Wuhan University
Journal of Natural Sciences

2021, Vol.26 No.6, 507-512

Article ID 1007-1202(2021)06-0507-06
DOI https://doi.org/10.1051/wujns/2021266507

A Wire-Line Secure Communication System Based on CCFD Self-Interference Cancellation

□ **LU Wenjian**[1], **LIU Sanjun**[1†], **LAI Guohong**[1,2]

1. School of Information Engineering, Hubei Minzu University, Enshi 445000, Hubei, China;

2. College of Physical Science and Technology, Central China Normal University, Wuhan 430070, Hubei, China

© Wuhan University 2021

Abstract: This paper presents a design scheme of wire-line telephone system using self-interference (SI) cancellation technology in co-frequency co-time full-duplex (CCFD) system to realize absolute secure communication at the physical layer. This scheme can hide the target signal by skillfully releasing the high-power artificial noise to the whole link at the receiving node, and then make use of the receiver's knowledge of the SI signal to achieve high dB SI cancellation with the help of analog domain SI cancellation technology in CCFD domain, so that the signal-to-noise ratio (SNR) received by the eavesdropper at any position of the link is far lower than that of the legitimate receiver, so as to realize the absolutely secure communication in the sense of Wyner principle. This paper not only puts forward the specific design scheme of absolutely secure communication telephone, but also analyzes the calculation of security capacity under different eavesdropping positions, different SI cancellation capability and different system parameters according to Shannon theory.

Key words: co-frequency co-time full-duplex(CCFD); physical layer security; self-interference cancellation; security capacity; wire-line communication

CLC number: TP 391.8

Received date: 2021-09-16

Foundation item: Supported by the Natural Science Foundation of Hubei Province (2019CFB593), the National Natural Science Foundation of China (61961016), Ph.D. Research Start-up Foundation of Hubei Minzu University (MY2018B08) and Graduate Education Innovation Plan of Hubei Minzu University (DC2000000119)

Biography: LU Wenjian, male, Master candidate, research direction: embedded system and artificial intelligence. E-mail: 202030343@hbmzu.edu.cn

† To whom correspondence should be addressed. E-mail: liusanjunbox1@126.com

0 Introduction

Traditional wire-line secure communication systems mostly adopt encryption algorithms based on cipher key, such as DES algorithm[1] and AES algorithm[2]. However, with the improvement of large-scale computing ability and resources, any key is in danger of being leaked or decoded. In recent years, physical layer security[3] has become one of the effective methods to solve the drawbacks of traditional secrecy. It was first proposed by Wyner based on Shannon information theory[4], and also known as the absolute security of the physical layer communication. The theory points out that if the capacity C_e of the eavesdropper is less than the capacity C_b of the legitimate receiver by skillfully designing the circuit, the system can realize absolutely secure communication with the security capacity $C_s = C_b - C_e$, as shown in Fig. 1, where Alice is the transmitter node, Bob is the receiver and Eve is the eavesdropper. The larger the C_s is, the more the information can be safely transmitted in unit time. Compared with the traditional secure communication technology, the physical layer secure communication technology[5-7] does not rely on computational complexity and cannot be cracked by computing power, which can realize absolutely secure communication.

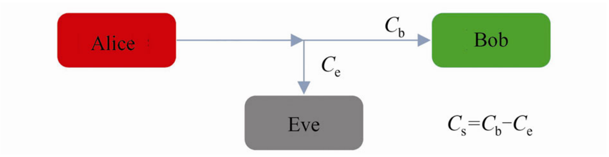

Fig. 1 Physical layer security criterion based on Wyner principle

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (https://creativecommons.org/ licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

However, at present, the physical layer security technology based on Wyner principle is mostly used in the field of wireless communication. For example, Ref. [8] discusses that the artificial noise in Null Space can greatly reduce the signal quality received by the eavesdropper without affecting the reception of the legitimate receiver. The premise of this method is to accurately obtain the channel state information (CSI) of the receiver, but it is difficult to realize in practical communication. Ref. [9] is the first to use self-interference (SI) from co-frequency co-time full-duplex (CCFD) receiver to improve system confidentiality, and Refs. [10, 11] improved this theory. However, due to the openness of the wireless channel, Eve can intentionally choose a location very close to the transmitter for eavesdropping, resulting in a surge in eavesdropping capacity and the system security capacity becomes negative. In order to realize absolute physical layer security in the whole space, it must be ensured that there is a very high self-interference cancellation effect in all positions, which is difficult to achieve in practical applications. Therefore, these studies do not give the specific SI cancellation scheme.

Recently, it has been proposed to use wire-line communication to achieve absolutely secure communication. For example, although Ref. [12] puts forward the idea of polluting wire-line channel with artificial noise, it only analyzes the impact of different SI cancellation capabilities on channel capacity from the theoretical level, and does not give a specific circuit scheme. Compared with the wireless communication system, the wire-line communication system transmits signals with the help of wired media, and its anti-interference and stability are better than the wireless communication system. When the physical layer security technology is applied to wire-line communication, the power attenuation is small, and the effect of "hiding" the target signal with artificial noise is better. Since wire-line communication technology is still widely used in military, medical, financial and information systems, it is extremely important to realize absolutely secure communication in wire-line communication system. Therefore, based on Wyner principle, this paper proposes a new design scheme of wired secure communication system, which gives up the traditional confidential methods, and uses the analog domain SI cancellation technology in CCFD[13] to enable both nodes of the full-duplex system to eliminate the artificial noise. Concurrently, the system can ensure that there is always high-power artificial noise in each frequency band, thus preventing eavesdroppers from eavesdropping on the target signal. Both the system security capacity calculation method and its relationship between SI cancellation capability will be studied in this paper.

1 System Model

The wire-line secure communication system proposed in this paper is based on CCFD technology for communication. We call the legal communication nodes are Alice and Bob, the eavesdropper node is called Eve. The main structure and principle of the system are shown in Fig. 2, where the communication distance between the two nodes is L, and Eve is eavesdropping at a distance of x meters from Alice. In the communication process, when the transmitter sends the target signal to the link, the receiver will send the artificial noise signal at the co-frequency co-time to hide the target signal. At the same time, the receiver can eliminate the artificial noise by using the SI canceller (SIC) to make the SNR of the legal channel much higher than that of the eavesdropping channel before ensuring the receiver to receive the target signal smoothly. We suppose that f_1 and f_2 are the local oscillation signals staggered with each other, and the center frequencies are f_{c1} and f_{c2}, respectively; the signal generator S_{a} and N_{b} separately send out the modulated target signal S_{a1} and the modulated artificial noise signal N_{b1} which are up-converted by f_1; Similarly, the modulated target signal S_{b2} and the modulated artificial noise signal N_{a2} both are up-converted by f_2, which are sent out by S_{b} and N_{a}, respectively.

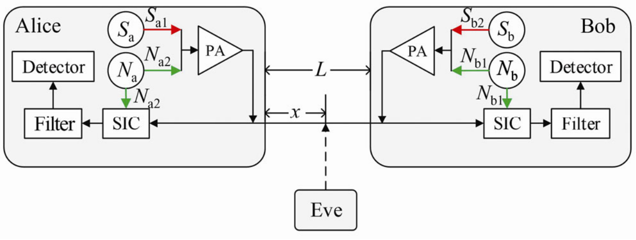

Fig. 2 Main structure and principle of the wire-line secure communication system

Since the CCFD system is known about the artificial noise signal, we analyze how the receiver receives the target signal from Alice to Bob, as shown in Fig. 3. When Bob receives the target signal, the known artificial noise signal N_{b1} is adjusted by amplitude adjuster α_0 and phase adjuster φ_0 through SIC, so the artificial noise signal N_{b1} on the link can be eliminated by adder. Then, the interference of different carrier signals is filtered through the filter, and the detector can detect the signal to be received.

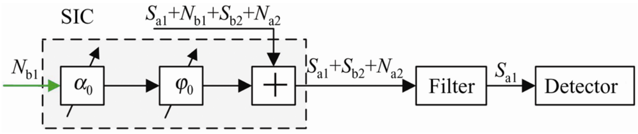

Fig. 3 SI cancellation and detection process

According to SI cancellation theory, we eliminate the known artificial noise signal N_{b1} through SIC; By eliminating the signals N_{a2} and S_{b2} with the carrier f_{c2} through the band-pass filter with the center frequency of f_{c1}, the signal S_{a1} with the carrier f_{c1} can be detected by the detector, and the baseband target signal can be obtained after the signal S_{a1} is correctly demodulated. Due to the symmetry of the system, the processing process of signal S_{b2} is similar to that of signal S_{a1}, which will not be repeated in this paper.

2 Analysis of System Security Capacity

This paper measures the security communication capability of the system by analyzing the security capacity of the wire-line communication system: if the maximum eavesdropping capacity obtained by Eve when eavesdropping the target signals from Alice and Bob at any eavesdropping position is less than the security capacity of the legal channel, the absolute physical layer security communication can be realized, otherwise there is the possibility of eavesdropping. According to Fig. 2, due to the symmetry of wire-line secure communication system, we analyze the system security capacity of Alice signal S_{a1} transmitted to Bob node, similarly, and we can see the system security capacity of Bob signal S_{b2} transmitted to Alice.

We set the power of signal S_{a1}, N_{a2}, S_{b2} and N_{b1} as P_{S_a}, P_{N_a}, P_{S_b} and P_{N_b}, respectively; The thermal noise power of the system is N_0; The power gain of the power amplifier is A_P, and the power gain of the power amplifier is

$$A_P=10\lg\frac{P_2}{P_1} \tag{1}$$

where P_1 and P_2 represent the input and output power of the power amplifier respectively, so we can know the power amplification factor of the power amplifier:

$$\alpha_P=10^{\frac{A_P}{10}} \tag{2}$$

The propagation of the signal in the wire-line medium follows the exponential attenuation law[14], as shown in Fig. 4.

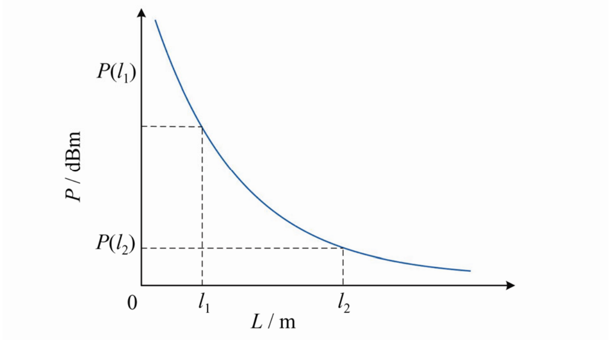

Fig. 4 Attenuation law of signal in wired medium

dBm: Decibel relative to one milliwatt

Its characteristic is

$$-10\lg\frac{P(l_2)}{P(l_1)}=\beta_s(l_2-l_1) \tag{3}$$

In Fig. 4 and Eq. (3), $P(l_1)$ and $P(l_2)$ represent the power of the electromagnetic wave signal at the position of l_1 and l_2 on the conductor $P(l)$, respectively. β_s is the attenuation value per unit length of the conductor. The attenuation value characteristics are determined by the material and structure of the conductor. Let $\alpha(l)$ be the attenuation multiple of the signal power transmitted in the conductor. According to Eq. (3), let $l=l_2-l_1$, and the attenuation multiple of the signal power can be obtained:

$$\alpha(l)=10^{-\frac{\beta_s l}{10}} \tag{4}$$

The system eliminates the artificial noise signal through SI cancellation technology. We define its SI cancellation ability as $H=-10\lg\lambda$, where λ is the residual factor of SI. If $H=20$ dB, it can be seen that $\lambda=10^{-2}$, and the residual artificial noise power after SI cancellation is λP_{N_a} and λP_{N_b}.

According to Eqs. (2), (4) and SI cancellation ability *H*, the signal powers received by Alice and Bob are:

$$P_A=\alpha_P\alpha(L)P_{S_b}+\lambda\alpha_P P_{N_a}+N_0 \tag{5a}$$

$$P_B=\alpha_P\alpha(L)P_{S_a}+\lambda\alpha_P P_{N_b}+N_0 \tag{5b}$$

At the eavesdropping position $x(0\leqslant x\leqslant L)$, the power of Eve eavesdropping on the signals sent by Alice and Bob can be expressed as:

$$P_{E1}=\alpha_P\alpha(L-x)P_{S_b}+\alpha_P\alpha(x)P_{N_a}+N_0 \tag{6a}$$

$$P_{E2}=\alpha_P\alpha(x)P_{S_a}+\alpha_P\alpha(L-x)P_{N_b}+N_0 \tag{6b}$$

According to (5a), (5b) and Shannon's law, the communication capacity of Alice and Bob legal channels are

$$C_{\mathrm{A}} = w_2 \log_2 \left(\frac{\alpha_{\mathrm{P}} \alpha(L) P_{S_{\mathrm{b}}}}{\lambda \alpha_{\mathrm{P}} P_{N_{\mathrm{a}}} + N_0} + 1\right) \tag{7a}$$

$$C_{\mathrm{B}} = w_1 \log_2 \left(\frac{\alpha_{\mathrm{P}} \alpha(L) P_{S_{\mathrm{a}}}}{\lambda \alpha_{\mathrm{P}} P_{N_{\mathrm{b}}} + N_0} + 1\right) \tag{7b}$$

where w_1 and w_2 are the bandwidths of local oscillation signals f_1 and f_2, respectively.

According to (6a), (6b) and Shannon's law, the communication capacity of Eve eavesdropping channels are:

$$C_{\mathrm{E1}} = w_2 \log_2 \left(\frac{\alpha_{\mathrm{P}} \alpha(L-x) P_{S_{\mathrm{b}}}}{\alpha_{\mathrm{P}} \alpha(x) P_{N_{\mathrm{a}}} + N_0} + 1\right) \tag{8a}$$

$$C_{\mathrm{E2}} = w_1 \log_2 \left(\frac{\alpha_{\mathrm{P}} \alpha(x) P_{S_{\mathrm{a}}}}{\alpha_{\mathrm{P}} \alpha(L-x) P_{N_{\mathrm{b}}} + N_0} + 1\right) \tag{8b}$$

When conditions are met:

$$C_{\mathrm{S}} = \begin{cases} C_{\mathrm{A}} - C_{\mathrm{E1}} > 0 \\ C_{\mathrm{B}} - C_{\mathrm{E2}} > 0 \end{cases} \tag{9}$$

It can be seen that absolutely secure communication can be achieved for any eavesdropping position x.

From the perspective of Eve, when the eavesdropping position is $x = L$, it is the optimal eavesdropping point for eavesdropping Bob to send the target signal S_{b2}, and when the eavesdropping position is $x = 0$, it is the optimal eavesdropping point for eavesdropping Alice to send the target signal S_{a1}. At the optimal eavesdropping point, the attenuation of the target signal is the weakest and the attenuation of the artificial noise signal is the strongest. At this time, the communication capacity of the eavesdropping channel reaches the maximum and the system security capacity is at the minimum. Therefore, it can be seen that the maximum communication capacity of the eavesdropping channel is:

$$C_{\mathrm{E1}}^{x=L} = w_2 \log_2 \left(\frac{\alpha_{\mathrm{P}} P_{S_{\mathrm{b}}}}{\alpha_{\mathrm{P}} \alpha(L) P_{N_{\mathrm{a}}} + N_0} + 1\right) \tag{10a}$$

$$C_{\mathrm{E2}}^{x=0} = w_1 \log_2 \left(\frac{\alpha_{\mathrm{P}} P_{S_{\mathrm{a}}}}{\alpha_{\mathrm{P}} \alpha(L) P_{N_{\mathrm{b}}} + N_0} + 1\right) \tag{10b}$$

The system security capacity shall meet the formula:

$$C_{\mathrm{A}} > C_{\mathrm{E1}}^{x=L} \tag{11a}$$

$$C_{\mathrm{B}} > C_{\mathrm{E2}}^{x=0} \tag{11b}$$

Then the wire-line communication system can realize absolutely secure communication. Formulas (7a), (10a), and (11a) are derived to satisfy the following relationship:

$$\lambda < \alpha^2(L) \tag{12}$$

By substituting into Eq. (4) and the definition of SI cancellation capability *H*:

$$H > 2\beta_{\mathrm{s}} L \tag{13}$$

Formula (13) reflects the conditions that must be met to realize absolutely secure communication in wire-line communication system, that is, the premise of realizing absolutely secure communication is that the SI cancellation ability is at least twice the total attenuation value of the conductor.

3 Simulation Results and Analysis

According to the theoretical analysis and formula derivation of the above system security capacity, the system security capacity has the strongest correlation with factors such as SI cancellation ability and conductor attenuation characteristics. Next, by setting simulation parameters, the corresponding relationship between system security capacity and relevant parameters in telephone secure communication system is further analyzed. The relevant parameter settings involved in the simulation process are shown in Table 1.

Table 1 Channel capacity simulation parameter setting

Parameter	Set value
$P_{S_{\mathrm{a}}}, P_{S_{\mathrm{b}}}$	10 dBm
$P_{N_{\mathrm{a}}}, P_{N_{\mathrm{b}}}$	12 dBm
w_1, w_2	1 MHz
Thermal noise power spectral density n_0	174 dBm/Hz
N_0	114 dBm
Conductor model	Twisted pair (UTP Cat 5)
Conductor attenuation factor	0.014 87 dB/m
A_{P}	30 dB

According to Eqs. (7a)-(9) and (13), Fig. 5 can be obtained by simulation, in which we set the SI cancellation ability H to be 2.5 times of the total attenuation value of the conductor. The simulation diagram shows the relationship between Eve eavesdropping position and system security capacity when the conductor length is 1 km.

According to the simulation results in Fig. 5, the two curves are symmetrically distributed. For the target signal S_{a1}, the system security capacity gradually increases

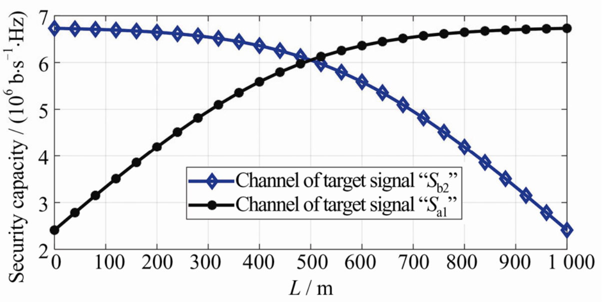

Fig. 5 Relationship between eavesdropping location and channel security capacity

as the Eve eavesdropping position is far away from Alice. The reason for this trend is that when $x=0$, the attenuation of the target signal is the smallest, while the attenuation of the artificial noise signal is the most severe, resulting in the maximum communication capacity and the minimum system security capacity of the Eve eavesdropping channel. As the eavesdropping location is far away from Alice, the attenuation of the target signal becomes more and more serious, but the attenuation of the artificial noise signal becomes weaker, resulting in the gradual reduction of the SNR of Eve and the communication capacity of the eavesdropping channel, and the gradual increase of the system security capacity; When Eve eavesdropping capacity tends to zero, the system security capacity curve tends to be flat, that is, the system security capacity is close to the communication capacity of Bob. The analysis of S_{b2} curve of target signal is the same.

According to Eqs. (7b), (8b), (9) and (13), Fig. 6 can be simulated, in which the SI cancellation capability H is set to be 2.5, 3 and 3.5 times of the total attenuation value of the conductor.

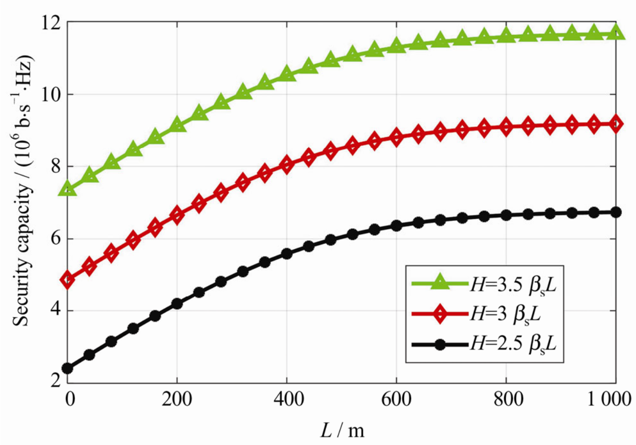

Fig. 6 Relationship between SI cancellation ability and security capacity

The simulation diagram shows the relationship between Eve eavesdropping position, SI cancellation capability H and system security capacity when Alice transmits target signal S_{a1} to Bob and the wire length is 1 km. The simulation results in Fig. 6 show that the stronger the SI cancellation ability of Bob, the greater the system security capacity, that is, the more secure the wire-line communication system. The simulation curve clearly shows that when the SI capability H differs by the same times of the total attenuation value of the conductor, the two adjacent curves are parallel and differ by the same value. This result can effectively know the actual development and application evaluation of the wire-line communication system.

4 Conclusion

This paper presents a wire-line secure communication system based on the co-frequency co-time SI cancellation technology, and studies the problem of absolutely secure communication in the process of wire-line communication. Through CCFD technology, Alice sends the target signal, and Bob releases the artificial noise signal to the channel through the noise generator, so that it can effectively interfere with the target signal in the communication process, ensure that the wire-line communication system can realize secure communication, and make Bob only receive the target signal through the SIC. As the saying goes, "Knowing yourself and the enemy is invincible in a hundred battles", we study the effect of eavesdropping from the perspective of Eve, that is, the state of system security capacity when Eve eavesdropping at any point of the conductor. The research work shows that Eve can be effectively prevented from eavesdropping through artificial noise signal and SI cancellation technology, and the SI cancellation ability can directly affect the security capacity of the system. We deduce the expression of the system security capacity, and analyze the relationship between the system security capacity, wire length, Eve eavesdropping point position and SI cancellation ability through simulation, so as to obtain the absolute confidential communication effect of the system.

References

[1] Pan J S, Kong S P, Cheng S. Analysis and research on security of DES encryption algorithm [J]. *Cyberspace*

Security, 2020, **11**(4): 104-107(Ch).

[2] Yang J. Design and implementation of an AES algorithm encrypted transmission system [J]. *Electronic Design Engineering*, 2019, **27**(3): 123-126+131(Ch).

[3] Wyner A D. The wire-tap channel [J]. *Bell System Technical Journal*, 1975, **54**(8): 1355-1387.

[4] Shannon C E. Communication theory of secrecy systems [J]. *Bell System Technology Journal*, 1949, **28**(4): 656-715.

[5] Liu Z S, Wang J, Sun R, *et al*. Overview of physical layer security technology in wireless communication [J]. *Communications Technology*, 2014, **47**(2): 128-135(Ch).

[6] Huang K Z, Jin L, Zhong Z. 5G physical layer security technology Promoting security by communication [J]. *ZTE Technology*, 2019, **25**(4): 43-49(Ch).

[7] Tang Y Q, Li W, Zhang L J, *et al*. Endogenous secure communication technology based on characteristics of wireless channel [J]. *Radio Communication Technology*, 2020, **46**(2): 159-167(Ch).

[8] Goel S, Negi R. Guaranteeing secrecy using artificial noise [J]. *IEEE Transactions on Wireless Communications*, 2008, **7**(6): 2180-2189.

[9] Li W, Ghogho M, Chen B, *et al*. Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis [J]. *IEEE Communications Letters*, 2012, **16**(10): 1628-1631.

[10] Zhou Y K, Zhu Y, Li F B, *et al*. Securing communication via transmission of artificial noise by both sides: Bipolar-Beamforming optimization [J]. *Mathematical Problems in Engineering*, 2013, **18**(5): 708-716(Ch).

[11] Zhou Y K, Xiang Z Z, Zhu Y, *et al*. Application of full-duplex wireless technique into secure MIMO communication: Achievable secrecy rate based optimization [J]. *IEEE Signal Processing Letters*, 2014, **21**(7): 804-808.

[12] Zhang J H, Liu S J, Ma M, *et al*. Research on a wired secure communication method based on artificial noise [J]. *Research on Information Security*, 2017, **3**(8): 686-691(Ch).

[13] Jiao B L, Ma M. Analysis of the co-frequency co-time full duplex technology [J]. *Telecommunication Network Technology*, 2013(11): 29-32(Ch).

[14] Pinto P C, Barros J, Win M Z. Wireless physical-layer security: The case of colluding eavesdroppers [C] // *IEEE International Symposium on Information Theory*. Piscataway: IEEE, 2009: 2442-2446.

□