Machine Learning for Optical Network Security Management

Machine Learning for Optical Network Security Management

Marija Furdek, Carlos Natalino
Electrical Engineering Department, Chalmers University of Technology, SE-41296 Gothenburg, Sweden
furdek@chalmers.se

Abstract: We discuss the role of supervised, unsupervised and semi-supervised learning techniques in identification of optical network security breaches. The applicability, performance and challenges related to practical deployment of these techniques are examined.

1. Introduction

The development of optical communication networks into trustworthy and reliable ecosystems that satisfy the tight performance requirements of 5G and beyond services entails high target levels of resilience to a variety of failures. Apart from resilience to inadvertent failures caused by e.g. equipment aging or misconfiguration, optical networks must also be able to sustain deliberate man-made attacks aimed at violating confidentiality, integrity or availability of communication. Methods of attacks targeting the optical layer can vary diversely in their sophistication, scope, persistence, difficulty of detection, etc. Fiber cut attacks, for example, are relatively straightforward to perform, their effect can be boosted by targeting more critical links (e.g., links with the highest betweenness), they affect all carried services, and last until repaired. Fiber tapping for traffic analysis and eavesdropping purposes, e.g. via microbending, requires more effort from an attacker but can also be more difficult to detect if the incurred losses are low and/or occur sporadically. Harmful signals can also be inserted into a breached fiber to jam the co-propagating signals at the same (in-band-jamming), or a different wavelength (out-of-band-jamming). Moreover, service quality can be degraded without necessarily breaching the fiber. If fiber is squeezed at a sufficiently high frequency, the incurred changes in the state of polarization will be too fast for the coherent receiver to compensate for, which will result in erroneous detection. Efforts in improving optical network security are typically categorized according to their objectives into security assurance, diagnostics, and remediation. Each of these categories entails a set of challenges, summarized in Fig. 1.

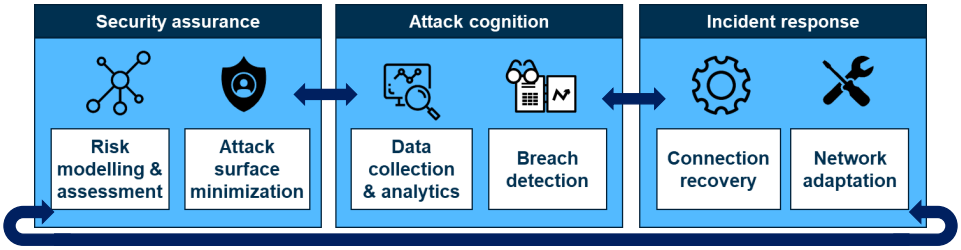

Fig. 1. Three pillars of optical network security management.

Security assurance Guaranteeing a certain level of robustness to deliberate attacks requires detailed risk analysis, identification of attack vectors, and evaluation of the size of the network exposed to attacks, possibly combined with the definition of new risk measures. Based on such evaluation, security-enhancing network design should then apply known good practices and/or develop novel methods to decrease network vulnerability to known attack methods and reduce attack surface. This step needs to be periodically revisited to account for the emergence of novel security threats or the elimination of existing ones by new technological solutions.

Attack cognition Detection of security breaches in optical networks requires deep knowledge about potential attack entry points and effects (so-called signatures) of a variety of attack techniques to the optical signal parameters. Continuous collection of Optical Performance Monitoring (OPM) data and its real-time analysis is paramount for quick and accurate diagnostics of security breaches. In optical networks, collection of OPM data is a challenge due to the sparse deployment of costly OPM devices and a lack of a standardized set of OPM parameters to be provided by such equipment. Modern, commercially available coherent optical receivers offset this issue by collecting a rich OPM dataset and exposing it to the network management plane via standardized interfaces. As different attack techniques cause intricate changes in the relations of different signal parameters, and exact models

of physical-layer impairments under attacks do not exist, detecting and identifying security breaches can greatly benefit from the application of Machine Learning (ML) techniques.

Incident response Once a breach has been detected and localized, affected services need to be recovered as quickly and efficiently as possible, and the attack source needs to be neutralized. The complexity of service recovery steps can vary for different attack techniques, and it can encompass, e.g., adaptation of the applied encryption mechanisms to protect from eavesdropping, adaptation of the modulation format to counterbalance service degradation, changing of the spectrum and/or routing of the connections, etc.

Although described separately, the three facets of optical network security management are intertwined and require joint considerations as well as feedback loops among all steps to boost their efficiency. In this paper, we focus on the latest advances and integration of ML for attack detection.

2. Supervised, Unsupervised and Semisupervised Learning for Security Diagnostics

Machine learning is regarded as an attractive tool for solving many problems in optical communications that require insight into complex phenomena when explicit models or complete information are unavailable. Diagnostics of optical layer security entail *(i)* detecting that a breach has occurred, *(ii)* identifying the properties of the breach (e.g. its type and intensity) and *(iii)* determining the location of the breach. This needs to be done under the evolving threat environment, where a new, previously unseen type of attack can occur at any time.

Based on the dataset requirements and training procedures, ML approaches can be divided into supervised, unsupervised and semisupervised learning (SL, UL, SSL, respectively) [1]. Supervised learning, e.g., Artificial Neural Networks (ANNs) as a representative SL model, rely on extensive training over a representative dataset labeled by experts. Details of the attack scenarios analyzed by ANN can be as finely granular as the data gathering process allows. Once the characteristics of the considered dataset are learned through training, ANN can detect the presence of an attack and determine its type and intensity [2]. This comes at the expense of high training complexity and the necessity of re-training whenever the status of the connections in the network changes. As SL techniques can only distinguish among the known attack types, new attack type discoveries also require re-training.

The underlying principle of unsupervised learning, e.g., Density-Based Spatial Clustering of Applications with Noise (DBSCAN) as a representative UL model, is to cluster the OPM data such that the data from the attack conditions appear as outliers from the data characterizing normal operating conditions. UL can only detect the presence of a security breach and cannot provide as finely-granular information on the attack profile as SL. UL typically does not require training, but unlike SL, the complexity of inference is high, and it also requires a certain number of prior samples to form a baseline to which anomalies are compared. However, a major advantage of UL over SL lies in the fact it is able to react to samples matching a new, previously unseen and untrained for attack method. UL models do not require re-training upon introduction of new attack types, or when the network connection status changes.

Semi-supervised learning, e.g., One-Class Support Vector Machine (OCSVM) model, lies between SL and UL as it applies training on an amount of labeled data, in an effort to adjust the model parameters and achieve tight enclosure of normal samples within a spatial region. The model can then be applied on large amounts of unlabeled data, detecting samples that fall outside the learned region as outliers. This approach is very attractive for applications where the number of anomalies (i.e., attacks) is not bounded or it is impractical to represent all of them in the training dataset. Consequently, SSL cannot provide fine-granular identification of attacks but its advantages refer to the fact that, unlike SL, it does not require a complete labeled dataset, while, unlike UL, it does not require prior samples at every inference either, and has lower inference complexity. SSL models do not need re-training when a new attack type is discovered, but it is necessary when a new connection is established.

The above properties have important implications on the practical deployment of SL, UL and SSL modules, not only in terms of their performance, but also for the design and implementation choices. For example, SL and SSL support stateless operation, which means that these ML modules can run on the data provided by the Network Management System (NMS) for a snapshot of the network state. On the other hand, UL requires the prior network states to be delivered from the NMS as well in order to support stateless operation, which increases the memory and communication overhead with the network control, but allows the ML modules to be simpler, and more easily migrated and scaled. An alternative is to deploy the security diagnostic approaches as stateful services, where each module maintains the necessary long-term information for its execution. This reduces the communication overhead with the NMS, but makes the modules more resource-demanding and less adaptable.

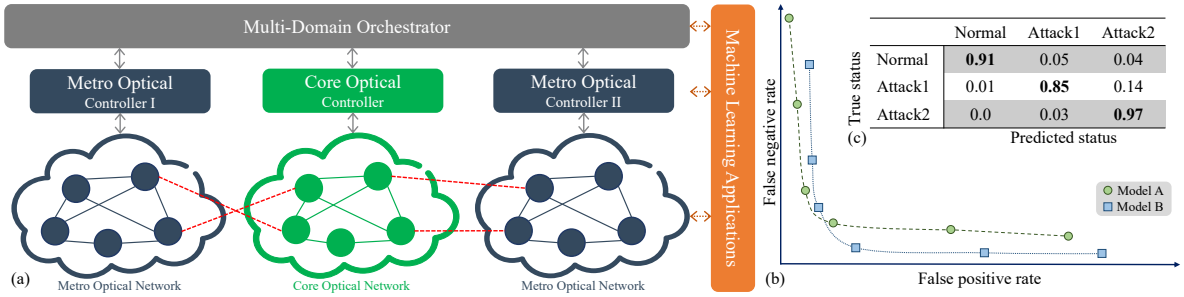

Fig. 2. (a) ML-assisted security management in multi-domain optical networks. (b) Performance trade-off among different ML models. (c) Confusion matrix for SL models.

3. Challenges of Applying ML to Carrier-Grade Optical Network Security

The benefits of ML models in optical network use cases have been studied and demonstrated for several years. Still, the deployment of these models in production carrier-grade environments is in its infancy. This reflects several challenges faced by operators in making ML execution reliable and tightly integrated to the workflows and tools already in place.

First, ML models should be accessible to a variety of network elements, ranging from optical nodes (enabling paradigms known as federated or hierarchical learning [3]) to multi-domain orchestrators (enabling multi-domain security management). Fig. 2(a) illustrates ML applications with multi-protocol adaptive interfaces, capable of exposing their services to the different network elements involved in the security management process. In the context of Software-Defined Networking (SDN), applications are external modules that implement functionalities by consuming or manipulating information from the SDN controller.

Second, the accuracy of single-model single-sample ML might not meet the expectations for carrier-grade deployments. Fig. 2(b) illustrates a typical trade-off (for UL and SSL models) important to consider when deciding which model to use. While *Model A* offers lower false negative rates, *Model B* offers lower false positive rates. The decision of which model is more acceptable depends greatly on the use case. Fig. 2(c) shows a confusion matrix (applicable for SL models), where it is usual not to observe perfect accuracy, in addition to possible inaccuracies that may arise when new data is introduced. In this case, advanced strategies can be used to reduce or even eliminate inaccuracies. For instance, a sliding-window-based approach can improve accuracy by smoothing out inaccuracies scattered over an observation window with several correctly identified samples. Another alternative is to use ensemble models, which combine multiple ML models to obtain better performance. Finally, symbolic models can be used to combine specialist knowledge with the results from ML models, benefiting from the powerful ML models while leveraging on long-term learned experiences from experts.

A third requirement is related to the execution performance of the ML models. Carrier-grade deployments adopt an interval-defined monitoring cycle. Within this cycle, OPM data must be gathered from devices and sent to ML applications, while the ML assessment should be consolidated in the SDN controller. With the evolution of optical networks and the services they support, this cycle interval is expected to tighten in the near future. Therefore, low-complexity (training and/or inference) models used in conjunction with purpose-specific ML accelerators, containerization and load balancing are key to the implementation of encompassing security management without impacting control procedures in place.

Finally, current operator deployments have a mix of current-generation and legacy devices that must be supported by the ML models. This means that the OPM data will not always be readily available from coherent transceivers usually considered [4]. A potential solution is to exploit computer vision models to perform security management tasks. In this case, graphical representations of the channel state, e.g., constellation or eye diagrams, can replace OPM data and provide a unified characterization of optical channel state. However, computer vision models are usually more complex, challenging the aforementioned monitoring cycle intervals.

4. Conclusions

This paper summarizes the main aspects of optical network security management, discusses the role of different ML techniques in diagnosing security breaches, examines their advantages and trade-offs, and elaborates on the challenges of adopting these techniques in real-world carrier-grade deployments.

References

1. F. Musumeci *et al.*, J. Light. Technol. **37**, 4125–4139 (2019). DOI: 10.1109/JLT.2019.2922586.
2. C. Natalino *et al.*, J. Light. Technol. **37**, 4173–4182 (2019). DOI: 10.1109/JLT.2019.2923558.
3. G. Liu *et al.*, J. Light. Technol. **37**, 218–225 (2019). DOI: 10.1109/JLT.2018.2883898.
4. M. Furdek *et al.*, in *Proc. of ECOC,* (2019), p. We2.58.