



Local Positioning System Using Near Field Communication

Baldeep Singh, Arvind Rajput, Sabhyata Soni
ECE, UIET, Panjab University,
Chandigarh, India

Abstract: Near Field Communication is an emerging technology which is an extended version of RFID. It has gained importance with the advent of smart devices and is capable of bootstrapping other wireless communication technologies such as wi-fi, Bluetooth, etc. In this paper, a Local Positioning System is designed to locate the users within the premises of the building which can be a hospital, university, etc. NFC readers are used to read the NFC tags which contain information of the respective personnels. For the security purposes, if the location of the user is not desired to be revealed then the use of conditional privacy preservation protocol is done. The design is simple and effective as NFC tags are already in use in various purposes but the locating the user with help of NFC tags can be more accurate.

Keywords: GPS, Local Positioning System, NFC tags, NFC tag reader, RFID.

I. Introduction

Near field communication (NFC) is a set of standards for smart phones and similar devices to generate radio communication with one another by different means like by touching them with one another or by bringing them into proximity i.e. no more than few centimeters. Anticipated and present applications have contactless data exchange, simplified setup and transactions, of more complex communications such as Wi-Fi. Communication is also possible between a NFC device and an unpowered NFC chip, called a "tag". In ISO 18092 details of NFC specification can be found [1]. NFC main character is that it's a wireless communication interface with a working distance limited to about 10 cm. it could be operated in different modes. The modes are differentiated either it create its own RF field or by retrieving the power from RF field generated by another device [2]. Active devices are the devices with generates their own field if not then is it known as passive device. Active devices mainly have their own power supply where as passive don't. Three different configurations are possible when two devices communicate with each other. Currently, NFC technology is treated more as an input mechanism for launching other communications technologies than as a radio type for actual data transfer in targeted use cases. While the NFC technology supports extension mechanisms for transfer of large amounts of data, the current radio frequency allocation to NFC requires close proximity of NFC devices during interactions, which creates a user experience that is not conducive to long data transfers. This is why NFC is typically expected to be used for either small data transfer interactions or for launching larger data transfers with an alternative mobile wireless communication technology, such as Bluetooth, WI-Fi, and mobile data service [3]. NFC provides a capability for initiating wireless communication interactions. There are four main reference use cases for these interactions: □ Service initiation (e.g., read a "smart" tag on a poster to acquire information, or to launch a web browser and exchange for product discount coupons) □ Pairing of devices (e.g., send a camera photo to a printer, or activate a Bluetooth headset by tapping on the mobile accessory) □ Peer-to-peer data transfer (e.g., quickly transfer information between mobile devices with a simple touch, such as to exchange business cards or play a multi-player game) □ Secure NFC card (e.g., mobile device acts as an access, loyalty, or payment contactless smart card that is read by others) The UID (unique identifier) element in NFC tags is subject to the potential threat of tampering and spoofing. The typical mitigation of this threat is to provide a tamper-resistant "seal" and to sign the object with a credential from a trusted authority, thus providing a reference of authenticity for recipient entities. The NFC Forum specifications include a framework for signing multiple NFC data exchange format records (NDEF) in NFC tags, to help assure that the originator of the tag and its information are trusted. However, NFC ecosystem participants might additionally consider agreeing on a set of reference certificate authorities (e.g., providers of root certificates) and also adding the signature framework to their NFC interoperability certification for use in future products and services [4].

Additionally, NFC standards should be periodically reviewed with the intent of new work items to supplement the stack of specifications with additional standards or implementation profiles to address identified gaps in the current version of these standards. For example, as noted above, current NFC standards do not completely provide a common approach to ensuring the authenticity of NFC tag data. For example, a digital signing

approach could be standardized to help ensure that the originator of the tag and its information is trusted and not tampered with.[5] International Journal of Information and Education Technology, Vol. 4, No. 5, October 2014

II. Proposed work

This work focuses to design a local positioning system using NFC or RFID cards. In our design NFC readers are installed at various positions in the building. These can be the entrance of the rooms of respective personnel or common meeting places. NFC tags are attached to the respective person's ID cards which can be read by the NFC readers.

A. Design:

The design focuses on following objectives which are helpful in generating the local positioning system.

- a.) To design an environment where NFC readers and tags can be used.
- b.) To create a common server where all the information of tags can be read.
- c.) To accommodate privacy preservation protocol within our designed system.

Basic block design:- The basic block design shows a single corridor or hallway with rooms of different persons. NFC tag readers are installed at each door. Figure 1 shows the basic block design of LPS.

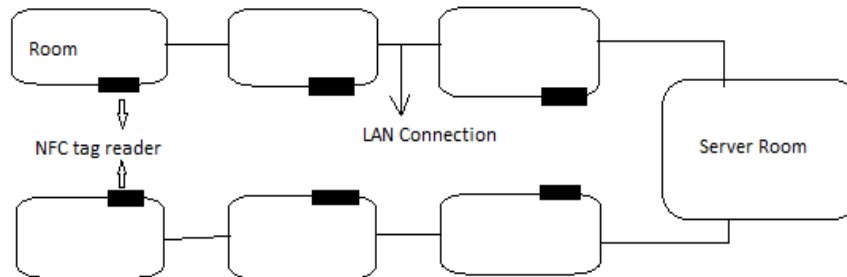


Fig. 1: Basic Block design of LPS

Rooms can be interconnected with each other and with the server with the LAN wires which are already installed in each building now a days.

B. Working of LPS:

NFC readers are capable of reading tags at close proximity i.e from few centimeters to few meters. Whenever a person carrying NFC tag opens a door, tag reader can read the location of the person and can communicate it with the server.

The working the Local Positioning System is explained with the help of a flowchart as shown in figure 2.

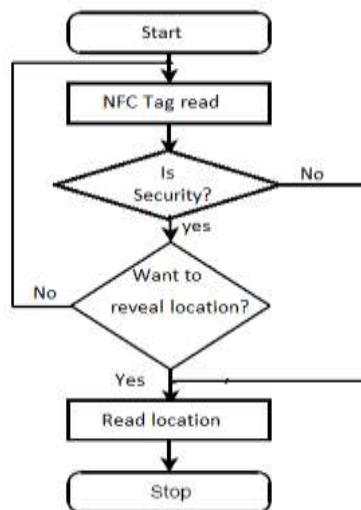


Fig. 2: Working flowchart of LPS

Various steps which are carried out are explained as under.

- 1.) The system is initialized and the server is connected to the all the locations where the NFC tag readers are installed.
- 2.) Whenever someone wants to the position of a particular person, its tag ID is entered and the most recent location of the concerned person is known.
- 3.) If the system is sitting idle then the locations of the different users are stored in the server whenever their tags are read and is updated as soon as the tag is read again.

- 4.) As it is not safe for the security persons to reveal their location at all the times because the security can be compromised, server first communicates with the concerned security personnel and checks whether his conditional privacy preservation protocol allows to reveal the identity or is selected to remain anonymous.
- 5.) If the security personnel allows to reveal his identity then location of the person is conveyed otherwise it is kept anonymous. Thus, not compromising the security.

III. Comparison with GPS

Local positioning system locates a person within the vicinity of the premises where the system is installed. Although not as technically advanced as global position system which uses satellite interface to locate a person, the accuracy of local positioning system is much more than GPS. GPS is able to locate the thing with accuracy of few feet but LPS can be used to locate the thing accurately. The cost effectiveness of LPS also makes it more effective than GPS. Also, to locate a person within a building, GPS is not an attractive method to be used and alternative to that can be the Local Positioning system.

IV. Conclusion and Future scope

In present scenario where the importance of time is recognized, LPS can be used to locate a person or accurately. This type of system can be used in any premises like universities, hospitals, corporate offices etc. Security is also enhanced using this system where position of the person is accurately known and for a person who doesn't require to reveal its location, use of conditional privacy preservation protocol can be made. This type of system can be used effectively in day to day life and is cost effective.

References

- [1] Wikipedia, "Near field communication", http://en.wikipedia.org/wiki/Near_field_communication, Last accessed on 29 January, 2014.
- [2] J. Yu, W. Lee, and D.-Z. Du, "Reducing Reader Collision for Mobile RFID," *IEEE Transactions on Consumer Electronics*, Vol. 57, No. 2, pp. 574-582, May 2011.
- [3] ISO/IEC 18092, "Information technology: Telecommunications and information exchange between systems", Near field Communication Interface and Protocol (NFCIP-1), ISO/IEC, April 2004.
- [4] Ernst Haselsteiner, "Security in Near Field Communication", *Proceedings of the ACM Networking Conference*, pp.14-18, December 2010
- [5] Baldeep Singh, Arvind Rajput, Sabhyata, "Optimization of Conditional Privacy Preservation Protocol for NFC applications using Genetic Algorithm", *International Journal of Computer Applications (0975 – 8887) Volume 102 – No.9, September 2014*
- [6] Media Anugerah Ayu, Barroon Ismaeel Ahmad, "TouchIn: An NFC Supported Attendance System in a University Environment", *International Journal of Information and Education Technology*, Vol. 4, No. 5, October 2014