Blind frame synchronization technique of sparse parity check matrix codes on secure communications

Zhou Jing, Huang Zhiping, Su Shaojing, Zhang Yimeng

***Abstract*—It's present in this paper an extended application of blind frame synchronization technique on secure communication systems which use sparse parity check matrix codes as forward error-correcting (FEC) coding to control the errors during transmissions. We address this problem on the secure communication context that a transmitter sends a sequence of encoded packets but without synchronization words, the legal receiver detects the beginning of each packet blindly from the noisy channel by employing the relationship between the codes and their parity check matrices. Without synchronization words and FEC parameters, illegal receivers are difficult to analyze the existence of transmitted packets and synchronize to the frames. We also insert some random symbols between packets to increase the concealment of transmitted information and simulation results show that the proposed approach performs well.**

***Index Terms*—blind frame synchronization, channel coding, information hiding, secure communications.**

I. INTRODUCTION

In the secure communications systems, legal users hope to conceal the transmitted information to avoid wiretapping. The developing of cryptology on communications increases the difficulty of understanding the information for an eavesdropper [1-4]. However, the cryptanalysis is always bringing challenges to secure communications [5-6]. But it's clear that the eavesdropper must synchronize to the transmitter before analysing the encrypted information. If the packets is hidden into a random noise sequence and the frame synchronization word is removed, it is difficult for the eavesdropper to discover the existence of his interested information and difficult to synchronize to the transmitter. Without synchronization words, the legal receiver must synchronize the transmitted packets blindly. Usually, if an encrypted packet contains errors, the receiver cannot decrypt it correctly. So the channel coding technique should be applied after encrypting [7-8] as shown in figure 1. This makes the packets contain some constraints that are only known by legal users. To achieve synchronization, those constraints could be employed.

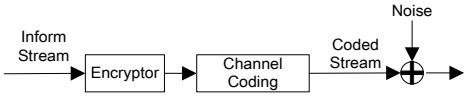

Fig. 1 Transmitters of secure communication systems

Inspired by the iterative decoding idea of low density parity check (LDPC) codes [9-11], The authors of [12-13] proposed the method of blind frame synchronization for packet communication systems. In [14], the authors proposed to correct some missed details in [12-13] and proposed the general approach of blind frame synchronizations for error-correcting codes having a sparse parity check matrix which gave promising results. And the corresponding theoretical analyse of the algorithm in [14] is shown in [15]. Furthermore, the algorithm idea is extended to Bose-Chaudhuri-Hocquenghem (BCH) product codes [16] and Reed-Solomon (RS) codes [17].

In our work, we find that there is a mistake exists in the expression of the Log-Likelihood-Ratios (LLR) of syndrome elements introduced in [14] and referenced in other corresponding literatures [15-17]. In this paper, we present a designation of information hiding technique by applying the blind synchronization algorithm of LDPC and convolutional coded systems to increase the information transmission safety and correct the mistake in the blind synchronization technique introduced in [14].

The rest of this paper is organized as follow. In section 2 we introduce the algorithm of blind frame synchronization of error correcting codes having a sparse parity check matrix proposed by [14], correct the mistake in the algorithm and prove it. Section 3 proposes the application of the blind frame synchronization technique on information hiding. Finally, the simulation results and conclusions are shown in section 4 and section 5.

II. BLIND FRAME SYNCHRONIZATION OF ERROR CORRECTING CODES HAVING A SPARSE PARITY CHECK MATRIX

In [14-15], the authors proposed a MAP algorithm to blindly synchronize the error-correcting codes having a sparse parity check matrix. They consider that when the synchronization position is not correct, a packet could contain arbitrary samples that do not form valid code words and therefore, some syndrome elements are not equal to zero. Inspired by this fact, the major principle is estimating the synchronization position t by minimizing the LLR of the syndrome:

$$\hat{t}_0 = \arg\min_{t=0,\cdots,n_c-1}\{\psi(t)\} \quad (1)$$

Where n_c is the length of each packet and $\psi(t)$ is the LLR of

Manuscript received Feb. 03, 2014.

Zhou Jing, College of Mechatronic Engineering and Automation, National University of Defense Technology, Changsha, China, +86-731-84576387.

Huang Zhiping, College of Mechatronic Engineering and Automation, National University of Defense Technology, Changsha, China, +86-731-84576387.

Su Shaojing, College of Mechatronic Engineering and Automation, National University of Defense Technology, Changsha, China, +86-731-84576387.

Zhang Yimeng, College of Mechatronic Engineering and Automation, National University of Defense Technology, Changsha, China, +86-731-84576387.

syndromes calculated at position *t*:

$$\psi(t)=\log\left(\frac{P_r\left\{\left[S_t(1),\cdots,S_t(n_r)\right]\neq 0\right\}}{P_r\left\{\left[S_t(1),\cdots,S_t(n_r)\right]=0\right\}}\right) \quad (2)$$

The syndromes are calculated as follow:

$$S_t=[S_t(1),\cdots,S_t(n_r)]=H\times C_t \quad (3)$$

Where H is the parity check matrix of the codes and C_t denotes a code word received from t with the supposing that t is the synchronization position.

For the error-correcting codes having a sparse parity check matrix, syndrome elements can be assumed independent and therefore:

$$P_r\left\{\left[S_t(1),\cdots,S_t(n_r)\right]=0\right\}\approx\prod_{k=1}^{n_r}P_r\left[S_t(k)=0\right] \quad (4)$$

Let $L((S_t(k))=\log\frac{P_r[S_t(k)=1]}{P_r[S_t(k)=0]}$ be the LLR of the k^{th} syndrome element. According to [14],

$$P_r[S_t(k)=0]=\frac{1}{1+\exp(L(S_t(k)))} \quad (5)$$

And having $\prod_{k=1}^{n_r}(1+\exp(L(S_t(k))))$ much larger than 1, the LLR of the syndromes can be written as:

$$\psi(t)=\sum_{k=1}^{n_r}\log(1+\exp(L(S_t(k)))) \quad (6)$$

In [14], the authors proposed to calculate the $L(S_t(k)$ in Eq. 6 as follow:

$$L(S_t(k))=(-1)^{u_k+1}\operatorname{atanh}\left(\prod_{j=1}^{u_k}\tanh\left(\frac{\tilde{r}(t+k_j)}{2}\right)\right) \quad (7)$$

And an approximation expression of Eq. 7 is as follow:

$$L(S_t(k))=(-1)^{u_k+1}\left(\prod_{j=1}^{u_k}sign(\tilde{r}(t+k_j))\right)\min_{j=1,\ldots,u_k}\left|\tilde{r}(t+k_j)\right| \quad (8)$$

Where $\tilde{r}(i)=\frac{2}{\sigma^2}r(i)$ is the LLR of the i^{th} received sample in the time window starts from t and σ^2 is the variance of the noise. u_k and k_j represent the number of ones in the k^{th} row of the parity check matrix of the code and the position of the j^{th} non zero element in the k^{th} row, respectively.

We propose in this paper that the equals Eq. 7 and Eq. 8 introduced in [14] has a small but serious mistake. The coefficient $(-1)^{u_k+1}$ in Eq. 7 and Eq. 8 is redundant and the correct expression of $L(S_t(k)$ should be:

$$L(S_t(k)=-2\operatorname{atanh}\left(\prod_{j=1}^{u_k}\tanh\left(\frac{\tilde{r}(t+k_j)}{2}\right)\right) \quad (9)$$

The proof is as follow.

Being similar to [14], we assume that the transmitter is sending a binary sequence of codewords and using a Binary Phase Shift Keying (BPSK) modulation i.e. let +1 and -1 be the modulated symbols of 0 and 1. The modulation operation from code bit c to modulated symbol s could be written as follow:

$$s=1-2c \quad (10)$$

And we assume that the propagation channel is a Binary Symmetry Channel (BSC) and corrupted by an Additive White Gaussian Noise (AWGN) with the variance $\sigma_n^2=N_0/2$.

The soft decisions of the received sequence could be expressed as follow:

$$r_i=s_i+w_i \quad (11)$$

According to the previous assumption, s_i follows a binomial distribution and the probabilities of s_i being +1 and -1 are both 1/2:

$$P_r(s_i=+1)=P_r(s_i=-1)=1/2 \quad (12)$$

$$f(x)=\frac{1}{\sqrt{2\pi}\sigma}\exp\left(-\frac{r^2}{2\sigma^2}\right) \quad (13)$$

So the conditional PDF of r is

$$f(r\mid s)=\frac{1}{\sqrt{2\pi}\sigma}\exp\left(-\frac{(r-s)^2}{2\sigma^2}\right) \quad (14)$$

where $\sigma^2=\frac{1}{2(E_s/N_0)}$ is the variance of the noise. For a given received bit r, we can obtain the following conditional probabilities:

$$P_r(s=+1\mid r)=\frac{f(r\mid s=+1)\times P_r(s=+1)}{f(r\mid s=+1)\times P_r(s=+1)+f(r\mid s=-1)\times P_r(s=-1)}=\frac{\exp(2r/\sigma^2)}{1+\exp(2r/\sigma^2)} \quad (15)$$

$$P_r(s=-1\mid r)=1-P_r(s=+1\mid r)=\frac{1}{1+\exp(2r/\sigma^2)} \quad (16)$$

Let $\boldsymbol{r}=\{r_1, r_2, \ldots, r_n\}$ be a received soft decision vector corresponding to the random modulated vector $\boldsymbol{s}=\{s_1, s_2, \ldots, s_n\}$. We now calculate the conditional probabilities of $s_1\oplus s_2=+1$ and $s_1\oplus s_2=-1$. According to the mapping operation defined by Eq.10,

$$\begin{aligned}P_r(s_1\oplus s_2=+1\mid\boldsymbol{r})&=P_r(s_1=+1\mid r_1)\times P_r(s_2=+1\mid r_2)\\&+P_r(s_1=-1\mid r_1)\times P_r(s_2=-1\mid r_2)\\&=\frac{1}{2}+\frac{1}{2}\prod_{i=1}^{2}\frac{\exp(2r_i/\sigma^2)-1}{\exp(2r_i/\sigma^2)+1}\end{aligned} \quad (17)$$

$$P_r(s_1\oplus s_2=-1\mid\boldsymbol{r})=1-P_r(s_1\oplus s_2=+1\mid\boldsymbol{r})=\frac{1}{2}-\frac{1}{2}\prod_{i=1}^{2}\frac{\exp(2r_i/\sigma^2)-1}{\exp(2r_i/\sigma^2)+1} \quad (18)$$

Similarly, we could calculate the conditional probabilities of $s_1\oplus s_2\oplus s_3=+1$ and $s_1\oplus s_2\oplus s_3=-1$ as follow:

$$\begin{aligned}P_r(s_1\oplus s_2\oplus s_3=+1\mid\boldsymbol{r})&=P_r(s_1\oplus s_2=+1\mid\boldsymbol{r})\times P_r(s_3=+1\mid r_3)\\&+P_r(s_1\oplus s_2=-1\mid\boldsymbol{r})\times P_r(s_3=-1\mid r_3)\\&=\frac{1}{2}+\frac{1}{2}\prod_{i=1}^{3}\frac{\exp(2r_i/\sigma^2)-1}{\exp(2r_i/\sigma^2)+1}\end{aligned} \quad (19)$$

$$P_r(s_1\oplus s_2\oplus s_3=-1\mid\boldsymbol{r})=1-P_r(s_1\oplus s_2\oplus s_3=+1\mid\boldsymbol{r})=\frac{1}{2}-\frac{1}{2}\prod_{i=1}^{3}\frac{\exp(2r_i/\sigma^2)-1}{\exp(2r_i/\sigma^2)+1} \quad (20)$$

We define the XOR-SUM operation as follow:

$$\sum_{i=1}^{n}\otimes s_i=s_1\oplus s_2\oplus\cdots\oplus s_n \quad (21)$$

We assume that the conditional probabilities of XOR-SUM

could be expressed as follow:

$$\begin{cases} P_r(\sum_{i=1}^{n}\otimes s_i=+1\,|\,\boldsymbol{r})=\frac{1}{2}+\frac{1}{2}\prod_{i=1}^{n}\frac{\exp(2r_i/\sigma^2)-1}{\exp(2r_i/\sigma^2)+1} \\ P_r(\sum_{i=1}^{n}\otimes s_i=-1\,|\,\boldsymbol{r})=\frac{1}{2}-\frac{1}{2}\prod_{i=1}^{n}\frac{\exp(2r_i/\sigma^2)-1}{\exp(2r_i/\sigma^2)+1} \end{cases} \quad (22)$$

Then,

$$\begin{aligned} &P_r(\sum_{i=1}^{n+1}\otimes s_i=+1\,|\,\boldsymbol{r}) \\ &=P_r(\sum_{i=1}^{n}\otimes s_i=+1\,|\,\boldsymbol{r})\times P_r(s_{n+1}=+1\,|\,\boldsymbol{r}) \\ &+P_r(\sum_{i=1}^{n}\otimes s_i=-1\,|\,\boldsymbol{r})\times P_r(s_{n+1}=-1\,|\,\boldsymbol{r}) \\ &=\frac{1}{2}+\frac{1}{2}\prod_{i=1}^{n+1}\frac{\exp(2r_i/\sigma^2)-1}{\exp(2r_i/\sigma^2)+1} \end{aligned} \quad (23)$$

$$\begin{aligned} &P_r(\sum_{i=1}^{n+1}\otimes s_i=-1\,|\,\boldsymbol{r})=1-P_r(\sum_{i=1}^{n+1}\otimes s_i=+1\,|\,\boldsymbol{r}) \\ &=\frac{1}{2}-\frac{1}{2}\prod_{i=1}^{n+1}\frac{\exp(2r_i/\sigma^2)-1}{\exp(2r_i/\sigma^2)+1} \end{aligned} \quad (24)$$

According to induction principle, the expression of conditional probabilities in Eq.21 is proved correct and could be expressed simply as follow:

$$\begin{cases} P_r(\sum_{i=1}^{n}\otimes s_i=+1\,|\,\boldsymbol{r})=\frac{1}{2}+\frac{1}{2}\prod_{i=1}^{n}\tanh(r_i/\sigma^2) \\ P_r(\sum_{i=1}^{n}\otimes s_i=-1\,|\,\boldsymbol{r})=\frac{1}{2}-\frac{1}{2}\prod_{i=1}^{n}\tanh(r_i/\sigma^2) \end{cases} \quad (25)$$

By employing Eq.23, one could calculate the probability $P_r[S_t(k)=0]$ as follows:

$$\begin{aligned} P_r[S_t(k)=0]&=P_r\left(\sum_{j=1}^{u_k}\oplus s_j=+1\middle|\boldsymbol{r}\right) \\ &=\frac{1}{2}+\frac{1}{2}\prod_{j=1}^{u_k}\tanh(r_j/\sigma^2) \end{aligned} \quad (26)$$

Therefore, the LLR of $S_t(k)$ is

$$P_r[S_t(k)=0]=\log\left(\frac{P_r\left(\sum_{j=1}^{u_k}\oplus s_j=-1\middle|\boldsymbol{r}\right)}{P_r\left(\sum_{j=1}^{u_k}\oplus s_j=+1\middle|\boldsymbol{r}\right)}\right)$$

$$=\frac{\frac{1}{2}-\frac{1}{2}\prod_{j=1}^{u_k}\tanh(r_j/\sigma^2)}{\frac{1}{2}+\frac{1}{2}\prod_{j=1}^{u_k}\tanh(r_j/\sigma^2)}=-2\text{atanh}\left(\prod_{j=1}^{u_k}\tanh\left(\frac{r_j}{2}\right)\right)$$

$$=-2\text{atanh}\left(\prod_{j=1}^{u_k}\tanh\left(\frac{\tilde{r}(t+k_j)}{2}\right)\right) \quad (27)$$

Now the Eq. 9 has been proved up and according to [18], the approximation expression of $P_r[S_t(k)=0]$ is shown in Eq. 28:

$$L(S_t(k))=-\left(\prod_{j=1}^{u_k}sign\left(\tilde{r}(t+k_j)\right)\right)\min_{j=1,\ldots,u_k}\left|\tilde{r}(t+k_j)\right| \quad (28)$$

The parity check matrices of LDPC and convolutional codes are sparse especially when the code length is long and so the algorithm is suitable for the LDPC and convolutional coded systems. But there exists a problem when applying the blind frame synchronization algorithm on the convolutional codes that the parity check matrices are usually in the form as:

$$H=\begin{pmatrix} h_0 & & & \\ h_1 & h_0 & & \\ h_2 & h_1 & h_0 & \\ & h_2 & h_1 & \ddots \\ & & h_2 & \ddots \\ & & & \ddots \end{pmatrix} \quad (29)$$

Most of the rows (columns) are a shift of another row (column). This fact largely affects the independence of syndromes elements and the algorithm performance is degraded. To reduce the correlations between syndromes elements, we interleave every transmitted packet and the parity check matrix *H*. Than the influence of non-independence is degraded. The interleaver is followed by the channel encoder, the details of it is described in the next section.

III. Information Hiding Based on Blind Frame Synchronization

To transmit a sequence of packets in security, we design a transmission system as shown in figure 2. The information sequences are firstly encrypted and then separated to packets of length *k* to be encoded by the channel encoder. The length of coded packets is *l* (*l*>*k*). Interleave the coded packets randomly before transmitting. Finally, some random sequences are introduced into the transmitted streams to increase the randomicity of the coded streams. The length and contents of the introduced sequences are randomly chosen so that it's more difficult for eavesdroppers to get each packet regularly. In other words, the coded packets are hidden among random sequences, as shown in figure 3. But the legal receiver knows the interleave parameters, the packets length and the parity check matrix of the codes, so the legal receiver could synchronize the transmitted packets blindly from the random sequences in the received stream. After the synchronization, the receiver can recover the information by de-interleaving and error-correcting decoding and then decrypting.

Note that when estimating the synchronization positions, Eq. 1 requires comparing the LLRs at different positions and choose the minimal one. It's not convenience for real-time processing of the synchronization procedure as the signal and noise power is unknown. To adaptively capture the packets, we can make some restrictions in the transmission system as follow:

(1) Set a time window contains a sequence of transmitted symbols in the channel with fixed length *L* which is known by the transmitter and receiver both.

(2) On the transmitter side, though the length of the introduced random sequences between packets is randomly chosen, the range could be limited to make sure that each window includes at least 2 encoded packets and the packets length is fixed and also known by the receiver.

(3) On the receiver side, set a time window with length *L* and fill the window with received samples. Compare the values of $\psi(t)$ on different positions in each window and

choose the positions t that make the $\psi(t)$ be previously lower than others as the estimation of the synchronization points.

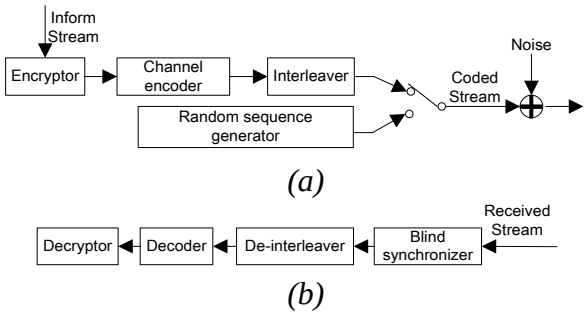

Fig. 2 *Structure of transmitter (a) and receiver (b) of the secure communication systems with blind synchronization technique*

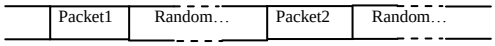

Fig. 3 *Introduce random sequences between packets*

The "previously lower" is difficult to judge by the computer program. So we propose a comparison algorithm to find the synchronization positions expediently. Because the packets from unsynchronization positions do not have the constraint relationship with the parity check matrices, the data seems randomly for the blind synchronizer and the values of $\psi(t)$ at unsynchronization positions are high and normal. And the values of $\psi(t)$ corresponding to the packets start from correct synchronization positions are low and the differences between them are not large. Inspired by this, we propose to find the "previously lower" $\psi(t)$ in a received time window follow the following steps:

Step1. Calculate $\psi(t)$ for each position t in the window.

Step2. Sort $\psi(t)$ from the highest to the lowest to form a new vector $\{\psi_{t_1},\psi_{t_2},...,\psi_{t_L}\}$ and record the index.

Step3. Calculate the ratios between the neighboring elements in the sorted vector generated in Step2 to form the vector $\boldsymbol{R}(1\sim L\text{-}1)$ where $R(1)=\psi_{t_1}/\psi_{t_2}$, $R(2)=\psi_{t_2}/\psi_{t_3}$, and so on.

Step4. Find the largest one in $\boldsymbol{R}$, record $R(k)$ and get the corresponding ψ_{t_k} and $\psi_{t_{k+1}}$. Choose all the ψ_{t_j} $(j>k)$ as the syndrome LLRs on the estimated synchronization positions. According to the recorded indexes in Step2, the positions could be obtained.

Some assistant conditions could be employed to reduce the probability of error synchronizations. Firstly, the number of packets in a time window is limited. For example, in the time window with length L, if the length of transmitted packets is N, the number of packets is must below L/N. Secondly, according to the second restriction condition descript previously, each window contains at least 2 packets. So the range of the number of packets in a window is limited to the range of 2 to L/N. Therefore, in the Step4, we just need to search the largest element in the vector $\boldsymbol{R}$ in a very short range, which is $R(m)$ to $R(L\text{-}2)$, where L is the length of the time window and m is the smallest integer above $L\text{-}L/N$.

IV. Simulation Results

In this section, simulation results of our blind synchronization technique are proposed. These simulations are present to verify the performance of synchronization of legal receivers while the information is hidden for illegal eavesdroppers. In the simulations, we consider that the transmitter is sending a binary sequence of LDPC and convolutional coded packets and is using a Binary Phase Shift Keying (BPSK) modulation. The propagation channel is corrupted by an AWGN with the variance $\sigma_n^2 = N_0/2$. On the transmitter side, we firstly separate the encrypted information to packets of length 256 bits and secondly these packets are encoded using LDPC or (7, 5) convolutional codes which have a 1/2 code rate and therefore, the length of the coded packets are 512 bits. Finally, interleave these packets before transmission. Between coded information packets, we fill random deceptive sequences, length and symbols of which are randomly chosen. Both the transmitter and receiver sides all set a time window contains 3000 bits. To show the algorithm performance more clearly, we draw the stems of $\psi^{-1}(t)$ instead of $\psi(t)$ and estimate the synchronization positions in each time window follow the steps descript in the previous section.

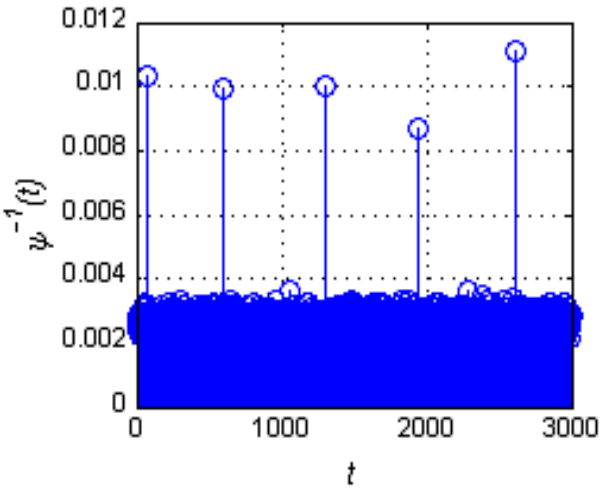

Fig. 4 Values of $\psi^{-1}(t)$ at different positions

Figure 4 shows the values of $\psi^{-1}(t)$ at different positions in a time window when the proposed algorithm is applied on a transmission system using convolutional codes as the channel coding with the signal-noise-ratio (SNR) $E_b/N_0 = 5dB$. It is clear that at synchronization positions, $\psi^{-1}(t)$ is obviously larger than others. According to the figure, the synchronization of every packet could be easily achieved in the time window. But the transmitted information is very difficult to be understood by illegal receivers. Firstly, the wiretappers are very difficult to discover and synchronize to the packets without synchronization words. Secondly, the length of the introduced random sequences between the packets are randomly variable so the wiretappers are very difficult to analyze the coding and interleaving parameters because according to [19-22] the blind recognition of coding and interleaving parameters must be based on a sequence of consecutive code words.

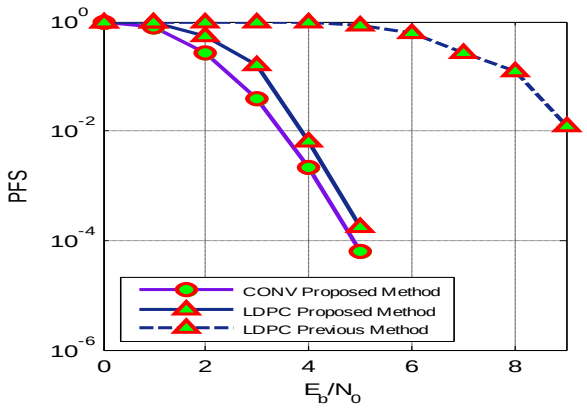

Fig. 5 Performance of proposed method on different SNRs and comparing with previous synchronization approach

The noise level influences the algorithm performances. Probabilities of false synchronizations (PFS) on different SNRs are shown in figure 5. The legends "CONV Proposed Method" and "LDPC Proposed Method" denote the performances of synchronizations when employing our proposed method to the convolutional codes and LDPC codes. Packets length and code rate are 512 and 1/2 and the length of time window is 3000. The LDPC code applied in the simulation is an irregular LDPC code in order to show the difference of the performances between the calculation equations of syndromes LLR based on Eq. 8 introduced in [14] and Eq. 28 proposed in this paper. The parity check matrix of the LDPC code is a 256×512 matrix, 66 of the 256 rows have 5 ones and the remained 190 rows have 6 ones. We also draw the PFS curve based on Eq. 8 in figure 5 and its legend is "LDPC Previous Method". It is shown in the figure that the corrected syndromes LLR calculation based on Eq. 28 yields better performance and Eq. 8 introduced in [14] is not correct.

V. Conclusion

An application of blind frame synchronization technique on secure communications is proposed and an error in the syndromes LLR calculation equation introduced in some previous research papers is corrected. By removing the synchronization words and hiding the coded packets among random sequences, the information is transmitted more cryptically and legal receivers could synchronize the packets blindly and recover the information. Simulations show that our algorithm yields a good performance. Though the cases of false synchronizations still exist, retransmission technique on the protocol layers could be used to improve the transmission quantity.

References

[1] T. Hongbin, L. Xinsong, "Cryptanalysis of a dynamic ID-based remote user authentication with key agreement scheme," *International Journal of Communication Systems*, vol. 25, 2012, pp. 1639-1644.

[2] C. Yuchi, L. Chaoliang, "Cryptanalysis of some user identification schemes for distributed computer networks," *International Journal of Communication Systems*, Published online: 14 FEB 2013, DOI: 10.1002/dac.2514.

[3] A. Marcos, Jr. Simplicio, R. M. Rony, Sakuragui, "Cryptanalysis of an efficient three-party password-based key exchange scheme," *International Journal of Communication Systems*, vol. 25, 2012, pp. 1443-1449.

[4] R. Putthacharoen, P. Juleang, S. Mitatha, "Novel Optical Cryptography using PANDA ring resonator for highly secured communication," *Optical Engineering*, vol. 50, 2011, pp. 075001-1 – 075001-6.

[5] R. Vimalathithan, M. L. Valarmathi, "Cryptanalysis of Simplified-AES using Particle Swarm Optimisation," *Defence Science Journal*, vol. 62, 2012, pp. 117-121.

[6] C. Hakan, N. Osman, Ucan, N. Odabasioglu, A. Sonmez, "Performance of joint multilevel/AES-LDPCC-CPFSK sckemes over wireless sensor networks," *International Journal of Communication Systems*, vol. 23, 2010, pp. 77-90.

[7] A. K. Nanda, L. K. Awasthi, "Joint Channel Coding and Cryptography for SMS," *Proceedings of 2011 International Siberian Conference on Control and Communications (SIBCON2011)*, 2011, pp. 51-55.

[8] W. K. Harrison, S. W. McLaughlin, "Physical-Layer Security: Combining Error Control Coding and Cryptography," *Proceedings of IEEE International Conference on Communications (IEEE ICC 2009)*, 2009.

[9] J. Chen, M. P. Fossorier, "Near Optimum Universal Blief Propagation and Convolutional Codes," *IEEE Transactions on Communications*, vol. 50, 2002, pp. 406-414.

[10] F. R. Kschischang, B. J. Fery, "Iterative Decoding of Compound Codes by Probability Propagation in Graphical Models," *IEEE Journal on Selected Areas in Communications*, vol. 16, 1998, pp. 1-11.

[11] L. Chiayu, C. Shucheng, K. Mongkai, "Operation reduced low-density parity-check decoding algorithms for low power communication systems", *International Journal of Communication Systems*, vol. 26, 2013, pp. 68-73.

[12] J. Sun, "Synchronization for Capacity-Approaching Coded Communication Systems," *Degree Thesis of University of West Virginia*, Morgantown, USA 2004.

[13] J. Sun, M. C. Valenti, "Optimum frame synchronization for preamble-less packet transmission of turbo codes," *Asilomar Signals, Systems, Computers* vol.1, 2004, pp. 1126-1130.

[14] R. Imad, G. Sicot, "Houcke S. Blind frame synchronization for error correcting codes having a sparse parity check matrix," *IEEE Transactions on Communications*, vol. 57, 2009, pp. 1574-1577.

[15] R. Imad, S. Houcke, "Theoretical Analysis of a MAP Based Blind Frame Synchronizer," *IEEE Transactions on Wireless Communications*, vol. 8, pp. 5472-5476.

[16] R. Imad, S. Houcke, C. Jego, "Blind frame synchronization of product codes based on the adaptation of the parity check matrix," *Proceedings of IEEE International Conference on Communications (IEEE ICC 2009)*, 2009.

[17] R. Imad, C. Poulliat, S.Houcke, "Blind Frame Synchronization of Reed-Slolomon codes: Non-Binary vs. Binary Approach", *Proceedings of IEEE Eleventh International Workshop on Signal Processing Advances in Wireless Communications (SPAWC 2010)*, 2010.

[18] J. Hagenauer, E. Offer, L. Papke, " Iterative Decoding of Binary and Convolutional Codes," *IEEE Transactions on Information Theory*, vol. 42, 1996, pp. 429-445.

[19] J. Barbier, J. Letessier, "Forward error correcting codes characterization based on rank properties," *International conferences on Wireless Communications*, 2009.

[20] X. Yang, N. Wen, "Recognition method of BCH codes on roots information dispersion entropy and roots statistic," *Journal of Detection & Control*, vol. 32, 2010, pp. 69-73.

[21] N. Wen, X. Yang, "Recognition methods of BCH codes," *Electronic Warfare*, Jun. 2010, pp. 30-34.

[22] X. Lv, Z. Huang, S. Su, "Fast recognition method of generator polynomial of BCH codes," *Journal of Xidian University*, vol.38, 2011, pp.187-191.

Zhou Jing is now a graduate student in National University of Defense Technology (NUDT). His research interests include error control coding and information theory, especially the blind signal processing and cognitive networks. Now his focus is on blind parameters recognizing of error-correcting codes.

Huang Zhiping received the Ph.D. degree from Beijing Institute of Technology in 1993 and now is a professor and Ph.D. supervisor in the national university of defense technology. His research interests include information and communication theory, high speed information processing and modern measurement and instruments.

Su Shaojing received the Ph.D. degree in from the national university of defense technology (NUDT), in 2001. Now he is an associate professor in NUDT. His research interests include optical communication test and high-speed optical communication systems.