Machine Learning for Cognitive Optical Network Security Management

Machine Learning for Cognitive Optical Network Security Management

Marija Furdek, Carlos Natalino
Chalmers University of Technology, Hörsalsvägen 11, 412 96 Gothenburg, Sweden
furdek@chalmers.se

Abstract: This talk surveys the security threats pertinent to the optical network and outlines the progress and challenges in developing machine learning approaches for cognitive management of optical network security. © 2020 The Author(s)

1. Security Challenges in Optical Networks

As the only communications technology capable of supporting the incessant network traffic growth, optical networks are critical communication infrastructure carrying massive amounts of data over ultra-long distances. Because of their vital role in supporting services crucial for the society to function, they must be secured from various types of deliberate man-made attacks aimed at service disruption or unauthorized access to the carried data. Despite its extensive implications to overlaying communication services, optical-layer security has not been systematically addressed and incorporated into the overall network security management [1]. Network operators still lack the tools to achieve cognitive optical network security management, leaving important aspects of attack prevention, detection and remediation uncovered. Such a framework, supporting autonomous security diagnostics and management, is critical for realizing the Observe-Analyze-Act control loop to improve network performance and cost efficiency [2].

Security-oriented design of optical networks requires an assessment of various risks and attack vectors and incorporating this knowledge into optimization frameworks for solving complex network design problems. Examples of such approaches include attack-aware upgrade of the network infrastructure by sparsely adding links and/or nodes [3] or carefully distributing the content across a data center network [4] to alleviate the impact of targeted fiber cut attacks. Techniques to reduce the network exposure to harmful signal insertion attacks include strategic placement of devices with attack-thwarting capabilities, as well as attack-aware Routing [5] and Spectrum Assignment [6] under static [7], dynamic [8] and multi-hour traffic [9]. Eavesdropping attacks can be counteracted via encryption at various network layers – for example, using quantum shot noise-assisted ciphers at the optical layer [10]; or by increasing confidentiality levels via network coding and spread-spectrum techniques [11]. Network planning techniques to aid remediation of service disruption attacks can benefit from the identification of attack radii of each connection's working path and ensuring that the backup path does not fall within range of the same attack [12]. While classical optimization techniques (e.g., linear programming and heuristics) have been shown to substantially improve optical network resiliency to targeted attacks when applied to the above problems of attack surface reduction and remediation, they are incapable of eliminating the threat, calling for intelligent solutions for cognitive and automated attack detection.

2. Machine Learning for Security Monitoring Automation

Physical-layer attacks can have vastly different effects on the distinct Optical Performance Monitoring (OPM) parameters, which makes their detection extremely challenging. For example, a harmful jamming signal adds unfilterable noise to optical channels with whose spectrum it overlaps (in-band jamming), but it can also affect optical channels sufficiently separated from it in the spectral domain (out-of-band jamming), typically reducing the signal power at the received and degrading the Optical Signal to Noise Ratio (OSNR), leading to transmission errors. A polarization scrambling attack, in which the fiber is squeezed at a high frequency to cause fast-varying changes in the channel polarization state, can cause error bursts without affecting the channel power levels or OSNR. Encompassing experimental studies of physical-layer attacks at the optical link- and network level were performed in [13] and [14], respectively. Due to the complex interplay among different OPM parameters and the absence of models capable of capturing these effects or even consistent observable trends in OPM parameter values for different attack regimes, it is not possible to rely on a threshold-based approach for detection and identification of physical-layer attacks. Even more so, the use of pre-determined thresholds as triggers for (re)configuration actions is considered unreliable, ineffective and unscalable in the forthcoming transition towards cognition-driven automation of network planning and management workflows urged by network operators [15].

Due to their ability to process massive amounts of data and identify intricate patterns among a great number of performance indicators without the need to explicitly specify models or parameter thresholds, machine learning (ML) techniques are highly suitable for optical layer security diagnostics. ML has been applied to the detection of unauthorized signal presence by scrutinizing the received optical spectrum [16], and to the detection and identification of in-, out-of-band jamming and polarization scrambling [13,14], demonstrating strong potential to perform these functions in runtime environments. Despite this huge potential, carrier-grade deployment of ML techniques is still in its infancy and many challenges need to be overcome before achieving cognitive and autonomous optical network security management.

The choice of suitable ML techniques and their adaptation to runtime environments in Software-Defined Optical Networks is not trivial. It should take into account the requirements and performance of ML in terms of their accuracy, granularity of the diagnostic information they can provide, their applicability to novel emerging threats in the evolving network and security landscape, the complexity of their learning and/or inference phases, memory and processing requirements, etc. For example, as shown in [14], supervised learning techniques (e.g., Artificial Neural Networks, ANNs) can provide highly accurate and fine-granular information on the type and intensity of physical-layer attacks, learned through training. This comes at a trade-off of a relatively complex training phase, relying on abundant, representative data labeled by experts with prior specialist knowledge on the attack specifics, and the need to retrain upon admittance of a new connection or an emergence of a new type of threat. However, once trained, the inference complexity is relatively low. Unsupervised learning (e.g., Density-Based Spatial Clustering of Applications with Noise), on the other hand, does not perform any (re)training and hence, does not require attack-specific training data, but identifies attacks, i.e. anomalies as outliers in the clustered data. This allows for detection of new, previously unseen attack methods, at the expense of being unable to provide any fine-granular information about the attack type. The clustering requires obtaining and processing prior data, yielding high inference complexity. Semi-supervised learning (e.g., one-class support vector machine) combines the two aforementioned ML approaches and is applicable when data labelling is too costly or infeasible, so only a small subset of the data is labeled. This reduces its training complexity but also incurs inability of fine-granular attack identification. The lower accuracy of semi- and unsupervised learning (as opposed to supervised) requires embedding extra intelligence in the usage of ML modules' output using observation window and threshold definition, ensemble models that combine multiple ML models, and symbolic models that combine specialist knowledge with ML models.

References

[1] 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.
[2] L. Velasco, A. C. Piat, O. González, A. Lord, A. Napoli, P. Layec, D. Rafique, A. D’Errico, D. King, M. Ruiz, F. Cugini, and R. Casellas, “Monitoring and data analytics for optical networking: Benefits, architectures, and use cases,” IEEE Network, pp. 1–9, 2019.
[3] C. Natalino Silva, A. Yayimli, L. Wosinska, M. Furdek, “Infrastructure upgrade framework for content delivery networks robust to targeted attacks,” Opt. Switching Netw., vol. 31, pp. 202-210, Jan 2019.
[4] C. Natalino Silva, A. de Sousa, L. Wosinska, M. Furdek, “Content Placement in 5G-enabled Edge/Core Datacenter Networks Resilient to Link Cut Attacks,” Wiley Networks, vol. 75, no. 4, pp. 392-404, June 2020.
[5] N. Skorin-Kapov, J. Chen, L. Wosinska, “A New Approach to Optical Networks Security: Attack Aware Routing and Wavelength Assignment,” IEEE/ACM Trans. Netw., Vol. 18, Issue 3, pp 750-760, June 2010.
[6] M. Furdek, N. Skorin-Kapov, M. Grbac, “Attack-Aware Wavelength Assignment for Localization of In-band Crosstalk Attack Propagation,” IEEE/OSA J. Opt. Commun. Netw., Vol. 2, Issue 11, pp. 1000-1009, November 2010.
[7] K. Manousakis, G. Ellinas, “Attack-aware planning of transparent optical networks,” Opt. Switching Netw., vol. 19, pp. 97-109, Jan 2016.
[8] J. Zhu, B. Zhao, Z. Zhu, “Leveraging game theory to achieve efficient attack-aware service provisioning in EONs,” IEEE/OSA J. Lightwave Technol., vol. 35, pp. 1785–1796, May 2017.
[9] K. Manousakis, P. Kolios, G. Ellinas, “Multi-Period Attack-Aware Optical Network Planning under Demand Uncertainty,” in Optical Fiber and Wireless Communications, R. Roka (Ed.), Intech Open, June 2017.
[10] K. Tanizawa, F. Futami, “Single-channel 48-Gbit/s DP PSK Y-00 quantum stream cipher transmission over 400- and 800-km SMF,” Optics Express, vol. 27, no. 18, pp. 25357-25363, Sept. 2019.
[11] G. Savva, K. Manousakis, G. Ellinas, “Eavesdropping-Aware Routing and Spectrum/Code Allocation in OFDM-Based EONs Using Spread Spectrum Techniques,” IEEE/OSA J. Opt. Commun. Netw., vol. 11, no. 7, pp. 409-421, July 2019.
[12] M. Furdek, N. Skorin-Kapov, L. Wosinska, “Attack-aware dedicated path protection in optical networks,” IEEE/OSA J. Lightwave Technol., vol. 34, no. 4, pp. 1050-1061, Feb. 2016
[13] C. Natalino, M. Schiano, A. Di Giglio, L. Wosinska, M. Furdek, “Experimental study of machine-learning-based detection and identification of physical-layer attacks in optical networks,” IEEE/OSA J. Lightwave Technol., vol. 37, no. 15, pp. 4173–4182, Aug 2019
[14] M. Furdek, C. Natalino, F. Lipp, D. Hock, A. Di Giglio, M. Schiano, “Machine learning for optical network security management: A practical perspective [Invited],” IEEE/OSA J. Lightwave Technol., ECOC 2019 Special Issue, pp. 1-12, April 2020.
[15] D. Rafique, T. Szyrkowiec, H. Grießer, A. Autenrieth, J.-P. Elbers, “Cognitive assurance architecture for optical network fault management,” IEEE/OSA J. Lightwave Technol., vol. 36, no. 7, pp. 1443–1450, Apr 2018.
[16] Y. Li, N. Hua, Y. Yu, Q. Luo, and X. 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.