An Overview OfMachine Learning's Uses In Recognizing Common Network Attacks

Hari Singh Rajpoot[1*], Ravindra Chauhan[2]

[1*,2]Department of Computer Science and Engineering, R D Engineering College, India

***Corresponding Author:** Hari Singh Rajpoot
*Email:-hs2rajpoot@gmail.com

Abstract- The number of intelligent devices has increased at an unprecedented rate over the last ten years, and the spread of intelligent machines has increased dramatically in recent years. In order to guarantee constant communication amongst networked IoT devices, computer networks are essential. Unfortunately, the significant rise in the usage of smart devices has opened the door for significant unethical behavior within networks. The primary network danger under investigation in this study is the "Low Rate/Slow Denial of Service (LDoS) attack," which seriously jeopardizes the integrity of the internet. Due to the fact that these assaults do not produce large amounts of bandwidth or abrupt increases in network activity, identifying their source is quite difficult. This study investigates the use of machine learning to improve the detection.

Keywords—LDoSattack,DDoSattack,Anomalydetection,ML,RL,IDS,Hyperparameteroptimization

1. Introduction

A growing number of technologies are emerging in this era of digitalization, but they must successfully affect "privacy" and "security" safeguards. The "Internet of Things" (IoT) increases its susceptibility to abuse. There are several security flaws in the Internet of Things space that might compromise end-user data and services. In the world of cutting-edge technology, "Denial of Service (DoS)" or "Distributed Denial of Service (DDoS)" attacks are among the most common and significant security risks.

"Denial-of-service" (DoS) attacks are a type of malicious cyberattack tactic where the attacker attempts to permanently or temporarily disrupt the service of an internet-connected host in order to prevent the targeted users from accessing the resources. The target machine is flooded in order to do this.

There is an increasing number of smart gadgets connecting to the internet, but many of them lack basic security features, leaving the internet vulnerable to many types of assaults. These smart devices are susceptible to distributed denial-of-service assaults, which are coordinated by botnets like Mirai.As a result, A significant threat to essential internet infrastructure. For example, picture a living area that has over 10 smart gadgets in it. It is possible to use these devices to perform denial-of-service attacks against the internet.

This paper thoroughly examines "low-rate denial-of-service" attacks, which are the most common type of network assault (LDoS). A stealthy network attack known as a "slow or low DoS" attack aims to degrade network service quality while staying undetectable or concealed.

1.1 Importanceofthestudy

Even if there are many security measures in place, we still live in an insecure period despite the fact that several techniques for identifying such a subtle assault have been proposed across a variety of domains and circumstances. When it comes to thwarting "LDoS" assaults, security procedures frequently fall short against security risks. It is crucial to have a system that supports robust security measures that can manage unpredictable network traffic and increasingly dynamic types of assaults.

The following is the outline for the remainder of the paper. The forms of low-rate DoS attacks are covered in Section 2. Section 3 discusses machine learning in relation to cyber security.

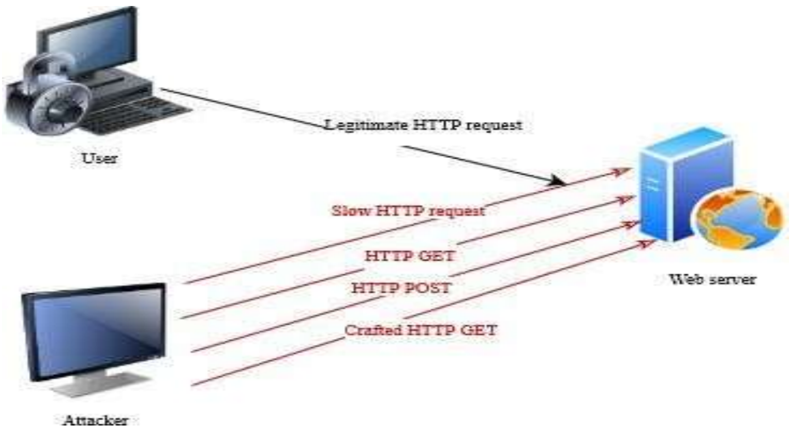

Figure1. Low-rateDoSattack Scenario

Section 4 clarifies related work. Methodology: ML-based detection techniques is covered in Section 5. The study's results and comments are presented in Section 6. Section 7 discusses challenges. Research work is concluded with future directions in Section 8.

2. Low rateDoS attacks

The term "low-rate denial of service (LDoS)" refers to an attack technique designed to interfere with or take down a target system by using techniques that gradually deplete its resources over a lengthy period of time, making it difficult to detect and counteract. Unlike classic DDoS assaults, which often include large volume and obvious patterns, LDoS attacks stream traffic slowly and persistently. A possible LDoS assault scenario is shown in Figure 1. These attacks frequently take advantage of holes in the target's protocols or resources, which enables the attacker to gradually deplete system resources.

There are large numbers ofdata packets intraditional ‘denial- The branch of artificial intelligence called "machine learning" tries to create models and algorithms, or "classifiers," that allow computers to learn and make decisions on their own without the need for human input. It is not necessary to use explicit programming. These days, machine learning has many applications. It is important for a number of computer network elements. A variety of machine learning applications in the field of cyber security are shown in Figure 2.

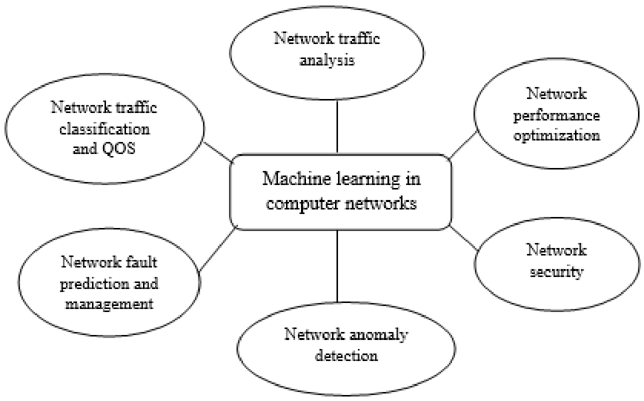

Figure2. Applicationsofmachinelearningwithintherealmofcybersecurity

Malicious traffic in intrusion detection systems (IDS) can be identified using machine learning techniques. An algorithm known as the machine learning classifier identifies patterns in the given data and categories the data according to these patterns. An ML classifier or model is trained with a dataset (a wide range of assaults) in Intrusion Detection Systems (IDS), and the model is tested withof-service’ attacks, resulting in anomalies within the network traffictodetectDoS-relatedtraffic.Conversely, LDoSattacks sustain consistently low average rates. and are intricately mixed within the network data stream. This leads to a reduction in the average network traffic, and attackers no longer require a sustained high attack rate. Instead, they frequently employ short bursts of traffic when targeting their victims [1]. The average packet rate during these bursts closely resembles 10–20% of the usual data traffic, which is relatively low, making it difficult to distinguish from regular networkactivity.Thiscomplicatesthedifferentiationbetween LDoS flows and regular data flows [2]. Its extended incubation period substantially reduces the throughput of its victims. Therefore, it is imperative to urgently devise novel methods and effective strategies for detecting and safeguarding against LDoS attacks [3].

3. MachineLearningin Cybersecurity

Table 1 shows different types of 'LDoS' attacks and attack target. Method of exploiting an attack is specified for each type of attack.

Table1. TypesofLDoSattacks

S.No	Attacktype	Target	Method
1	Slowread attack	Servers	Sendingrequeststhatare intentionallyslowtoread
2	RUDY	HTTP/H TTPs protocol s	SendHTTPrequestswithvery slow payload, keeping connectionsopenforextended periods and consuming server resourcesovertime.
3	Slowloris	HTTPserver	Senddataslowlyandconsume server resources.
4	HULK	Web applications	SendmanyHTTPGET/POST requests and keep the server busy.
5	Apache killer	Apache web servers	Crafted HTTP GET request withlong-rangeheadersand a serverconsumesmorememory.
6	Hash collision attack	SSL/ TLSor DNS	Exploits hash collision vulnerabilities in various protocols and sends crafted inputsthatgeneratemanyhash collisions.
7	Application layer protocol attacks	TCP,UDPor DNS	Exploitsvulnerabilitiesinthe protocols.

Table2. LiteratureReviewOnLdosAttack

Category	Method/ Proposal	Environment	Algorithm	Dataset	Area for improvement
Machine Learning	[3]	Feature based	XGBoost (Supervised)	Abilene	May result high false negative rate.
	[6]	Anomaly based	SVM, J48, RF, Random tree, REP tree, Multi-layer perseptron (SVM- derive significant features)	CIC DOS 2017	May result high false positive rate. Additional features may reduce false alarm.
	[10]	Feature based (Unsupervised)	OFA	Simulated in NS2 Test in Testbed	The model produces more accurate results when it is demonstrated with up-to-date datasets
	[12]	Feature based	SVM	Simulated in NS2 Test in Testbed	SVM is used for model training & extract feature parameters, Demonstration with other algorithms and multi-level classification can provide more accurate results.
	[14]	Feature based	Adaboost (Classification)	Simulated in NS2 Test in Testbed	Demonstrating the proposed model with up-to-date datasets is essential for enhancing detection accuracy.
Deep Learning	[7]	FFCNN	-	CIC DOS 2017 & CIC IDS 2017	Require to demonstrate with recent real time datasets in order to deal with dynamic & evolving attacks.
	[8]	Time-frequence analysis	-	LLDoS simulated in NS-3	To enhance model performance and address dynamic and evolving cyber threats, it is advisable to explore alternative evaluation metrics and showcase the model's effectiveness using real-time datasets.
Hybrid	[5]	DL + HPO	Sailfish		Model performance can be enhanced using other optimization algorithms and effectively lower false positive rate.
	[11]	ML (Traffic analysis) + DM	-	Public datasets	Multiclass classification can be employed to improve detection accuracy through various evaluation metrics.
	[13]	AI + Traditional	SVM	KDD99	The suggested Intrusion Detection System (IDS) did not rely solely on AI and always involved a trade-off between detection accuracy and detection speed. Need more efficient proactive mechanism for dynamic nature LDoS attacks.
Traditional	[15]	Mathematical model			Infeasible to implement this model in IOT environment which is resource-constrained.

4. Methodology: ML based detectionapproaches

Among many defense methods proposed for detecting LDoS attacks, machine learning-based methods address challenges posed by such a predominant network attack. It hassignificant usage in cyber security. AI-driven attack detection methods can be categorized as "signature-based" or"anomaly-based" [6]. In the "signature-based" technique, the known attacks' signature is compared withincomingnetwork flowto identify malicious network flow. Harun et al. [7] "In the anomaly- based approach,theincoming network flowiscontrasted with a benign flow of the model. If the flow's attributes deviate fromthose of the benign flow, it is categorized as malicious." The detection of 'LDoS' attacks can be categorized into two main approaches: feature-based detection and time-frequency domain detection [8]. Feature-based 'low denial of service attack detection' identifies and analyzes specific features or patterns in the traffic data to detect and mitigate slow DoS attacks. Time-frequency domain detection of LDoS attacks involves the examination of traffic data in both the time and frequency domains to detect the existence of 'low-rate DoS attacks.' This method offers a more in-depth insight into the attack attributes by capturing the time-dependent frequency aspects of network traffic [9]. These are low DoS attack detectioncategoriesused byresearchers, and these techniques may have the following drawbacks,

a. The present research has a conflict between detection rate and detection accuracy. Therefore, detection accuracy might compromise the detection rate.
b. Intensiverequirementofresources
c. High false positive rate(FPR) and High false negative rate (FNR)

d. Lackofproactiveandadaptive characteristics
e. Lack of detection methods for more dynamic and diverse LDoS attacks
f. Timecomplexity
g. Researchgapbetweendatasetandnewvulnerabilities
h. Overfittingandunderfittingofdata

5. ResultsandDiscussion

Machine learning classifiers are widely used in research for “anomaly detection.” The selection of an appropriate datasetis an essential step in this intrusion detection research. In this survey, two different datasets are considered, and its importance and insights are observed.

5.1 Detectionof‘DDoSattacks’usingNSL-KDDdataset (Machine learning classifiers)

The dataset contains 42 different features. The features are extracted according to 3 different attack types. First, “TCP Syn attack” the features extracted are,
“service, src_bytes, wrong_fragment, count, num_ compromised, srv_count, srv_serror_rate, serror_rate”
Second,“ICMPattack”thefeaturesextractedare,
“duration, src_bytes, wrong_fragment, count, urgent, num_compromised, srv_count”
Third,“UDPattack”thefeaturesextractedare,
“service, src_bytes, dst_bytes, wrong_fragment, count, num_compromised, srv_count, dst_host_srv_count, dst_host_diff_srv_rate”
The following observations are made from Figure 3. Observation 1: The detection accuracy of UDP flood attacksis low,whereas TCP and ICMP attack detection accuracy is almost 100%.

Observation2:Falsealarm(FPR)isgenerallyveryhighin network anomaly detection systems.
Observation3:Thefalsepositiverate(FPR)isrelatively higher for UDP attacks than the other two.

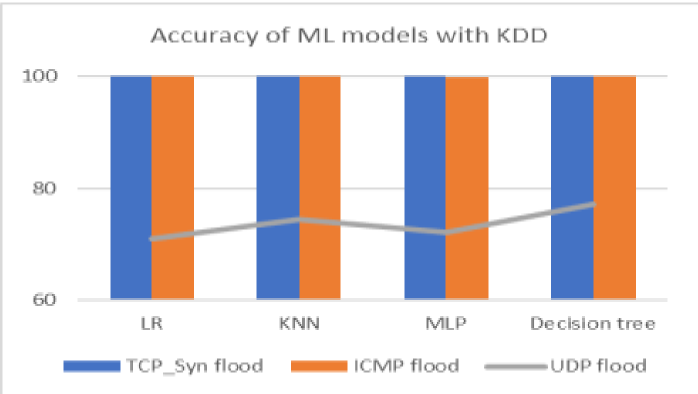

Figure3. Accuracyofmodelsfordifferentattackflows

Table 3 illustrates the confusion matrix representation for the UDP flood attack. The false positive rate is high for LR,MLP,andDT.Threeoutoffourclassifiersproducehigh FPR.

Table3. ConfusionmatrixforUDPattack

ConfusionMatrixforLR: [[28522005] [319 2835]]	ConfusionMatrixforKNN: [[4046 811] [1237 1917]]
ConfusionMatrixforMLP: [[26742183] [51 3103	ConfusionMatrixforDT: [[38341023] [801 2353]]

5.2 Detectionof‘DDoSattacks’usingNSL-KDDdataset (Reinforcement Learning)

The dataset contains 42 features, all used bythe RLsystemas an environment. Figure 4 shows the performance in terms of reward and loss in the RL model. Each episode in the RL model records the agent's states and actions from the start to the end state. Reward is something that an RL agent receives from its environment for its action (prediction). Loss is the difference(error) between predicted and actual values. Increasing the number of episodes leads to greater rewardsand diminished losses.

Observation: When the number of episodes is less (say, episode=2 or 5), the RL system clearly shows a spike in the loss signal and a drop in the reward signal.

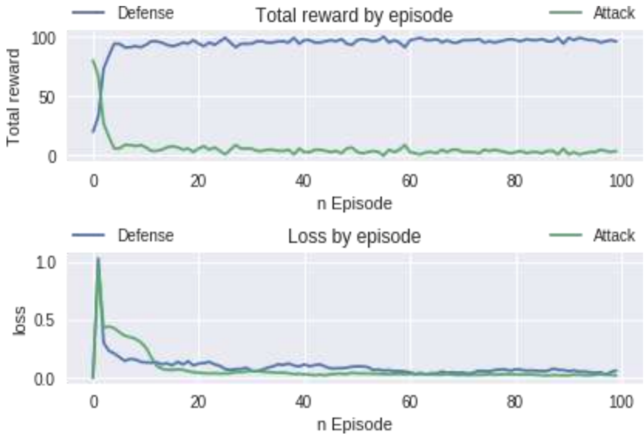

Figure4. PerformanceofRLmodelintermsofreward&loss

5.3 Multiclassclassificationofnetworktraffic(SDN dataset)

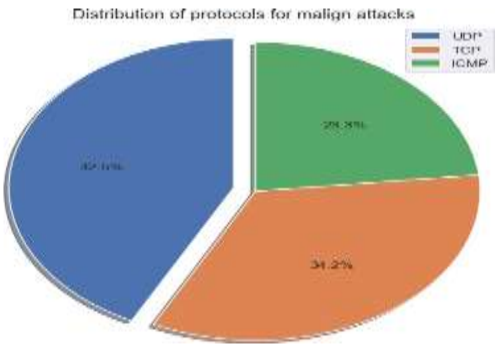

Figure5. Distributionstatisticsofprotocolsformaliciousactivity

SDN-specific (generated) datasets have been used for multi- class classification of network traffic data. There are 23 features in the dataset. All the features were considered and grouped into numerical, categorical, discrete-numerical, and continuous.

Figure 5 shows the protocol distribution statistics for maliciousactivityinthe network. Inthe statistics, UDP attack flows are relatively high. When the statistics in Figure 5 and the performance in Figure 3 are compared, identification of "DDoS attacks" exploited through UDP flood is challenging.

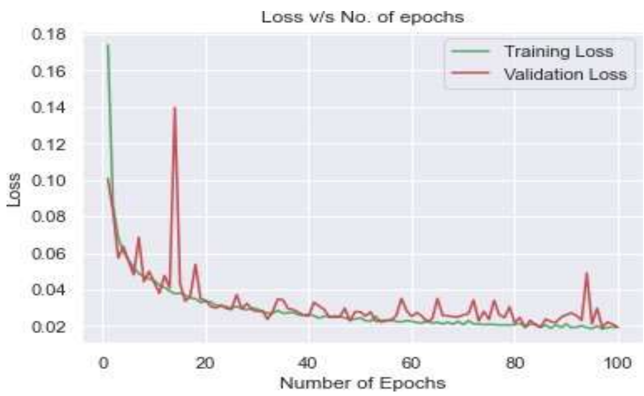

Figure6. PerformanceofMLmodelbasedonepochcount&Loss

Figure6andFigure7showtheperformance oftheMLmodel in terms of accuracy and loss. Epoch refers to the passing of training data through an algorithm. Each pass represents an epoch. Loss is high if there are few epochs, and accuracy increases with a hike in epochs.

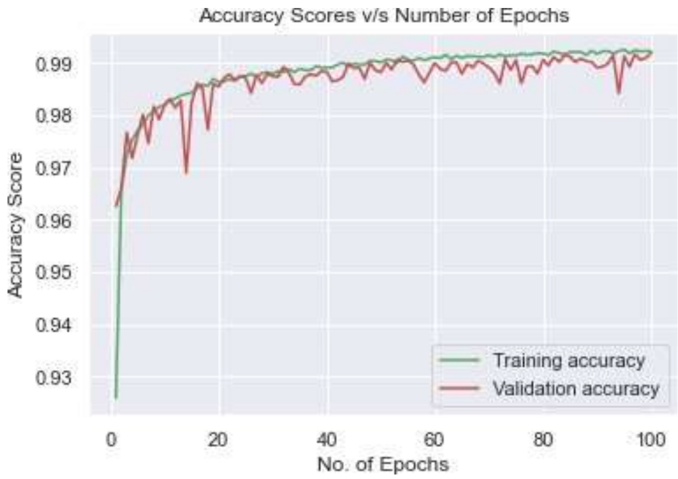

Figure7. PerformanceofMLmodelbasedonepochcount&Accuracy

Observation 1: Increasing the number of passes or epochs typically leads to better outcomes and enhanced performance. Observation 2: There is an observed stability in training loss and training accuracy, whereas validation loss and accuracy experienced a sudden minor fluctuation.

6. Conclusion

The study examined the identification of slow Denial of Service (DoS) attacks using both conventional and machine learning methods. Various attack detection methods were explored, including those rooted in machine learning, deep learning, anomaly detection, and traditional techniques. Limitations in these approaches were documented. Specifically, the current binary classification methods lead toa significant number of false alarms. Furthermore, integrating reinforcement learning into hybrid approaches can greatly improve the model's effectiveness, resulting in a robust Intrusion Detection and Prevention System (IDPS) capable of effectively mitigating a broader spectrum of complex and diverse attacks.

6.1 Futurescope

Reinforcement Learning (RL): Identifying ‘low-rate denial- of-service (LDoS)’ attacks usually entails dealing with subtle and gradual attack patterns that can readily circumvent conventionaldetectiontechniques.However,theattackcanbe effectively identified using Reinforcement Learning (RL) algorithms that still need to be focused in the research. In reinforcement learning (RL), The agent learns from feedback in terms of reward or punishment and adapts their behavior to maximize rewards in complex and dynamic environments. Since these RL models can be applied to complex and dynamic problems, it is most appropriate to use them to mitigate “LDoS attacks.”

Research towards a vital model variable is ongoing. These variablesareexternaltoa machinelearningmodelandarenot learning from the data during the model is trained. It has a significantroleindeterminingitsabilitytolearnand generalize from the data. With these characteristics, the detection rate of such dynamic attacks can be improvised. Either of methods may develop a hybrid model,

i. Through investigating such external parameters using reinforcement learning.
ii. Combining reinforcement learning and a feature-based method. Some feature-based methods are traffic analysis, protocol-specific analysis, and resource utilizationmonitoring.

References

[1] Tang D, Gao C, Li X, Liang W, Xiao S and Yang Q, “A Detection and Mitigation Scheme of LDoS Attacks via SDN Based on the FSS-RSR Algorithm,” IEEE Transactions on Network Science andEngineering, Vol.**10**, Issue.**4**, pp.**1952-1963**, **2023**, DOI: 10.1109/TNSE.2023.3236970.

[2] Zhan S, Tang D, Man J, Dai R and Wang X, “Low-Rate DoS Attacks Detection Based on MAF-ADM,” MDPI Sensors, Vol.**20**, Issue.**1**, pp.**189**, **2020**, https://doi.org/10.3390/s20010189.

[3] Liang Liu, Yue Yin, Zhijun Wu, Qingbo Pan and Meng Yue,“LDoS attack detection method based on traffic classification prediction,” IET information security, WILEY, Vol.**16**, Issue.**2**, pp.**86-96, 2022**, DOI: 10.1049/ise2.12046.

[4] Wu Zhijun, Li Wenjing, LiuLiang andYueMeng, “Low-RateDoS Attacks, Detection, Defense and Challenges: A Survey,” IEEE access, Vol.**8**, pp.**43920-43943, 2020**, DOI: 10.1109/ACCESS.2020.2976609.

[5] Wenwen Sun,Shaopeng Guan,Peng Wang,Qingyu Wu, “A hybrid deep learning model based low-rate DoS attack detection methodfor software defined network,” Emerging telecommunications technologies, Wiley, Vol.**33**, Issue.**5, 2022**, https://doi.org/10.1002/ett.4443.

[6] Harun Surej Ilango, Maode Ma and Rong Su, “A FeedForward– Convolutional Neural Network to Detect Low-Rate DoS in IoT,” Engineering applications of artificial intelligence, Elsevier,Vol.**114, 2022**,

https://doi.org/10.1016/j.engappai.2022.105059.

[7] Harun Surej Ilango, Maode Ma and Rong Su, "Low Rate DoS Attack Detection in IoT - SDN using Deep Learning," IEEE international conference on iThings, Australia, **2022**, DOI: 10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics53846.2021.00031

[8] Yazhi Liu, Ding Sun, Rundong Zhang and Wei Li, "A Method for Detecting LDoS Attacks in SDWSN Based on Compressed Hilbert–Huang Transform and Convolutional Neural Networks," MDPI Sensors, Vol.**23**, Issue.**10**, pp.**4745**, **2023**, https://doi.org/10.3390/s23104745.

[9] D. Tang, S. Wang, B. Liu, W. Jin and J. Zhang, "GASF-IPP: Detection and Mitigation of LDoS Attack in SDN," IEEE Transactions on Services Computing, pp.**1-12, 2023**, DOI: 10.1109/TSC.2023.3266757.

[10] Dharamveer, Samsher, D. B. Singh, A. K. Singh, N. Kumar, Solar Distiller Unit Loaded withNanofluid- A Short Review. Lecture Notes in Mechanical Engineering, Springer, Singapore, (2019) 241-247, https://doi.org/10.1007/978-981-13-6577-5_24.

[11] Shiv Kumar, Dharamveer Singh, "Energy And Exergy Analysis Of Active Solar Stills Using Compound Parabolic Concentrator" International Research Journal of Engineering and Technology Vols. 6, Issue 12, Dec 2019, ISSN (online) 2395-0056. https://www.irjet.net/archives/V6/i12/IRJET-V6I12327.pdf

[12] Dharamveer and Samsher, Comparative analyses energy matrices and enviro-economics for active and passive solar still, materialstoday: proceedings, 2020, https://doi.org/10.1016/j.matpr.2020.10.001

[13] Dharamveer, Samsher, Anil Kumar, Analytical study of N^{th} identical photovoltaic thermal (PVT) compound parabolic concentrator (CPC) active double slope solar distiller with helical coiled heat exchanger using C_uO Nanoparticles, Desalination and water treatment, 233 (2021) 30-51, https://doi. org/10.5004/dwt.2021.2 7526

[14] Dharamveer,Samsher, Anil Kumar, Performance analysis of N-identical PVT-CPC collectors an active single slope solar distiller with a helically coiled heat exchanger using CuO nanoparticles, Water supply, October 2021, https://doi.org/10.2166/ws.2021.348

[15] M. Kumar and D. Singh, Comparative analysis of single phase microchannel for heat flow Experimental and using CFD, International Journal of Research in Engineering and Science (IJRES), 10 (2022) 03, 44-58. https://www.ijres.org/papers/Volume-10/Issue-3/Ser-3/G10034458.pdf

[16] Subrit and D. Singh, Performance and thermal analysis of coal and waste cotton oil liquid obtained by pyrolysis fuel in diesel engine, International Journal of Research in Engineering and Science (IJRES), 10 (2022) 04, 23-31. https://www.ijres.org/papers/Volume-10/Issue-4/Ser-1/E10042331.pdf

[17] Rajesh Kumarand Dharamveer Singh, "Hygrothermal buckling response of laminatedcomposite plates with random material properties Micro-mechanical model," International Journal of Applied Mechanics and MaterialsVols. 110-116 pp 113-119, https://doi.org/10.4028/www.scientific.net/AMM.110-116.113

[18] Anubhav Kumar Anup, Dharamveer Singh "FEA Analysis of Refrigerator Compartment for Optimizing Thermal Efficiency" International Journal of Mechanical and Production Engineering Research and Development (IJMPERD) Vol. 10 (3), pp.3951-3972, 30 June 2020**.**

[19] Shiv Kumar, Dharamveer Singh, "Optimizing thermal behavior of compact heat exchanger" International Journal of Mechanical and Production Engineering Research and Development (IJMPERD) Vol. 10 (3), pp. 8113-8130, 30 June 2020**.**

[20] Xinmeng Li, Kai Zheng, Dan Tang, Zheng Qin, Zhiqing Zheng, Shihan Zhang, "LDoS Attack Detection Based on ASNNC-OFA Algorithm," IEEE wireless communications and networking conference, China, **2021**, DOI:10.1109/WCNC49053.2021.9417400

[21] Dan tang, Jingwen chen, Xiyin wang, Siqi zhang,Yudongyan, "A new detection method for LDoS attacks based on data mining," Future generation computer systems, Elsevier, Vol.**16**, Issue.**128**, pp.**73-87, 2022**, https://doi.org/10.1016/j.future.2021.09.039

[22] Wei shi, Dann tang, Sijia Zhan, Zheng Qin and Xiyin wang, "An approach for detecting LDoS attack based on cloud model," Forensics of computer science, Springer, Vol.**16**, Issue.166821, **2022**, https://doi.org/10.1007/s11704-022-0486-1.

[23] Naiji Zhang; Fehmi Jaafar; Yasir Malik, "Low-Rate DoS Attack Detection Using PSD Based Entropy and Machine Learning," 6th IEEE international conference on cyber security and cloud computing, Paris, France, pp.**59-62, 2019**, DOI 10.1109/CSCloud/EdgeCom.2019.00020.

[24] Dan tang, Liu tang, Rui dai, Jingwen chen, Xiong Li and Joel J.P.C.Rodrigues, "MF-Adaboost: LDoS attack detection based on multi-features and improved Adaboost,", Future generation computer systems, Elsevier, Vol.**106**, pp.**347-359, 2020**, https://doi.org/10.1016/j.future.2019.12.034.

[25] Jingtang Luo, Xiaolong Yang, Jin Wang, Jie Xu, Jian Sun and Keping Long, "On a Mathematical Model for Low-Rate Shrew," IEEE Transactions on Information Forensics and Security, Vol.**9**, Issue.**7**, pp.**1069-1083, 2014.**