TAMPEREEN AMMATTIKORKEAKOULU
Tietotekniikka, Tietoliikennetekniikka

Opinnäytetyö

Ossi Koistinen

NFC-TEKNIIKKA

Ohjaava opettaja: Kai Poutanen

Tampere 2010

Tekijä	Ossi Koistinen
Työn nimi	NFC-tekniikka
Sivumäärä	28
Päivämäärä	Joulukuu 2010
Ohjaava opettaja	Kai Poutanen

TIIVISTELMÄ

Työn tarkoituksena oli tutustua NFC-tekniikkaan ja sen keskeisiin teknisiin rakenteisiin. NFC on lyhenne sanoista Near Field Communication ja se on hyvin lyhyen etäisyyden tiedonsiirtomenetelmä. Tekniikan avulla voidaan lukea ja muokata jo olemassa olevia, esimerkiksi älykorteissa käytettyjä, tunnisteita ja NFC:n omia tunnisteita. Sen odotetaan yleistyvän mobiililaitteissa ja sovellusalueita ovat mm. mobiilimaksaminen ja avaimen tapaan toimiva tunnistautuminen. Tunnisteiden toiminnan taustalla pitkälti olevaan RFID-tekniikkaan verrattuna NFC on monikäyttöisempi mm. siksi, että laitteet voivat toimia lukijan lisäksi myös kirjoittajana.

Tekniikan toiminnot on määritetty vuonna 2004 julkaistussa ISO 18092 –standardissa. Standardisoinnin edistämiseksi perustettu voittoa tavoittamaton NFC-Forum huolehtii keskeisten spesifikaatioiden julkaisemisesta.

Toiminnan fysikaalinen perusta on sähkömagneettikentän induktiossa, ja sitä käytetään hyväksi tiedon siirtämiseen ilmarajapinnan yli. NFC-tekniikka on jaettu kolmeen eri alatekniikkaan ja näistä jokainen käyttää hieman eri signalointitapoja sekä kehysrakenteita tiedon siirtämiseen rajapinnan yli.

Rajapinnan läpi siirtyvää tietoa voidaan kuljettaa protokollapinossa molempiin suuntiin LLCP-protokollan avulla, jolla on oma kehysrakenteensa.

Avainsanat NFC, NFC-tunniste, LLCP, RFID

Author	Ossi Koistinen
Work Label	NFC-technology
Number of pages	28
Date	December 2010
Thesis supervisor	Kai Poutanen

ABSTRACT

The purpose of this thesis was to gain knowledge about NCF-technology and to report essentially how it works. NFC is an abbreviation of Near Field Communication which is a short-range wireless communication technology enabling the exchange of data between devices over about a 10 centimeter distance. NFC is used in communication between pre-existing tags, i.e. in smartcards, as well as in tags defined in NFC's own specification. It is expected to become very common in mobile devices. Possible applications include mobile commerce and identification. Technically closely related to RFID, NFC has advantage in wider range of possible applications, not least because of its ability to act both as a tag reader and writer.

The technology is defined in ISO 18092–standard released in 2004. A non-profit organization established for promoting the adaptation of NFC is NFC Forum and it releases technical specifications as the technology develops.

Electromagnetic induction of the magnetic field is the basis of the operation and NFC can be divided in to three different sub-technology categories which all use different ways to alternate the magnetic field. Each sub-technology has their own frame format to exchange the data.

Data exchanged through the magnetic field can be moved in the protocol stack by the LLCP-protocol, which also has its own frame format.

Keywords NFC, NFC-tag, LLCP, RFID

ALKUSANAT

Tutkintotyön aiheen valitsimme yhdessä koulutuspäällikkö Ari Rantalan kanssa omasta ehdotuksestani. Haluan kiittää yliopettaja Kai Poutasta avusta työn kanssa. Lisäksi haluan kiittää molempia opettajia erinomaisesta opetuksesta.

Tampereella 17.12.2010

Ossi Koistinen

SISÄLLYSLUETTELO

TIIVISTELMÄ i
ABSTRACT ii
ALKUSANAT iii
SISÄLLYSLUETTELO iv
KÄYTETYT LYHENTEET JA TERMIT v
1 JOHDANTO 1
2 NFC:N HYÖDYT JA VERTAILUA 2
2.1 Erot RFID -tekniikkaan 3
2.2 Erot Bluetooth-tekniikkaan 4
3 TEKNIIKKA 5
3.1 Standardi 5
3.2 Toiminnan fysikaalinen perusta 6
3.3 Laitteiden toimitilat 7
3.4 Fyysinen rajapinta 7
3.4.1 NFC-A 8
3.4.1.1 NFC-A-siirtokomennot ja hyötykuorman sisältö 9
3.4.1.2 Miller-koodaus 10
3.4.1.3 Manchester-koodaus ja OOK 11
3.4.2 NFC-B 12
3.4.2.1 NFC–B:n synkronointi 13
3.4.2.2 NFC-B-kehysrakenne 14
3.4.2.3 NFC-B:n siirtokomennot ja hyötykuorman sisältö 14
3.4.3 NFC-F 15
3.5 Half-Duplex-käytäntö 16
3.6 Tagityypit 17
3.6.1 Tagityyppi yksi 17
3.6.2 Tagityyppi kaksi 18
3.6.3 Tagityyppi kolme 19
3.6.4 Tagityyppi 4A ja 4B 19
3.7 LLCP-protokolla 20
3.7.1 LLC kehysrakenne 22
3.7.2 Linkin avaus 23
3.7.3 Normaali toiminta ja yhteyden katkaiseminen 25
4 YHTEENVETO 25

KÄYTETYT LYHENTEET JA TERMIT

ASK	Amplitude-shift keying. Amplitudiavainnus.
BLE	Bluetooth Low Energy. Bluetoothin vähävirtainen toimintamoodi.
Bluetooth	Langaton lyhyiden etäisyyksien tiedonsiirtotekniikka.
CRC	Cyclic redundancy check. Tarkistussumma.
EoD	End of Data
EoF	End of Frame
EoS	End of sequence
Ecma	European Computer Manufacturers Association. Kansainvälinen tietotekniikan- ja tiedonsiirron-standardointiorganisaatio.
FeliCa	Felicity Card. Japanissa Sonyn kehittämänä älykorttistandardi.
IEC	International Electrotechnical Comission. Sähköalan kansainvälinen standardointijärjestö.
ISO	International Organization for Standardization. Kansainvälinen standardointijärjestö.
ISO 18092	NFC:n määrityksen sisältävä kansainvälinen standardi.
ISO 14443	Kansainvälinen standardi kontaktittomille älykorteille.
LLCP	Logical Link Control Protocol. NFC:n käyttänä tiedonsiirtoprotokolla.
MAC	Media Access Control. Protokollapinon toiseksi alin kerros.
NFC	Near Field Communication. Hyvin lyhyiden etäisyyksien langaton tiedonsiirtojärjestelmä
NDEF	NFC Data Exchange Format. NFC:n käyttämä formaatti, jossa tieto tallennetaan.
NRZ	Non-Return to Zero.
OOK	On-off keying.
OSI-malli	Open Systems Interconnection model. Protokollapinon referenssimalli.
RFID	Radio Frequence Identicifation. Radiotaajuustunnistus.
SoD	Start of data
SoF	Start of frame

SoS	Start of sequence
Tagi	kts. tunniste.
TKL	Tampereen kaupungin liikennelaitos.
Tunniste	Älykorttijärjestelmien käyttämä laite, johon tieto on tallennettu.
VTT	Valtion teknillinen tutkimuskeskus.
WLAN	Wireless Local Area Network. Langaton lähiverkkotekniikka.

1 JOHDANTO

NFC on korkeataajuuksinen langaton hyvin lyhyen etäisyyksien tiedonsiirtomenetelmä, jonka avulla voidaan lukea jo olemassa olevia tai NFC:n oman määrityksen mukaisia tunnisteita tai siirtää muuta tietoa laitteiden välillä. Kantomatkassa NFC:ssä puhutaan muutamista senteistä. Tekniikka on yhteensopiva jo olemassa olevien älykorteissa ja muissa langattomissa tunnisteissa, kuten vaikkapa avaimissa, käytetyn tekniikan kanssa. NFC laitteilla onnistuu myös tunnisteiden muokkaus. NFC:n protokollarakenteen ansiosta ei tarvitse tyytyä tunnisteiden ominaisuuksiin, vaan voidaan siirtää ohjelmille suunnattua tietoa tunnisteesta laitteelle käynnistämään palveluja tai talteen ohjelman käyttämään muistiin.

Tekniikka on suunnattu erityisesti mobiililaitteisiin ja sen odotetaan yleistyvän seuraavan 3-5 vuoden ajanjaksolla niin, että vähintään joka kolmannessa matkapuhelimessa on NFC-siru. Suurimmiksi käyttökohteiksi odotetaan mobiilimaksamista, mobiililippuja, käyttöä kaupankäynnissä yleensä sekä tunnistautumista ja käyttöä julkisessa liikenteessä. Tekniikan avulla toteutettavissa olevia käyttökohteita on paljon.

NFC-tekniikan todellinen salaisuus piilee siinä, että sen avulla voidaan toteuttaa todella helppokäyttöinen rajapinta tekniikan ja käytännön välille. Kosketuksen kaltaisella eleellä voidaan ohjata haluttuja toimintoja ilman ainaisia vaivalloisia asetusparametrien virittämisiä. Kosketus tuo laitteen lähemmäksi ihmistä ja helpottaa uuden teknologian omaksumista. Maksaminen, lisäinformaation haaliminen tai nopean tiedonsiirtoyhteyden avaaminen kahden laitteen välille voi tuskin enää juuri helpommaksi muuttua, kun pelkkä laitteiden kosketus riittää toiminnon suorittamiseen. Kaiken lisäksi vain yksi NFC-laite riittää kaikkien näiden asioiden hoitamiseen ilman esimerkiksi nykyisen kaltaista määrää erilaisia kortteja.

Tämän työn tarkoitus on selvittää NFC-tekniikan mahdollisuuksia ja teknisen toiminnan keskeisiä periaatteita. Keskeisimmiksi toimintaperiaatteiksi on katsottu fyysinen rakenne, signalointitavat ja tiedonsiirron käsky- ja kehysrakenne sekä tekniikan kannalta oleellisimman protokollan toiminta.

Työn pohjalta ei ole tarkoitus olla mahdollista rakentaa toimivaa NFC-järjestelmää, vaan sen avulla selviävät toiminnan keskeisimmät periaatteet ja mahdollisuudet. NFC-laitteilla olevia erilaisia toimintatiloja kuten lepotilaa, valmiustilaa ja kortinemulointitilaa eikä niihin pääsemiseksi vaadittavia toimia käsitellä tässä työssä. Laitteiden oletetaan olevan saatettu tiedonsiirron sallivaan tilaan.

NFC:n menneisyys seuraa pitkälti RFID:n jälkiä. Radiotaajuustunnistuksen esi-isänä pidetään usein toisen maailmansodan aikana kehitettyä tutkaa, sillä siinäkin periaate on se, että aktiivisen laitteen lähettämä radiokenttä kerää tietoa kohteesta saaden tietonsa heijasteesta. Yhtälailla kuin tutkan muodostamasta kuvasta voidaan tunnistaa asioita, RFID-tunnisteen sisältämän tiedon signaaliin aiheuttaman heijasteen avulla voidaan tunnistaa erilaisia asioita. Kuusikymmentä ja seitsemänkymmentäluvuilla kohti nykyistä suuntaansa alkanut kehitys alkoi mm. myymälävarkauksien tunnistamiseen kehitetystä sovelluksesta ja ensimmäinen muistilla varustettu tunniste puolestaan oli kehitetty tietullimaksujen helpottamiseen. /1/

Nykyisin yleiset logistiikan tunnistetagit alkoivat tulla käyttöön kahdeksankymmentäluvun loppupuolelta alkaen. Suuri taustavoima tunnisteiden kehityksessä oli Yhdysvaltain armeija, joka tarvitsi järjestelmän tavaroidensa tunnistamiseen ja sijainnin seuraamiseen. Yhdysvaltalaiset logistiikka-alan yritykset olivatkin tuolloin mukana kehitystyössä, johtuen juuri tavaroiden seurannan luomasta tarpeesta.

Omaksi haarakseen NFC alkoi haarautua vasta 2000-luvulla. Vielä tänäkin vuonna päivityksiä saanut NFC:n määrityksen sisältävä ISO 18092 –standardi (Information technology -- Telecommunications and information exchange between systems -- Near Field Communication -- Interface and Protocol) julkaistiin vuonna 2004. Kehitys tekniikan suhteen on tällä hetkellä jatkuvaa.

2 NFC:N HYÖDYT JA VERTAILUA

Nykyään hyvin yleiset älypuhelimet ovat tuoneet mukanaan uudenlaisia mahdollisuuksia erilaisten sovellusten kehittämiseen. Riittävä laskentakyky ja viimeistään kosketusnäyttöjen myötä hyvin suureksi kasvanut näyttöpinta-ala ovat tehneet mielekkääksi perinteisen internetinkin käytön mobiililaitteilla. Internet

matkapuhelimen yhteydessä on mahdollistanut uudenlaisen jatkuvan yhteydenpidon erilaisiin palveluihin paikasta riippumatta tehden samalla mahdolliseksi yhä useampien toimintojen samaan laitteeseen yhdistämisen. Eri tietokanavissa sijaitseva tieto on melko konkreettisesti käden ulottuvilla laitteen ollessa sovelluksen tai käyttäjän pyynnöstä heti yhteydessä palvelun sisältämään tietoon. Esimerkkinä voidaan ajatella tuotteesta suoraan luettavaa internetin kautta päivittyvää hintatietoa tai muuta lisäinformaatiota, ostoksen maksamista pankkiin yhteydessä olevaa matkapuhelinta vilauttamalla tai elektronista avainta. Kaikki nämä toiminnot voisivat siis löytyä yhdestä ja samasta laitteesta. Jokaiseen taloon ei tarvitsisi enää olla erillistä avainläpykkää, riittää kun avaimen tunnistenumero on sähköisessä tietokannassa, josta sen oikeudet selviävät. Saatu oikeus voidaan tämän jälkeen vielä tallentaa paikalliseen tunnisteeseen. NFC mahdollistaa myös uudentyyppistä mainontaa, sillä esimerkiksi tapahtumajulisteeseen liitetty tagi voi lisätä tapahtuman tiedot suoraan käyttäjän laitteen kalenteriin ja vaikka lisäksi ehdottaa lippujen ostoa. Älyjulisteeksi kutsuttua tekniikkaa on testattu myös Tampereella TKL:n bussiaikatauluissa.

Käyttäjäystävällisyydestäkään ei tekniikan yleistyminen jääne kiinni. Pelkästään vieressä käyttämällä tai koskettamalla NFC-laitteella toista, voidaan käynnistää toimintoja. Esimerkkinä tästä voisi olla vaikkapa hälytyslaitteen pois kytkeminen kotiin saapuessa ja samassa toiminteessa oman maun mukaisten valojen päälle laittaminen. Hyödyllistä ja helppoa kaikille iästä tai teknisistä taidoista riippumatta.

Toistensa lähelle tuodut laitteet voivat siirtää tietoa NFC:n oman tiedonsiirtoprotokollan välityksellä, mutta myös käynnistää laitteesta mahdollisesti löytyvän toisen kenties käyttöön sopivamman tiedonsiirtomenetelmän kuten WLAN tai Bluetooth. Tietojen vaihto matkapuhelimesta toiseen tai vaikkapa tietokoneeseen helpottuu, kun käyttäjän ei tarvitse kuin pyytää tietojen siirtoa viereiseen laitteeseen ja NFC huolehtii lopusta, eli vaikka juuri mahdollisen Bluetooth-yhteyden avaamisesta.

2.1 Erot RFID -tekniikkaan

Perinteisiin RFID-tunnisteisiin nähden NFC-laitteilla on eronsa. Siinä missä RFID-tunniste on lukittu siihen rooliin, mihin se alun perin on valmistettu, NFC-siru voi muuttaa rooliaan. Laite voi tarpeen mukaan toimia luku/kirjoittaja-laitteena, käyttäytyä kuin se olisi pelkkä tunniste tai toimia ns. peer to peer –tilassa toisen NFC-laitteen

kanssa. Lukijana/kirjoittajana toimittaessa voidaan olla vuorovaikutuksessa ISO 14443 ja FeliCa-standardien mukaisten, eli NFC-Forumin määritysten mukaisten, tavallisten tagityyppien kanssa ja tarvittaessa muokata niitä. Pelkkänä tunnisteena toimiva laite on käytännössä passiivitilassa, ja se toimii aivan kuten esimerkiksi tavallinen älykortti. Peer to peer, eli laitteelta-laitteelle, tilassa NFC-yksiköt voivat siirtää periaatteessa mitä tahansa tietoa keskenään ja käyttää sen tallentamiseen isäntälaitteen ominaisuuksia. Siirrettävä data voi luonnollisesti tulla protokollapinon korkeammilta tasoilta, aina ohjelmiin asti. Laitteiden oma tiedonsiirtostandardi huolehtii tiedon kehysrakenteesta ja esimerkiksi virheenkorjauksesta. /2/

Vaikka RFID-tunnisteet ovat suosittuja ja käteviä monessa käyttökohteessa, niissä on omat rajoituksensa. Yhden suuren rajan muodostaa tagien sisällön muokkaamisen vaikeus tunnisteiden ollessa käytännössä vain luetuiksi, ei muokattavaksi, tarkoitettuja. NFC-laite voi toimia tunnisteen ohella myös luku- ja kirjoituslaitteena toisin kuin RFID:ssä. NFC:n kanssa yhteensopivat RFID-tunnisteet toimivat 13,56 megahertsin taajuudella. Taajuus kattaa suuren osan käytössä olevista tunnisteista, mutta silti yhteensopivuutta kaikkiin ei ole ainakaan tällä hetkellä.

2.2 Erot Bluetooth-tekniikkaan

Bluetooth-tekniikkaa on hyödynnetty matkapuhelimissa ja muissa mobiililaitteissa jo pitkän aikaa. Bluetooth-yhteys on merkittävästi nopeampi NFC-yhteyteen verrattuna ja myös sen kantama on moninkertainen. Luokan yksi Bluetooth-laite yltää noin sadan metrin kantamaan heikoimman kolmannen luokankin ollessa metrin kantamallaan ainakin viisi kertaa NFC:tä pidemmälle kuuluva. Tämän hetken NFC-standardin maksiminopeuskin on murto-osa uusimman Bluetooth-version teoreettiseen maksiminopeuteen 24 Mbit/s verrattuna.

Pitkässä kantamassakin on kuitenkin haittapuolensa, eikä ole vain umpimähkään päätetty NFC:n toimivan hyvin lyhyillä etäisyyksillä. Pitkä kantomatka vaatii enemmän tehoa, joka mobiililaitteessa on muutenkin rajallista. Signaali kärsii väistämättä pidemmällä matkalla myös suuremmasta määrästä häiriöitä, olivat ne sitten luontaisia tai tahallaan aiheutettuja. Periteinen Bluetooth vaatii lisäksi yhteyden muodostuksen hyväksynnän, ja pariliitoksen aikaansaamiseen vierähtää helposti suhteessa tehtävään asiaan nähden paljon aikaa ja vaivaa. NFC muodostaa yhteyden noin kymmenesosasekunnissa. Huhtikuussa 2010 valmiiksi standardiksi saatu Bluetooth 4.0

sisältää uutena ominaisuutena matalan energiatason Bluetoothin (Bluetooh Low Energy, BLE), jonka avulla eroja NFC:hen on kurottu umpeen. Kymmenen metrin kantamaan yltävä BLE yltää samaan maksimissaan noin viidentoista milliampeerin virrankulutukseen kuin NFC ja yhteydenmuodostuksen vaiheita karsimalla on päästy jopa NFC:tä hieman nopeampaan linkinavausaikaan. Toisaalta BLE toimii vain noin kahdensadan kilobitin sekuntinopeudella eikä yhteensopivuutta RFID-tunnisteisiin olla kehittämässä. /3/

3 TEKNIIKKA

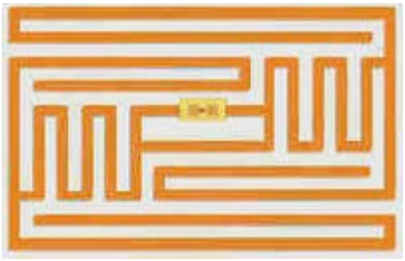
3.1 Standardi

Kansainvälisissä ISO/IEC 18092 (Interface and Protocol -1) sekä ISO/IEC 21481 (Interface and Protocol -2) -standardeissa on määritetty rajapinta ja protokolla 13,56 megahertsin taajuudella toimivalle lyhyen etäisyyden tiedonsiirrolle. Standardin nimenä on Near Field Communication, NFC. Käytännössä NFC on siis korkeintaan noin kahdenkymmenen senttimetrin etäisyydellä toimiva langaton tiedonsiirtotekniikka. Standardi on yhteensopiva RFID-tekniikan sekä kontaktittomissa älykorteissa käytetyn ISO/IEC 14443-määrityksen kanssa ja sitä voidaankin pitää niiden laajennuksena. NFC sisältää suuren joukon uusia ominaisuuksia edeltäviin tekniikoihin nähden. Kuitenkin pelkästään yhteensopivuus älykorttistandardin kanssa takaa NFC:lle miljoonia käyttäjiä maailmanlaajuisesti jo tälläkin hetkellä. /2/

Standardien ylläpidosta vastaa vuonna 1961 perustettu Ecma International -järjestö. ISO/IEC 18092 ja ISO/IEC 21481 -standardit ovat hallinnollisesti kansainvälisen ISO/IEC JTC 1/SC 6 -komitean vastuulla, kun taas ISO/IEC 14443 -standardisarjasta vastaa kansainvälisen ISO/IEC JTC 1/SC 17 -komitea. Suomen osalta komiteoiden työtä seuraa ja kansallisia kannanottoja lähettää SFS:n IT-standardisointi /2/.

Standardisoinnin edistämiseksi Nokia, Philips ja Sony perustivat vuonna 2004 voittoa tavoittelemattoman NFC-Forumin. Sen nykyiset yli sata jäsentä muodostavat kahdeksan työryhmää, joiden toimialoja ovat muun muassa markkinointi, tekniikan kehitys ja yhteensovittaminen sekä testaus. Forum itse ei vastaa standardoinnista. Jäsenten joukosta löytyy perinteisten tietotekniikka-alan yritysten lisäksi myös tunnettuja luottokorttifirmoja, joka ei liene yllättävää tekniikan ollessa suunniteltu myös

maksamiseen. Suomessa Nokian lisäksi VTT ja lukuisat muut yritykset ovat tehneet maailmanlaajuisestikin edellä käyvää työtä tekniikan parissa.
Kesällä 2006 NFC-Forum esitteli standardisoidun teknisen arkkitehtuurin ja spesifikaation NFC-yhteensopiville laitteille ja tageille. (engl. Tag). Tagi eli tunniste on käytännössä antenniin kytketty mikropiiri, jossa tieto sijaitsee. Spesifikaatiot sisälsivät NFC:n tiedonsiirrossa käytetyn protokollan LLCP (Logical Link Control Protocol), NDEF:n (Data Exchange Format) ja RTD:n (Record Type Definition) sekä neljä erilaista tagiformaattia, joita NFC-yhteensopivan laitteen on tuettava. Julkaisuja on tullut ja on yhä tulossa tämän jälkeen lisää /4/



Kuva 1: Tyypillinen tagi /12/

3.2 Toiminnan fysikaalinen perusta

Käytetty 13,56 megahertsin taajuus on yleisesti lisenssivapaa, eikä näin ollen tarvitse erillistä lupaa. Samaa taajuutta voidaan myös käyttää globaalisti. Fysikaalinen perusta toiminnalle on sähkömagneettikentän induktiossa. Toistensa lähelle tuodut silmukka-antennit muodostavat magneettikentän, jota muokkaamalla tietoa siirretään. Kytkentä on siis ikään kuin ilmasydäminen muuntaja. Antennina toimii metallinen, usein kuparinen, silmukoille käämitetty johdinkalvo. Lukijalaite johtaa antenniinsa vaihtovirtaa, jolla se synnyttää magneettikenttänsä. Magneettikentän on päästävä luettavan laitteen käämin läpi, joten polarisaatiolla on merkityksensä. Käytännössä magneettikentässä siirtyvä energia indusoituu kohdelaitteen antenniin ja sitä kautta tagissa oleva mikropiiri saa virtansa, kunhan se ensin tasasuunnataan tasasuuntaajalla. Piirissä oleva data moduloi tämän jälkeen tagin käämin virtaa, joka näkyy lukijalaitteessa antennisilmukan jännitteen vaihteluna. Tunnisteessa olevat käämi ja antennin kanssa rinnan kytketty kondensaattori on mitoitettu siten, että antenni virittyy oikealle toimintataajuudelle komponenteista syntyvän rinnakkaisresonanssipiirin avulla. Väärin mitoitettu resonanssipiiri johtaa tilanteeseen, jossa tunnisteeseen ei siirry magneettikentän virtaa ja laite ei toimi. Tämän vuoksi lukijan ja tunnisteen taajuuksien on oltava samat. /1/ /2/

3.3 Laitteiden toimitilat

Protokollan mukaisessa tiedonsiirrossa on aina kaksi laitetta. Luku- ja/tai kirjoitinlaite sekä tagi (engl. Tag). Tiedonsiirto useampaan laitteeseen kerralla eli ns. broadcasting ei ole tuettua. Laitteilla on kaksi mahdollista tilaa. Passiivisessa tilassa aloittava laite (engl. initiator) luo kantoaallon, eli sähkömagneettisen kentän, jota kohde (engl. target) siis moduloi. Aktiivisessa tilassa molemmat laitteet luovat ja muokkaavat sähkökenttäänsä vuorotellen niin, että luettavana oleva laite sulkee oman kenttänsä luvun ajaksi. Periaatteessa toinen osapuoli on siis aina passiivinen. Aktiivinen laite tarvitsee myös aina oman virtalähteen kentän luomiseksi, kun taas passiivinen voi olla virtalähteetön. Samalla se tarkoittaa myös sitä, että passiivinen laite ei käytännössä voi koskaan olla aloittava laite. /2/

Aloittava laite on aina vastuussa tiedonsiirrosta yhteyden ajan. Huomattavaa on, että protokollassa on määritetty, ettei vastaanottava laite voi koskaan aloittaa tiedonsiirtoa saamatta ensin jonkinlaista pyyntöä aloittavalta laitteelta. Aivan tarkalleen ottaen aloittava laite voi olla yhteydessä useampaan vastaanottajaan, mutta sen on valittava niistä vain yksi vastaanottaja kerrallaan ja muiden datan kuulevien laitteiden on hylättävä saamansa tiedot. Tämän vuoksi broadcast-lähetys ei ole mahdollista NFC:llä ja tiedonsiirto tapahtuu käytännössä aina kahden laitteen välillä. /2/

Passiivista tilaa voidaan pitää hyvin tärkeänä mobiililaitteissa, joissa energian kulutusta on tarkkailtava tarkemmin. Toisaalta ilman passiivitilaa ei edes voitaisi käyttää täysin virtalähteettömiä sovelluksia, kuten vaikka tuotteeseen painettua tunnistetietoa. NFC-protokollassa on määritelty lisäksi erillinen virransäästötila, jossa esimerkiksi jatkuvaa virtaa käyttävä laite voi toimia aktiivisena osapuolena, säästäen näin mobiili- tai muun laitteen paristoa.

3.4 Fyysinen rajapinta

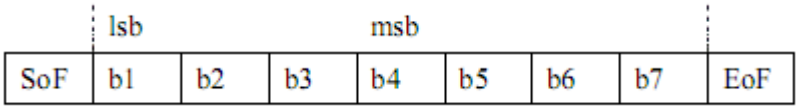
Tiedonsiirto kanavassa tapahtuu 14 kilohertsin kaistanleveydellä ja tiedonsiirtonopeus siinä voi olla 106, 212 tai 424 kbit/s riippuen tunnisteen tyypistä. Nopeampia yhteyksiä on kehitteillä. Tunnisteen tyypistä riippuen käytetään myös eri signaalinkoodaustapoja. Laitteet jaetaan kolmeen luokkaan käytetyn signalointitavan sekä käsky- ja kehysrakenteen mukaan.

3.4.1 NFC-A

Laitteiden välillä lähetettävät bittijonot pakataan kehyksiin. NFC-A-tekniikassa on käytössä kolme eri kehystä. Hyötydatan lisäksi lähetetään tarkistussuman laskemiseksi pariteettibitti jokaisen kahdeksan hyötybitin jälkeen ja kehyksien alkuun ja loppuun lisätään SoF (Start of Frame) sekä EoF (End of Frame). SoF ja EoF muodostetaan määrätyillä signaalimuodoilla. Signaalimuoto riippuu lisäksi siitä, kommunikoidaanko lukijalta tunnisteelle vai päinvastoin. /5/

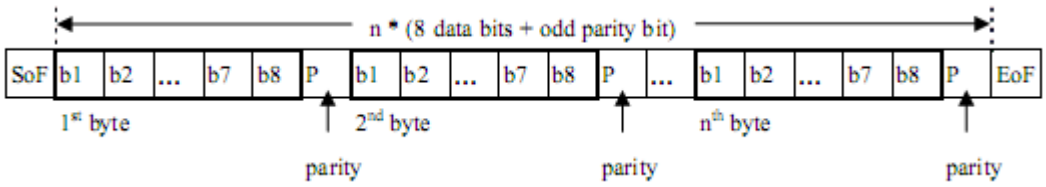
Lukijalta tunnisteelle lähettäessä SoF kuvataan NFC-A:n signaloinnin mukaisella loogisella nollalla. Päinvastaiseen suuntaan esitystapana on signalointimuodoin looginen yksi. Kehyksen loppua merkitsevä EoF merkitään lukijaltapäin loogisella nollalla ja päinvastoin signaalimuodolla F. Signaalimuoto F ja muut muodot selviävät kohdasta 3.4.1.3. /5/

Kolme käytettävää kehystyyppiä ovat lyhyt kehys (Short Frame), normaalikehys (Standard Frame) sekä SSD. Lyhyt kehys on tarkoitettu yhteyden alustukseen ja sen rakenne on kuvassa 2. Bittiarvot lähetetään alkaen vähiten merkitsevästä bitistä (lsb). Muista kehyksistä poiketen pariteettibittiä ei ole. /5/



Kuva 2: Short Frame-yhteydenalustuskehys./5/

Normaalikehyksessä siirretään varsinainen hyötykuorma. Kehys koostuu vähintään yhdestä kahdeksan bitin sarjasta, toisin sanoen tavusta, jonka perässä on pariteettibitti. Alussa ja lopussa on SoF ja EoF. Tavujen maksimimäärä kehyksessä määritetään linkin asetuksissa./5/



Kuva 3: Normaalikehys. /5/

Viimeisenä kolmesta mahdollisesta olevaa SSD-kehystä käytetään virheistä toipumiseen. Rakenteeltaan normaalikehystä muistuttava SSD on ulkoisesti seitsemän hyötytavun mittainen normaalikehys pariteetteineen. Kehys jaetaan kuitenkin kahtia niin, että ensimmäisen osan lähettää lukijalaite ja toisen tunniste vastauksena ykkösosaan. Kahtiajako voidaan tehdä mistä vain, mutta mikäli se tapahtuu juuri ennen pariteettia, pariteettibitti otetaan mukaan osaan yksi. Seitsemän hyötytavun kiinteän mitan avulla tiedetään molempien osien yhteenlasketun hyötybittien tarkaksi määräksi 7 * 8 = 56, jota voidaan käyttää tarkistuksessa. Lisäksi ensimmäisen osan minimipituudeksi on määrätty 16 bittiä ja maksimiksi 55. Tästä seuraa, että toisen osan vastaavat arvot ovat 8 ja 40 bittiä. Huomionarvoista on, että jos katkaisu tapahtuu minkä tahansa kahdeksan hyötybitin jälkeen, kehys on aivan samanlainen kuin normaali. /5/

3.4.1.1 NFC-A-siirtokomennot ja hyötykuorman sisältö

Itse hyötykuorma koostuu protokollapinon ylemmiltä tasoilta tulevasta bittivirrasta, jonka sisältöön NFC ei ota kantaa, sekä siirtoon liittyvistä komennoista. Kaksi viimeistä tavua normaalikehyksestä on lisäksi varattu tarkistussummien laskemiseen tarkoitetuille CRC_A1- ja CRC_A2-summille. Ennen EoF signaalia tulevaa tarkistussummaosaa kutsutaan myös nimellä EoD (End of Data). Tarkastussumman ollessa virheellinen pyydetään datan uudelleensiirtoa ja ilmoitetaan siirtovirheestä alemmalle protokollatasolle. CRC lasketaan hyötykuormabittien arvon summana ja CRC_A1:n ensimmäinen bitti on arvon vähiten merkitsevä bitti ja A2:n viimeinen eniten merkitsevä. /5/

Eri komennot tunnistetaan niiden kiinteiden heksadesimaaliarvojen tavun pituisista binääriesityksistä. Käytössä on kaikkiaan kahdeksan komentoa. Komennon lähettää aina lukija ja vastauksen tunniste.

Komento	Vastaus	EoD	Kehys
ALL_REQ,SENS_REQ	SENS_RES	Ei	Lyhyt
SDD_REQ	SDD_RES	Ei	SDD
SEL_REQ	SEL_RES	Kyllä	Normaali
SLP_REQ	---	Kyllä	Normaali

Kuva 4: Luettelo NFC-A- komennoista.

ALL_REQ tai SENS_REQ-komennolla tiedustellaan linjalla olevia laitteita. Vastauksena tagi antaa kaksitavuisen sarjan, jossa se ilmoittaa, käyttääkö se neljän, seitsemän vai kymmenen tavun pituista NFCID1-tunnistetta. Samalla se kertoo, onko se normaaleilla ykköstyypin tunnisteen vai mahdollisesti joillakin muilla asetuksilla toimiva sekä raportoi nykyisen toimitilansa. Karkeasti yksinkertaistettuna komennolla SDD_REQ saadaan varsinaisesti tiedusteltua laitteen NFCID1-numero. Komentoa SEL_REQ puolestaan käytetään, kun valitaan mahdollisesti kantoetäisyydellä olevista laitteista se, jonka kanssa kommunikoidaan. SLP_REQ on kehote siirtyä lepotilaan. NFCIDx-tunnisteet ovat laitteiden kiinteitä tai dynaamisia arvoja kunkin laitteen tunnistamiseksi yhteyden aikana. /5/

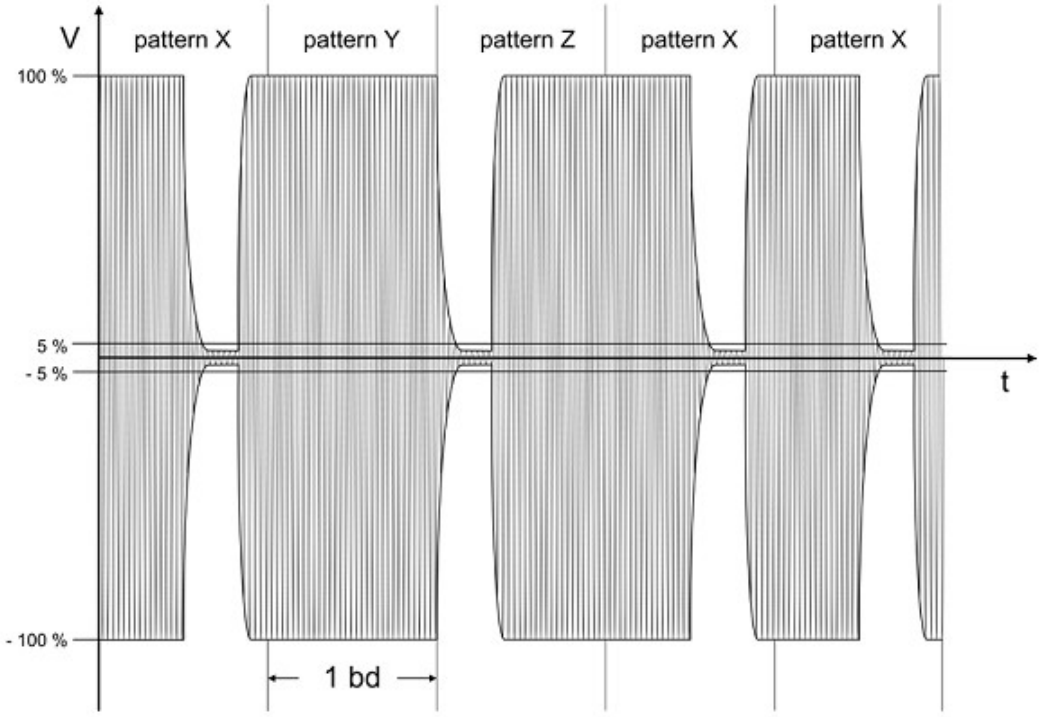
A-tyypin laitteet käyttävät lukijalaitteelta kommunikoidessaan muokattua sadan prosentin moduloitua Miller-koodausta. Modulaatiomenetelmänä on amplitudiavainnus (ASK – Amplitude-shift keying), jossa kantoaaltoa moduloiva datasignaali nähdään kantoaallon jännitteen vaihteluina. Tunnisteelta lukijalle kommunikoidessa käytössä on Manchester-koodaus OOK-apukantoaaltomodulaatiolla. Apukantoaallon taajuus on 847,5 kilohertsiä. /5/

3.4.1.2 Miller-koodaus

Miller-koodissa yhden bitin aikaväli on jaettu kahtia alku- ja loppubittiin. Perinteisessä Miller-koodissa nollabittiä esittää tauko alkubitissä ja tilan vaihdos loppubitin osalla. Ykkösbitillä tilanne on muuten sama, mutta toisinpäin puolien osalta. Toisin sanoen mahdollinen tilan muutos näkyy ikään kuin puolen kellojakson viiveellä, ja siksi Miller-koodaus tunnetaan myös nimellä viivekoodaus (engl. Delay encoding). Käytettävä muokattu Miller eroaa kuitenkin hieman tavallisesta. Jos signaalissa on ykkösen jälkeen nolla, kahdessa peräkkäisessä puolijaksossa olisi nolla. Tämä kuitenkin vältetään koodaamalla nolla, jota seuraa ykkönen. Signaali siis käännetään ja kahden taukopuolikkaan tilalla onkin näin kaksi ykköstä. Toinen muutos koodauksessa on, että yhtä bittiä voi esittää kaksi, neljä tai jopa kahdeksan jaksoa ko. bitin aaltomuotoa. /5/

Kuvasta kaksi nähtäviä lukijalaitteen kehittämiä signaalimuotoja X, Y ja Z tulkitaan laitteessa eri loogisiksi tiloiksi. Alkubitin osalta moduloimaton ja lopusta moduloitu X esittää loogista ykköstä. Täysin moduloimattomalla Y-signaalimuodolla esitetään nollaa. Z on käytössä vain, jos signaalin ensimmäinen bitti on nolla, tai aina toisesta

nollasta alkaen, jos nollia on signaalissa peräkkäin vähintään kaksi. Muotoa Y käytetään myös komentosarjan lopetuksen merkiksi, eli sillä koodataan EoS (End of Sequence). /5/

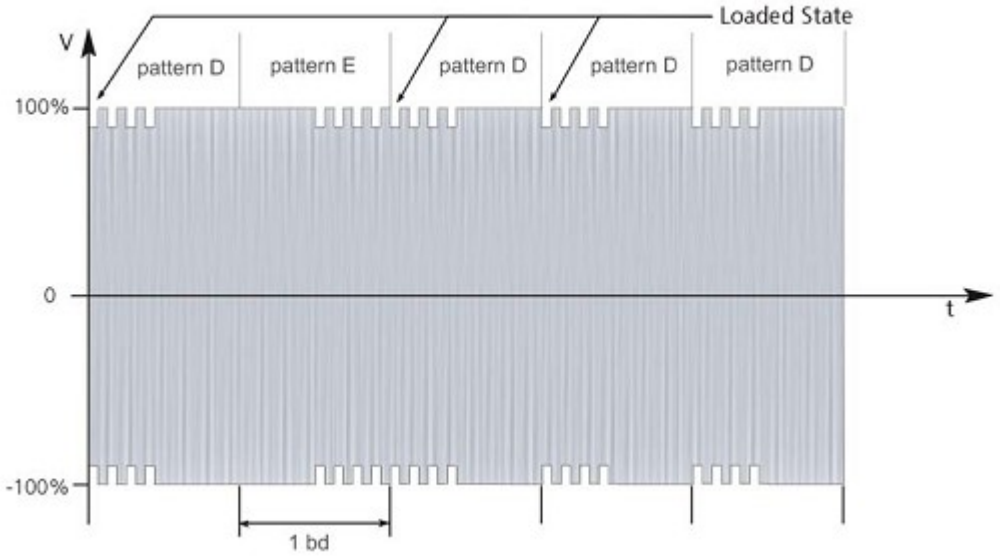


Kuva 5: Amplitudimoduloitua Miller-koodia. /5/

3.4.1.3 Manchester-koodaus ja OOK

Manchester-koodauksessa bittiä edustaa tilanmuutos. Jos kyseessä on bitti yksi, tila muuttuu ylhäältä alas, nollalla päinvastoin. Koodauksesta on tosin olemassa kaksi varianttia, joista toisessa tilan vaihdos onkin päinvastaisen suuntainen kuin toisessa. Tilanvaihdos tapahtuu aikavälin keskellä, eikä muulla kuin tilanvaihdon suunnalla ole merkitystä. Siksi bitin alku tai loppupuoli voidaan tauottaa tai moduloida. Käytännössä tilan vaihdos on 180 asteen vaiheensiirto, tämän vuoksi Manchester-koodi puolestaan tunnetaan myös vaihe-koodauksena (engl. Phase encoding). Manchester-koodi on itsestään synkronoituvaa, eli erillistä kelloa tai synkronointivaihetta ei tarvita./5/

Signaalin modulaatiomenetelmä OOK on yksinkertaistettu versio ASK:sta ja ero näkyy käytännössä siten, että tauon kohdalla ei lähetetä yhtään mitään. Tässä yhteydessä käytetty 10 % modulaatio näkyy näin ollen signaalissa kantoaaltoa pienempänä amplitudina. /5/



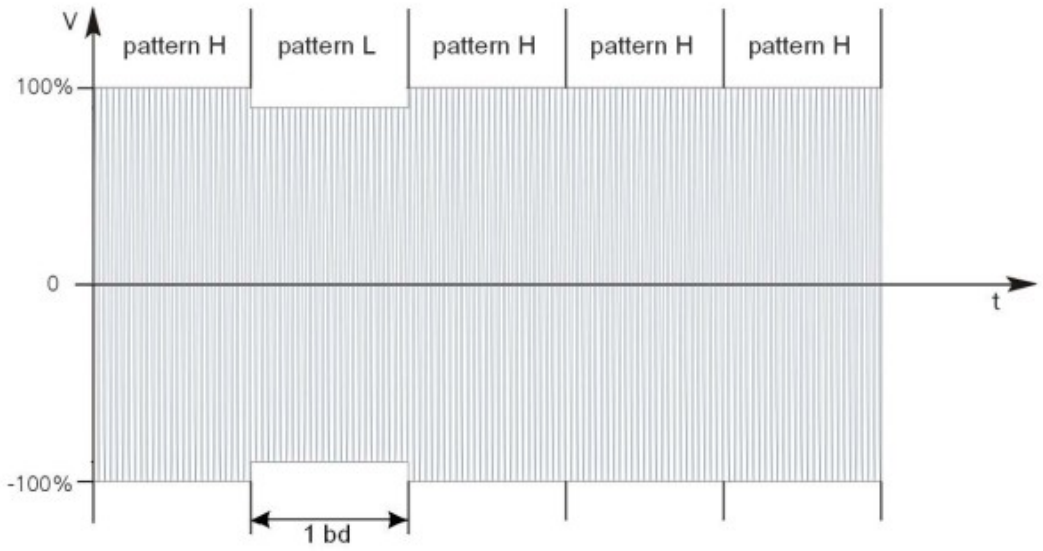
Kuva 6: Manchester-koodaus OOK-modulaatiolla. /5/

Kuvassa 6 näkyvät signaalimuodot D ja E sekä kuormitettu tila (Loaded state). Kuormitettua tilaa, eli matalammalta tasolta aloittamista, tulee käyttää aina, jos bittijakso alkaa moduloidulla osuudella. Moduloidulla alkujaksolla alkava kuvio D merkitsee loogista ykköstä. E on nolla. Kuvasta puuttuu vielä mahdollinen muoto F, jossa koko jakso on moduloimaton eikä mitään lähetetä. Kanttiaaltokuvio syntyy, kun 13,56 megahertsin kantoaaltoa moduloidaan vielä käytetyllä apukantoaallon taajuudella. Tarkalleen apukantoaaltomoduloitu osuus on 82 %:a kantoaallon amplitudista. /5/

3.4.2 NFC-B

ISO 14432-pohjainen NFC-B-signalointi käyttää kymmenen prosentin ASK-moduloitua signaalia, joka on NRZ-L-koodattu. Tunnisteelta lukijalle voidaan lisäksi vaihtoehtoisesti käyttää samoin koodattua, mutta BPSK-moduloitua signaalia. Tämä ei kuitenkaan ole siis pakollista.

NRZ-eli Non-Return to Zero -koodaus on yksinkertainen menetelmä, jossa on kaksi eri amplituditasoa tilojen esittämiseen. Kuvassa seitsemän näkyvä korkeampiamplitudinen signaalimuoto H esittää ykköstä ja matalampi L nollaa. Matalampiamplitudinen L aikaansaadaan moduloinnin avulla. H on moduloimaton. Koodaustavan huonona puolena voidaan pitää helposti menetettävää synkronointia, jos samaa bittiä lähetetään pitkään peräkkäin. NRZ:n ja NRZ-L:n ero on se, että NRZ-L on tasasuunnattua. Signaali ei siis missään vaiheessa käy negatiivisella jännitealueella ja sen keskiarvo on suurempi kuin yksi. /5/



Kuva 7: NRZ-L-koodaus. /5/

Valinnaisesti käytettävä BPSK (Binary Phase-Shift Keying) on yksinkertaisin vaihemodulaation muoto. Siinä signaalin vaihetta siirretään 180 astetta eteen tai taaksepäin riippuen siitä, ollaanko siirtymässä ykkösestä nollaan vai päinvastoin. Signaalia purettaessa tarvitaan referenssisignaalia, johon vastaanotettua verrataan. Ilman vertailuarvoa ei voida tietää, kumpi vaihe on mitäkin loogista arvoa varten./5/

3.4.2.1 NFC–B:n synkronointi

Koodaustapana oleva NRZ-Z ei ole Manchester- ja Miller-koodien tavoin itsestään synkronoituvaa. Jokaisen komentokehyksen alkuun ja loppuun on signaalissa siis lisättävä synkronointivaiheet SoS (Start of Sequence) ja EoS.

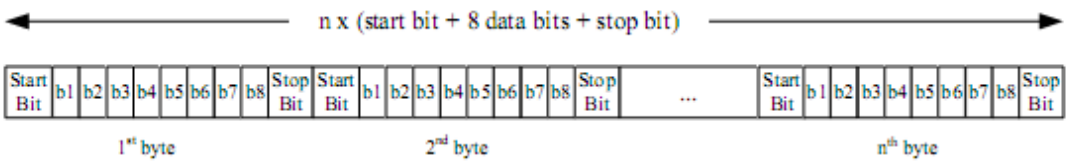
Käytännössä synkronointi suoritetaan signaalin tasolla ja se koostuu kolmesta vaiheesta. Kun edellinen komento on saatu lähetettyä tai lähetettävä kehys on datan ensimmäinen, asettuu lukija määrätyksi ajaksi tilaan, jossa se ensin on piittaamatta mahdollisesti vastaanottamastaan apukantoaallosta ja lopuksi kuuntelee sitä ja ottaa senhetkisen vaiheen referenssikseen. Tunniste puolestaan katkaisee edellisen komennon jälkeen apukantoaaltonsa kokonaan ja sitten lähettää sitä hetken ilman vaiheenkääntöjä, antaen tunnisteelle referenssin. Seuraavaksi referenssin saanut lukija odottaa kuulevansa +180 asteen vaiheensiirron apukantoaallossa ja tämän jälkeen määrätyn ajan verran vaihesiirrettyä apukantoaaltoa. Lopuksi pitää vielä havaita toinen +180 asteen vaihesiirto takaisin alkuperäiseen vaiheeseen ja tätä seuraava jakso tämän vaiheista signaalia, jotta lukija voi katsoa saaneensa SoS-signaalin ja olevansa synkronoitu. Ajat

vaihesignaalien kestoille ja komentojen välisille tauoille ovat ennakkoon määritettyjä ja noudattavat tiettyjä raja-arvoja. /5/

Kehyksen lopussa suoritettava de-synkronointi, eli EoS, on hieman synkronointia yksinkertaisempi toiminne. Apukantoaallon +180 asteen vaihesiirto, jota seuraa määrätyn pituinen jakso tämän vaiheista signaalia ja toinen +180 asteen siirto, tulkitaan siirron lopetukseksi. /5/

3.4.2.2 NFC-B-kehysrakenne

Myös kehysrakenteessa on eroja A-tyypin tekniikkaan nähden. Siinä missä NFC-A ei tarvitse synkronointia ja on siltä osin B-tyyppiä yksinkertaisempi, on B kehysrakenteeltaan yksinkertaisempi. Käytössä on ensinnäkin vain yksi kehystyyppi.



Kuva 8: NFC-B:n siirtokehyksiä ja niiden rakennetta. /5/

Jokainen tavu alkaa aloitusbitillä ja päättyy lopetusbittiin. Tavuja voi kehyksessä olla linkin asetuksissa määrätty määrä. Aloitusbitti esitetään signaalimuodon loogisella nollalla ja lopetusbitti ykkösellä. Yhden tavun siirtämiseen kuluu siis aina kymmenen bittisymbolia. /5/

3.4.2.3 NFC-B:n siirtokomennot ja hyötykuorman sisältö

Lähetettyjä tavuja seuraa aina kaksitavuinen tarkistussummakenttä EoD, aivan kuten NFC–A-tekniikassakin. Muu osa on komentoja ja varsinaista hyötykuormaa, sillä erillistä SoD osaa ei tarvita tässäkään tekniikassa.

Komentoja on käytössä kaikkiaan seitsemän, kun vastaukset lasketaan mukaan. Käskyjen sisäistä rakennetta yksityiskohtaisesti tarkastelematta komentojen tehtävät ovat pääpiirteittäin seuraavanlaisia:

- Käsky ALLB_REQ tai vaihtoehtoinen SENSB_REQ tiedustelee linjalla olevien tunnisteiden NFCID0 tunnusta ja muita ominaisuuksia, kuten bittinopeutta, kehyksen välisen ajan arvoa ja kehyksen maksimipituutta. Komento on kolmen

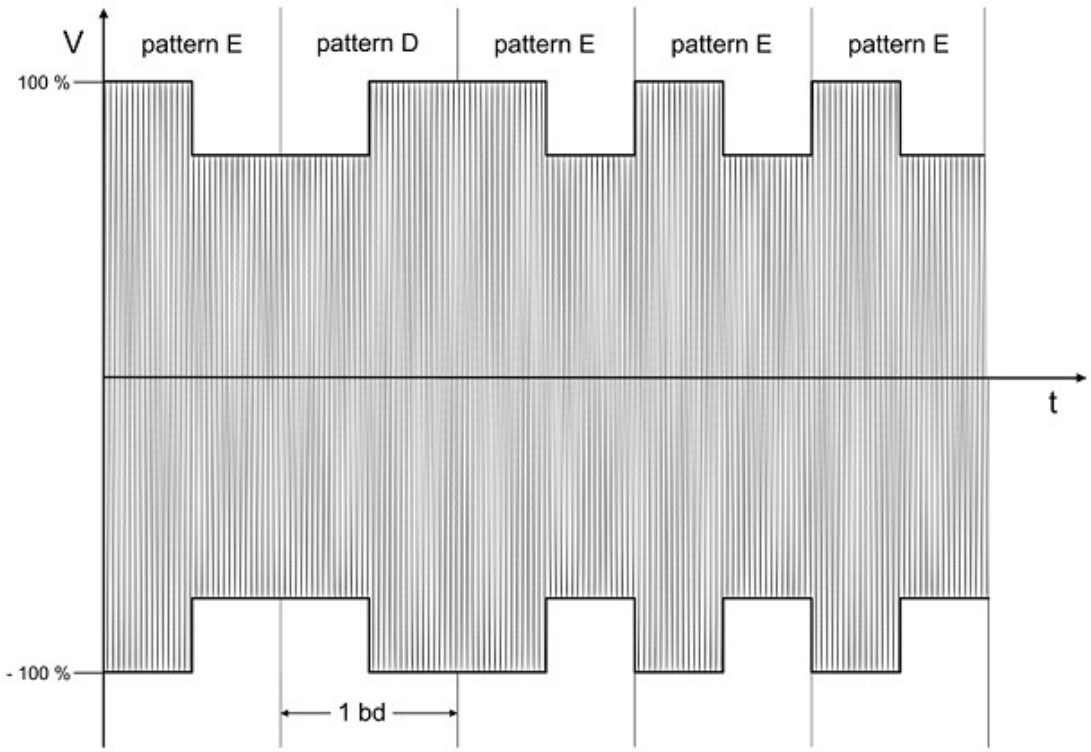
tavun mittainen, mutta paluukomennossa SENSB_RES tulevaa tietoa voi olla kolmetoistakin tavua.

- Komennolla SLOT_MARKER määrätään vastauksen aikaväli, mikäli ISO 14443-määrityksen mukainen signaalien törmäyksenesto on käytössä. Komennon tuki on vapaaehtoista ja paluuarvo käytettävästä aikavälistä annetaan SENSB_RES-komennon kentässä.
- SLPB_REQ määrää tunnisteen lepotilaan. Komennossa on käskyn mukaisen heksadesimaaliarvon binääriesityksen lisäksi komennettavan tunnisteen NFCID0 arvo. Vastauksena saatava SLPB_RES on tavu nollia./5/

3.4.3 NFC-F

Modulaatiomenetelminä molempiin suuntiin F-tekniikassa on ASK ja koodauksena Manchester. Bitin aikaväli on jaettu kahteen osaan ja muutos tapahtuu sen keskellä kuvan 9 mukaisesti. Kuvassa näkyvä pattern E on looginen 1-tila ja pattern D looginen 0-tila.

Synkronointi suoritetaan aina komentojen välissä tai signaalin alussa. Se tapahtuu siten, että kantoaaltomodulaatio katkaistaan määrätyksi ajaksi, jonka jälkeen lähetetään 48 nollabittiä, muodostaen näin SoS:n. Tämän jälkeen lähetetään SoF, joka on F-tekniikassa määrätty esitettävän heksadesimaaliarvon B24Dh esityksenä. EoF signaaliksi tulkitaan yhden bittijakson mittainen moduloimaton signaali./5/



Kuva 9: NFC-F-signaalia./5/

Kehysrakenteeltaan signaali on yksinkertaista. Kehyksessä ei ole aloitus-, lopetus-, tai pariteettibittejä. Pelkästään SoF, jota seuraa hyötykuorma. Hyötykuorma koostuu SoD-kentästä, datasta ja EoD:stä. SoD on tavun mittainen ja ilmoittaa hyötyosan pituuden lisättynä yhdellä. EoD on jälleen kaksitavuinen tarkistussumma, sen laskemiseen käytetään varsinaisen datan lisäksi SoD-kenttää./5/

Komentoja NFC-C:ssä on kaksi, SENSF_REQ ja sen vastaus SENSF_RES. Käskyissä kuljetetaan kaikki mahdollinen tieto asetuksista ja tiedoista, kuten aikajakopaikka ja NFCID2, normaalidataan./5/

3.5 Half-Duplex-käytäntö

Kaikki NFC laitteet käyttävät tiedonsiirrossa Half-Duplex-menetelmää, eli laitteet lähettävät tietoa vuorotellen, eivät samaan aikaan. Tapa vaatii laitteilta selkeää menettelyä.

Kun tunniste on valmiustilassa, sen on odotettava kehystä lukijalta. Saatuaan kehyksen se lähettää vastauksensa ja siirtyy takaisin kuuntelutilaan. Lukijan on taas odotettava

vastausta tunnisteelta, ennen kuin se voi lähettää lisää kehyksiä. Jos tunnisteelta ei tule kehystä määrättyyn aikaan mennessä, yhteys katkeaa aikakatkaisuun./5/

3.6 Tagityypit

Tunnisteiden muistin tarkkaa sisäistä rakennetta, kuten vain-luku-tyyppisten tai muuten kiinteiden muistisolutyyppien paikkoja ja määrää ei käsitellä, mutta muistin sisältöön viitataan yleisen käytännön mukaisesti tiedossa olevilla heksadesimaaliosoitteilla. Tieto muistin koosta sijaitsee määrätyssä paikassa tagin ensimmäisten tavujen joukossa, samoin kuin tieto siitä voidaanko sitä sekä lukea että kirjoittaa vai vain lukea. Alkutavujen joukossa on myös binäärimuotoinen tieto tagin tyypistä.

Muistin pienin käsiteltävissä oleva yksikkö on käytännössä tavu. Tavusta seuraava yksikkö on blokki (tai lohko), joka on kahdeksan tavua. Isoin yksikkö, segmentti, on 16 blokkia eli 128 tavua. Muistialueesta voidaan kutsua tiettyä tavua tietyssä blokissa. Muistia käsitellään hieman eri komennoilla riippuen kyseessä olevasta tunnisteen tyypistä. Komennot sisältävät vähintään käsiteltävän muistisolun osoitteen. Tunnisteen ohjainpiiri tietää heksadesimaalista binäärimuotoon muutetun muistiosoitteen sijainnin.

Tunnisteeseen tallennettu tieto on aina NDEF-tiedostoformaatin mukaista. NDEF on suhteellisen yksinkertainen dataformaatti, jossa varsinaisen hyötykuorman rajoja merkitään eri lipuilla. Liputus MB (Message Begin) tarkoittaa datan alkua ja ME (Message End) loppua. Muilla lipuilla voidaan myös kertoa esimerkiksi hyötykuorman pituus ja määrittää jonkinlainen tietosisällön tyyppi. /6/

3.6.1 Tagityyppi yksi

Uudelleenkirjoitusta kestävät ykköstyypin tunnisteet ovat ISO/IEC 14443A-yhteensopivia ja niissä on muistia 96 tavusta kahteen kilotavuun. Kirjoitussuojaus voidaan kytkeä haluttaessa päälle. Käytettävä signalointi on NFC-A-tekniikan mukaista, kehys- ja synkronointimuotoineen kaikkineen./7/

Tunnisteen sisällön käsittelyyn käytetään kahdeksaa komentoa vastauksineen. Luettelo komennoista on kuvassa 10.

KOMENTO
RID
RSEG
READ
READ8
RALL
WRITE-E
WRITE-NE
WRITE-E8
WRITE-NE8

Kuva 10: Kaikki tagityypin yksi komennot.

RID-komennolla tiedustellaan tunnisteen yksilökohtaista tunnistenumeroa ja muita arvoja kuten tunnisteen kokoa ja tilaa. Käskyllä READ voidaan lukea yksittäinen tavu ja RALL lukee määritetyn osoitevälin. READ8 lukee blokin määrätystä osoitteesta alkaen ja RSEG koko segmentin. /7/

Kirjoituskomennoista WRITE-E on tavallisin ja se tyhjentää muistialueen ennen sille kirjoitusta. WRITE-NE on muuten sama, mutta se ei tyhjennä muistia ensin. Sitä käytetään lähinnä jos muistisolun tila halutaan esimerkiksi muuttaa lukituksi (lukittuun ei siis voi kirjoittaa) tai jos tiedetään muistin olevan jo tyhjä. Se on selvästi tavallista WRITE-E komentoa nopeampi. WRITE-N8 ja WRITE-NE8 ovat edellisten komentojen variantteja, joilla voidaan kirjoittaa koko blokki kerralla. /7/

3.6.2 Tagityyppi kaksi

Tyypin kaksi tunniste käyttää niin ikään NFC-A-signalointia sekä kehysmuotoa ja on myös kirjoitussuojattavissa. Komennot lähetetään normaalikehyksiä käyttäen, mutta paluuviesteissä käytetään lyhyitä kehyksiä. Komentoja on kolme ja vastauksia neljä.

KOMENTO	VASTAUS	VAST.KEHYSTYYPPI
READ	READ, NACK	Normaali, Lyhyt
WRITE	ACK,NACK	Lyhyt
SECTOR_SELECT	ACK,NACK	Lyhyt

Kuva 11: Tagityypin kaksi komennot.

Komennoista READ on normaali lukukomento, johon vastauksena saadaan kuusitoista tavua dataa komennossa määritetystä sijainnista. Jos luku ei onnistu, vastaus on NACK. Kirjoituskomentoa WRITE käyttäen voidaan kirjoittaa kolmesta kuuteen tavua tietoa määrättyyn muistiin. Vastauksena saadaan toiminnon onnistuessa ACK, muulloin NACK. Sektorinvalintakäsky SECTOR_SELECT voidaan implementoida tageihin, joissa on yli kilotavu muistia. Komennolla valitaan missä kilotavun alueessa, eli sektorissa, liikutaan. Vastaus sektorin vaihdon onnistumisesta joko positiivinen ACK tai negatiivinen NACK. /8/

3.6.3 Tagityyppi kolme

Japanilaisen FeliCa-standardin mukaisissa kolmannen tyypin tageissa käytetään NCF-F-signalointia. Tunniste valmistetaan joko myös kirjoitettavaksi tai vain luettavaksi, eikä tähän voi myöhemmin vaikuttaa. Siirtonopeus on aiempia tyyppejä nopeampi ollen 212 tai 424 kilotavua sekunnissa. Tyyppi yksi ja kaksi ovat nopeudeltaan siis vain 106 kbit/s. Muistin maksimimääränä pidetään maksimissaan yhtä megatavua.

Komentoja on kolme, ne ovat POLLING, UPDATE ja CHECK, ja niillä on lisäksi saman nimiset vastauskomennot. POLLING suorittaa kantoalueella olevien tunnisteiden tietojen kyselyn, sekä alustuksen. Siirrettävää tietoa siinä on esimerkiksi IDm tunnistenumero. CHECK-komennolla luetaan tietoja, mutta myös tarkistetaan POLLING-tiedot kuten lohkojen määrä ja tunnisteen kirjoitussuojauksen tila. UPDATE on kirjoituskomento. Kaikkien komentojen sisäinen rakenne on ykkös- ja kakkostyypin tunnisteita paljon monimutkaisempi. /9/

3.6.4 Tagityyppi 4A ja 4B

Tyyppi 4A käyttää NFC-A-tekniikan mukaista signaalirakennetta. Komentoja on käytössä neljä vastauksineen. Yhteyden alustukseen ja arvojen, kuten kehyksen maksimipituuden, kehysten välisen tauon ja käytettävän tiedonsiirtonopeuden valinta suoritetaan komennolla RATS. Komennolla UpdateBinary kirjoitetaan ja ReadBinaryllä luetaan muistia./10/

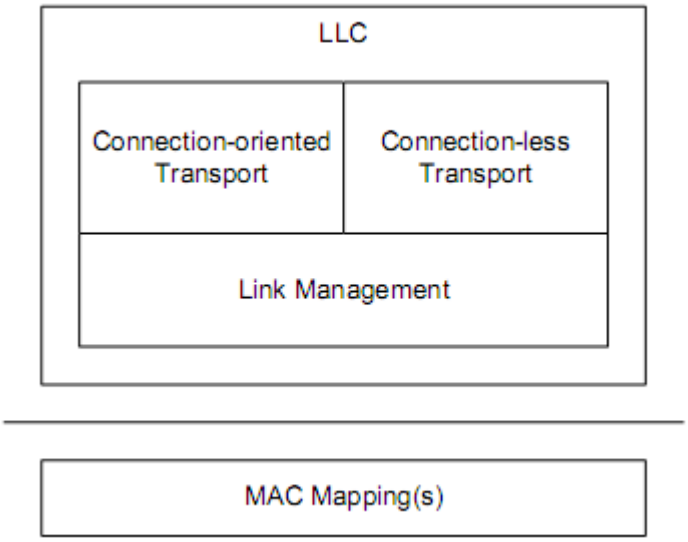
4B-tagit toimivat muuten samalla tavalla, mutta signalointi on NFC-B:n mukaista ja RATS:n sijasta käytetään hieman siitä eroavaa komentoa ATTRIB. Molemmissa nelostyypin tunnisteissa voi lisäksi toimia samaan aikaan useampi palvelu, jotka kaikki

käyttävät omia maksimissaan 32 kilotavun muistialueitaan. Tagit rakennetaan joko luku- ja kirjoitusvalmiiksi tai vain lukuvalmiuteen. /10/

3.7 LLCP-protokolla

Yksi NFC-Forumin julkaisemista protokollista on LLCP - Logical Link Control Protocol. Sen tehtäviin kuuluu linkin käynnistys, hallinta ja valvonta. Lisäksi se tarjoaa keinot virheiden havaitsemiseen ja niistä toipumiseen. OSI-referenssimallissa se sijoittuu siirtoyhteyskerroksen kahteen ylempään kolmannekseen. Käytännössä se on NFC:n matalimman tason protokolla. Sen alapuolella protokollapinossa on vain fyysinen rajapinta. /11/

Itse protokolla on jaettavissa neljään osaan, jotka huolehtivat eri tehtävistä. Osat ovat MAC-osoitus, linkin hallinta, yhteydellinen tiedonsiirto ja yhteydetön tiedonsiirto.



Kuva 12: LLCP-protokollan osat. /11/

MAC-osoitus (MAC Mapping) osan tehtävä karkeasti on liittää fyysinen radiotaajuuskerros protokollapinoon. Yhteydellinen (Connection oriented) ja yhteydetön (Connection-less transport) tiedonsiirto-kerrokset ylläpitävät kaikkea tiedonsiirtoa ja ne huolehtivat yhteyden avauksesta ja sulkemisesta. /11/

Tiedonsiirron komponenteista vain toinen on pakollinen ja NFC-laitteet jaetaankin kolmeen luokkaan sen mukaan minkä komponentin ne sisältävät. Luokan yksi laitteissa on vain yhteydetön komponetti. Luokan kaksi laitteista löytyy yhteydellinen ja

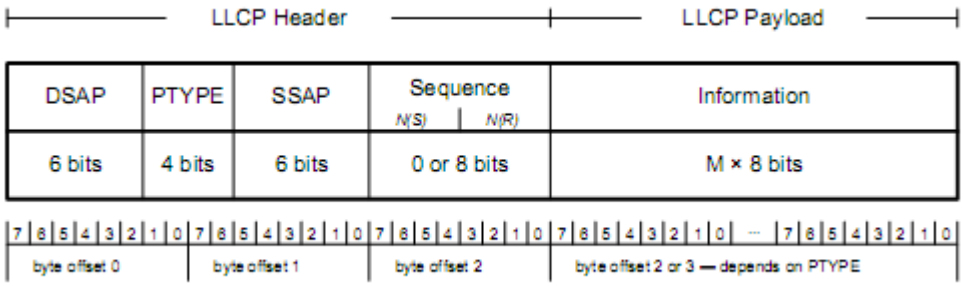
kolmannen luokan laitteista molemmat komponentit. Erona osilla on se, että yhteydetön komponentti ei sisällä virheenkorjausta eikä se takaa tiedon siirron onnistumista muuta kuin fyysisellä tasolla. Käytännössä se tarkoittaa sitä, että protokolla ei takaa tiedon sisällön oikeellisuutta eikä se takaa sen saapumista perille palvelun tasolle asti. Pakettien oikeina siirtyminen laitteiden LLC-kerrosten välillä on kuitenkin taattu johtuen alempana toimivan MAC-kerroksen ominaisuuksista. Yksinkertaistettu komponentti voi olla järkevä valinta jos korkeamman tason protokollat sisältävät jo virheenkorjauksen tai datan oikeellisuudella ei muuten ole niin väliä. Sisäisen virheenkorjauksen voidaan myös katsoa lisäävän tiedonsiirron nopeutta. Komponentista on karsittu myös yhteyden avauksessa ja lopetuksessa käytetty alustussignaali. Tämä pienentää yhteyden alustuksen viemää aikaa, joka voi joskus olla tarpeen vaikkakin se tapahtuu virhebittimäärän kustannuksella. /11/

Yhteydellinen vaihtoehto tarjoaa virheen havainnoinnin ja se varmentaa jokaisen paketin saapumisen perille asti. Kaikissa paketeissa on yksilölliset tunnisteet lähettäjästä ja vastaanottajasta, mutta sen lisäksi PDU-paketteihin lisätään tässä menetelmässä juokseva numero, jonka perusteella kyseisen datapaketin siirron onnistumista tarkkaillaan. Muodostettu yhteys on avoinna niin kauan kunnes sen katkaisua pyydetään tai se katkeaa jonkin häiriön vuoksi. /11/

Yhteydettömässä vaihtoehdossa pakettien numerointia ei siis ole, tunnisteet kylläkin. Tunnisteiden avulla voidaan erotella mihin mahdollisesti samaan aikaan yhteydessä oltavista laitteista tieto on menossa. Tietoturvan kannalta voidaan myös ajatella, että lähde- ja kohdetiedot ovat olemassa sen vuoksi, ettei dataa voida (niin helposti) kaapata.

Viimeisenä komponenttina oleva linkin hallinta pakkaa ja purkaa PDU-datakehyksiä. Se siis lisää ja tulkitsee datapakettien lähetystiedot ja muut LLC-protokollan mukaiset kehystiedot. Jos kehystiedoissa on virhe, se pyytää uudelleenlähetystä./11/

3.7.1 LLC kehysrakenne



Kuva 13: LLCP-kehyksen rakenne. /11/

Kehys koostuu neljästä kentästä ja hyötykuormasta. Yhteensä sen pituus on 32 bittiä. Hyötykuormaa siitä on vain neljännes. DSAP- ja SSAP-kentät kertovat osoitteet. DSAP on lyhenne sanoista Destination service access point, eli se sisältää vastaanottavan palvelun osoitteen. SSAP on puolestaan Source service access point, eli lähteen osoite. Sequence-kenttä ei ole käytössä yhteydetöntä protokollakomponenttia käytettäessä, sillä se sisältää virheiden tunnistuksessa ja korjauksessa käytetyn pakettinumeroinnin. Viimeisenä kenttänä kehyksessä on PTYPE. /11/

Kaikki kehykset eivät sisällä varsinaista hyötykuormaa, vaan ne voivat kuljettaa pelkästään yhteyden ylläpitoon tai hallintaan liittyvää tietoa. Tämän vuoksi PTYPE-kentässä määritellään kehyksen tyyppi, josta selviää sen tarkoitus. Nelibittisessä PTYPE-kentässä siis kuljetetaan tietoa esimerkiksi yhteyden avauksesta ja sen sulkemisesta. Muita mahdollisia kehystyyppejä ovat mm. parametrinvaihtokehys PAX, vastaanottovalmiudesta kertova kehys RR, viallisesta kehyksestä kertova Frame Reject -kehys, symmetriakehys SYMM jne. Listan erikoisimpana kehystyyppinä voidaan pitää niin kutsuttua Aggregated Frame eli AGF-kehystä. Sen avulla voidaan lähettää useampi hyötykuorma peräkkäin samassa kehyksessä, kunhan ensin ilmoitetaan kehyksen olevan tulossa ja lähettävässä kehyksessä vielä sen pituus. Mahdollisesta kuudestatoista kehystyypin arvosta käytössä on tällä hetkellä kaksitoista. Loput ovat varattuna tulevaisuudessa mahdollisesti tarvittaville yhteydenhallinnan komennoille. Kaikki komennot eivät ole käytössä yhteydettömän tiedonsiirron komponenttia käytettäessä, mutta yhteydellinen tukee näistä kaikkia. Bittiarvoina ilmoitettuna kehystyypit asettuvat luonnollisesti välille 0000-1111. /11/

Molemmat osoitekentät ovat kuusibittisiä. Se tarkoittaa, että käytössä on 64 osoitetta. Kaikki osoitteet eivät kuitenkaan ole tarkoitettu paikallisesti määriteltäviksi, vaan osa

on varattu erilaisille kiinteille palvelukutsuille. Osoitteista ensimmäinen on varattu linkin hallintakomponentille ja toinen osoittaa palvelun kartoitukseen tarkoitettua SDP-protokollaa (Service Discovery Protocol). Osoitteet 2-15 ovat puolestaan varattuna NFC-Forumin määrittämille palvelukutsuille. Tästä ylöspäin olevat osoitteet osoitteeseen 31 asti ovat paikallisille LLC-palveluille määriteltävissä. Loput osoitteet on jälleen varattu, tällä kertaa LLC:tä korkeammalla olevien kerrosten palvelukutsuille. Ne eivät tarkoituksellisesti näy SDP:n ylläpitämässä palvelulistauksessa. Osoitteista käytetään heksadesimaalimuotoa ja ne löytyvät väliltä 00h – 3Fh (0-63). Lähde ja kohdeosoitteet ovat samanmuotoisia ja käyvät näin ollen molempiin kenttiin. /11/

Jos käytössä on sekvenssikenttä, se on kahdeksanbittinen ja se on jaettu kahteen osaan. Ensimmäiset neljä bittiä kertovat lähetettävän kehyksen numeron ja loput vastaanotettavan. Ensimmäisissä biteissä kulkee juuri lähetyksessä olevan kehyksen numero ja vastaanotettavassa numero, jonka vastaanottaja on viimeksi kuitannut perille saapuneeksi. Sekvenssikentällisiä kehyksiä on olemassa kolme: Information (I), sekä vastaanottovalmiudesta kertovat kehykset Receive Ready (RR) ja Receive Not Ready (RNR). Vastaanottaja kuittaa vastaanottamansa kehykset lähettämällä RR-kehyksen lähettäjälle, kertoen näin olevansa valmis uusien vastaanottoon. Jos vastaanottaja ei mahdollisesti epäonnistuneesta siirrosta tai muusta syystä ole valmis uusien kehysten vastaanottoon, se lähettää RNR-kehyksen, jossa se ilmoittaa viimeksi saamansa PDU:n numeron. Sekvenssikehyksistä I-kehykset voivat olla informaatiokentättömiä, muiden on oltava informaatiokehyksettömiä. /11/

3.7.2 Linkin avaus

Tiettyjä kehyksiä on tarve lähettää yhteyttä toiseen laitteeseen muodostettaessa. Itse yhteyden muodostus laitteiden välillä alkaa, kun paikallinen MAC ilmoittaa LLC:lle protokollan kanssa yhteensopivan laitteen tulosta yhteysetäisyydelle ja kun MAC itse on onnistuneesti suorittanut oman tehtävänsä yhteyden muodostuksessa. /11/

Jos MAC-linkin muodostuksessa on määritelty LLC-linkin asetuksien määrittäminen tapahtuvaksi jo tässä vaiheessa, MAC-kerros vaihtaa omia kehyksiään käyttäen tiedot linkin asetuksista. Mikäli MAC-linkkiä muodostettaessa ei vielä ole vaihdettu yhteysparametrejä, tämä tapahtuu vasta MAC yhteyden muodostuttua

parametrinsiirtokehysten PAX avulla. Parametrien vaihto tapahtuu yhteyden muodostuksen aikana vain kerran, joten se ei voi tapahtua molemmissa vaiheissa. /11/ Yhteyden muodostuksessa ei ole välttämätöntä käyttää PAX-kehyksen lisäarvoja, eli voidaan käyttää pelkästään kehyksen version kenttää. Ainoa pakollinen yhteyden avauksessa siirrettävä tieto on siis juuri protokollan versionumero, sillä se siirtyy PAX-kehyksessä, vaikka siihen ei olisi määritetty mitään muita parametrejä. Tietojen vaihto protokollan versiosta on ymmärrettävää, sillä ilman versioinformaatiota linkki voisi versioiden välisten erojen, esimerkiksi parametriarvoissa, vuoksi toimia vähintään huonosti tai olla jopa täysin käyttökelvoton. Vaikka PAX:n pakollisena tehtävänä on siis ainoastaan ilmoittaa LLC:n versionumero, voidaan sen avulla neuvotella muitakin ominaisuuksia kuten aikakatkaisun kesto, tietopaketin suurin mahdollinen pituus ja paljon muuta. Parametrinvaihtokehys on rakenteeltaan samanlainen kuin normaali PDU, eli se sisältää vastaanottajan ja lähettäjän osoitteen, kehystyyppikentän sekä informaatiokentän. Sekvenssikenttää ei ole, jotta kehys olisi yhteensopiva molempien mahdollisten tiedonsiirron komponenttien kanssa. Parametrien siirto tapahtuu informaatiokentässä./11/

MAC-kerroksen osalta toiminnot yhteyden muodostuksessa riippuvat laitteen roolista. Havaittuaan toisen laitteen toimintaetäisyydellä, aloittava laite lähettää kohdelaitteelle Attribute Request –komennon (ATR_REQ). Komento sisältää kolmen oktetin kiinteän NFC:n tunnistenumerosarjan 46h 66h 6Dh, jonka avulla yhteensopivuus ISO 18092-standardin kanssa tarkistetaan. Jos sama numerosarja löytyy kohdelaitteesta, laite lähettää aloittajalle Attribute Response –komennon (ATR_RES), joka myös sisältää samat numerot. Mahdolliset yhteysasetusparametrit siirretään myös tässä vaiheessa kehysten informaatiokentän loppuosassa. Tämän jälkeen MAC siirtyy normaaliin toimintaan ja ilmoittaa LLC:lle muodostaneensa yhteyden. Mikäli numerosarjat eivät vastaa toisiaan laitteet eivät ole yhteensopivia keskenään ja yhteyden muodostus katkeaa. /11/

LLC-protokolla ei vaadi ISO 18092:n mukaisen MAC-kerroksen käyttöä, mutta käytettävän kerroksen on pystyttävä siirtämään kaikkia protokollan mukaisia kehystyyppejä laitteiden LLC-kerrosten välillä sekvensoidusti ja tarjottava oma kehysrakenteensa kehysten pakkaamisineen ja purkamisineen. Lisäksi sen on kyettävä

havaitsemaan ja korjaamaan siirtovirheensä ennen kehyksen siirtoa LLC:lle tai ilmoittamaan jos virhe on korjaamattomissa. /11/

3.7.3 Normaali toiminta ja yhteyden katkaiseminen

Yhteydessä olevat laitteet voivat siirtää välillään kaikkia kehystyyppejä. MAC pakkaa LLC kehykset kehyksiensä DEP_REQ (Data Exchange Protocol Request) ja DEP_RES (Data Exchance Protocol Response) avulla riippuen tiedon kulun suunnasta. Kaikkien ISO 18092 -standardin mukaisen MAC-kehysten tarkka rakenne on määrätty standardissa. Kun koko LLC paketti on saatu siirrettyä virheettömästi, MAC purkaa oman kehysrakenteensa ja siirtää tietopaketin ylöspäin protokollapinossa. Samalla se ilmoittaa paketin pituuden oktetteina. Jos data on jouduttu jakamaan useampaan MAC-kehykseen, sen on ensin koottava se takaisin yhdeksi ennen siirtoa ylöspäin. /11/

Yhteyden katkaiseminen alkaa aloittavan laitteen LLC-kerroksen pyynnöstä tai jos yhteyden ylläpitäminen on muuttunut mahdottomaksi virhemäärän vuoksi. Muiden kehysten siirto katkeaa kun kohde vastaanottaa komennon DSP_REQ (Deselect Request), johon se vastaa omalla käskyllään DSP_RES (Deselect Response) ennen irroittautumistaan linkistä. Jos aloittavan laitteen muodostama radiokenttä katkeaa, vastaanottaja ilmoittaa protokollalleen MAC-yhteyden katkenneen. LLC:n osalta komentokehys yhteyden katkaisuun on DISC (disconnect), ja sen onnistumisesta kertoo DM (disconnected mode). Näistä DISC koostuu pelkästä osoitekentistä ja tyyppikentästä. DM sisältää lisäksi yksi oktettisen informaatiokentän, jossa voidaan ilmaista katkaisun syy. /11/

4 YHTEENVETO

NFC-tekniikkaa kohtaan on asetettu kasvavia odotuksia niin markkinoiden kuin uusien sovellustenkin kannalta. Aika näyttää mitkä odotuksista toteutuvat, mutta tekniikan ei työn perusteella luulisi juuri esteitä asettavan uusien sovelluksien tielle. Valmiiksi nykyisten älykorttiratkaisuiden kanssa yhteensopivat lukulaitteet tarvitsevat yleistyäkseen kuitenkin laitevalmistajien tukea. Matkapuhelinvalmistajista ainakin Nokia on jo luvannut sisällyttää NFC-piirin jokaiseen älypuhelinmalliinsa vuodesta 2011 alkaen. Samansuuntaisia sävyjä on ollut kuultavissa myös Samsungin matkapuhelinleiristä. Painettavalla elektroniikallakin tehdyt edulliset tunnisteet, esimerkiksi laskun maksamiseen, voisivat kuitenkin olla täysin toteutettavissa NFC:llä.

Vaikka tekniikka itse alkaa olla hyvinkin valmis, se ei ole vielä kovinkaan vanhaa ja puutteitakin siinä on. Esimerkiksi digitaalista rajapintaa, kuten modulaation käyttöä digitaalisen informaation siirtoon, käsittelevä dokumentaatio on alun perin päivätty joulukuulle 2009 ja viimeksi sitä on päivitetty marraskuussa 2010. Tämän lisäksi signaalin analogiaa, kuten jännitearvoja, käsittelevä spesifikaatio on vielä julkaisematta. Päivityksiä on ilmestynyt myös tagityyppien spesifikaatioihin, vaikka näiden pitäisi olla pitkälti samoja kuin RFID:ssä.

Protokollan ja tiedon kehysrakenteen osalta ei pitäisi olla mitään epäselvyyksiä, vaan kaikki näyttäisi olevan hyvin toimivan oloista tältä osin.

LÄHDELUETTELO

Sähköiset

1. Requirements of ISO/IEC 14443 Type B Proximity Contactless Identification Cards [online][viitattu 8.11.2010] Saatavissa: http://www.atmel.com/dyn/resources/prod_documents/doc2056.pdf

2. OULU NFC-WEEK 2009 [online] [viitattu 12.11.2010] Saatavissa: http://www.nfcoulu.com/aboutNFC.html

3. Bluetooth.com, Core Specification Version 4.0 [online] [viitattu 12.11.2010] Saatavissa: http://www.bluetooth.com/English/Technology/Works/Pages/Bluetooth_low_energy_technology.aspx

4. NFC-FORUM [online] [viitattu 15.11.2010] Saatavissa: http://www.nfc-forum.org

5. NFC-FORUM, NFC Digital Protocol Technical Specification [online] [viitattu 15.11.2010] Saatavissa: http://www.nfc-forum.org/specs/spec_license

6. NFC-FORUM, NFC Data Exchange Format (NDEF) Technical Specification [online][viitattu 15.11.2010] Saatavissa: http://www.nfc-forum.org/specs/spec_license

7. NFC-FORUM , NFC Forum Type 1 Tag Operation Specification [online] [viitattu 1.12.2010] Saatavissa: http://www.nfc-forum.org/specs/spec_license

8. NFC-FORUM , NFC Forum Type 2 Tag Operation Specification [online] [viitattu 1.12.2010] Saatavissa: http://www.nfc-forum.org/specs/spec_license

9. NFC-FORUM , NFC Forum Type 3 Tag Operation Specification [online] [viitattu 1.12.2010] Saatavissa: http://www.nfc-forum.org/specs/spec_license

10. NFC-FORUM , NFC Forum Type 4 Tag Operation Specification [online] [viitattu 1.12.2010] Saatavissa: http://www.nfc-forum.org/specs/spec_license

11. NFC-FORUM , Logical Link Control Protocol Technical Specification [online] [viitattu 5.12.2010] Saatavissa: http://www.nfc-forum.org/specs/spec_license

12. Wikimedia Commons, EPC-RFID-TAG.jpg [online] [viitattu 18.11.2010] Saatavissa: http://commons.wikimedia.org/wiki/File:EPC-RFID-TAG.jpg?uselang=fi