Enhancing optical network security with machine learning

Citation for the original published paper (version of record):
Furdek Prekratic, M., Natalino Da Silva, C. (2019)
Enhancing optical network security with machine learning
International Conference on Transparent Optical Networks, 2019-July
http://dx.doi.org/10.1109/ICTON.2019.8840458

Enhancing optical network security with machine learning

Marija Furdek, Carlos Natalino
Department of Electrical Engineering, Chalmers University of Technology,
Hörsalsvägen 11, 412 96 Gothenburg, Sweden
Tel: (46) 31 772 6028, e-mail: furdek@chalmers.se

ABSTRACT

As the critical communication infrastructure, optical networks have a vital role in safe and dependable transmission of massive amounts of data, supporting essential societal services. However, these networks are inherently vulnerable to a multitude of deliberate, man-made attacks targeting service disruption at the physical layer. Physical-layer attack techniques can range in their scope and effects, level of sophistication, locality, detectability, etc. An example of a relatively unsophisticated attack method is a deliberate fiber cut, typically targeting critical network elements (e.g., links with the highest betweenness) and resulting in straightforward transmission interruption [1]. More refined attack techniques rely on the insertion of harmful signal (e.g. in- and out-of-band jamming), or on external tampering with the fiber to degrade the transmission quality (e.g., polarization scrambling via fiber squeezing) [2]. Diverse attack techniques cause different effects, which complicates their detectability. For example, some attacks add unfilterable noise, some reduce the power of the affected optical channels, while some inflict changes in the state of polarization too quick for the coherent receiver to compensate [3]. Therefore, monitoring only the spectrum [4], or individual signal parameters such as the power, optical signal-to-noise ratio (OSNR), or presence of errors may result in inaccurate diagnostics and root cause attribution. This obstacle in quick recovery of affected services is further pronounced for newly emerging attack techniques whose effects may deviate from the attack signatures previously known to the network management system [5].

The complexity of the evolving physical-layer security landscape and the intricate interplay of different optical performance monitoring (OPM) parameters in the presence of diverse attack methods can greatly benefit from the application of machine learning techniques capable of deep data analysis. In this talk, we present how different data analytics and machine learning approaches can be applied to interpret the OPM data reported from the commercially available coherent receivers to identify anomalous operation and trigger security threat warnings. The analytical techniques are applied to experimental data obtained from an operator's metropolitan testbed subjected to in- and out-of-band jamming, and external polarization scrambling attacks. We begin with an analysis of the optical signal degradation caused by the different attack methods. We then investigate the application of several supervised learning approaches that, once trained on the experimental data, can detect the presence of an attack and identify its type and intensity. The accuracy of several classifiers is scrutinized, along with the relevance of OPM parameters reported by the coherent receivers and the impact of missing features. To gain insight into the potential of the network to detect emerging, previously unseen attack techniques, we further analyse the performance of unsupervised learning techniques that detect the anomalies in signal parameters introduced by attacks. The presented findings help achieve timely and accurate detection of physical-layer attacks and serve as a prerequisite for fast and effective attack response and network recovery.

Keywords: machine learning, anomaly detection, physical-layer attacks, optical network.

ACKNOWLEDGEMENTS

This article is based upon work from COST Action 15127 RECODIS and Celtic-Plus project SENDATE-EXTEND. We gratefully acknowledge Marco Schiano and Andrea Di Giglio from Telecom Italia for providing the experimental data used for analysis, and Coriant for providing the Groove G30 transponder used in the experiments.

REFERENCES

[1] J. L. Marzo, S. Gomez Cosgaya, N. Skorin-Kapov, C. Scoglio, H. Shakeri: A study of the robustness of optical networks under massive failures, *Opt. Switching Network.,* vol. 31, pp. 1-7, Jan. 2019.

[2] N. Skorin-Kapov, M. Furdek, S. Zsigmond, L. Wosinska: Physical-layer security in evolving optical networks, *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 110-117, Aug. 2016.

[3] C. Natalino, M. Schiano, A. Di Giglio, L. Wosinska, M. Furdek: Machine-learning-based detection and identification of physical-layer attacks in optical networks, submitted to *IEEE/OSA J. Lightwave Technol.,* Apr. 2019.

[4] Y. Li, N. Hua, Y. Yu, Q. Luo, Z. Zheng: Light source and trail recognition via optical spectrum feature analysis for optical network security, *IEEE Commun. Lett.*, vol. 22, no. 5, pp. 982-985, May 2018.

[5] M. Furdek, C. Natalino, M. Schiano, A. Di Giglio: Experiment-based identification of service disruption attacks in optical networks, in *Proc. SPIE Photonics West,* Feb. 2019, invited.