# Man-in-the-Middle Attacks Through Re-Shaping I-Q Optical Constellations

**Marc Ruiz, Jaume Comellas, and Luis Velasco***

*Optical Communications Group (GCO), Universitat Politècnica de Catalunya (UPC), Barcelona, Spain*
*e-mail: luis.velasco@upc.edu*

**Abstract:** A module to re-shape optical constellations making the optical signal resembles as it has traversed some distance is presented. Armed with this module, Main-in-the-Middle attacks can be performed, which could be undetectable by security systems. 

## 1. Introduction

Huge efforts have lastly been paid to study the application of Machine Learning (ML) techniques to optical transport networks [1]. Applications include Quality of Transmission (QoT) estimation, failure and attack detection, and network automation, just to mention a few [2]. The role of ML is especially relevant in the current evolution towards open, scalable, and cost-efficient optical transport networks, through disaggregation and programmability. In this regard, the development of Optical Layer Digital Twins (DT) able to accurately model the optical layer, reproduce scenarios and generate expected signals are of paramount importance for failure management and anomaly detection. As an example, the In-Phase and Quadrature (IQ) Optical Constellation (OC)-based DT (OC-DT) in [3] is able to analyze the received OC samples by means of Deep Neural Network (DNN) models and predict the optical connection (*lightpath*) length, from transmitter (Tx) to receiver (Rx).

However, the added network complexity brought by disaggregation can increase optical layer vulnerabilities, which can be exploited by attackers. In case of a Man-in-the-Middle (MitM) attack [4], the affected lightpath is intercepted by the attacker (*Mallory*) at an intermediate site between the Tx (*Alice*) and the Rx (*Bob*), with the objective of altering transmitted data. To do so, Mallory needs a pair of optical transceivers to receive the optical signal from Allice, alter the received data, and generate a new optical signal that is sent to Bob. In consequence, the optical signal received by Bob has different physical properties, since the signal has been propagated through different distance. In such case, OC-DTs can detect tampering fast and accurately.

Our intention in this paper is to reveal vulnerabilities that could be exploited, in the hope that OC-DTs can be improved. Specifically, we focus on how Mallory can successfully cancel the effectiveness of OC-DTs to achieve undetectable MitM attacks. To this end, we present the *Hacking Optical Constellations throUgh re-Shaping* (*HOCUS*) module. HOCUS modifies I-Q symbols fingerprints in a way that Mallory's OC samples reaching Bob resemble the expected for the original signal.

## 2. Concept and Scenario

Fig. 1a shows the reference network scenario, where a lightpath is transparently routed from Allice to Bob, being its length $L$ km. At a given intermediate site between Alice and Bob, the optical signal has traversed $L_1$ km from Alice site and has to travel additional $L_2$ km to arrive Bob site. Without loss of generality, let us assume 16-QAM modulated optical signals.

At Bob site, the optical signal is monitored and thus, OC samples are collected, which are afterward processed by an OC-DT. In the OC-DT in [3], the analysis consists of three different phases: 1) a Gaussian Mixture Model (GMM) is applied to each OC sample in order to obtain the mean ($\mu$) and covariance ($\Sigma$) of the bi-variate Gaussian distributions that better characterize each of the constellation points; 2) features are forwarded through a DNN model that estimates lightpath length ($L'$) based on the dispersion of the received IQ symbols around the expected centroids; and 3) a decision-making test determines whether $L' \cong L$ or conversely, $L'$ is significantly different (shorter or longer) than $L$.

Fig. 1b considers the lightpath under a MitM attack. Without loss of generality, we consider that Mallory has gained physical access to the intermediate site, so the attacker can receive the original optical signal from Alice, alter data and forward the new signal to Bob. In addition, Mallory could need remote access to other sites along the route of the lightpath, e.g., if physical access to an intermediate site in the route of the lightpath is not possible and some sort of configuration of switching in the optical nodes is needed. Finally, let us assume that the attack can be conducted with negligible optical transmission disruption, and therefore no *loss-of-light* alarm is raised.

The OC-DT can detect differences w.r.t. the expected lightpath length $L$. In the example in Fig. 1b, the OC-DT would infer that the optical signal received by Bob has been generated by a transmitter located at $L' \cong L_2$. Therefore, a warning notification will be sent to Software Defined Networking controller, which eventually can trigger countermeasures.

The research leading to these results has received funding from the HORIZON ALLEGRO (G.A. 101092766) and the MICINN IBON (PID2020-114135RB-I00) projects and from the ICREA Institution.

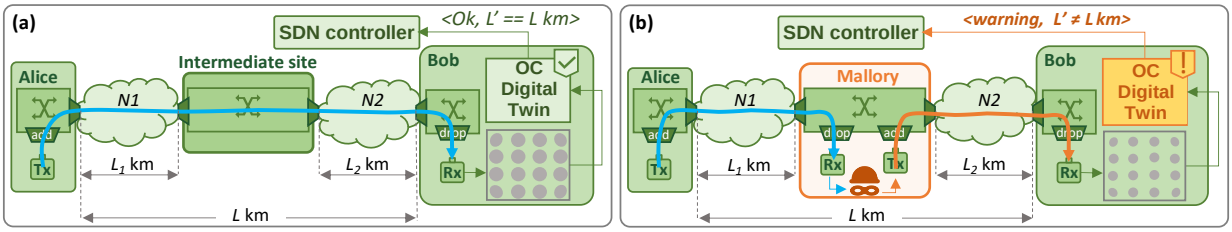


Fig. 1: Reference network scheme (a). MitM attack and tamper detection by OC analysis (b)

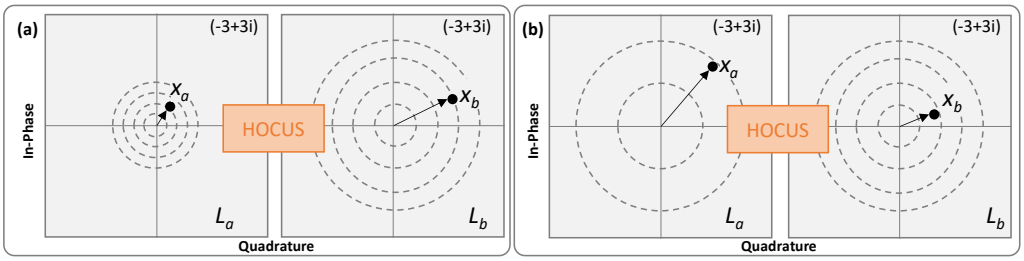


Fig. 2: HOCUS symbol reshaping for $L_a < L_b$ (a) and $L_a > L_b$ (b)

In view of the above, Mallory needs to perform additional processing to bypass security systems based on OC-DT. In particular, we propose the HOCUS module that re-shapes optical symbols in a way that an OC-DT would infer a value of the distance travelled by the received signal as desired by Mallory.

Fig. 2 illustrates the bi-variate Gaussian distributions of constellation point (-3 +3i) for two different scenarios where HOCUS can be deployed. In both cases, HOCUS receives source optical symbols ($x_a$) with total accumulated length $L_a$ and produces modified target optical symbols ($x_b$) with a dispersion around the OC point that resembles length $L_b$. Fig. 2a shows the scenario in Fig. 1, where HOCUS is executed in an intermediate site in the route of the lightpath, and then $L_a < L_b$, e.g., $L_a = 0$ and $L_b = L_1$. In this case, HOCUS modifies the shape of the input symbols with zero accumulated length to the target ones, so they appear have been propagated along $L_1$ km. Hence, the OC of the generated signal would have a shape similar to the expected at any point along the route of the lightpath.

Another possibility is to install HOCUS at Bob site while keeping signal generation at the intermediate site. In particular, the monitored OCs are reshaped before reaching the OC-DT. In this case, $L_a < L_b$ as before, but $L_a = L_2$ and $L_b = L$.

However, Mallory could only gain physical access to a site that is not in the original route of the lightpath. Then, the attacker could silently reroute the lightpath so it crosses the desire intermediate site. In this case, $L_b$ might be shorter than $L_a$, as in Fig. 2b.

## 3. The HOCUS module

Formally, HOCUS is defined as a parametric function that requires from a set of coefficients $\theta$ to be trained before performing any re-shaping. Assuming 16QAM signals, $\theta=\{\theta_1, \ldots, \theta_{16}\}$, where $\theta_i$ initially contains the expected bi-variate Gaussian distribution of constellation point $i$ for both $L_a$ and $L_b$ lengths (eq. (1)).

Without loss of generality, we assume that Mallory can access monitoring data repositories, obtain true OC samples from all or part of the lightpaths in operation, and train $\mu$ and $\Sigma$ coefficients before performing MitM attacks. However, OCs for distances $L_a$ and/or $L_b$ might not be available, so polynomial interpolation is used to estimate missing $\mu$ and $\Sigma$ coefficients from the available lightpath lengths. Note that both $\mu$ and $\Sigma$ present high correlation with length among all constellation points [3].

Once $\mu$ and $\Sigma$ for lengths $L_a$ and $L_b$ are obtained, transformation matrices $W$ are computed and added to $\theta$. Since every $\Sigma$ is a covariance matrix, it is semi-definite positive and hence, a decomposition $\Sigma = P \cdot D \cdot P^*$ exists, being $P$ a unitriangular matrix, $D$ a diagonal one and $P^*$ the conjugate transpose of $P$ [5]. Then, transformation matrix $W_i(L_a, L_b)$ for constellation point $i$ is computed as eq. (2). Individual symbol transformation can then be easily performed. Let us denote $x_a(t)$ as the source symbol processed by HOCUS at time $t$. Assuming that it belongs to constellation point $i$, the target symbol $x_b(t)$ is obtained applying the following transformation (eq. (3)).

$$\mu_i(L_a),\ \Sigma_i(L_a),\ \mu_i(L_b),\ \Sigma_i(L_b). \quad (1)$$

$$W_i(L_a, L_b) = P_i(L_b) \cdot D_i^{\frac{1}{2}}(L_b) \cdot P_i^*(L_b) \cdot P_i(L_a) \cdot D_i^{-\frac{1}{2}}(L_a) \cdot P_i^*(L_a) \quad (2)$$

$$x_b(t) = W_i(L_a, L_b) \cdot (x_a(t) - \mu_i(L_a)) + \mu_i(L_b) \quad (3)$$

## 4. Illustrative Results

To evaluate HOCUS, a Matlab-based simulator of a coherent optical system with 100 GHz channel spacing has been developed to generate 16QAM@64GBd signals under different scenarios. The signal is propagated through

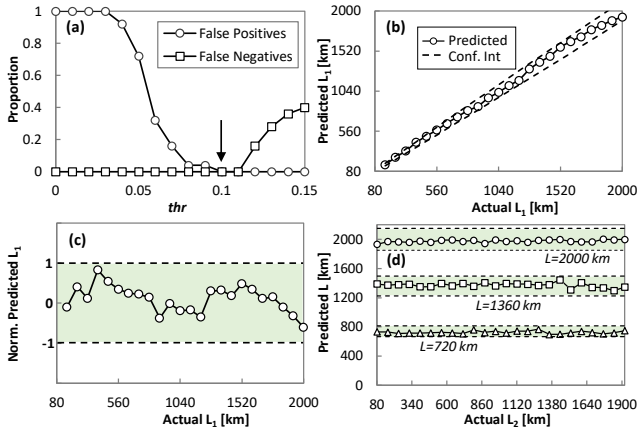


Fig. 3: OC-DT training (a). Performance of HOCUS(0->$L_1$) absolute (b) and normalized (c), and of HOCUS($L_2$->L) (d).

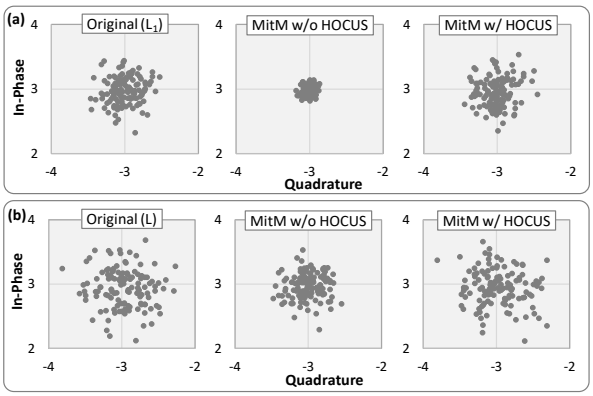


Fig. 4: Detail of constellation point *-3 +3i* when HOCUS is applied at an intermediate site (a) and at the Rx site (b).

standard single mode fiber over 80-km spans characterized by optimal power of -1 dBm, attenuation factor of 0.21 dB/km, dispersion parameter of 16.8 ps/nm/km, and nonlinear parameter of 1.141 $(W \cdot km)^{-1}$. At the Rx, a digital signal processing block performs ideal chromatic dispersion compensation and phase recovery. With the aforementioned configuration, signals with 2,048 symbols for lightpaths with total distance ranging from 80 to 2,000 km were generated; data are openly available in [5].

We implemented the OC-DT in [3] and trained the DNN-based lightpath length estimator with: *i*) 20 input neurons (5 GMM-based features of 4 selected inner and outer constellation points); *ii*) three hidden layers with 20, 20, and 12 neurons and *tanh* activation function; and *iii*) one output neuron. Moreover, we implemented a decision-making function that detects unexpected length if the relative error between the predicted and the expected length exceeds a predefined threshold *thr*.

Fig. 3a shows the accuracy of OC-DT to detect MitM attacks without applying HOCUS. To this aim, we emulated normal and attacker signals for lengths ranging from 80 km to 2000 km and evaluated the detection of both false positives and false negatives for a wide range value of *thr*. We observe that *thr* = 0.1 produces no false detections, which indicates 100% attack detection accuracy in the whole length range, even when $L_1$ is only 80 km.

After validating OC-DT as accurate MitM attack detector, we evaluate the effectiveness of the proposed HOCUS module. Firstly, we focus on evaluating HOCUS when it is applied at the same intermediate site where the MitM attack is performed. To this aim, we use the DNN-based lightpath length predictor to estimate $L_1$ at the intermediate site. Fig. 3b shows predicted vs. actual $L_1$; dotted lines represent the confidence interval assuming *thr* = 0.1. Complementing Fig. 3b, Fig. 3c shows the normalized prediction accuracy, where predictions within the interval [-1, 1] entail that the decision making module cannot detect any distance inconsistence in the received signal. Owing to the fact that the attacker can use HOCUS to generate signals leaving the intermediate site with similar distance than that of original signals, the MitM will be undetectable.

Let us now evaluate HOCUS when applied at the Rx site, i.e., far from the site where MitM attack is performed. Fig. 3d presents results for actual $L$={760, 1360, 2000} km, when the MitM attack was performed at $L_2$ in the range [80, 1920] km from Rx. As in the previous case, the attack is not detected since the predicted $L$ is within the accuracy interval regardless of the actual $L_2$.

Finally, Fig. 4 shows the detail of constellation point (-3 + 3i) before (original) and after the MitM attack, without and with HOCUS. Two different cases are considered: <$L$ = 800 km, $L_1$ = 720 km, HOCUS(0->720)> (Fig. 4a) and <$L$ = 1600 km, $L_1$ = 800 km, HOCUS(800->1600)> (Fig. 4b). We observe that in both cases HOCUS introduces additional dispersion in the symbols that results in constellation points similar to the original ones.

## 5. Conclusions

The HOCUS module showed its ability to complement MitM attacks in a way that they cannot be detected by optical security mechanisms based on OC-DT. It is then of paramount importance to analyze the patterns introduced by re-shaping tools, like HOCUS so as to improve the capabilities of OC-DTs in detecting MitM attacks.

## References

[1] A. Lau and F. Khan, *Machine Learning for Future Fiber-Optic Communication Systems*, Elsevier, 1st Ed, 2022.
[2] D. Rafique *et al*., "Machine Learning for Optical Network Automation: Overview, Architecture and Applications," IEEE/OPTICA JOCN, 2018.
[3] M. Ruiz *et al*., "Deep Learning -based Real-Time Analysis of Lightpath Optical Constellations," IEEE/OPTICA JOCN, 2022.
[4] M. Ghonge *et al*., *Cyber Security and Digital Forensics: Challenges and Future Trends*, Wiley, 1st Ed., 2022.
[5] H. Yanai *et al*., *Projection Matrices, Generalized Inverse Matrices, and Singular Value Decomposition*, Barnes & Noble, 1st Ed., 2011.
[6] M. Ruiz *et al*. "Replication Data for Optical Constellation Analysis (OCATA)," https://doi.org/10.34810/data146, V1, 2021.