Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 5, May 2021: 2427 – 2436

Traffic Analysis Based Intrusion Detection System For Wireless Systems Using GNN

K.Naresh Kumar Thapa[a], Kumaran R[b], Sahith Reddy D[c], Thilak M[d], T.Suresh , Raghavendran Sivakumar[f]

[a*] Associate Professor, Department of ECE, R.M.K Engineering College, R.S.M. Nagar, Kavaraipettai, Tamil Nadu, knt.ece@rmkec.ac.in.
[b]UG Student, Department of ECE, R.M.K Engineering College, R.S.M. Nagar, Kavaraipettai, Tamil Nadu, kuma17226.ec@rmkec.ac.in
[c] UG Student, Department of ECE, R.M.K Engineering College, R.S.M. Nagar, Kavaraipettai, Tamil Nadu, sahi17338.ec@rmkec.ac.in
[e] UG Student, Department of ECE, R.M.K Engineering College, R.S.M. Nagar, Kavaraipettai, Tamil Nadu, thil17428.ec@rmkec.ac.in
[f] H.O.D, Department of ECE, R.M.K Engineering College, R.S.M. Nagar, Kavaraipettai, Tamil Nadu, hod.ece@rmkec.ac.in
[g]Department of ECE, R.M.K Engineering College, R.S.M. Nagar, Kavaraipettai, Tamil Nadu, raghavendran.sivakumar@gmail.com

Abstract

Analysing and predicting the traffic of network will improve security. Network traffic analysis is implemented in different areas of applications such as banking, e commerce, etc. Different traffic analysis techniques are proposed like algorithms-based prediction, time series-based prediction model, Data mining-based analysis and ML based analysis. However, detecting intrusions with better accuracy is a nightmare while analysing vast congested traffic. In this paper to overcome the shortcomings of earlier proposed approaches, Gated Recurrent Neural Network is employed. Gated RNN provides better performance in detection, prediction and classification of intrusions in the real time network traffic. Proposed method is compared with earlier methods and validated with security metrics like accuracy and complexity

Keywords:

1. Introduction

The fast improvement of Internet, traffic observing and anticipating become to an ever-increasing extent basic to arrange the board and control. The scientists construct a long reach reliance (LRD) organization traffic model by utilizing the development of authentic traffic to improve organization's presentation. During the early exploration, network traffic is frequently demonstrated as Poisson measure dependent on Poisson appropriation and Markov measure which gain from the model of public traded phone network traffic.Malware traffic could also be of any kind where the system functionality changes completely Traffic may be a very sensitive data that deals with a top quality of services like gaming, surfing and social media and other packet-based data.Malware

may be a malicious software, which infects the pc via network. Modern malwares are propagating via networks are very stronger and not captured by present antivirus or anti-malware systems. Hence analysing the network traffic and system traffic is far important and needed as per this security compliance.

2. Contributions In This Paper

- We proposed a novel malicious traffic classification system using combination of K-means and GRU model. The highlight of using GRU and K-mean is its nature of stacking the LSTM models and concurrently executing the same.
- We also profile the traffic and characterize the features available into the useful form. A generalized packet processing adapter is also designed and developed for live testing
- We also emphasis to attempt the auto-tuning of the features while processing it in GRU. However, the system cannot auto-tune the entire features but few highly correlated features are auto-tuned which are achieved in the very first time in the traffic classification.
- We also validated the proposed system with the MTA-KDD'19 dataset to understand the efficacy of the system. From the experimental evaluation, it is also observed that the proposed system can work as same in both the collected data and the live data, which indeed produced an average accuracy of 97% for the both.
- further data is classified with k-means algorithm to improve the accuracy of detection in the networks.
- Finally, the proposed system would pave the pathway for the security researchers who are focusing more towards the online DL system add automation.

3. Literature Survey

Rajendra Prasad *et al*. 2017 presented review on Manet's intrusion detection system with multitier energy system. The multitier energy system solves the intrusion detection issues like authentication, data integrity, and confidentiality. They discuss the various wireless intrusion detection system and analysis the performance and listed the wireless system in detection rate. It result the designing challenges of the manet's IDS, which is require the distributed system design and it is lacked in recent available wireless IDS system design. Rafathsamrin and D Vasumathi*et al.* 2017 presented review on the anomaly-based intrusion detection system. They use differ data set and algorithms to analyze the performance and security aspects of the anomaly based network. They use KDD cup data set to analyze different proportion of the system. It results the drawbacks of the previous IDS system and they describe the solution to overcome the problem. Azad *et al*. 2017 proposed the optimization techniques and neural network classification using the fuzzy min-max logic. They use KDD 99 data set, the system provide the adaption facility on online system and minimize the learning timing of the system. It results the improvement of system classification error and accuracy. They also improve the performance of the system.

Altwaijry*et al*. 2012 proposed the classification of Bayesian based intrusion detection system with KDD 99 dataset. The system is able to improve the classifier and detect the intrusion in high positive rate. It result the improvement in system accuracy. The only drawback of this system is lack of probability data availability. Sivanantham*et al*. 2019 presented the comparison of adaptive boosted classifier and anomaly based intrusion detection system. This author research is comparison of three different classifiers performance and system throughput. They use the native bayes classifier, correlation based and random tree algorithm for comparison. In this process they conclude the system to minimize the attacking rate in anomaly based intrusion detection with the detection rate of 98.79% and best accuracy rate of 99.98% in native bayes network. Kunal singh*et al*. 2019 presented the comparison analysis of the IDS by using the deep belief network and state preserving extreme learning algorithms to identify the performance of the system. In this comparison they use the NSL-KDD dataset. It results the accuracy of 52.8% in deep belief network algorithm and 66.83% in state preserving extreme learning machine algorithm. The deep belief network takes computational time of 90.8 seconds and state preserving extreme learning machine takes 102 seconds to detect the intrusion.

Md Zahangiralom*et al*. 2015 proposed the online digital system intrusion detection mechanism by using the deep belief neural network. The object of this research is to detect and protect the system from intrusion attacks and also prevent the system from malicious attacks by using Deep Belief Neural Network (DBN) algorithm. Wang *et al*. 2017 proposed novel intrusion detection system called hierarchical spatial-temporal feature-based intrusion detection system (HAST-IDS).their system used the deep convolutional neural network for learning the low-level spatial features of network traffic, LSTM networks (long short-term memory networks) for learning high-level temporal features. They used the standard DRAPA and ISCX2012 dataset to evaluate the performance of their proposed system. Their model is computationally expensive compared to our approach because they used two stages for feature learning. David ahmad effendi *et al*. 2017 proposed the system to detect the intrusion by manual detection algorithms to prevent the system from malicious attacks. They create a

system patterns to detect the intrusion. This system only detects the normal attacks and not used for strong and new intrusion detection attacks.

Jianguo Yu *et al.* 2018 proposed the subway BAS intrusion detection on the expert system. The authors design the subway model, which is focus on the knowledge base inference engine based intrusion detection system. This model is used to identify the anomalous attacking and prevent system by the defined rule. The system separates the rules by black and white rules to control the system from intrusion. Klymashyulia & strykhalyukbogdam 2017 proposed the intrusion system to increase distribution system reliability. The authors use the support vector machine and restricted Boltzmann machine algorithm to prevent the system from intrusion attacks. They use the KDD-99 dataset to analyze the false positive and negative rate of the system. The research results the better accuracy in combination two algorithms. Ashfaq *et al.* 2017 developed a new method by using the fuzziness approach based on semi-supervised learning for intrusion detection. This method uses a neural network with random weights and plays an important role in the detection rate of NIDS because it decreases the computational cost. The model was evaluated on the NSL-KDD dataset but the performance of the model was studied on only the binary classification task.

Justin Lee *et al.* 1999 presented a survey on Intrusion detection analysis method. They discusses about two major problems in IDS are statistical and rule-based behavior analysis. D.-Y. Yeung & C. Chow, *et al*. 2002 proposed a non-parametric density estimation method based on parse- window estimators with Gaussian kernels and Normal distribution. It is based on ensemble of decision trees. L Ertöz*et al.* 2013 proposed the performance of the shared nearest neighbor (SNN) based ID model it was reported as the best algorithm with high detection rate. It reduces the datasets they were able to report that SNN performed well in comparison to the K-means for U2R attack. However, the system failed to show the entire dataset testing report. W. Li, *et al.* 2004 proposed the Generic algorithm based NIDS was facilities to the model for temporal and spatial- information to identify the complex anomalous behavior. C. Koliass*et al.* 2011 proposed the model as Swarm intelligence techniques for IDS using Ant colony optimization and Colony clustering and particle swarm optimization of systems.

Mukherjee *et al*. 2012 proposed the native bayes classification to improve the accuracy of the classification in the intrusion detection system. They use the NSL-KDD dataset for training and test the classification algorithms. The authors also use the feature vitality based reduction method algorithm with native bayes classification to decrease the intrusion in the system. Wang *et al*. 2010 proposed the classification methodology based on the artificial neural network and fuzzy clustering to increase the performance of the intrusion system. The authors use the KDD-CUP 1999 dataset for training and testing. The training data set is dividing the sub dataset by using the fuzzy clustering then they apply the artificial neural network to reduce the complexity in the intrusion detection. Saleh *et al*. 2017 proposed the hybrid intrusion detection method. They use the optimized support vector machine and prioritized K-nearest neighbors classification algorithms to increase the intrusion detect rate. The authors use the KDD-CUP-99 data set for training and testing.

Al-yaseen*et al*. 2017 proposed the multilevel hybrid intrusion detection in Extreme Learning Machine (ELM) & Support Vector Machine (SVM) based on the redefined K- means algorithm. The proposed system is used to decrease the training time in the classification and improve the detection efficiency in intrusion detection. Amiri *et al*. 2011 proposed the IDS based on modified mutual information based feature selection by using the KDD CUP 1999 dataset. The system is used to increase the detection efficiency and it also improves the accuracy in the remote to local and user to root attacks. Elbasiony*et al*. 2013 proposed the hybrid IDS network based on the weighted K-means and random forest algorithms to detect the intrusion in the network with improvement in the false positive rate. Zhang *et al*. 2008 proposed the IDS based on the random forest algorithm to increase the IDS detection accuracy. The authors use the KDD-99 dataset, and this methodology used in misuse and anomaly detection systems. Thaseen*et al*. 2016 proposed the network IDS system based on SVM multi class & chi-square feature selection algorithm to improve the detection accuracy in the network attacks. The authors use the KDD_CUP 99 data set for training and testing the classification models.

Sindhu *et al*. 2012 proposed the IDS system with decision tree algorithm by using the wrapper method. This system reduces the classifier computational time and complexity, also removes the redundant of the system to reach the detection rate improvement. Changcheng wang 2015 proposed the system for infrared dim small detection by using the traffic queue based pipeline filter algorithms to improve the efficiency in IR detection false rate. Chen Yang *et al*. 2013 proposed the semi supervised clustering technique in the multispectral images by using the affinity propagation algorithm. This system increases the performance of the system and corrects the accuracy in the matrix similarity. Patricnader*et al*. 2014 proposed the IDS for SCADA system by using the one class classification algorithm with machine learning approach. The authors use the two possible approaches of one class classification algorithm such as kernel component analysis and support vector data description algorithms to detect and analyse the cyber-attacks in the system

Iberia Medeiros *et al*. 2016 proposed the system to detect and remove the vulnerability in web application by static analysis & data mining algorithms. This system protects the network protocols and automatically detects the vulnerability in the program codes with more accuracy. Omar y *et al*. 2016 proposed the botnet IDS by cluster-based partitioning & data randomization approach. This system includes the machine learning algorithms such as deep neural network, reduced error pruning tree, random tree, and C4.5 to improve the detection rate in the botnet IDS. Amreen Sultana &M.A.Jabbar*et al.* 2016 proposed the system to detect malicious activity in the network IDS. The authors describe security threads, privacy issues in the social networks and online transaction. The methodology uses the Averaged One-Dependence Estimator algorithm to improve the classification strategies, detection rate and performance in the network IDS.

Yuliaet al. (2017) proposed an intrusion detection based on the expert system. The authors designed the subway model, which focuses on the knowledge base inference engine. Their model used defined rule set to identify the anomalous traffic. Their system separates the rules by black and white rules to control and differentiate the system from intrusion and normal traffic [23]. SibiChakkaravarthyetal.(2018) proposed the intrusion system to increase wireless system reliability. The authors used the Tandem Queuing Model and Kernel Density Estimation to detect the intrusions and attacks. They used their own self-developed dataset to analyze the false positive and negative rate of the system. Their research results the better accuracy in combination of the two algorithms [13]. SibiChakkaravarthy et al. (2020) developed a new model by modelling the leopard behaviour based on semi-supervised learning for intrusion detection. Their method uses a Social Leopard Algorithm with random weights and plays an important role in the detection rate of network traffic. Their model is evaluatedusing the self-developed ransomware dataset but the performance of their model was studied only for the ransomware [1].

The major challenges in the existing machine learning based models always require a high-level design to process the feature set for getting more accuracy. Further, the accuracy of the existing ML models completely depends on the quality and amount of processed features. However, there are many claim raising that their research progress achieves an accuracy of 98% - 99%. However, these are well working models of existing, old and outdated datasets [5]. Further, it is well know that the deep learning based research has solved the above-mentioned issues to some extent. However, the problems related to accurate feature selection, feature interdependencies, feature correlativity etc., makes the model to suffer. A mismatch in the above-mentioned can subject to the reduced accuracy. Moreover, the traffic data, which is fed as the input to the system, is completely varying and non-correlating which is a major problem for DL models [4]. DL models always require a fixed pattern and huge database for accuracy. To address the mentioned issues, this paper utilizes auto-tuning mechanism to self-learn the process of feature learning. This completely removes the barrier of feature correlativity.

4. Proposed Malware Traffic Classification System

Gated Recurrent Units (GRU)

Gated Recurrent Units (GRU) provides solution to the vanishing gradient problem and short-term memory problem. GRU is similar to LSTM with less parameter, so GRU is faster to train than LSTM. Using the internal gates GRU regulates the flow of information. GRU uses hidden states to transfer information instead of cell state. It contains only reset gate and update gate. These two gates can retain information for a long time.

Update gate

They are similar to the forget gate and input gate of LSTM. Deletion or adding of incoming information is decided by the update gate of GRU. The update gate helps in retaining of past information. If the model retains all the past information, the vanishing gradient problem will be eliminated.

The update gate for time t is computed as follows:

$$z_t = \sigma(W^{(z)}x_t + U^{(z)}h_{t-1})$$

Notation	Abbreviation
z_t	Update gate vector
x_t	Input vector
$W^{(z)}$	Weight of the input vector

h_{t-1}	Output vector of previous state.
$U^{(z)}$	Weight of past output vector
Σ	Sigmoid activation function
LSTM	Long Short Term Memory
GRU	Gated Recurrent Unit
RNN	Recurrent Neural Network
CNN	Convolutional Neural Network
MTA	Malicious Traffic Analysis

Table 1: Represents notation and its abbreviation

The result of update gate varies from 0 to 1.

Reset gate

Reset gate decide on the how much past information to be forgotten. Following is the formula to calculate the value of reset gate.

$$r_t = \sigma(W^{(r)}x_t + U^{(r)}h_{t-1})$$

Where r_t is reset gate vector, $W^{(r)}$ and $U^{(z)}$ is weight of input and past output vector.

Current memory content

A new memory content which will use the reset gate to store the past relevant information. It is calculated as follows

$$h_t = tanh(Wx_t + r_t \odot Uh_{t-1})$$

The Hadamard (element-wise) product is calculated between the reset gate r_t and Uh_{t-1}, which decides the information removal of previous state.

Final memory at current time step

Finally, theh_t vector is calculated, the information of current unit is passed down for update gate. The current memory content h'_tgives information to the output vector. The h_t is calculates as follows:

$$h_t = z_t \odot h_{t-1} + (1 - z_t) \odot h'_t$$

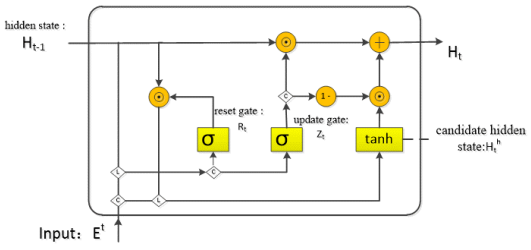

Figure 1: Gated Recurrent Unit

GRU can be used to efficiently predict network traffic. Prior prediction of huge volume of network traffic might help in DDoS attack detection, some of the influx traffic of HTTP, TCP and ICMP initiated by DDoS attack can be disguised as normal traffic. GRU works best in such scenarios.

K-means algorithm

K-means is a supervised leaning approach in machine learning. It used as clustering algorithms for training and testing the data sets. This algorithm clustering the data by point of similar data in the cluster and differentiate the neighboring clusters. It is one of the iterative approaches to clustering the data with possible or similar groups in the clustering. K-means algorithm follows given steps to process the data.

Step 1: identify the number clustering attributes in the dataset denoted as k.

Step2: initialize the fix the centroids by shuffling data and then select the k points with randomly chosen centroids without any replacements.

Step3: repeat step1 and step2 until no changes in the centroid value.

Step4: identify the closer cluster from the centroid.

Step5: calculate average of the data points in every clusters.

5. Experimental Setup

Figure 2 shows the experimental setup used for the dataset collection. A single standalone computer with three independent VM is used to generate the traffic. Normal transactions are performed for 24 hours to collect the normal data whereas for abnormal or malicious traffic generation the attacks as listed in the Table 1 are launched and all the traffic were tapped for a duration of 10 hours.

Legitimate traffic is captured and saved as different pcap files. Each pcap file size is around 700MB. The split up among pcap file is to avoid the bigger sized file, which may leadsto loading and processing problem. Each pcap file is extracted for useful information with the self-written python script. The extracted information are processed and stored in the separate csv file with label for each record.

Legitimate traffic is captured and saved as different pcap files. Each pcap file size is around 400MB. The extracted information are processed and stored in the separate csv file with label for each record. The test bed hosting machine is protected with anti-virus and intrusion detection system. AV and IDS are deployed to flag the attack traffic as malicious. The present pcap file totally sized around 4.79 GB.

The conventional approach to process the data is to build a detection model which automatically gets executed and monitors the traffic flow in a secured environment.

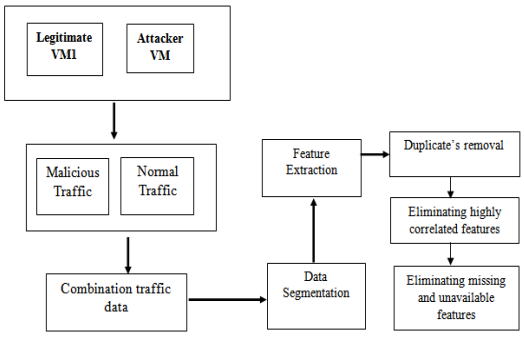

Figure2. Experimental setup used for dataset collection.

6. Dataset Description

The dataset used for experimentation includes the self-developed dataset (Refer Table 2) and MTA-KDD'19 (Refer Table 3).

Table2. Description of the dataset processed and validated in real time.

Category	Description	Size in GB
Benign	Normal traffic which includes traffic of torrent client such as utorrent, Office 365, Zoom, Teams, Watchdog, WhatsApp web	46 GB

Malicious	Malicious traffic includes attack traffic of BlackNurse, a self-developed DDoS attack tool, Various malicious malwares downloaded from virustotal	50 GB

Table 3: Description of MTA-KDD'19

Category	Description	Size in GB
Benign	Normal traffic which includes traffic features such as Number of connections, SynAcksynRatio, TCP flags {Ack,Syn,Fin,Psh,Urg,Rst}, IP features {TCP,UDP,DNS}, Other statistical features such as MaxLen, MinLen, AvgLen, StdDevLen, MaxIAT, MinIAT, AvgIAT, AvgDeltaTime, MaxLenRx, MinLenRx, AvgLenRx, StdDevLenRx, MaxIATRx, MinIATRx, AvgIATRx,StartFlow, EndFlow, DeltaTime, FlowLen, FlowLenRx, packet features such as packet information, packet input/output ratio, packet length, Repeated packet length ratio, small and large packet length ratio, DNS features such as DNSQDist,DNSADist,DNSRDist,DNSSDist, URL features such as AvgDomainChar, AvgDomainDot, AvgDomainHyph, AvgDomainDigit, ValidUrlRatio, average time-to-live (TTL), Number of destination address, Number of ports, Distinct User Agent, Average Distinct User Agent Length, HTTP packets etc.	7.1 GB
Malicious	Abnormal traffic which includes traffic features such as Number of connections, SynAcksynRatio, TCP flags {Ack,Syn,Fin,Psh,Urg,Rst}, IP features {TCP,UDP,DNS}, Other statistical features such as MaxLen, MinLen, AvgLen, StdDevLen, MaxIAT, MinIAT, AvgIAT, AvgDeltaTime, MaxLenRx, MinLenRx, AvgLenRx, StdDevLenRx, MaxIATRx, MinIATRx, AvgIATRx,StartFlow, EndFlow, DeltaTime, FlowLen, FlowLenRx, packet features such as packet information, packet input/output ratio, packet length, Repeated packet length ratio, small and large packet length ratio, DNS features such as DNSQDist,DNSADist,DNSRDist,DNSSDist, URL features such as AvgDomainChar, AvgDomainDot, AvgDomainHyph, AvgDomainDigit, ValidUrlRatio, average time-to-live (TTL), Number of destination address, Number of ports, Distinct User Agent, Average Distinct User Agent Length, HTTP packets etc.	4.7 GB

7. Results And Analysis

In this section we highlights the performance of the proposed GRU based malicious traffic classification system with the existing state of the art deep learning models. The use of random forest for best feature selection plays a major role. Further, the use of GRU on the MTA KDD'19 dataset allows for a much lesser human guesswork required than other approaches such as mRMR or MIFS. The dataset while being optimized for malware analysis still has 33 features, most of which do not have high correlations with each other, this fact alone causes severe problems during training using methodologies such as a standard dense network or even while using a CNN based neural network. The inherent nature of Random Forest of "bagging" different decision trees to find the best feature possible allows us to skip the step of optimizing the dataset further such as the methods used by (Letteri et al., 2020 [26]).

	Accuracy	**Precision**	**Recall**
Random Forest	97.07	97.09	97.07
K-means algorithm	97.06	97.08	97.06
Bayesian network	87.46	87.70	85.41

JMI	84.35	85.25	84.35
CMIM	88.19	88.52	88.21
DISR	81.27	81.56	81.26
Random Forest + GRU+ K-means algorithm	99.97	99.97	99.99

Table 4: Comparison with MI Algorithm Ranking

From Table 4, we can clearly see that while MI ranking algorithms such as the Random Forest applied on to the dataset provide for very high scores, they still do not match up with the robust approach of the random forest whilst finding the most relevant feature in the dataset. Beyond that, also applied the ranking while reducing the overall number of features from the dataset, see Figure 3, to make the process of finding the most relevant feature from the 33 features, this process can also be ignored while using Random Forests since they adds additional randomness to the model, while growing the trees. Instead of searching for the most important feature while splitting a node, it searches for the best feature among a random subset of features. This results in a wide diversity that generally results in a better model while still being able to operate on all the 33 features.

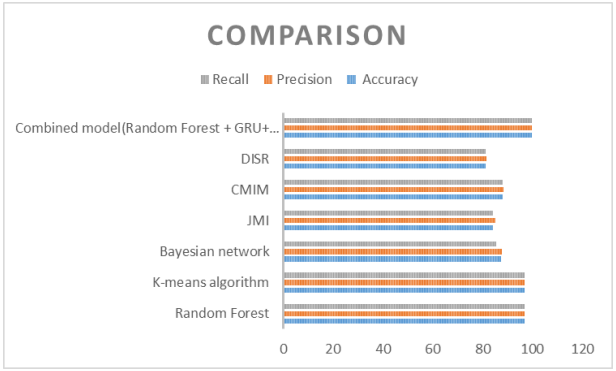

Figure 3: Comparison of combined model vs other ml algorithms

Looking at the ROC curve obtained, see Figure 4, by using Random Forests we can see that we achieve the best possible results between the true positive rate and false positive rate for a predictive model using different probability thresholds. As we can see clearly, the all the evaluation metrics have improved rather than fallen while using Random Forests even while applying no feature selection or dimension reduction algorithms. While optimization of the dataset allows for further advantages such as having a smaller model for online training, the time taken to train the Random Forest was negligible compared to strategies such as using Auto Encoders as experimented (Letteri et al., 2020 [26]). Thus the usage of our model should be applicable in most scenarios whilst still providing for a small and fast model that out performs current state of the art models.

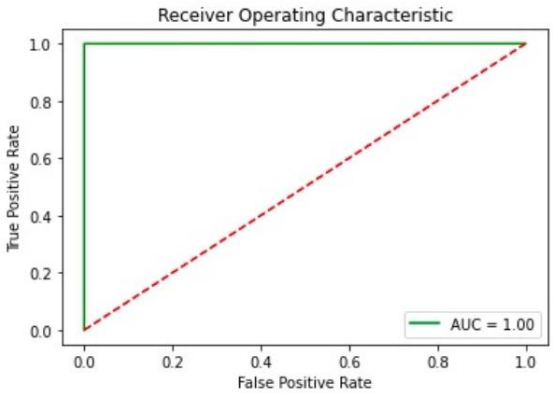

Figure 4: ROC curve plot for the proposed GRU based traffic classification system.

8. Conclusion

In this research, we presented a robust malicious traffic classification system. From the experimental results, it is clearly shown that the proposed method is effective in classifying the malicious traffic. Furthermore, the classification results exhibits that the proposed combined model can accurately classify the traffic with nearly 99% accuracy in overall with less than 1% False Positives and False negatives. The robustness of the proposed system is less packet flow inspection due to reduced and pre-processed dataset. The proposed system examines the flow by averaging the packets sum costing around 4 packets per flow and not more than 100 bytes from each packet. Hence, the classification time taken to detect malicious traffic is much reduced at the rate of 2.78% in increased efficiency. In future, the security researchers may focus on the optimization methods used in the functional components of neural networks for building an effective online traffic classification system.

References

[1] S. Jayaprakash and K. Kandasamy, "Database Intrusion Detection System Using Octraplet and Machine Learning," 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, 2018, pp. 1413-1416, doi: 10.1109/ICICCT.2018.8473029.

[2] W. Hu, W. Hu and S. Maybank, "AdaBoost-Based Algorithm for Network Intrusion Detection," in IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), vol. 38, no. 2, pp. 577-583, April 2008, doi: 10.1109/TSMCB.2007.914695.

[3] A. K. Idrees, W. L. Al-Yaseen, M. A. Taam and O. Zahwe, "Distributed Data Aggregation based Modified K-means technique for energy conservation in periodic wireless sensor networks," 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM), 2018, pp. 1-6, doi: 10.1109/MENACOMM.2018.8371007.

[4] I. S. Thaseen and C. A. Kumar, "An integrated intrusion detection model using consistency based feature selection and LPBoost," 2016 Online International Conference on Green Engineering and Technologies (IC-GET), 2016, pp. 1-6, doi: 10.1109/GET.2016.7916729.

[5] A. Koziolek, L. Happe, A. Avritzer and S. Suresh, "A common analysis framework for smart distribution networks applied to survivability analysis of distribution automation," 2012 First International Workshop on Software Engineering Challenges for the Smart Grid (SE-SmartGrids), 2012, pp. 23-29, doi: 10.1109/SE4SG.2012.6225713.

[6] C. Wang, Y. Shen, D. Zhang and Y. Cai, "A dynamic queue based pipeline filter for infrared dim small target detection," 2015 34th Chinese Control Conference (CCC), 2015, pp. 3770-3775, doi: 10.1109/ChiCC.2015.7260222.

[7] Y. Yan, L. Chen and C. K. Chan, "MVS-based semi-supervised clustering," 2013 9th International Conference on Information, Communications & Signal Processing, 2013, pp. 1-5, doi: 10.1109/ICICS.2013.6782907.

[8] P. Nader, P. Honeine and P. Beauseroy, "${l_p}$-norms in One-Class Classification for Intrusion Detection in SCADA Systems," in IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2308-2317, Nov. 2014, doi: 10.1109/TII.2014.2330796.

[9] N. Al-Falahy and O. Y. K. Alani, "The Impact of Higher Order Sectorisation on the Performance of Millimetre Wave 5G Network," 2016 10th International Conference on Next Generation Mobile Applications, Security and Technologies (NGMAST), 2016, pp. 1-5, doi: 10.1109/NGMAST.2016.20.

[10] I. Medeiros, N. Neves and M. Correia, "Equipping WAP with WEAPONS to Detect Vulnerabilities: Practical Experience Report," 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2016, pp. 630-637, doi: 10.1109/DSN.2016.63.

[11] A. Sultana and M. A. Jabbar, "Intelligent network intrusion detection system using data mining techniques," 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), 2016, pp. 329-333, doi: 10.1109/ICATCCT.2016.7912017.

[12] K. Zwolak et al., "An unmanned seafloor mapping system: The concept of an AUV integrated with the newly designed USV SEA-KIT," OCEANS 2017 - Aberdeen, 2017, pp. 1-6, doi: 10.1109/OCEANSE.2017.8084899.

[13] S. SibiChakkaravarthy, D. Sangeetha, M. V. Cruz, V. Vaidehi and B. Raman, "Design of Intrusion Detection Honeypot Using Social Leopard Algorithm to Detect IoT Ransomware Attacks," in IEEE Access, vol. 8, pp. 169944-169956, 2020, doi: 10.1109/ACCESS.2020.3023764.

[14] R. Mohan, V. Vaidehi, Ajay Krishna A, Mahalakshmi M and S. S. Chakkaravarthy, "Complex Event Processing based Hybrid Intrusion Detection System," 2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN), 2015, pp. 1-6, doi: 10.1109/ICSCN.2015.7219827.