Regular Paper

Lightweight Secure Communication Considering Network Path Reliability in IPv6 Wireless Sensor Network

Shunya Koyama[*], Yoshitaka Nakamura [**], and Hiroshi Inamura [**]

[*]Graduate School of Systems Information Science, Future University Hakodate, Japan
[**] School of Systems Information Science, Future University Hakodate, Japan
{g2117020, y-nakamr, inamura}@fun.ac.jp

Abstract - In recent years, IPv6 wireless sensor networks have been widely spread in various fields including IoT environments, because of the development of low-power sensor devices and wireless communication technologies. However, on these sensor networks, it is difficult to use secure communication technologies that can become large overhead, due to power saving of the wireless nodes is important. As one approach to deal with this problem, a method of focusing on Nonce which is one element of security, and separating it from secure communication is proposed, though this method can be used only when the reliability of communication ensured. Therefore, it remains a problem that not suit in environments such as wireless sensor networks where the reliability of communication is not ensured, since multi-hop networks and the like is used. In this paper, we propose a Nonce truncation method that can deal with such environments. Our method is implemented on the nodes that establish secure communication, and transfer information of about several bits that can estimate the Nonce associated the ciphertext as the truncated Nonce value. We also evaluated the effectiveness of our method by comparing the lifetime of the devices between our method and the previous method, and could confirm the effectiveness in a simple secure communication model.

Keywords: IoT, Reliability of Communication, Secure Communication, Nonce

1 INTRODUCTION

Recently, IPv6 (Internet Protocol version 6) wireless sensor networks have been widely spread in various fields including IoT environments, because of the development of low-power sensor devices and wireless communication technologies. The penetration rate of these devices has been increased, and as can be seen from Fig.1, about 50 billion devices will be interconnected in 2020 [1]. It is also expected to be utilized in various fields.

On the other hand, these sensor networks are typically composed of communication devices with limited computing resources such as battery capacity, CPU performance, and little memory. These characteristics are often due to cost constraint and physical constraints on such as size and available energy. Also, these tight limits make it difficult to attain some high load functions like secure communication that are pretty much taken for granted for conventional networks. So, mechanisms considering these resource constraints are required in the sensor networks.

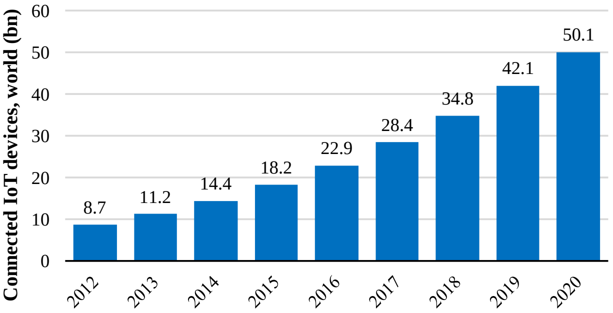


Figure 1: The number of connected IoT devices in the world

In addition, wireless sensor networks that called LLNs (Low power and Lossy Networks) are about to become widely spread. LLNs have restrictions not only on the resource constraint of the above-mentioned but also on the networks. The network constraint involves instabilities such as low data rate and high packet loss rate are accompanied in the communication environment, its reliability is not guaranteed. These tight constrained networks are needed to meet the demand for IoT services in various fields. Therefore, there are various factors that impose these restrictions, such as an introduction of simple and highly scalable UDP, and use of a multi-hop network to deal with a wide range of sensing.

In general, in these wireless sensor networks including LLNs, low power consumption wireless communication standard represented by Zigbee [3] is introduced. However, these standards are based on IEEE 802.15.4 [4] as a data link layer technology, and its frame size is small. Therefore, considering resource constraints, it is required some data size reduction scheme for side information like protocol control information. As the information to be reduced, the IPv6 header that supports the IoT service is no exception.

As one of the proposals for introducing IPv6 into such constrained networks, IETF (Internet Engineering Task Force) has established a policy to expand part of these low power consumption wireless communication standards. As a typical example of this, there is a method of providing an adaptation layer for using IPv6 technology on IEEE 802.15.4. Specifically, there are 6LoWPAN (IPv6 over Low-Power

ISSN1883-4566 © 2020 - Informatics Society and the authors. All rights reserved.

Wireless Personal Area Networks) [5] which compresses IPv6 header or UDP header for alleviating a problem that the frame size of IEEE802.15.4 is too small in the introduction of the IPv6 technology, RPL (IPv6 Routing Protocol for Low Power and Lossy Networks) [6] which is a routing protocol to support the above-mentioned unstable communication environment, and so on. Here, there are many techniques related to the introduction of IPv6, but there are many reasons why this approach is mainly performed. First, IPv6 allows for a huge amount of addresses and provides easy participation in the network by such as SLAAC (StateLess Address Auto Configuration). Thus, it is possible to deal with the interconnection of the aforementioned enormous number of IoT devices, which is difficult in IPv4. In addition, IPv6 based networks can be interconnected readily between the devices including other IPv6 networks because the networks don't need intermediate entities like protocol translation. In consequence, the network scalability is high, and it can deal with various scenarios requested by IoT services. There are many other advantages, but it is said that IPv6 is more appropriate than IPv4 for the reasons mentioned above. Therefore, IPv6 has a high affinity wireless sensor networks including LLNs, and these technologies are expected to be used in various environments including smart grid, smart factory, and others as the core technology.

While it is expected that such communication scheme targeting LLNs based on IEEE 802.15.4 with IPv6 will become widespread, security problems such as unauthorized access aimed at valuable information assets exchanged over the wireless sensor network are also becoming apparent [7]. However, most of the research on this communication scheme is concerned with the network construction, and discussion on security has not been sufficiently done. For example, 6LoWPAN technology described above compresses only the header information, so does not support large size security elements for secure communication. Moreover, although the constraint on the small frame size is relaxed by the compression scheme, the header information occupies much of the frame size remains. Therefore, the importance of considering reduction of side information like secure elements is higher than sensor networks without IP. Therefore, the importance of considering reduction of side information like secure elements is higher than sensor networks without IP. In addition, despite there are proposals for the lightweight secure communication methods for wireless sensor networks without IP which was a major before the spread of IoT service, it has a big different background from recent sensor networks with network constraints like LLNs. For example, a method of separating Nonce which is one security element from communication and reducing its size to zero is proposed. However, in the lossy network, it is difficult to operate the Nonce correctly in this method, so it can become a heavy process. Hence, in an actual scenario, it is necessary to consider a lightweight truncation of Nonce method that can properly operate according to the frame loss rate. For this reason, it is difficult to apply conventional security technology for the LLNs environment. Especially, the problems that cannot support IEEE802.15.4 small frame size, and unstable communication quality are left.

In this paper, we discuss the unstable communication quality and the resource constraints of sensor devices which are the features of LLNs. Then, we design a secure communication method that can deal with these features. To this end, we focus on Nonce (Number used once) which is one of the security elements and address a method to truncate this. Also, in this method, we design a lightweight secure communication scheme that can operate without applying excessive overhead to sensor devices at any frame loss rate.

2 RELATED WORK

As the previous method, a lightweight secure communication method has been proposed, which is focusing on Nonce that is a part of security elements, and completely separating this from the communication. In the following, we describe the mechanism of the previous method and its applicability to LLNs, based on the basic secure communication technology.

2.1 Overview of Basic Secure Communication

In this section, we describe the general secure communication establishment method, and the secure design when applying it to the LLNs based on IEEE 802.15.4, in consideration of the data frame structure.

2.1.1 Establishing General Secure Communication

Strictly speaking, the establishment method of secure communication differs depending on the required security requirements and the Block Cipher Modes of Operation selected according to the requirements. As famous examples of the Modes of Operation, there are CBC (Cipher Block Chaining) mode and CTR (CounTeR) mode that provide confidentiality of communication data, and CCM (Counter with CBC-MAC) mode combines confidentiality and authenticity in an efficient way as authenticated encryption mode [8]. Among them, CCM mode can deal with processing resource constraints and frame size restriction of sensor devices. That's because this mode can process of encryption and decryption in parallel by the same algorithm, and does not expand data size of ciphertext. Moreover, this mode is known as high versatility because has many security requirements that can be provided, can apply various fields. Hence, it also coincides exactly with the design concept of the communication scheme for LLNs. Therefore, we describe how to establish secure communication in CCM mode on the premise of introduction to LLNs. The overview of the operation is depicted in Fig.2.

Figure 2 shows the flow from an establishment of secure communication between sensor devices until the Sender generates an encrypted frame from the plaintext, and then from this frame to the plaintext by the Receiver. In this figure, Key is a secret key, Nonce is a security element to make it possible to use the same Key multiple times without security risk, and MAC (Message Authentication Code) is a security element to provide integrity or authenticity, added

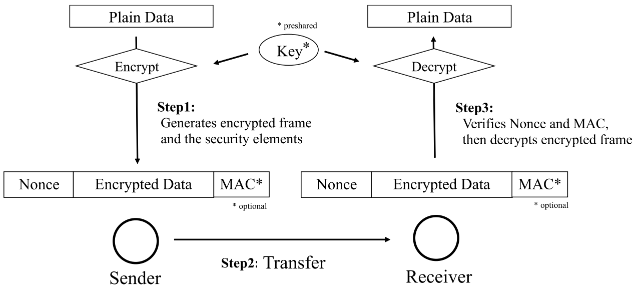


Figure 2: Basic operation of secure communication

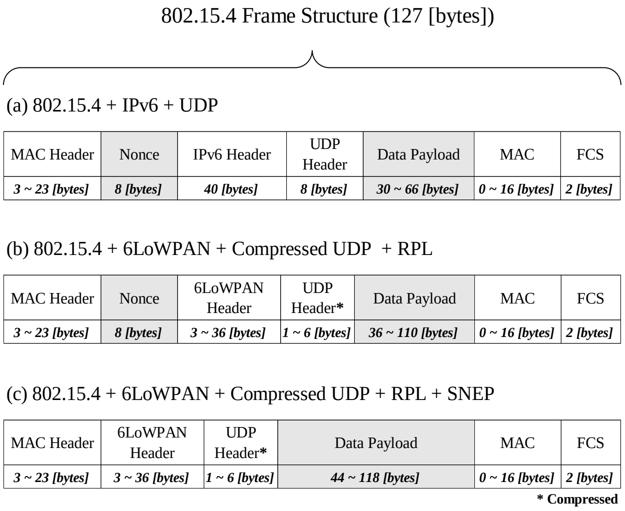
only when using CCM mode. As the initial operation of secure communication establishment, sensor devices share the key being secret information, then communicate Nonce, MAC, and encrypted frame as public information. Thereafter, Nonce and MAC that change according to the corresponding encrypted frame are continuously communicated, and these are verified whether each value is correct when the Receiver decrypts the frame.At this time, in particular with respect to the calculation method of Nonce, the value corresponding to each encrypted frame must be unique from the viewpoint of security risk. In the NIST (National Institute of Standards and Technology), they have listed several recommended specifications and calculation methods of Nonce, and the size should be 8 bytes or more [9]-[10]. Further, as one of the calculation methods, a method using a counter value starting from an arbitrary value (for example, zero) is recommended. The value is incremented and shared every time different ciphertexts are generated. SNEP described later in section 2.2 and our proposed method described later in chapter 3 are based on this calculation method.

2.1.2 Secure Communication Design in LLNs (Low power and Lossy Networks)

Figure 3 shows an example of a simple data frame structures when the above described secure communication is applied to LLNs.

In Fig.3, (a)(b)(c) commonly indicate the frame structure when IP technology is introduced on IEEE 802.15.4 and encrypted using CCM mode. In addition, for each frame structure, (a) is introduced UDP into IPv6, (b) is introduced 6LoWPAN and RPL over (a), and(c) is introduced SNEP described later in section 2.2 of the previous method over (b). As can be seen from the figure, the security elements communicated can be large overhead and suppress MAC payload in the environment with limited frame size as LLNs. Therefore, there is a possibility of increasing the processing load of sensor devices through fragment processing, it is desirable to make the size as small as possible. In particular, in each frame structure excluding (c), the ratio of Nonce to MAC payload occupies so large that if Nonce can be completely eliminated, on average about 16% and about 12% of the payload can be expanded.

In order to properly operate the Block Cipher Modes of Operation, there is no strict restriction that each security element must secure a certain size or more. However, if you select the smallest value among the simply selectable sizes, there is also the possibility of impairing the safety of secure communication. From that point of view, NIST recommends the size of Nonce is 8 bytes or more. Thus, a method of reducing the size without losing the safety of secure communication is ideal.



802.15.4 Frame Structure (127 [bytes])

(a) 802.15.4 + IPv6 + UDP

MAC Header	Nonce	IPv6 Header	UDP Header	Data Payload	MAC	FCS
3 ~ 23 [bytes]	*8 [bytes]*	*40 [bytes]*	*8 [bytes]*	*30 ~ 66 [bytes]*	*0 ~ 16 [bytes]*	*2 [bytes]*

(b) 802.15.4 + 6LoWPAN + Compressed UDP + RPL

MAC Header	Nonce	6LoWPAN Header	UDP Header*	Data Payload	MAC	FCS
3 ~ 23 [bytes]	*8 [bytes]*	*3 ~ 36 [bytes]*	*1 ~ 6 [bytes]*	*36 ~ 110 [bytes]*	*0 ~ 16 [bytes]*	*2 [bytes]*

(c) 802.15.4 + 6LoWPAN + Compressed UDP + RPL + SNEP

MAC Header	6LoWPAN Header	UDP Header*	Data Payload	MAC	FCS
3 ~ 23 [bytes]	*3 ~ 36 [bytes]*	*1 ~ 6 [bytes]*	*44 ~ 118 [bytes]*	*0 ~ 16 [bytes]*	*2 [bytes]*

*** Compressed**

Figure 3: Structure pattern of encrypted frames in LLNs (Low power and Lossy Networks)
(a): 802.15.4 + IPv6 + UDP
(b): 802.15.4 + 6LoWPAN + Compressed UDP + RPL
(c): 802.15.4 + 6LoWPAN + Compressed UDP + RPL + SNEP

2.2 SNEP (Secure Encryption Network Protocol)

Following the previous section, a method of separating Nonce from communication and reducing its size to zero without reducing the safety of secure communication called SNEP (Secure Network Encryption Protocol) has been proposed as a part of a large security schema named SPINS (Secure Protocols for Sensor Networks) [11]. Figure 4 shows the simple operation flow. Specifically, SNEP is the method of sharing only the initial value of Nonce, and thereafter incrementing the Nonce value stored in the sensor devices according to the number of received encrypted frames. If an encrypted frame is lost in the middle due to interruption of communication, decryption fails because the Nonce corresponding to the subsequent encrypted frame does not mesh. For this reason, the resynchronization process is performed to transmit the entire value of Nonce every time the encrypted frames are lost. By taking such a series of procedures, it is shown that in an environment with the stable communication quality, the communication overhead on the sensor devices by secure communication is reduced. On the other hand, in the environment such as LLNs which the communication quality is unstable and the frame loss rate can be high, the resynchronization process frequently occurs. Therefore, this means secure communication overhead of sensor devices is actually increasing, and network congestion problem may occur.

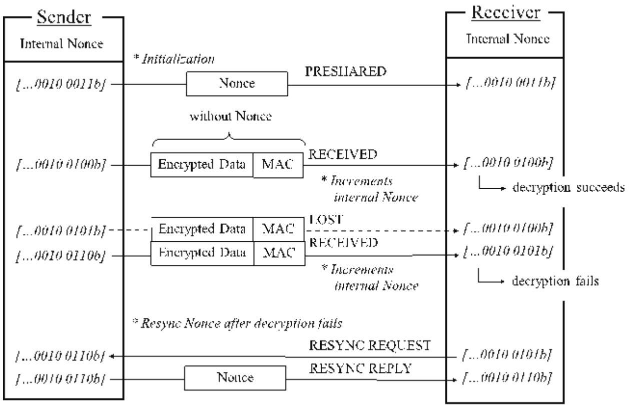


Figure 4: Simple operation flow of SNEP (Secure Network Encryption Protocol)

3 PROPOSAL METHOD

3.1 Research Tasks

In the previous method, if an encrypted frame is lost in the middle due to interruption of communication or the like, it is necessary to repeat the resynchronization process of Nonce for recovery secure communication. Therefore, it is not supported in the environment where the frame loss rate can be high. Also, according to a general secure communication method, the ratio of encrypted frames occupied by Nonce is large, and there is a possibility that a heavy load is applied to the sensor devices and the network itself due to inefficient fragment processing. For this reason, any method is difficult to adapt to LLNs where communication quality is unstable and frame size is limited, and a method capable of dealing with these problems is required.

In this paper, we propose a method to deal with the above problem by estimating Nonce only by sensor devices itself from the truncated value that the size changes according to the frame loss rate.

3.2 Basic Operation

In this section, we describe the basic mechanism for truncating a Nonce. As the block cipher mode of operation for establishing secure communication, CCM mode is used. Also, as a calculation method of Nonce corresponding to each encrypted frame, a counter value that increments the value according to the frame is used.

As a basic idea, we propose the method to minimize Nonce resynchronization processing for frame loss which the problem in the related research. The overview of the proposed method, the device sends a small amount of information that can estimate Nonce as a hint instead of transmitting the entire Nonce value. Then, the receiver estimates the entire Nonce value to be synchronized from this hint and Nonce stored on the device. Hereafter, we describe the operation flow according to Fig.5.

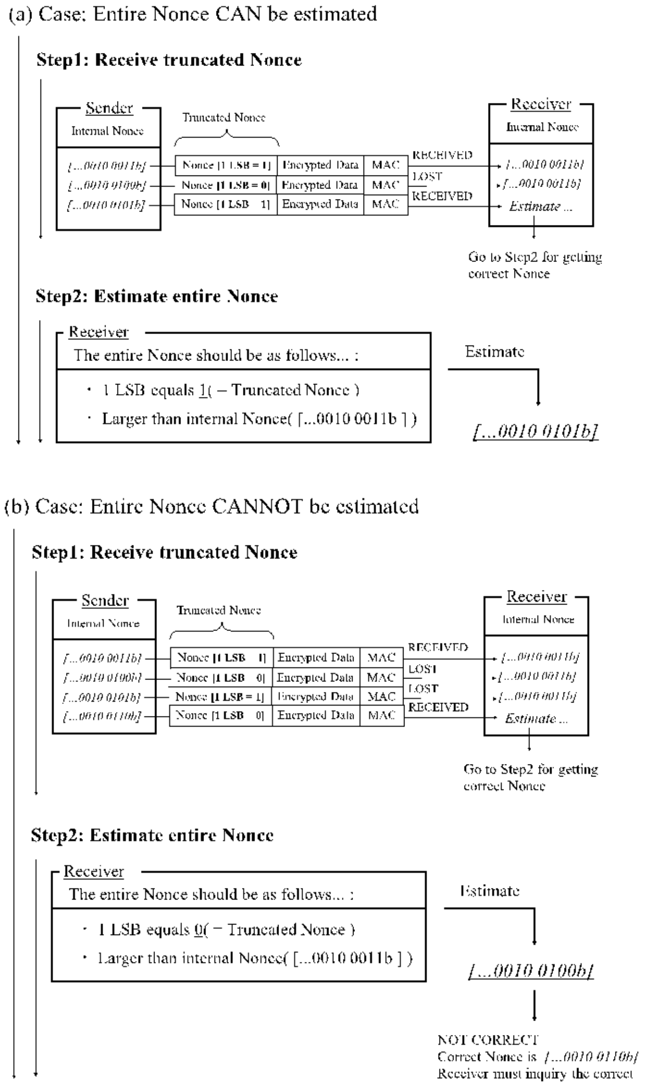


Figure 5: Operation flow in the case where the truncated Nonce length is 1
(a): entire Nonce value can be estimated
(b): entire Nonce value cannot be estimated

The first step, the initial value of Nonce is shared between Sender and Receiver, and the whole value is stored in the sensor device as in the previous method. Thereafter, in the sharing of Nonce, only the N of least significant bits (N LSBs) are assigned on communication. Hereinafter, this N bit is called a truncated Nonce length. Figure 5 shows the operation flow in the case where the truncated Nonce length is 1 as the specific example.

In Fig.5, (a)(b) commonly begin already synchronized entire Nonce between Sender and Receiver devices and estimate the entire Nonce value from the truncated value while the devices communicate several encrypted frames. First, (a) shows that the receiver succeeds in receiving the third encrypted frame after losing only the second encrypted frame. At this time, since there is a difference in the entire value of Nonce internally stored between the two sensor devices, receiver fails in decryption the third encrypted frame. At this stage, move on to step 2 of (a). Since the value of the received truncated Nonce is 1, the receiver can decrypt the third encrypted frame by estimating the entire value of

Nonce that is greater than internal Nonce value and 1 LSB equals 1. On the other hand, in the case of (b), the receiver receives the fourth encrypted frame after losing the second and third encrypted frames, hence fails in decryption even if estimates the entire value of Nonce like (a). This is because there was a big difference in the entire values of Nonce internally stored between both sensor devices. In the case (b) shown in this figure, although correct Nonce is "*...0010 0110b*", in fact, it is estimated "*...0010 0100b*" by mistake. In such a case, recovery secure communication by performing resynchronization process sharing the entire value of Nonce. Generally, such resynchronization process occurs only when the truncated Nonce length is *x* bits and the frame is lost consecutively for 2^x times or more. For example, in the case of (b), this process occurs because the frame has been lost 2^1 times that is twice consecutively.

Therefore, depending on the selection of the truncated Nonce length, the same problem as SNEP may still occur. For this reason, it is necessary to select the truncated Nonce length flexibly so as to minimize the number of the resynchronization process according to the frame loss rate of the communication environment. Table 1 shows the occurrence probability of the resynchronization process according to *x* bits of truncated Nonce length and frame loss rate.

3.3 Optimization of the Resynchronization Process Occurrence Count

Considering the characteristics of LLNs, it is necessary to minimize the occurrence probability of the resynchronization process as much as possible so that the same problem as SNEP does not occur. For that purpose, it is ideal to flexibly select the truncated Nonce length as short as possible according to the frame loss rate. For example, referring to Table 1, if we fix the truncated Nonce length to 4 bits, it seems that can support any frame loss rate. However, in actual fact, there is a possibility that the frame loss rate suddenly changes due to temporary noise or the like, so it is required to deal with dynamic link quality.

In order to deal with this problem, we use ETX (Expected Transmission Count) [12] adopted in routing protocols used in many wireless sensor networks including RPL.

ETX is a metric index using link quality, and its value is defined as the reciprocal of the frame arrival rate. Specifically, it can be found using the following equation (1) where E_{pt} is the frame loss rate.

Table 1: Probability of the resynchronization process occurrence according to the truncated Nonce length and frame loss rate

Frame Loss Rate Truncated Nonce Length	**80%**	**60%**	**40%**	**20%**	$\mathbf{E_{pt}}$
1	64%	36%	16%	4%	$E_{pt}^{2^1}$
2	40%	13%	2.5%	0%	$E_{pt}^{2^2}$
4	2.8%	0%	0%	0%	$E_{pt}^{2^4}$
x	$80\%^{2^x}$	$60\%^{2^x}$	$40\%^{2^x}$	$20\%^{2^x}$	$E_{pt}^{2^x}$

$$ETX = \frac{1}{1 - E_{pt}} \qquad (1)$$

By solving this equation (1) for E_{pt}, the packet loss rate can be obtained. Therefore, in the sensor devices having information corresponding to Table 1, it is possible to select the truncated Nonce length dynamically to minimize the occurrence probability of the resynchronization process to any value or less.

4 EVALUATIONS

About the proposed method and previous methods in this research, we performed evaluation experiments after implementing these on the network simulator. Hereinafter, we describe the experimental environment, evaluation method, experiment method and the detail of these.

4.1 Experiment Environment

We implemented the proposed method and (b)(c) in Fig.3 as the previous methods on ContikiOS, which is a built-in OS for sensor networks, and operated on the network simulator Cooja [13] attached to ContikiOS.

Specifically, as shown in Fig.6, we created a simple small-scale model that established secure communication between two sensor devices such as Sender and Receiver, operated each method in this model. At this time, we emulated all sensor devices as Zolertia Z1 hardware [14].

For simplicity, unidirectional communication is performed from the Sender to the Receiver, and encrypted frames are transmitted and received in this scenario.

Detailed simulation parameters in the experimental environment are shown in Table 2. The communication standard conforms to (b) in Fig.3 as the general standard. In addition, only the length of Nonce is selected from among 0 to 8 bits or 8 bytes different according to the frame loss rate. Furthermore, the 0 bit corresponds to SNEP as the previous method and the 8 bytes without special handling to Nonce corresponds to the general method. In the block cipher mode of operation, we used AES-CCM* mode standardized on Zigbee which extended the CCM mode. Also, a frame loss rate is used as an index representing communication quality in LLNs. Moreover, considering the resynchronization process due to frame loss, experiments were performed until all data arrives at Receiver and completely decrypted after establishing secure communication.

4.2 Evaluation Method

In each experimental method, we measured the lifetime of the sensor device from the power consumption of the Sender emulated as Zolertia Z1 hardware on Cooja. We evaluate the effectiveness by calculating and comparing the lifetime ratio of each method where general method (b) in Fig.3 as 1 value.

4.3 Experimental Method

One experiment for each combination of frame loss rate and truncated Nonce length and the other experiment in the case of continuing to select the optimal truncated Nonce length to minimize the number of the resynchronization process. We describe the details of each experiment method below.

4.3.1 Experiment for Each Combination of Frame Loss Rate and Truncated Nonce Length

In this experiment, we evaluate whether the length of each Nonce can correspond to any communication quality assuming LLNs environment as the proposed method and the previous method. First, about the lifetime ratio of each sensor devices, we calculated from the power consumption until the Receiver took 1,000 KB of data from the Sender 10 times and decrypted all the data. At this time, to evaluate the performance for each length of Nonce in accordance with the frame loss rate, the experiment was proposed at intervals of 10% to 20% in the frame loss rate in Table 2.

4.3.2 Experiment for Continuing to Select the Optimal Truncated Nonce Length

In this experiment, we evaluate whether the effectiveness can be shown compared with the previous method when dynamically selecting optimum Nonce length using the proposed method. The basic simulation parameters were as shown in Table 2, but the frame loss rate was changed randomly between 20% and 80%, and the occurrence probability of resynchronization process was always 5% or less using ETX. Also, it was assumed that 1000 KB of data was transmitted ten times a day. In such an environment, we calculated the average lifetime ratio of sensor devices in each method.

5 RESULTS AND DISCUSSION

5.1 Results

The results obtained in each experimental method are shown in the following section.

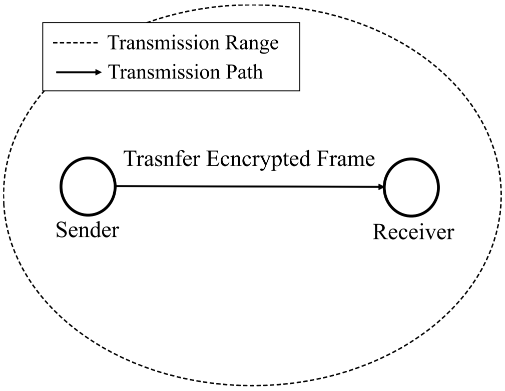
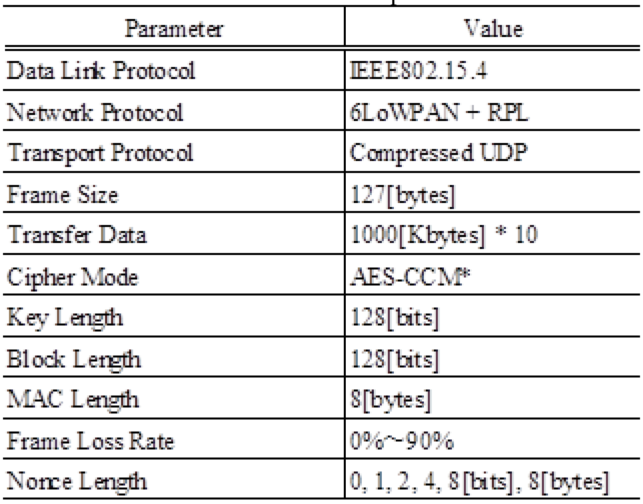


Figure 6: Experiment environment

Table 2: Simulation parameters



Parameter	Value
Data Link Protocol	IEEE802.15.4
Network Protocol	6LoWPAN + RPL
Transport Protocol	Compressed UDP
Frame Size	127[bytes]
Transfer Data	1000[Kbytes] * 10
Cipher Mode	AES-CCM*
Key Length	128[bits]
Block Length	128[bits]
MAC Length	8[bytes]
Frame Loss Rate	0%~90%
Nonce Length	0, 1, 2, 4, 8[bits], 8[bytes]

5.1.1 Experimental Results for Each Combination of Frame Loss Rate and Truncated Nonce Length

The result obtained by the experiment according to the combination of frame loss rate and the truncated Nonce length is shown below.

Figure 7 shows the Sender's lifetime ratio measured for each frame loss rate and truncated Nonce length (hereinafter referred to as *x*) in the simulation parameters shown in Table 2. In the case where the frame loss rate was 20% or less, all the proposed method and the previous method had improved the lifetime compared with the general method of transmitting 8 bytes of Nonce. On the other hand, when the frame loss rate exceeded 20%, the lifetime sharply decreased according to the length of Nonce. In particular, the rate of decrease was remarkable when the truncated Nonce length was 4 bits, but in the case of 8 bits, any frame loss rate was improved. Also, it could be seen that the truncated Nonce length at which the lifetime improves most was different depending on the frame loss rate except 0%.

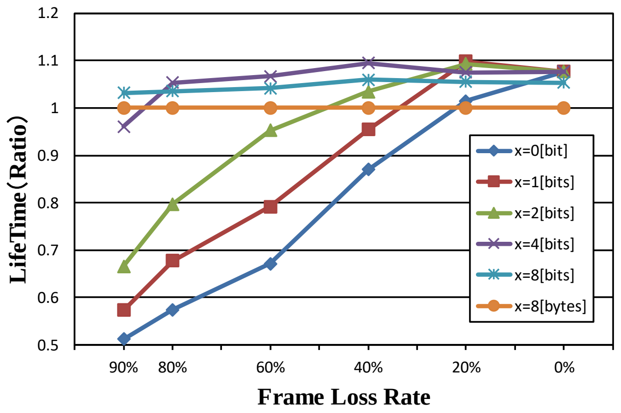


Figure 7: Lifetime ratio according to truncated Nonce length and frame loss rate by simulation

Table 3: Lifetime ratio obtained for each method by simulation

Method	Lifetime Ratio
General(Nonce Length: 8[bytes])	1
Previous(Nonce Length: 0[byte])	0.625
Proposal	1.058

5.1.2 Experimental Results for Continuing to Select the Optimal Truncated Nonce Length

The result obtained by the experiment for continuing to select the optimal truncated Nonce length so that the occurrence probability of the resynchronization process within 5% is shown in following Table 3. The effectiveness of the proposed method is clear because the proposed method was improved the lifetime by about 6%, while SNEP that previous method dropped the lifetime about 37% when compared with the lifetime of the general method that transmitted 8 bytes of Nonce.

5.2 Discussion

From the results shown in Fig.7 and Table 3, the effectiveness of the proposed method is clarified because previous methods cannot deal with unstable communication quality such as LLNs, whereas the proposed method improves the lifetime. This is considered because the number of resynchronization process has decreased, and the number of fragmentation data has also decreased because the ratio in the encrypted frame occupied by Nonce is reduced. Also, if the truncated Nonce length is about 4 to 8 bits, the lifetime is roughly improved in any frame loss rate, except when the loss rate is extremely high. This means that truncated Nonce length is enough size to operate in the LLNs environment. On the other hand, depending on the select of the truncated Nonce length, it is also clear that the possibility of greatly decreasing the lifetime also remains, and as also shown from the results in Table 3. So, it is effective to select continually the optimum truncated Nonce length.

However, in the experimental environment, since evaluation is limited to a simple secure communication model between two devices, in the future it is necessary to verify the effectiveness from many aspects according to the real environment. Particularly, there are many problems such as dealing with frame delay, handling burst loss caused by network congestion problem. It is also necessary to consider approaches to deal with these problems. Moreover, in order to further improve the proposed method, we will adjust the number of times to estimate the entire Nonce value according to the truncated Nonce length. Therefore, it is necessary to measure the processing load in the decryption process and the resynchronization process, and to measure how many times the decryption process can be increased.

6 CONCLUSION

In this paper, we discussed the unstable communication quality and the resource constraints of sensor devices which are the features of LLNs. Then, we designed the secure communication method that could deal with these features. To this purpose, we focused on Nonce which is one of the security elements and proposed the method to truncate this. As a result, we prevent the frequent occurrence of Nonce resynchronization processing at the time of frame loss, which was a problem of the conventional method, and minimize the number of times of processing. In consequence, we showed the effectiveness of the proposed method as a lightweight secure communication method that deals with unstable communication quality, and without excessive secure communication overhead to sensor devices by reducing encrypted frame size. As the evaluation method, we implemented the proposed method and the conventional method on sensor terminal which emulated, measured its lifetime ratio and compared it. Specifically, we first measured the effect of each method on the lifetime for each frame loss rate. After that, we assumed an environment in which the frame loss rate varies randomly, and compared the influence of each method on the lifetime.

As future prospects, there are we should address examine experiments and evaluation methods considering various more real environments. In particular, we consider that the high frame loss rate in the assumed environment is not practical in the real environment, which is limited to the simple performance evaluation of the methods. Therefore, first of all, it is important to focus on this situation and strictly evaluate the usefulness of the proposed method. And, it is also necessary to deal with the response to burst loss of encrypted frames and the delay problem in real connectionless network. Furthermore, in order to improve the performance of the proposed method, we will adjust the number of times to estimate the entire Nonce value according to the truncated Nonce length by measuring and comparing the processing load in the decryption process and resynchronization process.

REFERENCES

[1] D. Evans (Cisco Internet Business Solutions Group), "The Internet of Things - How the Next Evolution of the Internet Is Changing Everything," <https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf > [Accessed May 20, 2018].

[2] C. Bormann, M. Ersue, and A. Keranen, "Terminology for Constrained-Node Networks," Internet Engineering Task Force RFC7228, (2014).

[3] ZigBee Alliance., "Zigbee specification. Technical Report Document 053474r20," Zigbee Alliance, (2014).

[4] IEEE Std 802.15.4-2017, "IEEE Standard for Low-Rate Wireless Networks," IEEE Standard, (2017).

[5] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. P. Vasseur, and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," Internet Engineering Task Force RFC6550, (2012).

[6] N. Kushalnagar, G. Montenegro, and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)," Internet Engineering Task Force RFC4919, (2007).

[7] D. Airehrour, J. Gutierrez, and S. K. Ray, "Secure Routing for Internet of Things: A survey," Journal of Network and Computer Applications, Vol.66, pp.404-412, (2016).

[8] Information technology Promotion Agency, "The Survey Regarding Block-cipher Modes of Operation Usable for Confidentiality, Message Authenticity, and Authenticated Encryption," <https://www.ipa.go.jp/security/enc/CRYPTREC/fy15/documents/mode_wg040607.pdf > [Accessed May 20, 2018].

[9] National Institute of Standards and Technology, "FIPS PUB 140-2 Security Requirements for Cryptographic Modules," (2002).

[10] National Institute of Standards and Technology, "Recommendation for Block Cipher Modes of Operation," <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-38a-add.pdf > [Accessed May 20, 2018].

[11] A. Perrig, R. Szewczyk, J. D. Tygar, V. Web, and D. E. Culler, "SPINS: security protocols for sensor networks," Wireless Networks Journal, Vol.8, pp.521-534, (2002).

[12] D.S.J. De Couto, D. Aguayo, J. Bicket, and R. Morris, "A High-Throughput Path Metric for Multi-Hop Wireless Routing," Proceedings of ACM MobiCom, pp. 134-146, (2003).

[13] "Cooja Simulator," <http://anrg.usc.edu/contiki/index.php/Cooja_Simulator> [Accessed May 20, 2018].

[14] Zolertia, "Zolertia Z1 Datasheet," <http://zolertia.sourceforge.net/wiki/images/e/e8/Z1_RevC_Datasheet.pdf> [Accessed May 20, 2018].

(Received October 21, 2018)
(Revised June 24, 2019)

Shunya Koyama received B.E. degree in systems information science from Future University Hakodate, Japan in 2017. He is a graduate student of Future University Hakodate. His research interests include lightweight security in IPv6 wireless sensor network. He is a student member of IPSJ.

Yoshitaka Nakamura received B.E., M.S., and Ph.D. degrees from Osaka University in 2002, 2004 and 2007, respectively. He is currently an associate professor at the School of Systems Information Science, Future University Hakodate. His research interest includes information security and ubiquitous computing. He is a member of IEEE, IEICE, and IPSJ.

Hiroshi Inamura He is a professor of School of Systems Information Science, Future University Hakodate, since 2016. His current research interests include mobile computing, system software for smart devices, mobile/sensor network and their security. He was an executive research engineer in NTT docomo, Inc. He received B.E., M.E. and D.E. degree in Keio University, Japan. He is a member of IPSJ, IEICE, ACM and IEEE.