Distributed Denial of Service Attacks

Subjects: Others

Contributor: Olusola Adeniyi, Ali Safaa Sadiq, Prashant Pillai, Mohammad Aljaidi, Omprakash Kaiwartya

Mobile Edge Computing (MEC) has revolutionized the landscape of the telecommunication industry by offering low-latency, high-bandwidth, and real-time processing. With this advancement comes a broad range of security challenges, the most prominent of which is Distributed Denial of Service (DDoS) attacks, which threaten the availability and performance of MEC's services. In most cases, Intrusion Detection Systems (IDSs), a security tool that monitors networks and systems for suspicious activity and notify administrators in real time of potential cyber threats, have relied on shallow Machine Learning (ML) models that are limited in their abilities to identify and mitigate DDoS attacks.

Keywords: mobile edge computing ; DDoS ; machine learning ; detection ; classification

1. Introduction

The advent of Mobile Edge Computing (MEC) has signaled a paradigm shift in the design and management of wireless communication systems, especially in the current environment of pervasive network connectivity and expanding data-driven applications. This innovative idea involves assigning computational work and data processing to edge nodes located near end users, reducing latency and increasing system effectiveness. As MEC gains popularity for its potential to revolutionize network architecture, it simultaneously presents a variety of complex cyber-security concerns that demand in-depth scholarly research.

The MEC framework faces a wide range of cyber-security challenges. One prominent concern is the intensification of DDoS attacks. A DDoS attack, characterized by the orchestrated flooding of network resources, poses a significant threat to the reliability and availability of edge-hosted services [1]. The dynamic and distributed nature of MEC environments, encompassing various devices connected through heterogeneous networks, is well suited for DDoS attacks. Therefore, the threat of DDoS attacks on MEC networks highlights the need for effective and flexible cyber-security measures. These measures should include proactive detection, quick response, and mitigation of malicious activities. Additionally, MEC networks should be monitored continuously to identify any suspicious activities and take necessary actions to prevent them.

In the field of cyber security, Intrusion Detection Systems (IDSs) are used to carefully monitor network processes, in order to identify and prevent future security breaches [2]. These solutions carefully examine data flow and engage in a discriminating analysis of patterns that differ from the norm, actions that raise suspicion, or attack signs that may be easily identified. IDS solutions play a crucial and useful role in bolstering a network's defensive perimeter and minimizing the negative effects of cyber attacks. However, the use of shallow machine learning is a notable drawback when it comes to IDSs.

While these techniques have been widely employed for anomaly detection and pattern recognition, they often exhibit limitations in handling the complex and evolving nature of modern cyber threats. Shallow machine learning models, such as SVM, decision trees, and K-nearest neighbours are characterized by their relative simplicity and shallow hierarchical structures. These algorithms may struggle to discern intricate patterns and subtle deviations that are indicative of sophisticated attacks [3].

Deep learning, a subfield of machine learning, has emerged as a potent and promising avenue for enhancing IDS [4]. Unlike traditional shallow machine learning techniques, deep learning leverages multi-layered neural networks to automatically extract intricate features and patterns from complex data, enabling it to more accurately capture the subtle and dynamic nature of contemporary cyber threats.

In the age of information proliferation, where data are generated at an unprecedented pace across diverse domains, the emergence of high-dimensional datasets is creating new challenges for data analysis [5]. Analyzing data in high-dimensional spaces requires new techniques and tools to uncover patterns and extract meaningful insights. As the

dimensionality of data increases, the efficiency, interpretability, and generalization capacity of machine learning models, particularly deep learning architectures, can be profoundly impacted. As a result of this intricate interplay among the high-dimensional data environment, the need for optimal accuracy and efficient model performance calls for innovative approaches to feature reduction [6].

AE is an example of a feature reduction method with the overarching purpose of identifying the salient features in data that contain the core information necessary for model learning [7]. This transformative process seeks to strike a delicate balance between retaining meaningful attributes and discarding redundant or noise-laden variables. By condensing the data while preserving its intrinsic structure, these techniques not only facilitate computational efficiency but also hold the potential to significantly bolster the accuracy and generalization prowess of deep learning models.

2. Detection and Classification of DDoS Attacks

Detection and classification of DDoS attacks are crucial to preventing malicious activities on a network. It is necessary to have a system in place that can detect and classify these attacks in real time. In addition, this system should be able to identify the different types of DDoS attacks and respond accordingly.

A series of approaches have been utilized by researchers to address the detection and classification of DDoS attacks. For instance, Wani et al.'s [8] study focused on the analysis and detection of DDoS attacks using ML. The study utilized some ML algorithms, including Naïve Bayes, random forest, and support vector machine. Overall, SVM performed better than others with an accuracy of 99.7%. The research identified SVM as an effective algorithm for detecting DDoS attacks with high accuracy. Bindra and Sood [9] also examined five ML models to determine which one would produce the best DDoS detection results. The research revealed that random forest achieved the highest accuracy of 96%.

Khare et al. [10] presented DT as a model for DDoS attack detection. The process involves extracting features, and the information obtained is calculated. Using the information obtained, a decision tree is constructed that identifies DDoS attacks and categorizes them. The researcher claimed the model achieved a 90.2% success rate. Kousar et al. [11] also show that the decision tree outperforms SVM and Naive Bayes.

Arshi et al. [12] presented a survey of machine learning techniques to detect DDoS attacks. The research discussed techniques, such as SVM, Naive Bayes, and DT. The researcher also provided more information on different types of DDoS attacks. The researcher concluded that the use of machine learning techniques is essential for understanding DDoS attacks and taking the necessary precautions to minimize them.

It is worth noting that all these methods are based on shallow machine learning, which has been widely studied and deployed for years, and has shown success in many ways. However, in recent times, the use of deep learning has been on the increase. This is partly due to the fact that shallow ML methods—though they may have high accuracy—perform poorly when used with large datasets [13]. Generally, in ML, dataset features play an important role in the outcome of the model. Getting the appropriate features that well represent the dataset is of uttermost importance. Dimensionality reduction is an important step in data pre-processing [14]. It helps to reduce noise, eliminate irrelevant features, and reduce the computational complexity of algorithms. It also helps to increase the accuracy of the model by removing redundant features. Researchers in recent times have utilized various methods to reduce high data dimensions and achieve the necessary accuracy.

For instance, Elsayed et al. [15] proposed Ddosnet to address DDoS attacks in SDN environments. The researchers utilized a combination of RNN and autoencoder to build a model and evaluated the model's performance with the CIDDoD2019 dataset. According to the researcher, the results showed that the method offered a substantial improvement over alternative methods in detecting attacks.

Yuan et al. [16] proposed an approach called deep defense. The approach focuses on the optimal feature representation of the dataset. Recurrent deep neural networks were used to identify patterns from batches of network traffic and track network attack activity. The researcher claimed the model achieved a better performance when compared with other ML models. However, the dataset used is old and may not contain the latest form of attacks.

Mushtaq et al. [17] explored the feasibility of designing an effective intrusion detection system for the protection of networks from cyber attacks. The researchers propose a hybrid framework that combines deep autoencoder (AE) with long short-term memory (LSTM) and bidirectional long short-term memory (Bi-LSTM) for intrusion detection. The researcher validated the performance of the proposed model on the well-known NSL-KDD dataset. The results indicate

that the proposed AE-LSTM framework outperforms other deep and shallow machine learning techniques, as well as recently reported methods.

Lee and Park [18] addressed the development of a high-performance network intrusion detection system (NIDS) using deep learning, specifically focusing on situations where there are significant imbalances between normal and abnormal network traffic data. The researchers proposed an AE-CGAN (Autoencoder-Conditional GAN) model that combines autoencoders and generative adversarial networks to improve intrusion detection in data-imbalanced situations [19]. The model's performance was evaluated on the CICIDS2017 dataset. According to the researcher, the proposed model effectively reduces false detections and improves the detection of rare classes, leading to better intrusion detection performance.

To improve the accuracy and efficiency of Network Intrusion Detection Systems (NIDSs) using deep learning techniques, Kunang et al. [20] combined a DNN with a Pretraining Technique with Deep Autoencoder (PTDAE) to create a deep learning Intrusion Detection System (IDS [21]. An automated optimal hyperparameter procedure was developed through grid search and random search techniques. The pretraining phase involves applying three feature extraction methods: Deep Autoencoder (DAE), Autoencoder, and Stack Autoencoder (SAE). According to the researcher, the results show that the DAE method provides the best performance, outperforming previous approaches in terms of performance metrics in multiclass classification.

Ultimately, to effectively address DDoS attacks in a high-dimensional data environment, there is a need for feature reduction to enhance the quality and efficiency of deep learning outcomes as demonstrated by the state-of-the-art research carried out.

References

1. Xiao, L.; Wan, X.; Dai, C.; Du, X.; Chen, X.; Guizani, M. Security in mobile edge caching with reinforcement learning. IEEE Wirel. Commun. 2018, 25, 116–122.
2. Kaja, N.; Shaout, A.; Ma, D. An intelligent intrusion detection system. Appl. Intell. 2019, 49, 3235–3247.
3. Zainudin, A.; Ahakonye, L.A.C.; Akter, R.; Kim, D.S.; Lee, J.M. An efficient hybrid-dnn for ddos detection and classification in software-defined iiot networks. IEEE Internet Things J. 2022, 10, 8491–8504.
4. Ahmad, Z.; Shahid Khan, A.; Wai Shiang, C.; Abdullah, J.; Ahmad, F. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Trans. Emerg. Telecommun. Technol. 2021, 32, e4150.
5. Oo, M.C.M.; Thein, T. An efficient predictive analytics system for high dimensional big data. J. King Saud-Univ.-Comput. Inf. Sci. 2022, 34, 1521–1532.
6. Jia, W.; Sun, M.; Lian, J.; Hou, S. Feature dimensionality reduction: A review. Complex Intell. Syst. 2022, 8, 2663–2693.
7. Naina Chaturvedi. Dimensionality Reduction Using an Autoencoder in Python. 2021. Available online: https://medium.datadriveninvestor.com/dimensionality-reduction-using-an-autoencoder-in-python-bf540bb3f085 (accessed on 5 August 2023).
8. Wani, A.R.; Rana, Q.P.; Saxena, U.; Pandey, N. Analysis and detection of DDoS attacks on cloud computing environment using machine learning techniques. In Proceedings of the 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates, 4–6 February 2019; pp. 870–875.
9. Bindra, N.; Sood, M. Detecting DDoS attacks using machine learning techniques and contemporary intrusion detection dataset. Autom. Control Comput. Sci. 2019, 53, 419–428.
10. Khare, M.; Oak, R. Real-Time distributed denial-of-service (DDoS) attack detection using decision trees for server performance maintenance. In Performance Management of Integrated Systems and Its Applications in Software Engineering; Springer: Singapore, 2020; pp. 1–9.
11. Kousar, H.; Mulla, M.M.; Shettar, P.; Narayan, D.G. Detection of DDoS attacks in software defined network using decision tree. In Proceedings of the 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT), Bhopal, India, 18–19 June 2021; pp. 783–788.
12. Arshi, M.; Nasreen, M.D.; Madhavi, K. A survey of DDoS attacks using machine learning techniques. E3S Web Conf. 2020, 184, 01052.
13. Suthishni, D.N.P.; Kumar, K.S. A review on machine learning based security approaches in intrusion detection system. In Proceedings of the 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 23–25 March 2022; pp. 341–348.

14. Kasun, L.L.C.; Yang, Y.; Huang, G.B.; Zhang, Z. Dimension reduction with extreme learning machine. IEEE Trans. Image Process. 2016, 25, 3906–3918.
15. Elsayed, M.S.; Le-Khac, N.A.; Dev, S.; Jurcut, A.D. Ddosnet: A deep-learning model for detecting network attacks. In Proceedings of the 2020 IEEE 21st International Symposium on “A World of Wireless, Mobile and Multimedia Networks” (WoWMoM), Cork, Ireland, 31 August–3 September 2020; pp. 391–396.
16. Yuan, X.; Li, C.; Li, X. DeepDefense: Identifying DDoS attack via deep learning. In Proceedings of the 2017 IEEE International Conference on Smart Computing (SMARTCOMP), Hong Kong, China, 29–31 May 2017; pp. 1–8.
17. Mushtaq, E.; Zameer, A.; Umer, M.; Abbasi, A.A. A two-stage intrusion detection system with auto-encoder and LSTMs. Appl. Soft Comput. 2022, 121, 108768.
18. Lee, J.; Park, K. AE-CGAN model based high performance network intrusion detection system. Appl. Sci. 2019, 9, 4221.
19. Hara, K.; Shiomoto, K. Intrusion detection system using semi-supervised learning with adversarial auto-encoder. In Proceedings of the NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary, 20–24 April 2020; pp. 1–8.
20. Kunang, Y.N.; Nurmaini, S.; Stiawan, D.; Suprapto, B.Y. Attack classification of an intrusion detection system using deep learning and hyperparameter optimization. J. Inf. Secur. Appl. 2021, 58, 102804.
21. Li, X.; Chen, W.; Zhang, Q.; Wu, L. Building auto-encoder intrusion detection system based on random forest feature selection. Comput. Secur. 2020, 95, 101851.

Retrieved from https://encyclopedia.pub/entry/history/show/123712