Multicast Activation Scheme based on LoRaWAN for Multicast MAC Transmission

Sun Hwa Lim, Kang Bok Lee
IoT Research Division
Electronics and Telecommunications Research Institute
218, Gajeong-Ro, Yuseong-gu, Daejeon, Korea
e-mail: {limsh, kblee}@etri.re.kr

***Abstract*—Internet of Things (IoT) is a rapidly emerging technology which involved both a variety of research and a very wide range of industrial fields. It is increasingly interested in the use of a long range wide area network (LoRaWAN) to remotely monitor and manage the number of devices in real-time. In order to better manage and control a lot of devices, multicast is sometimes more suitable than unicast. However, in the LoRaWAN specification, unicast MAC transmission is only described but multicast MAC transmission is not specified. In this paper, we propose the multicast activation scheme to support multicast MAC transmission based on LoRaWAN. The presented scheme can reduce the energy consumption required for downlink and be used as a guideline for developing LoRaWAN-based IoT applications.**

Keywords- IoT; LPWA; LoRaWAN; multicast; activation.

I. INTRODUCTION

Internet of Things (IoT) have been studied [1]-[3] and applied to a very wide range of fields such as intelligent buildings, manufacturing, agriculture, and goods transportation to remotely monitor and better manage things in real-time [4]-[7]. The devices in these applications typically send tiny amounts of data with limited low power in a long coverage area. In order to guarantee the characteristics of the devices, low power wide area (LPWA) technologies have become more popular than Wi-Fi or LTE [8][9]. Many LPWA technologies have arisen in the licensed spectrum (LTE Cat-0, LTE-M, NB-IoT, etc.) as well as unlicensed (LoRaWAN, SigFox, Ingenu, etc.). Among LPWA technologies, a long range wide area network (LoRaWAN) is widely employed in various applications (for example, shipping and transportation for industrial applications, temperature and moisture monitoring for agriculture, waste management for smart city) [10]-[13].

A large number of devices need to be grouped so as to better manage and control devices (e.g., configuring parameters, initializing devices). Multicast is more suitable than unicast to send small amounts of control information to a lot of devices. However, in the LoRaWAN specification [14], unicast MAC transmission is only described but multicast MAC transmission is not specified. Therefore, in this paper, we propose the detailed and possible multicast activation scheme to provide multicast MAC transmission based on LoRaWAN. The presented scheme can be used as a guideline for developing LoRaWAN-based IoT applications.

This paper is organized as follows. In Section II, we briefly introduce the LoRaWAN network architecture and protocol stack for a multicast activation. In Section III, we propose the multicast activation scheme based on LoRaWAN. In Section IV, we compare unicast and multicast in terms of energy consumption of transmitter over the air. Finally, Section V presents the conclusions.

II. LORAWAN NETWORK

In this section, we introduce the LoRaWAN network architecture and protocol stack for a multicast activation.

A. Architecture

Fig. 1 shows the network architecture of LoRaWAN for a multicast activation. There are an end device, a gateway, a network server, an authentication, authorization, and accounting (AAA) server, and an application server. The end device can transfer and receive data packet to and from the gateway with PHY of LoRa. The gateway shall forward data packet between end devices and the network server. The network server can route data packet from the gateway to the AAA server or the application server, and back. The AAA server shall perform an authentication procedure for the end device and generate session keys such as a network session key and an application session key. The application server can collect and analyze data receiving from the network server. It is also able to process an authentication function without the AAA server.

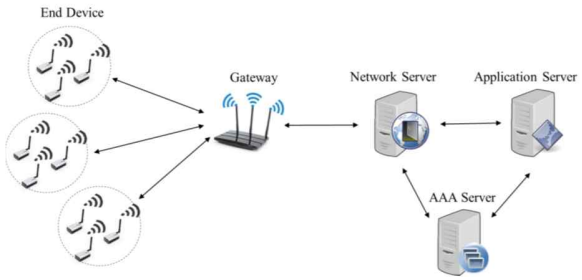

Figure 1. LoRaWAN-based network architecture for a multicast.

B. Protocol Stack

Fig. 2 shows the protocol stack of LoRaWAN for a multicast activation. An end device is composed of the LoRa

 ISBN: 978-1-61208-650-7

PHY layer, the LoRaWAN MAC layer, and the application layer. For the radio interface, a gateway is communicated with the end device based on the LoRa technology. The gateway is connected to a network server over IP networks. The network server is connected to an AAA server based on RADIUS [15] over UDP/IP networks.

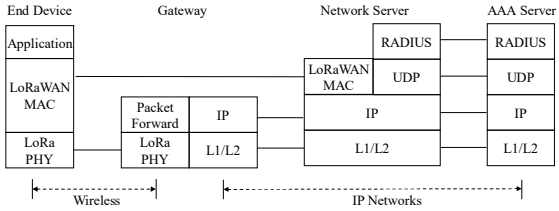

Figure 2. LoRaWAN-based protocol stack for a multicast activation.

III. PROPOSED MULTICAST ACTIVATION SCHEME

In this section, we present the multicast activation scheme to provide multicast MAC transmission based on LoRaWAN.

A. New defined multicast MAC messages

For an end device to join a multicast group over LoRaWAN, it is necessary for us to define new multicast MAC message types. Table 1 shows the newly defined MAC message types. The LoRaWAN specification allows the use of 3-bits message type (MType) and already defines six different MAC message types. The MAC types of a *multicast join request* message and a *multicast join accept* message are defined by 110 and 111, respectively.

TABLE I. MAC MESSAGE TYPES

Message Type	Description
000	Join Request
001	Join Accept
010	Unconfirmed Data Up
011	Unconfirmed Data Down
100	Confirmed Data Up
101	Confirmed Data Down
110	Multicast Join Request
111	Multicast Join Accept

Fig. 3(a) and Fig. 3(b) illustrate the detailed format of a *multicast join request* message and a *multicast join accept* message. In order to generate session keys, the messages can contain the following parameters.

Size(bytes)	8	4	4
Multicast Join Request	MultiAppEUI	DevAddr	DevNonce

(a)

Size(bytes)	8	4
Multicast Join Request	MultiAppEUI	DevAddr

(b)

Figure 3. New defined multicast MAC messages. (a) Multicast Join Request. (b) Multicast Join Accept.

A *multicast join request* message contains MultiAppEUI, DevAddr, and DevNonce. MultiAppEUI is a multicast application identifier, i.e., the MultiAppEUI is a global application ID that uniquely identifies the entity able to process a *multicast join request* message. DevAddr is used to identify an end device within the current network. DevNonce is a random value generated by an end device. A *multicast join accept* message contains MultiNonce and MultiAddr. MultiNonce is a random value generated by an AAA server. MultiAddr is an identifier to identify a multicast group.

B. Integrity of Multicast MAC Messages

In order to ensure the integrity of multicast MAC messages, a message integrity code (MIC) should be appended to the end of the messages. For a *multicast join request* message integrity, MultiAppKey, MHDR, MultiAppEUI, DevAddr, and DevNonce are used as input parameters of the CMAC algorithm. An end device has been pre-configured with MultiAppEUI and MultiAppKey. MultiAppKey is an AES-128 root key specific to a multicast group. MHDR is the MAC header field. | is represented the concatenation of character strings. The MIC can be calculated by

cmac = aes128_cmac (MultiAppKey, MHDR | MultiAppEUI | DevAddr | DevNonce),

MIC = cmac[0..3].

For a *multicast join accept* message integrity, MultiAppKey, MHDR, MultiNonce, and MultiAddr are used as input parameters of the CMAC algorithm. An AAA server has been pre-configured with MultiAppKey. The MIC can be calculated by

cmac = aes128_cmac (MultiAppKey, MHDR | MultiNonce | MultiAddr),

MIC = cmac[0..3].

For a network server to send a secure *multicast join accept* message to an end device, the message is encrypted with MultiAppKey as follows:

aes128_decrypt (MultiAppKey, MultiNonce | MultiAddr | MIC).

MultiAppKey is pre-configured in a network server and the MIC is the value calculated above.

C. Derivation of Multicast Session Keys

After verifying the MIC of multicast MAC messages, an end device and an AAA server can derive the two multicast session keys which are a multicast network session key (MultiNwkSKey) and a multicast application session key (MultiAppSKey). The session keys are calculated as follows:

MultiNwkSKey = aes128_encrypt (MultiAppKey, 0x03 | MultiNonce | MultiAddr | DevNonce | pad16),

 ISBN: 978-1-61208-650-7

MultiAppSKey = aes128_encrypt (MultiAppKey, 0x04 | MultiNonce | MultiAddr | DevNonce | pad16).

MultiNwkSKey is used to encrypt and decrypt the payload field of multicast MAC data messages between end devices of a multicast group and a network server. MultiAppSKey is used to encrypt and decrypt the payload field of application-specific data messages between end devices of a multicast group and an application server.

D. Multicast Activation Procedure

Fig. 4(a) shows a unicast join procedure and Fig. 4(b) shows a multicast join procedure. The detailed description of each step is as follows:

- Once initialization for the LoRaWAN wireless link access is finished, a unicast join procedure is performed between an end device and an AAA server via a gateway and a network server.
- If this procedure is successful, the end device and the AAA server should generate a network session key (NwkSKey), and an application session key (AppSKey).
- The end device may already have the pre-configured multicast group information that it wants to join.
- For joining a multicast group, the end device sends a *multicast join request* message to the network server including MultiAppEUI, DevAddr, and DeviceNonce through a gateway over LoRaWAN.
- The network server sends an *access request* message which includes the parameters of the *multicast join request* message to the AAA server based on the RADIUS protocol.
- If the end device is successfully authenticated, the AAA server shall respond to the network server with an *access accept* message which includes MultitNonce and MultiAddr.
- After the AAA server can generate the two session keys which are MultiNwkSKey and MultiAppSKey, it sends MultiNwkSKey to the network server. The AAA server also sends MultiAppSKey to the application server.
- Upon receiving an *access accept* message, the network server shall send a *multicast join accept* message with the above parameters (MultiNonce and

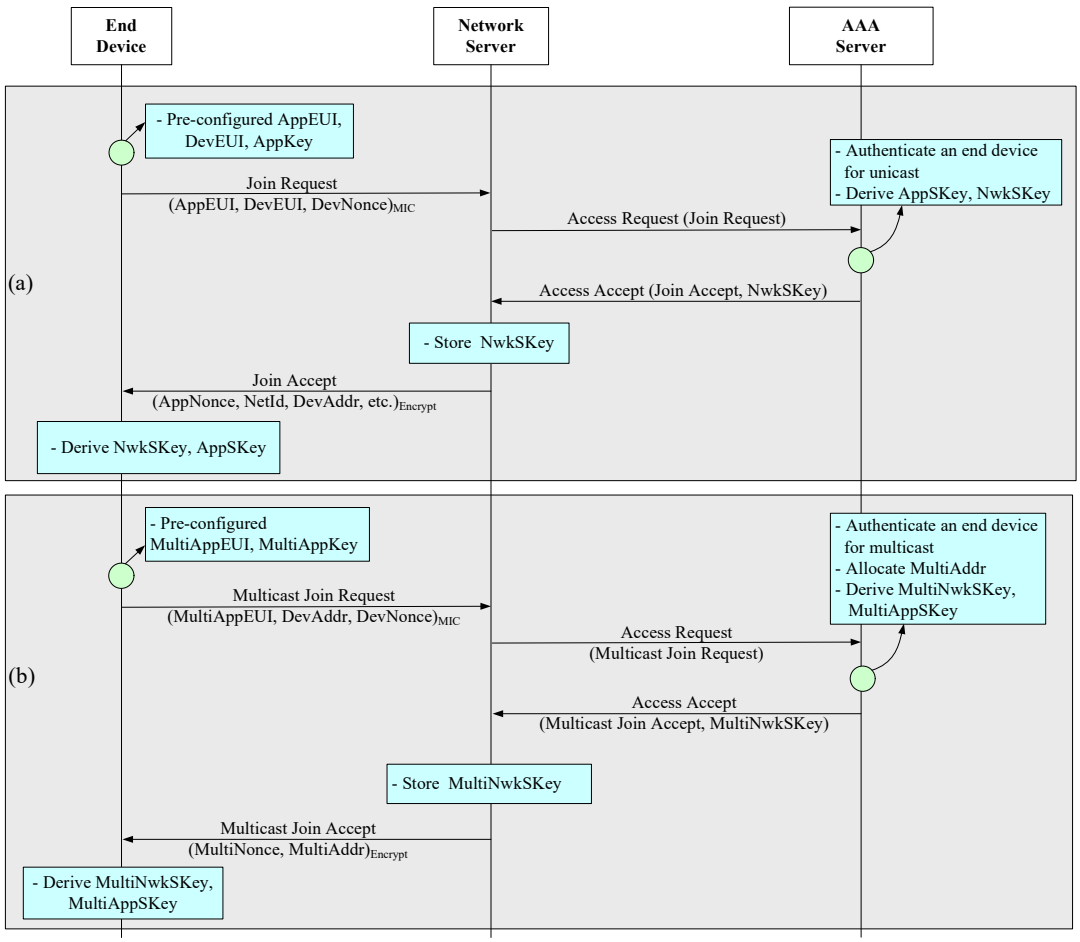

Figure 4. Over-the-air activation procedure based on LoRaWAN. (a) Unicast join activation procedure. (b) Multicast join activation procedure.

 ISBN: 978-1-61208-650-7

MultiAddr) to the end device through the gateway over LoRaWAN.
- The network server shall store MultiNwkSKey receiving from the AAA server.
- When the end device receives a *multicast join accept* message from the network server, it should derive MultiNwkSKey and MultiAppSKey.

We have designed a similar multicast join procedure based on a unicast join procedure described in the LoRaWAN specification. We believe that the proposed scheme is helpful to developers in implementing MAC multicast protocols based on LoRaWAN.

IV. PERFORMANCE ANALYSYS

We compare unicast and multicast in terms of energy consumption of transmitter over the air. A transmitter is a gateway and a receiver is an end device or a multicast group. Energy consumption of transmitter which is located in the distance of d with n bit can be expressed as follows [16]:

$$E_{Tx}(n,d) = E_{Tx-elec}(n) + E_{Tx-amp}(n,d) = E_{elec} \times n + E_{amp} \times n \times d^2. \quad (1)$$

Energy consumption of receiver can be expressed as

$$E_{Rx}(n) = E_{Rx-elec}(n) = E_{elec} \times n. \quad (2)$$

In unicast and multicast, to analyze the total energy consumption of transmitter with the number of end devices and multicast groups, the following terms are defined:
- *unitCost* : the energy consumption of transmitter, i.e., $E_{Tx}(n, d)$,
- *deviceNum* : the number of end devices,
- *groupNum* : the number of multicast groups.

In unicast, the total energy consumption of transmitter can be calculated by

$$E_{Tx\_unicast}(n,d) = unitCost \times deviceNum. \quad (3)$$

In multicast, the total energy consumption of transmitter can be calculated by

$$E_{Tx\_multicast}(n,d) = unitCost \times groupNum. \quad (4)$$

In unicast and multicast, we assume that energy consumption of receiver is equal and examine the total energy consumption of transmitter with the varied weight value of *unitCost* as Sets 1, 2, 3 followed by Table 1.

TABLE II. SETS OF UNITCOST

	unitCost
Set 1	0.1
Set 2	0.2
Set 3	0.4

For our experiments, we consider that *deviceNum* is increased by 10 from 1 to 100 and *groupNum* is given by 1, 2, 4, 5, and 10 with a 100-end devices. We can use the Gnuplot as a performance analysis tool. The simulation results are shown in Fig. 5 and Fig. 6. As illustrated in Fig. 5 and Fig. 6, as *deviceNum* and *groupNum* become increased, the total energy consumption of each transmission increases linearly. Especially, we note that *groupNum* is smaller, the difference of the total energy consumption of unicast and multicast is larger. Therefore, multicast can help to manage and configure a lot of end devices with less energy consumption of transmitter than unicast.

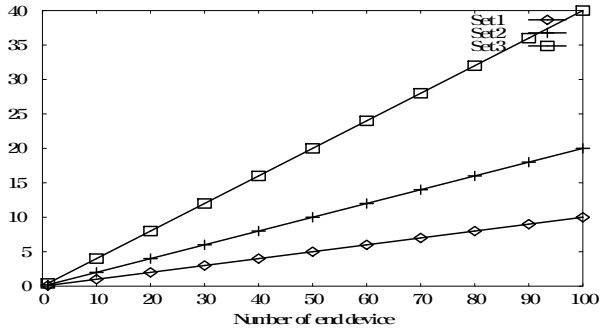

Figure 5. Energy consumption of transmitter in unicast.

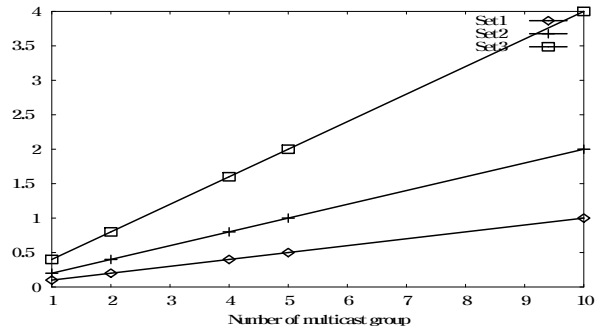

Figure 6. Energy consumption of transmitter in multicast.

V. CONCLUSIONS

We presented the multicast activation scheme to efficiently control the number of end devices based on LoRaWAN in this paper. We defined new multicast MAC messages, create the MIC, and generated multicast session keys. Additionally, we proposed a multicast join procedure for an end device. Finally, we compared unicast and multicast in terms of the total energy consumption of transmitter over the air. The presented scheme can reduce the energy consumption required for downlink. The proposed scheme can be used as a guideline for developing LoRaWAN-based IoT applications.

ACKNOWLEDGMENT

This work was supported by Electronics and Telecommunications Research Institute (ETRI) grant funded by the Korean government. [18ZH1120, Distributed Intelligence Core Technology of Hyper-Connected Space]

 ISBN: 978-1-61208-650-7

REFERENCES

[1] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," *Business Horizons*, vol. 58, pp. 431-440, Aug. 2015.

[2] A. AI-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Communications Surveys & Tutorials*, vol. 17, pp. 2347-2376, June, 2015.

[3] M. Tahmassebpour and A. Otaghvari, "Increase efficiency big data in intelligent transportation system with using IoT intergation cloud," *Journal of Fundamental and Applied Sciences*, vol. 8, pp. 2443-2461, 2016.

[4] K. Zheng, S. Zhao, Z. Yang, X. Xiong, and W. Xiang, "Design and Implementation of LPWA-Based Air Quality Monitoring System," *IEEE Access*, vol. 4, pp. 3238-3245, 2016.

[5] M. Centenaro, L. Vangelista, A. Zanella, and M. Zorzi, "Long-range communications in unlicensed bands: the rising stars in the IoT and smart city scenarios," *IEEE Wireless Communications*, vol. 23, pp. 60-67, Nov. 2016.

[6] K. Akkaya, I. Guvenc, R. Aygun, N. Pala, and A. Kadri, "IoT-based occupancy monitoring techniques for energy-efficient smart buildings," *Wireless Communications and Networking Conference Workshops* (WCNCW), Mar. 2015, pp. 58-63, ISBN: 978-1-4799-8760-3.

[7] M. Hassanalieragh, et al. "Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-Based Processing: Opportunities and Challenges," *Services Computing* (SCC), Jun. 2015, pp. 285-292, ISBN: 978-1-4673-7281-7.

[8] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low Power Wide Area Networks: An Overview," *IEEE Communications Surveys & Tutorials*, vol. 19. pp. 855-873, Jun. 2017.

[9] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "A comparative study of LPWAN technologies for large-scale IoT deployment," *ICT Express*, Available online, Jan. 2018.

[10] R. Sinha, Y. Wei, and S. Hwang, "A survey on LPWA technology: LoRa and NB-IoT," *ICT Express*, vol. 3, pp. 14-21, Mar. 2017.

[11] Y. Beyene, et.al, "NB-IoT Technology Overview and Experience from Cloud-RAN Implementation," *IEEE Wireless Communications*, vol. 21, pp. 26-32, Jun. 2017.

[12] A. Wixted, et.al, "Evaluation of LoRa and LoRaWAN for wireless sensor networks," *IEEE SENSORS*, Nov. 2016. pp. 1-3, ISBN: 978-1-4799-8287-5.

[13] M. Shirvanimoghaddam, M. Dohler, and S. J. Johnson, "Massive Non-Orthogonal Multiple Access for Cellular IoT: Potentials and Limitations," *IEEE Communications Magazine*, vol. 55, pp. 55-61, Sep. 2017.

[14] LoRaWAN Specification, V1.0.2, 2016.

[15] RFC 2865, Remote Authentication Dial In User Service (RADIUS), IETF, Jun. 2000.

[16] A. Wang, W. Heinzelman, and A. Chandrakasan, "Energy-scalable protocols for battery-operated microsensor networks," *Proc. 1999 IEEE Workshop Signal Processing Systems* (SiPS), pp. 483–492, Oct. 1999.

 ISBN: 978-1-61208-650-7