Middle-East Journal of Scientific Research 21 (7): 1130-1135, 2014
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2014.21.07.21578

Access Control and Management System Based on NFC-Technology by the Use of Smart Phones as Keys

[1]Nurbek Saparkhojayev, [2]Aybek Nurtayev and [3]Gulnaz Baimenshina

[1]Department of Electronics and Telecommunications, POLITO, Torino, Italy
[2]Masters Student, International IT University, Almaty, Kazakhstan
[3]Department of Applied Physics, K.I. Satpayev Kazakh National Technical University, Almaty, Kazakhstan

Abstract: In today's world, we always carry all sorts of keys (house keys, garage keys, office keys, car keys) and/or pass cards. Furthermore, we keep all of them in our pockets or wallets; they occupy a lot of space and weigh a lot. In addition to this, we carry gadgets (smart phones, tablets, smart watches, etc.) which are essential in today's life. After thinking all this, authors came up to the idea of replacing usual keys by smartphones to use for opening/closing and locking/unlocking doors. Smartphones have already been used as payment smart cards. Most of the modern mobile devices are equipped with NFC module and by using such devices, it is possible to get rid of carrying heavy, metal keys, pass-cards, etc. People often forget keys at home and they are relatively small and easy to lose. Instead of carrying all these keys, authors of this research paper present an NFC-enabled Access Control and Management System, which by the help of mobile devices, NFC technology and HCE mode, introduced in Android 4.4, makes possible for people to use only one single key. To emulate a smart card and the data exchange between the mobile device and NFC-reader, ISO 7816-4 smart card standard is used.

Key words: NFC-technology · Smart phones android · Access control and management system

INTRODUCTION

In today's fast-growing technology world, most of mobile devices are equipped with wireless modules, which can be used to solve the problems with keys. Almost all of them are equipped with Bluetooth and infrared, latest ones also have NFC on board. Compared to other short-range technologies, NFC has the following advantages:

- Slow speed and short range – this allows NFC to consume as little power as possible so it can be left on at all times and not affect the phone's battery by that much (vs. Bluetooth);
- Hassle-free approach to connections – with NFC, bringing the two devices within range is enough to facilitate the communication between the two (vs. Bluetooth);
- Free-line of sight – no direct line of sight is required to establishes connection (vs. Infrared) [1].

NFC-enabled Access Control System will let people lock/unlock doors just by tapping mobile device to NFC reader. It will also perform all the functionality that other ACMS's do, such as logging entrance time, controlling access privileges, etc. This system can be applied as:

- Independent and complete ACMS (Access Control and Management System);
- The system for checking attendance of students in educational institutions, as well as observation of student location within the institution;
- Small ACMS for home, as an addition to "smart house" system.

NFC is one of the popular latest wireless communication technologies. With NFC technology, communication occurs when an NFC-compatible device is brought within a few centimeters of another NFC device or an NFC tag. The big advantage of the short transmission range is that it inhibits eavesdropping on

Corresponding Author: Nurbek Saparkhojayev, Department of Electronics and Telecommunications, POLITO, Torino, Italy.

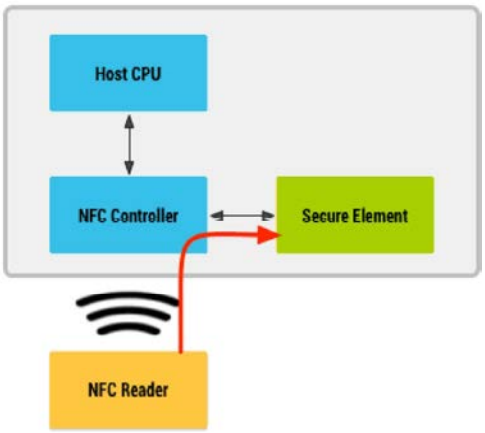

Fig. 1: NFC card emulation using a secure element (Before HCE was introduced)

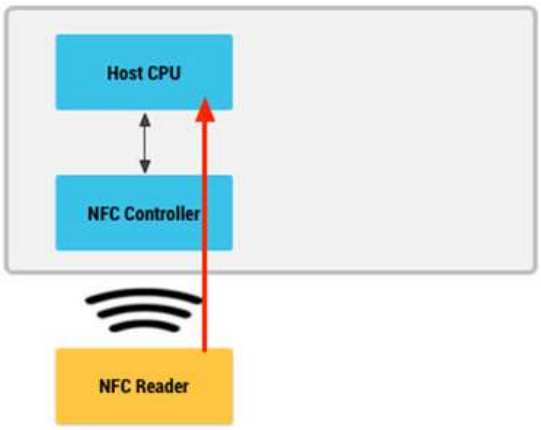

Fig. 2: NFC card emulation without secure element (after HCE was introduced)

NFC-enabled transactions. NFC technology opens up exciting new usage scenarios for mobile devices [2]. Until recently, payments using smart phones were possible using NFC card emulation combined with secure element (Fig. 1). Traditionally, you would have to store security information, for example the security keys from a debit card (which are stored in the tamper resistant card chip) in a similarly tamper resistant chip on your device – the Secure Element. The Secure Element emulates the card and can be found either on the SIM card or in a chip embedded in the phone handset. When NFC card emulation is provided using a secure element, the card to be emulated is provisioned into the secure element on the device through an application. Then, when the user holds the device over an NFC terminal, the NFC controller in the device routes all data from the reader directly to the secure element [3].

In general, the SIM is controlled by the mobile operator and the embedded chip by the handset manufacturer. This creates difficulties for both the application developer and the end user, since the developer will need to negotiate with the service provider or device manufacturer and the user needs to change the SIM card or device, if he/she wants to take advantage of the services offered [3].

Android 4.4 introduced an additional method of card emulation that does not involve a secure element, called host-based card emulation (Fig.2). This allows any Android application to emulate a card and talk directly to the NFC reader. When an NFC card is emulated using host-based card emulation, the data is routed to the host CPU on which Android applications is running directly, instead of routing the NFC protocol frames to a secure element [4].

Motivation: There were some research done in previous years for implementing the attendance control systems in universities. Authors of [5] research work used RFID-technology as an automatic monitor of student classroom attendance. They demonstrated how to automate an entire student-attendance registration system within an educational institution by the use of Ethernet. However, there were some other research work done with different views for attendance checking system. In [6], authors designed and implemented wireless iris recognition attendance management system, whereas in [7] authors proposed attendance management system extended with computer vision algorithms. And finally, in [8], authors implemented a system for attendance checking based in RFID-technology. In most of this research work, RFID-technology was used a framework for building systems, whereas authors of this research paper presents an NFC-enabled Access Control System, which by the help of mobile devices, NFC technology and HCE mode, introduced in Android 4.4, makes possible for people to use only one single key.

To emulate a smart card and the data exchange between the mobile device and NFC-reader, ISO 7816-4 smart card standard is used. NFC-enabled Access Control System will let people open doors and not only doors, just by tapping mobile device to NFC reader. It will also perform all of the functionality that other ACSs do, such as logging entrance time, controlling access privileges, etc. This system can be applied as:

- Independent and complete ACMS (Access Control and Management System);
- The system for checking attendance of students in educational institutions, as well as observation of student location within the institution;

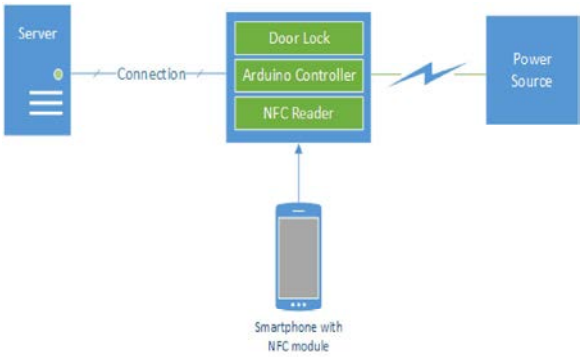

Fig. 3: Components of the system and their relationships

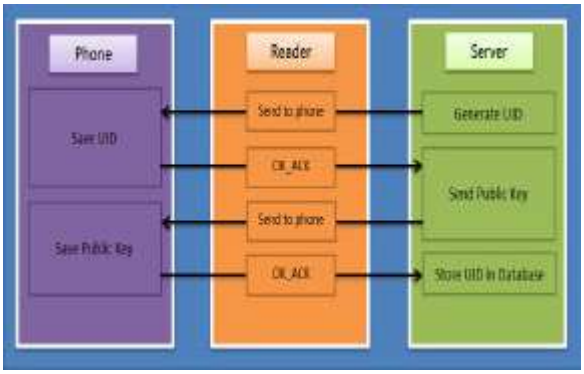

Fig. 4: Scheme of registration phase

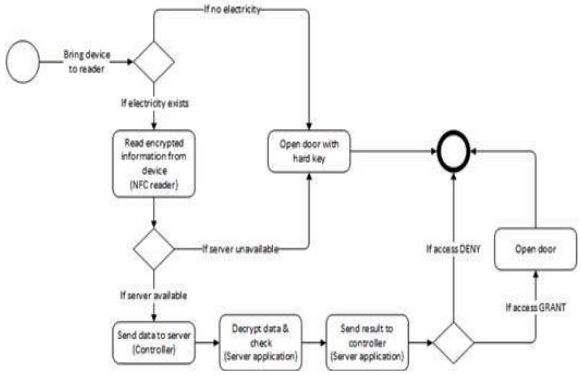

Fig. 5: General workflow of door lock/unlock phase

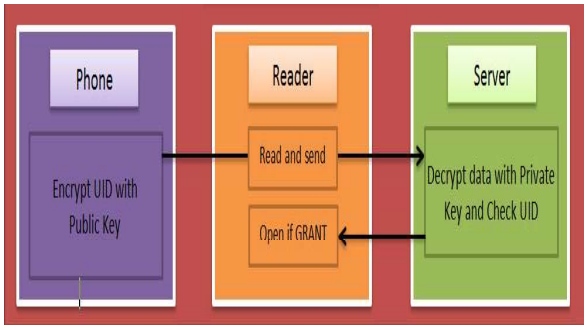

Fig. 6: Scheme of door lock/unlock phase

- Small ACMS for home, as an addition to "smart house" system.

User brings his device to the reader; reader reads the data from device using NFC interface and transmits it to the server for authentication. If authentication succeeds, door will be opened immediately. Mobile device can store a lot of virtual keys from different doors/locks.

System Description: The system consists of following multiple modules:

- Server application;
- NFC reader (connected to controller);
- Controller (microcontroller is connected to the network from one side and to the door lock from the another side);
- Smartphone application, which emulates NFC cards;

The main use of the system is divided into two phases:

- Registration phase;`
- Door lock/unlock phase;

Registration Phase: Prior to the use of mobile devices as keys to lock/unlock door locks, it must be registered in the system. Since this system might be deployed in different places, such as at home, in the offices, or in universities, we have used identification number for distinguishing these systems. Moreover, suppose that any user wants to get access to doors by the help of smart phones. And, before starting any user should register in these systems and get a key (UID) for this specific system. Furthermore, each system has its own identification number (the system-id). To register any device in the system, it must be brought to special registration device. At this point, server generates unique key-identification (the UID) and then sends it to the device, together with public-key of the system (the p-key), which is used to encrypt transmitted data and system-id. If system-id, UID and p-key are successfully received, then server permanently stores UID in database. Now device can be used to lock/unlock the doors.

Door Lock/Unlock Phase: To unlock the door, device must be brought to the reader close enough (approx. 1-2 cm) for the start of data transmission. UID is encrypted with p-key of corresponding system and is sent to the server. At server side, it is validated with data from

database and if there is a presence of such UID in the database, then the command for opening the door is sent back.

Both registration and lock/unlock operations are implemented using the "smart card standard" named ISO 7816-4. This standard specifies:

- The contents of messages, commands and responses transmitted by the interface device to the card and conversely;
- The structure and content of the historical bytes sent by the card during the answer to reset;
- The structure of files and data, as seen at the interface when processing inter-industry commands for interchange;
- Access methods to files and data in the card;
- Methods for secure messaging;
- Access methods to the algorithms processed by the card. It does not describe these algorithms [9].

Data Exchange: There are two different data exchanges that are performed during two different phases: registration and door lock/unlock phases. The first data exchanges at registration phase are performed in 8 consecutive command-response pairs grouped into 2 sub-phases.

Sub-Phase 1: Between Server and Controller data exchange. Data exchange is initiated by server application.

- Server sends "reg" command to controller, performing handshake procedure. Controller responds with ACK_REG_OK acknowledgement.
- Server generates UID and sends it with "uid" command. Controller responds with ACK_UID_OK acknowledgement.
- Server sends systems public key with "key" command. Controller responds with ACK_KEY_OK acknowledgement.
- Server sends "end" command, indicating that data exchange is finished and now UID and key can be transferred to device.

Sub-phase 2: Controller – Device data exchange. Controller waits until device is brought close enough to begin data exchange.

- Controller sends SELECT APDU instruction to start communicating with required AID at device (*Registration AID*). Device responds with 90 00 OK acknowledgement.
- Controller sends WRITE BINARY instruction with UID to device. (P1 = 0x00). Device responds with 90 00 OK acknowledgement.
- Controller sends WRITE BINARY instruction with public key to device. (P1 = 0x01). Device responds with 90 00 OK acknowledgement.

This step continues in loop until public key is completely transferred to device.

- Controller sends WRITE BINARY instruction indicating end of data exchange (P1 = 0x02).

Device Responds with 90 00 Ok Acknowledgement: The latter data exchanges at door lock/unlock phase are always initiated by mobile device and performed in consecutive command-response pairs supplemented with requests to server. Controller always waits device to be brought close enough to begin data exchange.

- Controller sends SELECT APDU instruction to start communicating with required AID at device (*Unlock AID*). Device prepares data to send (encrypts UID with public key). Device responds with 90 00 OK acknowledgement.
- Controller sends READ BINARY instruction to device (P1 = 0x00).
- Device responds with part of encrypted data concatenated with 90 00 OK acknowledgement.
- Controller sends encrypted data to server.

Steps 2-4 are continued in the loop until encrypted data is completely transferred from device to server.

- Server decrypts and validates data. If everything is OK, responds with GRANT command, else responds with DENY command.
- If controller receives GRANT command, signal to unlock the door is sent.

Security Aspects: The UID for device is generated by using KeyGenerator class for AES-256 algorithm. Asymmetric keys are generated automatically one time upon server's first start, but can be regenerated manually from server application. Keys are generated by using RSA algorithm with 1024-bit as the size of the key. In order to prevent man-in-the-middle attack, before sending UID to server, it is concatenated with mobile device's system time and then encrypted with system's public key. At server side, data is decrypted, UID and System time are checked so that difference between device's system time and server's system time is less than 5 second (this

parameter will be configurable at server application). In this way, even if encrypted data is intercepted by attacker, it cannot be reused as it is.

DISCUSSION AND RESULT

Let us now examine how changes in the main control parameter, such as injection strength and detuning frequency affect the system dynamics behavior.

Using the approximate numerical methods, in particular the Runge - Kutta fourth order method, we present the results of numerical solutions of the rate equations (1), (2), (3) and the corresponding phase portraits.

Consider the values of the system parameters $\Omega = -0.1$, $\eta = 0.01$. In this case, the cubic equation (5) has one real root or one equilibrium point of the original differential equations. The solution is unstable, since the real parts of the eigenvalues of a complex - conjugate pair of the characteristic polynomial (13) are positive. The phase space trajectory and time responses confirm these analytical results (Fig. 1) as well.

Raise the value of the injection $\eta = 0.03$. In this case the cubic equation has three real roots. According to the eigenvalues of a polynomial, two equilibrium points are stable whereas the third point is unstable. The saddle-node bifurcation is occurred. The system performs the relaxation oscillations.

Consider the value of the injection force $\eta = 0, 04$. For a given value of the parameter the pair of complex eigenvalues crosses the imaginary axis. There is a qualitative change in the phase portrait. The system goes to the periodical mode. The curve is a limit cycle in the phase space of *R-ø-Z*. The Hopf bifurcation is occurred.

Let us raise the value of the injection to the value $\eta = 0.9$. The detuning parameter is left unchanged. The saddle node bifurcation is occurred for given values of the parameters. The stability of the equilibrium point turns back.

Consider the positive values of the detuning Ω, in particular $\Omega = 0.1$ and $\eta = 0.01$. In this case, the system has one unstable solution. The real parts of the eigenvalues of a complex - conjugate pair of the characteristic polynomial are positive. The time series and phase portraits for positive detuning value are plotted in Fig. 2.

Let us see what happens if we raise the value of $\eta = 0.04$. According to their eigenvalues all three solutions are unstable again. The reason is that in this case, the leading coefficient of characteristic equation for positive values of detuning is always

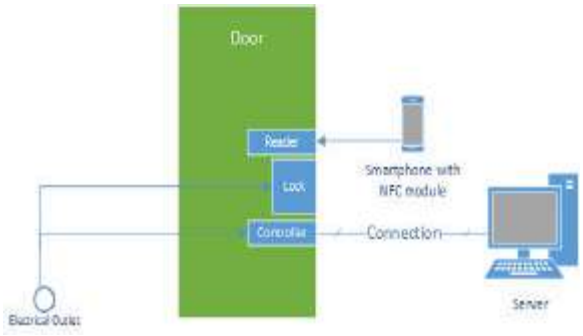

Fig. 7: The overall architecture of access control and management system based on NFC-technology.

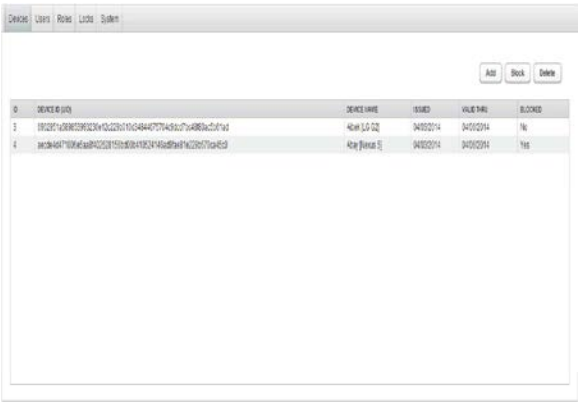

Fig. 8: Devices' panel screenshot

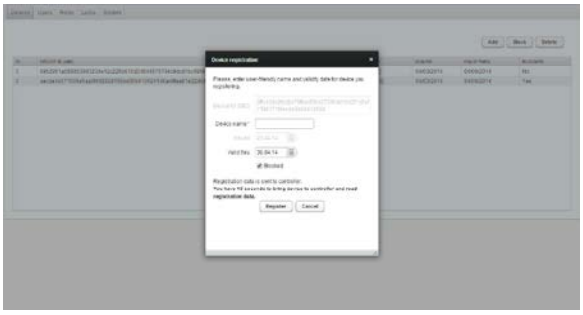

Fig. 9: Devices' registration procedure screenshot

negative. (C_1 =-1.9984 < 0). According to the criterion of Routh – Hurwitz, this condition is not satisfied with the condition of stability of equilibrium point. Thus, the transitions between relaxation and periodic oscillations described in Fig. 2. can occur only for negative detuning values.

CONCLUSION

Access control systems are always in demand and are used everywhere. Reducing the number of physical

keys and cards people need to carry and using smart phone as a single device to access to multiple locations is a good choice against lost, left at home or work keys. In addition, even if smart phone is lost, no need to change the lock at door, just disable or delete lost devices UID, registered in system from centralized DB. In the future, we plan to replace the connection to the wireless connection as well as improve the safety aspects, including replacing system time to something more efficient.

REFERENCE

1. Ben Joan, April 2, 2012. Difference between NFC and Bluetooth". Retrieved from: http://www. difference between. net/technology/hardware-technology/difference-between-nfc-and-bluetooth
2. Dan Nosowitz, January 3, 2011. Everything you need to know about Near Field Communication. Retrieved from Popular Science online web-resource: http://www.popsci.com/gadgets/article/2011-02/near-field-communication-helping-your-smartphone-replace-your-wallet-2010/
3. Consult Hyperion. Host Card Emulation- why it matters". Retrieved from: http://www. chyp. com/assets/uploads/Documents/2013/11/hce.pdf.
4. Host-based card emulation. Retrieved from web-resource for Android-developers: http://developer. android. com/guide/topics/connectivity/nfc/hce.html
5. Silva, F., V. Filipe and A. Pereira, 2008. Automatic control of students' attendance in classrooms using RFID", in 3rd International Conference on Systems and Networks Communication, pp: 384-389.
6. Kadry, S. and M. Smaili, 18 June, 2010. Wireless attendance management system based on iris recognition, Scientific Research and Essays, 5(12): 1428-1435.
7. Shehu, V. and A. Dika, 21-24 June 2010. Using real time computer vision algorithms in automatic attendance management systems, Proceedings of the ITI 2010 32rd International Conference on Information Technology Interfaces, Cavtat, Croatia.
8. Saparkhojayev, Nurbek and Selim Guvercin, 2012. Attendance Control System based on RFID-technology. International Journal of Computer Science Issues (IJCSI) 9(3).
9. ISO 7816- 4: Interindustry Commands for Interchange, sections 5 and 6. Retrieved from the website: http://www.cardwerk. com/smartcards/smartcard_standard_ISO7816-4.aspx.