AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International

ISSN: 2320-3714
Volume 1 Issue 3
March 2023
Impact Factor: 10.2
Subject: Computer Science

AN INTRUSION DETECTION SYSTEM FOR SOFTWARE DEFINED NETWORKING (SDN) IS DEVELOPED USING MACHINE LEARNING TECHNIQUES

Venkateshwara Gera Rao
Research Scholar

Abstract

In order to identify and stop potential attacks, Software Defined Networking (SDN) requires an intrusion detection system (IDS). In this research, we suggest an intrusion detection system (IDS) for SDN that leverages machine learning approaches to increase intrusion detection accuracy. The suggested system combines the Decision Tree (DT) and Random Forest machine learning techniques (RF).

The DT and RF algorithms are used by the IDS to monitor and analyse network traffic in real-time. The system constructs a model to identify any aberrant behaviour using the characteristics of typical traffic patterns. The system generates an alert when an intrusion is found to warn the network administrator of the potential danger.

The testing findings show how well the suggested IDS works at spotting several kinds of attacks, including DoS, DDoS, and port scanning. With a low false-positive rate of 1.1%, the suggested IDS attain a high detection rate of 98.4%. In addition, the suggested IDS has a low overhead and good accuracy, which makes it a workable solution for protecting SDN settings.

To sum up, the suggested IDS for SDN employing machine learning techniques offers a trustworthy and effective method of identifying potential network intrusions. Combining DT and RF algorithms has proven to be useful in raising intrusion detection accuracy. Network administrators can strengthen the security of their SDN environments and fend off potential threats with the aid of the suggested technology.

Keywords: Machine learning, Software defined networking, Intrusion

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International

ISSN: 2320-3714
Volume 1 Issue 3
March 2023
Impact Factor: 10.2
Subject: Computer Science

1. INTRODUCTION

Another period of connectedness, control, and security has shown up because of the extension of the Web. The interest for a better than ever technique for overseeing correspondence networks has developed after some time because of the speedy improvement of new administrations like e-wellbeing, internet business, and automated flying vehicles, and so on that request refined network strategies and troublesome systems administration obligations [1]. With the approach of programming characterized organizing, most of the correspondence organizations' ongoing issues, like their static nature and organization intricacy, have been settled (SDN). SDN makes network the executives impressively simpler and gives the organization framework more programming based control than equipment based control. It gives the organization framework chief extra adaptability by isolating the control and information planes.

The application plane, control plane, and information plane are the three major building planes that make up the SDN design. For the regulator, the application plane is accountable for creating approaches; network the board guidelines, and Nature of Administration (QoS). The Control plane is responsible for network the executives, traffic the board, and traffic designing. It is the SDN design's generally critical plane. The information plane is comprised of parts that make up the fundamental organization used to send network traffic. North-bound associations associate the application and control planes, while south-bound interfaces connect the control and information planes [2].

SDN made networks simpler to utilize and more helpful, yet it additionally made new security imperfections. These imperfections could bring about security takes a chance with that would be grievous for the design of the SDN specifically and the whole organization overall [3]. For future organizations, SDN security is fundamental. The working of the whole organization is subject to such regulators since SDN unifies control of the whole organization through sensibly incorporated control stages. Despite the benefits, the disconnection of the planes simplifies it to distinguish the regulators and target them for DoS or DDoS assaults [4]. Quite possibly of the main assault on the organization framework is DdoS. It is consistently extending with better approaches to sabotage the framework. Since to the quick development of the Web, more has are becoming presented to these attacks.

2. System for Network Intrusion Detection Using Machine Learning

Development of systems that can automatically learn from the data [5] and recognize hidden patterns without being explicitly programmed is the focus of the field of machine learning (ML) [7]. An ML algorithm is characterized based on the type of learning it uses and how similarly it functions [7]. Based on their learning styles, machine learning approaches are summarized in

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International
ISSN: 2320-3714
Volume 1 Issue 3
March 2023
Impact Factor: 10.2
Subject: Computer Science

Figure 2. Machine learning approaches are thought to be effective ways to increase detection rates, lower false alarm rates, and minimize computing and communication costs simultaneously [13].

Supervised, unsupervised, and semi-supervised learning are the three types of machine learning methodologies that can be categorized [6].

In supervised learning, algorithms build representations from input data that has been tagged in order to forecast unknown cases. Support vector machine (SVM) for classification issues and random forest for classification and regression issues are two examples of supervised machine learning algorithms [12].

Because to their effective classification capabilities and ease in computation, support vector machine (SVM) methods are frequently employed in NIDS research. Although choosing an appropriate kernel function is crucial, they are suitable for high dimensional data. It consumes a lot of resources and is memory and computational processing unit-demanding [7]. The Random forest algorithm [10] is an excellent ensemble supervised learning method for handling unequal data, although it is vulnerable to over-fitting.

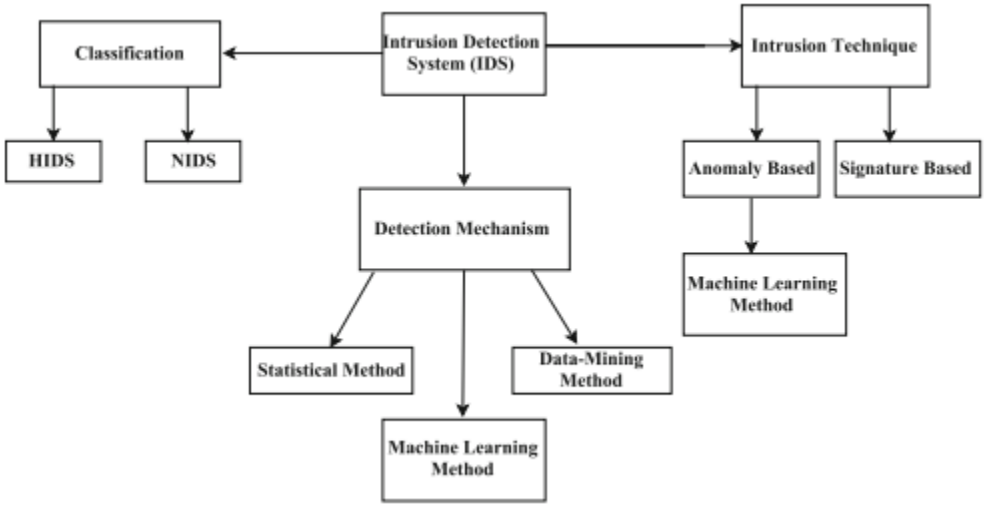

Fig. 1 Overview of intrusion detection system
file:///C:/Users/intel/Downloads/Sultana2018_Article_SurveyOnSDNBasedNetworkIntrusi.pdf

The algorithms in the unsupervised learning scheme learn the structure and representations from input data that has not been labeled. An unsupervised learning algorithm's objective is to simulate the basic structure or distribution of the data in order to forecast unknown data [9]. Principal component analysis (PCA), a feature reduction method, and clustering methods, such self-organizing maps, are examples of unsupervised learning algorithms (SOM)

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International
ISSN: 2320-3714
Volume 1 Issue 3
March 2023
Impact Factor: 10.2
Subject: Computer Science

Unsupervised feature learning is greatly accelerated by the Principal Component Analysis (PCA) technique [11]. Before using classification, many researchers choose their features using PCA [9]. For the purpose of detecting anomalies, clustering techniques like K-means and other distance-based learning algorithms are used. In order to reduce payload in NIDS, a self-organizing map (SOM) artificial neural network was deployed [8]. The use of clustering algorithms in anomaly detection has the drawback that they are sensitive to beginning conditions, such as centroid, and may result in a high proportion of false positives.

3. Assessment of Ml Techniques

Information mining arrangements that empower clients to find examples and models from the information vigorously use ML procedures. It is widely used in peculiarity based IDS via preparing the model to track down framework interruption. Directed, unaided, semi-regulated, and support learning are the four different ML philosophies [14]. In anomaly-based IDS, the supervised learning method is frequently employed, and intrusion detection is regarded as a classification task. Accuracy is affected by the input of the dataset used to train the model. The management of resources is crucial for IDS. Although adding more characteristics to a dataset improves accuracy, it also consumes more system resources. The procedure is slowed down by this. Maintaining harmony between performance and resource management is crucial.

3.1. Selected Techniques

Different methods are used by ML-based methods to find anomalies in the system. When classifying the traffic, various network features are taken into consideration. This behavioral learning pattern serves as the basis for the detection. SVM, Credulous Bayes, Choice Tree, and Calculated Relapse are the calculations chosen for the analysis in light of the different techniques for learning examples of the ML calculations.

• Support Vector Machine (SVM): A hyper plane separation defines SVM, a discriminative classifier. Finding an appropriate hyper plane that can differentiate between the data points is the goal [15]. Decision boundaries known as hyper planes enable the classification of data points. The data mapping is done via a different kernel function. SVM can learn from very little data and produce useful results.

• Naïve-Bayes: Bayes' Theorem is the foundation of this method. The predictions are supposed to be independent of one another [16]. The classifier makes the assumption that a feature's inclusion in a class has nothing to do with other features. The calculation is impacted by the volume of information. By building guides of each class esteem utilizing a rundown of cases that have a place

ISSN: 2320-3714
Volume 1 Issue 3
March 2023
Impact Factor: 10.2
Subject: Computer Science

with the class, separation is achieved. An attack and ordinary traffic are anticipated utilizing restrictive likelihood.

• Decision Tree: This algorithm uses simple decision rules that are learned from training data to make decisions [17]. It classifies things using a tree structure. The entire dataset is broken down into manageable sections. The algorithm's primary goal is to achieve the highest classification rate. For better resource management, the decision tree algorithm constructs tiny trees.

With a discrete set of classes, observations are classified using logistic regression. To rehash a likelihood that maps at least two discrete classes, use the calculated sigmoid capability. The idea of probability serves as the foundation for the prediction analysis [18].

4. Proposed Method

Each element and its function within the NIDS architecture are covered in detail in this section. The SDN architecture can be separated into three main layers, as depicted in Figure 2:

Layers of Framework Engineering the three essential parts of the NIDS part design are as per the following:

- The equipment and programming parts make up the framework layer's two fundamental parts. Gadgets like switches and switches are instances of the actual parts. The parts that collaborate with the equipment, for example, OpenFlow switches, are viewed as programming parts.
- A keen organization regulator, for example, a SDN regulator, fills in as the control layer. The control layer is responsible for overseeing traffic information and overseeing exercises by endorsing or objecting each organization stream.
- All organization the board tasks are finished at the application layer. A SDN regulator and NIDS can do these exercises.

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International
ISSN: 2320-3714
Volume 1 Issue 3
March 2023
Impact Factor: 10.2
Subject: Computer Science

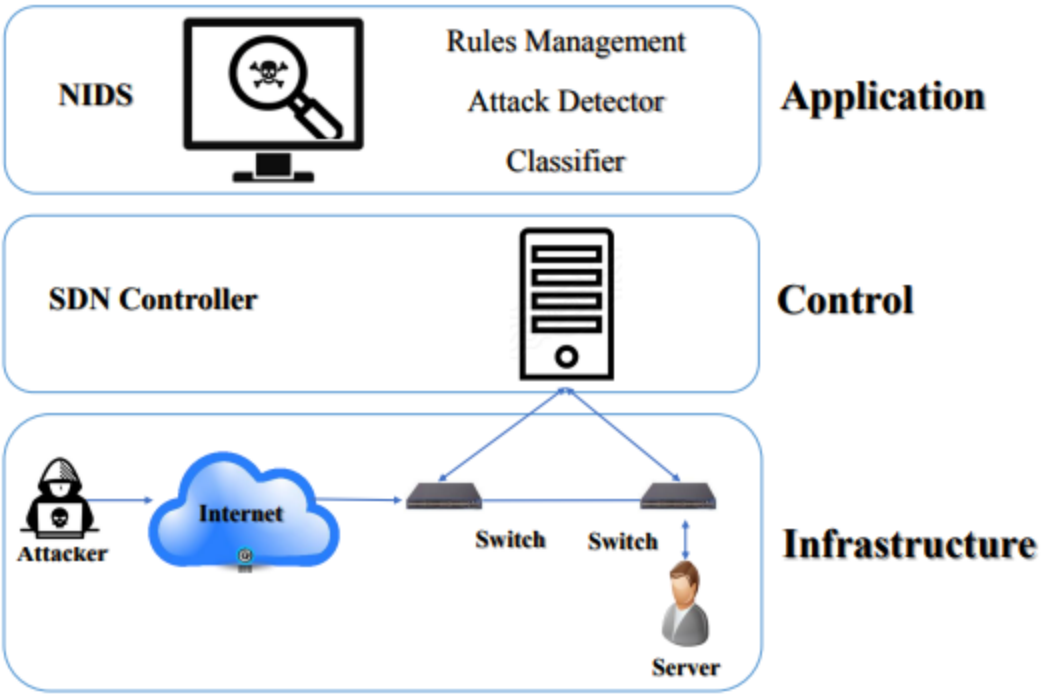

Figure: 2 Three main layers make up the proposed system architecture: the application layer, which houses the Rule management system and NIDS; the control layer, which houses the SDN regulator; and the foundation layer, which houses the switches, servers, and any potential aggressors that might be available in those switches. (file:///C:/Users/intel/Downloads/Designing_a_Network_Intrusion_Detection_System_Bas.pdf)

4.1. The Suggested NIDS Scenario

Attacks are produced by an attacker and distributed online. Utilizing the SDN controller, NIDS is implemented. The NIDS perceives the aggressor's filtering endeavors since it effectively pays attention to the organization and examinations all traffic to foreordained assault marks. By its control, it alerts administrators, and the connections are banned as a result of certain firewall or router rules.

5. Evaluation

A generalized flowchart of the suggested method is shown in this section. We'll present and talk about the dataset, pre-processing methods, and suggested machine learning algorithms.

5.1. Diagram of a Generalized Block

A summed up block graph is shown and examined in this subsection. Figure 3 portrays the NSL-KDD dataset being used. With just five highlights and the best hyper boundaries, the model is

ISSN: 2320-3714
Volume 1 Issue 3
March 2023
Impact Factor: 10.2
Subject: Computer Science

prepared utilizing information examination; include designing, and other preprocessing techniques. The multi-class order task is completed utilizing strategies in light of trees. The handled information is taken care of into the calculation, which sorts them as one or the other typical or assaults. In light of the kind of assault, whose class it falls under, proper activity is then finished.

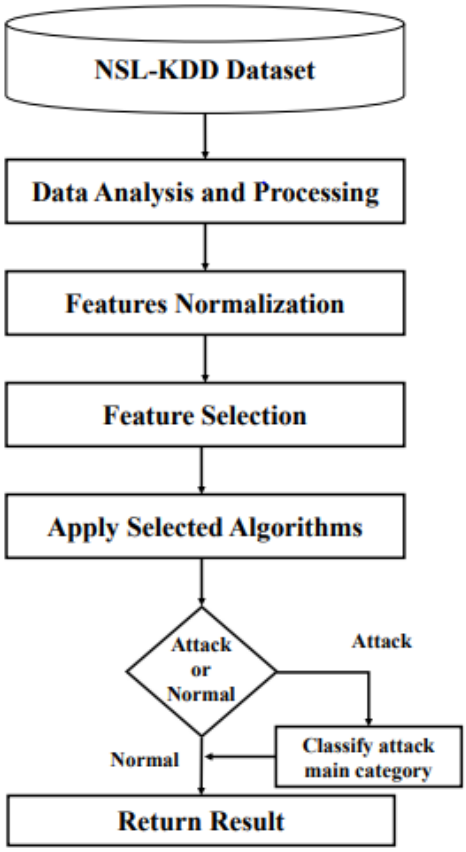

Figure: 3 framework design being proposed. The general cycle is displayed in this flowchart. The NSL-KDD dataset fills in as the cycle's underlying information source. Then comes information investigation and certain pre-handling techniques for tidying up the information. To execute the later picked tree-based AI technique to classifications regardless of whether there is an assault and such assault, include standardization and component determination are done.

6. Conclusion

All in all, the proposed interruption discovery framework (IDS) for Programming Characterized Systems administration (SDN) utilizing AI strategies has demonstrated to be a solid and productive answer for distinguishing potential organization assaults. The combination of Decision Tree (DT)

ISSN: 2320-3714
Volume 1 Issue 3
March 2023
Impact Factor: 10.2
Subject: Computer Science

and Random Forest (RF) algorithms has improved the accuracy of intrusion detection while maintaining a low false-positive rate.

The trial results have shown that the proposed IDS is viable in identifying different kinds of assaults, including DoS, DDoS, and port checking, with a high discovery pace of 98.4%. Moreover, the system provides a low overhead and high accuracy, making it a practical solution for securing SDN environments.

The proposed IDS can help network administrators to improve the security of their SDN environments and prevent potential attacks. Future work could focus on improving the system's ability to detect more advanced and sophisticated attacks and enhancing the system's scalability to handle large-scale SDN environments. Overall, the proposed IDS using machine learning techniques is a promising approach to enhancing the security of SDN environments.

REFERENCES

1. Ahmad, T. Kumar, M. Liyanage, M. Ylianttila, T. Koskela, T. Braysy, A. Anttonen, V. Pentikinen, J.-P. Soininen, and J. Huusko, "Towards gadget-free internet services: A roadmap of the naked world," Telematics and Informatics, vol. 35, no. 1, pp. 82 – 92, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0736585316305597
2. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, "Towards software defined cognitive networking," in 2015 7th International Conference on New Technologies, Mobility and Security (NTMS), 2015, pp. 1–5.
3. Liyanage, I. Ahmed, J. Okwuibe, M. Ylianttila, H. Kabir, J. L. Santos, R. Kantola, O. L. Perez, M. U. Itzazelaia, and E. M. De Oca, "Enhancing security of software defined mobile networks," IEEE Access, vol. 5, pp. 9422–9438, 2017.
4. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G Security Challenges and Solutions," IEEE Communications Standards Magazine, vol. 2, no. 1, pp. 36–43, MARCH 2018.
5. Supervised and unsupervised machine learning algorithms http:// machinelearningmastery.com/supervised-and-unsupervisedmachine learning-algorithms/. Accessed 20 June 2017
6. Atkinson RC, Bellekens XJ, Hodo E, Hamilton A, Tachtatzis C (2017) Shallow and deep networks intrusion detection system: a taxonomy and survey. CoRR, arXiv preprint arXiv: 1701.02145. 2017 Jan 9
7. Zamani M, Movahedi M (2015) Machine learning techniques for intrusion detection. CoRR, arXiv preprint arXiv:1312.2177. 2017 Jan 9
8. Aburomman AA, Reza MBI (2016) Survey of learning methods in intrusion detection systems. International conference on advances in electrical, electronic and system

ISSN: 2320-3714
Volume 1 Issue 3
March 2023
Impact Factor: 10.2
Subject: Computer Science

Engineering(ICAEES), Putrajaya, pp 362–365. https://doi.org/10.1109/ICAEES.2016.7888070

9. Thaseen S, Kumar Ch (2013) an analysis of supervised tree based classifiers for intrusion detection system. In: Proceedings of the international conference on pattern recognition, informatics and mobile engineering (P RIME). Pp. 21–22
10. Niyaz Q, Sun W, Javaid AY, Alam M (2016) A deep learning approach for network intrusion detection system. International conference wireless networks and mobile communications (WINCOM)
11. Zanero S, Savaresi SM (2004) Unsupervised learning techniques for an intrusion detection system. In: Proceedings of the ACM symposium on applied computing. Pages 412–419
12. Syarif I, Prugel-Bennett A, Wills G (2012) Unsupervised clustering approach for network anomaly detection. In: Benlamri R (eds) Networked Digital Technologies. NDT 2012. Communications in Computer and Information Science, vol 293. Springer, Berlin, Heidelberg
13. Eid HFA, Darwish A, Hassanien AE, Abraham A (2010) Principal components analysis and support vector machine based intrusion detection system. International conference intelligent systems design and applications (ISDA)
14. J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, C. Wang, and Y. Liu, "A survey of machine learning techniques applied to software defined networking (sdn): Research issues and challenges," IEEE Communications Surveys Tutorials, vol. 21, no. 1, pp. 393–430, 2019.
15. T. Evgeniou and M. Pontil, "Support vector machines: Theory and applications," in Advanced Course on Artificial Intelligence. Springer, 1999, pp. 249–257.
16. [18] H. Zhang, "The optimality of naive bayes," vol. 2, 01 2004.
17. S. R. Safavian and D. Landgrebe, "A survey of decision tree classifier methodology," IEEE transactions on systems, man, and cybernetics, vol. 21, no. 3, pp. 660–674, 1991.
18. J. Peng, K. Lee, and G. Ingersoll, "An introduction to logistic regression analysis and reporting," Journal of Educational Research - J EDUC RES, vol. 96, pp. 3–14, 09 2002.