www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 7 Issue 9 September 2018, Page No. 24197-24205
Index Copernicus Value (2015): 58.10, 76.25 (2016) DOI: 10.18535/ijecs/v7i9.01

NFC Communication Protocol

LN Harnaningrum
STMIK AKAKOM Yogyakarta,
Jl. Raya Janti 143 Yogyakarta 55198

Abstract
Near Field Communication (NFC) is a short-range communication technology. Because of its popularity, NFC is widely applied in the field of Internet of Things (IoT). NFC technology reduces the use of many other devices, so that only smartphones, which have NFC embedded in them, are then widely used for various purposes. Smartphones are becoming quite popular equipment today, because smartphone users are increasing from time to time. With this development, NFC is embeded in smartphones widely used and quite popular.

Implementation of NFC has been done in various fields, such as health, business, transportation and others. NFC applications in the Service Domain include healthcare, location, finance, social networking, entertainment, education etc. In the field of healthcare applications, NFC can facilitate communication between patients and paramedics, such as doctors, nurses, pharmacists, and other sections. In other fields there are social networking applications, entertainment applications, education applications, NFC miscellaneous applications.

In terms of the development of the tag itself, NFC can be discussed with 2 kinds of approach. Firstly is from the side of tag, and secondly is in terms of communication technology. There are 4 types of NFC tags, type 1, type 2, type 3 and type 4. Each type has its own specifications. Frames, data and payload formats have their own different specifications. In its technological side there are 3 types of NFC A, B and F. Each type has its different way in signals and the data format sent. NFC type A is used in this testing

Such rapid development, however, gives positive and negative impacts. One of the effects is that with the use of NFC cards that there will be more possibilities for multiple cards to be read simultaneously. For this reason, a reader is required to read more than one card. Trials show that some cards can be read by a reader sequentially and can write or read.

Keyword: Card, multitag, format, data.

1. Introduction

The development of the current network is not just a computer network, but also a network that connects equipment. And with people's desires who always want to be practical, the relationship between equipment is also done without using cables. One area that is now growing rapidly is the mobile phone network. In addition to developments in the network at large, the telephone equipment itself now has enough to have additional facilities that can be utilized.

One network that can be built between equipment is a mobile telephone network with a mobile phone or mobile phone with other equipment. The mobile phone itself is now equipped with equipment that supports access between equipment. There is wifi, bluetooth, infrared, and Near Field Communication (NFC). Each of the communication media has its own work area and

protocol. Likewise the development of the use of wireless communication equipment also depends on the application that uses it. One that is quite developing is the use of NFC.

The use of NFC already covers many aspects. NFC is a development of Radio Frequency Identification (RFID). RFID systems use frequencies that vary from around 100 kHz to above 5 GHz. While NFC, which is the development of RFID, works on a frequency of 13.56 MHz and follows ISO14443 and ISO 18092 for low-level data exchange between two NFC devices. Specifically, these two ISO standards specify operating frequency, modulation, coding schemes, anti-collision routines, and communication protocols. NFC data exchange format (NDEF) and NFC tag format defined by the NFC Forum. When compared to the connection speed of Bluetooth and WiFi, NFC has a slower data transfer rate of up to 424 kilobits per second (kbps). Communication distance from NFC is the lowest among other communication technologies. Besides being used for communication between mobile phones, NFC has also been used for business purposes, such as retail, credit cards and other applications. One that is now also developing is the application that utilizes NFC for medicine.

In the field of medicine, NFC is used to record inpatient daily medical measurement data.[1] The system built is by taping the NFC device to the patient's TAG to ensure patient data, and then the nurse takes measurements, the results are recorded on NFC devices (smartphone). After completing the measurements and taking notes, tap again to mark the end of a patient's data. This is done for other patients. Recorded data is sent to the storage (PC) using NFC peer to peer communication. In addition, in the field of medicine as well, NFC is used to store patient medical record data.[2][3][4]

Memory capacity in NFC is not much. The largest capacity only reaches 2 KB after exploitation. With this limited capacity, the data that can be stored must be truly selected. In many applications, the data stored on the card is only data related to the identity. Meanwhile, in other applications and situations, it is possible to require substantial data storage. This is due to the need for fast and precise data. Therefore, if data can be available on-site, data acquisition becomes easier and data execution can be done immediately.

Limited capacity and the need for data storage that is quite important and easily accessible is a significant requirement in the current era. Likewise, data communication between storage media (NFC tags) and other communication equipment that requires data will also be an important concern.

The use of NFC still leaves enough opportunities to be developed.[5] One of them is in the issue area of memory capacity that is quite small in NFC tags. This is also accompanied by the existence of important security issues. The issue of security is important because without a good security system, data stored and should only be accessed by interested parties will be accessible to other parties. The data can be misused by other people who might cause harm to the data owner. For that, the easier and faster the data can be accessed the better. Small enough memory capacity becomes something that should get enough attention. How to make a small enough memory can store a lot of data, and how to make good communication between NFC tags and other communication equipment.

This research is directed to identify data communication protocols between mobile devices and NFC. In this case, it is tested to communicate the NFC card reader device in order to communicate with more than one NFC card.

2. Literature review

NFC technology reduces the use of many other devices, so only smartphones, which have embedded NFCs in them, are then widely used for various purposes. Smartphones are becoming quite popular nowadays, as smartphone users are become increasing over time. With that development, the embedded NFC inside the smartphone is widely used and quite popular.[5]

Research on NFC for health applications has been carried out since 2013. By using one of the NFC communication methods, namely NFC peer to peer communication, research is obtained to record the results of patient examinations.[1] This research focuses on the success of data transfer between devices and the time taken to work on recording.

Year 2014 conducted a study that utilizes NFC for patient hospital data collection based on the presence of patients in the hospital. Research focuses on indoor geo-localization the in hospitals.[3]

The research conducted is about the use of security systems on data transfer by utilizing the Android API on a low level.[2] This device uses peer to peer communication. Another research about using NFC is to store a patient's medical data. Data is entered to the server and doctors can access the data directly after obtaining patient data by retrieving it from NFC tags carried by patients. The study focuses on the ease of obtaining data for the purposes of physician decision making.[11]

Research has also been carried out by creating a framework to record patient data on NFC tags in a limited number and other data stored in the EMR.[4] This protocol has four phases, namely: Phase 1: Patient Registration and Delivery, Phase 2: Med pack preparation, Phase 3: Nurses Station and expenses (administration) of drug (online and offline procedures), and Phase 4: Monitoring, controling and recycling.

3. Analysis and Design

NFC has been widely used in many applications. In 2011, mobile phones with NFC facilities have started to circulate in Indonesia (nasional.kompas.com, "Mari sambut kehadiran teknologi NFC", 28/01/2011). In other countries, the use of NFC has been widely developed (inet.detik.com, "Tren baru, transaksi dengan NFC", 19/03/2012). Currently, the use of NFC for payment at toll booths is being developed (ekonomi.kompas.com, "Ke depan, bayar tol pakai ponsel", 10/10/2017).

With the increasing use of NFC, the more NFC devices are involved. This also affects the communication that occurs. Many NFC tags are involved in one application that allows many transactions.

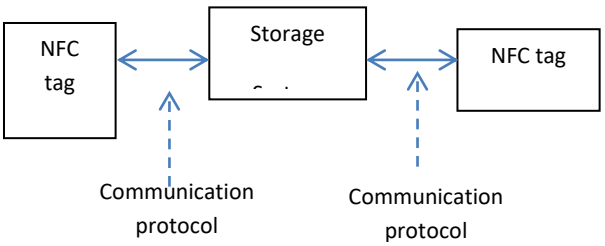

Figure 1: NFC Multitag Communication System Overview

This research was testing how NFC tags communicate if there are more than one tag. Pricipally, if there is only one communication path, it will be done alternately. Problems occur if in one area there are more than one reader and many tags. There is a possibility that the reader will collide with each other and the information sent will change. This study did not discuss the handling of anticollision, but only reached the reading of more than one card by a reader.

4. System Implementation and Discussion.

4.1. NFC tag testing process.

In this test, NFC tags used for testing are Mifare. MIFARE is a NXP Semiconductor trademark of a series of chips that are widely used on contactless smart cards and proximity cards. The MIFARE name includes proprietary technology based on various levels of standard ISO / IEC 14443 Type A card 13.56 MHz smart type contactless card. It combines AES and DES / Triple-DES encryption standards, as well as older proprietary encryption algorithms. The technology is owned by NXP Semiconductors, who was fired from Philips Electronics in 2006. This technology is contained in cards and readers, as well as contact smart cards, in the case of SAM AV2. All types of cards are in accordance with ISO / IEC 14443 Type A. The MIFARE name (derived from the term MIkron FARE Collection System) includes four families of contactless cards:

(a) MIFARE Classic: Use proprietary protocols that are in accordance with components 1-3 of ISO / IEC 14443 Type A, with NXP exclusive security protocols for authentication and encryption. Subtype: EV1 (other subtypes are no longer used).

(b) MIFARE Plus: Replace MIFARE Classic with certified security (AES-128 based) and fully compatible with MIFARE Classic. Subtype S / X, SE

(c) Ultralight MIFARE: Low cost ICs that are useful for high volume applications such as public transportation, loyalty cards and event tickets. Subtype: C, EV1

(d) MIFARE DESFire: Smart cards that comply with components 3 and 4 ISO / IEC 14443-4 Type A with the NXP mask-ROM operating system. 'DES' in the name refers to the use of DES, 2K3DES, 3K3DES and AES encryption; whereas 'Api' is an acronym for 'Fast, innovative, reliable and perfected'. Subtype: EV1, EV2.

There is also a MIFARE SAM AV2 smart contact card. This can be used to handle encryption in communicating with contactless cards. SAM (Secure Access Module) provides secure storage of cryptographic and cryptographic keys. And the card reader used is a module from Arduino and then tested.

4.2. Analysis of test results

NFC tags used are mifare based on ISO / IEC 14443 Type A 13.56 MHz standard contactless smart cards.[12]

Table 1: NFC Type A Specifications.

Specification	Description	
Sequence Format		
-Poll→Listen Modulation	Modified Miller coding dengan ASK modilasi 100%	
-Listen→Poll Modulation	Manchester coding dengan OOK modulasi subcarrier	
-Synchronization	Does not require a synchronization signal, so the SoS does not exist	
-De-synchronization	EoS indicates the end of the sequence.	
Bit Level Coding	The patterns X, Y, and Z are used to code the digital alphabet Logic “0” and Logic “1”. Logic “0”s and Logic “1”s are the components of frames.	
- Poll→Listen Coding Scheme	Poll Mode. NFC Forum Tools MUST make Logic code "0" and Logic "1" as follows • Logic “1” pattern X • Logic “0” pattern Y With the following exceptions: • The Z MUST pattern is used for the first logic code "0" (SoF) • If there are two or more adjacent logics "0" s, the Z pattern MUST be used from the second logic "0"	Listen Mode The NFC Forum device MUST decode Logic "0" and Logic "1" as follows • The first pattern of Z MUST be translated as Logic "0". • If the NFC Forum Device detects an X pattern, it MUST make this decode as "1" Logic. • If the NFC Forum Device detects the Y pattern after the X pattern, it MUST decode the Y pattern as Logic "0". • If the NFC Forum Device detects the Z pattern after the Y pattern, then MUST decodes the Z pattern as Logic "0".

		• If the Forum NFC Tool detects the Z pattern after the Z pattern, it MUST decode the last Z pattern as "0" Logic.
- Listen→Poll Coding Scheme	E and D patterns are used for the Logic "0" digital alphabet code and "1" Logic. Logic "0" and Logic "1", referred to as data bits as follows, are component frames.	
	Poll Mode The NFC Forum device MUST decipher the "0" Logic code and "1" Logic as follows • If the Forum NFC Tool detects the D pattern, it MUST break this code as "1" Logic. • If the Forum NFC Tool detects an E pattern, it MUST break this code as Logic "0".	Listen Mode The NFC Forum Tool MUST encode Logic "0" and Logic "1" as follows • Logic "1": pattern D • Logic "0": pattern E
Frame Format	Data bits, when transmitted between NFC Forum Devices, are grouped in frames. The frame format is different for each technology. NFC-A technology classifies data bits together in frames by adding SoF and EoF. The parity bit (P) is added at the end of every 8 bits of data. Using three types of frames: short frame, standard frame, and bit-oriented SDD frame. Short frames are used to start communication (wake up). Standard frames are used for data exchange. The bit-oriented SDD frame is used for collision resolution.	
- Short Frame	The short frame is used to start communication and consists of the following: • SoF • Up to 7 bits of data are sent lsb first • EoF No parity added.	
- Standard Frame	The standard frame is used for data exchange and consists of the following (see Figure 4): • SoF • n * (8 data bit + odd parity bit), with $n \geq 1$ • EoF (Poll → Just Listen to communication)	
- Bit Oriented SDD Frame	The bit-oriented SDD frame is used for collision resolution and the result of a standard frame with a length of 7 bytes divided into two parts. The split can occur after there is little data. Figure 5 shows an example with split after the first bit of the second byte.	
Data and Payload Format	Data embedded in NFC-A short frames or NFC-A oriented SDD frames has little to no SoD and EoD.	
Command Set	Payload exchanged between NFC Forum Devices consists of Orders and Responses	
ALL_REQ and SENS_REQ	The ALL_REQ and SENS_REQ commands are sent by the NFC Forum Tool in Poll Mode to investigate the Operation Field for NFC Forum Devices in Listen	

	mode that is configured for NFC-A Technology.
SDD_REQ	The SDD_REQ command is used to get NFCID1 from the NFC Forum Device in Listen Mode and to detect whether more than one device The same technology is in the NFC Forum Operation Device Field in Polling Mode. Furthermore, the SDD_REQ command is used for collision resolution if there is more than one NFC Forum Device in Listen Mode in the operations field. See [ACTIVITY] for details on the impact resolution mechanism.
SEL_REQ	Use the SEL_REQ Command to select the NFC Forum Tool in Listen mode using its NFCID1.
SLP_REQ	Use the SLP_REQ command to place the NFC Forum Device in Listen Mode under SLEEP
- Frame Delay Time Poll→Listen	*Polling Frame Delay Time* → Listen (FDTA, LISTEN) is the time between the Poll Frame and Listen Frame. The time between the minimum value of FDTA, LISTEN, MIN and the maximum value of FDTA, LISTEN, MAX defines the time interval in which the Listen Frame is allowed to be sent by NFC Forum Tools in Listen Mode to respond to the NFC Forum Frame Frame Forum in Poll Mode. For NFC-A, FDTA technology, LISTEN relies on the last bit logic value before EoF is sent by the NFC Forum Tool in Poll Mode.
- Frame Delay Time Listen→Poll	Frame Delay Time Listen → Poll (FDTA, POLL) is the time between Listen Frame and Poll Frame. The minimum value of FDTA, POLL, MIN defines the time the NFC Forum Tool in Poll Mode must wait before sending a new Frame Poll after receiving a LISTEN Frame. The maximum value of FDTA, POLL, MAX is not defined. For NFC-A technology, the FDTA definition, POLL relies on the logic value of the last data bit from Listen Frame sent by the NFC Forum Device. However, FDTA, POLL is not limited to certain discrete. values like FDTA, LISTEN.
- Guard Time	This section determines the Operator's guard time that is not modified after which the NFC Forum Device in Listen Mode must be ready to accept the ALL_REQ or SENS_REQ Command.

4.3. Protokol ISO 14443 A/B and ISO 15693.[12]

4.3.1. Data Format

Data formats (Start Bit, Data Bits, Parity, Stop Bit) can be configured with software, and can be arranged to suit the specific needs of data transmission between two communication devices. The general data format is defined as follows.

Table 2: Data Format Protocol ISO14443

Parameter	Description
Baud Rate	Selective: 9600, 19200, 38400, 57600, 1152000 (can be changed by commands sent from the host)
Data bit	Fix : 8 bit
Start bit	Fix : 1 bit
Stop bit	Selective : 1 bit
Paritas	Selective : odd, even, none

The following is the default setting.

Table 3: Setting the default ISO 14443 protocol data format

Baud Rate	Data bit	Start bit	Stop bit	Parity

9600	8	1	1	None

4.3.2. Link Layer

The communication protocol is a packet-oriented protocol that all data exchanged between the two communication devices will be based on the packet format. This protocol is designed for multi-drop mode and where point-to-point mode can be treated as a special case of multi-drop mode. The data package starts with the .STX control character. and ends with .ETX., which follows an 8-bit BCC checksum. In addition to checksums used for error checking, time-out characters (bytes) and packet timeouts (commands) are used to resync the communication.

4.3.3. Packet Format

There are two types of data packages. Command Message is a Send package from Host to the reader device. Message Reply is a Send package from reader to Host. Package format for Command Messages (Host to Reader)

STX	STATION ID	DATA LENGTH	CMD	DATA[0..N]	BCC	ETX

Packet format for Reply Message (Reader to Host)

STX	STATION ID	DATA LENGTH	STATUS	DATA[0..N]	BCC	ETX

Table 4 describes the package field used for operations on the Mifare card.

Table 4: Field paket

Field	Length	Description
STX	1	0Xaa- "Start of Text". Is the beginning of a data package.
DADD	1	Address device, which is used for multidrop mode, only the reader (device) with the programmed address of the pre-programmed device that will respond to the received command packet. The 0x00 address is a special address for point-to-point communication mode. The reader responds to all packets that have a "0" address. (There is no checking of matching addresses to be done)
Data length	1	The length of the data byte in the package. Length = Number of_bytes (time / status + DATA [0 ... N]. Data length includes time / status and DATA fields, but not BCC
CMD	1	*Command field*: *command field* consist of one *command byte.* Refer to the Command table for a list of commands
STATUS	1	Reply Status byte: status sent back from reader to host. This byte is only used for packet replies.
DATA [0-N]	0 – 255	Data Field is a data stream with variable length, depending on the Command word. There are also several Commands that have zero length. If the Data Field from Command / Reply Message has more than 80 bytes, the reader will not respond and treat this command as an error and wait for the other command.
BCC	1	Eight checksum block bits. Checksum calculation includes all bytes in the package, but does not include STX, ETX
ETX	1	0xBB "END of TEXT" - Which indicates the END of the package.

4.3.4. Command Set

Command is grouped into different categories. The groups are the System command, the ISO14443A standard command, the ISO14443B standard command, the MIFARE command and the ISO15693A standard command.[12]

Table 5: Group Command

ISO14443 TYPE A Command (0x03 – 0x08)		
0x03	ReqA	ISO14443A Request Command
0x04	AnticolA	ISO14443A Anti-collision
0x05	SelectA	ISO14443A Select
0x06	HaltA	ISO14443A Halt
ISO14443B Command (0x09 – 0x0E)		
0x09	Request_B	ISO14443B REQB Command
0x0A	AnticolB	ISO14443B Anti-collision
0x0B	Attrib_B	ISO14443B ATTRIB Command
0x0C	Rst_TypeB	Integration of REQB and ATTRIB Command
0x0D	ISO14443_TypeB_ Tranfer_Command	ISO14443-4 command transparent Type B Card
Mifare Application Command (0x20 – 0x2F)		
0x20	MF_Read	Command Read integrates low level commands (request, anti-collision, select, authentication, write) to achieve write operations with a one-step command.
0x21	MF_Write	Command Write integrates low level commands (request, anti-collision, select, authentication, write) to achieve write operations with a one-step command.
0x22	MF_InitVal	The initialization command integrates the low level command (request, anti-collision, select, authentication, write) to achieve the write operation with a one-step command.
0x23	MF_Decrement	Command Decrement integrates low level commands (request, anti-collision, select, authentication, write) to achieve write operations with a one-step command.
0x24	MF_Increment	Command Increments integrate low level commands (request, anti-collision, select, authentication, write) to achieve write operations with a one-step command.

From these results it can be seen that the NFC card, especially the Mifare type used in this trial has a certain structure. The application must be able to recognize the card to be able to read and write in it. From the pilot that has been done, the application can recognize the card and read many cards in a sequential way.

The result of the research can furtherly developed to create a system where many readers and cards that communicate do not collide with one another.

5. Conclusion

The test results show that the NFC card has its own structure. The reader must be able to structure the card to be able to read and write on the card. A lot of cards can be read by one customer sequentially.

This research can be developed to create a system where many reader environments and many cards communicate do not collide with one another. Safe communication in any situation can also be developed here.

Reference

[1] Chao-Hsi Huang, Shao-Liang Chang, **Study on the Feasibility of NFC P2P Communication for Nursing Care Daily Work**, Journal of Computers Vol.24, No.2, July 2013

[2] Bankar Kartik, Joshi Bhargav, Mungal Mahajan, Subhash Rathod, **NFC Based Android API Healthcare System,** International Journal of Inventive Engineering and Sciences (IJIES) ISSN: 2319–9598, Volume-3 Issue-4, March 2015.

[3] Philipp MENG, Karsten FEHRE, Andrea RAPPELSBERGER, and Klaus-Peter ADLASSNIG, **Framework for Near-Field-Communication-Based Geo-Localization and Personalization for Android-Based Smartphones—Application in Hospital Environments.** *This article is published online with Open Access by IOS Press and distributed under the terms of the Creative Commons Attribution Non-Commercial License, 2014.*

[4] Devendran, R. Jayam and P. Sindhuja, **Electronic Medical Records Using NFC Technology**, ARPN Journal of Engineering and Applied Sciences, Vol. 10, No. 3, March 2015.

[5] Vedat Coskun · Busra Ozdenizci · Kerem, **A Survey on Near Field Communication (NFC) Technology**, 2014.

[6] *Erick Macias and Josh Wyatt*, **NFC Active and Passive Peer-to-Peer Communication Using the TRF7970A,** Texas Instruments Incorporated, 2014.

[7] Shreya Kumar, Uma Mounika K., Kavya Kumar, **Peer-to-Peer Acoustic Near Field Communication.** *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 9, Issue 2, Ver. VIII (Mar - Apr. 2014), PP 06-10*

[8] *Erick Macias, Ralph Jacobi, and Josh Wyatt*, **NFC Card Emulation Using the TRF7970A,** Texas Instruments Incorporated, 2014.

[9] *Devendran, R. Jayam and P. Sindhuja*, **ELECTRONIC MEDICAL RECORDS USING NFC TECHNOLOGY.** ARPN Journal of Engineering and Applied Sciences VOL. 10, NO. 3, MARCH 2015 ISSN 1819-6608.

[10] *Deesha Vora , Amarja Adgoankar , 3Anil Chaturvedi*, **Mobile Health Monitoring Privacy System based on Cloud** *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*. Volume 4, Issue 6, June 2015 ISSN 2319 – 4847.

[11] *Mehmet Hilal Ozcanhan, Gokan Dalkilic, Semih Utku*, **CRIPTOGRAPHICALLY SUPPORTED NFC TAGS IN MEDICATION FOR BETTER INPATIENT SAFETY**, *Jmet Syst (2014) 38:61*.

[12] NFC Forum Inc., "NFC Digital Protocol Technical Specification NFC Forum TM," *Technology*, 2010.