TAMPEREEN
AMMATTIKORKEAKOULU

NEAR FIELD COMMUNICATION

Juha Honkakorpi

Opinnäytetyö
Marraskuu 2015
Tietotekniikka
Sulautetut järjestelmät ja elektroniikka

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietotekniikka
Sulautetut järjestelmät ja elektroniikka

Honkakorpi, Juha:
Near field communication

Opinnäytetyö 28 sivua
Marraskuu 2015

Tässä työssä perehdyttiin NFC-tekniikaan standardien, komponentti- ja laitevalmistajien sekä tutkijoiden laatimien julkaisujen kautta. NFC on lyhenne sanoista near field communication. Se tarkoittaa lyhyen etäisyyden yhteyttä eli tiedonsiirtoa, mikä tapahtuu esimerkiksi matkakorttia käytettäessä lukijan päällä tai kannettavan kaiuttimen ja puhelimen NFC-parituksessa. Pohjimmiltaan NFC- ja RFID-tekniikka ovat samankaltaisia, koska ne perustuvat osittain samoihin standardeihin.

Työssä selvitetään aiheeseen liittyvien standardien merkitys ja tuodaan esille eri valmistajien yhteensopivuusongelmia ja -mahdollisuuksia. Tuoteluokat ja tuotetyyppien ominaisuuksia esitellään yleisellä tasolla vertailevasti. Työssä käsitellään laitteiden eri muodot toiminta- ja yhteystapoineen sekä perehdyttiin signaali- ja viestimuo-toihin.Työssä esitellään siirtyvän datan kehysrakenteita. Koska kyseessä on langaton tiedonsiirtomenetelmä, tutustutaan myös tietoturvauhkiin.

Asiasanat: nfc, lyhyen matkan yhteys, rfid, nfc-tunniste

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree programme in Information Technology
Option of Embedded Systems and Electronics

Honkakorpi, Juha:
Near Field Communication

Bachelor's thesis 28 pages
November 2015

The purpose of this thesis was to collect and open the information about the technology of NFC. The used sources were mostly standards but manufacturers and specialists writings were too taken into account. The abbreviation NFC points to near field communication, in other words, a short range communication which is used e.g. within travel cards at NFC touch points or mobile Bluetooth speaker with NFC enabled pairing. The roots of NFC-technology are based in RFID that shares partly the same standardization and frequencies.

In this thesis there is a light walkthrough concerning standards and its purposes but also the different manufacturers compatibility problems and possibilities. The product types and the features were brought up contrastively in the basic level. The connection methods and operating models are shown with some data structures and modulation schemes. Some of the security issues have been noted too.

Key words: nfc, near field communication, rfid, nfc-tag

SISÄLLYS

1 JOHDANTO 6
2 NFC-tekniikka 7
2.1 Standardit 7
2.2 Toimintamoodit 8
2.2.1 Passiivinen 8
2.2.2 Aktiivinen 9
2.3 Yhteystavat 11
2.3.1 Korttiemulaatio 11
2.3.2 P2P 12
2.3.3 Luku- tai kirjoitustila 12
2.4 Signaalitekniikat 12
2.4.1 NFC-A 13
2.4.2 NFC-B 13
2.4.3 NFC-F 14
2.5 NFC-laitteet 14
2.6 NFC-tag 15
2.6.1 Tunnistetyyppi 1 16
2.6.2 Tunnistetyyppi 2 16
2.6.3 Tunnistetyyppi 3 16
2.6.4 Tunnistetyyppi 4 17
2.7 RTD-tiedosto 18
2.8 NDEF 19
2.9 LLCP 22
3 TIETOTURVAUHKAT 23
3.1 Urkinta 23
3.2 Datakorruptio ja -modifiointi 23
3.3 Datan lisäys 24
3.4 Man-in-the-middle 25
3.5 Haitalliset tunnisteet ja ohjelmat 25
4 POHDINTA 27
LÄHTEET 28

ERITYISSANASTO

NFC	Near Field Communication, lyhyen matkan tiedonsiirto
HF	High-frequency, suurtaajuus (13,56 MHz)
RFID	Radio frequency identification, radiotaajuustunnistus
FeliCa	Felicity Card, Sonyn standardin mukainen älykortti
RTD	Record type definition, tallennetyypin määritelmä
NDEF	NFC data exchange format, NFC-dataformaatti
ASK	Amplitude shift keying, amplitudiavainnus
ATR_REQ	Attribute request, yhteydenmäärittelypyyntö
ATR_RES	Attribute response, yhteydenmäärittelyvastaus
PSL_REQ	Parameter selection request, parametrinvalintapyyntö
DEP_REQ	Date exchange protocol request, datanvaihtoprotokollan pyyntö
PDA	Personal digital assistant, kämmentietokone
P2P	Peer-to-peer, kahden lukijalaitteen välinen yhteys
LLCP	Logical Link Control Protocol, P2P-yhteysprotokolla
URI	Uniform Resource Identifier, resurssin nimi tai paikkatieto
PDU	Protocol Data Unit, pakettimuoto OSI-kerroksien välillä
OSI-malli	Open System Interconnection, tiedonsiirtoprotokollamalli
AND-piiri	Looginen AND/JA, logiikkapiiri joka suorittaa kertolaskun sisääntulojen kesken
oktetti	tavu, kahdeksan bitin ryhmä
SSD	Single Device Detection, pollaukseen liittyvä laitteen valintaan liittyvä algoritmi

1 JOHDANTO

Tämä insinöörityö käsittelee NFC-tekniikan perusteita. Työssä käsitellään enimmäkseen NFC-Forumin mukaisia menetelmiä ja määritelmiä. NFC-tekniikalla tarkoitetaan lyhyen matkan tiedonsiirtomenetelmää, jonka yhteys muodostetaan sähkömagneettisesti kahden NFC-standardin mukaisen laitteen välille. NFC on kuluttajille suunnattu ja muunneltu tekniikka RFID-tekniikan hyötyjä käyttäen. Tiedonsiirtonopeus ei ole kovinkaan suuri, mutta hyöty saadaan kuitenkin nopeasta laiteparituksesta, jonka jälkeen tiedonsiirto voidaan suorittaa nopeammalla menetelmällä. Esimerkkinä Bluetooth-kaiutin, jossa normaalin Bluetooth-käytännön helpotuksena parittamiseen voidaan käyttää sisäänrakennettua NFC-tekniikkaa. Sen lyhyen toimintasäteen ja salatun lähetyksen ansiosta käyttö vaikkapa mobiilimaksamisessa on lähes turvallista.

Tekniikkaa kehittämään muodostettu voittoa tavoittelematon NFC-Forum perustettiin toukokuussa vuonna 2004. Perustajina olivat Nokia, Philips ja Sony, ja forumiin kuuluu tällä hetkellä yli 180 jäsenyritystä. NFC-Forum tuo tekniikan lähemmäksi harrastelijoita ja muita kiinnostuneita standardisoimalla valmiita rakenteita yhteensopivuuden ylläpitämiseksi. NFC-Forumin tarkoituksena yleisesti on NFC-tekniikan kehittäminen tietoturvan, helppokäyttöisyyden ja tunnettavuuden suhteen. Perustamisen jälkeen vuonna 2006 NFC-Forum julkaisi ensimmäiset määritelmänsä NFC-tunnisteille. Samana vuonna sai määrityksensä myös Smart Poster, mikä voisi sisältää kaikenlaista osoittamastaan kohteesta. Tähän pieneen tarraan voidaan sisällyttää julisteesta tai opasteesta luettava tieto, sekä enemmän tietoa antava verkkosivuston osoite, mikä älypuhelimen tai muun mobiililaitteen ruudulta on helppo lukea.
(http://nfc-forum.org/about-us/join-the-forum/membership-overview/)

Historian ensimmäinen NFC-yhteensopiva puhelin oli Nokian 6131, mikä julkaistiin vuonna 2006. Teknologian kasvettua ja yleistyttyä vuonna 2010 Samsung julkaisi ensimmäisen NFC-puhelimensa Android-pohjaisen Samsun Nexus S:n. Tällä hetkellä NFC-yhteensopivia puhelimia/tabletteja on markkinoilla yli 330 eri mallia.
(http://www.nearfieldcommunication.org/smartphone-development.html)

2 NFC-tekniikka

2.1 Standardit

Lyhyen matkan yhteyksien laitteita ja teknologiaa kehitettäessä NFC-standardit on täytettävä. Standardien tarkoituksena on kaikkien "lyhyen matkan yhteyden" laitteiden yhteensopivuuden takaaminen ja sen, että uudet laitteet ovat yhteensopivia edeltäjiensä kanssa. ISO/IEC 14443 ja ISO/IEC 18000-3 ovat kaksi laajempaa standardia NFC-tekniikassa. Nämä ovat yleisiä lyhyen matkan langattoman tiedonsiirron standardeja. ISO/IEC 14443 määrittää henkilökorttien ja tunnisteiden sisältämän tietomuodon. ISO/IEC 18000-3 on kansainvälinen standardi kaikille langattomille HF-taajuusaluetta käyttäville laitteille, jotka käyttävät A- ja B-tyypin tunnisteita. Määrityksenä on mm. 4 cm maksimietäisyys, jolloin laitteet voivat lähettää dataa, sekä kuinka lukulaitteen ja luettavan laitteen on kommunikoitava keskenään.
(http://www.nearfieldcommunication.org/technology.html)

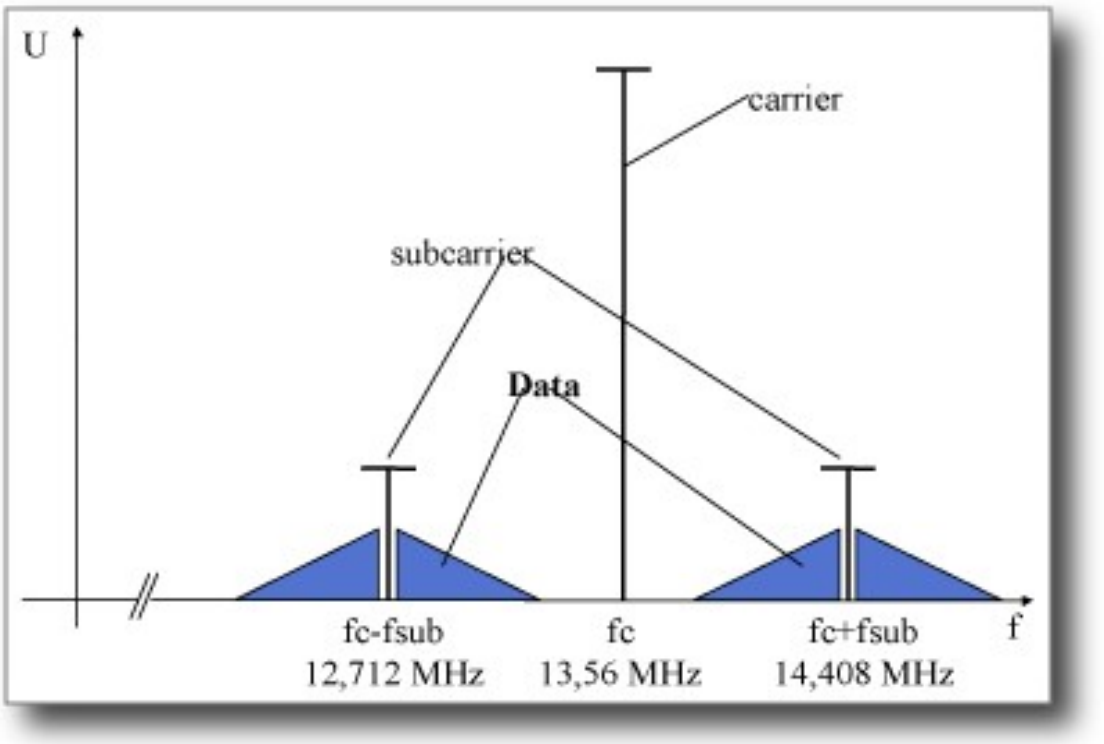
Kolmas standardi on ISO/IEC 18092 (ECMA-340), joka määrittää rajapinnan ja protokollan (NFCIP-1) kahden langattoman lähekkäin olevan laitteen väliseen tiedonsiirtoon. Se määrittää aktiivi- ja passiivilaitteen väliset tiedonsiirtotavat, modulointikaaviot, koodaukset, siirtonopeudet, RF-rajapinnan kehysmuodon, alustuskaaviot ja ehdot datan päällekkäin lähettämisen välttämiselle. Tiedonsiirto-nopeudet ovat joko 106, 212 tai 424 kbps. Oman standardinsa luonut Sony noudattaa japanilaista teollisuusstandardia (JIS) X 6319-4. Tässä määritellään Sonyn FeliCa-tuotepiiriin kuuluvien laitteistojen toimintaperiaatteet ja vaatimukset. FeliCan lukijalaitteista jotkin ovat kuitenkin yhteensopivia NFC-Forumin A-tyypin tunnisteiden kanssa.
(http://www.ecma-international.org/publications/files/ECMA-ST/Ecma-340.pdf)

2.2 Toimintamoodit

Toimintamoodi valikoituu yhteyden ensiaskelilla. Suurimman osan ajasta kaikki NFC-laitteet ovat kuuntelijoita, mutta jaksottain ne siirtyvät lukutilaan, jolloin ne "pollaavat" eli etsivät toimintasäteeltään kuuntelijalaitteita. Tämä on siis mahdollista vain aktiivilaitteille, jotka pystyvät muodostamaan oman sähkömagneettisen kenttänsä. "Pollauksen" jälkeen lukija siirtyy takaisin kuuntelijatilaan. Jos lukija löytää laitteen, yhteyden alustusprotokolla ja mahdollinen tiedonsiirto voi alkaa.
(http://www.nfc.cc/technology/nfc/)

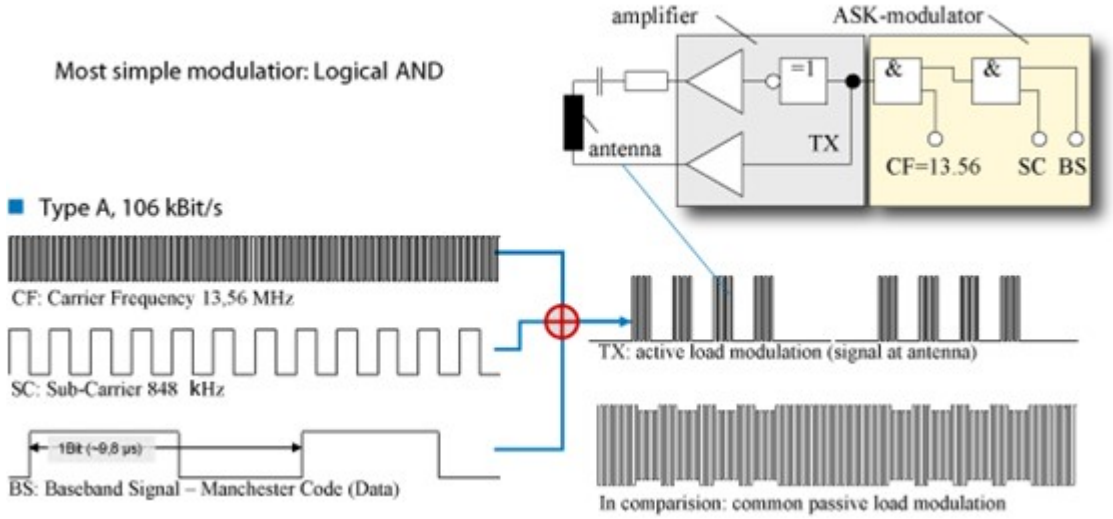
2.2.1 Passiivinen

Kun "pollauksen" tuloksena on löytynyt laite ja yhteysmuodoksi on valittu passiivinen, keskustelun aloittanut lukijalaite muodostaa 13,56 MHz kantoaaltoisen RF-kentän. Luettava laite ei muodosta omaa kenttäänsä, mutta voi ottaa käyttövirtansa lukijan kentästä. Kohdelaite lähettää datan moduloimalla apukantoaaltoja, jotka se luo 848 kHz:n päähän kantoaallosta. Siirrettävä data löytyy näiltä sivutaajuuksien kaistoilta (kuva 1). (http://rfid-handbook.de/about-rfid/active-load-modulation.html)



KUVA 1:Kantoaalto ja passiivimoodissa dataa sisältävät sivukantoaallot. (http://rfid-handbook.de/about-rfid/active-load-modulation.html)

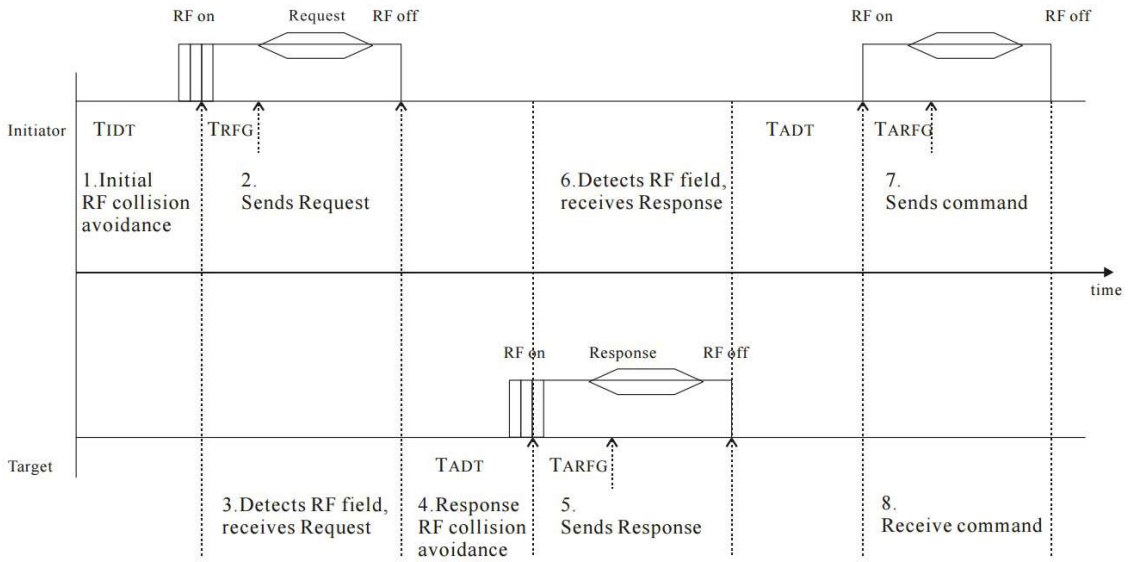
Alla oleva kuva näyttää RF-rajapinnan RFID-vastaanottimessa, mikä on toteutettu yksinkertaisella AND-piirillä ja sitä seuraavalla vahvistinpiirillä. Datan lähetykseen vaadittu signaali on binäärinen, joten piiri voidaan toteuttaa näin. Siinä kerrotaan keskenään Manchester-koodattu datasignaali ja sillä moduloitava sivukantoaalto. Muoto on ASK-modulaation kaltaista ja kelpaa näin lähetysmuodoksi. Tulos kerrotaan vielä kantoaallon kanssa toisella AND-piirillä, minkä lukijapiiri käsittelee datana (kuva 2).
(http://rfid-handbook.de/about-rfid/active-load-modulation.html)



KUVA 2: Looginen AND-piiri signaalin käsittelyssä (http://rfid-handbook.de/about-rfid/active-load-modulation.html)

2.2.2 Aktiivinen

Kun aktiivimoodi on valittu, molemmat keskustelijalaitteet muodostavat oman 13,56 MHz RF-kenttänsä ja lähettävät datansa ASK-moduloimalla sitä. Päällekkäisten lähetysten välttämiseksi laitteet vuorottelevat niin, että vain lähettävä laite muodostaa RF-kentän. Kuuntelevan laitteen RF- kenttä on kiinni, kunnes se on saanut datan, jonka jälkeen se alkaa taas lähettämään omassa kentässään. Hyötyjä passiiviseen yhteystapaan verrattuna ovat pidempi (noin 20 cm) kantama ja nopeampi tiedonsiirto jopa (1 MBit/s).
(http://www.nfc.cc/technology/nfc/)



KUVA 3: Aktiivitunnisteen ja lukijan vuoropuhelu alustuksessa.
(ECMA-340-standardi)

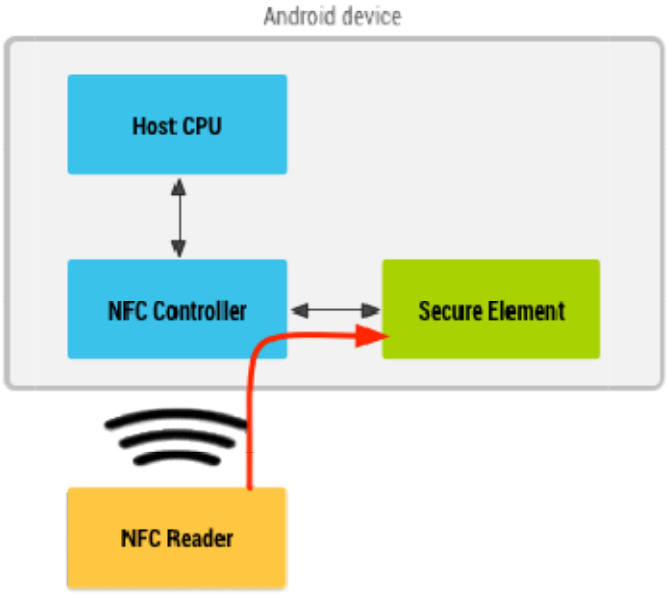
1. Lukija suorittaa standardin mukaisen päällekkäisen liikenteen haistelun.
2. Lukijan ensimmäinen käsky on ATR_REQ aktiivimoodissa ja valitulla siirtonopeudella, jonka jälkeen se sulkee RF-kenttänsä.
3. Tunniste havaitsee kentän ja saa datan.
4. Tunniste suorittaa standardin mukaisen törmäysvarotoimenpiteen.
5. Tunniste lähettää ATR_RES-viestin vastauksena lukijan ATR_REQ-viestiin. Samalla nopeudella, kuin vastaanotti ATR_REQ-viestin, ja sen jälkeen sulkee RF-kenttänsä.
6. Lukija havaitsee kentän ja saa datan.
7. Lukija suorittaa paketin törmäykseen liittyvät varotoimenpiteet.
8. Lukija lähettää PSL_REQ-viestin, jos parametreja halutaan muuttaa. Muutoin se lähettää DEP_REQ-viestin aloittaakseen tiedonvaihtoprotokollan mukaisen liikenteen.
(ECMA-340-standardi)

2.3 Yhteystavat

Yhteysmuodot jaetaan kolmeen eri kategoriaan: korttiemulaatio, P2P ja lukija/kirjoittaja. Yhteysmuoto vaikuttaa tiedonsiirtonopeuksiin ja yhteyden ominaisuuksiin. Käyttötarkoitukseen sopiva yhteystapa valikoituu aina yhteyden muodostavien laitteiden mukaan. Yhteystavat määräytyvät erilaisiksi esimerkiksi, kun matkakorttia käytetään päätelaitteella tai dataa siirretään kahden mobiililaitteen välillä. (http://www.nfc.cc/technology/nfc/)

2.3.1 Korttiemulaatio

Korttiemulaatiossa aktiivinen NFC-laite, kuten puhelin, muunnetaan passiivisen tunnisteen kaltaiseksi keskusteluraja-pinnaksi. Emulointi mahdollistaa saman NFC-laitteen toiminnan useana eri älykorttina. Kortti, mitä halutaan käyttää, voidaan valita puhelimen emulointiohjelmistossa. Tätä toimintamuotoa voidaan käyttää esimerkiksi lähimaksamisessa tai kertalipun ostossa. Lisäominaisuutena NFC-laitteessa voi olla tietoturvalohko "secure element", johon tallennetaan raha- tai henkilö-tietoliikenteeseen liittyviä arkaluontoisia tietoja. Tähän tallennettava tieto menee suoraan lähettäjältä, jonka jälkeen se on vasta hallitusti saatavilla puhelimen ohjelmistoille (kuva 4). (http://www.nfc.cc/technology/nfc/)



KUVA 4: Informaation kulku NFC-laitteessa missä on secure element -lohko (http://developer.android.com/guide/topics/connectivity/nfc/hce.html)

2.3.2 P2P

"Peer-to-peer" -yhteysmuoto vaatii kaksi NFC-kytkettyä laitetta ja vähintään toisen pitää olla aktiivitilassa. Oli toimintamoodi sitten aktiivi- tai passiivimoodi, niin keskustelun aloittava laite luo aina ensimmäisenä RF-kenttänsä. Kohdelaite sen sijaan käyttää omaa kenttäänsä vain aktiivimoodissa, vuorotellen aloitelaitteen kanssa. Standardi ISO 18092 mahdollistaa kahden NFC-laitteen kaksisuuntaisen liikenteen LLCP-protokollan avulla. Kontaktien vaihto, Bluetooth-paritustiedot tai muu datanvaihto onnistuu vaivattomasti ja ilman suurempaa verkkoasetusten konfigurointia. (http://www.nfc.cc/technology/nfc/)

2.3.3 Luku- tai kirjoitustila

Luku- tai kirjoitinlaitteena toimivaa NFC-järjestelmää voidaan käyttää esimerkiksi älykorttien lukuun tai kirjoituksen sallivien tunnisteiden muokkaukseen. Yhteyden muodostuksessa laite etsii (pollaa) ympäristöstä kortteja. Jos kortteja on kaksi tai useampi, laite valitsee niistä yhden kerrallaan käyttäen SSD-algoritmia "Single Device Detection". Kaikkeen liikenteeseen liittyy aina ensimmäisenä päällekkäisviestinnän estävä algoritmi, jolla pyritään estämään hukkaliikenne. Tässä käytössä on half-duplex-liikenne. (http://www.nfc.cc/technology/nfc/)

2.4 Signaalitekniikat

NFC-tekniikassa käytettyjä signaalitekniikoita on kolme. Jokainen eroaa ominaisuuksiltaan modulaation koodauksen ja tiedonsiirron suhteen. Tekniikat ovat yhteensopivia RFID:n vastaavien signaalimääritelmien kanssa. Protokolla laitteiden ja tunnisteiden välillä määräytyy, kun laitepari ensimmäisen kerran keskustelee. (http://www.nearfieldcommunication.org/nfc-signaling.html)

TAULUKKO 1. Tiedonsiirtonopeudet yhteystavan mukaan

Siirtonopeus	Aktiivilaite	Passiivilaite
424 kbps	Manchester, 10 % ASK	Manchester, 10 % ASK
212 kbps	Manchester, 10 % ASK	Manchester, 10 % ASK
106 kbps	Modifield Miller, 100 % ASK	Manchester, 10 % ASK

2.4.1 NFC-A

NFC-A vastaa RFID:n A-tyyppiä ja sopii ISO/IEC 14443-standardin yhteys-protokollaan. Tämä signaalin käsittely tapahtuu Miller-koodauksella, mitä kutsutaan myös viivekoodaukseksi. Siinä on käytössä sadan prosentin amplitudimodulaatio. Se tarkoittaa, että lähetettävän signaalin amplitudin vaihtuminen sadasta prosentista nollaan prosenttiin rekisteröi tilamuutoksen. A-tyypin yhteydellä tieto siirtyy nopeudella 106 kbps. (http://www.nearfieldcommunication.org/nfc-signaling.html)

2.4.2 NFC-B

NFC-B vuorostaan vastaa RFID:n B -tyyppiä ja perustuu samaan ISO/IEC 14443 -standardiin kuin NFC-A. Koodauksena Manchester-koodaus, jossa on myös amplitudimodulointi, mutta tilamuutos huomioidaan jo kymmenen prosentin amplitudin muutoksella. Kymmenen prosentin Manchester-koodauksella tila ”1” saadaan vastaavasti 90 prosentista sataan prosenttiin siirryttäessä ja tila ”0” sadasta 90 prosenttiin siirryttäessä. Napaisuus voi olla myös käänteinen eli tilan luku tapahtuu toisinpäin. Napaisuus tunnistetaan sykronointihetkellä.
(http://www.nearfieldcommunication.org/nfc-signaling.html)

2.4.3 NFC-F

NFC-F on japanilaiseen teollisuuden standardiin (JIS) X 6319-4 perustuva. Se on Sony:n kehittämä tekniikka lyhyen matkan yhteyksiin, jonka tuotenimi on FeliCa. FeliCa käyttää Manchester-koodausta 8 % - 30 % ASK modulaatiolla. Myöskin kantoaallon taajuus on 13,56 MHz. FeliCa on osaksi yhteensopiva NFC-tekniikan kanssa ja tähän pyritään jatkossakin. FeliCan tiedonsiirtonopeus on parempi kuin tyypin- A/B menetelmät (poislukien tyypin 4 tagit) ja siinä on pidempi kantama. Nopeudet voivat olla 212 kbps tai 424 kbps. Yhteystyyppeinä FeliCa tarjoaa suojatun ja suojaamattoman yhteysmuodon. (http://www.nfc.cc/technology/felica/)

2.5 NFC-laitteet

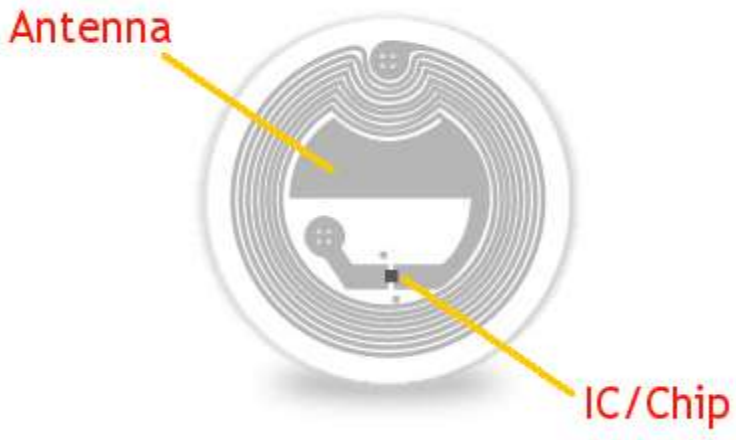
NFC-tekniikkaa käytetään useissa langatonta tiedonsiirtoa käyttävissä laitteissa. Useissa uusissa puhelimissa ja tableteissa on NFC-tekniikkaa. Myös useissa PDA-laitteissa toiminto löytyy, mikä mahdollistaa viivakoodien luvun lisäksi myös NFC-tunnisteen luvun. Esimerkiksi logistiikka- ja varastosovelluksissa tavaroiden kuittaus voi olla paljon yksinkertaisempaa, kuin optisen vaurioituneen viivakoodin luku. Yhtenä NFC-tekniikan hyötynä on laitteiston helppo paritus, mutta myös luettavien ja/tai kirjoitettavien tunnisteiden käsittely. Mobiililaitteiden tiedonsiirto voi tapahtua helposti vain kytkemällä NFC päälle kummastakin laitteesta ja kun laitteet asetetaan lähekkäin, tiedonsiirto voi alkaa. Mobiilimaksaminen on mahdollista NFC-varustetulla mobiililaitteella samoin matkakortin matkustusmäärän lukeminen. Laitteet ja palvelut, missä NFC on käytössä, on merkattu yleensä valmistajan omalla NFC-logolla, mutta yleisiä langattoman liikenteen merkkejä käytetään myös (kuva 5).
(http://www.rfidlab.fi/nfc)

KUVA 5: NFC-palveluita käyttävän laitteen tai tunnisteen merkintätapoja. Vasemmalla RapidNFC:n logo ja oikealla NFC-Forumin N-Mark.
(http://rapidnfc.com/nfc_tag_logos/)

2.6 NFC-tag

NFC-Tag on NFC-piiri, joka toimii luku- ja/tai kirjoitinlaitteen parina. Tunniste voi olla joko aktiivinen tai passiivinen. Aktiivitunniste sisältää oman virtalähteensä, joka mahdol-listaa pidemmän lukuetäisyyden. Kallis hinta on huomattava ero passiivitunnisteeseen verrattuna, joten käyttö rajautuu erityiskäyttötarkoituksiin. Passiivi- tai aktiivitunnisteen ja lukijan välinen liikenne tapahtuu vuorosuuntaisesti. (http://www.rfidlab.fi/)

Passiivitunniste sen sijaan ei tarvitse omaa virtalähdettä, vaan se indusoi tarvittavan virran NFC-lukulaitteen muodostamasta sähkömagneettisesta kentästä omaan antenniinsa (kuva 6). Passiivitunnisteen aktivoituessa lukulaitteen magneettikentässä se vastaa protokollan mukaisesti lukijalaitteen pyyntöihin. Passiivitunnisteet on yleensä suunniteltu kertakäyttöiseksi, koska valmistuskustannukset ovat pienet. Näitä voidaan käyttää esimerkiksi logistiikassa pakettitietoihin, mainoksissa mobiiliversion hakua varten tai laitevalmistuksessa tuotteen teknisten tietojen sisällyttämiseksi. Tunnisteet ovat käyttökohteen mukaan räätälöityjä esimerkiksi liimattava tarra tai avaimenperä. Tunniste voidaan käytännössä päällystää laminoimalla eri ominaisuuksisten materiaali-kerrosten väliin sen mukaan, halutaanko sen olevan vedenpitävä tai vaikka metallipinnalle liimattava. Metallipintaan liimattaessa täytyy huomioida, että tunnisteen antennin ja liimattavan pinnan välillä täytyy olla eristekerros joko päällä tai alla, riippuen siitä, kummalla puolella liimapinnan halutaan olevan. (http://www.rfidlab.fi/)



KUVA 6: Tyypillinen passiivitunniste (http://www.ubitap.com/whatisnfc)

2.6.1 Tunnistetyyppi 1

Tyypin 1 tunniste on ISO/IEC 14443A -standardin mukainen. Se voidaan lukea ja uudelleenkirjoittaa. Haluttaessa tunniste voidaan pakottaa "vain luku" -tilaan. Muistia tämä sisältää 96 bittiä ja voidaan laajentaa maksimissaan kahteen kilobittiin. Hinta nykymarkkinoilla voidaan saada muutamiin sentteihin kappaleelta.
(http://members.nfc-forum.org/specs/spec_list/)

2.6.2 Tunnistetyyppi 2

Tyypin 2 tunniste on myös ISO/IEC 14443B -standardin mukainen. Se voidaan myös lukea ja uudelleenkirjoittaa tai asettaa ”vain luku” -tilaan kuten tyypin 1 tunniste. Muistia tällä on 48 bittiä ja on laajennettavissa myös kahteen kilobittiin. Tyypin 2 tunniste on ominaisuuksiltaan laajempi ja nopeampi kuin tyyppi 1, mutta luonnollisesti hieman kalliimpi. Tyypin 2 sirut ovat kuitenkin toimintavarmempia, koska joidenkin lukijoiden tai puhelimien sanotaan toimivan huonosti 1-tyypin tunnisteiden kanssa. Näistä johtuen 2-tyypin tunniste onkin yleisin käytössä oleva tunnistetyyppi.
(http://members.nfc-forum.org/specs/spec_list/)

2.6.3 Tunnistetyyppi 3

Tyypin 3 tunniste perustuu Sony:n FeliCa-standardiin (JIS) X 6319-4. Sitä käytetään japanilaisissa älykorteissa mm. lähimaksamiseen ja metrossa. Tunnisteet konfiguroidaan valmistettaessa luettavaksi ja uudelleenkirjoitettavaksi tai vain luettavaksi. Muistin määrä vaihtelee, mutta teoriassa mahdollinen muisti voi olla yksi megatavu palvelua kohden. FeliCa-järjestelmä noudattaa NFC-standardia ISO 18092, minkä Sony ja NXP Semiconductors ovat yhdessä sopineet.
(http://www.sony.net/Products/felica/about/scheme.html)

2.6.4 Tunnistetyyppi 4

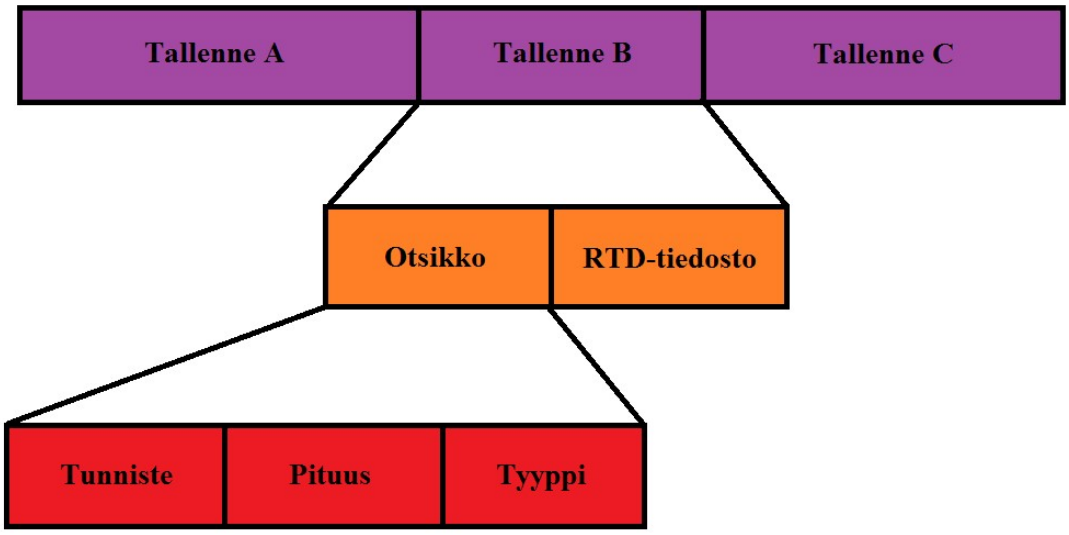
Tyypin 4 tunniste on standardin ISO/IEC 14443 mukainen. Myös tyypin 4 tunniste määritellään valmistettaessa luku/uudelleenkirjoitus tai ”vain luku” -tilaan. Muistin määrä voi maksimissaan olla 32 kilotavua palvelua kohden. Nopeus on joko 212 kbps tai 424 kbps.
(http://members.nfc-forum.org/specs/spec_list/#protts)

TAULUKKO 2: Tunnistetyyppien vertailua

	Tyyppi 1	**Tyyppi 2**	**FeliCa**	**Tyyppi 4**	**Mifare classic**
Plussat	Pieni hinta. Isohko muisti.	Laaja toimivuus. 1-Tyyppiä nopeampi.	Nopea. Massiivinen muisti.	Kehittynyt. Turvallinen. Nopea. Suuri muisti	Halpa. Kevyt turvallisuus. Muokattavissa.
Miinukset	Hidas. Ei toimi kaikissa puhelimissa	Salasana, mutta ei tunnistautumista	Ei täysin yhteensopiva.	Kallis. Monimutkainen.	Yhteensopivuus vain NXP tekniikalla
Tyypilliset brandit	Topaz Jewel	NTAG203 NTAG216 Ultralight Ultralight C	4K FRAM FeliCa Lite-S	DESFire SmartMX SmartMX2	NXP Fudan F08
Tyypilliset sovellukset	Wifi/BT paritus. Käyntikortit Vain-luku mainokset	Pienet rahasiirrot. Matkakortti. Tapahtumaliput.	Rahasiirrot Matkakortti	Pankki. Tilisiirrot. Henkilökortit.	Tapahtumaliput. Halpaliput.

2.7 RTD-tiedosto

RTD eli Record Type Definition on tallenteeseen ohjelmoidun tietokuorman tyypin määritelmä. Se määrittää säännöt ja rakenteen muodon standardin mukaisen tallennetiedon luomiseen, jotka ovat käytössä NFC-Forumin ja kolmansien osapuolien NDEF-muotoa noudattavissa määritelmissä. RTD-tiedostoja käytetään tallenteiden sisältämän tiedon ja niiden eri osa-alueiden jakamiseen tietotyypeiksi. RTD-määritelmien noudattaminen mahdollistaa käyttäjien tekemien NFC-sovellusten yhteensopivuuden.
(http://members.nfc-forum.org/specs/spec_list/#protts)

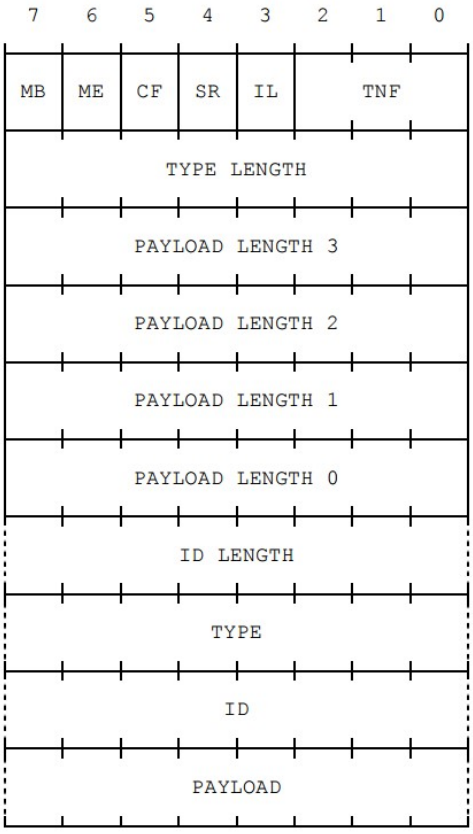


KUVA 7: NDEF-viestiesimerkki ja siihen sisältyvä RTD-tiedosto

Hyvä esimerkki eri RTD-määritelmien käytöstä on NFC-Forumin Smart Poster, jossa käytetään ”NFC RTD TEXT” ja ”NFC RTD URI” valmiita määritelmiä. Myös muita vaihtoehtoisia määritelmiä voidaan lisätä, jos halutaan liittää esimerkiksi kuva tai vaikka lukevaa laitetta informoiva tyyppi-ilmoitus.
(http://flomio.com/2012/05/ndef-basics/)

2.8 NDEF

NDEF-tietomuoto on kevytrakenteinen binäärinen viestimuoto, missä siirrettävä data kuljetetaan ohjelmistojen välityksellä kahden NFC-Forumin mukaisen laitteen tai laitteen ja tunnisteen välillä. Se on siis tietomuoto NFC-tunnisteen tiedon sisällyttämiseen. Jokainen NDEF-viesti muodostuu yhdestä tai useammasta NDEF-tallenteesta (kuva 7), jotka sisältävät satunnaisen ohjelmaperäisen tietokuorman ja kokonaisuudessaan yksittäisen viestirakenteen. NDEF-tallenne voi olla maksimikooltaan 4 194 303 oktettia. Tallenteet voidaan ketjuttaa toisiinsa, jotta saadaan suurempia tietokuormia. NDEF-tallenne kantaa kolmea parametriä, joilla kuvaillaan tietokuormaa. Ne ovat tyyppi, pituus ja yksi valinnainen osoitin, mihin voidaan tallentaa esimerkiksi osoitetieto URI-pohjaista ketjutusta varten. Pituus ilmoittaa, kuinka monta oktettia tietokuorma on pitkä. Tyyppi taas ilmoittaa RTD-tiedoston tyypin eli tietokuorman asiasisällön luonteen.
(http://www.eet-china.com/ARTICLES/2006AUG/PDF/NFCForum-TS-NDEF.pdf)



KUVA 8: NDEF-tallenteen oktettirakenne (http://www.eet-china.com/ARTICLES/2006AUG/PDF/NFCForum-TS-NDEF.pdf)

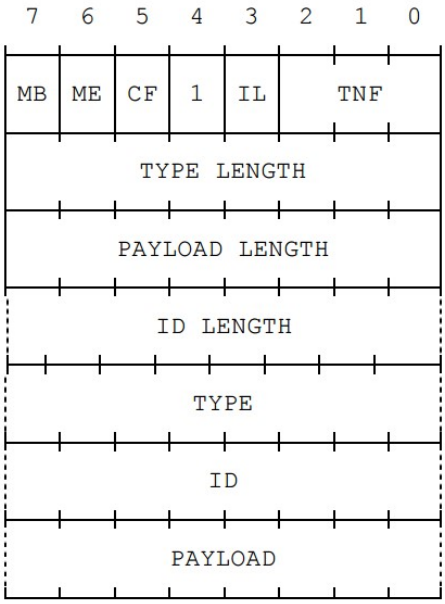
NDEF-tallenteen oktettirakenteen bittien selitykset:

MB Message Begin, lippubitti, joka on "1", kun NDEF-viestin alku on kyseessä.

ME Message End, lippubitti, joka on "1", kun NDEF-viesti päättyy. Pilkotussa NDEF-viestissä tämä lippu on "1" vain silloin, kun pilkottu viestiketju päättyy.

CF Chunk Flag, lippubitti, joka on "1", kun se osoittaa NDEF-tallenteen olevan joko ensimmäinen tai keskimmäinen pilkotun NDEF- viestin tallenne.

SR Short Record, lippubitti, joka on "1", silloin kun tietokuorman pituus -atribuutti on yhden oktetin mittainen tai lyhyempi.



KUVA 9: Short record -pohja (http://www.eet-china.com/ARTICLES/2006AUG/PDF/NFCForum-TS-NDEF.pdf)

Short record -pohja on tarkoitettu kompakteille tietokuormille, jotka mahtuvat maksimissaan 255 oktetin tietokuormakenttään. Työkalua käyttävien on kuitenkin huomioitava, että rakenteista molempien pitää olla käytettävissä. Vaikka itse suosisi vain normaalia tai siistimpää Short record -pohjaa. Yksittäinen NDEF-viesti voi sisältää kumman vaan. (http://www.eet-china.com/ARTICLES/2006AUG/PDF/NFCForum-TS-NDEF.pdf)

IL ID_LENGTH, lippubitti, joka on "1", kun otsikkotietona halutaan käyttää ID_LENGTH kenttää. Muutoin otsikkotieto periytyy tallenteen otsikosta ja ID tulee samoin tallenteen mukaan.

TNF Type Name Format, TYPE-kentän arvon rakenteen.

Type Name Format, TNF -kentän arvot:

Tyhjä	0x00
NFC-Forum tunnettu tyyppi [NFC RTD]	0x01
Mediatyyppi, mikä on määritelty [RFC 2046 standardissa]	0x02
Absoluuttinen URI, määritelty [RFC 3986 standardissa]	0x03
NFC-Forum ulkoinen tyyppi [NFC RTD]	0x04
Tuntematon	0x05
Muuttumaton	0x06
Varattu	0x07

0x00 arvoa käytetään, kun tallenteeseen ei liity tietokuormaa tai tyyppiä. Käytettäessä kentät TYPE_LENGTH, ID_LENGTH, ja PAYLOAD_LENGTH täytyy olla nolla, silloin muut kentät periytyy tallenteelta. TYPE, ID ja PAYLOAD.

0x01 arvoa käytetään, kun TYPE-kenttä sisältää arvon, joka noudattaa NFC-Forumin RTD type name format määritelmiä.

0x02 käyttö, kun TYPE-kenttä sisältää media-type BNF rakenteen mukaisen arvon.

0x03 käyttö, kun TYPE-kenttä sisältää absolute-URI BNF rakenteen mukaisen arvon.

0x04 arvoa käytetään, kun TYPE-kenttä sisältää arvon, joka noudattaa NFC-Forumin RTD type name format määritelmiä ulkoisille tietotyyppinimille.

0x05 arvoa pitäisi käyttää, kun TYPE-kentän tyyppi on tuntematon. Käytettäessä TYPE_LENGTH-kenttä pitää olla nolla, jolloin TYPE-kenttä periytyy tallenteen tyypin mukaan. Suosituksena on, että 0x05 TNF-arvon sisältäviä viestejä ei prosessoida eteenpäin, silti tallennus on suositeltavaa.

0x06 arvoa täytyy käyttää kaikkien pilkottujen tallennepalojen keskimmäisille ja päättäville tallennepalalle. Sitä ei saa käyttää muissa tallenteissa. Käytettäessä TYPE_LENGTH-kenttä pitää olla nolla, jolloin TYPE-kenttä periytyy tallenteen tyypin mukaan.

0x07 arvo on varattu tulevaisuudessa käytettäväksi. Sitä ei kuulu käyttää.

(http://www.eet-china.com/ARTICLES/2006AUG/PDF/NFCForum-TS-NDEF.pdf)

2.9 LLCP

LLCP on OSI-mallin toisen alemman tason protokolla, joka on kehitetty tukemaan peer-to-peer -yhteyksien kulkua kahden NFC-aktiivisen laitteen välillä. LLCP perustuu teollisuusstandardiin IEEE 802.2. Se mahdollistaa kaksisuuntaista liikennettä käyttävän ohjelman tietoliikenteen NFC-laitteessa. LLCP hoitaa kahden laitteen välisen yhteyden avauksen, hallinnan ja valvonnan Määritelmä tarjoaa kaksi yhteystapaa: yhteydellinen ja yhteydetön, joista käyttöön valitaan toinen tai kummatkin.
(http://members.nfc-forum.org/specs/spec_list/)

Yhteydetön palvelu takaa nopeimmat asetukset, mutta huonon luotettavuuden, eikä datavirtauksen seurantaa. Vaikkakin nämä puutteet voidaan korvata protokollapinon aikaisemmalla tasolla MAC-kerroksessa. Tai mahdollisesti datan sallitaan sisältävän tietyn määrän virheitä.
(http://members.nfc-forum.org/specs/spec_list/)

Yhteydellinen palvelu sen sijaan takaa järjestyksellisen datan lähetyksen, datan lähetyksen seurannan, datavirtauksen seurannan, istuntoon perustuvan palvelutason multipleksoinnin. Tässä palvelussa kaikki paketit on tunnistettavissa lähettäjän ja vastaanottajan suhteen, sekä siinä on OSI-kerroksien väleissä liikkuvien PDU-pakettien juokseva numerointi.
(http://members.nfc-forum.org/specs/spec_list/)

3 TIETOTURVAUHKAT

3.1 Urkinta

Niin NFC:ssä kuin muissakin langattomissa yhteysmuodoissa on ilmeistä, että urkinta on huomioitava asia. Kaikki RF-alloilla liikkuva signaali on kenen tahansa saatavilla, jos on vain antenni ja se on vaaditulla etäisyydellä, sekä oikein suunnattu. Tiedot datan purkamiseen NFC-tekniikan osalta löytyy vapaasti internetistä, joten pienelläkin pohjatietämyksellä asiaan perehtyvä voi hommaan ryhtyä. Signaalin keräämiseen ja sen purkamiseen tarvittavan välineistön voi ostaa tekniikan kehitykseen tarkoitettuna laitteena. Asiaan on silti huomattavasti perehdyttävä. Signaalin kaappaukseen kohdistuva urkinta on hyvin haastava aihe. NFC-tekniikan turvallisuusominaisuudeksi sanottu lyhyt kantama ei ole ainoa ratkaiseva seikka, koska etäisyys ei ole tekniikan läheskään ainoa muuttuja. Tilanteeseen vaikuttaa moni asia, kuten NFC-signaalin teho, urkinta-antennin ominaisuudet, lukulaitteen suunnattavuus, urkintalaitteen laatu ja urkintalaitteen dekooderin laatu. On kuitenkin merkittävää kummassa toimintamoodissa urkittava laite on. Passiivisen laitteen moduloimaa signaalia on paljon vaikeampi urkkia, koska se on herkempi häiriöille. Karkeasti arvioiden aktiivisen laitteen urkinta voidaan suorittaa noin 10 metrin päästä, kun taas passiivista pääsee hyödyntävästi kuuntelemaan vasta 1 metrin etäisyydeltä.
(http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf)

3.2 Datakorruptio ja -modifiointi

Datan korruptointi hyökkäyksenä voi olla keino estää NFC-laitteiden välinen tapahtuma. Tähän tarvitaan tietämystä kuitenkin signaalimuodoista ja -ajoituksista, mitä tekniikassa käytetään. Jotta korruptointi voisi onnistua, niin hyökkääjän tarvitsee lähettää signaalia sallituilla taajuuskaistoilla, mutta ajoitus täytyy osua modulaation ja koodauksen osalta kohdalleen.
(http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf)

Datan modifionti eroaa paljon datakorruptoinnista. Tässä hyökkääjä haluaa lähettää hyväksyttävää, mutta manipuloitua dataa lukijalle. Myös suoritustapa on monimutkainen riippuen käytetävästä modulointikoodauksesta. Kun käytetään Miller-koodausta 100 prosentin amplitudilla, niin kaikkia bittejä ei pysty muokkaamaan huomaamatta. Signaalista on mahdollista poistaa tauot, mutta ei lisätä niitä. Hyökkääjä ei voi muuttaa bittiä "1" bitiksi "0", mutta bitin "0" bitiksi "1", jota edeltävän bitin pitää olla "1". Manchester-koodatussa lähetyksessä signaalitasot 82 prosenttia ja 100 prosenttia huomioidaan muutosrajoiksi. Tämä mahdollistaa hyökkääjän lisäämään 82 prosenttiseen signaaliin voimakkuutta oikeassa suhteessa niin, että se näyttäisi 100 prosentin signaalilta. Tällöin alkuperäinen 100 prosentin signaali olisi tulkittavissa uudeksi 82 prosentin amplitudiksi. Nämä on mahdollista vain, jos vastaanottavan laitteen signaalin sisääntulorajat pystytään olemaan ylittämättä. On myös todennäköistä, koska mahdollisesti juuri tämän takia laitteiston rajat voidaan asettaa sopiviksi. (http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf)

3.3 Datan lisäys

Tämä tapa ei ole kovinkaan mahdollinen, mutta käytännössä se voi onnistua, jos keskustelun vastaajaosapuoli tarvitsee huomattavan pitkän ajan vastatakseen. Tällöin hyökkäysviesti voidaan yrittää lähettää ennen odotettavaa viestiä. Jos viestit menevät päällekkäin, niin lähetysdata menee kelvottomaksi. (http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf)

3.4 Man-in-the-middle

Man-in-the-middle on tyypillinen hyökkäystapa, jota kutsutaan myös nimellä "Relay attack". Siinä kaksi keskustelevaa laitetta luulevat, että ne keskustelevat toisillensa. Tosiasiassa ne keskustelevat välittäjälaitteen kanssa, joka vastaanottaa ja lähettää tietoa viestin alkuperäisvastaanottajalle ja päinvastoin. Silloin kaikki siirtoon liittyvä tieto on kerättävissä välittäjälaitteen muistista. Asiaa kuitenkin vaikeuttaa NFC-tekniikan kohdalla häirintäsignaalin havainnointimahdollisuudet. Tämä kuitenkin luokittuu mahdottomaksi tilanteessa, jossa toinen laitteista toimii passiivisena. Sillä tässä tapauksessa välittäjälaiteen on samanaikaisesti muodostettava lähetystä häiritsevä kenttä ja toinen kenttä tiedon välittämiseksi vastaanottavalle osapuolelle. Se siis osoittautuisi mahdottomaksi jo sen takia, että kaksi RF-kenttää on mahdotonta järjestää täydellisesti. Sen lisäksi häirintä voi lopettaa siirtoprotokollan.
(http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf)

Toisaalta mahdollisempi tilanne olisi, jos kummatkin laitteet toimisivat aktiivimoodissa. Kenttiä vuorotellessa, kuten aktiivi-aktiivi -yhteydessä on käytäntönä. Tällöin hyökkäyslaite voi keskittyä vain tiedon välittämiseen ja ajoittaiseen häirintään. Kuitenkin ongelmana sama häirinnän havainnointimahdollisuus, sekä tilanne missä jo lähettänyt laite odottaa vastausta, mutta saakin välittäjälaitteen välittämän viestin. Tämä on siis sama viesti mahdollisesti muokattuna, minkä itse on juuri lähettänyt. Tässä siis uusi mahdollisuus häiriön havainnoitsemiseksi ja siirtoprotokollan keskettyttämiseen.
(http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf)

3.5 Haitalliset tunnisteet ja ohjelmat

Yksi helpoista hyökkäyksistä voidaan suorittaa käyttäjän piittaamattomuutta tai hyväuskoisuutta käyttäen. Sillä tunnisteet ovat usein uudelleenohjelmoitavissa tai vaikkapa yksinkertaisesti korvattavissa liimaamalla uusi päälle. Haitallisen linkkitiedon uudelleenohjelmointi tai valmiiksi ohjelmoidun tunnisteen huomioiminen arkipäivässä voi olla lähes mahdotonta. Kuten kehysrakenteita tarkastellessa kuvassa 8 ja 9 voidaan hyvin todeta, että mahdollinen haittasivulle ohjaus ei näkyisi mitenkään asiallisesti

muotoillun otsikon vuoksi. Päälle liimattu uusi tunniste voi olla helpommin havaittavissa, jos sitä osaa etsiä.

Haitallisten ohjelmat voivat esiintyä muuneltujen tai muuten asiattomien tunnisteiden osoittamana ja ladattavana ohjelmana. Viesti mikä näytössä lukee, ei välttämättä tarkoita mitään tai ohjaa käyttäjää yksiselitteisesti hyväksymään asennuksen naamioituna tilanteena (kuva 10).

KUVA 10: Haitallista anti-virusohjelmaa suositteleva mainos (https://grahamcluley.com/2013/12/android-scareware/)

4 POHDINTA

NFC-tekniikka on aiheena hyvin mielenkiintoinen jo pelkästään suuresti kuluttaja-kuntaa koskevana asiana, mutta myös sen lukemattomien käyttömahdollisuuksien takia. Standardit ovat ymmärrettäviä ja nopeasti sisäistettävissä perustasolla. Eikä tekniikkaan ohjelmallisesti perehtyminen luulisi olevan hankalaa, koska esimerkkejä löytyy hyvin.

Työssä selvisi tekniikan keskeiset modulointitavat ja yhteyden ominaisuudet. Datavirran muodostuminen ja siihen liittyviä seikkoja tuli esille. Tekniikkaan vaikuttavat tahot ja niiden suhteiden vaikutus tekniikan kehittämiseen voidaan tulkita positiiviseksi. Elektroniikan valmistuksen kehityksen myötä tekniikka tulee yhä yleisemmäksi ja mahdollisuudet tekniikan suurkulutukseen lähenevät. Hyvänä esimerkkinä Japanissa käytännössä toimiva FeliCa-järjestelmä.

Yhteisen ja toimivan toimintamallin luominen on edelleen hyvässä vauhdissa. Paljon on tehtävää esimerkiksi hyökkäyksien torjumiseksi, sillä tekniikka ja sitä väärinkäyttävät kehittyvät saman suuren tietoverkkorakenteen sisällä. Käytön turvallisuus on kuitenkin lopulta suurin ratkaiseva tekijä tekniikan menestymiselle, kun kyseessä on käyttäjän omaisuuden hallinta.

LÄHTEET

nearfielcommunication.org, Technology Standards, Luettu 20.10.2015
http://www.nearfieldcommunication.org/technology.html

nearfielcommunication.org, Signaling, Luettu 20.10.2015
http://www.nearfieldcommunication.org/nfc-signaling.html

eet-china.com, NFC Forum NDEF specification, Luettu 10.11.2015
http://www.eet-china.com/ARTICLES/2006AUG/PDF/NFCForum-TS-NDEF.pdf

rfidlab.fi, NFC ja hyödylliset termit, Luettu 23.10.2015
http://www.rfidlab.fi/

Haselsteiner, E & Breitfuß, Security in Near Field Communication, Luettu 11.10.2015
http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf

nfc-forum.org, NFC Forum technical specifications, Luettu 23.10.2015
http://members.nfc-forum.org/specs/spec_list/

sony.net, Felica system, Luettu 5.11.2015
http://www.sony.net/Products/felica/about/scheme.html

ecma-international.org, Standard ECMA-340, Luettu 20.10.2015
http://www.ecma-international.org/publications/files/ECMA-ST/Ecma-340.pdf

nfc.cc, NFC technology, Luettu 1.11.2015
http://www.nfc.cc/technology/nfc/

rfid-handbook.de, Active load modulation, Luettu 29.10.2015
http://rfid-handbook.de/about-rfid/active-load-modulation.html

grahamcluley.com, Kuva, Saatavissa 11.11.2015
https://grahamcluley.com/2013/12/android-scareware/

developer.android.com, Kuva, Saatavissa 12.11.2015
http://developer.android.com/guide/topics/connectivity/nfc/hce.html

nearfielcommunication.org, NFC compatible smart phones, Luettu 21.10.2015
http://www.nearfieldcommunication.org/smartphone-development.html

nfc-forum.org, Membership overview, Luettu 21.10.2015
http://nfc-forum.org/about-us/join-the-forum/membership-overview/