Polarization Mode Dispersion-Based Physical Layer Key Generation for Optical Fiber Link Security

Imam Uz Zaman, Anthony Bahadir Lopez, Mohammad Abdullah Al Faruque, and Ozdal Boyraz
Department of Electrical Engineering and Computer Science, University of California, Irvine, California, USA
{zamani, anthl10, alfaruqu, oboyraz} @ uci.edu

Abstract: A novel physical layer secret key generation technique for point-to-point optical fiber link security is proposed. It can efficiently generate high entropy symmetric cryptographic keys based on Polarization Mode Dispersion in optical fiber links.

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

1. Introduction

The Point-to-Point Optical Link (PPOL) is employed in various applications ranging from Ethernet systems to telecommunications backbone infrastructure as well as military communication system. Like any other communication media, optical fibers are susceptible to many security threats, including jamming, eavesdropping, interception, and physical infrastructure attacks [1]. For this reason, it is desirable to have a reliable cryptographic design to ensure security. Most of the state-of-the-art cryptographic algorithms require pre-shared secret keys, which can be easily accessible to attackers if they have comprehensive knowledge of the system. To address this issue, researchers have recently proposed to generate secret keys from the randomness of the physical environment [2–4]. In this paper, we present a novel symmetric secret key generation scheme for Point-to-Point Optical Link (PPOL) communication by exploiting underlying physical layer properties of the optical fiber under tight performance and memory constraints. In particular, we propose to exploit the Polarization Mode Dispersion (PMD) phenomenon to generate symmetric random distortion for a bidirectional fiber transmission line. Evolution of PMD in the standard Single Mode optical Fiber (SMF-28) is totally stochastic [5], so the security strength of generated keys based on PMD is appreciably high. However, strong PMD distortions primarily manifest itself over long distance fiber links that are >1000km. For this reason, we propose to use a cross-spliced random segment of PM fibers at both ends of the SMF link to mimic a strong PMD effect. In this paper, we show that random modulation of a probe signal caused by PMD is reciprocal despite the presence of optical nonlinearities, dispersion, and noise at the system. We also show that up to 128-bit symmetrical secret keys can be generated for different bitrates of 40Gb/s and 60Gb/s over link lengths >50km. Further, if necessary, the key generation technique can be used to create 256 bit keys and is limited by only the computational power of the software.

2. Method overview

The proposed physical layer secret generation method is based on the changes of PMD in the long optical fiber. PMD is a random effect since it relies on the details of the instantaneous weak birefringence state of the fiber link. Over time, the PMD varies with physical parameters such as temperature, pressure, external and internal stress etc. However, depending on the data rate in a normal telecommunication link with a state-of-the-art SMF-28 with PMD coefficient of $0.04 ps/\sqrt{km}$, the PMD effect manifests itself beyond 2000km. To mimic the effect of the PMD in a long haul communication link in a small PPOL, (Fig. 1) we incorporate two pieces of Randomly Spliced Polarization Maintained fibers (RSPMF) at both transceiver ends. The proposed system works in two modes i.e. communication mode and key generation mode. The switching time between these two modes is below a half millisecond due to the use of fast opto-mechanical MEMS switches. As a result, during the key-generation mode, the Differential Group Delay (DGD) between two Principal States of Polarization (PSP) will be higher and stochastic due to the long SMF-28 fibers in between transceivers and SMF pigtails. This approach facilitates the key generation technique and

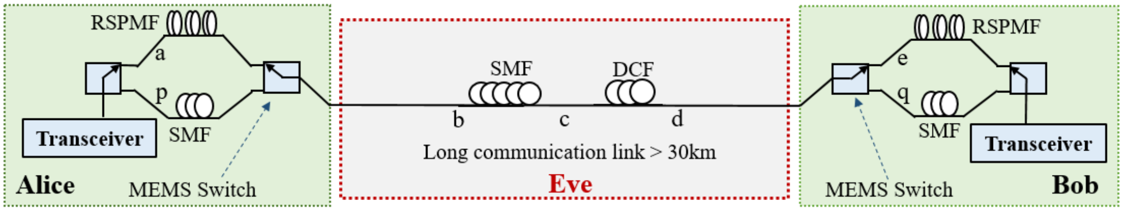

Fig. 1. Proposed Key Generation Scheme

increases the entropy of the keys. To assess the feasibility of our proposed system, we develop a model of the communication link with two transceivers, *Alice* and *Bob*. When *Alice* and *Bob* want to generate a symmetric key, they need to exchange a pre-defined probe signal (PRBS modulated bit pattern with a predefined length). During the key generation mode, this signal will go through a high PMD effect due to the randomly spliced PMF segments. This can be described as the data path of (a-b-c-d-e) in Fig. 1. The changes in the Differential Group Delay (DGD) in a long fiber is entirely stochastic and follows a Maxwell probability distribution as given in equation 1[5], where $\boldsymbol{\Delta\tau}$, $\boldsymbol{l}$, $\mathbf{q^2}$ are the average DGD, fiber length and the variance of the Maxwell distribution, respectively.

$$P(\Delta\tau, l) = \frac{2\,\Delta\tau^2}{\sqrt{2\Pi}q^3} exp[-\frac{\Delta\tau^2}{2q^2}] \qquad (1)$$

Owing to the orthogonality of the input principle state of the polarization (PSP), any input polarization can be written as a vector sum of its components. The output electric field vector in the time domain will look like:

$$\overrightarrow{E_{out}(t)} = r_+ \overrightarrow{\varepsilon_{out+}} e^{j\phi+} E_{in}(t+\tau_+) + r_- \overrightarrow{\varepsilon_{out-}} e^{j\phi-} E_{in}(t+\tau_-) \qquad (2)$$

Where r_+ and r_- are the complex projection, ε_{out+} and ε_{out-} are unit vectors of the output PSP and $\phi\pm$ are the constant phases picked by the polarization modes, $\Delta\tau = |\tau_+ - \tau_+|$ represents the DGD. DGD will result in random complex modulation of the probe signal. For our simulation, we followed the famous discrete wave plate model and Jones matrix calculation[6,7]. If we ignore the polarization dependent loss, the frequency dependent Jones matrix for any wave plate can be represented by equation 3, where $S(\theta)$ denotes the rotation of the fast axis of the wave plate by θ degree from +x axis, L is the fiber length, n_{fast} and n_{slow} are the refractive indices for fast and slow mode respectively.

$$M(\omega) = S(-\theta) e^{\frac{-j\omega L(n_{fast}+n_{slow})}{2c}} \begin{bmatrix} e^{\frac{-j\omega L(n_{fast}-n_{slow})}{2}} & 0;0 & e^{\frac{j\omega L(n_{fast}-0n_{slow})}{2}} \end{bmatrix} S(\theta) \qquad (3)$$

For a high speed (>10Gbps) transmission system, the data transmission rate is higher than the rate of change of average DGD[8]. For this reason, we approximate the communication channel response as constant during the probe signal propagation. In our simulation, we found that there is high reciprocity of the modulated probe signal (> .85 Pearson correlation coefficient between *Alice* and *Bob*'s signals), and there is also high randomness (approx. > 12 bits of Shannon entropy for each group of samples). Conventionally, *Eve* does not have direct access to the transceiver systems, but may have access to a point along the communication link as shown in Fig.1. As a result, *Eve* will not be able to observe the randomly spliced PMF, the probe signal, or input polarization state of the signal. Moreover, even if we assume *Eve* has information about these systems or features, *Eve* will not be able to generate the same keys as *Alice* and *Bob* due to the stochastic nature of the PMD. As a result, *Eve* will not be able to eavesdrop on the encrypted channel. After the key establishment agreement between *Alice* and *Bob*, the system will go into communication mode and send signals via the p-b-c-d-q path just as in a conventional point-to-point optical fiber link.

In our key generation technique, each transceiver will take a set of samples from the pre-defined probe signal (PRBS) and quantize their signal strengths (in Amps) into symmetric key bits. Each transceiver will compute upper (*Thr*$_{upper}$) and lower (*Thr*$_{lower}$) thresholds of a group of samples, SampleGroup, with group size ***(g)***, based on their mean and variation [4,9]. The upper threshold, $Thr_{upper} =< SampleGroup > +\alpha \times \sigma(SampleGroup)$ and the lower threshold, $Thr_{lower} =< SampleGroup > -\alpha \times \sigma(SampleGroup)$, where **< x >** and **σ(x)** represent mean and variance of ***x*** respectively. Both ***g*** and **α** are parameters that can be derived or altered according to the variance of the system (the higher the variance, the higher **α** and ***g*** should be). The bit quantization rule for each sample value is:

if SampleStrength >= Thr$_{upper}$ *then Key Bit = 1;*
else if SampleStrength <= Thr$_{lower}$ *then Key Bit = 0;*
else do not quantize.

In the case of potential mismatching key bits, we include an index mismatch removal step, which takes the indices of the values selected for quantization and removes the mismatching ones. More specifically, during the sampling step, both Alice and Bob store the index of each value they selected into their private lists, *Indices*$_{Alice}$ and *Indices*$_{Bob.}$ Then they exchange and remove mismatching indices in their respective lists. The result will be matching sets of indices to be used for generating the symmetric keys. Since this step involves no sharing of information about the actual signal strength values or the actual bits, *Eve* will not gain valuable information about the symmetric keys. After the algorithm meets the required key size, the resulting key will be tested and used for encrypting future messages.

3. Simulation results and model verification

Signal propagation through the system is modeled by a combination of commercial simulation tools including VPI transmission Maker and Matlab. In particular, we used VPI transmission Maker to generate the PRBS, to create the modulated NRZ optical signal, to detect the signal at the detector and to include all the noises like Relative Intensity Noise (RIN), shot noise, thermal noise etc. The propagation of the optical signal in both directions, the reciprocity check, entropy estimation, and the key generation algorithm are all implemented in MATLAB based on the split-step method. We performed simulations according to different bit rates (40Gb/s, 60Gb/s) and different link lengths to check the reciprocity and entropy of the modulated signal due to high PMD. Fig.2 shows the randomly modulated signal received by Alice and Bob at 60Gb/s. Corresponding threshold levels to generate keys are also shown in Fig. 2. The generated keys for different link lengths and data communication rate are showed in Fig.3. To minimize the simulation times, we used a 2^7-1 PRBS and 256 bits to emulate data propagation. Calculations are performed for 50km and 60km links to generate up to 128-bit secret keys. Results show that symmetric secret keys can be generated with little or no bit mismatch rates (0-3.6% when generating 200-500 secret key bits according to different $\boldsymbol{g}$ and $\boldsymbol{\alpha}$ values). By using the same approach with longer PRBS streams, it is also possible to generate >256-bit secret keys, if necessary.

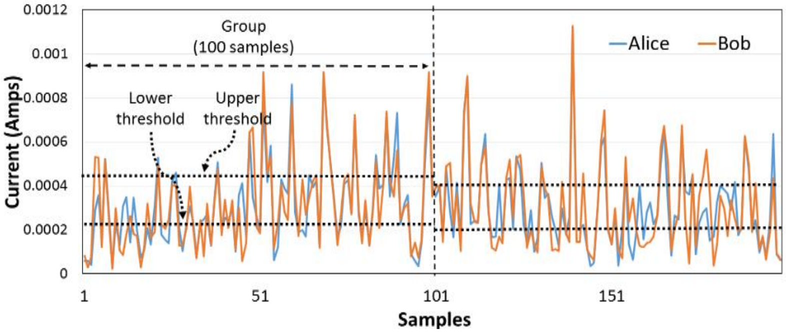

Fig. 2. Samples and Thresholding for 60Gb/s PMD Modulated Data

<table>
<tr><th>Parameters</th><th>Generated 128-Bit Keys of Alice/Bob (60Gb/s - 50km link)</th><th>Parameters</th><th>Generated 64-Bit Keys of Alice/Bob (60Gb/s - 50km link)</th></tr>
<tr><td rowspan="3">g = 150
α= .6</td><td rowspan="3">00001000000100010010110100111010011100001101011110001100010010001100001000001000100101101001110100111000011010111100011000100100011</td><td>g = 100
α = .8</td><td>0000100001000011101011110111000111111111001010001100111010110000</td></tr>
<tr><td><b>Parameters</b></td><td><b>Generated 32-Bit Keys of Alice/Bob (40Gb/s - 60km link)</b></td></tr>
<tr><td>g = 64
α = .5</td><td>01101010010010010001000001001011001</td></tr>
</table>

Fig. 3. Examples of Generated Symmetric Keys

4. Conclusion

We proposed and simulated a novel key generation scheme which can be incorporated in any existing PPOL to establish secret keys for symmetric encryption. We showed that the PMD effect can be exploited as a source of physical randomness to generate high entropy symmetric secret keys. With our proposed system, we successfully generated 32, 64 and 128 bit-keys.

5. References

[1] P.R. Prucnal, Optical Code Division Multiple Access: Fundamentals and Applications, CRC Press, 2005.

[2] M. Rostami, J.B. Wendt, M. Potkonjak, F. Koushanfar, Quo Vadis, PUF?: Trends and Challenges of Emerging Physical-disorder Based Security, in: Proc. Conf. Des. Autom. Test Eur., European Design and Automation Association, 3001 Leuven, Belgium, Belgium, 2014: p. 352:1–352:6.

[3] K. Kravtsov, Z. Wang, W. Trappe, P.R. Prucnal, Physical layer secret key generation for fiber-optical networks, Opt. Express. 21 (2013) 23756. doi:10.1364/OE.21.023756.

[4] J. Wan, A.B. Lopez, M.A. Al Faruque, Exploiting Wireless Channel Randomness to Generate Keys for Automotive Cyber-physical System Security, in: Proc. 7th Int. Conf. Cyber-Phys. Syst., IEEE Press, Piscataway, NJ, USA, 2016: p. 13:1–13:10.

[5] C.D. Poole, Statistical treatment of polarization dispersion in single-mode fiber, Opt. Lett. 13 (1988) 687. doi:10.1364/OL.13.000687.

[6] F. Curti, B. Daino, Q. Mao, F. Matera, C.G. Someda, Concatenation of polarisation dispersion in single-mode fibres, Electron. Lett. 25 (1989) 290. doi:10.1049/el:19890202.

[7] N.C. Pistoni, Simplified approach to the Jones calculus in retracing optical circuits, Appl. Opt. 34 (1995) 7870. doi:10.1364/AO.34.007870.

[8] M. Brodsky, N.J. Frigo, M. Boroditsky, M. Tur, Polarization Mode Dispersion of Installed Fibers, J. Light. Technol. 24 (2006) 4584–4599.

[9] K. Ren, H. Su, Q. Wang, Secret key generation exploiting channel characteristics in wireless communications, IEEE Wirel. Commun. 18 (2011) 6–12. doi:10.1109/MWC.2011.5999759.