Machine Learning and Network Security

Hamzah Ahmed Faraj Al-Rubaye

College of Electrical and computer engineering, Altinbas university

Machine Learning, an essential element of artificial intelligence, plays a vital role in fortifying network security. Despite its global acceptance, mastering the utilization of machine learning for network security requires substantial investment of time. Nonetheless, machine learning equips us with indispensable abilities to detect sophisticated hacker attacks proactively, often evading traditional human detection methods. Incorporating machine learning models has quickened the advancement of decision support systems in network security, boosting their speed, precision, and overall effectiveness. However, the efficacy of machine learning in this realm faces significant obstacles due to the increased susceptibility to adversarial attacks, particularly in crucial areas such as malware detection, intrusion detection, and spam filtering. The inherently adversarial nature of these applications perpetuates an ongoing battle between attackers and defenders. Recent advancements in machine learning have showcased its effectiveness in addressing complex issues, frequently rivalling or even surpassing human capabilities. Nonetheless, research indicates that machine learning models are susceptible to various attacks, posing a significant risk to both the models themselves and the systems they safeguard. Critically, these attacks operate covertly, exploiting the inherent opacity of deep learning models. While machine learning presents promising avenues for enhancing network security, it also introduces new challenges and threats that demand continuous research and innovation to counter evolving adversarial tactics.

Keywords: Machine Learning, Network, Security, Artificial Intelligence, Hacker.

1. Introduction

Machine Learning serves as the cornerstone of artificial intelligence (AI), enabling systems to accumulate knowledge and evolve independently from data without explicit programming. In essence, the primary goal is to develop computer programs with the capability to access data and autonomously improve their comprehension through self-directed learning. This process starts with exposure to data, whether through specific experiences or instructions, enabling the identification of patterns within the data. Ultimately, this leads to making informed decisions guided by predefined criteria.. The ultimate objective is to empower computers to learn and act autonomously, without human intervention, adapting actions as necessary (Expertsystem.com, 2017). In the domain of computer networks, significant emphasis is placed on network security. While humans traditionally oversee security protocols, their susceptibility to errors highlights the importance of training machines to strengthen and improve network safety. Although the journey toward fully integrating machine-driven

network security may span decades, investing in research and development within this technological domain is crucial to bolstering network security by Rahul [2].

Application of Machine Learning in Network Security

Harnessing Machine Learning for security network requires extensive research, and the transition from traditional security measures may take longer than initially anticipated. Nevertheless, the current landscape showcases numerous instances of machine learning applications in network discovery, as outlined below [3].

Network security is of paramount importance for organizations, encompassing both corporate entities and governmental bodies. Ensuring robust cybersecurity is crucial for safeguarding sensitive data against potential breaches or leaks. With the growing prominence of AI and ML, these technologies have become indispensable assets in the realm of cybersecurity. ML offers a broad spectrum of applications in cybersecurity, spanning from threat identification to enhancing existing antivirus systems and combating AI-driven cyber threats [4].

Fig. 1. delineates five primary applications of Machine Learning in Cybersecurity, providing companies with tools to bolster their security measures. The process can initiate by integrating AI into current cybersecurity protocols and gradually transitioning to specialized AI and ML cybersecurity solutions. This may involve employing predictive analytics for threat detection, leveraging natural language processing to augment security measures, and refining biometric-based authentication techniques [5];

1. Cyber Threat Identification

Given the potential catastrophic consequences of a system breach, cybersecurity stands as a vital cornerstone for all companies. A significant challenge in this field is distinguishing between legitimate connection requests and potentially suspicious activities, such as large-scale data transfers. This differentiation between genuine company operations and cyber threats poses a formidable obstacle for cybersecurity professionals, particularly within large corporations where the sheer volume of requests can overwhelm human oversight. This is where the integration of machine learning becomes invaluable, offering substantial support to professionals. An AI and ML-driven cyber threat identification system plays a crucial role in monitoring both incoming and outgoing communications, as well as system requests, effectively identifying and flagging suspicious activities. For example, companies like Versive offer cybersecurity software that utilizes artificial intelligence to bolster defense mechanisms against potential threats.

2. AI-based Antivirus Software

Installing antivirus software before using any system is highly recommended. This is because antivirus programs protect your system by carefully examining new files on the network to confirm if they match known virus or malware signatures. However, traditional antivirus software requires frequent updates to stay synchronized with the constantly evolving landscape of new viruses and malware. This is where machine learning can provide significant assistance. Antivirus software integrated with machine learning is tailored to detect viruses or malware based on their abnormal behavior rather than solely relying on signatures. This method enables it to effectively combat both known threats and newly emerging viruses or

malware. For example, Cylance, a software company, has developed an intelligent antivirus that learns to identify viruses or malware from scratch, thereby reducing the reliance on signature identification alone.

3. User Behavior Modeling

Certain cyber threats target specific companies by illicitly obtaining the login credentials of their users in an attempt to gain unauthorized access to the network. When user credentials are legitimate, traditional antivirus software may face difficulty in detecting such attacks, potentially allowing cyberattacks to slip under the radar. In such scenarios, machine learning algorithms play a crucial role in modeling user behavior. These algorithms are trained to understand the behavior of individual users, including their patterns of logging in and out. If a user deviates from their typical behavior, the machine learning algorithm detects it and notifies the cybersecurity team for further investigation. While some alterations in user behavior may be normal, this approach enhances the identification of cyber threats compared to conventional methods. For instance, Darktrace offers cybersecurity software employing machine learning to scrutinize network traffic data and establish the typical behavioral patterns of all users within a system. This capability enables the system to detect deviations in behavior, potentially indicating cyber threats.

4. Fighting AI Threats

With the progression of technology, many hackers are harnessing machine learning to exploit security vulnerabilities and breach systems. Hence, it is crucial for companies to address such threats by incorporating machine learning into their cybersecurity strategies. This tactic may soon become widespread for defending against increasingly sophisticated cyber-attacks. Consider the notable example of the NotPetya attack, which exploited EternalBlue, a software vulnerability in Microsoft's Windows OS. Such attacks might escalate in their severity in the future, leveraging artificial intelligence and machine learning unless cybersecurity software integrates similar technologies. Crowdstrike, a cybersecurity technology company, provides a prime example of this proactive approach by employing the Falcon Platform, a security software enriched with artificial intelligence, to combat various cyber threats.

5. Email Monitoring

It's crucial to closely monitor official email accounts to combat cybersecurity attacks like phishing. Companies often prioritize educating their employees about the associated risks. Phishing attacks typically involve sending deceptive emails to employees, aiming to extract sensitive information such as job-related data, banking details, credit card information, and company passwords. Employing cybersecurity software integrated with machine learning can aid in thwarting these phishing attempts by monitoring employees' professional emails for signs of potential threats. Additionally, utilizing natural language processing techniques allows for the analysis of emails to detect suspicious patterns and phrases indicative of phishing attempts. For instance, Tessian, a reputable software company, provides email monitoring software specifically designed to identify phishing attempts and potential data breaches. This software employs natural language processing and anomaly detection technologies to detect and address potential threats.

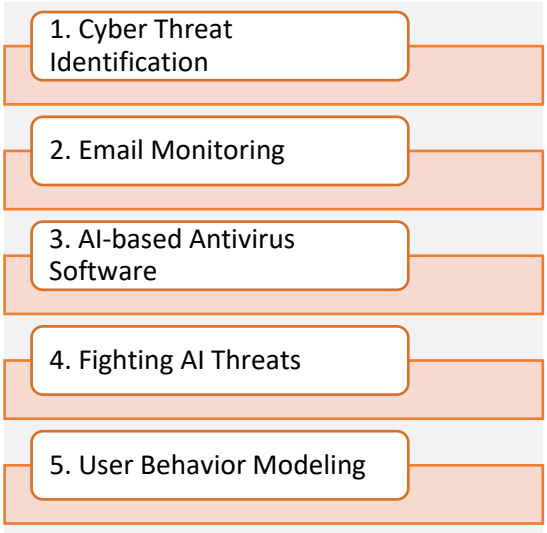

Fig. 1. Applications of ML in Cyber Security

2. Future of Machine Learning and Cybersecurity

Despite machine learning being relatively new in the domain of cybersecurity, the five applications mentioned above demonstrate significant advancements in the field. Emphasizing the importance of minimizing false positives with machine learning algorithms is crucial, as they have the potential to misclassify actions as malicious or indicative of a cyber-attack. Companies ought to collaborate closely with their cybersecurity specialists to bolster the detection and mitigation of diverse cyber threats with heightened accuracy by leveraging machine learning technologies [6].

Algorithms of ML in Security

Machine Learning Algorithms Commonly Used in Security [7]:

- Support Vector Machines (SVMs): The Support Vector Machine (SVM) is a supervised learning algorithm frequently utilized in classification tasks like malware analysis or fraud detection. SVMs operate by segregating internal data points into two categories and then determining the optimal boundary between these categories.

- Decision Trees: Decision trees, which are supervised learning algorithms, are used in tasks such as classifying network intrusions. They function by dividing data into smaller subsets based on specific criteria and then making decisions based on the attributes of each subset.

- Neural Networks: Neural networks, categorized as deep learning algorithms, are extensively used by data scientists. In the realm of security, they are especially crucial for tasks like malware detection and user behavior analysis.

When choosing the right machine learning algorithm for a given security task, there are several factors to consider:

- Data type: Various machine learning algorithms are crafted to Customizing for specific data types is essential in machine learning. The characteristics of the analyzed data significantly influence prediction accuracy and performance. Choosing the suitable machine learning algorithm for a given data type is vital for comprehensive analysis and precise predictions. For instance, Support Vector Machines (SVMs) demonstrate superior performance with text data, while neural networks are better suited for processing image and speech data.

- Data size: Some machine learning algorithms are crafted to handle large datasets efficiently, while others are better suited for smaller ones. Larger datasets often require sophisticated algorithms like neural networks, which can effectively manage the increased volume of data. Conversely, simpler algorithms such as decision trees or logistic regression may be preferable for smaller datasets, where algorithm complexity is less critical compared to the priority of achieving accurate predictions.

- Task Complexity: The complexity of a task is a critical consideration when selecting the appropriate machine learning algorithm for a security task, as certain algorithms surpass others in handling complex tasks. Variables such as the number of features, the degree of data interdependence, and the desired output type impact task complexity. For instance, neural networks excel in addressing intricate tasks like malware detection, whereas decision trees are better suited for simpler tasks such as identifying the type of network intrusion.

- Accuracy requirements: The necessary level of accuracy varies depending on the specific security threat and the impact of false positives or false negatives. Machine learning algorithms exhibit diverse levels of accuracy, with some being better suited for tasks requiring high precision. For example, SVMs are highly esteemed for their accuracy and are frequently used in tasks such as identifying fraudulent transactions. Integrating machine learning into security systems requires meticulous planning, including essential steps such as model selection, training, testing, and deployment of the machine learning models.

- Model Selection: Selecting the appropriate algorithm is the initial step in deploying a machine learning model. This process entails choosing an algorithm that aligns with the type of data, the complexity of the task, and the desired level of accuracy.

- Training: Once the model is selected, it must undergo training using a substantial dataset of labeled data to identify patterns and relationships between inputs and outputs. The accuracy of the model can be significantly affected by both the quality and quantity of the training data.

- Testing: To guarantee the model's correct and consistent operation, it should undergo testing on a distinct dataset after training. This process helps reveal any potential issues or biases in the model. Deployment entails integrating the trained and evaluated model into the security system. This integration involves incorporating it into existing infrastructure, such as a security information and event management (SIEM) system, to deliver real-time warnings and insights.

3. Related work

In the realm of network monitoring, data stream machine learning is rapidly gaining

momentum as large amounts of data generated by end-user terminals and network devices exceed the memory capacity of conventional monitoring apparatus. Fast and continuous techniques for online data stream analysis are needed for primary network monitoring applications encompass identifying anomalies, network intrusions, and attacks. This section will include earlier research conducted between 2018 and 2023:

The researchers explored flow-based machine learning methods for network security and anomaly detection. They developed and evaluated several machine learning algorithms for analyzing dynamic network data flows. The ongoing enhancement of data flow analysis algorithms originated from data flow mining, together with the multitude of evaluation methods employed to evaluate these algorithms, make choosing the appropriate machine learning model difficult. Determining which strategy best represents the algorithm's performance is crucial, since multiple approaches may provide results that differ significantly. Following this, they performed an extensive comparison of results employing advanced evaluation methods for on-chain data. They employed common batch-based machine learning algorithms along with their flow-based extensions to address the particular challenge of online network security and anomaly detection. Their findings demonstrated that through ongoing retraining during drift detection periods, adaptive random forests and random gradient descent models were able to maintain remarkable accuracy, even in the presence of significant conceptual shifts in the underlying network data streams [8].

To begin, we will introduce a taxonomy encompassing machine learning tasks, techniques, and depth, providing an overview of how machine learning is classified in network security applications. Subsequently, we will delve into various adversarial machine learning attacks within the domain of network security and suggest two methodologies for categorizing adversarial assaults. Initially, we will categorize adversarial risks in network security using a taxonomy based on applications. Second, use a dimensional classification approach that splits adversarial attacks into issue space and feature space to categorize them in network security. Next, look at the many ways that network security apps based on machine learning might prevent adversarial assaults. In conclusion, we offer a grid map of adversarial risks and Evaluate multiple adversarial attacks aimed at machine learning within the present landscape of network security, also pinpoint the location of each attack categorization on the hostile risk grid map [9].

They provided a thorough analysis of the security difficulties associated with machine learning, with a focus on existing attacks on these systems, associated defenses or secure learning techniques, and security assessment methodology. Instead of focusing on a particular stage or kind of attack, take into account all aspect of machine learning security, from testing to training. The machine learning model is first demonstrated adversarial, and then possible attack routes are examined. Next, training set poisoning, training group back doors, frequent hostile attacks, model theft, and retrieving private training data are the five categories used to group machine learning security challenges. Next, do a thorough analysis of threat models, attack tactics, and defense systems. To show that these risks are an actual concern in the real world [10].

Operators are looking to machine learning (ML) to automate network management and diagnostics in order to operate complex optical communications networks at a fair cost. To

allow for cognitive and autonomous control of optical network security, more capacity is required. Furdek et al. addressed the difficulties in integrating machine learning-based techniques for optical layer attack localization and detection with conventional network management systems (NMSs), as well as the efficacy of those techniques. Their proposed cognitive security diagnostics framework integrates an attack detection module that utilizes supervised learning (SL), semi-supervised learning (SSL), and unsupervised learning (UL) techniques. Additionally, it features an attack localization module aimed at identifying compromised links or malicious connections. The innovative window-based attack detection (WAD) method effectively addresses concerns regarding false positives and false negatives. Moreover, they have assembled the most extensive experimental dataset for optical layer security to date and provided valuable guidance for implementing the framework into a network management system (NMS). The effectiveness of the framework was also assessed in a tested experimental network that was vulnerable to intrusions [11].

Security is essential for a network to be as truly independent as feasible, that is, to be able to recognize and prevent attacks. Management of optical network security is grounded on three fundamental pillars: attack reaction, attack prevention, and attack detection. Attack prevention encompasses diverse activities like risk modeling, vulnerability assessment, and minimizing attack surfaces through network design and operation, all while considering potential threats. Detailed analyses of physical-layer vulnerabilities in dynamic optical networks and the attack methods that exploit these weaknesses to disrupt service delivery are discussed in references [12],[13]. In optical network design, connection routing was initially used to create physical-layer security [14]. Techniques for attack-aware spectrum allocation and routing have been proposed for three categories of traffic: dynamic, static, and periodic [15],[16],[17]. The main focus of this initiative is attack detection, which involves identifying the source of the attack, accurately attributing observed degradation to a security breach, and continuously monitoring the performance of optical channels. By tracking associated power decreases or surges, specific attack methods such as tapping or high-power jamming can be detected. Reference [18] provides a detailed description of a method for identifying intrusion-triggered power losses in passive optical networks.

The algorithms described in [19],[20] identify anomalies in connections by detecting power spikes and comparing power levels at the input and output of each node. This procedure aids in pinpointing the source of high-power jamming attacks. Optical spectrum analyzers (OSAs) play a crucial role in various Optical Power Monitoring (OPM) techniques, as summarized in [21]. Additionally, [22] elaborates on an OSA-based approach for detecting intrusion signals. Because OSAs are so expensive, they are often only deployed at a small number of network locations. Now that coherent transceivers have advanced due to Digital Signal Processing (DSP), the NMS may acquire an extensive OPM dataset. When paired with data processing tools, this dataset may be utilized for security diagnostics without the need for expensive monitoring equipment. Binary concepts called Attack Syndromes (AttSyns) were created to solve the problem of recognizing assaults that do not always lead to changes in power levels [23]. These terms represent the degree of destructive connections. From the subset of affected connections, it is feasible to determine which damaged connection started the attack if AttSyns are distinct for every attack scenarioIn the absence of AttSyn disambiguation, additional security monitors or monitoring probes are required to provide it. A resource-minimizing

architecture for these monitors was proposed in [24]. Attack mitigation involves both promptly restoring impacted services and modifying the network to decrease vulnerability to future attacks. Reference [25] suggested rapid frequency hopping over the fewest-shared-link multi-paths as a potential defense against jamming and eavesdropping threats.

To coordinate defensive resources against jamming assaults, the approach outlined in [26] entails determining overlaps in the attack ranges of the working and backup channels for each link. In order to defend optical networks with quantum key distribution (QKD) from physical-layer assaults aimed at lowering key-rates, the authors of [27] present experimental support. In the field of network analytics, machine learning-based Attack Detection and Identification (ADI) services have just lately become popular. Artificial Neural Networks (ANN) were employed in [28] to recognize high-power jamming and provide useful attack mitigation techniques. Experimental Optical Power Monitoring (OPM) data from a coherent receiver was analyzed in [29] to identify in-band, out-of-band, and polarization scrambling assaults on an optical connection using a variety of supervised learning methods. In [30], it was initially shown how to include attack detection and localization with optical network management.

In [31], a brand-new ensemble-based machine learning technique for intrusion detection is presented. Several publicly accessible datasets and multi-clustering methods, including Random Forest, Gradient Boosting, Adaboost, Gradient XGBoost, Bagging, and Simple Stacking, were used to evaluate the efficacy of the proposed method. The most crucial aspects for intrusion detection are identified using three methods: mutual information, correlation analysis, and principal components analysis. Through our study with multiple ensemble approaches, we demonstrate that the Random Forest methodology-based proposed strategy outperforms the existing approaches, frequently outperforming them by more than 99% in terms of accuracy and FPR, including precision, recall, F1 score, balanced precision, Cohen's Kappa, etc. The defenses of computer networks and systems against new attacks can be reinforced by utilizing this technique.

4. Conclusion

The world is evolving to the point where systems and networks are present in all sizes of enterprises. Our lives are made simpler by these networks, but the businesses that rely on them for security are constantly seeking methods to make their services better. It appears that machine learning is a difficult, although maybe negotiable, long-term answer to the expanding network security issue. But human-built computers are hardly the most intelligent things ever envisaged at this point in time. Robots won't be able to manage network security in the near future since it will take a lot of work to make them intelligent and competent to control security. Machine learning has made significant progress in identifying many sorts of network assaults, including as DDoS attacks, frauds, irrigation pit attacks, and other attacks. Nevertheless, we are unable to rely only on machine learning for network security at this time due to its low cost. Therefore, further research is needed in the area of machine learning course summarization, which has a lot of potential to enhance network security. Learning technologies are not yet developed enough to fully replace security specialists in the human network, even if they are being used.

5. Future work

Future networks will be increasingly intricate, which will increase their susceptibility to intrusions. As a result, users will find it more difficult to protect their networks against infiltration. However, machines can perform many more tasks and are faster and more precise than people [32]. Therefore, if people have a rudimentary understanding of future engines, they might be able to protect themselves against threats that are difficult for humans to understand but easy for engines to identify. Consider the Internet of Things (IoT) as an example. More people than ever before are using IoT services, and IoT usage patterns are growing. IoT devices are connected via networks, and these systems are completely safe as usual. As a result, networking equipment and Internet of Things services are becoming more sophisticated. But we can protect networks in the future by obtaining cutting-edge IoT service security solutions.

References

1. Expertsystem.com. (2017). What is Machine Learning? A definition - Expert System. [online] Available at: https://www.expertsystem.com/machine-learning-definition/ [Accessed 20 Feb. 2024].
2. Rahul Reddy Nadikattu, "THE EMERGING ROLE OF ARTIFICIAL INTELLIGENCE IN MODERN SOCIETY", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.4, Issue 4, pp.906-911, December 2016, Available at :http://www.ijcrt.org/papers/IJCRT1133435.pdf or http://doi.one/10.1729/Journal.24110.
3. Apiumhub. (2016). Applications of machine learning in cybersecurity. [online] Available at https://apiumhub.com/tech-blog-barcelona/applications-machine-learning-cyber-security/ [Accessed 19 Sep. 2018].
4. Kemmerer, R. A. (2003, May). Cybersecurity. In 25th International Conference on Software Engineering, 2003. Proceedings. (pp. 705-715). IEEE.
5. Ford, V., & Siraj, A. (2014, October). Applications of machine learning in cyber security. In Proceedings of the 27th international conference on computer applications in industry and engineering (Vol. 118). Kota Kinabalu, Malaysia: IEEE Xplore.
6. Apruzzese, G., Laskov, P., Montes de Oca, E., Mallouli, W., Brdalo Rapa, L., Grammatopoulos, A. V., & Di Franco, F. (2023). The role of machine learning in cybersecurity. Digital Threats: Research and Practice, 4(1), 1-38.
7. Chio, C., & Freeman, D. (2018). Machine learning and seurity: Protecting systems with data and algorithms. " O'Reilly Media, Inc.".
8. Mulinka, P., & Casas, P. (2018, August). Stream-based machine learning for network security and anomaly detection. In Proceedings of the 2018 workshop on big data analytics and machine learning for data communication networks (pp. 1-7).
9. Ibitoye, Olakunle, et al. "The Threat of Adversarial Attacks on Machine Learning in Network Security--A Survey." arXiv preprint arXiv:1911.02621 (2019).
10. Xue, M., Yuan, C., Wu, H., Zhang, Y., & Liu, W. (2020). Machine learning security: Threats, countermeasures, and evaluations. IEEE Access, 8, 74720-74742.
11. Furdek, M., Natalino, C., Lipp, F., Hock, D., Di Giglio, A., & Schiano, M. (2020). Machine learning for optical network security monitoring: A practical perspective. Journal of Lightwave Technology, 38(11), 2860-2871.
12. N. Skorin-Kapov, M. Furdek, S. Zsigmond, and L. Wosinska, “Physical-layer security in evolving optical networks,” IEEE Commun. Mag., vol. 54, no. 8, pp. 110–117, Aug 2016,

DOI: 10.1109/MCOM.2016.7537185
13. M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, "Optical layer security in fiber-optic networks," IEEE Inf. Foren. Sec., vol. 6, no. 3, pp. 725– 736, April 2011, DOI: 10.1109/TIFS.2011.2141990.
14. N. Skorin-Kapov, J. Chen, and L. Wosinska, "A new approach to optical networks security: Attack-aware routing and wavelength assignment," IEEE Trans. Netw., vol. 18, no. 3, pp. 750–760, June 2010, DOI: 10.1109/TNET.2009.2031555.
15. N. Skorin-Kapov, M. Furdek, R. Aparicio-Pardo, and P. Pavon-Mari ´ no, ˜ "Wavelength assignment for reducing in-band crosstalk attack propagation in optical networks: ILP formulations and heuristic algorithms," European J. Oper. Res., vol. 222, no. 3, pp. 418–429, Nov 2012, DOI: 10.1016/j.ejor.2012.05.022.
16. K. Manousakis, P. Kollios, and G. Ellinas, "Multi-period attackaware optical network planning under demand uncertainty," in Optical Fiber and Wireless Communications, R. Roka, Ed., June 2017, DOI: 10.5772/intechopen.68491.
17. J. Zhu, B. Zhao, and Z. Zhu, "Leveraging game theory to achieve efficient attack-aware service provisioning in EONs," IEEE/OSA J. Lightwave Techn., vol. 35, no. 10, pp. 1785–1796, May 2017, DOI: 10.1109/JLT.2017.2656892.
18. A. Saltykov, S. Glagolev, J. B. Jensen, and I. T. Monroy, "Security attacks in optical access networks - simultaneous detection and localization," in Proc. of IEEE Photonic Society 24th Annual Meeting, Oct. 2011, pp. 935–936, DOI: 10.1109/PHO.2011.6110867.
19. C. Mas, I. Tomkos, and O. K. Tonguz, "Failure location algorithm for transparent optical networks," IEEE J. Sel. Areas Commun., vol. 23, no. 8, pp. 1508–1519, Aug 2005, DOI: 10.1109/JSAC.2005.852182.
20. Tao Wu and A. K. Somani, "Cross-talk attack monitoring and localization in all-optical networks," IEEE/ACM Trans. Netw., vol. 13, no. 6, pp. 1390–1401, Dec 2005, DOI: 10.1109/TNET.2005.860103.
21. Z. Dong, F. N. Khan, Q. Sui, K. Zhong, C. Lu, and A. P. T. Lau, "Optical performance monitoring: A review of current and future technologies," IEEE/OSA J. Lightwave Technol., vol. 34, no. 2, pp. 525–543, Jan 2016, DOI: 10.1109/JLT.2015.2480798.
22. 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, DOI: 10.1109/LCOMM.2018.2801869.
23. F. Pederzolli, M. Furdek, D. Siracusa, and L. Wosinska, "Towards secure optical networks: A framework to aid localization of harmful connections," in Proc. of OFC, March 2018, p. Th2A.42.
24. M. Furdek, V. W. S. Chan, C. Natalino, and L. Wosinska, "Networkwide localization of optical-layer attacks," in Proc. of ONDM, Athens, Greece, May 2019, pp. 310–322, DOI: 10.1007/978-3-030-38085-4 27.
25. Y. Li, N. Hua, Y. Song, S. Li, and X. Zheng, "Fast lightpath hopping enabled by time synchronization for optical network security," IEEE Commun. Lett., vol. 20, no. 1, pp. 101–104, Jan 2016, DOI: 10.1109/LCOMM.2015.2497703.
26. M. Furdek, N. Skorin-Kapov, and L. Wosinska, "Attack-aware dedicated path protection in optical networks," IEEE/OSA J. Lightwave Techn., vol. 34, no. 4, pp. 1050–1061, Feb 2016, DOI: 10.1109/JLT.2015.2509161.
27. E. Hugues-Salas, F. Ntavou, D. Gkounis, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Monitoring and physical-layer attack mitigation in SDN-controlled quantum key distribution networks," IEEE/OSA J. Opt. Commun. Netw., vol. 11, no. 2, pp. A209–A218, Feb 2019, DOI: 10.1364/JOCN.11.00A209.
28. M. Bensalem, S. Kumar Singh, and A. Jukan, "On detecting and preventing jamming attacks with machine learning in optical networks," arXiv:1902.07537 [cs.NI], Jun 2019.

29. C. Natalino, M. Schiano, A. Di Giglio, L. Wosinska, and 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, DOI: 10.1109/JLT.2019.2923558.
30. M. Furdek, C. Natalino, F. Lipp, D. Hock, N. Aerts, M. Schiano, A. Di Giglio, and L. Wosinska, "Demonstration of machine-learning-assisted security monitoring in optical networks," in Proc. of ECOC, Sept 2019.
31. Hossain, M. A., & Islam, M. S. (2023). Ensuring network security with a robust intrusion detection system using ensemble-based machine learning. Array, 19, 100306.
32. Apiumhub. (2017). Applications of machine learning in cybersecurity. [online] Available at: https://apiumhub.com/tech-blog-barcelona/applications-machine-learning-cyber-security/ [Accessed 19 Sep. 2018].