ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)

https://doi.org/10.17559/TV-20210604113859
Original scientific paper

Dynamic Defense Mechanism for DoS Attacks in Wireless Environments Using Hybrid Intrusion Detection System and Statistical Approaches

Magudeeswaran PREMKUMAR*, Tharai Vinay Param SUNDARARAJAN, Gopalakrishnan MOHANBABU

Abstract: Security in wireless frameworks is a significant and difficult task because of the open environment. The Denial of Service (DoS) is as yet significant endeavour to make an online assistance inaccessible. The objective of this attack is to keep the authentic nodes from getting to the administrations. Intrusion detection systems assume an essential job in identifying DoS attacks that improve the performance of the system. However massive information from the system presents huge difficulties to the discovery of DoS attack, as the identification framework needs adaptable techniques for gathering, storing and processing a lot of information. In order to defeat these difficulties, this paper proposes Hybrid Intrusion Detection System (HIDS) framework dependent on different MLP strategies. In this article HIDS utilizes Naive Bayes (NB), irregular random forest (RF), decision tree (DT), multilayer perceptron (MLP), K-nearest neighbours (K-NN) and support vector machine (SVM) for better outcomes. The NSL-KDD dataset and UNSW-NB15 dataset are taken to examine the detection accuracy. The experiment results show that the proposed defence system is accomplished with high accuracy, high detection rate and low false alarm rate in both the datasets.

Keywords: denial-of-services; DoS defense; hybrid mechanism; intrusion detection; machine learning; wireless sensor networks

1 INTRODUCTION

The wireless sensor networks (WSNs) are comprised of several tiny sensors networked with low- yield wireless environments. Wireless sensor networks are used in many devices for healthcare tracking, habitat monitoring, military applications, battlefield monitoring, smart grid and so on. These networks are endowed with sensing, data pre processing and communication modules. In this thousands of sensors were composed with a network Id which is rapidly deployed to collect the critical information from hostile and unattended circumstances. A node is comprised of four components: one sensing unit, one transceiver, one processer and one battery. The first component is comprised of optical converters and sensors. The phenomenon detected by sensing system is transformed by A to D converters into full digital signals. The processing circuit is followed by a small storage unit and the sensor node communicates with the other nodes. The transceiver system acts as a connection between the node and the network. Li, Ni MH batteries or power-saving devices such as solar powered systems use an electrical unit. The main constraint of the network is the node having limited energy resources, minimal processing memory, safety risks, and the least communication and processing capacity. In a device, DOS attacks are propelled by remotely controlled, powerful, and narrowly disseminated botnet PCs of zombies. Many of the traffics or administration demands are at the same time or persistently sent to the objective framework. The objective framework gets unusable, reacts gradually, or crashes totally because of the attack [7].

The distinguishing proof of the first aggressors is hard for the protection strategies on the grounds that the aggressors have caricature IP addresses and secured inside zombies with the intention of heavily influenced by them [5].

The DoS attack detection based on the KNN classifier is shown in Fig. 1. The KNN algorithm is based on the iterative relocation of a dataset separated into k clusters. The average square distance between cluster centres and data points is reduced.

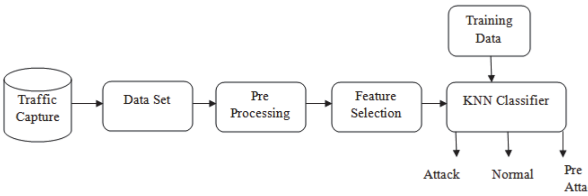


Figure 1 DoS attack detection based on KNN classifier

Before the last attacks are dispatched, the DoS attacks are manual and must perform a few steps, including identification of traded off devices to create zombies on the internet, port filtering, and sending malware. Parameters unique to the target can also be organised by the perpetrators, while the others can be tracked using mechanised instruments [12]. The FC resembles the attacks as far as numerous clients access a framework simultaneously. In FC there is an unusual and abrupt ascent in real rush hour gridlock as a result of extraordinary occasions. It is hard for guarded frameworks to recognize FC unusual traffic from DoS attacks. Some entrenched audit and reviews on DoS attacks and safeguard strategies are accessible in the writing, including [12]. The survey researches the guard techniques that are sent for distinguishing, alleviating, as well as forestalling DoS attacks. It orders DoS safeguard strategies as indicated by the class of defencelessness, the level of mechanization, effect, and elements. In addition, this survey incorporates typical testing sets and assessment strategies. The aim of this survey is to expand the scope and shape the course of DoS study. It leads to some open research issues and gives a few thoughts for future research.

2 RELATED WORKS

In the last few years, several detection and mitigation mechanisms have been recorded for DoS attacks aimed at service providers [16]. For DoS attack detection, many methods have been suggested so far. Some of the latest work in DoS attack detection is summarized in this section.

Song and Liu [10] are proposing an authentic detection method that employs dynamic K-Nearest Neighbours (K-

NN) algorithm. In their proposed approach, a Storm delivery system is used which considers three aspects: feedback in real-time, the sophistication of processing bulk information, and analytical method.

Hameed and Ali [3] suggest a counter base detection method for DoS attacks that performed better while targeting DoS flood attacks using Hadoop technology. However, their research is unable to achieve effective delays in processing.

The Singular Value Decomposition (SVD) based detection mechanism is proposed [11] to construct the multi classifiers. The SVD is helpful to determine system reliability when extended to realtime scenario. The reports of SVD indicate improvement in performance when compared with the previous algorithms.

Bovenzi et al. [20] are proposing a DoS attack mitigation system in a Hadoop cluster using a Genetic Algorithm (GA). This DoS detection incorporates different patterns to overcome the weakness in a static pattern matching approach. Their research shows that the number of nodes is proportional to GA conclusion time. Their outcome would be more valuable if they had tested their algorithm's accuracy.

"Rehman et al propose an IDS model for recurrent neural networks using a deep learning approach. To construct the model, they use the LSTM architecture and their evaluation results using the performance metrics demonstrate that the deep learning approach is successful for IDS", [17].

The DNN is the well-known Network Intrusion Detection (NIDS) deep learning models that are tested by Green et al [16]. Both LSTM and Autoencoder are the basis of the NIDS and their reviews rely on the algorithm's consistency and precision. It claims that the coder can attain 98.9 percent accuracy, while only 79.2 percent accuracy is attained by the LSTM model.

"Deep learning is computationally more expensive and is expected to outperform conventional learning algorithms", [2]. It was proposed in [5] that computation is one way of minimising latency in DNNs. Conversely, it is also a daunting job to assess maximum parallelism in DNNs.

The proposed article incorporates advantages of the fuzzy system to construct classification models in a distributed environment, while providing reliable and efficient isolation of DoS attacks. Based on the selected machine learning algorithm the detection rate ability is limited and proposed method dynamically select the method using fuzzy.

3 HYBRID IDS FOR DOS DETECTION

The proposed framework is shown in Fig. 2. The framework consists of distributed system, different classification algorithms and fuzzy logic. To distinguish traffic packets, classification algorithms are used to locate DoS attacks from regular traffic. To facilitate the execution of these classification algorithms, we implemented a distributed framework using spark. The fuzzy logic approach is used to provide the intended classification algorithm to manage the process with a dyamic collection. Defense framework technique begins at the client side and data are compared with database after some advancement. In this event that if the data id not attacked, it continue to the agent side. Finally, if data is interpreted as natural, it goes to the server.

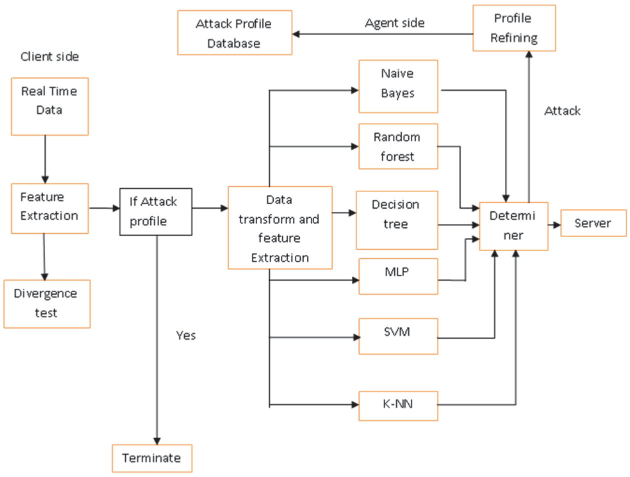
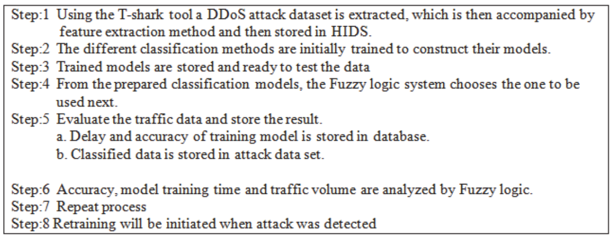


Figure 2 Hybrid IDS framework for DoS detection


Step:1 Using the T-shark tool a DDoS attack dataset is extracted, which is then accompanied by feature extraction method and then stored in HIDS.
Step:2 The different classification methods are initially trained to construct their models.
Step:3 Trained models are stored and ready to test the data
Step:4 From the prepared classification models, the Fuzzy logic system chooses the one to be used next.
Step:5 Evaluate the traffic data and store the result.
a. Delay and accuracy of training model is stored in database.
b. Classified data is stored in attack data set.

Step:6 Accuracy, model training time and traffic volume are analyzed by Fuzzy logic.
Step:7 Repeat process
Step:8 Retraining will be initiated when attack was detected

Figure 3 Framework workflow

According to AI algorithms, the detection of DoS attacks involves Artificial Neural Network (ANN) [1], Fuzzy Sets (FS) [2] and Genetic Algorithm (GA) [3]. The ANN uses the unsupervised learning to detect the attacks more effectively. In case of huge and complex networks, the above methods will not be scaled easily. The traditional machine learning (ML) approaches are employed to detect the attacks such as Decision Tree (DT) [3], Support Vector Machine (SVM) [9], Logistic Regression [2], Naive Bayes (NB) [3] etc.

Computational complexity, a qualitative metric, can indicate the difficulties involved with the development and overhead of a novel system. Its utility comes from its usage in comparing different techniques. According to [12], a type of network should be utilized that has features such as research functionality, extensibility, fidelity, repeatability, and programmability.

3.1 Naive Bayes Algorithm

It is extensively used in numerous classification applications [3]. Naive Bayes provides better accuracy compared to other algorithms. But it requires some features as it relies on the principle of independence of attributes. The posterior probability $P(h|D)$ of the classification is given by the Eq. (1).

$$P(h|D)=\frac{P(D|h)P(h)}{P(D)} \tag{1}$$

where $P(h \mid D)$ represents predictor probability given class, $P(h)$ is prior class probability, and $P(D)$ is the predictor's prior probability. In our data set, binomial model is used to segregate the attacker and normal node. For this the Bernoulli distribution is selected from other distributions like Gaussian, Multinomial, etc.

3.2 Random Forest Algorithm (RF)

"The RF algorithm is specifically proposed to have high prediction accuracy by integrating a large number of decision trees", [7]. The training processes are re-sampling, feature selection, tree bagging and DT growing. The RF algorithm is an ensemble of K trees $T_1(X), T_2(X), ..., T_K(X)$, where $X = X_1, X_2, ..., X_1$ is 1 dimension input vectors. The resulting ensemble produces K outputs $\psi_1 = T_1(X), \psi_2 = T_2(X), ... \psi_K = T_K(X)$. The training ψ can be obtained from regression trees by considering the mean prediction results will be denoted as

$$\Phi = \frac{1}{\tau}\sum_{\alpha=1}^{\tau} f_\alpha(x') \tag{2}$$

where τ represents tree bagging time and f_α denotes regression tree.

3.3 Decision Tree (DT)

Based on supervised learning, the decision tree builds the model in order to estimate the output from the previously learned attribute. In certain implementations, the decision tree is commonly used [8]. "The characteristics of DT in the training dataset affect the predictive accuracy, as the number of characteristics increases and the predictive accuracy decreases", [4]. Two variants are used to construct to determine the correct split in each stage. The Entropy in the data set X is given by

$$H(X) = \sum_{x=1}^{\varsigma} -f_x \log(f_x) \tag{3}$$

The Gini impurity is fluctuation entropy the calculation from previous to after port X is cleaved on an aspect.

$$G = \sum_{x=1}^{\varsigma} f_x(1 - f_x) \tag{4}$$

where f_x denotes x^{th} label frequency at a given node and ζ is unique labels.

3.4 Multilayer Perceptrons (MLP)

The MLP is a dynamic attack detection using the concept of feature selection and feedback. In this, original features initially determine the number of input neurons that will be modified during the iteration process of feature selection. The logistic sigmoid function is defined as

$$P(\alpha) = \frac{1}{1 + \exp(-\alpha)} \tag{5}$$

The model's output layer has a single neuron. The outcome of the MLP is according to conditional probability of attack and normal nodes. Given a training data set consisting of input vectors along with the related target vectors. The cross-entropy function is

$$H = -\frac{1}{N}\sum_{n=1}^{N}\left[\tau_1 \ln y_1 + (1 - \tau_n)\ln(1 - y_n)\right] \tag{6}$$

3.5 SVM Classification

In different applications a non-linear classifier gives better accuracy. The essential standard of SVM is finding the ideal straight hyperplane in the segment space that maximally withdraws the two objective classes [9]. In this the SVM classifier is built by Gaussian kernel which is denoted as

$$\Phi(x_i, x_j) = \exp\left(-\frac{\left\|x_i - x_j\right\|^2}{2\sigma}\right) \tag{7}$$

σ signifies width of the capacity. The SVM classifier is developed by picking Gaussian kernel and its parameters. The hyper plane margin that is parameters are identified by the SVM training which is denoted as hyper parameters.

3.6 K-Nearest Neighbors

This algorithm is based on the iterative relocation of a dataset separated into k clusters. The average square distance between cluster centres and data points is reduced. The function is specified as

$$D = \sum_{i=1}^{k}\sum_{x \in C_i}\sum_{m=1}^{l}\left\|W_m\left(C_{mi} - x_m\right)\right\|^2 \tag{8}$$

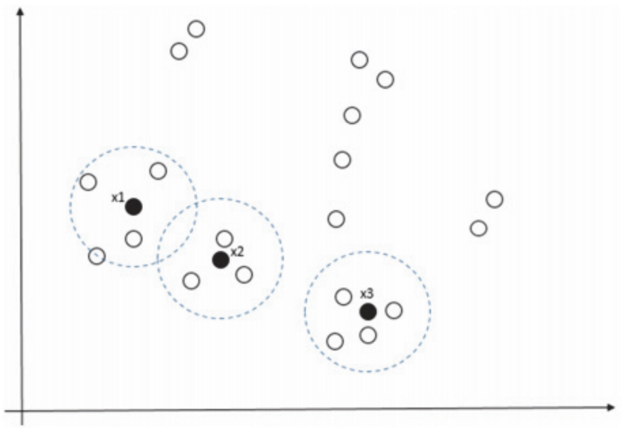


Figure 4 Feature selection in KNN classifier

where X denotes the dataset, center of each cluster is represented as C_i and the W represents weight factor. The algorithm uses a minimal number of labelled data to restrict the collection of initial centre points in order to boost classification accuracy.

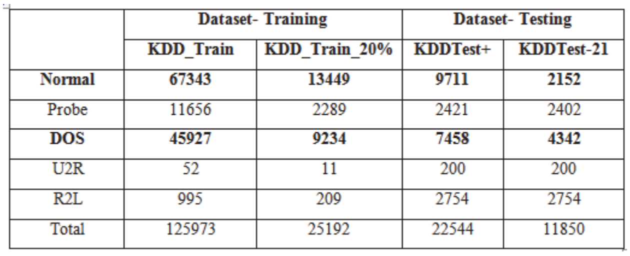
4 EXPERIMENTAL SETUP AND DISCUSSIONS

Presently two datasets, to be specific NSL-KDD and UNSW-NB15 are acquainted with identify the attacks in the system. Here the test settings are offered to approve the exhibition of the proposed hybrid IDS framework. Additionally the hybrid IDS is correlation made with some significant parameters.

4.1 NSL-KDD Dataset

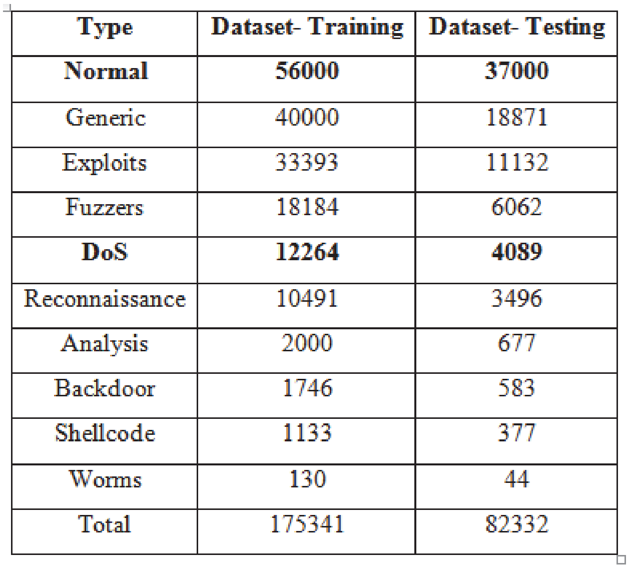
The NSL-KDD is one of the worldwide accepted databases for detecting the attacks in arrangements. "KDDTrain and KDDTrain_20% are the two sets for preparing and KDDTest+ and KDDTest-21 are testing sets which incorporate 41 highlights. Right now the system situations like typical, output to discover known vulnerabilities (Probing), DoS, U2R and R2L which is shown in Tab. 1", [3].

Table 1 Evaluation Parameters



	Dataset- Training		Dataset- Testing	
	KDD_Train	KDD_Train_20%	KDDTest+	KDDTest-21
Normal	**67343**	**13449**	**9711**	**2152**
Probe	11656	2289	2421	2402
DOS	**45927**	**9234**	**7458**	**4342**
U2R	52	11	200	200
R2L	995	209	2754	2754
Total	125973	25192	22544	11850

Table 2 UNSW-NB15 dataset details



Type	Dataset- Training	Dataset- Testing
Normal	**56000**	**37000**
Generic	40000	18871
Exploits	33393	11132
Fuzzers	18184	6062
DoS	**12264**	**4089**
Reconnaissance	10491	3496
Analysis	2000	677
Backdoor	1746	583
Shellcode	1133	377
Worms	130	44
Total	175341	82332

4.2 UNSW-NB15 Dataset

The UNSW-NB15 using the IXIA Perfect Storm tool is proposed by Moustafa and Slay in Cyber Range Lab of the ACCS. It is entirely different from NSL-KDD that reflects the complex and huge threat to environment. This new data set has 49 features and it develops more categories of attacks. The some standard attack categories in the current scenario as shown in Tab. 2.

4.3 Evaluation Metrics

The above hybrid technique evaluation is based on the classification of DOS attack from normal network. Based on correct or incorrect classification the represented as True positive ($True_{pos}$), True Negative ($True_{neg}$), False Positive ($False_{pos}$) and False negative ($False_{neg}$).

The accuracy defines how the algorithm identifies the DOS attacks from normal nodes in the dataset perfectly which is represented as

$$Accuracy = \frac{True_{pos} + True_{neg}}{True_{pos} + True_{neg} + False_{pos} + False_{neg}} \tag{9}$$

The detection rate is ratio of the algorithm identifies the DOS attacks from normal nodes in the dataset correctly which is represented as

$$Detection\ rate = \frac{True_{pos}}{True_{pos} + False_{neg}} \tag{10}$$

The False Alarm Rate (FAR) is defined as the ratio that the nodes incorrectly recognized as the attacks. It can be denoted as

$$FAR = \frac{False_{pos}}{True_{neg} + False_{pos}} \tag{11}$$

5 RESULTS AND DISCUSSION

The hybrid IDS is contrasted with other different ML methods, such as NB [3], LR [12], XGBoost [13], Gradient Boosting Decision Tree (GBDT) [3], K Nearest Neighbours [6], Multilayer Perceptrons [6] and Support Vector Machine (SVM) [9] with various kernel functions. The performance of the distinctive datasets and confusion matrix is given in Tabs. 3 and 4 respectively.

The presentation of the hybrid IDS and LR calculations shown in Fig. 3 that are superior to the next contrasting calculations of both KDDTestC and KDDTest-21.

The proposed method is presented as Algorithm 1 during the model training phase. The first cluster centres are calculated using a modest number of labelled data. Until the process converges, the equation is employed to determine the similarity between other unlabeled data and the original cluster centres.

The proposed system gets the accuracy of 99.963% for KDDTest+ dataset and 99.892% for KDDTest-21 individually. The experimental results of both datasets are given in Tab. 3.

The proposed detection system is evaluated in terms of detection rate, false alarm rate and accuracy of the detection. The detection parameters for varying classifiers are shown in Figs. 5 to 7. Average value of detection parameters the data sets are varied and tabulated. According to the result in Tab. 3, the detection rate of

HIDS is 99.6 %, which can be improved by increasing the number of training samples. The false alarm rate is 0.02867. The false alarm rate is high as the network is analyzed only with few attackers. As the number of attackers increases the false alarm rate reduces. Accuracy is 98 %.

The proposed detection system is evaluated in terms of detection rate, false alarm rate and accuracy of the detection. The detection parameters for varying classifiers are shown in Figs. 5 to 7. Average value of detection parameters the data sets are varied and tabulated. According to the result in Tab. 3, the detection rate of HIDS is 99.6 %, which can be improved by increasing the number of training samples. The false alarm rate is 0.02867. The false alarm rate is high as the network is analyzed only with few attackers; as the number of attackers increases the false alarm rate reduces. Accuracy is 98 %.

Table 3 Performance comparison with different datasets

Classifiers	KDDTest+			KDDTest-21			UNSWSS-NB15		
	ACC%	DR %	FAR	ACC%	DR %	FAR	ACC%	DR %	FAR
Hybrid IDS	99.963	99.946	0.049	99.892	99.931	0.185	98.751	98.979	1.075
NB	93.695	98.280	8.194	85.478	98.652	28.223	92.488	93.398	6.645
LR	98.959	99.946	0.031	98.863	98.908	0.230	81.214	-	-
XGBoost	90.731	95.547	11.184	77.139	92.340	38.160	97.606	97.570	1.387
GBDT	92.176	97.844	10.209	80.965	96.756	34.440	97.582	97.818	1.464
KNN	98.802	98.802	11.101	98.812	98.802	11.110	96.822	86.427	3.232
SVM	85.772	91.877	16.534	64.226	84.642	51.278	93.134	98.546	6.614
RF	88.546	91.703	12.435	71.559	85.533	43.691	94.606	97.072	4.797
MLP	98.400	98.627	0.788	98.000	96.897	18.575	89.566	97.452	18.754

Discernibly, the HIDS performance is superior to other measurements in detection provided that all documents are known as regular in LR and results of the assessment are correct. The similarities between these two system groups could lead to dissatisfaction of LR with the perception of Normal/DoS (Tab. 3).

Table 4 Confusion Matrix with different datasets

Type of data set		KDD TEST+		KDD TEST-21		UNSW-NB15	
Prediction	Actual	DDoS	Normal	DDoS	Normal	DDoS	Normal
Hybrid IDS	DDoS	6858	368	3992	3	7608	456
	Normal	5	8930	4	1976	3674	51064
NB	DDoS	6059	44	3223	44	10725	226
	Normal	802	8890	772	1936	558	51294
LR	DDoS	6858	4	3991	4	0	0
	Normal	3	8931	5	1975	11283	51520
SVM	DDoS	5150	399	2283	387	7597	35
	Normal	1711	8535	1711	1593	3741	51485
MLP	DDoS	5642	449	2776	437	8668	172
	Normal	1219	8485	1219	1543	2615	51348
RF	DDoS	5260	506	2393	494	7090	16
	Normal	1602	8428	1602	1486	4193	51504
KNN	DDoS	5140	399	2283	387	7597	35
	Normal	1701	8535	1711	1593	3741	51482
GBDT	DDoS	5842	69	2975	69	10511	127
	Normal	1019	8865	1019	1911	772	51393
XG boost	DDoS	6026	208	2883	208	10553	155
	Normal	1111	8726	1111	1772	730	51365

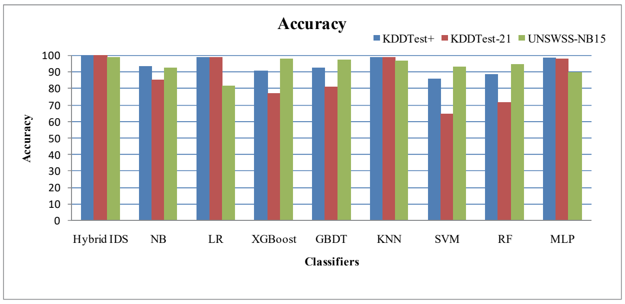


Figure 5 Accuracy comparison with different datasets

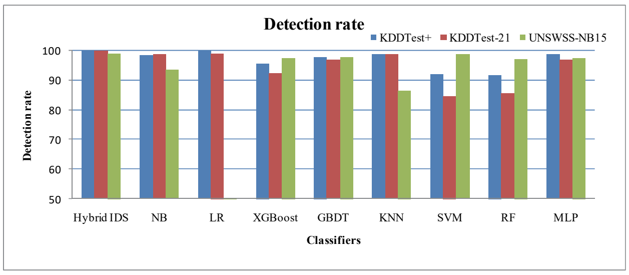


Figure 6 Detection rate comparison with different datasets

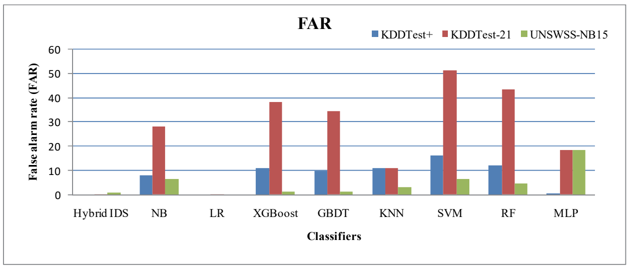


Figure 7 False alarm rate comparison with different datasets

From the above difference, the HIDS accomplishes great outcomes in the recognition of DOS attacks, followed by a low FAR. Our proposed strategy is additionally contrasted with various recognition techniques with confirm the acquired outcomes. This section utilizes the NSL-KDD dataset and UNSWSS-NB15 on the grounds that it is the most broadly utilized correlation dataset. Right now, proposed strategy is contrasted and Hybrid-ADE [15], semi supervised learning method [14], Marliboost [2] and their results are summarized in Tab. 5.

Table 5 Proposed Hybrid IDS Comparison with various DoS detection methods

Approach	Accuracy %	FAR %
Proposed Hybrid IDS	99.963	0.049
Hybrid-ADE	98.128	0.328
Semi supervised learning	97.369	0.449
Marliboost	96.379	0.010

Our hybrid IDS technique achieves 99.963% accuracy with 0.049% FAR. Hybrid-ADE is used to minimise network traffic information loss and thereby achieve accuracy improvement which uses density calculation auto encoder's hidden layer. Semi-supervised learning method uses method of that eliminates irrelevant normal network traffic data to increase the accuracy of detection. Among this beginning state of art draws near, its FAR is the most noteworthy. Despite the fact that by utilizing an outfit technique, Marliboost accomplished the least FAR of 0.010%, it is restricted as far as exactness.

6 CONCLUSION

This article tries to offer an insight into DoS attacks detection in wireless environments based on Hybrid IDS. It consists of modules for capturing network traffic and detection. The collection module makes the use of micro-batch processing system to collect and extract traffic features. In detection module the malicious nodes are isolated based on Hybrid IDS Based classification algorithm. We performed experiments more on the location accuracy of the identifiable proof module to measure the influence of the proposed hybrid IDS structure. The examination uses two customary datasets for benchmarks: NSL-KDD, UNSW-NB15. The test outcomes give extraordinary results with an accuracy of 99.963% and 98.751%, and the FAR of 0.049% and 1.08%, exclusively, as rather than various DoS attack acknowledgment methods. Because of the restrictions of the exploratory establishment, this article examined the HIDS structure in real time data. In future work, we plan to move on the appropriate state of the proposed Hybrid IDS, use DoS devices to initiate attacks, and then verify the performance of the system.

7 REFERENCES

[1] Saied, A., Overil, R. E., & Radzik, T. (2016). Detection of known and unknown DDoS attacks using artificial neural networks. *Neurocomputing*, *172*, 385-393. https://doi.org/10.1016/j.neucom.2015.04.101

[2] Boroujerdi, A. & Ayat, S. (2013). A robust ensemble of neuro-fuzzy classifiers for DDoS attack detection. *Proceedings of 2013 3rd IEEE International Conference on Computer Science and Network Technology*, 484-487. https://doi.org/10.1109/ICCSNT.2013.6967159

[3] Hameed, S. & Ali, U. (2018). HADEC: Hadoop-based live DDoS detection framework. *EURASIP Journal on Information Security*, *1*, 1-19. https://doi.org/10.1186/s13635-018-0081-z

[4] Sahi, A., Lai, D., Li, Y., & Diykh, M. (2017). An efficient DDoS TCP flood attack detection and prevention system in a cloud environment. *IEEE Access*, *5*, 6036-6048. https://doi.org/10.1109/ACCESS.2017.2688460

[5] Premkumar, M. & Sundararajan, T. V. P. (2020). DLDM: Deep learning-based defense mechanism for denial of service attacks in wireless sensor networks. *Microprocessors and Microsystems*, *79*, 103278. https://doi.org/10.1016/j.micpro.2020.103278

[6] Wang, M., Lu, Y., & Qin, J. (2020), A dynamic MLP-based DDoS attack detection method using feature selection and feedback. *Computers and Security*, *88*, 101645. https://doi.org/10.1016/j.cose.2019.101645

[7] Jiang, T., Gradus, J. L., Lash, T. L., & Fox, M. P. (2021). Addressing measurement error in random forests using quantitative bias analysis. *American Journal of Epidemiology*. https://doi.org/10.1093/aje/kwab010

[8] Zhu, B. et al. (2021). IoT Equipment Monitoring System Based on C5. 0 Decision Tree and Time-series Analysis. *IEEE Access*. https://doi.org/10.1109/ACCESS.2021.3054044

[9] Gopinath, S., Vinoth Kumar, K., & Jaya Sankar, T. (2019). Certain Investigation on Secured Multicast Authenticated Routing Scheme for MANET. *Cluster Computing*, 13609-13618. https://doi.org/10.1007/s10586-018-2020-7

[10] Song, R. & Liu, F. (2014). Real-time anomaly traffic monitoring based on dynamic k-NN cumulative-distance abnormal detection algorithm. 2014 IEEE 3rd International *Conference on Cloud Computing and Intelligence Systems*, 187-192. https://doi.org/10.1109/CCIS.2014.7175727

[11] Premkumar, M. & Sundararajan, T. V. P. (2021). Defense Countermeasures for DoS Attacks in WSNs Using Deep Radial Basis Networks. *Wireless Personal Communications*, 1-16. https://doi.org/10.1007/s11277-021-08545-6

[12] Yao, K., Li, Z., Yao, L., & Lang, K. (2020). Popularity prediction caching based on logistic regression in vehicular content centric networks. *International Journal of Ad Hoc and Ubiquitous Computing*, *35*(3), 150-161. https://doi.org/10.1504/IJAHUC.2020.110821

[13] Li, D., Zhang, P., & Li, R. (2021). Improved IMM algorithm based on XGBoost. *Journal of Physics: Conference Series*, 1748(3), 032017. https://doi.org/10.1088/1742-6596/1748/3/032017

[14] Idhammad, M., Afdel, K., & Belouch, M. (2018). Semi-supervised machine learning approach for DDoS detection. *Applied Intelligence*, *48*(10), 3193-3208. https://doi.org/10.1007/s10489-018-1141-2

[15] Odiathevar, M., Seah, W. K., Frean, M., & Valera, A. (2021). An Online Offline Framework for Anomaly Scoring and Detecting New Traffic in Network Streams. *IEEE Transactions on Knowledge and Data Engineering*. https://doi.org/10.1109/TKDE.2021.3050400

[16] Öney, M. U. & Peker, S. (2018). The use of artificial neural networks in network intrusion detection: A systematic review. *2018 International Conference on Artificial Intelligence and Data Processing (IDAP)*, 1-6. https://doi.org/IEEE. 10.1109/IDAP.2018.8620746

[17] Rehman, S. et al. (2021). DIDDOS: An approach for detection and identification of Distributed Denial of Service (DDoS) cyberattacks using Gated Recurrent Units (GRU). *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2021.01.022

Contact information:

Dr. Magudeeswaran PREMKUMAR, Assistant Professor
(Corresponding author)
Department of ECE,
SSM Institute of Engineering and Technology,
Dindigul, Tamilnadu, India
E-mail: prem53kumar@gmail.com

Dr. Tharai Vinay Param SUNDARARAJAN, Professor
Department of ECE,
Sri Shakthi Institute of Engineering and Technology,
Coimbatore, Tamilnadu, India
E-mail: suntvp@yahoo.co.in

Dr. Gopalakrishnan MOHANBABU, Professor
Department of ECE,
SSM Institute of Engineering and Technology,
Dindigul, Tamilnadu, India
E-mail: shamyubabu@gmail.com