

Overview of Near Field Communication (NFC)

Amandeep Sheoran¹, Prof. Sukhwinder Singh²

¹Student, E & EC Department, PEC University Of Technology, Chandigarh, India

²Mentor, E & EC Department, PEC University of Technology, Chandigarh, India

Abstract: Mobile payment systems backed by major financial institutions are either already being tested or in plans to start tests, while smartphones with built-in NFC chips are making their way into the U.S. and Europe. But beyond payments, NFC has the potential to reach many other industries, from location-based services to ticketing and public transportation. It's not too far-fetched to imagine a world where all we need to carry around with us is a single do-it-all device. NFC could allow our smartphone to pay for products, open doors, as well as act as our personal ID or a virtual ticket for transport and attractions. Say goodbye to your keys, wallet, cards and any extra weight in your pockets.

Of course, there are loose ends that will need to be worked out before the technology actually catches on, like ensuring the proper infrastructure is there and addressing any security concerns. In this piece we are going to tell you the things that you should know about Near Field Communication and how it could make your life easier in the future.

Keywords: Communication, NFC, payment, range, tag, tapping.

I. INTRODUCTION

In the near future, your technological world might be overtaken by near field. No, not the corn field that's across the road. We're talking about **near-field communication (NFC)**, which gadget manufacturers, retailers and many other organizations hope will bring powerful new features to smart phones and much more. NFC is a type of radio communication standard, much like Bluetooth, Wi-Fi and other networking technologies. It's different in that it operates at very slow speeds and only at a short range of just a few centimetres. [1] NFC isn't a new-fangled technology, but it's just now beginning to filter into mainstream products like smart phones. With an NFC chip and antenna, you can use your smart phone to make **contactless payments** at NFC retail terminals, parking meters, taxis and many other places. What's more, with NFC, you can bump smart phones to exchange information with friends or business colleagues, or use your phone to read smart tags. **Smart tags** are tiny, read-only chips that can appear in informational posters and identification documents, such as corporate badges or passports. You can even use NFC to connect to secure networks without having to enter complex authorization codes. For instance, you may be able to tap an NFC tablet to a wireless router and after the NFC chip confirms your identity, your tablet is cleared to connect to the much faster Wi-Fi signal so that you can get to work. Ultimately, NFC makes it a whole lot easier to perform a huge range of digitized tasks. But with that kind of power in such a tiny chip, is this technology really secure? Many experts say NFC really is fundamentally secure by virtue of its extremely short range. In order to snag your NFC signal, a hacker would need to be very close to you. Uncomfortably close. In other words, you'd know they were there. And unless it was a very intimate friend of yours, you'd likely not be happy about it. There's more to the physical aspects of NFC that make it troublesome for even determined hackers.

II. HOW DOES NFC WORK?

[5] At its core, all NFC is doing is identifying us, and our bank account, to a computer. The technology is simple. It's a short-range, low power wireless link evolved from radio-frequency identification (RFID) tech that can transfer small amounts of data between two devices held a few centimetres from each other.

Unlike Bluetooth, no pairing code is needed, and because it's very low power, no battery in the device being read. By tapping your phone on a contactless payment terminal in a shop, train station or coffee shop is able to identify your account (and even your personal preferences, shopping habits and even your most frequently travelled route home) and takes payment through an app on your phone. Passive NFC 'tags' on posters, in shops and on trains could contain a web address, a discount voucher, a map or a bus timetable that passers-by could touch their phones on to receive – or to instantly pay for absolutely anything.

"The SIM card in your mobile phone is a smart card identifying your account to the network," says John Elliott, Head of Public Sector at Consult Hyperion, who's worked on the Oyster Card. "On NFC phones, the SIM is being extended to act as the Secure Element that can hold other apps such as payment cards.[2] **“Are there any alternatives to NFC?”** Yes – and there are plenty within it, too. One debate in the mobile and finance industry is between the 'mobile wallet' as

represented by NFC, or the 'digital wallet'. Calling NFC 'a technology, not a strategy,' PayPal's Kerry Wong, MD for Hong Kong, Korea and Taiwan, promotes the latter.

"The 'digital wallet' exists in the cloud, and it is not tethered to one specific device such as a mobile phone, but accessible from a variety of devices such as laptop, iPad, ultra book or even Xbox," she says. Wong thinks that it's the ability to work easily, safely and on any device or platform that will win the day. [8] NFC is only one technology, with Bluetooth and RFID just as able to strike-up a conversation between two gadgets, but there are distinctions within NFC, too. It comes in both passive and active flavours, including P2P mode (exchanging information, such as business cards or contacts) and Secure Element NFC (where a machine recognises a NFC phone as a bankcard).

III. How is NFC different to the new contactless bank cards?

It does away with plastic, but otherwise it's very similar to the chip-and-PIN killer.[4] Most new Barclaycard, American Express, MasterCard Pay Pass and Visa Europe cards have NFC contactless tech within, and with 30 million already in circulation in the UK (look for the Wi-Fi-like logo on the back) this is where the 'digital wallet' exists for now; in, err, your wallet. Such cards can be used to make small purchases (typically under £15) in shops. "The foundations of the NFC ecosystem are now largely in place," says Gerry Kelliher, Europe Sales Operations Leader at Research in Motion. "Large scale initiatives like Visa's Pay Wave and MasterCard's Pay Pass mean that NFC terminals are appearing in thousands of UK high street shops."

IV. NFC based wireless charging system (Overview)

Wireless charging is starting to become popular in products such as smart phones. It eases battery charging of portable devices and makes cables and connector's redundant. [6] The Rennes's NFC-wireless charging technology widens the charging area to about 10 cm. It incorporates the technology of the existing NFC MCU, and utilizes the NFC antenna to implement a wireless charging system that uses a single RX antenna for NFC communication and receiving power, when call is connecting the user thereby improving reliability while reducing the bill of material of a receiver design.[9] The Rennes's NFC-wireless charging system has the following advantages. 1) Power transmission and communication via one single antenna with NFC. 2) Expansion of charging area with NFC (flexibility with the charging position, easy-to-use). 3) Downsizing of the antenna size due to use of high frequency band. 4) Certification is possible due to use of NFC. 5) Ability to build wireless charging systems with a high level of safety by inter communication. The Rennes's NFC-wireless charging system is not only for smart phones but also it can be applied in healthcare devices, digital still cameras, and other consumer or industrial applications.

V. Weakness of NFC

Mobile devices that allow for system-to-system data transfers, or pairing of devices to enable Interaction, may trigger privacy concerns, including the following [10]:

- a. Unwanted data leakage or collection;
- b. Tracking of a user's location;
- c. Identifying users in situations where they wish to remain anonymous;
- d. Improper redirection to an unknown website;
- e. Initiation of an unknown service; and
- f. Receipt of unwanted content.
- g. Eavesdropping threats.
- h. Man in the middle threats.
- i. Data modification threats.

However, the NFC technology and ecosystem addresses some of these privacy concerns, for example:

- a) NFC requires less than 4 centimetres of close proximity for interactions. At this Close range, users will have foreknowledge of the person or device that they are Interacting with;
- b) NFC interactions are based on a "tapping" consumer gesture, where both NFC Devices either touch or are within a few centimetres of each other in order to initiate An NFC interaction. This makes "skimming" and "eavesdropping" very difficult.
- c) NFC capabilities should be disabled when the screen or keyboard of an NFC-enabled Mobile phone is locked. Additionally, the mobile platform should permit users to Disable the NFC function, as well as any alternative communication technology (e.g., Bluetooth or Wi-Fi) used for peer-to-peer transfer of personal information. This prevents unintended NFC interactions;
- d) NFC implementations should provide user feedback on interaction requests from Another NFC-enabled device. This reduces hidden or unwanted NFC interactions;

e) NFC-initiated sharing of personal data should be accomplished with use of regenerated identifiers, to avoid association of a device and its user with an NFC interaction.

Conclusion

Near Field Communication is all about making our daily interactions easier-easier to pay for goods and services, easier to use public transport, easier to interact with business etc. At the heart of the technology is its ease of use, increasing convenience rather than enabling something new. It will be a while longer until we are able to ditch our keys, wallets, cards and more in favour of a single device to rule it all. And if it ever comes to that point, it is sure that smartphones are the best medium to accomplish this. In the end I can only say that NFC is certainly a technology to keep our eyes on it as it has the potential to bring a new level of convenience to many aspects of a typical person's life.

References

- [1]. E. Rukzio, G. Broll, K. Leichtenstern, A. Schmidt, —Mobile Interaction with the Real World: An Evaluation and Comparison of Physical Mobile Interaction Techniques,| in Proc. Aml-07: European Conference on Ambient Intelligence, 2007, Darmstadt, B. Schiele et al. (Eds.), Springer, pp. 1-18, Lecture Notes in Computer Science 4794.
- [2]. m-Health e-Emergency System : Current Status & Future Directions : Department of computer Science by E. Kyriacou, M.S.Pattichis, C.S.Pattichis, A.Panayides ,And A.Pitsillides.
- [3]. P. Vällkynen, M. Niemelä, T. Tuomisto, —Evaluating Touching and Pointing with a Mobile Terminal for Physical Browsing|, in Proc. NordiCHI, 2006, Norway, ACM, ISBN:1-59593-325-5/06/0010.
- [4]. Y. Anokwa, G. Borriello, T. Pering, R. Want, —A User Interaction Model for NFC Enabled Application|, in Proc. 5th Annual IEEE International Conference on Pervasive Computing and Communications Workshops, 2007, New York, IEEE Computer Society, pp. 357-361, ISBN:0-7695-2788-4.
- [5]. T. Koskela, V. Käisa, L. Lauri, —Home is where your phone is: usability evaluation of mobile phone UI for a smart home,| in Proc.6th International Symposium on MobileHCI, 2004, Glasgow, S. Brewster, M. Dunlop (Eds.), Springer, pp. 74-85, Lecture Notes in Computer Science 3160.
- [6]. A. Zoe, V. Srikant, —Intuitive Mobile User Interaction in Smart Spaces via NFC-Enhanced Devices,| in Proc. 3rd International Conference on Wireless and Mobile Communication, 2007, Guadeloupe, IEEE Computer Society, p. 86, ISBN:0-7695-2796-5.
- [7]. Juniper Research, Mobile Tickets Please!, Public White Paper, 2008. Available: <http://www.juniperresearch.com/shop/viewwhitepaper.php?id=100&whitepaper=59>.
- [8]. International Journal of Infinite Innovations in Technology|
- [9]. <http://www.techspot.com/guides/385-everything-about-nfc>.
- [10]. Global Journal of Computer Science and Technology, Volume 11 Issue Version 1.0 March 2011
- [11]. Type: Double Blind Peer Reviewed International Research Journal Publisher: Global Journals Inc. (USA) Online ISSN: 0975-4172 & Print ISSN: 0975-4350.