International Academic Institute for Science and Technology

International Academic Journal of Science and Engineering
Vol. 8, No. 4, 2021, pp. 6-11.

ISSN 2454-3896

International Academic Journal of Science and Engineering

www.iaiest.com

Machine Learning Assisted Intrusion Detection System against Slow Rate Http/2 Dos Attacks

Ajay Malhotra [a], Nidhi Mehra [b]

[a] *Department of Computer Science and Engineering, Byte Bridge School of Technology, Ghaziabad, India.*
[b], *Department of Computer Science and Engineering, Byte Bridge School of Technology, Ghaziabad, India.*

Abstract

The recently defined HTTP/2 protocol has additional benefits over HTTP/1.1 and is intended to make effective use of TCP's transmission rate. Its threat pathways are still not fully recognized, though. Research on security flaws or vulnerabilities is extremely limited. It's critical to comprehend potential risks. Slow rate DoS (Denial of Service) attacks are among the most successful. In this research, we use machine learning to develop an intrusion detection system against slow rate HTTP/2 DoS assaults. We use one class SVM method for classification of attacks. Proposed OIDS system has two modules in which first one is feature extraction module and one-class SVM classification module. We contrasted our suggested model with state-of-the-art models including Random Forest, ANN, KNN, Decision Tree, and Naïve Bayes. Measures including as accuracy, sensitivity, specificity, precision, TPR, FPR, and detection rate are used to assess these models. With excellent precision, the suggested model (OIDS) performed better.

Keywords: DoS Attacks, HTTP/2, Intrusion Detection, Machine Learning.

DOI:10.71086/IAJSE/V8I4/IAJSE0824
Received: 06 September 2021/Revised: 08 October 2021/Accepted: 03 November 2021/Published: 31 December 2021

Introduction

Since extremely effective network infrastructure has been developed, networking research is currently concentrating on creating reliable application layer protocols that fully leverage the capabilities and potential of the underlying infrastructure. For instance, TCP is used as a transport layer protocol for dependable data delivery in the application layer Hypertext Transfer Protocol (HTTP/1.1) (Tripathi & Hubballi, 2018). Hypertext links are used to load online pages via HTTP. It 1. HTTP/1.0 only permits one request per TCP connection at a time. Although HTTP/1.1 introduced request pipelining, head-of-line blocking still affects request concurrency. This inspired researchers to create HTTP/2, the most recent iteration of the HTTP protocol. As network latency increases, HTTP/2 PDT (Page Download Time) stays 15% less than HTTP/1.1 PDT. In addition to using TCP inefficiently and employing message multiplexing to manage several requests concurrently, HTTP/2 is more susceptible to attacks than HTTP/1.1. The research community has not yet focused much on the security flaws or vulnerabilities in HTTP/2 because it is a new protocol. There aren't many publications in the literature that address some of HTTP/2's security vulnerabilities: In-depth Analysis of the Top Four Flaws of the Next Generation Web Protocol) (Adi et al., 2017), (Attacking HTTP/2 Implementations). We think that developing flexible detection and mitigation techniques requires a thorough grasp of potential risks that could interfere with the regular operation of a widely used protocol like HTTP/2. In this research, we develop an intrusion detection system with machine learning support to defend against slow-rate HTTP/2 DoS attacks (Adi et al., 2017). Multiplexing a Connection through Streams shown in Fig. 1.



Fig. 1: Multiplexing a Connection through Streams

Related Works

Anderson's well-known writings served as the starting point for intrusion detection research. In order to identify the "masquerader" that deviates from the established normal model, Anderson et al. suggested a model based on statistics of users' typical behaviors. This model built the groundwork for intrusion detection and unveiled the fundamental concept of anomaly identification. Subsequent studies on anomaly identification also use a variety of statistical techniques, such as frequency and basic significance tests, multivariate statistics, Bayesian analysis, and principal component analysis.

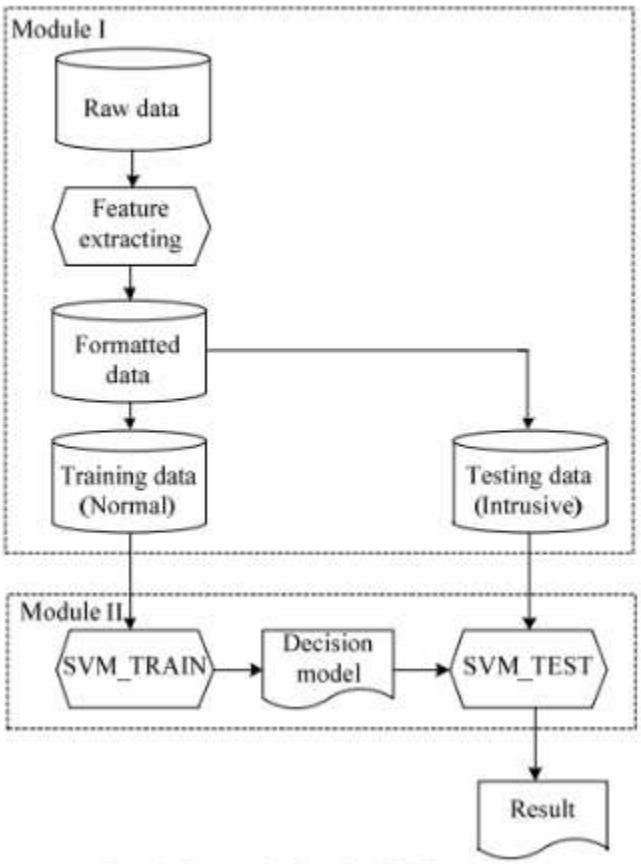
Kruegel et al., (2003) were the first to introduce signature-based detection, often known as abuse detection (Praseed, 2020). One way to think about the author's proposed intrusion detection paradigm is as a rule-based pattern matching system. Both statistics-based anomaly detection and abuse detection have drawbacks, including low intelligence and a limited capacity to adjust to different application settings. Additionally, the detection results might deteriorate while dealing with larger datasets. Sinclair et al. have employed a variety of machine learning techniques to address the shortcomings of the aforementioned models; the two most popular approaches may be Support Vector Machines (SVMs) and Artificial Neural Networks (ANNs). ANN and SVM are frequently used to create hybrid models that can identify intrusions. In this paper, our work relates to SVM and ANN is used as a comparison. Multi-class SVM is also an alternative (Kushwah & Ranga, 2020).

Intrusion Detection System

Framework of One-Class SVM Model

The one-class SVM-based model's framework is shown in Fig. 2. From the original packets, almost no intrusion detection algorithm is able to differentiate between normal and invasive connections. Formatted data must be entered into them. The process of feature extraction involves taking valuable information out of raw data and formatting it so the detecting module can understand it. A permanent standard for feature extraction does not exist. To determine whether certain assaults are concealed in connections, it can be preferable to extract features based on the real network environment. Proper feature extraction enables the detection module to produce predictions that are more accurate (Erfani et al., 2016). The length (number of seconds) of the connection, the kind of protocol (tcp, udp, etc.), the number of data bytes sent, the number of "root" accesses, and other widely used aspects are important to consider when

discussing network invasions. The feature extracting module of our one-class SVM-based detection model uses the raw data as inputs and then extracts the predicted features to create the formatted data.



Fig, 2: Framework of One-Class SVM Model

Additionally, the task of splitting the prepared data into training and testing data falls to the feature extracting module (Zhang et al., 2015). It's a rather easy process. The testing data is made up of the remaining (intrusive) records, whereas the training data is made up of the normal records. This pertains to the one-class SVM's detection process.

Results and Discussion

The comparison of models with overall performance is shown in Table 1. Model comparison graphs showing overall performance, accuracy, sensitivity, specificity, precision, and F-measures are shown in Fig. 3, 4, 5, and 6, respectively. The True Positivity Rate (TPR) and False Positive Rate (FPR) of several models are shown graphically in Fig. 7 (Perdisci et al., 2006). The detection rate, 93.25%, where our model performs better than another model is shown in Fig. 8.

Table 1: Overall Performance Measures

Classification methods	Accuracy (%)	Sensitivity (%)	Specificity (%)	Precision (%)	F-measure (%)
Decision Tree	74	75.05	91.78	65	93.71
ANN	84.78	81.59	81.59	83.26	82.09
KNN	86.36	78.08	79.08	79.65	78.62
Random Forest	89.02	80.35	86.6	75.36	87.84
Naïve Bayes	90.12	84	95.77	80.22	91.25
OIDS (Proposed)	93.25	90.95	97.52	85.01	96.74

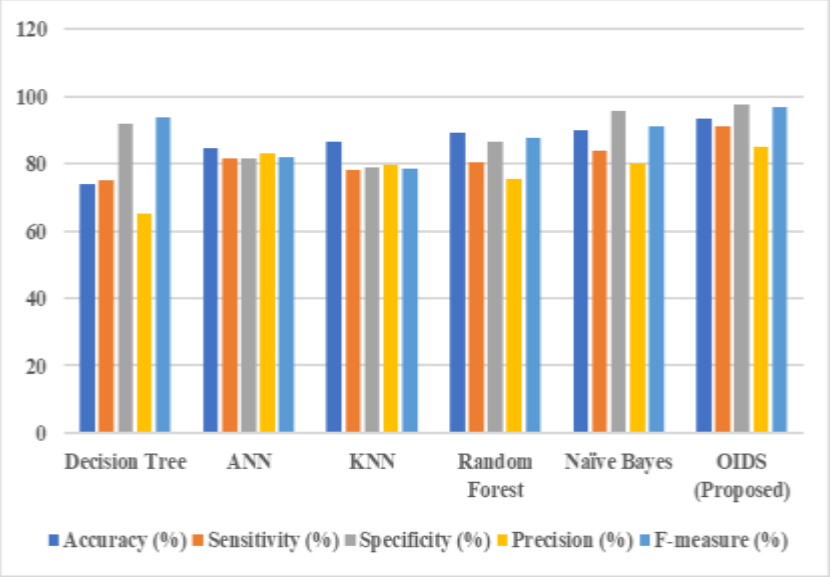


Fig. 3: Overall Performance of Models

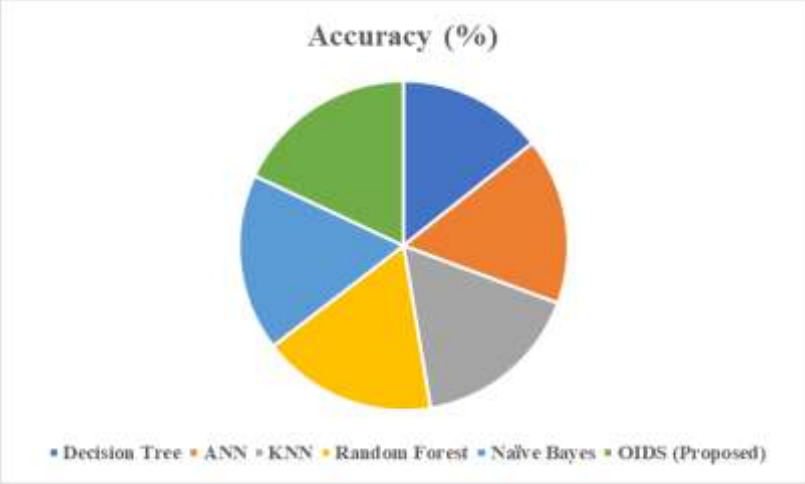


Fig 4: Models v/s Accuracy

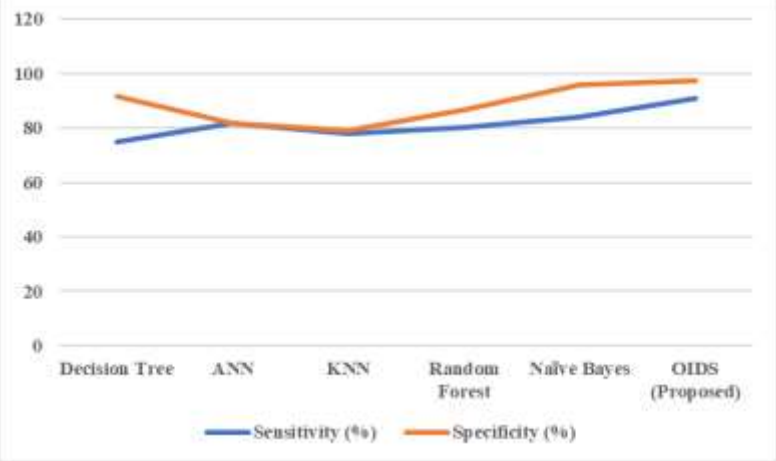


Fig. 5: Models v/s Sensitivity and Specificity

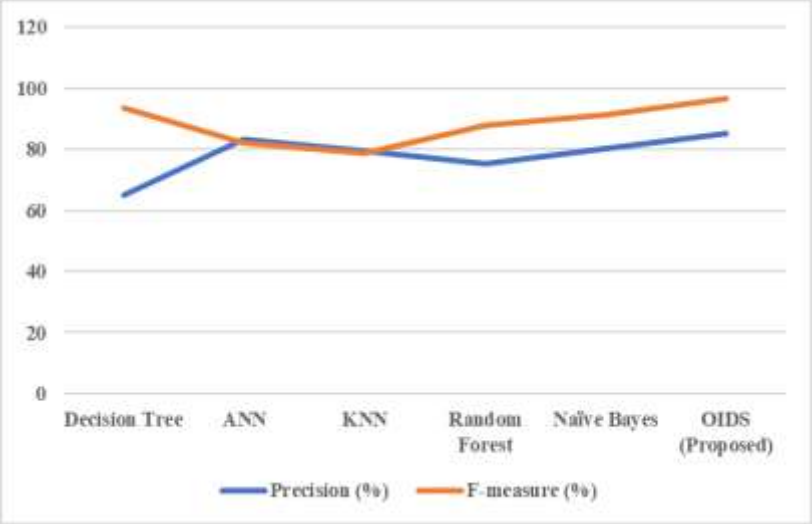


Fig. 6: Models v/s Precision and F-Measure

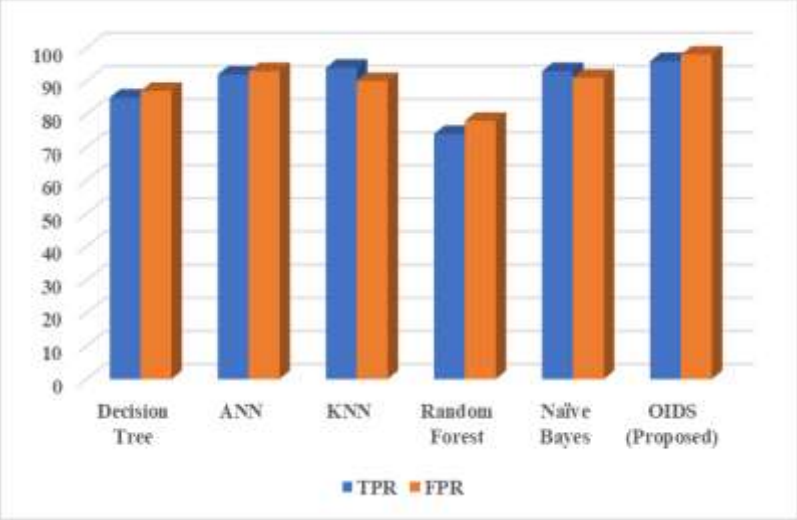


Fig. 7: Models v/s TPR, FPR

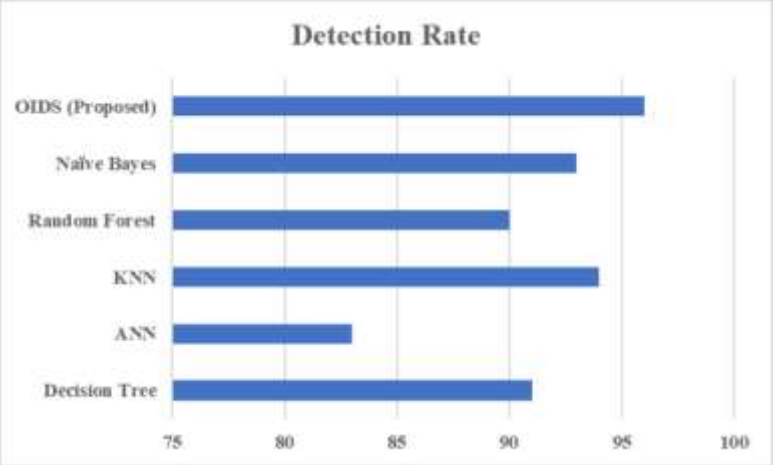


Fig. 8: Models V/s Detection Rate

Our proposed model shows good overall performance. Proposed OIDS have the highest accuracy of 93.25%. Next to ours Naïve Bayes model possesses high accuracy of 90.12%. Decision Tree model has the least value for accuracy. In the case of sensitivity as accuracy ours has highest value and naïve bayes has second to it (Khreich et al., 2017). Decision tree has least value in this measure too. Our model and naïve bayes model has high value for both specificity and precision. But, in the case of F-measures ours and Decision tree possesses higher values of 96.74% and 93.71%.

Conclusion

In this research, we present a machine learning-based intrusion detection system (OIDS) to defend against slow rate HTTP/2 DoS assaults. We learn the significance of protecting the device from malevolent attacks from this work. The globe is currently concentrating on enhancing security in a number of ways, starting with stopping data leaks. We are classifying assaults using a one-class SVM. There are two modules in the suggested system. One class SVM model classifies it into attack and normal, while the other is a feature extraction module that extracts features from the datasets. Since we initially only have one type of traffic or data, we are utilizing a one-class classification technique. We have compared our model with some cut edge models such as Decision Tree, ANN, KNN, Random Forest and Naïve Bayes under performance measures such as Accuracy, Specificity, Sensitivity, Precision, F-measure. Our proposed OIDS outperformed well with an accuraccy of 93.25%.

References

Tripathi, N., & Hubballi, N. (2018). Slow rate denial of service attacks against HTTP/2 and detection. *Computers & security*, *72*, 255-272. https://doi.org/10.1016/j.cose.2017.09.009

Adi, E., Baig, Z., & Hingston, P. (2017). Stealthy Denial of Service (DoS) attack modelling and detection for HTTP/2 services. *Journal of Network and Computer Applications*, *91*, 1-13. https://doi.org/10.1016/j.jnca.2017.04.015

Praseed, A. (2020). *Modelling Behavioural Dynamics for Application Layer Distributed Denial of Service Attack Detection* (Doctoral dissertation, National Institute of Technology Karnataka, Surathkal).

Kushwah, G. S., & Ranga, V. (2020). Voting extreme learning machine based distributed denial of service attack detection in cloud computing. *Journal of Information Security and Applications*, *53*, 102532. https://doi.org/10.1016/j.jisa.2020.102532

Erfani, S. M., Rajasegarar, S., Karunasekera, S., & Leckie, C. (2016). High-dimensional and large-scale anomaly detection using a linear one-class SVM with deep learning. *Pattern Recognition*, *58*, 121-134. https://doi.org/10.1016/j.patcog.2016.03.028

Zhang, M., Xu, B., & Gong, J. (2015, December). An anomaly detection model based on one-class svm to detect network intrusions. In *2015 11th International conference on mobile ad-hoc and sensor networks (MSN)* (pp. 102-107). IEEE. https://doi.org/10.1109/MSN.2015.40

Perdisci, R., Gu, G., & Lee, W. (2006, December). Using an ensemble of one-class svm classifiers to harden payload-based anomaly detection systems. In *Sixth International Conference on Data Mining (ICDM'06)* (pp. 488-498). IEEE. https://doi.org/10.1109/ICDM.2006.165

Khreich, W., Khosravifar, B., Hamou-Lhadj, A., & Talhi, C. (2017). An anomaly detection system based on variable N-gram features and one-class SVM. *Information and Software Technology*, *91*, 186-197.