International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 26th Dec 2022. Link :http://www.ijiemr.org/downloads.php?vol=Volume-11&issue=Issue12

10.48047/IJIEMR/V11/ISSUE 12/226

TITLE: A STUDY OF NIDS TO DETECT NORMAL OR ATTACK TRAFFIC

Volume 11, ISSUE 12, Pages: 1716-1729

Paper Authors **KEERTI, DR. RAJEEV YADAV**

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

A STUDY OF NIDS TO DETECT NORMAL OR ATTACK TRAFFIC

KEERTI, DR. RAJEEV YADAV

DESIGNATION- RESEARCH SCHOLAR MONAD UNIVERSITY HAPUR
DESIGNATION= (PROFESSOR) MONAD UNIVERSITY HAPUR

ABSTRACT

This research aspires to fill the void by suggesting a novel approach to dealing with the ever-evolving dangers posed by the internet. Minimizing the impact of cyber assaults requires timely identification and prevention of breaches. Due to the time it takes to analyze network data, traditional intrusion detection systems generally fail to identify threats in real time. The goal of this research is to create an effective system that can scan network packets quickly, spot abnormalities, and trigger alarms or preventative measures in real time. In order to keep up with the increasing sophistication of cyber threats, intrusion prevention and detection systems must also advance. The system is able to continually adapt to new situations, recognize new risks, and generate accurate forecasts thanks to the combination of artificial intelligence and machine learning. The goal of this research is to create a self-improving, self-protecting system that can anticipate and prevent novel forms of attack, including zero-day vulnerabilities. Maintaining operations and safeguarding private data depend critically on the reliability of the underlying computer network. The purpose of this research is to strengthen computer networks by creating a reliable intrusion detection and prevention system. If implemented, the suggested system would safeguard against data breaches, keep network resources secure, and prevent unwanted access.

KEYWORDS: Attack Traffic, cyber threats, detection systems, self-protecting system.

INTRODUCTION

Module I (HyFSA-HEIC) of the proposed NIDPS and its methodology is provided in this chapter. This module's job is to figure out whether the incoming network communication is benign or malicious. To make the NIDS more reliable and effective in real time, it is recommended to cut down on the FPR, FNR, TBM, and TTM. The first module's (HyFSA-HEIC) approach is outlined in four distinct parts. The first part of Module I (HyFSA-HEIC)

is its block diagram, which is shown below. In the last part, we analyze the experimental findings. In this last part, the chapter's key points are outlined.

BLOCK DIAGRAM OF MODULE I (HyFSA-HEIC)

In-depth discussion of the proposed Module I for intelligent light-weight accurate and efficient anomaly-based NIDS, HyFSA-HEIC, is presented here. Module I (HyFSA-HEIC) block diagram as shown in Figure

It contains following 3 phases:

Phase 1: Preprocessing of dataset

Phase 2: Selection of features using HyFSA

Phase 3: Model development using HEIC

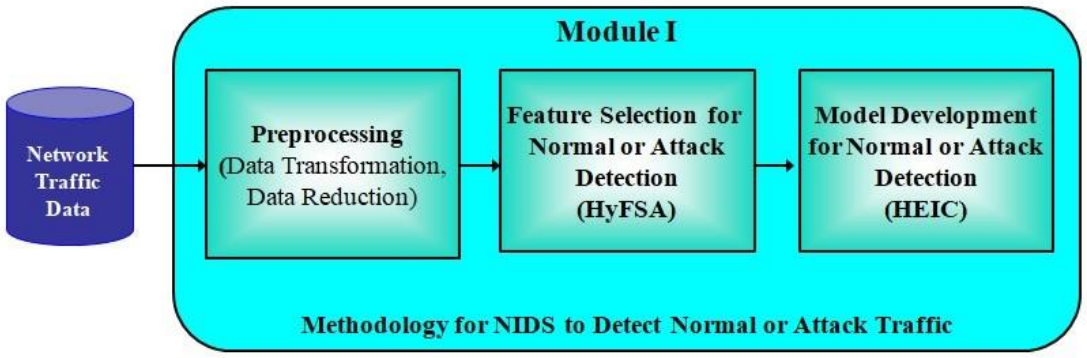

Figure 1: Block diagram of proposed Module I (HyFSA-HEIC)

EXPERIMENTAL SETUP

The feature selection strategies, classifiers, and ensembles used in this unit all make use of the software package Weka. Experiments will use the "10% KDD" and "Corrected Test". The requested module is implemented using the aforementioned steps.

Phase 1: Preprocessing of dataset

Normal and attack traffic detection have already been preprocessed on the "10% KDD" and "Corrected Test" datasets. There are 3 stages to this stage.

1) The first change is a renaming of the "attack" label on each record of an attack connection.

2) As a consequence of the data reduction process, almost 70% of the original entries were deemed unnecessary. As a result, we are excluding these records from further analysis. The resulting "Uni KDD" and "Uni Corr" datasets.

3) A training dataset ("Uni Train") and a test dataset ("Uni Test") are generated from "Uni KDD" by splitting it into two equal portions, each of which has 72793 entries. In the second phase, 6 features are chosen from the "Uni Train" and "Uni Test" datasets, and those datasets are reduced to form the "Red Uni Train" and "Red Uni Test" datasets. The "Uni Corr" and "Red Uni Corr" datasets are used for testing, with the former containing 41 characteristics and the latter just six.

Phase 2: Feature Selection using HyFSA

Applying HyFSA on the "Uni KDD" dataset yields the 6 top features out of a total of 41 features. Service, Src-bytes, Dst-bytes, Hot, Numcompromised, and Same-srv-rate are the feature numbers and names.

Phase 3: Model development using HEIC

The HEIC is used in Module I (HyFSA-HEIC) to construct the normal or assault detection model.

1) Classifiers to use in an ensemble are selected. Base classifiers for the ensemble are chosen to be the DT (C4.5), NB, NN-SGD, k-NN (k=3), RIPPER, and RF. The "Red Uni Train" dataset is used to train these classifiers. Comparisons are made using the TPR, FPR, ACC, PRE, ROC, TBM, TTM, and RMSE. Table 1 displays the outcomes of these classifiers on a 6-feature training dataset. Out of 6 possible base classifiers, only NB, NN-SGD, RIPPER, DT (C4.5), and RF were chosen for use in the ensemble. The Ensemble and Combiner Method, Stage 2

The heterogeneous ensemble is built using a parallel ensemble structure, with each of the five classifiers (NB, NN-SGD, RIPPER, DT (C4.5), and RF) being trained separately on the "Red Uni Train" dataset (6 features). After that, we apply the five laws of algebraic combination (Average, Product, Majority Voting, Minimum, and Maximum) to put together five different ensembles. Table 2 displays the evaluation metrics-based outcomes of these 5 ensemble models on the "Red Uni Train" dataset.

EXPERIMENTAL RESULTS AND ANALYSIS

Module I (HyFSA-HEIC) has been evaluated via a series of studies to determine its precision and efficiency. Weka is used for all experiments. Both the "Uni Train" and "Red Uni Train" datasets were used for training throughout the trials, while the "Uni Test" and "Red Uni Test" datasets were utilized for testing, along with the "Uni Corr" and "Red Uni Corr" datasets. TPR, FPR, ACC, PRE, ROC, TBM, TTM, and RMSE are utilized as performance measures in the studies. Table 3 displays the results of an evaluation of the classifiers on the test dataset "Red Uni Test" using TPR, FPR, ACC, PRE, ROC, TBM, TTM, and RMSE; Table 4 displays the results of the same evaluation for the datasets "Uni Corr" (41 features) and "Red Uni Corr" (6 features). Table 5 shows the results of 5 ensembles using 6 features from the "Red Uni Test" dataset, whereas Table 6 compares the results of 5 ensembles using 41 features from the "Uni Corr" dataset and 6 features from the "Red Uni Corr" dataset.

Table 1: Experimental results of classifiers on training dataset (6 features)

Classifiers	Evaluation Metrics							
	TPR (%)	FPR (%)	ACC (%)	PRE (%)	ROC (%)	TBM (sec)	TTM (sec)	RMSE (%)
NB	95.1	6.1	95.12	95.2	99.2	0.45	1.61	21.97
NN-SGD	97.2	3.7	97.16	97.2	96.7	170.56	1.61	16.86
k-NN(k=3)	99.9	0.1	99.87	99.9	100	0.08	5087.73	3.09
RIPPER	99.8	0.2	99.83	99.8	99.8	46.28	0.21	4.05
C4.5	99.9	0.2	99.88	99.9	100	3.24	0.35	3.32
RF	99.9	0.1	99.9	99.9	100	38.11	8.85	2.85

Six classifiers and five ensembles are trained and evaluated using a total of six and forty-one characteristics, respectively. Then, 6 features are compared with 41 features across several evaluation measures, and the best classifiers and ensembles are determined.

Table 2: Experimental results of ensemble on training dataset (6 features)

Ensemble of Classifier	Evaluation Metrics							
	TPR (%)	FPR (%)	ACC (%)	PRE (%)	ROC (%)	TBM (sec)	TTM (sec)	RMSE (%)
Average	99.9	0.1	99.9	99.9	100	227.6	8.42	7.49
Product	99.6	0.5	97.16	99.6	98.3	227.12	9.91	6.14
Majority Voting	99.9	0.1	99.91	99.9	99.9	226.54	9.09	3.06

Minimum	99.6	0.5	97.16	99.6	98.3	264.01	10.39	6.14
Maximum	97.8	3.2	97.85	97.9	99.9	253.69	10.47	11.59

Table 3: Experimental results of classifiers on test dataset (6 features)

Classifiers	Evaluation Metrics					
	TPR(%)	FPR(%)	ACC(%)	PRE(%)	ROC(%)	RMSE(%)
NB	95.2	6.1	95.17	95.2	99.3	21.87
NN-SGD	97.2	3.6	97.23	97.3	96.8	16.64
k-NN	99.9	0.2	99.84	99.8	100	3.67
RIPPER	99.9	0.2	99.86	99.9	99.9	3.62
C4.5	99.8	0.2	99.85	99.8	99.9	3.63
RF	99.9	0.1	99.92	99.9	100	2.54

Table 4: Experimental results of classifiers on "Uni Corr" (41 & 6 features)

Classifiers	Evaluation Metrics & # Features											
	TPR (%)		FPR (%)		ACC (%)		PRE (%)		ROC (%)		RMSE (%)	
	41	6	41	6	41	6	41	6	41	6	41	6

NB	91.5	90.4	12.3	15	91.52	90.41	91.8	91.3	93.3	97.9	29.02	30.91
NN-SGD	92.8	91.8	10.7	12.8	92.77	91.78	93.1	92.4	91	89.5	26.88	28.67
k-NN	94.2	95.4	9	6.8	94.2	95.36	94.5	95.5	93.9	94.6	23.19	20.89
RIPPER	94.5	95.2	8.5	7.5	94.52	95.15	94.8	95.4	93.1	93.8	23.41	22.08
C4.5	94.5	92.6	8.6	11.2	94.51	92.61	94.8	93	94.6	94	23.26	25.41
RF	94.2	94.6	9.1	7.1	94.21	94.61	94.6	94.6	99.3	97.1	19.73	20.64

compare and contrast the results achieved by six classifiers using various evaluation metrics after being exposed to datasets containing 41 and 6 features from the "Uni Train" and "Red Uni Train" datasets, respectively. The TBM and TTM for the full set of 41 characteristics are much higher than those for the condensed set of 6. Reducing the TBM

Table 5: Experimental results of ensembles on test dataset (6 features)

Ensemble of Classifier	Evaluation Metrics					
	TPR (%)	FPR (%)	ACC (%)	PRE (%)	ROC (%)	RMSE (%)
Average	99.9	0.2	99.87	99.9	100	7.5
Product	99.6	0.5	97.22	99.6	98.4	6.27
Majority Voting	99.9	0.2	99.88	99.9	99.9	3.42
Minimum	99.6	0.5	97.22	99.6	98.4	6.27

Maximum	97.8	3.2	97.84	97.9	99.9	11.6

Table 6: Experimental results of ensembles on "Uni Corr" (41 & 6 features)

Ensemble of Classifier	Evaluation Metrics & # Features											
	TPR (%)		FPR (%)		ACC (%)		PRE (%)		ROC (%)		RMSE (%)	
	41	6	41	6	41	6	41	6	41	6	41	6
Average	94.3	93.5	8.9	10.3	94.3	93.5	94.7	93.9	99.2	97.9	21.9	22.7
Product	93.7	93.2	9.5	11	92.7	91.1	93.9	93.8	91.7	90.3	25.2	26
Majority Voting	94.3	93.6	8.9	10.1	94.3	93.6	94.7	94	92.7	91.8	23.8	25.3
Minimum	93.7	93.2	9.5	11	92.7	91.2	93.9	93.8	91.7	90.3	25.2	26
Maximum	91	92.1	13.7	12.7	91	92.1	91.6	92.8	99	98	21.3	21.8

For 5 out of 6 feature sets, the reduction is between 68 and 96%, with k-NN and TTM seeing reductions of 40 to 94%. Both TBM and TTM are compared through graph in Figures 4 and 5, albeit for different sets of characteristics (41 and 6, respectively). Classifiers' results on the "Uni Test" and "Red Uni Test" datasets are shown in As can be using an optimized features set results in less computation time being used during the training and testing phases while yet preserving the same classification performance as the original features set.

Both the Majority Voting and Average ensembles outperformed the other four ensemble methods on the smaller dataset in terms of TPR (99.9%), FPR (0%), and PRE (100%). Aside from that, Majority Voting fared better than the others in ACC (99.91%) and ROC (100.0%) on the trimmed-down dataset. When compared to other ensembles, Majority Voting has the

lowest RMSE, at 1.85% for 6 features and 3.06% for 41 features. As a result, Majority Voting ensemble is the most effective combining rule for ensemble.

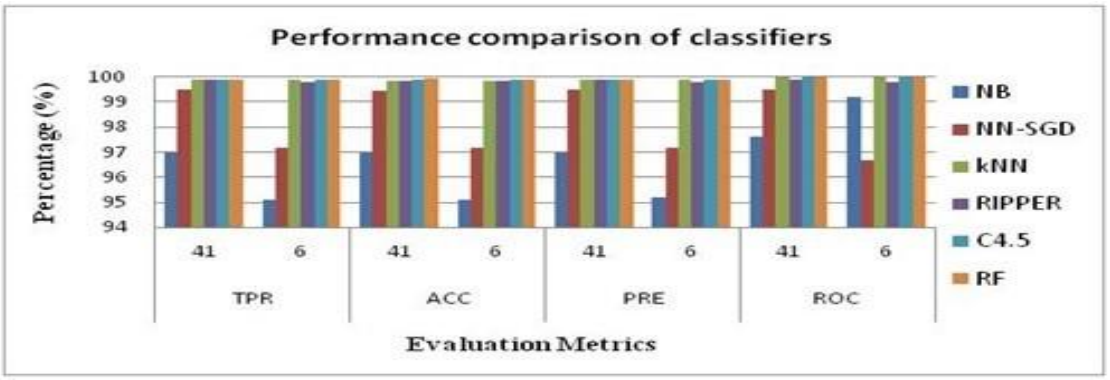

Figure 2: TPR, ACC, PRE & ROC of classifiers (41 & 6 features)

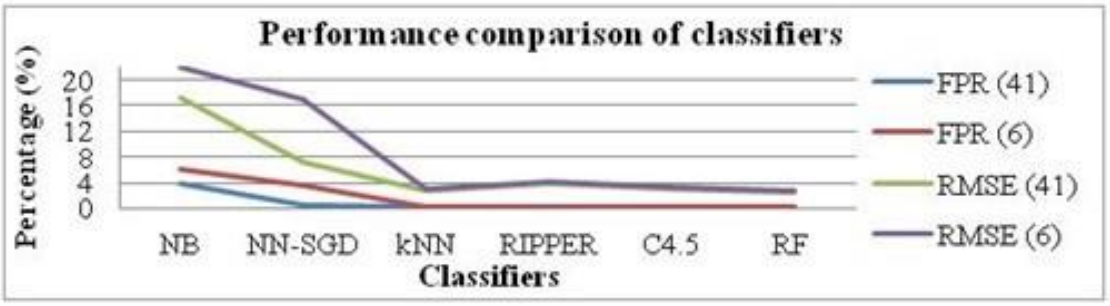

Figure 3: FPR & RMSE of classifiers (41 & 6 features)

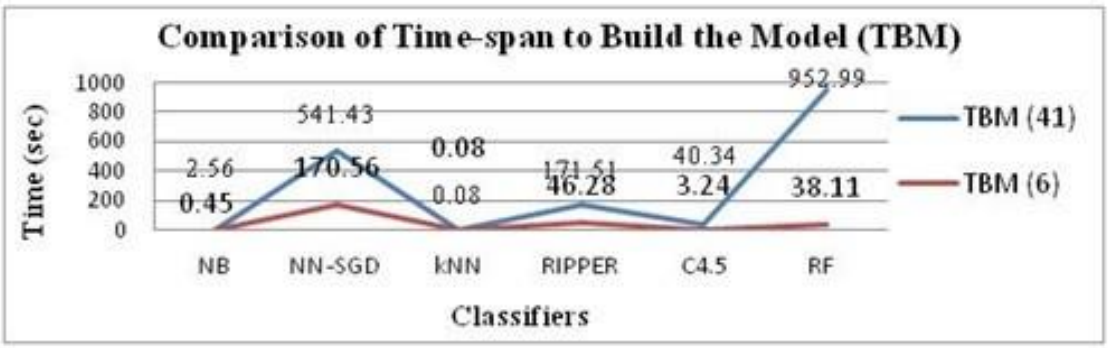

Figure 4: TBM (in sec) of classifiers (41 & 6 features)

The TBM and TTM of ensembles have dropped significantly by around 58-64% and 42-56%, respectively, for 6 characteristics. Figure 6 displays a comparison of the ensembles' TPR, ACC, PRE, and ROC, Figure 7 displays the ensembles' FPR and RMSE, Figure 8 displays the ensembles' TBM, and Figure 9 displays the ensembles' TTM for 41 and 6 features,

respectively. Tables 4 and 6 reveal that the performance of classifiers and ensembles evaluated on the "Red Uni Corr" test dataset is comparable to that with 41 features across all assessment measures.

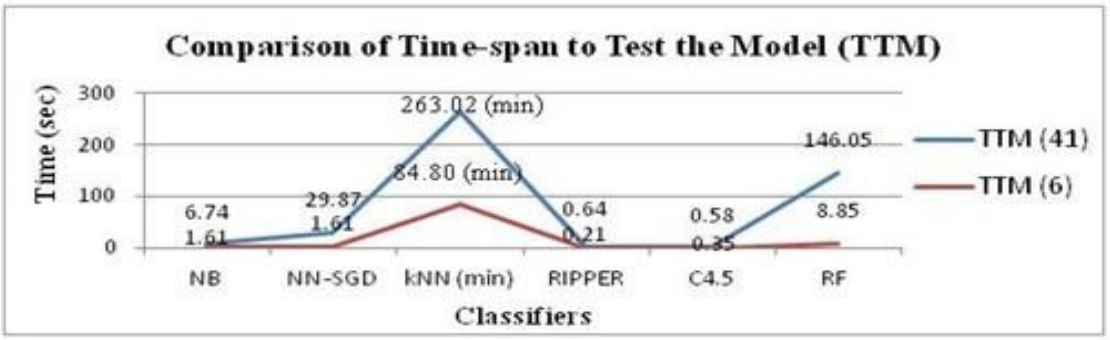

Figure 5: TTM (in sec & for k-NN in min) of classifiers (41 & 6 features)

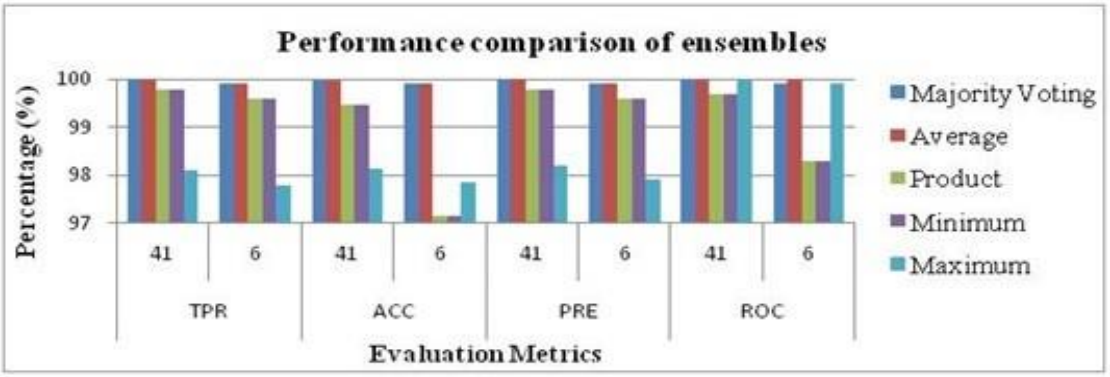

Figure 6: TPR, ACC, PRE & ROC of ensembles (41 & 6 features)

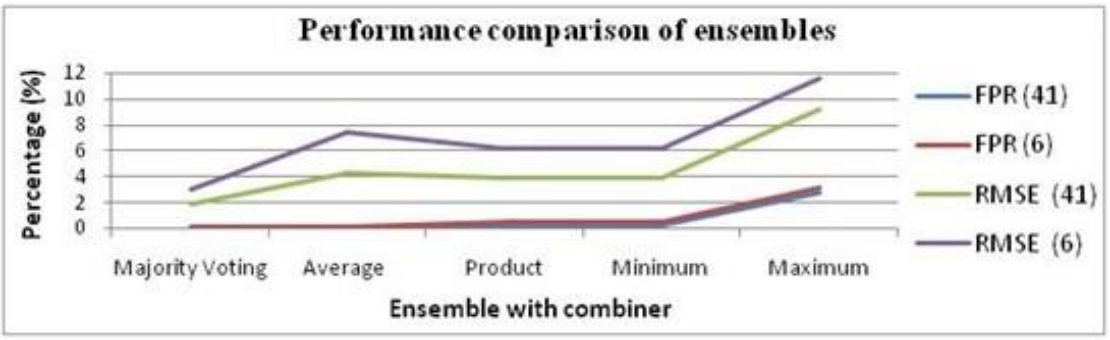

Figure 7: FPR & RMSE of ensemble (41 & 6 features)

The ensemble utilizing Majority Voting performed better than the other ensembles and single classifiers based on the comparison of their performance on several evaluation metrics on the reduced set of six characteristics. Therefore, it is more effective and trustworthy for NIDS. As

a result, it has been chosen as the Module I (HyFSA-HEIC) ensemble model. Module I (HyFSA-HEIC) Performance Evaluation Against Stand-Alone Classifiers NB,

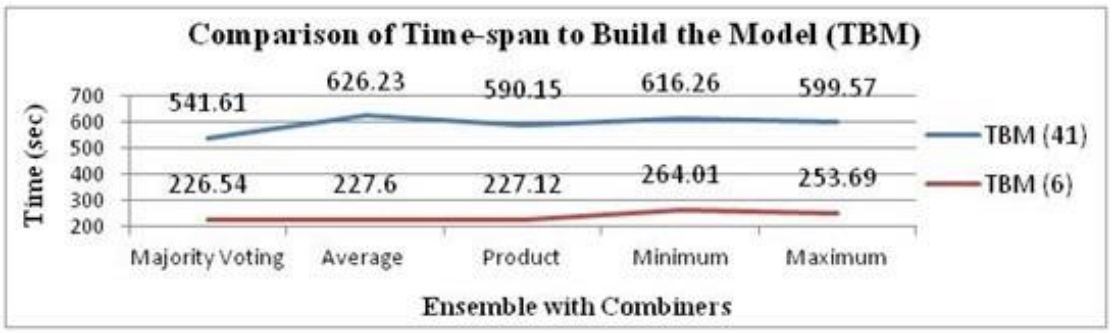

Figure 8: TBM (in sec) of ensembles (41 & 6 features)

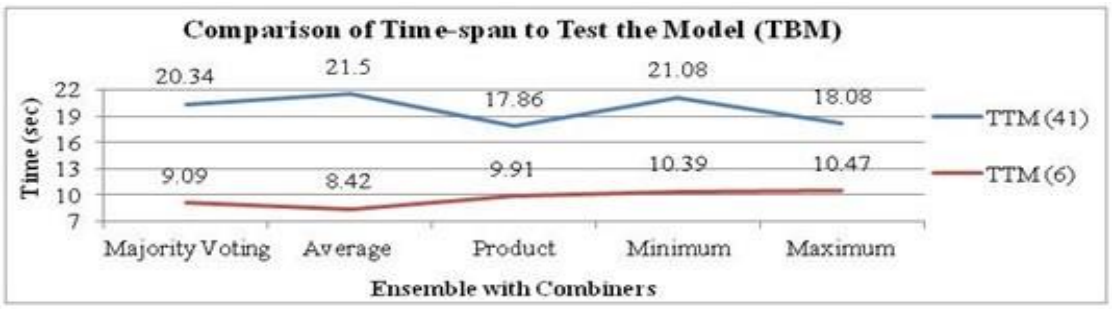

Figure 9: TTM (in sec) of ensembles (41 & 6 features)

Figure 10 displays the TPR, ACC, PRE, and ROC of NN-SGD, RIPPER, C4.5, and RF, while Figure 11 displays the FPR and RMSE. Module I (HyFSA-HEIC) now outperforms the ensemble with complete features set in terms of TRP (99.9%), ACC (99.91%), PRE (99.9%), ROC (99.9%), FPR (0.1%), and RMSE (3.06%), and boasts quicker TBM and TTM.

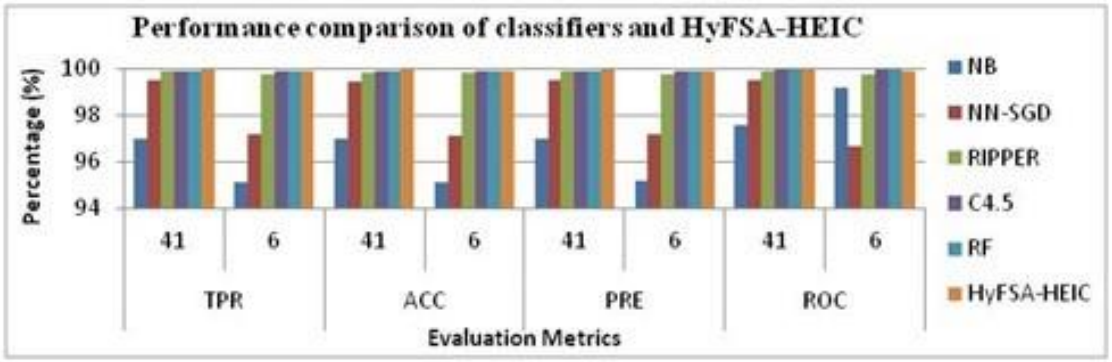

Figure 10: TPR, ACC, PRE, & ROC of classifiers and HyFSA-HEIC

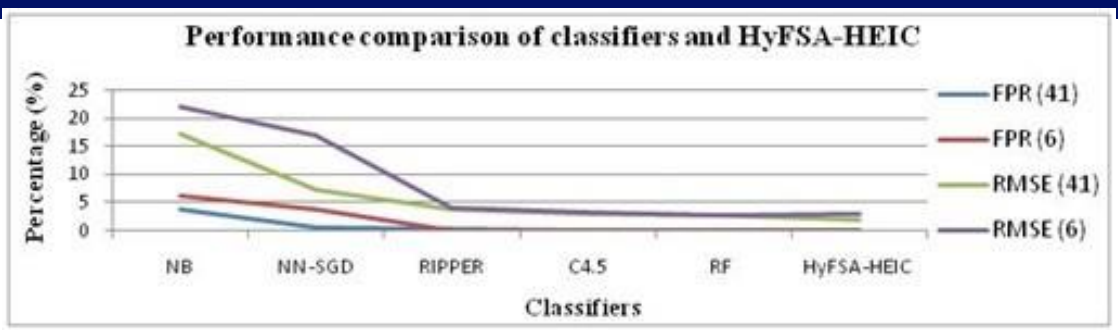

Figure 11: FPR & RMSE of classifiers and HyFSA-HEIC (41 & 6 features)

CONCLUSION

This component's goal is to identify potentially harmful network activity. Lighter systems with improved performance in terms of higher ACC and lower FPR, FNR, TBM, and TTM are offered. It combines HyFSA and HEIC to boost NIDS performance, with HyFSA used to pick the best possible feature subset. Large-scale high-dimensional dataset handling, optimizing overall ACC with a minimum of false alarms, and similar problems present themselves as the primary challenges in IDS. These concerns are dealt with in Module I (HyFSA-HEIC) by combining HyFSA and HEIC. Using just 6 carefully chosen characteristics (representing only 15% of the original 41), it used 5 different accurate intelligent classifiers (NB, NN-SGD, RIPPER, DT (C4.5), and RF) and Majority Voting to determine the final conclusions of these 5 classifiers. Module I (HyFSA-HEIC) had the best results overall, with a TPR of 99.9%, an ACC of 99.91%, a PRE of 99.9%, a ROC of 99.9%, a low FPR of 0.1%, and an RMSE of 3.06% with just 6 features being chosen. On a minimal feature set, it cut TMB by 50.79 percent and TTM by 55.30 percent. In conclusion, the TPR, ACC, PRE, and ROC are all enhanced, the FPR, FNR, and ERR are decreased, and the calculation time required is minimized when the feature selection strategy is integrated into the heterogeneous ensemble of intelligent classifiers.

REFERENCES

Bhuyan, M.H., Bhattacharyya, D.K., and Kalita, J.K. (2014) 'Network anomaly detection: methods, systems and tools', *IEEE Communications Surveys and Tutorials,* 16(1), 303–336.

Bhuyan, M.H., Bhattacharyya, D., and Kalita, J. (2016) 'A multi-step outlierbased anomaly detection approach to network-wide traffic', *Information Sciences,* 348, 243–271.

Birkinshaw, C., Rouka, E., and Vassilakis, V.G. (2019) 'Implementing an intrusion detection and prevention system using software-defined networking: Defending against port-scanning and denial-of-service attacks', *Journal of Network and Computer Applications*, 136, 71–85.

Blum, A.L. and Langley, P. (1997) 'Selection of relevant features and examples in machine learning', *Artificial Intelligence*, 97(1–2), 245–271

Borji, A. (2007) Combining heterogeneous classifiers for network intrusion detection. In: Cervesato, Iliano, (ed.) *Advances in Computer Science - SIAN 2007, Computer and Network Security : Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, 4846, pp. 254–260.

Bostani, H. and Sheikhan, M. (2015) 'Hybrid of binary gravitational search algorithm and mutual information for feature selection in intrusion detection systems', *Soft Computing*, 21(9), 2307–2324. doi:10.1007/s00500-015-1942-8

Bottou, L. (2010) Large-scale machine learning with stochastic gradient descent. In: *Proceedings of the 19th International Conference on Computational Statistics (COMPSTAT'10)*, Paris France, pp. 177–187.

Branco, P., Torgo, L., and Ribeiro R.P. (2016) 'A Survey of Predictive Modeling on Imbalanced Domains', *ACM Computing Surveys (CSUR)*, 49(2), 31.

Breiman, L. (1996) 'Bagging Predictors', *Machine Learning*, 24, 123–140.

Breiman, L. (2001) 'Random forests', *Machine Learning*, 45(1), 5–32.

Chae, H.S., Jo, B.O., Choi, S.H., and Park, T.K. (2015) 'Feature selection for intrusion detection using NSL-KDD', *Recent Advances in Computer Science*, 960– 978.

Chalak, A., Harale, N.D., and Bhosale, R. (2011) 'Data mining techniques for intrusion detection and prevention system', *International Journal of Computer Science and Network Security*, 11(8), 200–203.

Chawla, N.V., Bowyer, K.W., Hall, L.O., and Kegelmeyer, W.P. (2002) 'SMOTE: Synthetic Minority Oversampling Technique', *Journal of Artificial Intelligence Research (JAIR)*, 16, 321–357.

Chawla, N.V., Japkowicz, N., and Drive, P. (2004) 'Editorial: Special issue on learning from imbalanced data sets', *ACM SIGKDD Explorations Newsletter*, 6(1), 1–6.

Chen, T., Pan, X., Xuan, Y., Ma, J., and Jiang, J. (2010) A Naive Feature Selection Method and Its Application in Network Intrusion Detection. In: *International Conference on Computational Intelligence and Security (CIS)*, pp. 416–420.

Chen, Y., Li, W., and Cheng, X. (2007a) Toward Building Lightweight Intrusion Detection System Through Modified RMHC and SVM. In: 15th

IEEE International Conference on Networks (ICON), pp. 83–88. doi: 10.1109/ICON.2007.4444066

Chen, Y., Dai, L., Li, Y., and Cheng, X. (2007b) Building Lightweight Intrusion

Detection System Based on Principal Component Analysis and C4.5 Algorithm. In: 9th *International Conference on Advanced Communication Technology*, pp. 2109–2112. doi: 10.1109/ICACT.2007.358788

Chung, Y.Y. and Wahid, N. (2012) 'A hybrid network intrusion detection system using simplified swarm optimization (SSO)', *Applied Soft Computing*, 12(9), 3014– 3022.

Cohen, W.W. (1995) Fast effective rule induction. In: *Proceedings of the 12th International Conference on Machine Learning*, Paris, France, pp. 115–123.

Das, S. (2001) Filters, wrappers and a boosting-based hybrid for feature selection. In: *Proceedings of 18th International Conference on Machine Learning*, pp. 74–81.

Dash, M. and Liu, H. (2003) 'Consistency-based search in feature selection', *Artificial Intelligence*, 151(1–2), 155–176. http://dx.doi.org/10.1016/s00043702(03)00079-1

Debar, H., Thomas, Y., Cuppens, F., and CuppensBoulahia, N. (2008) 'Response: Bridging the link between intrusion detection alerts and security policies', *Intrusion Detection Systems*, 38, 129–170.