Ratko Pilot Project: ICT System for Management and Self- Management of Diabetes. International Conference on Biomedical and Health Informatics. ICBHI 2015. IFMBE Proceedings, vol 64 / Zhang, Yuan-Ting ; Carvalho Paulo ; Magjarevic Ratko (ur.). Singapore: Springer, 2018., pp. 199-203 doi:10.1007/978-981-10-4505-9_45

3. Žulj, Sara; Šeketa, Goran; Džaja, Dominik; Šklebar, Filip; Drobnjak, Siniša; Celić, Luka; Magjarević, Ratko Supporting Diabetic Patients with a Remote Patient Monitoring Systems. IFMBE Proceedings book series (IFMBE, volume 60) Bucaramanga, Santander, Kolumbija, 2016. pp. 577-580

4. Begovac, Juraj; Šeketa, Goran; Celić, Luka; Lacković, Igor; Magjarević Ratko Quality of Human Activities Measurement from Accelerometer Data of a Smartphone. IFMBE Proceeding Volume 45 Lacković, Igor ; Vasić, Darko (ur.). Cham Heidelberg New York Dordrecht London: Springer, 2015., pp. 268-272

5. Šeketa, Goran; Ortiz, Gabriel; Wilches, Carlos; Perdomo, Oscar; Celić, Luka; Lacković, Igor; Zequera, Martha; Magjarević, Ratko Simultaneous Measurement of Trunk Orientation and Centre of Pressure for Postural Stability Evaluation. IFMBE Proceedings Volume 45 / Lacković, Igor ; Vasić, Darko (ur.). Cham Heidelberg New York Dordrecht London: Springer, 2015., pp. 363-366

6. Džaja, Dominik; Varga, Matija; Šeketa, Goran; Žulj, Sara; Celić, Luka; Lacković, Igor; Magjarević, Ratko System for Assisted Exercising and Qualitative Exercise Assessment. // IFMBE Proceedings Volume 45 / Lacković, Igor ; Vasić, Darko (ur.). Cham Heidelberg New York Dordrecht London: Springer, 2015., pp. 682-686

7. Žulj, Sara; Šeketa, Goran; Džaja, Dominik; Celić, Luka; Magjarević, Ratko Virtual reality system for assisted exercising using WBAN. // IFMBE Proceeding Volume 45 / Lacković, Igor ; Vasić, Darko (ur.). Cham Heidelberg New York Dordrecht London: Springer, 2015., pp. 719-722

8. Šeketa, Goran; Džaja, Dominik; Žulj, Sara; Celić, Luka; Lacković, Igor; Magjarević, Ratko Real-Time Evaluation of Repetitive Physical Exercise Using Orientation Estimation from Inertial and Magnetic Sensors. // IFMBE Proceedings Volume 50 / Jobbagy, Akos (ur.). Budimpešta, Mađarska: Springer, 2015., pp. 11-15

9. Zanesco, Antonio; Sacerdoti, Francesco; Esteve, Angel Blanch; Magjarević, Ratko; Celić, Luka Wearable Sensor for Real-Time Monitoring of Exercise Routines. // IFMBE Proceedings Vol. 42 / Lacković, Igor ; de Carvalho, Paulo ; Zhang, Yuan-Ting ; Magjarević, Ratko (ur.). Cham Heidelberg New York Dordrecht London: Springer, 2014., pp. 355-359

10. Pozaić, Tomislav; Džaja, Dominik; Varga, Matija; Matec, Ivan; Celić, Luka; Lacković, Igor; Magjarević, Ratko Quantitative and Qualitative Assessment of Assisted Strength

Exercising. // IFMBE Proceedings Vol. 42 / Lacković, Igor ; de Carvalho, Paulo ; Zhang, Yuan-Ting ; Magjarević, Ratko (ur.). Cham Heidelberg New York Dordrecht London: Springer, 2014., pp.. 71-75

11. Celić, Luka; Varga, Matija; Pozaić, Tomislav; Žulj, Sara; Džaja, Dominik; Magjarević, Ratko WBAN for Physical Activity Monitoring in Health Care and Wellness. // IFMBE Proceedings Vol. 39, 2013 / Mian Long (ur.). Heidelberg: Springer Berlin Heidelberg, 2013., pp.. 2228-2231

12. Celić, Luka; Trogrlić Darko; Paladin Ivan; Prašek Manja; Magjarević, Ratko Integration of Measurement Devices Supporting Diabetic Patients into a Remote Care System. // IFMBE Proceedings 37 / Akos Jobbagy (ur.). Budimpešta: Springer, 2011., pp.. 39-42

13. Varga, Matija; Pozaić Tomislav; Žulj Sara; Celić Luka; Magjarević Ratko Raspoznavanje i kvantifikacija tjelesne aktivnosti. // Proceedings of MIPRO 2011, 1 (2011), pp. 130-134.

14. Žulj, Sara; Celić, Luka; Drobnjak, Siniša; Magjarević, Ratko Evidence based Information Fusion for Enabling Personalized Treatment of Diabetic Patients. // The IEEE International Conference on Biomedical and Health Informatics (BHI2016) Las Vegas, Nevada, SAD, 2016.

Biografija

Luka Celić rođen je u Puli. Diplomirao je na Sveučilištu u Zagrebu, Fakultetu elektrotehnike i računarstva 2011 godine. Kao aktivan student i zaljubljenik u tehnologiju, tijekom studija osvojio je pet studentskih nagrada, uključujući i prestižnu Rektorovu nagradu Sveučilišta u Zagrebu. Studij prvostupnika i diplomski je završio pod mentorstvom prof. dr. sc. Ratka Magjarevića. Po završetku studija, zapošljave se na Fakultetu elektrotehnike i računarstva Sveučilišta u Zagrebu kao znanstveni novak na FP7 projektu *Advanced solution for Supporting Cardiac Patients in Rehabilitation* - HeartWays voditelja prof. dr. sc. Ratka Magjarevića. U sljedeće tri i pol godine uspješno završavaju projekt HeartWays. Luka se uključuje u projekt „Tehnološka platforma za nove ICT strategije u terapiji i kontroli dijabetesa – diabICT“. Pocetkom 2016. godine seli se u Dublin, Irsku i zapošljava se u konzultantskoj tvrtki specijaliziranoj za integraciju i razvoj sustava za rad s korisnicima. Krajem 2016 godine zapošljava se u globalnoj korporaciji Accenture sa skoro pola milijuna zaposlenika u Centru za inovacije, namijenjenom pružanju usluga korporacijama. Krajem 2018 godine zapošljava se kao voditelj inovacija i solucija u Websummit tvrtki, koja organizira najveće svjetske start-up konferencije. Sredinom 2019 zaposlio se kao pomoćnik potpredsjednika za financijsku tvrtku u Dubaiju.

Tijekom svoje karijere, publicirao je kao autor ili koautor članke u časopisima i zbornicima konferencija te predstavljao radove na znanstvenim i zdravstvenim konferencijama i skupovima. Tijekom svoje karijere, kao vodeća načela djelovanja i učenja bili su mu poštivanje i uvažavanje tuđih znanja, vještina i iskustva. Znanja stečena kroz znanstveno djelovanje pomogla su mu da se prilagodi tehnologijama s kojima prethodno nije imao doticaja. Jednako tako znanja i načela gospodarstva pomogla su mu u znanstvenom istraživanju s ciljem na primjenjiva unaprjeđenja.