European Conference on Optical Communication (ECOC) 2022 © Optica Publishing Group 2022

Network Authentication, Identification, and Secure Communication through Optical Physical Unclonable Function

Pantea Nadimi Goki[(1)], Thomas Teferi Mulugeta[(1)], Nicola Sambo[(1)], Luca Potì[(2,3)]

[(1)] Scuola Superiore Sant'Anna, Pisa, Italy, pantea.nadimigoki@santannapisa.it
[(2)] Photonic Netowrks and Technologies Laboratory, CNIT Pisa, Italy
[(3)] Universitas Mercatorum, Rome, Italy

Abstract *We propose a new method for network authentication, identification, and secure communication, using the optical photonic physical unclonable function Challenge-Response (PUF-CRPs) database protocol. We investigated the database performance generated with the proposed protocol by identifying 150 networks ID.*

Introduction

Recently, research effort has been directed to methods and models for uniquely identifying unknown elements (e.g., fiber type) in a network. Among them, the work in [1] exploits the Rayleigh backscattering to identify the fiber type: indeed, the manufacturing features of an optical fiber drive a specific Rayleigh backscattering pattern over the fiber. Thus, this pattern can be seen as a "signature" of the fiber and can be exploited to identify the fiber type. Such "signature" identification method may find applications within several use cases, such as network devices' census and network security. Regarding network device census, as highlighted in [2], it is quite common that network operators may be not fully aware of all the deployed fiber types in a network. This implies problems in quality of transmission estimation, increasing estimation inaccuracy and forcing the operator in assuming even higher network margins than what expected, with a consequent underestimation of the optical reach and an increase of the costs for regeneration [3]. Security is a fundamental aspect to assure reliable communication networks and to avoid unauthorized access to the information transmitted over a system [4]. Indeed, network infrastructures may be subject to attacks aimed at violating the availability, the integrity, and the confidentiality of communications. Attacks may be of several types: e.g., tampering consisting of making fake nodes or jamming introducing harmful signals in the network. Thus, the extension of "signature" from fibers to a generic network element may be fundamental for network operators, e.g. to detect the presence of a fake network element (tampering).

In this paper, we propose a method for enhancing network security by devoting a signature to the network, exploiting optical Physical Unclonable Functions (PUFs). PUF is an unclonable and randomly disordered physical system that reacts to external stimuli. PUFs define new identification techniques based on the *challenge-response* pairs (CRPs) protocol. The PUF function maps a determined input (*Challenge*) to an output (*Response*) and provides a unique database made of CR pairs (CRPs). The function is individual for each PUF. PUFs are categorized into several types. Among them all, the optical PUF has superiority due to its high ML-attack resistance [5]. Rayleigh backscattering pattern (RBP) of any optical fiber is a unique and unclonable feature that is caused at the molecular level structure and can be used as optical PUF for the fiber signature [1, 6]. In this paper, we extend the fiber signature to the network signature. Incorporating the fibers' signature (RBP) as the network fingerprint, we propose a PUF-based ID for the network authenticity. This method comprises two strategies: CRP-based remote identification and direct measurements for utilizing long-haul and short-haul communication networks, respectively.

Network Identification

PUF CRPs must be unique, unpredictable, and numeric modeling attacks (digital clones) resistible. Hence, no simulation will predict the exact PUF *response* over the input *challenge*. We extend the concept of PUF from fibers to network, defining the PUF-based network ID as a merge of the fibers' signature and relying on fiber parameters in [1]. A distributed Rayleigh scattering-based optical frequency domain reflectometry (OFDR) system has been employed in [1] to generate a PUF database for the identification of a single-mode fiber (SMF). In this case, SMF with the light propagating into it represents the *challenge*, whereas stimulated RBP the *response*. Moreover, the CRPs' uniqueness is experimentally demonstrated [1]. Here the PUF function is given by randomly distributed particles, much smaller than the

Disclaimer: Preliminary paper, subject to publisher revision wavelength of the light, along the fiber core that causes the fluctuation in material density along the fiber due to the fabrication process. The interaction of propagating light with these fiber particles results in Rayleigh scattering. Differences in the Rayleigh scatter patterns are due to the unknown position and different distribution of the particles into the fiber length. Exploiting this phenomenon, we simulated RBPs with a random number of scattering particles randomly located in each section of the fiber. We follow the same OFDR and fiber parameters employed in [1]. Hence, in our simulation, we chose 10m fiber, separated into 2500 sections with a length of 4mm. RBP has been obtained with the total acquisition time of 0.5s for 4mm fiber under test (FUT). The RBP detection is based on coherent optical frequency domain reflectometry, wherein, the source, a CW laser whose frequency is linearly swept, is separated into the local oscillator (LO) and the signal beam propagating into the FUT. The back reflected beam is detected through the coherent receiver (Rx) while beating with the LO. Since the reflected beam at a single point in a FUT is a time-delayed replica of the linearly frequency-swept beam, a single reflection point yields the photocurrent of a single beat frequency [7]. The detected optical power is given by the summation of the single reflection components and their interference together [1,7]. The OFDR system is able to collect spatially continuous RBPs along the fiber with sub-millimeter level spatial resolution, and we can select any arbitrary length of the fiber for collecting its signature [1]. The RBP signal obtained in the frequency domain will transform to the spatial domain by applying a Fast Fourier transform (FFT), where the result is the fiber signature. It is worth mentioning that applying the same *challenge* used in the simulation will not give the same *response* as in experimental measurement due to the PUF's unpredictability nature. We performed the simulation proof of concept by generating the CRPs database for the network identification. We demonstrate a network signature, considering a simple network composed of two fiber-type elements, and then we extend the method for extensive networks. Demonstrating signature with high security to the cascaded fiber elements is performed following five steps. In the first step, we extract the RBP of each fiber element in the spatial domain by performing FFT to the optical frequency domain signal. In the next step, a scanning window is applied to the spatial domain signal of each fiber to select the query data for exerting the KNN algorithm (finds k-nearest neighbor), as is illustrated in Fig. 1(a). Using the KNN algorithm leads to selecting a different set of data for each fiber, depending on its RBP, and makes the signature stronger. By overlapping the obtained KNN results of two fibers, we acquire the intersection points of the overlapped patterns. After that, the intersections data points are encoded into the binary domain. Afterward, the obtained result are converted to a binary image (genuine image) utilizing a binary key. The key is a binary sequence generated randomly and stored in the database. The binary image is stored in the database as the signature (ID) of the network. By performing a cross-correlation between the interested network ID and the stored images in the database, it is possible to uniquely identify the genuine network from the impostor one. Encoding the intersection data to the binary domain and storing the binary image instead of them in the database helps to provide very high accuracy and enhances the security of ID. Even though an adversary accessed the data points for generating the binary image, the generated image without the key would be different from the genuine one. For the performance evaluation of the proposed method, 125 independent network IDs (binary images) were generated and enrolled in the database. The created database consists of 125 *challenge/response* pairs and the related keys. Thus, the *challenge* is the RBP of the selected part of the fibers in the networks, and the *response* is the binary image. We also generated 25 new IDs without enrolling them in the database. Afterward, we investigated 150 IDs employing a cross-correlation to match the given image with the database. None of those 25 IDs was identified by the database, only those 125 IDs, which had been enrolled, were identified, and each image had only one match.

Direct Measurements and CRP-based Remote Identification

We considered a network with three components and proposed two ways for generating databases (D_1 and D_2 respectively). D_1 is obtained by overlapping the KNN data of the three fibers. Here, the converted data into the binary domain have the same length as the binary data of the overlapping two fibers (320bits, that can be increased to enhancing security). The binary image (ID) is obtained by adding the key_1. The key_1 is randomly generated for this network and is stored in the database.

D_2 is generated using the intersection data of each couple of fibers (1,2&2,3). Data points are converted to the binary domain and cascaded. Consequently, the length of the binary data is

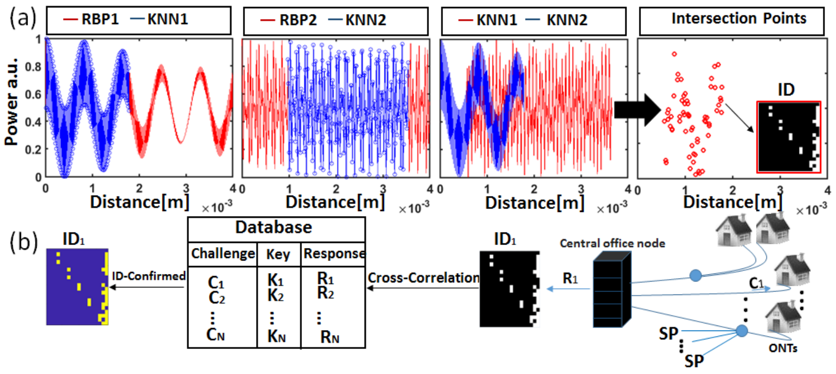

Fig. 1: (a) Simulated RBP in the spatial domain, and the KNN acquired data from fibre1 and fibre2.The obtained intersection points are converted to the binary image ID (b) Networks architectures with proposed identification methods. SP: service provider. ONT: optical network terminals.

twofold compared with the binary data of overlapping two fibers. In this step, a new key (key$_2$) is generated randomly. Key$_2$ is an integer number (key$_2$ >10) showing the start point for choosing binary data with the same length as overlapped two fibers data (320bits). The imposed restriction on key$_2$ is for selecting data from both intersection data (1,2&2,3). Finally, by randomly generating another key (key$_1$) and adding it up to the binary data, the binary ID will be generated and stored in D$_2$. The same methods can employ more than three elements. Consider different network architectures along with one of the proposed databases. In the p2p architecture, the central node can identify each node by sending a CW to that and measuring the RBP, adding the key from the database, and generating the ID. Performs a cross-correlation to match the ID with the database and confirms that (i.e., direct-measurement (DM)). In PON architecture that implements a point-to-multipoint layout in which a single optical fiber serves multiple endpoints, every node can identify the central office. Whereas, in the multipoint-to-point scheme in which service providers (SP) exist, each node can get identified by SPs using DM, Fig. 1(b). Despite the random nature of the RBP, which introduces it as a high-level PUF, they are intrinsically weak and are hard to acquire [7], which makes them inconvenient identification solutions for long-distance. We propose a strategy for using the CRP-RBPs database for the long-distance. In this case, instead of RBP measurement by the central node (p2p), the ID is sent to the central node by each nominated node. Despite the first strategy, in which only the central node accessed the whole database, with this strategy, everyone can access the *challenges*/keys library unrestrictedly. The crucial point here is the unclonable feature of PUF, where the adversary cannot generate the binary image without accessing the RBP. This strategy requires two databases (D$_1$ and D$_2$) in which one *challenge* has two *responses* (i.e., 2 different IDs generated with different keysD_1andD_2). In this way, the nominated node measures the RBP on his side, following the given *challenge* by the central node. Then, it uses one of the two key libraries to generate the binary image and sends it to the central node. In the central node, a cross-correlation is performed with both databases to match the single matching image. If the ID exists in one of two databases, the central node asks for the key. This step is for confirming that the ID is attack-free. If the adversary knows the *response* image of the given *challenge* and sends it to the central node without sending the key, the ID would not be accepted. Having two databases increases security. Even if the adversary accessed the image of the *challenge*, he cannot find out whether generating this image required two keys (D$_2$) or just one key (D$_1$). However, each time, after transferring the key to the central node, the used CRP must be removed from database since the key will be transmitted through the public channel and is accessible to the adversary. The central node asks only for the key$_1$. Thereby, database of the transformed image remains secret, which will protect the key of the other image (generated in the other database) of the same *challenge* for the next time identification. In this manner, the adversary again cannot predict if the other image of the same *challenge* required one or two keys.

Conclusions

We proposed a novel method based on PUF to uniquely identify the signature ID of a network based on its composition (e.g. deployed fibers). The proposed method is demonstrated upon the optical-PUF function based on the variety and randomness of RBPs as a function of distance in fibers. We evaluated the method's performance by generating a CRP database and verifying the network's ID. The method may find applications for network security, e.g. tampering would cause a change of the PUF function.

References

[1] Y. Du, S. Jothibasu, Y. Zhuang, C. Zhu and J. Huang, "Unclonable Optical Fiber Identification Based on Rayleigh Backscattering Signatures," Journal of LIGHTWAVE TECHNOLOGY, vol. 35, no. 21, pp4634-4640, 2017, DOI: 10.1109/JLT.2017.2754285.

[2] E. Seve et al., "Automated Fiber Type Identification in SDN-Enabled Optical Networks," Journal of LIGHTWAVE TECHNOLOGY, vol. 37, no. 7, pp1724-1731, 2019, DOI: 10.1109/JLT.2019.2896041.

[3] P. Soumplis, K. Christodoulopoulos, M. Quagliotti, A. Pagano and E. Varvarigos, "Network Planning With Actual Margins," Journal of LIGHTWAVE TECHNOLOGY, vol. 35, no. 23, pp5105-5120, 2017, DOI: 10.1109/JLT.2017.2743461.

[4] M. Furdek, C. Natalino, A. Di Giglio and M. Schiano, "Optical network security management: requirements, architecture, and efficient machine learning models for detection of evolving threats [Invited]," Journal of Optical Communications and Networking, vol. 13, no. 2, pp A144-A155, 2021, DOI: 10.1364/JOCN.402884.

[5] F.Pavanello, I. O'Connor,U. R¨uhrmair, A.C.Foster, D.Syvridis,''Recent Advances in Photonic Physical Unclonable Functions,'' 2021 26th IEEE European Test Symposium (ETS) , DOI:10.1109/ETS50041.2021.9465434

[6] Z.Chen, Y. Zeng, G. Hefferman,Yan. Sun, T.Wei," FiberID: Molecular-level Secret for Identification of Things,'' 2014 IEEE International Workshop on Information Forensics and Security (WIFS), DOI: 10.1109/WIFS.2014.7084308

[7] F.Ito, X.Fan,and Y. Koshikiya," Long-Range Coherent OFDR With Light Source Phase Noise Compensation [Invited]," Journal of LIGHTWAVE TECHNOLOGY, vol. 30, no. 8, pp1015-1024, 2012, DOI: 10.1109/JLT.2011.2167598