Volume 4, Issue 8, August 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Near Field Communication

Chetna Bajaj
Department of Computer Science & Engineering,
Ambedkar Institute of Advanced Communication Technologies and Research, Delhi, India

Abstract— Near Field Communication (NFC) is a new trend in communication's era. Being a simple and safe technology, it facilitates its users in many applications to provide comfort to their life. Communication has accelerated through many years to provide this exotic 'Touch-n-go' facility to its users. The paper introduces Near Field Communication technology along with its standards, features, working principle, etc. NFC technology has evolved to an extent of success that it has left other technologies behind the wall. Comparison of NFC technology with other technologies, performed in paper, reveals the success story of NFC. It also describes various application areas of NFC technology. Along with wide range of applications (pros), NFC technology also faces some threats (cons), these threats make NFC technology vulnerable to the privacy. The paper also elaborated various threats and their remedies. Besides these threats, NFC is a promising technology that shows an energetic world to a wide variety of users by facilitating them in various applications.

Keywords—NFC; Applications; Security threats and measures.

I. INTRODUCTION

Near Field Communication is an innovation in communication field. It is an emerging technology and a great achievement. It allows devices to communicate and transfer data packets by just placing them close. The technology has provided a new way of communication which left other technologies behind. Near Field Communication technology is a wireless communication technology and it is growing very fast to let world use it in their day to day operation.

II. RELATED WORK

A. NFC Standards

NFC technology was founded in 2004, when it was standardized by NFC forum. NFC forum act as an authority to define NFC standards and specifications. It is also responsible for technology's further improvement. NFC standards are defined in ISO 18092 and in its equivalent ECMA-340 standard. NFC technology has been evolved from RFID (Radio frequency Identification) and is also compatible with it. In fact, NFC technology is considered RFID's successor and RFID is its descendant. The products designed for RFID technology i.e. RFID tags or devices are developed with standard ISO 14443 and are also suitable to operate with NFC technology. Moreover, NFC devices are also compatible with RFID tags from MIFARE and FeliCa brands, developed by Philipa and Sony respectively [1].

B. NFC Operating Characteristics/Features

Near Field Communication, being a wireless communication technology, operates on short-range radio frequency. Near Field communication forms a peer-to-peer network for data communication. Near Field Communication operates on a globally available and unlicensed radio frequency band of 13.56 MHz. The technology works when NFC enabled devices brought within close proximity i.e. a small distance around 4 cm to 20 cm. It can provide transfer data rate of up to 424 Kbps. It also allows data transfer in the chunks of 106 Kbps and 212 Kbps. It can provide a bandwidth of approximately 2 MHz [2] [3].

Two NFC devices participating in communication, works in two variants [4] [5]:

1) *Active mode*: NFC device operating in active mode, can generate its own carrier frequency, resulting its own RF field for transmission purpose. It is equipped with a power supply for operation. Active NFC device act as an initiator in communication. Two active NFC devices can alternatively generate RF field to form a two-way communication link to transfer data.

2) *Passive mode*: NFC device operating in passive mode, would not be able to generate its own carrier frequency. Passive device acts as a target. Initiator device produces RF field for communication and Target device use inductive coupling for responding them back. Target device modulates to initiator's RF field, for replying back to initiator. Target device uses power from initiator's generated RF electromagnetic field and saves energy. Resultant, Passive device can be provided a small battery for its operation to restrict energy sources consumption.

C. NFC Devices and Chips

Near Field Communication provides contactless communication. NFC technology is based on Radio Frequency Identification (RFID). It uses magnetic field induction, produced by devices to enable communication between them. NFC technology grows very fast as it's applications are increasing day by day in every sphere of life. And most importantly, if NFC technology is being used in combination with mobile phone, then it can offer great opportunities. NFC technology allows users to just wave his mobile phone near NFC enabled tag and get the job done. Prerequisite of the technology is to acquire NFC enabled device. Users must get NFC enabled mobile phone and vendor i.e. other party must also be equipped with NFC device to complete the procedure. Nowadays, Mobile phone is integrated with NFC chips to make them NFC enabled mobile phone [7]. Likewise, we need to insert NFC chip or NFC tags, readers etc. in devices to make them operate in NFC environment. NFC chip and tags build interface to let NFC work and the rest underlying layers of NFC technology are implemented in ISO, ECMA and ETSI standards [8].

NFC chip is very small and light weighted, embedded in device along with an aluminium antenna to use technology. NFC chips is a micro chips, capable to store information. A NFC micro chip or NFC tag can store data from 98-4096 bytes. These chips also come in Read, and Read/Write variant. Earlier only Sony and Philips developed this chip and now semiconductor companies like Broadcom and Texas instruments are also participating in the development of NFC chips. Apart from mobile phones, NFC chips have started to get its place in laptop as well [9]. So, the key to Near Field Communication is a NFC tag. Tag is the main hardware required to enable Near Field Communication, without which it would not be possible for NFC to work. Tag communicates by transmitting small data packets to each other.

D. NFC devices Operation modes

Near Field Communication is considered as a proximity coupling technology compatible with the standards of proximity of smart cards specified in ISO 14443. NFC devices mainly operate in three different modes [3] [10]:

1) *Peer-to-Peer mode:* Peer-to-peer mode is a simple or classic mode of NFC operation. It allows data transfer at a rate of up to 424Kbps. It works on NFCIP-1 protocol, whose protocol's detail and electromagnetic properties are standardized in ISO 18092 and ECMA 320/340 [11].

2) *Reader/Writer mode:* NFC device can also operate as Reader/Writer for tags and smart cards. In Reader/Writer mode, NFC active device act as an initiator and passive tag act as target [4]. This mode allows data transfer rate of 106 Kbps

3) *Tag Emulation mode*: In emulation mode, NFC device emulates ISO 14443 smart card chip. These smart chips are integrated in mobile devices and get connected to NFC module for communication to occur. Smart chips used in emulation are considered as secure elements [12]. It provides an advantage that it's not required to replace already existing infrastructure to make it able to work with new infrastructure, even that a legacy smart card reader can't distinguish between a smart card and a mobile phone operating in tag emulation code.

III. COMPARISON OF NFC WITH IRDA AND BLUETOOTH

Prior to NFC, other technologies like Bluetooth and Wi-Fi served for wireless communication. A large number of users are still using them but are shifting to NFC as it provides a varied range of applications. Table 1 point out the comparison of NFC with IRDA and Bluetooth on different parameters [1].

Table 1: Comparison between NFC and other technologies

Parameters	NFC	IRDA	Bluetooth
Network Type	Point-to-point	Point-to-point	Point-to-multipoint
Set-up Time	<0.1ms	~0.5s	~6s
Range	Up to 10cm	Up to 5m	Up to 30m
Speed	424kbps	115kbps	721kbps
Modes	Active-active, active-passive	Active-active	Active-active
Usability	Human centric, Easy, Intuitive, Fast	Data Centric, Easy	Data Centric, Medium
Selectivity	High, given security	Line of sight	Who are you?
Use Cases	Pay, get access, Share, Initiate service, Easy set up	Control & Exchange data	Network for data exchange headset
Consumer Experience	Touch, Wave simply connect	Easy	Configuration needed
Costs	Low	Low	Moderate

The integration of technologies like NFC, Bluetooth, Wi-Fi, etc. into mobile phones, has provided extensive capabilities to users. But when we compare NFC with other technologies i.e. Bluetooth or IRDA, it simplifies the interaction method between devices to obtain faster connection. In 1993, people came across infrared communication

technology, which is the oldest wireless technology as of now. Infrared communication sensitively reacts to external environment such as light and reflecting objects [13]. This shortcoming makes it vulnerable and also restricts users to use it.

NFC provides significant advantages over Bluetooth. NFC's set-up time is less as compared to Bluetooth. Therefore, NFC can establish connection very fast, say in less than 0.1s, but other technologies manually configure itself to identify other's phones. All mentioned protocols are point-to-point protocols. Bluetooth also supports point-to multipoint communication along with point-to-point communication. NFC operates in the shortest range i.e. within 10 cm. Shorter range provides better security and makes NFC suitable to operate in busy areas. NFC allows a data transfer rate of approximately 424 kbps, which is slower than Bluetooth i.e. 721 kbps, but it is faster as compared to data transfer rate of infrared communication, i.e. 115 kbps. Lastly, NFC is more compatible with RFID as compared to Bluetooth.

IV. NFC APPLICATIONS

Near Field Communication has provided a long list of applications to facilitate their users. The technology has attracted many users by providing an ability to perform a complex task in just a second by just swiping NFC enabled mobile phones in front of NFC enabled mobile readers. Following are some applications of Near Field Communication:

A. Mobile Payments (m-payments)

Mobile payment concept has originated from an idea which states that the user does not require carrying neither wallet nor any credit card. He would be able to make payments for his goods by their mobile phones. The idea is supported by mobile applications e.g. Google Wallet, which are specially developed for making mobile payments. The application gets installed in mobile phone to work in collaboration with NFC enabled payment system to facilitate payments [14]. Mobile payment along with NFC technology would support a wide chain of businesses. As an example of Mobile payment, Google Wallet from Google has been used in 2012 London Olympics. Google estimates that a massive number of retailers and users would use NFC enabled systems in near future and the number of users will substantially grow over years [15].

B. Credit Cards Replacement

Customers use credit cards to make payments. They prefer to acquire credit cards from different vendors. Carrying multiple credit cards can be a hoax for users. In case, user loses his credit cards mistakenly, then it would result in loss of time and money. Another problem with credit card is due to magnetic strip and chip. The magnetic strip and chip used in cards have a limited lifetime and are also vulnerable to demagnetizing and breakage. To avoid all of this chaos's, we can use card emulation mode of NFC to reduce credit cards usage [5].

C. Advertising

Near Field Communication technology has served its benefits in advertising too. Two components are used in advertising, one is a NFC enabled mobile phone that operates as NFC reader, used to read the information and the other one is NFC tags in smart posters. NFC enabled mobile phone reads advertising information from NFC tags installed in smart posters. NFC reader collects all information required to provide service. Information may contain a website URL or a phone number, etc [5] [16]. By just swiping a phone, we would get all necessary information, be it a movie, pictures, interviews, etc. Advertisers use NFC tags in banners to deliver information about available offers, coupons, product launches, brand interaction service, etc. to customers [9] [15]. It can also be used in acquiring feedback from users by just transferring information from one NFC device to other by keeping them close to each other.

D. Educational purpose

Implementing NFC technology in school and college campus, students with NFC enabled mobile phone and notice board, can make student's life easy. They can instantly receive information from notice board [14]. They can also get updates about their schedules, coursework, etc. The researchers have also thought of developing a NFC based system to provide university based services including an automated attendance system, Access Control and Smart Posters in campus [17].

E. Electronic Ticketing

Electronic Ticketing, a NFC application, brings a new phase in transportation. A recent example of electronic ticketing system is implemented in German city Frankfurt. The transport authority has merged to 'tap-in' payment system, to allow commuters to access travel schedules and other related information. Aconite and Procama has also implemented electronic ticketing system in South Africa. Electronic Ticketing accomplished with NFC enabled mobile phones and tags [16]. User needs to swipe mobile phone at NFC enabled ticket collector. Ticket collector deducts fare amount from associated credit card and provide relief to travellers from making manual payments [14].

F. Medical Healthcare Applications

In medical field, NFC tags can be used as patient ID. Doctors can use it to maintain patient's diagnosis files from remote storage location. It allows doctors to quickly observe patient's prescription and medical history, due tests and procedures [14]. As an example, a NFC enabled system was implemented in Pakistan to treat and monitor infants, diagnosed with pneumonia.

G. Visiting Cards

NFC technology can be used to provide user's contact information. User will provide his contact information in a file and simply transfer it by just tapping two smart phones [9].

H. Parking Lots

NFC technology has found its application in parking lot as well. Parking service provider uses NFC technology to transfer information about vacant space, parking lot number, map and other information. User can tap his phone on NFC tag to provide information about the location of his parked car. The information transfer would also help users to locate their car in parking lot easily by using map and parking lot number [9].

I. Keyless Entry

Keeping door keys every time may be tedious and loosing or misplacing keys can be very frustrating sometime. NFC technology is being used to open closed door of hotels. NFC enabled mobile phones and NFC reader in door lock accomplishes the process [15].

J. Device Pairing

NFC technology provides its abilities in configuring two devices, belonging to same group, for communication purpose. NFC technology allows easy exchange of data to serve the purpose. NFC devices must be brought closer, and with the help of NFC protocol, it establishes a connection to transfer data between devices. NFC reduces user's overhead because of navigating through menus and selecting devices from available devices [16]. Users can send small files over NFC as its less bandwidth is not suitable for sending image files.

Other application examples of NFC technology are E-passports, identity cards, Security clearance or authorized access, starting car engine by waving mobile, etc.

V. THREATS TO NEAR FIELD COMMUNICATION

NFC has facilitated in various application fields with his capabilities. It has grown to an extent that every user is using it in their day to day operations to make life easy. Along with these much advantages, there are some threats that inadvertently come by using NFC technology. These threats resist users to use NFC technology [18]. Following are some threats to NFC technology are mentioned:

A. Eavesdropping

Eavesdropping attack looks for confidential information. It is the simplest form of attack and allows other vulnerable attacks to occur. NFC is a wireless communication that uses RF (radio frequency) waves. Wireless communication is more vulnerable as compared to wired communication, so NFC does. Attacker can interrupt Near Field Communication very easily. It just requires equipments that receives RF signal and can extract information from it. Attacker may use same equipments that a receiver uses to receive signal and decode important information [19].

NFC communication occurs between two devices placed in close proximity i.e. within 10cm. The attacker must choose its position very carefully to eavesdrop signal between devices, which depends on various factors [16]:

- RF field characteristic of sender device
- Characteristic of attacker's antenna.
- Quality of Attacker's receiver.
- Quality of attacker's RF signal decoder.
- Environment conditions like noise level, etc.
- Power sent by NFC device.

Device's operating mode also affects attack. Active device produces its own RF field for communication and Passive device uses other device's RF field for communication. Communication from passive device is much harder to eavesdrop as compared to communication from active devices. Briefly, data communicating in active mode is more susceptible to get eavesdrop from a distance of 10m, as compared to data communicating in passive mode reduces this distance significantly to 1m only [12]. Hence, data communication in passive mode is safer as compared to active mode.

B. Data Corruption

Data Corruption involves data manipulation in between its transmission. Attacker corrupts data to make it unreadable by receiver. In Near field communication, Data corruption disturbs communication. It is performed very easily by transmitting valid frequencies of data spectrum at specified time period. Attacker calculates the time period. He must have wide knowledge about modulation scheme and coding used for transmission purpose [16].

C. Data Modification

Data corruption attack only corrupts data and make it unreadable, but does not allow attacker to manipulate it. Data modification attack alters data's content and its meaning. Data modification attack is performed by applying amplitude modulation to signal. Strength of amplitude modulation on data signal determines the probability of data modification [12].

D. Data Insertion

Data Insertion attack inserts its own data message in data transmission between two devices. Data insertion attack is possible when device take much time to respond [16]. If device 1 transmits data to device 2 and device 2 takes sufficient time for responding, then in between attacker can reply to device 1, making illusion that device 2 has sent the reply. Data insertion attack can be performed from both sides. If attacker and device, both reply at same time, the data will get overlapped and corrupted.

E. Man-in-the-Middle-Attack(MIM Attack)

Man-in-the-middle attack states a situation where two parties communicate via third party, without knowing about the existence of third party in between the communication path. It is also considered as interception [19]. In NFC communication, if devices operate in active-passive mode, then it would not be possible to conduct this attack. Contrary to it, if both devices operate in active mode, then there is probability of attack's occurrence. Practically, man-in-the-middle attack is not possible because devices regularly change their states to active/passive mode [12].

F. Denial of Service

If a user touches NFC device with an empty or corrupted tag, then an error message would get produce and occupy tag memory space to an extent that it would not be able to accommodate authentic messages, resulting system would stop working. The situation is considered as Denial of Service where device is not available to operate [11]. It also refers as Interference. Precaution to the attack, there must be a mechanism that turn on NFC devices to resume its functionality [2].

NFC is being used in many important applications. Threats to NFC applications could lead to great business loss. NFC application developers must find some way to protect NFC communication to make it reliable to use.

VI. PROTECTIVE MEASURES FOR SECURING NEAR FIELD COMMUNICATION

It's important to secure a technology like Near Field Communication which provides a wide range of applications to their users. Threats mentioned earlier made NFC technology vulnerable and restricts users to use it. Therefore, there must be some countermeasures for handling these threats [12]. Following are some measures that can helps in securing NFC [16]:

A. Eavesdropping

Near Field Communication cannot be protected against eavesdropping. Eavesdropping can be restricted on passive mode of communication. But, it is not possible to enforce passive mode of communication only i.e. it will restrict application's functioning. So, we can just try to use NFC's passive mode of communication for its protection.

B. Data Corruption

Data Corruption attack can be restricted by observing RF field on which data is being transmitted. NFC devices must look for RF field's power as significantly high power is required to corrupt data. By this way, attack can be detected.

C. Data Modification

For protecting NFC communication from data modification attack:

- Both NFC devices must operate in active mode. It would be impossible for attacker to modify data in this case. But it can create room for other attacks like eavesdropping.
- Devices must regularly observe RF fields for attack and they must stop transmission upon detecting attack.
- Best solution is to secure NFC channel.

D. Data Insertion

Data Insertion attack can be protected by three methods:

- Devices must immediately (without any delay) provide response to other device. By this way, attacker would not get a change to insert his data on communication channel.
- The replying device must actively listen channel for unauthorized activities. As, channel is open and it is starting point of transmission, any activity like insertion can be easily detected.
- Securing communication channel is the best solution for protecting NFC.

E. Man-in-the-Middle Attack (MIM Attack)

For protecting NFC communication from man-in-the-middle attack, active-passive communication mode must be used. By using this mode, only active devices would generate RF field for valid recipients and don't let attacker to send its data in between. Moreover, NFC devices can also pay their attention to observe RF field to detect any disturbance by attacker.

F. Denial of Service

For eliminating denial of service attack, a precautionary mechanism must be placed that turn on NFC devices to resume their functionality if in case their services got terminated due to some reason [2].

G. Securing NFC channel

Securing NFC channel would resemble the best solution for secured communication. Be it eavesdropping, data modification or insertion, almost all attacks can be prevented through securing NFC channel. NFC channel can be secured by key agreements like RSA based Diffie-Hellmann algorithm or Eliptic Curves to create shared or symmetric keys like AES or 3DES. These shared keys are used in between NFC devices for communication purpose. This method ensures confidentiality, integrity, and authenticity to data transmission.

VII. CONCLUSION

Near Field communication technology enables its users to visualize and experience a new and exciting world. It has facilitated its users with a variety of applications. As, there exits two sides of coin, NFC technology also suffers from some cons as well. There are some threats that restrict users to use it. The paper describes various applications of NFC. It also explains number of threats and its respective countermeasures to protect NFC technology. These solutions could be used to provide security to applications using NFC technology and also attract more users to use it without any problem.

Moving forward, the paper would be very helpful for new learners to understand NFC technology, its applications, threats and security constructs used for protecting it. It also encourages researchers to invent some better remedies for securing NFC from threats to build user's confidence in technology to use it further.

REFERENCES

[1] V. S. Jahagirdar, Naresh Sen, Santosh Kumar Tiwari, "Near Field Communication", 2014, Available at URI: http://hdl.handle.net/123456789/658.

[2] C. Mulliner, "Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones", International Conference on Availability, Reliability and Security, IEEE Computer Society, Proceedings of the 1st International Workshop on Sensor Security (IWSS), 2009.

[3] A. Alzahrani, A. Alqhtani, H. Elmiligi, F. Gebali, M. S. Yasein, "NFC Security Analysis and Vulnerabilities in Healthcare Applications", IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM), ISBN: 978-1-4799-1501-9, 27-29 Aug. 2013, pp. 302 – 305.

[4] R. Ramanathan and J. Imtiaz, "NFC in Industrial Applications for Monitoring Plant Information", Fourth ICCCNT, IEEE-31661, Tiruchengode, India, July 4-6, 2013.

[5] Bekir Bilginer and Paul-Luis Ljunggren, "Near Field Communication", Master's Thesis, Lund University, February 2011.

[6] M. Mareli, S. Rimer, B. S. Paul, K. Ouahada, and A. Pitsillides, "Experimental evaluation of NFC reliability between an RFID tag and a Smartphone", IEEE AFRICON, 2013, pp. 1-5.

[7] X. Yu-ning, "Research on NFC and SIMpass Based Application", Proceedings of the International Conference on Management and Service Science, IEEE, ISBN: 978-1-4244-4638-4, 20-22 September 2009, Wuhan, China, pp. 1-4.

[8] O. Lundahl, "Usability of mobile applications for Near Field Communication", Master of Science Thesis in the Programme Interaction Design, Department of Computer Science and Engineering, Chalmers University of Technology, 2009.

[9] Online Documentation Available at URL:http://mohdaslam.com/smartphone_with_nfc_google_wallet_nfc_tags/

[10] U. Biader Ceipidor, et. al., "Mobile Ticketing with NFC management for transport companies. Problems and solution", Fifth International Workshop on Near Field Communication (NFC), IEEE, 5-5 February 2013, pp. 1 – 6.

[11] G. Madlmayr, J. Langer and C. Kantner, "NFC devices: Security and Privacy", Proceedings of Third International Conference on Availability, Reliability and Security, pp. 642–647, 2008.

[12] F. Jia, Y. Liu, L. Zhang, "Threat Modeling for offline NFC Payments", Journal of Convergence Information Technology (JCIT), Volume 8, Number 4, February, 2013. Available at: http://www.aicit.org/JCIT/ppl/JCIT2782PPL.pdf.

[13] V. Sharma, P. Gusain and P. Kumar, "Near Field Communication", Proceeding of the Conference on Advances in Communication and Control Systems, 2013.

[14] M. U Yaqub and U.A Shaikh,"Near Field Communication, its application and implementation in K.S.A" 2012.

[15] Online Documentation Available at URL:http://www.geektime.com/2014/04/17/how-nfc-technology-could-be-used-in-the-future/

[16] E. Haselsteiner and K. Breitfuß, "Security in Near Field Communication, Strength and Weaknesses", Workshop on RFID Security 2006.

[17] G. M. Miraz, I. L. Ruiz and M. A. Gomez-Nieto, "How NFC can be used for the Compliance of European Higher Education Area Guidelines in European Universities", Proceedings of the First International Workshop on Near Field Communication, IEEE, Computer Society, ISBN: 978-0-7695-3577-7, 24-26 February 2009, Hagenberg, Austria, pp. 3-8.

[18] M. Pasquet, J. Reynaud, and C. Rosenberger, "Secure Payment with NFC Mobile Phone in the SmartTouch Project," in Proceedings of the 2008 international symposium on Collaborative Technologies and Systems. IEEE, May 2008, pp. 95-98.

[19] H. Eun, H. Lee, H. Oh, "Conditional Privacy Preserving Security Protocol for NFC Applications", Consumer Electronics, IEEE Transactions on Consumer Electronics, Vol. 59, Issue. 1, pp. 153-160, 2013.

BIBLIOGRAPHY

Chetna Bajaj (chetnabajaj7@gmail.com) is a research scholar, pursuing Masters of Technology in Information Security from Ambedkar Institute of Advanced Communication Technologies and Research, Guru Gobind Singh Indraprastha University, Delhi, India. She has completed her B.Tech in Computer Science & Engineering from Guru Premsukh Memorial college of Engineering, Guru Gobind Singh Indraprastha University, Delhi, India. Her research interests are Near Field Communication, Software Security Testing and their tools, Mobile Ad-hoc Network, and Virus Detection.

