UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN INFORMACIJSKE TEHNOLOGIJE

Zaključna naloga

NFC - Near Field Communication

(NFC - Near Field Communication)

Ime in priimek: Matej Filipović
Študijski program: Računalništvo in informatika
Mentor: izr. prof. dr. Peter Korošec

Koper, september 2014

Ključna dokumentacijska informacija

Ime in PRIIMEK: Matej FILIPOVIĆ

Naslov zaključne naloge: NFC - Near Field Communication

Kraj: Koper

Leto: 2014

Število listov: 50 Število slik: 15 Število tabel: 1

Število referenc: 40

Mentor: izr. prof. dr. Peter Korošec

Ključne besede: NFC, RFID, pametni, telefoni, plačila, varnost, Bluetooth

Izvleček:
Zaključna naloga predstavlja tehnologijo NFC (ang. Near Field Communication), ki se iz leta v leto bolj razvija in tako tudi njena uporabnost v vsakdanjem svetu. Glavni cilj zaključne naloge je predstaviti NFC na razumljiv način in prikazati možnosti ter prednosti njene uporabe. Na začetku zaključne naloge je predstavljena tehnologija RFID, ki je predhodnik tehnologije NFC, nato je opisano kako se je NFC razvil iz RFID-a in katere so njune skupne značilnosti. Sledi podroben opis delovanja NFC-ja, kakšne nevarnosti obstajajo pri uporabi te tehnologije in kako se izognemo le-tem. Za konec so predstavljeni primeri uporabe tehnologije NFC, kjer je predstavljena njena uporaba v realnem svetu in primerjava z drugimi tehnologijami, kot sta Bluetooth in Bluetooth Low Energy. Namen zaključne naloge je seznaniti ljudi s to tehnologijo in s tem povečati njeno uporabo.

Key words documentation

Name and SURNAME: Matej FILIPOVIĆ

Title of final project paper: NFC - Near Field Communication

Place: Koper

Year: 2014

Number of pages: 50 Number of figures: 15 Number of tables: 1

Number of references: 40

Mentor: Assoc. Prof. Peter Korošec, PhD

Keywords: NFC, RFID, smart, phone, payments, security, Bluetooth

Abstract:
The final thesis will present the NFC (Near Field Communication) technology, whose development is rapidly raising and so does its applicability in our day-to-day routine. The main objective of this research is to present the NFC in an understandable way and to show the possibilities and advantages of its use. As an introduction to the thesis RFID technology (a predecessor of NFC) is presented. Following that is a description of the evolution from RFID to NFC, including their common features. The thesis then further deatils the NFC functionality, its safety and possible dangers of using this technology. In conclusion examples of the use of NFC technology are presented, as well as the application of NFC technology in the real world. A comparison with other technologies is given, such as Bluetooth and Bluetooth Low Energy. The purpose of this thesis is to acquaint people with NFC and thereby increase its use.

Zahvala

Zahvalil bi se rad mentorju izr. prof. dr. Petru Koroščcu za pomoč pri izdelavi in oblikovanju zaključne naloge. Zahvalil bi se svoji družini, ki me je ob študiju moralno in finančno podpirala ter osebju UP FAMNIT, brez katerih ne bi pridobil ustreznega znanja.

Kazalo vsebine

Seznam tabel

Seznam slik

Seznam kratic

NFC	Komunikacija s sosednjim poljem (ang. Near field communication)
RFID	Radiofrekvenčna identifikacija (ang. Radio frequency identification)
RF	Radiofrekvenca (ang. Radio frequency)
UHF	Ultra visoka frekvenca (ang. Ultra high frequency)
POS	Prodajno mest (ang. Point of sale)
EPC	Elektronska šifra izdelka (ang. Electronic product code)
ISO	Mednarodna organizacija za standardizacijo (ang. International organisation of standardisation)
IEC	Mednarodna komisija za elektrotehniko (ang. International electrotechnical commission)
ETCI	Evropski inštitut za telekomunikacijske standarde (ang. European Telecommunications standards institute)
FCC	Zvezna komisija za komunikacije (ang. Federal communications commission)
NFCIP	Vmesniški protokol komunikacije s sosednjim poljem (ang. Near field communication Interface and protocol)
ASK	Amplitudna modulacija (ang. Amplitude shift keying)
AES	Napredni standard šifriranja (ang. Advanced encryption standard)
BLE	Nizko energijski Bluetooth (ang. Bluetooth low energy)

1 UVOD

V življenjskih situacijah se velikokrat srečamo z različnimi tehnologijami, ki nam pohitrijo in olajšajo vsak dan, ena izmed njih je NFC. Ta posamezniku lahko zelo olajša delovanje mnogih storitev, med njimi plačevanje, omogočanje dostopa v stavbe ter uporaba mobilnega telefona namesto vozovnic za javni promet. NFC omogoča varno, hitro in povsod dosegljivo interakcijo, ki jo lahko opravimo z napravo, ki jo imamo vedno pri sebi. V zadnjih letih se je uporaba NFC sistema razširila s prihodom pametnih telefonov, saj večina vsebuje NFC tehnologijo.

NFC tehnologija omogoča komunikacijo med dvema NFC napravama kot tudi branje podatkov iz NFC oznake oz. zapis podatkov na le-te. NFC oznaka je čip z anteno, ki vsebuje majhne količine podatkov. Običajno so oznake oblikovane kot nalepke, kartice ali plakati. V primerih, ko svoj mobilni telefon z NFC-jem položite na POS terminal za plačilo računa v trgovini, se z njim približate muzejskem eksponatu in tako pridobite njegove podatke, ali približate telefone s svojim prijateljem in tako delite najnovejše igre, se lahko vidi, da nam NFC tehnologija omogoča plačevanje, igranje in hitro učenje.

Če primerjamo NFC tehnologijo z drugimi tehnologijami vidimo, da je NFC najboljša rešitev za varno plačevanje, ob tem tehnologija omogoča hitro povezljivost in je zelo enostavna za uporabo, zato jo dan danes uporabljamo za plačevanje, pridobivanje podatkov iz NFC oznak in pošiljanje podatkov med dvema napravama NFC.

V drugem poglavju bo predstavljen RFID, ki je predhodna tehnologija NFC-ja. V tretjem poglavju bo podrobno predstavljena tehnologija NFC. V četrtem poglavju bo predstavljena primerjava NFC-ja z drugimi tehnologijami, kot sta Bluetooth in Bluetooth Low Energy. V petem poglavju bodo predstavljeni primeri uporabe tehnologije NFC. Zaključno nalogo bom zaključil s predstavitvijo prihodnosti tehnologije NFC.

Motivacijo za izdelavo ključne naloge sem dobil, ker sem opazil pri prijateljih in družini, da nihče ne ve kaj je NFC in kako se ta tehnologija uporablja. Čeprav tehnologija obstaja od leta 2004 in je zelo uporabna, njena uporabnost ni vidna, če jo ljudje ne bodo znali uporabljati.

2 PREDHODNE TEHNOLOGIJE

2.1 RFID

Radio frekvenčna identifikacija (ang. Radio Frequency Identification - RFID) je brezžična ter brezkontaktna uporaba radio-frekvenčnih elektromagnetnih polj za prenos podatkov. Namenjena je za samodejno prepoznavanje in sledenje oznak, ki so pritrjene na predmete. Oznake, ki vsebujejo elektronsko shranjene informacije, so z napajanjem berljive na kratkih razdaljah (nekaj metrov) preko magnetnih polj z elektromagnetno indukcijo. Le-te lahko uporabljajo lokalni vir energije, kot so baterije, ali pa nimajo baterije, temveč zbirajo energijo iz elektromagnetnega polja in se nato obnašajo kot pasivni odzivnik, ki oddaja mikrovalove ali UHF radio valove (npr. elektromagnetna sevanja pri visokih frekvencah). Oznake, ki za vir energije uporabljajo baterije, lahko delujejo na več sto metrih in za razliko od črtne kode, le-te ne potrebujejo biti v vidnem polju čitalnika in so lahko vgrajene v predmet, ki mu sledimo.

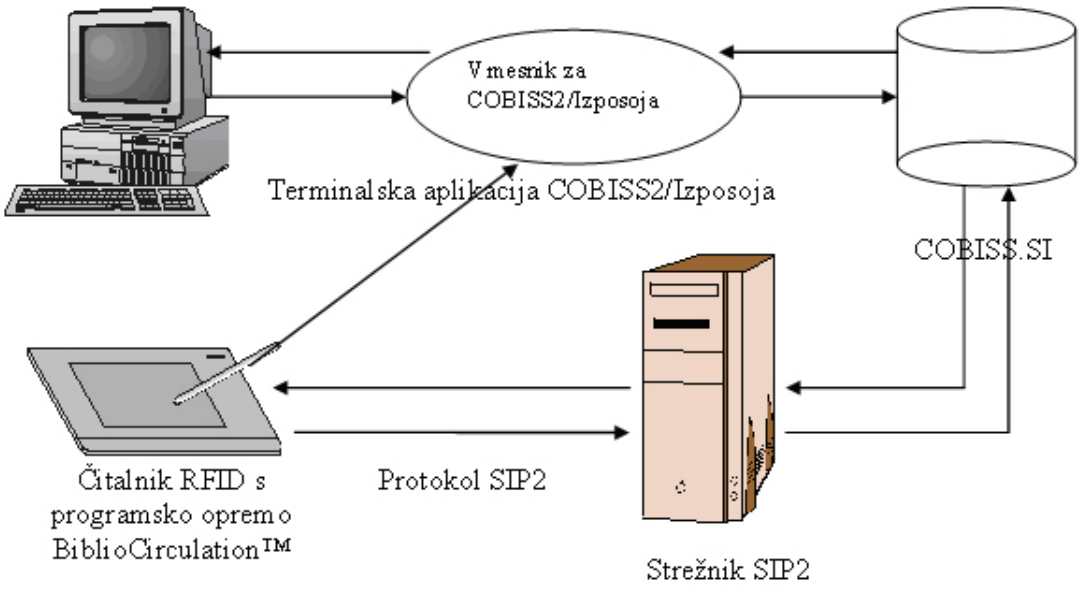
Ne glede ali se tega zavedamo, predstavlja RFID sestavni del našega življenja. Z RFID sistemi olajšamo in pohitrimo določene procese, kot so na primer dostopanje v zavarovana področja, kjer je potrebna avtentikacija ali plačilo cestnin na avtocestah. V obeh primerih zmanjšamo število delavcev in pohitrimo postopek ter se tako posledično povečata produktivnost sistema in naše udobje.

RFID se uporablja v tisočih aplikacijah kot so:

- preprečevanje kraje vozila, kjer pri vžigu vozila RFID bralec na volanskem drogu prebere pasivno RFID oznako v plastičnem ohišju okoli ključa. V primeru nepravilne identifikacijske številke avto enostavno ne vžge.
- preprečevanje kraje v trgovini, kjer je RFID oznaka nameščena v plastičnih zaščitah na izdelkih in v primeru, da nekdo želi izdelek odnesti iz trgovine, RFID bralci pri izhodu zaznajo signal RFID oznake in se sproži alarm.
- pobiranje cestnine brez ustavljanja, kjer je RFID oznaka nameščena na napravi, ki jo imamo v vozilu, RFID bralci pa so nameščeni na cestninskih postajah. Ko pripeljemo vozilo v bližino RFID bralca, ta prebere RFID oznako in odbije znesek na našem računu.

- pridobivanje vstopa v stavbe, avtomatizacija parkiranja in zagotavljanje dostopa do žičnic na smučišču uporabljajo podoben način uporabe RFID-ja, kjer je RFID oznaka nameščena v kartici, ki jo uporabnik prisloni k RFID bralcu, ki je nameščen tam kjer je potrebna avtentikacija. Če bralec ne prebere ustrezen id iz oznake ne dovoli uporabniku vstop.

- izposoja knjig v knjižnici, kjer ima vsaka knjiga svojo RFID oznako. Pri izposoji knjig uporabnik položi knjigo po knjigo na napravo, ki med drugim vsebuje RFID bralca, ki zazna katere knjige smo položili. Preko strežnika se prenesejo podatki na podatkovno bazo COBISS.SI, kjer preko aplikacije na prej omenjeni napravi potrdimo izposojo ali jo zavržemo. Predstavljen sistem lahko vidimo na 1.



Slika 1: Izposoja knjig s pomočjo RFID-ja v slovenskih knjižnicah [10].

Na splošno je RFID označen kot uporaba enostavne naprave na enem koncu radiofrekvenčne povezave, ki je povezana s kompleksnejšo napravo na drugem koncu. Preproste naprave (pogosto imenovane oznake ali odzivniki) so majhne in poceni, ter se lahko ekonomično razporedijo na predmete v zelo velikem številu. Bolj zapletene naprave (pogosto imenovane bralci ali čitalniki) so bolj sposobni in so običajno povezani z gostiteljskim računalnikom ali omrežjem, kjer se izvajajo računske operacije bistvenega pomena za izvajanje aplikacije.

Oznake lahko pošljejo podatke na bralca z ustvarjanjem, moduliranjem in oddajanjem radijskega signala. Uporabljene so različne tehnike modulacije in kodiranja. Obstajajo RFID sistemi, ki so namenjeni samo za branje (podatki se prenesejo samo v eni smeri, od oznake do bralca) ali za branje in pisanje (dvosmerna komunikacija). Tipičen RFID sistem prenaša podatke iz oznake do bralca, tako da bralec pošlje moduliran signal do oznake, nato oznaka prebere shranjene podatke v svojem pomnilniku in s šifriranjem naloži shranjene podatke iz pomnilnika na anteno oznake. Tak signal je moduliran in poslan s šifriranimi informacijami. Ta moduliran signal sprejme čitalnik bralca, ga demodulira z uporabo homodinskega sprejemnika (ang. homodyne receiver) [23] in dekodira njegov izhod v obliki digitalnih podatkov, ki vsebujejo podatke shranjene v oznaki. V postopku pretvorbe signala je homodinskem sprejemniku demoduliran povratni signal oznake s pomočjo vgrajenega amplitudnega demodulatorja, ki se nahaja v mešalniku. Signal je nato generiran v I/Q kanal signalov, v katerem opazimo spremembe v magnitudi (ali amplitudi) in fazi sinusnega vala. Pri pošiljanju podatkov iz bralca na oznako amplituda bralca modulira (shrani podatke v amplitudo valovanja) prenesen radijski signal, ki ga prejme oznaka. Podatki so lahko uporabljeni za nadzor delovanja oznake, ali pa za shranjevanje podatkov nanjo. Več podatkov o modulaciji se nahaja v poglavju 2.2.

Od leta 1600 do leta 1800 so se začele pospešeno razvijati znanosti elektrotehnike, magnetizma in optike, in tako je leto 1800 zaznamovalo začetek razumevanja elektromagnetne energije. Angleški eksperimentalni znanstvenik Michael Faraday je leta 1864 pokazal, da sta radijski in svetlobni signal obliki elektromagnetne energije. Istega leta je Škotski fizik James Clerk Maxwell objavil svojo teorijo o elektromagnetizmu, ki jo je potrdil nemški fizik Heinrich Rudolf Hertz (1887). Poleg tega je Hertz uspel raziskati in proizvesti elektromagnetne valove oz. radijske valove. Leta 1896 je Guglielmo Marconi demonstriral prvi uspešen prenos radijskih valov preko atlantskega oceana. V začetku 20. stoletja (1906) je Ernst F.W. Alexanderson demonstriral prvo neprekinjeno generiranje in prenašanje radijskih signalov. Ta dosežek označuje začetek moderne radijske komunikacije, kjer so vsi vidiki radijskih valov nadzorovani. Leta 1939 so izumili tudi radar, ki je bil eden od bolj pomembnih tehnoloških dosežkov med 2. svetovno vojno. Radar pošilja radijske valove za odkrivanje in lociranje objekta z odbojem radijskih valov, preko katerih se lahko določi lokacijo in hitrost objekta. Pomembnost radarja je hitro opazila vojska, tako da je zgodnji razvoj zavit v skrivnost. Ker je ena od oblik RFID-a kombinacija radijske tehnologije oddajanja in tehnologije radarja, ni čudno, da se je zamisel RFID sistema pojavila prav ob radarjevem razvoju.

Prvi pravi prednik modernega RFID-a je naprava, ki jo je patentiral Mario Cardullo, 23. 1. 1973. To je bil prvi radijski oddajnik s pomnilnikom. Prvotna naprava je bila pasivna in je imela 16 bitni pomnilnik, uporabljala pa naj bi se kot naprava za

cestnine. Osnovni Cardullov patent zajema uporabo radio frekvenc, zvoka in svetlobe, ki bi bila uporabljena kot prenosni medij [7]. Prvotni poslovni načrt, ki je bil predstavljen medijem leta 1969 je pokazal uporabo v transportu (identifikacijo avtomobilov, avtomatski cestninski sistem, elektronske registrske tablice, usmerjanje vozil), bančništvu (elektronske čekovne knjižice, elektronske kreditne kartice), na področju varnosti (identifikacija osebja, avtomatska vrata) in zdravstvu (identifikacija, zgodovina bolnikov).

V tem času je tudi ameriška vlada začela razvijati RFID sisteme. V letu 1970 so v državnem laboratoriju v Los Alamosu, po zahtevi ministrstva za energijo, začeli razvijati sistem za sledenje jedrskih materialov. Skupina znanstvenikov je razvila koncept pri katerem so odzivnike dali v vrata tovornjakov, bralce pa na vhodna vrata varovanih objektov. Antena v vhodnih vratih bi zbudila odzivnik v tovornjaku, ki bi odgovoril z identifikacijsko številko, kot tudi z drugimi podatki (npr. identifikacija voznika). Ta sistem je bil komercializiran v 1980-ih, ko so Los Alamosovi znanstveniki, ki so delali na projektu le-tega zapustili z namenom ustanovitve podjetja za razvoj avtomatiziranih plačilnih cestninskih sistemov. Ti sistemi so se začeli uporabljati na cestah, mostovih in predorih po celem svetu.

Na zahtevo ministrstva za kmetijstvo so v Los Alamosu razvili pasivne RFID oznake za sledenje krav. Obstajal je namreč problem sledljivosti hormonov in zdravil, ki naj bi jih krave prejele ob bolezni, in sicer nemogoče je bilo natančno določiti ali so vse krave prejele pravilen odmerek, ali je slučajno katera prejela dvojnega. V Los Alamosu so se domislili pasivnega RFID sistema, ki je uporabljal ultra visoke frekvenčne (UHF) signale. Naprava je dobila energijo iz bralca in preprosto "odbila"nazaj moduliran signal k bralcu z uporabo tehnike znane pod imenom povratnega signala (ang. backscatter) [39]. Kasneje so podjetja razvila nizko frekvenčni sistem (125 kHz), ki vsebuje manjše oddajnike, kateri so vgrajeni v steklo in se lahko vbrizgajo pod kožo krave. Ta sistem mnogi uporabljajo še danes.

Sčasoma so podjetja komercializirala 125 kHz sisteme in so začela uporabljati radijski spekter z visoko frekvenco (13,56 MHz), ki je bila neregulirana in neuporabljena v številnih predelih sveta. Visoka frekvenca je ponujala hitrejši prenos podatkov. Podjetja, zlasti tista v Evropi, so jo začela uporabljati za sledenje zabojnikov za ponovno uporabo. Danes se 13,56 MHz RFID sistemi uporabljajo za nadzor dostopa, plačilne sisteme, brezkontaktne pametne kartice, kot naprave proti kraji v avtomobilih, itd.

V začetku 1990-ih so IBM-ovi inženirji dodatno razvili koncept iz Los Alamosa in patentirali RFID sistem ultra visoke frekvence (UHF). UHF omogoča daljšo razdaljo branja (do 6 metrov v dobrih pogojih) in hitrejši prenos podatkov. IBM je naredil nekaj testnih primerov z Wal-Martom toda nikoli niso komercializirali rešitve. Ko je IBM zašel v finančne težave v sredini 1990-ih, je prodal patente Intermec-u, ponudniku

sistemov črtnih kod. Tako so bili kasneje Intermecovi RFID sistemi nameščeni v številnih različnih aplikacijah, od sledenja skladiščnega materiala do kmetijstva. Ampak RFID tehnologija je bila ta čas draga zaradi nizkega obsega prodaje in pomanjkanja mednarodnih standardov.

UHF RFID je dobil nov zagon leta 1999, ko so Uniform Code Council, EAN international, Procter and Gamble in Gillette zbrali sredstva za vzpostavitev Auto-ID centra na Massachusetts Institute of Technology (MIT). Dva profesorja na inštitutu, David Brock in Sanjay Sarma, sta raziskovala možnost uvedbe nizkocenovnih RFID oznak za vse produkte, namenjeno za sledenje po dobavni verigi. Njuna ideja je bila, da na oznako dajo samo eno informacijo, serijsko številko, in tako znižata njeno ceno, saj bi bil preprost mikročip, ki shranjuje zelo malo informacij cenejši za izdelavo kot kompleksnejši čip z več pomnilnika. Podatki, povezani s serijsko številko na oznaki bi bili shranjeni v podatkovni bazi, ki je dostopna preko interneta.

Sarma in Brock sta bistveno spremenila način mišljenja ljudi o RFID-u v dobavni verigi. Pred tem so bile oznake mobilne podatkovne baze, ki so prenašale informacije o produktu ali kontejnerju na katerem so se nahajale. RFID sta obrnila v omrežno tehnologijo, ki povezuje predmete z internetom preko oznake. Za podjetja je bila to pomembna sprememba, saj je prodajalec lahko samodejno sporočil poslovnemu partnerju, kdaj je pošiljka zapustila dok v proizvodnem obratu ali skladišču in trgovec je lahko samodejno sporočil proizvajalcu kdaj je blago prispelo.

Med letoma 1999 in 2003, je Auto-ID pridobila podporo več kot 100 velikih podjetij, ameriškega ministrstva za obrambo in veliko ključnih prodajalcev RFID-a. Odprli so raziskovalne laboratorije v Avstraliji, Veliki Britaniji, Švici, na Japonskem in Kitajskem. Razvili so dva vmesniška protokola, ki sta zasnovana na radijski komunikaciji (Class 1 in Class 2), Electronic Product Code (EPC) shemo oštevilčenja in omrežno arhitekturo za iskanje podatkov, povezanih z RFID oznako.

Da so dosegli obsežno uporabo RFID sistemov v dobavni verigi, je bilo potrebno RFID standardizirati. Za zagotovitev globalne interoperabilnosti proizvodov so številne organizacije ustanovile številne standarde za RFID [40]. Ti standardi so vsebovali skladnost, učinkovitost in interoperabilnost testov.

Obstaja več organov za standardizacijo, ki sodelujejo pri razvoju in opredelitvi RFID tehnologije, vključno z:

- International Organisation of Standardisation (ISO),
- EPCglobal,
- European Telecommunications Standards Institute (ETSI), in
- Federal Communications Commission (FCC).

RFID frekvence ureja ISO 18000, družina standardov RFID brezžičnega vmesnika. Celoten sklop je izšel leta 2004:

- ISO 18000-1 - globalno uveljavljeni generični parametri brezzičnega vmesnika,
- ISO 18000-2 - standard za frekvence pod 135 kHz,
- ISO 18000-3 - standard za frekvenco 13,56 MHz,
- ISO 18000-4 - standard za frekvenco 2,45 GHz,
- ISO 18000-6 - standard za frekvence od 860 do 960 MHz, in
- ISO 18000-7 - standard za frekvenco 433 MHz.

Obstajajo tudi starejši standardi RFID tehnologije, kot na primer standard sistema sledenja goveda (ISO 11785), plačilne kartice, ki temeljijo na oznakah (ISO 14443), sistem elektronskega plačila cestnine (ISO 15653) ter mnogi drugi.

2.2 Podrobnejše delovanje RFID tehnologije

Globalno ima vsaka država svoje dodeljevanje frekvenc za RFID tehnologijo. Na primer, RFID UHF pasovi so: 866-869 MHz v Evropi, 902-928 MHz v Severni in Južni Ameriki in 950 - 956 MHz na Japonskem in v nekaterih azijskih državah. Tipičen pasivni RFID oddajnik se imenuje oznaka in je sestavljena iz antene ter čipa. RFID oznake so lahko aktivne (z baterijo) ali pasivne (brez baterije).

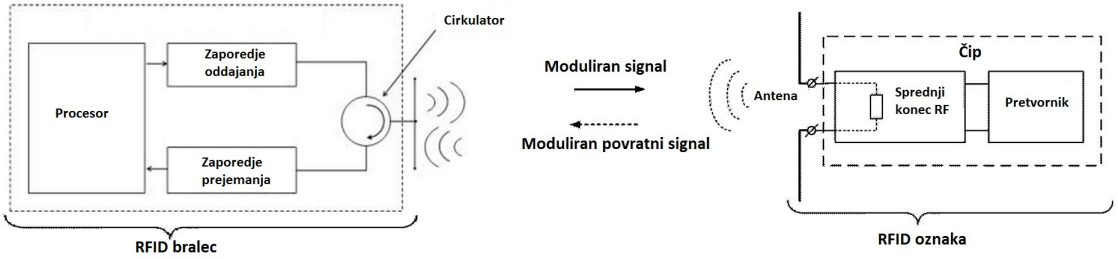
RFID sistem s povratnim signalom deluje tako, da bralec oddaja moduliran signal, ki ga prejme antena RFID oznake.

RFID bralec: Večina RFID bralcev uporabljajo RF komponento treh vrat (ang. three-port RF component) imenovano tudi cirkulator, ki omogoča, da uporabljamo isto anteno pri pošiljanju in sprejemanju podatkov. Za pošiljanje in sprejemanje imamo dva zaporedja, v katerih se shranjujejo prejeti in poslani podatki, ki čakajo, da jih obdela

procesor ali da se pošljejo na oznako. Bralec ima vgrajen procesor za moduliranje, demoduliranje in generiranje ukazov v kratkem časovnem intervalu. Ta oblika je zelo podobna FPGA RFID merilnim sistemom [1].

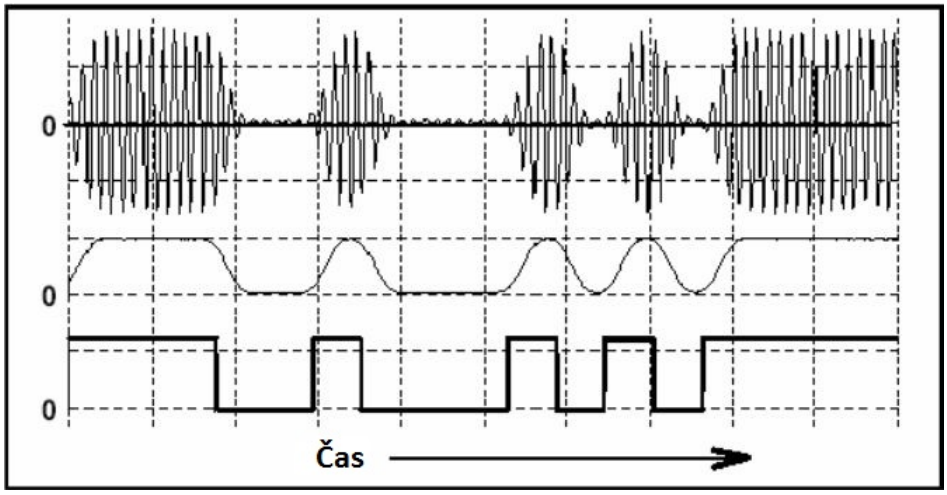
RFID oznaka: Sprednji konec RF (ang. RF Front End) je splošen izraz za vsa vezja med anteno in digitalnim sistemom. V našem primeru vsebuje filtre, ojačevalce z nizko stopnjo šuma in mešalnike, ki so potrebni za obdelavo sprejetega moduliranega signala v signale primerne za vnos v pretvornik signala. Le-ta pretvori analogni signal v digitalni in pošlje moduliran povratni signal k bralcu. Radiofrekvenčni signal, ki ga oddaja bralec napaja čip, ki pošlje podatke nazaj na bralca.

Opisano shemo lahko vidimo na sliki 2.



Slika 2: RFID sistem s povratnim signalom [1], [33].

Za učinkovito pošiljanje podatkov med oznako in bralcem, podatke položimo na sinusni nosilni val v določenem frekvenčnem pasu. To prekrivanje imenujemo modulacija. Modulacija se izvede s spreminjanjem vrednosti enega od treh osnovnih značilnosti sinusnega nosilnega vala - njegove amplitude, frekvence ali faze. Za moduliranje signala pri RFID-u se uporablja amplitudna modulacija s katero zmanjšamo število napak med pošiljanjem podatkov. Modulacija je grafično predstavljena na sliki 3, kjer lahko vidimo, da najprej iz originalnega sporočila (digitalni signal), ki je sestavljen iz različnih bitov (enic in ničel), s pomočjo pretvornika dobimo analogni signal, nakar z amplitudno modulacijo pridobimo moduliran

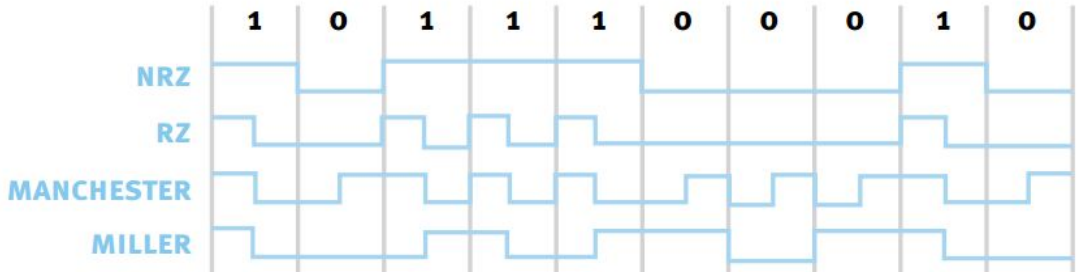


Slika 3: Grafičen prikaz razlik pri originalnem sporočilu (spodaj), analognem signalu (sredina) in moduliranem signalu (zgoraj) [3].

Kodiranje se nanaša na vzorec modulacije, ki ga razumeta oddajnik in sprejemnik. Pri RFID-u se uporabljajo štiri različne sheme kodiranja.

- **NRZ kodiranje**: je enostavno kodiranje pri katerem enice predstavljajo visok signal, ničle pa nizek signal.
- **RZ kodiranje**: je podobno NRZ kodiranju. Razlika je le, da pri visokem signalu kodiranje ne zasede celotnega intervala bita z vrednostjo ena, ampak je bit razdeljen na dva pol bita, kjer ima prvi del vrednost ena, drugi del bita pa vrednost nič.
- **Manchester kodiranje**: za razliko od RZ kodiranja Manchester kodiranje predstavlja nizek signal z dvema pol bitoma, kjer ima prvi del vrednost nič, drugi del bita pa vrednost ena. Več podatkov o Manchester kodiranju lahko najdemo v poglavju 3.4.
- **Miller kodiranje**: v tej shemi je visok signal predstavljen s prehodom, kjer se vrednost pol bitov zamenja (bodisi iz enice na ničlo ali iz ničle na enico), medtem ko nizek signal ohranja vrednost predhodnega bita. Več podatkov o Miller kodiranju lahko najdemo v poglavju 3.4.

Za lažjo predstavo so kodiranja grafično predstavljena na sliki 4.



Slika 4: Grafično predstavljene sheme kodiranja pri RFID-u, ki predstavljajo razlike pri kodiranju naključnega zaporedja enic in ničel [32].

Najpomembnejša lastnost RFID oznake je zmogljivost največje razdalje oddajanja, torej največja razdalja na kateri RFID bralec zazna povratni signal iz oznake. Ker je občutljivost bralca običajno višja v primerjavi z oznako, je območje branja opredeljeno s pragom odzivnosti oznake. Bralno območje je tudi občutljivo na umerjenost oznake in materiala, na katerem je oznaka.

Razdalja branja se lahko izračuna z uporabo Friis free-sapace formule [33]:

$$r = \frac{\lambda}{4\pi}\sqrt{\frac{P_t G_t G_r \tau}{P_{th}}},$$

kjer je λ valovna dolžina, P_t moč signala, ki ga oddaja bralec, G_t zmogljivost oddajne antene, ki pretvarja vhodne moči signala v radijske valove usmerjene v določeno smer, G_r zmogljivost prejemne antene, ki pretvarja radijske valove, ki prihajajo iz določene smeri v električno energijo, P_{th} je minimalni prag moči, ki ga je potrebno zagotoviti, da bo čip RFID oznake imel dovolj energije in τ je koeficient za prenos moči. Slednjega izračunamo s formulo:

$$\tau = \frac{4R_c R_a}{|Z_c + Z_a|^2}, \quad 0 \leq \tau \leq 1,$$

kjer $Z_c = R_c +_j X_c$ impedanca čipa in $Z_a = R_a +_j X_a$ impedanca antene. Impedanca je razmerje med izmenično napetostjo in tokom v električnem krogu.

3 NFC TEHNOLOGIJA

3.1 Prehod iz RFID-a na NFC

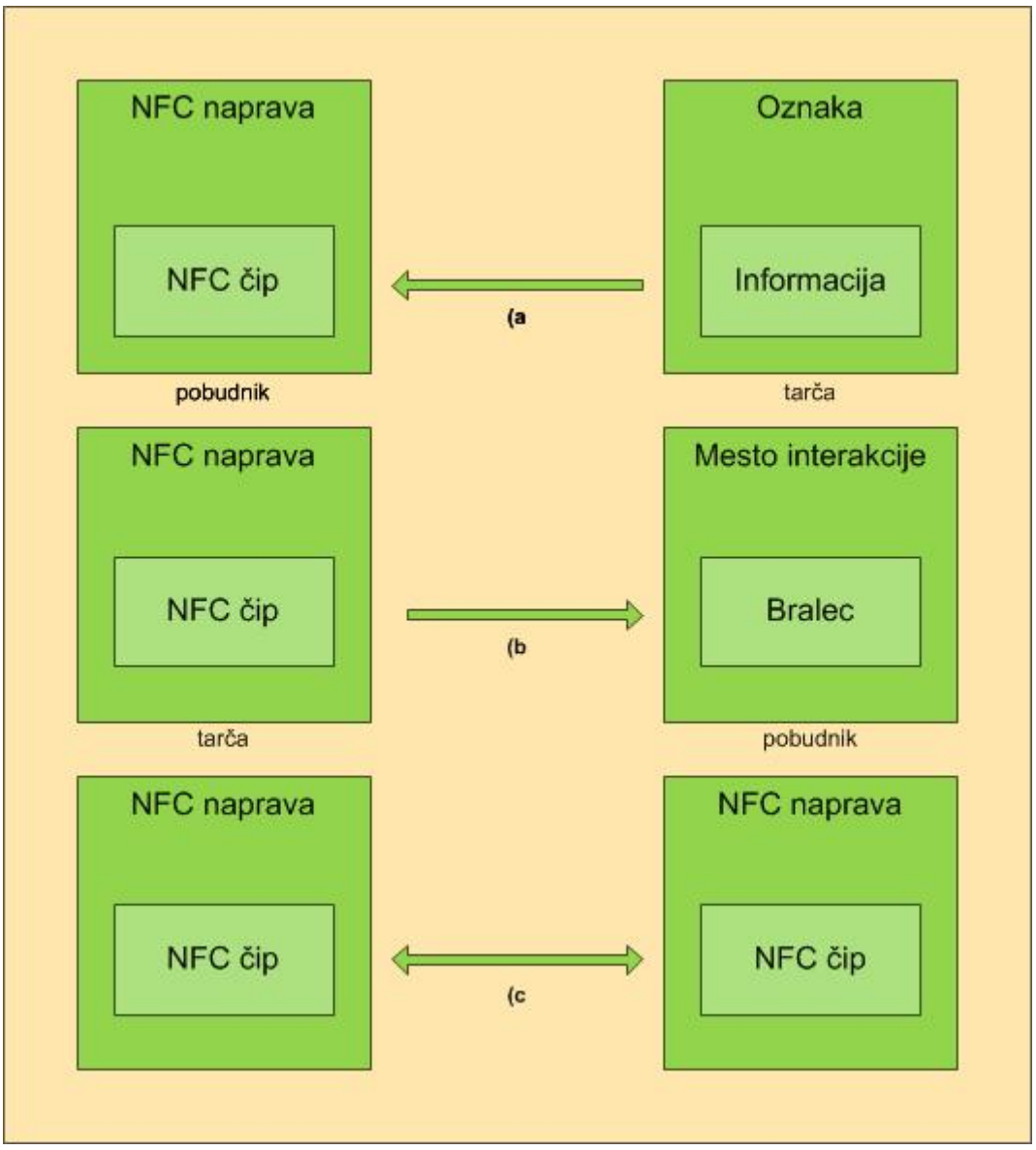
NFC temelji na RFID tehnologiji in uporablja enaka delovna načela kot RFID. Obe tehnologiji uporabljata radio-frekvenčna elektromagnetna polja za prenos podatkov ter tudi omogočata branje RFID oznak. Standard NFC je bil izdan leta 2003 in je tehnologija za podatkovno komunikacijo kratkega dosega, ki deluje na frekvenčnem pasu 13,56 MHz. NFC je standardiziran v standardu ISO/IEC 18092 in je združljiv s standardom ISO/IEC 14443 in 15693, ter s Sony-jevim brezkontaktnim sistemom pametnih kartic FeliCa [17]. Tako lahko NFC uporablja obstoječe infrastrukture, ki temeljijo na omenjenih standardih, s čim se odpravi potreba po ločeni NFC infrastrukturi. Ključna značilnost NFC naprav je, da lahko preberejo in simulirajo RFID oznake, ob tem pa tudi omogočajo dvosmerno komunikacijo ob približanju dveh NFC naprav (ang. peer-to-peer), česar ni možno doseči z RFID napravami zaradi drugačne arhitekture sistema. Razlika med RFID in NFC oznakami je ta, da vse NFC oznake delujejo na frekvenci 13,56 MHz, medtem ko obstajajo RFID oznake, ki delujejo na različnih frekvencah. Poleg tega pri RFID-u lahko uporabljamo oznake z napajanjem, katere pri NFC-ju ne obstajajo. NFC sistemi lahko uporabljajo le tiste RFID oznake, ki delujejo na frekvenci 13,56 MHz.

Tehnologiji NFC in RFID uporabljata radio-frekvenčna elektromagnetna polja ter tudi omogočata branje oznak, toda tehnologiji imata različno strukturno sestavo, ki je predvsem opazna pri RFID in NFC bralcih. Skupna značilnost je, da pri obeh za moduliranje in demoduliranje podatkov skrbi procesor, ter da se moduliran signal pošlje preko antene. Pri RFID-u obstajata dve zaporedji, ki zagotavljata, da prejete podatke pravilno obdela procesor ter da se poslani podatki pravilno pošljejo na oznako. Te strukture pri NFC-ju ni, temveč za to skrbi NFC krmilnik. Kot bomo videli v prihodnjih poglavjih je prednost NFC tehnologije varnost, za katero je zadolžen varnostni element v NFC sistemu, ki pri RFID-u ne obstaja, saj pri njem ni tolikšnega poudarka na varnost. RFID sistemi so namenjeni pošiljanju enostavnih podatkov na čim večji razdalji, zato so razvili oznake z napajanjem, ki omogočajo širše območje delovanja.

Načini komunikacije, ki jih podpira NFC so prikazani na sliki 5, ki prikazuje različne mobilne interakcije, ki so možne z uporabo NFC tehnologije. NFC čip, ki je integriran v

mobilno napravo lahko prebere podatke iz oznake (slika 5a), posnema pametno kartico, tako da bralec dostopa do svojih podatkov (slika 5b), ali neposredno komunicira z drugo NFC napravo (slika 5c).

V nasprotju z NFC so klasični RFID sistemi izdelani samo kot bralno-pisalne naprave priključene na računalnik. NFC tehnologija je bila zasnovana z namenom omogočitve komunikacije z drugimi subjekti in ponuja intuitiven način izmenjave podatkov med elektronskimi napravami. NFC tehnologija združuje dve paradigmi, komunikacijo med napravami z aktivnim napajanjem in zmogljivostjo izvajanja računskih operacij, ter komunikacijo med aktivnimi napravami z napajanjem in pasivnimi oznakami.



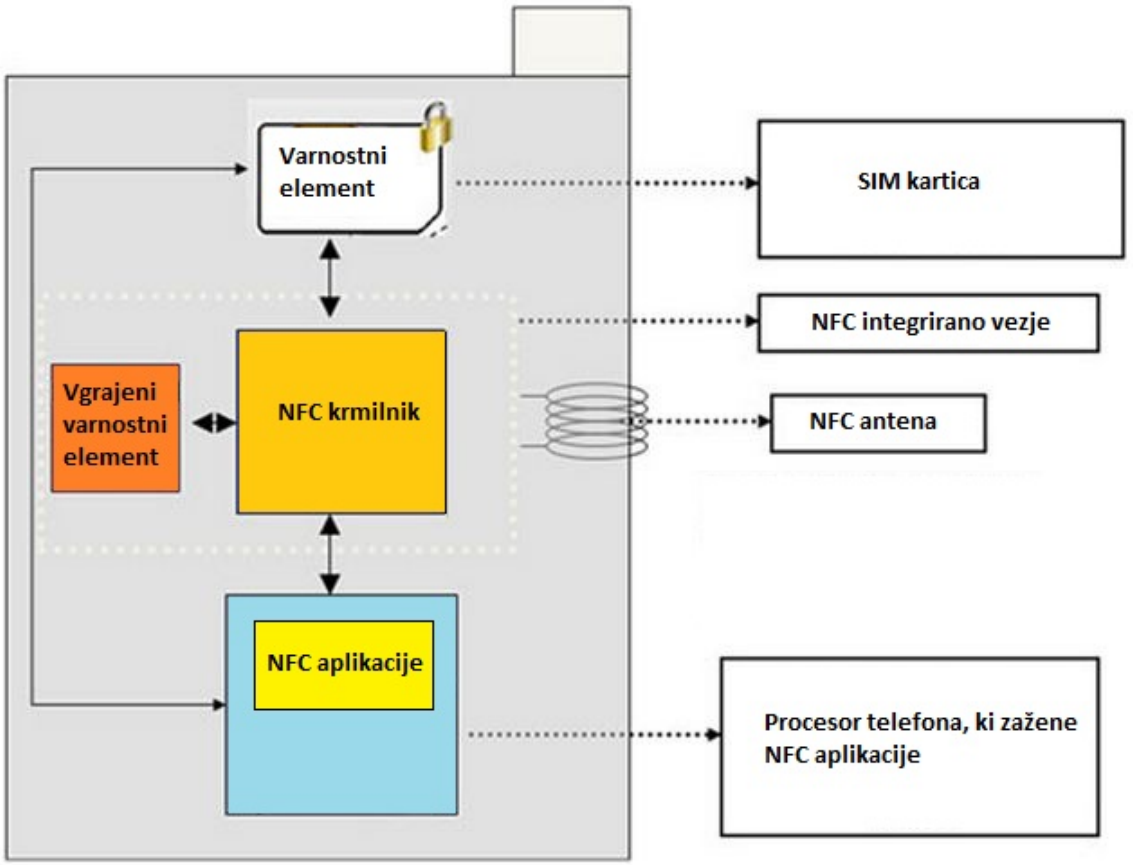
Slika 5: Tipi interakcij, ki jih podpira NFC; a) NFC naprava lahko prebere podatke iz oznake; b) NFC naprava posnema pametno kartico; c) NFC naprava neposredno komunicira z drugo NFC napravo [17].

Obseg delovanja NFC sistemov je približno do deset centimetrov. NFC je zasnovan, da naredi komunikacijo med dvema napravama zelo intuitivno. Uporabniki, ki želijo doseči komunikacijo med dvema napravama, jih samo približajo. Nato se protokol samodejno sproži in omogoči se dvosmerna povezava. Nujna majhna razdalja pri izmenjavi informacij med NFC napravama otežuje prisluškovanje iz zunanjega vira in omogoča dodatno varnost za podatkovno komunikacijo.

NFC je enostavno uporabljati za fizične mobilne interakcije. Primer takšne interakcije je med mobilnimi napravami opremljenimi z NFC čipi in predmeti, ki vsebujejo RFID oznake.

NFC je določen v dveh ECMA standardih [17]. Vsak od standardov je opredeljen s protokolom, ki mora biti implementiran znotraj NFC naprav.

NFC sistem v mobilnem telefonu je sestavljen iz več različnih komponent, kot lahko vidimo na sliki 6. NFC antena je potrebna za komunikacijo z drugimi napravami in oznakami, saj preko nje pošljemo radiofrekvenčni signal. NFC krmilnik je sestavljen iz vmesnika strojne opreme krmilnika (ang. Hardware Controller Interface - HCI) in NFC modema, ki je tudi imenovan brezkontaktni sprednji konec (ang. Contactless Front End - CLF). NFC krmilnik je povezan z NFC anteno in skrbi za preusmeritev radiofrekvenčne komunikacije k trenutno izbranem varnostnem elementu. Varnostni element je komponenta, ki je sposobna zaganjati manjše programe. Ti programi lahko komunicirajo z zunanjim okoljem (npr. z POS terminali) z uporabo NFC komunikacijskih protokolov. Varnostni element zagotavlja normalno delovanje takšnih programov in s tem poveča varnost NFC sistema. NFC sistemi imajo lahko 2 varnostna elementa, eden je vgrajen v integrirano vezje ob krmilniku, drugi je pa SIM kartica. Le eden od zgoraj omenjenih varnostnih elementov je lahko istočasno aktiven. Varnostni elementi so lahko pametne kartice, SIM kartice, pametne SD kartice ali čipi, ki so neposredno vezani na matično ploščo telefona. Varnostni element nam zagotavlja logično varnost (tj. ukaz za šifriranje) in fizično varnost (tj. onemogočanje ponarejevanja ter zaščita pred kopiranjem), ki omogočajo mobilnim NFC aplikacijam izvajanje v varnem okolju. Za zagon NFC aplikacij in nemoteno delovanje skrbi procesor naprave.



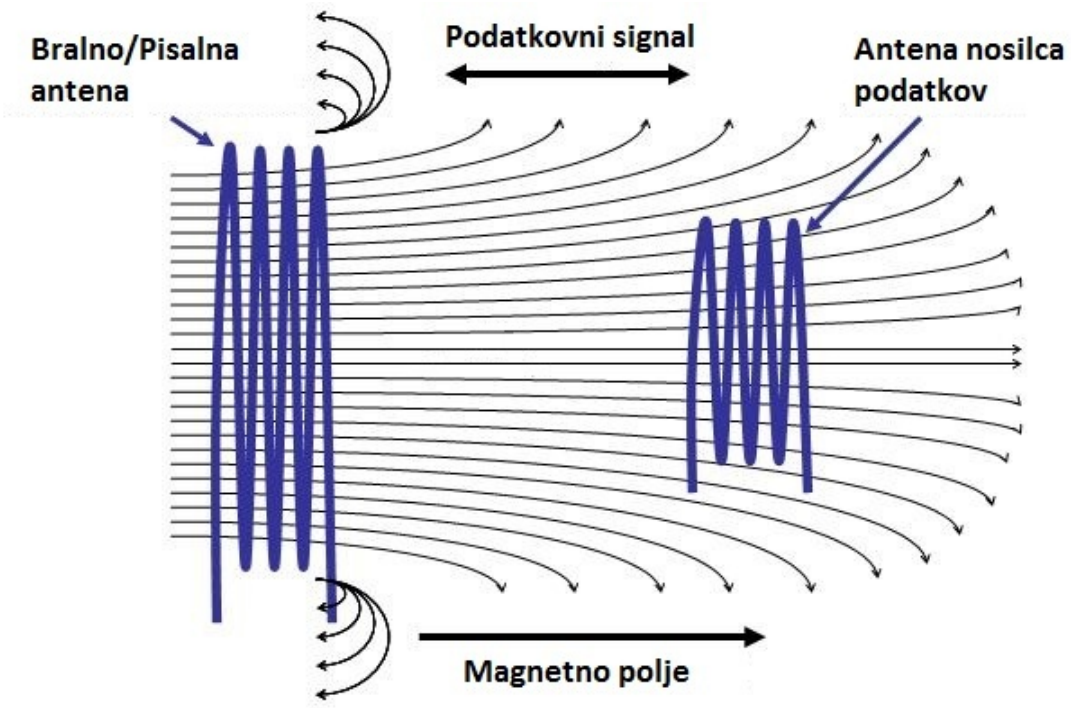
Slika 6: Shema NFC sistema [28].

3.2 NFC protokoli

3.2.1 NFC vmesniški protokol – 1

NFC vmesniški protokol 1 (NFCIP-1) je opredeljen v ECMA-340 [14] ter ISO/IEC 18092 [22]. Standardi opredeljujejo modulacijo in sheme kodiranja bitov ter arhitekturno ogrodje za podprte hitrosti prenosa 106, 212 in 424 kb/s. Poleg tega sta vmesnik komunikacijskega signala in splošni potek podatkov standardizirana. V NFC sistemih lahko sočasno komunicirata največ dve napravi. Napravi si izmenjujeta podatke z uporabo induktivnega spenjanja (slika 7) in radijskih signalov. Induktivno spenjanje imenujemo proces, ko NFC naprava kreira magnetno polje za sprejem oz. zapis podatkov. Nato bralno/pisalna antena iz ene naprave pošlje moduliran podatkovni signal preko magnetnega polja s pomočjo antene nosilca podatkov na drugo napravo. Eden od komunikacijskih udeležencev se imenuje pobudnik in ima aktivno vlogo, drugi s pasivno vlogo se imenuje tarča. Obe vlogi sta vedno dodeljeni, tudi v primeru, kadar

komunicirata NFC napravi z baterijskim napajanjem.



Slika 7: Induktivno spenjanje [35].

NFCIP-1 opredeljuje aktivne in pasivne načine komuniciranja. V aktivnem načinu tako pobudnik kot tarča preko radiofrekvenčnih anten ustvarita radiofrekvenčno polje za brezžično oddajanje ali komuniciranje s pošiljanjem toka preko anten. Pobudnik prične s komunikacijo z uporabo protokola NFCIP-1, nato se poveže z tarčo ter prične prenos podatkov. V pasivnem načinu samo pobudnik ustvari radiofrekvenčno polje. Tarča se napaja z induktivnim spenjanjem in je zmožna pošiljanja ali sprejemanja podatkov. S pomočjo tega načina dosežemo precejšnje prihranke energije. Poleg tega NFCIP-1 določa metode za preprečevanje trkov, ki skrbijo za odkrivanje in odpravljanje trkov na ravni protokola, izbiro tarč, inicializacijo za pasivni način in transportni protokol. Slednjega lahko razdelimo na tri dele:

1. Aktivacija protokola, ki vključuje funkcije ATR_REQ, ki jo pošlje pobudnik tarči, za zahtevo atributov in PSL_REQ, ki določa izbor parametrov za pobudnika.

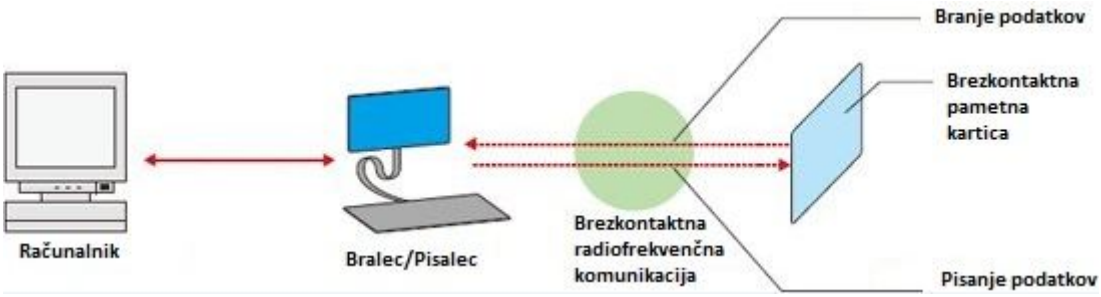
2. Protokol za izmenjavo podatkov, ki podpira usmerjen prenos podatkov z obravnavanjem napak. Protokol vključuje funkcije DEP_REQ, ki določa ukaz za izmenjavo podatkov za pobudnika in DEP_RES, ki določa ukaz za izmenjavo podatkov za tarčo.

3. Deaktiviranje protokola s sprostitvijo, ki vključuje funkcijo DSL_REQ, ki jo pošlje pobudnik tarči za sprostitev atributov.

3.2.2 NFC vmesniški protokol – 2

NFC vmesniški protokol 2 (NFCIP-2) je definiran v ECMA-352 [15]. Standard določa metodo za izbiro enega od treh možnih načinov komunikacije opredeljenih v ECMA-340 (tj. NFCIP-1), ISO/IEC 14443 in ISO/IEC 15693 (npr. oznake RFID). Kot izid omogoča NFCIP-2 prehod med obstoječimi standardi vmesnikov. Naprave, ki izvajajo NFCIP-2 morajo imeti funkcije pobudnika ter tarče, ki so definirane v ECMA-340 ter implementirane standarde za identifikacijske kartice (ISO/IEC 14443 in ISO/IEC 15693).

To naredi NFC naprave združljive z obstoječimi FeliCa [12] ter MIFARE [26] sistemi in mnogimi drugimi. FeliCa in MIFARE sta blagovne znamke podjetij Sony (FeliCa) in NXP Semiconductors (MIFARE). Obe izdelujeta brezkontaktne RFID sisteme pametnih kartic. Pametne kartice so kartice velikosti navadnih plačilnih kartic ampak za razliko od le-teh imajo vgrajena integrirana vezja, ki lahko obdelujejo in shranjujejo podatke ter se povežejo z NFC bralcem preko radiofrekvenčnih valov. Primer delovanja sistema FeliCa lahko vidimo na sliki 8, kjer je predstavljen zapis podatkov na brezkontaktno kartico in branje podatkov iz brezkontaktne kartice. Pri prvem računalnik pošlje na pisalca podatke, ki jih želi zapisati na kartico in ko približamo kartico v bližino pisalca se preko brezkontaktne radiofrekvenčne komunikacije podatki zapišejo na kartico. Pri branju podatkov iz kartice, le-to približamo bralcu, ki prebere podatke preko brezkontaktne radiofrekvenčne komunikacije in prenese podatke na računalnik.



Slika 8: Delovanje sistema FeliCa brezkontaktnih pametnih kartic [12].

Vendar prej omenjeno združljivost ni mogoče doseči pri posnemanju pametne kartice, ki uporablja standarde ISO/IEC 14443B in ISO/IEC 15936, čeprav je omogočeno branje iz kartice in urejanje podatkov na le-tej. Drugi cilj protokola je, da ne moti

nobene stalne komunikacije na delovni frekvenci 13,56 MHz. To je doseženo z nosilcem večkratnega dostopa (ang. carrier sense multiple access - CSMA). CSMA je protokol dostopa do medija (ang. media access control - MAC) v katerem vozlišče preveri odsotnost drugega prometa pred prenosom na skupni medij, kot je električno vodilo ali pas elektromagnetskega spektra [8]. Zaradi tega naprava NFCIP-2 ne bo aktivirala radiofrekvenčnega polja, ko zazna zunanje radijsko polje, ki presega določen prag.

Podedovanje standardov omogoča NFC prednosti uporabe z obstoječimi aplikacijami RFID, kot so aplikacije za nadzor dostopa ali plačilo vozovnic javnega prometa. To je pogosto mogoče upravljati s staro infrastrukturo, npr. tudi če se RFID kartica nadomesti z mobilnim telefonom, ki ima možnost uporabe NFC-ja. To je mogoče zaradi NFC-jeve zmožnosti posnemanja RFID oznak. Strojna oprema NFC-ja lahko ob NFC kontrolerju vključuje varnostni element za povečanje varnosti v aplikacijah, kjer je to nujno. Npr. plačila, kjer je kreditna kartica integrirana v mobilni telefon in uporabljena preko NFC-ja.

V esenci uporabljata tehnologiji radiofrekvenčne identifikacije in NFC-ja enake delovne standarde. Vendar je pri razširitvi RFID-a na NFC bistvena možnost komunikacije med dvema aktivnima napravama. Dodatno k brezkontaktni pametni kartici (ISO 14443), ki podpira komunikacijo med aktivnimi napravami in pasivnimi oznakami, omogoča NFC tudi komunikacijo med dvema aktivnima napravama (ang. peer-to-peer). Torej NFC združuje funkcije za branje in posnemanje RFID oznak in hkrati omogoča pošiljanje podatkov med elektronskimi napravami, ki so »aktivne«.

3.3 Izboljšani NFC

Podjetje INSIDE Contactless je razvilo izboljšan NFC sistem imenovan tudi eNFC, združljiv z večimi obstoječimi sistemi. eNFC dodatno podpira standarde ISO/IEC 14443B (npr. MIFARE) in ISO/IEC 15936 (RFID oznake) za posnemanje pametne kartice. Glavna prednost ISO/IEC 14443B je, da omogoča posnemanje kartic, četudi je baterija mobilnega telefona prazna ali je naprava izključena. Ta funkcija je zelo uporabna pri aplikacijah za plačila vozovnic. Brez tega potniki ne bi mogli plačati vozovnico v primeru, da je baterija njihovega mobilnega telefona prazna [17].

Za razširitev razumevanja delovanja NFC-ja z nizkim stanjem baterije oz. s prazno baterijo lahko pogledamo tri različne primere delovanja:

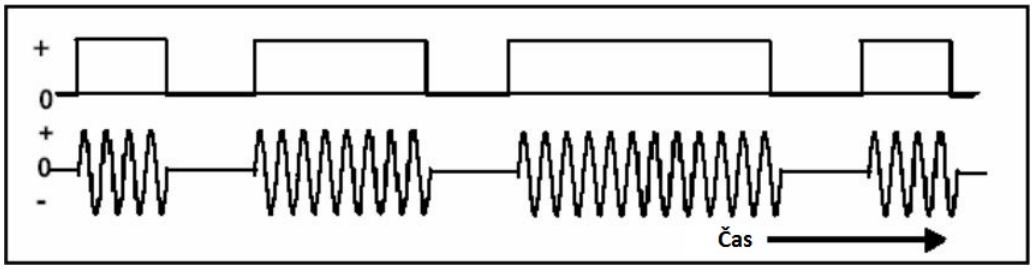
- **polna baterija**: Napravo lahko vključimo in zagotavlja polno moč NFC čipu, tudi če je naprava izključena.
- **nizko stanje baterije**: Napravo zaradi premajhne količine baterije ne moremo vključiti, saj nima dovolj moči za zagon operacijskega sistema. Vseeno mobilna

naprava zagotavlja zadosti energije za normalno delovanje NFC čipa.

- **prazna baterija oz. odstranjena baterija**: Edini preostali vir energije NFC čipa je nabiranje energije iz radiofrekvenčnega polja, ki ga pridobi od NFC bralca. Če je radiofrekvenčno polje dovolj močno, je delovanje NFC čipa omogočeno.

3.4 Varnost NFC-ja

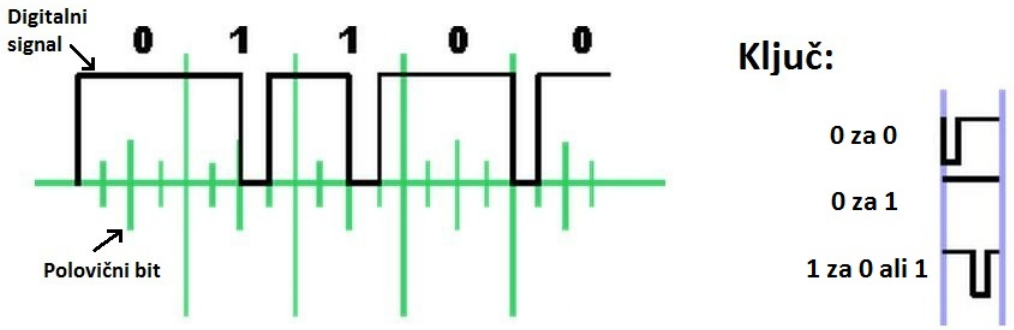
V aktivnem stanju se podatki pošiljajo s pomočjo amplitude modulacije (ang. amplitude shift keying - ASK). To pomeni, da je baza radiofrekvenčnega signala modulirana s podatki v skladu s shemo kodiranja. Na sliki 9 lahko vidimo primer binarnega ASK signala z binarno sekvenco. ASK je oblika amplitudne modulacije, ki predstavlja digitalne podatke kot razlike v amplitudi nosilnega vala. Nosilni val je valovna oblika (občajno sinusoidna), ki je modulirana z vhodnim signalom za transport informacij. Če je hitrost prenosa 106 kb/s ali manj, se uporabi Millerjeva shema kodiranja [19], kot lahko vidimo na sliki 10. Kasneje sledi opis slike in podrobnejša obrazložitev kodiranja. V primeru, da je hitrost prenosa večja od 106 kb/s se pa uporablja Manchesterjeva shema kodiranja [19], kot lahko vidimo na sliki 11. Kasneje sledi opis slike in podrobnejša obrazložitev kodiranja. Pri obeh shemah kodiranja se pošlje samo en bit podatkov v fiksni časovni reži. Reža je razdeljena na dve polovici, imenovani pol-bit.



Slika 9: Slika ponazarja binarni ASK signal (spodnji), skupaj z binarno sekvenco, ki je sestavljena iz različnih bitov (zgornji) [3].

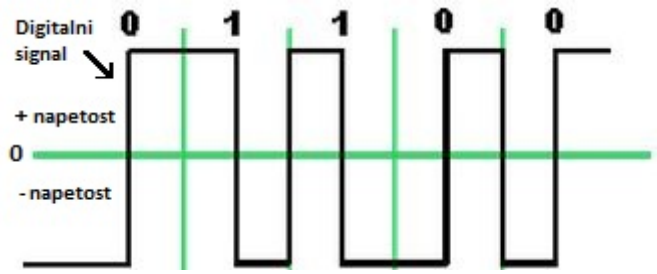
V Millerjevem kodiranju je ničla kodirana s premorom v prvi polovici bita in brez premora v drugi polovici bita. Enka je kodirana brez premora v prvi polovici bita, ampak s premorom v drugi polovici. V spremenjenem Millerjevem kodiranju se uporabljajo dodatne določbe za kodiranje ničel. V primeru, da enki sledi ničla, bosta dva naslednja pol-bita vsebovala premor. Spremenjeno Millerjevo kodiranje se izogiba tega, tako da kodira ničle, katerim sledi enka z dvema pol-bitoma brez premora. Na sliki

10 je prikazana naključna sekvenca bitov in spremenjeno Millerjevo kodiranje bitov. Za lažje ločevanje med biti so meje med celotnimi biti ponazorjene z največjo zeleno navpično črto, meje polovičnih bitov z srednjo veliko zeleno navpično črto in četrtinski biti z najmanjšo zeleno navpično črto. Na desni strani slike je prikazan ključ kodiranja, kjer prikažemo kako so določeni biti kodirani glede na predhodni bit.



Slika 10: Grafičen prikaz spremenjenega Millerjevega kodiranja [31].

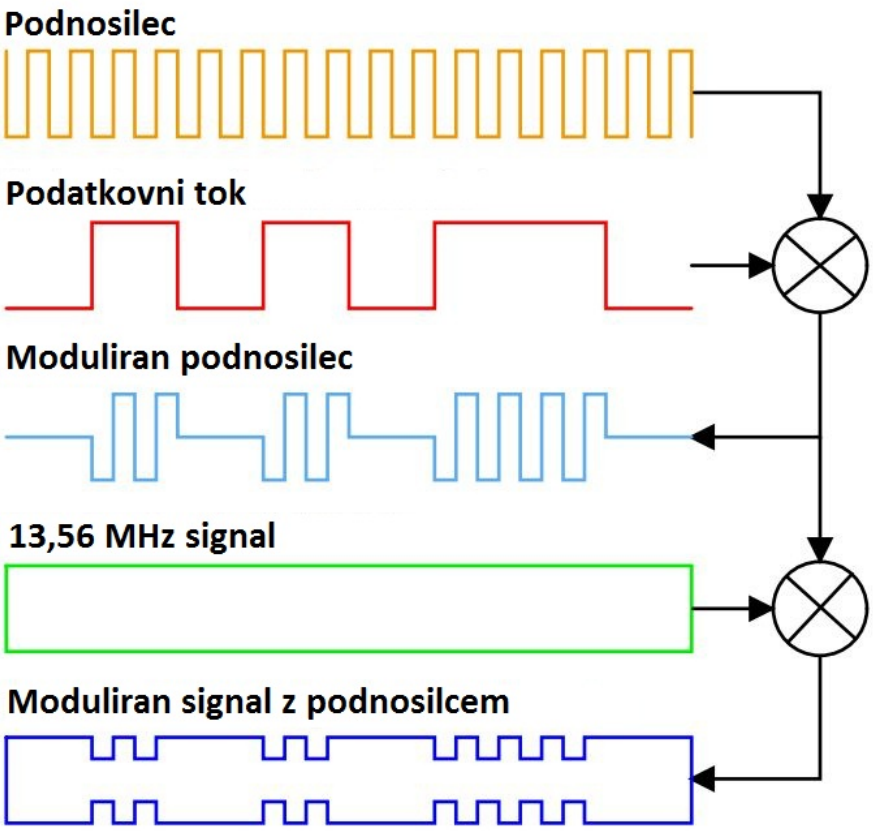
V Manchesterjevem kodiranju je situacija podobna, vendar namesto da je premor v prvem ali drugem pol-bitu, je celoten pol-bit premor ali moduliran signal. Poleg sheme kodiranja je tudi moč modulacije odvisna od hitrosti prenosa. Za 106 kb/s se uporablja 100% modulacija. To pomeni, da se noben radiofrekvenčni signal ne pošilja med premorom. Za hitrosti prenosa višje od 106 kb/s se uporablja 10% modulacija. V skladu z definicijo tega razmerja modulacije [9] pomeni, da je v premoru radiofrekvenčni signal na približno 82% višine signala brez premora. Razlika v moči modulacije je zelo pomembna s stališča varnosti, kot bomo videli kasneje v poglavju 3.5.3. Na sliki 11 je prikazana naključna sekvenca bitov in Manchesterjevo kodiranje. Za lažje razumevanje slike je z vodoravno zeleno črto predstavljena napetost z vrednostjo nič in z navpičnimi zelenimi črtami so ponazorjene meje med celotnimi biti. Pri Manchesterjevem kodiranju se menjava napetosti vedno spremeni na pol bitu in je vsak bit predstavljen s pozitivno in negativno napetostjo. Tako kodiranje ohranja enako količino pozitivne in negativne napetosti in preprečuje kopičenja toka napetosti. S tem načinom omogočamo večjo razdaljo med repetitorji.



Slika 11: Grafičen prikaz Manchesterjevega kodiranja [31].

V pasivnem načinu so podatki vedno kodirani z Manchesterjevim kodiranjem z 10% modulacijo. Za hitrosti do 106 kb/s je uporabljen podnosilec (ang. subcarrier) [19] frekvence za modulacijo, za hitrosti prenosa večje od 106 kb/s je moduliran osnovni radiofrekvenčni signal na frekvenci 13,56 MHz. Zaradi šibke vezi med bralcem in anteno od tarče je odziv 80 dB nižji od napetosti, ki jo ustvarja bralec. Zato namesto neposredne obremenitvene modulacije signala uporabimo podnosilec frekvence. S tem ustvarimo signal z istimi spektralnimi značilnostmi kot modulacijski signal za aktivno pošiljanje signala bralcu.

Postopek uporabe podnosilca za frekvenčno modulacijo poteka tako, da tarča ustvari podnosilec frekvence 847,5 kHz za hitrost prenosa 106 kb/s. Nato se podatkovni tok kodira z uporabo Manchester-jevega kodiranja na frekvenci podnosilca iz česar dobimo moduliran podnosilec. Podatkovni tok je sestavljen iz bitov, ki vplivajo na to kakšen bo moduliran podnosilec. Če je vrednost bita na podatkovnem toku nič je tudi vrednost signala na moduliranem podnosilcu nič. V primeru, da je bit imel vrednost ena, se signal normalno zapiše na moduliran podnosilec. Moduliran podnosilec nato moduliramo s pomočjo 13,56 MHz signala in dobimo moduliran signal s podnosilcem in tako končamo frekvenčno modulacijo podnosilca. Ravnokar opisani pristop modulacije s podnosilcem lahko vidimo na 12.



Slika 12: Grafičen prikaz generiranja moduliranega signala s podnosilcem [5].

3.5 Nevarnosti

3.5.1 Prisluškovanje

Ker je NFC brezžični komunikacijski vmesnik, obstaja možnost prisluškovanja, kar je seveda velika težava. Ko dve napravi komunicirata preko NFC-ja, uporabljata radiofrekvenčne valove za medsebojno prenašanje podatkov. Napadalec lahko uporabi anteno in pridobi poslane podatke, kar lahko doseže z eksperimentiranjem ali preučevanjem literature in se tako seznani, kako pridobiti podatke iz sprejetega radiofrekvenčnega signala. Ampak za to je potrebna oprema za prestrezanje, kot tudi oprema za dekodiranje tega signala.

NFC komunikacija se uporablja med dvema napravama na kratkih razdaljah. To pomeni, da napravi nista oddaljeni več kot 10 cm ena od druge. Pomembno vprašanje je, kako blizu mora biti napadalec, da lahko prestreže uporaben radiofrekvenčen signal. Na žalost ni enoličnega odgovora na to vprašanje. Na razdaljo vpliva več različnih dejavnikov, kot so:

- radiofrekvenčna karakteristika naprave, ki oddaja signal (tj. geometrija antene, zaščitni ovitek naprave, tiskano vezje naprave),
- karakteristike napadalčeve antene (tj. geometrija antene, možnost usmerjanja antene v vse tri dimenzije),
- kvaliteta napadalčevega sprejemnika,
- kvaliteta napadalčevega dekodirnika radiofrekvenčnega signala,
- nastavitve lokacije kje se izvaja napad (npr. ovire kot so stene ali kovine, talni hrup), in
- moč signala, ki ga pošilja NFC naprava.

Posamezni odgovor velja samo za točno izbrane dejavnike iz zgornjega seznama in se ne more uporabljati za izpeljavo splošne varnostne smernice [19].

Hkrati je zelo pomembno v katerem načinu deluje pošiljatelj podatkov. Pošiljatelj lahko uporablja svoje radiofrekvenčno polje (aktivni način), ali radiofrekvenčna polja, ki jih ustvari druga naprava (pasivni način). V obeh primerih je uporabljen drugačen način za prenos podatkov in sicer je veliko težje prisluškovati napravam, ki pošiljajo podatke v pasivnem načinu. Ko naprava pošilja podatke v aktivnem načinu, je možno prisluškovanje iz približno desetih metrov, medtem ko za napravo v pasivnem načinu velja, da je možno prisluškovanje iz približno enega metra.

3.5.2 Napake v podatkih

Namesto da napadalec samo posluša, lahko tudi poskuša spremeniti podatke, ki se pošiljajo preko NFC vmesnika. V najpreprostejšem primeru napadalec samo moti komunikacijo, tako da sprejemnik ne more razbrati podatkov, ki jih je poslala druga naprava.

Napadalec oddaja radijske signale, tako da zmanjša signale na naključne šume in tako uniči vsebino poslane informacije. Ta napad ni preveč zapleten, vendar napadalcu ne omogoča manipulacije dejanskih podatkov.

3.5.3 Spreminjanje podatkov

Pri modifikaciji napadalec želi, da sprejemna naprava sprejme veljavne podatke, ki so bili spremenjeni z njegove strani. Ta način je zelo drugačen od prejšnjega. Izvedljivost napada je zelo odvisna od uporabljene moči amplitudne modulacije. To je zato, ker se dekodiranje signala razlikuje za 100% in 10% modulacijo.

Pri 100% modulaciji dekoder dejansko preveri dva polovična bita za radiofrekvenčni signal brez pavze ali za radiofrekvenčni signal s pavzo. Da bi dekodirnik zaznal enko kot ničlo in obratno, mora napadalec narediti dve stvari. Prvič, premor modulacije napolniti z nosilno frekvenco. To je izvedljivo, ampak mora ustvariti pavzo radiofrekvenčnega signala, ki ga prejme sprejemnik. To pomeni, da mora napadalec poslati radiofrekvenčni signal, tako da se signal popolnoma prekriva z originalnim signalom na anteni sprejemnika, kar je praktično nemogoče. Vendar spremenjeno Milerjevo kodiranje to omogoča v primeru dveh zaporednih enk, kjer napadalec lahko zamenja drugo enko v ničlo z zapolnitvijo pavze, ki kodira drugo enko. Dekodirnik ne bi prebral pavze v drugem bitu in bi dekodiral signal v ničlo, ker je pred njim enka. Pri 100% modulaciji napadalec ne more nikoli spremeniti bita, ki ima vrednost nič, v enko, lahko pa zamenja bit z vrednostjo ena v ničlo, v primeru da je pred tem bitom enka.

Pri 10% modulaciji dekodirnik izmeri moč obeh signalov (82% in 100% signal) in jih primerja. V primeru, da sta v pravilnem območju, je signal veljaven in se dekodira. Napadalec lahko poskusi dodati signal k 82% signalu, tako da 82% signal prikaže kot polni signal in dejansko poln signal postane 82% signal. Na ta način bi dekodirnik zaznal veljaven bit nasprotne vrednosti bita, ki ga je poslal pravilni pošiljatelj. Ali je napad izvedljiv, je zelo odvisno od dinamičnega vhodnega območja sprejemnika. Zelo verjetno je, da bo veliko višji nivo spremenjenega signala presegal morebitno vhodno območje.

Če povzamemo, je pri spremenjenem Milerjevem kodiranju s 100% modulacijo napad izvedljiv za nekatere bite in ni možen za druge, medtem ko je pri Manchesterskem kodiranju z 10% modulacijo ta napad izvedljiv na vseh bitih.

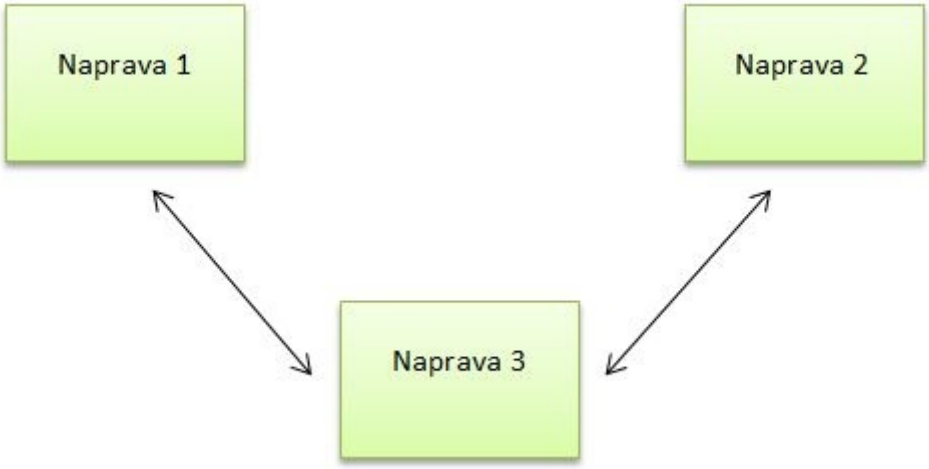
3.5.4 Vstavljanje podatkov

Tu napadalec vstavi sporočila ob izmenjavi podatkov med dvema napravama. Toda to je mogoče le v primeru, da naprava, ki pošlje odgovor potrebuje za to zelo veliko časa. V tem primeru napadalec lahko pošlje svoje podatke pred veljavnim sprejemnikom. Vstavitev bo uspešna le, če se vstavljeni podatki lahko prenesejo preden originalna naprava prične z odgovorom. Če se oba podatkovna toka prekrivata, se bodo podatki popačili.

3.5.5 Napad s posrednikom

V klasičnem napadu s posrednikom (ang. Man-in-the-Middle attack) obe strani, ki želita medsebojno komunicirati, v bistvu ne komunicirata med seboj, ampak dejansko pošiljata in sprejemata sporočila preko tretje naprave, kot lahko vidimo na sliki 13. Taka postavitev je klasična grožnja v nepreverjenih protokolih za izmenjavo ključev,

kot je npr. Diffie-Hellmann protokol [13]. Obe strani se dogovorita o skrivnem ključu, ki se nato uporabi za varen kanal komunikacije. Vendar pa je mogoče, da tretja naprava, ker je na sredini, vzpostavi ključ s prvo napravo, kot tudi z drugo. Ko napravi uporabita svoj ključ za komunikacijo, tretja naprava prisluškuje in upravlja z vsemi podatki, ki se prenesejo.



Slika 13: Prikaz delovanja napada s posrednikom (naprava 3 je vmesna naprava, ki prisluškuje podatkom in simulira normalen pretok podatkov med napravama 1 in 2) [19].

Napad s posrednikom preko NFC-ja: Ob predpostavki, da prva naprava uporablja aktivni način in druga pasivni način, imamo sledečo situacijo. Prva naprava generira radiofrekvenčno polje in pošlje podatke na drugo napravo. V primeru, da je tretja naprava dovolj blizu, lahko prisluškuje podatkom, ki jih je prva naprava poslala. Poleg tega mora aktivno motiti prenos podatkov, tako da druga naprava ne prejme podatkov. To je možno, toda naprava, ki pošilja podatke lahko zazna motnje in v tem primeru prekine protokol.

V primeru, da prva naprava ne zazna motnje in se protokol nadaljuje, mora tretja naprava poslati podatke na drugo napravo. Tukaj se že pojavi problem, saj je radiofrekvenčno polje, ki ga je ustvarila prva naprava še vedno ohranjeno, tako da mora tretja naprava tvoriti novo radiofrekvenčno polje. Kot posledica sta hkrati aktivni dve radiofrekvenčni polji. Praktično nemogoče je pa te dve polji uskladiti. Tako da je skoraj nemogoče, da bi druga naprava razumela podatke, ki jih je poslala tretja naprava. Zaradi tega in zaradi možnosti, da prva naprava napad odkrije veliko prej, ugotovimo, da je v tej postavitvi napad s posrednikom praktično nemogoč.

Edina druga možnost postavitve je, da prva in druga naprava uporabljata aktiven način. V tem primeru prva naprava pošlje podatke na drugo napravo in ponovno mora tretja naprava motiti prenos podatkov tako, da druga naprava podatkov ne prejme. Na tej točki bi lahko prva naprava zaznala motnje in ustavila protokol. Če ponovno privzamemo, da naprava ni zaznala motenj in ne ustavi protokola, mora tretja naprava poslati podatke na drugo napravo. Zaradi aktivno-aktivne komunikacije je na prvi pogled napad navidez uspešnejši, saj je prva naprava izklopila radiofrekvenčno polje. Tretja naprava vzpostavi radiofrekvenčno polje in lahko pošlje podatke. Do problema pride, zato ker prva naprava posluša in pričakuje odgovor od druge naprave, namesto tega pa prejme podatke iz tretje naprave. Prva naprava ponovno preverja protokol ter lahko zazna motnje in protokol ustavi. V tej postavitvi je nemogoče, da tretja naprava pošlje podatke bodisi prvi ali drugi napravi in zagotovi, da bosta napravi prejeli podatke v tem zaporedju.

Zato lahko trdimo, da je posledično praktično neizvedljivo izvesti napad s posrednikom v realnem svetu.

3.6 Rešitve in priporočila

3.6.1 Varen kanal za NFC

Vzpostavitev varnega kanala med dvema NFC napravama je nedvomno najboljši način za zaščito pred prisluškovanjem in kakršni koli spremembi podatkov. Zaradi lastne zaščite NFC-ja proti napadu s posrednikom je namestitev varnega kanala ne samo priporočljiva ampak tudi precej enostavna.

ECMA-385 [16] je standard za varnost vmesniškega protokola NFCIP-1. Ta standard definira NFC-SEC protokol, ki omogoča neodvisno šifriranje na podatkovnem nivoju. NFC-SEC opredeljuje storitev skupne skrivnosti (ang. Shared Secret Service - SSE), ki določa skupno skrivnost med NFC napravama. Za vzpostavitev skupne skrivnosti med napravama bi lahko uporabili standardni protokol, na primer Diffie-Hellmann, ki temelji na RSA [13] ali epileptičnih krivuljah [25].

Skupna skrivnost je lahko uporabljena za izpeljavo simetričnega ključa, kot sta 3DES ali AES, ki se nato uporabi za zagotavljanje zaupnosti, celovitosti in avtentičnosti prenesenih podatkov varnega kanala. Uporabljeni so lahko različni načini delovanja 3DES in AES za varni kanal, te najdemo v literaturi [9].

3.6.2 Prisluškovanje

Kot je opisano v poglavju 3.5.1, se NFC sam ne more zaščititi pred prisluškovanjem. Pomembno je opozoriti, da je težje prisluškovati podatkom, ki so posredovani v pasiv-

nem načinu, ampak uporaba samo pasivnega načina verjetno ne zadostuje za večino aplikacij, ki prenašajo občutljive podatke. Edina prava rešitev proti prisluškovanju je vzpostavitev varnega kanala, ki je opisan prejšnjem poglavju.

3.6.3 Napake v podatkih

NFC naprave lahko ustavijo ta napad, saj lahko preverijo radiofrekvenčno polje med prenosom podatkov. Moč, ki je potrebna za poškodovanje podatkov je bistveno večja od moči, ki jo tvori NFC naprava. Zato bi moral biti vsak tak napad zaznaven.

3.6.4 Spreminjanje podatkov

Pred spreminjanjem podatkov se lahko zaščitimo na več načinov. Z uporabo hitrosti prenosa 106 kb/s v aktivnem načinu postane za napadalca nemogoče spreminjati vse podatke, ki se pošiljajo preko radiofrekvenčne povezave. To pomeni, da morata obe napravi biti v aktivnem načinu, da se zaščitita pred takšnim spreminjanjem. Medtem ko ta način lahko onemogoči spreminjanje podatkov, je pa obenem najbolj ranljiv za prisluškovanje. Tudi zaščita pred spremembo podatkov ni popolna, ker se celo pri hitrosti prenosa 106 kb/s lahko spremenijo nekateri biti.

NFC naprave lahko preverijo radiofrekvenčno polje pri pošiljanju podatkov. To pomeni, da naprava, ki pošilja podatke, lahko nenehno preverja za takšnimi napadi in lahko prepreči prenos podatkov, ko je napad zaznan.

Tretji način z uporabo varnega kanala je bil predstavljen v poglavju 3.6.1.

3.6.5 Vstavljanje podatkov

Obstajata dva možna protiukrepa. Eden je, da naprava, ki pošlje odgovor, odgovori brez zakasnitve. V tem primeru napadalec ne more biti hitrejši od prave naprave. Napadalec je lahko enako hiter kot prava naprava, ampak v tem primeru se podatki poškodujejo, saj obe naprave odgovorita hkrati.

Še ena možnost je varen kanal med dvema napravama opisan v poglavju 3.6.1.

3.6.6 Napad s posrednikom

Kot je bilo omenjeno, je praktično nemogoče narediti napad s posrednikom (ang. Man-in-the-Middle attack) na NFC povezavi. Vseeno je priporočljivo uporabiti aktivno-pasiven način komunikacije, tako da se radiofrekvenčno polje nenehno generira. Poleg tega bi morala aktivna naprava poslušati radiofrekvenčno polje med pošiljanjem, da bi lahko ugotovila morebitne motnje, ki jih povzročajo potencialni napadalci.

4 PRIMERJAVA NFC-JA Z DRUGIMI TEHNOLOGIJAMI

4.1 Primerjava Bluetooth-a in NFC-ja

NFC, kot tudi Bluetooth, uporabljata radijske valove kratkega dometa za zagotavljanje komunikacije med dvema napravama, vendar ima vsak svoje prednosti in slabosti.

4.1.1 Prednosti Bluetooth tehnologije v primerjavi z NFC tehnologijo

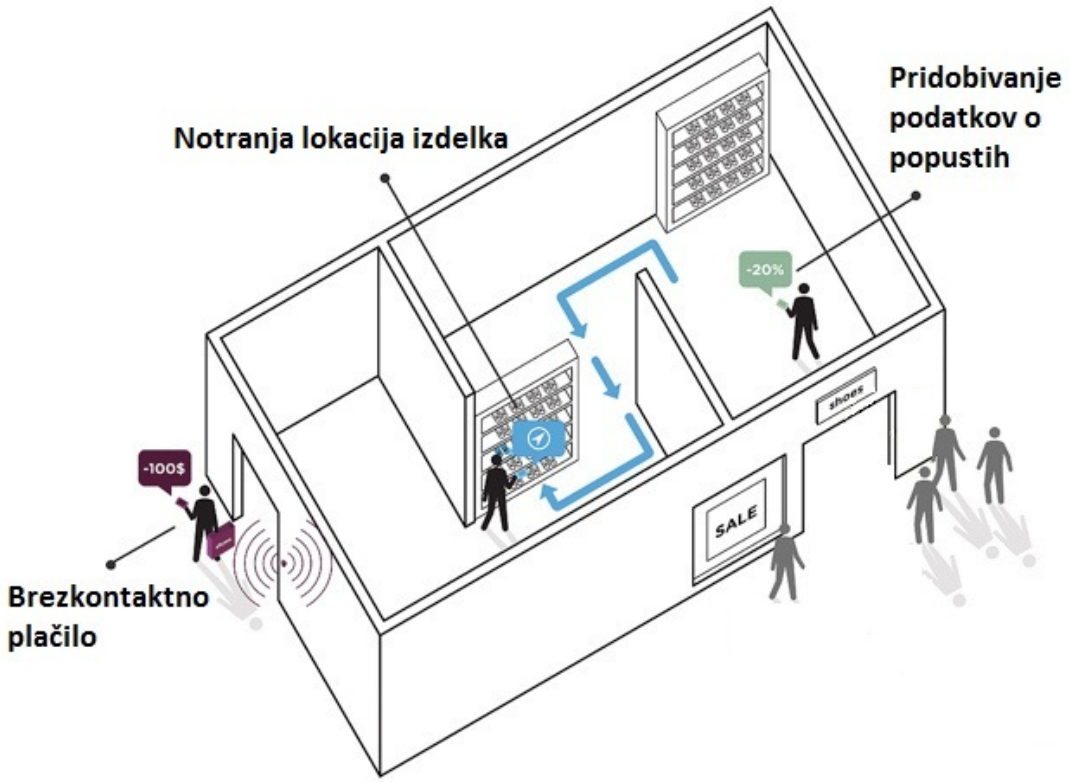
NFC območje je omejeno na razdaljo do 10 cm, medtem ko Bluetooth pokriva razdaljo do približno 100 m. Glede na velikost razdalje je Bluetooth boljši od NFC-ja, saj omogoča večji obseg delovanja. Prednost Bluetooth-a lahko tudi opazimo pri hitrosti prenosa, saj prenaša podatke s hitrostjo nekaj več kot 2 Mb/s, in je primeren za npr. pošiljanje slik, medtem ko hitrost NFC-ja znaša nekaj več kot 400 kb/s, saj ni bil nikoli načrtovan za pošiljanje datotek in večjih podatkov.

4.1.2 Prednosti NFC tehnologije v primerjavi z Bluetooth tehnologijo

NFC porabi manj energije v primerjavi z Bluetooth-om, saj z nizko hitrostjo prenosa in majhno oddaljenostjo od druge naprave ne potrebuje zmogljivega oddajnika. Podobno je tudi, ko je mobilnik v stanju pripravljenosti, saj tudi takrat NFC porabi dosti manj energije v primerjavi z Bluetooth-om. Poleg tega kratka razdalja delovanja NFC-ja omogoča večjo varnost kot pri Bluetooth-u, saj otežuje napade med prenosom podatkov [34]. Prednost, ki jo ima NFC pred Bluetooth-om, je prav tako enostavnost uporabe. Da bi se izmenjava podatkov pričela, zahteva Bluetooth povezavo med obema napravama, ki ju določimo ročno, to pa lahko traja kar nekaj časa. Prednost NFC-ja je, da se povezava vzpostavi samodejno v delčku sekunde, če sta oba mobilna uporabnika v neposredni bližini. Še ena prednost, ki jo ima NFC je sposobnost za delo s pasivnimi RFID oznakami, medtem ko Bluetooth ni kompatibilen z RFID-om in ne more delovati na tak način.

4.2 Izboljšave Bluetooth Low Energy glede na tehnologijo Bluetooth

Bluetooth Low Energy (BLE) je tehnologija, ki se je razvila iz koncepta Bluetooth tehnologije. Inženirji so zmanjšali energijsko porabo, povečali varnost in pohitrili povezljivost naprav. Zaradi manjše porabe energije se je zmanjšalo območje delovanja iz 100 m na 50 m, toda območje je še zadovoljivo za normalno delovanje tehnologije. Prednost BLE tehnologije je, da z njo lahko izvajamo plačila, medtem ko z Bluetooth tehnologijo to ni mogoče. Pri BLE tehnologiji lahko omenimo prednost pridobivanja podatkov iz BLE oddajnikov imenovanih BLE Beacons, ki so velikosti velike škatlice vžigalic. BLE Beacons neprestano oddajajo signal, ki ga lahko preberejo naprave z BLE tehnologijo. Uporabnost BLE oddajnikov lahko vidimo na primer v trgovini, kjer kupci lahko preberejo na svojih mobilnikih trenutne popuste in kje natančneje najdejo znižane izdelke v trgovini. Uporabniku ni potrebno stati v vrsti za plačilo, saj se le-to samodejno izvede pri izhodu iz trgovine. Grafično prikazan primer lahko vidimo na sliki 14.



Slika 14: Grafična predstavitev uporabe BLE tehnologije v trgovini [18].

4.3 Primerjava tehnologij Bluetooth Low Energy in NFC

Bluetooth Low Energy (BLE) in NFC sta tehnologiji kratkega dosega brezžičnega prenosa podatkov. Optimizirani sta za pošiljanje in sprejemanje majhnih podatkovnih paketov. Ko pogledamo energijsko porabo tehnologij lahko vidimo, da je poraba obeh približno enaka.

4.3.1 Prednosti Bluetooth Low Energy tehnologije v primerjavi z NFC tehnologijo

Ko pride do plačilne transakcije ima BLE prednost pred NFC-jem, saj zagotavlja svobodo plačila. BLE omogoča povezavo s POS terminali kjerkoli v trgovini, kar strankam omogoča, da se izognejo čakalnim vrstam. NFC je s tega vidika slabši, saj se morajo plačilne transakcije izvesti v bližini POS terminala in tako ni omogočeno prostoročno plačevanje. Prednost BLE-ja je tudi območje delovanja, saj je območje na katerem deluje dosti večje od območja NFC-ja. BLE deluje na razdalji 50 m, medtem ko NFC deluje na razdalji le nekaj centimetrov. Večje območje delovanja, ki ga omogoča BLE poveča priročnost (prilagodljivost) uporabe. BLE tako lahko uporabimo za pridobivanje informacij o položaju naprave glede na okolico (npr. lokacija v nakupovalnem centru). Ena izmed razlik je pa tudi ta, da je NFC tehnologija osredotočena na izmenjavo podatkov med dvema napravama, medtem ko BLE omogoča več hkratnih povezav.

4.3.2 Prednosti NFC tehnologije v primerjavi z Bluetooth Low Energy tehnologijo

NFC ima pri plačilnih transakcijah več prednosti napram BLE. Kratek obseg NFC tehnologije zagotavlja večjo varnost pri prenosu podatkov in plačilo z NFC-jem omogoča dodatno vizualno varnost (kupec vidi POS terminal, s katerim se poveže). Ena izmed prednosti je tudi ta, da je NFC združljiv z večino obstoječih brezkontaktnih in tranzitnih sistemov, saj vsi delujejo na isti radijski frekvenci, medtem ko BLE deluje na drugačnem frekvenčnem pasu. NFC infrastruktura je že nameščena v plačilnih sistemih. In to je tudi razlog zakaj industrija bolj vlaga v NFC tehnologijo. Prednost NFC-ja je prav tako, da se z NFC-jem transakcija med kupcem in trgovcem izvede z dotikom telefona in POS terminala, dokler je z BLE tehnologijo stranka identificirana glede na svoj položaj, določen z BLE triangulacijo, ki je nato posredovan trgovcu, kateri opravi dodatno fazo selekcije, ki je potrebna za povezovanje kupca s pravo tran-

sakcijo. NFC-jev krajši obseg otežuje prisluškovanje in spreminjanje podatkov ter s tem zviša raven varnosti pri opravljanju plačilnih transakcij. Kratek obseg delovanja NFC-ja omogoča tudi pridobivanje podatkov posameznega izdelka, ki vsebuje NFC oznako, kar nam BLE tehnologija ne omogoča.

4.4 Pogled na vse tri tehnologije

Razlike pri zgoraj opisanih tehnologijah enostavno pojasnimo z nameni uporabe. Bluetooth je namenjen za dolgotrajnejše povezave z drugimi napravami, kot so računalniki, slušalke, tipkovnice in drugi mobilni telefoni. Zato je potrebna večja hitrost prenosa in večja razdalja uporabe. BLE je namenjen za manjše podatkovne prenose podatkov z nizko porabo energije, zato ima manjšo hitrost prenosa in tudi manjše območje delovanja kot Bluetooth, ampak omogoča opravljanje transakcij, medsebojno pošiljanje podatkov med dvema napravama ter sprejemanje podatkov iz BLE oddajnikov na spodobni razdalji, ki je dosti večja od NFC tehnologije. NFC se uporablja za preverjanje identitete uporabnika, varne prenose podatkov in plačilne transakcije ter pridobivanje podatkov iz oznak. Zato je potrebna majhna razdalja in varna povezava, ki jo je možno zagotoviti le z NFC-jem. Podrobnejšo primerjavo lahko vidimo v tabeli 1.

Dejavnik	**NFC**	**Bluetooth**	**BLE**
Frekvenca delovanja	13,56 MHz	2,4 GHz	2,4 GHz
Hitrost povezljivosti	0,1 ms	6 s	0,03 s
Območje delovanja	do 10 cm	do 100 m	do 50 m
Uporabnost	Enostavna, intuitivna in hitra	Srednje enostavna in osredotočena na podatke	Hitra in enostavna
Aplikacije	Plačevanje, pridobivanje dostopa, posredovanje podatkov	Omrežje za izmenjavo podatkov	Pridobivanje podatkov od oddajnikov, posredovanje podatkov in plačevanje
Povezovanje z drugimi napravami	Brezkontaktno, enostavno in varno	Zahtevana avtentikacija in odobritev druge naprave	Brezkontaktno, enostavno in srednje varno

Tabela 1: NFC v primerjavi s tehnologijami Bluetooth in BLE [2], [21].

5 PRIMERI UPORABE

NFC ima sedaj že širok spekter uporabe. Tipično se uporablja preko naprav kot so mobilni telefoni in tablični računalniki. Spodaj je naštetih nekaj primerov, ki opisujejo uporabo naprav z možnostjo NFC-ja.

Plačila: Naprave z NFC-jem se lahko uporabljajo kot kreditne kartice za plačevanje na obstoječih brezkontaktnih POS terminalih.

V juniju 2010 so CASSIS International, INSIDE Contactless, Sagem Wireless in Sagem Orga, v sodelovanju z Mobitelom (trenutni Telekom Slovenije) in banko Koper, pričeli poskus, kjer so uporabljali mobilne telefone z možnostjo NFC-ja kot brezkontaktne kreditne kartice. Udeleženci v raziskavi so lahko opravljali nakupe na kateri koli od trgovskih lokacijah v Sloveniji, kjer sprejemajo brezkontaktne MasterCard in Maestro PayPass plačilne kartice. Posamezniki, ki so sodelovali pri poskusu, so uporabljali tudi interaktivne mobilne storitve preko NFC tehnologije, ki temeljijo na pametnih plakatih. Le-ti so vsebovali turistične informacije, oglase in kupone. Kot rezultat poskusa so podjetja osvojila tehnično znanje ekosistema NFC, opredelila vlogo mobilnega operaterja in vzpostavila poslovni model, ki zamenjuje klasično plačevanje s kreditno kartico [29].

Transport: Naprave, ki uporabljajo NFC tehnologijo, lahko uporabimo tudi kot vozovnice in prepustnice. Potniki lahko približajo svoj telefon k prvemu NFC bralcu, ko vstopijo na vlak oz. na kakšno drugo prevozno sredstvo, in približajo svoj telefon k drugemu NFC bralcu, ko izstopajo iz prevoznega sredstva. Nekaj poskusov implementacij je opisanih spodaj.

V letu 2008, je nemški železniški operater Deutsche Bahn pričel s pilotskim programom za vozovnice, ki temeljijo na NFC-ju. Sodelovalo je 200 potnikov, tako da so ob vstopu na vlak prislonili svoje telefone na eno NFC oznako, in na drugo oznako, ko so izstopali iz njega. Uporabnikom se je cena vozovnice avtomatsko izračunala in se dodala k stroškom mobilnega računa. V januarju 2010 so program uspešno razširili s 3000 dodatnih uporabnikov.

Ravno tako je leta 2008 Transport for London (TfL) v sodelovanju s podjetji Nokia, Visa in TranSys ustvaril plačilni transportni sistem z Oyster karticami. Združenje je naredilo preizkus NFC tehnologije na mobilnih telefonih, kjer so 500 Londončanom podelili mobilne naprave z NFC-jem, katere so lahko uporabili na bralcih kartic Oyster

v podzemni železnici in avtobusih v Londonu. Mobilne telefone z NFC tehnologijo in naloženo Oyster kartico so lahko uporabili kot karto za vstop na postajo. Tako so zmanjšali celoten čas vstopa na postajo, saj se vstopnica na NFC bralcu obdela v približno 300 ms.

Leta 2009 so Air France, Amadeus in IER skupaj z letališčem Nice Cote d'Azur naredili enega izmed največjih NFC pilotskih programov. Ideja projekta je bila razumevanje možnosti poenostavitve prepoznavanja potnikov, knjiženje točk zvestobe in vkrcavanje potnikov z brezžično tehnologijo. Za omogočitev tega projekta je Amadeus razvil zahtevane NFC aplikacije za mobilne telefone, medtem ko je letalska družba Air France sodelovala s svojimi partnerji pri razvoju bralcev NFC in sistema za nadzor odhodov. Z izdelano infrastrukturo je bila mogoča interakcija med mobilnimi telefoni z NFC-jem in NFC bralci. Projekt je bil uspešen in podjetja so začela preučevati nadaljnjo uporabo NFC tehnologije.

Zdravstvo: NFC oznake ne le zagotavljajo zdravstvenim delavcem informacije o tem, kakšno zdravljenje naj bi bolnik prejel, ampak lahko tudi spremljamo kdaj so medicinske sestre ali zdravniki preverili zdravstveno stanje pacienta. Vsakič kadar je oznaka skenirana, se podatki o tem, kdo je skeniral in kdaj, prenesejo v bazo podatkov.

Nacionalna zdravstvena služba Združenega kraljestva (ang. UK National Health Service) izvaja več pilotskih programov nove HomeCare rešitve podjetja O2, ki je zasnovana tako, da pomaga delavcem in pacientom dostopati do informacij in jih izmenjevati. Z uporabo O2 HomeCare lahko negovalci prenesejo in preverijo evidenco bolnikov ter zahteve za njihovo nego, tako da položijo svoj mobilni telefon z NFC-jem čez NFC oznako, ki je nameščena na bolnikovem domu. Aplikacija prav tako beleži, kdaj je posamezen negovalec obiskal bolnika, s čimer skrbijo za varnost in skladnost sistema.

Bolniki, ki uporabljajo ta sistem, lahko položijo svoj telefon na NFC oznako, ki je nameščena v njihovem domu, in se jim prikažejo podrobnosti o naslednjem obisku negovalca. Aplikacija pacientom omogoča tudi, da enostavno pokličejo negovalca ali naročijo pregled, tako da izberejo željene možnosti iz seznama v aplikaciji in položijo telefon na NFC oznako.

Oglaševanje in mediji: NFC naprave se lahko uporabljajo za branje NFC oznak in drugih naprav za pridobitev informacij. Z dodajanjem NFC oznak plakatom in oglasom v revijah lahko oseba takoj prebere oznako z mobilnim telefonom, ki vsebuje NFC.

Pri Radio Taxis, ki je ena od največjih taksi služb v Londonu, so maja 2014 pričeli promocijo svoje mobilne aplikacije, tako da so v več kot 2500 svojih vozil namestili NFC oznake. Uporabniki taksi službe lahko podrsajo svoj mobilni telefon z NFC-em čez oglas v vozilu, ki ima NFC oznako, ter izkoristijo multimedijske zmogljivosti telefona, tako da prenesejo aplikacijo taksi službe in pokličejo številko iz oglasa ali

obiščejo njihovo spletno stran s pomočjo aplikacije.

Marketinška agencija The Picture Works je leta 2013 pričela s promocijo filmov s pomočjo NFC-ja. Reklamne plakate so opremili z NFC oznakami in tako omogočili uporabnikom, da se dotaknejo plakatov z mobilnimi telefoni in prenesejo napovednik filma.

5.1 NFC v povezavi z mobilnimi operacijskimi sistemi

Razvijalci mobilnih operacijskih sistemov so ob osnovni implementaciji uporabe NFC-ja razvili dodatne funkcionalnosti za hitrejši prenos podatkov. Podrobneje so opisane v spodnjih poglavjih.

5.1.1 Android

Android je edini mobilni operacijski sistem, ki ob enostavnem pošiljanju podatkov preko NFC tehnologije povezuje druge tehnologije, kot sta Bluetooth in Wi-Fi. S tem je dosežen ne samo večji prenos podatkov, ampak tudi večja razdalja med napravama. Spodaj sta opisani dve implementaciji.

Android Beam je funkcionalnost, ki omogoča prenos podatkov med dvema Android napravama s pomočjo NFC tehnologije. Ta možnost je implementirana v Androidu od verzije 4.0 (2011). Po verziji Androida 4.1 (2012) so razvijalci razširili hitrost prenosa podatkov, tako da so vključili tehnologijo Bluetooth. Android naprave se še vedno povežejo z NFC-jem, nato se kliče metoda SetBeamPushUris() [4], nakar Android preda prenos podatkov na Bluetooth in tako dosežemo večjo hitrost prenosa.

S-Beam je aplikacija, ki jo je razvilo podjetje Samsung. Aplikacija temelji na značilnostih, ki so vključene v Android Beam. Naprave se povežejo preko NFC-ja, podatki se pa pošljejo preko Wi-Fi Direct-a. Naprave, ki vsebujejo Wi-Fi Direct se lahko med seboj povežejo brez dostopne točke, kar omogoča komunikacijo med napravama z hitrostjo povezave do 300 Mb/s.

Uporaba S-Beam:

1. Odpremo vsebino, ki jo želimo deliti. Lahko delimo slike, video posnetke, kontakte, povezave spletnih strani in celo povezave do Google Play trgovine. Če želimo deliti povezavo do aplikacije v trgovini Google Play, aplikacijo odpremo in sledimo spodnjim korakom.

2. Približamo napravi, tako da se dotikata s hrbtnima stranema.

3. Na napravi, iz katere pošiljamo podatke, se na ekranu prikaže napis, "dotaknite se ekrana za začetek prenosa".

4. Ko nam aplikacija sporoči, da sta napravi povezani, se začne prenos in napravi lahko oddaljimo.

5. Ko se prenos konča, se prenesena vsebina prikaže na zaslonu naprave, ki je podatke prejela.

5.1.2 Windows Phone

Pri Windows Phone mobilnem operacijskem sistemu so pričeli uporabljati NFC tehnologijo od verzije 8 naprej. Operacijski sistem omogoča navadno pošiljanje ali branje podatkov preko NFC tehnologije. Ker implementacija ne vsebuje Bluetooth oz. Wi-Fi tehnologije, je hitrost prenosa podatkov in oddaljenost med napravama oz. med napravo in NFC oznako omejena s samimi omejitvami tehnologije NFC.

5.1.3 IOS

Mobilni operacijski sistem podjetja Apple ne vsebuje NFC tehnologije. Za pošiljanje podatkov med napravami in pridobivanje podatkov od oddajnikov uporabljajo BLE tehnologijo. Pred izidom mobilnika iPhone 4S (2011) in tako tudi BLE tehnologije, so za izmenjavo podatkov lahko uporabljali le tehnologijo Bluetooth.

5.2 Opis uporabe NFC oznak

Z NFC oznako lahko hitro pridobimo podatke o izdelku ali nastavimo nastavitve svoje naprave z NFC-jem po lastni želji. Na primer, če želimo doma imeti vključen brezžični internet, Bluetooth in povečati svetilnost naprave, lahko na NFC oznako zapišemo lastnosti funkcionalnosti katere želimo spremeniti. To lahko storimo z aplikacijami, kot sta npr. Trigger (Android) [38] in NFC interactor (Windows Phone) [27]. V aplikacijah izberemo funkcionalnosti, ki jih želimo zapisati na oznako ter jim določimo željene lastnosti. Ko zaključimo postopek, položimo napravo na oznako in podatki se nanjo zapišejo. NFC oznako lahko postavimo na katerokoli zaželjeno mesto in ko pridemo tja, napravo položimo na oznako in ta bo preko NFC-ja prebrala podatke ter spremenila trenutne nastavitve na napravi. NFC oznake so majhne, poceni in ne zasedejo veliko prostora, zato jih lahko postavimo na več različnih mestih (npr. doma, v avtu, v službi itd.). Primer NFC oznake lahko vidimo na sliki 15.

Slika 15: NFC oznaka [20].

Na NFC oznako lahko med drugimi zapišemo lastnosti kot so:

- nastavitve brezžičnega omrežja,
- nastavitve Bluetooth-a,
- nastavitve zvoka in melodij,
- nastavitve svetilnosti zaslona,
- nastavitve alarmov,
- pošiljanje določenega obvestila na socialna omrežja,
- pošiljanje določenega sporočila sms,
- pošiljanje podatkov o stiku,
- nastavitev glasbenega predvajalnika,
- nastavitve GPS-a,
- nastavitev koledarja, in
- sprožitev klica na določeno številko.

Celotna seznama vseh lastnosti lahko vidimo v literaturah [38] in [27].

6 PRIHODNOST TEHNOLOGIJE NFC

NFC tehnologija je lahko uporabljena na veliko različnih načinov, v različnih aplikacijah za različne namene. Če bo število aplikacij iz leta v leto naraščalo, je zelo verjetno, da bomo lahko plačevali vsakodnevne nakupe in položnice, tako da bomo podrsali svoj telefon preko NFC bralca, in plačila bodo opravljena. Tako bodo vrste v trgovinah, poštah, bankah in podobnih institucijah krajše. Večina aplikacij, ki so v razvoju so financirane s strani državnih institucij, občin ali velikih podjetij. V prihodnosti lahko pričakujemo veliko novih inovativnih aplikacij, ki bodo uporabljale NFC tehnologijo, in s tem upamo, da nam olajšajo vsakodnevna opravila. Lahko vidimo svetlo prihodnost v tej smeri, če pogledamo primere aplikacij v razvoju. Med temi so: plačevanje parkirnih metrov v San Franciscu [30], pomoč vodenja turistov z NFC oznakami v popularnem nacionalnem parku The Rocks v bližini Sydneya [37], One Card sistem univerze v San Franciscu, s katero bodo študentje lahko vstopali v sobe, plačevali obroke ter stroške pralnice, kot tudi druge storitve [36], obiskovanje koncertov brez papirnatih vstopnic, temveč z mobilnim telefonom [6] in sistem podjetja BMW, ki izdeluje NFC ključ za avtomobile s pomočjo katerega bodo lahko uporabniki rezervirali in vstopali v hotelske sobe [11]. NFC tehnologijo omogočajo podjetja, ki izdelujejo mobilne telefone, le-te so tudi vključile NFC v pametne telefone in tako pospešile razvoj te tehnologije. V prihodnje je namen različnih podjetij razširiti NFC tehnologijo na vse vrste elektronskih naprav, saj vidijo prednost v njeni enostavni uporabi.

7 ZAKLJUČEK

NFC tehnologija se je razvila iz RFID tehnologije, ki je namenjena za samodejno prepoznavanje in sledenje oznak, ki so pritrjene na predmete. NFC uporablja enaka delovna načela kot RFID. Tako lahko NFC uporablja obstoječe RFID infrastrukture, s čim se odpravi potreba po ločeni NFC infrastrukturi. NFC je tehnologija za podatkovno komunikacijo kratkega dosega, ki deluje na frekvenčnem pasu 13,56 MHz in njena ključna značilnost je, da njene naprave ne samo preberejo in simulirajo RFID odzivnike, ampak prav tako omogočajo dvosmerno komunikacijo ob približanju dveh NFC naprav. NFC tehnologijo definirata dva vmesniška protokola, kjer so opisani standardi, ki opredeljujejo modulacijo in sheme kodiranja bitov ter arhitekturno ogrodje sistema. Za zagotovitev varnosti NFC tehnologije se uporabljata Miller in Manchester kodiranja, ampak kljub temu obstajajo različni napadi na sistem, kot so prisluškovanje, napake v podatkih, spreminjanje podatkov, vstavljanje podatkov in napad s posrednikom. Toda zahvaljujoč strukturi NFC tehnologije lahko napade več ali manj preprečimo oz. se jim izognemo. Če primerjamo NFC tehnologijo z drugimi tehnologijami, kot so na primer Bluetooth in Bluetooth Low Energy (BLE), so vidne tako slabosti, kot tudi prednosti NFC-ja. Iz primerov uporabe je razvidno, da NFC tehnologija služi svojemu namenu, saj predstavlja hitro, enostavno in varno interakcijo za pohitritev vsakodnevnih opravil.

NFC tehnologija lahko pospeši plačilne transakcije, poenostavi pridobivanje informacij o izdelku ali potrdi avtentičnost osebe, ki želi vstopiti v nadzorovan prostor. NFC tehnologija ima svetlo prihodnost, saj veliko investitorjev vidi potencial v enostavnosti uporabe in hitrosti delovanja te tehnologije. V prihodnosti lahko tako pričakujemo veliko novih aplikacij in naprav, ki bodo vsebovale NFC. S širjenjem NFC tehnologije se bo tako tudi širilo ozaveščanje ljudi o tem kakšne ugodnosti nam ponuja NFC in kako to tehnologijo lahko uporabljamo in si s tem olajšamo naš vsakdan.

8 LITERATURA IN VIRI

[1] Advanced RFID Measurements: Basic Theory to Protocol Conformance Test, http://www.ni.com/white-paper/6645/en/, 2013 *(Citirano na straneh VIII in 8.)*

[2] P. Agrawal, S. Bhuraria in N. Gibbs, Near Field Communication, *SETLabs Briefings* VOL 10 NO 1 (2012), 67-74. *(Citirano na straneh VII in 30.)*

[3] Amplitude Shift Keying & Frequency Shift Keying, http://www.ele.uri.edu/Courses/ele436/labs/ASKnFSK.pdf *(Citirano na straneh VIII, 9 in 18.)*

[4] Android 4.1 APIs, http://developer.android.com/about/versions/android-4.1.html#Connectivity *(Citirano na strani 33.)*

[5] B. Bilginer, P. Ljunggren, Near Field Communication, Lund University, Sweden, http://cwi.unik.no/images/a/ae/Master_thesis_lu_NFC.pdf, 2011 *(Citirano na straneh VIII in 21.)*

[6] D. Brogan, Samsung brings ticketless technology to festivals and gigs, http://www.pocket-lint.com/news/115975-samsung-using-ticketless-technology-for-music-events *(Citirano na strani 36.)*

[7] M. Cardullo, Genesis of the Versatile RFID Tag, RFID JOURNAL http://www.rfidjournal.com/articles/view?392 2003 *(Citirano na strani 5.)*

[8] Carrier sense multiple access, http://www.princeton.edu/~achaney/tmve/wiki100k/docs/Carrier_sense_multiple_access.html *(Citirano na strani 17.)*

[9] C. Castelluccia in G. Avoine, Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags, *Proceedings of CARDIS* (2006), 289-299. *(Citirano na straneh 19 in 25.)*

[10] M. Cigrovski, UVAJANJE TEHNOLOGIJE RFID V SLOVENSKIH KNJIŽNICAH, http://home.izum.si/COBISS/OZ/2005_3/html/clanek_03.html *(Citirano na straneh VIII in 3.)*

[11] S. Clark, BMW uses NFC car keys to open hotel room doors, http://www.nfcworld.com/2012/04/23/315235/bmw-uses-nfc-car-keys-to-open-hotel-room-doors/ *(Citirano na strani 36.)*

[12] Contactless IC Card Chip RC-SA00 RC-SA01, http://www.sony.net/Products/felica/business/products/RC-SA00.html, 2014 *(Citirano na straneh VIII in 16.)*

[13] W. Diffie in M.E. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory 22* (1976), 644-654. *(Citirano na straneh 24 in 25.)*

[14] ECMA-340 Near Field Communication - Interface and Protocol (NFCIP-1) http://www.ecma-international.org/publications/files/drafts/tc47-2008-002.pdf, 2008 *(Citirano na strani 14.)*

[15] ECMA-352 Near Field Communication Interface and Protocol -2 (NFCIP-2), http://rfidspec.wordpress.com/2010/07/26/choosing-rfid-for-industrial-applications-part-2/, 2013 *(Citirano na strani 16.)*

[16] ECMA-385 NFC-SEC: NFCIP-1 Security Services and Protocol, http://www.ecma-international.org/publications/files/ECMA-ST/ECMA-385.pdf, 2013 *(Citirano na strani 25.)*

[17] O. Falke, E. Rukzio, U. Dietz, P. Holleis, A. Schmidt, Mobile Services for Near Field Communication, Technical Report *(Citirano na straneh VIII, 11, 12, 13 in 17.)*

[18] H. Gottipati, With iBeacon, Apple is going to dump on NFC and embrace the internet of things, http://gigaom.com/2013/09/10/with-ibeacon-apple-is-going-to-dump-on-nfc-and-embrace-the-internet-of-things/, 2013 *(Citirano na straneh VIII in 28.)*

[19] E. Haselsteiner, K. Breitfuß, Security in Near Field Communication (NFC) *(Citirano na straneh VIII, 18, 20, 22 in 24.)*

[20] B. Hedrington, Playing with stickers: Writing NFC Tags with Google's Android Nexus S, http://buildcontext.com/blog/2011/nfc-tag-sticker-writing-programming-google-android-nexus-s *(Citirano na straneh VIII in 35.)*

[21] Swen van Klaarbergen, Mobile Payment Transactions: BLE and/or NFC?, UL transactions *(Citirano na straneh VII in 30.)*

[22] INTERNATIONAL STANDARD ISO/IEC 18092 Information technology — Telecommunications and information exchange between systems — Near Field Communication — Interface and Protocol (NFCIP-1), 2013 *(Citirano na strani 14.)*

[23] K.Y. Jeon, C.S. Yoon in S.H. Cho, A Performance Enhanced UHF RFID System with Modified I/Q Diversity Receiver, *The Journal of Korea Information and Communications Society* VOL 33 NO 7 (2008), 751-756. *(Citirano na strani 4.)*

[24] J. Landt, The history of RFID, *IEEE POTENCIALS* (2005), 8-11. *(Ni citirano.)*

[25] K. Lauter, THE ADVANTAGES OF ELLIPTIC CURVE CRYPTOGRAPHY FOR WIRELESS SECURITY, *IEEE Wireless Communications* (2004), 62-67. *(Citirano na strani 25.)*

[26] MIFARE, `http://www.mifare.net/en/home/`, 2014 *(Citirano na strani 16.)*

[27] NFC interactor, `http://www.windowsphone.com/sl-si/store/app/nfc-interactor/4e1598fe-4885-4e2b-9c69-8d3f882c545b` *(Citirano na straneh 34 in 35.)*

[28] NFC Primer for Developers, `https://supportforums.blackberry.com/t5/Java-Development/NFC-Primer-for-Developers/ta-p/1334857`, 2013 *(Citirano na straneh VIII in 14.)*

[29] PAYMENT AND WIRELESS INDUSTRY LEADERS TEAM TO BRING NFC MOBILE PAYMENTS TO SLOVENIA, `http://www.insidesecure.com/Media/Press-releases/Payment-and-Wireless-Industry-Leaders-Team-to-Bring-NFC-Mobile-Payments-to-Slovenia`, 2010 *(Citirano na strani 31.)*

[30] N. Podmore, M. Fournell, PayByPhone Adds Near Field Communications to Mobile Payments for San Francisco's 30,800 Parking Spaces, `https://paybyphone.com/paybyphone-adds-nfc/` *(Citirano na strani 36.)*

[31] I. Poole, NFC Modulation & RF Signal, `http://www.radio-electronics.com/info/wireless/nfc/near-field-communications-modulation-rf-signal-interface.php` *(Citirano na straneh VIII, 19 in 20.)*

[32] S.E. Sarma, S.A. Weis in D.W. Engels, RFID Systems, Security & Privacy Implications, massachusetts institute of technology, 2002 *(Citirano na straneh VIII in 10.)*

[33] K.V. Seshagiri Rao, P.V. Nikitin in S.F. Lam, Antenna Design for UHF RFID Tags: A Review and a Practical Application, *IEEE TRANSACTIONS ON*

ANTENNAS AND PROPAGATION 53 (2005), 3870-3876. *(Citirano na straneh VIII, 8 in 10.)*

[34] V. Sharma, P. Gusain in P. Kumar, NEAR FIELD COMMUNICATION, *Conference on Advances in Communication and Control Systems (CAC2S 2013)* (2013), 342-345. *(Citirano na strani 27.)*

[35] M. Sippel, Choosing RFID For Industrial Applications, `http://rfidspec.wordpress.com/2010/07/26/choosing-rfid-for-industrial-applications-part-2/` *(Citirano na straneh VIII in 15.)*

[36] So Many Uses, Just One Card, `http://www.usfca.edu/onecard/` *(Citirano na strani 36.)*

[37] Sydney's the Rocks Set to Deploy NFC Technology, `http://www.rfid-blog.com/?p=1004` *(Citirano na strani 36.)*

[38] Trigger, `https://play.google.com/store/apps/details?id=com.jwsoft.nfcactionlauncher` *(Citirano na straneh 34 in 35.)*

[39] B. Violino, The History of RFID Technology, RFID JOURNAL `http://www.rfidjournal.com/articles/view?1338` 2005 *(Citirano na strani 5.)*

[40] M. Ward, R. van Kranenburg, G. Backhouse, RFID: Frequency, standards, adoption and innovation, JISC Technology and Standards Watch, May 2006 *(Citirano na strani 6.)*