A Hybrid Transmission System Based on NFC-Enabled Mobile Phones

Jinlong E
College of Software, Nankai University, Tianjin 300071, China
Email: ejinlongnk@163.com

Jie Ma
College of Software, Nankai University, Tianjin 300071, China
Email: majie1765@nankai.edu.cn

***Abstract*—Taking advantage of the characteristics of high security, convenience, and low power consumption in Near Field Communication (NFC) technology, this paper proposes programs of using NFC to establish a connection for Bluetooth and WiFi transmission. The combination of NFC, Bluetooth and WiFi can avoid the complex process of searching devices, pairing or joining the LAN in the traditional Bluetooth and WiFi transmission. It can ensure the security of the data transmission, and solve the problems of complex connection, poor security and large power consumption. The paper also proposes a strategy to choose a proper program for transmission according to the file size. Then a "Hybrid Transmission system" is designed and implemented in Android OS based on the proposed programs and the strategy. The performance of the system proves to be fine, overall superior to the traditional Bluetooth and WiFi transmission. The results show that this system has a high usability in actual use.**

***Index Terms*—Near Field Communication (NFC), Bluetooth, Wireless Fidelity (WiFi)**

I. INTRODUCTION

With the popularity of smart phones and the Internet of Things (IOT), Near Field Communication (NFC), a new technology, has been adopted as the basic configuration of the system on more and more smart phones. The development of this technology makes the idea of integrating the function of smart RF cards into mobile phones possible. As a traditional near field communication technology, Bluetooth has evolved to version 4.0, with a greatly improved protection for the security of transmitted data. However, there are still a variety of attack methods aimed at Bluetooth that have been proposed. Wireless Fidelity (WiFi), the standard of Wireless Local Area Networks (WLAN), has higher data transmission rate, farther communication distance and better encryption and authentication architecture when compared with Bluetooth. With more and more researches on the Ad Hoc network and WiFi Direct technology on new mobile phone products, WiFi is expected to be the most important means for data transmission between devices instead of Bluetooth. However, there are still a series of problems on WiFi transmission, such as long time consumption during connection and large power consumption of the hotspot equipment. As NFC is characterized by convenience of data exchange, high security and low power consumption, it can help exchange parameters to establish a connection for Bluetooth and WiFi transmission. By combining NFC with Bluetooth and WiFi, we can not only avoid all kinds of attacks to the PIN code for pairing of the traditional Bluetooth and the password for joining the LAN of WiFi transmission, but also reduce time consumption of connection before data transmission and the overall power consumption of the system.

Nowadays, NFC Forum has already begun to jointly discuss a program about using NFC to establish a secure connection for Bluetooth with Bluetooth Special Interest Group (SIG). And there are also some studies about the combination of NFC and Bluetooth. [1] has proposed a telemonitoring concept based on NFC enabled mobile phones and sensor devices. Combing Bluetooth with NFC technology, they propose several methods to establish a wireless interface between sensor devices and mobile phones for telemonitoring use. It is mainly about the connection between the sensor device and the mobile phone with an NFC or RFID tag. [2] implements a ubiquitous data delivery system by combining NFC, Bluetooth, WiFi and Zigbee, which can be used in hybrid wireless environments. They propose two policies in terms of high bandwidth and power saving respectively. They are mainly about the switching policies between NFC and other wireless technologies but not the method of using NFC to establish a connection for Bluetooth or WiFi. The researches on combing NFC with WiFi still stay in the concept stage. There are few studies focusing on using NFC to establish a secure connection for Bluetooth and WiFi rapidly. As the NFC hardware module has not been considered as the standard configuration on smart phones yet, only several software applications implement the combination of NFC and

This work was supported by China's Ministry of Science and Technology: Science and Technology based SME Technology Innovation Fund (Granted No. 10C26211200143).
Corresponding author: Jie Ma

doi:10.4304/jsw.8.11.2738-2748

Bluetooth by certain methods without consideration of security. Moreover, no software about NFC and WiFi are developed.

By analysing pairing process, security authentication, encryption mechanisms and the upper connection process by Socket about Bluetooth and WiFi transmission, and by explaining the technological characteristics of NFC, this paper will propose two programs of using NFC to establish a secure connection for Bluetooth and WiFi transmission respectively. And then we take one program of Bluetooth and WiFi each and a program selection strategy to design and implement a "Hybrid Transmission System" in Android OS. Finally, we will test the time consumption about the connection and transmission process and verify the overall performance of the system by comparison with that of the traditional Bluetooth and WiFi transmission.

The rest of this paper is organized as follows: Section II analyses the problems of Bluetooth and WiFi transmission, explains the characteristics of NFC and provides programs to solve these problems by NFC. Section III presents the implementation of a "Hybrid Transmission System" by showing the selection strategy of Bluetooth and WiFi, and the process of connection and data transmission. Section IV tests the performance of the system and compares it with traditional Bluetooth and WiFi transmission. At last, Section V gives a conclusion and the future work.

II. NFC Solutions to Problems of Bluetooth and WiFi Transmission

A. Bluetooth Transmission Problems

The design goal of Bluetooth is to set up a LAN without base stations (similar to Ad Hoc networks), which makes the near field communication possible between multiple devices. For the considerations of band multiplexing and security, the connection between devices is needed before data transmission every time in the design of Bluetooth. For the unpaired devices, security for active devices nearby and pairing with them by the PIN code are also needed. However, this designed transport layer protocol is not easy for setting when the users are connecting their devices. According to some material, the pairing process between some Bluetooth devices costs 5 or 6 seconds, or even as long as 30 seconds in the crowded environment [3]. And a manual intervention is also needed when reconnecting the devices which have been identified in the past, with a poor user experience. As most users only transmit files between two devices through Bluetooth, which seems to be a "peer-to-peer" mode, it will bring additional burden to users when the mechanism of searching and pairing is implemented on the mobile system.

In addition, Bluetooth devices still need to call each other to determine whether it is still online when in the standby mode without data transmission. Although the new version of Bluetooth reduces the workloads through the mechanism of "sniff-subrating" [4], this "polling" type operation still seriously increases the power consumption of the device.

The most serious problem of Bluetooth transmission is the security. By the PIN code entered, Bluetooth devices can generate the link key and the encryption key by E2, E3 and other internal algorithms. Then they can establish a secure connection through authentication and encryption process and verify that the devices are connected at any time thereafter. However, the process is a great risk. Someone has proposed a theoretical process of "estimating the security settings of the paired Bluetooth devices" [5]. The attacker monitors the initial pairing process, and then estimates the security key by a certain algorithm. Then he can masquerade as one of the paired Bluetooth devices. There have been technologies which can shorten the attack time by improving the estimation process. Another method is to intercept the data packet in the first communication process, and then attempt "Brute-force Attack" (through an exhaustive search) aiming at the PIN code for deducing various security parameters. Moreover, we can even forcibly attempt to remove the security key of one of two Bluetooth devices, and then start a new pairing process. Therefore, the Bluetooth equipment manufacturers even suggest that the pairing process of Bluetooth devices should not be in public, but in some hidden occasions. When we usually use the Bluetooth of mobile phones for file sharing, the conventional PIN code by the two sides is easy to be stolen. Thereafter, the interception and decryption of the transmitted data will be not so difficult for hackers.

In short, the Bluetooth transmission technology is a very good short-distance data communication technology, but there are mainly three aspects of problems to be solved: complex establishment of the connection process, large device power consumption and poor transmission security.

B. WiFi Transmission Problems

As Ad Hoc networks is not customized by most mobile devices with a formally unified industry standard, joining the LAN of a wireless router to obtain the corresponding dynamic IP address is still needed for mobile devices before the communication and data transmission between them. Currently, this process is adopted by most LAN chatting and video sharing software applications on the mobile devices. In recent years, many mobile device manufacturers are trying to define Ad Hoc networks communication protocols and security mechanisms on their own device, so no unified standards are promoted. WiFi Alliance, the organization for maintaining WLAN, is not keen on unifying Ad Hoc network standards, but it has defined the WiFi Direct standard which is used to establish WiFi connection and to transmit data rapidly between two mobile devices. This transmission mode is only applicable to the latest mobile phones, which is not widely used. As most mobile devices can be configured as "portable WLAN hotspots", a feasible program of WiFi transmission without an AP besides WiFi Direct can be the following process. One device is configured as a WiFi hotspot, and another one or more devices establish

association with it to join the WLAN of the hotspot device, like associating with an AP. Specifically, searching the surrounding WiFi signal, and making a connection request to the chosen hotspot device (entering a password in the WEP or WPA security mode) are necessary for the associated devices, while authentication and assigning dynamic IP addresses with DHCP are necessary for the hotspot device. Thereafter, the Socket connection of the network layer is completed with IP addresses every time before communication and data transmission between devices. Here we just call this program the "portable WLAN hotspots" program.

WiFi has a significantly higher transmission rate, a larger transmission range and better security than Bluetooth. However, WiFi authentication methods based on protocols such as WEP, WPA, are more complex than the Bluetooth pairing authentication based on the PIN code. Moveover, compared to the Bluetooth connection with device MAC addresses, WiFi uses a dynamically assigned IP address on the network layer to establish a connection for increasing transmission security. Therefore, it will take more time to join the LAN for WiFi than the pairing process of Bluetooth. The same as Bluetooth, it is also necessary to search for hotspots and to send connection request to the manually chosen hotspot. For the "point-to-point" file transmission between two devices, the time consumption for joining the network and manual intervention of the devices undoubtedly bring much burden and poor experience effect to users.

In addition, the hotspot device needs to open WiFi first, waiting for responding and authenticating the associated devices joining the LAN. Then it needs to maintain the status and IP address changes of the devices in the current LAN. It is also necessary to find out devices exiting the LAN by "polling" method. These operations increase its power consumption seriously, and bring a great challenge to the device power management. The same thing also happens to the "server" device of WiFi Direct, which needs to maintain several "client" devices connected with it. But for its not wide use, we only take the "portable WLAN hotspots" program as the WiFi transmission mechanism throughout the rest of the paper.

The initial authentication mechanism of WiFi based on WEP security protocol is quite easy to crack [6]. This protocol does not contain the key management protocol, but only depends on the security of sharing a secret key among users [7]. Therefore, many "wireless network crackers" can invade WEP encrypted LAN easily. With WPA, especially widely used WPA2, the security of WiFi has a great degree of improvement. There is still no effective attack aimed at WPA2, to which the security protocol of WLAN instead of WEP is recommended to be set to by most experts. Compared with the security problems of Bluetooth [3] [5], the WiFi transmission encrypted by WPA2 protocol can be considered safer to some extent.

In summary, there are two aspects of problems to be solved: "the complexity and long time consumption in the process of devices joining WLAN" and "large power consumption of the 'hotspot' or 'server' device".

C. Characteristics of NFC

NFC technology is proposed by Philips, SONY, Nokia, etc. It is a new short-range wireless communication technology, which evolves from the combination of Radio Frequency Identification (RFID) technology and traditional near field interconnection technologies such as Bluetooth, WiFi, etc. This technology makes two devices communicate with each other by touching in a very close range (about 10cm). It works in the 13.56MHz band, with transmission a rate such as 106kb/s, 212kb/s and 424kb/s which can be chosen. Compared to RFID and other near field interconnection technologies, it has the characteristics of near transmission distance, high bandwidth, low power consumption, etc. NFCIP-1, identified as Standard ISO/IEC 18902, elaborates control principles of NFC devices [8]. NFCIP-2, identified as Standard ISO/IEC 21481, defines a flexible gateway system to detect and select the 3 operating modes of the NFC technology: tag-emulation mode, reader/writer mode, and peer-to-peer communication mode [9]. In this way, NFC devices can be used as electronic tickets and electronic wallets, and they can read smart posters and transmit data peer-to-peer by touching.

NFC is applied for communication in a very short distance (10cm~20cm). Such a short distance limits the potential eavesdropping and access by hackers. Therefore, the technology has a very high security. In addition, NFC logic link layer also includes an encryption and authentication procedure and an anti-collision mechanism. It can choose the only target to communicate in the initialization process, to exclude the third-party from controlling the link as the role of "middleman". In the case of sensitive applications such as mobile payment in the tag-emulation mode, the AES encryption algorithm and Triple DES encryption algorithm can also be added, which are adopted by the standard smart card, to the upper application [3].

D. Solutions Based on NFC

In order to solve the problems of Bluetooth and WiFi transmission, several programs can be proposed with the characteristics of NFC technology. Specifically, Bluetooth or WiFi connection can be established by touching two mobile devices which are configured with the NFC module (called "handshake"). Here we do not use the pairing process of the traditional Bluetooth transmission and the associating process of the traditional WiFi transmission.

For Bluetooth, since its secure transmission has a strong dependence on the PIN code and the pairing process, a series of follow-up authentication and the generation of link keys and encryption keys are completed on the basis of the PIN code. However, the generation and exchange of the PIN code are not secure enough during the pairing process, which will cause the encrypted data to be easily intercepted by a third party during the latter transmission process. To solve this problem, a program can be proposed in which the two

devices can be touched together. By exchanging the randomly generated Bluetooth PIN code in NFC active mode, the two devices can verify each other automatically and establish a secure connection. The overall time consumption of this process will be far less than that of the traditional Bluetooth pairing process. Moreover, mobile devices using NFC to establish a connection don't need to search devices and then select the correct one among the numerous searched devices. Instead, they pair with each other directly by touching which greatly simplifies the complicated connection steps of the traditional Bluetooth.

For WiFi, although its security authentication protocol is fairly complete, it still has to rely on the associated devices with the LAN password before joining the LAN built by the hotspot device. The generation and exchange of the password is also not secure, which may result in the interception of transmitted data by a third party. To solve this problem, a program is proposed. The hotspot device can be used to build its LAN based on WPA2 protocol authentication; then two devices are touched, and NFC is used to pass the password randomly generated by the hotspot device to the associated device; finally, the hotspot device verifies the associated device according to the password and let it join the LAN. As NFC can be used to pass the password and other hotspot information, the associated device avoids searching hotspots. Thus, it greatly reduces the time consumption of joining the LAN when compared to the traditional WiFi communication.

The two programs proposed above also improve the user experience by simplifying the user's operation during the connection process of Bluetooth and WiFi transmission. But such programs are involved with the mechanism of the Bluetooth PIN code and the WiFi LAN password settings, and the mechanism of Bluetooth pairing process and WiFi authentication process of joining the LAN. They are in the underlying framework of the system and cannot be called through the SDK interface for security reasons. Therefore, if these two programs are expected to be implemented, it is necessary to use some complex underlying invocation mechanisms.

Besides the above programs, another program can also be used, which encrypts the transmitted data in the application layer in the non-secure mode, or to say, the open mode. Since the symmetric encryption algorithm is simpler and performs better than the public key encryption algorithm, and since NFC can prevent the key from intercepting in the process of transferring, the symmetric encryption proves much better in using the same random key to encrypt and decrypt data. We choose the commonly used AES algorithm as the encryption algorithm in this program both for Bluetooth and WiFi transmission. In fact, the encryption and authentication of WPA2 security protocol is also based on the AES algorithm. Specifically, for Bluetooth, the data sender generates a random key and passes the key to the data receiver through NFC touch; then the sender encrypts the transmitted data with the key and sends the encrypted data to the receiver in the non-secure mode, which makes the pairing process and mutual authentication not necessary between two Bluetooth devices. Thus, the time consumption is further reduced in establishing the connection between two devices before transmission. And for WiFi, as the hotspot device, the data sender sets up a LAN in the open mode. It then generates a random key and passes the key to the data receiver through NFC touch, just the same as Bluetooth. After the receiver joins the LAN built by the sender, the sender can encrypt the transmitted data with the key and send the encrypted data to the receiver. Since the associated device joins the LAN in the open mode, the hotspot device doesn't need to authenticate the associated device rigorously, which can further reduce the time consumption of joining the LAN before data transmission.

Since NFC is designed to have a very short working distance (about 10cm) and not in the same frequency band with Bluetooth and WiFi communication, it is extremely secure to exchange the Bluetooth PIN code, the WLAN password or the encryption key on the application layer with this out-of-band transmission. A third-party device cannot eavesdrop or intercept the exchanged key in such a short distance and low frequency, which will greatly improve the security of data transmission. Moreover, the transmitted data by NFC will be encrypted by AES algorithm or Triple AES algorithm before the transmission, and even some devices have specialized security controls, with hardware-level encryption measures. That will further ensure the security of the transmission process. Therefore, using NFC to establish a connection for Bluetooth and WiFi transmission is particularly suitable for data transmission in the "peer-to-peer" mode between two devices.

At last, the power consumption improvement of these programs should be considered. Considering the "polling" call mechanism to maintain the pairing relationship of two devices, for the program of transmitting the Bluetooth PIN code with NFC, the pairing between devices can be canceled after the completion of the data transmission and pair the devices again before the data transmission next time. However, that brings extra time consumption while reducing power consumption. For the program of maintaining security in the application layer, since the pairing between two devices is not needed before data transmission, the "polling" call can be completely avoided. That will greatly reduce the power loss of the devices brought by Bluetooth. For the programs of WiFi transmission, in order to reduce the power consumption of the device as a hotspot, the hotspot can be closed after the completion of data transmission, so the associated devices will exit the LAN of the hotspot device automatically; then the process of joining the LAN is still needed before data transmission next time. However, this method will also bring extra time consumption. In order to balance these two factors, a power management module can be added. A time threshold can be set, and if the hotspot device is not used for data transmission within a certain period of time, the hotspot device can be closed. That reduces power consumption to a certain extent while avoiding

frequent connections between devices. Due to low power consumption of NFC, there is not too much additional power consumption. Therefore, the overall power consumption of devices will be reduced.

Through the description and analysis above, several programs of establishing a connection for devices before Bluetooth and WiFi data transmission are proposed. The program of maintaining security of transmitted data by the AES algorithm in the application layer is easier to implement and performs somehow better in the aspect of reducing power consumption, so it will be adopted by the "Hybrid Transmission System" described below.

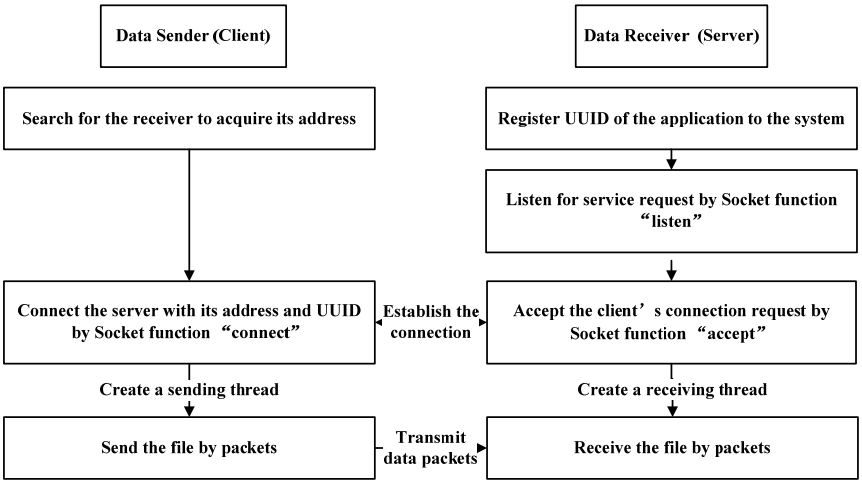

Figure 1. The process of the traditional Bluetooth transmission.

III. A "HYBRID TRANSMISSION SYSTEM" IN ANDROID OS

Here a data transmission system is implemented, which can transmit files with NFC, Bluetooth and WiFi. A strategy is also proposed, which can choose the transmission method among NFC, "NFC + Bluetooth" and "NFC + WiFi" based on the size of the transmitted file. The system is implemented in Android 4.0 OS, so it is necessary to consider some characteristics of NFC, Bluetooth and WiFi implemented by Android. Another two transmission methods (the traditional Bluetooth transmission and the WiFi transmission based on the "portable WLAN hotspots" program mentioned above) are also implemented, and the performance is verified by comparing them with the method adopted in our system.

A. NFC Transmission in Android OS

NFC technology implemented in Android OS can be considered as a kind of "Push" mechanism: Two NFC mobile devices touch together, and one device send the data to the other. The receiver application needs to register to the system of the receiver device. When the receiver device receives the transmitted data, one of the registered applications with a specific identity will be selected to handle the data.

For the way of the implementation of such a transmission method, the transmitted files are generally encapsulated into NDEF (NFC Data Exchange Format) [10], which is defined by the NFC Forum. Specifically, the sender divides the file into small packets and adds them into a corresponding number of "NDEFRecord" arrays; and then they are encapsulated into the "NDEFMessage" object, which will be processed and sent by the bottom level of the Android OS; the receiver resolves the data reversely and merges them into a file.

Android 4.0 OS sets a time limit for NFC link connection in the implementation of NFC. If the data transmission cannot be completed within that time, the transmission will fail. This time period is so short that only a few k-bytes size of data can be transmitted according to the test. Therefore, transmission by independent NFC touch can only transmit small files such as text, business cards, etc.

B. The "NFC + Bluetooth" Program in Android OS

The traditional Bluetooth transmission can be implemented by using the TCP Socket over RFCOMM on the Bluetooth protocol stack. The transmission process can be described as the flow chart in Figure 1.

Two programs of establishing the Bluetooth connection with NFC are proposed. By analysis, it can be found that the first program, i.e. exchanging the randomly generated PIN code, is difficult to be implemented. If the Bluetooth security mode is adopted but the two devices are not paired previously, the pairing dialog will pop up to prompt the user to confirm the pairing. It is implemented by the bottom level of the system to protect the transmitted data, but to some extent it reduces the user experience. The "exchanging PIN code" program can be not implemented by applications unless the Bluetooth Driver and compile the system is modified again. Therefore, here the latter program, i.e. encrypting data in the application layer, is chosen. The flow chart in Figure 2 shows the transmission process.

C. The "NFC + WiFi" Program in Android OS

The "portable WLAN hotspots" program mentioned above can also be regarded as a traditional method of WiFi transmission in the P2P mode compared to WiFi Direct. We will compare it with the "NFC + WiFi" program used in the system. The program can be implemented in Android OS as the description in Figure 3.

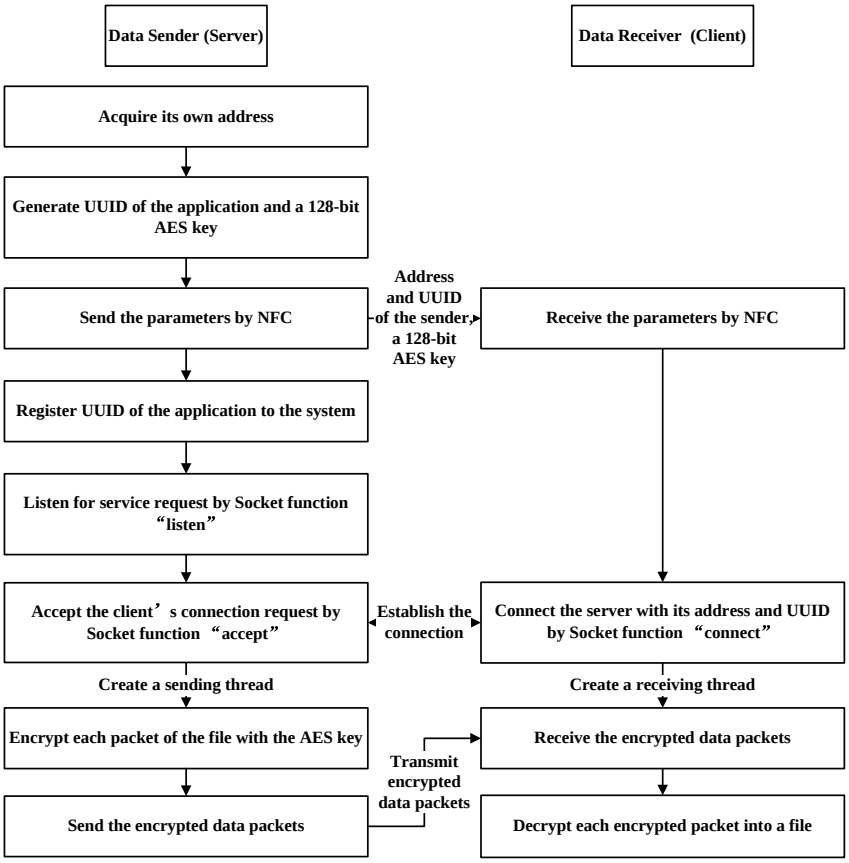

Figure 2. The process of the "NFC + Bluetooth" transmission program.

Two programs are also proposed for establishing a WiFi connection with NFC. Joining the LAN automatically with the encryption and authentication such as WPA2 by the application is not supported by Android OS, because the system only provides the method of entering the password for the searched hotspot to join the LAN. The SDK interface hides the correlative function, and even the correlative class at the bottom level of the system has also been protected by the settings and cannot be called by the upper programs. Here we also implement the program of encrypting data with AES algorithm in the application layer in our system, similar to the "NFC + Bluetooth" program. Figure 4 describes the "NFC + WiFi" transmission program.

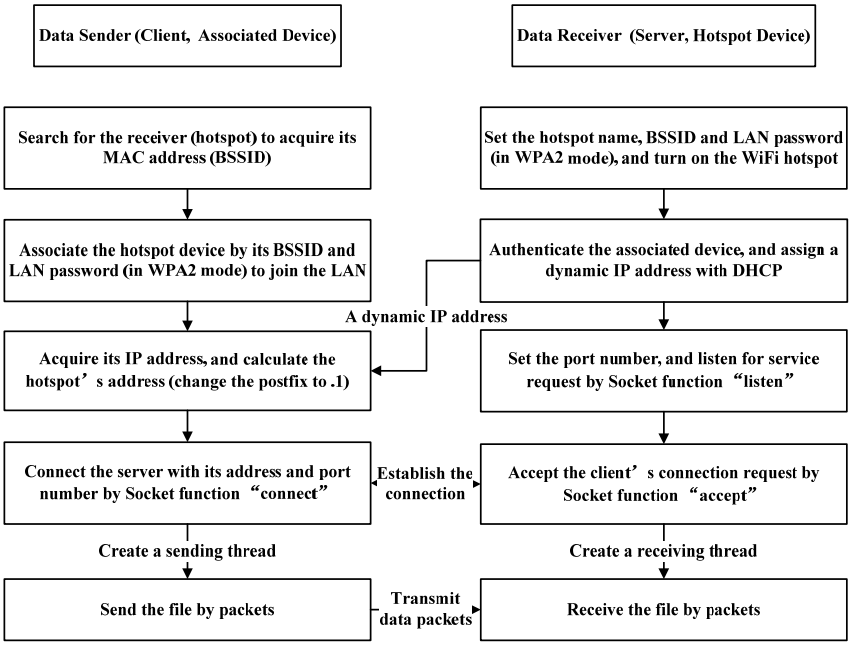

Figure 3. The process of the traditional WiFi transmission.

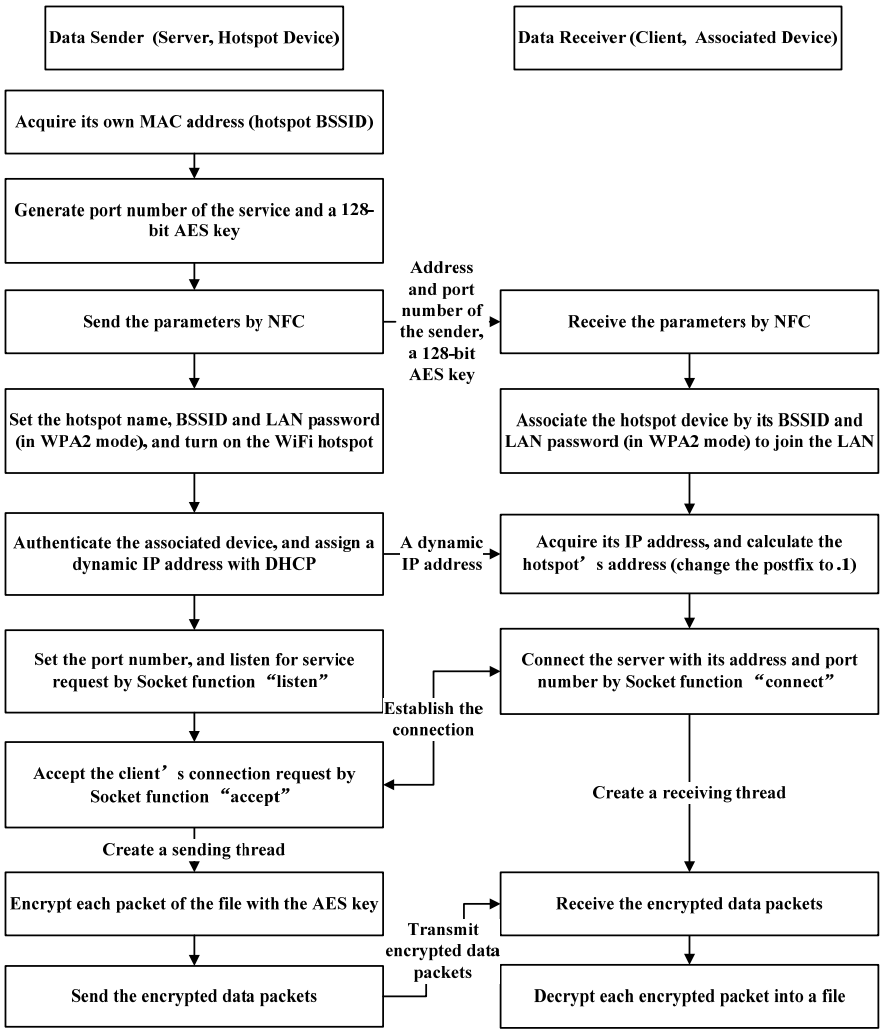

Figure 4. The process of the "NFC + WiFi" transmission program.

In the traditional Bluetooth and WiFi transmission process, as the server, the data server needs to register the service listening mechanism to the bottom level of the system. It starts the service before the sender, and waits for a connection from the sender, which is a typical "waiting for connection" method. Maintaining the listening and waiting thread will also consume a certain amount of system resources. From the flow charts we described above, it can be learnt that using NFC to establish the connection for Bluetooth and WiFi transmission can solve the problems mentioned in Section II, such as poor security, long time consumption, bad user experience and large power consumption. It can also reduce the system resources consumption by reversing the roles between the data sender and receiver. In the program of "NFC + Bluetooth" and "NFC + WiFi", as the Socket server, the data sender can start its listening thread according to the feedback message of successful parameters transmission by NFC. The " Push" mechanism of NFC avoids the "waiting for connection" method adopted by the traditional Bluetooth and WiFi transmission.

D. A Strategy of Transmission Program Selection Based on the File Size

It is necessary to design a strategy for the "Hybrid Transmission System", and select the appropriate transmission program in different cases, for balancing several factors including "the time consumption for establishing a connection between devices", "transmission rate" and "power consumption of devices".

As we all know, WiFi has a quite high transmission rate when compared with Bluetooth. 802.11b, which is commonly used by most mobile devices, has a theoretical transmission rate of 11Mbps, and the transmission rate of 802.11a/g is up to 54Mbps. The Bluetooth, which also works in the 2.4GHz frequency, has a theoretical transmission rate of only about 1Mbps in order to reduce power consumption. The actual transmission rates tend to be lower than the theoretical rate. As tested, the actual transmission rate of WiFi is 4Mbps, which is still higher than 950kbps of Bluetooth [2]. The transmission rate of

NFC is much lower, generally with three kinds of rates including 106kbps, 212kbps and 424kbps. The actual transmission rate of NFC on a mobile device is about 210kbps, which is the middle one of the above three rates.

Then the connection time of these transmission programs are considered. It includes the time consumption of searching devices, pairing between devices and establishing the upper Socket connection for the traditional Bluetooth transmission, and the time consumption of searching hotspots, joining the LAN of the hotspot device and establishing the upper Socket connection for the traditional WiFi transmission. In addition, due to waiting for a connection of the receiver device, there will be extra time consumption during these two transmission methods. As analyzed above, the proposed transmission programs of "NFC + Bluetooth" and "NFC + WiFi" has improved the connection process when compared with the traditional Bluetooth and WiFi transmission. They all include "using NFC to transmit parameters instead of the pairing process" and "establishing the Socket connection reversely in order to avoid the receiver waiting". Comparing these two programs, the "NFC + WiFi" program does not avoid the process of joining the LAN of the hotspot device, and this makes more time consumption than the "NFC + Bluetooth" program. As for the independent NFC touch transmission program, pairing, joining the LAN or establishing the Socket connection are not needed. We only need to establish the NFC connection and then transmit data through the NDEF format packets. The time of establishing an NFC connection is extremely short and can be ignored. Section IV.A will compare the time consumptions of establishing a connection and transmitting data on various transmission methods.

Finally, it is also necessary to consider the power consumptions of several transmission programs. Due to the "sniff-subrating" mechanism, Bluetooth has better reduced power consumption than WiFi with the same working frequency. Bluetooth only consumes 25mW per second when compared to 256mW per second for WiFi in a power-saving mode [11]. Some people also propose to use low-power wireless technology (e.g. Bluetooth) to wake up high-power wireless technology (e.g. WiFi) [12]. But in the actual transmission process, the power consumption of WiFi is a little lower than that of Bluetooth. WiFi provides an energy/bit at 0.14mW/kbps, Bluetooth requires 0.22mW/kbps, and NFC at only 0.0012mW/kbps as the lowest one according to a test [13]. However, the device is used as a hotspot in the "NFC + WiFi" program, so it's necessary to minimize the use of this program.

Above all, the characteristics of these three transmission programs can be summarized as follows: The independent NFC touch program has a low transmission rate, but the connection between devices needs very short time and the power consumption is extremely low. Due to the "link connection time limit" set by Android OS, this program is suitable for the transmission of small files. The "NFC + Bluetooth" program has a normal transmission rate, the process of establishing a Socket connection with parameters transmitted by NFC requires certain time consumption, and the power consumption is low in contrast with WiFi. The "NFC + WiFi" program has a much higher transmission rate, but the extra time consumption of joining the LAN of the hotspot device is also needed when compared to the "NFC + Bluetooth" program, and the power consumption of the hotspot device is very high. Now a strategy of transmission program selection is proposed based on the size of the transmitted file to balance the three factors. Considering the advantages and disadvantages of the three transmission programs, the "NFC + Bluetooth" program should be taken as the main transmission method of the "Hybrid Transmission System". In addition, two file size threshold values are set S1 and S2. When the size of the file is smaller than S1, the independent NFC touch program is used in order to avoid the connection time and reduce the power consumption. When the size of the file is large enough and larger than S2, the "NFC + WiFi" program with higher transmission rate should be used to reduce the possibility of blocking, which is caused by transmitting a large number of packets through the "NFC + Bluetooth" program. The selection of S1 and S2 can be determined according to the time consumption test and statistics of these transmission programs in the process of devices connection and data transmission in Section IV.B. Both the programs of "NFC + Bluetooth" and "NFC + WiFi" adopt AES encryption in the application layer. However, when the file is too large, such as the file size exceeds the threshold value S3, users are recommended to choose the non-encrypted transmission to reduce time consumption. Users can decide whether to adopt it according to the importance degree of the file.

IV. System Performance Testing Experiments

In the "Hybrid Transmission System", three transmission methods are implemented: independent NFC touch transmission, "NFC + Bluetooth" transmission and "NFC + WiFi" transmission. We also implement two traditional transmission methods: the traditional Bluetooth transmission and a transmission using the "portable WLAN hotspots" program (here we just call it "the traditional WiFi transmission"). The time consumptions of establishing a Bluetooth or WiFi connection between devices and transmitting files in different sizes with these transmission methods will be tested, and the results will be analyzed next. All these tests are on two mobile devices—Samsung Galaxy Nexus (CPU 1228MHz, Memory 1GB RAM) and Google Nexus S (CPU 1024MHz, Memory 512MB RAM), which are all configured with Android OS. In every test, the former device acts as a data sender, the latter device as a receiver.

A. Time Consumption Comparisons of Establishing a Connection

Now first the time consumptions of establishing a Bluetooth or WiFi connection by several transmission methods are compared: traditional Bluetooth transmission (by pairing), traditional WiFi transmission (by searching

for hotspots), "NFC + Bluetooth" transmission and "NFC + WiFi" transmission (by NFC touch). In order to reduce errors caused by the different delay time of devices touch or finger click in each time of the test and the interference by other unknown events in the system environment, we carry out 30 groups of tests and average the test results. The time consumption comparisons of these transmission methods are shown in Table I.

TABLE I.
THE TIME CONSUMPTION COMPARISONS OF ESTABLISHING A CONNECTION BETWEEN DEVICES (MS)

Device Side	Traditional Bluetooth	NFC + Bluetooth	Traditional WiFi	NFC + WiFi
Data Sender	3266.13	3209.56	15256.27	7460.80
Data Receiver	4018.73	1780.40	14772.97	6012.30

The noticeable thing in Table I is that the connection process includes two stages: the first stage is pairing for Bluetooth and joining the hotspot's LAN for WiFi; the second stage is establishing a Socket connection in the upper layer.

Among the results in the table, the result of traditional Bluetooth transmission is tested between two devices which have been already paired. If a connection between two devices which have been not paired previously is established, it is necessary to consider the process of one device searching for another, the bottom level of the system of two devices randomly generating and exchanging the PIN code and the user confirming the pairing. All of them will cost about 25 seconds together and have a poor performance. In order to illustrate using NFC to establish a Bluetooth connection is superior to the traditional Bluetooth, it is compared with the "devices paired" situation. As it can be seen from the comparison of the data in the table, ignoring the statistical error, these two methods have almost the same speed in the sender device. That is because using NFC touch to transmit parameters costs little time, and the authentication and encryption key generation process is also needed for the paired devices in the Bluetooth security mode. However, from the aspect of the receiver device, the receiver of the traditional Bluetooth transmission, as the server, starts service before the sender and waits for the connection from the sender. The connection time is very long due to waiting. In comparison, the receiver of "NFC + Bluetooth" transmission establishes the connection with the sender reversely after it acquires the parameters pushed by the sender, so the connection time is much shorter.

Unlike the Bluetooth transmission, the result of the WiFi transmission in the table includes the time consumption of joining the LAN of the hotspot. From the comparison of the data in the table, we can find the latter saves about half the time. That is because the traditional WiFi transmission needs to choose the "server" hotspot to join the LAN after searching for hotspots, while the hotspot transmits the parameters such as BSSID to the associated device in NFC touch method, and avoid the process of searching for the signal of hotspots.

Comparing "NFC + Bluetooth" and "NFC + WiFi", the former one costs less time even though both use NFC to establish a connection for the later transmission. The results demonstrate that after transmitting parameters by NFC touch, joining the LAN of the hotspot is still needed for the "NFC + WiFi" program, while the pairing is no more needed for the "NFC + Bluetooth" program, which can go on the Socket connection directly.

Therefore, from Table II, it can be concluded that using the NFC touch method to establish a connection consumes much less time than the connection of the traditional Bluetooth and WiFi transmission. With this method, the overall time consumption of the transmission is shortened and user experience is improved during the transmission process. In addition, the "NFC + Bluetooth" program costs less time in the process of establishing the connection than the "NFC + WiFi" transmission.

B. Time Consumption Comparisons of Transmitting Files in Different Size

Next, the time consumptions of transmitting files in different size by these transmission methods are compared. Several typical types of files on the mobile device are selected as test cases, including a text file in the size of 2.00KB, a picture file in size of 95.76KB and an audio file in the size of 3.68MB. 10 groups of tests are carried out and the test results are averaged. Table II shows the time consumption comparison.

As it can be seen from Table II, the time consumption of the data receiver is much longer than that of the data sender. That is because the sender reads data from the file and writes it to the Socket file stream, and the bottom level encapsulates the data into packets and sends them to the receiver gradually, during which there is no blocking problem. However, the receiver needs to loop waiting and read the Socket file stream which is parsed from the packets received by the bottom level into the memory buffer, and then writes it into files, until the entire file stream has been read. Both the process of looping waiting and determining the end of the file stream increase the time consumption. The buffer size may also become the efficient bottleneck. For the transmission method with AES encryption, the receiver also needs to process the

AES decryption after reading data from the Socket file stream, which will cost more time.

TABLE II.
THE TIME CONSUMPTION COMPARISON OF TRANSMITTING DIFFERENT SIZES OF FILES (MS)

File Size	Device Side	Traditional Bluetooth (Secure Mode)	NFC + Bluetooth (Non-secure Mode + AES Encryption)	Traditional WiFi (WPA2 Mode)	NFC + WiFi (Open Mode + AES Encryption)
2.00KB	Data Sender	7.5	18.3	11.7	18.7
	Data Receiver	44.0	69.6	42.0	70.2
95.76KB	Data Sender	179.6	412.8	104.3	228.6
	Data Receiver	526.1	621.2	406.1	628.1
3.68MB	Data Sender	19196.3	21420.3	8555.0	12676.5
	Data Receiver	19547.7	24875.4	10680.0	15150.8

If the data results of the first two columns and the last two columns in the table are compared respectively, it can be found that using AES encryption in the application layer with an open mode (for WiFi) or a non-secure mode (for Bluetooth) in the bottom level of the system will cost much more time than the traditional Bluetooth transmission in a secure mode and the traditional WiFi transmission in a WPA2 mode. From the transmission of large files, the time consumption caused by encryption is more obvious. The process of AES encryption and decryption of data in the application layer will increase the burden on the receiver to some extent, so it's difficult to match the speed of receiving and decrypting packets for large files. From this point of view, for large but not important files, only NFC touch should be used to transmit parameters for establishing the connection for Bluetooth or WiFi transmission and transmit the pain text without encryption in the application layer. The traditional "searching and sending a request" connection method will not be taken in the stage of pairing or joining the LAN and establishing the Socket connection. In this way, the time consumption is a little less than the traditional transmission method according to our test, which takes "NFC + Bluetooth" without AES encryption as an example. But we have to say, the data can be easily intercepted by a third party if the transmission process is with little encryption and authentication mechanism. Here we think of the programs of using NFC to transmit WiFi LAN password and Bluetooth PIN code to establish the connection again. By these programs, we can take full advantage of the perfect encryption and authentication mechanisms of Bluetooth and WiFi modules in the system. However, as mentioned above, these programs can be hardly implemented in Android OS. In addition, it will bring much higher power consumption than the program used in our system. Sometimes, it is necessary to make trade-offs between transmission rate, data security and power consumption. In the "Hybrid Transmission System", the program of AES encryption in the application layer is adopted as a default. Users can change the settings to transmit a file without AES encryption in order to enhance the transmission rate.

Moreover, it is necessary to mention the time consumption of the independent NFC touch transmission. Due to the settings of link connection time limit in Android OS, only a few k-bytes size of data can be transmitted by NFC within the time limit, which makes only string parameters and small text files possible. Therefore, 10 groups of test transmitting a file only in the size of 2.00KB are carried out. The average overall time consumption is 1870.2ms, which includes NFC touch with fingers and the transmission process. The transmission rate of NFC transmission is far lower than that of Bluetooth and WiFi transmission, which is also the reason that smart phones set the time limit to prevent large file transmission. NFC technology is more suitable to transmit small size of data and some parameters used to start other transmission technologies.

TABLE III.
THE PERFORMANCE PARAMETERS COMPARISON OF SEVERAL TRANSMISSION METHODS

Performance Parameters	NFC Touch	Traditional Bluetooth	NFC + Bluetooth	Traditional WiFi	NFC + WiFi
Connection Speed	Very Fast	Slow	Fast	Very Slow	Middle
Transmission Speed	Very Slow	Middle	Slow	Very Fast	Fast
Security	Very High	Very Low	Middle	Low	High
Power Consumption	Very Low	High	Low	Very High	Middle
Properly Transmitted File Size	Very Small (about 1KB)	Middle (about 10MB)	Small (about 1MB with AES; about 10MB without AES)	Very Large (about 100MB)	Large (about 10MB with AES; about 100MB without AES)

The comparison of data results in Table I and Table II verifies the feasibility of the strategy of transmission program selection in the "Hybrid Transmission System" proposed in Section III.D. Considering the data results in Table I and Table II, and the above-mentioned test of the independent NFC touch program, we set the file size threshold in the strategy S1 to 1KB and S2 to 1MB. The selection of S3 is more flexible, and here we recommend setting it to 10MB. Of course, it can also be a smaller size. After all, it requires the user to decide whether to encrypt the data in an actual situation.

Through the test, analysis and discussion above, the performance parameters comparison of these transmission methods can be summarized in different aspects of the characteristics shown in Table III.

V. Conclusion

In this paper, programs of using NFC to establish a connection for Bluetooth and WiFi transmission are proposed to ensure the security of the data transmission while reducing the time consumption of the entire transmission process. A strategy of program selection is also proposed to choose the proper program for transmission according to the file size. Then the "Hybrid Transmission System" is designed and implemented which adopts three proposed transmission programs and the strategy, and the performance of these programs in the system has been tested. Compared with the traditional Bluetooth and WiFi transmission program, the "NFC + Bluetooth" and "NFC + WiFi" program have increased the overall performance, and solve the problems of long connection time, complex operation, poor security and large power consumption. Moreover, the strategy makes the system use three programs flexibly based on the file size threshold values, and balance the time consumption of connection and transmission as well as the power consumption. The problem of blocking appears when transmitting large files encrypted in the application layer. This problem is solved by recommending non-encrypted transmission when the file size exceeds another threshold value. Actually, the programs of exchanging the randomly generated PIN code and LAN password can be successfully implemented, to further improve the overall efficiency and security in the transmission process. These programs will be further studied in the future.

Acknowledgment

The authors wish to thank the members of the Embedded System and Information Security Lab, College of Information Technical Science, Nankai University for their support and help. This work is supported in part by a grant from China's Ministry of Science and Technology: Science and Technology based SME Technology Innovation Fund (Granted No. 10C26211200143).

References

[1] J. Morak, H. Kumpusch, D. Hayn, etc. Design and Evaluation of a Telemonitoring Concept Based on NFC-Enabled Mobile Phones and Sensor Devices, *IEEE Transactions on Information Technology in Biomedicine*, Vol. 16, No. 1, pp.17~23, 2012.1

[2] C. H. Wu, C. H. Wu, Z. W. Hong, K. S. Huang, A Ubiquitous Data Delivery System in Hybrid Wireless Environments, *Journal of Convergence Information Technology*, Vol. 6, No. 2, pp.329~341, 2011.2

[3] T. Ghanname, How NFC can to speed Bluetooth transactions today, *EETimes*, 2006.2.14, http://www.eetimes.com/design/communications-design/4012606/How-NFC-can-to-speed-Bluetooth-transactions-151-today

[4] Bluetooth Special Internet Group (SIG). *IEEE 802.15.1 Specification of the Bluetooth System Profile v2.1+EDR*, 2007.7

[5] Y. Shaked, A. Wool, Cracking the Bluetooth PIN, *Proceedings of 3rd USENIX/ACM Conference on Mobile System, Application and Service, MobiSys 2005*, pp.39~40

[6] S. Fluhrer, I. Mantin, A. Shamir, Weaknesses in the Key Scheduling Algorithm of RC4, *Eighth Annual Workshop on Selected Areas in Cryptography*, Vol. 2259, pp. 1~24, 2001

[7] N. Cam-Winget, R. Housley, D. Wagner, J. Walker, Security Flaws in 802.11 Data Link Protocols, *Communications of the ACM*, Vol. 46, No. 5, pp. 35~39, 2003.3

[8] NFC Forum, *Near Field Communication Interface and Protocol (NFCIP-1) 2nd Edition*, 2004.12

[9] NFC Forum, *Near Filed Communication Interface and Protocol (NFCIP-2) 1st Edition*, 2003.12

[10] NFC Forum, *NFC Data Exchange Format (NDEF) Technical Specification 1.0*, 2006.7.24

[11] Y. W. Bai, C. H. Huang, Remote Power On/Off Control and Current Measurement for Home Electric Outlets Based on a Low-power Embedded Board and Zigbee Communication, *Proceedings of the International Symposium on Consumer Electronics, ISCE 2008*, 2008

[12] Y. Agarwal, C. Schurgers, R. Gupta, Dynamic Power Management Using on Demand Paging for Networked Embedded Systems, *Proceedings of the Asia and South Pacific Design Automation Conference, ASP-DAC 2005*, Vol. 2, pp. 755~759, 2005

[13] Y. Agarwal, T. Pering, R. Want, R. Gupta, SwitchR: Reducing System Power Consumption in a Multi-client, Multi-radio Environment, *Proceedings of International Symposium on Wearable Computers, ISWC 2008*, pp. 99~102, 2008

Jinlong E received his B.S. degree in Software Engineering in 2007 from Nankai University, China. He is current a master student in Computer Software and Theories, College of Software, Nankai University, China. His research interests are Wireless Networks, Mobile Computing and Internet of Things (IOT).

Jie Ma received his B.S degree in Physics in 1982 from Nankai University, China. He is current a professor in College of Software, Nankai University, China. He publishes many research papers in journals. A number of his studies have won the provincial and ministerial awards of china. He has a number of social part-time jobs and many projects in research supported by national, provincial and ministerial funds. His research interests are New Media, Embedded System and Wireless Networks.