Brief Report

Review of Advancing Anomaly Detection in SDN through Deep Learning Algorithms

Shirmohammad Tavangari * and Somayeh Taghavi Kulfati

Posted Date: 15 August 2023

doi: 10.20944/preprints202308.1089.v1

Keywords: SDN, Machine Learning, Algorithms, GRU-LSTM

Brief Report

Review of Advancing Anomaly Detection in SDN through Deep Learning Algorithms

Shirmohammad Tavangari [1,*] and Somayeh Taghavi Kulfati [2]

[1] University of British Columbia, ElectricalandComputerEngineering Faculty, 2332 Main Mall, Vancouver, BC Canada V6T 1Z4

[2] Mehrastan Education Institute, Faculty of Technical Engineering, Computer Science Department, P9CQ, Mehrastan, Iran, fanavari_17shahrivar@gums.ac.ir

* Correspondence: s.tavangari@alumni.ubc.ca

Abstract: Recent SDN advances address traditional network management challenges through centralized control and plane separation. SDN prevents breaches using a centralized controller but introduces risks. The controller can be a single point of failure. Thus, an OpenFlow Controller's flow-based anomaly detection enhances SDN security. Our research explored two OpenFlow intrusion detection methods. The first employed machine learning, NSL-KDD dataset, and feature selection, yielding 82% accuracy with random forest. The second combined deep neural networks with GRU-LSTM, achieving 88% accuracy using ANOVA F-Test and feature elimination. Experiments highlighted deep learning as superior for OpenFlow intrusion detection.

Keywords: SDN; machine learning; algorithms; GRU-LSTM

Introduction

IP's role is delivering packets based on their addresses, encapsulating data and labeling datagrams. [1] To enhance network flexibility, the software-defined networking (SDN) paradigm separates control and data planes, allowing programmable devices and centralizing control in SDN controllers. [2] SDN introduces layers of abstraction, fostering flexibility. In dynamic environments, effective traffic monitoring is crucial, aiding management applications. SDN employs data plane forwarding elements (switches, routers) and the controller in the control plane. [3,4] This decoupling and programmability grant network managers significant control, simplifying administration. By separating routing and forwarding activities, the control plane handles topology info and routing, while the data plane manages traffic per control unit settings. [5] This architectural shift enhances network management.

The SDN paradigm emerged as a response to research advocating for programmable networks to facilitate practical protocol experimentation within production networks. Since its inception, it has garnered substantial interest from both academia and industry. Industry leaders such as Google, Cisco, HP, Juniper, and NEC, along with standardization bodies like the Open Network Foundation (ONF) and the Internet Engineering Task Force (IETF), have thrown their support behind it, underscoring its considerable potential for success. [6] A pivotal development was the introduction of the OpenFlow protocol in 2008, acting as a significant catalyst for the paradigm's advancement. [7]

Materials

For the methodology, a deep learning approach incorporating RNN, LSTM, GRU, and Multi-Layer GRU RNN was employed. To enhance feature selection, a univariate analysis of variance (ANOVA) F-test was utilized. ANOVA scrutinizes if group means differ through the F-test, assessing the equality of means. Individual features were assessed to quantify their relationship with labels,

yielding a feature-strength measure. Feature selection was then performed using the Select Percentile method based on high-score percentiles.[8,9]

Further refinement involved recursive feature elimination (RFE). RFE constructs models while excluding features iteratively, eliminating them until all are assessed. Classifier weights aid in generating feature rankings. [10] By combining ANOVA F-test and RFE, a subset of selected features was determined. [11,12]

Notably, the NSL-KDD dataset's attack groups were categorized into four types[13] : DoS, Probe, R2L, and U2R. This comprehensive approach, integrating deep learning and advanced feature selection techniques, aimed to optimize intrusion detection by effectively identifying relevant features and classifying distinct attack types within the dataset.[14,15]

EXPRIMENTS

Google TensorFlow served as the platform for conducting the experiments, offering an interface for network visualization. These experiments were conducted on an Ubuntu 16.10 Dis tribution Operating System, utilizing an environment featuring an Intel i5 3.2 GHz processor, 16 GB RAM, and an NVIDIA GTX 1070 graphics card. The tf.train.AdamOptimizer function from TensorFlow was employed, with hyper parameters outlined.

Controlling the learning rate, the Adam algorithm by Kingma and Ba was utilized through the tf.train.AdamOptimizer. The conducted tests were based on selected features from the complete NSL-KDD dataset. To contextualize the results, other approaches from different researchers were presented, showcasing the deep learning algorithm's accuracy in comparison.

However, it's essential to note that no pre-processing of the database was executed, and the feature selection for testing and training was made without alterations. This methodology aimed to provide a comprehensive assessment of the deep learning algorithm's performance, leveraging TensorFlow's capabilities while presenting a comprehensive evaluation against other approaches.

Conclusion

This paper presents two distinct methodologies for predicting flow-based anomalies in software-defined networking. The first method involves the application of the GRU-LSTM model, utilizing deep learning principles, while the second method employs the random forest (RF) model based on machine learning techniques. Both were developed to identify network interferences within the SDN framework. Furthermore, by incorporating ANOVA F-Test, RFE feature selection, and the gain ratio feature selection method, the study crafted an optimal classifier model, excelling across various evaluation metrics.

Although both approaches yield noteworthy experimental results in comparison to prior research, they signify valuable contributions to the realm of intrusion detection within SDN. Notably, the deep learning approach outperformed the machine learning approach marginally, underscoring the GRU-LSTM model's indispensability for achieving heightened accuracy and expediting intrusion detection within SDN. The results make a strong case for adopting the GRU-LSTM model.

Looking forward, the proposed model is slated for real-world implementation within an actual SDN environment, incorporating genuine network traffic. This practical deployment aims to validate the model's effectiveness under authentic conditions, enhancing the understanding of its potential impact on bolstering SDN's intrusion detection capabilities.

References

1. M.R.Hadi, A.S.Mohammad. A Novel Approach to Network Intrusion Detection System Using Deep Learning For Sdn: Futuristic Approch. Arxive. 2022 Aug. https://doi.org/10.48550/arXiv.2208.02094.
2. R.Chaganti, W.Suliman, V.Ravi, A.Dua. Deep Learning Approach For SDN- Enabled Intrusion Detection System In IoT Networks. MDPI. 2023 Jan. https://doi.org/10.3390/info14010041
3. V.Ravi, R.Chagnati, M.Alazab. Deep Learning feature Fusion Approach for an Intrusion Detection System In SDN-Based IoT Network. 2022 Jun. https://doi.org/10.1109/IOTM.003.2200001

4. W.C.Chanhemo, M.H.Mohsini, M.M.Mjahidi, F.U.rashidi. Deep Learning For SDN-Enabled Campus Network:Proposed Solution , Challenges and Future Direction. International Journal of Intelligent Computing and Cybernetics. 2023 March. https://doi.org/10.1108/IJICC-12-2022-0312
5. C.Fathy, S.N. Saleh. Integrating Deep Learning- Based IoT And Fog Computing With Software Defined Network for Detecting Weapons In Video Surveillance Systems. MDPI. 2022 July. https://doi.org/10.3390/s22145075
6. T.E.Ali, Y.Chong, S.Manickam. Machine Learning Techniques to Detect a DDoS Attack In SDN: A Systematic Review. MDPI. 2023 March. https://doi.org/10.3390/app13053183
7. Y.Liu, T.Zhi, M.Shen, L.Wang, Y.Li, M.Wang. Software-Defined DDoS Detection With Information Entropy Analysis And Optimized Deep Learning. Future Generation Computer System Journal(Elsevier). 2022 April. https://doi.org/10.1016/j.future.2021.11.009
8. S.Tavangari. A Novel Approach To Accessing The Scheduled Network. TechRxiv. 2022Nov. https://doi.org/10.36227/techrxiv.21579456.v1
9. O.E.Tayfour,A.Mubarakali, A.E.Tayfour, M.N.Marsono, E.Hassan, A.M. Abdelrahman. Soft Computing Journal (Springer). 2023 May. https://doi.org/10.1007/s00500-023-08348-w
10. R.Etengu, SC.Tan, TC. Chuah, JG.Jimenez. Deep Learning-Assisted Traffic Predation In Hybrid SDN/OSPF Backbone Networks. IEEE. 2022 June. https://doi.org/10.1109/NOMS54207.2022.9789868
11. C.Zhao, M.Ye, X.Xue, J.Lv, Q.Jiang, Y.Wang. DRL-M4MR: An Intelligent Multicast Routing Approach Based on QDN Deep Reinforcement Learning In SDN. Physical Communication Journal (Elsevier). 2022 Dec. https://doi.org/10.1016/j.phycom.2022.101919
12. M.A.Kumar, A.H.Pai, J.Agarwal, S.Christa, G.M.S. Prasad, S.Saifi. Deep Learning Model To Defend Against Cover Channel Attacks In The SDN Networks. IEEE. 2023 April. https://doi.org/10.1109/ACCTHPA57160.2023.10083336
13. L.Kou, S.Ding, T.Wu, W.Dong, Y.Yin. An Intrusion Detection Model For Drone Communication Network In SDN Environment. MDPI. 2022 Nov. https://doi.org/10.3390/drones6110342
14. S.Tavangari, S.T.Kulfati, A.Yelghi. Improve The Security Of Cloud Computing Ton Enhance Network Security. Preprint.Org. July 2023. https://doi.org/10.20944/preprints202307.1222.v1
15. W.G.Negara, F.Schwenker, T.G.Debelee, H.M. Melaku, Y.M.Ayano. MDPI. 2022 Dec. https://doi.org/10.3390/s22249837