A Method of Lightweight Secure Communication Considering 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 - Recently, IPv6 wireless sensor networks are widely spread in various fields including IoT environments. 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. However, it remains a problem that not suit in environments such as wireless sensor networks where reliability of communication is not ensured. In this paper, we propose a Nonce truncation method that can deal with such environments. Our method transfer information of about several bits that can estimate the Nonce associated the ciphertext as the truncated Nonce value. We evaluated the effectiveness of our method by comparing the lifetime of the nodes between the method and previous methods.

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

1 INTRODUCTION

IPv6 wireless sensor networks are widely spread in various fields including IoT environments lately, because of the development of low-power sensor devices and wireless communication technologies. The penetration rate of these device has been increased, and about 50 billion devices will be interconnected in 2020 [1]. It is also expected to be utilized in various fields.

On the other hand, there are constrained networks that impose strict restrictions on the computing power and the communication quality of the sensor devices. They are called LLNs (Low power and Lossy Networks) [2], are composed of communication devices with limited computing resources. Also, the reliability of communication is not guaranteed due to high packet loss rate and so on. These strictly constrained networks are needed to meet the demand of IoT services in various fields.

As one of the proposals for dealing with such constrained networks, IETF (Internet Engineering Task Force) has established a policy to expand part of it based on communication standards used in conventional wireless sensor networks representing Zigbee [3]. As a typical example of this, there is a method of providing an adaptation layer for using IPv6 (Internet Protocol v6) technology on IEEE 802.15.4 which is a data link layer technology for power saving of communication equipment. Specifically, there are 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) which compresses IPv6 header or UDP header, RPL (IPv6 Routing Protocol for Low Power and Lossy Networks) which is a routing protocol to support the above-mentioned unstable network path reliability, and so on.

While it is expected that such communication scheme targeting LLNs based on IEEE 802.15.4 will become widespread, security problems aimed at these constrained networks are also becoming apparent [4]. Also, there are proposals for the lightweight secure communication methods for sensor networks not using IP which was a major before the spread of IoT service, but it has a background which is very different from recent sensor network. For this reason, it is difficult to apply conventional security technology for the LLNs environment. Especially, the problems that be not able to 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 the secure communication method that can deal with these features. To this end, we focus on Nonce 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 previous method, a lightweight secure communication system has been proposed, which is focusing on Nonce (Number used once) that is a part of security elements. 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 Block Cipher Modes of Operation selected. As famous example of the

Modes of Operation, there is CCM (Counter with CBC-MAC) mode combines confidentiality and authenticity in an efficient way as authenticated encryption mode. The CCM mode coincides exactly with the design concept of the communication scheme for LLNs from the viewpoint of its versatility, resource constraints, frame size limitation. Therefore, we focus on the CCM mode and explain the operation outline.

CCM mode provides security using secret key and Nonce, and MAC (Message Authentication Code). Here, Nonce is a security element to make it possible to use the same Key multiple times without security risk, and MAC is an arbitrary security element to provide integrity or authenticity.

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 [5]. Further, as one of the calculation methods, a method using a counter value starting from an arbitrary value is recommended. The value is incremented and shared every time different ciphertexts are generated. The methods are described later are based on this calculation method.

2.1.2 Secure communication design in LLNs

Fig.1 shows an example of a simple data frame structures when the above described secure communication is applied to LLNs.

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 1: Structure pattern of encrypted frames in LLNs

In Fig.1, (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 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 size of Nonce is 8 bytes or more. Thus, a method of reducing the size without losing the safety of secure communication is ideal.

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) [6] has been proposed. Specifically, this method shares only the initial value of Nonce using communication, and thereafter incrementing 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, resynchronization process is performed to transmit the entire value of Nonce. It is shown that in an environment with the stable communication quality, the communication overhead by the secure communication is reduced. On the other hand, in the environment such as LLNs which the communication quality is unstable, the resynchronization process frequently occurs. Therefore, this means secure communication overhead is actually increase, and network congestion problem may occur.

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 support to 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 adopt 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 are used. Also, as a calculation method of Nonce corresponding to each encrypted frame, a counter value that increment the value according to the frame is used. 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. Fig.2 shows the operation flow in the case where the truncated Nonce length is 1 as the specific example.

In Fig.2, (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, receiver can decrypt the third encrypted frame by estimating 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), receiver receives the fourth encrypted frame after losing the second and third encrypted frames, hence fails in decryption even if estimates entire value of Nonce like (a). 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 re-synchronous process according to the frame loss rate of the communication environment. Table 1 shows the occurrence probability of resynchronization process according to x bits of truncated Nonce length and frame loss rate.

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

Frame Loss Rate / Truncated Nonce Length	80%	60%	40%	20%	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	$80\%^{2^x}$	$60\%^{2^x}$	$40\%^{2^x}$	$20\%^{2^x}$	$E_{pt}^{2^x}$

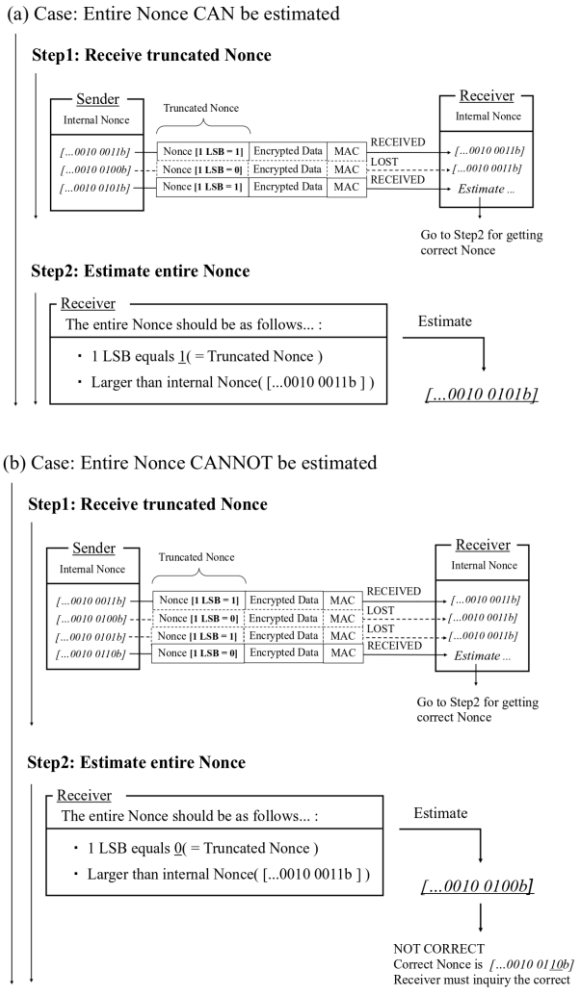

Figure 2: Operation flow in the case where the truncated Nonce length is 1

3.3 Optimization of resynchronization process occurrence count

Considering the characteristics of LLNs, it is necessary to minimize the occurrence probability of 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.

In order to deal with this problem, we use ETX (Expected Transmission Count) adopted in routing protocols used in many wireless sensor networks. ETX is a metric index using link quality, and its value is defined as the reciprocal of the frame arrival rate. Therefore, the sensor devices having information corresponding to Table 1, can select the truncated Nonce length dynamically to minimize the occurrence probability of the resynchronization process to any value or less by using this value.

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.1 as the previous methods on devices and operated on the network simulator. Specifically, 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 [7]. 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.1 as general standard. In addition, a frame loss rate is used as an index representing communication quality in LLNs. Also, only the length of Nonce is selected from among 0 to 8 bits or 8 bytes different according to the frame loss rate. Moreover, considering resynchronization process due to frame loss, experiments were performed until all data arrives at Receiver and completely decrypted after establishing secure communication.

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]

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. We evaluate the effectiveness by calculating and comparing the lifetime ratio of each method where general method (b) in Fig.1 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 synchronization 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 proposed method and 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 result obtained in each experimental method are shown in the following section.

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 truncated Nonce length is shown below.

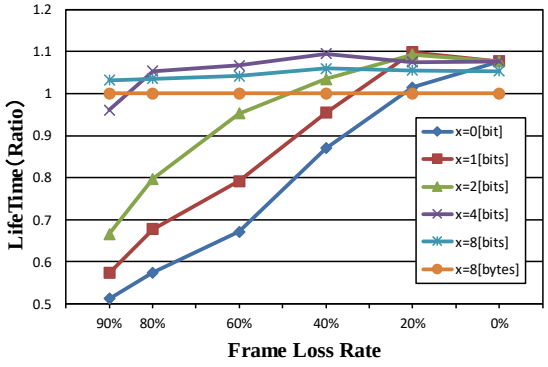

Figure 3: Lifetime ratio according to truncated Nonce length and frame loss rate by simulation

Fig.3 shows 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 decreased 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 cloud be seen that the truncated Nonce length at which the lifetime improves most was different depending on the frame loss rate except 0%.

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 re-synchronous process within 5% is shown in following Table 3.

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

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 general method that transmitted 8 bytes of Nonce.

5.2 Discussion

From the results shown in Fig.3 and Table 3, the lifetime of the proposed method is better than previous methods. 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. 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.

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 confirmed the proposed method improved the lifetime as lightweight secure communication method that deal with unstable communication quality which was the problem of the previous method. As the evaluation method, we implemented the proposed method and conventional method on sensor terminal which emulated, measured its lifetime ratio and compared it.

As future prospects, there are we should address examine experiments and evaluation methods considering various more real environments. And, it is also necessary to deal with the response to burst loss and the delay problem of the encrypted frames in connectionless network. Furthermore, in order to improve 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 Bussiness Solutions Group), “The Internet of Things - How the Next Evolution of th e Internet Is Changing Everything, ” <https://www.cisc o.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 Rep ort Document 053474r20,” Zigbee Alliance, 2014.

[4] D.Airehrour, J.Gutierrez, and S.K.Ray, “Secure Routin g for Internet of Things: A survey, ” Journal of Networ k and Computer Applications, Vol.66, pp.404-412,201 6.

[5] National Institute of Standards and Technology, “FIPS PUB 140-2 Security Requirements for Cryptographic Modules, ” 2002.

[6] A.Perrig, R.Szewczyk, J.D.Tygar, V.Web, and D.E.Cul ler.,“SPINS: security protocols for sensor networks,” Wireless Networks Journal, Vol.8, pp.521-534, 2002.

[7] Zolertia, “Zolertia Z1 Datasheet,” <http://zolertia.sourc eforge.net/wiki/images/e/e8/Z1_RevC_Datasheet.pdf> [Accessed May 20, 2018].