Eavesdropping Against Bidirectional Physical Layer Secret Key Generation in Fiber Communications

Wenxiu Hu
School of Engineering
University of Warwick
Coventry, UK
wenxiu.hu@warwick.ac.uk

Zhuangkun Wei
SATM
Cranfield University
Milton Keynes, UK
zhuangkun.wei@cranfield.ac.uk

Mark Leeson
School of Engineering
University of Warwick
Coventry, UK
mark.leeson@warwick.ac.uk

Tianhua Xu
School of Engineering
University of Warwick
Coventry, UK
tianhua.xu@warwick.ac.uk

***Abstract*—Physical layer secret key exploits the random but reciprocal channel features between legitimate users to encrypt their data against fiber-tapping. We propose a novel tapping-based eavesdropper scheme, leveraging its tapped signals from legitimate users to reconstruct their common features and the secret key.**

Keywords—eavesdropping, two-way secret key generation, physical layer security, fiber communications

I. Introduction

Fiber tapping has been shown as a threaten technology to extract the transmitted data from fiber links [1]. To provide secure communications in the face of potential tapping, cryptography encrypts the transmitted data via secret key, making the tapped data uninterpretable to eavesdroppers (Eve). Traditional cryptography, however, requires high computational complexity based key computation and distribution, therefore less attractive to confront the largely increased civil and commercial demands of communications. To address the security issue, physical layer secret key generation (PL-SKG) has been proposed, which leverages the random and reciprocal channel properties extracted by Alice and Bob to generate the shared secret key [2]–[5]. To prevent brute force decoding by Eve, current studies propose to (i) increase the channel randomness (e.g., phase fluctuation [2], polarization mode dispersion, PMD [3], Stokes parameters [4]), and (ii) use random signals (known as the two-way or bidirectional key generation method [5]) to increase the randomness of the secret key. However, the eavesdropping study has been overlooked by most of the studies. The information entropy induced by either channel or signal level randomness are all reflected by the observations (received signals) of a fiber-tapping Eve. This therefore motivates us and enables the potential of a more efficient Eve design than brute force.

II. Single Mode Fiber Channel Model & How two-way SKG is used

Alice and Bob are considered to generate a shared secret key, leveraging the channel reciprocity of the single mode fiber (SMF) between them. The channels from Alice to Bob and from Bob to Alice are modelled as $\mathbf{H}_{AB}(\omega), \mathbf{H}_{BA}(\omega) \in \mathbb{C}^{2\times 2}$, i.e., [3]:

$$\mathbf{H}_{AB}(\omega) = \prod_{n=1}^{N_{AB}} l(\omega)\mathbf{S}(-\theta_n)\begin{bmatrix} e^{-\frac{j}{2}(\bar{\Delta}_\tau\omega+\phi_n)} & 0 \\ 0 & e^{\frac{j}{2}(\bar{\Delta}_\tau\omega+\phi_n)} \end{bmatrix}\mathbf{S}(\theta_n) = \left(\prod_{\substack{n=\\N_{AB}}}^{1} l(\omega)\mathbf{S}(-\theta_n)\begin{bmatrix} e^{-\frac{j}{2}(\bar{\Delta}_\tau\omega+\phi_n)} & 0 \\ 0 & e^{\frac{j}{2}(\bar{\Delta}_\tau\omega+\phi_n)} \end{bmatrix}\mathbf{S}(\theta_n)\right)^T = \mathbf{H}_{BA}^T(\omega) \tag{1}$$

where ω is the angular speed. $N_{AB} = 20$ is the number of simulated fiber segments. $l(\omega) \triangleq e^{-d_z\cdot\alpha/2-jD\lambda^2 d_z\omega/(4\pi c)}$is the chromatic dispersion component, with $d_z = 0.5km$ the step size, $\alpha = 0.46\,dB/km$ the attenuation parameter, $c = 3\times 10^8\ m/s$ the light velocity, $\lambda = 1550nm$ the reference wavelength, and $D = 17\,ps/nm/km$ the dispersion parameter at λ. $\theta_n, \phi_n \sim \mathcal{U}[0,2\pi)$ are the random rotation angle and phase for nth fiber segment. $\mathbf{S}(\cdot)$ is the 2×2 rotation matrix. $\bar{\Delta}_\tau = 8\,ps$ is the average differential group delay. In (1), $\mathbf{H}_{AB}(\omega) = \mathbf{H}_{BA}(\omega)^T$is the channel reciprocity, deduced by reversing the order of 1, …, N_{AB} fiber segments.

To generate the secret key by the bidirectional (two-way) method, Alice and Bob send random signals to each other, denoted as $\mathbf{x}_A(\omega), \mathbf{x}_B(\omega) \in \mathbb{C}^{2\times 1}$in terms of the frequency domain. Then, they multiply their sent and received signals as the common feature:

$$\begin{aligned} u_A &= \mathbf{y}_A(\omega)^T\cdot\mathbf{x}_A(\omega) \overset{(a)}{=} \mathbf{x}_B(\omega)^T\cdot\mathbf{H}_{AB}(\omega)\cdot\mathbf{x}_A(\omega) + \mathbf{n}_A^T\cdot\mathbf{x}_A(\omega), \\ u_B &= \mathbf{x}_B(\omega)^T\cdot\mathbf{y}_B(\omega) = \mathbf{x}_B(\omega)^T\cdot\mathbf{H}_{AB}(\omega)\cdot\mathbf{x}_A(\omega) + \mathbf{x}_B(\omega)^T\cdot\mathbf{n}_B, \end{aligned} \tag{2}$$

where $\boldsymbol{y}_A(\omega) = \mathbf{H}_{BA}(\omega)\cdot\mathbf{x}_B(\omega) + \mathbf{n}_A$ and $\boldsymbol{y}_B(\omega) = \mathbf{H}_{AB}(\omega)\cdot\mathbf{x}_A(\omega) + \mathbf{n}_B$ are the received signals at Alice and Bob, with $\mathbf{n}_A, \mathbf{n}_B \sim \mathcal{CN}(0, \sigma_n^2\mathbf{I}_2)$ (the noise components where $\mathbf{I}_2$ is the 2×2 identity matrix). In (2), (a) is by taking the expression of $\mathbf{y}_A(\omega)^T$, and then replacing $\mathbf{H}_{BA}(\omega)^T$ with $\mathbf{H}_{AB}(\omega)$ using (1). As such, u_A and u_B share random but common feature $\mathbf{x}_B(\omega)^T\mathbf{H}_{AB}(\omega)\mathbf{x}_A(\omega)$, and thereby can be used to generate shared secret key using the quantization method, i.e., [3]

$$k_a = \begin{cases} 1 & v_a > \gamma_+ \\ 0 & v_a < \gamma_- \end{cases}, \quad a \in \{A, B\}, \qquad \begin{aligned} & with\, v_a = \mathrm{Re}[u_A]\, or\, \mathrm{Im}[u_A], \\ & \gamma_\pm = mean(v_a) \pm C\sqrt{\mathrm{var}(v_a)}, C\in[0,1]. \end{aligned} \tag{3}$$

This work was supported by EU Horizon 2020 Grant (No. 101008280).

III. Eavesdropping Design

In this section, we elaborate our eavesdropping scheme, which aims to reconstruct the common feature and the secret key relying on it. Here, we assume a fiber-tapping Eve in the SMF between Alice and Bob that passively receives the random signals sent from Alice and Bob. As such, Eve's received signals from Alice and Bob, denoted as $\mathbf{z}_A(\omega), \mathbf{z}_B(\omega) \in \mathbb{C}^{2\times 1}$, are:

$$\begin{aligned} \mathbf{z}_A(\omega) &= \beta \cdot \mathbf{H}_{AE}(\omega) \cdot \mathbf{x}_A(\omega) + \acute{\mathbf{U}}_A, \\ \mathbf{z}_B(\omega) &= \beta \cdot \mathbf{H}_{BE}(\omega) \cdot \mathbf{x}_B(\omega) + \acute{\mathbf{U}}_B, \end{aligned} \tag{4}$$

where $\mathbf{H}_{AE}(\omega)$ ($\mathbf{H}_{BE}(\omega)$) is the channel from Alice (Bob) to Eve, and is modelled by replacing B (A) of $\mathbf{H}_{AB}(\omega)$ ($\mathbf{H}_{BA}(\omega)$) in (1). β denotes the tapping gain, determined by the specific tapping methods (e.g., the bend loss in [1]). $\boldsymbol{\epsilon}_A, \boldsymbol{\epsilon}_B \sim \mathcal{CN}(0, 2\sigma_n^2 \mathbf{I}_2)$ are the receiving noise components. Then, Eve is able to reconstruct the common feature of Alice and Bob, denoted as u_E, by:

$$\begin{aligned} u_E &= \frac{1}{\beta^2} \cdot \mathbf{z}_B(\omega)^T \cdot \mathbf{z}_A(\omega) = \mathbf{x}_B(\omega)^T \cdot \mathbf{H}_{BE}(\omega)^T \cdot \mathbf{H}_{AE}(\omega) \cdot \mathbf{x}_A(\omega) + \varepsilon \\ &= \mathbf{x}_B(\omega)^T \cdot \underbrace{\mathbf{H}_{EB}(\omega) \cdot \mathbf{H}_{AE}(\omega)}_{A \to E \to B} \cdot \mathbf{x}_A(\omega) + \varepsilon = \mathbf{x}_B(\omega)^T \cdot \mathbf{H}_{AB}(\omega) \cdot \mathbf{x}_A(\omega) + \varepsilon \end{aligned} \tag{5}$$

where $\varepsilon \triangleq \mathbf{x}_B(\omega)^T \cdot \mathbf{H}_{BE}(\omega)^T \cdot \boldsymbol{\epsilon}_A/\beta^2 + \boldsymbol{\epsilon}_B^T \cdot \mathbf{H}_{AE}(\omega) \cdot \mathbf{x}_A(\omega)/\beta^2 + \boldsymbol{\epsilon}_B^T \cdot \boldsymbol{\epsilon}_A/\beta^2$. It is compared with (2) that u_E and u_A (u_B) shares the same feature $\mathbf{x}_B(\omega)^T \mathbf{H}_{AB}(\omega) \mathbf{x}_A(\omega)$. This therefore enables Eve to reconstruct the shared secret key between Alice and Bob by taking $v_E = Re[u_E]$ or $Im[u_E]$ into the quantization method, i.e., (3).

IV. Results and Discussion

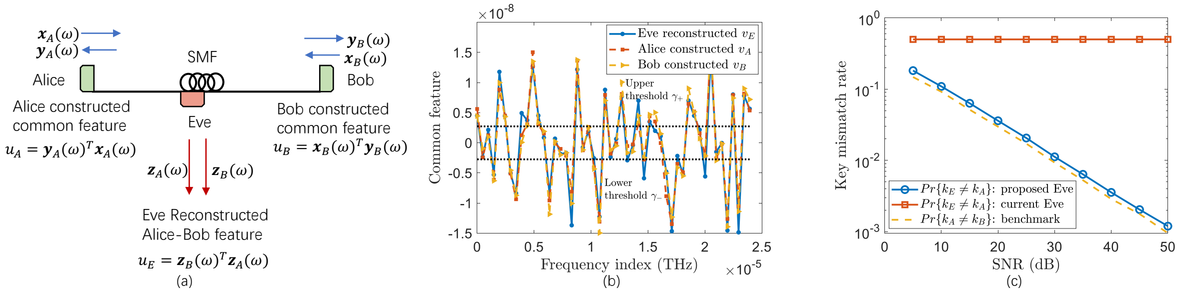

Fig. 1. (a) Alice, Bob and Eve scenario in SMF, (b) Eve reconstructed Alice-Bob features, and (c) the key mismatch rate of our proposed Eve scheme.

Fig. 1(a) illustrates the simulated SMF between Alice and Bob with the tapping Eve. The transmission setting is provided in the description of (1). Random 32-Gbaud 16-QAM signals have been sent between Alice and Bob. Fig. 1(b) shows that Eve's reconstructed feature is similar to that of Alice and of Bob, i.e., $v_E \approx v_A \approx v_B$, which validates the deduction in (5). Then, Fig. 1(c) gives the key mismatch rate between Eve and Alice, i.e., $Pr\ \{k_E \neq k_A\}$ (blue line), which is close to that between Alice and Bob, i.e., $Pr\ \{k_A \neq k_B\}$ (yellow dash line), and is much lower than the current brute force Eve. Combining the results in Fig. 1(b)-(c), and the mathematical deduction in (5), our designed Eve scheme can decode the two-way based physical layer secret key in SMF.

We revealed the eavesdropping potential for current physical layer secret key in fiber communications. Unlike wireless communications where the randomness comes from the propagation multi-paths that will be partially missed by Eve, in fiber communications, all the randomness (from transmitted signals or from channel phases) are contained in the transmitting signals, and therefore will be received by a fiber-tapping Eve. Leveraging this, we provided the demonstration eavesdropping scheme, which, as shown by (5) and our results, can successfully reconstruct the legitimate common feature and the secret key relied upon. This therefore should be warned by further more secure secret key design to protect the confidentiality of fiber communications.

References

[1] M. Z. Iqbal, H. Fathallah and N. Belhadj, "Optical fiber tapping: Methods and precautions," International Conference on High-capacity Optical Networks and Emerging Technologies, pp. 164-168, 2011.

[2] K. Kravtsov, Z. Wang, W. Trappe and P. R. Prucnal, "Physical layer secret key generation for fiber-optical networks," Optics Express, vol. 21, no. 20, pp. 23756–23771, 2013.

[3] I. U. Zaman, A. B. Lopez, M. A. A. Faruque and O. Boyraz, "Physical layer cryptographic key generation by exploiting PMD of an optical fiber link, " Journal of Lightwave Technology, vol. 36, no. 24, pp. 5903–5911, 2018.

[4] A. A. Hajomer, L. Zhang, X. Yang and W. Hu, "Accelerated key generation and distribution using polarization scrambling in optical fiber," Optics Express, vol. 27, no. 24, pp. 35761–35773, 2019.

[5] Y. Wu, Y. Yu, Y. Hu, Y. Sun, T. Wang and Q. Zhang, "Channel-based dynamic key generation for physical layer security in OFDM-PON systems," IEEE Photonics Journal, vol. 13, no. 2, pp. 7900209, 2021.