A Secure Device-to-Device Link Establishment Scheme for LoRaWAN

Jaehyu Kim, *Student Member, IEEE*, and JooSeok Song

***Abstract*— In the Internet of Things (IoT) era, the importance of communication technology to support communication between the various types of devices has become greater than ever before. Long Range (LoRa) and Long Range Wide Area Network (LoRaWAN) are newly designed communication technologies for low-power long-distance communication in the IoT environment. Recently, LoRa and LoRaWAN have received much attention in academia and industry because low-power long-distance communication has not been supported by traditional communication technologies. Current LoRaWAN supports only communication between the end node and the central server. A recently introduced study enables device-to-device (D2D) communication in the LoRaWAN environment, which is not supported by the current LoRaWAN standard. This paper shows that direct communication between devices can reduce battery consumption. However, security is not considered in this paper and the security features of the LoRaWAN standard are also not applicable, which means that LoRaWAN D2D communication is exposed to a security threat. Therefore, we propose a secure link establishment scheme to protect the LoRaWAN D2D communication. With our scheme, both D2D nodes can securely share cryptographic keys for protecting the D2D communication. Through the security analysis, we prove that our scheme guarantees mutual authentication, confidentiality, and integrity. Performance evaluation shows that our scheme increases power consumption by approximately 5% compared with the basic scheme without security, but has little impact on overall battery lifetime. Consequently, the proposed scheme guarantees fundamental security requirements with sufficient feasibility.**

***Index Terms*— IoT, LPWAN, long range (LoRa), LoRa wide area network (LoRaWAN), D2D, Security.**

I. Introduction

WITH the Internet of Things (IoT) becoming an essential concept in modern society, various kinds of devices are now connected each other. From micro sensors to home appliances and automobiles, we can remotely access most things in the world. The interactions between these devices and human are the core of the IoT, and what makes these connections possible is the communication technology. In other words, communication technology plays an important role in the IoT environment.

Low-Power Wide Area Networks (LPWANs) are emerging technologies in the IoT environment to support a low-power long-distance wireless communication. LPWANs have received much attention because low-power long-distance wireless communication is not properly supported by the conventional technology. Long Range (LoRa), a physical layer solution developed by Semtech, satisfies LPWAN requirements by using chirp spreading spectrum modulation [1]. With Long Range Wide Area Network (LoRaWAN) [2], a network protocol standard that minimizes message exchanges, LoRa can provide 15 km coverage area and ten years of battery lifetime [3]. As a result, LoRa and LoRaWAN provide the most suitable network environment for battery-constrained devices, which makes LoRa and LoRaWAN the most widely used LPWAN technologies at present.

The network topology defined by the LoRaWAN standard is a star topology. The only communication type supported by the current LoRaWAN standard is the one between the end node and the network server [2]. However, a recently introduced study [4] proves that a device-to-device (D2D) communication is possible in the LoRaWAN environment. It technically implements the direct communication between two LoRaWAN end nodes with the assistance of the network server. According to the authors, D2D enables a higher data rate to be used between two end nodes in proximity, thereby improving performance in terms of delay and energy consumption. Unfortunately, this D2D scheme lacks security considerations which are as important as the performance. In the paper, the authors mention the importance of the security, but do not give specific details on how to protect the D2D communication. LoRaWAN supports basic security functions for the communication between the end node and the central server. However, we cannot expect such protection for D2D communication because it is not officially supported by the LoRaWAN standard. To use D2D communication widely, security should be applied.

The current LoRaWAN security research is in the very early stage, so we cannot find proper references for protecting the newly proposed D2D communication. Therefore, we focus on cellular networks that have many previous studies about the secure D2D communication [5], [6]. LoRaWAN and cellular networks have a structural similarity in that most communications are basically made through a central network server or base station. Unfortunately, most secure D2D communication studies on cellular networks are not suitable for LoRaWAN's resource-constrained environment. However, we found that some symmetric key-based approaches [7]–[10]

Manuscript received November 3, 2017; accepted December 26, 2017. Date of publication January 1, 2018; date of current version January 31, 2018. This work was supported by the Basic Science Research Program through the National Research Foundation of Korea, Ministry of Education, under Grant NRF-2015R1D1A1A01058928. The associate editor coordinating the review of this paper and approving it for publication was Prof. Nitaigour P. Mahalik. *(Corresponding author: Jaehyu Kim.)*

The authors are with the Department of Computer Science, Yonsei University, Seoul 03722, South Korea (e-mail: jaehyu_kim@yonsei.ac.kr; jssong2526@yonsei.ac.kr).

Digital Object Identifier 10.1109/JSEN.2017.2789121

are applicable to the environment of LoRaWAN. Thus, we analyze these works and try to design a security scheme for LoRaWAN.

In this paper, we propose a new secure D2D link establishment scheme to protect the basic D2D communication introduced in [4]. Our scheme newly defines the SecureD2DReq and SecureD2DAns messages. The two D2D nodes exchange these messages with the network server. The two nodes receive the same security parameters from the network server through this process. These security parameters are used for cryptographic key generation. Eventually, both nodes share the same key and following D2D communication can be secured. Our security analysis shows that mutual authentication, confidentiality, and integrity can be guaranteed. For performance evaluation, we compute the energy consumption at the end node of the basic D2D scheme and the proposed scheme. In this process, we use the real-world measurement results for the calculations. The calculation results show that the energy consumption of the proposed scheme increases about 4-5%, which has little effect on the battery lifetime of the end node. In conclusion, our scheme provides basic security and is sufficiently feasible.

The remainder of this paper is organized as follows. In section 2, we provide related works about the symmetric key-based secure D2D schemes for cellular networks. Section 3 provides the background knowledge necessary to understand the proposed scheme. Section 4 is a security analysis of the proposed scheme. In section 5, for performance evaluation, we compare the proposed scheme and the basic D2D scheme in terms of the energy consumption. Section 6 is our conclusion about this research.

II. Related Works

Among many secure D2D studies in cellular network environments, we found that symmetric key-based approaches [7]–[10] are applicable to the LoRaWAN environment. In this section, we describe how they work and analyze them.

Liu and Zhang [7] proposed a key agreement scheme between two nodes participating in D2D communication in cellular networks. Before D2D communication, a node receives the session key to protect the D2D communication from the core network and the parameters used to generate the session key. After receiving the parameters, the node sends the received parameters to the other node. Then the corresponding node can generate the session key using the parameters. Eventually, two nodes share the same session key and can perform secure D2D communication.

A similar approach was proposed in [8]. In this scheme, when the core network receives a D2D communication request from D2D nodes, it sends a common master key to D2D nodes. Then, each node can use the master key to generate a session key to be used for secure D2D communication. In addition, an individual authentication method for each node and a mutual authentication method between two nodes have also been proposed.

According to [5], there are vulnerabilities in these two schemes, as both directly send the session key used for D2D communication or the master key for session key generation. If the transmission between the core network and the node is endangered, D2D communication can also be dangerous together. The following two studies, which used an XOR operation, can be a more secure way to resolve this problem.

In [9], the core network creates a session key similar to other schemes and distributes it to both nodes. The main feature of this scheme is that the keys of two nodes are combined by an XOR operation before transmission. After receiving the combined key, each node generates its own key and then extracts the key of corresponding node from the combined key. The two nodes can securely communicate with each other using the shared session keys.

A D2D key distribution process proposed in [10] also uses an XOR operation. One difference is that each node generates a base value and sends it to the core network in the request phase. The core network uses these values to generate keys for the two nodes, combines them with the XOR operation, and sends the combined key to both D2D nodes.

Based on the analysis of these four studies, we design a proposed secure D2D link establishment that can be applied to LoRaWAN. In particular, we adopt a structure in which the core network distributes security keys to D2D nodes. We also use an XOR operation to prevent the direct leakage of the key used in the D2D communication when the communication channel between the end node and the network server is exploited.

III. Background

In this section, we provide a brief description of basic LoRaWAN communication and basic LoRaWAN D2D communication.

A. Basic LoRaWAN Communication

Figure 1 shows the LoRaWAN network environment. The LoRaWAN network consists of an end node, a LoRaWAN gateway, a network server, and an application server. The LoRaWAN standard defines the role of network entities and their relationships. The end node is deployed in various places and transmits data through the LoRa wireless channel. The LoRaWAN gateways receive the message from the end node through the LoRa channel and send it to the network server via the IP connection. The network server checks the validity of the received message and forwards the data to the application server. The network server also manages the entire LoRaWAN network. The application server uses the data to provide the application to the user. In this LoRaWAN environment, only communication between the end node and the server side is supported.

The basic security of LoRaWAN communication is provided by the network session key (NwkSKey) and the application session key (AppSKey). When the end node is activated, the session keys are shared between the server-side and the end node. Figure 2 shows how each key protects LoRaWAN messages. The NwkSKey is used to calculate the message integrity code (MIC) to detect unauthorized modification of

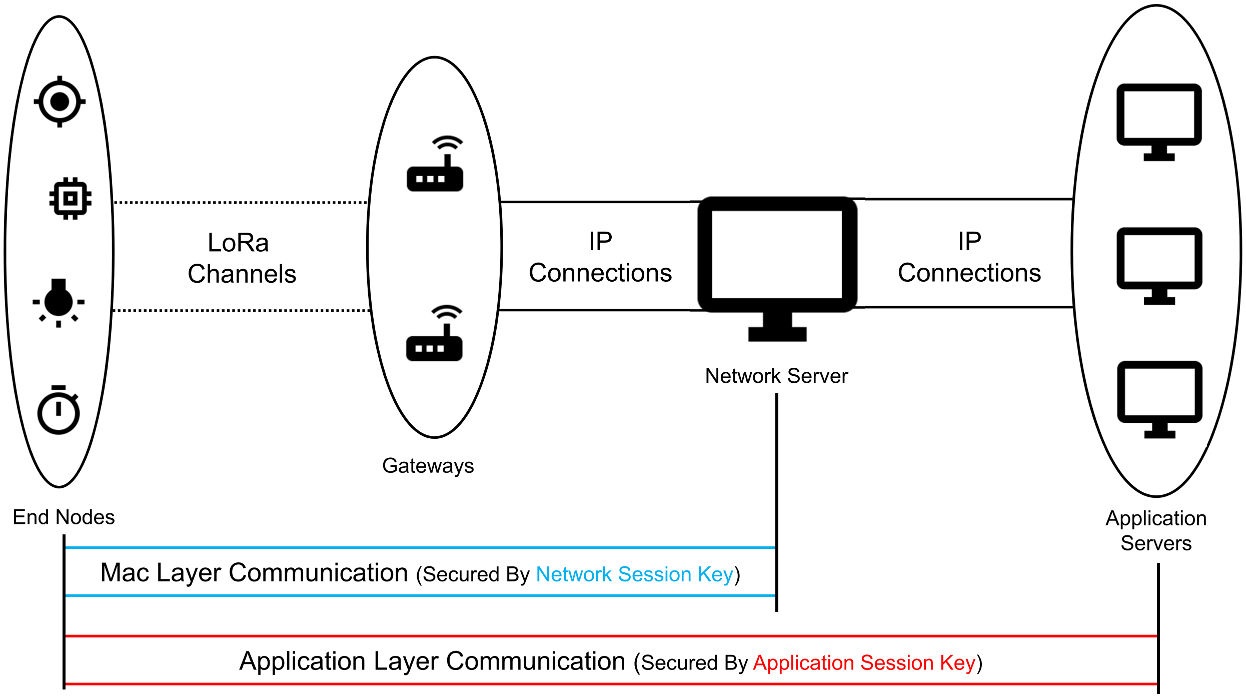

LoRa
Channels
IP
Connections
IP
Connections
Network Server
Gateways
End Nodes
Application
Servers
Mac Layer Communication (Secured By Network Session Key)
Application Layer Communication (Secured By Application Session Key)

Fig. 1. LoRaWAN network environment.

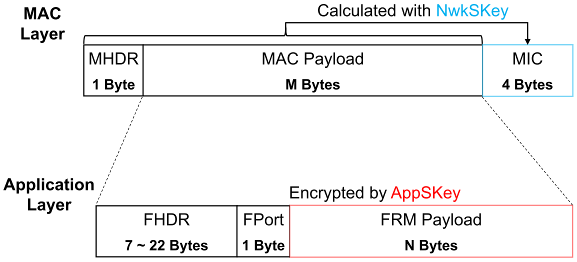


Fig. 2. LoRaWAN packet structure.

LoRaWAN messages. The AppSKey is used to encrypt the data payload.

B. Basic LoRaWAN Device-to-Device Communication

Figure 3 shows the whole process of the basic D2D communication [4], which is not defined in the current LoRaWAN standard. In the D2D link establishment stage, node A sends a Report message to the network server. This message requests the network server to assign a network channel for the D2D communication. The network sever sends an Init_D2D message in reply to the Report message. The Init_D2D consists of the channel parameters required for the D2D communication. According to [4], these parameters are frequency, data rate, transmission power, and timer values. End node B also obtains these parameters by communicating with the network server, as node A does. After receiving the Init_D2D, each node waits for a certain period of time for synchronization, and then performs the D2D link operation.

The D2D communication has advantages in terms of energy consumption. A higher data rate can be used when two neighboring LoRaWAN nodes communicate directly. As a result, the overall transmission time is reduced, and eventually the energy consumption of the end node is also reduced [4]. However, basic D2D communications have a fatal disadvantage of not considering security. Since the LoRaWAN standard does not support the D2D, LoRaWAN's session key-based security mechanism cannot be applied either. In other words, current basic D2D communication cannot guarantee basic security requirements like mutual authentication, confidentiality, and integrity at all. This means that the communication can easily be exposed to an attacker. Security should be considered to take full advantage of LoRaWAN D2D communication.

IV. Proposed Scheme

Our proposed secure D2D link establishment scheme is based on the LoRaWAN MAC command. The MAC command is a message defined by the LoRaWAN to exchange network management related information such as link status, data rate, device status, and channel information. The LoRaWAN specification [2] provides an official MAC commands list. In this paper, we newly define two MAC commands SecureD2DReq and SecureD2DAns. Both messages are exchanged between the D2D nodes and the network server, and are responsible for transferring security parameters from the network server to the D2D nodes. By using the received security parameters, two D2D nodes generate the cryptographic keys for securing D2D communication. Figure 4 shows the whole procedure of two D2D nodes A and B performing the proposed scheme, and the following is a detailed description of each step.

1) End Node A ⟶ Network Server: **SecureD2DReq**
   As the first step, the end node A sends the SecureD2DReq to the network server. As shown in Figure 5, payload of the SecureD2DReq consists of CID,

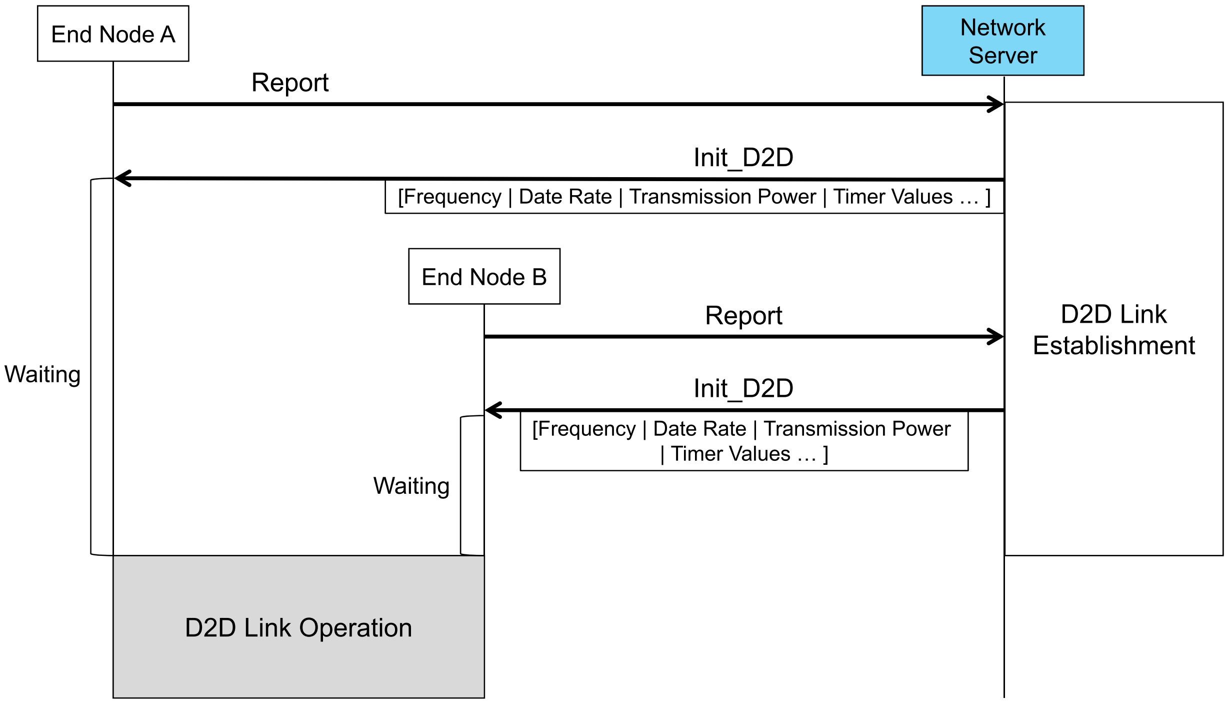

End Node A
Network Server
Report
Init_D2D
[Frequency | Date Rate | Transmission Power | Timer Values …]
End Node B
Report
D2D Link Establishment
Waiting
Init_D2D
[Frequency | Date Rate | Transmission Power | Timer Values …]
Waiting
D2D Link Operation

Fig. 3. Basic LoRaWAN D2D communication.

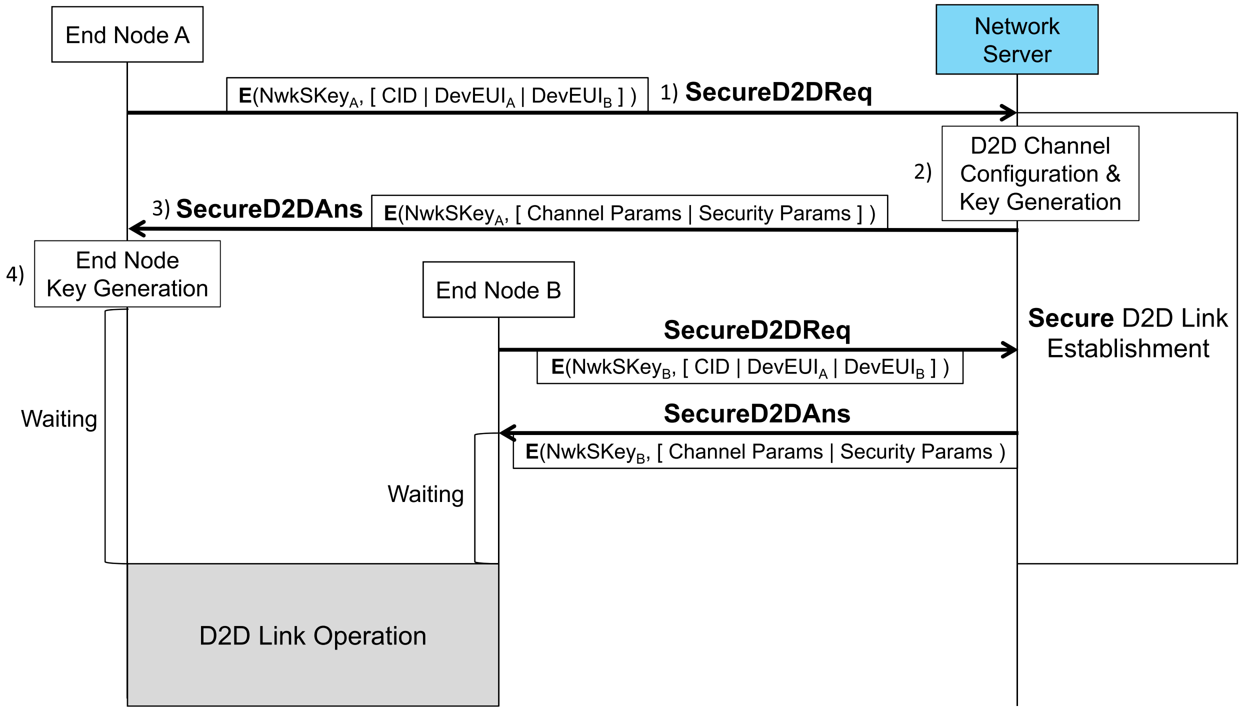

End Node A
Network Server
E(NwkSKey$_A$, [CID | DevEUI$_A$ | DevEUI$_B$])
1) SecureD2DReq
2)
D2D Channel Configuration & Key Generation
3) SecureD2DAns
E(NwkSKey$_A$, [Channel Params | Security Params])
4)
End Node Key Generation
End Node B
SecureD2DReq
E(NwkSKey$_B$, [CID | DevEUI$_A$ | DevEUI$_B$])
Secure D2D Link Establishment
Waiting
SecureD2DAns
E(NwkSKey$_B$, [Channel Params | Security Params)
Waiting
D2D Link Operation

Fig. 4. Secure D2D link establishment.

DevEUI$_A$, and DevEUI$_B$. The CID field indicates the type of the MAC command. DevEUI$_A$, and DevEUI$_B$ are global identifiers of end node A and B, which follow the IEEE EUI-64 address space format. The fields of the payload, except for the CID, may change depending on the type of LoRaWAN application. The payload of the SecureD2DReq is encrypted with the NwkSKey$_A$. We assume that the NwkSKey$_A$ is shared between the end node A and the network server through the previous activation process.

2) Network Server: **D2D Channel Configuration & Key Generation**
After receiving the SecureD2DReq, the network server determines the channel parameters and security

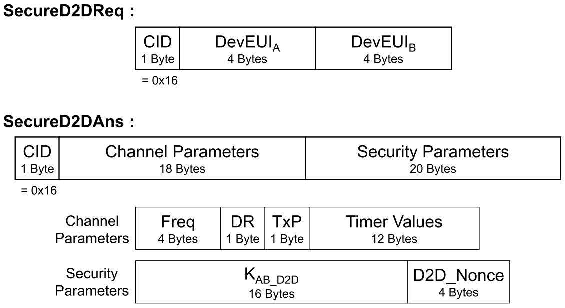


Fig. 5. Secure D2D messages paylod.

parameters to be used for D2D communication. As shown in Figure 5, the channel parameters consist of frequency (Freq), data rate (DR), transmission power ($T \times P$), and timer values as defined in [4]. Security parameters are K_{AB_D2D} and $D2D\_Nonce$. $D2D\_Nonce$ is a 4-byte random value generated by the network server. K_{AB_D2D} is a combined key, which is generated by the XOR operation of K_{A_D2D} and K_{B_D2D}. K_{A_D2D} and K_{B_D2D} are the D2D root keys of end nodes A and B, which are used to generate the encryption and integrity keys at the later step. K_{AB_D2D}, K_{A_D2D} and K_{B_D2D} are generated as follows.

$$K_{A\_D2D} = aes128\_encrypt\,(\mathbf{NwkSKey_A},\ D2D\_Nonce)$$
$$K_{B\_D2D} = aes128\_encrypt(\mathbf{NwkSKey_B},\ D2D\_Nonce)$$
$$K_{AB\_D2D} = K_{A\_D2D}\ XOR\ K_{B\_D2D}$$

K_{A_D2D} and K_{B_D2D} are generated with aes128_encrypt, which is officially used for key generation in the LoRaWAN standard. The NwkSkey of each node and $D2D\_Nonce$ are used as arguments.

3) Network Server ⟶ End Node A: **SecureD2DAns** When all parameters are determined, the network server sends the SecureD2DAns message, which consists of channel parameters and security parameters, to end node A. The message is encrypted by the NwkSKey$_A$ as the SecureD2DReq message is. Figure 5 shows the structure of the SecureD2DAns message.

4) End Node A: **Key Generation** After end node A receives the SecureD2DAns, it generates the K_{A_D2D} in the same way as the network server using the received security parameters and its NwkSKey$_A$. Then, end node A extracts the K_{B_D2D} as follows.

$$K_{B\_D2D} = K_{AB\_D2D}\ XOR\ K_{A\_D2D}$$

With K_{A_D2D} and K_{B_D2D}, end node A generates K_{A_enc}, K_{A_int}, K_{B_enc}, and K_{B_int}. The K_{A_enc} and K_{B_enc} are encryption keys of end nodes A and B. The $K_{A_int}$and K_{B_int} are integrity keys of the end node A and B. These keys are generated as follows.

$$K_{A\_enc} = aes128\_encrypt(K_{A\_D2D}, 0 \times 01|D2D\_Nonce)$$
$$K_{A\_int} = aes128\_encrypt(K_{A\_D2D}, 0 \times 02|D2D\_Nonce)$$
$$K_{B\_enc} = aes128\_encrypt(K_{B\_D2D}, 0 \times 01|D2D\_Nonce)$$
$$K_{B\_int} = aes128\_encrypt(K_{B\_D2D}, 0 \times 02|D2D\_Nonce)$$

If the same key is used for encryption and integrity checking, the attacker may be able to forge a valid message as well as just eavesdrop data when the key is leaked. Thus, we use 0×01 and 0×02 to generate different encryption and integrity keys. LoRaWAN standard uses a similar method to create a NwkSKey and AppSKey. After the key generation is completed, end node A waits until the D2D link operation starts.

End node B also exchanges the SecureD2DReq and the SecureD2DeAns with the network server as end node A. K_{A_enc}, K_{A_int}, K_{B_enc}, and K_{B_int} are generated as a result of this process. After completing key generation, two nodes share the four keys. These keys are used to protect communications between the two nodes, as the NwkSKey and the AppSKey are used in the LoRaWAN standard. For example, when end node A transmits D2D data, it encrypts the data with K_{A_enc} and generates an integrity code with K_{A_int}. Then end node B can decrypt and check the integrity of the received data with the K_{A_enc} and the K_{A_int}, respectively. In this message exchanging procedure, the two nodes can authenticate each other by verifying the corresponding node has a valid key.

V. Security Analysis

In this section, we provide the security analysis of the proposed scheme in two ways. The first involves the security of the proposed D2D link establishment process. We analyze whether the SecureD2DReq and the SecureD2DAns messages are exchanged safely. The second is an analysis of how the proposed scheme protects the D2D communication between two nodes.

A. Security Analysis of the Mac Command

In this paper, we newly defined two mac commands, SecureD2DReq and SecureD2DAns. Both follow the mac command specification defined in the LoRaWAN standard. Thus, security mechanisms provided by the LoRaWAN for protecting the mac command can also be applied to the SecureD2DReq and the SecureD2DAns. For instance, the payload of each message is encrypted by the NwkSKey. The integrity code is also generated with the NwkSKey for detecting the unauthorized change of the message. Since the NwkSKey is shared only between the end node and the network server, message authentication of the mac command can also be guaranteed.

B. Security Analysis of the D2D Communication With the Proposed Scheme

The two devices participating in the D2D can share cryptographic keys (K_{A_enc}, K_{A_int}, K_{B_enc}, K_{B_int}) by performing the proposed secure D2D link establishment. With these keys, D2D communication can satisfy the following three security requirements: mutual authentication, confidentiality, message integrity.

1) Mutual Authentication: The two nodes need to mutually authenticate each other in the process of the D2D communications. In the proposed secure D2D link establishment phase, the network server authenticates each node using the NwkSKey and sends the security parameters for key generation only to the legitimate node. The two nodes can generate the same cryptographic keys using the transferred security parameters. Therefore, the two nodes can perform mutual authentication by checking whether corresponding node has a valid key.

2) Confidentiality & Message Integrity: The LoRaWAN standard uses the NwkSkey and the AppSKey to satisfy the confidentiality and integrity of the transferred data. Through the proposed secure D2D link establishment process, D2D communications can be secured in a similar way to the LoRaWAN standard by using cryptographic keys. For instance, K_{A_enc} and K_{B_enc} is used to encrypt the payload just as the AppSKey is used in the LoRaWAN standard. K_{A_int} and K_{B_int} are also used to compute the message integrity code just as the NwkSKey does. In conclusion, D2D communication can satisfy confidentiality and integrity with the proposed scheme.

VI. Performance Evaluation

In this section, we compare the performance of proposed secure D2D link establishment and basic D2D link establishment in which the security function is not applied. We use an energy consumption as a comparison metric, which is also used in the basic D2D research [4]. According to [11], TRANSMIT and RECEIVE states of the LoRa transceiver have a substantial effect on the energy consumption of the LoRaWAN end node. Thus, we measured the TRANSMIT and RECEIVE states duration time on the actual LoRaWAN device and, based on the measurement results, calculated the total energy consumption of our scheme and the basic D2D scheme.

In our research, the duration of the TRANSMIT state is determined by the time it takes for an end node to send the SecureD2DReq message of the proposed scheme or the Report message of the basic D2D scheme. The duration of the RECEIVE state is determined by the time it takes for the end node to receive the SecureD2DAns message of the proposed scheme or the Init_D2D message of the basic D2D. We expected that the increased length of SecureD2DAns due to the security parameters would increase the RECEIVE state duration of the end node and this would also increase total energy consumption of the end node. To accurately measure the effect of the increased RECEIVE state duration, we designed experiments to make an effect of the TRANSMIT state be applied identically to both schemes. According to the basic D2D [4], the Report messages can contain any uplink data, and our proposed SecureD2DReq also contains only basic data that can be changed according to applications or policies. In this context, we implemented the payload of the Report and SecureD2DReq message equally so that the TRANSMIT state duration becomes equal for both schemes. As a result, we could precisely evaluate how the increased RECEIVE state duration affects the overall battery lifetime of the end node.

A. Device Setup

As a LoRaWAN end node, we used an iM880B demo board [12]. We implemented the function to monitor the operation of the LoRa transceiver based on the source code provided by Semtech [13]. To establish a LoRa gateway, we first connected the the Raspberry Pi 2 and iC880A module [14]. Then, we installed software for the LoRa gateway provided by the Semtech [15], [16]. The server-side was implemented with Brocaar‘s open-source projects [17]–[19].

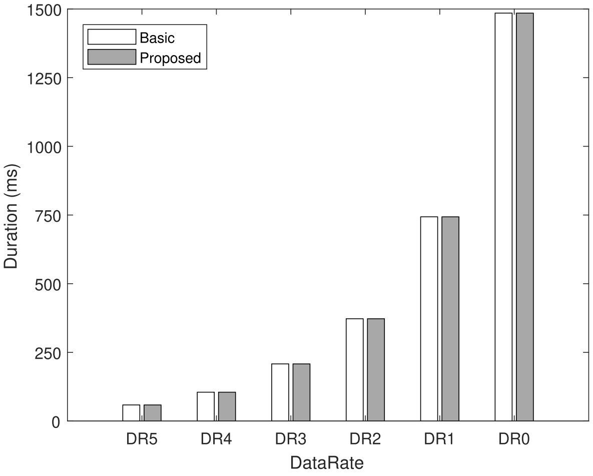


Fig. 6. TRANSMIT state duration on the LoRaWAN end node.

B. Measurement Results

The duration time of the TRANSMIT state and the RECEIVE state varies with the data rate. We measured the duration time from DR0 to DR5, which are defined as the default data rates in the LoRaWAN. The details of each data rate can be found in the LoRaWAN regional parameters document [20].

Figure 6 shows TRANSMIT state duration time of the proposed scheme and the basic scheme. The values are measured on the end node. We implemented both the Report and SecureD2DReq messages have the same payload that includes the DevEUI of two D2D nodes as described in section 3 to ensure that the TRANSMIT state duration of both schemes are equal. As s result, we can confirm that TRANSMIT state duration is almost the same for both schemes.

Figure 7 is the result of measuring the RECEIVE state duration of the end node. The proposed scheme shows the 35-40% increased RECEIVE state duration time compared with the basic scheme. This is because the network server sends the longer packet to the end node in the proposed scheme. In the basic scheme, the Init_D2D message received by the end node does not consider security, so it only contains the channel parameter. However, the SecureD2DAns of the proposed scheme contains additional 20 bytes of security parameters for key distribution. As a result, the duration of the RECEIVE state of the end node in the proposed scheme become longer.

C. Energy Consumption

According to the [11], the energy consumption of the LoRaWAN end node can be calculated as follows:

$$P \cong \text{VDD} * (I_{tx} * T_{tx} + I_{rx} * T_{rx})$$

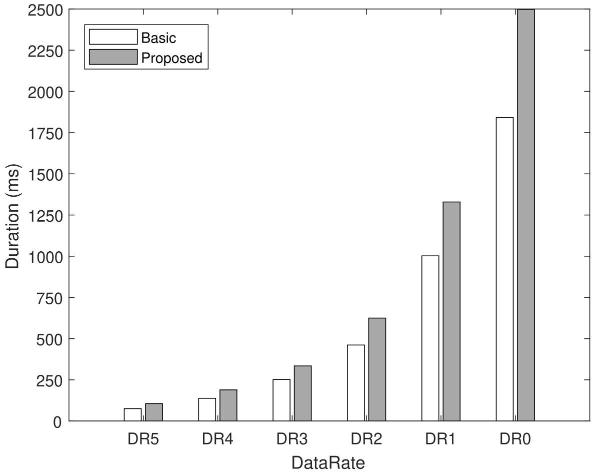


Fig. 7. RECEIVE state duration on the LoRaWAN end node.

TABLE I
PARAMETERS FOR CALCULATING ENERGY CONSUMPTION

Supply Voltage (VDD)	3 V
Current Consumption TRANSMIT (I_{tx}) - Transmission power : 14 dbm	88 mA
Current Consumption RECEIVE (I_{rx})	11.2 mA

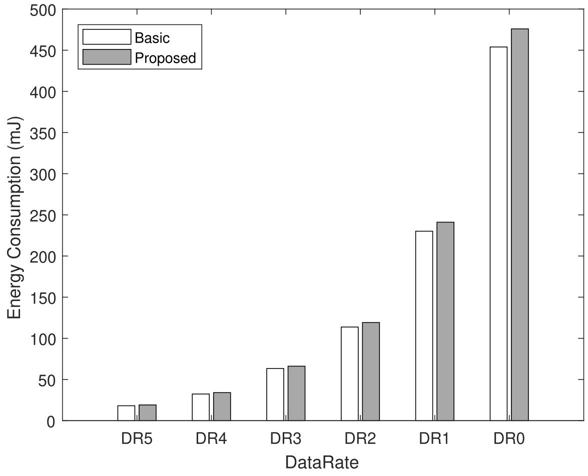


Fig. 8. Energy consumption of the LoRaWAN end node.

T_{tx} and T_{rx} mean the duration time of the TRANSMIT and RECEIVE state of the end node, respectively. In this paper, their values are measured on the actual LoRaWAN device. I_{tx} and I_{rx} are the current consumption at the end node in the TRANSMIT and RECEIVE state, respectively. VDD is the supply voltage value. TWe set the values of I_{tx}, I_{rx}, and VDD according to iM880B datasheet [21] and Table I list them. We calculate the total energy consumption P of the end node with these parameters. Figure 8 and Table II shows the average amount of energy consumed in the end node when performing the proposed and basic scheme once.

TABLE II
ENERGY CONSUMPTION OF THE LORAWAN END NODE

	DR5	DR4	DR3	DR2	DR1	DR0
Proposed Scheme (mJ)	19.06	34.07	66.17	119.31	240.91	475.90
Basic Scheme (mJ)	18.05	32.27	63.38	113.70	229.88	453.92

TABLE III
ENERGY CONSUMPTION OF THE LORAWAN END NODE
AFTER 10-YEAR OPERATION

	DR5	DR4	DR3	DR2	DR1	DR0
Proposed Scheme (J)	69.57	124.36	241.51	435.49	879.35	1737.06
Basic Scheme (J)	65.87	117.78	231.33	415.04	839.06	1656.81

We can confirm that the energy consumption of the proposed scheme is increased overall. As shown in Figure 6, the duration of the TRANSMIT state is the same for both schemes. Therefore, the main reason for the increased energy consumption in the proposed scheme is the longer RECEIVE state duration due to the added security parameters. It can be said that energy consumption has increased as a trade off for the security function. However, compared with the energy consumption of the basic D2D scheme, the increased rate is only 5%, which is negligible considering the capacity of the battery in general use. Assuming the LoRaWAN end node performs D2D link establishment every day for 10 years, the total energy consumption of the proposed scheme and the basic scheme is calculated as Table III. As for the DR0, which has the largest difference between two schemes, the proposed scheme uses approximately 80J more energy than the basic scheme. The iM880B board we used in the experiment uses two AAA batteries, which can store about 12,960J of energy when using an alkaline battery. Therefore, the additional energy consumed by our scheme for 10 years is only approximately 0.6% of the total battery capacity. If other data rate is applied, this ratio is further reduced. This means that our scheme scarcely affect the lifetime of the end node, and that our scheme has sufficient feasibility.

VII. CONCLUSION

In this paper, we propose a secure D2D link establishment scheme to protect D2D communication in LoRaWAN. The proposed scheme consists of the SecureD2DReq and SecureD2DAns messages. These messages are exchanged between the end nodes and the network server. The two nodes participating in the D2D share cryptographic keys through this process. With these keys, D2D communication can satisfy mutual authentication, confidentiality, and message integrity. We evaluate the performance by comparing the energy consumption of the proposed scheme and the basic D2D scheme. To calculate energy consumption, we monitored the operation of the LoRa tranceiver installed on the actual LoRaWAN device. The calculation results show that the energy consumption in the proposed scheme increases by approximately 4-5%, which has little effect on the lifetime of the end node. In conclusion, our scheme provides a secure D2D communication with sufficient feasibility.

References

[1] "A technical overview of LoRa and LoRaWAN," LoRa Alliance, San Ramon, CA, USA, Tech. Rep., Nov. 2015. [Online]. Available: https://docs.wixstatic.com/ugd/eccc1a_ed71ea1cd969417493c74e4a13c55685.pdf

[2] N. Sornin, M. Luis, T. Eirich, T. Kramp, and O. Hersent, "LoRaWAN specification," LoRa Alliance, San Ramon, CA, USA, Tech. Rep. Version 1.0.2, Jul. 2016.

[3] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," *IEEE Commun. Surveys Tuts.*, vol. 9, no. 2, pp. 855–873, 2nd Quart., 2017.

[4] K. Mikhaylov, J. Petäjäjärvi, J. Haapola, and A. Pouttu, "D2D communications in LoRaWAN low power wide area network: From idea to empirical validation," in *Proc. IEEE Int. Conf. Commun. Workshops*, Paris, France, May 2017, pp. 737–742.

[5] M. Wang and Z. Yan, "A survey on security in D2D communications," *Mobile Netw. Appl.*, vol. 22, no. 2, pp. 195–208, Apr. 2017.

[6] M. Haus, M. Waqas, A. Y. Ding, Y. Li, S. Tarkoma, and J. Ott, "Security and privacy in device-to-device (D2D) communication: A review," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1054–1079, 2nd Quart., 2017.

[7] Y. Liu and D. J. Zhang, "Methods and apparatus for generating keys in device-to-device communications," U.S. Patent 9 660 804, May 23, 2017.

[8] J.-T. Wang and T.-M. Lin, "Authentication system for device-to-device communication and authentication method therefore," U.S. Patent 9 232 391, Jan. 5, 2016.

[9] M. Alam, D. Yang, J. Rodriguez, and R. Abd-alhameed, "Secure device-to-device communication in LTE-A," *IEEE Commun. Mag.*, vol. 52, no. 4, pp. 66–73, Apr. 2014.

[10] S.-J. Hakola, T. Koskela, and H. M. Koskinen, "Method and apparatus for device-to-device key management," U.S. Patent 8 989 389, Mar. 24, 2015.

[11] S. Barrachina-Muñoz, B. Bellalta, T. Adame, and A. Bel, "Multi-hop communication in the uplink for LPWANs," *Comput. Netw.*, vol. 123, pp. 153–168, Aug. 2017.

[12] IMST, Kamp-Lintfort, NRW, Germany. (2016). *SK-iM880B—Long Range Radio Starter Kit*. Accessed: Sep. 12, 2017. [Online]. Available: https://wireless-solutions.de/products/starterkits/sk-im880b.html

[13] Semtech, Camarillo, CA, USA. (2013) *LoRaWAN Endpoint Stack Implementation and Example Projects*. Accessed: Sep. 12, 2017. [Online]. Available: https://github.com/Lora-net/LoRaMac-node

[14] IMST, Kamp-Lintfort, Germany. (2016) *iC880A—LoRaWAN Concentrator 868 MHz*. Accessed: Sep. 12, 2017. [Online]. Available: https://wireless-solutions.de/products/radiomodules/ic880a.html

[15] Semtech, Camarillo, CA, USA. (2013) *LoRa Gateway Project*. Accessed: Sep. 12, 2017. [Online]. Available: https://github.com/Lora-net/lora_gateway

[16] Semtech, Camarillo, CA, USA. (2013). *LoRa Network Packet Forwarder Project*. Accessed: Sep. 12, 2017. [Online]. Available: https://github.com/Lora-net/packet_forwarder

[17] O. Brocaar. *LoRa Gateway Bridge*. Accessed: Sep. 12, 2017. [Online]. Available:https://github.com/brocaar/lora-gateway-bridge

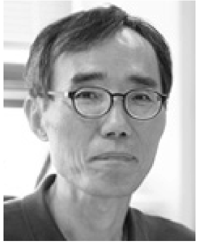
[18] O. Brocaar. *LoRa Server*. Accessed: Sep. 12, 2017. [Online]. Available: https://github.com/brocaar/loraserver

[19] O. Brocaar. *LoRa App Server*. Accessed: Sep. 12, 2017. [Online]. Available: https://github.com/brocaar/lora-app-server

[20] LoRa Alliance Technical Committee, "LoRaWAN regional parameters," LoRa Alliance, San Ramon, CA, USA, Tech. Rep. Version 1.0, Jul. 2016.

[21] IMST, Kamp-Lintfort, NRW, Germany. (2016). *WiMOD iM880B Datasheet*. Accessed: Sep. 12, 2017. [Online]. Available: https://wireless-solutions.de/images/stories/downloads/Radio%20Modules/iM880B/General_Information/iM880B_Datasheet_V1_4.pdf

Jaehyu Kim (S'17) received the B.S. degree in computer science from Yonsei University, Seoul, South Korea, in 2011, where he is currently pursuing the Ph.D. degree. His research interests include network and computer security.



JooSeok Song received the B.S. degree in electrical engineering from Seoul National University, Seoul, South Korea, in 1976, the M.S. degree in electrical engineering from the Korea Advanced Institute of Science and Technology, Daejeon, South Korea, in 1979, and the Ph.D. degree in computer science from the University of California at Berkeley, Berkeley, in 1988.

From 1988 to 1989, he was an Assistant Professor with the Naval Postgraduate School, Monterey, CA, USA. He is currently a Professor of Computer Science with Yonsei University, Seoul. His research interests include cryptography and network security.