Nonlinear Tolerant Conjugated RoF System Secured by Physical Layer Encryption with Deliberate Signal Randomization

Tatsuki Ishijima[1], Shuhei Otsuka[1], Shun Harada[1], Takahide Sakamoto[1], Ken Tanizawa[2] and Fumio Futami[2]
[1]Tokyo Metropolitan University, 6-6, Asahigaoka, Hino-shi Tokyo, 191-0065, Japan
[2]Quantum ICT Research Institute, Tamagawa University, 6-1-1 Tamagawagakuen, Machida, Tokyo, 194-8610, Japan
ishijimja-tatsuki@ed.tmu.ac.jp

Abstract: We propose and demonstrate conjugated RoF (C-RoF) secured by physical layer encryption with deliberate signal randomization, for high-RF-link-gain and high-security analog RoF transmission. 19.4-dBm high-power secured C-RoF-QPSK is experimentally achieved with improved fiber nonlinearity tolerance.

1. Introduction

In future Beyond 5G or 6G communication systems, analog Radio-over-Fiber (RoF) technologies can be a solution to achieve high capacity and low latency connectivity [1]. Highly secure encryption system is also demanded to protect analog RoF systems [2]. In analog RoF systems, it is important to increase optical power launched into fiber links as high as possible, aiming for obtaining higher RF link gain. In the higher optical power regime, however, transmitted signals experience significant waveform distortion due to nonlinearities in optical fibers. Typical approaches for equalizing the nonlinearly distorted signals are based on digital signal processers (DSPs), which require heavy computational resources, seriously increasing latency of the system. We have recently demonstrated conjugated RoF (C-RoF) that can equalize nonlinear waveform distortion by using optoelectronic processing [3] based on phase conjugation [4], without relying on any DSPs. The C-RoF technology is ideal for constructing RoF systems with higher RF link gain and with minimal latency. In addition, unlike typical equalizers relying on data-assisted digital signal processing, fiber nonlinearity is blindly canceled in the C-RoF system; therefore, the signals can be equalized even if any optical coding and/or encryption is physically applied to the optical data streams.

Physical layer encryption utilizing a pre-shared short private key for the advantage of legitimate reception is a promising security measure that directly prevents signal interception. Quantum-noise randomized stream cipher, known also as $\alpha\eta$ [5] or Y-00 protocol [6], utilizes high-order signal modulation with a private key and achieves secrecy based on the effect of quantum noise on a signal. The keyed high-order signal modulation was applied not only to optical communications but also to wireless communications, where RoF technologies played an important role in transferring the large effect of noise at optical frequencies to microwave region and masking signals for high security [2]. Recently, deliberate signal randomization (DSR) using a quantum random number generator (QRNG) was proposed to enhance the security of the quantum-noise stream cipher in optical communications [7]. The DSR imposes true uncertainty independent of optical power and achieves high signal security in high-optical power regime.

In this paper, we propose a secured C-RoF transmission system utilizing the keyed high-order signal modulation with DSR. Combination of C-RoF and the signal encryption with DSR allows us constructing highly secure analog RoF systems in high optical power regime. The systems totally protect both of optical and radio links from illegitimate signal interception. Higher RF link gain enables higher efficiency of RF signal transfer in extended transmission distance. We experimentally demonstrate a C-RoF transmission system secured by the signal encryption with DSR, carrying QPSK with an RF carrier frequency of 5 GHz and a symbol rate of 250 Mbaud. Waveform distortion due to fiber nonlinearity is mitigated, allowing us the RoF transmission with a fiber launched power of 19.4 dBm. A symbol error ratio (SER) for an eavesdropper closely approaches 1, resulting in high security, even at such a high power.

2. Principles

In the secured C-RoF, the optoelectronic phase conjugation processing enables fiber nonlinearity cancellation; the keyed high-order signal modulation with DSR allow us physical-layer encryption, as explained in this section.

Fig. 1 shows the concept of secured C-RoF system and here explains how the fiber nonlinearity is mitigated in the system. In the system, nonlinear distortion caused by self-phase modulation (SPM) and cross-phase modulation (XPM) is naturally compensated for in the photonic up- and downconversion process [3]. Different from conventional single-sideband RoF systems, dual-sideband transmission technology is utilized in the C-RoF system. Double side

band (DSB) modulation is used for the photonic upconversion on the transmitter side; the DSB signal is photonic downconverted by using asymmetric heterodyne on the receiver side. In the C-RoF system, the upper-sideband (USB) and lower-sideband (LSB) components generated by the DSB modulation both are input to the fiber link. The USB and LSB components are phase conjugated with each other, which means symbol arrangements of their constellations are mirrored each other in the complex IQ plane. In the fiber link, the sideband components experience the same amount of nonlinear waveform distortion. In the photonic downconversion, an asymmetric heterodyne technique is used in order to independently detect the USB and LSB signals. It should be noticed that, under the downconversion process from the optical to the RF frequencies, the LSB components are naturally conjugated back. This means that the RF signals originated from LSB and USB are no longer phase conjugated. The signals have the same symbol arrangement; however, the nonlinear phase shifts revealed in the signal have the counter sign. Therefore, the fiber nonlinearity is naturally cancelled out if we simply superpose the downconverted signals inphase in the RF receiver. No other processing is additionally required for the fiber nonlinearity cancellation.

Keyed high-order signal modulation with DSR is employed for the secured C-RoF. A short private key, typically 256 bits, is assumed to be securely shared in advance. Fig. 2 shows the operating principles for QPSK data modulation. At the first step of the PSK-based signal encryption (Step 1), QPSK is converted to extremely high-order PSK signals, for example 2^{18} PSK [8]. This process is achieved by rotating the phase of QPSK in a symbol-by-symbol manner, where the rotation angle $\theta_{\mathrm{key}}(i)$ is determined based on the key information. Provided that the order of PSK is high, illegitimate reception of the encrypted high-order PSK signals is seriously affected by noise. Thus, signal security against interception is achieved. Even if an eavesdropper has an ideal receiver, quantum noise is unavoidable, which promises lower bound of security. Then, DSR is utilized to enhance the security in the high optical power regime. DSR is key-less signal randomization using a QRNG at the transmitter side [7]. As shown in Step 2 of Fig. 2, symbol-by-symbol random phase rotation $\theta_{\mathrm{DSR}}(i)$ is intentionally added to the encrypted high-order PSK signals. The range of DSR phase rotation is set to a few tens of percentages of the full range of $\pi/2$ in the QPSK data modulation. The phase uncertainty imposed by DSR is independent of the signal power, and high signal security is achieved even at high optical power. On the other hand, even after the decryption with a private key (Step 3 in Fig. 2), the DSR phase rotation remains. Thus, the signal encryption with DSR enhances the security of C-RoF system operating at high power, although the residual phase noise reduces the signal quality for a legitimate receiver.

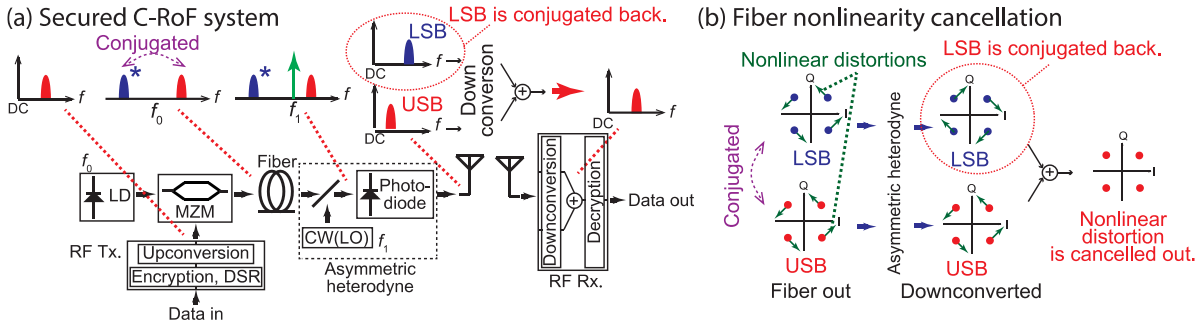

Fig. 1. Concept of secured C-RoF and mechanism of fiber nonlinearity cancellation

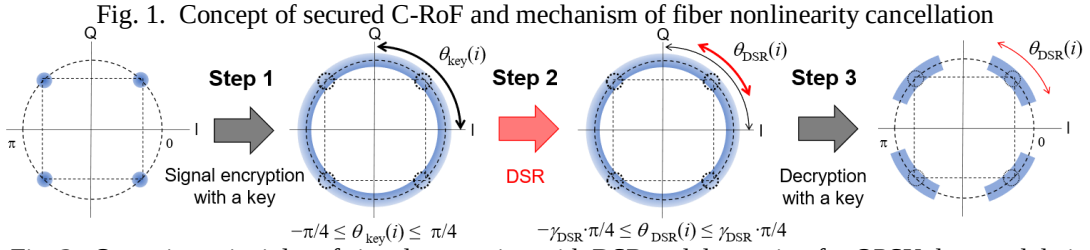

Fig. 2. Operating principles of signal encryption with DSR and decryption for QPSK data modulation.

3. Experiments

Fig. 3 shows the experimental setup of the proposed secured C-RoF transmission system. On the transmitter side, encrypted C-RoF signal was generated with an arbitrary waveform generator (AWG), a CW laser diode (LD), and an MZM. The CW light at 1550 nm was DSB modulated with the MZM driven by a radio frequency (RF) signal generated from the AWG clocked at 25 GSa/s. In the offline DSP, first, a baseband signal in QPSK format was generated. Next, the signal was encrypted by the keyed high-order signal modulation with DSR. The length of a private key was 256 bits. The encrypted signal followed a 2^{16} PSK template. The DSR was driven with true random numbers from a QRNG, and phase fluctuation between -$\pi/20$ and $\pi/20$ is added to the signal. Then, the signal was upconverted to the RF region.

The symbol rate was 250 Mbaud; the RF carrier frequency of the directly upconverted signal was 5 GHz. The secured C-RoF signal was launched into a standard single-mode fiber (SMF) whose length was 9.2 km after amplification with an Erbium-doped fiber amplifier. On the receiver side, the received secured C-RoF signal was combined with a CW local-oscillator (LO) light by using a 3-dB optical coupler. The wavelength of the LO was detuned in 1 GHz from the center wavelength of the carrier light of the received secured C-RoF signal. The combined light was input to a photodiode (PD) with a bandwidth of 8 GHz. The photodetected signal was analog-to-digital-converted with a high-speed real-time oscilloscope. The USB and LSB were downconverted, then superposed inphase each other. The signal was decrypted using the private key. Finally, the signal was orthogonally demodulated after a carrier phase estimation.

Figs. 4 show the experimental results when the optical input power was 19.4 dBm. Figs. 4(a) and (b) show the constellations without and with fiber nonlinearity cancellation by C-RoF for reference signals without DSR, respectively. From Figs. 4(a) and (b), it is found that the C-RoF technique successfully compensated for the nonlinear waveform distortion. Figs. 4(c) ~ (e) show the cases for (c) encrypted signals with DSR, (d) decrypted signals w/o conjugation processing, and (e) decrypted signals with conjugation processing, respectively. From Fig. 4(c), it is found that the encrypted high-order signals cannot be discriminated as we intended. Fig. 4(d) indicates that we can recover the QPSK signals with residual phase fluctuations due to the DSR. However, the constellations were still unclear because of waveform distortion due to fiber nonlinearities. Comparing Fig. 4(d) and (e), it is clear that the waveform distortion was canceled by the conjugation process in C-RoF.

Next, we quantitatively investigated fiber nonlinearity tolerance of the proposed system. Figs. 5 and 6 show EVMs measured for different optical fiber-input powers without and with DSR, respectively. In each plot, the EVM verses power was measured when the fiber nonlinearity cancellation by C-RoF was applied, denoted as (a), whereas (b) was obtained without C-RoF (i.e. w/ conventional RoF) applied. It can be seen that the C-RoF overall outperforms the conventional RoF. In both cases, the improvement of EVM was higher in the higher input power region, which means the fiber nonlinearity cancellation works well in the regime. Comparing Figs. 5 and 6, we can observe an EVM penalty of approximately 3 % caused by the DSR. An SER an eavesdropper potentially reaches is estimated to be 0.9997 when the DSR is applied. This means that the illegitimate signal detection involves numerous errors, and signal interception is effectively prevented at such a small cost to signal quality.

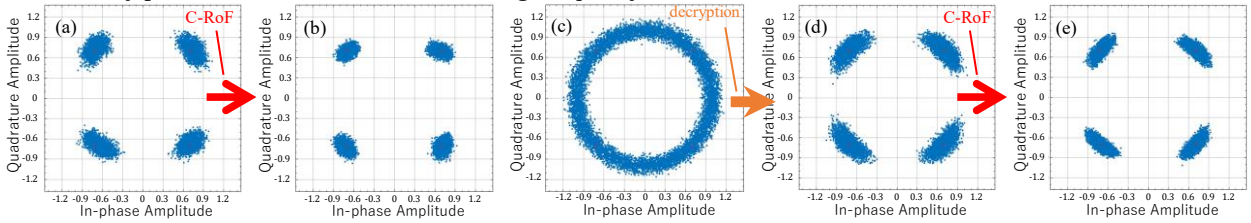

Fig. 4. Measured constellations
(a) w/o C-RoF w/o DSR (b) w/ C-RoF, w/o DSR (c) encrypted signals w/o C-RoF w/ DSR
(d) decrypted signals w/o C-RoF w/ DSR (e) decrypted signals w/ C-RoF w/ DSR

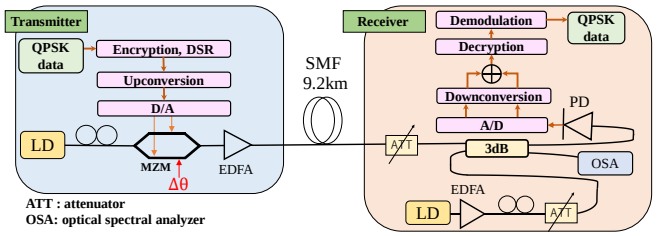

Fig. 3. Experimental setup

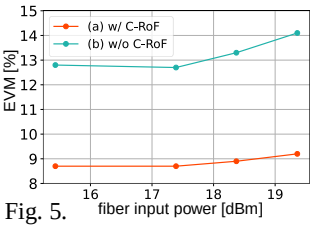

Fig. 5. EVM vs. fiber input power (w/o DSR)

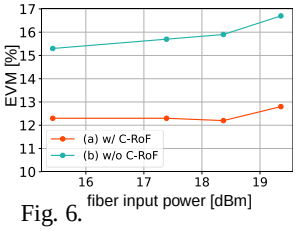

Fig. 6. EVM vs. fiber input power (w/ DSR)

4. Conclusions

We proposed and demonstrated secured C-RoF secured by physical layer encryption with deliberate signal randomization, for high-RF-link-gain and high-security analog RoF transmission. 19.4-dBm high-power secured C-RoF QPSK was experimentally achieved with improved fiber nonlinearity tolerance.

This work was partly supported by JSPS KAKENHI Grant Number JP21H01329, 18H03788; CREST, Japan Science and Technology Agency, Japan; NEDO Extensive Support for Young Promising Researchers.

References

[1] K. Nishimura, et al, MWP2020, 21-24 (2020). [2] K. Tanizawa, and F. Futami, J. Lightwave Technol. **38**, 16, 4244-4249 (2020).
[3] T. Sakamoto, et al, MWP2014, WD.4 (2014). [4] X. Liu et al, Nature Photon. **7**, 560-568 (2013).
[5] E. Corndorf, et al, Phys. Rev. A. **71**, 062326 (2005). [6] O. Hirota, et al, Phys. Rev. A, **72**, 022335 (2005).
[7] F. Futami, et al, CLEO 2022, JW3B.107 (2022). [8] K. Tanizawa, and F. Futami, Optics Express, **29**, 7, 10451-10464 (2021)