Network Traffic Classification Using Deep Autonomous Learning Approach

N. G. Bhuvaneswari Amma

1 Introduction

The exponential growth of the Internet has contributed to today's dynamic, large scale, and complex networks [8]. These networks experienced an exponential rise of traffic owing to the increased usage of smart devices and are vulnerable to attacks. Despite the recent advancements in computer networks and its security, current network protection solutions against never-ending Distributed Denial of Service (DDoS) attacks remain open challenge for the research community. These DDoS attacks target critical Internet services with the deceptive goal of making online crucial services inaccessible on time to legitimate users. As the technology advances, the frequency and size of DDoS attacks are also on the increase. This attack follows many to one structure and if the attack is initiated, the complexity and impact become proportionally high. The reason for these attacks is the availability of enormous amount of attack tools in the Internet. Even a novice can launch such attacks with the available tools [9]. Therefore, classification of network traffic is a challenge and design of an autonomous attack detection system is needed for on the fly detection of DDoS attacks in evolving large network traffic data streams [10].

Nowadays attack detection can be performed using statistical, data mining, and machine learning approaches. Among these approaches, the research community is preferring deep learning-based attack detection systems that learn the network traffic by identifying correlations in the traffic with different learning levels [7]. The deep learning techniques used for attack detection includes Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), Long Short Term Memory (LSTM), auto-encoder, etc. These conventional deep learning approaches perform static and offline-based detection. In reality, the network traffic evolves as data streams, i.e., continuous arrival of traffic data which requires on the fly detection of DDoS attacks.

N. G. Bhuvaneswari Amma (✉)
Indian Institute of Information Technology Una, Himachal Pradesh 177 005, India
e-mail: bhuvaneswari@iiitu.ac.in

U. P. Rao et al. (eds.), *Security, Privacy and Data Analytics*, Lecture Notes in Electrical Engineering 848, https://doi.org/10.1007/978-981-16-9089-1_15

In order to achieve this objective, incremental learning can be used which learns the evolving data as and when it arrives [6]. The incremental learning algorithms adapt to rapidly changing network environments [10]. Further, these algorithms perform well on classifying known and unknown classes of network traffic. These characteristics motivated to propose a Deep Autonomous Learning (DAL) classifier which automatically extracts and learns features to classify the network traffic data stream. The arriving new classes are learned by incorporating a generalized structure for each of the new class with the existing structure. The key contributions are listed as follows:

1. A Deep Autonomous Learning (DAL) structure to construct network traffic classification system.
2. A DAL methodology to train the network traffic classification system.
3. DAL classifier to classify the network traffic.

2 Related Works

This section discusses the existing literature related to the proposed approach. DDoS attacks shut down the targeted server or network by flooding with huge Internet traffic either partially or fully. The goal of the attacker is to disrupt the normal traffic flow to the targeted server or network. In the earlier days, the DDoS attacks were generated from a single machine and launched to a single server. Nowadays, as low security Internet of Things (IoT) devices, viz., web cameras, monitoring devices, printers, etc., evolved, these attacks were generated from single or multiple machines and launched to single or multiple servers or devices [1]. These IoT devices were compromised to form a botnet to reroute high traffic to the servers for disrupting the regular services. Therefore, the research community is on urge to design and develop network traffic classification systems.

The function of the attack detection models is to detect the known and unknown DDoS attacks and to discriminate the normal traffic from the attack traffic. If DDoS attack detection system is used, legitimate users are not denied while requesting for a service or accessing the service [11]. Recently, the DDoS attacks detection systems are designed based on deep learning techniques that accurately assign weights in stages for learning the network traffic data in each processing layer in abstract way. From the literature, it is studied that the existing deep learning approaches used for attack detection include CNN, RNN, LSTM, and auto-encoder [2, 12]. These methods are capable of handling data in fixed network capacity leading to static and offline detection of attacks. But the attackers are creating intelligent IoT botnets to generate traffic. These evolving traffic can be handled by techniques that are capable of adapting to dynamically changing network environments. To overcome this issue, Deep Autonomous Learning (DAL) can be used for DDoS attacks detection. The DAL is a continual learning algorithm in which the learning model can be constructed

from scratch without an initial network model [10]. The incremental and flexible nature of DAL motivated to propose a DAL-based network classification approach.

3 Proposed DAL-Based Network Traffic Classification

DAL classifier is proposed to detect DDoS attacks by extracting the relevant features and learns the extracted features automatically by adapting to dynamically changing network environments. It consists of learning and classification modules. The learning phase learns the extracted features automatically using Fully Connected Network (FCN) with Distilled Cross Entropy (DCE) [4]. The detection phase uses the learning modules in the DAL-based attack detection except DCE computation. The architecture of the DAL traffic classification is depicted in Fig. 1. The learning module is depicted using solid lines and the classification module is depicted using dotted lines.

3.1 Network Traffic Data Representation

The network traffic dataset is denoted as $NT_D = [ntr_1, ntr_2, \ldots, ntr_k, C_m]$, where $ntr_a = [ntf_{a1}, ntf_{a2}, \ldots, ntf_{an}]$, $1 \leq a \leq k$, is the ath network traffic data record

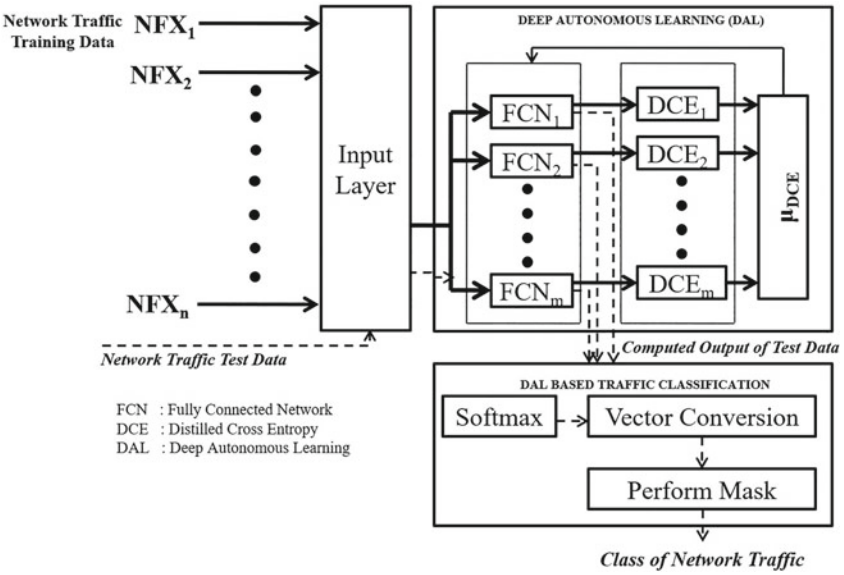

Fig. 1 Architecture of proposed DAL-based network classifier

and C_m be the class of the traffic data. The network traffic features are in the following forms: binary, continuous, and ordinal. The ordinal values are converted to numerical using ordered numbers. Furthermore, the features are normalized using min-max normalization in the range of 0–1. The raw data is normalized as follows:

$$NFX_n^k = \frac{ntf_n^k - min_{fn}}{max_{fn} - min_{fn}}, \tag{1}$$

where ntf_n^k is the data to normalize, min_{fn} is the minimum value of the feature, and max_{fn} is the maximum value of the feature. The normalized data is passed to the proposed DAL-based traffic classifier for learning and classification.

3.2 Deep Autonomous Learning

The DAL module consists of multiple Fully Connected Networks (FCNs) and the number of FCNs are based on the classes in the traffic dataset. As the traffic evolves due to the technology advancement, there is a possibility of new class of attacks to be generated. To tackle this situation, a FCN for the new class of attack needs to be added in the learning network structure. The structure of FCN is $NFX_i - 9 - 7 - 1$, where NFX_i be the number of input features. The reason behind this structure is that the extracted features are learned layer-wise with different level of abstractions. The normalized network traffic is passed to the input layer and this layer passes the traffic to the FCN.

The computation in the hidden layers (HLs) is performed by computing the product of the sum of the values of the transformed pooling layer with the corresponding weights and is as follows:

$$I_j^{HL_i} = \sum_{i=1}^{p} NFX_i \times W_{ij}^{HL_i}, \tag{2}$$

where W^{HL} is the weight vector from input layer to HL. In the HL, Rectified Linear Unit (ReLU) activation function has been utilized and computed as follows:

$$f_{RL}\left(I_j^{HL_{i+1}}\right) = max\left(I_j^{HL_i}, 0\right). \tag{3}$$

The computation in the output layer of FCNs is performed as follows:

$$O_i^c = \sum_{i=1}^{p} HL_i \times W_{jk}^{HO} + B, \tag{4}$$

where B is the Bias term which is added to place the traffic record to the suitable class. In the output layer, sigmoid activation function has been utilized and computed as follows:

$$f_{Sig}\left(O_i^c\right) = 1/(1 + exp^{-O_i^c}). \tag{5}$$

The rate of loss in the learning process is computed using Distilled Cross Entropy (DCE). The DCE provides generalization ability by distilling the knowledge gained from the model and is computed as follows:

$$DCE_l(DT_i, DO_i) = -\sum_{i=1}^{n} DT_i log\left(DO_i\right), \tag{6}$$

where $DT_i = (T_i)^{1/D}$, T_i is the target class in the training dataset and $DO_i = (O_i)^{1/D}$, O_i is the computed output, D is the distillation parameter, and l ranges from 1 to m. The training continues till the mean of DCE reaches the threshold and is computed as follows:

$$\mu_{DCE} = \frac{1}{m} DCE_l. \tag{7}$$

3.3 DAL-Based Network Traffic Classification

The DAL-based traffic classification is similar to that of the learning procedure but instead of DCE, the softmax is used to classify the type of traffic. The reason for using softmax activation function is to squash the output between 0 and 1 which is similar to sigmoid activation function but it also divides the output in such a way to make the sum of the output is equal to 1 and computed as follows:

$$f_{SM}\left(O_{ij}\right) = \frac{Exp\left(O_{ij}\right)}{\sum_{j=0}^{k} Exp\left(O_{ij}\right)}. \tag{8}$$

The output of softmax is converted to a vector and the class of the network traffic is detected using the vector value.

Table 1 Statistics of datasets

Dataset	Feature	Training data		Testing data	
		Normal	DDoS attack	Normal	DDoS attack
KDD Cup	41	97278	391458	60593	229057
NSL KDD	41	13449	9195	2152	3603
UNSW NB	48	20520	4076	56000	12264

4 Results and Discussions

Experiments were conducted on desktop PC under Windows 10 with Intel Core 2 Quad CPU Q9650 @ 3.00 GHz processor and 16 GB RAM. MATLAB R2019a was utilized for constructing the traffic classification model and also to test the proposed classifier. The datasets used for experimentation are KDD Cup, NSL KDD, and UNSW NB15. Table 1 tabulates the statistics of datasets. For experimentation, normal and DDoS attacks traffic in the benchmark datasets are only considered [3].

4.1 DCE Loss Computation in Autonomous Learning

The number of FCNs used for training in DAL module were 6 for KDD Cup, 6 for NSL KDD, and 2 for UNSW NB based on the number of classes in each of the datasets. Figure 2 depicts the DCE loss variation for different epochs. It is observed from the graphical representation that the proposed approach converges around 82th epoch for KDD Cup dataset, 78th epoch for NSL KDD dataset, and 89th epoch for UNSW NB dataset. As the number of classes in UNSW NB is small, the convergence of UNSW NB dataset becomes slow. It is observed that the DAL works better for more number of classes. The proposed classifier acts as a framework as the FCN and DCE blocks to be added for the upcoming new target classes which satisfies on the fly detection.

4.2 Performance Evaluation of Proposed DAL Classifier

The performance of the proposed classifier is evaluated using the following metrics: True Positive Rate (TPR), False Positive Rate (FPR), Accuracy, Loss Rate, and Area Under the Curve (AUC) [9]. The performance metrics are tabulated in Table 2. It is noted from table that the achievement of accuracy 99.62% for KDD Cup dataset, 99.77% for NSL KDD dataset, and 97.16% for UNSW NB dataset with the loss rate of 0.38% for KDD Cup dataset, 0.23% for NSL KDD dataset, and 2.84% dataset for UNSW NB dataset using the proposed DAL approach.

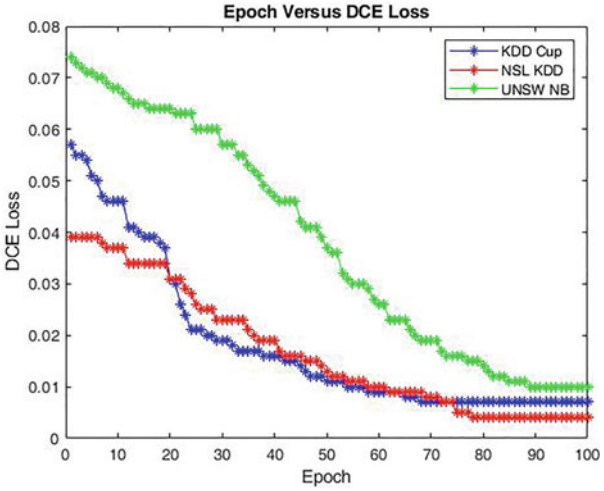

Fig. 2 Epoch versus DCE loss

Table 2 Performance metrics of proposed approach

Dataset	Performance metrics				
	FPR(%)	TPR(%)	Accuracy (%)	Loss rate(%)	AUC(%)
KDD Cup	0.12	99.55	99.62	0.38	99.71
NSL KDD	0.19	99.75	99.77	0.23	99.78
UNSW NB	2.71	96.53	97.16	2.84	96.91

Table 3 Comparison of proposed classifier with state-of-the-art classifiers

Classifier/Year	Accuracy (%)	FPR (%)
Reference [12]/2017	83.34	–
Reference [2]/2018	99.3	0.7
Reference [5]/2018	98.23	0.33
Reference [1]/2019	99.69	0.28
Proposed DAL	99.77	0.19

The proposed classifier was compared with four state-of-the-art deep learning classifiers. The reported results tabulated in Table 3 are for the experiments conducted using NSL KDD dataset. It is observed that the proposed classifier exhibits significant performance compared to the existing classifiers in terms of accuracy and FPR.

5 Conclusion

In this article, DAL classifier is proposed for on the fly classification of traffic in computer networks. The objective is to overcome the static nature of learning process in the existing deep learning classifiers. The features of network traffic were extracted and trained using DAL module. The performance of the proposed DAL classifier was analyzed using benchmark network traffic datasets by considering only the normal and DDoS attack records. It is evident from the results that the proposed classifier achieves promising performance for all the datasets. As part of the future work, the number of nodes in the hidden layers of FCN be optimized using evolutionary algorithms.

References

1. Amma BN, Selvakumar S (2019) Deep radial intelligence with cumulative incarnation approach for detecting denial of service attacks. Neurocomputing 340:294–308. https://doi.org/10.1016/j.neucom.2019.02.047
2. Amma NGB, Subramanian S (2018) Vcdeepfl: Vector convolutional deep feature learning approach for identification of known and unknown denial of service attacks. In: TENCON 2018-2018 IEEE region 10 conference. IEEE, pp 0640–0645
3. Amma NB, Selvakumar S, Velusamy RL (2020) A statistical approach for detection of denial of service attacks in computer networks. IEEE Trans Netw Serv Manag 17(4):2511–2522. https://doi.org/10.1109/TNSM.2020.3022799
4. Hinton G, Vinyals O, Dean J (2015) Distilling the knowledge in a neural network. arXiv:1503.02531
5. Idhammad M, Afdel K, Belouch M (2018) Semi-supervised machine learning approach for ddos detection. Appl Intell 1–16. https://doi.org/10.1007/s10489-018-1141-2
6. Istrate R, Malossi ACI, Bekas C, Nikolopoulos D (2018) Incremental training of deep convolutional neural networks. arXiv:1803.10232
7. Mishra P, Varadharajan V, Tupakula U, Pilli ES (2018) A detailed investigation and analysis of using machine learning techniques for intrusion detection. IEEE Commun Surv Tutor 21(1):686–728. https://doi.org/10.1109/COMST.2018.2847722
8. Moustafa N, Slay J, Creech G (2017) Novel geometric area analysis technique for anomaly detection using trapezoidal area estimation on large-scale networks. IEEE Trans Big Data 5(4):481–494. https://doi.org/10.1109/TBDATA.2017.2715166
9. NG BA, Selvakumar S (2020) Anomaly detection framework for internet of things traffic using vector convolutional deep learning approach in fog environment. Future Gener Comput Syst **113**, 255–265. https://doi.org/10.1016/j.future.2020.07.020
10. Pratama M, Ashfahani A, Ong YS, Ramasamy S, Lughofer E (2018) Autonomous deep learning: Incremental learning of denoising autoencoder for evolving data streams. arXiv:1809.09081
11. Shone N, Ngoc TN, Phai VD, Shi Q (2018) A deep learning approach to network intrusion detection. IEEE Trans Emerg Top Comput Intell 2(1):41–50. https://doi.org/10.1109/TETCI.2017.2772792
12. Yousefi-Azar M, Varadharajan V, Hamey L, Tupakula U (2017) Autoencoder-based feature learning for cyber security applications. In: 2017 International joint conference on neural networks (IJCNN). IEEE, pp 3854–3861