International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 8, ISSN No. 2455-2143, Pages 255-259
Published Online December 2019 in IJEAST (http://www.ijeast.com)

ANTI EAVESDROPPING CODE SYSTEM BASED ON FOUNTAIN CODES

Safiyo.M.Ahmed[1*] Master's Student
NIU Fang-lin[2] Associate Professor
H.Hasnain Imtiaz[1] Master's Student
Asim Zaman[2] Master's Student
School of Electronics and Information Engineering
Liaoning University of Technology
Jinzhou, Liaoning, P.R China

Abstract— **Digital fountain code and network coding are both effectual practical methods to increase the efficiency of network transmission. Network fountain code created by the organic combination of the two important theoretical significance and application value. In this paper for the security of wireless communication, a method of anti-eavesdropping combined with the physical layer fountain code is proposed. By adding the artificial noise on both sides to destroy the eavesdropper fountain code MP decoding sequence. in order to maintain the normal communication of the main channel, the eavesdropper error rate has been greatly increased. The MATALB simulation results show that the method builds the eavesdropper's error rate reach upto 30% to 50%. It can be more in the situation of increasing the noise of artificial interference.**

Keywords— ***Fountain code, Anti-Eavesdropping, MATALB, Wireless communication, Network***

I. INTRODUCTION

With the rapid development of mobile communications and related business such as; mobile intelligence terminals in politics, military affairs, foreign relations and other areas are playing a major role. In recent years all kind of fast services are introducing in mobile communication networks [1]. But at the same time also facing security concerns day-to-day in messages and information transferring. In other words, wireless communication networks such as cellular mobile communications and wireless sensing relay usage develops the quantity and coverage of the network range. In recent years, relay network research has achieved many important results [2]. The knowledge of some results comes essentially from the multi-input multi-output (MIMO) antenna system. MIMO systems spatial diversity gains by using multiple transmitting and multiple receiving antennas to combat fading in wireless channels and improve system performance [3]. In traditional wireless networks, it is difficult for terminal equipment to understand multi-day line due to factors such as volume, weight, power consumption and cost. In addition, in networks system with essential nodes such as cellular mobile communication, the coverage range of the system can also be enhanced by means of collaborative relay [4] [5]. In a data communication system that transmits by erasing the channel, if there is data loss in the transmission or if there is an unrecoverable error, the receiving end needs to send a feedback signal to the originating and request for reissue [6] [7]. Channel using a hybrid error correction method to ensure that by wiping channel reliable transmission can also be achieved. When the probability of erasing is high, the amount of feedback data in transmission is very large. Digital Fountain Code can effectively solve the problem of eavesdropping in the system. Using the digital fountain code transmission system, the sender first encodes the information into fountain and the information can be compared, whether it is larger than the length of the original information or not [8]. The encoding information can be translated. The receiving end obtains sufficient coding information to feedback, the sender controls the fountain coding and the transmission of coding information according to the feedback information [9] [10].

Traditional eavesdropping technology mainly in the communication network layer is to add non-disclosure protocols. Which is adding PINs to the information by forgoing the difficulty of information to ensure the information security [11]. For the background, it is difficult to reproduce, for the reason so researchers are looking at whether channel coding can be used to protect information. McEliece, first time combined error-correcting codes with encryption systems [12]. However, this method is expensive and low-rate, but the researchers have focused the direction of the study on the low-density parity code with better characteristics. In the research paper, use of feedback system to combine channel noise with LDPC code to successfully achieve anti-eavesdropping purposes. The feedback factor is added to the eavesdropping channel to achieve a better determination of avoiding eavesdropping. Fountain code and LDPC [13] code in many features of coding decoding have a better match to its characteristics in the information security application to use its decoding cost and other characteristics can essentially improve the transmission efficiency of wireless communications. Consequently, in this paper to achieve the purpose of secure communication. Procedure of the randomness of noise signal is difficult to imitate the characteristics of the fountain code and artificial noise combined coding method, while

International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 8, ISSN No. 2455-2143, Pages 255-259
Published Online December 2019 in IJEAST (http://www.ijeast.com)

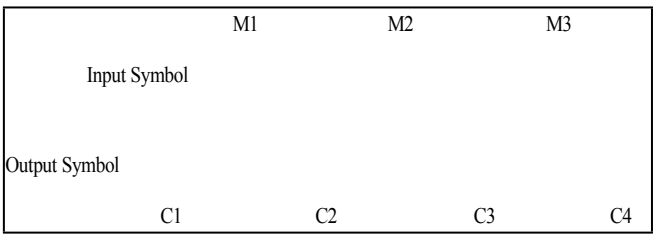
eavesdroppers through decoding, it is difficult to recover all the information by decoding, resulting as high deceptive symbol rate of eavesdropping failure [14] [15].

II. FOUNTAIN CODE

Fountain code is a class of rate less code, in which the length of K's information sequence within the encoder produced codeword sequence can be infinite length, different from the traditional fixed rate code (code word length in the sender has been determined) [16]. The word length of fountain code is determined by the receiving side, when the receiving side defines that can be successfully translated, the confirmation signal will be send to the sender through the feedback channel (Only one bit). Fountain code is ideal for time-change channels and multicast channels [17]. Luby designed the LT code for the first practical fountain code, it can progressively spread the channel capacity in the binary delete channel (BEC), but the LT code cannot achieve linear time compilation code [18]. Afterwards, Shokrollahi intended the coding and decoding time complexity of both Linear Fountain Code - Raptor Code. Raptor code is an extension of LT code is composed of a high-code low-density check (LDPC) code and an LT-grade connection [19] [20]. The LT coding method is given as follow:

1) Randomly select an output symbol Ω according to the set node size distribution port d.
2) Select d input signal using uniform distribution.
3) The corresponding output symbol is the module of the d input symbol selected in 2.
4) Repeat the first three steps until receive a pick-up feedback signal.

In the design of LT code, the choice of degree distribution is a key factor, in order to achieve excellent performance of the LT code, Luby proposed the Soliton distributed and the Robust Soliton distribution, while in the Design of the Raptor code, Shokrollahi chose a degree distribution with an average output of constants [21] [22]. In the encoding schematic diagram of the LT code shown in figure 1. The degree of the 4 output symbols they are 2, 3, 2, 1.



Schematic diagram of LT codes

At present, the typical representative of the fountain code Raptor code has been DVB-H standard MBMS standards for mock and 3GPP for organizations.

III. PRINCIPLE OF ANTI-EAVESDROPPING CHANNEL MODEL

The simplest eavesdropping channel consists of three main parts: information sender, the recipient of the information and the eavesdropper [23]. Third-party eavesdropper between the legal sender and receiver, the third-party eavesdropper eavesdropping on their communications information. The block diagram is given in figure 2, where Alice is set up for the information sender, Bob is the receiver and Eve represents the eavesdropper. The main communication between Alice and Bob, channel noise is N_{ab}, Eve and Alice are eavesdropping channels and the channel noise between them is N_{ae}. N_{be} is between Bob and Eve.

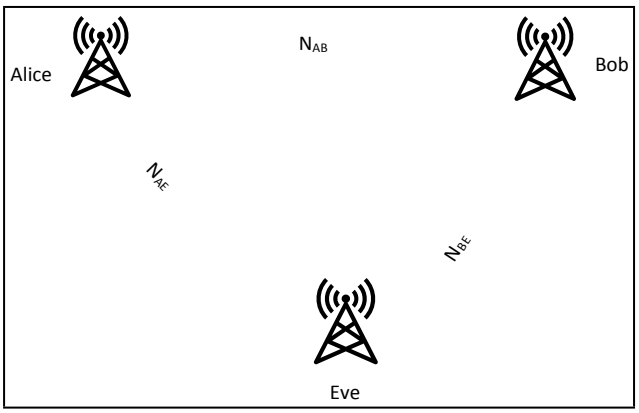


Fig. 2. Anti-eavesdropping channel model

This article adopts that the eavesdropper Eve knows all the communication protocols between Alice and Bob. When Alice sends the signal to Bob through the radio and Eve can effectively eavesdrop the Alice signal as the eavesdropper. The location of Eve eavesdropping is difficult for the communicator to detect.

Noise contained in the Eve signal:

$$N_{EVE} = 2N_b + N_{ae} + N_{ab} + N_{be} \quad (1)$$

$$N_{Bob} = N_b + N_{ab} + N_{ab} \quad (2)$$

There is an Eve signal that contains noise greater than or equal to the Bob signal, which confirms that the eavesdropper, eavesdrops on the signal sent by the sender at any position where the signal is received by the signal than the main channel. When the main channel noise is too small, the artificial noise N_b can be turned on to increase the eavesdropper's channel noise, increase the d number of error symbols to ensure communication security between the sender and the receiving side [24].

International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 8, ISSN No. 2455-2143, Pages 255-259
Published Online December 2019 in IJEAST (http://www.ijeast.com)

IV. SIMULATION RESULTS AND ANALYSIS

The anti-eavesdropping channel designed by the formula (2), it can clarify that the eavesdropper receives more noise than the main channel, when the main channel noise is too low, it can ensure that the eavesdropper receives a higher noise by adjusting the size of the artificial noise. The fountain code coding method combined with the layer fountain code can guarantee the wireless transmission of the voice signal. In this paper we add nice in the both side receiver and sender.

It is assumed that the sender Alice needs to send the number of message k to the receiver Bob and the eavesdropper eve understand the communication protocol of the main channel. The listening position is random. Here, Eve is selected in the middle of the main channel that is $N_{ae} + N_{be} = N_{ab}$. Then the resulting channel probability is $P_{(Nae+Nbe)} = P_{(Nab)} = P_{ab}$.

Alice signal is encoded using fountain codes, both Bob and Eve are decoding using MP decoding method. RSD function used for encoding is; δ=0.5, c=0.03, Crand is set as; e=0.5k. Experiment was simulated in MATLAB/Simulink software, MATLAB code for the experiment is given in figure bellow.

```
clc;clear all; close all;
P1=xlsread('safiyo.xlsx','sheet1','B7:T7');
% OVERHEAD1=xlsread('m.safiyo.xlsx','sheet1','B3:X3');
OVERHEAD2=xlsread('safiyo.xlsx','sheet1','B9:T9');
OVERHEAD3=xlsread('safiyo.xlsx','sheet1','B15:T15');
%%%%%%%%%FIG1%%%%%%%%%%%%%%%%%%%%%
% figure
%
% plot(P1,OVERHEAD2,'o-');
% hold on
% plot(P1,OVERHEAD3,'*-k');
% xlabel('P_A_B')
% ylabel('OVERHEAD')
% legend('P_A_B-P_A_E=\Delta=0.01','P_A_B-P_A_E=\Delta= 0.02')
% title('overhead vs p1,k=1000')
% %%%%%%%%%%FIG2%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%Rx
%
% DC=xlsread('safiyo.xlsx','sheet1','B10:T10');
%
%
%
% figure
% plot(P1,DC,'*-');
% title('the number of decoding vs p1,k=2000')
%
% xlabel('P_A_B')
% ylabel('the number of decoding')
% legend('P_A_B-P_A_E=\Delta= 0.02')
```

Fig. 3. Simulation Code

```
BER11=xlsread('safiyo1.xlsx','sheet1','E43:W43');
BER21=xlsread('safiyo1.xlsx','sheet1','E38:W38');
BER31=xlsread('safiyo1.xlsx','sheet1','E31:W31');

figure
plot(P2,BER11,'S-');
hold on
plot(P2,BER21,'o-');
hold on
plot(P2,BER31,'b*-');

xlabel('P_A_B')
ylabel('BER')
legend('P_A_B-P_A_E=\Delta=-0.02','P_A_B-P_A_E=\Delta=-0.01','P_A_B-P_A_E=\Delta=0')

title('ber vs P_A_B,k=1000')

% %%%%%%%%%%%fig7%%%%%%%%%%%%%%%%%%%%%%%%
BER111=xlsread('safiyo1.xlsx','sheet1','E43:W43');
BER222=xlsread('safiyo1.xlsx','sheet1','B43:T43');
figure
plot(P2,BER111,'*-');
hold on
plot(P1,BER222,'o-');

xlabel('P_A_B')
ylabel('BER')
legend('add noise,','no noise')

title('compere add noise with no noise in the source vs P_A_B,k=1000')
```

Fig. 4. Simulation Code

(1) Select k=1000, compare the influence of increased artificial noise on the eavesdropper error rate of listening. Channel deletion probability P_{ab} due to main channel noise P_{ae} represents the probability caused by artificial noise and the eavesdropper bit error rate BER. Simulation result is shown in figure 5 and 6.

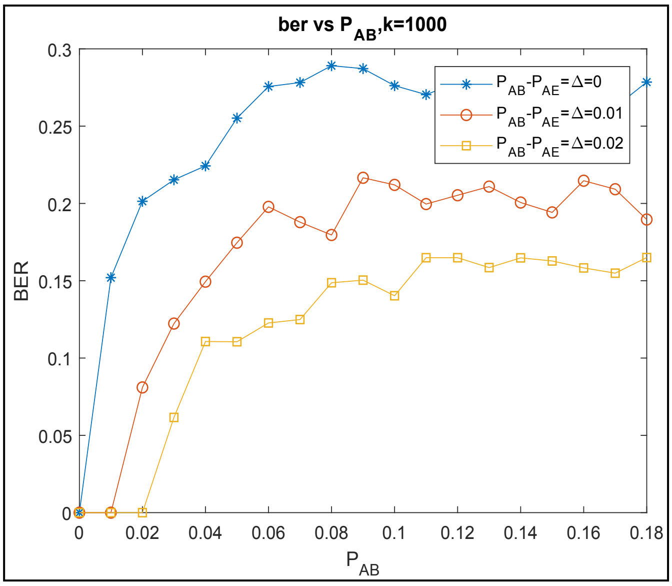


Fig. 5. Effect of P_{ab} and P_{ae} on eavesdropper's BER, When max P_{ab}-P_{ae}=0 to 0.02

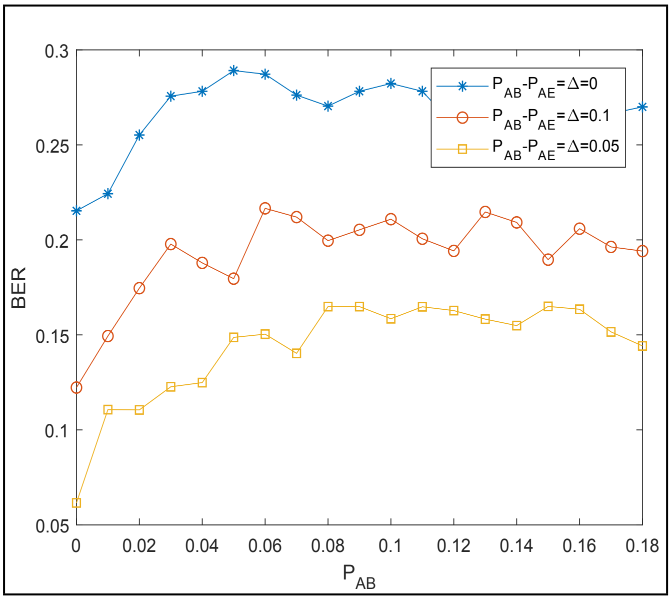


Fig. 6. Effect of P_{ab} and P_{ae} on eavesdropper's BER, When max P_{ab}-P_{ae}=0 to 0.05

Simulation result in figure 5 and 6 shows that the eavesdropper Eve is related to the size of P_{ab} according to the BER. When P_{ab} increases, BER varies as well. Mainly due to the increase in the number of error symbols caused by the addition of P_{ab} and the increasing number of different decoding symbols between Bob and Eve, resulting in Bob

International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 8, ISSN No. 2455-2143, Pages 255-259
Published Online December 2019 in IJEAST (http://www.ijeast.com)

decoding ends. Therefore, the number of miscodes increased when the number of decoding symbols is sufficient Lynforth almost self-based. The translation of the self-decoding in sequence is no longer based on the Bob order, so the error rate decreases as the P_{ab} increases.

(2) when k=1000, change in $P=P_{ab}-P_{ae}=0$ to -0.02, to compare the effect of adding artificial noise on the error code of eavesdropper's is shown in figure 7 and 8.

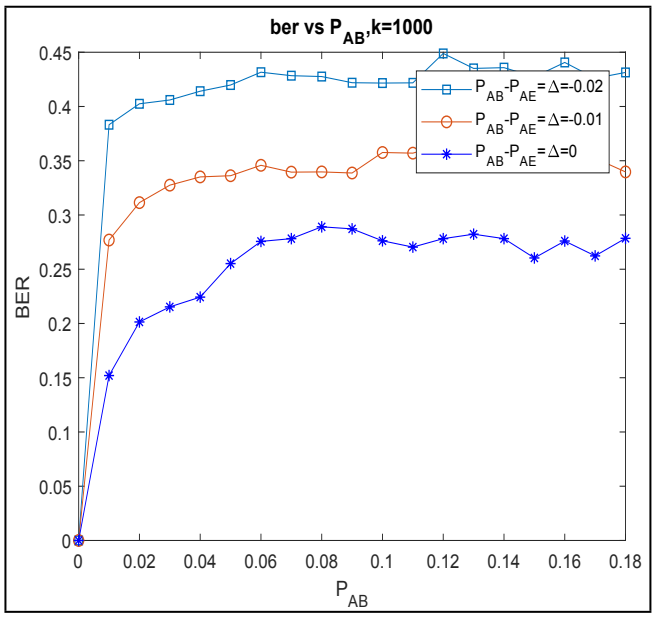


Fig.7. effect of P_{ae} on eavesdropper's BER

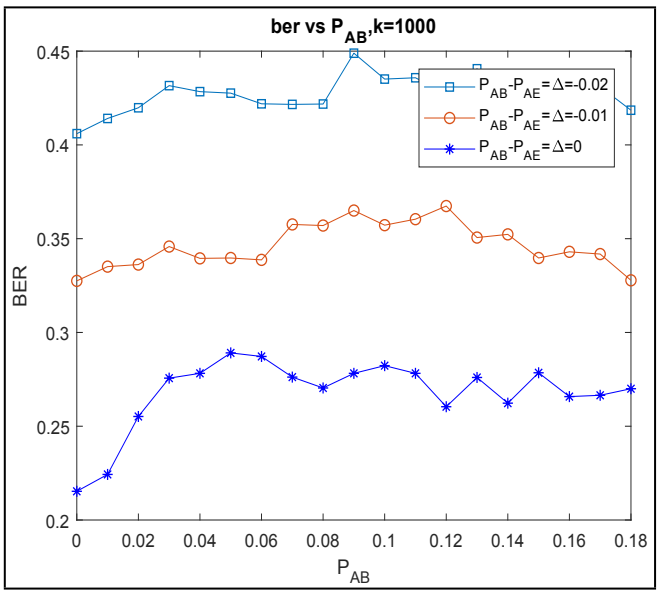


Fig.8. effect of P_{ae} on eavesdropper's BER

Thus, it can be seen that the method of coding the anti-eavesdropping source is that when k is large, the k cannot increase the error rate of eavesdroppers by increasing the P_{ab}, but the artificial noise method proposed in this paper can efficiently improve the security of wireless communication.

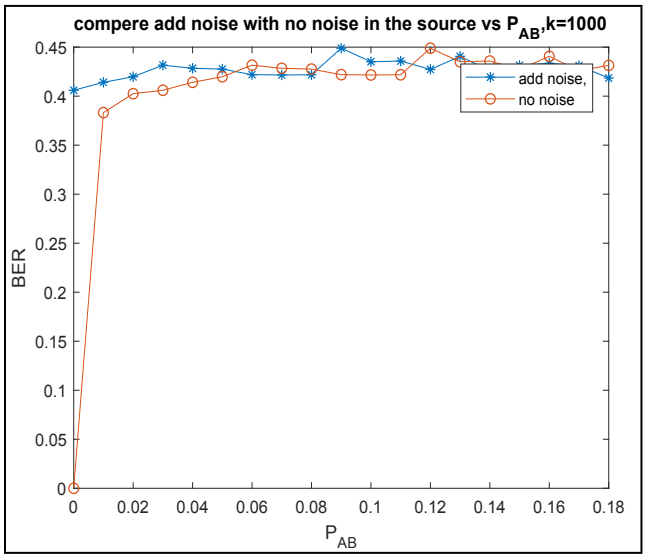


Fig.9. compare add noise with no noise vs P_{ab} when k=1000

V. CONCLUSION

In this paper introduce the fountain code and LT code first. Analyzed the principle of fountain code and principle of Anti-Eavesdropping channel model. At the end anti-eavesdropping channel combined with fountain code proposed method introduced. The simulation results show the anti-eavesdropping method that effectively blocks eavesdroppers under the condition of ensuring the safe communication of the main channel. Eavesdropping into the relevant information ensures the security of wireless communication.

VI. REFERENCES

[1] G. Savva, K. Manousakis and G. Ellinas, "Eavesdropping-Aware Routing and Spectrum/Code Allocation in OFDM-Based EONs Using Spread Spectrum Techniques," Journal of Optical Communications and Networking, vol. 11, no. 7, p. 409, 2019.

[2] R. Gummadi and R. Sreenivas, "Relaying a fountain code across multiple nodes," in IEEE Information Theory Workshop, 2008.

[3] L. Ze, C. Youhua, X. Peng, W. Zhibin, C. Yuanyuan and L. Jinyu, "Research on eavesdropping source localization of anti-laser eavesdropping early warning system," Journal of Applied Optics, vol. 39, no. 3, pp. 126-129, 2018.

[4] V. Jyoti and R. Kaler, "Security enhancement of OCDMA system against eavesdropping using code-switching scheme," Optik, vol. 122, no. 9, pp. 787-791, 2011.

[5] L. Zheng, N. Fang-lin, Q. D.-x. C. Xi-biao and G. Ying, "Design of anti¯eavesdropping code based on fountain

codes," Journal of Shandong University (Natural Science), vol. 53, no. 7, 2018.
[6] H. Zhu, T. Pu, Y. Chen, T. Fang and J. Zheng, "A novel code-shift-keying scheme against upstream eavesdropping in optical code division multiple access network," in Proceedings of 2013 3rd International Conference on Computer Science and Network Technology, 2013.
[7] H. C. Ji Choi, H. Lee, J. Cha and H. Lee, "Code-Division Multiplexing Based MIMO Channel Sounder with Loosely Synchronous Codes and Kasami Codes," in IEEE Vehicular Technology Conference, 2006.
[8] L. Liu and X. Qiu, "Research of digital fountain code based on network transmission," in nformation Science and Management Engineering II (Set), 2014.
[9] J. Béranger, "The Code is Ethics and Ethics is the Code," in The Algorithmic Code of Ethics, 2018, pp. 55-120.
[10] R. Gummadi and R. Sreenivas, "Relaying a fountain code across multiple nodes," in IEEE Information Theory Workshop, 2008.
[11] A. J. Mendez, "Design of encoders and decoders for code/pulse-position-swapping (C/CPPS) based on sonar codes," in Free-Space Laser Communication Technologies XXIV, 2012.
[12] H. Kobayashi, "Improvement of the 2D code based localization by using multiple codes," in IEEE International Conference on Industrial Technology (ICIT), 2018.
[13] D. Matas and M. Lamarca, "Analysis of LDPC code syndrome entropy based on subgraphs," in 9th International Symposium on Turbo Codes and Iterative Information Processing (ISTC), 2016.
[14] J. Liu, J. Yang, Z. Cheng and M. Wang, "Anti-eavesdropping Network Coding Algorithm Based on T-N Threshold," Chinese Journal of Electronics, vol. 26, no. 2, pp. 372-376, 2017.
[15] J. Jiang, Y. Li, X. Ma, P. Zhang, Y. Fan and Q. Hao, "Research on noise quality in anti-eavesdropping system based on acoustic masking," in International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2017.
[16] N. Zhao, F. R. Yu, M. Li and V. C. M. Leung, "Anti-Eavesdropping Schemes for Interference Alignment (IA)-Based Wireless Networks," IEEE Transactions on Wireless Communications, vol. 15, no. 8, pp. 5719-5732, 2016.
[17] G. Gangadharan, "From legal code to digital code: making software services rights-aware," International Journal of Private Law, vol. 4, no. 2, p. 299, 2011.
[18] H. Zhou and W. Lei, "Anti-eavesdropping Scheme on Physical Layer for Full-Duplex Relay System Based on SWIPT," in International Conference on Computer Technology, Electronics and Communication (ICCTEC), 2017.
[19] D. Sejdinovic, V. Ponnampalam, R. J. Piechocki and A. Doufexi, "The Throughput Analysis of Different IR-HARQ Schemes Based on Fountain Codes," in IEEE Wireless Communications and Networking Conference, 2008.
[20] J. Yang, J. An, X. Li, L. Yuan and N. Yang, "Fountain codes based partial cooperation in cooperative communications," in Proceedings of the 6th International Wireless Communications and Mobile Computing Conference on ZZZ - IWCMC '10, 2010.
[21] Z. Deng, X. Tong and L. Gan, "A Decoding Method For Modulo Operations-Based Fountain Codes Using the Accelerated Hopfield Neural Network," in Proceedings of the 2016 International Conference on Computer Engineering, Information Science & Application Technology (ICCIA 2016), 2016.
[22] L. Mu, L. Caoyuan, W. Yan, G. Fengyue and Y. Rui, "The research on improvement of narrowband radio channel communication protocol based on fountain codes," in 6th International Conference on Electronics Information and Emergency Communication (ICEIEC), 2016.
[23] W. Zhu, L. Gan, B. Yi and Q. Xie, "The application of fountain code in differential frequency hopping systems," in International Conference on Cyberspace Technology (CCT 2014), 2014.
[24] Z. Yan, F. Xin, J. Zhicheng and T. Hongmei, "The Application of Fountain Code in Image Wireless Transmission," Procedia Engineering, vol. 29, pp. 3322-3326, 2012.