IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DDos Attack Detection Model

Prof. S.V.Reddy [1], Rohit Nanaware [2], Shubham Indavat [3], Sakshi Garud[4]

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

Abstract: In the last few years, the smart grid has grown into a major trend in the power industry around the world, and researchers have paid more attention to the security problems it poses. In smart grids, for example, physical control has been used. To make sure their data is safe, they encrypt it and use authentication. But finding them quickly and effectively is still hard. Techniques keep hackers from getting into the grid without permission. To deal with this problem, a machine learning model has been made. Using this technology, DoS attacks on the smart grid have been found. recommended First, the model gathers and looks at data about networks. PCA is used to figure out how many dimensions the data has. SVM algorithms are then used to make the dataset as small as possible.

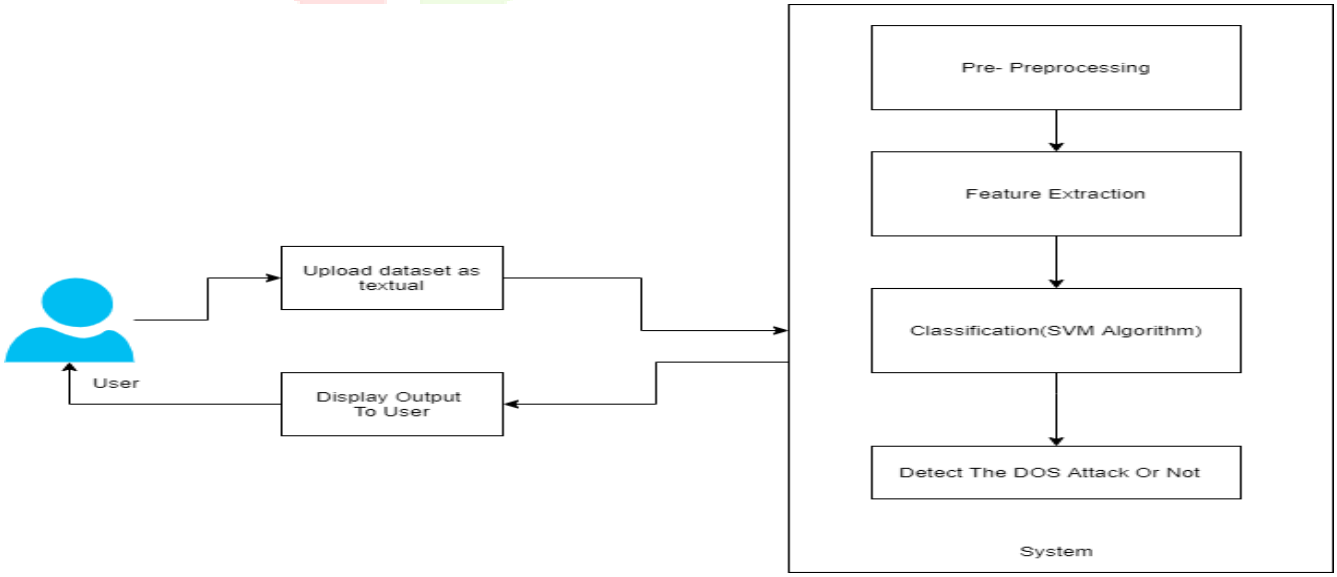
Index Terms **– Machine Learning, SVM.**

I. INTRODUCTION

The industrial industry is undergoing fast development as a result of the information era. The smart grid concept evolved as the times dictated, and it has since gained significant global acceptance, becoming a typical development trend in the global power sector. Smart grid penetration has, however, been seen in the past. On January 6, 2016, hackers infiltrated the Ukrainian electrical grid infrastructure, forcing hundreds of families to turn off their lights. A cyber-attack has triggered power shortages for the first time in history. This cyber-attack on industrial control systems is without a doubt unprecedented.

.

II. SYSTEM ARCHITECTURE



The SOM method detects DoS assaults by extracting flow statistics associated with DoS attacks. This approach has a low consumption rate and a high detection rate. The crucial issue is the extraction of time intervals. The disadvantage of this strategy is that the detection has some hysteresis and the attack has some hysteresis. Behavior is not discovered in a timely and accurate manner. The authors presented a structure for It is suitable for large-scale network detection and mitigation of DoS assaults, but it is not suitable for small-scale implementation. In this case, a DoS attack detection technique is based on aIt is planned to create a

legal source and destination IP address database. It evaluates the anomalous properties using the nonparametric cumulative technique CUSUM.

III. ALGORITHM : SVM (Support Vector Machine)

- SVM-Support vector machines (SVMs) are a set of supervised learning methods used for classification , regression and outlier's detection.
- The advantages of support vector machines are:
- Effective in high dimensional spaces.
- Still effective in cases where number of dimensions is greater than the number of samples.
- Uses a subset of training points in the decision function (called support vectors), so it is also memory efficient.
- Versatile: different Kernel functions can be specified for the decision function. Common kernels are provided, but it is also possible to specify custom kernels.

IV. LITERATURE SURVEY :

1) Paper Name : Early Detection of DOS Attacks in VANET Using Attacked Packet Detection Algorithm (APDA).

Authors : S. RoselinMary, M. Maheshwari, M. Thamaraiselvan .

Description : The safety of VANETs, also known as Vehicle Ad Hoc Networks, is of the utmost importance given the correlation between their presence and potentially fatal circumstances. The MANET can be further subdivided into the VANET. In this configuration, each mobile node takes the form of a self- contained vehicle furnished with an On-Board Unit (OBU), which grants them the ability to communicate with other network nodes and send and receive messages. In addition to communication between individual vehicles, VANET also connects with the communication points that are given by the infrastructure that is located on the road. A significant number of researchers have previously established that safety messages are secure. The VANET network is susceptible to a variety of security flaws as well. Previous VANET systems made use of a detection approach to find out about attacks at the time of verification, which was also when the delay overhead took place. Misbehaving nodes, which provide false information, Sybil attacks, attacks on selfish drivers, and other security holes are only some of the many problems that need to be addressed. In this research work, we presented 1 an Attacked Packet Detection Algorithm (APDA), which is an algorithm that may detect potential DOS (Denial-of-Service) assaults before those attacks are really confirmed. This improves VANET's security while simultaneously lowering processing costs

2) Paper Name : Wavelet Based Image-Text Fusion Algorithm for Encrypted Message Transmission"

Authors : fshan Mulla∗, Amol Baviskar†, Jaypal Baviskar‡ Mugdha Gulati § and Amruta Mhatre.

Description : Because of the rising requirement for secure network communication, the demand for robust algorithms has increased. To ensure the anonymity, authenticity, and integrity of the communications delivered, the algorithms must be extremely successful.We created a technique for sharing secret messages in
this study by encrypting them in coloured images processed with the Dwt algorithm (DWT). To use the essential properties of DWT and insert a text message in the removed sub-band, the method uses a revolutionary sub[1] band removal algorithm. The energy output of each band is used to guide the band minimization procedure. The proposed method ensures that only an authenticated receiver with the access key receives the text message. This method has been proved to contain both reliable data transmission and appropriate compression ratios. The algorithm is also thoroughly examined in this publication.

3) Paper Name : IoT DoS and DDoS Attack Detection using ResNe.

Authors : Faisal Hussain,Syed Ghazanfar Abbas, Muhammad Husnain, Ubaid U. Fayyaz, Farrukh Shahzad, Ghalib A. Shah

Description : IoT-related assaults are becoming more frequent and more severe as the number of connected devices grows. Threats to the Internet of Things (IoT) networks have been detected as denial of service (DoS) and distributed denial of service (DDoS) (DDoS). Traditional security solutions, such as firewalls and intrusion detection systems, are unable to detect complex DoS and DDoS attacks because they filter normal and attack traffic based on established, static rules. Artificial intelligence (AI)-based technologies can make these solutions more dependable and efficient. Recent advances in image processing have made deep learning models such as convolutional neural networks increasingly prominent. With the use of convolutional neural networks (CNNs), network traffic information can be shown in order to better detect DDoS and DoS attacks. This led us to create an image-to- image conversion mechanism and use the images to train ResNet, a cutting-edge CNN model. For DoS and DDoS detection accuracy of 99.99 percent, the provided approach was the best. Additional to that, it has an average precision of 87%, which is 9% higher than the current state-of-the-art in DoS and DDoS assault detection.

4) Paper Name: Event-triggered Switching-type Fault Detection and Isolation for Fuzzy Control Systems under DoS Attacks.

Authors : Xiang-Gui Guo, Xiao Fan, Jian-Liang Wang, and Ju H. Park.

Description : Researchers in this research examine the challenge of nonlinear networked control systems with memory adaptive event triggered systems being subjected to periodic denial-of-service (DoS) assaults, and they use fuzzy Takagi–Sugeno models with uncertain membership functions to simulate the nonlinear systems. It all starts with the development of a new, event-triggered method that saves time and energy in the communication process. Instead than relying on the most recent triggering data set, the threshold is adaptively adjusted based on a large number of previous sampling data sets. Second, a switching state-feedback controller is created and exponential stability is estimated while taking denial-of-service attacks and event-triggered mechanisms into account. In the meantime, a piecewise Lyapunov function is being used to construct the controller and the event-triggered mechanism simultaneously. After that, a system of switching T–S fuzzy observers is constructed to realize FDI in the face of DoS attacks. It is also introduced to address the issue of inconsistencies in the event-triggered mechanism's premise variables. Finally, the proposed FDI strategy is demonstrated through a series of simulated examples.

5) Paper Name : Thwarting DoS Attacks: A Framework for Detection based on Collective Anomalies and Clustering.

Authors : Mohiuddin Ahmed

Description : Information security must be a top priority for any firm that wishes to protect its intellectual property from increasingly sophisticated cyberattacks. A host, router, or even an entire network can be brought down by a denial-of-service (DoS) assault, in which an attacker sends an excessive number of connection or information requests to overload the target system. Systems of targeted companies can be rendered worthless in minutes and remain that way for days, incurring in substantial losses for the company. Several DoS attack toolkits are also freely available and simple to use. DoS attacks are likely to become more sophisticated as the Internet of Things (IoT) becomes more widespread. DoS detection systems are going to have a tough time scaling up in the future because of this. What if anomaly detection, which tries to locate anomalous data from a dataset and frequently uncovers new and distinct patterns, is to blame? There has been a lot of attention paid to anomaly detection in statistics and machine learning, often known as outlier, novelty, or deviation identification, or exception mining, It's unfortunate, but typical methodologies rely on the assumption that individual data instances are aberrant, which is incompatible with the characteristics of denial-of-service assaults, such as nearest neighbour, grouping, and statistics.

Problem Statement :

To determine the best method of detecting a DOS assault with a low false alarm rate, and comparing the various detection strategies.

CONCLUSION :

To address the difficulty of smart grid intrusion detection, this work proposes a machine learning-based smart grid DoS attack detection methodology. The method collects network communication data in real time between the smart metre and the data server. Using feature selection and PCA dimension reduction to select more representative [1] resentative features, the trained SVM classifier model is utilised to identify and detect DoS attacks. On the KDD99 dataset, the SVM classification model beats the Naive Bayesian Network and Decision Tree classification algorithms. This method offers a higher detection rate and classification accuracy, which can help to improve the security of the smart grid.

REFERNCES

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] Jianye Hao, 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 IEEE Transaction on system, Man and Cybernetics, Vol.40, No.1, January 2010.
[4] Jiaxuan Fei,Tao Zhang,Yuanyuan Ma,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 (INFOCOMWKSHPS), 2013 IEEE Conference on, Turin, Italy, Dec. 2014
[6] Mina Rahbari and Mohammad Ali Jabreil Jamali, "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] Mushtak Y. Gadkari , Nitin B. Sambre, "VANET: Routing Protocols, Security Issues and Simulation Tools," IOSR Journal of Computer Engineering, JulyAug. 2012
[9] Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, Aamir Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," Springer Science +Business Media, LLC 2010.
[10] Wikipedia "Vehicular Ad-Hoc Network" http://en.wikipedia.org/wiki/Vehiculard−hocnetworkthispagewasthispagewaslastmodi fiedon5January2013.