International Journal of Advances in
Soft Computing and Intelligent Systems (IJASCIS)
2024, Vol 03, Issue 02, 337-348
ISSN: 3048-4987

Original Paper

ENHANCE INTRUSION DETECTION BY ANALYZING THE BEHAVIOR OF LABELED AND UNLABELED CLASSIFICATION TO OBTAIN BETTER ACCURACY

Suriya Prakash J[a], Srinidhi N N[b,*], Latha A[c] , Chaithra[d], Kiran S[e]

[a] Department of Computer Science and Engineering, JAIN (Deemed-to-be-University), Bengaluru, Karnataka, India
[b,*] Department of Computer science and engineering,Manipal Institute of Technology Bengaluru, Manipal Academy of Higher Education,Manipal, India, srinidhi.nn@manipal.edu.
[c] Department of Computer Science and Engineering, Sri Krishna Institute of Technology, Visvesvaraya Technological University, Bengaluru, Karnataka, India.
[d] Department of Computer Science and Engineering, REVA University, Bengaluru, Karnataka, India.
[e] Department of Mathematics, Nitte Meenakshi Institute of Technology, Bangalore, Karnataka, India.

ABSTRACT

Intrusion Detection System has accelerated globally as a result of the need to identify intrusions that occur in network data flow. The two IDS methods that are primarily used by machine learning and network pattern detection are anomaly-based and signature-based methods. A network can be made fool proof by keeping it safe by keeping an eye out for any hazardous activity. In network dataflow systems, network traffic can be produced via simulators. Simulators are a useful tool for detecting harmful behaviour. Intrusions that are host-based, protocol-based, application protocol-based, network-based, and hybrid-based are some of the most prevalent kinds that have been discovered. In this paper, open source datasets ISP datasets and WIDE datasets are employed for experimentation. The crux of this paper is to carry out network classification by using minimal training sets and classifying maximal test sets for procuring accurate results. Lastly, the Labelled and Un-labelled technique is used to compare various accuracy outcomes. The suggested scheme's effectiveness is confirmed by the empirical investigation conducted on ISP and WIDE data. In this paper, the labeled and unlabeled classification proposed here identifies the intruder application with minimal labeled dataset. Most importantly automatic labeling of large test sets with small training set is accomplished. The analysis process for classification methods involving ISP and WIDE datasets by an experimental way has produced efficient classification results. The Labeled classification algorithm produces 93% accuracy and the unlabeled classification algorithm produces 84% accuracy.

KEYWORDS

Intrusion, Attacks, Network, Features, Accuracy

1. INTRODUCTION

Huang et al. [1], developed an original Imbalanced Generative Adversarial Network (IGAN) to address the issue of class imbalance. By incorporating convolution layers and an imbalanced data filter into the conventional GAN, For minority classes, the authors were able to offer additional representative samples. Additionally, an IGAN-based intrusion detection system, or IGAN-IDS, was designed to ad-dress class-imbalanced IDS, which uses instances generated by IGAN. The authors conducted a thorough comparison between the performance of IGAN-IDS

and other methods on NSL-KDD. AUC, recall, F1 Score, and precision all improve by at least 1%, 6%, 10%, and 1%, respectively, when using IGAN-IDS. Devan et al. [2], In the XGBoost–DNN model, a deep neural network uses the XGBoost algorithm—which was first suggested for feature selection—to continue classifying network intrusions. The method is cross-validated and contrasted with state-of-the-art machine learning techniques including SVM, naive Bayes, and linear regression. We calculate and evaluate the assessment criteria with the state-of-the-art shallow techniques for an F1-score that considers accuracy, precision, and recall. The results show that the suggested model outperforms earlier models with a consistent level of 97 percent classification accuracy. A technique for assessing the effectiveness of a network intrusion detection system (IDS) that used the auto encoder unsupervised learning approach was presented by Choi et al. [3]. The suggested model has an accuracy of 91.70 percent, which is higher than previous research that employed cluster analysis approaches to achieve an accuracy of 80 percent. Hajisalem et al. [4], presented a classification-based strategy to boost IDS performance using the Fish Swarm algorithm and an artificial Bee Colony. With a detection rate of 99 per-cent and a false positive rate of 0.01 percent, the suggested technique exceeds in terms of performance metrics. Safaldin et al. [5], An improved IDS was created by combining a support vector machine (GWOSVM-IDS) with the modified binary grey wolf optimizer. The recommended approach is to raise the detection rate and accuracy of intrusion detection while also decreasing processing time by lowering false alarm rates and the amount of features generated by IDS. According to the findings, the proposed GWOSVM-IDS beats all prior proposed and comparable methods. Ding et al. [6], suggested IDS model based on Convolution Neural Networks (CNN), a standard deep learning approach, and utilizes the whole NSL-KDD dataset. According to the results of the trials, the proposed IDS model outperforms models based on standard ML methods in multi-class classification. Mittal et al. [7], In order to analyses the overall network lifespan, a suggested LEACH procedure using a Levenberg-Marquardt neural network is tested. The authors concentrated on normal and abnormality detection in wireless sensor networks using deep learning models. GRU has a detection rate of 97.84 percent and LSTM has a detection rate of 97.85 percent, with the lowest false positive rate of 5.87 and 3.88 percent, respectively, for GRU and LSTM. Karami et al. [8], suggested a unique anomaly-based intrusion detection system (IDS) that makes use of a modified Self-Organizing Map (SOM) and a neural projection architecture to accurately identify intrusions and anomalies while also providing the client user with information in the presence of long-range independence data known as benign outliers. The recommended visualization abilities allow for improved analysis and intuitive response by accounting for the limitations of human cognitive capacities while interacting with IDS, particularly large amounts of data.

1.1 Major Contribution

This research work proposes to identify better accuracy by analysing different labelled and unlabelled classification algorithm. To serve as the standard for the re-searcher, a novel intrusion detection accuracy analysis approach has been proposed. The steps involved in suspicious flow detection analysis are demonstrated via a unique intrusion detection method. We've run experiments using the WIDE and benchmark ISP datasets. The suggested model performed better than the other models on both datasets, according to the results. This is how this paper's remaining portion is organised. A review of prior studies and models pertaining to intrusion detection in network traffic is provided in Section 2. The research work's methodology, which comprises a unique intrusion detection algorithm and novel framework for network traffic analysis, is covered in Section 3. The suggested model's experimental results are discussed in Section 4. Section 5 wraps up the study and provides an outline for further steps.

2. LITERATURE SURVEY

The In the real world, computer networks are used by several applications, and net-work security is unbreakable. Intrusion detection is essential for maintaining net-work security and plays a key role in the security of network infrastructure. Mohammadpour et al. [9], proposed that the System administrators can utilize Net-work IDSs to identify possible security breaches (NIDS). Using the benchmark dataset NSL-KDD, the researchers applied convolution neural networks (CNNs), an advanced deep learning technique, to network penetration. Comparing the proposed experimental results to the NSL-KDD test, the detection rate is 99.79 percent. In order to achieve a high detection rate (DR) with a low false positive rate (FPR), Mazini et al. [10], introduced the artificial bee colony (ABC) and AdaBoost techniques for an anomaly network-based intrusion detection system (A-NIDS). The proposed approach has the best performance among the others, with an error of less than 0.006. Mohammed et al. [11], proposed Particle swarm optimization (PSO)-based fast learning network (FLN).The created model has been contrasted with a wide range of meta-heuristic algorithms. The authors obtained 93.21% accuracy on KDD-CUP dataset. Vijayanand et al. [12], proposed wireless mesh networks, a distinct IDS with multiple support vector machine classifiers and feature selection based on evolutionary algorithms. The suggested method looks for the instructive components of each sort of attack rather than choosing traits that are common to all assaults. The trials' findings show that the recommended solution is very accurate in identifying attacks and is a good fit for wireless mesh network intrusion detection. In order to solve the problem of class disparity, Huang et al. [1], developed a novel Imbalanced Generative Adversarial Network (IGAN). By incorporating convolution layers and an imbalanced data filter into the conventional GAN, the authors were able to provide more samples that are typical for minority classes. Moreover, class-imbalanced IDS was addressed by an IGAN-based intrusion detection system, or IGAN-IDS, which uses instances generated by IGAN. The authors conducted an ex-tensive performance comparison between IGAN-IDS and other methods on NSL-KDD. AUC, recall, F1 Score, and precision all improve by at least 1%, 6%, 10%, and 1%, respectively, when using IGAN-IDS. Mighan et al. [13], proposed a hybrid SAE–SVM technique for an effective and rapid IDS for cyber security. The suggested method used SVM as the classifier and a stacked auto encoder network for feature extraction. Compared to other feature extraction methods, the deep network platform performs the best. Yang et al. [14], recommended LM-BP neural network model to construct an IDS with a 75 percent accuracy for the KDD-CUP Dataset.

Iftikhar et al. [15], used well-known ML techniques such as, the support vector machine, random forest, and Extreme Learning Machine to detect intrusions. The percentage of accuracy was 93 percent. Tao et al. [16], developed an FWP-SVM-genetic technique for intrusion categorization. This method minimises the mistake rate, shortens the classification time, and increases the true positive rate with a 97 percent accuracy. Zhang et al. [17], have provided information on recently developed nonparametric traffic classification techniques. The authors stress that improving classification accuracy occurs when correlated information is used throughout the procedure. Additionally, the authors have conceptually and practically validated their proposed system. Unknown flows created by unknown applications were detected with 85 percent accuracy using NCC and compound categorization. Spj et al. [18], in a huge data context, created a clustering technique for IDS generation that was proven to be 78 percent accurate.

Table 1: Summary of various Intrusion Detection Approaches

Author& Year	Approach	Remarks
Intrusion Detection Techniques		
Iftikhar *et al. [15]*	Well-known machine learning techniques	• Support Vector Machine (SVM), Random Forest (RF), and Extreme Learning Machine (ELM) were used. • 93% accuracy was obtained
Ali *et al*. [11]	Fast learning network (FLN) based on particle swarm optimization (PSO)	Obtained accuracy of about 98.4%. Based on the well-known dataset KDD99, the model was applied to the problem of intrusion detection and validated.
Tao *et al. [16]*	Two-step hybrid method based on binary classification and k-NN technique.	On the NSL-KDD data set, the proposed technique produces credible findings. Accuracy obtained is 94.92%
Yang *et al. [14]*	Novel unsupervised methodology	The MitM attack had a 100% true positive rate (TPR) and a 4.23 percent false positive rate (FPR), while the deauthentication attack had a 100% TPR and 2.44 percent FPR.

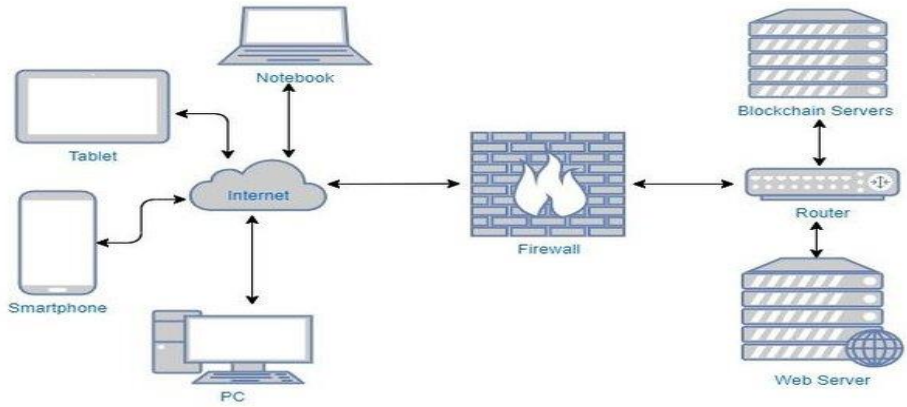

Figure 1: General schematic of IDS, Li [19]

Figure 1 shows the general schematic of an IDS. Here IDS puts a barrier between the firewall and end users. It notifies end users of intrusions and is used to identify them. Using this technology, real-time network flow is used to produce intrusion datasets over a predetermined period of time. The primary flaw in This system uses datasets that are simulated don't perform much better when it comes to study analysis accuracy. The duplicate datasets created during various intrusion data flows, which results in a complicated categorization procedure, is another disadvantage. In critical scenarios, the current traffic classification method performs poorly. In complicated networks, adopting robust traffic classification is a major difficulty.

3. METHODOLOGY

A. Dataset

The WIDE and Internet service provider (ISP) datasets from Wired Ethernet link is used in this work. Ethernet link is a widely used Local Area Network Technology is sometimes referred to as the TCP/IP stack's link layer protocol. ISP was traced in Australia from the date of 27/11/2010 to 03/12/2010 with 100 Mbps of Ethernet link. It has 11 classes of 200k flows. The WIDE dataset is taken from 150 Mbps of Ethernet link traced on 03/2008.It is 72 hours long dataset and acts as the backbone line between the USA and Japan. It has 6 classes with 182K-flows. In the WIDE data set there are 6 classes and the class named HTTP occurs frequently in comparison to other classes. In ISP dataset 11 classes exists and for this work 30,000 data flows are randomly taken from each major class to avoid the class domination.

3.1 System Model

The proposed methodology for Intrusion Detection classification is applied on the ISP and WIDE Dataset. This dataset is open dataset. The performance of the proposed IDS is analyzed in terms of accuracy. Non-uniform classification problem can be addressed through oversampling method. Before fitting a model, this can be accomplished by simply replicating the cases from the minority class in the training dataset. The class distribution is balanced by this oversampling technique, which does not add any new information. In order to balance the non-uniform dataset the method synthesizes new examples from the minority class. This method is very effective and augments the datasets to achieve uniform classification

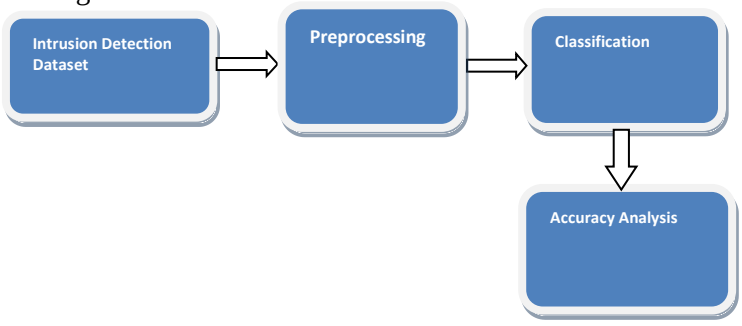

Figure 2: Flow Diagram of Proposed Intrusion Detection System

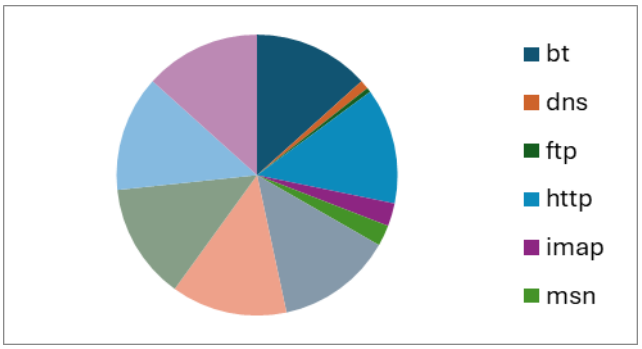

Figure 3: ISP class distribution

ISP dataset contains 30K data in each class namely bt, pop3, smtp, ssh and ssl3. A Minimal data is taken for training purpose while maximal data is considered for testing.

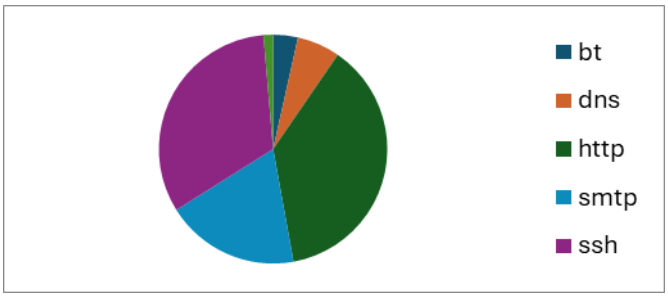

Figure 4: WIDE class distributions

WIDE dataset contains classes named http having 40K rows, ssh having 34k rows and smtp having 20k rows are selected to avoid sample bias. The Figures 3.4 and 3.5 describes the data flow among ISP and WIDE Datasets. It also depicts the total number of transport protocols dealing with the network traffic flow of those datasets.

3.1.1 Labelled Traffic Classification Method

Statistical methodology in identifying Intrusion detection system is proposed. It consists of Labelled classifications. The proposed flow of Intrusion recognition is illustrated in Figure 3.2. The proposed method describes the Labelled classification by finding the representative mean value for every individual class. Then the variance between all the individual test sets with the representative mean value of every class is identified. The least variance of representative mean value class is considered and allotted for test data.

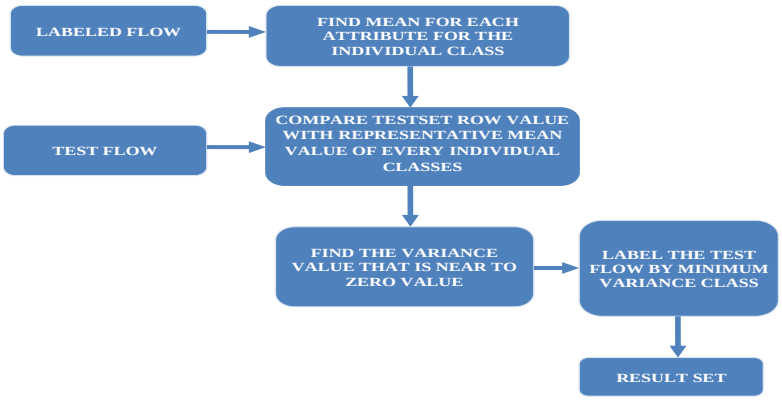

Figure 5 : Proposed Labelled IDS

The crux of this work is to carry out network classification by using minimal training sets and classify maximal test sets. In this process the statistical attributes are extracted by using the following properties i.e., time elapsed between two packet arrivals, flow timing, flow ideal time and its duration. For the WIDE and ISP packets a deep packet inspection is carried out using the following attributes: c2spkts, c2spsmax, c2spsmin, c2spsvar, s2cpkts and s2cpsmax.During this process, mean value of the labelled class of each attribute is considered. This is done in order to find the representative class.
Finally, the common mean value is retrieved for each individual class. The classes analysed are blue tooth, domain name system, the internet message access protocol, Microsoft notification protocol, file transfer protocol, hypertext transfer protocol, post office protocol, simple mail transfer protocol, and secure shell secure socket layer and extensible messaging and presence protocol in Internet Service Provider dataset. Hence 11 different common Mean values are calculated for each class of ISP. For the WIDE dataset 6 different traffic classes named as bt, dns, http, smtp, ssh and ssl2 are considered. By applying this method nearly 6 different common mean values are acquired.

Table 2: represents the representative mean value of the every individual class named bt, dns, ftp, http, imap, msn, pop3, smpt, ssh, ssl3 and xmpp.

c2s_psmax	**c2s_iptmin**	**s2c_psmax**	**s2c_psmin**	**s2c_psvar**	**s2c_iptmin**	**class**
0.14856257	0.000445247	0.163101	0.027232	0.020188	0.001043117	bt
0.03339209	1.02918E-06	0.167721	0.031545	0.032995	0.000658785	dns
0.02409498	6.84923E-05	0.358424	0.027736	0.065586	1.38153E-05	ftp
0.49985546	0.000132697	0.648502	0.029442	0.205696	0.000174091	http
0.07630115	2.80925E-05	0.557268	0.030301	0.096999	1.09275E-05	imap
0.34474635	1.54051E-05	0.417664	0.028461	0.074996	3.48105E-06	msn
0.01426842	3.66333E-05	0.577805	0.028435	0.189648	1.19013E-06	pop3
0.66367955	0.000229296	0.107222	0.027576	0.002486	2.84023E-05	smtp
0.11225542	6.26867E-07	0.444643	0.034836	0.040876	2.64833E-07	ssh
0.55165955	2.15007E-05	0.855523	0.027909	0.27535	4.49923E-06	ssl3
0.42350238	4.21051E-06	0.719103	0.0271	0.075121	1.88367E-08	xmpp

Algorithm 1: The proposed algorithm for Labelled Classification is given below.

Stepwise Description of the Algorithm

- Step-1:Minimal Labeled flow set LF with its label flow row {LFr1, LFr2,...}Maximal Test data T and its individual row {Tr1, Tr2, ...}.
- Step-2: Final Labeled Flow FLF
- Step-3: Finding Mean $\overline{\mathrm{LF_{ri}}}$ for Labelled Flow for each ri
- Step-4: for i ← 1 to n do
- Step-5 and 6: $\overline{LF_{ri}} \leftarrow \sum LF_{ri}$ divide by total number of *ri* per class.
- Step-7: Finding σ^2 between T and representative$\overline{LF_{r1}}$
- Step-5: Find the near to zero value of σ^2
- Step-8: Label the Test set T by Minimal Variance Class C to Test set T
- Step-9: FLF≈T←C

3.1.2 Unlabelled Traffic Classification Method

Unlabelled dataset can handle unknown data arriving from the intruder application. It can also handle the encrypted data that cannot be classified by supervised classification methods. In addition, it can classify all the data efficiently and produce accurate results. Figure 3.3 describes unlabelled classification Method that aims at minimal training sets with maximum test sets for clustering process. To avoid sampling bias, 10K random data were selected from each class. The unlabelled flow will be clustered according to the transport protocol class. In the next step the centroid of the cluster is identified as representative centroid value for that particular cluster. Then the variance between all the individual test sets with representative centroid value of every class is identified. The least variance of representative centroid value class is considered and allotted for test data.

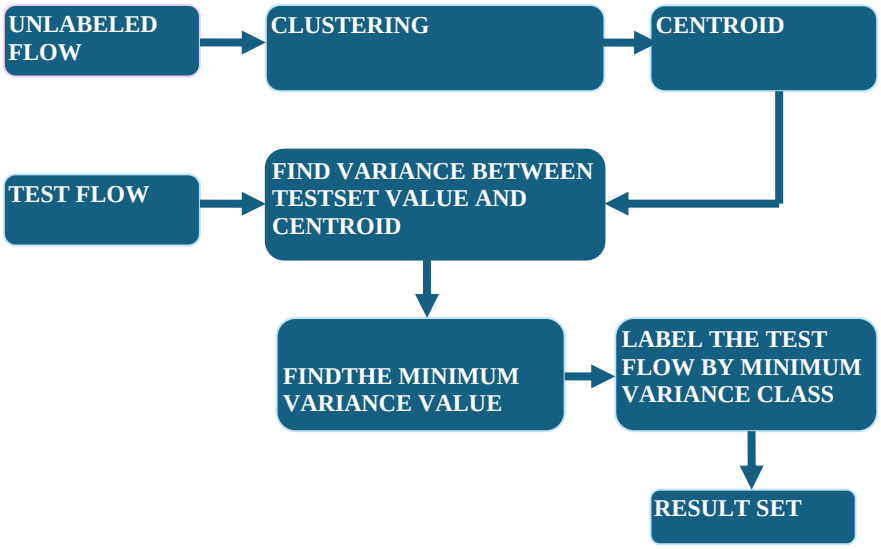

Figure 6. Unlabelled classification method

Algorithm 2: The proposed algorithm for Unlabelled Classification is given below.

Stepwise Description of the Algorithm

- Input: large unlabeled flow set UF≈{UF_{r1}, UF_{r2},...} and its individual row r_i; Test Flow T and its corresponding row T_{ri};
- Output: Labeled Flow LF
- Step-1: The Flow create n clusters and find its individual Centroids.
- Step-2: Finding σ^2 between T_{ri} and cen_i.
- Step-3 and 6: For each Test flow T_{ri} do
- Step-4: Finding $\sigma^2$for T_{ri} and cen_i
- Step-5: Find the Minimal variance σ^2
- Step-6: Label the Test flow by Minimal Variance representative centroid
- Step-7: LF≈T_{ri}←L

4. RESULTS AND DISCUSSION

4.1 Classification Accuracy

Figures 7 and 8 denotes performance comparison between proposed method with state of art for labelled and unlabelled methodology. K value predictions are made by averaging the k neighbours in the ISP and WIDE dataset. If the k value is larger, then the distance will be more this contradicts the principle behind KNN which shows that the neighbours that are nearer have similar densities or classes.

Table 3: Represents the comparative analysis of proposed methodology with state of art techniques.

Methodology	**Accuracy (%)**
Proposed Methodology	93
Erman Semi supervised Method	70
Navie Bayes	45
C4.5	63
Bayes Networks	60
KNN	61

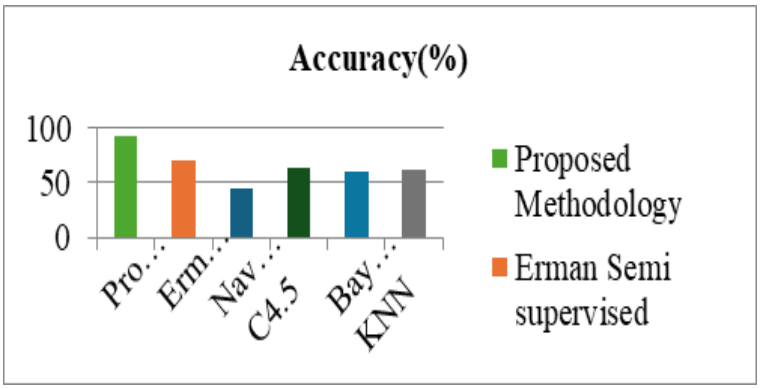

Figure 7 Performance comparisons of proposed labelled methodology

Figures 7 and 8 denotes performance comparison between proposed method with state of art for labelled and unlabelled methodology. K value predictions are made by averaging the k neighbours in the ISP and WIDE dataset. If the k value is larger, then the distance will be more this contradicts the principle behind KNN which shows that the neighbours that are nearer have

similar densities or classes. Optimal k value can be achieved through Elbow curve method. In existing method using KNN algorithm the K value considered is 5 and obtained the accuracy of 62%. However if k value increases then accuracy value decreases subsequently. K means algorithm is used in Erman Semi supervised approach to form clusters in order to achieve an accuracy of 60%. C4.5 algorithm considers normalized information gain ratio to identify the attribute with highest normalized information gain to create decision &children nodes. Algorithm considers criterion as entropy and random state to achieve an accuracy of 63%.

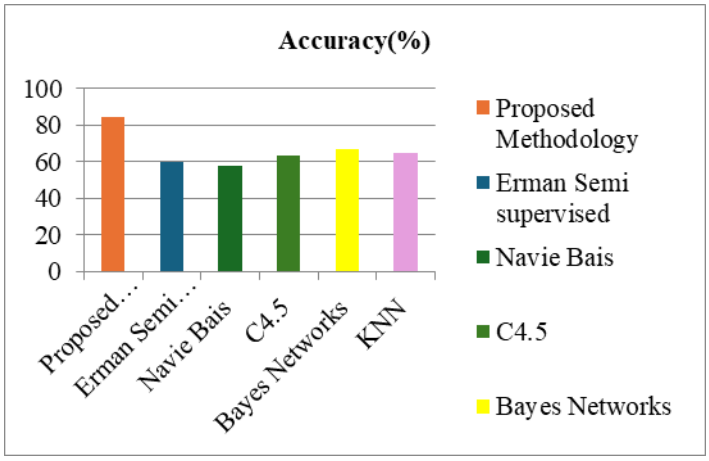

Figure 8. Performance comparisons of unlabelled methodology

5. CONCLUSION

The labelled classification classifies only the supervised samples and the unlabelled algorithm can classify the correlated flows and unknown flows in a very accurate manner. With this method, handling the unknown data is easier. Also, it has been tested with statistical data from ISP and WIDE dataset. Here the transport protocol will be varied in a specific period of time. The servers can change their address without changing the DNS which makes labelling a complex task. In addition, using labelling across the networks is not possible. Labels in WIDE and ISP are different and it cannot be used until server gains popularity among both setups. So in this method only traffic classification on WIDE and ISP network flows is addressed. The authors have addressed non uniform class distribution by duplicating the samples of the minority class and then applied to Naive Bayes Algorithm. The paper proposed an automatic detection and classification of Intrusion recognition system. The source dataset is WIDE and ISP datasets. The performance analysis is carried out with respect to IDS in terms of accuracy. This chapter proposed statistical methodology in identifying Intrusion using labelled and unlabelled datasets. The proposed methodology stated in this chapter achieves 93% of accuracy in labelled classification and 84% accuracy in unlabelled classification.

REFERENCES

[1] Huang, S & Lei, K, "IGAN-IDS: An imbalanced generative adversarial network towards IDS in ad-hoc networks", Ad Hoc Networks, vol. 105, pp. 102177, 2020.
[2] Devan, P & Khare, N, "An efficient XGBoost–DNN-based classification model for network IDS", Neural Computing and Applications, pp. 1-16, 2020.
[3] Choi, H, Kim, M, Lee, G & Kim, W, "Unsupervised learning approach for network IDS using autoencoders", The Journal of Supercomputing, vol. 75, no. 9, pp. 5597-5621, 2019.

[4] Hajisalem, V &Babaie, S, “A hybrid IDS based on ABC-AFS algorithm for misuse and anomaly detection”, Computer Networks, vol. 136, pp. 37-50, 2018.
[5] Safaldin, M, Otair, M &Abualigah, L, “Improved binary gray wolf optimizer and SVM for IDS in wireless sensor networks”, Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 2, pp. 1559-1576, 2021.
[6] Ding, Y & Zhai, Y, ‘IDS for NSL-KDD dataset using convolutional neural networks’, in Proceedings of the 2018 2nd International Conference on Computer Science and Artificial Intelligence, pp. 81-85, 2018.
[7] Mittal, M, Iwendi, C, Khan, S & Rehman Javed, A, “Analysis of security and energy efficiency for shortest route discovery in low energy adaptive clustering hierarchy protocol using Levenberg Marquardt neural network and gated recurrent unit for IDS”, Transactions on Emerging Telecommunications Technologies, vol. 32, no. 6, pp. 3997, 2021
[8] Karami, A, “An anomaly-based IDS in presence of benign outliers with visualization capabilities”, Expert Systems with Applications, vol. 108, pp. 36-60, 2018.
[9] Mohammadpour, L, Ling, TC, Liew, CS & Chong, CY, “A convolutional neural network for network IDS”, Proceedings of the Asia-Pacific Advanced Network, vol. 46, pp. 50-55, 2018.
[10] Mazini, M, Shirazi, B & Mahdavi, I, “Anomaly network-based IDS using a reliable hybrid artificial bee colony and AdaBoost algorithms”, Journal of King Saud University-Computer and Information Sciences, vol. 31, no. 4, pp. 541-553, 2019.
[11] Ali, Mohammed Hasan, Bahaa Abbas Dawood Al Mohammed, Alyani Ismail, and Mohamad Fadli Zolkipli. "A new intrusion detection system based on fast learning network and particle swarm optimization." IEEE Access vol. 6, pp. 20255-20261, 2018.
[12] Vijayanand, R, Devaraj, D &Kannapiran, B, “IDS for wireless mesh network using multiple support vector machine classifiers with genetic-algorithm-based feature selection”, Computers and Security, vol. 77, pp. 304-314, 2018.
[13] Mighan, SN & Kahani, M, “A novel scalable IDS based on deep learning”, International Journal of Information Security, vol. 20, no. 3, pp. 387-403, 2021.
[14] Yang, A, Zhuansun, Y, Liu, C, Li, J & Zhang, C, “Design of IDS for Internet of Things Based on Improved BP Neural Network”, in IEEE Access, vol. 7, pp. 106043-106052, 2019. DOI: 10.1109/ACCESS.2019. 2929919.
[15] Iftikhar, Saman, Danish Khan, Daniah Al-Madani, Alheeti Khattab M. Ali, and Kiran Fatimah. "An intelligent detection of malicious intrusions in IoT based on machine learning and deep learning techniques." Computer Science Journal of Moldova, vol. 90, no. 3, pp. 288-307, 2022.
[16] Tao, Peiying, Zhe Sun, and Zhixin Sun. "An improved intrusion detection algorithm based on GA and SVM." Ieee Access vol. 6 pp. 13624-13631, 2018.
[17] Zhang, J, Chen, C, Xiang, Y, Zhou, W & Vasilakos, AV, ”An effective network traffic classification method with unknown flow detection”, in IEEE Transactions on Network and Service Management, vol. 10, no. 2, pp. 133-147, 2013. DOI: 10.1109/TNSM.2013.022713.120250.
[18] S. P. J, C. H. Guntupalli, S. N. Chilamkurthy, G. Kowshik and A. Alekhya, “Enhancing the Security by Analyzing the Behaviour of Multiple Classification Algorithms with Dimensionality Reduction to Obtain Better Accuracy“, IEEE 3rd Mysore Sub Section International Conference (Mysuru Con), HASSAN, India, pp. 1-7, 2023. doi: 10.1109/MysuruCon59703.2023.10396971.
[19] Li, Xiaoming. "Inventory management and information sharing based on blockchain technology." Computers & Industrial Engineering, vol. 179, pp. 109196, 2023.

Authors

Dr. Suriya Prakash Jambunathan is an Assistant Professor in the School of Computer Science and Engineering at Jain (Deemed-to-be) University. He holds a B.E. degree in Computer Science and Engineering from Anna University and an M.E. degree in Computer Science and Engineering from St Peters University. In 2022, he completed his Ph.D. from Anna University.
With over 15 years of experience in academia, Dr. Suriya Prakash specializes in Network Intrusion Detection, Machine Learning, Artificial Intelligence, and Deep Learning. He is a certified SUN JAVA Programmer.

Dr. N N Srinidhi holding Ph.D in Computer Science and Engineering. Currently, working as an Assistant Professor in the Department of Computer Science & Engineering at Manipal Institute of Technology Bengaluru, MAHE Manipal. He has published more than 40+ research articles in International Journals including Elsevier, Inderscience, Springer, Taylor & Francis and International Conferences.

Mrs. Latha A, Assistant Professor in Department of Computer science and Engineering at Sri Krishna Institute of Technology,Bangalore, INDIA. Completed M.Tech in Computer science and Engineering, Having 20 years of teaching experience. Published 2 books. Published 10 articles in various National / International Conferences and 15 articles in various International Journals. Filed one Patent.

Dr. Kiran S is an Associate Professor at Nitte Meenakshi Institute of Technology, Bangalore, with over 20 years of experience in teaching Mathematics at the undergraduate and postgraduate levels. He holds a Master's degree from Central College, Bangalore University, and a Ph.D. from Visvesvaraya Technological University (VTU). Dr. Kiran has authored two books and holds six patents in his name. He has also published more than 20 research articles in prestigious international journals.

Dr. Chaithra has completed B.E (Computer Science & Engineering) from Sir.MVIT Engineering College, Bangalore and M.Tech (Computer Science & Engineering) from AMC Engineering College,Karnataka. She obtained PhD from Visvesvaraya Technological University, Belagavi in the year 2023, India. Currently working as Associate Professor in the Computer Science and Design Department, KSIT, Bengaluru, Karnataka, India. Her current research interests include Data Mining, Web Mining, Machine Learning, Artificial Intelligence and Deep Learning. She is a life member of the Indian Society for Technical Education (ISTE) and also IAENG Member. Published the several Scopus indexed journals.