Autonomous Security Management in Optical Networks

Autonomous Security Management in Optical Networks

Carlos Natalino[1], Andrea Di Giglio[2], Marco Schiano[2], Marija Furdek[1]

[1] *Electrical Engineering Department, Chalmers University of Technology, 41296 Gothenburg, Sweden*
[2] *Telecom Italia, Via Guglielmo Reiss Romoli, 274 – 10148 Turin, Italy*

furdek@chalmers.se

Abstract: The paper describes the Optical Security Manager module and focuses on the role of Machine Learning (ML) techniques. Issues related to accuracy, run-time complexity and interpretability of ML outputs are described and coping strategies outlined.

1. Secure Optical Networks Enabling Network Evolution Beyond 5G

The growing deployment of 5G networks across the world starts to enable industry and academia to contrive the next milestones for networks Beyond 5G (B5G). Among the expectations, higher data rates, stricter latency requirements and the need for more power/spectrum efficient networks are a recurrent consensus [1]. Stronger integration between optical and wireless networks blended with edge/cloud computing can enable significant advances in fulfilling these requirements. This may require transition from the provisioning of 5G end-to-end services towards end-to-end optical-transparent services, eliminating intermediate exchange points and optical-electrical-optical conversions. End-to-end optical-transparent services would mean that lightpaths transparently connect base stations to edge/cloud sites that perform base-band processing co-located with the service processing. This requires extending the optical domain further towards the edge, and establishing lightpaths across multiple network segments and domains.

Although very beneficial in many aspects, end-to-end optical-transparent services may aggravate security risks at the optical layer and their impact to overlay services. When lightpaths traverse different network segments (e.g., access, metro, core, intra-datacenter), attacks targeting the optical layer can have higher disruption potential than in current architectures with optical-electrical-optical conversions at each segment exchange point. Filtering optical devices can mitigate a subset of attacks and reduce their propagation in the network. However, certain networking solutions such as filterless architectures reduce or completely eliminate the use of filtering devices to maximize cost-efficiency [2, 3], which intensifies the disruption potential of attack techniques such as jamming.

The increasing deployment of fiber and the transition towards networks supporting rapid and frequent state changes calls for intelligent, fast and reliable management of optical network security. Autonomous security management frameworks are essential for the secure and stable operation of optical networks in the evolving security threat scenario. Such frameworks represent an important novel feature in the cognitive NMS (C-NMS) paradigm [4] that relies on controllers to provide end-to-end services demanded by an orchestrator and easily accessible to users and external systems via standard application programming interfaces (APIs).

Our proposed optical security assurance framework, illustrated in Fig. 1, entails functionalities for telemetry, detection and identification of security breaches, remediation and neutralization of threats [5]. Telemetry functions include collection and storage of the optical performance monitoring (OPM) data from the coherent optical transceivers (potentially from other devices as well), or from the network controller. Detection and identification of threats requires a deep insight into the OPM data to identify anomalies and correctly attribute them to different attack techniques, which is a task that greatly benefits from machine learning (ML) techniques as the most promising approach to enable such a concept. Security statuses of individual connections derived by ML from the data retrieved from the coherent transceivers can then be correlated to perform localization of the breached network element. The detection and localization of the breach are important preconditions for remediation of the threat, which can be performed in two steps. The first step refers to a quick fix (e.g. simple rerouting) aimed at minimizing the down time, while the second entails a more complete set of tailored countermeasures for ultimate elimination of the breach.

Adoption of ML in network Security Operation Centers (SOCs) meets important challenges related to, among others, the availability of representative data, the accuracy and run-time complexity of ML models, the reliability and interpretability of the models' outputs, and the model resilience to adversary attacks. We address a fraction of these challenges linked to model accuracy, run-time complexity and interpretability, and outline strategies to overcome them.

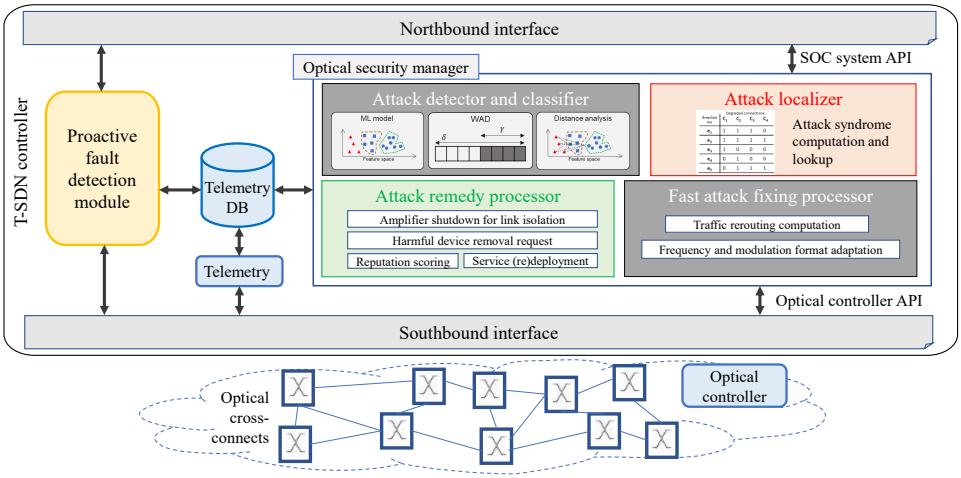

Fig. 1. Architecture of the optical security manager embedded into the cognitive transport software defined (T-SDN) controller.

2. Machine Learning for Network Security Diagnostics

Machine learning techniques are an auspicious contender for automation of many complex network control and management tasks ranging from Quality of Transmission (QoT) estimation of unestablished lightpaths [6] to failure detection [7]. These techniques play a particularly relevant role in the context of security, where their demonstrated effectiveness in distinguishing intricate effects of various security breaches on OPM parameters can provide important diagnostic support to network security specialists.

Supervised learning (SL) approaches, such as Artificial Neural Networks (ANNs), rely on *a priori* available complete information about what needs to be learned in the form of an expert-labeled representative dataset. This allows them to provide fine-granular diagnostic information upon training, e.g. the type of the breach and its intensity. Unsupervised learning (UL) techniques, such as Density-Based Spatial Clustering of Applications with Noise (DBSCAN), do not have a labeled dataset at their disposal. Instead, they learn to cluster the data so as to separate the normal from anomalous samples that appear as outliers. Consequently, they can only provide coarse information on the presence of an attacks without further details. However, due to the ability to detect previously unseen events they have a major advantage in detecting new types of security breaches. Semi-supervised learning (SSL) approaches, such as One-Class Support Vector Machine (OCSVM), are similar to UL in the absence of previous knowledge of attacks (and, hence, in their ability to detect novel types of breaches), and are akin to SL in the training on a small amount of labeled normal-condition data that facilitates outlier detection.

2.1. *Achieving High Accuracy of ML Models*

To provide high accuracy, an ML model should attain excellent performance in matching the predicted outputs to the actual inputs, measured, e.g., in terms of false positive and false negative rates. The former refers to raising false alarms under attack-free conditions, while the latter refers to unnoticed attack presence. Due to the *a priori* defined mappings between inputs and outputs, SL techniques have been reported to obtain high accuracy in detection and identification of attacks [8]. However, studies on SSL and UL have identified difficulties in achieving equivalently high accuracy in attack detection [9], demanding additional scrutiny in using the ML models' diagnostic outputs.

A promising strategy to overcome the issue of false positive and false negative rates of the ML algorithms and reduce the impact of possible fast oscillations in the detected security status is Window-based Attack Detection (WAD) [9]. Instead of directly using the output of an ML model obtained in each monitoring cycle, WAD observes the diagnostic output over a pre-defined window and raises an alarm only when the number of samples categorized as an attack exceeds a pre-defined threshold. By tuning the values of the window size and the threshold, a trade-off can be achieved between the false detection probability and the time to raise an alarm upon an attack.

2.2. *Reducing Run-time Complexity of ML Models*

Commercially available coherent digital signal processing (DSP)-enabled transceivers can provide a rich set of analog and digital signal parameters. For example, in each minute, the Network Management System (NMS) can receive minimum, maximum and average values of a dozen optical performance monitoring (OPM) parameters. Such high number of features processed at high recurrence is beneficial for many ML models, but it may result in a high processing load. Therefore, to reduce run-time complexity, the relevance of the features should be examined, and additional dimensionality reduction techniques should be applied.

In SL, the rich labeled dataset can be manipulated during training and testing to understand the relevance of the

features to the accuracy. In [8], it was shown that the number of features reported to the NMS can be almost halved without impacting the classification error of the ANN. However, eliminating OPM parameters from UL and SSL processing may cause these models to miss emerging types of threats. Instead, these models can be combined with dimensionality reduction techniques that transform the dataset while encoding its diversity.

In [5], the DBSCAN and OCSVM are combined with three dimensionality reduction approaches. The first, principal component analysis (PCA), tries to encode as much variance as possible from the original dataset into the encoded dataset. The second approach, called t-distributed stochastic neighbor embedding (t-SNE), tries to approximate the distances between samples in the encoded dataset to the ones found in the original dataset. The third technique, an autoencoder, is a neural network trained containing a feature extraction layer, and trained such that the output matches the input as closely as possible. After training, the encoder part of the neural network is used for dimensionality reduction. The observed benefit of these techniques is the most significant for DBSCAN combined with PCA, improving both the accuracy and the run time compared to processing the full data set.

2.3. Achieving Interpretability of ML Models' Outputs

While the automation of security management is expected to reduce the requirements on interventions by human experts, they are unlikely to be completely eliminated. Instead, effort is needed to improve the interaction between the humans and ML by, among other aspects, making the output of the ML models more easily interpretable by the security specialists. This would allow the security managers to understand why an ML model attributes a particular setting to an attack and which trends in various OPM parameters triggered such a response. To this end, a Root Cause Analysis (RCA) framework was proposed that analyzes the clusters of OPM data constructed by a UL algorithm [10]. When an anomaly is detected, the framework computes the difference between the average value of each feature in the anomalous samples and the average value of the same feature in the closest normal cluster. The computed difference is then visualized across all features in the form of an anomaly vector. The vector goes beyond simple time series visualization that is the currently used approach and provides meaningful insights into the detected deviations in the entire feature set.

3. Open Challenges and Opportunities

As a challenging and evolving subject, the management of optical network security requires numerous novel procedures to be developed and incorporated in dynamic production settings. One of the still largely unaddressed problems is attack remediation, which should encompass definition of protocols and strategies to reconfigure the optical network upon the detection/identification of an attack. Here too ML techniques can play an important role in e.g. long-term tracking of reputation of different network elements and services, as well as adaptation of initially deterministic remediation strategies to cope with an intelligent and adaptive adversary. As attack reports and data may be subject to non-disclosure agreements, security-enhancing collaboration among multiple network stakeholders may benefit from the application of federated ML to preserve privacy. Maintaining security of the control plane and using blockchain can help ensure data integrity and exchange of verified model updates.

Acknowledgements This work has been carried out with support from the Swedish Research Council (2019-05008), VINNOVA (AI-NET-PROTECT), and the European Commission 5GPPP TeraFlow (101015857).

References

1. I. Tomkos *et al.*, "Toward the 6G network era: Opportunities and challenges," IT Prof. **22**, 34–38 (2020).
2. E. Archambault *et al.*, "Routing and spectrum assignment in elastic filterless optical networks," Transactions on Netw. **24**, 3578–3592 (2016). DOI: 10.1109/TNET.2016.2528242.
3. P. Pavon-Marino *et al.*, "Techno-economic impact of filterless data plane and agile control plane in the 5G optical metro," J. Light. Technol. **38**, 3801–3814 (2020). DOI: 10.1109/JLT.2020.2982131.
4. D. Rafique *et al.*, "Cognitive assurance architecture for optical network fault management," J. Light. Technol. **36**, 1443–1450 (2018). DOI: 10.1109/JLT.2017.2781540.
5. M. Furdek *et al.*, "Optical network security management: requirements, architecture, and efficient machine learning models for detection of evolving threats," J. Opt. Commun. Netw. **13**, A144–A155 (2021). DOI: 10.1364/JOCN.402884.
6. C. Rottondi *et al.*, "Machine-learning method for quality of transmission prediction of unestablished lightpaths," J. Opt. Commun. Netw. **10**, A286–A297 (2018). DOI: 10.1364/JOCN.10.00A286.
7. L. Velasco *et al.*, "Learning from the optical spectrum: Soft-failure identification and localization," in *OFC,* (2018).
8. C. Natalino *et al.*, "Experimental study of machine-learning-based detection and identification of physical-layer attacks in optical networks," J. Light. Technol. **37**, 4173–4182 (2019). DOI: 10.1109/JLT.2019.2923558.
9. M. Furdek *et al.*, "Machine learning for optical network security monitoring: A practical perspective," J. Light. Technol. **38**, 2860–2871 (2020). DOI: 10.1109/JLT.2020.2987032.
10. C. Natalino *et al.*, "Root cause analysis for autonomous optical networks: A physical layer security use case," in *ECOC,* (2020), pp. We2K–1.