

Small rate DDoS Violence Documentation and Protection by SDN built on Machine Learning Technique

¹Shibi. M. S, ²Suresh A. T. K, ³Nisha M. D, ⁴P Ebby Darney

¹Lecturer, Computer Engineering, Government Polytechnic College, Neyyattinkara. Directorate of Technical Education Kerala

²Lecturer, Computer Engineering, Government Polytechnic College, Vechoochira. Directorate of Technical Education, Kerala.

³Lecturer in Computer Technology, Government Women's Polytechnic College, Thiruvananthapuram

⁴Professor & Head, EEE, Raja Rajeswari College of Engineering Bangalore

⁴Research Supervisors, LIPS Research Foundation India

Abstract- Application defined networking architectural framework eases the life of the network administrators by isolating the data plane from the control plane. This facilitates easy configuration of the network, provides a programmable interface for developing applications related to management, security, logging etc. and the centralized logical controller gives more control over the entire network, which has the total visibility of the network. These advantages of SDN also expose the network to the vulnerabilities and therefore the impact of the attacks are much severe in comparison to standard networks, where the network devices in itself provided protection against different attacks and limits the scope of the safety threats. During this paper, we explore various attacks which will be launched on SDN controller at different layers and secure the SDN against threats. A Distributed Denial of Service (DDoS) Violence may be a DoS Violence utilizing multiple distributed Violence sources. Increase in randomness causes decrease in vulnerabilities of system. To extenuate this threat, this paper proposes to use different techniques for the central control of SDN for various Violence detection and introduces an answer that's effective and light-weight in terms of the resources that it uses. More precisely, this project shows how DDoS attacks can exhaust controller resources and provides an answer to detect such attacks supported the variation of the destination IP address. Gridlock characteristics through statistical flow table information and uses the support vector machines (SVM) method to identify the Violence gridlock. The experiment is conducted using KDD99 dataset.

Keywords- Application Defined Network (SDN), Distributed Denial of Service (DDoS), Machine Learning (ML), Support Vector Machines (SVM), security threats.

I. INTRODUCTION

Security has been regarded as the dominant barrier of the development of Internet service. Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attacks are the main methods to destroy availability of Internet service. DDoS attacks refer to the use of client/server technology to combine multiple computers as an Violence platform to launch a DoS Violence on one or more targets. Thus, the power of DoS attacks mainly used IDC is multiplied to forge source IP attacks. DDoS attacks are common in these years. These Violence incidents incurred heavy downtime, business losses, to name but a few. There are some noted Violence examples. In 2015, Lizard Squad attacked cloud-based game services of

Microsoft and Sony, leading to the decline of QoS on Christmas day. Cloud service provider, Rackspace, was targeted by a massive amount of DDoS Violence on its servers. Amazon EC2 cloud servers were attacked by a massive DDoS attack [1]. Thus, strengthening DDoS Violence detection and defense is an urgent task. The security of the campus network is paid much attention by the government [2]. Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) flooding attacks are the main methods to destroy availability of campus network. In traditional networks, hardware and application applications based on DDoS Violence detection and defense are expensive and difficult to deploy [3]. Application Defined Network (SDN) has attracted great interests as a new paradigm in the network. In SDN, the control planes and data planes are decoupled. Network intelligence and Network state are logically centralized. The underlying SDN infrastructure is abstracted from the specific applications. SDN can improve network manageability, scalability, controllability and dynamism [4]. Thus, SDN can dynamically modify forwarding rules to defend DDoS gridlock and improve network security. To mitigate the DDoS attacks and reduce the restrictions, gridlock classification needs to be performed to identify Violence gridlock. Machine learning technology based network gridlock classification

has become a hot topic and has achieved encouraging results in intrusion detection [5]. In this paper, we propose an SDN framework to identify and defend DDoS attacks based on machine learning for the campus network. This system framework consists of 2 phases which are network gridlock collection module, DDoS Violence identification module. Gridlock collection module extracts network gridlock characteristics to prepare for gridlock identification in the system. The Support Vector Machine (SVM) is applied to identify the DDoS gridlock. The Ryu controller [6] is employed to build the flow table decision delivery module.

The objective of this paper is as follows:

- Combining the characteristics of the SDN network, we propose network features that are easy to extract in the SDN environment.
- Abstracting the DDoS Violence detection problem as an Violence gridlock classification problem and using SVM to establish a classification detection model.
- Designing and implementing the Violence detection and prevention framework using Ryu controllers.

II. PROBLEM STATEMENT

With a listing of different security concerns in Application Defined Networks, one of the main security threats we are concentrating upon in this research work is on Distributed Denial-Of-Service. When a large number of packets are forwarded to a network device with an intent to either stop the service or decrease the performance then such attacks are termed as Distributed Denial-of-service attacks. In DDoS attacks, an outsized number of packets are sent to a number or a gaggle of hosts during a network. If the source addresses of the incoming packets are spoofed, which they typically are, the switch won't find a match and has got to forward the packet to the controller. The collection of legitimate and therefore the DDoS spoofed packets can bind the resources of the controller into continuous processing that exhausts them. This will ultimately causes controller to be unreachable for the newly arrived valid packets and may crash the controller causing the loss of the SDN architecture. Even if there is another one a backup controller in the SDN, it has to face the same issue as the previous one.

This kind of attacks can be detected at an early stage by monitoring few hundreds of packets based on the entropy changes. The early detection of DDOS Violence prevents the controller going down. The term "early" is subjected to tolerance level and gridlock being handled by the controller [7] [8]. If detection happens early say first few hundreds of packet then, the impact of flooding of malicious packets can be controlled significantly. The early detection mechanism must be of light weight and should have a high response time. The high response time saves the controller in the period of Violence to regain the control by terminating the DDOS attack.

III. MOTIVATION

The main objective of this research is detecting a DDoS Violence in its early stages using various machine learning techniques. The term early depends on the network itself. Since the controller application are often run on a laptop or a strong desktop, the term early would depend upon the tolerance of the device and gridlock properties. However, if the detection happens within the first few hundred packets, the mitigation is applied before the controller is totally swamped with the massive number of malicious packets.

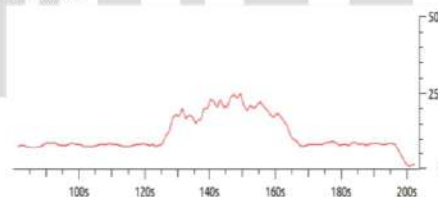


Figure 1 Sample Violence on the controller

Figure 1 shows a high DDoS Violence on the SDN controller where the normal incoming packet rate is around 100 packets per second. When the Violence happens, the speed rises sharply to, approximately, 250 packets per second. The simulated DDoS Violence was directed to a SDN controller that's connected to a network with 64 hosts and nine switches. This Violence lasted for 40 seconds and sent over 500 packets with spoofed source addresses all destined for one host over nodes. For the aim of this research, all packets will have spoofed IP addresses. Because of this way, the switches do not have a match and all the packets are sent to the controller and works effectively. To accomplish this goal, a fast and effective method is needed that works within the controller. One of the functions of the controller is collecting statistic.

In this study, this attribute is used for adding another set of statistics collection to the controller; various destination IP addresses.

I. DDOS VIOLENCE IDENTIFICATION AND DEFENSE FRAMEWORK

A. Scenario Assumptions

Figure 2 shows the simplified illustration of the system architecture in the hypothetical scenario. The system is composed of a web server, an SDN controller and the DDoS Violence identification module running on the controller and two Open Flow switches. In addition, there are some normal visitors and some attackers. In order to better describe the DDoS Violence identification and defense framework, we give the following assumptions about the above system architecture.

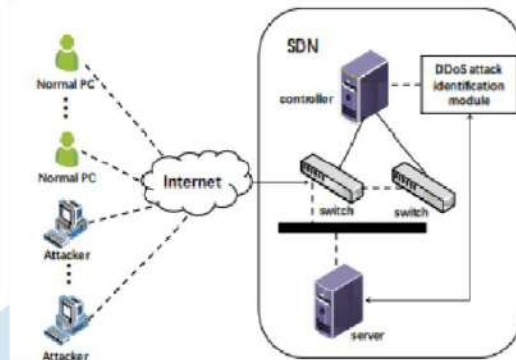


Figure 2 The system architecture in the hypothetical scenario

- ❖ All attackers come from external networks.
- ❖ DDoS attacks are HTTP flood attacks against web servers.
- ❖ Web server is used to simulate the website of a university.

B. The detection process

The detection process is divided into two steps. Firstly, the IP entropy is detected to determine whether a DDoS Violence has been generated. If the IP entropy detection result is a DDoS attack, the system sets the flag to 1. After that, the gridlock collection module performs feature extraction based on the flow table entries and the message packets when the flag is 1. Then the DDoS Violence detection is applied to perform DDoS recognition. When a DDoS Violence is identified the controller sends out the flow table to filter this packet. The detection process is done.

C. The DDoS Violence identification and defense framework

According to the above DDoS Violence detection process, we propose a DDoS Violence identification and defense framework showed in Figure 3. The framework consists of 3 parts which are gridlock collection, DDoS Violence identification and flow table delivery. The sniffer is used to collect statistical information from the package-in message and flow tables then convert statistical information into a feature vector which the classifier can handle. Assuming that the originator of the Violence is all in the external network, the sniffer only needs to check the flow table of the switch1 connected to the external networks and the package-in message initiated by this switch. The Violence identification model passes the recognition result to the flow table delivery model. The flow table delivery model conducts the control strategy: The gridlock will be forwarded as usual unless it is dropped because of having the DDoS Violence packet.

II. THE DDOS GRIDLOCK IDENTIFICATION MODEL

A. Feature Extraction

When a packet arrives at the switch, if there is no matching rule in the flow entry, the switch will send a package-in message to the controller. After the controller receives the package-in message, it will design the forwarding rule through the internal decision and return flow table to the switch with the package-out message. After the switch updates the flow table, the packets are processed according to the matching rules. The gridlock statistics information can be obtained from the package- in message and flow table.

Combining the characteristics of the Open Flow, flow table, we extract 8 features based on the original data set features. Table1 depicts the features. All data packet features are collected and extracted by the sniffer.

Table 1 The description of features which we extract

Label	Description
count	In the past two seconds, the number of connections between the target hosts and the current connections is the same.
srv_count	In the past two seconds, the number of connections with the current connection has the same service.

same_srv_rate	In the past two seconds, the percentage of connections that have the same service as the current connection has the same service as the current connection.
dst_host_count	In the first 100 connections, the number of connections with the same target host is the same as the current connection.
dst_host_srv_count	In the first 100 connections, the number of connections that have the same target service as the current connection is the same as the current connection.
dst_host_same_src_port_rate	In the first 100 connections, the connection with the current connection has the same target host, the same service and the same port.
dst_host_syn_error_rate	In the first 100 connections, the percentage of SYN error connections is the same as the current connection with the same target host.
dst_host_syn_rej_rate	In the first 100 connections, the percentage of REJ error connections is the same as the current connection with the same target host.

B. Support Vector Machine based DDoS gridlock Identification Model

The real-time requirement of DDoS Violence detection is relatively high. Support Vector Machine (SVM) is a supervised learning method with associated learning algorithms that analyze data used for classification and regression analysis. In this study, the main goal is to classify each packet as an attacker or a normal one. Therefore, we select SVM to establish the DDoS Violence recognition model. SVM has a higher robustness than other machine learning algorithms. The gridlock classifier construction process is showed in figure3.

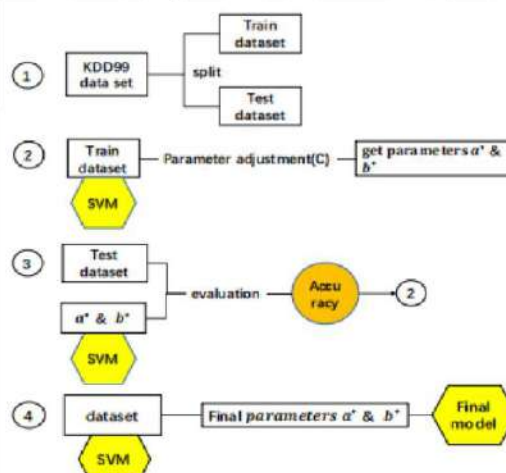


Figure 3 The gridlock classifier construction process

Firstly, the raw dataset is separated into train dataset and test dataset. Then the training dataset is used to build the DDoS Violence recognition model. And determining the best parameters through repeated tests.

The gridlock data is collected from the flow table based flow table entries. The gridlock dataset X has N gridlocks $X = \{x_1, x_2, x_3, \dots, x_n\}$, and x_i denotes a TCP connection that is made up of 8 features. These features denote the hostbased network gridlock features and time-based network gridlock features. We use -1 to represent "attacker packet" for the packet from the attacker pool, and we use 1 to represent "normal packet" for the packet from normal pc.

Step 1: we use SVM to solve the following the optimization problem. The linear kernel function $K(x,y)$ and the appropriate parameter C is selected to build the SVM model. The linear kernel function $K(x, y) = x^T y + c$ is used to map input space the to high-dimensional feature space. C is the regularization parameter, which must be greater than zero. We let the C is 1. $\alpha^* = (\alpha_1^*, \alpha_2^*, \dots, \alpha_N^*)^T$ is the LaGrange multiplier vector. It is the best solution of above.

$$\min \left(\frac{1}{2} \sum_{i=1}^N \sum_{j=1}^N \alpha_i \alpha_j y_i y_j K(x_i, x_j) - \sum_{i=1}^N \alpha_i \right) \quad (1)$$

$$\text{s. t } \sum_{i=1}^N \alpha_i y_i = 0 \quad (2)$$

$$0 \leq \alpha_i \leq C, i = 1, 2, \dots, N$$

$$\alpha^* = (\alpha_1^*, \alpha_2^*, \dots, \alpha_N^*)^T \quad (3)$$

Step 2: Select a positive component from $\alpha^* (0 \leq \alpha_j^*)$ to

calculate b^* which is the parameter of objective function:

$$b^* = y_j - \sum_{i=1}^N \alpha_i^* y_i K(x_i, x_j) \quad (4)$$

Step 3: Construct decision function.

$$f(x) = \text{sgn}(\sum_{i=1}^N \alpha_i^* y_i K(x_i, x_j) + b^*) \quad (5)$$

Finally, we get the decision function. The decision function

is used to decide how to forward packets. If the output of the function is -1, it is a DDoS Violence packet, otherwise, it is a normal packet.

IV. EXPERIMENT

A. Training and Test Dataset

To explain the effectiveness of the DDoS identification method based on SVM, We select the KDD99 dataset as training and test Dataset [9]. It is widely used in academic research, such as IDS and machine learning studies [10].

The KDD99 dataset includes five major categories, which are normal, DoS, Probe, R2L, U2R. It uses 41 features to describe a connection. The statistical analysis of the dataset is shown in table 2.

Where TP indicates the true positives, TN indicates negatives, FN indicates false negatives and FP indicates false positives. The experiment results are shown in table 4. that denotes the effectiveness of our model. We can get the accuracy is 0.998. It can be seen that our model for identifying DDoS attacks has a high recognition rate.

Table 2 KDD99 Data Set

Type	Number
Normal	12060
DoS	46074
Probe	849
R2L	3266
U2R	8
TOTAL	62206

We focus on the HTTP flood attacks in this paper. Thus, the data with DoS and Normal label are selected. And the TCP network connections are used as a dataset.

Table 3 Experiment data division

Dataset	Type of attribute	Total instances	Percent
All	Normal & attacks	(769670+1174241) 1842911	100%
Training	Normal & attacks	(576845+805442) 1382287	75%

Testing	Normal & attacks	(191827+268901)4 60727	25%
---------	------------------	---------------------------	-----

Then we divided the dataset into train dataset and test dataset after feature selection. Table3 describes the datasets in details respectively.

V. RELATED WORK

A. DDoS Defense Based on Machine Learning

Machine learning method based DDoS Violence detection are paid much attention. Most frequently used algorithms include Naive Bayes, Decision Tree, K-Nearest Neighbor (KNN) and Support Vector Machine. IAO Fu et al. propose an improved KNN algorithm to classify the Violence gridlock [11]. However, this method is suitable for offline detection. He Z et al. propose a DDoS Violence detection algorithm based on machine learning to prevent attacks on the source side in the cloud [12]. They evaluate nine machine learning algorithms and carefully compare their performance. They found that machine learning methods had a good effect in identifying DDoS attacks. They only did experiments about the effectiveness of the detection algorithm without proposing the way to defend against DDoS attacks.

Ahmed ME et al. propose a method for mitigating DNS Query-Based DDoS attacks based on DPMM(Dirichlet Process Mixture Model) [13]. Although the method has a good effect on mitigating DNS Query-Based DDoS attacks, the miscarriage rate is high.

Chuanhuang Li and Yan Wu et al. propose a DDoS Violence detection and defense method based on deep learning, and they apply it to OpenFlow-based SDN[14]. The result shows deep learning is a good method to detect DDoS attack.

B. Research on defense DDoS in SDN based Networks

Alshamrani A et al. propose a defense system for defeating DDoS attacks in SDN based networks[15]. The system unlike most of the existing ML-based approaches, the extensive range of prediction features are used to cover more types of DDoS attacks as well as to ensure better DDoS detection accuracy. However, the extracted features are based on the subset of valid features. The easy accessibility of the features is not actually considered in the SDN environment. Hong, Kiwon et al. propose an SDN-assisted DDoS Violence defense method that can detect and mitigate Slow HTTP DDoS attacks (SHDA), which relies on an SHDA in the SDN controller [16]. They use a proprietary controller so that the portability is poor.

Yang Xu and Yong Liu studied how to utilize SDN to detect DDoS attacks by capturing the flow volume feature as well as the flow rate asymmetry feature [17]. But their methods only consider one factor. We propose a framework to identify and defend DDoS attacks that based on SDN and machine learning for the campus network. This framework can be deployed online to identify the DDoS Violence and defense DDoS attack. Our framework enables online real-time detection of DDoS attacks and corresponding defense strategies. This framework design does not depend on other hardware and has good portability.

VI. CONCLUSION

Protecting the operating system of SDN (i.e. the controller) by detecting LR-DDoS attacks is the primary objective of this research. In this paper, we design an SDN framework to identify and defend against DDoS attacks. This framework consists of 2 parts which are gridlock collection module, Violence identification module and flow table delivery module. Gridlock collection module extracts the features to prepare for gridlock identification from the data. Currently, we have applied SVM to DDoS gridlock identification. The experiment results on the KDD99 dataset show the effectiveness. This classification model is deployed on the simulated SDN environment for campus network as a DDoS detection module. All gridlock is identified by this model. If Violence gridlock is identified, the controller will discard packets according to the predefined rule. If the packet is not attacked, the forwarding policy will be executed normally. In the future, we will optimize that the ratio of convection and single flow are used to judge whether the growth of network gridlock is DDoS. And we will improve the flow table delivery module and deploy the model to the SDN environment for the campus network.

VII. FUTURE WORK

One limitation that our method has is the detection of attacks when the entire network is being targeted by DDoS. It might slow down the entire detection process till the network gridlock cleared.

Having addressed the detection in one controller network, two more tasks to be done are:

i) Detection of Violence in a multi-controller SDN structure. ii) Mitigation of the attack.

In SDN, networks are connected to controllers and, several controllers might be connected to each other. Detecting an Violence in one of them could show the source of the Violence and make discovery of the source much easier.

This method requires an inter-controller communication that sends the threat alert to all the

controllers. Adding this communication process to SDN will be an extension to the current work and a topic for future work. Mitigation of Various in SDN will be next objective for this research. The first step of mitigation will be detection of the source or sources of the attack. Adding more specific statistics collection to the controller will enable it to monitor the packet flow rate at the switch level where Violence flows are directed to the controller. Then, more elaborate techniques can be used to pinpoint the malicious hosts. This is a very interesting future work that can be a baseline for any detection scheme in SDN structure.

REFERENCES:

1. Panchal, D., Chatterjee, P., Tyagi, M., & Singh, R.P. (Eds.). (2023). Optimization Methods for Engineering Problems (1st ed.). Apple Academic Press Chapter Chapter 13|13 pages Systematic Survey, Performance Evaluation, And Truth Flow Analysis Of Two Subsonic Wind Tunnels With Two-Hole Spherical Flow Analyzer By Akhila Rupesh, J. V. Muruga Lal Jeyan <http://dx.doi.org/10.1201/9781003300731-13>
2. Dhara, A. and Muruga Lal Jeyan, J.V. (2023), "Assessment on fuel economy of MoM transport aircraft using empirical approach: modelling with a case study", Aircraft Engineering and Aerospace Technology, Vol. 95 No. 6, pp. 912-925. <https://doi.org/10.1108/AEAT-03-2022-0081>
3. John B, A., Jeyan, J. V. M. L., NT, J., Kumar, A., Assessment of the Properties of Modified Pearl Millet Starch. *Starch*. 2022, 2200160. <https://doi.org/10.1002/star.202200160>
4. Systematic Survey, Performance Evaluation, and Truth Flow Analysis of Two Subsonic Wind Tunnels with Two-Hole Spherical Flow Analyzer - Akhila Rupesh and J. V. Muruga Lal Jeyan In Production Pub Date: October 2022 Hardback Price: \$159.95 USD | £124.00 Hard ISBN: 9781774911303 <https://www.appleacademicpress.com/optimization-methods-for-engineering-problems-/9781774911303>
5. K.S. Priyanka, J.V.M.L. Jeyan and S. Vihar. 2022. Investigation of Flow Separation Over NACA 24015 and 24021 Airfoils using Flow Injection Method, *Int. J. Vehicle Structures & Systems*, 14(3), 300-305. doi: 10.4273/ijvss.14.3.02.
6. P. S. RAMESH, J. V. MURUGA LAL JEYAN, *Comparative Analysis of Fixed-Wing, Rotary-Wing and Hybrid Mini Unmanned Aircraft Systems (UAS) from the Applications Perspective*, pp. 137-151, <https://doi.org/10.13111/2066-8201.2022.14.1.12>- INCAS BULLETIN, Volume 14, Issue 1/ 2022, pp. 137 – 151 Published: March 2022
7. P. S., R., & J. V. Muruga Lal, J. (2022). Hover performance analysis of coaxial Mini unmanned aerial vehicle for applications in mountain terrain. *Aviation*, 26(2), 112–123. <https://doi.org/10.3846/aviation.2022.16901> Published in Issue Jun 21, 2022
8. P.S., R. and J.V., M.L.J. (2022), "Evaluation of design criteria for mini unmanned aircraft systems (UAS) applications", *Aircraft Engineering and Aerospace Technology*, Vol. 94 No. 3, pp. 327-335. <https://doi.org/10.1108/AEAT-03-2021-0089> Issue publication date: 10 February 2022
9. Aishwarya Dhara and Jeyan Muruga Lal 2021 IOP Conf. Ser.: Earth Environ. Sci. 889 012068
10. <https://iopscience.iop.org/article/10.1088/1755-1315/889/1/012068/meta>
11. R. Sabari VIHAR, J. V. Muruga Lal JEYAN, K. Sai PRIYANKA, *Effect of camber on the flutter characteristics of different selected airfoils*, pp. 215-223, Published: September 2021 <https://doi.org/10.13111/2066-8201.2021.13.3.18>
12. Mathew, B. C., Sahu, S. K., Dutta, P., Savale, R., & JV, M. (2021). Albatross and Falcon inspired Bionic UAV: An Aerodynamic Analysis. *International Journal of Aviation, Aeronautics, and Aerospace*, 8(3). Retrieved from <https://commons.erau.edu/ijaaa/vol8/iss3/1>
13. Bilji C Mathew et al 2021 IOP Conf. Ser.: Earth Environ. Sci. 775 012002 <https://iopscience.iop.org/article/10.1088/1755-1315/775/1/012002> Evolutionary and Hereditary Traits of an Albatross and its Aerodynamic Optimality Bilji C Mathew, J V Muruga Lal Jeyan, Prantik Dutta and Rushikesh R. Savale Published under licence by IOP Publishing Ltd
14. R. S. Vihar, K. S. Priyanka and J. V. M. Lal Jeyan, "Design and analysis for the flutter behaviour of different selected wing plan forms computationally," 2020 International Conference on Interdisciplinary Cyber Physical Systems (ICPS), 2020, pp. 72-78, doi:10.1109/ICPS51508.2020.00018. <https://ieeexplore.ieee.org/document/9434601>
15. B. c. Mathew, K. S. Priyanka and J. V. M. Lal Jeyan, "Computational study on chamber morphing wing concept for efficient lift at various angle of attack," 2020 International Conference on Interdisciplinary Cyber Physical Systems (ICPS), 2020, pp. 68-71, doi: 10.1109/ICPS51508.2020.00020. <https://ieeexplore.ieee.org/document/9434576>
16. R. Balaji and M. L. Jeyan, "Performance analysis on varies bluff bodies at hypersonic speed," 2020 International Conference on Interdisciplinary Cyber Physical Systems (ICPS), 2020, pp. 62-67, doi: 10.1109/ICPS51508.2020.00017. <https://ieeexplore.ieee.org/document/9434600>

17. A. Rupesh, J. V. Muruga Lal Jeyan, , "Aerodynamic Design and Flow Analysis of Two Taping Spherical Flow Analyser and Mirror Edge Flow Analyser for Subsonic Wind Tunnel Calibration," 2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), Bhilai,India,2021,pp.1-6,doi:10.1109/ICAECT49130.2021.9392535, <https://ieeexplore.ieee.org/document/9392535>
18. Ramesh, P.S. and MurugaLalJeyan, J.V. (2021), "Terrain imperatives for Mini unmanned aircraft systems applications", International Journal of Intelligent Unmanned Systems, Vol. ahead-of-print No. ahead-of-print. <https://doi.org/10.1108/IJIUS-09-2020-0044>
19. Akhilarupesh, JV Muruga lal jeyan Experimental and Computational Evaluation of Five Hole Five Probe Flow Analyzer for Subsonic Wind Calibration - International Journal of Aviation, Aeronautics, and Aerospace , Published by Scholarly CommonsEmbry-Riddle Aeronautical University Volume 7 Issue 4 Article 3 2020
20. Ramesh PS, JV Muruga lal jeyan Mini Unmanned Aerial Systems (UAV) - A Review of theParameters for Classification of a Mini UAV - International Journal of Aviation,Aeronautics, and Aerospace , Published by Scholarly CommonsEmbry-Riddle Aeronautical University Volume 7 Issue 3 Article 5 2020
21. K.SaiPriyanka , J V MurugaLalJeyan*, R.SabariVihar. (2020). A Review on a Reassess Swot up on Airfoil Stall and Flow Separation Delay for a Range of Limitations Associated with Aerodynamics and Wing Profile. International Journal of Advanced Science and Technology, 29(06), 7659-7668.
22. R. SabariVihar, J. V. MurugaLalJeyan, K. SaiPriyanka. (2020). A Review on Aerodynamic Parameters, Methodologies and Suppression Techniques Explored in Aircraft Wing Flutter. International Journal of Advanced Science and Technology, 29(04), 3494
23. AkhilaRupesh, Dr. J V MurugaLalJeyan. (2020). Performance Evaluation of a Two Hole and Five Hole Flow Analyzer for Subsonic Flow. International Journal of Advanced Science and Technology, 29(05), 7512-7525
24. JV MurugalalJeyan Kavya S nair Amit Kumar Thakur Deepak Kumar Aerodynamic stability on piezoelectric multi Rotor UAV with numerical case learning European Journal of Molecular & Clinical Medicine, 2020, Volume 7, Issue 7, Pages 1558-1568 https://ejmcm.com/article_4636.html
25. GopinathShanmugaraj, J V MurugaLalJeyan, Vijay Kumar Singh "Effects of secondary injection on the performance of over expanded single expansion ramp nozzle" Journal of Physics: Conference Series, volume/ issue 1473 march 2020 012002, IOP Publishing
26. JV MurugaLalJeyan, Kavya S Nair and Krishna S Nair "Aerodynamics and flow pattern performance evaluation of offroad vehicle for various velocity range and angle of incidence" Journal of Physics: Conference Series, volume/ issue 1473 march 2020 012001, IOP Publishing
27. Abhinav Kumar, J V MurugalalJeyan "Electromagnetic Analysis on 2.5MJ High TemperatureSuperconducting Magnetic Energy Storage (SMES) Coil to be usedin Uninterruptible Power Applications "Materials Today: Proceedings 21 (2020) 1755–1762, 2214-7853© 2019 Elsevier LtdInternational Symposium on Functional Materials (ISFM-2018): Energy andBiomedical Application January 2020
28. J. V. MurugaLalJeyan , Abhinav Kumar, Anil Chamoli, Shahid Khan, ArfajAhamed Anwar, "Density of Kerosene AluminiumNanofluid used for Regenerative Cooling Applications of Thrust Chambers "International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-1S3, December 2019,
29. Abhinav Kumar, J V MurugalalJeyan "Feasibility Analysis on Cryogenic Properties of Supercritical Nitrogen to be used in the Cooling of Hg-Based High Temperature Superconductors for Electric Aircraft Propulsion "International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-1S3, December 2019,
30. Abhinav Kumar, Ashish Agrawal, J V MurugalalJeyan "A Numerical Model Comprising the Effect of Number of Turns on AC Losses in 2G HTS Coated Conductor at 77K using H-formulations "2019 IEEE 2nd International Conference on Power and Energy Applications , ISBN-978-1-7281-1596-2 , 29 August 2019,
31. J V MurugalalJeyan,Krishna S nair , Kavya S nair "The Low Speed Aerodynamic Analysis Of Segmental Wing Profile "International Journal of Mechanical and Production Engineering Research and Development (IJMPERD) ISSN (P): 2249–6890; ISSN (E): 2249–8001 Vol. 9, Issue 4, Aug 2019, 1303–1310
32. J V MurugalalJeyan, AkhilaRupesh "Methodical Assessment of River Periyar to Encounter Water Parameter Variation", International Journal of Engineering & Technology IJET , Vol.No.07, Issue 03, July 2018, PP 1056-1061, ISSN 2227-524X
33. J V MurugalalJeyan , Dr. M. Senthil Kumar, "Performance Evaluation of Yaw Meter With the Aid of Computational Fluid Dynamic", International Review of Mechanical Engineering (IREME). ISSN: 1970-8734, Vol No. 8,Issue 02 .

34. J V MurugalalJeyan ,Dr. M. Senthil Kumar , “Performance Evaluation for Multi-Hole Probe With the Aid of Artificial Neural Network” International Journal of Theoretical and Applied Information Technology (JTAIT). ISSN 1992-8645Vol No: 65 , Issue 3 , PP: 665 July 31, 2014
35. Suman Rana,Bhavin Soni,Dr. P. Ebby Darney,Jyothi NT, "EFFECTS OF T4 HORMONES ON HUMANBODY AND THEIR ANALYSIS", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.10, Issue 10, pp.d332-d339, October 2022,
36. Ashika Parveen¹, JV Muruga Lal Jeyan², Jyothi NT³ International Study on Application of Value Stream Mapping to Identify the Necessity of Lean System Implementation , International Journal of Scientific Research in Engineering and Management (IJSREM) Volume: 06 Issue: 09 | September - 2022 Impact Factor: 7.185 ISSN: 2582-3930
37. JV Muruga lal Jeyan, Jyothi NT Rashi Kaushik Systematic Review and Survey on Dominant Influence of Vedas and Ignorance Transpired in Space Science and Aviation", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.9, Issue 7, page no.b490-b493, July-2022,
38. JV Muruga lal Jeyan, Jyothi NT , Boopesh Raja, Rajarajan G "THEORY STRATEGY OF SUBSONIC WIND TUNNEL FOR LOW VELOCITY " , International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.9, Issue 6, page no.j572-j580, June-2022,
39. JV Muruga lal Jeyan, Jyothi NT, Reshmitha Shree, Bhawadharanee S, Rajarajan, THEORETICAL STUDY OF HYPERSONIC WIND TUNNEL TEST FACILITY IN INDIA " , International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.9, Issue 6, page no.j512-j518, June-2022,
40. JV Muruga lal Jeyan, Jyothi NT , V S Devika Thampuratty, B Nithin, Rajarajan, CONCEPT DESIGN AND DEVELOPMENT OF SUPERSONIC WIND TUNNEL " , International Journal of Emerging Technologies and Innovative Research (www.jetir.org | UGC and issn Approved), ISSN:2349-5162, Vol.9, Issue 6, page no. ppj209-j217, June-2022,
41. Muthu Venkatesh, Rajarajan G Jyothi NT JV Muruga Lal Jeyan "Systematic Survey of Wind Tunnel Test facility in India", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.9, Issue 6, page no.h830-h840, June-2022,
42. Ashika Parveen, JV Muruga Lal Jeyan, Jyothi NT "Investigation Of Lean Developments And The Study Of Lean Techniques Through Event Studies" Internation Journal for Science and Advance Research In Technology, 8(4)
43. P Gopala Krishnan, JV Muruga Lal Jeyan, Jyothi NT "Novel Evaluation Of Aircraft Data Structure Optimization Techniques And Opportunities" International Journal for Science and Advance Research In Technology, 8(4)
44. Suryansh Upadhyay, JV Muruga lal Jeyan, Jyothi NT Preliminary Study on Brain Computer Interface © August 2021| IJIRT | Volume 8 Issue 3 | ISSN: 2349-6002 IJIRT 152537 INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN TECHNOLOGY 720
45. Sruthi.s.kumar, Jyothi Nt , Jv Muruga lal jeyan . Computational Turbine Blade Analysis with Thermal Barrier Coating International Journal of Engineering Research and Applications www.ijera.com ISSN: 2248-9622, Vol. 12, Issue 4, (Series-I) April 2022, pp. 01-08, DOI: 10.9790/9622-1204010108
46. FUNDAMENTALS OF AIRCRAFT AND FLYING CONCEPT , How aircraft fly and its environment - Book author by Dr.JV Muruga Lal Jeyan JYOTHI NT LIPS Research April 29, 2022 ISBN-13 : 979-8813761799, ASIN:B09Z9VS4WN