DOI: 10.3745/KIPSTA.2010.17A.3.137

W-USB를 위한 NFC Handover 기술

한 영 선† · 김 태 선†

요 약

최근 모바일 장치 시장이 급격히 성장하면서 모바일 장치의 기능성 또한 빠르게 발전하고 있다. 소비자는 모든 환경에서 이기종 모바일 장치간 데이터 전송 또는 무선 인터넷을 통한 멀티미디어 데이터 전송이 가능하기를 원한다. 이와 더불어, 단일 모바일 장치가 블루투스, 와이파이(Wi-Fi), W-USB, NFC와 같은 다양한 connectivity 기술을 채용하는 경향도 보인다. 이와 같은 시장의 흐름에 따라 이기종간 association 기술의 중요성이 점차 부각되고 있다. 본 논문은 기존 NFC handover 프로토콜을 확장하여 W-USB 기술의 NFC association을 지원하는 방법을 다룬다. 또, W-USB 기술의 NFC association 표준과 NFC handover 프로토콜 간의 차이점을 설명하고 기존 NFC handover 프로토콜을 확장하여 이를 해결할 수 있는 방법을 제시한다. 마지막으로 본 논문은 W-USB handover 프로토콜 지원을 위한 NFC 시스템 구현에 대해 기술한다.

키워드 : NFC, 무선 USB, 핸드오버, 통신 협약, 연결성

NFC Handover Technology for W-USB

Youngsun Han† · Taeseon Kim†

ABSTRACT

Recently, as the consumer market of the mobile device is explosively getting bigger and bigger, both of the usability and applicability of the mobile device are also growing rapidly. The customers prefer to transfer data between the different mobile devices and download multimedia data via the wireless connection even wherever they are. The trend of mobile devices also shows the tendency of employing the various connectivity technologies such as Bluetooth, Wi-Fi, W-USB, NFC, and so on in a single mobile device. With this market trend, the importance of the technology associating different devices is getting increased gradually. In this paper, we present how to support the NFC association of the W-USB technology by extending the existing NFC's handover protocol. We also explain the differences between the NFC association and the handover protocol, and propose the method to resolve the differences by extending the handover protocol of the NFC technology. Finally, we describe how to implement the NFC system supporting the W-USB handover protocol.

Keywords : NFC, W-USB, Handover, Association, Connectivity

1. Introduction

The near field communication (NFC) [1-3] is a high frequency, especially 13.56 MHz, wireless communication technology, which is able to transfer data between devices in the short range, about under 10 cm. The NFC can support both the reader and card functionalities on one single device. The NFC technology is completely compatible with the existing contactless smartcard infrastructure, which is being used for the electric payment. Also, the technology supports the following functionalities additionally [4]: RFID reader [5], Peer-to-Peer (P2P) communication, and Handover. Although the handover is still an optional specification, the demand for the technology is being expected to dramatically increase in the consumer market, especially in the mobile phone market.

The wireless universal serial bus (W-USB) [6, 7] is also a short range RF communication technology based on the ultra wide band (UWB) technology [8]. The UWB is able to transfer data with up to 480 Mbps at distances up to 3 meters and operates with radio frequency range from 3.1 to 10.6 GHz. Also, since the W-USB has the root on the universal serial bus (USB), one of the most commonly used connectivity standard, it performs the as-

† 정 회 원 : 삼성전자 시스템 LSI 책임 연구원
논문접수 : 2010년 5월 31일
심사완료 : 2010년 6월 4일

sociation-based communication like the USB technology. In order to securely associate a pair of W-USB devices, the W-USB specification proposes the following four association models: Cable, Numeric, Fixed PIN, and NFC based association frameworks.

First, the cable association model is derived from the existing USB technology. It occupies a USB cable in order to associate between a host and device. If the association process is completed, the connection via the USB cable is not needed any more and the wireless communication can be followed. Since the model is supposed to use the USB Cable-Based Association Framework (CBAF), a certified wireless USB device must report whether the CBAF is supported or not when the device is connected through a cable with its wired USB port.

Second, the numeric association model performs the first time association over the UWB communication using the standard certified wireless USB control requests. In order to temporarily establish a secure channel against the man-in-the-middle attack, the Diffie-Hellman cryptographic protocol [9, 10] is employed. Thus a user has to personally verify the match of the two values from the Diffie-Hellman keys respectively displayed on the two additional displays.

Third, the fixed PIN association model also uses the UWB communication like the numerical model. But different from the numerical one, this model uses the devices preliminarily programmed with the fixed PIN at the manufacture time using a random secret. The PIN information will be secretly described in the user manual and a user can perform the association by entering it to both the host and device.

Finally, the NFC association model uses the NFC technology to associate different W-USB devices. Because the association could be completed by just approaching two different W-USB devices with the NFC supporting, it provides enough usability being able to be widely employed in the market. Also, due to the close proximity, it provides the secure nature against the malicious attacks. However, because this model was designed without considering the existing handover protocol of the NFC technology, it therefore might not be compatible with the NFC technology.

As previously mentioned, different from that the NFC Forum has not specified the handover information for the WUSB yet, the W-USB technical group already described the NFC association methodology in its specification [11]. Although the handover protocol is capable of being extended to support the NFC association, it is also apparent to have significant differences between both of them. In this paper, we present how to extend the NFC handover protocol in order to support the NFC association of the W-USB technology. With this approach, we provide a new method efficiently resolving the protocol conflict. We exploit the differences of the NFC association from the handover protocol in detail, and describe the way to resolve the differences in a point of view of the NFC technology. In the case of the security channel, we propose two feasible solutions for further research. We also describe how we implemented the W-USB handover protocol in both of software and hardware manners.

This paper is organized as the following: In Section 2, we analyze both the NFC handover protocol and the NFC association technology of W-USB. In Section 3, we describe the differences between the two protocols. We also present the way to combine the two protocols into one in aspect of the NFC technology. The implementation details of the integrated protocol are shown in Section 4. Finally, the conclusion is made in Section 5.

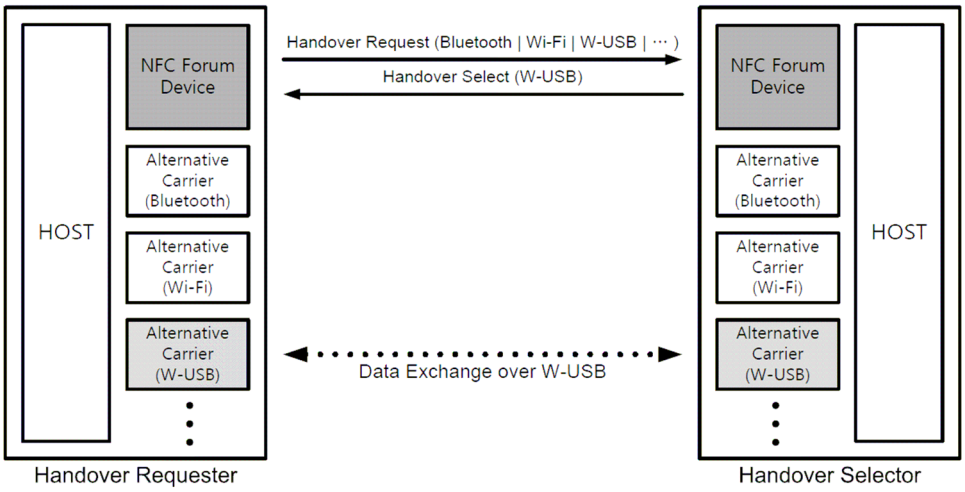
2. Protocol Analysis

In this section, we are going to briefly describe both of the negotiated handover protocol of NFC and the NFC association protocol of W-USB.

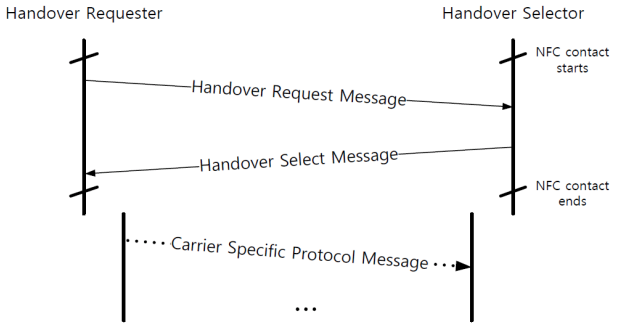
2.1 Negotiated Handover Protocol of NFC

The handover protocol is designed to support a pair of NFC devices to negotiate one or more alternative carriers for further data exchange. As shown in (Figure 1), the handover process is performed between a handover requester and a selector. Each NFC device can contain several kinds of alternative carriers such as Bluetooth, Wi-Fi, W-USB, and so on. After the handover negotiation is finished, the additional data exchange will be continued by the one or more selected carriers.

As in the example described in (Figure 1), the handover requester sends a handover request message first to the selector while announcing its alternative carriers, Bluetooth, Wi-Fi, W-USB, and so on. Also, the handover selector chooses only the W-USB as an available data carrier for the further data exchange. As a result, it will be performed to associate the W-USB devices and transfer data between each other. (Figure 2) shows the sequence of the negotiated handover messages between the handover requester and selector. After the NFC contact is started, one or more pairs of handover request and select messages would be transferred between each other by the



(Figure 1) Negotiated Handover with Single Selection [4]

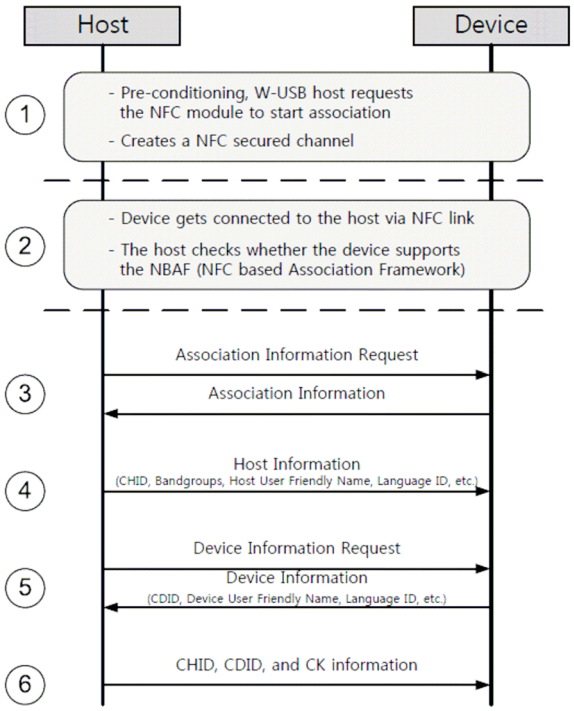


(Figure 2) Handover Message Sequence [4]

end of the contact. If the handover process is performed adequately, the carrier specified data communication will be followed.

2.2 NFC Association Protocol of W-USB

(Figure 3) shows the NFC association protocol specified in the W-USB specification [11]. As shown in the figure, the association protocol mainly consists of the six steps. First of all, a host asks its NFC module to start the association with other W-USB devices near itself. If an NFC secured channel is established between the host and the device, the host will check if the device supports the NBAF (NFC based Association Framework). Finally, after performing the previous processes, the data transfer for the association will be followed. The host provides it's CHID (Connection Host ID) to the device along the additional information such as band groups, host user friendly name, language ID, and so on. If the device has a valid CC (Connection Context) matching to the CHID, the device will transfer the association information including the CDID (Connection Device ID) extracted from



(Figure 3) NFC Association Protocol Overview [11]

the CC. The CC is comprised of CHID, CHID, and CK. Also if the CDID is correctly matched with the host's CC, the host will generate and send all of the CHID, CDID and CK (Connection Key) to the device. Since it means that the device has been associated before, the NFC association process will be completed. However, if the host has no matching CC with the CDID from the device, explicit user conditioning may be optionally required for the association. A new association could be performed by the conditioning.

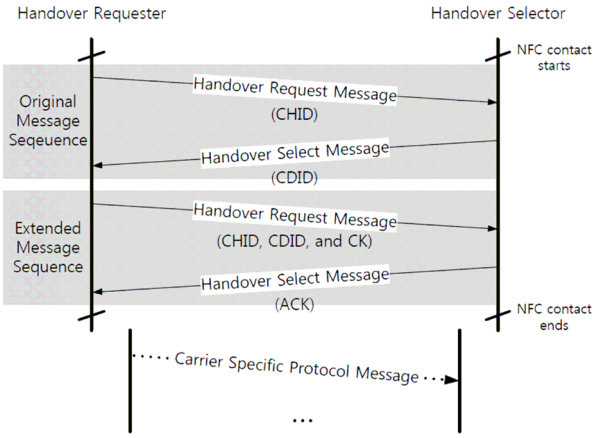
3. Protocol Integration

In this section, we will exploit the difference between the two protocols and propose the way to combine them into an integrated protocol in the point of view of the NFC technology.

3.1 Association Sequence

(Figure 4) shows the extended handover message sequence for the association of the W-USB. A pair of handover request and select messages is appended after the original message sequence in order to complete the NFC association. Although the association protocol is originally ended by the action that the host sends the CHID, CDID and CK to the device, in the extended message sequence, the device is also supposed to finally transfer an acknowledgment message to the host. This is because the NFC handover message sequence basically consists of one or more pairs of the messages: Handover Request and Handover Select. With the acknowledgment message, the handover selector will let the requester know whether the association is completely terminated or not. We also discard to require the explicit user conditioning of the NFC association even if the handover requester does not have a CDID copy matched with the CDID in the handover select message.

Instead of performing additional conditioning procedure, the requester will just send a new CC to the selector. Because of the NFC's natural characteristic originated from the close proximity, we can simplify the protocol while avoiding the accidental or malicious associations. But we also have to make sure that we can optionally

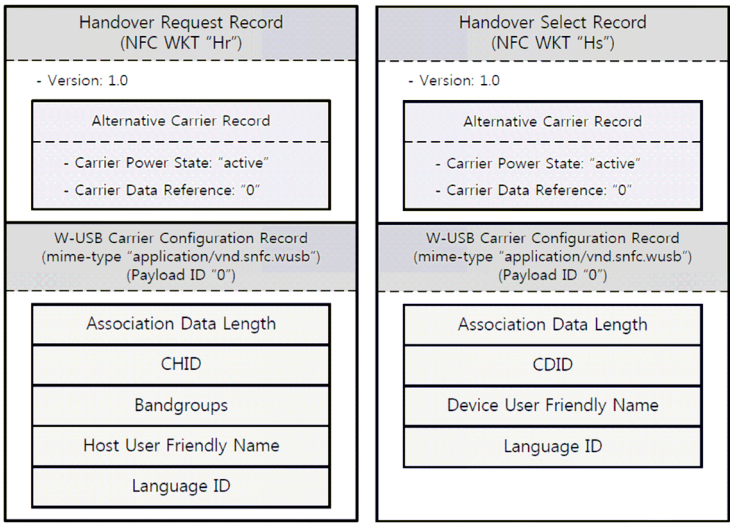


(Figure 4) Extended NFC Handover Message Sequence

employ additional conditioning steps in order to reinforce the security of the NFC communication for the future usage. The normal W-USB communication will be possible after the extended handover message sequence.

3.2 Association Information Structure

(Figure 5) shows the organization of the handover request and select records for the NFC association of W-USB. The records are constructed by exactly following the NFC handover specification [12]. Each of the handover record contains its version number, alternative carrier record, and carrier configuration record. The alternative carrier record shows the current power state of the alternative carrier device specified by the following carrier configuration record. The current power state has totally four states: Inactive, Active, Activating, and Unknown. Only of the alternative carrier device in the Active state is able to be employed for the alternative



(Figure 5) NFC Handover Request and Select

communication after the handover process. The Inactive state means the carrier device is currently turned off and the Activating state does the device is not active yet.

The W-USB carrier configuration record contains the record type and association information. In the examples shown in the figure, the type of the configuration record is configured to the mime-type, "application/vnd.snfc.wusb", and the association data including either CHID or CDID is just followed. Also, the records for the extended NFC handover message sequence was designed by respectively replacing the association data with the CHID and CDID with a group of CHID and CDID, and CK and an acknowledgment.

3.3 Secured Channel

The NFC association protocol is recommended to transfer its association data via the NFC secured channel in the W-USB specification [11]. But, unfortunately the NFC-Forum has not formally determined to adopt the specification of the NFC-SEC secure channel [13]. This is because eavesdropping of the communication between the NFC devices is difficult due to its close proximity. Therefore, even if the demand to the NFC security is becoming bigger, we will not employ the secured channel in the current version of the W-USB handover protocol. However in order to support the secured channel in the future research, we propose the following two methodologies.

3.3.1 NFC Specific Key Agreement

As described in [9], because the NFC technology has the inherent protection feature against the man-in-the-middle attack, in order to significantly reduce the computational power requirement we don't have to employ any heavy asymmetric cryptography. The key agreement scheme in [9] uses the synchronized RF signals from two devices to be associated in order to share the secure secret. Since they send and receive the randomly generated bits stream with the same amplitudes and phases to each other, the outside eavesdropper cannot distinguish the separated two bits streams. However each device knows what it sent to the other, the secure secret could be transferred securely.

3.3.2 Secure Element Employment

Because the NFC is specified to support the Single Wired Protocol (SWP) [14] to communicate with secure elements (SEs) [15], we could use the SEs for decoding and encoding the cryptography information. These SEs are usually employed by the mobile phone in order to support the mobile commerce. Due to this reason, although this approach may not be generally used for the W-USB handover protocol, it could be one of the attractive methods for providing the secured channel with a few efforts during the NFC association.

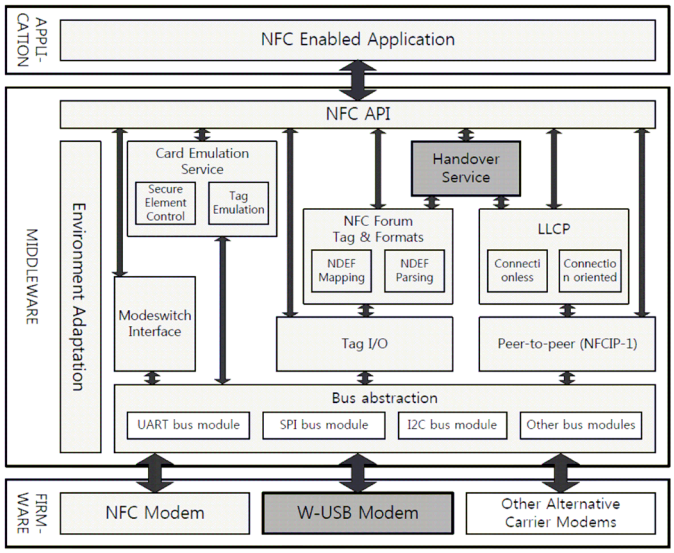
4. Implementation

In this section, we will describe how to support the W-USB handover protocol by extending our existing NFC software framework. Also the brief description of the hardware design will be followed.

4.1 NFC Software Support

(Figure 6) shows the overall structure of our NFC software framework. The middleware interfaces with both of the NFC enabled application and the firmware. It communicates with the application by using our proprietary API and does with the firmware using ETSI [14] HCI (Host Controller Interface) specified interface over the communication channel provided by bus abstraction. As shown in the figure, our software framework is able to support the following four protocols: Card emulation, NFC data exchange format (NDEF), Logical link control protocol (LLCP), and Handover. The mode switch interface was implemented to support the firmware's autonomous mode switch functionality specified in the NFC specification [4]. Also the tag I/O module was designed to provide arbitrary data transmission and reception according to the currently selected tag type. The NFCIP-1 module supports the peer-to-peer data transfer between two different NFC devices. The handover service is designed to be able to control both of the components for NDEF and LLCP protocols. The handover service performs the NFC association process of the W-USB by using the LLCP protocol. It also employs the NDEF protocol implementation in order to encode and decode the NFC handover records. All of the commands from the handover service unit can be transferred to the firmware of the W-USB modem through the abstracted bus interface. The handover process also could be commonly applicable to other alternative carriers.

(Figure 7) shows the structure of the HCI message of our NFC software framework. The middleware can communicate with the firmware by following the format of the HCI message. The chaining bit indicates whether more data will come after this message or not. If it is zero, we could expect additional message. The pipe ID is the value of the pipe identifier. The pipe could be created

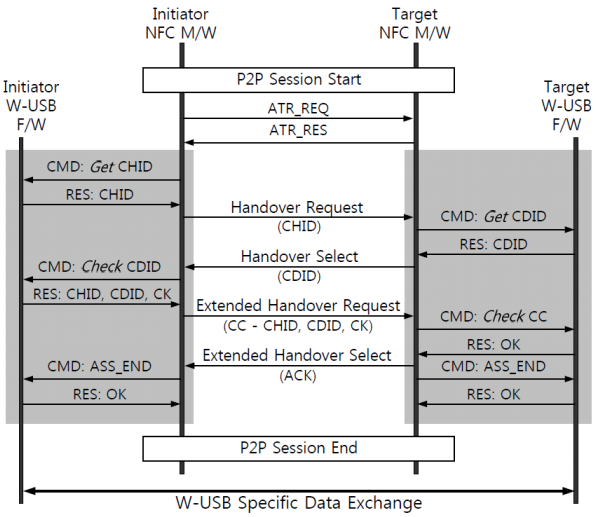


(Figure 6) NFC Software Framework for W-USB

(Figure 7) HCI Message Structure

either statically or dynamically depending on the service. Also the HCI message can have the following three types: command, response, and event. When the command message is sent, the response message will be always waited back. The event message will never get the response. The command ID has to be defined differently for the each service. Finally, the data field is optionally occupied in the message. The gray-colored part in (Figure 8) shows the HCI command sequence for the W-USB handover.

In order to construct the handover messages, the NFC



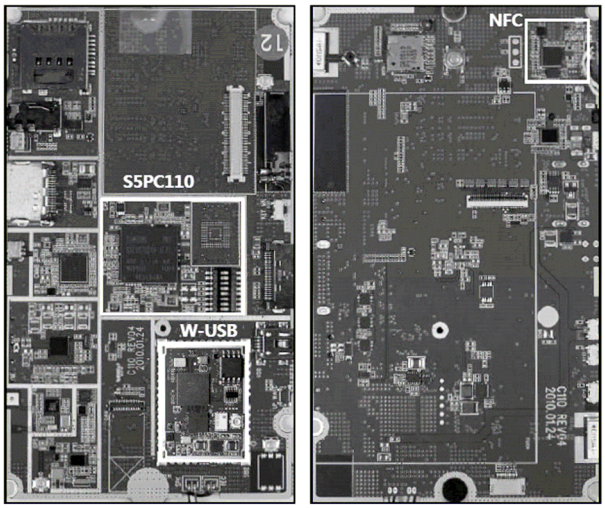
(Figure 8) HCI Message Sequence Diagram

middleware on each device sends the HCI commands to and receives the responses from the W-USB firmware. After the handover is completed, the P2P session will also be terminated and the W-USB specified data communication will be followed.

The total delay for the handover process is comprised of the P2P session establishment and actual NFC association time. Although the current NFC handover specification [12] does not specify the time limit for the handover protocol, we minimized the latency by simplifying the HCI message sequence and renouncing the secure channel attribute. As a result, the extension generates only a small time overhead not perceptible by users.

4.2 NFC Hardware Design

(Figure 9) shows our NFC development board supporting the verification of the W-USB handover. The board is originally designed as a Smartphone to demonstrate the functionality of the Samsung''s private application processor, especially Samsung S5PC110, and has its root on the SMDK-C110 code development kit for the S5PC110 processor, based on ARM Cortex A9. It provides the Android OS 2.0 running on the application processor. It also supports several connectivity technologies such as NFC, W-USB, Bluetooth, Wi-Fi, and so on. <Table 1> describes the brief hardware information for both of our NFC and W-USB implementations. The NFC hardware employs an 8051 based asynchronous HT80C51MX HandShake processor [16], 128K flash memory for code storage, and 4K ram for data. It works with 13.56 KHz operating clock frequency derived from the radio frequency and supports up to 424 Kbps data rate for the



(Figure 9) NFC Hardware Design

〈Table 1〉 Hardware Specification of NFC and W-USB

	NFC	W-USB
Processor	HT80C51MX	ARM 926-EJS
Memory Size	128K Flash, 4K RAM	96K TCM, 256K RAM
Operating Clock Freq.	13.56 MHz	200 Mbps
I/O Interface	I2C, SPI, UART	I2C, UART, USB, SDIO
Maximum Data rate	424 Kbps	480 Mbps

P2P communication. Several I/O interfaces such as I2C, SPI, UART, and so on are included to support the flexible host control interface. The W-USB hardware occupies an ARM 926-EJS processor including 96K TCM (Tightly Coupled Memory) and 256K RAM. It operates with 200 MHz system clock and provides maximum 480 Mbps data transmission speed. In our development environment, both of the NFC and W-USB chips communicate with the host application processor via the I2C interface.

5. Conclusion

In these days, since the consumer market demand to the various connectivity technologies, such as Bluetooth, Wi-Fi, W-USB, NFC, and so on, in a mobile device is getting bigger and bigger, the importance of the association technology is also gradually getting increased. In this paper, we described the negotiated handover protocol of the NFC technology which is specified to support more user-friendly and simple association. Also, we presented how to extend the conventional NFC handover protocol in order to support the NFC association protocol of the W-USB. With this approach, we could provide a new method for the W-USB handover resolving the conflict between the existing NFC handover protocol and the NFC association of the W-USB technology. Finally, we showed the implementation details of the handover protocol for the W-USB. For the future research, we also proposed two methodologies supporting the secure channel. We are going to study the methodologies more and employ them in the next version of the W-USB handover protocol.

References

[1] Yaw Anokwa, Gaetano Borriello, Trevor Pering, and Roy Want. A user interaction model for NFC enabled applications. In *Proc. 5th IEEE Int. Conf. on Pervasive Comput. Commun. Workshops*, pp.357-361, 2007.

[2] Arjan Geven, Peter Strassl, Bernhard Ferro, Manfred Tscheligi, and Harald Schwab. Experiencing real-world interaction. results from a NFC user experience field trial. In *Proc. 9th Int. Conf. on Human computer interaction with mobile devices and services (MobileHCI)*, Vol.309, pp.234-237, 2007.

[3] Robert Hardy, Enrico Rukzio, Matthias Wagner, and Massimo Paolucci. Exploring expressive NFC-based mobile phone interaction with large dynamic displays. In *Proc. Int. Workshop on Near Field Commun. (NFC'09)*, Feb., 2009.

[4] NFC Forum. *NFC Specifications*. http://www.nfc-forum.org.

[5] 전용성, 박지만, 주홍일, 전성익. RFID를 위한 내장형 비접촉 (Type-B) 프로토콜 지원 모듈 설계 및 구현. 정보처리학회논문지A, Vol.10-A, No.3, pp.255-260, 2003.

[6] Neal Leavitt. For wireless USB, the future starts now. *IEEE Computer*, 40(7):14-16, 2007.

[7] P. Subramanian, Jagonda Patil, and Manish Kumar Saxena. FPGA prototyping of a multi-million gate system-on-chip (SoC) design for wireless USB applications. In *Proc. Int. Conf. on Wireless Commun. and Mobile Computing (IWCMC '09)*, pp.1355-1358, New York, NY, USA, 2009.

[8] Domenico Porcino and Walter Hi. Ultra-wideband radio technology: potential and challenges ahead. *IEEE Commun. Mag.*, 41(7):66-74, 2003.

[9] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Trans. Info. Theory*, T-22(6):644-654, 1976.

[10] 양대헌, 이경희. 변형 Diffie-Hellman 키교환 프로토콜. 정보처리학회논문지C, Vol.14-C, No.6, pp.471-474, 2007.

[11] WiMedia Alliance. *Association Models Supplement to the Certified Wireless Universal Serial Bus Specification 1.1.*

http://www.wireless-usb.eu.
[12] NFC Forum. *Connection Handover Specification 1.1*. http://www.nfc-forum.org.
[13] ECMA. *NFC-SEC: NFCIP-1 Security Services and Protocol*. http://www.ecma-international.org.
[14] European Telecommunications Standards Institute (ETSI). *Smart Cards; UICC - Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics*. http://www.etsi.org.
[15] Marie Reveilhac and Marc Pasquet. Promising secure element alternatives for NFC technology. In *Proc. Int. Workshop on Near Field Commun. (NFC'09)*, Feb., 2009.
[16] Handshake solutions. *HT80C51MX microcontroller*. http://www.handshakesolutions.com.

한 영 선

e-mail : ysun.han@samsung.com
2003년 고려대학교 전기전자전파공학부(학사)
2009년 고려대학교 전자컴퓨터공학과(박사)
2009년~현 재 삼성전자 시스템 LSI 책임연구원
관심분야 : 컴파일러, 임베디드 시스템, 컴퓨터 구조

김 태 선

e-mail : karl.kim@samsung.com
1997년 단국대학교 전기공학과(학사)
1999년 단국대학교 전산통계학과(석사)
2002년~2005년 KBET 자바카드 개발팀 팀장
2005년~현 재 삼성전자 시스템 LSI 책임연구원
관심분야 : 스마트카드, NFC