Evaluation on performance enhancement for secret key generation

Meixiang Zhang°, Ziqing Wang°,*, and Sooyoung Kim*

°Yangzhou University, *Jeonbuk National University.

maehyang@foxmail.com, ziqingang@foxmail.com, *sookim@jbnu.ac.kr

보안 키 생성을 위한 성능 향상 기법 평가

장매향 °, 왕자청 °,*, 김수영*

° 양주대학교, *전북대학교

Abstract

This paper presents a generalized system model for secret key generation, and evaluates the performance of various modulation schemes and post processing methods. Simulation results demonstrated that performance can be improved by fuzzy extraction. In addition, the proposed scheme does not degrade the secret key rate for QAM because no information leaked from the amplitude of the modulated symbol.

Ⅰ. Introduction

The main research direction of channel-based physical layer security is Secret Key Generation (SKG). Physical layer security of wireless communications is being increasingly significant, as a wide range of new applications have emerged. To improve the performance, the fuzzy secret key generation scheme has been proposed [1]. However, the eavesdropper may obtain some information from the amplitude of the constellation points. To this end, we present a system model which can be further generalized to many cases.

Ⅱ. System model

The SKG system includes channel estimation, post processing, constellation rotation and expansion, and key reconciliation. Firstly, legitimate users Alice and Bob take turns sending pilot signals to each other and estimate their channels, $\hat{h}_A$ and $\hat{h}_B$, respectively, using minimum mean square error (MMSE) method [2]. Representing the channels from Alice to Bob, and from Bob to Alice, as h_{AB} and h_{BA}, respectively, the channel estimates at Alice and Bob can be expressed as:

$$\hat{h}_A = h_{BA} + n_A, \quad (1)$$

$$\hat{h}_B = h_{AB} + n_B, \quad (2)$$

where $n_A \sim CN(0,\sigma^2)$ and $n_B \sim CN(0,\sigma^2)$ are the additive white Gaussian noise (AWGN) at Alice and Bob, respectively. Due to the channel reciprocity, we have $h_{AB} = h_{BA} = h$.

Afterwards, post processing on the estimated channels is performed for performance improvement before features extraction, and we denote the processed result as $\tilde{h}_A$ and $\tilde{h}_B$, respectively. Meanwhile, Alice randomly generates secret key bits K_A, and performs encoding and modulation to obtain the modulated symbol s_A. Then, s_A is expanded and rotated by $\tilde{h}_A$ using the following equation:

$$x_A = \tilde{h}_A s_A. \quad (3)$$

After passing through the channel, the received signal at Bob is represented as:

$$y_B = x_A + n_B = \tilde{h}_A s_A + n_B. \quad (4)$$

Bob expands and rotates the received information with $\tilde{h}_B$, resulting in s_B as follows:

$$\begin{aligned} s_B &= \frac{\tilde{h}_B^*}{|\tilde{h}_B|^2} y_B = \frac{\tilde{h}_B^*}{|\tilde{h}_B|^2}\left(\hat{h}_A s_A + n_B\right) \\ &= \frac{\tilde{h}_B^* \hat{h}_A}{|\tilde{h}_B|^2} s_A + \frac{\tilde{h}_B^*}{|\tilde{h}_B|^2} n_B \\ &= \frac{|\tilde{h}_B| \cdot e^{-i\emptyset_{\tilde{h}_B}} \cdot |\hat{h}_A| e^{i\emptyset_{\hat{h}_A}}}{|\tilde{h}_B|^2} s_A + \frac{\tilde{h}_B^*}{|\tilde{h}_B|^2} n_B \\ &= \frac{|\hat{h}_A|}{|\tilde{h}_B|} e^{j\left(\emptyset_{\hat{h}_A} - \emptyset_{\tilde{h}_B}\right)} s_A + \frac{\tilde{h}_B^*}{|\tilde{h}_B|^2} n_B \\ &\approx s_A + n_B' \end{aligned} \quad (5)$$

where $|h|$ and $\emptyset_h$ represent the amplitude and phase of the estimated channels, and $n_B' \sim CN(0, \sigma'^2)$ is the AWGN. Afterwards, demodulation and decoding are performed sequentially to obtain the secret key K_B.

The following summarize the special cases of the proposed system model: 1) omitting n_B in (4) results in an error free channel; 2) post processing using $\tilde{h}_A = \hat{h}_A$ and $\tilde{h}_B = \hat{h}_B$ (A&P) indicates amplitude and phase extraction; 3) post processing using $\tilde{h}_A = e^{j\emptyset_{\hat{h}_A}}$ and $\tilde{h}_B = e^{j\emptyset_{\hat{h}_B}}$ (P) indicates amplitude and phase extraction. 4) In addition, fuzzy extraction can be used to improve the performance by selecting the estimated channels whose amplitude is greater than a threshold, e.g., $\hat{h}_A > \mu\sqrt{1+\sigma^2}$.

Ⅲ. Simulation results

We evaluated the key disagreement rate (KDR) using various modulation schemes, post processing methods, and channels, as shown in Figures 1-3. As expected, the performance with $\mu = 0.5$ is much better than that with $\mu = 0$, regardless of the modulation schemes and the channel type. Post processing using $\tilde{h}_A = e^{j\emptyset_{\hat{h}_A}}$ and $\tilde{h}_B = e^{j\emptyset_{\hat{h}_B}}$ outperforms that using $\tilde{h}_A = \hat{h}_A$ and $\tilde{h}_B = \hat{h}_B$ for 16QAM, except for QPSK and 16-PSK with $n_B = 0$. This is reasonable, because post processing affects both amplitude and phase of the modulated symbols, which does not degrade the performance of PSK without additive noise. On the other hand, omitting n_B does not improve the KDR performance much, regardless of the channel, especially when $\mu = 0$. This is because the multiplicative noise $\frac{|\tilde{h}_A|}{|\tilde{h}_B|} e^{j\left(\emptyset_{\tilde{h}_A} - \emptyset_{\tilde{h}_B}\right)}$ has greater impact on s_A than the additive noise $\frac{\tilde{h}_B^*}{|\tilde{h}_B|^2} n_B$, and the smaller the $|\tilde{h}_B|$, the greater the impact. Table I shows the proportion that the Euclidean distance between s_A and its multiplicative noised symbol is further than the distance between s_A and its additive noised symbol.

Table I. The proportion of $\left|\frac{|\tilde{h}_A|}{|\tilde{h}_B|} e^{j\left(\emptyset_{\tilde{h}_A} - \emptyset_{\tilde{h}_B}\right)} s_A - s_A\right| \geq \left|s_A + \frac{\tilde{h}_B^*}{|\tilde{h}_B|^2} n_B - s_A\right|$ for QPSK.

snr (dB)	-5	0	10	15	20
proportion (%)	22.27	55.02	91.09	99.89	100

IV. Conclusion

In this paper, we presented a generalized physical layer secret key generation system, which is applicable for PSK, QAM. Simulation results show that A&P approximates P; fuzzy extraction improves more than error free channel.

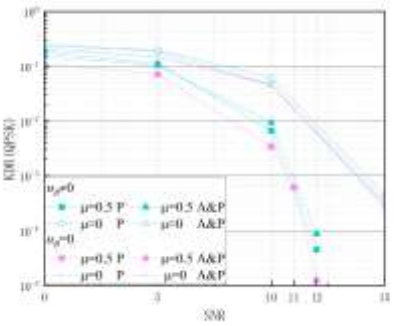

Figure 1. KDR comparisons for QPSK.

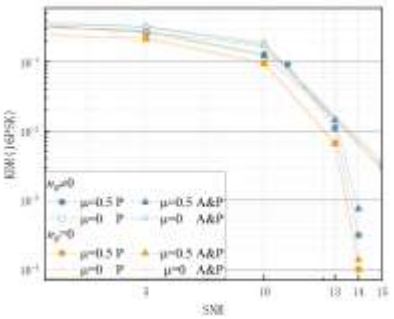

Figure 2. KDR comparisons for 16-PSK.

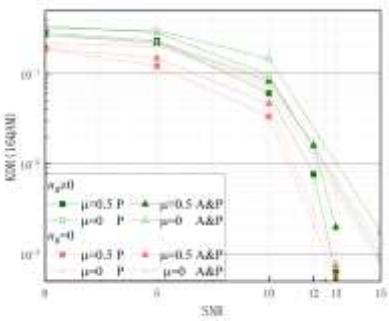

Figure 3. KDR comparisons for 16QAM.

ACKNOWLEDGMENT

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT).(No NRF-2021R1A2C1003121)

REFERENCES

[1] N. Shen, Q. Du, L. Lu and S. Zhao, "Fuzzy Secret Key Generation based on Phase Extraction and Constellation Rotation," 2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring), Florence, Italy, 2023, pp. 1-5.

[2] T. Nazzal and H. Mukhtar, "Evaluation of Key-Based Physical Layer Security Systems," 2021 4th International Conference on Signal Processing and Information Security (ICSPIS), Dubai, United Arab Emirates, 2021, pp. 84-87.