Physical-Layer Secret Key Generation in Satellite Communication Systems

Ziye Tang[1,2], Meixiang Zhang[1,2], Sooyoung Kim[2]

[1]Yangzhou University, [2]Jeonbuk National University

[1,2]1689125033@qq.com, [1,2]maehyang@foxmail.com, [2]sookim@jbnu.ac.kr

위성 통신 시스템의 물리 계층 보안 키 생성

탕즈예 [1,2], 장매향 [1,2], 김수영 [2]

[1] 양주대학교, [2] 전북대학교

Abstract

Although physical-layer secret key generation (SKG) has exhibited strong potential in various wireless communication scenarios, its direct application to satellite communication systems remains challenging due to the long coherence time and significant round-trip delays. To address these challenges, we propose a novel SKG scheme using the randomness contained in the transmitted data, eliminating the need for additional probing signals. Simulation results demonstrate that this approach not only introduces sufficient randomness for SKG but also provides lower key disagreement rate (KDR).

Ⅰ. Introduction

In recent years, SKG technology has provided the possibility to solve the perfect secrecy problem. By leveraging the reciprocity, space-time uniqueness, and rapid time-varying characteristics of the wireless channel, both legitimate communication parties can independently generate keys in real-time using the wireless channel as a random source[1].

Randomness is the most important condition to keep perfect security, but in many cases, the coherence time of the wireless channel is comparatively long, which does not promise this condition. In[2], a method for generating randomness was created by changing the antenna mode randomly. However, the direct application of the SKG schemes to the satellite systems will cause serious problems. Because a satellite system is located at an altitude greater than about 500 km, it will have much longer coherence time which results in a reduced rate of secret key generation and low randomness of secret keys[3].

In order to solve these problems, this paper proposes an efficient method to generate secret key for encrypted data transmission in satellite systems. Our method introduces randomness by reusing the transmitted data, assuming that the transmitted data in the previous time frame is shared at the legitimate parties and has sufficient randomness. We simulated the proposed method to verify its performance.

The remainder of the paper is organized as follows. In Section Ⅱ, the system model is described. Section Ⅲ introduces the proposed method. The simulation results are shown in Section Ⅳ, and this paper is concluded in Section Ⅴ.

Ⅱ. System model

We consider a low earth orbit (LEO) satellite system model. In this system, we consider the downlink communications, where the system consists of a LEO satellite (Alice) and a legitimate user (Bob). At the same time, Eve is a passive eavesdropper trying to crack private messages. We consider a Rician block-fading channel between Alice and Bob, which does not change during one coherence time interval.

Assuming the channel reciprocity, the channel state information (CSI) from Alice to Bob denoted as h_{AB} and channel from Bob to Alice denoted as h_{BA} are the same during each coherence interval. To generate secret keys, conventional method relies on the quantization of the correlated information c_A and c_B at Alice and Bob, respectively, as shown in (1) :

$$c_A = h_{BA},\ c_B = h_{AB} + n_B \tag{1}$$

where $n_B \sim CN(0,\ \sigma^2)$ denotes the channel estimation error with Gaussian distribution at Bob.

Ⅲ. Proposed method

We propose an efficient SKG scheme for satellite communication systems, which generates the secret keys using the previously transmitted data to introduce randomness.

Firstly, in the initial frame, the secret key for encryption is initialized to zero. Initial data information at Alice and Bob are prepared to introduce randomness. Then, for each data transmission frame, Alice and Bob obtain channel estimates firstly. The data information transmitted in the previous frame are modulated to be QPSK symbols denoted as x. Next, the correlated information c_A and c_B are generated by adding the modulated symbol of the previous data information to the channel estimates, which can be represented as follows:

$$c_A = x + h_{BA}, \; c_B = x + h_{AB} + n_B \tag{2}$$

where $n_B \sim CN(0, \sigma^2)$ denotes the channel estimation error with Gaussian distribution at Bob. Next, Alice quantizes c_A to obtain initial secret key, while Bob estimates LLR of c_B. Finally, information reconciliation and privacy amplification are performed to generate the secret keys for encryption and decryption.

Ⅳ. Simulation results

We evaluate the KDR performance of the proposed SKG scheme and validate the improvement by using simulation result. For the LEO satellite system, we consider the LEO satellite orbit altitude is 500 km, and the maximum Doppler shift is about 51 KHz. In this case, we can transmit 20 bits in each coherence time with the data transmission rate of 1 Mbps. For the conventional method, we use independent random signals to compose a shared randomness as (1) and (2). In the simulation, we assume perfect channel reciprocity. For the information reconciliation, we employ polar codes with different codeword length and information length.

The KDR performances are compared according to signal to noise ratio (SNR) of the channel. As shown in Fig. 1., we compare the performance of the proposed SKG method with the conventional method. The application of polar codes significantly contributes to enhanced performance and the KDR performance improves with longer codeword length. The proposed method achieves much lower KDR compared to the conventional method.

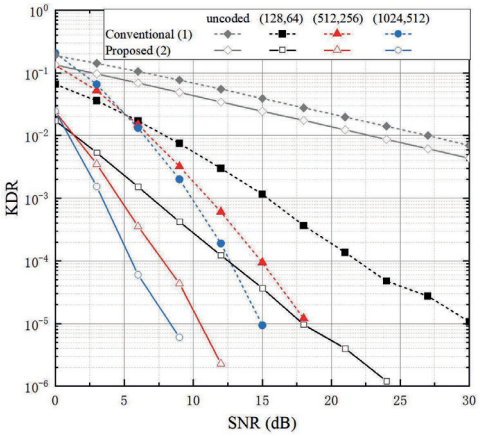

Fig. 1: KDR comparisons among various codeword lengths.

Ⅴ. Conclusion

In this paper, we proposed a novel SKG scheme using data information as random signals to generate secret keys for data encryption transmission in LEO satellite systems. The simulation results show that the proposed method outperforms the conventional method in terms of KDR.

ACKNOWLEDGMENT

This research was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MIST) (RS-2024-00459799).

REFERENCES

[1] M. Zhang, Z. Zhuang and S. Kim, "IRS-assisted hybrid secret key generation," *Symmetry*, vol. 15, no. 10, pp.1906, 2023.

[2] Y. Pan, Z. Xu, M. Li and L. Lazos, "Man-in-the-middle attack resistant secret key generation via channel randomization," *Proceedings of the Twenty-second International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing*, pp. 231 - 240, 2021.

[3] Y. Hao, P. Mu, H. Wang and L. Jin, "Key generation method based on multi-satellite cooperation and random perturbation," *Entropy*, vol. 23, no. 12, pp.1653, 2021.