

Scheme to Guarantee IP Continuity for NFC-based IoT Networking

Younghwan Choi^o, Yunchul Choi, Dongmyoung Kim, Jungsoo Park

Protocol Engineering Centre, Electronics and Telecommunications Research Institute

218 Gajeong-ro, Yuseong-Gu, Daejeon, 34129, Republic of Korea

{yhc, cyc79, dm.kim, pjs}@etri.re.kr

Abstract— The key idea of IoT services and technologies is connectivity among all kinds of devices. The devices of the future would include very tiny things. Such a tiny device should support low-powered technology. However, the low-power technology could bring potential problems to device functions. This paper give a solution to overcome one of the problems for IoT devices based on NFC networking. NFC, which is from RFID technology, supports peer-to-peer communication on the link layer. Link addresses of NFC devices are not physically fixed values, so this give negative influences to IP networking; especially, connection continuity. Therefore, this paper gives a scheme to guarantee IP continuity for NFC-based IoT networking.

Keywords— Internet of Things, IoT, networking, Near Field Communication, NFC, IPv6-over-NFC, adaptation layer

I. INTRODUCTION

It is stated in the ITU Report 2005 [1] that Internet of things (IoT) can be defined as a vision “First, in order to connect everyday objects and devices to large databases and networks a simple, unobtrusive and cost-effective system of item identification is indispensable. Second, data collection can of course benefit from the ability to detect changes in the physical status of things. Finally, advances in miniaturization and nanotechnology mean that smaller and smaller things will have the ability to interact and connect”.

As one of low-power networking technologies for the IoT devices, Near Field Communication (NFC) is a set of standards for smartphones and portable devices to establish radio communication with each other by touching them together or bringing them into proximity, usually no more than 10 cm. NFC standards cover communications protocols and data exchange formats, and are based on existing radio-frequency identification (RFID) standards including ISO/IEC 14443 and FeliCa. The standards include ISO/IEC 18092 and those defined by the NFC Forum [2]. NFC peer-to-peer communication is possible, provided both devices are powered. NFC builds upon RFID systems by allowing two-way communication between endpoints, where earlier systems such as contactless smart cards were one-way only. It has been used in devices such as mobile phones.

This paper gives a solution to overcome one of the problems for IoT devices based on NFC networking. NFC, which is from RFID technology, supports peer-to-peer

communication on the link layer. Link addresses of NFC devices are not physically fixed values, so this give negative influences to IP networking; especially, connection continuity. Therefore, this paper gives a scheme to guarantee IP continuity for NFC-based IoT networking.

The rest of this paper is organized as follows. What the problem is targeted for this paper to deal with is analysed in section II. Section III describes a solution and algorithms, section IV give performance evaluation. Lastly, section V gives concluding remarks.

II. PROBLEM STATEMENTS

An IPv6 address consists of two 64-bit values, i.e., prefix and interface identifier (IID). The prefix is obtained from gateways for identifying a network which the address belongs to, and the IID is used for identifying a device which the address belongs to in the network. Therefore, unless the prefix is not for a link-local address, the 128-bit IPv6 address is a globally unique value for a device.

In IoT environments based on the Internet, low-power networking devices, such as G.9959, Bluetooth Low Energy (BLE), LoBAC (MS/TP networks), and NFC, have different schemes and format for IID generation of an IPv6 address [3]. For example, in a NFC case, an IID is generated by only putting 6-bit SSAP (i.e., NFC link layer ID [4]), based on the modified EUI-64 format with ‘0’ padding (see Figure 1); however, the 6-bit link layer address of a NFC devices is not a physically fixed value but temporarily logical value for identifying NFC services. Therefore, it could not guarantee the fact that the same IPv6 address is generated whenever a NFC device makes a different TCP/IP connection. This would be also happening frequently because almost all NFC applications exploit a single-touched approach; for instance, ID validation and mobile payment [5].

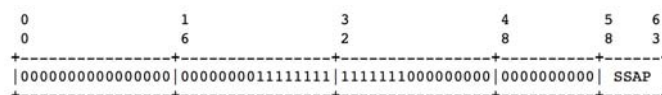


Figure 1. Formation of IID from NFC-enabled device address [5]

For instance, there are two NFC-enabled mobile phones which want to connect each other. NFC allows devices to communicate within less than 10 cm physically for usually

very short connection time, so it has a strong point of secure data transfer. However, since the connection is not really reliable, network session would be disconnected if network failures occur over data transferring. Even though the two devices try to reconnect each other, it is not always guaranteed that the same network session is restarted with the same IP addresses.

III. SCHEME TO GUARANTEE IP CONTINUITY FOR NFC-BASED IOT NETWORKING

The proposal is organized as two parts: architectures and algorithms.

A. Architectures and Protocol Stacks

Originally, peer-to-peer communications of NFC only supports direct connections of link layer between two devices. As mentioned in section II, if NFC is put together TCP/IP networking technology, it is worthy of services and applications for secure data transferring. In addition, when NFC and BLE devices want to communicate in the Internet, The NFC device should use TCP/IP networking technology.

IETF 6lo WG has started to develop a standard of IPv6 networking over NFC [4, 5]. Regarding “IPv6-over-NFC”, Figure 2 shows an example of protocol stacks between NFC and BLE devices.

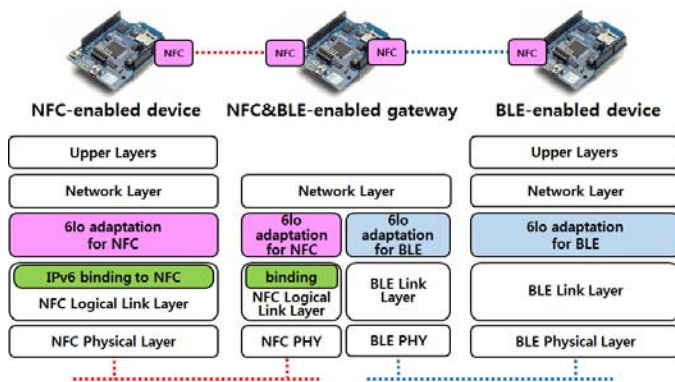


Figure 2. Example of communication and protocol stacks between NFC and BLE devices

As shown in Figure 2, the IPv6-over-NFC adaptation layer [5] is basically required for NFC-based TCP/IP networking. Of course, BLE also requires the adaptation layer [6]. In addition, NFC devices require another module to guarantee IP continuity, so called “IPv6 binding to NFC” in link layer. The IPv6 binding to NFC has specific functional requirements as follows:

- Link layer ID binding: LLCP of NFC [4] has a 6-bit address (i.e., SSAP) in link layer. The SSAP should be forwarded to IPv6-over-NFC adaptation layer to generate an IID of an IPv6 address.
- Caching: When an IID is generated, a logical SSAP should be stored in cache.
- Reusing: If a device wants to make the same network session with the same IPv6 address, the SSAP stored in cache should be reused for next session.

B. Algorithms to guarantee IP continuity

The specific functions are designed as two following algorithms: Request for link layer ID and Generate/Reply link layer ID.

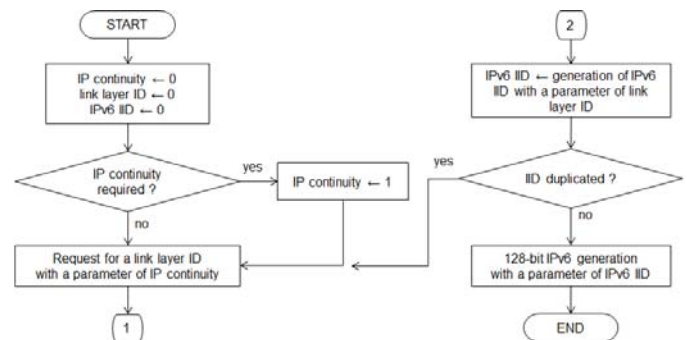


Figure 3. Algorithm of request for link layer ID

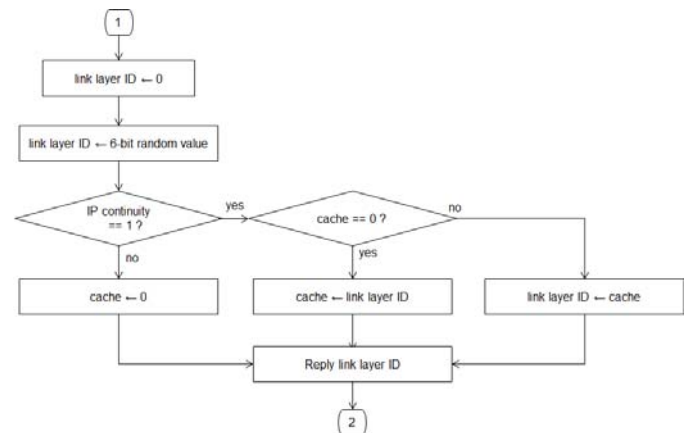


Figure 4. Algorithm for generate/reply link layer ID

Firstly, the algorithm for the request for a link layer ID is conducted in IPv6-over-NFC adaptation layer (see Figure 3). It should be checked whether a brand-new IPv6 address should be the same as the previous network session or not before requesting for a link layer ID to the module, “IPv6 binding to NFC”. If so, a previously used link layer ID stored in the cache is replied back to the adaptation layer. If not, a brand new link layer ID is created and replied.

IV. PERFORMANCE EVALUATION

Implementations and tests have been conducted with two Intel Edison® boards with NFC shields as shown in Figure 5.

As a matter of fact, NFC technology has not been usually used for network interfaces but only data input/output in all kinds of operating systems. In other words, NFC device drivers are just operated as device I/O but not network interface like NIC. Thus, a brand-new network interface driver should be implemented for the first in the world. The testbed environments are as follows:



Figure 5. Testbed for IPv6 networking between two NFC-enabled devices

- H/W: Intel Edison® boards with Adafruit (PN532 chipset) NFC shields
- S/W: Yacto Linux 2.0 with a new NFC network driver, Fedora Linux (kernel ver. 3.18)

The main objective of this paper is to guarantee IP continuity with NFC-based networking. Therefore, performance evaluation in this short paper has only targeted to figure out whether IP continuity is guaranteed or not with Ping6 tests. The following figures show the simple results.

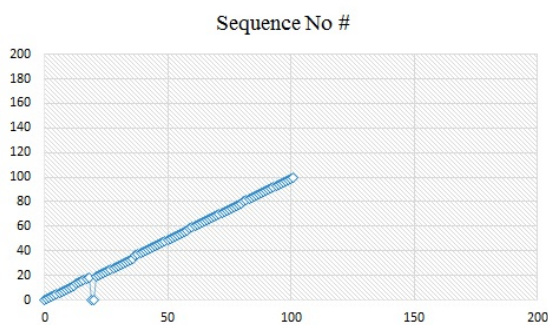


Figure 6. Sequence no. of the existing IPv6-over-NFC networking

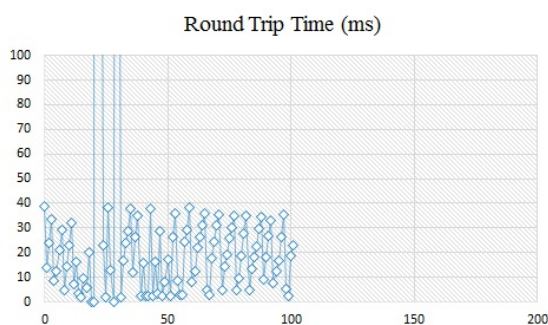


Figure 7. RTT of the existing IPv6-over-NFC networking

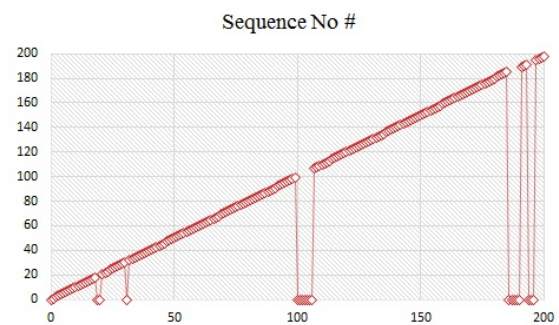


Figure 8. Sequence no. of the proposed solution

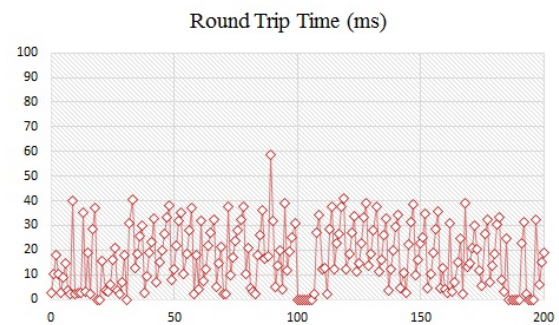


Figure 9. RTT of the proposed solution

The X-axis of all Figures means the time (sec.), Y-axis in Figure 6 and 8 means sequence numbers and Y-axis in Figure 7 and 9 means round trip time (ms). Figure 6 and 7 illustrate the sequence numbers and the round trip time obtained from the ping results for 200 seconds. Even though the two devices tried to get touched for reconnection after a network failure was given at the 100 second, there is no response in the existing IPv6-over-NFC networking. This is because the IPv6 address of the destination device was changed. However, the proposed scheme shows different results. After the 100 second, there is no response for a short time (around 5 seconds), and then the connection is restarted (see Figure 8 and 9).

V. CONCLUDING REMARKS

Internet-based low-power networking technology would enable energy-limited devices to have interconnectivity as a base technology as well as enable a variety of advanced services and applications. This paper gives a solution with the performance evaluation to deal with the IP continuity problem that can occur in low-power IoT networking. This study is working on the further implementation for more depth performance analysis.

Regarding this study, standardization has been developing for the "NFC-based IPv6 networking", led by South Korea in IETF 6lo WG. This is expected to be completed within half a year. In addition, the technical implementation and test bed for NFC-based IP networking technology has been tested in ETSI's 6lo plugtest [7]. NFC-based IPv6 networking is expected to pass 100% tests in the next plugtest event.

ACKNOWLEDGMENT

This work was supported by ICT R&D program of MSIP/IITP. [R0166-16-1008, Internet based IoT Interworking Technology Standards Development]

REFERENCES

- [1] ITU Internet Reports, "The Internet of Things," 2005.
- [2] The NFC Forum website. [Online]. Available: <http://nfc-forum.org>.
- [3] The IETF 6lo WG website. [Online]. Available: <https://datatracker.ietf.org/wg/6lo/documents/>.
- [4] NFC Forum Technical Specification, "NFC Logical Link Control Protocol version 1.3," NFC Forum, March 2016.
- [5] Y. Choi *et al.*, "Transmission of IPv6 Packets over Near Field Communication," IETF draft-ietf-6lo-nfc-04 (working on progress), July 2016.
- [6] J. Nieminen *et al.*, "IPv6 over BLUETOOTH(R) Low Energy," IETF RFC7668, October 2015.
- [7] ETSI 6tisch-6lo plugtests. [Online]. Available: <http://www.etsi.org/news-events/events/1077-6tisch-6lo-plugtests>.



Younghwan Choi (B'02–M'05–P'09) received the B.S. and M.S. degrees in Computer Science from Chungnam National University, Daejeon, Rep. of Korea, in 2002 and 2005, respectively. He received the Ph.D. in Computer Engineering from Chungnam National University, Daejeon, Rep. of Korea, in 2009. He joined the Protocol Engineering Center (PEC), Electronics and Telecommunications Research Institute (ETRI) as Senior Researcher in 2009. His research interests include wired and wireless networks, routing and protocol technologies, Internet of Things (IoT), low power device networking.



Yunchul Choi (B'07–M'10) received the B.S. and M.S. degrees in Information Communications Engineering from Chungnam National University, Daejeon, Rep. of Korea, in 2007 and 2010, respectively. From 2012, he has been with the Protocol Engineering Center (PEC), Electronics and Telecommunications Research Institute (ETRI) as Senior Researcher. His research interests include software-defined networking, Internet of Things (IoT), low power device networking.



Dongmyoung Kim (B'05–P'12) received the B.S. and Ph.D. degrees in Electrical Engineering from Seoul National University, Seoul, Rep. of Korea, in 2005 and 2012, respectively. From 2012 to 2015, he was a senior researcher in the Samsung Electronics, Suwon. He joined the Protocol Engineering Center (PEC), Electronics and Telecommunications Research Institute (ETRI) as Senior Researcher in 2015. His research interests include Internet of Things, 5G communications, and heterogeneous cellular networks.



Jungsoo Park (B'92–M'94–P'13) received the B.S. and M.S. degrees in Electronics Engineering from Kyungpook National University, Daegu, Rep. of Korea, in 1992 and 1994, respectively. He received the Ph.D. in Electronics Engineering from Kyungpook National University, Daegu, Rep. of Korea, in 2013. He joined the Protocol Engineering Center (PEC), Electronics and Telecommunications Research Institute (ETRI) as Senior Researcher in 1994. His research interests include security, wireless adhoc networks, mobile network, routing and protocol technologies, Internet of Things (IoT), low power device networking.