TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214
DOI: 10.26599/TST.2020.9010022
Volume xx, Number x, xxxxxxx 20xx

Intrusion Detection System using Voting based Neural Network

Mohammad Hashem Haghighat∗, Jun Li∗

Abstract: Several security solutions have been proposed to detect network abnormal behavior. However, successful attacks are still a big concern in computer society. Lots of security breaches like DDoS, Botnets, spam, phishing and so on are reported every day, while the number of attacks are still increasing.

In this paper, a novel voting based deep learning framework, called VNN, is proposed to take the advantage of any kinds of deep learning structures. Considering several models created by different aspects of data and various deep learning structures, VNN provides the ability to aggregate the best models in order to create more accurate and robust results. Therefore, VNN helps the security specialists to detect more complicated attacks.

Experimental results over KDDCUP'99 and CTU-13 as two well known and more widely employed datasets in computer network area, revealed the voting procedure was highly effective to increase the system performance, where the false alarms were reduced up to 75%, in comparison with the original deep learning models including DNN, CNN, LSTM, and GRU.

Key words: Deep Learning; Voting based Neural Network; Network Security; Pearson Correlation Coefficient.

1 Introduction

Computer network plays an important role in nowadays life. Various internet based services like Voice over IP, internet banking, P2P file sharing, online gaming, and so on have been using every day. However, the number of network malicious activities are increasing dramatically [1]. According to McAfee, “Ransomware Attacks” as type of malware aiming at blocking the access of a user to its computer until specific amount of money is paid, are increasing by 118% during 2019 [2].

Dozens of behavior-based detection techniques have been proposed to protect networks from such attacks. The key challenge of these methods is to lowering the false alarms using machine learning algorithms [3–14].

Nowadays, deep learning provides a suitable infrastructure to automatically learn features from raw data. This advantage enables the scientists to employ deep learning techniques in different areas like natural language processing, image and voice recognition, and computer networks.

Generally, various types of deep learning models have been developed including Deep Neural Network (DNN), Recurrent Neural Network (RNN), Convolutional Neural Network (CNN), Boltzmann Machine (BM), and Stacked Auto-Encoder (SAE).

RNNs enable previous outputs to be used for the input of the next step as depicted in Figure 1. Since RNNs are suitable for time series data, they are widely utilized in network anomaly based detection techniques in the literature.

Kim et. al. applied RNN to IDS and achieved magnificent results on KDDCUP'99 [16]. They improved their method by employing LSTM as the learning engine which the performance test showed the

• Mohammad Hashem Haghighat is with Department of Automation, Tsinghua University, Beijing,China. E-mail: l-a16@mails.tsinghua.edu.cn
• Jun Li is with Research Institute of Information Technology, Tsinghua University, Beijing, China. E-mail: junl@tsinghua.edu.cn
∗ To whom correspondence should be addressed.
Manuscript received: 2020-03-24; revised: 2020-07-02; accepted: 2020-07-10

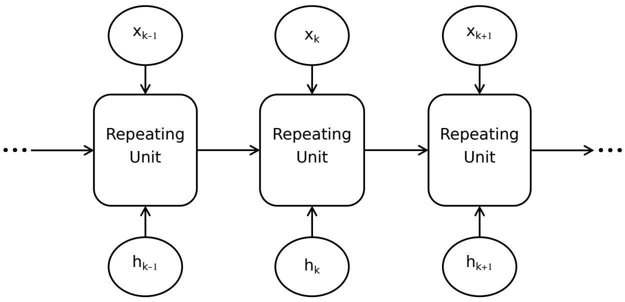


Fig. 1 RNN Architecture [15].

system was suitable for IDSes [17]. Chuan-long et. al. in [18, 19] compared the performance of RNN with traditional machine learning methods including Naive Bayes, Random Forest, and SVM using KDDCUP'99 in both multi-class and binary classifiers and revealed RNN overwhelmed all the traditional methods well. A Gated Recurrent Unit Recurrent Neural Network (GRU-RNN) was proposed by Tuan Tang et. al. [20] with the performance of 89% on KDDCUP'99 using only 6 raw features.

CNN is a special deep learning architecture firstly developed for image recognition problem. However, Yu et. al. proposed a CNN based method to detect time-delayed attacks. The authors reported that the method was highly accurate for DARPA'98 dataset [21]. Wu et. al. in [22] employed CNN in order to select traffic properties automatically from raw dataset. They evaluated the method by KDDCUP'99 and argued that the method performs better in terms of performance and false alarm rate, compared to the conventional standard algorithms.

SAE is a specific type of Neural Network with the exactly the same size output of its input. The main goal if SAE is to reconstitute of the output from the input. Figure 2 depicts the SAE architecture where the input is compressed and then decompressed to compute the output.

Aminento et. al. in [23] applied SAE as a classifier on KDDcup'99 dataset and presented four different IDSes: Application Layer IDS, Transport Layer IDS, Network Layer IDS, and Data Link Layer IDS. Then Niyaz et. al. used SAE to learn features from NSLKDD in [24].

Farahnakian et. al. proposed Deep Auto Encoder (DAE) to extract features from high dimensional data. They achieved more than 97% detection precision in case of using 10% KDDcup'99 as test case [25].

BM is a type of Stochastic RNN to make decisions concerning being either on or off. BM provides the

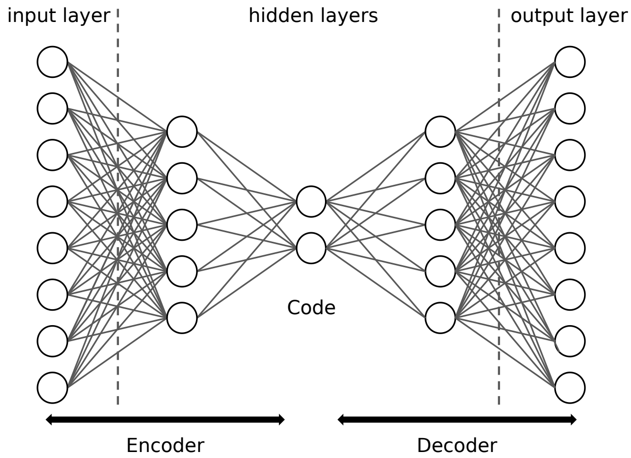


Fig. 2 SAE Architecture.

ability to simply learn systems and provide interesting features from datasets having binary labels [26].

A multi-layer DoS attack detection technique based on Deep Boltzmann Machine (DBM) was provided by Ni GAO et. al. [27]. The authors argued that their method gained better precision on KDDCUP'99 compared to SVM and simple ANN. Xueqin Zhang [28] sped up the training time by combining SVN, BM, and Deep Belief Network (DBN). Khaled et. al. achieved 97.9% precision on 10% KDDCup'99 dataset as the test case [29]. Recently Vinayakumar et. al. in [30–34] provided a comprehensive study of various CNN, LSTM, CNN-LSTM, CNN-GRU, and DNN to select the optimal network architecture using KDDCUP'99 and NSLKDD datasets.

Haghighat et. al. [35] also developed a sliding window based deep learning technique (called SAWANT) which achieved 99.952% accuracy on CTU-13 dataset. The authors used only one to ten percent CTU-13 dataset as training to conduct their tests.

The aforementioned methods took the advantage of deep learning to detect network malicious activities. Although their performance was considerable, aggregating different deep learning models provides the capability to utilize the strength of each model and detect attacks incredibly more efficient.

In this paper we propose "Voting based Neural Network (VNN)" as a general infrastructure voting based mechanism to aggregate and take the advantages of any kinds of deep learning algorithms. In other word, several deep learning based models can be created by the state-of-the-art techniques, with different performance. Giving test data, VNN provides a procedure to perform a weighted voting function on the most suitable models to achieve higher accurate results. Due to selecting and aggregating only the best models for each test sample, VNN incredibly boosted the system accuracy. Experimental results proved our argument as the false alarms were reduces up to 75%.

Table 1 summarized all the relevant acronyms employed throughout the paper.

Table 1 Acronyms used through the paper

Acronym	Expression
VNN	Voting based Neural Network
DDoS	Distributed Denial of Service
ANN	Artificial Neural Network
DNN	Deep Neural Network
CNN	Convolutional Neural Network
RNN	Recurrent Neural Network
LSTM	Long Short-Term Memory
GRU	Gated Recurrent Unit
BM	Boltzmann Machine
SAE	Stacked Auto-Encoder
SNM	Support Vector Machine
P2P file sharing	Point to Point file sharing

The paper is structured as follows. In section 2, an overview of VNN is explained. Then, VNN is deeply studied by two well-known KDDCUP'99 and CTU-13 datasets in sections 3 and 4, using two different configurations: high and low accuracy, respectively. Finally, in section 5, the paper is concluded and future research plans are explained.

2 Voting based Neural Network

Voting based Neural Network (VNN) is a general infrastructure to create several models using different aspects of data or various types of deep learning architectures, and merging them, aiming at increasing the system performance.

As illustrated in VNN architecture (Figure 3), several inputs are extracted from the original data to be modeled by various kinds of deep learning techniques like DNN, CNN, RNN, SAE, and so on. As a result, in the prediction phase, a heuristic function called "Voting Engine" processes all the models to select the best candidates in a way to minimize the errors. The chosen models perform voting procedure in order to predict test data label. Algorithm 1 describes the whole VNN procedure in detail.

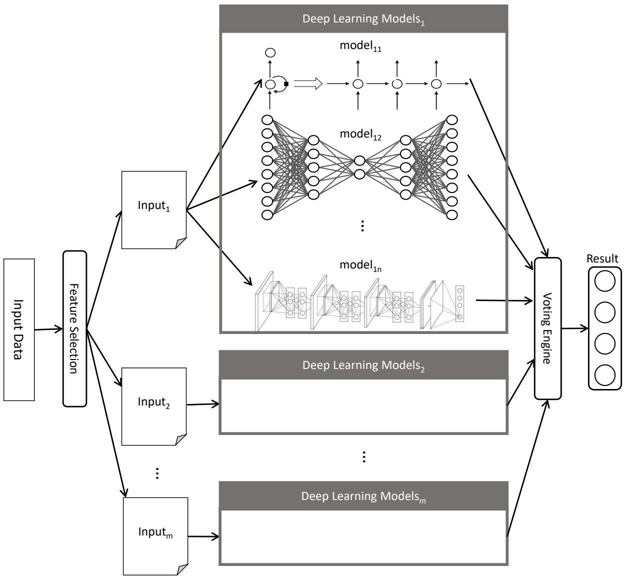


Fig. 3 VNN Architecture.

Algorithm 1 VNN Whole Procedure.

input1: $train_{data} = \{\vec{F_1}, \vec{F_2}, \cdots, \vec{F_l}\}$ //input train Data
input2: $test_{data} = \{\vec{F_1}, \vec{F_2}, \cdots, \vec{F_l}\}$ //input test Data
where $\vec{F_i} = \{\vec{a_{i_1}}, \vec{a_{i_2}}, \cdots, \vec{a_{i_k}}\}$// k different attributes
input3: $\Theta = \{\theta_1, \theta_2, \cdots, \theta_n\}$ //n different models
output: Prediction Result
//Initialization
$\psi \longleftarrow \{\}$ //empty set as training data
$\omega \longleftarrow \{\}$//empty set as testing data
$\Delta \longleftarrow \{\}$//empty set as prediction results
$\Xi \longleftarrow \{\}$//empty set as voting candidates
//selecting n different train and test feature
vectors with randomely chosen attibutes
for $i \longleftarrow range(1, n)$
  $A \longleftarrow$ randomely select i attricuted
  $\Psi_i \longleftarrow select_attributes(train, A)$
  $\Omega_i \longleftarrow select_attributes(test, A)$
end
foreach models θ_i, train data ψ_j, and test data ω_j
  $model_{ij} \longleftarrow$ train(θ_i, ψ_j)//Train model
  $\Delta_{ij} \longleftarrow$ predict($model_{ij}$, ω_j)//Prediction Result
end
$\Delta' \longleftarrow$ select best voting candidates
result $\longleftarrow$ vote(Δ')
return result

In the next two sections different case studies on well known KDDCup'99 and CTU-13 datasets are presented to make the voting procedure clearer.

3 Case Study 1: KDDCUP'99

KDDCUP'99 [36] is the mostly used dataset to evaluate anomaly based detection systems in the literature [37]. The dataset was built based on DARPA'98 project [38] and contains about 4.9 million records including 41 different features with normal and four attack types (Denial of Service, User to Root, Remote to Local, and Probing) labels. Hereafter, Tavallaee et al. removed the duplicated records of KDDCUP'99 to create NSLKDD dataset [39]. Figure 4 shows the evolution of NSLKDD dataset.

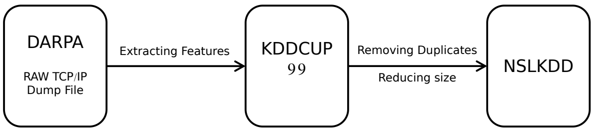


Fig. 4 Evolution of NSLKDD dataset [40].

3.1 Voting Procedure

The main idea behind VNN is to make a general infrastructure to create several models using different deep learning approaches or data aspects. Then, given a test sample, select those models whose likely more suitable to find the accurate label.

Definition 1 Let n be the number of models. Uncertainty factor γ of the i^{th} model is defined according to the following equation.

$$\gamma_i = 1 - \rho_i \tag{1}$$

where ρ_i is the probability of the output layer achieved by the i^{th} model.

The below procedure is defined to select k best candidate models of the voting procedure.

- Considering ζ_i as the accuracy of i^{th} model reported by the system training procedure, normalize all ζ values according to "Normal Distribution Equation" provided by equation 2 [41].

$$f(x, \mu, \delta) = \frac{1}{\sqrt{2\pi}\delta} e^{-\frac{(x-\mu)^2}{2\delta^2}} \tag{2}$$

- Assuming λ as "Unsatisfied Models Threshold (UMT)", remove all the models whose their normalized accuracy are less than λ.
- Consider "Total Uncertainty (TU)" threshold as ϵ.
- Sort all the remained models based on their uncertainty factors in ascending order.
- Select the models until the total sum of uncertainty factor (γ_i) is less than ϵ.
- Perform the majority voting mechanism on the selected models.

Algorithm 2 describes the procedure in detail.

Algorithm 2 Multi-class Output Best Model Selection.

```
input1: Γ = {γ1, γ2, ··· , γn} //Uncertainety factors of n models
input2: Z = {ζ1, ζ2, ··· , ζn} //Accuracy of the models
input3: ε //Total uncertainty threshold
input4: λ //Unsatisfied model threshold
output: Δ as set of k best models
//Initializing the voting parameters
E ⟵ 0 //Total sum of uncertainty factors
Δ ⟵ {} //Inittializing the output
M ⟵ {} //Inittializing the set of satisfies models

foreach ζi ∈ Z
    ni ⟵ normalize(ζi)
    if ni > λ
        //Adding corresponding uncertainty factor to M
        M ⟵ add(γi)
    end
end
Msorted ⟵ sort(M) // Sorting the
while true
    E ⟵ E + pop(Msorted)
    if E > ε
        break
    else
        Add corresponding model to Δ
    end
end
return Δ
```

3.2 Experimental Results

Several test cases were conducted on KDDCUP'99 using different deep learning architectures including CNN, LSTM, GRU, CNN-LSTM, and DNN models. In order to highlight the efficiency of voting mechanism, we configured the hyper parameters of these deep learning techniques using two different approaches to see the impact of the voting procedure on in different situations.

(1) Achieving highly accurate results (performance>99%).

(2) Having lots of false alarms (55%<performance<80%).

Table 2 describes the models hyper parameters configuration in detail.

Table 2 Hyper parameters used to test KDDCUP'99

Hyper Parameters	Values
Train Size	90%
Test Size	10%
Dropout	0.5
Batch Input	On
Activation Function	Relu
CNN #Layers	4
LSTM #Layers	2
CNN-LSTM #Layers	4
DNN #Layers	2
GRU #Layers	2
#Input attributes	37
#Input subsets	38
Output	binary, five-classes
UMT	0.7
TU	0.5

Generally, 90% of KDDCUP'99 were chosen to train the models, while the rest of 10% were used for testing. In addition, 38 different training and testing datasets were generated from the input data, in which each dataset includes 37 random KDDCUP'99 attributes. We conducted binary classification as our highly accurate test, while the less accurate test was performed based on five-classes classifier. Figures 5 depicts the accuracy reported by the system during the training phase.

As illustrated in Figure 5, 0.7 was chosen for UMT where all the models with less normalized accuracy values than UMT were removed.

The voting procedure was conducted over the remained models and the result was depicted by Figure 6. The results proved that VNN increased the true responses magnificently in both higher and less accurate deep learning structures. VNN resolved 708 errors out of 1804 (more than 39%) for binary classification based GRU architecture, and 63,675 false alarms out of about 85,000 (around 75%) for five-class classification based CNN-LSMT models. The detailed number of false alarms and their correction rates were explained by Table 3.

Table 3 KDDCUP'99 Error Correction.

	Method	#Errors	#Corrections	Correction Rate
Binary	DNN	777	29	3.73%
	CNN	872	97	11.12%
	LSTM	1,551	551	35.53%
	CNN-LSTM	993	148	14.90%
	GRU	1,804	708	39.25%
Five-classes	DNN	205,439	25,497	12.41%
	CNN	205,306	7,463	3.64%
	LSTM	208,849	81,263	38.90%
	CNN-LSTM	85,068	63,675	74.85%
	GRU	208,513	28,374	13.61%

We also performed the voting procedure over all the models created by any deep architectures, in which the performance result is summarized in Tables 4 and 5.

Table 4 KDDCUP'99 Binary Classification Confusion Matrix.

		Predicted		
		Normal	Malicious	Total
Actual	Normal	301031	203	301234
	Malicious	486	188121	188324
	Total	301519	188324	489843

Different measurements of the experiment including False Positive Rate, False Negative Rate, Accuracy,

Table 5 KDDCUP'99 five-classes Classification Confusion Matrix.

		Predicted					
		Normal	DoS	R2L	U2R	Probing	Total
Actual	Normal	277269	219	20608	0	0	298096
	DoS	490	188107	5	7	0	188609
	R2L	0	62	3060	0	0	3122
	U2R	0	1	0	0	0	1
	Probing	0	14	1	0	0	15
	Total	277759	188403	23674	7	0	489843

Precision, Recall, and F_Score are computed in Table 6. These values were achieved by the equations 3 to 8.

$$FPR = \frac{FP}{FP+TN} \tag{3}$$

$$FNR = \frac{FN}{FN+TP} \tag{4}$$

$$Precision = \frac{TP}{TP+FP} \tag{5}$$

$$Recall = \frac{TP}{TP+FN} \tag{6}$$

$$Accuracy = \frac{TP+TN}{All\ Data} \tag{7}$$

$$F\_Score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{8}$$

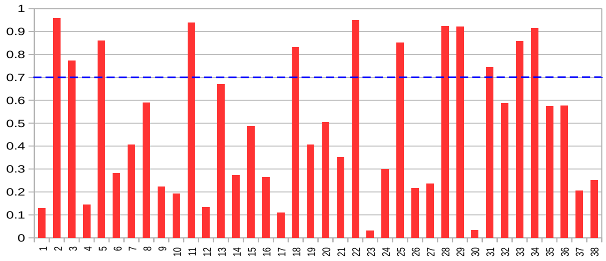
Table 6 KDDCUP'99 False Positive and Negative Rates, Accuracy, Precision, Recall, and F_Score.

	FPR	**FNR**	**Accuracy**	**Precision**	**Recall**	**F_score**
Binary Classification	0.0011	0.0016	0.9986	0.9993	0.9984	0.9989
5-classes Classification	0.0982	0.0021	0.9563	0.9302	0.9979	0.9628

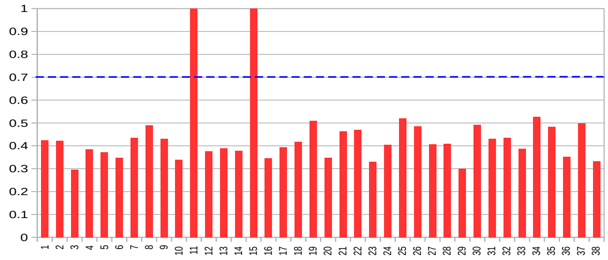
The result proved that VNN achieved higher accuracy compared to any deep learning structures for both binary and five-class classifiers efficiently. Figure 7 compares VNN with DNN, CNN, LSTM, CNN-LSTM, and GRU methods.

4 Case Study 2: CTU13

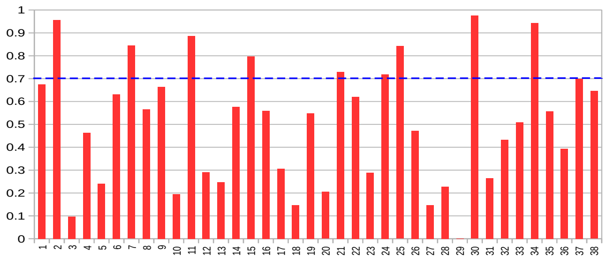
CTU13 contains thirteen days labeled traffic, captured by CTU University, Czech Republic, in 2011 [42]. It has about twenty million netflow records including IRC, P2P, HTTP, Fast Flux, Spam, Click Fraud, Port Scan, and DDoS traffic. The goal of CTU13 was to collect a large real botnet traffic mixed with the normal user activities in the network. Table 7 describes the distribution of labels in the netflow traffic per day.



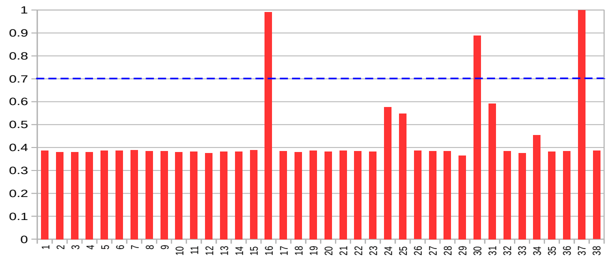
((a)) CNN - binary classes



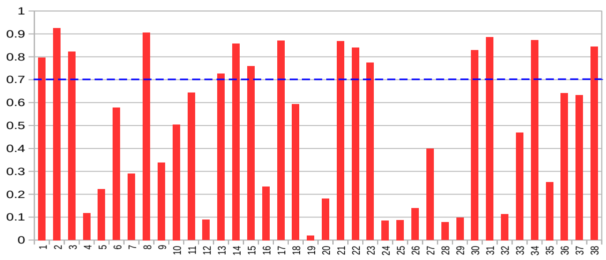
((b)) CNN - five-classes



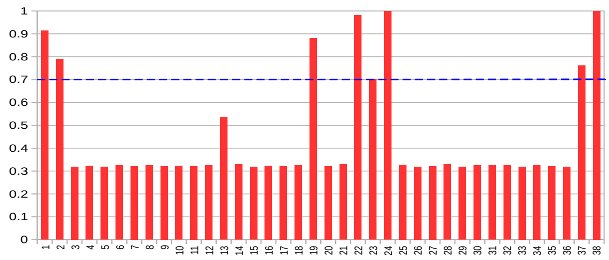
((c)) DNN - binary classes



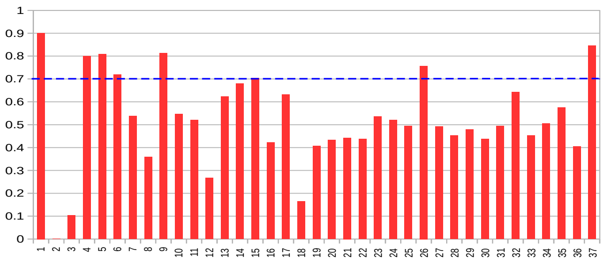
((d)) DNN - five-classes



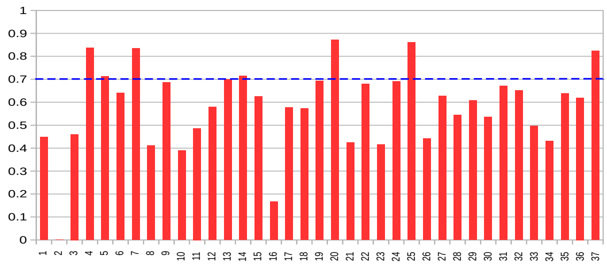
((e)) LSTM - binary classes



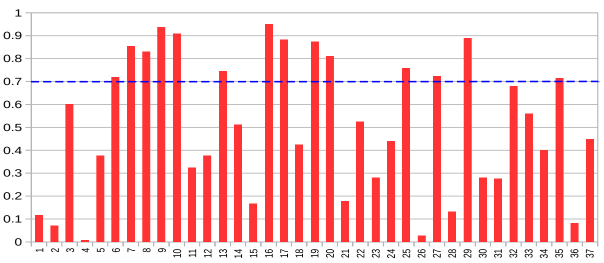
((f)) LSTM - five-classes



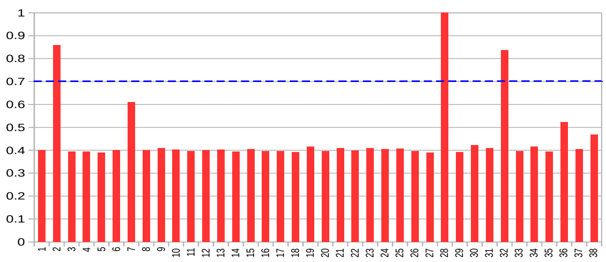
((g)) CNN-LSTM - binary classes



((h)) CNN-LSTM - five-classes



((i)) GRU - binary classes

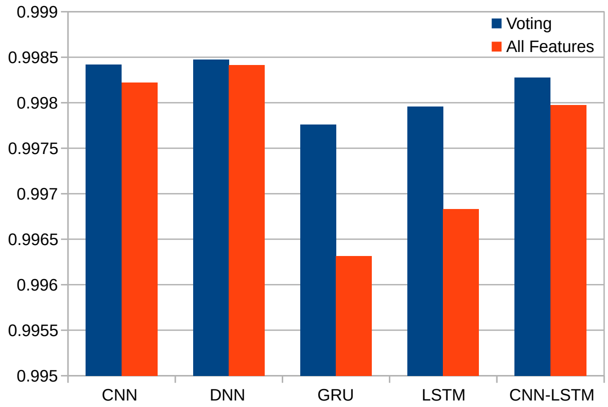


((j)) GRU - five-classes

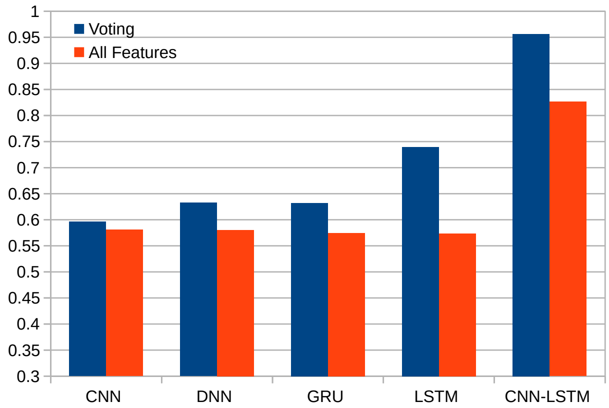
Fig. 5 The normalized form of model accuracy.

4.1 Deep Learning Models

Netflow traffic contains high level network activities information including source IP/Port numbers, destination IP/Port numbers, Protocol, TCP Flags, Flow Duration, Flow Size, Number of Packets, Input and Output SNMP Interface, and Next Hop Router.



((a)) Binary Classification



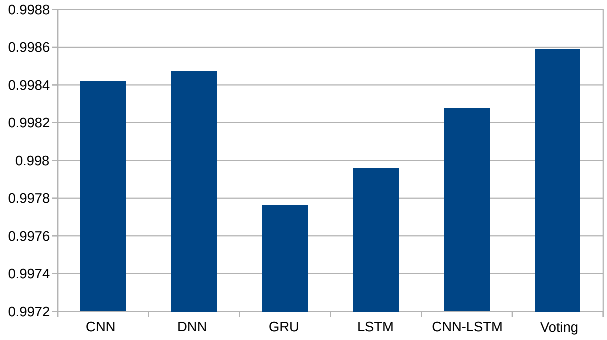
((b)) Five-classes Classification

Fig. 6 System Accuracy: Voting-based vs Normal-based using KDDCUP'99 dataset.

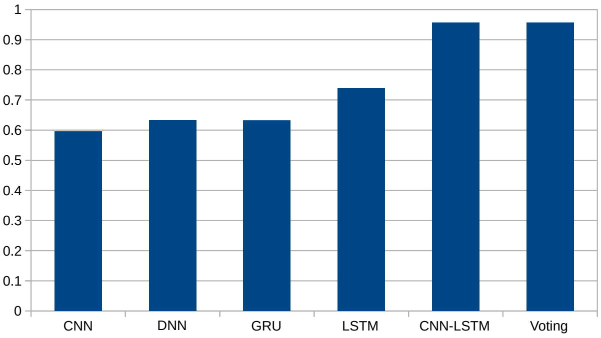
Table 7 CTU13 Label Distribution

Day	#flows	Botnet	Normal	C&C	Background
1	2.82 million	1.41%	1.07%	0.03%	97.47%
2	1.81 million	1.04%	0.5%	0.11%	98.33%
3	4.71 million	0.56%	2.48%	0.001%	96.94%
4	1.21 million	0.15%	2.25%	0.004%	97.58%
5	0.13 million	0.53%	3.6%	1.15%	95.7%
6	0.56 million	0.79%	1.34%	0.03%	97.83%
7	0.11 million	0.03%	1.47%	0.02%	98.47%
8	2.95 million	0.17%	2.46%	2.4%	97.32%
9	2.75 million	6.5%	1.57%	0.18%	91.7%
10	1.31 million	8.11%	1.2%	0.002%	90.67%
11	0.11 million	7.6%	2.53%	0.002%	89.85%
12	0.33 million	0.65%	2.34%	0.007%	96.99%
13	1.93 million	2.01%	1.65%	0.06%	96.26%

These attributes are too simple to be used in a deep learning method to detect network attacks. As a result, Haghighat et. al. in [35] developed a sliding window based technique, called SAWANT (Smart Window based Anomaly detection using Netflow Traffic), in which it aggregates netflow records and extracts several meaningful attributes using sliding window algorithm.



((a)) Binary Classification



((b)) Five-classes Classification

Fig. 7 VNN vs. other deep learning architectures.

4.1.1 SAWANT

The highlighted contribution of SAWANT was the ability to highly accurate training data using a very small subset of netflow records (one to ten percent). As illustrated in Figure 8, new feature vectors were extracted from netflow traffic according to the following procedure. In addition, the label of each vector was called malicious rate, describing how much the aggregated vector was abnormal.

(1) Slide a window of size w through the netflow records.

(2) For each position of the window calculate these attributes:

- Number of unique values of Source IP/Port, Destination IP/port, Duration, Source Bytes, Number of Packets, and Flow Size per incoming and outgoing flows.
- Entropy values of Source IP/Port, Destination IP/port, Duration, Source Bytes, Number of Packets, and Flow Size per incoming and outgoing flows.
- Minimum, Maximum, Average, Sum, and Variance of Duration, Source Bytes, Number

of Packets, and Flow Size per incoming, outgoing, and total flows.

(3) Calculate malicious rate (ρ) as the label of each vector based on equation 9.

$$\rho = \frac{\text{number of malicious netflow records}}{\text{Window Size}} \tag{9}$$

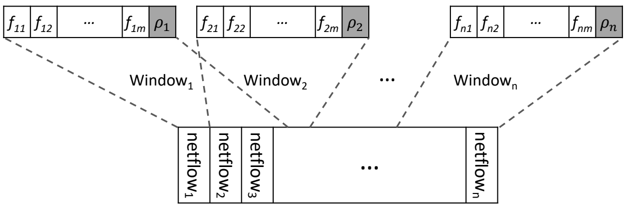


Fig. 8 SAWANT Window based Feature Extraction Procedure.

The new feature vectors were used to train ANN model as depicted in figure 9, where the output layer expressed the malicious rate.

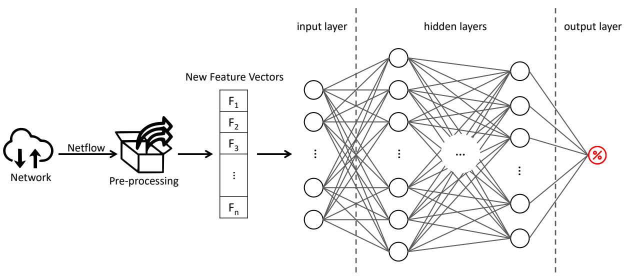


Fig. 9 SAWANT Architecture.

The results of the test dataset were compared with the actual malicious rate values using "Pearson Correlation Coefficient" function, described by equation 10.

$$\begin{aligned} r_{X,Y} &= \frac{E[XY] - E[X]E[Y]}{\sqrt{E[X^2] - E[X]^2}\sqrt{E[Y^2] - E[Y]^2}} \\ &= \frac{\sum_{i=1}^{n} x_i y_i - n\bar{x}\bar{y}}{\sqrt{\sum_{i=1}^{n} x_i^2 - n\bar{x}^2}\sqrt{\sum_{i=1}^{n} y_i^2 - n\bar{y}^2}} \end{aligned} \tag{10}$$

where X and Y were two different variable sets.

Definition 2 Let X and Y be two different data series. X and Y are positively correlated ($r = 1$), where:

$$\forall x_i \in X, y_i \in Y \mid y_i = \alpha x_i + \beta$$

when α and β are two arbitrary numbers.

4.2 Voting Procedure

As described in the previous section, a ranking mechanism is defined in order to select a subset of more probable models to achieve more accurate results, in the voting procedure. The more decisive models were selected in the classification environment (like case study 1 with "malicious" and "benign" classes), the more likely to have more accuracy. However, the main challenge of SAWANT is its predicted malicious rate which is numerical (not categorical). In fact, the SAWANT predicted results were not equal to the actual values respectively, meaning finding more decisive models impossible. Therefore, the aforementioned majority voting procedure explained in section 3.1 is not practical here. As a result, we developed a new heuristic procedure to rank and select better models for any arbitrary test case as t.

- Normalize the accuracy of all the models according to equation 2 and remove less accurate models based on UMT.
- Compute the sum of Pearson Correlation Coefficient (r) of each predicted model with all the others.
- Sort the models based on the computed value and remove the last 50% models.
- For each two remaining predicted sets i and j:
  - Compute α as the Pearson Correlation Coefficient of S_i and S_j ($r(S_i, S_j)$).
  - Remove t from both S_i and S_j and compute β as the Pearson Correlation Coefficient of the two sets ($r(S_i - \{t\}, S_j - \{t\})$).
  - Compare the Pearson Correlation Coefficient calculated from the above steps.
  - mark S_i and S_j are similar for test case t if α is greater than β
- Put similar models into a single set.
- Return the largest set as the voting candidate.
- Compute the result based on the majority voting schema over a the parties inside the selected set.

Algorithm 3 describes the model selection procedure in detail.

Algorithm 3 SAWANT Best Model Selection Procedure.

input1: $\Gamma = \{\gamma_1, \gamma_2, \cdots, \gamma_n\}$ //Predicted Malicous Rates Set
where $\gamma_i = \{pmr_{i_1}, pmr_{i_2}, \cdots, pmr_{i_m}\}$
//Predicted Malicous Rates of m test cases
input2: $Z = \{\zeta_1, \zeta_2, \cdots, \zeta_n\}$ //Accuracy of the models
input3: λ //Unsatisfied model threshold
input4: $pivot$
output: A set of k best γ of the testcase $pivot$
//Initializing the voting parameters
$E \longleftarrow 0$ //Total sum of uncertainty factors

```
Δ ⟵ {} //Inittializing the output
M ⟵ {} //Inittializing the set of satisfies models

foreach ζ_i ∈ Z
    n_i ⟵ normalize(ζ_i)
    if n_i > λ
        //Adding corresponding uncertainty factor to M
        M ⟵ add(γ_i)
    end
end

foreach γ_i, γ_j ∈ M
    δ_{γ_i} ⟵ δ_{γ_i} + r(γ_i, γ_j) //r is Correlation Coefficient
end
Δ_sorted ⟵ sort(Δ)
Γ' ⟵ remain the top 50% Γ based on Δ_sorted
foreach γ_i, γ_j ∈ Γ'
    r ⟵ r(γ_i, γ_j)
    r' ⟵ r(γ_i − {pmr_{i_pivot}}, γ_j − {pmr_{j_pivot}})
    if r is greater than r'
        θ_{i,j} ⟵ 1
    else
        θ_{i,j} ⟵ 0
    end
end
partition Γ' based on Θ
return the largest partition as the voting candidate
```

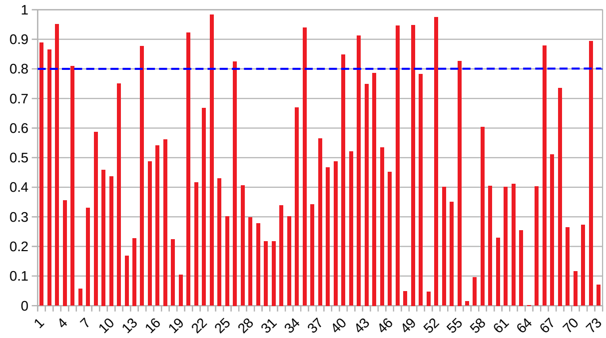
4.3 Experimental Results

We chose DNN, CNN, LSTM, and GRU as the deep learning structure of SAWANT and perform the voting procedure to evaluate VNN. The SAWANT pre-processed data contains 92 different attributes. We extracted 73 unique subsets each containing 72 features. Table 8 explains the hyper parameters to test CTU-13 dataset.

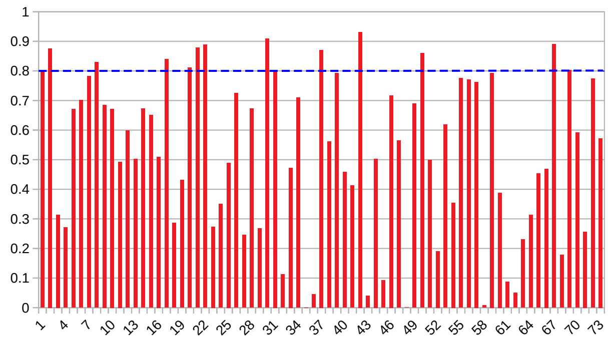
Table 8 Hyper parameters used to test CTU-13

Hyper Parameters	Values
Train Size	10%
Test Size	90%
Dropout	0.2
Batch Input	On
Activation Function	Relu
CNN #Layers	4
LSTM #Layers	2
DNN #Layers	2
GRU #Layers	2
#Input attributes	72
#Input subsets	73
Output	Malicious Rate
UMT	0.8
TU	0.5

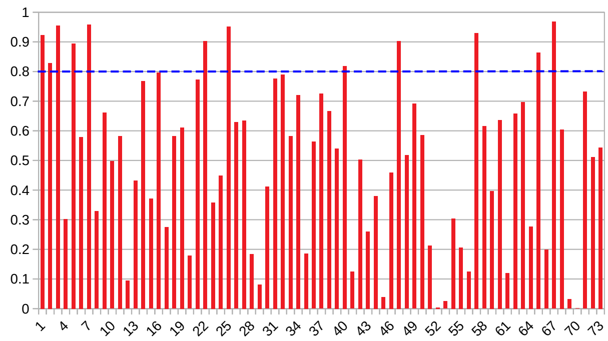
We configured the deep learning structure in a way to result both higher and lower accuracy, in which the performance of DNN, CNN, GRU, and LSTM was 99%, 94%, 76%, and 70%, respectively. UMT was also configured as 0.8 to select better models in the voting procedure. Figure 10 illustrates the accuracy of each model created by various extracted subsets and deep learning architectures.



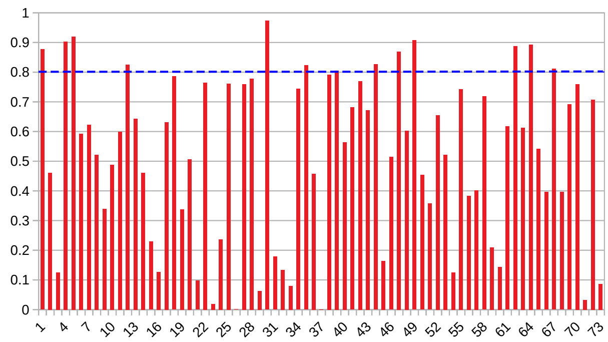
((a)) CNN - Normalized form of Accuracy



((b)) DNN - Normalized form of Accuracy



((c)) LSTM - Normalized form of Accuracy



((d)) GRU - Normalized form of Accuracy

Fig. 10 Model Accuracy - reported by the system during the training phase.

Figure 11 compares the accuracy of VNN with the utilized deep learning structures (DNN, CNN, LSTM, and GRU). VNN decreased false alarms significantly, especially for LSTM and DNN methods where 273K out of 669K errors (around 40%), and 12K out of 17K (about 72%) where corrected, respectively. Table 9 expresses the detail of error correction over CTU-13 dataset.

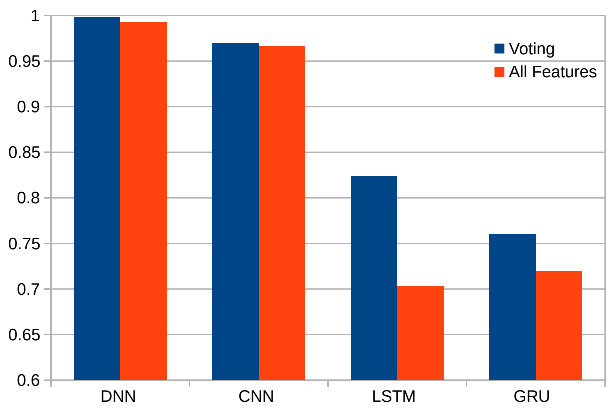


Fig. 11 System Accuracy: Voting-based vs Normal-based using CTU-13 dataset.

Table 9 CTU-13 Error Correction.

Method	#Errors	#Corrections	Correction Rate
DNN	17,112	12,418	72.57%
CNN	76,523	8,251	10.78%
LSTM	668,597	272,507	40.74%
GRU	630,541	90,902	14.42%

Tables 10 and 11 also summarized VNN performance over DNN as the best suited model in our case study.

Table 10 CTU-13 Confusion Matrix.

		Predicted		
		Normal	Malicious	Total
Actual	Normal	2103058	254	2103312
	Malicious	767	145921	146688
	Total	2103825	146175	2250000

Table 11 KDDCUP'99 False Positive and Negative Rates, Accuracy, Precision, Recall, and F_Score.

FPR	FNR	Accuracy	Precision	Recall	F_score
0.0017	0.0004	0.9995	0.9999	0.9996	0.9998

5 Conclusion

This paper presents a novel voting based deep learning framework, called VNN, to correct false alarms reported by other deep learning structures and increase the system performance. The key novelty of VNN was the ability to create several models using various kinds of deep learning structures and different aspects of data, then choosing the best models to achieve higher accuracy.

Experimental results revealed VNN was highly effective for any kinds of deep learning structures with various hyper parameters where it corrected false labels interestingly up to 75%.

Although VNN provides high accurate prediction, creating several models is a really time consuming procedure. In fact, 190 different models were created for each binary and 5-classes classification problems over KDDCUP'99 dataset. 292 models were also generated on CTU-13. In the future, we plan to overcome this issue by developing a heuristic function, in order to ignore generating less effective models in advance. In addition, giving feedback from the candidates and utilizing the results to create more robust deep learning architecture is another direction to work in the future. Deeper analysis on different attack types (e.g. those provided in KDDCUP'99 - DoS, R2L, U2R, and Probing) will gives us a suitable feedback to create more robust models. The proposed method missed U2R and Probing attacks, however the number of samples were too small. But we plan to address this issue in the future.

Acknowledgment

This work was supported by National Natural Science Foundation of China (No. 61872212) and the National Key Research and Development Program of China under Grant No. 2016YFB1000102.

References

[1] SophosLabs research team. Sophos 2020 Threat Report, https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophoslabs-uncut-2020-threat-report.pdf, 2020.

[2] McAfee. McAfee Labs Threats Report, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf, 2019.

[3] S. Behal, K. Kumar and M. Sachdeva, D-FACE: An anomaly based distributed approach for early detection of DDoS attacks and flash events, Journal of Network and Computer Applications, vol. 111, pp.49-63, 2018.

[4] O. Elejla, B. Belaton, M. Anbar and A. Alnajjar, Intrusion detection systems of ICMPv6-based DDoS attacks, Neural Computing and Applications, vol. 30, no. 1, pp.45-56, 2018.

[5] M.H. Haghighat and J. Li, Edmund: Entropy based attack Detection and Mitigation engine Using Netflow Data, in Proc. 8th International Conference on Communication and Network Security., Chengdu, China, 2018, pp. 1-6.

[6] M. Idhammad, K. Afdel and M. Belouch, Semi-supervised machine learning approach for DDoS detection, Applied Intelligence, vol. 48, no. 10, pp.3193-3208, 2018.

[7] D.S. Terzi, R. Terzi and S. Sagiroglu, Big data analytics for network anomaly detection from netflow data, in Proc. 2017 International Conference on Computer Science and Engineering (UBMK)., Antalya, Turkey, 2017, pp. 592-597.

[8] J.M. Vidal, A.L.S. Orozco and L.J.G. Villalba, Adaptive artificial immune networks for mitigating DoS flooding attacks, Swarm and Evolutionary Computation, vol. 38, pp.94-108, 2018.

[9] R. Wang, Z. Jia and L. Ju, An entropy-based distributed DDoS detection mechanism in software-defined networking, in Proc. 2015 IEEE Trustcom/BigDataSE/ISPA., Helsinki, Finland, 2015, pp. 310-317.

[10] G. Aceto, D. Ciuonzo, A. Montieri and A. Pescapé, Multi-classification approaches for classifying mobile app traffic, Journal of Network and Computer Applications, vol. 103, pp. 131-145, 2018.

[11] M. Lotfollahi, M.J. Siavoshani, R.S. Hosseinzade and M.S. Saberian, Deep packet: A novel approach for encrypted traffic classification using deep learning, Soft Computing, vol. 24, no. 3, pp.1999-2012, 2020.

[12] G. Aceto, D. Ciuonzo, A. Montieri and A. Pescapè, MIMETIC: Mobile encrypted traffic classification using multimodal deep learning, Computer Networks, vol. 165, 2019.

[13] N. Mansouri and M. Fathi, Simple counting rule for optimal data fusion, in Proc. 2003 IEEE Conference on Control Applications., Istanbul, Turkey, 2003, pp. 1186-1191.

[14] D. Ciuonzo, A. De Maio and P.S. Rossi, A systematic framework for composite hypothesis testing of independent Bernoulli trials, IEEE Signal Processing Letters, vol. 22, no. 9, pp. 1249-1253, 2015.

[15] A. Khan and F. Zhang, Using recurrent neural networks (RNNs) as planners for bio-inspired robotic motion, in Proc. 2017 IEEE Conference on Control Technology and Applications (CCTA)., Hawaii, USA, 2017, pp. 1025-1030.

[16] J. Kim, and H. Kim, Applying recurrent neural network to intrusion detection with hessian free optimization, in Proc. 2015 International Workshop on Information Security Applications., Jeju Island, Korea, 2015, pp. 357-369.

[17] J. Kim, J. Kim, H.L.T Thu and H. Kim, Long short term memory recurrent neural network classifier for intrusion detection, in Proc. 2016 International Conference on Platform Technology and Service (PlatCon)., Jeju Island, Korea, 2016, pp. 1-5.

[18] C. Yin, Y. Zhu, J. Fei and X He, A deep learning approach for intrusion detection using recurrent neural networks, Ieee Access, vol. 5, pp. 21954-21961, 2017.

[19] S. Althubiti, W. Nick, J. Mason, X. Yuan and A. Esterline, Applying Long Short-Term Memory Recurrent Neural Network for Intrusion Detection, in Proc. IEEE SoutheastCon 2018., Tamba Bay Area, FL, USA, 2018, pp. 1-5.

[20] T.A. Tang, L. Mhamdi, D. McLernon, S.A.R. Zaidi and M. Ghogho, Deep recurrent neural network for intrusion detection in sdn-based networks, in Proc. 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft)., Montreal, Canada, 2018, pp. 202-206.

[21] Y. Yao, Y. Wei, F. Gao and G. Yu, Anomaly intrusion detection approach using hybrid MLP/CNN neural network, in Proc. Sixth international conference on intelligent systems design and applications., Jinan, China, 2006, pp. 1095-1102.

[22] K. Wu, Z. Chen and W. Li, A Novel Intrusion Detection Model for a Massive Network Using Convolutional Neural Networks, Ieee Access, vol. 6, pp. 50850-50859, 2018.

[23] M.E. Aminanto and K. Kim, Deep learning-based feature selection for intrusion detection system in transport layer, in Proc. Summer Conference of Korea Information Security Society (CISC-S'16)., Korea, 2016, pp. 535-538.

[24] A. Javaid, Q. Niyaz, W. Sun and M. Alam, A deep learning approach for network intrusion detection system, in Proc. 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS)., Brussels, Belgium, 2016, pp. 21-26.

[25] F. Farahnakian and J. Heikkonen, A deep auto-encoder based approach for intrusion detection system, in Proc. 2018 20th International Conference on Advanced Communication Technology (ICACT), Gang'weondo, South Korea, 2018, pp. 178-183.

[26] R. Salakhutdinov and G. Hinton, Deep boltzmann machines, in Proc. Twelfth International Conference on Artificial Intelligence and Statistics, Clearwater, Florida USA, 2009, pp. 448-455.

[27] N. Gao, L. Gao, Q. Gao and H. Wang, An intrusion detection model based on deep belief networks, in Proc. IEEE 2014 Second International Conference on Advanced Cloud and Big Data, Huangshan, China, 2014, pp. 247-252.

[28] X. Zhang and J. Chen, Deep learning based intelligent intrusion detection, in Proc. 2017 IEEE 9th International Conference on Communication Software and Networks (ICCSN), GuangZhou, China, 2017, pp. 1133-1137.

[29] K. Alrawashdeh and C. Purdy, Toward an online anomaly intrusion detection system based on deep learning, in Proc. 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA), Anaheim, CA, USA, 2016, pp. 195-200.

[30] R. Vinayakumar, K.P. Soman and P. Poornachandran, A Comparative Analysis of Deep Learning Approaches for Network Intrusion Detection Systems (N-IDSs): Deep Learning for N-IDSs, International Journal of Digital Crime and Forensics (IJDCF), vol. 11, no. 3, pp. 65-89, 2019.

[31] R. Vinayakumar, M. Alazab, K.P. Soman, P. Poornachandran, A. Al-Nemrat and S. Venkatraman, Deep Learning Approach for Intelligent Intrusion Detection System, IEEE Access, vol. 7, pp. 41525-41550, 2019.

[32] R. Vinayakumar, K.P. Soman and P. Poornachandran, Evaluation of recurrent neural network and its variants for intrusion detection system (IDS), International Journal of Information System Modeling and Design (IJISMD), vol. 8, no. 3, pp. 43-63, 2017.

[33] R. Vinayakumar, K.P. Soman and P. Poornachandran, Evaluating effectiveness of shallow and deep networks to intrusion detection system, in Proc. 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Manipal, India, 2017, pp. 1282-1289.

[34] R. Vinayakumar, K.P. Soman and P. Poornachandran, Applying convolutional neural network for network intrusion detection, in Proc. 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Manipal, India, 2017, pp. 1222-1228.

[35] M.H. Haghighat, Z. Abtahi Foroushani and J. Li, SAWANT: Smart Window Based Anomaly Detection Using Netflow Traffic, in Proc. 2019 IEEE 19th International Conference on Communication Technology (ICCT), Xian, China, 2019, pp. 1396-1402.

[36] University of California,Irvine. KDD CUP 1999 dataset, http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html, 1999.

[37] T. Janarthanan and S Zargari, Feature selection in UNSW-NB15 and KDDCUP'99 datasets, in Proc. 2017 IEEE 26th International Symposium on Industrial Electronics (ISIE), Edinburgh, United Kingdom, 2017, pp. 1881-1886.

[38] R.P. Lippmann, D.J. Fried, I. Graf, J.W. Haines, K.R. Kendall, D. McClung, D. Weber, S.E. Webster, D. Wyschogrod, R.K. Cunningham and others, Evaluating intrusion detection systems: The 1998 DARPA off-line intrusion detection evaluation, in Proc. DARPA Information Survivability Conference and Exposition. DISCEX'00, Hilton Head, SC, USA, 2000, pp. 12-26.

[39] M. Tavallaee, E. Bagheri, W. Lu and A. Ghorbani, A detailed analysis of the KDD CUP 99 data set, in Proc. 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, Canada, 2009, pp. 1-6.

[40] A. Özgür and H. Erdem, A review of KDD99 dataset usage in intrusion detection and machine learning between 2010 and 2015, PeerJ Preprints, vol. 4, 2016.

[41] W. Hoeffding, A class of statistics with asymptotically normal distribution, Breakthroughs in Statistics, pp. 308-334, 1992.

[42] CTU. CTU-13 Botnet Traffic dataset, https://mcfp.weebly.com/, 2011.

Mohammad Hashem Haghighat received his B.S. degree in computer engineering from Shiraz Azad University, Shiraz, Iran in 2008, and his M.S. degree in computer engineering from Sharif University of Technology, Tehran, Iran in 2010. He is currently PhD candidate in Tsinghua University, Beijing, China. His research interests include network security, intrusion detection systems, deep learning, and information forensics.

Jun Li Dr. Jun Li is currently Dean of Research Institute of Information Technology, and Vice dean of School of Information Science and Technology, Tsinghua University. He is also a Deputy Director of Tsinghua National Lab for Information Science and Technology, China. Before rejoining Tsinghua University in 2003, Dr. Jun Li was Acting CEO and COO, Director of Operation, Director of Product Development, and GM of Canada and Beijing R&D centers of ServGate Technologies, a network security gateway company he co-founded in 1999. Prior that, Dr. Jun Li worked at EXAR and TeraLogic from 1997 to 1999 as Senior Software Engineer. During his PhD program, Dr. Jun Li worked at Electrical and Computer Engineering Department of NJIT (New Jersey Institute of Technology) as Research Assistant from 1992 to 1997. He worked at Automation Department of Tsinghua University as Teaching Assistant and Lecturer from 1986 to 1992. Dr. Jun Li graduated from Tsinghua University with BS and MS of Automation in 1985 and 1988, respectively. He got his Ph.D. degree in Computer Science from NJIT in 1997.