Defending Against Tampering Attacks by Received Optical Signals Comparison

Alex Ferrando Víctor Novelle Marc Ruiz Luis Velasco
Polytechnic University of Catalonia
{alex.ferrando,victor.novelle}@estudiantat.upc.edu {marc.ruiz-ramirez,luis.velasco}@upc.edu

Abstract

The introduction of Machine Learning (ML), Deep Learning (DL), and software-based systems in optical networks is an active field of research that seeks to investigate how these connections could benefit from the extensive capabilities that the later systems offer. An important branch of this field is Security monitoring, which aims to detect and neutralize attacks performed across the network structure. Even though these ML-based systems have been proved to work effectively against certain types of attacks it is necessary, as with any other defense method, to periodically revise them to ensure that protection against newer attacks and detected vulnerabilities is guaranteed.

In this paper, we present two types of defensive metrics that allow us to detect the 79% and 93% of the attackers' modified signals (using the attacks presented in [7]), which previously by-passed the proposed NN-based defense method.

1. Introduction

The growth of Internet use [26] has rapidly accelerated research and advances in technologies dedicated to the area. One of these emerging technologies that has experimented a rapid growth in recent years is fiber optics as they are extremely useful in guaranteeing fast communications between users in a network. However, hand in hand with the expansion of fiber optics installations it has appeared a major interest in manipulating the communications that occur through them and, in response, a concern in ensuring secure communications through the network [19, 20].

During the last 90s and the beginning of the 00s, several innovative defense proposals against fiber optics tampering attacks were made [16, 18, 27] which have been improved since then [12, 17, 29]. Nevertheless, most of the proposals are based on physical and hardware systems that in most cases would suppose a high economic cost if we wanted to implement them in the current systems on a large scale. For this reason, new proposals have been made to substitute physical-based security systems with software-based ones [28]. This would bring great advantages as software systems are easier and cheaper to build and distribute on a large scale. In addition (and in contrast to physical-based systems), software-based systems enable fast and low-cost upgrades if novel attacks appear exploiting the vulnerabilities of the already implemented systems.

In this way, several studies [4, 31] have been carried out recently to introduce software solutions in the optical networks security systems, especially in the field of Machine Learning [33], with promising results. However, these tend to be highly dependent on the given problem so it is still necessary to develop new software-based methods for the framework we are trying to work with (see Section 3).

The goal of the work developed and exposed throughout this paper is to propose a discriminator system that is able to discern whether a received sample has been modified with the methods proposed in [7]. The defenses exposed in this paper will try to exploit from a non-physical point of view the main weaknesses of the different attack strategies presented in the previous paper.

2. Related Work

Software-based systems in optical transmissions The implementation of software elements that aim to substitute or complement the current hardware present in optical fiber communications has received extensive attention recently [11, 21]. The field of research of these studies is extensive and can be divided into two groups, those that aim to improve the quality of the network communication and those that control that this performance is maintained over time.

Focusing on the quality group, ML techniques are promising solutions in the signal processing field, being able to satisfactorily compensate both linear and non-linear impairments, reducing the overall distortion of the communication [3, 22, 23]. Also, studies assessing the benefits of the usage of DL algorithms for optical network structure optimization show that the usage of these techniques allow

overcoming the restrictions of the traditional expert-based approach [24, 28].

Regarding the maintenance aspect, software-based systems enable the implementation of monitoring systems that are able to effectively detect a degradation in the quality of the transmitted optical signal [6, 9, 34], that could be produced due to unintentional or intentional errors introduced along the network. For the latter case, research around security-based monitoring systems have been performed as presented in Section 1.

3. Defense

In this section, we are going to propose a defense for each of both scenarios of knowledge presented in [7] in Section 3.2. As posed in the reference paper, there could be two different setups depending on the attackers' knowledge of the target system which we will review quickly next. It is important to note that, in this paper, we are going to utilize the same notation used and exposed in section 3.1 of [7]. We strongly suggest reviewing and being aware of the notation described in the reference paper as it is crucial to understand the equations and explanations in this paper.

Advanced Knowledge Scenario (AK) In this scenario, the attacker has control over the entire pipeline of pre-processing, which means that the attacker is able to modify the features extracted by the Gaussian Mixture model $\{\mu_{(i)}^{(d)}, \Sigma_{(i)}^{(d)}\}$. However, the attacker does not know anything about the model used to predict the distances (which features are used or the architecture of the system). The attack proposed in [7] consists in using polynomial regression to approximate the values of each position of the mean vector and the covariance matrix for each quadrant as a function of the distance (see equation 3 in [7]). In this way, the attacker is able to interpolate (and thus to mimic) the values of the mean vector and the covariance matrix for distances not present in the attacker's available dataset ($\mathcal{D}_{Att}$). We must take into account that even if this is a highly permissive attack scenario, it might be considered rare in a real circumstance.

Limited Knowledge Scenario (LK) In order to set up a more realistic framework, the reference paper also considers the scenario where the attacker is only able to modify the raw optical sample data. In this scenario, the attacker has only partial awareness of the security system's structure of the victim model. More specifically, the attacker knows the existence of a pre-processing stage where first and second-order moments of the symbols from each constellation point $C_{(i)}^{(d)}$ are extracted and also knows that those extracted features are the ones that are inputted to the distance predictor model. In addition, to ensure a realistic scenario, the set of transformations applied to the symbols of the constellation point, are reduced to the affine ones.

For this scenario, two different attacks based on the same idea are proposed: finding a matrix $M_{(i)}^{(d\to d^*)}$ and a vector $b_{(i)}^{(d\to d^*)}$ such that the affine transformation of the input symbols resembles the mean and variance of the target distribution of symbols. The target mean and covariance can be extracted using the available attacker's dataset ($\mathcal{D}_{Att}$) or, failing this, using the interpolation procedure of the AK-framework.

3.1. Feature mimic defense

This supposed scenario (AK) is the most difficult to defend due to the extensive knowledge that the attacker has of the system structure. Therefore, the defense method will consist in exploiting the unique disadvantage the attacker may have concerning the victim: the available data. We must take into account that this attack consists in mimicking the actual features of a target distance. Thus, our defense proposes to find little deviations in the mimicked features from the victim's train data $\mathcal{D}_{Tr}$ (dataset that the victim needs to know has not been modified). Note that this dataset will (almost surely) be bigger than the attacker's dataset. Indeed, in most real cases, the attacker's dataset will be a subset of the victim's train dataset $\mathcal{D}_{Att} \subset \mathcal{D}_{Tr}$.

For the defense method, we will suppose any value of a feature $\mathbf{f}$ (i.e each component of the mean vector and each component of the covariance matrix) generated as a result of a random draw from a univariate normal distribution whose mean and variance depend on the distance d, the constellation point i and which feature represents in the quadrant (we will indicate it with a variable k designating the 4 elements of the covariance matrix and the 2 of the mean vector). Thus, $\mathbf{f}_{k,(i)}^{(d)} \sim \mathcal{N}_{d,i,k}\big(\mu(d,i,k), \sigma(d,i,k)\big)$. In consequence, as the attacker will do the attack by mimicking its own estimation of the mean and covariance from the target distance in a given constellation point (using the attacker's dataset $\mathcal{D}_{Att}$ and a polynomial approximation), little deviations with respect to the victim's estimated features will be produced. It must be considered that these deviations should be almost imperceptible when analyzed feature by feature, but should be more noticeable when all the approximated features are observed on the whole.

Thus, we propose to the victim to calculate the absolute z-score for each of the extracted features using the distributions computed with the training data and average them in order to obtain a representative value of all the z-scores (i.e deviation with respect to the computed distribution). Even if, in an idealistic attack, we should not observe any noticeable deviation in any of the extracted features, in a realistic attack, the mean deviation of all the features should be higher in the modified observations due to the differences in the victim and attacker datasets and the errors in the polynomial approximation. So, given an optical sample $O^{(d)}$ with extracted features $\mathbf{f}_{k,(i)}^{(d)}$ and a computed defense distribution

$\mathcal{N}_{d,i,k}\big(\mu(d,i,k),\sigma(d,i,k)\big)$ we will define the score $\mathcal{Z}$ as:

$$\mathcal{Z} = \frac{1}{n}\sum_{i=1}^{16}\sum_{k=1}^{6}\left|\frac{\mathbf{f}_{k,(i)}^{(d)} - \mu(d,i,k)}{\sigma(d,i,k)}\right| \tag{1}$$

Finally, we can set a γ value as a boundary and discard all the constellation points whose $\mathcal{Z}$ surpasses the defined value. So, a constellation point will be considered as safe if $\mathcal{Z} < \gamma$ and will be rejected if $\mathcal{Z} \geq \gamma$.

3.2. Symbol-to-symbol defense

As it is has been commented before, the AK attack framework is barely probable to happen due to the extensive knowledge the attacker must have of the victim's system. In consequence, a more realistic set-up is proposed in [7] where the attacker is only able to modify the raw optical samples using a set of affine transformations.

Now in the LK scenario, the fact that we can utilize the modified optical sample to propose a defense supposes a clear advantage at the time of setting a defense. As the set of transformations applied to the constellation points is restricted to the affine ones, we know that the modified constellation points will be the result of applying some expansion/shrinking, rotation, and mirroring over the original constellation point; meaning, the overall shape of the original constellation points are kept in the resulting ones. This attack method is highly effective in mimicking the first and second moments of the target distribution and, therefore, fooling the defense network. This reflects the principal vulnerability of the defensive system, which is that it only operates over the GMM extracted features and do not evaluate at any time the raw received symbols. As a result, all the tampering attacks that are able to modify the constellation points in a way that the Gaussian Mixture Model feature extraction obtains the same results that in clean data will be able to bypass the actual defensive system. Thus, it is clear that these threats are exploiting the Anscombe's quartet phenomenon [1] and that additional security measures not only based on first and second-order moments are needed.

In consequence, we propose the usage of metrics that are able to measure the distances between the transformed and the target set of symbols in $\mathbb{C}$.

Hausdorff distance: A useful (dis)similarity metric that can be used to measure how far two subsets of a metric space are from each other is the Hausdorff distance [2, 13, 15]. This measure finds the maximum Euclidean distance d between two sets in a metric space (in our case $\mathbb{C}$). This distance can be exploited in our set-up to discriminate the modified constellation points from the real ones due to the fact that, as the original symbols' distributions are different, the expected resulting shape of the modified symbols will be different from the target distribution. This will produce higher Hausdorff distances between a modified constellation point and a real one than when measured between two non-modified constellation points. In this scenario the Hausdorff distance d_H would be defined as:

$$\mathrm{d}_H\left(C_{(i)}^{\prime(d)}, C_{(i)}^{(d^*)}\right) = max(e_1, e_2)$$
$$\begin{cases} e_1 = \sup\limits_{x_{(i)}^{\prime(d)} \in C_{(i)}^{\prime(d)}} \inf\limits_{x_{(i)}^{(d^*)} \in C_{(i)}^{(d^*)}} \mathrm{d}_E\left(x_{(i)}^{\prime(d)}, x_{(i)}^{(d^*)}\right) \\ e_2 = \sup\limits_{x_{(i)}^{(d^*)} \in C_{(i)}^{(d^*)}} \inf\limits_{x_{(i)}^{\prime(d)} \in C_{(i)}^{\prime(d)}} \mathrm{d}_E\left(x_{(i)}^{(d^*)}, x_{(i)}^{\prime(d)}\right) \end{cases} \tag{2}$$

However, we must take into account that this distance is highly sensitive to outliers [25]. For this reason, we propose to use a modified version of this distance more resilient to outliers.

Robust Hausdorff distance As proposed in [14, 25], a way to make the measure more resilient to outliers is not taking them into account when computing the distance. In order to do so, the authors suggest considering only the $K\%$ of the points ordered ascending by distance when doing the supremum. That means that after doing the infimum, instead of taking the supremum over all the Euclidean distances as in the classical Hausdorff, the Robust Hausdorff distance for a percentage $K\%$ is the result of getting the maximum over the $K\%$ lowest distances after sorting all of them in ascending order. We will indicate d_{H-K} as the robust Hausdorff distance considering only the $K\%$ of the computed infimum distances.

Chamfer distance: Another metric widely used for point cloud comparison consists in the Chamfer distance [5, 10, 32]. For computing this measure, for each point in each cloud, the nearest point in the other set is found and the Euclidean distance between them is computed, averaging the results afterward. Even though this distance is generally used for comparing clouds set in the $\mathbb{R}^3$ metric space, it can be adapted to work in $\mathbb{C}$, as needed in our case. As presented previously, we expect that the dissimilarity metric achieves notably higher values when comparing a modified constellation point with an original one than when two clean observations are compared. For our problem setup, the bi-directional Chamfer distance d_C can be formulated as:

$$\mathrm{d}_C\left(C_{(i)}^{\prime(d)}, C_{(i)}^{(d^*)}\right) =$$
$$\frac{1}{|C_{(i)}^{\prime(d)}|}\sum_{x_{(i)}^{\prime(d)} \in C_{(i)}^{\prime(d)}} \min_{x_{(i)}^{(d^*)} \in C_{(i)}^{(d^*)}} \mathrm{d}_E\left(x_{(i)}^{\prime(d)}, x_{(i)}^{(d^*)}\right) \; + \tag{3}$$
$$\frac{1}{|C_{(i)}^{(d^*)}|}\sum_{x_{(i)}^{(d^*)} \in C_{(i)}^{(d^*)}} \min_{x_{(i)}^{\prime(d)} \in C_{(i)}^{\prime(d')}} \mathrm{d}_E\left(x_{(i)}^{(d^*)}, x_{(i)}^{\prime(d*)}\right)$$

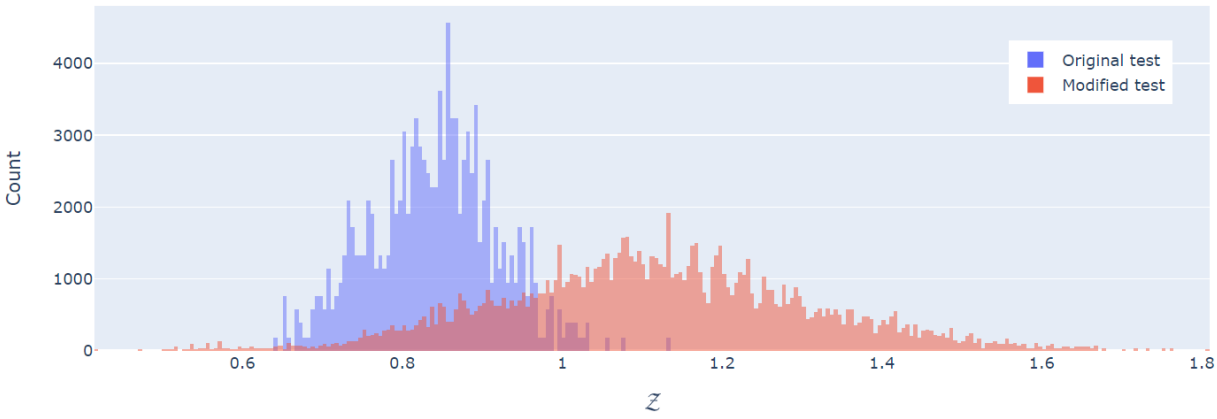

Figure 1. $\mathcal{Z}$ frequencies for both modified and non-modified features

To speed up the metric computation, K-d trees are used in the nearest neighbor search [8, 30].

4. Experiments

4.1. Basic Settings

Dataset We conduct our experiments using a dataset consisting of two distinct components. On the one hand, 25 unmodified 16-constellation point observations that make up our confidence set will be used to perform the comparisons. Indicate that in a real setup, this trust set can be increased by adding the observations that are considered secure by the defensive system.

The rest of the dataset is composed of observations of both clean and modified optical samples that will be used to simulate the data that arrives at the receiver through the network. For the modified data, the best-performing attack configurations presented in [7] have been used to ensure that the proposed defense methods perform well in the worst-case scenario.

All the clean optical signal samples have been provided by the Advanced Broadband Communications Center (*CCABA*) research center at the Polytechnic University of Catalonia (*UPC*).

Evaluation metric The efficiency of each presented defense method can be evaluated in terms of how good it is at the time to discriminate whether a constellation has been modified or not. Thereby, two errors must be considered when evaluating the proposed defense systems. On the one hand, we are interested to detect all the observations that have been modified by the attacker and rejecting them. On the other hand, we do not want our defense to misclassify clean observations as it implies a loss of useful information that might be critical in certain environments. A metric that allows to balance both objectives and that is widely used in binary classification problems is the F_1 score.

In all the performed experiments, 10 independent runs to select the trusted set of points have been executed. The obtained F_1 metrics are averaged to obtain a more robust metric.

4.2. Feature mimic defense performance

In this subsection, we present the experiment and the obtained results that allow the evaluation of the quality of the proposed defense in Section 3.2. In the executed test, the test dataset is duplicated, one for modification and the other remaining untouched. For each optical sample in the dataset for modification, a random distance greater than the original one is selected and the GMM extracted features are modified using the Feature Mimic attack. In this way, we can compute and save the defined measure $\mathcal{Z}$ for each observation from the original test dataset and the changed one. With all the results obtained for the non-modified test dataset and the modified one respectively, we can draw a histogram to observe whether the values of $\mathcal{Z}$ differ in both groups. Finally, with the two lists of $\mathcal{Z}$ values (one computed over the original test dataset and the other over the altered samples) we can find the optimal γ value that maximizes the F_1 score.

In Figure 1 we can corroborate the hypothesis that the modified optical samples will show generally a significantly higher $\mathcal{Z}$ value. We can also observe that the samples are not perfectly separable by a γ boundary. The original test data show $\mathcal{Z}$ scores normally distributed between 0.65 and 1.05 approximately. This result corroborates the hypothesis of normality in the distribution of the extracted features. On the other hand, the modified test dataset show higher $\mathcal{Z}$ values ranging from 0.4 up to 1.8 in the worst cases (higher variance). It must be considered though, that we are trying to defend an extremely permissive attack scenario where the attacker can modify directly the inputs to the distance predictor. Despite this fact, it can be seen that this method is able to achieve a fairly high discrimination level.

In order to find the optimal boundary γ that maximizes the F_1 score, several values have been tested between 0.8 and 1.16. As it can be seen in Figure 2 the maximum F_1 score is achieved with $\gamma = 0.96$, achieving an $F_1 = 0.8520179$, detecting 79.167% of the modified observations and misclassifying 6.667% of the clean optical signals.

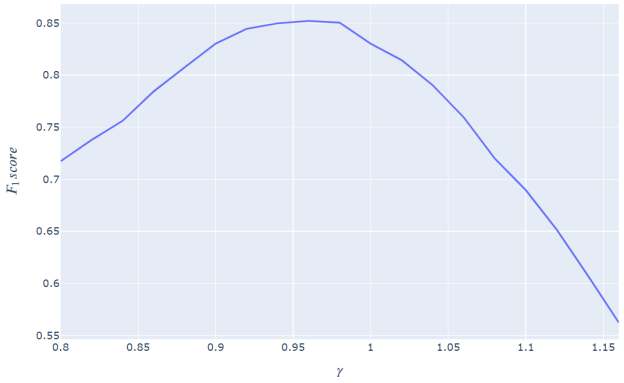

Figure 2. $F_1 score$ depending on the γ value.

Once that an optimal γ value has been defined, we can proceed to analyze the characteristics of those modified samples that have been incorrectly classified as real samples. In order to do that the percentage of false negatives for each $d \rightarrow d^*$ combination has been computed, obtaining the results presented in Figure 5.

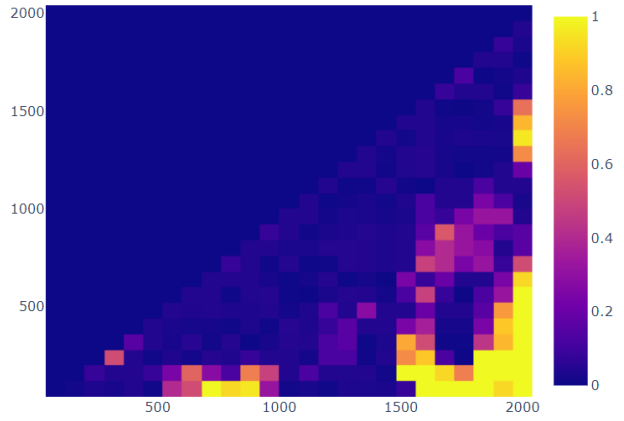

Figure 3. % of false negative per $d \rightarrow d^*$ mimicking for Feature mimic defense.

The obtained false negative percentages have a similar distribution to the polynomial errors presented in Figure 2 of [7] but inverted. This result demonstrates that in the areas where the polynomial approximation of the attacker differs more from the real data distribution, our proposed method can effectively detect the modification (2.5% of FN on average). However, for the distances where the attacker approximation is almost perfect, the modified samples effectively surpass the defense. This effect is specially noticeable for those transformations whose original distance is lower than 500 and the target distance is greater than 1420.

Thus, the performance of this defensive method greatly depends on the degree of accuracy that the attacker's polynomial approximation is able to achieve, However, for the best setup scenario for the attacker and the best threat presented in [7], we are able to detect almost 80% of the modified samples, classifying the defense as effective.

4.3. Symbol-to-symbol defense performance

In this subsection, the comparison between the three presented distances in Section 3.2 is performed, executing the same experiment as for the Feature mimic defense case. Thus, all the distances will be compared using the F_1 metric in order to determine which of them dispose of a higher value, and in consequence, is able to separate better the modified and the non-modified samples.

Notice that in the Robust Hausdorff distance case, an optimization over the $K\%$ parameter must be executed previously. The selection of the best $K\%$ will also follow the criteria of obtaining the highest F-score value. So, for each tested $K\%$, an optimal γ value is computed. In this way, we can effectuate a fair comparison between the defenses. The results of this optimization are presented in Table 2

$K\%$	γ	F_1 score
85	0.11	0.9451
90	0.125	0.9537
95	0.16	0.9321
98	0.20	0.8920

Table 1. F_1 score depending on $K\%$

As $K\% = 90$ has the highest value, it is the configuration chosen for the comparison against its non-modified version as well as the Chamfer distance, drawing the same histograms presented in subsection 4.2 but now with the studied distances in the x-axis instead of the $\mathcal{Z}$ value. In Figure 4 we can observe that the Robust Hausdorff distance defense provides a clearly higher security level with respect to the other distances. We can see the exact values obtained for the F_1 score, the true positive ratio, and the false positive ratio in Table 2. The Chamfer distance is the one that shows a lower F_1 score (0.83) but is the one that has a lower false positive rate. On the other hand, the Hausdorff distance shows a clearly higher performance achieving almost 0.9 of F_1 score. However, the presence of the outliers affects too much the performance of the defense system which is demonstrated with the improvement shown by the Robust Hausdorff distance defense. It must be noted that the three methods outperform the results obtained in subsection 4.2 proving that the additional information obtained by being able to analyze the raw constellation points is useful to dis-

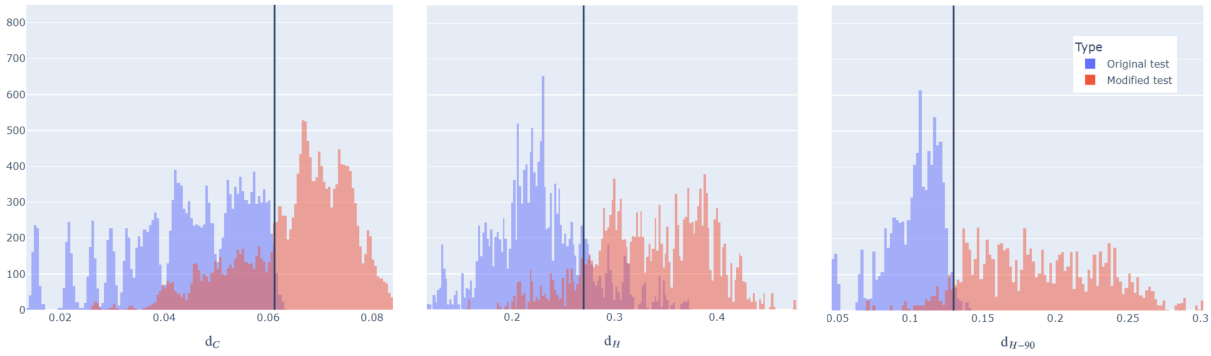

Figure 4. Frequencies of d_C (left), d_H (middle), and d_{H-90} (right) for both modified and non-modified observations

criminate whether an observation has been modified or not.

Distance	F_1 score	TP (%)	FP (%)
Chamfer	0.8328	72.21	1.2
Hausdorff	0.8605	89.82	18.95
Robust Hausdorff (90%)	0.9537	93.68	2.78

Table 2. Performance metrics for each distance

If we further analyze the behavior of those undetected modified samples with the Robust Hausdorff distance with $K = 90$ we can observe a clearly different behavior than the one presented in Figure 5. In this heat map we can observe that the proposed defense system fails mainly for those mimicking modifications where the attacker location is close to the trusted source while it has a perfect behavior when the difference between the original and the target distances is large. This phenomenon is accentuated when the attacker is located near the victim's defense system. The reason behind this behavior is that the constellation points for small differences in distances (and mainly when the original distance is lower than 800 km) are very similar between them. Nevertheless, for those cases where the attacker is established at a distance 1320 km or above, the attacker fails even when mimicking a target distance that is 80 km larger (5.84% FP on average with respect to 71.39% for smaller distances).

5. Conclusions

In this paper, we propose software-based defense systems for the attacks presented in [7]. These attacks are based on fooling a Machine Learning predictor that discriminates whether a message sent through an optical fiber has been modified or not by predicting the distance the message was sent from and the expected distance from the source. We demonstrate that we are able to defend the threats to both the AK and LK scenarios with good results and, thus, to prevent the tampering attacks presented

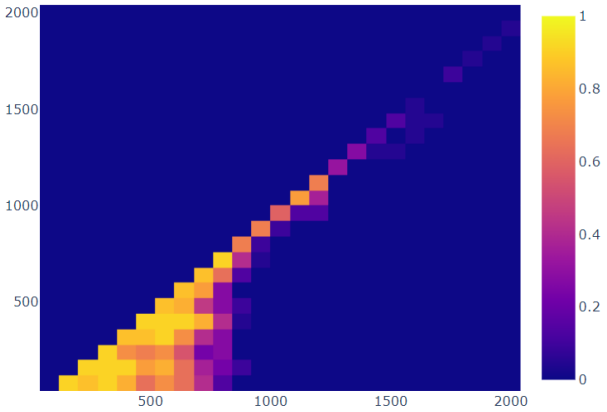

Figure 5. % of false negative per $d \rightarrow d^*$ mimicking for Symbol-to-symbol modification defense.

in the reference paper. Despite the good results, we have observed that our defense system fails in discriminating the manipulated from the non-modified samples for some pairs of distances (mainly small original distances and small differences between original and target distances) so further research should be done in this area.

References

[1] F. J. Anscombe. Graphs in statistical analysis. *The American Statistician*, 27(1):17–21, 1973.

[2] N. Aspert, D. Santa-Cruz, and T. Ebrahimi. Mesh: measuring errors between surfaces using the hausdorff distance. In *Proceedings. IEEE International Conference on Multimedia and Expo*, volume 1, pages 705–708 vol.1, 2002.

[3] Rick M Bütler, Christian Häger, Henry D Pfister, Gabriele Liga, and Alex Alvarado. Model-based machine learning for joint digital backpropagation and pmd compensation. *Journal of Lightwave Technology*, 39(4):949–959, 2020.

[4] Mayur Channegowda, Reza Nejabati, and Dimitra Simeonidou. Software-defined optical networks technology and

infrastructure: Enabling software-defined optical network operations [invited]. *J. Opt. Commun. Netw.*, 5:A274–A282, 10 2013.

[5] Haowen Deng, Tolga Birdal, and Slobodan Ilic. 3d local features for direct pairwise registration. pages 3239–3248, 06 2019.

[6] Xiaojie Fan, Yulai Xie, Fang Ren, Yiying Zhang, Xiaoshan Huang, Wei Chen, Tianwen Zhangsun, and Jianping Wang. Joint optical performance monitoring and modulation format/bit-rate identification by cnn-based multi-task learning. *IEEE Photonics Journal*, 10(5):1–12, 2018.

[7] Alex Ferrando and Víctor Novelle. Attack on distance predictor by mimicking target's constellation point distribution. 2022.

[8] Jerome H. Friedman, Jon Louis Bentley, and Raphael Ari Finkel. An algorithm for finding best matches in logarithmic expected time. *ACM Trans. Math. Softw.*, 3(3):209–226, sep 1977.

[9] Marija Furdek, Carlos Natalino, Fabian Lipp, David Hock, Andrea Di Giglio, and Marco Schiano. Machine learning for optical network security monitoring: A practical perspective. *Journal of Lightwave Technology*, 38(11):2860–2871, 2020.

[10] Thibault Groueix, Matthew Fisher, Vladimir G. Kim, Bryan Russell, and Mathieu Aubry. AtlasNet: A Papier-Mâché Approach to Learning 3D Surface Generation. In *Proceedings IEEE Conf. on Computer Vision and Pattern Recognition (CVPR)*, 2018.

[11] Rentao Gu, Zeyuan Yang, and Yuefeng Ji. Machine learning for intelligent optical networks: A comprehensive survey. *Journal of Network and Computer Applications*, 157:102576, 2020.

[12] Alexander T. Hoang, Kip D. Coonley, Faranak Nekoogar, and Matthew S. Reynolds. A battery-free rfid sensor tag with fiber-optic tamper detection. In *2016 IEEE SENSORS*, pages 1–3, 2016.

[13] Klanderman G.A. Rucklidge W.J. Huttenlocher, D.P. 1993.

[14] Alireza Javaheri, Catarina Brites, Fernando Pereira, and João Ascenso. A generalized hausdorff distance based quality metric for point cloud geometry. 03 2020.

[15] Oliver Jesorsky, Klaus Kirchberg, and R.W. Frischholz. Robust face detection using the hausdorff distance. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2091:90–95, 01 2001.

[16] R G Johnston. Tamper-indicating seals : practices, problems, and standards.

[17] Roger G. Johnston. Tamper detection for safeguards and treaty monitoring: Fantasies, realities, and potentials. *The Nonproliferation Review*, 8(1):102–115, 2001.

[18] R G Johnston and A R.E. Garcia. Physical security and tamper-indicating devices. 2 1997.

[19] Michael Majurski Dan Kilper Uiara Celine Darko Zibar Massimo Tornatore Joao Pedro Jesse Simsarian Jim Westdorp Josh Gordon, Abdella Battou. In *Summary: Workshop on Machine Learning for Optical Communication Systems*, volume 2100, 3 2020.

[20] S. Gray K. Shaneman. One pixel attack for fooling deep neural networks. *IEEE MILCOM 2004. Military Communications Conference, 2004.*, 2004.

[21] Boris Karanov, Mathieu Chagnon, Félix Thouin, Tobias A Eriksson, Henning Bülow, Domaniç Lavery, Polina Bayvel, and Laurent Schmalen. End-to-end deep learning of optical fiber communications. *Journal of Lightwave Technology*, 36(20):4843–4855, 2018.

[22] Faisal Nadeem Khan, Chao Lu, and Alan Pak Tao Lau. Machine learning methods for optical communication systems. In *Signal Processing in Photonic Communications*, pages SpW2F–3. Optical Society of America, 2017.

[23] Mingliang Li, Danshi Wang, Qichuan Cui, Zhiguo Zhang, Linhai Deng, and Min Zhang. End-to-end learning for optical fiber communication with data-driven channel model. In *2020 Opto-Electronics and Communications Conference (OECC)*, pages 1–3. IEEE, 2020.

[24] Ankush Mahajan. *Machine learning assisted QoT estimation for optical networks optimization*. PhD thesis, Polytechnic University of Catalonia.Signal Theory and Communications Department, 9 2021.

[25] Baraka Jacob Maiseli. Hausdorff distance with outliers and noise resilience capabilities. *SN Computer Science*, 09 2021.

[26] Mary Meeker and Liang Wu. Internet trends 2018, 2018.

[27] Munno, Turk, and Armstrong. Tamper detection of fiber optic links via modulation transfer function characterization. In *1994 Proceedings of IEEE International Carnahan Conference on Security Technology*, pages 112–119, 1994.

[28] Danish Rafique and Luis Velasco. Machine learning for network automation: overview, architecture, and applications [invited tutorial]. *Journal of Optical Communications and Networking*, 10(10):D126–D143, 2018.

[29] Nina Skorin-Kapov, Marija Furdek, Szilard Zsigmond, and Lena Wosinska. Physical-layer security in evolving optical networks. *IEEE Communications Magazine*, 54(8):110–117, 2016.

[30] Martin Skrodzki. The k-d tree data structure and a proof for neighborhood computation in expected logarithmic time. *arXiv:1903.04936v1*, 03 2019.

[31] Yongli Tang, Tao Liu, Xu He, Jinxia Yu, and Panke Qin. A lightweight two-way authentication scheme between communication nodes for software defined optical access network. *IEEE Access*, 7:133248–133256, 2019.

[32] Junzhe Zhang Tai Wang Ziwei Liu Dahua Lin Tong Wu, Liang Pan. Density-aware chamfer distance as a comprehensive metric for point cloud completion. *arXiv:2111.12702*, 11 2021.

[33] Abhishek Venketeswaran, Nageswara Lalam, Jeffrey Wuenschell, P. R. Ohodnicki Jr., Mudabbir Badar, Kevin P. Chen, Ping Lu, Yuhua Duan, Benjamin Chorpening, and Michael Buric. Recent advances in machine learning for fiber optic sensor applications. *Advanced Intelligent Systems*, n/a(n/a):2100067.

[34] Danshi Wang, Mengyuan Wang, Min Zhang, Zhiguo Zhang, Hui Yang, Jin Li, Jianqiang Li, and Xue Chen. Cost-effective and data size–adaptive opm at intermediated node using convolutional neural network-based image processor. *Optics express*, 27(7):9403–9419, 2019.