Advances in Computer, Signals and Systems (2022)
Clausius Scientific Press, Canada

DOI: 10.23977/acss.2022.060107
ISSN 2371-8838 Vol. 6 Num. 1

Physical-layer Security from Channel Resolvability

Jiajia Wu, Ming Xu*

College of Information Engineering, Shanghai Maritime University, Shanghai, 201306, China
mingxu@shmtu.edu.cn
**Corresponding author*

Keywords: Physical-layer security, Channel resolvability, Polar code, Hypothesis testing

Abstract: This paper discusses the performance of achieving physical layer security from channel resolvability in terms of secrecy and offers a kind of classification for different detection methods, including conventional hypothesis testing and active hypothesis testing. The difference between them is whether or not the detection time is a random variable. Moreover, this paper has a discussion on the applications of the practical case studies based on polar code from the channel resolvability, such as wireless channels with or without state information, point to point channel with an eavesdropper, multiple access channel with an eavesdropper, and communication networks at the physical layer. The channel resolvability is shown to be a promising method to achieve secrecy and covertness in the physical-layer.

1. Introduction

The fundamentals of physical-layer security schemes for secure communication can be built by exploiting the noise inherent to communication channels generally.

The ubiquitous communication networks with sensitive data can be interfered or tampered by malicious users. The legitimate users wish to convey information covertly and maintain their privacy to avoid attacks [1]. The main cause of information leakage is the attack of the eavesdropper. Since the eavesdropper can silently monitor the communication process between the legitimate users, collect and record valuable operation data for a long time without causing any interruption. Moreover, the eavesdropper can also detect the statistical characteristics of the signal by adopting the signal statistical detection technology based on the prior knowledge of the signals transmitted by the legitimate users, such as frequency range and packet duration.

Physical-layer security can achieve with significant benefits in terms of confidentiality and robustness against the eavesdropper. In this scenario, the legitimate users try to avoid the detection strategy designed by the eavesdropper without changing the statistical characteristics of the signal. The Low Probability Detection (LPD) method is based on the power detection threshold. It assumes that the eavesdropper judges whether legitimate users communicate or not according to the difference of the average symbol energy of the received signal in a unit time slot according to the power detection threshold. Therefore, it can realize the deniable of the information transmission state to the eavesdropper.

The classical physical-layer security schemes are based on capacity-achieving code, whereby reliability and secrecy can be handled jointly by means of appropriate coding schemes [3]. However, the theory of channel resolvability provides an alternative solution for the design of physical-layer security scheme. The notion of channel resolvability is defined as the minimum randomness rate required per channel use in order to generate an input that achieves arbitrarily accurate approximation of the output statistics for any given input process [2].

The main contributions of this paper can be summarized as follows:

1) Providing the systematic investigation of the channel resolvability for physical-layer security in wiretap channel.

2) Discussing the difference between the conventional hypothesis testing and the active hypothesis testing.

3) Presenting the significant potential of the physical-layer security and the channel resolvability with polar codes.

The remainder of the paper is organized as follows. Section 2 provides the related works. In Section 3, fundamentals of physical-layer security are reviewed and two different hypothesis testing is given. Section 4 provides an exhaustive discussion practical case studies based on polar codes. Section 5 summarizes the entire paper.

2. Related Work

Bash *et al*. [4] investigated LPD over quasi-static block fading channel based on deterministic noise model and proved that the amount of information bits that can be reliably transmitted to the receiver with LPD is $O(\sqrt{n})$ bits. The LPD communication problem has been extensively studied and it can be achieved by several aspects, such as spread spectrum communications, information-theoretic secrecy, anonymous communication and cognitive radio. In recently years, the theory of channel resolvability has been explored as an alternative to construct physical-layer security schemes. In [1], a coding scheme based on the channel resolvability is developed to ensure LPD in discrete memoryless channel. It proves that when the channel from the legitimate transmitter to the legitimate receiver is better than that to the eavesdropper, the amount of transmitted information bits satisfies square root law. Besides the case of discrete memoryless channel model, Bloch *et al*. [3] investigated the channel resolvability to formulate reliability conditions and secrecy conditions over arbitrary channel models with cost constraint, including continuous channels and channels with memory. Moreover, it proves that deriving secrecy from the channel resolvability provides stronger secrecy than capacity-achieving code that is based on random coding.

In the case of noise, fading and interference channels, researchers investigated physical-layer security schemes based on the practical coding method rather than random coding. LDPC and turbo codes with good performance have been widely studied. However, they may still have the problem of error floor. Arikan *et al*. [5] proposed the polar codes which is proved the achievability of Shannon limit, and polar codes can not be affected by the error floor. In [6], polar codes have been proved to be an alternative that hold for channel resolvability and any results obtained from random binning in random coding, such as reliability condition and privacy amplification. In [7], a covert communication scheme is proposed using polar codes and multilevel coding to achieve the covert capacity. In each level, a negligible randomness rate can be derived to satisfy the channel resolvability conditions. The error probability and information leakage rate decay fast with the code length.

3. System Model and Adversary Model

This section introduces the system model and the adversary model.

3.1. System Model

Considering a scenario where a legitimate transmitter X (Alice) sends information to a legitimate receiver Y (Bob) while avoiding the detection by an eavesdropper Z (Willie). Bob obtains the estimate $\hat{X}$ using a decoder. The sequence $X^n = \{X_1, X_2, ..., X_n\}$, where n denotes the code length. The lowercase x^n denotes the values of a random variable sequence. The error probability can be expressed as $P_e = \lim_{n\to\infty}[\hat{X}^n \neq X^n]$.

The joint probability distribution on random variables $X^n \times Y^n$ can be expressed as

$$P_{X^nY^n}(x^n, y^n) = P_{X^n}(x^n)P_{Y^n|X^n}(y^n \mid x^n), \tag{1}$$

Therefore, the mutual information between X^n and Y^n is

$$I(X^n;Y^n) = \log\frac{P_{X^nY^n}(x^n, y^n)}{P_{X^n}(x^n)P_{Y^n}(y^n)} , \tag{2}$$

where the distribution of $\frac{1}{n}I(X^n;Y^n)$ denotes the information spectrum. For all $\gamma > 0$ and sufficiently large n, the channel resolvability for secrecy in wiretap channel is given by [3]

$$R_n \geq \limsup_{n\to\infty}\frac{1}{n}I(X^n;Z^n \mid U^n) + \gamma, \tag{3}$$

where R_n refers to the rate to randomize the encoding of the information M^n that Alice sends to Bob. $U^n \to X^n \to \{Y^n, Z^n\}$ forms a Markov chain. Thus, we can obtain $\lim_{n\to\infty}\mathbb{E}[S_n] \leq \xi$, and $\xi > 0$. The strong secrecy S_n can be expressed as

$$S_n = \mathbb{V}(P_{M^nZ^n}, P_{M^n}P_{Z^n}). \tag{4}$$

3.2. Adversary Model

Considering an adversary model where the legitimate transmitter Alice transmits information to the legitimate receiver Bob, and the eavesdropper Willie is hidden somewhere. The legitimate parties hope to realize covert communication based on physical-layer security schemes. We assume that Willie uses a hypothesis testing method to make the best decision on the communication state of the legitimate parties obeying the information theory analysis. If the detection result shows that there is no communication between the legitimate parties, no further attacks will be carried out. On the contrary, when the detection result shows that the legitimate parties are communicating, further attacks such as imitation attacks or substitution attacks will be launched. For the eavesdropper Willie, the loss caused by missed detection is more serious than that caused by false alarm.

3.2.1. Conventional Hypothesis Testing

The conventional hypothesis testing ensures that it can be able to detect weak signal from a transmitter due to its robustness to noise uncertainty. However, it requires significantly long detection time to provide reliability [8]. In the conventional hypothesis testing, the detection time is a fixed parameter. In general, the code length or block length can be referred to be the amount of time slots.

We assume that Willie is uncertain about the starting time of Alice's transmission, i.e., Willie can intercept any part from the whole time period through the illegal link for analysis. Define a parameter Ω, $\{\Omega \subseteq \{1,2,...,n\}:|\Omega|=\omega\}$ to denote the channel indices corresponding to the elements in Ω in ascending order. Willie's observation of the codeword X_{Ω}^{n} corresponding to any time period transmitted by Alice is denoted as Z^{Ω}. Since Alice doesn't know the time when Willie's detection starts, Alice needs to maintain covertness from the whole transmission, and $\hat{\omega}=\frac{\omega}{n}$ is called the covertness level.

In a conventional hypothesis testing, the goal is to analyze two possible distributions on the space $\mathcal{X}$,

$$\mathcal{H}_0 : \boldsymbol{Z}^{\Omega} \sim Q_Z^{\otimes\omega} \quad \mathcal{H}_1 : \boldsymbol{Z}^{\Omega} \sim P_{\boldsymbol{Z}},$$

where $\mathcal{H}_0$ denotes the null hypothesis, $\boldsymbol{Z}^{\Omega}$ is distributed according to P, $\mathcal{H}_1$ denotes the alternative hypothesis, $\boldsymbol{Z}^{\Omega}$ is distributed according to Q. Assuming Willie adopts the likelihood ratio test (LRT) method to make the optimal decision on the communication state, and takes the likelihood ratio as the test statistic, which is expressed as

$$\eta=\frac{P_{\boldsymbol{Z}}(z^{\Omega})}{Q_Z^{\otimes\omega}(z^{\Omega})}. \tag{5}$$

Willie sets a detection threshold $d_T > 0$. As a result, Willie's criterion can be described as follows. If $\eta \le d_T$, the null hypothesis $\mathcal{H}_0$ is chosen, Willie determines that the legitimate users does not communicate. On the contrary, if $\eta \ge d_T$, the alternative hypothesis $\mathcal{H}_1$ is chosen, Willie determines that the legitimate users does communicate. These two cases can be expressed as

$$z^{\Omega}=\begin{cases} \mathcal{Z}_{\Gamma}^{\Omega}=\{z^{\Omega}:\dfrac{P_{\boldsymbol{Z}}(z^{\Omega})}{Q_Z^{\otimes\omega}(z^{\Omega})}\le d_T\}, & \text{choose } \mathcal{H}_0 \\ (\mathcal{Z}_{\Gamma}^{\Omega})^c=\{z^{\Omega}:\dfrac{P_{\boldsymbol{Z}}(z^{\Omega})}{Q_Z^{\otimes\omega}(z^{\Omega})}> d_T\}, & \text{choose } \mathcal{H}_1 \end{cases}. \tag{6}$$

3.2.2. Active Hypothesis Testing

Chang *et al.* [9] formulate a covert sequential testing such that process of communication between legitimate users keeps undetectable by the eavesdropper at any time before the test stops. In the active hypothesis testing, the detection time is a random variable. It is known that the sequential detection outperforms the fixed-time detection by a very wide margin, which requires one-half to one-third detection time in average.

Suppose the observation $z^i=(z_1,z_1,...,z_i)$ is i.i.d, the likelihood ratio of the observation is defined as

$$\rho(z^i)=\frac{f(z^i\,|\,\mathcal{H}_1)}{f(z^i\,|\,\mathcal{H}_0)}=\prod_{1}^{i}\frac{f(z_i\,|\,\mathcal{H}_1)}{f(z_i\,|\,\mathcal{H}_0)}, \tag{7}$$

where the false alarm probability $\mathbb{P}_{FA}=P\{\rho_0<\rho(z^{1:i-1})<\rho_1,\rho(z^i)>\rho_1\,|\,\mathcal{H}_0\}$, the missed detection probability $\mathbb{P}_{MD}=P\{\rho_0<\rho(z^{1:i-1})<\rho_1,\rho(z^i)<\rho_0\,|\,\mathcal{H}_1\}$. Besides, $\rho_0 \le \mathbb{P}_{MD}/(1-\mathbb{P}_{FA})$, $\rho_1 \ge (1-\mathbb{P}_{MD})/\mathbb{P}_{FA}$. The null hypothesis $\mathcal{H}_0$ is chosen when $\rho(z^i)<\rho_0$, and the alternative hypothesis $\mathcal{H}_1$ is chosen when $\rho(z^i)>\rho_0$. Willie does not make a decision when $\rho_0<\rho(z^i)<\rho_1$. Instead, the dimension of observation $z^i=(z_1,z_1,...,z_i)$ turns to z^{i+1} and the likelihood ratio $\rho(z^{i+1})$ is given by

$$\rho(z^{i+1}) = \prod_{1}^{i} \frac{f(z^{i+1} \mid \mathcal{H}_1)}{f(z^{i+1} \mid \mathcal{H}_0)}. \tag{8}$$

4. Practical Case Studies

Polar code is a practical case that holds for the channel resolvability. Any results obtained from random coding, including reliability condition and privacy amplification, make the particularly practical code design easier. In [7], an explicit low-complexity code construction approach using polar codes is proposed and the covert capacity of a binary-input discrete memoryless channel is derived based on the channel resolvability. The achievability part of resolvability is particularly useful, and coding theorems via resolvability have certain advantages over what is obtained from traditional typicality-based approaches. Moreover, source resolvability is intimately connected to almost-lossless source coding and can be applied to many communication scenarios, including wireless channels with or without state information, point to point channel, multiple access channel with an eavesdropper, and communication network at the physical layer. The design of wiretap codes based on polar codes ensures the physical-layer security.

5. Conclusions

The coding theory of physical layer channel resolvability provides a new solution for the design of confidential communication scheme. For any original signal output statistics of the sender, randomness is introduced in the coding process, such as using the secret-key as the randomness source, so as to realize the confidential communication. Two kinds of classification for different detection methods, including conventional hypothesis testing and active hypothesis testing is introduced in this paper. The difference between them is whether or not the detection time is a random variable. Moreover, this paper made a discussion on the practical case studies based on polar code from the channel resolvability.

The resolvability rate ensured the number of random bits required per channel use in order to generate an input that achieves arbitrarily accurate approximation of the output statistics for any given input process in wireless channels with or without state information, point to point channel with an eavesdropper, multiple access channel with an eavesdropper, and communication networks at the physical layer.

Acknowledgements

Thank the experts and editors for their guidance and suggestions on this paper.

References

[1] Bloch M. R. (2016) Covert Communication Over Noisy Channels: A Resolvability Perspective. IEEE Transactions on Information Theory, 62, 2334-2354

[2] Han T. S. and Verdu S. (1993) Approximation theory of output statistics. IEEE Transactions on Information Theory, 39, 752-772

[3] Bloch M. R. and Laneman J. N. (2013) Strong Secrecy From Channel Resolvability. IEEE Transactions on Information Theory. 59, 8077-8098

[4] Bash B. A., Goeckel D. and Towsley D. (2013) Limits of Reliable Communication with Low Probability of Detection on AWGN Channels. IEEE Journal on Selected Areas in Communications. 31, 1921-1930

[5] Arikan E. (2009) Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels. IEEE Transactions on Information Theory. 55, 3051-3073

[6] Chou R. A. and Bloch M. R. (2016) Polar Coding for the Broadcast Channel With Confidential Messages: A Random Binning Analogy. IEEE Transactions on Information Theory. 62, 2410-2429

[7] Kadampot I. A., Tahmasbi M. and Bloch M. R. (2020) Multilevel-Coded Pulse-Position Modulation for Covert Communications Over Binary-Input Discrete Memoryless Channels. IEEE Transactions on Information Theory. 66, 6001-6023

[8] Choi K. W., Jeon W. S. and Jeong D. G. (2009) Sequential detection of cyclostationary signal for cognitive radio systems. IEEE Transactions on Wireless Communications, 8, 4480-4485

[9] Chang M. C. and Bloch M. R. (2021) Evasive Active Hypothesis Testing. IEEE Journal on Selected Areas in Information Theory. 2, 735-746