A Method of Combining Scrambling Technology with Error Control Coding to Realize Both Confidentiality and Reliability in Wireless M2M Communication

Meng Zhang[1], Zhe Wang[1] , Menghan Guo[2]
[1] National ASIC Research Center, Southeast University
[2]Institute of RF- & OE-ICs, Southeast University
Nanjing, China
[E-mail: *zmeng@seu.edu.cn*, wangzhe0543@126.com, guomenghan@163.com]
*Corresponding author: Meng Zhang

Received September 1, 2011; revised November 18, 2011; revised January 9, 2012; accepted January 18, 2012; published January 31, 2012

Abstract

In this paper we present a novel method of applying image scrambling technology which belongs to the information hiding field in the error control coding to introduce confidentiality in wireless machine to machine communication. The interleaver in serial concatenated convolutional codes, which is the key module in overcoming burst errors, is deliberately designed with the scrambling function to provide a low error rate for those authorized transceivers. By contrast, the unauthorized transceivers without keys would get so high an error rate that decoding bits could bring little value, thus realizing both the confidentiality and reliability in wireless machine to machine communication.

Keywords: Confidentiality, SCCC, interleaver, scrambling

This research work of this paper was supported by the Natural Science Foundation of Jiangsu under Grant No.BK2010167 and the National Natural Science Foundation of China under No.61006029 and No. 61001104, and by the National Mega Project of Science Research, China, under Grant No.2010ZX03006-003-02.
DOI: 10.3837/tiis.2012.01.010

1. Introduction

Widely used in industry control, safety monitoring, retail, public services management, vehicle anti-theft, auto sales, mechanical maintenance, health and other industries, machine to machine(M2M) communication is seen as a form of data communications between entities that do not necessarily need any form of human intervention [1][2]. As a proper example, wireless multimedia transmission has created an inevitable trend to break boundaries of time and space for mobile TV. In [3], an OpenCore-based mobile TV framework for DVB-H/T wireless network was presented, realizing the playback functions of TV programs in hand-held device. In the recent few years great attention has been devoted to the improving the performance of multi-hop wireless networks, such as minimizing the video distortion and achieving certain fairness among multiple video streams [4]. The M2M communications are facing many existing challenges: energy efficiency, reliability, and especially confidentiality. An attacker could obtain confidential information of the key for M2M user or control data though eavesdropping user data, signaling data and control data on the wireless link or the signal exposes in public places, so can illegally access to the data on M2M device [2]. For a long time, the confidentiality issue has been processed through encryption of data, and the reliability issue was partially worked out by error control coding (ECC). Nowadays both of these two fields have gained considerable development. For instance, many sparse graph codes have been proven to be able to provide close to limits' performance in many different channels.

For a classic communication system, the procedure of encryption usually located between the source encoding and the ECC. **Fig. 1** illustrates a model of cryptographic channel. The data to be transmitted is noted as plaintext. The transmitter noted as encipher would produce the encrypted text C using the key K: $C = E_K(M)$. After the transmission process on the public channel, in the receivers' side(noted as the decipher) the same K obtained from the secure channel would be taken to recur the text: $M = D_K(C) = E_K^{-1}(C)$.

As is described, based on the key K, the sender encrypts messages noted by M to generate the ciphertext C which is transmitted over insecure channel, and the authorized receiver decrypts it using the same key that has helped in the encryption [5], and reobtain the transmitted plaintext M. The public channel is an opening environment that everyone can obtain the transmitted information from it, thus eavesdropping from the unauthorized receiver is unavoidable. Even encryption could not prevent the ciphertext from been reached by those attackers noted as cryptanalyst.

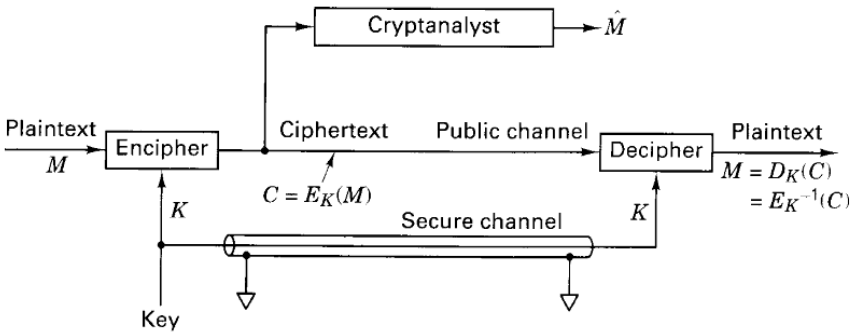


Fig. 1. The model of cryptographic channel [5]

In common communication systems confidentiality are ensured exclusively by encryption of the messages. Current Machine to Machine communication technology has not introduced new schemes in the physical layer to face this issue. Modern encryption algorithm such as AES are all based on the assumption that the public communication channel are prone to interception which means that messages could be captured by anyone. In this paper, we proposed a method that utilized information hiding technology in the error control coding to realize a different goal that prevent messages transmitted on the public channel being intercepted correctly let alone understood. For the unauthorized receivers, the lack of right keys would affirmatively lead to great errors in messages in the decoding process and gained meaningless results. As far as we know all secure wireless communication systems today adopt the strategy that messages would surely be received by both authorized and unauthorized receivers while difficulty shall occur for those unauthorized ones. Our method has a clear difference with traditional encryption methods in that it ensures that the message in the public channel wouldn't be obtained correctly for those eavesdroppers. We believe this method adds additional confidentiality to the public channel, i.e., it's a novel method to protect the messages transmitted on the public channel.

On the other hand, our method has also clear differences with information hiding technology from which we've got many ideas. Information hiding techniques have recently become important in a number of application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copyright notice or serial number or even help to prevent unauthorized copying directly [11]. Information hiding is also based on the assumption that messages would be properly received by anyone. The advantage of information hiding is that it hinders unauthorized receivers' interpreting the messages. By contrast, our method made use of error control coding to avoid messages' being correctly received by them.

Existing methods in M2M communication follows traditional encryption and protection methods wildly applied in Mobile communication and the Internet communication. Compared to traditional encryption methods, our method shares the same quantity of hardware resources. A Hash function chip rather than one encryption chip is adopted in the wireless communication system. The difference lies in that whether the transmitted data are prone to be obtained by anyone.

2. Design of error control code

The history of error correcting coding (ECC) started with the introduction of the Hamming codes , at or about the same time as the seminal work of Shannon (1948) [6]. For decades, ECC has been used to facilitate communication in the presence of interference. For most communication systems (power restricted systems such as ZigBee and some others are exception), the block diagram would like that in **Fig. 2**. After the Encoder, the original information(noted as Information Source) u are transformed into code v. The modulation process put the coded bits on the wireless radio wave and produce x. The decoder could get corresponding bits y from the demodulation of y which has been interfered by the noise, and the original information u could again reproduced.

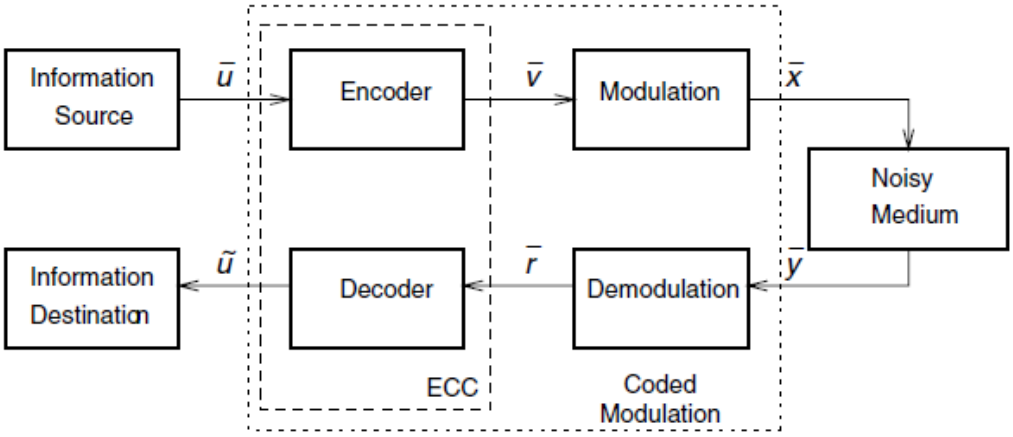


Fig. 2. Block diagram of a communication system [6]

Since the Hamming codes, many error control codes have been put forward, of which the class os sparse graph codes including Turbo codes [7] and LDPC codes are most powerful. For example, the best rate-1/2 binary code, with a block length of 10,000,000, is an LDPC code that achieved a record 0.0045 dB away from the Shannon limit for binary transmission over an AWGN channel [8]. In modern technology they have wide range of application from Mobile Communication to gigabit ethernet systems (10Gbase-T)[6].

In Machine to Machine communication, error control coding could bring benefits to those applications in severe environments such as noise power plant and underground mines. In those situations wireless signals which are prone to strong disturbance would become so weak that intercepting the information carried by them may become impossible. For example, BPSK modulated signal would have a 2.28% bit error rate in AWGN channel with the Signal to Noise rate(SNR) 3.0dB. This high error rate is unacceptable for sensitive users including dangerous chemical composition monitoring and financial information inquiry service. After Turbo coding and 3 iterations in decoding, however, the bit error rate would be reduced within 10^{-5} [7], the result could be further improved by more iterations.

Serial concatenated codes(SCCC) resemble Turbo codes in many aspects. SCCC were given by S. Benedetto etc.. Their encoder have an interleaver and two component encoders, which are usually recursive system convolutional encoders like those in Turbo codes. Contrary to turbo codes, serially concatenated codes do not exhibit “interleaver gain saturation” (i.e., there is no error floor) [6]. SCCC's encoder diagram is shown in **Fig.3**. In this **Fig.3**, v1 is the outcome of the first encoder, and after the process of interleaving Π, the second encoder generates the final code v2.

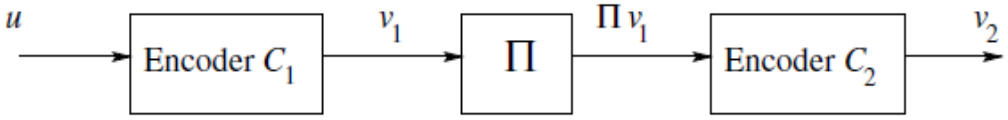


Fig. 3. The encoder of a serially concatenated code [6]

In this paper the SCCC was chosen based on a fact that besides its acceptable performance, SCCC differed with other codes in that original information bits(those bits in u shown above) would mainly disappear after coding. Codes such as Turbo code are mostly in systematic

format, i.e. the redundancy bits are transmitted before or after the information bits. To realize the goal of preventing unauthorized ones from correctly receiving the messages we choose SCCC with two recursive systematic convolutional component encoders. After encoding most original information bits have been buried in the coded bits and would not appear on the public channel.

In Turbo-like codes, interleaver is a critical component that determines the structural properties of the overall code, including the distance spectrum and the minimum distance [5].The interleaver can build very long codes with weight distributions that approach those of random codes, and meanwhile it help to resist the burst errors in channels. Put it simple, the interleaver does the work of throwing the input data into disorder. There are many interleavers, such as Ramsey interleaver and random interleaver. **Fig.4** is a schematic diagram of random interleavers. It shall be stressed that none of those interleavers mentioned above has any key-controlled scheme in design.

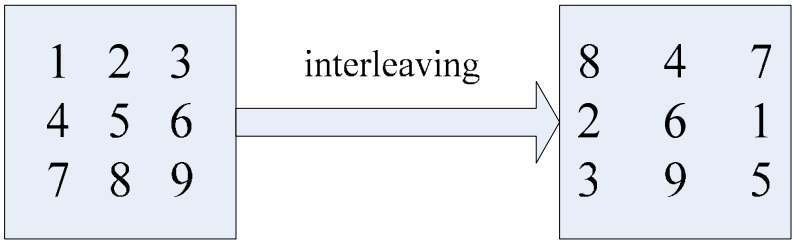
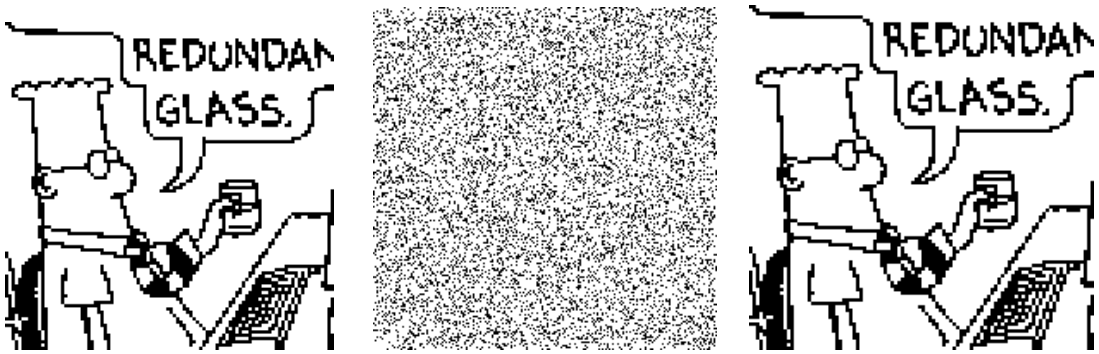


Fig. 4. Schematic diagram of interleavers

On the other hand, however, if wrong interleaver matrix were taken in the receiver's side, errors would occur. The proof can be found in the appendix.

Our purposed method was mainly based on the idea above. Designing inter- leavers using the technology from information hiding and image scrambling. In information hiding, image scrambling is an important way for image encryption. Image scrambling is to change the positional relations between image pixels and reduce the relativity of images [12]. **Fig.5** presents a vivid show of image scrambling in communication. **Fig.5-(b)** shows the scrambled image while **Fig.5-(c)** is the recovered image. It can be clearly noticed that the original information has been disturbed.



(a) **(b)** **(c)**

Fig. 5. Image scrambling in communication

As is shown above, image scrambling is such a technology that throwing the input data(for this it is elements in the picture) into disorder, i.e, the similar function with interleavers. This similarity reminded us that image scrambling methods can also be applied in the design of interleavers. More importantly, this key-controlled scrambling not only produces a vector π(i) for interleaving but also introduce a confidentiality scheme in error control coding. Just like that unauthorized receiver will see the scrambled picture as meaningless noise, some one without the right key would definitely obtain a incorrect interleaver operation that leads to decoding failure.

As emerging technology information hiding methods including image scrambling have gained deep research. Researchers have proposed many image scrambling algorithms, for instance, Arnold transformation, Baker transformation and magic cube transformation. Recently modern encryption such as AES has been considered in this field [12] .In our design in the next section, we have avoided those complex algorithm and acquired simple MD5 algorithm instead. MD5 and other Hash functions are not absolute safe, while in real practice more advanced method including AES could been applied.

3. Algorithm of designing interleavers of SCCC using MD5

MD5 function generates a unique output number for each input value or matrix. Let key1 to key3 be the keys used in generating MD5 outputs. Suppose the interleaver vector π has as much elements as $N=L^2$, for inputs x(i) , i=1,2...N, the algorithm blew generate the outputs π(i). This algorithm was once used in image scrambling[13], and here we take advantage of it to design the interleaver.

The rough flow goes like this. First arrange the input elements of the interleaver into the form of matrix. [index1, index2] are the coordinates. For the input x(i),i=1,2,...N, index1 and index2 would be [i/L] and (i mod L) respectively, where L is the number of elements in one row or column in the interleaver matrix, and [i/L] means the nearest integer less than i/L. Because Hash functions return a unique value for each input number, after the process in the middle box of **Fig.6**, the input x(i) obtains a new unique index which appears to be random. The method was used in image scrambling [13].

==========

% arrange the input elements of the interleaver into the form of matrix

for each input data bit with the index i:

Row = [i/L];
Column = i mod L;

% counting the new index in the matrix for the input data

Row_temp = (Row + MD5(Column + key1)) mod L;
Column_temp = (Column + MD5(Row_temp + key2)) mod L;
Row_temp = (Row_temp + MD5(Column_temp + key3)) mod L;

% counting the new index

Row_new = Row_temp;

```
Column_new = Column_temp;
i_new = Row_new * L + Column;

end of loop

==========================================================================
```

Fig. 6. Algorithm description of generating disturbed index

Take a 8*8 matrix as an example. All elements indexed form 1 to 64 are arranged in the ascending order shown in **Fig.7-(a)**. After processing becomes that in **Fig.7-(b)**.

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

49	4	61	33	35	48	28	13
62	12	58	41	7	5	36	21
63	25	64	44	15	3	47	16
43	31	8	57	20	11	52	37
51	39	19	34	2	54	45	6
56	18	24	14	10	27	9	42
38	55	1	22	29	60	17	50
46	32	53	59	26	40	30	23

Fig. 7 Disturbing results of a 8*8 matrix

In our simulation, the SCCC encoder is composed of 2 recursive system convolutional encoders both of whom the generator are [1 1 1; 1 0 1]. This choice is simple while practical. For the outer encoder, the code rate is 1/2, and after inner coding the rate becomes 1/4. During one simulation a frame containing 800 information bits is encoded into 3200 bits and interfered by the AWGN. For the reason that outer codes per frame have 800/0.5=1600 bits, the interleaver parameter N equals to 1600 and L is 40. After the interleaver the outer codes have been rearranged. In the receiver's side a reverse process shall be fulfilled before outer decoding. As shown above, 3 keys take part in generating the interleaver matrix. For the authorized receivers they shall use these keys to obtain the same matrix.

Decoding SCCC is similar to decoding Turbo codes. Mostly, the decoding process goes like that in **Fig. 8** [6]. The soft input-soft output decodes noted as SISO1 and SISO2 would process the received message r iteratively. The final decision $\hat{u}$ is given after several iterations.

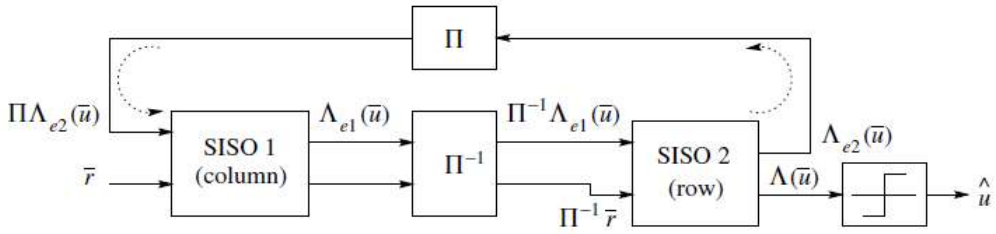


Fig. 8. Block diagram of a commonly used iterative decoder for SCCC

This iteration scheme has been adopted in most ECC systems. Berrou has shown that as the number of iterations grows, the error performance was improved [7]. In our experiment iteration has been omitted in that our main purpose is to introduce confidentiality scheme into ECC rather than showing the excellent performance of SCCC. The performance could be further increased by more iteration in real practice.

4. Simulation and results

Our simulation had two component parts. The first part was to explore the bit error rate performance in AWGN channel and Nakagami-m channel. Firstly, 1000 frames of random data were generated and encoded. After encoding the code words were sent through AWGN channel. Considering that outdoor device especially sensor nodes in wireless sensor network could only transmit signal at low power, and environment contains much background noise and interference, thus the strength of the received signal wouldn't be large. We set the Signal to Noise Ratio(SNR) ranging from 1 dB to 4 dB. In the receiver's side two groups of bit error rates was calculated in which one had the right keys for deinterleaving while the other didn't. As talked above no iteration has been carried out. This experiment was designed to determine how worse it can be without deinterleaving correctly. The result was shown in **Fig.9**.

The results showed that the unauthorized receiver who did not own the right keys obtained an average bit error rate 50.26% which was almost the worst case for communication(For communication systems, the worst bit error rate is 50%). For this receiver, nearly no valued information was obtained from these received bits. By contrast, the authorized receiver got the bit error rates 14.01%, 7.38%, 0.90% and 0.04% respectively with the SNR ranged from 1dB to 4 dB. The experiment demonstrated that SCCC with interleavers indeed provide safety for data. Meanwhile, for the authorized receiver, the error rates could be low enough for applications.

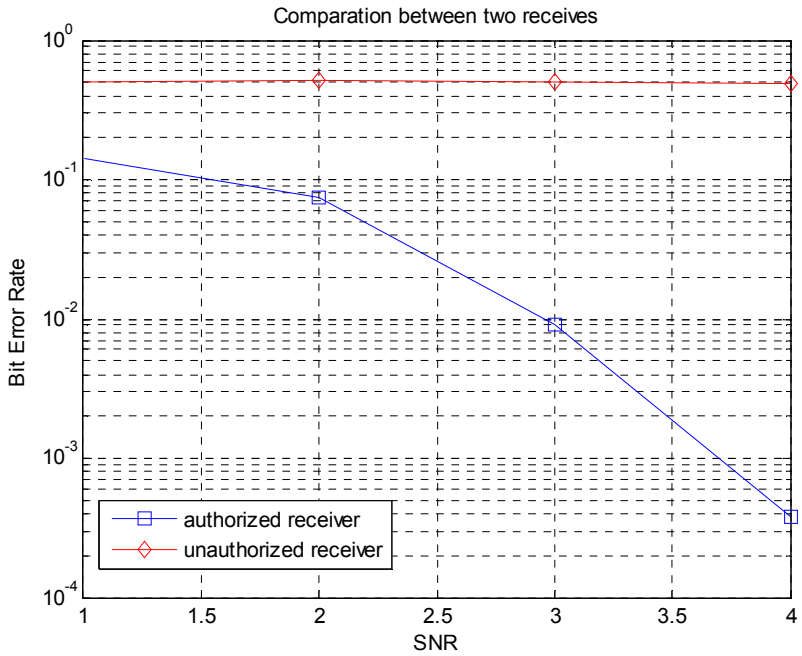


Fig. 9. Results of bit error rates

Another group of experiment was carried out to test whether our method could perform well in real communication system and environment. An OFDM system containing 64 sub- carriers in which 50 subcarriers carried the BPSK modulated signal were simulated under the Nakagami-m channel with the parameter m equaled to 0.5, 1.0 and 5.0 respectively. When m equals to 1.0, the Nakagami channel would become the |Rayleigh fading channel which is the mostly used channel model in modern communication research field. The parameters of the OFDM system are listed as follow in **Table 1**.

Table 1. Parameter setting of the OFDM system

Parameter	**Value**
FFT size	64
Number of subcarriers carrying data	50
Used subcarrier index	{-25 to -1, +1 to +25}
Cyclic prefix	16 subcarriers
Total Symbol	80 subcarriers
Number of Taps	10

The results of this group of simulation are in **Fig.10**. For the reason that all un- authorized receivers under different parameter m got nearly the same bits error rate, i.e., about 50%, those 3 curves were almost overlapped. The average bits error rates in those 3 circumstances were 49.95%, 49.97% and 49.97% respectively. The BER results of the authorized receivers are listed below.

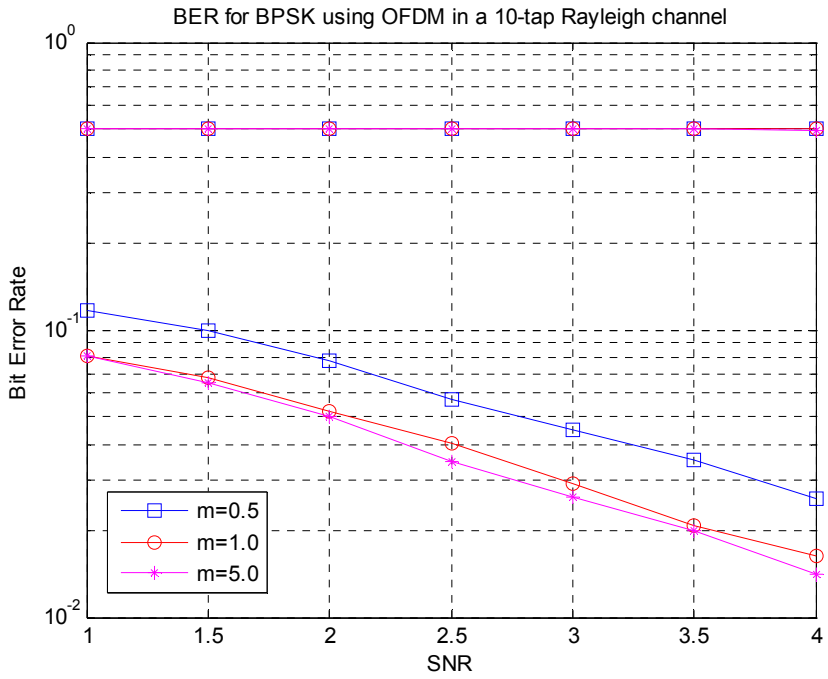
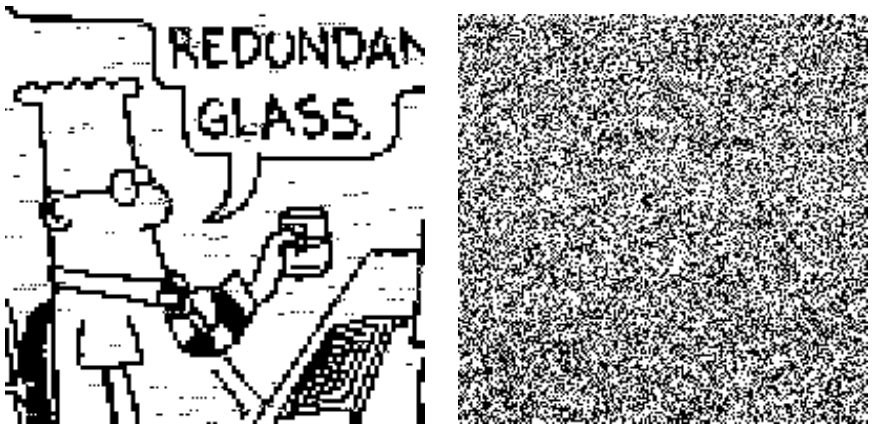


Fig.10. Results of bit error rates in Nakagami-m channel

It can be clearly seen that the error control performance decreased in the Nakagami channel compared to the AWGN channel. While for the unauthorized receivers the error rates remained values and leaded to transmission failure. The results demon- strated that our method had similar performance in different systems and could bring safety to the data transmitted.

The next part of experiment was to sent the picture in **Fig.5-(a)** to show what results would be in two situations. The original picture was in [6] and here we did some modification. The format of the picture was Bitmap(.bmp), and it had only 2 colors , i.e., black and white. In Matlab simulation it was stored in a 200*200 matrix composed of 1 and 0. For the reason that every frame took only 800 information bits, it was sent in 50 frames respectively. After receiving those 50 frames were decoded and the picture was recovered. The results are shown in **Fig.11**.



(a) **(b)**

Fig. 11 Two recovered pictures. **(a)** is the situation with the right keys while **(b)** is on the contrary

It can be clearly seen that **Fig.11-(a)** can be acceptable though there occurred some errors. On the other hand **Fig.11-(b)** had lost the original information and may have no value for receivers.

For wireless machine to machine communications, every single machine transceiver could hold three unique IDs and use them as keys. In this case our method provides an extra function of identification. In the sender's side a negotiated header message could be encoded using the target's IDs and sent and any receiver within the transceiver range would receive and decode it. If the head message were not decoded correctly, a receiver would get to realize that the message is for some others and go to sleep mode. The real target then confirms its task and prepares the following work. In this way, large wireless networks could perform the process of communication in a both secure and efficient way.

5. Conclusion

In this paper we combined the method of error control coding and image scrambling to provide both error resistant performance and safety for information transmitting on the channel. We adopted the Hash disturbing algorithm to design the interleaves of SCCC to realize this goal. The experiment result has proven the feasibility of this method.

In the future, more work could be done. Considering the Hash function's potential to be broken, more advanced technology could be adopted. Besides, whether this confidentiality scheme is strong enough to resist attack is still an open problem. In real practice, the design of hardware with moderate complexity is also an issue.

References

[1] Hu, R.Q., Yi Qian, Hsiao-Hwa Chen and Jamalipour, A., “Recent progress in machine-to- machine communications," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 24-26, Apr. 2011. Article (CrossRef Link)

[2] Du Jiang and Chao ShiWei, "A study of information security for M2M of IOT," in *Proc. of 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE),* vol. 3, pp. 576-579, pp. 20-22 Aug. 2010. Article (CrossRef Link)

[3] Chin-Feng Lai, Yueh-Min Huang, Jiann-Liang Chen, Wen Ji and Min Chen, “Design and integration of the OpenCore based mobile TV framework for DVB-H/ T wireless network,*” Jounal of ACM Multimedia Systems*, 2010. Article (CrossRef Link)

[4] L. Zhou, X. Wang, W. Tu, G. Muntean and B. Geller, "Distributed scheduling scheme for video streaming over multi-channel multi-radio multi-hop wireless networks,” *IEEE Journal on Selected Areas in Communications,* vol 28, no. 3, pp. 409-419, 2010. Article (CrossRef Link)

[5] B.Sklar, “Digital communications: Fundamentals and applications,” pp. 890-893. 2001. Article (CrossRef Link)

[6] Robert H. Morelos-Zaragoza, “The art of error correcting coding,” pp. 2-185, 2006. Article (CrossRef Link)

[7] C. Berrou, A. Glavieux and P. Thitimajshima, "Near shannon limit error-correcting coding and decoding: Turbo-codes," *in Proc. of IEEE International Conference on Communications(ICC'93),* pp. 1064–1070, May. 1993. Article (CrossRef Link)

[8] S.-Y. Chung, G. D. Forney, Jr., T. J. Richardson and R. Urbanke, “On the design of low-density

parity-check codes within 0.0045 dB of the Shannon Limit," *IEEE Communication Letter*, vol. 5, no. 2, pp. 58–60, Feb. 2001. Article (CrossRef Link)
[9] A. Huebner and R. Jordan, "On higher order permutors for serially concatenated convolutional codes," *IEEE Transactions on Information Theory*, pp. 1238-1248, 2006. Article (CrossRef Link)
[10] D.J.C. MacKay, "Information theory, inference, and learning algorithms," *Cambridge University Press*, pp. 8-12, 2003. Article (CrossRef Link)
[11] Fabien A. P. Petitcolas, Ross J. Anderson, and Markus G. Kuhn, "Information hiding :A survey," *Proeeding of the IEEE*, vol. 87, no. 7, pp. 1062-1078, Jul. 1999. Article (CrossRef Link)
[12] N. Jiping, Z. Yongchuan, H. Zhihua, and Y. Zuqiao, "A digital image scrambling method based on AES and error-correcting code," in *Proc. of CSSE* , vol.3, pp. 677-680, 2008. Article (CrossRef Link)
[13] Lixin, D., "A new approach of data hiding within speech based on hash and Hilbert transform," in *Proc. of ICSNC,* 2006. Article (CrossRef Link)
[14] S. Benedetto, D. Divsalar, G. Montorsi, and F. Pollara, "Serial concatenation of interleaved codes: Performance analysis, design, and iterative decoding," *Transactions on Information Theory,* pp. 909-926, 1998. Article (CrossRef Link)
[15] Mohamed El-Hadedy, Danilo Gligoroski , Svein J. Knapskog and Einar Johan Aas, "Low area FPGA and ASIC implementations of the hash function "Blue Midnight Wish-256,"," in *Proc. of International Conference on Computer Engineering & Systems*, pp. 10-14, 2009. Article (CrossRef Link)

Appendix

Here we give out the proofs of the idea about introducing wrong interleaver matrix given in the Section 2(Design of error control code).

Let x containing N elements stand for the initial information before the interleaving process.

The input symbol x_i to the permutation at time index i($i \in \{0,1,...N-1\}$) is written to the output symbol $y_{\pi(i)}$ at time index π(i):

$$y_{\pi(i)} = x_i \tag{1}$$

Huebner etc. adopted the square binary matrix $S=(s_{i,j}), i,j \in \{0,1,...N-1\}$ of size N*N that has exactly one "1" in each row and each column to describe the interleaver[9].

The nonzero entries of this matrix are given by

$$S_{i\pi(i)} = 1 \tag{2}$$

Take a 4*4 matrix as an example, i.e., N equals to 4.

The input sequence x=[x0,x1,x2,x3], and the matrix S is as follows:

$$S = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Then the output of the interleaver y would be:

$$
\begin{aligned}
y &= xS \\
&= [x_0, x_1, x_2, x_3]\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \\
&= [x_2, x_0, x_3, x_1]
\end{aligned}
$$

For the input sequence x with a length of N to a permutor, the output sequence y is given by

$$\mathrm{y} = \mathrm{xS} \tag{3}$$

On the receiver's side, a inverse permutation is performed with the inverse permutation matrix $\mathrm{S}^{-1} = (\mathrm{s}_{\mathrm{i,j}}^{-1}), \mathrm{i}, \mathrm{j} \in \{0,1,...\mathrm{N}-1\}$,

where the permutation matrix and the inverse permutation matrix satisfy

$$SS^{-1} = SS^{T} = I_N \tag{4}$$

Here $\mathrm{I_N}$ denotes the identity matrix of size N*N.

Thus the output sequence of the inverse permutor is

$$z = yS^{-1} \Rightarrow z = xSS^{-1} = xI_N = x \tag{5}$$

The effects of interleaver in SCCC has been given in [9].
The minimum distance of the SCCC is bounded by

$$d_{\min} \geq \frac{1}{2}(d_{free}^{o} + 1)d_{free}^{o}d_{free}^{i} \tag{6}$$

Where d_{free}^{o} and d_{free}^{i} denote the free distance of the outer and inner code respectively.

With sufficiently large separations of order ρ, the minimum distance grows like:

$$d_{\min} \sim (d_{free}^{o})^{\left\lfloor \frac{\rho}{2} \right\rfloor + 1} d_{free}^{i} \tag{7}$$

Where $d_{free}^{o} > 3$ [9].

As can be clearly shown, interleavers can increase the minimum distan- ces of codes thus providing greater error resistance performance.

Suppose in the sender's side the matrix S was taken, producing the disturbed message **y=xS**. In the receiver's side, a wrong matrix S_1^{-1} rather than S-1 was adopted to restore the original message.

Then the result would like this: $y_1 = xSS_1^{-1}$. Because S_1^{-1} was not the inverse matrix of S, the product of SS_1^{-1} would not be I_N. So carrying out the mode 2 addition, it would be:

$$\begin{aligned} y_1 &= xSS_1^{-1} = xSS_1^{-1} + x + x \\ &= x(SS_1^{-1} + I_N) + x \\ &= e + x \end{aligned} \tag{8}$$

where $e = x(SS_1^{-1} + I_L)$ is the extra error introduced by the process.

This shows that if the deinterlacing process were not carried out correctly, errors would occur.

Meng Zhang was born in Shandong, China, in 1964. He received the M.S. degree in bioelectronics engineering from Southeast University, Nanjing, China, in 1993. He is currently a Professor in National ASIC System Engineering Technology Research Center, Southeast University, Nanjing, China. His research interests include information security and assurance, and mobile security, cryptography, digital signal processing, digital communication and IC design. He is the author or coauthor of more than 20 papers and the holder of more than 10 patents.

Zhe Wang is currently a postgraduate student in National ASIC System Engineering Technology Research Center, Southeast University, Nanjing, China. Before that he received his B.S. degree in electronic science and technology from Shandong Normal University in 2010. His research interests include error control coding, digital communication and IC design.

Menghan Guo is currently a postgraduate student in Institute of RF- & OE-ICs, Southeast University, Nanjing, China. He is also a participator in developing the ground systems for the Alpha Magnetic Spectrometer in China. He received his B.S. degree in electronic science and technology from Shandong Normal University in 2010. His research interests include high speed IC design and Analog to Digital Converter design.