JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

NFC Type-A Technology

[1]Shrutha K V, [2]Dr. S G Srivani

[1] PG Student, [2]Professor and Associate PG Dean
[1]Electrical and Electronics Engineering,
[1]RV College of Engineering, Bangalore, India

Abstract : Near Field Communication (NFC) is a minuscule wireless networking technology that ease making transactions, contact free payments, switching digital content, and connecting in a single tap to electronic devices. World has millions of contactless cards and readers, NFC is compatible with those all. NFC transmits data employing radio waves in the analogously as Bluetooth. NFC will make use of RFID (Radio-frequency identification) technology postulation that depend on electromagnetic induction to transport data. NFC operates at a frequency of 13.56 megahertz, with data transmission rates of 106, 212, or 424 kilobits per second**.** NFC Type A uses Miller encoding. NFC permits two way interactivity between electronic gadgets with additional security and intelligibility. Transmission protocol initialization and anticollision sequence have notable value in the Contactless Interface. The main motivation to take advantage of contactless solutions is the speed, which is on the whole appealing for low-value transactions in retail environments.

***IndexTerms* – NFC, Anticollision.**

I. Introduction

NFC is a present day, minuscule wireless connectivity technology that grew from a combination of contactless identification and interconnection technologies. Sony and NXP Semiconductors (formerly Philips) jointly developed it. NFC is delineate to permit the exchange of various types of information, such as telephone numbers, MP3 files, pictures or digital authorizations between two NFC enabled devices like mobile phones, or between an NFC enabled mobile phone and compatible RFID (Radiofrequency identification**)** chip card or reader that are bear respectively. NFC is deliberated to be used as an access key to contents and services alike cashless payment and access control. NFC is grounded on inductive-coupling. NFC employs magnetic induction betwixt two loop antennas placed within each other's near field. NFC operates at 13.56 MHz and provides a data transmission rate of 106 kbit/s - 848 kbit/s within a distance of approximately 11 cm. NFC uses initiator and at the minimum one target device; the initiator diligently generates RF field that will power a passive target also called as a tag[1].

NFC is backward compatible with the Smart Card infrastructure based on ISO/IEC 14443 standard for proximity contactless smart cards as well as with the Sony FeliCa card standards. For the interchange of information betwixt two NFC devices, a new protocol evolved and defined in the ECMA-340 and ISO/IEC 18092 standards. NFC is extensively used across the globe for minuscule range communication with the application of low data rate. There are numerous modes, NFC compliant devices communicates. There are various types of NFC tags progressed for numerous applications as shown in the figure1.1. To communicate signaling protocol has to exits. The signaling protocol provides two devices to communicate and exchange information. There are three signaling modes in NFC referred as Type-A, Type-B and Type-F[3].

II. NFC - Technology

NFC is based on inductive-coupling. NFC tasks using magnetic induction between two loop antennas finded within each other's near field. NFC operates at 13.56 MHz and provides a data transmission rate of 106 kbit/s - 848 kbit/s within a distance of approximately 11 cm. NFC has two modes of operation mainly,

- Active mode: In Active mode of communication, both devices with NFC chip generates an electromagnetic field and exchange data.
- Passive mode: In Passive mode of communication, there is only one active device and the other uses that filed to exchange information.

In addition to mode of operation, there are three communication modes in NFC:

1. Reader/Writer mode: The NFC device performs as a reader for NFC tags, that is to say contactless smart cards and RFID tags. It discovers out a tag right away in close proximity by making use of the collision evasion mechanism. An application on an NFC device can read data and write to the detected tag using the read/write mode operations[2]. The reader/writer mode is regarding the communication of an NFC enabled mobile phone with an NFC tag for the intention of either reading or writing data to those tags. It inter defines two different modes: reader mode and writer mode.

2. Peer to Peer mode: Peer-to-peer mode authorizes two NFC enabled mobile devices to exchange information like a text message, or any other kind of data. Peer to Peer has two standardized options; NFCIP-1 and LLCP. NFCIP-1 takes upper hand of the initiator target paradigm where initiator and the target devices are described prior to begin the communication. But, In LLCP communication the devices are identical. The decision are made by the application which is running in the application layer is after the initial handshake[2]. To power the embedded mobile phones, both devices should be in active mode through the communication in peer-to-peer mode. Datas are dispatched over a bidirectional half duplex channel, where one device will transmitting, the other one will listen and it starts to transmit data once the first finishes.

3. Card Emulation mode: Card emulation mode supplies the chance for NFC enabled mobile device to operate as a contactless smart card. Mobile devices can store various contactless smart card applications inside the smart card. The supreme examples are credit card, loyalty card, debit card, transport cards and access cards. Card emulation mode removes the need of carrying the cards. One can anticipate that in the near future people might carry NFC enabled phones not to gain mobility but to carry out daily functions. All credit cards, tickets, keys and so on will be possibly embedded on mobile phones. Therefore, there will be enough opportunities to integrate everyday objects into NFC enabled phones in the future.

III. NFC TYPE A

NFC communication technology uses distinct coding for signaling and load modulation. Communication protocol used is compliant to the ISO/IEC 14443 Type A standard. Configuration between Proximity Coupling Device(PCD) and Proximity Card or Object(PICC) is shown in the figure 1.

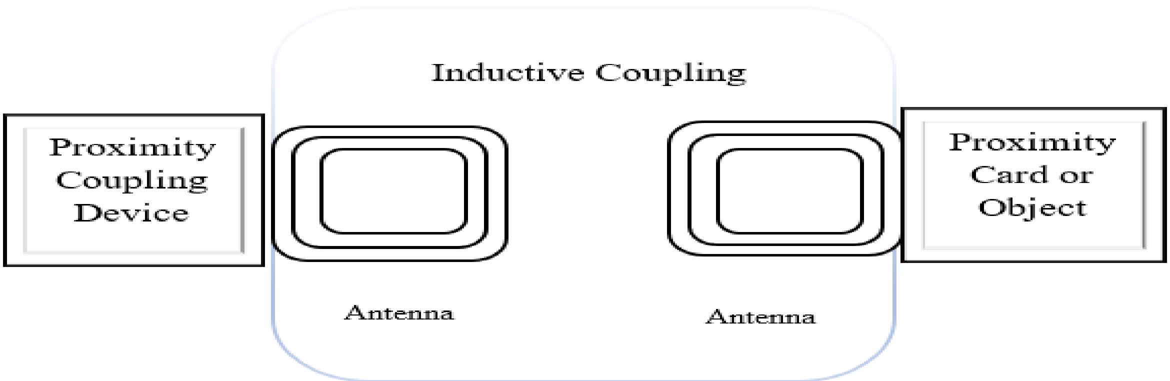

Fig.1 Proximity coupling device and proximity card or object configuration

Following are the Initial dialogue for proximity cards:

- activation of the PICC by the RF of the PCD
- the PICC will wait for a command from the PCD
- command transmission by the PCD
- command transmission by the PICC

The PCD will produce a high frequency magnetic field. This field inductively couples with PICC to transfer power and it is modulated to communication. The frequency of the RF will be 13.56 MHz ±7 kHz. The PCD modulates the amplitude of magnetic field with the modulation pulses to transmit data from the PCD to the PICC. PICC loads magnetic field with a modulated subcarrier signal in order to transmit data from the PICC to the PCD. NFC uses 100% ASK modulation principle to the RF field. Carrier frequency of 13.56MHz. Communication between PCD and PICC can be accomplished with four different bit rates. Bit rates of fc / 64, fc / 32 and fc / 16 are optional and might be independently reinforced by PCD and PICC in each direction communication[4].

PCD frame:

- start of PCD communication
- information
- error detection by the PCD
- end of communication of PCD

PICC frame:

- start of PICC communication
- information
- error detection by the PICC

- end of communication of PICC

There should be minimum frame delay between PCD to PICC and PICC to PCD

The figure 2 specifies all possible state transitions.

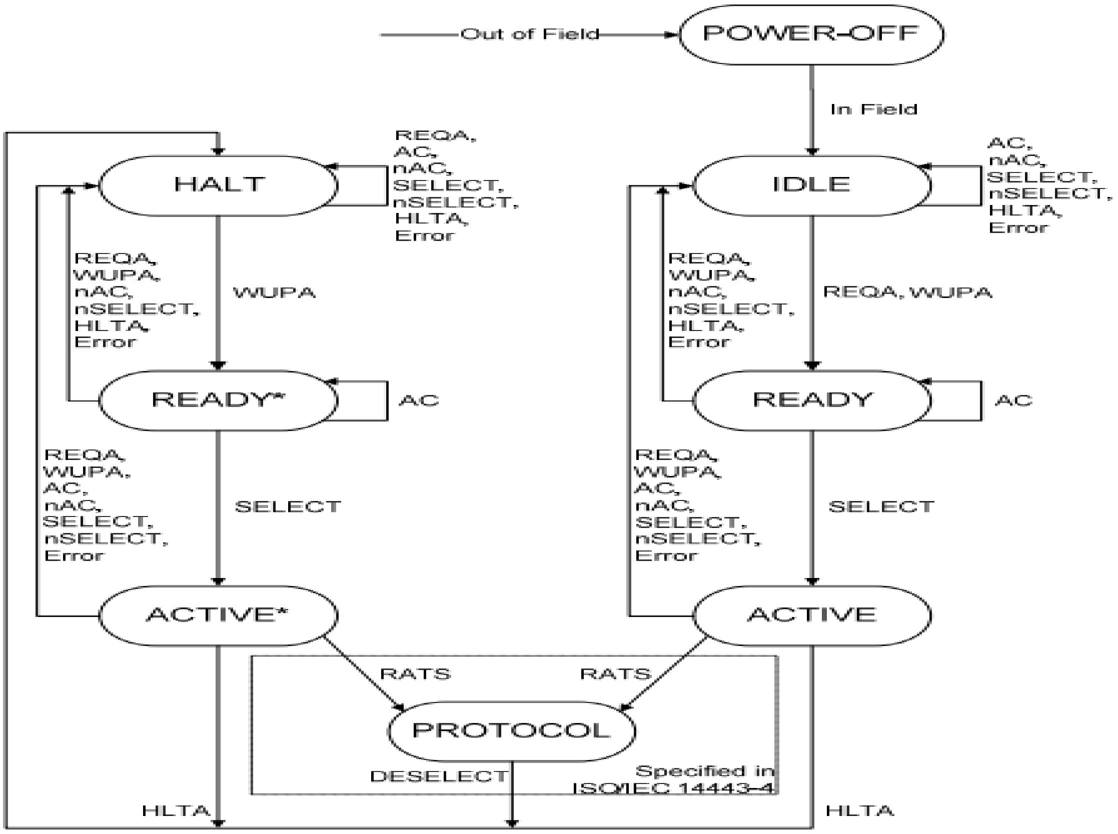

Fig.2 PICC State Diagram

The following symbols apply for the above state diagram:

AC →ANTICOLLISION command (matched UID)
nAC →ANTICOLLISION command (not matched UID)
SELECT →SELECT command (matched UID)
nSELECT →SELECT command (not matched UID)
RATS → RATS command
DESELECT →DESELECT command
Error →transmission error detected or unexpected frame

Following are the states;

1. POWER-OFF state:
In the POWER-OFF state, the PICC is unpowered by operating field of PCD.

2. IDLE state:
In the IDLE state, PICC is powered. PICC will listen to commands and it will recognize WUPA and REQA commands.

3. READY state:
In the READY state, the bit frame of anticollision method is applied. Cascade levels are controlled inside READY state to get the entire UID.

4. ACTIVE state:
If the PICC complies with ISO/IEC 14443-4 then the PICC should be get ready to accept the protocol activation command that is RATS which is specified in ISO/IEC 14443-4, otherwise it may continue with non ISO/IEC 14443-4 protocol.

5. HALT state:
In the HALT state, PICC should respond only to WUPA command. The PICC set into the READY* state after it received a correct WUPA command and ATQA transmitted.

6. READY* state:
The READY* is alike to the READY state. The differences are specified in Figure 2. The bit frame of anticollision method is applied. Cascade levels are handled inside to known UID.

7. ACTIVE* state:
The ACTIVE* is alike to the ACTIVE state. The differences are specified in Figure 2. If the PICC complies with ISO/IEC 14443-4 then the PICC should be ready to accept the protocol activation command that is RATS which is specified in ISO/IEC 14443-4, otherwise it may continue with non ISO/IEC 14443-4 protocol.

8. PROTOCOL state:
In the PROTOCOL state the PICC behaves according to the ISO/IEC 14443-4.

IV. Anticollision Algorithm

The following algorithm shall apply to the anticollision loop as shown in the figure 3:

Step 1:
The PCD should assign SEL to the code for the chosen anticollision level.

Step 2:
The PCD should assign NVB to the value of '20'. ‘20’ defines that the PCD will transmit no devision of UID CL*n*. Therefore, this command forces PICCs in the region to respond with entire UID CL*n*.

Step 3:
The PCD should transmit SEL and NVB.

Step 4:
All PICCs in the region should respond with their entire UID CL*n*.

Step 5:
A collision will occur, if more than one PICC responds. Steps 6 to 10 should be skipped, if no collision.

Step 6:
The PCD should recognize the first collision position.

Step 7:
The PCD should assign NVB with a valid bits of UID CL*n*. The valid bits should be part of the UID CL*n* which was received before a collision followed by a (0)b or (1)b. A implementation adds (1)b.

Step 8:
The PCD should transmit NVB and SEL, followed by valid bits.

Step 9:
Only PICCs part of UID CL*n* is equal to the valid bits transmitted by the PCD. It should transmit their UID CL*n* remaining bits.

Step 10:
If additional collisions occur, steps 6 to 9 should be repeated. 32 is the maximum number of loops.

Step 11:
If no collision occurs further, the PCD should assign ‘70’ to the NVB. This value tells that the PCD will transmit the entire UID CL*n*.

Step 12:
The PCD should transmit NVB and SEL, followed by UID CL*n* 40 bits followed by CRC_A.

Step 13:
The PICCs which UID CL*n* matches the 40 bits should respond with their SAK.

No need of performing the anticollision loop if the UID of a PICC is complete and known by the PCD[5].

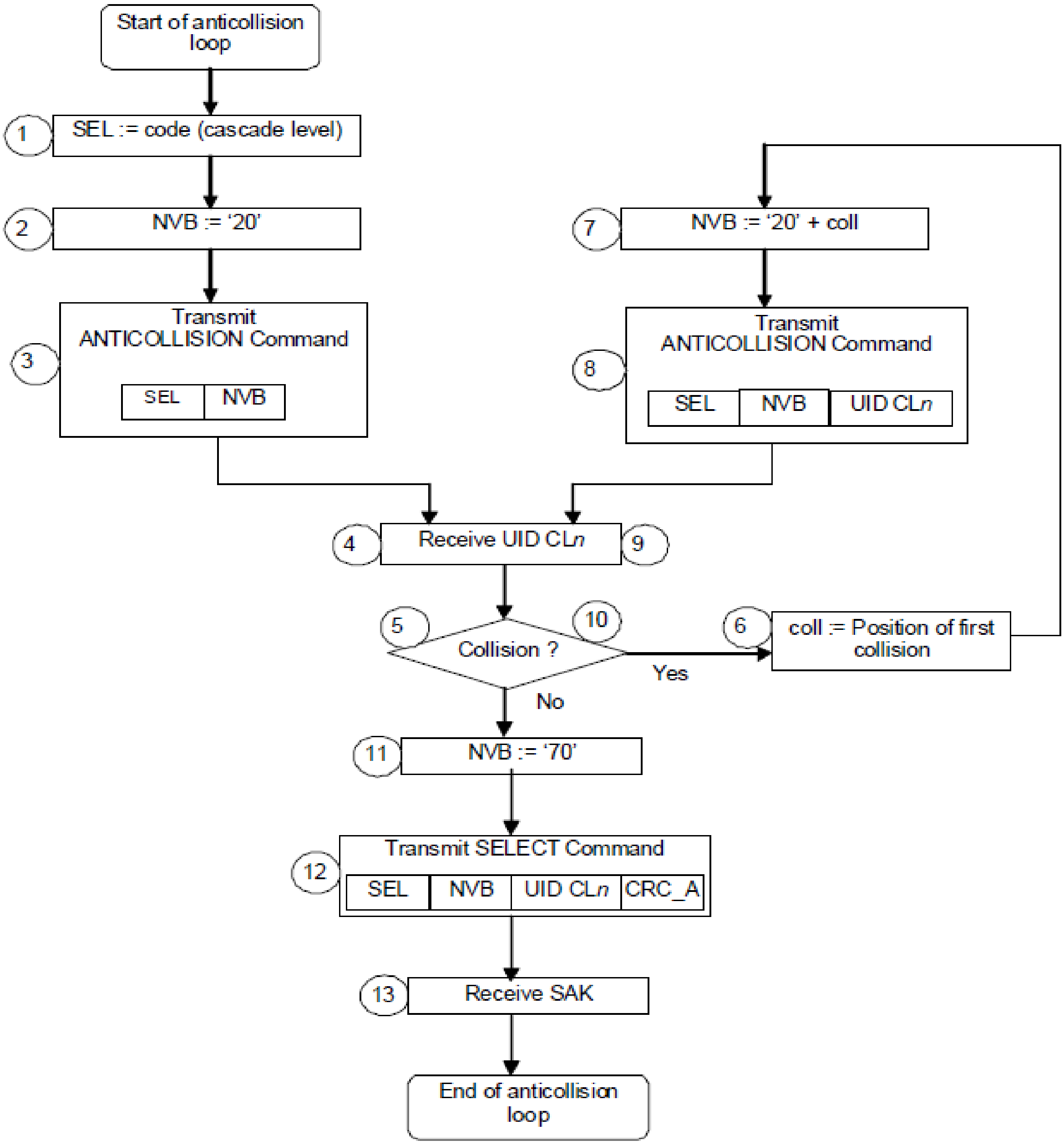

Fig.3 Anticollision loop

V. CONCLUSION

NFC would permit all the users to make payments straightforwardly by tapping their mobile phones with reader like debit card or credit card transactions. Numerous banks, mobile operators and companies are implementing NFC technology. NFC compliant to the ISO/IEC 14443 Type A standard results in NFC Type A and it undergoes anticollision to avoid uncertainty during multiple cards.

REFERENCES

[1] M. S. Chishti, C. T. King and A. Banerjee, "Exploring Half-Duplex Communication of NFC Read/Write Mode for Secure Multi-Factor Authentication," 2021 in IEEE Access, vol. 9, New Delhi, pp. 6344-6357, doi: 10.1109/ACCESS.2020.3048711.

[2] Bhoomika. P, Tabitha Janumala, "Operating Modes of Near Field Communication" , Research article in 2020, vol. 10, Bangalore, ISSN 2321 3361 2020 IJESC

[3] A. Albattah, Y. Alghofaili and S. Elkhediri, "NFC Technology: Assessment Effective of Security towards Protecting NFC Devices & Services," 2020 International Conference on Computing and Information Technology (ICCIT-1441), 2020, Tabuk, Saudi Arabia pp. 1-5, doi: 10.1109/ICCIT-144147971.2020.9213758.

[4] Cards — Contactless integrated circuit cards — Proximity cards — Part 3: Initialization and anticollision ISO/IEC 14443-3:2016 Identification

[5] Cards and security devices for personal identification — Contactless proximity objects — Part 4: Transmission protocol ISO/IEC 14443-4:2018