Advanced Science and Technology Letters
Vol.94 (Mobile and Wireless 2015), pp.85-88
http://dx.doi.org/10.14257/astl.2015.94.18

Authorization Protocol using a NFC P2P mode between IoT device and Mobile phone[1]

Byung Mun Lee

Dept. of Computer Engineering, Gachon University, Seongnam, GyeongGi-Do, Korea,
bmlee@gachon.ac.kr

Abstract. Some public institution provide a service to be used some public health devices such as weight scale and blood pressure monitor. In order to share the device among people, the device has to identify a user and manage authorization. In this paper, I proposed a authorization protocol on a NFC P2P mode between a mobile device and the public health device including NFC P2P facility and intelligent service algorithm. Moreover, the protocol has an authorization facility to control sharing devices with the people.

Keywords: Authorization, NFC P2P, IoT device, Mobile device

1 Introduction

Recently, research and development have become active on wearable devices as well as IoT (Internet of Things) devices[1][2]. In addition, there are variety of models that take advantage of the mobile device to the user interface of the wearable device. Smart light bulb is a good example [3]. An application on a mobile phone can be controlled to turn it on or off. Another one is a sleep care or sleep tracker [4]. The mobile device can be displayed graphical analysis of sleep data during a last night after sync with the sleep tracker.

However, some devices can be also shared for use by family at home or by patients at a medical center or for people at a public institution [5][6]. In order to share the devices, user authentication and authorization function play a significant role in customized service to the user including sharing. This facility also contributes to utilization rate of the device, and extends the range of use. It is possible to share devices and services using a mobile device as a user interface of the device after the IoT devices are registered on the open IoT platform [7]. It also may contribute to the development of the service platform.

Thus, we propose an NFC (Near Far Communication)-based authentication protocol for user authentication between the mobile device and the IoT devices. In particular, the mobile device acts as a NFC initiator [8], and also, IoT device acts as a NFC target in the authentication protocol. In addition to it, the protocol can be applied to

[1]This research was supported by the MSIP(Ministry of Science, ICT & Future Planning), Korea, under supervised by Incheon Information Service

ISSN: 2287-1233 ASTL

various application service, because it uses the P2P (Peer to Peer) mode to transmit user information and the Meta information of the device. Therefore, the protocol can be applied to the IoT devices for sharing them between people at their home or office, as well as for providing customized service to people.

2 Authorization Protocol on the NFC peer to peer mode

NFC supports three modes. They are P2P mode, Read / Writer Tag mode, and Card emulation mode. The authentication protocol proposed in this paper will be operated by P2P mode because various data can be transmitted between the IoT device and mobile device. NFC has a good security interface because it is available if only to be close less than 20cm.

The proposed protocol uses a NDEF (NFC Data Exchange Format) and RTD (Record Type Definition) for transmission over NFC standards of ISO 18092, as shown in Figure 1, and has an Authentication and Authorization function. The protocol has to check whether the IoT devices is registered in authentication server, as well as to check whether the user is registered in the server.

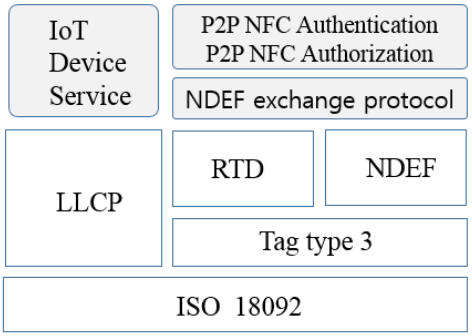

Figure 1. NFC Protocol stack

The user authentication and authorization control is required because they allow multiple users to share a single device to use at any one time. Figure 2 shows the protocols to support it.

First of all, the user is granted the user authentication and permissions to use the IoT devices. In order to do this, If an user takes his mobile device close to a IoT device, the mobile device sends a ServieSetup.req to IoT the mobile device. The device responses to send ServiceSetup.res to the mobile device after the device receives the request. After waiting for a response during a period of time, the mobile device sends the Authorization.req to the IoT devices on receiving the response.

Every device has its own identification code, which are used in every request and response message.

Mobile device receives a code from the IoT device, and sends token.req including the code and a mobile id (m-id) to an auth server, and then the device receives token

in the token.res message from the auth server. The mobile device having acquired the token is authorized to use the device for a certain period of time. Thus, the mobile device sends session.req to the device in order to use it. After completion of the session, all data transfer are valid for their session time.

When the session time is expired at the lifetime of the token, the IoT device can reject data transfer by sending unknown-session message to the mobile device.

The mobile device requests to get a new effective token to the auth server at this time. If the new one is available again, the data transfer resumes.

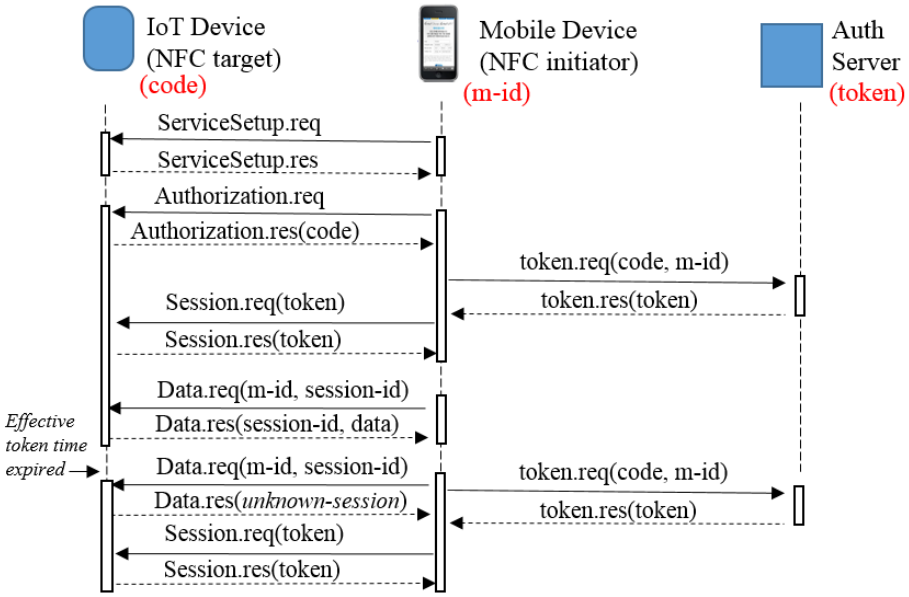

Figure 2. Protocol flow for authorization between IoT device and Mobile Device

Thus, user of the mobile device can use the IoT device using the authorization control from auth server.

3 Conclusions

In this paper, I proposed the NFC-based authentication protocol using mobile devices, so that multiple users can be effectively used to share IoT devices. The proposed protocol has the authorization management capabilities to shared resources by managing the effective time of the token from an auth server. This protocol can be applied to a variety of different IoT services, such as a u-health service. Furthermore, when equipped with the protocol proposed by the medical device, such as a blood pressure

monitor and scale, the effect that multiple users can use the device effectively will be expected.

References

1. X. M. Zhang, and N. Zhang: An Open, Secure and Flexible Platform Based on Internet of Things and Cloud Computing for Ambient Aiding Living and Telemedicine. KSII Trans. on Internet and Information Systems. 480--497 (2012)
2. Google fitness platform service web, https://developers.google.com/fit/
3. Peter Svensson.: Review: 'Smart' LED bulbs controlled by iPhones. http://phys.org/news/2013-03-smart-bulbs-iphones.html.
4. Fitbit One™ Wireless Activity, Sleep Tracker.: https://www.fitbit.com/#i.1o9dth18wleh8r
5. B. M. Lee and J. Ouyang: Application Protocol adapted to Health Awareness for Smart Healthcare Service, In the proc. of International Workshop of Multimedia 2013, Advanced Science and Technology Letters, Vol. 43, 101--104, (2013)
6. B. M. Lee and J. Ouyang :Intelligent Healthcare Service by using Collaborations between IoT Personal Health Devices, International Journal of Bio-Science and Bio-Technology, Vol. 6, No. 1, 155--164, (2014)
7. Min C., Jiafu W., Fang L.: Machine-to-Machine Communications: Architectures, Standards and Applications. KSII Trans. on Internet and Information Systems. 480--497 (2012)
8. Ekta Desai, Mary Grace Shajan.: A Review on the Operating Modes of Near Field Communication. International Journal of Engineering and Advanced Technology. 322--325 (2012)

