Bioinspired Photonics: Camouflage Strategies from Marine Hatchetfish for Optical RF Steganography

Qidi Liu
Lightwave and Microwave Photonics Lab
College of Engineering
University of Georgia
Athens, GA 30605, USA
qidi.liu@uga.edu

Mable P. Fok
Lightwave and Microwave Photonics Lab
College of Engineering
University of Georgia
Athens, GA 30605, USA
mfok@uga.edu

2021 IEEE Research and Applications of Photonics in Defense Conference (RAPID) | 978-1-6654-2223-9/21/$31.00 ©2021 IEEE | DOI: 10.1109/RAPID51799.2021.9521398

***Abstract*—Marine Hatchetfish camouflage strategies – silvering and counterillumination are imitated using photonics for enabling dynamic stealth transmission. 200MBaud/s 16-QAM-OFDM signal has successfully hidden in all domains during radio-over-fiber transmission and retrieved at the designated stealth receiver.**

Keywords— Optical security and encryption, RF photonics, bioinspired photonics.

I. Introduction

The emerging 5G and beyond RF systems facilitate the proliferation of high-demand large-bandwidth information technologies. Radio-over-fiber network technology is a critical part of such an RF system for supporting long distance and high-speed transmission that spans across large geographic domains encompassing different national interests. Currently, most security strategies are based on encryption in media access control (MAC) or higher layers [1], meaning only data frames are encrypted but not the control frames or the headers. This is problematic because the secret information is no longer secure once the attacker found the signature of the transmitted signal in the physical layer. To minimize vulnerability in the optical physical layer, optical encryption and steganography schemes have been proposed [2-4]. While most research has been focusing on optical encryption, it is critical to provide steganography at the physical layer for achieving effective cryptography. Cryptography requires both encryption and steganography to effectively secure the secret message, just like hiding valuables in a locked safe (encryption) behind a secret bookcase door (steganography).

Looking back to our nature, Marine Hatchetfish has two effective camouflage strategies helping them to hide from their predators and preys [5]. Marine Hatchetfish has microstructured skin on its sides to achieve constructive interference at the ocean color, such that the fish itself is invisible to the predators, referring as silvering. Furthermore, Marine Hatchetfish also generates and directs light to its bottom part for matching its color and intensity to the surrounding, removing its dark appearance as seen from below, referring as counterillumination. The camouflage strategies provide all-domain concealment of the presence of Marine Hatchetfish. In this work, we borrow the two ocean camouflage strategies, mimic them with photonic phenomena to achieve stealth transmission of 200 MBaud/s 16QAM OFDM signal at 5 GHz over a 25-km of optical fiber. The bioinspired steganography successfully conceals the secret signal in plain sight in temporal, RF spectral, and optical spectral domains, by turning invisible using silvering and blending in using counterillumination. The stealth signal can only be retrieved at the designated receiver at the expected location under precise condition.

II. Experimental Setup and Results

Figure 1(a) is an illustration explaining the camouflage strategies in Marine Hatchetfish. Without silvering, the fish appears at a different color than its surroundings, making it visible and vulnerable to attack. With silvering, the microstructured skin of the Marine Hatchetfish allows constructive interference to occur only at the ocean color but not any other colors that could reveal the presence of the fish. Therefore, the fish would be invisible to the predator and prey, as shown in the right figure in Fig. 1(a)i. Furthermore, the fish would appear darker when seen from below with the absence of counterillumination, making itself visible to predators and preys, as in Fig. 1(a)ii. With counterillumination, light is directed to the bottom of the fish to match the intensity and

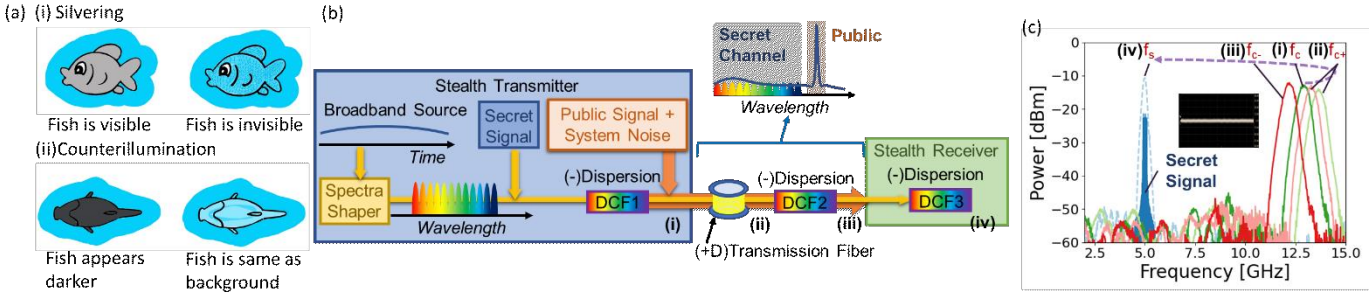

Fig. 1: (a) Illustration of camouflage strategies in Marine Hatchetfish. (i) Silvering - fish is constructively interfered at the ocean colors that makes the fish invisible; (ii) Counterillumination – fish illuminates itself to the same color and intensity as the background to blend in. (b)-(c) Illustration of steganography. (i) Destructive interference occurs at the stealth signal frequency (f_s); (ii) Transmission only pushes constructive interference condition to a much higher frequency (f_{c+}); (iii) Dispersion compensation fiber moves constructive interference condition back to f_c; (iv) An exact amount of dispersion at the stealth receiver allows constructive interference condition to occur at the stealth signal frequency.

978-1-6654-2223-9/21/$31.00 ©2021 IEEE

color of its surroundings, removing the darkness appearance as seen from below.

The optical implementation of the proposed bio-inspired dynamic RF steganography scheme is based on dynamic finite impulse response (FIR) through the generation of tunable optical comb carrier to match with the characteristic of the transmission channel. At the stealth transmitter, as shown in Fig. 1(b), the broadband light source is shaped by an optical wave shaper to construct the optical combs for the FIR. The corresponding optical comb spacing $\Delta\lambda_{FSR}$ [6] is expressed as $\Delta\lambda_{FSR} = 1/|D(L_{DCF1} + L_{DCF3})f_{FIR}|$, where D, L_{DCF1}, L_{DCF3}, f_{FIR} denote the dispersion coefficient, the lengths of the dispersive medium at the stealth transmitter (DCF1) and receiver (DCF3), and the desired constructive interference frequency. Therefore, the final shaped comb function would be, $T(\lambda) = cos\left(\frac{\Delta\lambda_{full}}{\Delta\lambda_{FSR}} \cdot \frac{\lambda}{2}\right) exp[-\frac{\lambda^2}{2\Delta\lambda_{FWHM}{}^2}]$, where $\Delta\lambda_{FWHM}$ and $\Delta\lambda_{full}$ are the full-width-half-maximum (FWHM) and total shaped optical bandwidth, respectively. Then, chromatic dispersion is used to introduce time delay between each of the optical comb line to form the FIR. The broadband nature of the optical comb carrier mimics counterillumination in Marine Hatchetfish, where the secret signal is spectrally blended in with and concealed by background optical noise.

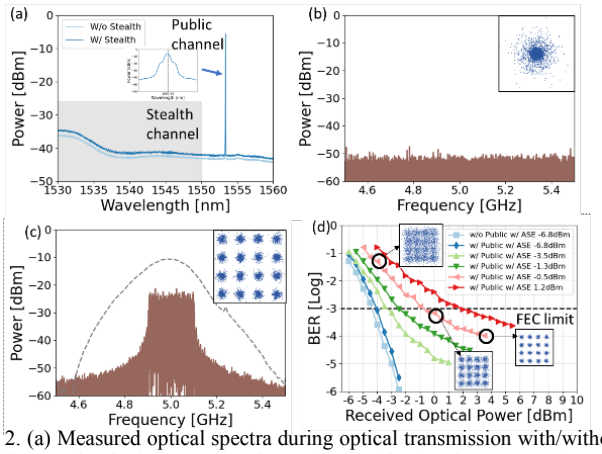

Fig. 2. (a) Measured optical spectra during optical transmission with/without stealth signal. Shaded area is where the stealth signal spectrum located; Measured RF spectra and constellation diagrams (b) during transmission, and (c) at the designated stealth receiver; (d) Meaured BER of the stealth 16QAM-OFDM signal and corresponding constellation diagram.

A 200 MBaud/s 16QAM-OFDM at 5 GHz generated from an arbitrary waveform generator is used as secret RF signal, which is modulated onto the optical comb carrier through a 12 GHz Mach-Zehnder electro-optic modulator. The modulated optical signal is launched to a dispersion compensating fiber (DCF1) to construct the desired FIR at a much higher frequency f_c (i.e. 13.22 GHz) than the secret signal f_s, as shown in Fig. 1(c)i. At the stealth transmitter, public optical channel at 1553.33 nm is combined with the stealth signal and broadband system noise, which is then sent to the radio-over-fiber network. The inherent dispersion in the 25-km transmission fiber will only move the FIR constructive interference frequency to an even higher frequency f_{c+}, keeping the stealth signal invisible (Fig. 1(c)ii). In a passive optical network, dispersion compensation (DCF2) may be applied to the last section of the transmission link. The amount of dispersion compensation needed will only move the constructive interference frequency back to a slightly lower frequency around f_{c-} but not enough to move it back to the stealth signal frequency at f_s (Fig.1(c)iii), keeping the stealth signal invisible through silvering. At the designated stealth receiver, a thin film filter at 1553.33 nm is used to drop the public channel and launch the rest of the transmission to the designated stealth receiver. The stealth receiver has a piece of dispersion compensating fiber (DCF 3) of the exact amount of dispersion to push the constructive interference frequency back to the stealth signal frequency f_s, as shown in Fig.1(c)iv. Therefore, silvering is achieved at any point of the transmission to make the stealth signal invisible to the attacker. First, time domain of the stealth signal looks like noise only (inset of Fig. 1(c)). Also, the stealth signal blended in well with the background noise in the optical spectrum using counterillumination (Fig. 2(a)). The RF spectra and constellation during transmission and at the designated stealth receiver (Fig. 2(b)(c)) prove that the stealth signal disappears in the attacker's eye unless a designated stealth receiver at the expected location is used to retrieve the stealth signal.

While the concelment of stealth signal is important and can be improved with the use of a stronger broadband optical system noise, the successful retrieval of stealth signal is equally important. There is a trade-off between the strength of system noise and the quality of the received stealth signal. Fig. 2(d) is the bit-error-rate (BER) measurement of the received stealth signal at different power level of system noise. It is observed that power penalty is increased while the BER is still below FEC limit as the system noise is increased. According to the blue and light blue curves, we also observed that the presence of public signal has insignificant effect on the stealth signal BER.

III. Conclusion

A novel RF steganography scheme inspired by ocean camouflage strategies – silvering and counterillumination of Marine Hatchetfish is proposed and experimentally demonstrated. Silvering is achieved using highly tunable finite impulse response to make the stealth signal invisible in the attacker's eyes, while counterillumination is achieved using broadband optical comb source to blend into the system noise. The secret signal is successfully concealed in all domains that the attacker could have access to. The experimental results of OFDM stealth transmission suggest that an effective steganography solution is achieved.

This work is supported by NSF (1653525 and 1917043).

References

[1] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography* (CRC press, 2018).

[2] M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, "Optical layer security in fiber-optic networks," IEEE Transactions on Information Forensics and Security **6**, 725-736 (2011).

[3] M. Bi, X. Fu, X. Zhou, L. Zhang, G. Yang, X. Yang, S. Xiao, and W. Hu, "A key space enhanced chaotic encryption scheme for physical layer security in OFDM-PON," IEEE Photonics Journal **9**, 1-10 (2017).

[4] B. Wu, Z. Wang, Y. Tian, M. P. Fok, B. J. Shastri, D. R. Kanoff, and P. R. Prucnal, "Optical steganography based on amplified spontaneous emission noise," Optics express **21**, 2065-2071 (2013).

[5] E. I. Rosenthal, A. L. Holt, and A. M. Sweeney, "Three-dimensional midwater camouflage from a novel two-component photonic structure in hatchetfish skin," Journal of The Royal Society Interface **14**, 20161034 (2017).

[6] Q. Liu, J. Ge, and M. P. Fok, "Microwave photonic multiband filter with independently tunable passband spectral properties," Optics letters **43**, 5685-5688 (2018)