Adaptive Photonic Beamforming for Physical Layer Security of Mobile Fronthaul Networks

John Chang\textsuperscript{1,2}, Neda Cvijetic\textsuperscript{2}, Ting Wang\textsuperscript{2}, Paul Prucnal\textsuperscript{1}
\textsuperscript{1}Princeton University, Lightwave Laboratory, Princeton, NJ 08540
\textsuperscript{2}NEC Laboratories America, Princeton, NJ 08540
\texttt{neda@nec-labs.com}

Abstract: We experimentally demonstrate adaptive photonic beamforming for physical layer security of mobile signals over optical fronthaul networks. 33dB signal suppression to eavesdroppers located 0.1m away from intended users is achieved after 8km SSMF transmission.

OCIS codes: (060.2330) Fiber optics communications; (060.4785) Optical security and encryption.

1. Introduction

Emerging mobile services, such as mobile banking and desktop-to-mobile applications, require both increasingly high data rates and high data security. To address the rising bandwidth demand, short-reach (≤10km) optical fronthaul networks that enable fiber-optic connectivity between a centralized cloud processing site and mobile users have emerged as the most promising approach for high-speed mobile data transfer [1-4]. However, enhancing data security via optical-layer techniques in fiber-optic fronthaul networks has not been considered. The potential of such physical-layer security is tremendous, however. For example, while encryption or steganography [5] can be cracked by malicious eavesdropping, optical-layer techniques such as photonic beamforming [6] can create a signal null in the spatial direction of an eavesdropper, preventing eavesdroppers from physically receiving data-sensitive signals in the first place. With sufficiently high beamforming resolution, this can enable mobile signals to be received solely by an intended user based on the user’s spatial location and mobile signal frequency. In this paper, we present the first experimental demonstration of adaptive photonic beamforming for physical-layer security in optical fronthaul of mobile data, achieving 33dB signal cancellation to an undesired eavesdropper located 0.1m from the intended user. High spatial resolution is thus confirmed for 8km standard single mode fiber (SSMF) fronthaul distances.

2. Proposed Physically-Secure Optical Fronthaul via Adaptive Photonic Beamforming

Fig. 1 shows the proposed secure fronthaul architecture using adaptive photonic beamforming. The adaptive finite impulse response (FIR) filters (i.e. frequency filter) and remote radio frequency (RF) antenna array (i.e. spatial filter) act jointly to form the photonic beamformer. Given the spatial co-ordinates and mobile signal frequencies of intended user(s), the photonic beamformer can create a signal null in unintended spatial directions by manipulating the beampattern that propagates through the optical fronthaul network. As shown in Fig. 1, the RF mobile signal from a centralized site is first applied as input to parallel optical adaptive FIR filters, which provide optical modulation and frequency filtering. The processed optical signals are then transmitted over parallel SSMF links to the remote RF antenna array. By proper assignment of the optical FIR filter coefficients, the remote antennas are turned into a distributed spatial filter that directs the output only to intended users. The configuration of Fig. 1 can thus be used to securely deliver data to users 1 and 3 while producing a null in the direction of user 2, or vice versa. By changing the weights of the FIR filters, the beamformer is made adaptive such that it can respond to mobile users and dynamically-changing environments. The adaptive coefficient assignment algorithm used in this work is based

![Fig. 1. Proposed secure optical fronthaul architecture.](image1)

![Fig. 2. Experimental setup; ADC: analog-to-digital converter.](image2)
on the $m$-ary random search, wherein one of $n$ possible filter coefficients is randomly selected and an $m$-ary search is performed on the entire weight space to find and store the optimal value. This is repeated until all $n$ coefficients are optimized, and only requires knowledge of mobile signal RF frequency, $f_{RF}$, and optical power parameters, supporting modulation format transparency. The detailed experimental setup is shown in Fig. 2. Continuous wave optical signals from 16 distributed feedback (DFB) lasers on $\lambda_1 = 1538.98 \text{nm}$ to $\lambda_{16} = 1563.05 \text{nm}$ were multiplexed with 200GHz spacing by an arrayed waveguide grating (AWG), optically amplified using an EDFA, and input to a 1:4 passive splitter for distribution to four parallel optical FIR filters. At each filter, a thermal-optic attenuator array controlled by a voltage signal determined by the $m$-ary random search algorithm (with $m = 10$, $n = 32$) was used to set filter coefficient amplitudes. The attenuators featured a 10$\mu$s per 0.1dB response time and a 30dB range, with outputs combined using an AWG. A Mach Zehnder modulator (MZM) with dual $\pi$-shifted outputs was used for optical modulation, with MZM outputs propagated through dual optical circulators (OCs) and fiber-Bragg grating (FBG) arrays with parallel delays, until reflected by a $\lambda$-specific grating to set filter coefficients delays. Each coefficient featured a positive and negative output, with the attenuator array used to select polarity. Upon exiting the FBGs, the dual OC outputs were combined by a 2:1 coupler to form an 8-tap optical FIR filter with 200 picosecond inter-tap delays. A sinusoid at $f_{RF} = 2.5 \text{GHz}$ was used as the mobile signal of interest (SOI) to be directed by the photonic beamformer to an intended user. After SSMF transmission (13dBm launch power) and photodetection (PD), the received RF signal power was measured at both intended user and eavesdropper locations, mutually separated by 0.1-0.5 meters. Beamformer performance was thus measured in terms of the signal strength ratio (SSR) at different locations. The received signal was digitized using an off-the-shelf ADC card and processed offline, with the adaptive algorithm used to maximize SSR via the coefficient assignment as described above. To also assess bit error rate (BER) of the fronthaul link, experiments were repeated with a baseband 6Gb/s pseudorandom binary sequence (PRBS)-based on off keying (OOK) signal connected as direct input to the optical modulators and FIR filters, and with BER measured using a cabled connection to a BER tester at the PD output.

Fig. 3 shows the experimental SSR measurements versus received power for various fronthaul distances. Maximum $SSR = 33 \text{dB}$ was achieved over 8km SSMF for intended user vs. eavesdropper separations from 0.1-0.5 meters, confirming high spatial resolution and accuracy of the proposed adaptive beamforming approach. Similar results were also obtained for an RF signal centered at $f_{RF} = 5 \text{GHz}$, verifying the adaptive beamformer performance across several $f_{RF}$ values corresponding to prominent mobile standards. From Fig. 3 it may also be observed that there is no SSR penalty for increasing fronthaul distance compared to optical back-to-back. Consequently, so long as minimum PD sensitivity requirements are met, increasing fronthaul reach will only result in optical FIR coefficient scaling that is proportional to aggregate received power and will not degrade SSR integrity. Fig. 4 plots measured BER curves for 6Gb/s OOK transmission, revealing a 2dB penalty for 8km SSMF transmission compared to optical back-to-back at forward error correction (FEC) limit $BER = 10^{-3}$, primarily due to chromatic dispersion effects.

4. Conclusions
We experimentally verified adaptive photonic beamforming for physical-layer security of mobile signals in optical fronthaul networks. 33dB signal suppression to an undesired eavesdropper was demonstrated with 0.1m separation between the intended user and eavesdropper after 8km SSMF transmission, confirming high spatial accuracy.

5. References