Physical Layer Network Security Based on Optical Processing using Compact Passive Devices

Mable P. Fok, Yanhua Deng, and Paul R. Prucnal
Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA
Email: mfok@princeton.edu

Abstract

We propose the use of optical processing for enhancing network security. Optical steganography, anti-jamming, and optical encryption is experimentally demonstrated. Service availability is also improved during physical infrastructure attacks using optical CDMA for backup channels.

Introduction

Network security is gaining lots of attention due to the dramatic increasing network usage in various personal, commercial and military applications. Therefore, it is important to improve security in different layers of the network. The physical layer of networks are vulnerable to different types of attacks, including jamming, physical infrastructure attacks, eavesdropping and signal detection [1]. In this paper, we demonstrate multilayer security implemented optical signal processing to improve both the confidentiality and availability. Optical signal processing is a good candidate for enhancing information security without introducing substantial latency into the system. Because of its inherent high speed and parallelism, optical implementation of physical layer security can match the increasing data rate of today’s communication networks. Besides, no electro-magnetic signature is generated by optical devices that protect the system from attacks.

Our work exploits several types of compact passive devices, including a 35-cm highly nonlinear bismuth oxide fiber (Bi-NLF), a pair of chirped fiber Bragg gratings (FBG), and FBG arrays for optical signal processing. The enhancement of information security using optical signal processing is discussed in four areas:

1. Preventing eavesdropping and side-channel detection using high-speed optical data encryption;
2. Inhibiting the observation of traffic patterns using optical steganography;
3. Reducing the probability of interception and altering the data using optical CDMA and code hopping;
4. Improving service availability in the presence of physical infrastructure attacks using anti-jamming and optical CDMA for backup channels.

Preventing Eavesdropping Using Optical Encryption

Encryption is important in information security since it enhances the confidentiality of the data network. Without the knowledge of the encryption key, the data content cannot be recovered. Our scheme is based on four-wave mixing (FWM) in a 35-cm Bi-NLF. The short length of Bi-NLF ensures that our scheme is compact and has a low latency. The optical polarization is used to carry the information in the key and the data as shown in Table 1. Pol A and Pol B are orthogonal to each other. KEY# is orthogonally polarized with respect to KEY. FWM is a polarization sensitive process, and the mixing effect is the strongest if the two input signals have the same polarization, while no FWM occurs when they are orthogonally polarized. Therefore, the generation of the new frequency component will be maximized when the key and the data possess the same polarization. Hence, an encrypted signal (FWM /wKEY) and its inverted form (FWM /wKEY#) are generated by FWM in the Bi-NLF according to Table 1.

Table 1: Operating condition of the FWM based optical encryption

DATA	KEY	KEY#	FWM /wKEY	FWM /wKEY#
0 (Pol A)	0 (Pol B)	0 (Pol A)	0	1
0 (Pol A)	1 (Pol A)	1 (Pol B)	1	0
1 (Pol B)	0 (Pol B)	0 (Pol A)	1	0
1 (Pol B)	1 (Pol A)	1 (Pol B)	0	1

In the FWM-based encryption scheme, DATA and KEY are launched to a short piece of Bi-NLF [2]. The encrypted signal is extracted from the FWM output using an optical bandpass filter. Figure 1 (a) – (c) shows the input signal, encryption key and the encrypted signal, respectively. The encrypted data pattern agrees with the output in Table 1.

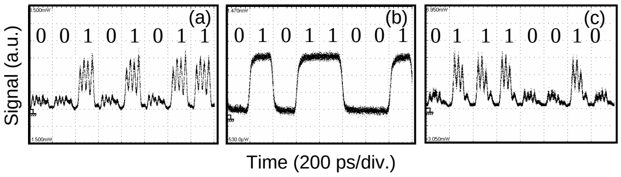

Fig. 1: Temporal profiles (a) demodulated optical CDMA signal with bit pattern of “00101011” (b) demodulated optical encryption key with bit pattern “01011001” (c) optically encrypted output.

To make it more difficult for the eavesdropper to analyze the encrypted signal, dual-pump four-wave mixing is employed to achieve optical encryption with interleaved waveband switching modulation [3]. Instead of on-off keying, two spectrally interleaved wavebands are used to represent bit 0 and bit 1 of the encrypted signal. The use of interleaved waveband switching modulation does not require an intensity change between bit 0 and bit 1. Thus, the encrypted data does not show any temporal signature of the plaintext or the ciphertext. To achieve interleaved-waveband switching modulation, both the KEY and KEY# are modulated at two wavelengths with a slight spectral offset. Both the encrypted signal and an inverted copy of it are generated, represented by two interleaved wavebands. Thus, by extracting the FWM output, an eye diagram as shown in Fig. 2 is resulted. Both the bit 0 and bit 1 are having the same intensity.

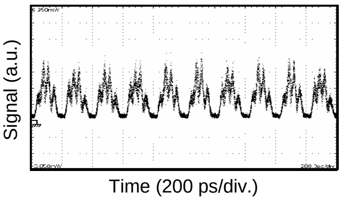

Fig. 2: Temporal profile of the encrypted signal with interleaved waveband switching modulation.

Inhibiting the Observation of Traffic Through Optical Steganography

To inhibit the observation of traffic patterns, we propose and demonstrate the use of optical steganography. Steganography by itself does not secure the signal, but it provides an additional layer of security that can supplement data encryption by hiding the existence of data transmission underneath an existing public channel. By spreading the optical signal in both the frequency and temporal domains, - a noise-like character having low power spectral density and low temporal amplitude is produced, which achieves optical steganography.

In our approach to optical steganography, the spreading function is implemented using group velocity dispersion in chirped FBGs [4]. The stealth signal submerges beneath the public channel and background noise. As a result, it is difficult for an eavesdropper to observe the signal without specific knowledge of the spreading function. Using chirped FBGs, compared with our previous work, the device length is dramatically reduced from 20 km to a couple of centimeters. We use an RZ signal as the stealth signal, while the public channel is a WDM signal. By spreading the stealth signal and launching it into the network with the public channel and system noise, both temporal and spectral domain hiding is achieved. Figs. 3(a) and (b) show the eye diagrams of the WDM signal without and with the stealth channel, respectively. The two eye diagrams look indistinguishable. At the receiver, the stealth signal is restored through the use of a matched pair of chirped FBGs with opposite signs of dispersion.

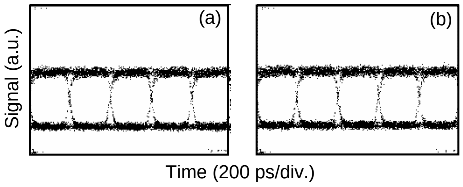

Fig. 3: Eye diagrams (a) WDM public channel only (b) WDM public channel with stealth channel.

Reducing the Probability of Interception Using Optical CDMA and Dynamic Code Hopping

Optical CDMA provides greater scalability and spectral efficiency than conventional optical multiplexing techniques such as WDM or TDM [5]. Using the same number of wavelengths, optical CDMA can accomodate many more channels. Optical CDMA codes are generated through the use of compact FBG arrays. In a multi-user system, the large number of codes obscures the signal. Therefore, brute force decoding is needed for the eavesdropper for detecting the signal. Though the large code set provides obscurity, they are not secure. Thus, dynamic code hopping based on a secure key is required to improve confidentiality. Dynamic code hopping can be achieved using high-speed switches or through the combination of frequency hopping and FBG arrays. Details will be discussed in the presentation.

Improving Service Availability Using Optical CDMA Backup-Paths and Anti-Jamming

Besides confidentiality, network availability is also an important issue of concern. Different types of attacks such as physical infrastructure attacks and signal jamming can result in the denial of service. Optical CDMA has the unique characteristic of soft-blocking resulted from the large cardinality of the optical CDMA code set. This unique characteristic can be used to protect the network without wasting any bandwidth. Unlike the conventional approach to provide backup paths that requires the permanent reservation of all or part of the bandwidth, optical CDMA allows all paths to be fully utilized to carry working data. In the event of failure of a path, the data is routed onto another working path, at the expense of a slightly higher BER.

To provide anti-jamming, FWM is used to translate the signal into another waveband. Due to the large nonlinear coefficient of the Bi-NLF, a short length of fiber is sufficient for FWM, resulting in a wide FWM conversion bandwidth. In the presence of optical jamming, FWM can be used to translate the frequency simply by controlling the pump wavelength [2].

Conclusions

We propose and demonstrate real-time optical signal processing using compact passive devices for enhancing physical layer network security. Optical encryption, optical steganography, obscurity, survivability, and anti-jamming are demonstrated. The compact passive devices we use, including highly nonlinear bismuth oxide fiber, chirped fiber Bragg gratings, and fiber Bragg grating arrays, make our approach both practical and have low latency.

References

1. P. R. Prucnal, Optical Code Division Multiple Access: Fundamentals and Applications, (Taylor and Francis, New York, 2006)
2. M. P. Fok et. al, IEEE/LEOS Annual Meeting 2008, ThG 3.
3. M. P. Fok et. al, “All-Optical Encryption Based on Interleaved Waveband Switching Modulation for Optical Network Security,” accepted by Optics Letter.
4. M. P. Fok et. al, OFC/NFOEC 2009, JThA57
5. V. Baby et al., IEEE Photon. Tech. Lett., vol. 17, no. 1, pp. 253-255, Jan. 2005.