International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 12 Issue 11, November-2023, Impact Factor: 7.751

Unmasking the Code Breakers: Empowering Cyber Defense with SVM – Based Intrusion Detection against Dos Attack

Prof. Anjali S. More[1], Aditya Murke[2], Aachal Harinkhede[3], Sakshi Mahajan[4], Bhagyashree Patil[5]

[1]Assistant Professor, Department of Computer Engineering, SRTTC FOE, MH, India,
[2,3,4,5] Student, Department of Computer Engineering, SRTTC FOE, MH, India,
(Savitribai Phule Pune University)

ABSTRACT

Smart grid has progressively become a widespread development trend in the global power business in recent years, and its security issues are becoming increasingly regarded by researchers. Physical control, for example, has been used in smart grids. To increase their security, they use data encryption and authentication. However, timely and effective detection remains a problem. Strategies to keep the grid safe from cyber- attacks invasions that are malicious In order to address this issue, a model based on Machine learning has been used to detect smart grid DoS attacks. Suggested. First, the model gathers network data, and then it analyses it. For data dimensionality, picks features and applies PCA Finally, SVM algorithms are used to reduce the size of the dataset.

Keywords: Machine Learning, Support Vector Machine Algorithm, Dos Attack Detection

INTRODUCTION

The industrial industry is undergoing a dramatic transition as a result of the information era. In this context, the notion of smart grid arose as the times demanded, and it has since gained widespread recognition on a global scale, becoming a common development trend in the global power business. However, there have been instances of smart grid intrusion in the past. On January 6, 2016, for example, hackers attacked the Ukrainian electricity grid infrastructure, forcing hundreds of houses to turn off their lights. This is the first time in history that a cyber-attack has resulted in power interruptions. This cyber-attack on industrial control systems is unquestionably a watershed moment.

LITERATURE REVIEW

Paper Name: Early Detection of DOS Attacks in VANET Using Attack Packet Detection Algorithm (APDA) Authors: S. RoselinMary, M. Maheshwari, M. Tamaraiselvan Abstract ::- Security of VANET (Vehicular Ad Hoc Network) is relevant in critical situations where its very existence is life-threatening. It is therefore very important.. VANET is a subtype of his MANET. All mobile nodes are vehicles equipped with an onboard unit (OBU) that can send and receive messages from other nodes in the network. In addition to vehicle-to-vehicle communication, VANET interfaces with communication points provided by the road infrastructure. Many researchers have already proven the safety information. Additionally, VANET is susceptible to several security attacks. In existing VANET systems, if delay overhead occurs, a detection algorithm is used to detect attacks during verification. Various security threats include rogue nodes providing false information, Sybil attacks, and selfish driver attacks. In this article, we proposed an APDA (Attack Packet Detection Algorithm) algorithm that is used to detect DOS (Denial of Service) attacks.) is used before checking the time. This minimizes the processing overhead delay and improves the security of VANET

Paper Name: IoTDoS and DDoS Attack Detection using ResNet Author: Faisal Hussain, Syed Ghazanfar Abbas, Muhammad Husnain, Ubaid U. Fayyaz, Farrukh Shahzad, Ghalib A. Shah Abstract : The network attacks are increasing both in frequency and intensity with the rapid growth of internet of things (IoT) devices. Recently, DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks are reported as the most common attacks in IoT networks. Traditional security solutions such as firewalls, intrusion detection systems, etc. are unable to detect complex DoS and DDoS attacks, as most of them filter normal and attack traffic based on static predefined rules. However, these solutions can become reliable and effective when integrated with artificial intelligence (AI)-based techniques. Over the past few years, deep learning models, especially convolutional neural networks, have achieved high prominence due to their

excellent performance in image processing. The potential of these convolutional neural network (CNN) models can be used to effectively detect complex DoS and DDoS by converting the network traffic dataset into images.Therefore, in this work, we proposed a methodology to convert the network traffic data into image form and trained a stateof- the-art CNN model, i.e., ResNet via converted data. The proposed methodology achieved a value of 99.99percent accuracy for detecting the DoS and DDoS in case of binary classification. Furthermore, the proposed methodology achieved 87 percent average precision for recognizing eleven types of DoS and DDoS attack patterns which is 9 percent higher as compared to the state-of-the-art.

Paper Name: Mitigation and Detection Strategy of DoS Attack on Wireless Sensor Network Using Blocking Approach and Intrusion Detection System Author: Faisal Mochamad Teguh Kurniawan, Setiadi Yazid Abdelrhman Mohammed, Iman Abuel Maaly Abdelrahman abstract: Wireless Sensor Network (WSN) has a big role in several fields such as military, health and even information technology such as IoT (Internet of Things). In addition to many advantages, WSN has a disadvantage in its application, where no embedded security system is built into the sensor device due to the limitations that sensor nodes have, such as memory, processor, and battery. As a result, WSN is vulnerable to attacks, one of the main attacks on WSN is DoS attack. DoS attacks aim to prevent authorized users from exploiting resources by throttling existing resources until network resources become busy, the network slows down, and eventually shuts down. So we need to detect and mitigate DoS attacks in order to stop these attacks. In this study, the DoS attack detection and mitigation method uses a signature-based intrusion detection system (IDS) by implementing a blocking approach on the attacking node by blocking all packets originating from the attacker until the attacker runs out of power. A blocking approach was successfully implemented in a WSN when the IDS detected a DoS attack. Thus, the blocking method can be used to mitigate DoS attacks by blocking all packets originating from the attacker.

Paper Name: Event-triggered Switching-type Fault Detection and Isolation for Fuzzy Control Systems under DoS Attacks Author: Xiang-GuiGuo, Xiao Fan, Jian-Liang Wang, and Ju H. Park, abstract :This paper investigates the memory adaptive eventtriggered (MAET) fault detection and isolation (FDI) problem for nonlinear networked control systems under periodic denial-ofservice (DoS) attacks, where the nonlinear systems are described by Takagi–Sugeno (T–S) fuzzy models with unknown membership functions. First, a new event-triggered mechanism for saving communication resources is proposed. The trigger threshold is adaptively adjusted by several previous sampled data, not only depending on the latest trigger data. Second, considering DoS attacks and an event-triggered mechanism, a state feedback controller is constructed and exponential stability is derived. Meanwhile, the controller and the event-triggered mechanism are simultaneously developed based on the piecewise Lyapunovfunction. Then, a set of switching T– S fuzzy observers are constructed to realize FDI under DoS attacks. In addition, a variable switching method is introduced to solve the problem of asynchronous premise variables caused by the event-triggered mechanism. Finally, simulation cases are presented to demonstrate the validity and benefit of the proposed FDI scheme.

Paper Name: Thwarting DoS Attacks: A Framework for Detection based on Collective Anomalies and Clustering Author: Mohiuddin Ahmed Abstract: Information security is integral to any organization aiming to protect its intellectual property in the face of escalating and increasingly novel cyberattacks.1 Among these, denial-of service (DoS) attacks—in which attackers typically send a volume of connection or information requests to overload the target system—have earned the reputation as one of the most severe threats because they can shut down the availability of a host, router, or even an entire network. The attacked system can be forced out of service in as quickly as a few minutes and remain that way for days, forcing the victimized organization to incur significant losses. Additionally, a number of toolkits for launching a DoS attack are freely available and easy to operate.2 Compounding the problem is the growth of the Internet of Things (IoT), which is expected to dramatically change the nature and size of DoS attacks. This does not bode well for existing techniques to detect DoS attacks, which tend to scale poorly. The solution might lie in some form of anomaly detection, which aims to identify anomalous or abnormal data from a given dataset, often discovering new and rare patterns. Also known as outlier, novelty, or deviation detection or exception mining, anomaly detection has been widely studied in statistics and machine learning. Unfortunately, traditional techniques—which are based on nearest neighbor, clustering, and statistics—assume that individual data instances are anomalous, an assumption that does not align with DoS attack characteristics.

Paper Name: Implementation of SDN-based IDS to protect Virtualization Server against HTTP DoS attacks Author: Saifudin Usman, Idris Winarno, Abstract: Virtualization and Software-defined Networking (SDN) are emerging technologies that play a major role in cloud computing. Cloud computing provides efficient use, high performance and availability of resources on demand. However, virtualization environments are vulnerable to various types of intrusion attacks, which include the installation of malicious software and Denial of Services (DoS) attacks. The use of SDN technology makes the idea of SDN-based security applications attractive in the fight against DoS attacks. Network Intrusion Detection System (IDS), which is used to perform network traffic analysis as a detection system implemented in SDN networks to protect virtualization servers from HTTP DoS attacks. Experimental results show that the SDN-based IDS is able to effectively detect and mitigate HTTP DoS attacks.

PROBLEM STATEMENT

To Comparing the different Detection techniques for the DOS attack at a low rate, and finding the appropriate detection technique to mitigate the attack having low false rate.

SYSTEM ARCHITECTURE

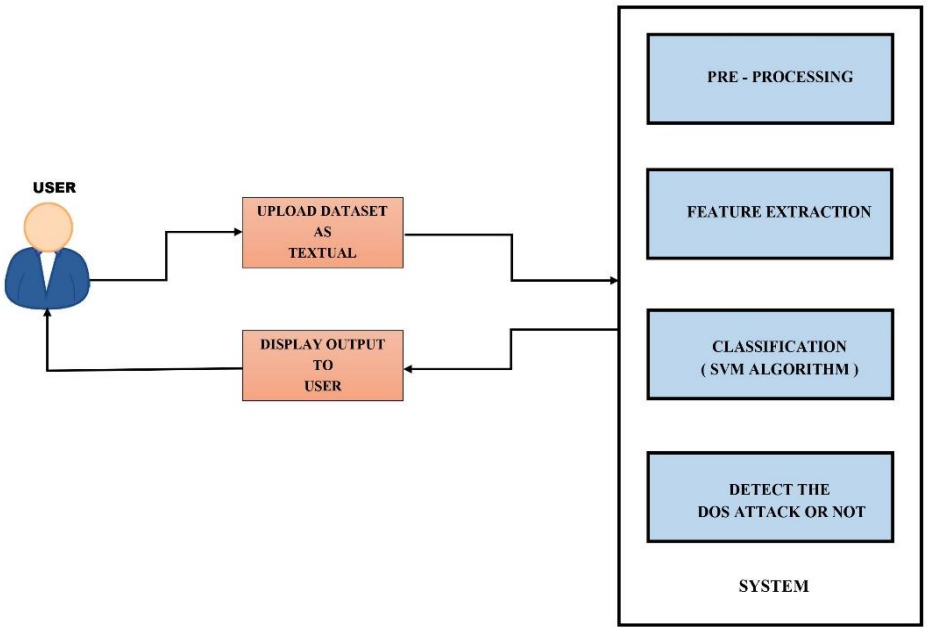

Figure 1: system architecture

PROPOSED SYSTEM DESIGN

Figure 2: data flow diagram (1)

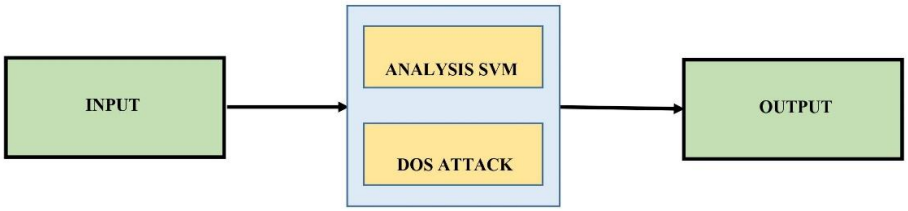

Figure 3: data flow diagram (2)

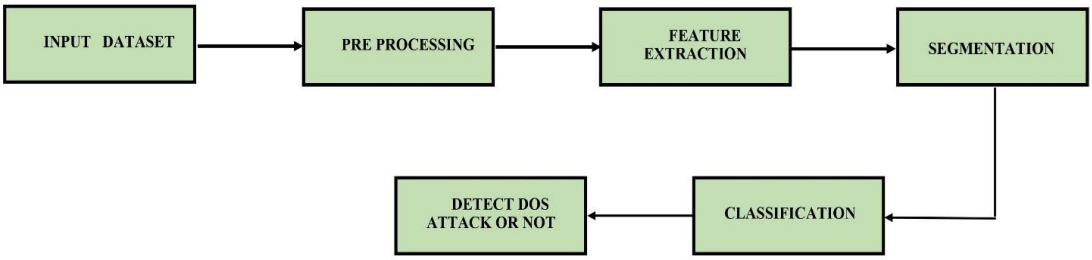

Figure 4: data flow diagram (3)

MODULE

Pre-processing, Data pre-processing is a very important and quite underestimated step in Machine Learning pipelines. It provides cleaned and relevant datasets which then can be used in further steps like classification or regression. Segmentation: - Support Vector Machine (SVM) is proposed for image segmentation. SVM is a machine learning algorithm that can reduce the segmentation error caused by fast object movement. First, frame difference combined with morphology mathematics is used to coarsely extract the object. • Feature extraction • in developing a successful SVM forecaster, feature extraction is the first important step. ... PCA linearly transforms the original inputs into uncorrelated College Short Form Name, Department of Computer Engineering 2020 21 features. KPCA is a nonlinear PCA developed by using the kernel method. In ICA, the original inputs are linearly transformed into statistically independent features. • SVM classification • Image result for classification svm algorithm "Support Vector Machine" (SVM) is a supervised machine learning algorithm that can be used for both classification and regression challenges. However, it is most commonly used in classification problems. ... The SVM classifier is the boundary that best separates the two classes (hyper-plane/line).

CONCLUSION

This work provides a smart grid DoS attack detection methodology based on machine learning to address the challenge of smart grid intrusion detection. In real time, the approach gathers network communication data between the smart metre and the data server. The SVM classifier trained model is used to identify and detect DoS assaults by using feature selection and PCA dimension reduction to choose more representative features. The SVM classification model outperforms the Naive Bayesian Network and Decision Tree classification algorithms on the KDD99 dataset. This method has a greater detection rate and accuracy for classification, which can help to improve the smart grid's security.

REFERENCES

[1]. Vidyaev I G, Ivashutenko A S, Samburskaya M A. Smart Grid Concept As A Modern Technology For The Power Industry Development[C]// 2017:012173.
[2]. Huang H B, Hong L, Chang-Yue Y U, et al. Analysis on Ukraine Power Grid Blackout and Its Enlightenment of ICS in China[J]. Standard Science, 2016.
[3]. JianyeHao, Eunsuk Kang, Jun Sun, Zan Wang, "An Adaptive Markov Strategy for Defending Smart Grid False Data Injection from Malicious Attackers", IEEE Transactions on Smart Grid. Sept. 2016.
[4]. JiaxuanFei,TaoZhang,YuanyuanMa,Cheng Zhou. A DDoS attack detection method for power grid industrial control system based on BF-DT-CUSUM algorithm[J]. Telecommunications Science.2015 (12).
[5]. Yanan Sun, Xiaohon Guan, Ting Liu, Yang Liu, "A cyber-physical monitoring system for attack detection in smart grid", Computer Communications Workshops (INFOCOM WKSHPS), 2013 IEEE Conference on, Turin, Italy, Dec. 2014.
[6]. Mina Rahbari and Mohammad Ali JabreilJamali, "Efficient Detection of Sybil Attack Based on Cryptography in VANET," IJNSA, Vol.3, No.6, November 2011.
[7]. Mohamed Salah Bouassida, Gilles Guette, Mohamed Shawky, and Bertrand Ducourthial, "Sybil Nodes Detection Based on Received Signal Strength Variations within VANET," International Journal of Network Security, Vol.9, No.1, PP.22- 33, July 2009.
[8]. Yi P, Zhu T, Zhang Q, et al. A denial of service attack in advanced metering infrastructure network[C]// IEEE International Conference on Communications. IEEE, 2015:1029-1034.
[9]. Wang K, Du M, Maharjan S, et al. Strategic Honeypot Game Model for Distributed Denial of Service Attacks in the Smart Grid[J]. IEEE Transactions on Smart Grid, 2017, PP(99):1-1.
[10]. Pooja B, Pai M M M, Pai R M, et al. Mitigation of internal and external DoS attack against signature-based authentication in VANETs[C]// Computer Aided System Engineering.IEEE, 2014:152-157.
[11]. Saxena H, Richariya V. Disturbance detection in the KDD99 dataset using SVM-PSO and Feature Reduction with Information Gain[J].International Journal of Computer Applications, 2014, 98(6):25-29
[12]. Sousa, P. H. F.; Nascimento, N. M. M.; Almeida, J. S.; Rebouças Filho, P. P. and Albuquerque, V. H. C. (2019). Intelligent incipient fault detection in wind turbines based on an industrial IoT environment. Journal of Artificial Intelligence and Systems, 1, 1–19.