ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 2, Issue 4, April 2017

# Development of NFC Based IAP For Wireless Sensor Nodes

[1] Anjali Rajan, [2] Dr. S. Rajkumar, [3] T.S. Shri Krishnan, [4] Jemimah Ebenezer, [5] R. Jehadeesan
[1] [2] Electronics and Communication Nehru College of Engineering and Research Centre, Pampady, Kerala
[3] [4] [5] Computer Division,Indira Gandhi Centre for Atomic Research, Kalpakkam

*Abstract*: ***In a large scale WSN deployment, reprogramming the WSN nodes with new firmware using In-System Programming (ISP) by opening the enclosure of WSN node will be a tedious job. Instead, reprogramming could be achieved by providing physical access to JTAG/SWD on the enclosure; but it will compromise the Ingress Protection (IP) rating of WSN node. Hence, Wireless based In-Application Programming (IAP) could be preferred. Near Field Communication (NFC) is a secure and promising short distance radio communication technology. This paper presents how an NFC transceiver can be utilized to program the microcontroller of WSN nodes. It also explains the development of boot loader program for WSN node to support wireless based IAP.***

*Keywords*: ***Wireless Sensor Network, In-System Programming, Wireless based In-Application Programming, Near Field Communication.***

## I. INTRODUCTION

Wireless Sensor Network (WSN) consists of several sensor nodes each connected to one or more sensors. These nodes transmit sensed data towards the basestation via a meshed network of routers. Generally, WSN is used for industrial monitoring, health care monitoring, environmental/earth sensing like air pollution monitoring, forest fire detection, water quality monitoring etc. [1]. Basic characteristics of the wireless sensor network are limited energy, multi-hop routing, dynamic network topology, node failure tolerance and mobility of the nodes with short-range broadcast communication [2].

Sensor node comprises of microcontroller, radio transceiver unit and signal conditioning circuit unit. Auxiliary units like external memory, RAM, ADC could be present based on the application requirement. Usually, batteries, both rechargeable and non-rechargeable, are the main source of power supply for sensor nodes. Energy harvesting techniques such as solar power, wireless power transfer (WPT), etc. are used to charge rechargeable batteries.

Microcontrollers in the sensor node can be programmed using ISP/JTAG. Microcontrollers that support ISP possess an internal circuitry to generate required programming voltage from the normal supply voltage of the system and to communicate with the programmer through a serial protocol using clock and data pins.

To facilitate easier integration with automated testing procedures, most of the programmable logic devices use a variant of the JTAG protocol. JTAG allows device programmer hardware to transfer data into internal non- volatile device memory. JTAG programmers also write software and data into flash memory.

Large scale or wide area deployment of WSN includes sensing of large number of physical parameters where continuous monitoring and situation analysis are of great interest. In such situations, reprogramming the microcontrollers using JTAG/ISP by opening the enclosure of sensor node will be difficult. For instance, to ease the reprogramming, if we provide physical access to microcontroller pins outside the enclosure of sensor node, it not only violates the ingress protection rating, but also breach security. So, Wireless based In-Application Programming (WIAP) is chosen to reprogram the microcontroller which is the combination of IAP and a short range wireless communication technology, NFC in our case.

## II. LITERATURE SURVEY

Ferro, Silva & Lopes [3] presented a specification for a compact, portable, data layer that can be used to support seamless dynamic reprogramming of WSN, based on the notion of periodic, non-preemptive tasks running in the base OS. Gohane & Khekare [4] developed a system that can be used to wirelessly reconfigure the software module of the industrial embedded devices and machines using application programming interface (API). Using these APIs, various machine parameters can be assigned to the software module. Doug & Kenji [5] proposed an open source platform of JavaMail NFC (JNFC) to emulate the functionality of the Android NFC P2P API. DroidWSN

model is implemented for data exchange, and even when the execution time of emulator was slower, the design was simple and flexible. Cai, Weng, & Liu [6] proposed a research model to utilize NFC to improve privacy and mobile authentication security during mobile payment services. Based on these papers mentioned above, an approach that uses NFC was chosen for Wireless based In- Application Programming of the microcontroller in WSN.

## III. COMPARISON OF WIRELESS TECHNOLOGY FOR IAP

There are different protocols for wireless communication including Bluetooth, WiFi, Zigbee, IrDA, NFC, etc. Table 1 illustrates the key features that lead to the selection of NFC over other wireless communication protocols. NFC has shorter working distance than Bluetooth, which reduces the unwanted interference. In contrast to ZigBee, NFC has faster transmitting speed with same set-up time and power consumption. When compared to NFC, WiFi costs more power and IrDA needs a direct line of sight to connect two devices, and a little longer (0.5s) set-up time. Hence, NFC is decided as the most suitable technology for transferring application code for a wireless based IAP.

Near-field communication (NFC) enables two electronic devices to establish wireless communication by bringing them within a short distance. NFC exploits electromagnetic radio fields operating at 13.56 MHz for

intercommunication. Devices using NFC may be active or passive. A passive device, such as an NFC tag, contains information that other devices can read; but the reverse is not possible. On the other hand, active devices like NFC reader and NFC transceiver operates in a bidirectional way.

An NFC tag usually consists of an antenna connected to a small memory chip, which is written with the information about the item to which it is attached. An NFC reader or transceiver brought near the tagged article powers the circuit through the electromagnetic field, and by this, the data stored in the memory chip can be read. NFC reader is an initiator which initiates the communication & controls the data exchange to the target device [7]. NFC transceivers support both reader and tag operations and they are cheaper than NFC readers. In the setup explained in this paper, NFC transceiver is selected in the NFC programming kit and also an NFC tag is connected to the microcontroller of the wireless sensor node.

## IV. SELECTION OF NFC CHIPS

NFC is a specified subset within the family of RFID technology. Precisely, NFC is a branch of High-Frequency (HF) RFID. There involve several key factors when selecting an RFID technology. The priority of these factors depends upon the application. They are namely reliability, security, compliancy, Read/Write range, Read/Write speed, Multi-tag capabilities, environment, cost, etc.

Table 1: Comparison of Wireless Technologies for WIAP

| **Property** | **NFC** | **Bluetooth 2.1** | **Zigbee** | **802.11(WiFi)** | **IrDa** |
|---|---|---|---|---|---|
| Network topology | Peer to peer | Adhoc,Very small networks | Adhoc, Peer to peer, Star or mesh | Point to hub | Point to point |
| Data rate | **424Kb/s** | 2.1 Mb/s | 250Kb/s | 54Mb/s | 16Mb/s |
| Frequency | 13.56MHz | 2.4-2.5GHz | 868MHz(EU),900-928MHz(NA),2.4GHz (worldwide) | 2.4 and 5 GHz | Not Applicable |
| Range | **0.1 m** | 30 m | 10-100 m | 50-100 m | 1 m |
| Setup time | **<0.1 s** | <6 s | 2.6 ms | | 0.5 s |
| Power Consumption | **<15 mA** | <30 mA | Very low | High | Not available |

Reprinted from "*NFC-Enable System Design in Wireless Sensor Network*", Available at: https://pdfs.semanticscholar.org/05d3/8261ae974c135ceac3fee578ba79d3691876.pdf

*A. NFC Tag*

For contact-less smart cards that operate at 13.56 MHz in proximity with a reader antenna, a four-part international standard named ISO/IEC 14443 standard is used. This specification supports two main communication protocols, namely Type A and Type B. NFC Type A uses Miller encoding and have an amplitude modulation of 100% and data transmission of 106Kbps. NFC Type B uses Manchester encoding instead of Miller encoding, and amplitude modulation is only 10%. So, we used NFC Type A tags.

Here, NFC Tag click™ that carries an M24SR64 NFC/RFID tag IC with a dual interface and 8KB of high- reliability EEPROM built-in is chosen for sensor node. It has NFC Forum Type 4 tag which is compatible with ISO/IEC 14443 Type A. These are tags that are pre- configured at manufacture to be either read and re-writable, or read-only.

B. *NFC Transceiver*

Table 2: Comparison of NFC Transceivers

| | ST95HF | TRF7970A |
|---|---|---|
| **Standards** | 1)ISO/IEC 14443 Type A and B<br>2)ISO/IEC 15693, ISO/IEC 18092<br>3)MIFARE® Classic compatible | 1)ISO15693<br>2)ISO18000-3<br>3)ISO14443A/B<br>4)FeliCa |
| **Modes Of Communication** | 1)Read/write mode<br>2)Card emulation mode | 1)Read/write mode<br>2)Card emulation mode |
| **Input Voltage Range** | 2.7 V to 5.5 V | 2.7 V to 5.5 V |
| **SPI Interface** | 528 byte FIFO | 127 byte FIFO |
| **Power Dissipation** | 1W | 1.1W |

Most commonly used proximity NFC transceivers are ST95HF and TRF series like TRF7970A, TRF7960A, TRF7962A, TRF7963A, TRF7964A, etc. Among the TRF series, TRF7970A is preferable since it operates at wider temperature range than others. Table 2 shows the comparison based on ISO standards, modes of communication, input voltage range, SPI interface and power dissipation. It reveals that ST95HF has a slightly better edge than the other transceivers. ST95HF also have dedicated internal frame controller, transmission and reception modes, optimized power management, tag detection mode and field detection mode. Hence, ST95HF has been chosen as NFC transceiver for this project.

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 2, Issue 4, April 2017

## V. SYSTEM OVERVIEW OF WIRELESS IN- APPLICATION PROGRAMMING

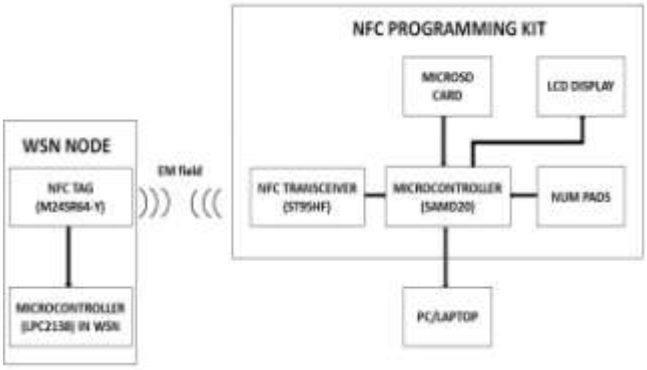
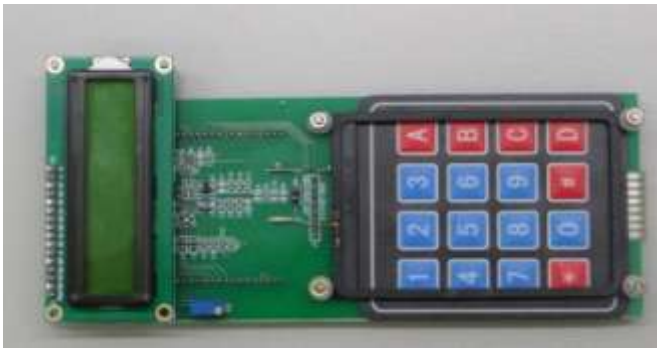



*Fig.1 Block Diagram of System Setup*

*A. Hardware Development*

An NFC programming kit is designed for the wireless reprogramming of each sensor nodes. NFC transceiver, micro SD card, Numpad, and LCD are interfaced to the microcontroller of NFC programming kit as depicted in fig 1. The base firmware to be updated in the WSN sensor node will be read from micro SD card. To select configurable parameters like unique node- ID, the rate of transmission, etc., Numpad and LCD are used. The firmware read from the micro SD card is then transmitted to the WSN microcontroller through NFC transceiver. It uses magnetic induction to create a radio-wave field to communicate with the target. This induction allows data to be transferred wirelessly over a relatively short distance. A four wire loop antenna is used for transmission. An antenna matching circuit is designed between the NFC transceiver and loop antenna for impedance matching. Here, the target will be the NFC tag which receives the code and flashes to the microcontroller of the wireless sensor node. Figure 2 shows the hardware implementation of NFC programming kit.



ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 2, Issue 4, April 2017

*Fig.2 NFC Programming kit*

*B. Software Development*

The developed embedded program is split into two parts. The first part involves interfacing of above mentioned peripherals with the microcontroller of the NFC programming kit and to transmit the firmware via NFC. The second part includes the bootloader programming for wireless sensor node to update its application firmware.

*1) Peripheral Driver Development for NFC Programming Kit*

i) RF transceiver and micro SD card

ST95HF is an NFC transceiver for a contactless application. It includes frame coding and RF modulation, thus allowing the connected microcontroller to send and receive NFC commands in the supported protocols. ST95HF is a slave device; hence a host (microcontroller) is required to control it. The ST95HF is connected to the microcontroller using SPI communication [8].

The application software has to perform three steps to send commands and receive replies.

- Send the command to the ST95HF.
- Poll the ST95HF until it is ready to transmit the response
- Read the response

The SPI_SS line is used to select a device on the common SPI bus. The SPI_SS is active low. All data sent by the master device is ignored when the SPI_SS line is inactive and the MISO line remains in high impedance state. So, the host asserts the SPI_SS line low and issues a command to read data. When all data is read, the SPI_SS line is asserted high by the application.

The NFC transceiver and micro SD card support SPI transfer mode 0. In other words, data is sampled at the rising edge of the SCK signal. It is configured by selecting clock polarity (CPOL) and clock phase (CPHA). In slave mode, the phase and polarization are defined with CPOL = 0 and CPHA = 0 which corresponds to transfer mode 0. The SPI character size is configured to eight bits. SPI communication is MSB first. It can be configured using Data Order (DORD) bit.

Writing a character starts the SPI clock generator, and transfers the character to the data register when it is empty. Once this is done, a new character can be written. When each character is shifted out from the master, a character is shifted in from the slave. If the receiver is enabled, the data is moved to the receive buffer at the completion of the frame and can be read by the slave.

ii) LCD Panel

In NFC programming kit, 16x2 Liquid Crystal Display (LCD) panel is used. LCD is very helpful for providing textual information to the user. LCD is a flat panel display that uses the light modulating properties of Liquid Crystals (LCs). Steps involved in writing a command or data into the LCD are:

- Place the Data/Command in the pins D0-D7 of the LCD.
- Make the RS(register select) pin of the LCD low that is RS=0 to write command
  Make this RS high that is RS=1 to write data.
  EN of the LCD must go through a high to low logic transition with some delay in between them, that is EN=1 to EN=0 with a specific delay.
  The R/W pin should remain in the Logic 0.

iii) Hex Keypad

Hex keypad 4x4 is used for loading numerics into the microcontroller. It consists of 16 buttons arranged in the form of an array containing four rows and four columns. Polling of keypad takes place by configuring a particular row as active low at a time and read the status of the column pins as input at that instant. This chain continues for all the rows and by this way microcontroller can read sequential key press. Steps involved in interfacing hex keypad are as follows:

Drive a 0 in a row. Read all the columns.
If any key is pressed, its column will be 0, else 1. Keep repeating in a loop for each successive row.

2) *Bootloader for Wireless Sensor Node*

Non-Volatile Memory (NVM) is a reprogrammable flash memory that retains the program and data storage even during power off condition. The bootloader program of sensor node utilizes NVMCTRL to write the application firmware onto its flash memory of microcontroller [9]. The SPI bootloader is initiated by the application program once it identifies a valid request for reprogramming is being sent via NFC. SPI bootloader checks for authentication and after the validation of the newly transmitted application program, it flashes the code onto the flash memory. Thus reprogramming/upgrading the application program of sensor node using NFC could be achieved.

## VI. CONCLUSIONS

In a large scale WSN deployment, reprogramming the sensor node is a cumbersome job. To ease the application program update, NFC-based IAP has been chosen. To provide node specific configurable parameters, an NFC programming kit with hex keypad and LCD has been developed. Application code can be loaded onto a micro SD, and after setting node specific parameters, NFC-based IAP could be performed by taking NFC programming kit near to the sensor node.

## VII. REFERENCES

[1] "*Wireless Sensor Network*", Available at:https://en.wikipedia.org/wiki/Wireless_sensor_network.

[2] Maraiya, K., Kant, K., & Gupta, N. (2011). "*Application based study on wireless sensor network",* International Journal of Computer Applications, 21(8), 9-15.

[3] Ferro, G., Silva, R., & Lopes, L. (2015, October). "*Towards Out-of-the-Box Programming of Wireless Sensor-Actuator Networks*". In Computational Science and Engineering (CSE), 2015 IEEE 18th International Conference on (pp. 110-119). IEEE.

[4] Gohane, S. P., & Khekare, G. S. (2015, January). "*Reconfiguration of industrial embedded system in WSN*". In Intelligent Systems and Control (ISCO), 2015 IEEE 9th International Conference on (pp. 1-5). IEEE.

[5] Doug Serfass, Kenji Yoshigoe, "*Wireless Sensor Networks using android virtual devices and Near Field Communication peer-to-peer emulation*", Southeastcon, 2012 Proceedings of IEEE

[6] Cai, C., Weng, J., & Liu, J. (2016, June). "Mobile Authentication System Based on National Regulation and NFC Technology". In Data Science in Cyberspace (DSC), IEEE International Conference on (pp. 590-595). IEEE.

[7]A Technical report on "*NFC for embedded applications*", (2014) Available at: https://www.nxp.com/documents/brochure/75017587.pdf

[8] User manual of "*EVAL-ST95HF firmware functionalities*", Available at: http://www.st.com/content/ccc/resource/technical/document /user_manual/34/4d/7b/b3/40/7b/4b/72/DM00123114.pdf/fi les/DM00123114.pdf/jcr:content/translations/en.DM00123 114.pdf

[9] "*SAM D20 SD Card Bootloader [APPLICATION NOTE] Atmel-42455A-SAM-D20-SD-Card-Bootloader_ApplicationNote_062015*", Available at: http://www.atmel.com/Images/Atmel-42455-SAMD20-SD- Card-Bootloader_Application-Note_AT06037.pdf

[10] Datasheet of "*Atmel SAM D20J / SAM D20G / SAM D20E*", Available at: http://www.atmel.com/images/Atmel-42129-SAM-D20_Datasheet.pdf

[11] A technical report on "*NFC-Enable System Design in Wireless Sensor Network*", Hua, Y. (2013).