Academic Education Publishing House

Industry Science and Engineering Vol. 2 No. 1, 2025

Near-field Communication Technology (NFC): Principle Analysis and Intelligent Life Application Research

Yibo Chang, Jiahong Wang*

College of Electronic Engineering, National University of Defense Technology, Hefei, Anhui, China

**Corresponding Author.*

Abstract: Near Field Communication (NFC) technology, as a short-range wireless communication method, enables secure and efficient data exchange between devices within a proximity of 10 cm. Leveraging its advantages in convenience and security, NFC has been widely adopted in mobile payments, smart access control, and IoT applications. This paper systematically explores the physical layer principles, protocol stack architecture, and security mechanisms of NFC, highlighting its performance superiority over RFID and Bluetooth. Through case studies of anti-counterfeiting, card emulation, and mobile payment scenarios, the research identifies key challenges such as transmission rate limitations and interoperability issues. Despite these challenges, NFC demonstrates significant potential in emerging fields like wireless charging and smart tourism. By optimizing chip design, strengthening encryption algorithms, and promoting cross-industry standardization, NFC is poised to become a critical infrastructure for the future Internet of Things (IoT) era.

Keywords: NFC; Mobile Payments; Smart Living; Wireless Communication; Application Scenarios

1. Introduction

NFC technology (Near Field Communication) is a short-range wireless communication technology that allows devices to exchange data and interconnect with each other at close range. NFC technology has been widely applied in various fields such as mobile payment, smart door locks, smart tags, etc., providing users with a more convenient and secure way of interaction. This paper will provide a brief introduction to the principles and applications of NFC technology, and explore its practical application scenarios and potential development prospects in real life.

Since its emergence, NFC has remained lukewarm in the domestic market. A significant part of the reason is that domestic banks, internet companies, and physical enterprises have failed to achieve coordination, lacking the sufficient determination to explore the NFC market. Eventually, in the aspect of mobile payment, it ended in failure with the comprehensive popularization of the QR codes launched by WeChat Pay and Alipay. It is only in recent years that software such as UnionPay QuickPass and the Digital Currency Electronic Payment (DCEP) have started to be widely popularized. Basic hardware facilities like buses and subways have gradually begun to support the NFC card-swiping method. Moreover, with the cooperation between major domestic internet companies and physical enterprises to support the NFC protocol, NFC, which is more convenient and secure than QR codes, is on the verge of ushering in its prime time.

NFC is a short-range wireless communication technology and a contactless identification and interconnection technology. By integrating the functions of an inductive card reader, an inductive card, and peer-to-peer communication on a chip, it is capable of identifying and exchanging data with compatible devices within a short distance. NFC also supports two-way connection and identification. Through NFC technology, the entire authentication and identification process can be simplified, making the mutual access between electronic devices more direct, secure, and clear. It can achieve the functions of simulating, reading, and writing IC cards and electronic tags, as well as auxiliary connection on a single chip. Benefiting from its short-range communication feature, it outperforms its predecessor, RFID technology, in terms of security, and its connection

technology far surpasses that of Bluetooth, WIFI, and the like.

2 Technical Characteristics and Advantages

2.1 Data Security and Integrity

NFC technology employs encryption and authentication mechanisms. Coupled with hardware-level security and an extremely short communication range, compared with software-level Bluetooth connections, it can better ensure the security and integrity of data. Rahul et al. NFC can effectively resist man-in-the-middle attacks through dynamic key exchange and two-way authentication protocols. Its hardware-level security features make it outperform the traditional RFID technology in financial payment scenarios [1]. When transmitting data, each NFC device has a unique identifier, the UID. Two-way authentication is carried out between NFC devices to ensure the legitimacy of the data source. At the same time, the data is encrypted to prevent it from being stolen or tampered with. When using NFC for operations such as payments or access control, authentication methods like passwords or fingerprints are required to ensure that only legitimate users can perform the operations. Since the data for each transaction is dynamically generated and requires the re-establishment of connections and authentication, this further enhances the security and credibility of the transactions.

2.2 Low Power Consumption Cost

NFC technology has extremely low power consumption, generally below 15mW. This can extend the service life and battery life of devices. At the same time, NFC technology also supports the passive mode, that is, only one device needs to be powered, and the other device can obtain energy from the electromagnetic field. This can save resources and costs.

Meanwhile, the hardware cost of NFC technology is relatively low, generally below 1 US dollar. This can reduce the manufacturing cost of devices and the purchasing cost for users. Moreover, NFC technology also supports NFC tags made of materials such as paper and plastic. These tags can be embedded in various items to achieve intelligence and interactivity.

2.3 Simple Portable

The use of NFC is very simple. Just bring an NFC-enabled device close to an NFC tag or an NFC bank card, and the information reading or payment operation can be completed without the need for complex settings. In addition, the NFC chip is small in size and light in weight, and can be easily integrated into various devices such as mobile phones and tablets, enabling these devices to have NFC functions, which is convenient for carrying and using.

Compared with scanning QR codes, NFC only requires a simple touch to complete functions such as scanning and payment. Moreover, it supports card emulation, allowing users to use their mobile phones as access cards, transportation cards, and bank cards.

3. Limitations

3.1 Transmission Rate Limit

The transmission rate limitation of NFC is also one of its characteristics. Although NFC has a relatively high transmission rate over a short distance, reaching about 424 kbps, it still has limitations in large data transmission. This is mainly due to the short transmission distance of NFC, generally within 10 centimeters, which limits the data transmission bandwidth. Also, the transmission rate of NFC is affected by signal attenuation, decreasing gradually as the distance increases. Additionally, the transmission rate of NFC is influenced by other factors like device performance and signal interference.

3.2 Low Degree of Standardization

The low standardization degree of NFC is also an important issue it faces. Compared with some other wireless communication technologies like WiFi and Bluetooth, NFC has a lower standardization degree and lacks unified standards and specifications. This leads to certain compatibility issues among NFC devices from different manufacturers, restricting the widespread application of NFC technology. The technical standards of NFC are not unified, and different manufacturers may adopt different technical standards and implementation methods. This results in differences in communication protocols, data formats, etc. among NFC devices from different manufacturers, making it difficult to achieve interoperability. At the same time, the

application scenarios of NFC are very diverse, involving multiple fields such as payment, identity authentication, access control, and electronic tags. Each field has different application requirements and characteristics, making it difficult to formulate unified standards and specifications. With the popularization of smartphones and the continuous expansion of the mobile payment market, the application of NFC technology is becoming more and more widespread. Different manufacturers are actively promoting their own NFC solutions, making the market competition fierce and it difficult to form unified standards and patterns.

3.3 Information Security Needs to be Strengthened

The lack of awareness of NFC information among people during transactions is another challenge to be faced. Moreover, since NFC uses radio waves during the signal transmission process, it may be potentially exposed to security attacks during transactions. Using devices with NFC may also lead to information leakage due to the reading of the UID on the NFC tag. Therefore, developers need to perfect a set of technologies for information encryption and password protection. At the same time, it is necessary to make people better understand how NFC is used for mobile payment on mobile phones and popularize the relevant knowledge among the public [2].

4. Communication Mode

4.1 Active Mode

In the active mode, an NFC terminal can act as a card reader, emitting a radio frequency field to identify, read, and write the information of other NFC devices. In this mode, both the target device and the device initiating the communication have power, and they can take turns transmitting signals to each other, enabling faster and more efficient communication. This communication method allows for faster and more efficient communication because each device can actively send and receive signals instead of just waiting to receive them. Additionally, devices in the active mode generally require more energy to generate the electromagnetic field and maintain the communication. However, due to the high communication quality and reliability of this mode, it has been widely applied in many application scenarios. For example, in a wireless local area network (WLAN), both the access point (AP) and the client devices need to generate their own electromagnetic fields for communication. In a smart home system, various smart devices also need to communicate and interact through the active mode.

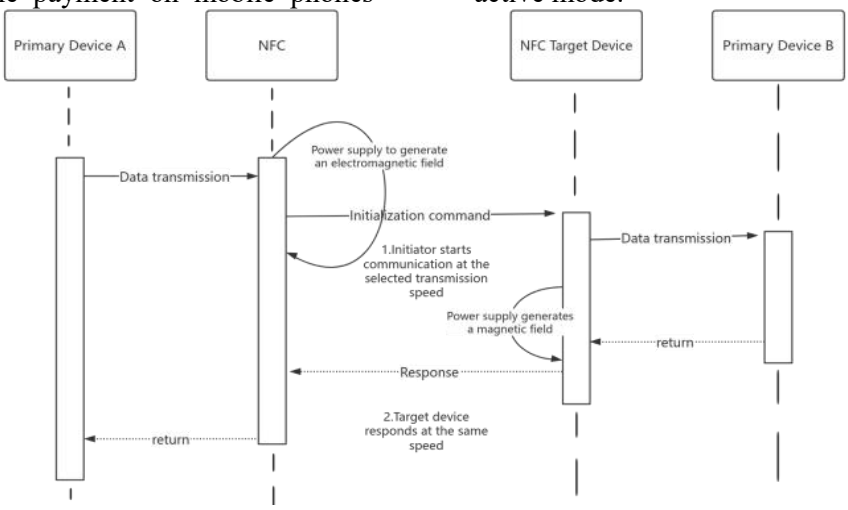

Figure 1. Schematic Diagram of NFC Active Mode Communication

In the active mode, every device that intends to send data must possess the ability to generate its own electromagnetic field. An electromagnetic field refers to the magnetic field generated by electric charges or currents, which can interact with the surrounding substances. In the active mode, a device sends data by generating its own electromagnetic field, and this electromagnetic field can be received by other devices and decoded into useful information, as shown in Figure 1.

4.2 Passive Mode

This mode is the opposite of the active mode. The NFC terminal simulates a card and only responds passively in the radio frequency field emitted by other devices, and its information is read and written. The initiating device will generate a radio signal, and the electromagnetic field of this signal provides energy for the target device. The target device responds to the initiating device by adjusting the characteristics of the electromagnetic field. In this case, the initiating device needs to generate an electromagnetic field, and other devices communicate with the initiating device through load modulation. Although these other devices cannot generate their own electromagnetic fields, they can achieve the purpose of communicating with the initiating device by changing the intensity or characteristics of the electromagnetic field generated by the initiating device.

In the passive mode, the tag card does not generate its own electromagnetic field but relies on the electromagnetic field generated by the initiating device to obtain energy. The tag card reduces the intensity of the electromagnetic field generated by the initiating device, thus creating an effect of load modulation between the initiating device and the tag card. In this way, the tag card can send data to the initiating device. The tag card in the passive mode has the advantages of low power consumption, miniaturization, and portability, so it is widely used in scenarios such as access control systems, transportation cards, bank cards, etc. The specific process is shown in Figure 2.

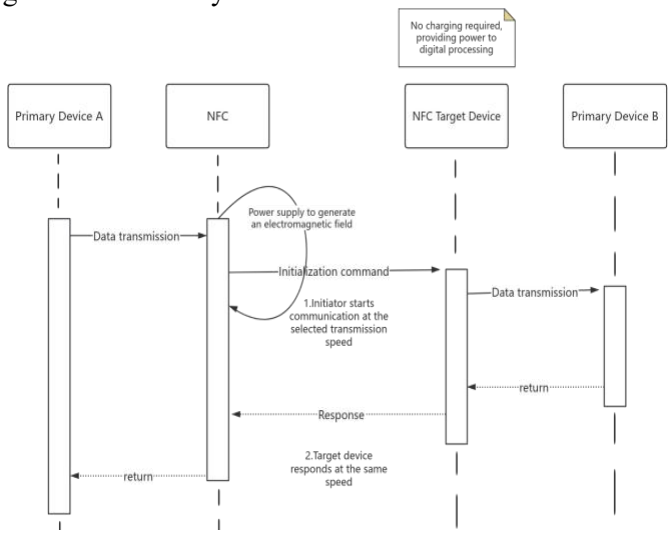

Figure 2. Schematic Diagram of NFC in Passive Mode Communication

5. System Structure

5.1 NFC Controller

The NFC Controller is an important component in the NFC system, which is responsible for controlling and managing the operations of NFC devices. The NFC Controller is usually an independent chip or module that communicates with the main processor (such as a smartphone or other devices) and provides support for NFC functions.

The NFC Controller is responsible for managing the wireless radio frequency communication between NFC devices and other devices. It controls the operation of the radio frequency front-end, including the transmission and reception of radio frequency signals, the selection and adjustment of frequencies, the control of power, etc. Through interaction with the RF layer, it ensures that the NFC device can communicate with other NFC-enabled devices, as specifically shown in Figure 3.

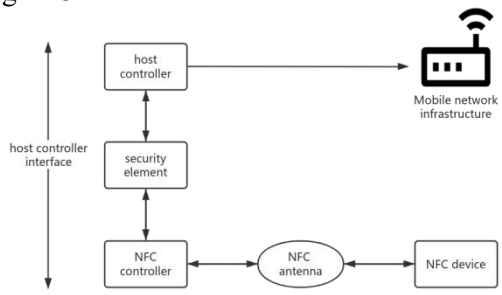

Figure 3. Schematic Diagram of the NFC System Structure

5.2 NFC Interface

The NFC interface consists of two parts: the NFC antenna and the integrated circuit called the NFC controller. This enables near-field communication transactions. The most critical component of any smartphone is the baseband controller or the main controller. The host controller and the NFC controller (which directs data from the NFC-enabled reader to the SE) are connected through the Host Controller Interface (HCI). The main controller is responsible for determining the operating mode of the NFC controller, processing the data sent and received through the HCI, and establishing the link between the NFC controller and the SE.

5.3 Safety Element

The SE (Secure Element) of NFC is a special hardware module used to protect sensitive data and information in NFC communication and ensure the security and integrity of the data. The SE plays an important role in NFC terminals, especially in scenarios involving sensitive information such as payments and identity authentication.

The SE of NFC can be implemented in different ways, including embedded secure chips, payment-type SD cards, and UICC (Universal Integrated Circuit Card), etc. The embedded secure chip is a kind of chip that integrates the functions of the SE inside the mobile phone. This implementation method is relatively concealed and not easy to be replaced or modified. The payment-type SD card is a card that integrates a security module on the SD card and can be used outside the mobile phone, but it requires specific security authentication and authorization before use. UICC is a common SIM card and can also be used as the SE of NFC.

When using NFC, if there is no SE in the terminal device or the SE is not enabled, then sensitive information cannot be used in NFC communication, and only some simple read and write operations can be carried out. If the SE has been enabled in the terminal device, then in NFC communication, sensitive information will be protected and managed by the SE to ensure the security and integrity of the data [3].

6. Key Issues and Key Technologies

6.1 Key Issues

The application of NFC technology in fields such as mobile payment and identity verification requires ensuring the security of data to prevent information leakage and malicious attacks. According to the investigation by NFC Forum, although the physical layer security design of NFC effectively reduces the risk of signal interception, it is still necessary to guard against replay attacks and side-channel attacks in complex network environments [4]. In addition, NFC devices also need to have good compatibility and be able to interoperate with other wireless communication technologies (such as Bluetooth and Wi-Fi) to achieve broader applications.

However, the reading and writing distance of NFC technology is relatively short, usually limited to a range of a few centimeters. Therefore, how to increase the reading and writing distance to meet the requirements of specific application scenarios has become a key issue. At the same time, in order to extend the battery life and improve the user experience, NFC devices need to minimize energy consumption and power consumption while ensuring performance.

Therefore, solving key issues such as security, compatibility, reading and writing distance, and energy and power consumption is an important direction for promoting the further development and application of NFC technology.

6.2 Key Technologies

In order to promote the development and application of NFC technology, first of all, it is necessary to design high-performance NFC chips and antennas to achieve stable communication and a relatively long reading and writing distance. Secondly, develop secure protocols and encryption algorithms to ensure the data security and protection capabilities during NFC communication. In addition, formulate and comply with NFC compatibility standards to ensure the interoperability and connectivity between different devices. Finally, by optimizing the chip design and communication protocols, reduce the energy consumption and power consumption of NFC devices, so as to improve the battery life of the devices and the user experience. The development and application of these key

technologies will further promote the widespread application and market popularization of NFC technology [5].

7. Application Scenarios

Nowadays, with the popularity of smart phones, the application of NFC technology in the mobile phone market also shows a blossoming trend. As a convenient wireless communication technology, NFC is widely used in access control, public transportation, payment, data transmission and other fields.

7.1 Anti-Counterfeiting Traceability

In the fields of branded liquor and luxury goods, NFC technology is widely used for anti-counterfeiting inquiry and verification. For example, Moutai liquor was the first to use NFC anti-counterfeiting tags. Users only need to touch the tags with their mobile phones to query the relevant information about Moutai liquor. This enables consumers to more conveniently distinguish the authenticity of the goods. At the same time, it provides brand owners with a more efficient anti-counterfeiting solution.

7.2 Card Simulation

The application of NFC technology in the public transportation sector is currently the most widespread. The bus and subway systems in many cities support the use of NFC-enabled mobile phones for payment and ticket verification. This provides passengers with a more convenient payment method and reduces the hassle of carrying physical cards [6]. At the same time, it also offers more efficient and secure payment solutions for urban traffic management departments.

In addition, some intelligent access control systems have started to introduce NFC technology, allowing users to use their mobile phones as access cards. This application provides a more convenient and secure access management method for places such as residential communities and offices. However, currently, the application of NFC access control systems is still relatively limited. In the future, with the continuous development of technology, it is expected to be more widely applied.

7.3 Mobile Payment

With the popularity of smartphones, mobile payment has become an indispensable part of people's daily life. NFC technology provides more convenient and secure solutions for mobile payment. Users only need to bind the bank card to the mobile phone, and can complete the payment by approaching the mobile phone to the POS machine when the shopping is settled. This payment method not only improves the payment efficiency, but also reduces the risk of password leakage [7].

8. Future Evolution

8.1 Wireless Charging Technology

Near Field Communication (NFC) wireless charging is a new application scenario of the existing NFC technology. It operates at 13.56 MHz and is particularly suitable for charging small devices. The combination of communication and power transmission reduces the complexity of the system and extends the battery life of the charging device. It is standardized by the NFC Forum and supports power transmission of up to 1 watt in its latest version. In addition, non-mobile products, such as remote controls or toothbrushes, will adapt to the data transmission and power supply transfer of NFC.

8.2 Integration with the Tourism Industry

In terms of transportation, NFC can be combined with QR codes to provide corporate services for passengers getting on and off vehicles [8]. In hotels, the NFC service offers customers the possibility of receiving room keys via NFC-enabled smartphones, allowing them to skip (or reduce) the check-in process and directly enter their rooms [9]. When guests tip the hotel staff through NFC, they can access various types of information, ranging from hotel-related information such as restaurant menus or the hotel's Wi-Fi password to local service-related information like weather forecasts, scenic spots, and public transportation details.

In restaurants, with the help of NFC devices, customers can receive personalized menus, and even filter food options according to ingredients, place orders, and receive reminders when the food is ready. In some souvenir shops, users with mobile phone NFC devices can conduct contactless shopping in the store [10]. At the same time, users can

obtain many coupons from physical stores or websites in their NFC-enabled mobile wallets and transfer money to others through applications [11].

9. Conclusion

With its advantages such as convenience, security, and low power consumption, NFC technology is becoming an important part of smart living. The application of this technology in multiple fields such as mobile payment, intelligent access control, and card emulation demonstrates huge development potential. However, NFC still faces challenges such as a short transmission distance, insufficient standardization, and information security issues.

In the future, by improving the design of NFC chips, strengthening the security encryption mechanism, and perfecting the technical standardization, NFC technology is expected to achieve wider popularization and application. At the same time, with the expansion of emerging application scenarios such as wireless charging and smart tourism, NFC will play a more important role in providing users with intelligent services, bringing more convenience and innovative experiences to daily life.

References

[1] Anusha Rahul; Gokul Krishnan G; Unni Krishnan H. Near Field Communication (NFC) Technology: A Survey. International Journal on Cybernetics & Informatics, 2015, Vol.4 (2): 133-144

[2] McCamon, Mike. THE FUTURE OF NFC. New Electronics, 2023, Vol.56(9): 44-45

[3] Sen, Roshni and Nagaraj Bhat. "An Overview of Near Field Communication and its Application in the Payment Sector." Journal of University of Shanghai for Science and Technology (2021): n. pag.

[4] Sritulasi Adigopula & M. V. Subramanyam. DCNN-RFF-NFC: a novel design of NFC security using deep Convolution neural network-based RF fingerprinting. Neural Computing and Applications, 2025, Vol.37(6): 4439-4453

[5] Lopez-Diaz, Daniel et al. "Unchain Wireless Power-The Future of NFC Wireless Charging." 2022 52nd European Microwave Conference (EuMC) (2022): 640-643.

[6] Gabriella Arcese; Giuseppe Campagna; Serena Flammini; Olimpia Martucci. Near Field Communication: Technology and Market Trends. Technologies (Basel), 2014, Vol.2 (3): 143-163

[7] Liu Tianshuo, Jin Kaili, Shao Zhenyu. The development problems and countermeasures of NFC payment methods. Shopping Mall Modernization, 2019, (24): 26-28

[8] Hou Chao. Application and development of NFC and QR code technology in subway AFC system. Economic and Technical Cooperation Information, 2020, (20): 101

[9] Teng Zhifei, Ma Jinyi, Li Shuang, Du Lei, Chen Le. Access control system based on NFC. Internet of Things Technology, 2016, 6 (6): 25-27

[10] Amaro S, Oliveira D. Determinants of intentions to use near field communication mobile payments in a pandemic context. International Journal of Mobile Communications, 2024, 23(4): 450-473.

[11] Yang Baohong. Analysis of the dynamic effect of the impact of mobile payment development on rural residents' consumption. Business Economics Research, 2023, (14): 47-50.