IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125262

ANOMALY DETECTION USING MACHINE LEARNING ON SOFTWARE DEFINED NETWORKING

Chetan Patil[1], Shubham Chakote[2], Rakshit Teli[3]

Department of Computer Engineering, Savitribai Phule Pune University, Pune, India[1-3]

Abstract: Software-defined networking (SDN) has experienced significant growth and can be leveraged across various network scenarios, ranging from data centres to wide-area 5G networks. It transfers control logic from individual devices to a centralized programmable controller, enabling efficient monitoring and management of network traffic. While a software-based controller enforces rules and policies on forwarded requests, it lacks the ability to identify abnormal patterns in network traffic. Consequently, the controller may inadvertently install flow rules that counteract these anomalies, resulting in reduced overall network performance. These anomalies could indicate potential threats to the network, thereby compromising its security and performance. To address this, machine learning (ML) approaches can be employed to detect such traffic flow patterns and anticipate impending threats to the system. In this study, we propose an ML-based system for detecting traffic anomalies in software-defined networks, specifically utilizing the Support Vector Machine (SVM) algorithm for anomaly detection.

Keywords: Software-defined networking, Abnormal patterns in network traffic, Machine learning, Support Vector Machine algorithm.

I. INTRODUCTION

Software-defined networking (SDN) has witnessed significant growth and proven to be advantageous in diverse network environments, including data centres and wide-area 5G networks. By centralizing control logic in a programmable controller, SDN facilitates efficient traffic monitoring and management, ensuring optimal performance and effective flow control.

However, a notable drawback of software-based controllers is their inability to detect abnormal traffic patterns. While these controllers diligently enforce rules and policies on forwarded requests, they lack the capability to identify deviations or irregularities in traffic flow. Consequently, the controller may unintentionally install flow rules that clash with these anomalies, resulting in a decline in overall network performance.

Such anomalies in network traffic may indicate potential threats or security vulnerabilities, thereby compromising both network performance and overall security. To address this challenge, machine learning (ML) techniques can be utilized to detect and recognize traffic flow patterns that may signify impending system threats.

In this study, we propose an ML-based system explicitly designed for identifying traffic anomalies in software-defined networks. Our system leverages the Support Vector Machine (SVM) algorithm, known for its efficacy in detecting anomalies. By analysing historical network traffic data and learning from it, the ML system can identify patterns that deviate from the norm, flagging them as potential anomalies.

The incorporation of ML algorithms, such as SVM, empowers the system to proactively identify and predict imminent threats to the network. By promptly detecting and addressing anomalies, network performance can be enhanced, and potential security risks can be mitigated.

Overall, our proposed ML-based system presents a robust solution for detecting traffic anomalies in software-defined networks. By harnessing the power of machine learning, we strive to enhance network performance, reinforce security measures, and ensure seamless operation of SDN environments across various network scenarios.

II. PROPOSED WORK

The growth and versatility of software-defined networking (SDN) have opened up numerous opportunities for network

DOI: 10.17148/IJARCCE.2023.125262

deployment, ranging from data centres to wide-area 5G networks. By centralizing control logic in a programmable controller, SDN facilitates efficient traffic monitoring and management. However, the inherent limitation of software-based controllers in detecting abnormal network traffic patterns hinders overall network performance. The inability to identify anomalies leaves the controller susceptible to installing flow rules that conflict with these patterns, leading to suboptimal network performance. These anomalies could potentially signify threats that compromise the network's security and performance. To mitigate this, the integration of machine learning (ML) techniques presents a promising approach. By employing ML approaches, such as the Support Vector Machine (SVM) algorithm, traffic flow patterns indicative of impending threats can be detected and anticipated. The ML-based system proposed in this study utilizes SVM for effective anomaly detection in software-defined networks.

III. LITERATURE SURVEY

1. “Deep learning-based network security data sampling and anomaly predication in future network” This paper the author Lan Liu, Jun Lin, Pengcheng Wang, Langzhou Liu and Rongfu Zhou proposes there is significant emphasis on researching and deploying new technologies and networks. Scientists are actively exploring the use of IPv6, software-defined networking (SDN), and 5G to build future networks that meet the requirements of reliability, low latency, and wide coverage. It is crucial to consider the new security aspects of future networks. The introduction of 5G has brought about massive communication capabilities and billions of device connections, necessitating flexible network architecture and high-performance networks. SDN is emerging as a promising networking platform, offering logical centralization of networks but also introducing new opportunities and challenges in network security. Detecting and predicting network data anomalies caused by malicious attacks are important problems to be addressed in future networks. Research on network data sampling strategies and appropriate anomaly detection models in the field of network security is crucial for preventing future network threats. In this paper, we propose and simulate a network data sampling strategy for SDN using a zero-sum game approach. This strategy helps identify important nodes that need protection. Additionally, we intend to employ deep learning methods to establish and analyse network anomaly flow in future networks.

2. “Software Defined Networking Architecture, Security and Energy Efficiency” This paper the author Danda B. Rawat, Swetha R. Reddy proposes Software-defined networking (SDN) is a modern approach that revolutionizes traditional networks by providing programmability through centralized network control. SDN enables dynamic adjustment of network parameters based on the operating environment, offering flexibility and ease of network management. The centralized architecture of SDN ensures efficient resource utilization and high performance by providing network visibility. It addresses security concerns, improves energy efficiency, and enables network virtualization to enhance overall network performance. This paper explores the security threats resolved by SDN, as well as new threats that arise due to its implementation. It also presents a comprehensive overview of security attacks, countermeasures, energy efficiency strategies, and network security in SDN, providing insights into ongoing research efforts, challenges, and future trends. The aim is to provide readers with a comprehensive understanding of SDN architecture, security aspects, and energy efficiency considerations.

3. “Some Special Issues of Network Security Monitoring on Big Data Environments” This paper the author Liu Lan, Lin Jun proposed The vast amount of data in Big Data holds valuable insights about our society and has a significant impact on various aspects of human life. Given the abundance of data from diverse network environments, it becomes essential to address specific challenges related to network security monitoring in Big Data environments. This paper introduces the concept of data cleaning for different data sources and explores the analysis of network security in Big Data through associations between security events and multiple rules. The study offers valuable insights and ideas for effectively monitoring network security in Big Data environments.

4. “An Efficient Sampling and Classification Approach for Flow Detection in Software-defined networking -Based Big Data Centres” This paper the author Feilong Tang, Lu Li, Leonard Barolli, Can Tang proposed SDN enables flexible management of datacenter networks through flow-level control. However, this fine-grained management leads to increased bandwidth usage between the data and control planes, limiting the scalability of SDN-based datacenters. The "elephant and mouse phenomenon" highlights that a small number of elephant flows carry the majority of data in datacenters. To enhance management efficiency, it is beneficial to detect and reroute these elephant flows while handling mice flows in the data plane using wildcard flow tables in OpenFlow. Existing mechanisms for elephant flow detection suffer from high bandwidth consumption and long detection times. In this paper, we propose an efficient approach called ESCA (Efficient Sampling and Classification Approach) for elephant flow detection. ESCA utilizes a two-phase process: in the first phase, it enhances sampling efficiency by estimating the arrival interval of elephant flows and filtering out redundant samples using a filtering flow table. In the second phase, ESCA classifies the samples using a new supervised classification algorithm based on correlation among data flows.

 This work is licensed under a Creative Commons Attribution 4.0 International License

DOI: 10.17148/IJARCCE.2023.125262

5. "Scalable network virtualization in software-defined networks" This paper the author Muhammad Salman Malik, Mirko Montanari, Jun Ho Huh, Rakesh B. Bobba, Roy H. Campbell Proposed In current Infrastructure-as-a-Service (IaaS) cloud environments, users have limited control and only access a logical view of the underlying network. There is a growing interest in delegating more network control to end users, but such delegation raises security concerns for the cloud provider. Software Defined Networking (SDN) technologies offer potential solutions by enabling network control delegation and providing network abstractions to end users. However, any delegation mechanism must strike a balance between the level of control granted to end users and the security constraints of the provider. This paper introduces an SDN-based framework designed to facilitate the delegation of certain network controls to end users, allowing them to monitor and configure their own network slices. We show the tradeoffs between security considerations and the degree of network abstractions offered to end users through two implementations of this framework.

IV. LITERATURE SURVEY CONCLUSION

Sr. No.	Paper title Publication Detail	Date of Publication	Conclusion
1	Deep learning-based network security data sampling and anomaly predication in future network	17 May 2020	A game theory and deep learning model detects anomaly traffic, enhances network defense, and protects crucial nodes. Tested with public datasets, the model's sampling strategy using a zero-sum game and deep learning analysis proves effective. Future research can explore game models, different deep learning methods, and parameter selection.
2	Software Defined Networking Architecture, Security and Energy Efficiency	19 October 2016	SDN architecture, security threats, and energy efficiency. Security attacks and countermeasures in SDN were summarized in a table. Energy efficiency strategies in SDN were surveyed and presented in a table. Challenges and research efforts in SDN were discussed. Optimal SDN parameters depend on the application. Future work should focus on designing low-power security mechanisms for improved network performance.
3	Some Special Issues of Network Security Monitoring on Big Data Environments	26 June 2014	This paper explores network security monitoring on Big Data environments, focusing on correlation algorithms and knowledge representation. It discusses data organization through cleaning, integration, and reduction, and analyses correlation algorithms such as fuzzy constraint, wavelet-based traffic rules, and sequence pattern-based rules
4	An Efficient Sampling and Classification Approach for Flow Detection in SDN-Based Big Data Centres	08 May 2017	In this paper, we propose ESCA, a new elephant flow detection scheme. ESCA utilizes effective sampling periods and a supervised classification method. It includes an algorithm to identify dense arrival time blocks and sampling based on a log-normal distribution. Additionally, a new classification algorithm based on flow correlation and probability is introduced. ESCA reduces sampling overheads and improves detection accuracy and speed. Experimental results demonstrate its superiority over other methods in terms of detection cost and performance.
5	Towards SDN enabled network control delegation in clouds	08 August 2013	In this paper, we investigated user control in cloud networks through OpenFlow and software-defined networks. We proposed an SDN-based framework for delegating network control to users and discussed

DOI: 10.17148/IJARCCE.2023.125262

			network view properties. Two architectures for exposing the network to users were explored, along with a prototype implementation. For future work, we aim to further explore network control delegation, analyse network view properties and security implications, and optimize bandwidth sharing in multi-tenant clouds.

V. CONCLUSION

In software-defined networking (SDN), detecting and addressing anomalies in network traffic is crucial for network efficiency and security. Anomalies are abnormal patterns in traffic that deviate from expected norms. Machine learning techniques can enhance the automatic identification of these anomalies in real-time by training algorithms on historical data and analyzing incoming traffic. This proactive approach optimizes network performance, mitigates security threats, and enables timely response and mitigation. Further research can explore advanced machine learning techniques and incorporate domain-specific knowledge to improve anomaly detection algorithms. Automatic anomaly detection through machine learning holds promise for enhancing network performance and security in SDN environments.

REFERENCES

[1]. D. B. Rawat and S. R. Reddy, "Software Defined Networking Architecture, Security and Energy Efficiency: A Survey," in IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 325-346, Firstquarter 2017, doi: 10.1109/COMST.2016.2618874.

[2]. D. B. Rawat and S. R. Reddy, "Software Defined Networking Architecture, Security and Energy Efficiency: A Survey," in IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 325-346, Firstquarter 2017, doi: 10.1109/COMST.2016.2618874.

[3]. F. Tang, L. Li, L. Barolli and C. Tang, "An Efficient Sampling and Classification Approach for Flow Detection in SDN-Based Big Data Centers," 2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA), Taipei, Taiwan, 2017, pp. 1106-1115, doi: 10.1109/AINA.2017.125.

[4]. L. Lan and L. Jun, "Some Special Issues of Network Security Monitoring on Big Data Environments," 2013 IEEE 11th International Conference on Dependable, Autonomic and Secure Computing, Chengdu, China, 2013, pp. 10-15, doi: 10.1109/DASC.2013.30.

[5]. A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," in IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153-1176, Secondquarter 2016, doi: 10.1109/COMST.2015.2494502.