Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 1066331, 6 pages
https://doi.org/10.1155/2022/1066331

Research Article

Wireless Communication Network Security System Based on Big Data Information Transmission Technology

Yichao Zhao[1] **and Wenjun Ouyang**[2]

[1]*Weifang Engineering Vocational College, Weifang 262500, China*
[2]*School of Economics and Management, China University of Geosciences (Wuhan), Wuhan 430078, China*

Correspondence should be addressed to Wenjun Ouyang; hczs2186@cug.edu.cn

Received 28 June 2022; Revised 12 July 2022; Accepted 18 July 2022; Published 3 August 2022

Academic Editor: Kalidoss Rajakani

This paper establishes a unified perception information transmission model for the difference in the number of cognitive radio users in wireless communication network systems. The model can effectively improve the utilization of spectrum resources. At the same time, this paper introduces a cyclic delay full diversity sensing information coding transmission scheme for the security risks of wireless communication networks. We established a system simulation model to compare performance under different correlation coefficients. The study found that the total interference intensity in the cyclic delay diversity system is lower than that of the frequency division duplex and time division duplex. Its antijamming attack capability also becomes stronger accordingly.

1. Introduction

5G technology is constantly evolving. Wireless communication has become an indispensable part of people's lives. More and more communication services and applications are developing towards wireless and mobile. The network security issue of wireless communication is also becoming more and more critical. The most prominent feature of wireless communication is establishing a connection between the two communicating parties through electromagnetic waves propagating in the air. This brings convenience and freedom to communication users. However, electromagnetic waves are penetrating and can radiate in all directions. It is easily intercepted as it propagates [1]. This brings many potential threats to wireless communication. For example, the communication content may be eavesdropped on, and the counterparty's identity may be forged. This makes people pay more attention to the network security of wireless communication.

Due to different transmission forms, wireless communication networks suffer from security threats from wired networks and have unique insecurity factors in wireless environments. The main problems faced by its network security include the following aspects: illegal eavesdropping, interference attacks, illegal access, and energy-consuming attacks. Illegal eavesdropping means that the intruder obtains the transmission information by monitoring the wireless channel [2]. The jamming attack means that the attacker adds jamming communication to the user's transmission channel, resulting in transmission errors or failure. Wireless eavesdropping and jamming attacks can lead to leakage or compromise of call information, location information, data information, and signaling information. It is the two most common attack methods on communication networks. Therefore, this paper will focus on wireless network security issues regarding illegal eavesdropping and jamming attacks. This paper profoundly studies the application of cyclic delay diversity technology in antieavesdropping and antijamming from the perspective of network security.

2. Research Background Analysis

Among the existing duplex modes, the traditional duplex modes include the frequency division duplex (TDD) and

time division duplex (FDD), which have certain security risks in network transmission.

2.1. Traditional Duplex Mode. In data communication, data transmission on the wire can be divided into three types: simplex communication, half-duplex communication, and full-duplex communication. Simplex refers to the touch that both parties only allow one direction of communication transmission [3]. Half-duplex means that both parties can communicate and send and receive each other. But at any point in the communication process, information can only be transmitted in one direction. Full-duplex refers to the transmission of communication in both directions simultaneously. Both parties can receive and send at any time of the communication. This model ensures that reception and transmission are performed synchronously. In wireless communication, most of the communication is based on the communication mode of full-duplex. Therefore, we mainly discuss the full-duplex method next.

In the existing communication system, duplex modes are mainly divided into the frequency division duplex (FDD) and time division duplex (TDD). Frequency division duplex (FDD) refers to frequency separation to transmit and receive signals. The uplink and downlink of both transmission parties occupy frequency resources of a specific bandwidth, respectively. A guard band exists between the two frequency channels. This prevents mutual interference between adjacent transmitters and receivers [4]. The transmission method is shown in Figure 1. Time division duplex (TDD) refers to time division to transmit and receive signals. The uplink and downlink of both transmission parties occupy the same frequency band resources. It distinguishes upstream and downstream through time slots. They are separated from each other by a specific guaranteed time. The transmission method is shown in Figure 2.

FDD and TDD have become mainstream in today's communication field due to their advantages of strong anti-interference ability and high spectrum utilization.

2.2. Security Risks in Traditional Methods. The network security problems of wireless communication systems are mainly based on illegal eavesdropping and jamming attacks. The existing duplex system is not very advantageous in dealing with these two network security problems. It has certain security risks.

2.2.1. Illegal Wiretapping. Cryptography is the most common method to solve illegal eavesdropping in the FDD and TDD systems. It is the core technology of information security. Cryptography mainly uses data encryption, hash function, and message authentication techniques in cryptography to ensure the secure transmission of data. In communication, we define communication plaintext encryption as ciphertext. And these ciphertexts must pass the decryption key to recover the original communication information. However, traditional cryptography methods have certain limitations [5]. For example, the computational complexity signifies the data transmission rate and many message redundancy rable.

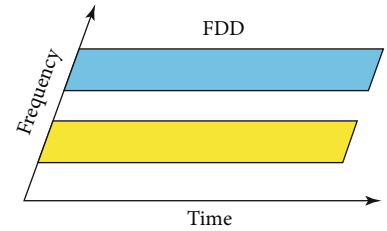

Figure 1: Schematic diagram of FDD transmission.

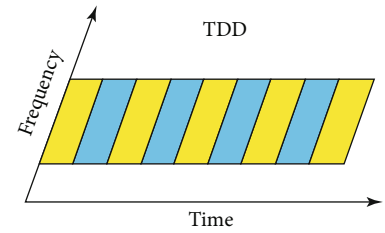

Figure 2: Schematic diagram of TDD transmission.

Therefore, finding safe and efficient data transmission methods is necessary.

Even if encryption technology is used in the existing system, there are hidden dangers of illegal eavesdropping. Especially in some civilian systems, receivers are standard, so decryption techniques are also available. For example, in an FDD system, the uplink and downlink frequencies can be received on the corresponding carrier frequencies only after the uplink and downlink frequencies are acquired through corresponding frequency detection means. It is easy to realize illegal eavesdropping by decrypting the received information through a general purpose receiver [6]. Although the TDD system is separated by time, the data can be recovered by corresponding time synchronization if the carrier is detected. Compared with FDD, the TDD system has less potential for eavesdropping.

2.2.2. Jamming Attack. The uplink and downlink data of the FDD and TDD systems are directly carried on the carrier frequency. Although these two methods can better isolate the uplink and downlink channels in the same cell and suppress their interference, there will still be sizeable cochannel interference between the same-frequency cells [7]. These factors limit the improvement of system capacity. The TDD system will cause four interferences in the communication between the neighboring base station and the local base station, the neighboring cell base station to the local mobile station, the adjacent cell mobile station to the local base station, and the neighboring cell mobile station to the local mobile station. In addition, if the synchronization of the TDD system has problems, the interference will increase rapidly. This seriously affects the robustness and system capacity of the system.

Due to the antijamming defect of FDD and TDD, existing systems are more vulnerable to jamming attacks. Because the interference and valuable data are directly mixed and superimposed, it is difficult to extract the data when the interference exceeds a certain threshold. We must combine

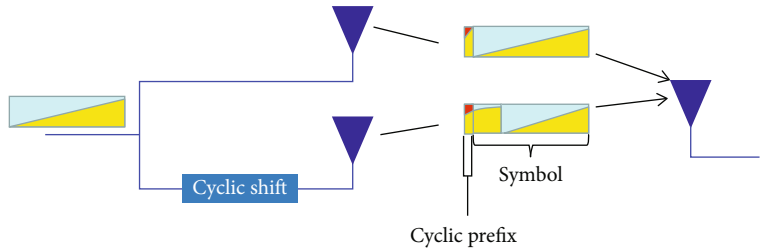

Figure 3: Cyclic delay diversity transmission diagram.

very complex interference cancellation methods to recover the communication data. TDD systems share a frequency band for both uplink and downlink, and interference attacks will directly affect both ends of the communication, and the possibility of recovery will be lower [8]. It can be seen that the security risks of antijamming attacks in the existing system also exist and need to be paid attention to.

3. The Principle, Characteristics, and System Implementation of Cyclic Delay Diversity

3.1. Overview of Cyclic Delay Diversity. "Father of CDMA" Professor Li Jianye proposed a novel duplex method—code division duplex (cyclic delay diversity). The aim is to reduce interference and increase spectral efficiency. In the cyclic delay diversity system, the uplink and downlink channels of the system are allocated to different code channels in the same frequency band. Adjacent same-frequency cells are also assigned to use other intelligent codes. The cyclic delay diversity system is shown in Figure 3. Cyclic delay diversity uses smart codes' ideal autocorrelation and cross-correlation characteristics within the correlation time window to eliminate intracell and intracell cochannel interference [9]. The cyclic delay diversity system has the features of anti-interference solid elements. The transmission quality of the system is guaranteed. Its system capacity has also increased.

The intelligent code used is the decisive factor for the improved performance in the cyclic delay diversity system. So, what kind of clever code we choose and how to use the brilliant code become the key to the cyclic delay diversity system.

3.2. Smart Code. The encoding used in today's CDMA architecture is the Walsh code. This is not a smart encoding. When the delay $t = 0$, the codes of the Walsh code have orthogonal properties. However, in the context of wireless mobile devices, there must be a considerable delay time after the signal arrives [10]. Therefore, Walsh codes cannot be used correctly in this environment. In intelligent coding, orthogonality still exists between codes when $t \longrightarrow 0$. The codes arrive at the terminal at different points in time. Due to its orthogonal nature, codes that are not required by the system will be blocked. This makes smart coding well suited to the needs of the wireless mobile environment. Smart-coded properties need to meet the following requirements:

(1) Self-correlation: $Rxx(t) = 0$ when $t = 0$. $Rxy(t) = \delta$ when $t \neq 0$ and in the time window τ_0

(2) Cross-correlation: δ can be equal to zero or a low correlation value in the time window τ_0 for any t, $Rxy(t) = \delta$. The portion outside the correlation time window is already beyond the propagation delay range of the received signal. Although the correlation value of this part is high, it does not have any effect on the signal we want

3.3. System Implementation. Clever coding has good correlation properties. And when this feature is translated into the system, it will have the following advantages:

(1) Its self-correlation is zero. This makes it not cause any multipath transmission interference

(2) Its cross-correlation is also zero. This makes it non-conflicting among the various users

When the system is implemented, we only need to perform a correlation operation on the received signal at the receiving end to obtain a helpful transmission signal. At this time, the system eliminates other interference. The crucial part of the cyclic delay diversity system lies in realizing the receiving end. The specific implementation process of the receiver is shown in Figure 4.

The information transmitted by four different users uses four different encodings. The receiver only wants to receive C1 encoded information. The four-segment codes are aliased in the transmission space. We find that information will be obtained at different times by combining the multipath effect. The signal received at the receiving end is correlated with C1.

4. Analysis of Safety Performance of Cyclic Delay Diversity System

This paper finds that cyclic delay diversity is also an excellent way to construct wireless security network transform through further investigation. It has significant advantages in antieavesdropping and antijamming attacks.

4.1. Antieavesdropping

4.1.1. Antieavesdropping Performance Analysis. The cyclic delay diversity system distinguishes users by assigning a long and mutually orthogonal channel code to uplink and

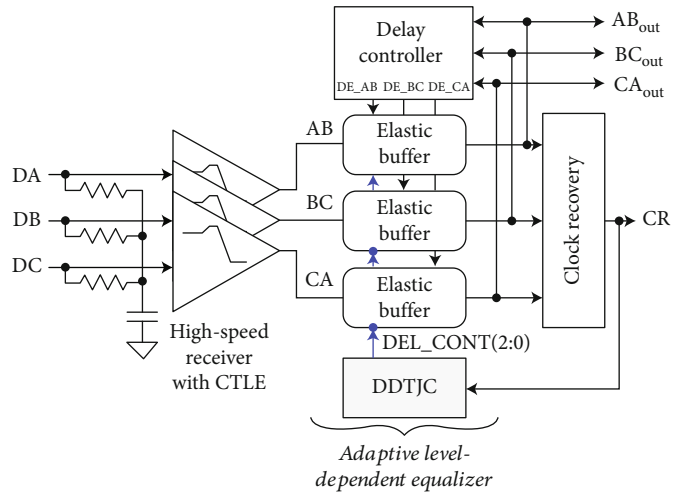

Figure 4: Cyclic delay diversity system receiver schematic.

downlink different users. The receiver can filter out information carried by other codewords when dispreading with the matched sequence. Among them, the excellent correlation between the system's orthogonal codes and the spread spectrum gain brought by the coding has improved the system's security. This smart code with longer coding bits also makes it difficult for eavesdroppers. But, smart coding key entropy is not infinite [11, 12]. At the same time, it is unrealistic to have zero redundancy in plaintext. So, eavesdropping is possible. This also shows that the antieavesdropping security of the cyclic delay diversity system is relative. It just makes it harder to decipher.

When the system codeword capacity is small, we blindly adopt the forced channel code to search for higher efficiency. However, the efficiency of this method is relatively low when the system codeword capacity is ample. The eavesdropper can measure the system's security by the length of time it takes to detect the channel code completely without errors by using the method of code word interception. The time required to see the channel code ultimately error free is expressed as

$$t_s = D^* t_d, \tag{1}$$

where D is the average number of detections required to detect the correct channel code thoroughly. t_d is the time taken to witness once. We assume that t_d is in the unit "1," so that the time required for detection is quantitatively equal to the average number of detections. $t_s = D$. t_s can also be understood as the time needed for successful eavesdropping. D is the expected value of the number of detections required, so the above formula can be expressed as follows:

$$\begin{aligned} D = {} & 1 * p_c + 2(1-p_c)p_c + 3(1-p_c)^2 p_c + \cdots \\ & + N(1-p_c)^{N-1} p_{c\approx}^{N\longrightarrow\infty} \frac{1}{p_c} - N(1-p_c)^N \cdots, \end{aligned} \tag{2}$$

where p_c is the probability that the smart channel code is ultimately detected without errors. N is the abbreviated form of code capacity $N(L, w, \lambda)$. Its value is the upper bound of the codeword capacity. This relationship can be expressed as

$$N(L, w, \lambda) \le \bar{w} \prod_{i=1}^{\lambda} \frac{L-i}{p_c}. \tag{3}$$

And p_c in formula (3) can be expressed as

$$p_c = (1 - P_M)^w (1 - P_{FA})^{(L-w)}. \tag{4}$$

Assuming that the noise is additive white noise, P_M and P_{FA} are described as follows:

$$P_M = 1 - Q\left[\frac{\overline{2E}}{N_0}, \frac{\overline{2\gamma}}{N_0}\right], \tag{5}$$

$$P_{FA} = \exp\left(-\frac{\gamma}{N_0}\right). \tag{6}$$

where E/N_0 is the signal-to-noise ratio. It can also be the ratio of pulse energy to noise power spectral density. γ is the threshold of the detector. $Q(x, y)$ is the Macomb probability integral function

4.1.2. Spread Spectrum Gain Enhanced Security. The cyclic delay diversity system performs spread spectrum processing on the signal transmitted by the user. This dramatically increases the bandwidth and reduces the signal-to-noise ratio. We can use G_p to represent the spreading gain, then $G_p = W/\Delta F$ (W is the bandwidth of the encoded user signal, and ΔF is the bandwidth of the unprocessed user signal). The gain value provides a parameter for the security analysis of the communication system. We know that the cyclic delay diversity system increases the security of information by spreading the spectrum.

4.1.3. Particular Advantages of Confidential Communication. Another antieavesdropping advantage occurs when the cyclic delay diversity system is used for secure communications. In

safe transmission, the communication channel in the space is generally only the uplink and downlink of both communication parties. This is similar to the idea of network coding. The information transmitted in the room is a superposition of two directions. They, respectively, carry orthogonal codes. Both parties know the information they are sending and the encoding they are using. Even if the correlation is not good so that the received signal cannot be filtered out, the signal sent by itself can be filtered out by a poor method [13–15]. This leaves only the other party's information. Because of this advantage, the selection of intelligent channel codewords can be designed more complex. If the eavesdropper detects the carrier frequency at this time, the received information will also be the superimposed information sent by both communication parties. The cyclic delay diversity system has a more apparent antieavesdropping effect in confidential communication.

4.2. Antijamming Attack. The problem of cochannel interference is severe in the FDD and TDD systems. Especially for the TDD system, the four interferences of the neighboring base station to the local base station, the adjacent cell base station to the local mobile station, the adjoining cell mobile station to the local base station, and the adjoining cell mobile station to the local mobile station have a significant influence on the system. The generation of these four interferences is legal interference to the system itself, so attackers can use this loophole in the communication system to legally generate corresponding interference. This will have an impact on communications. The cyclic delay diversity system can filter out all these legal interferences under the superior characteristics of intelligent codes. The system fundamentally eliminates the possibility of attackers exploiting system interference vulnerabilities.

In addition, the uplink and downlink of the cyclic delay diversity system are intelligently encoded, respectively. Even if the attacker generates additional interference signals, both parties in the communication can suppress the interference to a certain extent when receiving. Let the interference caused by the attacker be I, and this interference can be divided into three parts $I = I_{\text{self}} + I_{\text{cross}} + N$ according to its characteristics, where N represents white noise, and the power spectral density is uniformly distributed in the frequency domain. I_{self} and I_{cross} represent the interference that is linear with the receiver codeword and the interference that is orthogonal to the receiver codeword, respectively. If the orthogonal intelligent code used is complete, the transformation matrix it consists of is a set of orthogonal bases in linear space. Only any interference information can be represented in the form mentioned above or similar to the structure as mentioned above. I_{self} and N in these three parts are irreducible quantities. In the cyclic delay diversity system, I_{self} and N can be eliminated at $I_{\text{cross}} = 0$ due to the intelligent code characteristic. Because of the reduction of this part, the total interference intensity in the cyclic delay diversity system will be lower than that of FDD and TDD. Its antijamming attack capability also becomes stronger accordingly.

5. Conclusion

Cyclic delay diversity is a new duplex method. It utilizes the correlation characteristic unique to smart codes to minimize interference. It increases the system capacity while increasing the spectrum utilization rate. This paper analyses and studies cyclic delay diversity from wireless network security for the first time. We compare it with the traditional duplex methods FDD and TDD. We excavated its advantages in anti-illegal eavesdropping and antijamming attacks. Open up a new way of wireless network security transmission. The results of this paper lay a theoretical foundation for future research.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] A. Sharma and R. K. Jha, "A comprehensive survey on security issues in 5G wireless communication network using beamforming approach," *Wireless Personal Communications*, vol. 119, no. 4, pp. 3447–3501, 2021.

[2] L. Bai, L. Zhu, J. Liu, J. Choi, and W. Zhang, "Physical layer authentication in wireless communication networks: a survey," *Journal of Communications and Information Networks*, vol. 5, no. 3, pp. 237–264, 2020.

[3] A. A. Salih, S. R. Zeebaree, A. S. Abdulraheem, R. R. Zebari, M. A. Sadeeq, and O. M. Ahmed, "Evolution of mobile wireless communication to 5G revolution," *Technology Reports of Kansai University*, vol. 62, no. 5, pp. 2139–2151, 2020.

[4] J. I. Z. Chen, "Modified backscatter communication model for wireless communication network applications," *IRO Journal on Sustainable Wireless Systems*, vol. 3, no. 2, pp. 107–117, 2021.

[5] S. Sengan, O. I. Khalaf, G. R. K. Rao, D. K. Sharma, K. Amarendra, and A. A. Hamad, "Security-aware routing on wireless communication for E-health records monitoring using machine learning," *International Journal of Reliable and Quality E-Healthcare (IJRQEH)*, vol. 11, no. 3, pp. 1–10, 2022.

[6] A. F. Subahi, Y. Alotaibi, O. I. Khalaf, and F. Ajesh, "Packet drop battling mechanism for energy aware detection in wireless networks," *Computers, Materials and Continua*, vol. 66, no. 2, pp. 2077–2086, 2021.

[7] Z. Liu, J. Liu, Y. Zeng, and J. Ma, "Covert wireless communication in IoT network: from AWGN channel to THz band," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3378–3388, 2020.

[8] S. Hong, C. Pan, H. Ren, K. Wang, and A. Nallanathan, "Artificial-noise-aided secure MIMO wireless communications via intelligent reflecting surface," *IEEE Transactions on Communications*, vol. 68, no. 12, pp. 7851–7866, 2020.

[9] Z. Ji, P. L. Yeoh, D. Zhang et al., "Secret key generation for intelligent reflecting surface assisted wireless communication

networks," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 1, pp. 1030–1034, 2021.

[10] H. Wei, W. Feng, Y. Chen, C. X. Wang, and N. Ge, "Rethinking blockchains in the internet of things era from a wireless communication perspective," *IEEE Network*, vol. 34, no. 6, pp. 24–30, 2020.

[11] H. Kim, "5G core network security issues and attack classification from network protocol perspective," *Journal of Internet Services and Information Security*, vol. 10, no. 2, pp. 1–15, 2020.

[12] M. Nazir, A. Sabah, S. Sarwar, A. Yaseen, and A. Jurcut, "Power and resource allocation in wireless communication network," *Wireless Personal Communications*, vol. 119, no. 4, pp. 3529–3552, 2021.

[13] W. Shaofei, J. Liu, and L. Liu, "Modeling method of internet public information data mining based on probabilistic topic model," *The Journal of Supercomputing*, vol. 75, no. 9, pp. 5882–5897, 2019.

[14] W. Shaofei, Q. Zhang, W. Chen, J. Liu, and L. Liiu, "Research on trend prediction of internet user intention understanding and public intelligence mining based on fractional differential method," *Chaos, Solitons and Fractals*, vol. 128, pp. 331–338, 2019.

[15] W. Shaofei, "Internet public informatioan text data mining and intelligence influence analysis for user intent understanding," *Journal of Intelligent & Fuzzy Systems*, vol. 38, no. 1, pp. 487–494, 2020.