JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

SK

# DDOS ATTACK DETECTION

Prashant Shinde[1], Gauri Hegade[2], Siddhi Jagtap[3]Preeti Suryawanshi[4]

Department of E&TC, SKNCOE, SPPU, Pune

*Abstract*— A Distributed Denial of Service (DDoS) attack is an attempt to make a service unavailable by overwhelming the server with malicious traffic. DDoS attacks have become the most tedious and cumbersome issue in recent past. The number and magnitude of attacks have increased from few megabytes of data to 100s of terabytes of data these days. Due to the differences in the attack patterns or new types of attack, it is hard to detect these attacks effectively. In this paper, we devise new techniques for causing DDoS attacks and mitigation which are clearly shown to perform much better than the existing techniques. We also categorize DDoS attack techniques as well as the techniques used in their detection and thus attempt an extensive scoping of the DDoS problem. We also compare our attack module with a couple of tools available .

*Keywords*— DDos Attack Detection, Machine learning, Hyperplane SVM, Precision detection graphic.

## I. 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.

## II. LITERATURE SURVEY

**1.** Paper Name - Early Detection of DOS Attacks in VANET Using Attacked Packet Detection Algorithm (APDA)Year of Publication– 2019
Author - S. RoselinMary, M. Maheshwari, M. Thamaraiselvan

Description - The security of VANET (Vehicular Ad Hoc Networks) is crucial as their very existence relates to critical life threatening situations. VANET is a subtype of the MANET. In which the mobile nodes are all vehicles equipped with an On- Board Unit (OBU) that enable them to send and to receive messages to the other Nodes in the network. In addition to communication among the vehicles, VANET interface with communication points provided by on road infrastructure. Many of the Researchers have already proved about the securing safety messages. Moreover VANET face several security attacks. In existing VANET systems is using a detection algorithm to detect the attacks at the verification time in which delay overhead occurred. The various security threats are misbehaving nodes give false information, Sybil attacks, selfish driver attacks, and etc. In this paper we proposed an Attacked Packet Detection Algorithm (APDA) which is used to detect the DOS (Denial-ofService) attacks before the verification time. This minimizes the overhead delay for processing and enhances the security in VANET

**2.** Paper Name - IoT DoS and DDoS Attack Detection using ResNetYear of Publication - 2020
Author – Faisal Hussain,Syed Ghazanfar Abbas, Muhammad Husnain,Ubaid U. Fayyaz, Farrukh Shahzad,Ghalib A. Shah

Description – The network attacks are increasing both in frequency and intensity with the rapid growth of internet of things (IoT) devices. Recently, denial of service (DoS) and distributed denial of service (DDoS) attacks are reported as the most frequent attacks in IoT networks. The traditional security solutions like firewalls, intrusion detection systems, etc., are unable to detect the complex DoS and DDoS attacks since most of them filter the normal and attack traffic based upon the static predefined rules. However, these solutions can become reliable and effective when integrated with artificial intelligence (AI) based techniques. The proposed methodology accomplished 99.99 percent accuracy for detecting the DoS and DDoS incase of binary classification. Furthermore, the proposed methodology achieved 87 percent average precision for recognizingeleven types of DoS and DDoS attack patterns which is 9 percent higher as compared to the state-of-the-art

**3.** Paper Name - Mitigation and Detection Strategy of DoS Attack on Wireless Sensor Network Using Blocking Approachand Intrusion Detection System Year of Publication - 2020

Author – Faisal Mochamad Teguh Kurniawan, Setiadi Yazid Abdelrhman Mohammed, Iman Abuel Maaly Abdelrahman

Description - 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). Besides having many benefits, WSN has a disadvantage in its application where there is no builtin security system embedded in the sensor device due to limitations possessed by sensor nodes such as memory, processor, and battery. As a result, WSN is vulnerable to attacks, one of the main attacks on WSN is the DoS attack. DoS attacks aim to prevent users legitimate from using resources by reducing existing resources until the network resources are busy, the network becomes slow until finally off. So, we need to detect, mitigate DoS attacks that these attacks can be stopped. The blocking approach was successfully implemented on the WSN network when IDS detected a DoS attack. So, the method of blocking approach can be used as a mitigation of DoS attacks by blocking all packets sourced from the attacker

## III. METHODOLOGY

1) Data collection :- 1st of all we provide image dataset to the machine from kagal website. Dataset is of images of currency. We have to modify or prepare that dataset, for that next step is pre-processing.

2) Preprocessing :- In Pre-processing phase, in that removing the noisey and blur part of the dataset, and rescale, resizethe image dataset.

3) After preprocessing of dataset, next phase is trained that dataset. For that, dataset goes through feature extraction classification.

- Train the dataset :- In this process we train the dataset by following steps.

1) Feature extraction :- In Feature extraction extract the features like edges, size etc. from dataset. Extract the features for classifications. After Feature Extraction next step is segmentation.

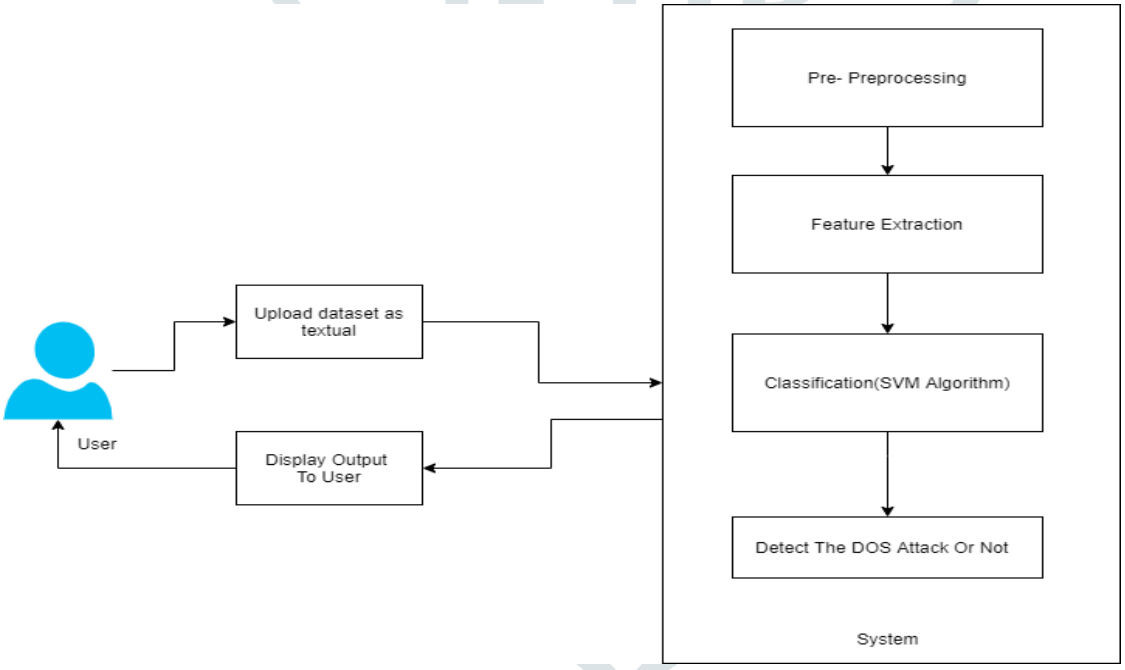


Fig1. System Design

2) Classification :- "Support Vector Machine" (SVM) is a supervised machine learning algorithm that can be used for both classification or regression challenges. However, it is mostly used in classification problems The SVM classifier is a frontier that best segregates the two classes (hyper-plane/ line). After all the training phase done Machine create model i.e. trained model. It is 80

- Testing :- Testing is 20We give input as image for testing. Then model can goes to testing phase and then provide theoutput to user. Output is to detect the currency is fake or not.

- 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 or regression challenges. However, it is mostly used in classificationproblems The SVM classifier is a frontier that best segregates the two classes (hyper-plane/ line)

IV. RESULTS AND DESCUSSION

The database generated by Snort was classified by machine learning algorithms Support Vector Machine, Random Forest and Naïve Bayes in weka tool. The confusion matrix was used to evaluate the classifiers and the results are shown in Table V. The overall accuracy was 99.7%, 97.6% and 98.0% of Support Vector Machine, Random Forest and Naïve Bayes respectively. The precision, recall and specificity are equally important because of the imbalanced data and should be put into consideration. Out of the three algorithms used SVM shows the better results in terms of accuracy, recall, precision, specificity and f measure closely followed by Random Forest.


Fig. Main Page


Fig . Registraition Page

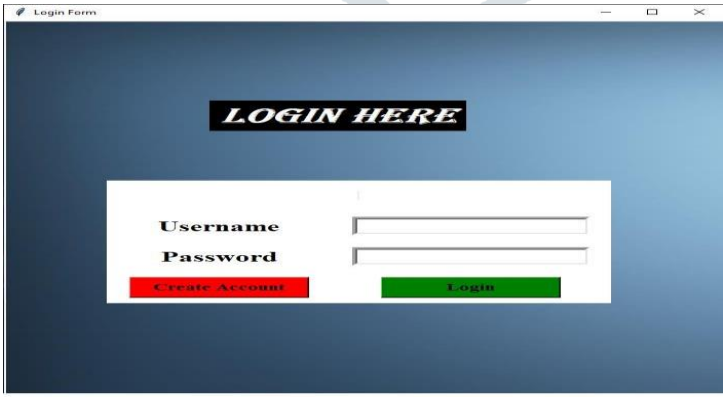


Fig . Login Page



Fig. Result PageV. 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 BayesianNetwork and Decision Tree classification algorithms on the KDD99dataset .This method has a greater detection rate and accuracy for classification, which can helpto improve the smart grid's security.

VI.ACKNOWLEDGMENT

We express our sincere gratitude towards the faculty members who makes this project phase II a successful . We would like to express our thanks to our guide Mrs. P.K.Suryavanshi for their whole hearted co-operation and valuable suggestions, technical guidance throughout the project work. Special thanks to our H.O.D. Dr. Ms. S.K.Jagtap for her kind official support and encouragement. We are also deeply thankful to our project coordinators Mr. P.S.Kokare and Ms. M.M.Sonkhaskar for their valuable guidance. Finally, we would like to thank all staff members and faculty members of E & TC Department who helped us directly or indirectly to complete this work successfully.

## VII. REFERENCES


1. Vidyaev I G, Ivashutenko A S, Samburskaya M A. Smart Grid Concept As AModern 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 GridBlackout 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.

4. Jiaxuan Fei,Tao Zhang,Yuanyuan Ma,Cheng Zhou. A DDoS attack detectionmethod for power grid industrial control system based on BF-DT-CUSUM al-gorithm[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 Work-shops (INFOCOM WKSHPS), 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 Vari-ations 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, July- Aug. 2012Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, Aamir Hassan, "Vehicular ad hoc networks (VANETS): status,results, and challenges," SpringerScience +Business Media, LLC 2010.

9. Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, Aamir Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," SpringerScience +Business Media, LLC 2010.