Using RFID Techniques for a Universal Identification Device

Roman Zharinov, Ulia Trifonova, Alexey Gorin
Saint-Petersburg State University of Aerospace Instrumentation
Saint-Petersburg, Russia
{roman, ulia}@vu.spb.ru, lex_93@bk.ru

Abstract

Radio-frequency identification (RFID) is a radio wave technology that uses to transfer data from a tag (also called RFID-tag or label), attached to an object, through a reader for the purpose of identifying the object. RFID technologies are widely deployed by various organizations as part of their authorization part of the systems. An RFID based system consists of two main parts which include: the hardware and the software. The hardware consists of the motor unit and the RFID reader. The software consists of security protocols for authorization and transfers the data. In this article we'll try to find basic techniques for creating a universal identification device.

Index Terms: RFID, NFC, Universal identification, Android.

I. Introduction

The rapid development of wireless Radio-frequency identification (RFID) technologies causes them to active use in various fields of modern life. The number of devices that are used to identify objects is growing very fast. That fact implies need for a universal identification device, in which can act as a symbiosis of modern smartphone and external RFID device for read and imitate RFID-tag. This device should have wireless communication such as WiFi or Bluetooth. Development of such a device will significantly simplify using and storage of identity data of various services. Final stage of project is developing software for smartphones based on operating system Android.

II. Main part

In this article we describe main information about RFID technologies, NFC as the part of it and main standards which use those technologies.

A. RFID technologies

Radio-frequency identification (RFID) [1] is the use of a wireless non-contact system that uses radio-frequency electromagnetic fields to transfer data from a tag attached to an object, for the purposes of automatic identification and tracking. Some tags require no battery and are powered and read at short ranges via magnetic fields (electromagnetic induction). Others use a local power source and emit radio waves (electromagnetic radiation at radio frequencies). The tag contains electronically stored information which may be read from up to several meters away. Unlike a bar code, the tag does not need to be within line of sight of the reader and may be embedded in the tracked object.

A radio-frequency identification system uses tags, or labels attached to the objects to be identified. Two-way radio transmitter-receivers called interrogators or readers send a signal to the tag and read its response. The readers generally transmit their observations to a computer system running RFID software or RFID middleware.

RFID tags can be either passive, active or battery assisted passive. An active tag has an on-board battery and periodically transmits its ID signal. A battery assisted passive (BAP) has a small battery on board and is activated when in the presence of a RFID reader. A passive tag is cheaper and smaller because it has no battery. Instead, the tag uses the radio energy transmitted by the reader as its energy source. The interrogator must be close for RF field to be strong enough to transfer sufficient power to the tag. Since tags have individual serial numbers, the RFID system design can discriminate several tags that might be within the range of the RFID reader and read them simultaneously [2].

Tags may either be read-only, having a factory-assigned serial number that is used as a key into a database, or may be read/write, where object-specific data can be written into the tag by the system user. Field programmable tags may be write-once, read-multiple; "blank" tags may be written with an electronic product code by the user.

Low-frequency RFID systems (30 KHz to 500 KHz) have short transmission ranges (generally less than 180 cm). High-frequency RFID systems (850 MHz to 950 MHz and 2.4 GHz to 2.5 GHz) offer longer transmission ranges (more than 3 meters). In general, the higher the frequency the more expensive the system.

1) ISO/IEC 14443 Identification cards: Proximity cards are an international standard that defines proximity cards used for identification, and the transmission protocols for communicating with it. The main consumers of proximity card are banking and access control systems. Standard defines all parameters of cards from the physical characteristics to frequency or radio parameters, through which the data is read from and written to the memory card in it.

The transmission protocol specifies data block exchange and related mechanisms [3]:

- Data block chaining.
- Waiting time extension.
- Multi-activation.

ISO/IEC 14443 uses following terms for components:

- PCD: proximity coupling device (the card reader).
- PICC: proximity integrated circuit card.
- UID: Unique Identification.
- Cascade level n, $3 \geq n \geq 1$.

The general scheme of the card according to this standart is presented on Fig. 1. There are 8 general state of the card [1]:

- POWER-OFF state. In this state, the PICC is not energized due to lack of carrier energy and shall not emit subcarrier.
- IDLE state. After the field has been active, the PICC shall enter its IDLE state. In this state, the PICC is powered on, and is capable of demodulating and recognizing valid REQA and WAKE-UP Commands from the PCD.
- READY state. This state is entered as soon as a valid REQA or WAKE-UP message has been received and exited when the PICC is selected with its UID. In this state either the bit frame anticollision or other optional anticollision method can be applied. Cascade levels are handled inside this state to get all UID CLn.
- ACTIVE state. This state is entered by selecting the PICC with its complete UID.
- HALT state. This state is entered by either the HALT Command defined in or by an application specific command not defined in this part of ISO/IEC 14443. In this state a

PICC shall respond only to a WAKE-UP Command, which transits the PICC to its READY State.

- REQA Command. The REQA Command is sent by the PCD to probe the field for PICCs of Type A.
- WAKE-UP Command. The WAKE-UP Command is sent by the PCD to put PICCs which have entered the HALT State back into the READY State. They shall then participate in further anticollision and selection procedures.
- ANTICOLLISION Command, SELECT Command. These commands are used during an anticollision loop.

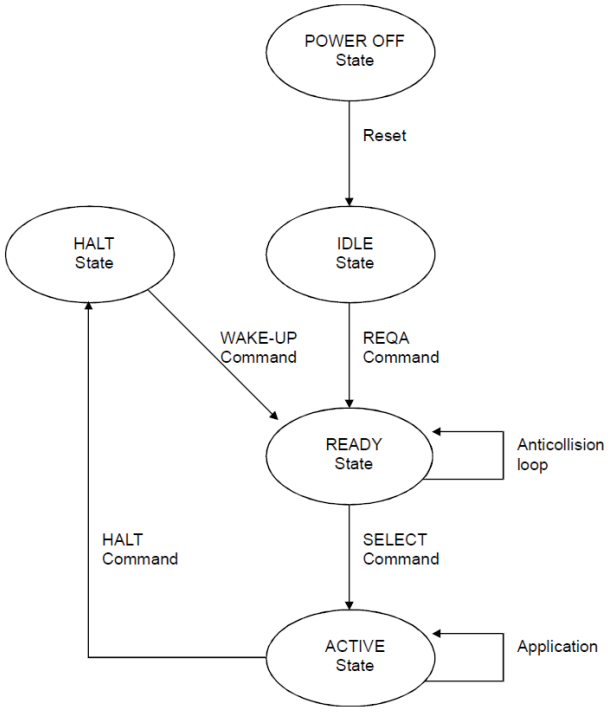

Fig. 1. The general scheme of the card according to ISO/IEC 14443

2) ISO/IEC 15693 Standard for non-contact smart payment and credit cards: This is an ISO standard for cards which can be read from a greater distance as compared to proximity cards. This standard is widely supported by the industry. In addition to the smart card, it corresponds to many transponders with a frequency of 13.56 MHz, which are assessed in the logistics industry and other fields. Widespread smart labels, disk labels, tags, key chains, based on the standard chips. In fact, ISO/IEC 15693 is the most popular standard for RFID with an operating frequency of 13.56 MHz.

B. NFC

Near Field Communication (NFC) is a technology for wireless short range, which enables the exchange of data between devices at a distance of about 10 centimeters [4]. This technology - a simple extension of the standard contactless cards (ISO 14443), which includes an interface smart card and reader into a single device. NFC device can

communicate with existing smart cards and readers of ISO 14443, and other devices with NFC, and thus compatible with the existing infrastructure of contactless cards already used in public transportation and payment systems. NFC is aimed primarily for use in smartphones. In this standard three different bit rates are defined: 106, 212 or 424 Kbit/s. Depending on the bit rate, different modulation and encoding schemes are used.

NFC has led to three basic modes of operation for NFC devices:

- Card Emulation Mode: The NFC device acts like a normal passive con- tactless card, emulating a smart card. The device is passive so it does not generate a RF field.
- Reader/Writer Mode: The NFC device acts like a normal active con- tactless card reader. It can then generate RF fields to communicate with contactless cards, RFID tags or NFC.
- Peer to Peer Mode: Two NFC devices can communicate together in both active and passive NFC mode. According to the master/slave principle, the initiator or master initiates a data transfer and waits for the target or slave to respond.

1) NFC Data Exchange Format: The NFC Data Exchange Format (NDEF) specification is a common data format for NFC Forum Devices and NFC Forum Tags. If the device is in the RF field of another device, it will work as a label; otherwise it will include its own field and work as a reader. When working as a reading device, the device will scan the environment for RF field and when entering the ranges switch to a label mode.

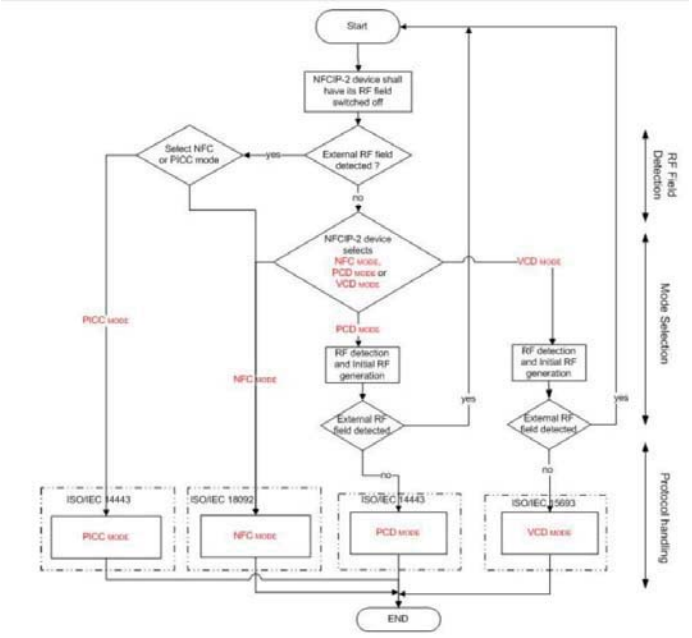

Fig. 2. NFC-device algorithm

General abbreviations of Fig. 2:

- NFC MODE - mode in which NFCIP-2 device operates as specified in ECMA-340.
- PICC - Proximity Integrated Circuit Card or Object as specified in ISO/IEC 14443.
- PICC MODE - mode in which NFCIP-2 device operates as PICC as specified in ISO/IEC 14443.

- PCD - Proximity Coupling Device as specified in ISO/IEC 14443.
- PCD MODE - mode in which NFCIP-2 device operates as PCD as specified in ISO/IEC 14443.
- VCD - Vicinity Coupling Device as specified in ISO/IEC15693.
- VCD MODE - mode in which NFCIP-2 device operates as VCD as specified in ISO/IEC 15693.

C. External devices

At the first stage we are limited to using a modern smartphone with a built-in NFC technology. Because, as described in section NFC, it can work with one of the popular standards for proximity cards (which widely using for authorization and a little more).

D. Getting dump of card's structure

In order to read data from the smartcard we need to get the authorization keys. As described in [5] there are four weeks in construction of the Mifare type. The MIFARE Classic card is used in physical access control systems (PACS) and contact less payment systems (including tollway and public transportation systems). Mifare Classic is a inexpensive, entry-level chip, based on ISO/IEC 14443 Type A, 1kB or 4kB. Uses 13.56 Mhz contactless smartcard standard, proprietary CRYPTO1 with 48 bits keys. There is no protection against cloning or modifications.

In distribution BackTrack [6] there are a lot of utilities which can restore keys to the sectors of Mifare Classic cards. Mifare Classic Offline Cracker (MFOC) [7] is one of them and it can compute all keys to all sectors, providing at least one of the keys is already known. Keys file is the file, where MFOC will store "forgotten" keys.

First of all we want porting this utility of penetration test to OS Android for creating dump of getting card.

III. Conclusion

In this article we describe main technologies and standards which using at radio-frequency identification smartcards.

Nowadays smartphones have the capability to do real calculation (cryptography in particular), so there's potential to build software, to combine a lot of smartcards into one mobile device.

References

[1] MIKE BURMESTER. Universally Composable RFID Identification and Authentication Protocols, Web: http://www.cs.fsu.edu/~burmeste/408.pdf.

[2] Ononiwu G. Chiagozie. Okorafor G. Nwaji. *RADIO FREQUENCY IDENTIFICATION (RFID) BASED ATTENDANCE SYSTEM WITH AUTOMATIC DOOR UNIT*. Academic Research International Web: http://www.savap.org.pk/journals/ARInt./Vol.2(2)/2012(2.2-18).pdf.

[3] ISO/IEC FCD 14443-3. Web: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50942.

[4] Brad Molen, *Engadget Primed: What is NFC, and why do we care?*, Web: http://www.engadget.com/2011/06/10/engadget-primed-what-is-nfc-and-why-do-we-care/.

[5] Roman Zharinov, Ulia Trifonova. «The Authentication Module Using Existing Infrastructure of Smart Cards in the Personified System for Information Filtering», *FRUCT13*.

[6] BackTrack Linux. Web: http://www.backtrack-linux.org/.

[7] RFID Cooking with Mifare Classic. Web: http://www.backtrack-linux.org/wiki/index.php/RFID_Cooking_with_Mifare_Classic.