Chapter 15
Intelligent and Optical Security Monitoring for 6G Communications

Sindhumitha Kulandaivel
National Institute of Technology, India

Madhumitha Kulandaivel
SRM University, India

Keerthana N. V.
https://orcid.org/0000-0001-8878-2083
Velalar College of Engineering and Technology, India

ABSTRACT

The infrastructure of communication technologies in recent years has grown more complex and autonomous to meet societal requirements. Advanced technologies such as optical communication due to their enormous bandwidth and less latency capabilities have become the most sought-after candidates for 6G communications. The optical networks provide an agile and secure platform for effective data transmission. Thus, it is important to include cognitive and intelligent security monitoring for autonomous optical network management to improve reliability. Machine learning is a great tool that provides advancements in security monitoring in terms of accuracy and cost-effectiveness for optical network diagnosis and management. This chapter discusses the vulnerability of optical networks to various security threats in the physical layer along with countermeasures for network survivability. Several monitoring techniques using various performance parameters are also discussed for effective attack identification and localization to ensure robust optical network performance for 6G communications.

1. INTRODUCTION

The fast-growing data consumption of the advanced applications of individual user practices and the exponentially growing number of users have resulted in the surge of data quantity and quality requirements. To meet these never-ending demands the communication networks are shifting to advanced technologies

DOI: 10.4018/979-8-3693-8799-3.ch015

such as optical communications which provide huge bandwidth capabilities, high data rates, long-distance transmission, and less loss and latency to provide efficient data transmission. Optical communication technologies are being actively embraced as an integral part of future communication networks such as 6G technology (Jeon et al., 2023). Communication technologies are evolving distinctively each decade to meet user requirements. In that way, the 6G technology aims to connect a massive number of devices at ultra-high speeds and minimal latency to enable robust networks.

The optical networks can be prone to varying levels of vulnerabilities resulting in service disruption to perform physical layer attacks (Skorin-Kapov et al., 2016). The attacks can be direct or indirect for example cutting the fiber is a direct attack that causes information loss also known as eavesdropping and introducing hard-to-detect jamming signals is an indirect attack that is more sophisticated to identify. The attack methods can vary depending upon the type, the damage potential of an attack, and the difficulty level of identifying the attack to apply appropriate counteractive measures. The extent of information loss depends upon the spectral strength of the jamming signal.

Security attacks can also be performed on the optical signal without necessarily affecting the optical fiber by introducing polarization scramblers. This polarization attack fast varies the polarization angle leading to errors in the receiving end. The complex effect of the physical layer attacks on the signal quality and its identification is a challenging task to enable efficient transmission. It is essential to implement the detect-isolate-correct cycle to support intelligent autonomous optical networks to improve performance and security while maintaining lower costs. Optical signal security breaches in the physical layer can cause correlated failures in the upper layers making security monitoring a challenging task. Effective mitigation of these attacks includes implementing fast and effective corrective measures as well as adaptation of the network to prevent similar future attacks (Hugues-Salas et al., 2019).

In recent times, the integration of various advanced ML techniques into several aspects of optical networks such as optical signal quality monitoring (Tizikara et al., 2022), resource allocation, and routing (Moharrami et al., 2017) has fostered a powerful tool for efficient autonomous optical networks. Hence, ML-based security monitoring in the physical layer has been successfully implemented to detect jamming and polarization attacks (Furdek et al., 2020). ML provides an effective alternative to existing traditional analytical methods of security monitoring using predetermined thresholds as an indicator. These threshold indicators are unreliable and ineffective in the case of reconfigurable and complex network architectures. ML has been successfully applied to various optical network problems such as light path establishing and rerouting, quality of transmission (QoT) estimation (Zhang et al., 2022), transmitter configuration (Musumeci et al., 2018), fault detection and diagnosis, non-linearity and filtering effects monitoring (Catanese et al., 2019) to maintain efficient error-free transmission. The various ML-based approaches are based on either supervised, unsupervised, or semi-supervised algorithms to perform the desired task. Since physical layer attacks can cause varying effects on the optical signal performance parameters, determining exact thresholds for applying countermeasures cannot be accurately determined. ML has proved to be a dependable solution for predictive identification and estimation for supporting network adaptability.

Various works have been carried out using techniques such as support vector machine (SVM), k-nearest neighbors (k-NN), artificial neural network (ANN), and deep learning (DL) for the detection of possible attacks using several ways at both link and network levels. For example, the optical signal distortion in the optical spectrum at the receiving end is monitored to identify the type and degree of attack. The ML algorithms are trained using optical performance monitoring (OPM) parameters for accurate identification of security breaches. On the other hand, using unsupervised and semi-supervised