Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 110 (2017) 290–296

Procedia Computer Science

www.elsevier.com/locate/procedia

The 12th International Conference on Future Networks and Communications (FNC-2017)

Software-defined Naming, Discovery and Session Control for IoT Devices and Smart Phones in the Constraint Networks

Younchan Jung[a,*], Marnel Peradilla[b], Akanksha Saini[a]

[a]*Catholic University of Korea, School of Information, Communications, and Electronics Engineering, Bucheon-si, Gyeonggi-do, 420-743, South Korea*

[b]*De La Salle University, Computer Technology, College of Computer Studies Manila, Philippines*

Abstract

This paper suggests the naming for Internet of Things (IoT) devices where a Fully Qualified Domain Name (FQDN) is assigned to each device instead of the IP address. This naming method enables the user equipments (UEs) to reach IoT devices easily. Nowadays, one of the main challenges in IoT is the discovery scheme. This paper explores the discovery scheme that can operate under the current DNS and its legacy Resource Record (RR) format. The IoT device with the group name of *GrpN*, the domain of *example.com* and the device name of *IoT77* can be discovered by means of the URL: *GrpN.example.com/IoTD77*. This paper explores how the UE behind the Network Address Translation (NAT) device discovers the destination IoT devices and establishes IoT Device-to-User Equipment (D2U) data session under the condition that IoT access networks tend to be constraint networks. Here, the discovery and session establishment processes are controlled by the software-defined control plane controller.

Peer-review under responsibility of the Conference Program Chairs.

Keywords: Control Plane Controller; Discovery; Fully Qualified Domain Name; Internet of Things; Naming

1. Introduction

Currently, the Internet Engineering Task Force (IETF) leads the direction for technologies and standards for the Internet of Things (IoT) devices [1,2]. These standards define how Device-to-Device (D2D) or Device-to-User Equipment (D2U) communication services operate through the Internet. The main direction of the IoT access networks is standardized by IPv6 over Low-Power Wireless Area Networks (6LowPAN). Also, in terms of application, there are two distinctive standards that can be developed: Constrained RESTful Environments (CoRE) for research groups and Constrained Application Protocol (CoAP) web delivery protocols [3,4,5]. This approach seems to be difficult to be realized considering the operating environment of IoT devices. Focused on the networking layer, main feature of several innovations to enable the extension of Internet technologies to constrained devices is related to transmission of IPv6 Packets over IEEE 802.15.4 Networks (RFC 4944). The IPv6-based standards are treated as the popular

* Corresponding author. Tel.: +82-2-2164-4364 ; fax: 02-2164-4581.
E-mail address: ycjung@catholic.ac.kr (Y. C. Jung).

1877-0509
Peer-review under responsibility of the Conference Program Chairs.
10.1016/j.procs.2017.06.097

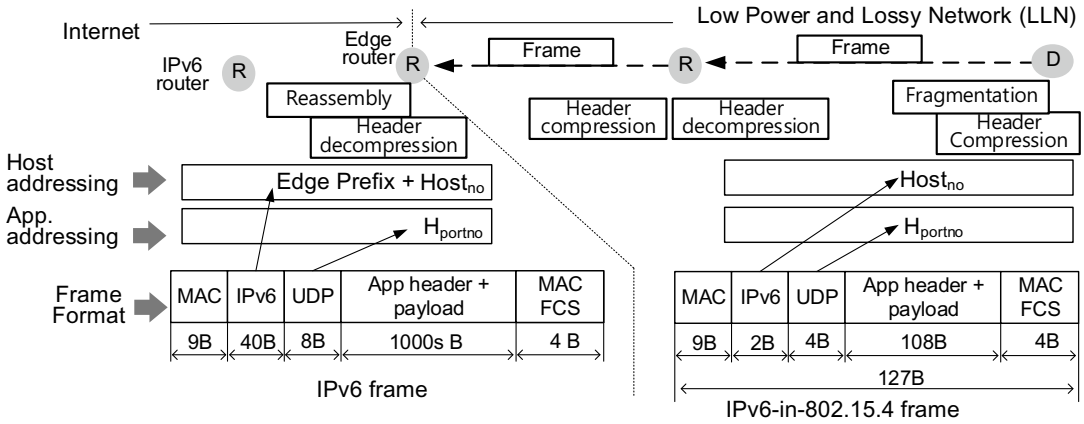

Fig. 1. IPv6-in-802.15.4 frame format and the methods of host addressing and application addressing

technologies to enable the realization of an Internet of Things, where end-to-end IPv6-based network connectivity becomes possible[6]. As shown in Fig. 1, RFC 4944 describes the IPv6-in-802.15.4 frame format, the methods of host addressing and application addressing, simple header compression and mesh-under routing for multi-hop IEEE 802.15.4 networks. These novel technologies seem to cause problems to realize end-to-end IP-based network connectivity with tiny objects such as sensors and actuators where the computing power of them is limited. The IPv6-based standards also confront with interoperable problems with legacy devices. The explosive growth of the smartphones and tablets as UEs created an instant demand on the extension of IP address space[7]. However, as the main solution of the IETF, IPv6 addressing implementation fails to solve address exhaustion because of the NAT (Network Address Translation)'s widespread uses[8,9]. This means that most of the UEs still use IPv4-based private IP addresses. Also, IoT devices tend to be accessed via IPv4-based constraint networks. Then, the UE's discovery process to the IoT device needs collaboration with current Domain Name System (DNS) dealing with current IPv4-based Resource Record (RR) format.

Despite the efforts of the IETF, the reality is that the IPv6 is not realized as intended[10]. Currently, the growing demand for smartphones and mobile devices require to keep on using Wi-Fi as main IPv4-based wireless access network. This is because the 32-bit IPv4 can use one public address and provides up to 65,000 private addresses with the NAT device. This paper considers the premise in the first[11,12], at the beginning stage of IoT age, most IoT applications aim to connect humans (UEs) to IoT Devices, that is, D2U IoT services will start first[13]. Second, for the time being, the NAT device should be operated in the circumstance of the wide spread use of smartphones (UEs). Third, in the near future, the current IPv4-based constraint networks, which provide links to IoT devices, would be difficult to switch to the IPv6-based IoT access networks. So, this paper explores how the UE behind the NAT device discovers the destination IoT devices and establishes D2U data sessions to them under the condition that their IoT access networks tend to be constraint networks. Here, the discovery and session establishment processes are controlled by the software-defined control plane controller.

The rest of this paper is organized as follows. In section II, provisioning, naming and discovery methods will be proposed and explained. And a series of protocol steps will be explained to show that the UE establishes Device-to-User Equipment data session under the condition that the UE uses the private IP address and the IoT device is handled only by its host number and Fully Qualified Domain Name. This paper will be concluded in section III.

2. IPv4-based Approaches for Proposed Discovery Scheme

The smart phones and tablets behave as UEs which satisfy the demand for the D2U IoT services. As shown in Fig. 2, NAT router, which extends internal addressing from the global IP addressing used over the Internet, enables UEs to be located anywhere and to establish D2U sessions. This paper assumes that IoT mesh networks as the access