Toward Trusted Optical Communications with Optical Physical Unclonable Functions and Blockchain

L. Velasco[1]*, S. Civelli[2], P. Nadimi Goki[3,4], S. Barzegar[1], M. Ruiz[1], L. Potí[4,5]

[1] Universitat Politècnica de Catalunya, Barcelona, Spain;
[2] CNR-IEIIT, Pisa, Italy; [3] Tecip Institute, Scuola Superiore Sant'Anna, Pisa, Italy; [4] CNIT, Pisa, Italy,
[5] Universitas Mercatorum, Roma, Italy
**luis.velasco@upc.edu*

Abstract: Trusted optical communications go beyond encryption and requires also the attestation of the integrity of the optical transponders. We propose optical identification and blockchain for the continuous remote attestation of optical systems with immutable traceability. © 2025 The Authors

1. Introduction

Classical optical systems have vulnerabilities that can be exploited by several attacks, such as eavesdropping, physical infrastructure attacks, interception, and jamming [1]. Although encryption can be implemented at the optical layer [2], validation of the integrity of the optical transponders (Tp) is still an open issue to achieve *Trusted Optical Communications*.

Optical identification (OI) [3] targets to identify optical systems (OS) by means of a *signature* and, consequently, improve the security of optical networks at the physical layer. OI can be implemented by taking advantage of the manufacturing imperfections of the optical fiber, which are unique and cannot be cloned. These imperfections, stimulated by light using the coherent optical frequency domain reflectometry (C-OFDR), generate a Rayleigh backscattering pattern (RBP). Remarkably, the fiber is an *optical physical unclonable function* (OPUF) with the RBP being its response. However, OI based on C-OFDR is a novel technique that currently has some limitations. For example, C-OFDR requires a fully bidirectional link to receive the backscattered light, which limits the total distance of the OS since amplifiers cannot be used. In addition, C-OFDR is an invasive technique, so the data stream needs to be disrupted during the time OI is performed.

In this paper, we show the application of OI on realistic scenarios and design an ad-hoc OI-based *remote attestation* scheme to continuously validate the integrity of the Tps while featuring cumulative security. The scheme is supported by blockchain, providing a secure, shared, immutable, and decentralized ledger of transactions [4].

2. Optical identification using C-OFDR

This section details the OI protocol including C-OFDR, signature definition, and Tp identification. We assume an OS with two Tps in remote sites A and B connected through a bidirectional fiber link of length d. Tps include a pigtail of very short length (L) that is used for the identification. Tp-A starts interrogating Tp-B using C-OFDR to read the RBP caused by the fiber as follows: Tp-A sends a linear frequency swept signal into the fiber link that arrives at Tp-B covering a frequency range of ΔF in a time T_{sw}, i.e., with rate $\gamma=\Delta F/T_{sw}$. Since all the elements in the optical link are bidirectional, the Rayleigh scattering causes a backreflected field that returns to Tp-A. This field is coherently received using as a local oscillator (LO) the same frequency swept field, and digital-to-analog converter (DAC) bandwidth $\geq 2\cdot\gamma\cdot(d+L)/v$, where v is the speed of light in the fiber. Note that C-OFDR can be performed with commercial transceivers, with minor modifications, using the architecture proposed in [5]. The resulting photocurrent is the RBP and uniquely characterizes the fiber [6]. In particular, the spectrum of the RBP is linearly mapped to the fiber link: a scattering point in position p corresponds to a frequency peak in $f=2\cdot p\cdot\gamma/v$.

The relationship between space, time, and frequency is described on the left-hand side of Fig. 1 for a single scattering point. Consequently, Tp-A acquires the RBP, filters it in the corresponding pigtail bandwidth, and obtains an N-long binary vector ($N=4\cdot\Delta F\cdot L/v$) with the measured signature of Tp-B by 2-level quantization. The measured signature is compared with the *true* signature in the database (DB) and Tp-B is labeled OK if the Hamming distance between them is smaller than a threshold (tailored to have equal probability of false positive and negative) [7]. Within this procedure, OI exploits the OPUF application of C-OFDR to read the random imperfections of the Tp's fiber pigtail.

3. Optical remote attestation and Control Architecture

The targeted OS is showed in Fig. 2, with sites A and B connected through a fiber link. A number of OPUF enabled Tps are available in the sites. Such OS fits well in scenarios with high-capacity requirements, e.g., (*i*) intra datacenter (DC) scenarios, where d~1km; and (*ii*) inter-DC and access/metro scenarios, where d~30km.

We assume that OI runs periodically and requires the identification of all the Tps in the OS. We name this as *remote attestation*. However, as previously introduced, using the OPUF for OI involves operations that impact the optical signal carrying data, which entails stopping the normal optical transmission between two Tps until the

The research leading to these results has received funding from the European Union's Horizon Europe research and innovation programme under G.A. No. 101092766 (ALLEGRO), the European Union under the Italian National Recovery and Resilience Plan of NextGenerationEU RESTART (PE00000001), and from ICREA.

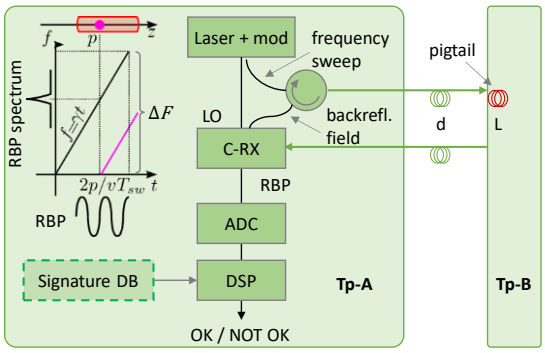

Fig. 1: Optical identification with C-OFDR measurement (simplified from [5]). Detail for one scattering point.

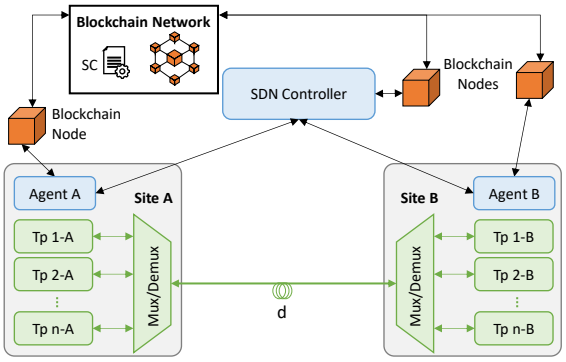

Fig. 2: Architecture overview and illustrative optical system.

remote attestation of the Tp finishes. To minimize such impact, two modes are provided: (*i*) a *quick* mode that provides a coarse identification and it is used when the Tp is supporting an optical connection; and (*ii*) *full* mode that provides a highly accurate identification and is used only if the attestation is run for Tps not supporting an optical connection.

The control architecture includes a Software-Defined Networking (SDN) controller for network automation, including provisioning of optical point-to-point connections involving one Tp at each site. The digital signatures of the Tps are securely stored in a repository ensuring its integrity for future verifications and they are made available to the local agents managing the Tps.

Finally, a blockchain infrastructure is also part of the solution, which sets up a smart contract (SC) that will be used to record the identification of the Tps during the remote attestation procedure. Records will be stored including the measurement and identification of the Tps and thus, the attestation of the entire OS allowing each site in the OS to check the identity of the remote site. It is worth mentioning that the same blockchain infrastructure can support other use cases, such as a federation of services.

4. Commissioning and Operation

The commissioning procedure involves the SDN controller creating blockchain accounts for the agents, including a public address and a private key, deployment of the SC to the blockchain network, and registering the agents' addresses. Once the addresses are registered, the SDN controller distributes the blockchain credentials to the agents involved in the control of the OS for interaction with the SC. In addition, the SDN controller distributes the fiber length (*d*) of the OS, which is needed for the remote attestation of the Tps. To face group attacks, where a corrupted agent verifies a corrupted OS, an initial *root of trust* (RoT) is established for the first OS verification. To that end, the first attestation is triggered by the SDN controller. For that initial attestation, the controller prepares a remote attestation plan and asks the agents to run their attestation functions for measurement and verification. The resulting measurement for each Tp is compared to the one stored in the secure repository and if it matches, the Tp is verified. A transaction is created for each remote attestation, including the measurement, the test result, a timestamp, and the updated RoT (i.e., the id of agent that verified the SO) in the SC.

Once in operation, Algorithm 1 presents the remote attestation procedure that runs periodically in the local agents. The algorithm receives a list with information about the local and remote Tps and returns the remote attestation results. For simplicity, we assume that Tps are deployed in pairs, so the information of the local Tp includes the digital signature of its peer. After some initializations (line 1), the algorithm runs the remote attestation of every individual Tp (lines 2-9). If the Tp is supporting an optical connection, the *quick* mode is used, otherwise the *full* mode is selected (lines 3-4). The attestation record includes the remote Tp attestation time, mode and result (lines 5-8). The TpAttestation() function (line 7) is used for coordinating the reflectometry and computing the Hamming distance between the stored signature and obtained measurement. The returned information includes the obtained measurement and the result and is stored (line 8). In case the measurement does not match for the current Tp, the result of the whole remote attestation is considered not valid (line 9). Note that storing the measurements allows for a more detailed tracking if the measurement is considered not valid. A transaction is next created through the smart contract and pushed to the blockchain and the next execution of the remote attestation is programmed (lines 10-11). Finally, the result of the remote attestation is returned (line 12).

Algorithm 1: runAttestation() function

	INPUT: *Tp* OUTPUT: *attestationResult*
1:	*record* ← {}; *res* ← VALID
2:	**for each** *tp* in *Tp* **do**
3:	**if** *tp*.connId = -1 **then** *mode* ← full
4:	**else** *mode* ← quick
5:	*tp*.lastAtt ← *getCurrentTime*()
6:	*tp*.AttMode ← *mode*
7:	*attRes* ← TpAttestation(*tp, mode*)
8:	*record*.add(<*tp*.id, *tp.lastAtt, mode, attRes.val, attRes*.measurement>)
9:	**if** *attRes.val* = KO **then** *res* ←NOT_VALID
10:	createTransaction(blockchain, *record*)
11:	scheduleNextAttestation()
12:	**return** *res*

Algorithm 2 specifies the procedure executed by the agents every time a new optical connection is requested. The algorithm receives a list with information representing the Tps, as well as the id of the connection to be

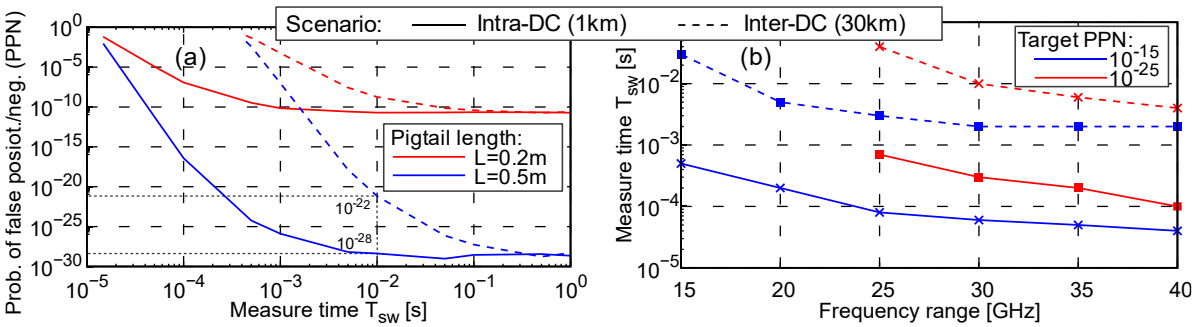

Fig. 3: PPN vs measure time (a) and time vs freq. sweep (b)

established, and it returns the result of the provisioning. The algorithm first selects the Tps that are not currently supporting any optical connection (line 1). If no Tp is available, the request is blocked (line 2). Next, the Tp that has been more recently verified is chosen (line 3) and the remote attestation time is checked. A validity period, typically shorter than the remote attestation one, is considered to keep attestation validity fresh and the remote attestation procedure is run if needed (lines 4-6). The connection is eventually setup with the selected Tp (lines 7-8).

Algorithm 2: Connection Setup

INPUT: *Tp, connId* OUTPUT: *result*

1: *freeTP* ← getFreeTPs(*Tp*)
2: **if** *freeTP* = {} **then return** BLOCKED
3: *tp* ← getLastAttestated(*freeTP*)
4: **if** *getCurrentTime()-tp*.lastAtt > *MAXT* **then**
5: *result* ← runAttestation(*Tp*) (Algorithm 1)
6: **if** *result* = NOT_VALID **then return** *result*
7: setUpConn(*tp*, *connId*)
8: **return** ACCEPTED

5. Simulation results and conclusions

The reliability of the attestation scheme is assessed by simulation in the following setup. We consider an O-band optical system with carrier frequency 255 THz, attenuation 0.34 dB/km, and Rayleigh loss 0.25 dB/km. Furthermore, we consider a single mode fiber having zero dispersion in the O-band and ideally compensated laser phase noise [8]. The practical applicability of the scheme is assessed on the scenarios previously introduced, i.e., (*i*) intra-DC with *d*~1km; and (*ii*) inter-DC with *d*~30km. Different measure time are considered, as it affects the reliability of the OI scheme.

Let us first study the C-OFDR measure considering pigtails of length L=0.2 and 0.5 m, ΔF=25 GHz (N=100 and 250, respectively), while we change T_{sw}. In addition, to estimate shot and electronic noise, we consider a photodetector noise equivalent power of 50 pW/√Hz, receiver responsivity of 0.8 A/W, and input power 0 dBm [5]. Fig. 3a shows the probability of false positive and false negative (PPN) vs T_{sw}. We observe that although the minimum sweep time is different, as it should be larger than $2\cdot(d+L)/v$, the behavior is similar in both scenarios; the performance improves by increasing the sweep time, as the signal-to-noise ratio improves, until it saturates to a level determined by the impact of $d+L$ and by the number of points N of the signature. In addition, we observe that pigtails of L=0.5m provide superior accuracy and hence, higher security to implement OPUFs, as a larger number of points is considered $N=250$. Next, Fig. 3b shows the required measure time for different frequency sweeps ΔF (related to DAC bandwidth), for target PPN values and for the considered scenarios, assuming L=0.5m. A freq. range as low as 15GHz is sufficient to achieve PPN ≤ 10^{-15}, while 25GHz is necessary for PPN ≤ 10^{-25} with limited DAC requirements. We observe that larger freq. ranges allow reducing the measure time, up to the minimum sweep time ~30 µs required for the intra-DC scenario.

In view of the results, the *quick* mode defined in the previous section can be implemented with measure time 10 ms, which provides PPN dependent of the distance of the fiber link but under 10^{-22} in the considered cases. With such measure time, the impact on the normal data transmission is very limited, e.g., 1 Gb of data rate reduction in a 100 Gb/s system, and only when OI is performed. Longer measure times can be considered for the *full* mode that is used when the Tps are not supporting an optical connection. For instance, considering measure times of 1 s results in PPN ~10^{-29}, which is independent of the length of the fiber link.

To conclude, OI based on the unique and unclonable imperfections of fiber pigtails has been proposed to support continuous remote attestation, a key element of trusted optical communications. Immutable traceability is achieved by using blockchain with a smart contract.

References

[1] M. Fok *et al*., "Optical layer security in fiber-optic networks," Trans. on Inf. Forensics and Sec., 2011.
[2] M. Iqbal *et al*., "LPsec: A Fast and Secure Cryptographic System for Optical Connections," JOCN, 2022.
[3] P. Nadimi Goki *et al*., "Optical identification using physical unclonable functions," JOCN, 2023.
[4] P. Gonzalez *et al*., "Experimental Evaluation of Secure Digital Twin Model Exchange Using DLT," ONDM, 2024.
[5] S. Civelli *et al*., "Coherent transceiver architecture enabling data transmission and optical identification" SUM, 2024.
[6] Y. Du *et al*., "Unclonable optical fiber identification based on Rayleigh backscattering signatures," JLT, 2017.
[7] S. Civelli *et al*., "Optical Identification for User Authentication in Quantum Key Distribution Systems," ECOC, 2023.
[8] F. Ito *et al*., "Long-range coherent OFDR with light source phase noise compensation," JLT, 2012.