Robustness of Optical Steganographic Communication Under Coherent Detection Attack

Chaoran Huang, Philip Y. Ma, Bhavin J. Shastri, Prateek Mittal, *Member, IEEE*, and Paul R. Prucnal, *Life Fellow, IEEE*

***Abstract*— In fiber-optic networks, optical steganographic communication hides the existence of stealth signals in public channels. The previous security analyses assumed threat models in which eavesdroppers rely only on the real-time key search in the optical domain for signal recovery. In this letter, we study a new threat model that uses coherent detection and offline digital signal processing (DSP) to recover the stealth signal, and we show the robustness of optical steganographic communication under this attack. We find that eavesdroppers equipped with the state-of-the-art coherent detectors and DSP technologies fail to estimate the secret key. In addition, even if the eavesdroppers are given the secret key, the stealth signal cannot be recovered from the signal using DSP. The histogram of the received signal after DSP displays a noise-like form which prevents eavesdroppers from detecting the existence of the stealth signal. We attribute the system robustness to the unique features of using amplified spontaneous emission noise as the signal carrier, including wide bandwidth, large phase variance, and fast phase fluctuation.**

***Index Terms*— Communication system security, digital signal processing, optical fiber communication.**

I. Introduction

THE tremendous capacity of today's optical networks is capable of supporting the growing traffic demand of the Internet, data centers and cloud computing systems. Because optical data channels can be easily compromised via fiber tapping, there are growing concerns over the security and privacy of optical networks [1], [2]. To address these concerns, optical signal processing has been used to enhance the security and privacy in the optical layer [1]–[4]. Optical encryption is aimed at making the data unreadable by a third party and has been extensively empolyed in optical networks. Optical steganography, on the other hand, aims at hiding the existence of optical signals from the eavesdroppers [5]–[9]. In effect, steganography differs from encryption because encryption attempts to prevent the data from being read once it has already been intercepted, whereas steganography attempts to reduce the probability that the data can be detected or intercepted in the first place. In the frequency domain, the stealth channels are hidden among the public channels using wideband amplified spontaneous emission (ASE) noise as the carrier. In the time domain, the signal is heavily dispersed to a level that cannot be distinguished from the true ASE noise. The spectral location and dispersion applied to the signal are secretly shared only between the legitimate users. Stealth signals cannot be recovered by the eavesdroppers unless they successfully find both the spectral location and dispersion which, together, account for a huge key space.

The robustness of the optical steganographic communication has been extensively studied under different attack models [5]–[9]. In those models, the eavesdropper launches brute-force attacks *in the optical domain and in real time*. They scan the dispersion using a reconfigurable dispersion module and recover the hidden signal by applying a complementary dispersion. The eavesdropper literally has only one chance to match the secret parameters, otherwise the messages will be lost at the very moment they are received. Nowadays, coherent detection and digital signal processing (DSP) become powerful tools that can recover heavily dispersed signals [10]. Additionally, the signals can be digitized and stored for future recovery. Therefore, by borrowing these advanced technologies in the fiber communications, the eavesdropper can potentially conduct off-line searches for the secret dispersions.

In this work, we use a simulation-driven approach to analyze and show the robustness of optical steganographic communication systems under an attack *in the digital domain*: the eavesdropper attempts to digitize and store the stealth signals, estimate the dispersion, and recover the stealth signals off-line using coherent detection and DSP. We discover that, the stealth signals can be concealed in the ASE noise under this attack. Not only can the signal not be recovered, but the noise-like feature of the stealth signal indicates the successful signal concealing. We point out that the robustness of our steganographic system relies on the unique properties of the ASE noise. The ASE noise imposes ultrafast fluctuating amplitude and phase to the stealth channel, which are extremely difficult to be tracked by the detection system and processed by DSP.

II. System Model

Fig. 1 shows a typical optical steganographic communication system [5]. At the transmitter, a continuous wave (CW)

Manuscript received December 3, 2018; accepted January 6, 2019. Date of publication January 10, 2019; date of current version February 5, 2019. This work was supported in part by NSF EARS under Grant 1642962 and in part by the Department of Electrical Engineering, Princeton University. *(Corresponding author: Chaoran Huang.)*

The authors are with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08542 USA (e-mail: chaoranh@princeton.edu; yechim@princeton.edu; shastri@ieee.org; pmittal@princeton.edu; prucnal@princeton.edu).

Color versions of one or more of the figures in this letter are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/LPT.2019.2891955

1041-1135 © 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

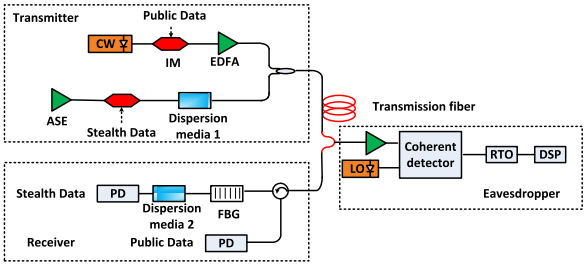

Fig. 1. Illustration of optical steganographic communication and attack model. CW: continuous wave; IM: intensity modulator; EDFA: erbium-doped fiber amplifier; FBG: fiber Bragg grating; PD: photo-detector; LO: local oscillator; RTO: real-time oscilloscope; DSP: digital signal processing.

laser is used as the public signal carrier and modulated with the public data. Meanwhile, the ASE noise generated from an erbium-doped fiber amplifier (EDFA) is used as the stealth signal carrier and modulated with the stealth data. The modulated stealth signal goes through a dispersive medium (e.g., chirped fiber Bragg grating) which applies a dispersion that is only known by the legitimate users. The dispersion can be shared between the the legitimate users using a secure channel, and can be updated frequently using a pseudo-random function with a fixed seed and time slot. As a result of dispersion, the pulses are heavily spread to a level that is completely hidden in the public channel. The public channel and stealth channel are combined and launched into a transmission fiber. Due to the large bandwidth of the stealth channel, its power is at a level which is indistinguishable to the ASE noise in the public channel. Being aware of the existence of the stealth channel and the dispersion, the legitimate receiver can easily filter the public channel and recover the stealth signal by using a module with a complementary dispersion. The stealth signal is then detected by a photo-detector. Our previous work has experimentally demonstrated that the optical steganographic communication successfully conceals and transmits the stealth channel over a 50 km fiber link [5].

III. Attack Model

In the optical steganographic communication, the goal of an eavesdropper is to identify the potential hidden signal, which leads to two-fold challenges: 1) stealth signal detection, the eavesdropper aims to identify if there is any stealth signal hidden beneath; 2) stealth signal recovery, the eavesdropper aims to reconstruct the stealth signal. We assume that the eavesdropper has the capability of accessing the signals via fiber tapping, but can only obtain 1% signal power. Otherwise, the cable monitor system will detect the existence of the eavesdropper [11]. The security of the steganographic communication system relies on the difficulty in finding the matched dispersion parameter.

In the previous attack models, the eavesdroppers conduct a brute-force attack in the optical domain where they attempt to discover the stealth signal by scanning the dispersion and recover the signal using a reconfigurable fiber Bragg grating (FBG) or optical phase mask. Due to the lack of efficient optical buffers (compared to their electronic counterparts), the eavesdropper has to find the dispersion and recover the stealth signal right at the moment it is received, otherwise the data will be lost. The reconfiguration speed of the state-of-the-art dispersive components is very limited, especially compared to the data rate of the stealth channel. The steganographic communication system can easily defend such attacks by frequently updating the dispersion. The optical-domain attack has been thoroughly analyzed in [5], and is beyond the scope of this letter.

Realizing the constraints of the optical-domain attack, this work focuses on studying the robustness of the steganographic communication under an alternative attack in which the eavesdropper exploits digitization and off-line analysis. The attack system is illustrated in Fig. 1. In this attack, the eavesdropper digitizes and stores the stealth signal, then he can search for the secret dispersion off-line without worrying about losing any data. As dispersion is a frequency-dependent phase change, the eavesdropper uses coherent detection to extract the stealth signal consisting of both its amplitude and phase. The coherent detection system consists of a local oscillator (LO), a coherent receiver and a real-time oscilloscope (RTO). The optical field is converted to the baseband by beating it with the LO. The complex field is then digitized by the RTO and stored for off-line processing. This allows the eavesdropper to scan the dispersion parameters and compensate the signal distortion off-line via DSP techniques [12]. Chromatic dispersion can be modeled as an all-pass filter given by $H_{CD}(\omega) = \exp(-jCD\lambda^2\omega^2/4\pi c)$, where CD is the secret chromatic dispersion applied to the stealth signal, λ is the signal wavelength and ω is angular frequency, respectively. The dispersion added to the stealth signal can be compensated by applying an inverse filter to $H_{CD}(\omega)$ in either the time domain or frequency domain [10], [12].

IV. System Security Against Coherent Detection Attack

To demonstrate the security of optical steganographic communication system, VPIphtonics is used to simulate this system. In the simulation, both public and stealth signals are modulated with 5 Gbit/s pseudorandom binary sequences (PRBSs). A dispersion of 7870 ps/nm is applied to the stealth signal. The sampling rate of the RTO is set to be 20 GSample/s, which is 4 times of the data rate. In this section, the eavesdropper is assumed to be equipped with an ideal coherent detection system: the coherent detector is perfectly IQ balanced, the RTO has infinite resolution, and the noise in the LO, coherent detector and RTO is neglected. However, the bandwidth of the coherent detection system is limited to 100 GHz according to the state of the art. Here the eavesdropper conducts a brute-force attack in the digital domain. CD is scanned off-line after the eavesdropper captures the signal. The eavesdropper attempts to verify the dispersion using two approaches.

In the first approach, the eavesdropper attempts to estimate the dispersion by evaluating the autocorrelation function corresponding the frequency spectrum of the compensated signal $S(n) = H_{CD}^{-1}R(n)$, where H_{CD} is the transfer function of dispersion, and $R(n)$ is the received signal after sampling [12]. The clock tone is extracted as the cost function and the largest

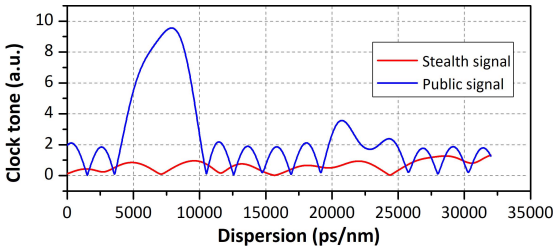

Fig. 2. Dispersion estimation of public signal and stealth signal.

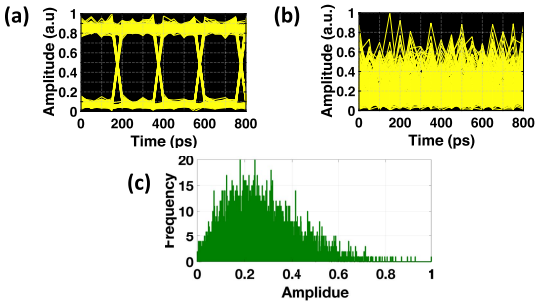

Fig. 3. Eye diagram of (a) public signal after dispersion compensation using DSP and (b) stealth signal after dispersion compensation using DSP. (c) Histogram of stealth signal after dispersion compensation using DSP.

value corresponds to the right dispersion. To illustrate the difference between the stealth signal and conventional signal, we intentionally apply a dispersion of 7870 ps/nm to the public channel. It is worth noting that, the public channel is dispersed here only for performance comparison. No such dispersion will be applied to the public channel in the real steganographic communication system. A dispersion estimation is conducted to the stealth channel and public channel respectively, and the results are shown in Fig. 2. For the public signal, a peak value at 7870 ps/nm indicates the applied dispersion. However, for the stealth signal, no peak appears at the applied dispersion. The results indicate that, using ASE noise as the signal carrier effectively prevents the eavesdropper from estimating the secret dispersion by parameter scanning.

In the second approach, the eavesdropper attempts to compensate for the dispersion with a guessed value using DSP and verify the guess by analyzing the signal after DSP. For steganography, the system must ensure that the eavesdropper cannot notice the existence of the stealth signal when the attack is ongoing. To demonstrate steganography, we assume the worst case that the eavesdropper conducts DSP with the right dispersion. The eye diagrams of the public signal and stealth signal after compensating the right dispersion of 7870 ps/nm are shown in Fig. 3(a) and (b). A clear open eye diagram is only observed for the public signal, while the stealth signal has no eye opening. The histogram in Fig. 3(c) shows an indistinguishable one and zero level as noise. The results indicate that, the eavesdropper cannot recover the dispersion in the digital domain even with the right dispersion. The stealth channel can be concealed when the attack is ongoing.

V. System Security Analysis

The failure of coherent detection attack is attributed to the unique properties of the ASE noise. ASE noise has

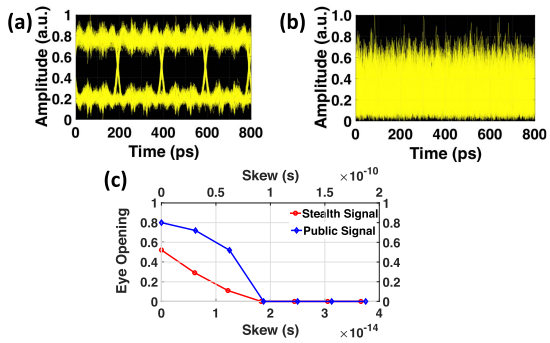

Fig. 4. (a) Eye diagram of dispersion compensated stealth signal using the ADC with 10 bit ENOB and sampling rate of 20 THz. (b) Closed eye diagram caused by phase ambiguity. (c) The influence of IQ skew on public data and stealth data.

an extremely wide bandwidth compared to the electronic devices. Therefore, the electrical field of ASE noise cannot be fully digitized by the state-of-the-art RTOs. The ASE phase can have a baseband bandwidth up to 4 THz. Digital dispersion compensation relies on appending the dispersion induced phase to the received signal. Therefore, a full digitalization and restoration of the electrical field is the prerequisite for an accurate dispersion estimation and compensation. Otherwise the signal will be buried under noise as shown in Fig. 3(b).

Considering the ASE noise as a wideband analog signal, an eligible RTO should have extremely high bandwidth, large effective number of bits (ENOB), and low timing jitter. However, the "Walden plot" indicates that the inherent confinement between the input bandwidth and the ENOB is due to the timing jitter [13]. We verify our claim by assuming that the eavesdropper is equipped with an ideal detection system: 1) the eavesdropper uses a RTO with unlimited bandwidth; 2) the phase variance of the ASE is small enough to avoid phase ambiguity; 3) the coherent detector is ideally IQ balanced. Under these assumptions, Fig. 4(a) shows the eye diagram of the signal after dispersion compensation, when the stealth signal is sampled beyond the Nyquist sampling rate required for the ASE bandwidth. An open eye is obtained at a cost of using a RTO sampling rate of 20 TSamples/sec—which is not practical, and is only feasible in a simulation environment. We then consider a realistic system in which ASE has an unpredictable and time-variable phase with large variance exceeding 2π [6]. As a result, phase ambiguity after a cycle slip occurs after dispersion compensation. Unlike those regularly modulated signals, phase ambiguity in the ASE noise cannot be estimated and recovered using DSP due to its randomness. Due to the phase ambiguity, the stealth signal after dispersion compensation has a closed eye (as shown in Fig. 4(b)) even when it is sampled at 20 TSamples/sec. Moreover, the common manufacturing and setup variances in optoelectronic circuits of a coherent detector such as IQ skew, easily ruin the received signal due to the ultrafast changes in the ASE noise. We compare the influence of IQ skew on the public signal and the stealth signal by evaluating the relative eye opening after dispersion compensation. The phase ambiguity is excluded from this analysis. The results

in Fig. 4(c) show that the stealth signal is $\sim 10^4$ times more sensitive to the IQ skew than the public signal. The eye is closed when the time-skew is only $\sim$20 fs, which is hard to avoid in the manufacturing process.

VI. Discussions

Our analysis indicates that, the ASE bandwidth is the key parameter that determines the security of the system. Meanwhile, the power of the stealth channel, which is related to the ASE bandwidth, determines the quality of the received stealth signal. Here, we discuss the system performances under two cases where the ASE bandwidth is reduced by the optical filters in the transmission links. The system reliability and security are addressed.

In the first case, ASE bandwidth is reduced in the networks where multiple add-drop filters are implemented for traffic routing. In a static point-to-point link, the spectrum and the power of the stealth channel can be planned and pre-assigned at the transmitter. To optimize the performances of both the stealth and the public channels, one should maximize the bandwidth of the stealth channel, while avoiding the interference between the stealth and the public channels. In a dynamic optical network where reconfigurable optical add drop multiplexers (ROADM) are actively used, implementing the steganographic system unfortunately becomes much more challenging. In this network, the spectral allocation is highly dynamic. Every node needs to be aware of the existence of stealth channel, and avoid channel adding or dropping at the spectra where the stealth channel exists. This increases the risk of node compromise attack in which the vicious node leaks the existence of the stealth channels to the eavesdropper [14].

In the second case, the eavesdropper inserts an optical filter after the optical tapping. This attack reduces the huge demand for the bandwidth and sampling rate of the coherent detection system. Assuming that the eavesdropper limits the noise bandwidth to that of a typical DWDM channel (e.g. 50 GHz), the coherent detection system will be able to digitize the stealth channel. Moreover, the recent advances in signal detection suggest that the eavesdropper can potentially get rid of phase ambiguity issue. Potential techniques include carrier recovery enabled self-homodyne detection and single-sideband direct-detection [15], [16]. We will study the attacks using those detection schemes in our future work.

Despite that optical filters reduce the required bandwidth and sampling rate of a detection system, they simultaneously reduce the received power by the eavesdropper. For example, assuming that the eavesdropper filters out 50 GHz spectrum from a 4 THz stealth signal, the filtered signal will be 19 dB lower than that of the tapped signal. With the additional tapping loss ($\sim$20 dB), the signal power received by the eavesdropper will be $\sim$40 dB lower than that received by the legitimate users. This significant power loss can potentially lead to a very poor signal to noise ratio (SNR) that buries the signal in the noise of a receiver. Therefore, the eavesdropper has to consider the tradeoff between the power loss and his digitization capability. The steganographic communication system designer, on the other hand, should maximize the ASE bandwidth while minimizing its power density.

VII. Conclusion

We have demonstrated the robustness of optical steganographic communication under the attack of coherent detection and DSP. We show that a state-of-the-art coherent detection system fails to estimate the secret chromatic dispersion applied to the stealth channel by scanning the dispersion. In addition, the modulated data cannot be recovered digitally even with the right dispersion. Optical steganography provides a secure communications for the following reasons: 1) the start-of-the-art coherent detection system cannot fully digitize the received ASE noise with sufficient sampling rate; 2) the large phase variance of ASE noise causes phase ambiguity that cannot be compensated by DSP; and 3) the stealth signal carried by ASE noise is extremely sensitive to the imperfections of the coherent detector which essentially plays a positive role in hiding the modulated data with ASE noise.

References

[1] N. Skorin-Kapov, M. Furdek, S. Zsigmond, and L. Wosinska, "Physical-layer security in evolving optical networks," *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 110–117, Aug. 2016.

[2] M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, "Optical layer security in fiber-optic networks," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 725–736, Sep. 2011.

[3] I. B. Djordjevic, "OAM-based hybrid free-space optical-terahertz multidimensional coded modulation and physical-layer security," *IEEE Photon. J.*, vol. 9, no. 4, Aug. 2017, Art. no. 7905812.

[4] K. Guan, J. Cho, and P. J. Winzer, "Physical layer security in fiber-optic MIMO-SDM systems: An overview," *Opt. Commun.*, vol. 408, pp. 31–41, Feb. 2018.

[5] P. Y. Ma, B. Wu, B. J. Shastri, A. N. Tait, P. Mittal, and P. R. Prucnal, "Steganographic communication via spread optical noise: A link-level eavesdropping resilient system," *J. Lightw. Technol.*, vol. 36, no. 23, pp. 5344–5357, Dec. 1, 2018.

[6] B. Wu, Z. Wang, B. J. Shastri, M. P. Chang, N. A. Frost, and P. R. Prucnal, "Temporal phase mask encrypted optical steganography carried by amplified spontaneous emission noise," *Opt. Express*, vol. 22, no. 1, pp. 954–961, Jan. 2014.

[7] E. Wohlgemuth, T. Yeminy, Z. Zalevsky, and D. Sadot, "Experimental demonstration of encryption and steganography in optical fiber communications," in *Proc. Eur. Conf. Opt. Commun. (ECOC)*, Sep. 2017, pp. 1–3.

[8] X. Hong, D. Wang, L. Xu, and S. He, "Demonstration of optical steganography transmission using temporal phase coded optical signals with spectral notch filtering," *Opt. Exp.*, vol. 18, no. 12, p. 12415–12420, Jun. 2010.

[9] T. Yeminy, D. Sadot, and Z. Zalevsky, "Spectral and temporal stealthy fiber-optic communication using sampling and phase encoding," *Opt. Express*, vol. 19, no. 21, p. 20182–20198, Oct. 2011.

[10] S. J. Savory, "Digital filters for coherent optical receivers," *Opt. Express*, vol. 16, no. 2, pp. 804–817, Jan. 2008.

[11] M. Z. Iqbal, H. Fathallah, and N. Belhadj, "Optical fiber tapping: Methods and precautions," in *Proc. 8th Int. Conf. High-Capacity Opt. Netw. Emerg. Technol.*, Dec. 2011, pp. 164–168.

[12] R. A. Soriano, F. N. Hauske, N. G. Gonzalez, Z. Zhang, Y. Ye, and I. T. Monroy, "Chromatic dispersion estimation in digital coherent receivers," *J. Lightw. Technol.*, vol. 29, no. 11, pp. 1627–1637, Jun. 1, 2011.

[13] C. Laperle and M. O'Sullivan, "Advances in high-speed DACs, ADCs, and DSP for optical coherent transceivers," *J. Lightw. Technol.*, vol. 32, no. 4, pp. 629–643, Feb. 15, 2014.

[14] H. Song, L. Xie, S. Zhu, and G. Cao, "Sensor node compromise detection: The location perspective," in *Proc. Int. Conf. Wireless Commun. Mobile Comput.*, New York, NY, USA, 2007, pp. 242–247.

[15] Z. Liu, J.-Y. Kim, D. S. Wu, D. J. Richardson, and R. Slavík, "Homodyne OFDM with optical injection locking for carrier recovery," *J. Lightw. Technol.*, vol. 33, no. 1, pp. 34–41, Jan. 1, 2015.

[16] Z. Li *et al.*, "SSBI mitigation and the Kramers–Kronig scheme in single-sideband direct-detection transmission with receiver-based electronic dispersion compensation," *J. Lightw. Technol.*, vol. 35, no. 10, pp. 1887–1893, May 15, 2017.