NEAR FIELD COMMUNICATION

VIBHOR SHARMA
Department of Computer Science & Engineering
TULA's Institute, The Engineering and Management College,
Dehradun, Uttarakhand 248001, India
vibhor.sharma.8sep@gmail.com

PREETI GUSAIN
Department of Computer Science & Engineering
TULA's Institute, The Engineering and Management College,
Dehradun, Uttarakhand 248001, India
preetigusain2010@gmail.com

PRASHANT KUMAR
Department of Computer Science & Engineering
TULA's Institute, The Engineering and Management College,
Dehradun, Uttarakhand 248001, India
prashantkumar32@gmail.com

Abstract

Near Field Communication (NFC) technology is being grown up at enormous speed. NFC technology provides the fastest way to communicate two devices with in a fraction of second. This technology has only been implemented on smart phones so far. Like Bluetooth it works only in short range and data transfer takes place at very low speed. Several security issues are attached with NFC, which is a big concern. Security attacks like eavesdropping, data corruption and modification, interference attacks and theft, are the most dangerous for the customer who is using his/her smart phone for payment purpose. In this paper we present the comparison of NFC with Bluetooth and security analysis of NFC.

Keywords: NFC Modes, NFC and RFID, NFC over Bluetooth, Security Issues, Protection Measures.

1. Introduction

NFC is wireless technology which provides communication between two mobile phones which contain NFC tags, using short range radio waves. It uses the magnetic field induction for this purpose. Both devices can communicate with each other using NFC technology when they touch each other or brought very close to each other. It requires short range of approximately four centimeters to perform the exchange of information between two devices. We can do payment using our NFC enabled phone by swiping it out in front of the phone reader and then the purchase price will automatically paid from credit card or debit card. Our mobile phone can be used in place of wallet, credit cards, debit cards etc. We don't need to carry our credit card or debit card with us. But with these advantages, we will have to face disadvantages too. There are some security threats to NFC technology, which should be prevented. NFC technology uses RFID (Radio Frequency Identification) for data/information exchange between two devices over a short distance like Bluetooth and Wi-Fi technology. NFC enabled smart phone users can make transactions and access information with only a simple touch. NFC devices can send and receive data simultaneously. So this technology has a very bright future scope. Since it is

a new technology, so NFC enabled mobile users need to be educated on how it will work for them to make payment or exchange any information. But there is a requirement of a protected infrastructure for NFC technology so that it could be widely adopted all over the world. This technology has several advantages over other wireless technology because it provides bidirectional communication for exchanging information.

2. NFC Modes

NFC works in active mode as well as passive mode. In active mode, both devices, tagged with NFC chip, generate their own electromagnetic field alternatively to exchange information. Both devices are active in this mode. One of the devices deactivates its electromagnetic field during data transfer. In passive mode, one of the devices acts as a transponder and uses the electromagnetic field of other device for its own operating power. In other words we can say that one device is active which generates its radio frequency field and the other device uses that field for data exchange.

3. NFC and RFID

NFC and RFID are two words which are used in wireless technology. NFC is compatible with RFID infrastructure. RFID stands for Radio Frequency Identification which consists of a reader, transponder, and IT system working in background. RFID transmits information via radio waves. Transponder is a small computer chip outfitted with an antenna. It is integrated into a carrier object such as a card. The number codes are stored on the chip. The code encrypts information stored in the database. Reader is an antenna that emerges signals to transponders and receives their Data. Information about objects can be stored in a database. For this the reader transmits the combination of numbers to the database. The IT system decrypts the code and links it to information stored in the database or on the Internet. The system's knowledge, or intelligence, is located in the database, not in the transponder. Information can also be stored on the chip. In these applications, the readers need not be linked to a database. Figure 1 is showing how NFC enabled devices make transactions using RFID technology.

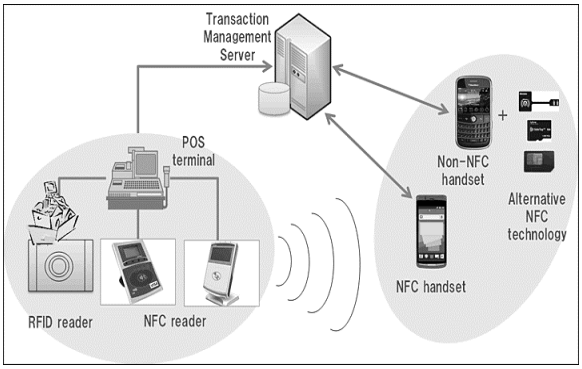

Figure-1 (NFC using RFID infrastructure)

4. NFC over Bluetooth

NFC communication and Bluetooth have several features in common; both use short range radio waves to provide communication between two devices. Both have their advantages and disadvantages, so they can be used in a combined way to fulfill the user's data transmission needs. NFC area is limited to a short distance of approximately four centimeters while Bluetooth covers the distance of approximately thirty feet. In this regard the Bluetooth is superior over NFC. But this close proximity provides the benefit to user when communication takes place in crowded location where interference may be occurred because several devices may be there in that close proximity and they can try to communicate too. Bluetooth may have trouble to deal with this condition. NFC consumes less power in comparison of Bluetooth. When NFC works in passive mode then it consumes more power than Bluetooth transmission. Another feature, provided by NFC, is ease of use. Bluetooth requires a connection between both devices, which should be established manually for information exchange and may take several seconds. On the other hand NFC connection is established automatically in a fraction of second if both mobile users are in close proximity. Thus NFC is fast and easier than Bluetooth technology. The data rate of NFC is lesser than Bluetooth. NFC operates on 13.56MHz band and the data rate's range starts from 106 Kbit/Sec to 848 Kbit/Sec. So It is not suitable to send large amount of data, But it can be used for identification and validation of person/device. NFC is compatible with RFID (Radio Frequency Identification) infrastructure.

In figure 2 we can see comparison of NFC with other technologies in terms of data rate and range.

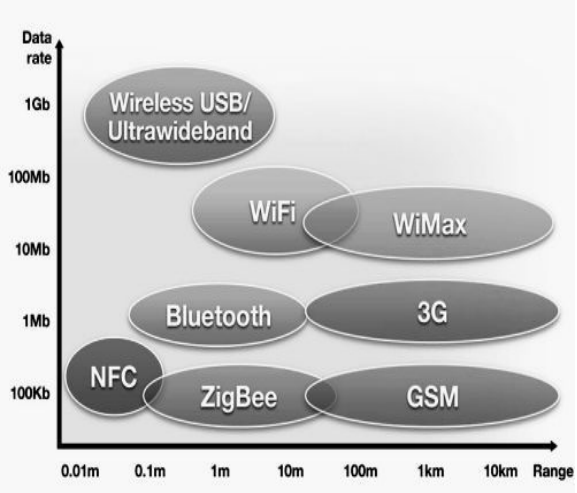

Figure-2 (Differentiation among various wireless technologies)

NFC has an advantage over Bluetooth is that it provides bidirectional communication between devices i.e. both devices can send and receive data simultaneously. Bluetooth provides unidirectional communication i.e. at a time, a device can send the data and another device can receive the data.

5. Security Issues

As NFC uses Radio waves for data transfer its security issues grow higher. Data being transferred can be intercepted, analyzed and modified. Insertion of error can be done on the transmitted data. The possible security attacks on NFC can be categorized as Eavesdropping, Data corruption, Data Modification, Imposter attacks, and Theft. Eavesdropping is when an opponent secretly listens to the private transactions between two devices. Opponent need not to listen all the NFC transactions. The opponent may take private information by any NFC transaction i.e. data confidentiality is broken. Data corruption occurs when the opponent intercepts the data, corrupts it and send further. If user makes any transaction with this corrupt data, He will not get the desired output due to the corrupted information. Another security issue related to NFC is data manipulation in which the opponent manipulates the data during transmission. So, the receiver will receive manipulated data i.e. data integrity is broken. Imposter attack can be a big threat to NFC technology too, because an imposter can hack the data between two parties during transmission and alter it. After that the imposter can pretend to be a different entity i.e. sender in front of receiver and receiver in front of sender. It is similar to man in the middle attack. Another major security issue is theft attempt. If the NFC enabled device is stolen, the thief can swipe the phone in front of card reader or tap phone with another NFC enabled phone and make transactions, no matter how strong encryption is applied. Thus these are some security issues which can be faced by NFC technology during any transaction or transmission.

6. Protection Measures

There are some protection measures which can be applied to prevent from security attacks on NFC transactions or transmission. First we will talk about the eavesdropping. In eavesdropping any opponent can listens to the transaction. But the opponent has limited range to intercept those signals. Secure channels can be used to get rid of data corruption and data modification. Since data being exchanged is encrypted therefore only authorized device can decrypt the data, no one in between can corrupt or manipulate the data. Imposter attack can be prevented by using the active-passive pairing between devices i.e. the communication should be unidirectional instead of bidirectional. Another security threat is theft which is impossible to prevent. The user can only take care of his NFC enabled phone and keep tight security on his phone i.e. installing a password or any other lock on mobile phone. If mobile phone is stolen then the thief couldn't be able to access the confidential information. NFC is safe enough. IN the payment environment, there are several security functions and NFC forum has already define several security paraameters. The real focus is on the application level where the banks, mobile companies and merchants require secured services through a trusted service manager at application level.

7. Future trend

We can think a number of things using NFC. Let's think that we are doing shopping at Mall and paying the bill not in cash or credit card but just by waving our mobile phone in front of the reader. We can also think to pay the electricity bill, water bill etc. not by waiting in the queue for hours but just to tap our phone and deduct the bill. Kenya has adopted this technology. NFC is provided by a few number of Mobile manufacturing companies to a very few handsets (Smart phones). But in future it will be provided in all kind of devices because of its ease of use. But the obstacle is to make people understand to make payment by their mobile phones instead of credit cards, debit cards or cash.

8. Conclusion

NFC would enable all the users to make payments simply by tapping their mobile phones with mobile phone reader like debit card or credit card transactions. Many banks, mobile operators, vendors and companies are implementing NFC technology. But NFC has been failed to make an impact so far. Since it is new technology therefore users need to learn about this technology on how it works. NFC needs collaboration among banks, merchants and mobile companies to provide a secured platform to users that support NFC technology. But it is very crucial to set up a secured platform for NFC so that users could adopt this technology easily.

9. References

1. http://www.cosic.esat.kuleuven.be/rfidsec09/Papers/rfidsec2.pdf
2. http://www.corerfid.com/Files/Product%20Fact%20Sheets/083%20NFC%20Guide.pdf
3. http://www.cnx-software.com/wp-content/uploads/2010/12/nfc_compared_to_bluetooth_zigbee_wifi_wimax_gsm_3g.png
4. http://www.nttdata.com/global/en/news-center/global/2012/img/032901-01.gif
5. http://www.nearfieldcommunicationnfc.net/nfc-vs-bluetooth.html
6. http://www.nearfieldcommunication.org/bluetooth.html
7. http://en.wikipedia.org/wiki/Near_field_communication
8. http://www.isuppli.com/automotive-infotainment-and-telematics/marketwatch/pages/nfc-and-bluetooth-complementary-or-competitive-both-offer-distinct-advantages-for-users-in-vehicles.aspx
9. http://www.nearfieldcommunication.org/nfc-security.html
10. https://www.cdt.org/blogs/harley-geiger/nfc-phones-raise-opportunities-privacy-and-security-issues
11. http://www.cso.com.au/article/440741/near_field_communication_security_risks_/
12. http://android.appstorm.net/general/opinion/near-field-communication-and-the-future-of-mobile/
13. http://www.nfc-forum.org
14. http://mondato.com/en/articles/newsletter-vol-4-issue-14-nfc-bypass-security-in-mobile-payments

Vibhor Sharma completed his B.Tech in Computer Science and Engineering from Tula's institute (Engineering and Management college), Dehradun. Presently he is doing M.Tech in Computer Science and Engineering from Tula's Institute, Dehradun. His research interest is in wireless networking.

Preeti Gusain completed her B.Tech in Computer Science and Engineering from Tula's institute (Engineering and Management college), Dehradun. Presently she is doing M.Tech in Computer Science and Engineering from Tula's Institute, Dehradun. Her research interest is in wireless networking.