LETTER Special Section on Information and Communication System Security

# Reliable Key Distribution Scheme for Lossy Channels

Ryuzou NISHI[†a)], Yoshiaki HORI[††], *and* Kouichi SAKURAI[††], *Members*

**SUMMARY** We address reliable key distribution scheme for lossy channels such as wireless or power line. In the key distribution over these lossy channels, if key information is lost, there is critical issue that the subsequent communication is disabled. In this paper, we show that our proposal has more reliable property than the related works and has the reliable property equivalent to the dedicated communication channels such as Ethernet.

***key words:*** *key management, key distribution, wireless communication systems, power line communication systems*

## 1. Introduction

In the key distribution over lossy channels such as wireless or power line, if key information is lost, there is issue that the subsequent communication is disabled. The issue of the key distribution over reliable channels has received much attention. However, the issue of the key distribution over lossy channels has received little attention. In this paper, we address the issue of the key distribution over lossy channels.

## 2. Related Works

Reliable key distribution scheme using forward error correction (FEC) is proposed in [1]. Generally, as a parameter which represents a performance of FEC, a coding gain is used. Key distribution scheme with the larger coding gain represents more reliable distribution scheme. Generally, the longer redundancy used in FEC is, the larger the coding gain is. However, the longer the redundancy becomes, the larger the computational amount becomes exponentially, that is, practically, the coding gain is limited. The proposal [1] uses a Reed-Solomon as FEC. According to [2], a coding gain of a Reed-Solomon is 6 dB.

In the paper [3], as a reliable key distribution scheme, self-healing key distribution scheme is proposed. This proposal uses secret sharing, that is, consecutive multiple packets include the shares of the key. Even though some packets are lost, when the receiver can receives remaining packets above a certain number, including the shares of the same key, the receiver can retrieve the key. However, in order to retrieve the key, the receiver must perfectly receive the multiple packets above a certain number without 1 bit error, over lossy channel.

## 3. Our Goal

As the countermeasures for reliable key distribution, there are also approaches of physical layer. However, when it adapts the proposal in the existing systems, large-sized modification including hardware is required. Hence, we have investigated the proposal in the upper layer, specifically, MAC (Media Access Control) layer.

Under the above limitations, our goal is to improve the reliability compared with the related works, the specific parameters are the packet loss rate of the key message over lossy channels and bit error rate of the key message over lossy channels. Furthermore, our goal is to make BER (bit error rate) equivalent to dedicated communication channels such as Ethernet. In Ethernet, requirement of BER is less than $10^{-9}$ at the link level [5].

## 4. Proposal

### 4.1 Process of the Proposal

Figure 1 shows the sender-side block diagram in the proposed key distribution. Figure 2 shows the timing chart of sender-side. In these figures, the key message represents the original key message which should be distributed in the key distribution that our proposal is not adapted.

In resampling process, transfer rate of key message become lower, as Fig. 2 shows. And, output of the resampling process is multiplied by Orthogonal Cyclic shift M-sequence (see Appendix). Specifically, this multiplying means exclusive OR (XOR) process. The time length of 1 bit of output of resampling process is equal to the time length of 1 period of Orthogonal Cyclic shift M-sequence. And, output of multiplexing (XOR) is distributed.

Noise is added to the above output of XOR over the lossy channels such as wireless channels or power line channels. Figure 3 shows the receiver-side block diagram in the proposed key distribution. Figure 4 shows the timing chart of receiver-side. In these figures, the received key message represents the message which is transferred to MAC layer from physical layer after receiver receives the output of XOR added with noise.

The received key message is multiplied by Orthogonal

Manuscript received July 31, 2007.
Manuscript revised December 7, 2007.

[†]The author is with Panasonic Communications Co., Ltd., Fukuoka-shi, 812–8531 Japan.
[††]The authors are with Department of Computer Science and Communication Engineering, Kyushu University, Fukuoka-shi, 819–0395 Japan.
a) E-mail: nishi.ryuzou@jp.panasonic.com

DOI: 10.1093/ietisy/e91–d.5.1485

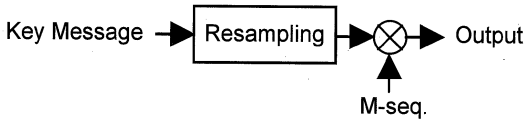


**Fig. 1** Sender-side block diagram.

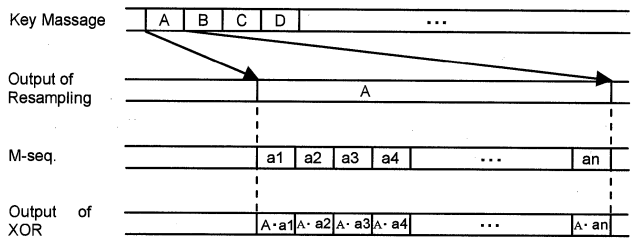


**Fig. 2** Timing chart of sender-side.

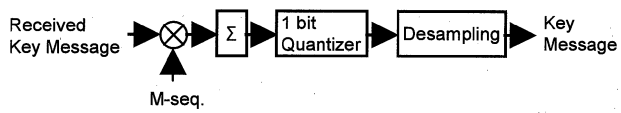


**Fig. 3** Receiver-side block diagram.

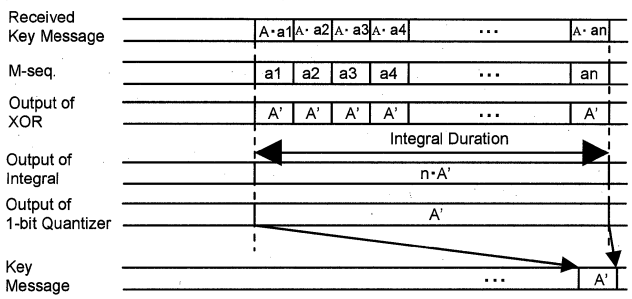


**Fig. 4** Timing chart of receiver-side.

Cyclic shift M-sequence which is the same as the sender-side's Orthogonal Cyclic shift M-sequence. The multiplied output (output of XOR) is integrated during one period of Orthogonal Cyclic shift M-sequence in Σ. And, at 1 bit quantizer, output of the integration is converted into +1 or −1 according to polarity of output of the integration, that is, if output of the integration is positive (+), +1, otherwise −1. In desampling process, transfer rate of output of 1 bit quantizer become the transfer rate of sender-side's the key message.

### 4.2 Analysis of Immunity against Noise

In this section, we discuss our proposal's immunity against noise. Immunity to noise depends on physical layer too. We analyze the immunity against noise based on the model as shown in Fig. 5 for simplicity. In Fig. 5, sender process is equal to sender-side process as shown in Fig. 1; receiver process is equal to receiver-side process as shown in Fig. 3. 1 bit quantizer converts output of multiplier to +1 or −1 according to polarity of output of multiplier. The output $S_i$ of

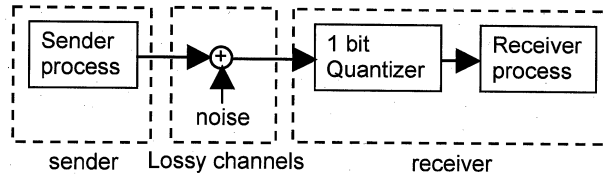


**Fig. 5** Key distribution model over lossy channels.

multiplier (XOR) in sender-side is expressed as follows,

$$S_i = A \times a_i \tag{1}$$

$A$ (= 1 or −1) is corresponding to 1 bit of output of resampling. $a_i$ (= 1 or −1, $i = 1-N$, $N$ is length of Orthogonal Cyclic shift M-sequence) is each bit of Orthogonal Cyclic shift M-sequence. In this case, received key message $R_i$ is expressed as follows,

$$R_i = S_i + N_i \tag{2}$$

$N_i$ is the noise which is added over lossy channels. $N_i$ is real number.

1 bit quantizer in Fig. 5 is non-linear process. For simplicity, at first, we consider the model without 1 bit quantizer. In the model without 1 bit quantizer, key message $A'$ in Fig. 4 is expressed in Eq. (3), by using Eqs. (1), (2).

In Eq. (3), the first term represents decoded output of desired signal. The second term represents the correlation between noise and Orthogonal Cyclic shift M-sequence.

$$\begin{aligned} A' &= \sum_{i=1}^{N} R_i \times a_i \\ &= \sum_{i=1}^{N} (S_i + N_i) \times a_i \\ &= \left(\sum_{i=1}^{N} S_i \times a_i\right) + \left(\sum_{i=1}^{N} N_i \times a_i\right) \\ &= A \times \left(\sum_{i=1}^{N} a_i \times a_i\right) + \left(\sum_{i=1}^{N} N_i \times a_i\right) \\ &= A \times N + \left(\sum_{i=1}^{N} N_i \times a_i\right) \end{aligned} \tag{3}$$

Assuming that bit error rate of lossy channels is $10^{-2}$ [6], signal-to-noise ratio (SNR) is about 4 dB, that is, SN = $10^{4/10} = 2.5$. Hence, the average amplitude of noise is about 0.4 (= 1/2.5). For simplicity, assuming that $a_i$ is all 1, the second term becomes 0.4 times of the first term. That is, effect of noise is enough low compared with desired signal. In practice, the correlation between noise and Orthogonal Cyclic shift M-sequence is very low. Hence, effect of noise is by far lower than the above calculated result, that is, it is considered that the second term of Eq. (3) practically is lower than 0.4 times of the first term.

Next, we discuss BER of key message in our proposal, based on the model of Fig. 5. We assume that length of Orthogonal Cyclic shift M-sequence is 128, BER ($pe$) of lossy

channels is 0.01 and the length of key message is 128. In such a case, when the number of bit error of Orthogonal Cyclic shift M-sequence is less than 64, 1 bit of key message is decoded correctly in receiver. Hence, BER $Be$ is expressed as follows,

$$\begin{aligned} Be &= 1 - \sum_{i=65}^{128} \left( {}_{128}\mathrm{C}_i \times (1-pe)^i \times pe^{128-i} \right) \\ &= 1.2 \times 10^{-15} \\ &< 1.0 \times 10^{-9} \end{aligned} \tag{4}$$

Hence, we find that our proposal's BER property satisfies Ethernet specification.

Furthermore, packet loss rate $Pl$ is expressed as follows,

$$\begin{aligned} Pl &= 1 - \left( \sum_{i=65}^{128} \left( {}_{128}\mathrm{C}_i \times (1-pe)^i \times pe^{128-i} \right) \right)^{128} \\ &= 1.6 \times 10^{-13} \end{aligned} \tag{5}$$

## 5. Comparison

In this section, we discuss comparison with related works, specifically, proposal [1] and proposal [3]. We discuss BER and packet loss rate of key message, as parameter of comparison. We assume that BER of lossy channels is 0.01 and the length of key message is 128. And key distribution model is based on the model as shown in Fig. 5.

In proposal [1], BER and packet loss rate of key message depend on coding gain of FEC. As described in Sect. 2, we assume that coding gain is 6 dB. A coding gain means attenuation of signal level achieving the same BER compared with the case without FEC, that is, apparently, it means that SNR of lossy channels is enhanced with 6 dB. When SNR of communication channels is $\gamma$, the BER of that channels is expressed as follows [4],

$$BER = 0.5 \times erfc(\sqrt{\gamma}) \tag{6}$$

In the above Eq. (6), erfc means error function and is expressed as follows,

$$erfc(x) = (2/\sqrt{\pi}) \times \int_x^{\infty} \exp(-t^2)\,\mathrm{dt} \tag{7}$$

From Eq. (6), when BER of lossy channels is 0.01, $\gamma$ is equal to 2.3. And, enhanced SNR $\gamma'$ is 9.2, it means that $\gamma$ is enhanced with 6 dB. Hence, from Eq. (6), in proposal [1], BER ($Be1$) of key message is expressed as follows,

$$\begin{aligned} Be1 &= 0.5 \times erfc(\sqrt{9.2}) \\ &= 2.1 \times 10^{-6} \end{aligned} \tag{8}$$

Hence, packet loss rate ($Pl1$) is expressed as follows,

$$\begin{aligned} Pl1 &= 1 - (1 - Be1)^{128} \\ &= 2.7 \times 10^{-4} \end{aligned} \tag{9}$$

In proposal [4], BER ($Be2$) of key message is equal to BER of lossy channels, because proposal [3] does not conduct the process per bit. Hence,

$$Be2 = pe = 0.01 \tag{10}$$

In proposal [3], we assume that one key message packet contains $M$ shares and key is recovered from $N$ shares. In secret sharing scheme, in order to assure the security of key, the length of each share requires the same length as original key. Hence, packet loss rate ($Pl2$) is expressed as follows,

$$\begin{aligned} Pl2 &= 1 - {}_M\mathrm{C}_N \times (1-pe)^{128 \times M \times N} \\ &> 9.9 \times 10^{-1} \qquad (\text{at } M = N = 2) \end{aligned} \tag{11}$$

As shown the above, packet loss rate of proposal [3] is very high. This reason is that one key message packet contains $M$ shares, the packet length become long and the bit error of the packet can not be tolerated.

As the result of the above discussion, we find that our proposal improves the reliability compared with related works. This main reason is that our proposal tolerates the high bit error of key message packet. Furthermore, in our proposal, the longer the Orthogonal Cyclic shift M-sequence becomes, the stronger the immunity against noise becomes. Then, the longer the Orthogonal Cyclic shift M-sequence becomes, the larger computational amount becomes linearly, while in the proposal [1], the larger the coding gain becomes, the larger the computational amount becomes exponentially. Hence, in our proposal it is easier to achieve the more reliable key distribution, compared with the proposal [1].

## 6. Analysis of Security

### 6.1 DoS (Denial-Of-Service) Attack

In the wireless communication systems or power line communication systems which are discussed in this paper, there is issue that the immunity against DoS attack is essentially weak. Because these systems are open networks and these communication media are shared by the third parties too. However, there are not enough discussions on the issue. Hence, in this section, we discuss on our proposal's immunity against DoS attack.

If the attacker does not know the Orthogonal Cyclic shift M-sequence, the proposal has the strong immunity against DoS attack. Because attacker's packets can not be accepted by the legitimate member because of the strong immunity against noise. However, attackers easily can get the Orthogonal Cyclic shift M-sequence, because the number of the Orthogonal Cyclic shift M-sequence is few. In the case that the length of the Orthogonal Cyclic shift M-sequence is $N$, the number of the Orthogonal Cyclic shift M-sequence is $N$. Hence, we should assume that attacker knows the Orthogonal Cyclic shift M-sequence which the legitimate member is using.

As other property of Orthogonal Cyclic shift M-sequence, there is precipitous auto-correlation property as shown in Fig. A· 1. By this property, the legitimate member can get the key update message which is received only in the accurate timing such as the bit-timing, and legitimate member can eliminate the messages which are received in other timing. That is, the legitimate member can filter only the key update message received only in the accurate timing. This timing depends on member's physical location; this is, practically, attacker can not get this timing. Hence, our proposal has strong immunity against DoS attack.

### 6.2 Replay Attack

In the wireless communication systems or power line communication systems, there is also issue that the immunity against replay attack is essentially weak. Because these communication media are shared by the third parties too. However, in replay attack, if the attacker does not do the accurate timing when the legitimate member receives the key update message, replay attack is not issue from the above reason.

## 7. Conclusion

This paper has proposed a new reliable key distribution scheme. This paper has shown that our proposal is more reliable key distribution scheme than the related works, and has shown that our proposal's reliability on key distribution is equivalent to the dedicated communication channel such as Ethernet. The main issue of our proposal is the communication overhead. However, this paper has shown that the communication overhead becomes lower in the application that the number of members is very large, e.g., pay-per-view TV, sensor network.

**References**

[1] X.B. Zhang, S.S. Lam, D.-Y. Lee, and Y.R. Yang, "Protocol design for scalable and reliable group rekeying," IEEE/ACM Trans. Netw., vol.11, no.6, pp.908–922, Dec. 2003.
[2] Development of Turbo code FEC LSI for 10 Gbs optical communication. http://www.mitsubishielectric.co.jp/newsdata/2005/pdf/1207.pdf
[3] J. Staddon, S. Miner, M. Franklin, D. Balfanz, M. Malkin, and D. Dean, "Self-healing key distribution with revocation," Proc. 2002 IEEE Symposium on Security and Privacy, pp.241–257, 2002.
[4] Y. Akaiwa, Digital Mobile Communications, Wiley-Interscience, 1997.
[5] IEEE Std 802.3-2002.
[6] T. Zwick, F. Demmerle, and W. Wiesbeck, "Simulation and measurement of bit error rates for a 2FSK-system in indoor environments," Vehicular Technology Conference, vol.1, no.18-21, pp.649–652, May 1998.

## Appendix

Orthogonal Cyclic shift M-sequence is the modification of M-sequence (Maximum-length sequence). M-sequence is the sequence that sequence's period is equal to $2^k - 1$ and is generated by the linear feedback shift-register of $k$ stages. M-sequence's auto-correlation property has the property shown by Fig. A· 1, that is, when M-sequence is $\{u_i\}$, $u_i = 1$ or $-1$, $i = 1, 2, \ldots, N$, and M-sequence's auto-correlation is $C_i$, $C_i$ is expressed as follows,

$$C_i = \sum_{j=1}^{N} u_{i+j} \times u_j \qquad \text{(A·1)}$$

$$= \begin{cases} N & \text{at } i = 0 \\ -1 & \text{at } i \neq 0 \end{cases}$$

The following Cyclic shift M-sequence $U_i$ is generated by cyclically shifting M-sequence $\{u_1, u_2, \ldots, u_N\}$ $i$ times.

$$U_i = \{u_{i+1}, u_{i+2}, \ldots, u_N, u_1, \ldots u_i\} \qquad \text{(A·2)}$$

The following Orthogonal Cyclic shift M-sequence $M_i$ is generated by joining +1 to Cyclic shift M-sequence $U_i$.

$$M_i = \{u_{i+1}, u_{i+2}, \ldots, u_N, u_1, \ldots u_i, +1\} \qquad \text{(A·3)}$$

The cross-correlation between $M_i$ and $M_j$ is $N$ at $i = j$, and 0 at $i \neq j$. That is, $M_i$ and $M_j$ is orthogonal at $i \neq j$.

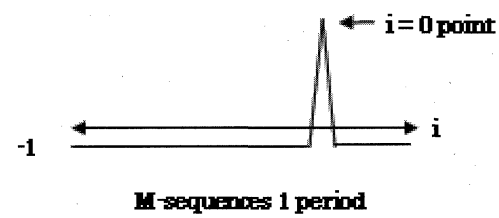


**Fig. A· 1** M-sequence's auto-correlation property.