ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Near Field Communication Detector – A Low Power SOC Implementation

S.P.Venu Madhava Rao
Department of ECE,
Sreenidhi Institute of Science and Technology,
Hyderabad, India.

V.Manogna
Department of ECE,
Sreenidhi Institute of Science and Technology,
Hyderabad, India.

Abstract:

A low power implementation of a Near Field Communication (NFC) detector on a system On Chip is proposed in this paper. The main idea behind this is to migrate the NFC technology from hand held devices like mobile phones to a System On Chip (SOC) to facilitate more number of applications to be developed using a single device. In this paper Raspberry Pi, which is a versatile SOC, is used for the implementation. NFC is an extension of RFID technology and the fundamental principle involved in the operation of NFC is magnetic field induction. A radio communication is established between the two devices by touching them or keeping them in proximity of few centimeters (less than 20cms). The proposed implementation has been successfully done on the target device.

Keywords:

NFC, RFID technology, Raspberry Pi, MFRC522 reader.

I. Introduction:

The world of RFID incorporates numerous gauges that work at low frequencies (LF), high frequencies (HF), and ultra-high frequencies (UHF). Within each of those frequency domains there are many standards, which are incompatible with each and are different. NFC is a subset of these norms working in the HF band at 13.56 MHz under the ISO 14443, ISO 18092, and FeliCa standards. This supports a data rate of 424 Kbits per second (kbps) up to distance of 20 cm. The NFC protocol not only establishes communication between a dynamic (active) reader and an inactive (passive) tag but also additionally takes into consideration peer-to-peer communication between two active readers. Along with this, a NFC proficient gadget can both read a label and transmit information to another NFC empowered gadget. Moreover, labels can contain read/compose memory, and today there are label items with 4 Kbytes of Flash.

There should be a NFC reader/writer and a NFC tag to establish near field communication between them. NFC provides bidirectional communication between two devices i.e. both devices can send and receive data simultaneously.Raspberry Pi is a Broadcom BCM2835 SoC (System-on-chip) multimedia processor. The ARM (32-bit ARM1176JZFS) instruction set architecture is the secret of how the Raspberry Pi is able to operate on just the 5V, 1A power supply provided by the onboard micro-USB port. Having the storage on an SD card makes it easy to swap with other SD cards running various Linux distributions, which quickly and easily changes the functionality of the Pi. Raspberry Pi provides an extremely low power draw, small form factor and low cost.NFC devices communicate via magnetic field induction; based on the principle that whenever two antennas are set within each other's near field they form an air-core transformer. The reader constantly generates RF carrier signals at 13.56MHz frequency, looking continuously for modulation to occur. The detection of modulation of the field would indicate the presence of a tag or label.A tag/label enters the RF field generated by the reader, and once the tag receives ample energy to work correctly, it divides down the carrier and begins clocking its information to an output transistor that is generally connected across the coil inputs. The tag's output transistor shunts the coil, sequentially corresponding to the information that is being clocked out of the memory array. Shunting the coil causes a short fluctuation of the carrier signal that is seen as a slight modification within the amplitude of the carrier. The reader peak detects the amplitude-modulated information and processes the resulting bit stream in accordance with the encoding and data modulation concepts used.

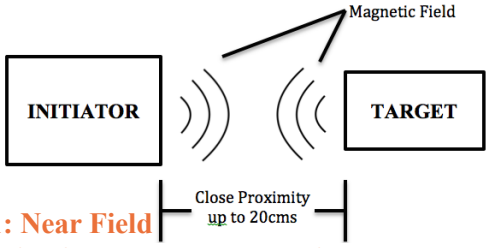

Figure 1: Near Field Communication between two devices

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

NFC has two communicative terminals: Initiator and Target. The 'initiator' is the one that starts the communication. The 'target' receives the initiator's communication request and replies to it. The initiator generates an RF field to power a passive target. The NFC employs two types of coding to exchange data. If an active device transfers data at 106Kbit/s, a 'Modified Miller' coding with 100% ASK (Amplitude Shift Keying) modulation is used. In all other cases 'Manchester coding' is used with a ASK modulation ratio of 10%.

II.Related work:

Near Field Communication is the technology that empowers devices to communicate remotely within a close proximity (less than 20cms). It is a wireless technology, which is an extension of RFID (Radio Frequency Identification) technology. The various advantages of NFC are that it does not depend on the type of operating system, hardware and also is independent of the operating systems application framework. The present stack of the NFC does not meet all the prerequisites. A novel NFC stack that distinguishes the services of OS and the forum standards of NFC was proposed by Xiao Kun and Luo Lei in [1]. Here the NFC stack routine is embodied in the administration services of the OS itself. This enables the NFC stack to adjust to the OS application framework. Therefore third party NFC applications called NFCTagInfo can run on the proposed NFC stack.As of late, there are different advanced mobile phones outfitting with NFC, which inspires engineers to make new and inventive applications. Jie Shen and Xin-Chen Jiang [2] introduced a structural planning for building NFC label administrations, where engineers, and in addition administration suppliers can make their own particular applications and NFC labels. The advantage of the system is that the innovative subtle elements are avoided so that the application designers in this way can concentrate just on the best possible execution of the business rationale and the client interface. Passive mode of operation in Near Field Communication is proficient by making utilization of the inductive coupling concept. The inductive coupling aides in exchanging power from NFC initiator to the NFC tag over the air. M.Mareli, S.Rimer, B.S.Paul and K.Ouahada, A.Pitsillides in [3] proposed parameters that can influence the ideal operation of passive NFC gadgets. The NFC system is facing a security downside that it's vulnerable to a relay attack. In [4] the authors analyzed the potential peer-to-peer modes and bestowed an OPEN-NPP.

The objective of this paper was the OPEN-NPP library. Such library is the initial resolution able to implement the NPP protocol for establishing a peer-to-peer bi-directional communication between a NFC enabled device and a NFC reader. In [5] the authors mentioned the conclusion of relay attack on a legitimate peer-to- peer NFC. Hsu-Chen CHENG, Wen-Wei LIAO, Tian-Yow CHI and Siao-Yun WEI [6] proposed the protection issues with key storage of NFC devices as reading and writing external cards, analyze the probability of risks for every solution, and additionally applying it on contactless mobile debit. The NFC technology standard doesn't provide inherent security measures. This implies that every developer would need to implement security measures in their NFC application on their own. Clearly, this setting may be a major impediment within the widespread adoption and deployment of NFC applications. In [7] the authors proposed the conception of a light-weight security middleware that might implement the various security safeguards required by an array of applications. The applications successively will then implement the protection features relevant to their scenarios. The evaluations showed that the protection middleware is light-weight and also has reasonable memory and CPU footprints.

Utilizing NFC as enabling technology for wireless sensors has intriguing prospects, considering academic researches of ambient intelligence, in addition to simple client applications on the basis of using mobile device. Hillukkala Mika, Heiskanen Mikko, Ylisaukko-oja Arto [8] gave practical implementations of passive as well as semi-passive NFC sensing element prototypes, based on two different industrial NFC chips. NFC has quick connection ability between devices and provides sure secure communication. However, when finding out NFC protocols, the authors [9] found six threats to protecting the confidential information and users' privacy that are unsolved. Retailers and shoppers can face a time when there's uncertainty about a specific product since product identity replication being abused all over, as barcodes are the sole way to determine the original details of a product, which may simply be forged. The introduction of new technology in security enforcement for the product was RFID (Radio Frequency Identification), which can scan and discover the main points of the product much easier without the need of any line of sight in contrast to barcodes. With the new technological upgrade from the RFID to NFC has a security system. Therefore the product originality is determined simply to assist track the item from the industrial plant to the stores.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

This method proposed in [10] consisted a NFC module that may be hooked up to the mainboard. In this method NFC is in a position to extend the safety measures of the product in maintaining its originality. This NFC capability encompasses a potential to switch the utilization of barcodes that may simply be scraped off and replaced.Nikolaos Alexiou, Stylianos Basagiannis, Sophia Petridou [11] conferred a probabilistic model checking approach verify resiliency of NFC protocol against relay attacks supported protocol, channel and application specific parameters that have an impression on the great fortune of the attack. Collin Mulliner [12] proposed a way to deal with security testing of NFC-empowered cellular telephones. Collin Mulliner displayed a novel technique to perform weakness investigation of NFC-empowered cellular telephones through the application of fuzzing utilizing NFC tags or labels. The author investigated the NFC-subsystem as well as segments that can be controlled through the NFC-interface, for example, the web program.

Gerald Madlmayr, Josef Langer, Christian Kantner [13] planned the subsequent measures to deal NFC security and privacy issues. From the present purpose of view there are some problems concerning security and privacy that might be solved by technical ways. However it's to be unbroken in mind that the standardization continues to be in progress.Roel Verdult and Francois Kooman [14] proposed that the NFC feature that invokes a Bluetooth affiliation with no user consent might be abused to sneakily install malicious package on the phone. This leads to a significant vulnerability once smart posters begin installing malicious software/package or spreading viruses. The goal of this study was to grasp how security service personnel experienced the usability, liableness and work performance effects of the present NFC service in use, what were the key development desires associated with the data management and communication in their work, and that of the longer term NFC scenarios were found to be probably most attractive. Based on the results of the study by Heljä Franssila [15], user acceptance of future NFC services in international intelligence agency work is probable. NFC services that support particularly person security of the guard and that create reportage kind the sphere easier, quicker and fewer error prone have the potential to be accepted well with security service personnel. Research endeavors regarding NFC seem to focus chiefly on development of NFC enabled services and applications. In [16] the authors examined the prevailing NFC applications, prototypes and studies from each domain and industry; analyzed these applications by classifying them into NFC operative modes to surface the character of underlying added services and advantages that they provide. Donald Norris in [17] proposed the Near Field Communication reader using a PN532 breakout board, which detects the presence of a tag and then lights an LED. The breakout board utilizes NXP PN532 microcontroller.

III.Raspberry Pi as NFC detector:

The interface between the Raspberry Pi and the MFRC522 reader requires only seven wires, as shown in the block diagram in figure 2. An LED is connected between pins 12 and 17 with a series-current-limiting resistor. Serial Peripheral Interface has been used to establish communication between Raspberry pi and MFRC522 reader.The LED will provide a visual indication when a tag is detected. Also an email will be sent to the user, which gives a message that a "NFC tag/card/label has been detected and matched."

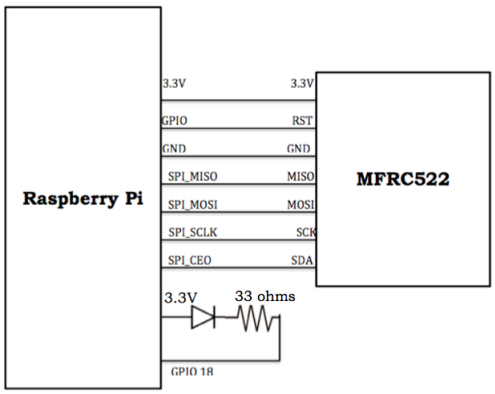

Figure 2: Raspberry Pi and MFRC522 interface

The physical layout of the hardware is shown below in the figure 3.

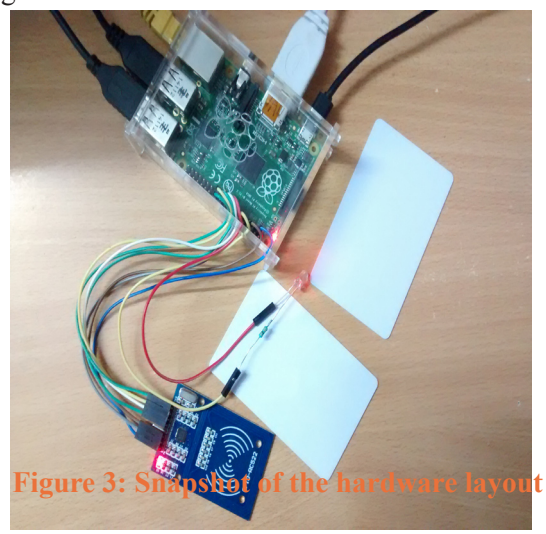

Figure 3: Snapshot of the hardware layout

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

IV.Results;

The project program is designed to detect a pre-designated tag ID and then turn on an LED if the reader detects the tag.

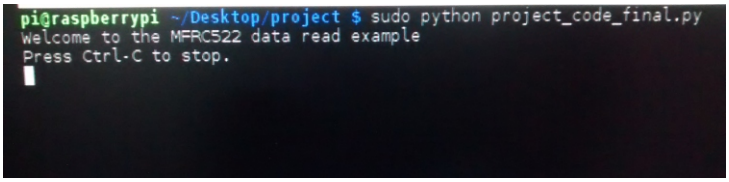

Figure 4: Snapshot of the terminal window executing the program.

A match will turn on the LED for 3 seconds, displays "match" on the console screen and also sends an email with the message "Card Matched." If the tag doesn't match, then the phrase "not match" appears on the console. The two figures 5 and 6 show both the card/tag ID matched and not matched conditions.

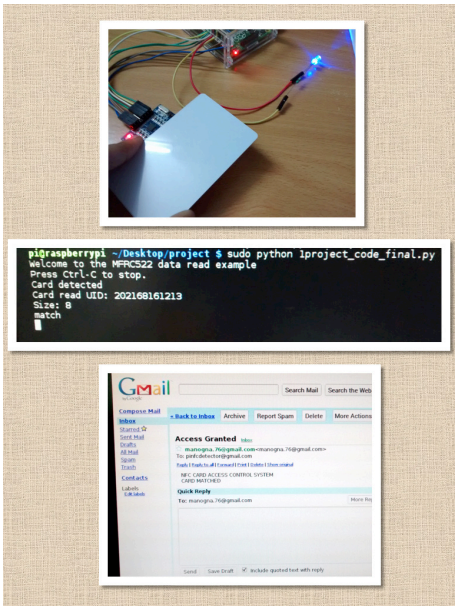

Figure 5: A snapshot of NFC card 'match' condition

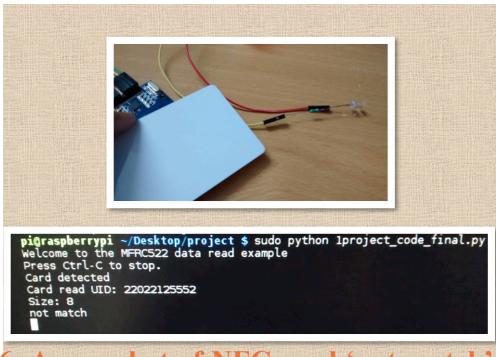

Figure 6: A snapshot of NFC card 'not match' condition

V.Conclusion:

Raspberry Pi, which is the System on Chip and MFRC522, which is the NFC/RFID reader communicate with each other when a NFC card/tag/label has been detected. The main objective is to migrate NFC technology from handheld devices like mobile phones to a SoC so that more number of applications can be served with a single device. On detection of the pre-designated tag ID e-mail will be sent to the user and also the LED blinks for 3sec notifying that the tag has been detected.The future enlargement can be to have the Raspberry Pi signal an electronically managed locking system to unlock when a licensed tag is detected. Normally, there will likely be multiple authorized tag holders who will need access to a field or a building. This may increasingly require a list of authorized tag IDs to be checked due to the fact that every tag involves a distinct ID. Python programming language can accomplish this function in several ways. Tag IDs could even be placed in a database that the program would question. These sorts of access functions are accomplished in real-time, which use commercial systems. Such systems are highly expensive, however using Raspberry Pi we will attain the desired access at an extraordinarily much less cost.Other expansion that might use tag-initiated events include residence duties, such as starting an irrigation system, pool cleaning, garage door opening/closing, home spa operations, and so on.

Acknowledgment:

I would like to express my sincere gratitude to my guide Dr.S.P.Venu Madhava Rao, Professor & Head, Dept. ECE, Sreenidhi Institute of Science & Technology, Hyderabad for his continued support and valuable guidance. I thank him for his painstaking efforts in guiding me throughout my research work.

References:

[1]Xiao Kun, Luo Lei, "A Novel Mobile Device NFC Stack Architecture", 11th International Conference on Dependable, Autonomic and Secure Computing, IEEE Press, pp. 169-173, 2013.

[2]Jie Shen, Xin-Chen Jiang, "A Proposed Architecture for Building NFC Tag Services", Sixth International Symposium on Computational Intelligence and Design, IEEE Press, pp. 48-52, 2013.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[3]M. Mareli, S. Rimer, B.S. Paul and K. Ouahada, A. Pitsillides, "Experimental evaluation of NFC reliability between an RFID tag and a smartphone", IEEE AFRICON, 2013.

[4]A.Lotito, D. Mazzocchi, "OPEN-NPP: an open source library to enable P2P over NFC", 4th International Workshop on Near Field Communication, IEEE Press, pp. 57-62, 2012.

[5]Zhao Wang, Zhigang Xu, Wei Xin, Zhong Chen, "Implementation and Analysis of a Practical NFC Relay Attack Example", Second International Conference on Instrumentation & Measurement, Computer, Communication and Control, IEEE Press, pp. 143-146, 2012.

[6]Hsu-Chen CHENG, Wen-Wei LIAO, Tian-Yow CHI, Siao-Yun WEI, "A Secure and Practical Key Management Mechanism for NFC Read-Write Mode", Journal of Computational Information Systems, Binary Information Press, November 2011.

[7]Sufian Hameed, Bilal Hameed, Syed Atyab Hussain, Waqas Khalid, "Lightweight Security Middleware to Detect Malicious Content in NFC Tags or Smart Posters", 13th International Conference on Trust, Security and Privacy in Computing and Communications, IEEE Press, pp. 900-905, 2014.

[8]Hillukkala Mika, Heiskanen Mikko, Ylisaukko-oja Arto, "Practical implementations of passive and semi-passive NFC enabled sensors", First International Workshop on Near Field Communication, IEEE Press, pp. 69-74, 2009.

[9]Cheng-Hao Chen, Iuon-Chang Lin, "NFC Attacks Analysis and Survey", Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IEEE Press, pp. 458-462, 2014.

[10]Norsuzila Ya'acob, Mohd Mikail Mohd Efendy Goon, Mohd Zikrul Hakim Noor, Azita Laily Yusof and Azlina Idris, "RFID (NFC) Application Employment on Inventory Tracking to Improve Security", IEEE Symposium on Wireless Technology and Applications (ISWTA), pp. 176-181, Sept 28 - Oct 1, 2014.

[11]Nikolaos Alexiou , Stylianos Basagiannis, Sophia Petridou, "Security Analysis of NFC Relay Attacks using Probabilistic Model Checking", International Wireless Communications and Mobile Computing Conference (IWCMC), IEEE Press, pp. 524-529, 2014.

[12]Collin Mulliner, "Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones", International Conference on Availability, Reliability and Security, IEEE Press, pp. 695-700, 2009.

[13]Gerald Madlmayr, Josef Langer , Christian Kantner, "NFC Devices: Security and Privacy", Third International Conference on Availability, Reliability and Security, IEEE Press, pp. 642-647, 2008.

[14]Roel Verdult , Francois Kooman, "Practical attacks on NFC enabled cell phones", Third International Workshop on Near Field Communication, IEEE Press, pp. 77-82, 2011.

[15]Heljä Franssila, "User experiences and acceptance scenarios of NFC applications in security service field work", Second International Workshop on Near Field Communication, IEEE Press, pp. 39-44, 2010.

[16]Kerem OK, Vedat COSKUN, Mehmet N. AYDIN, and Busra OZDENIZCI, "Current Benefits and Future Directions of NFC Services", International Conference on Education and Management Technology (ICEMT), IEEE Press, pp. 334-338, 2010.

[17]Donald Norris, "Raspberry Pi Projects for the Evil Geniu", McGraw-Hill Education, 2014.