A Deep Learning Approach for Intrusion Detection in Internet of Things using Focal Loss Function

Ayesha S. Dina, A. B. Siddique, D. Manivannan
Department of Computer Science,
University of Kentucky

Motivation

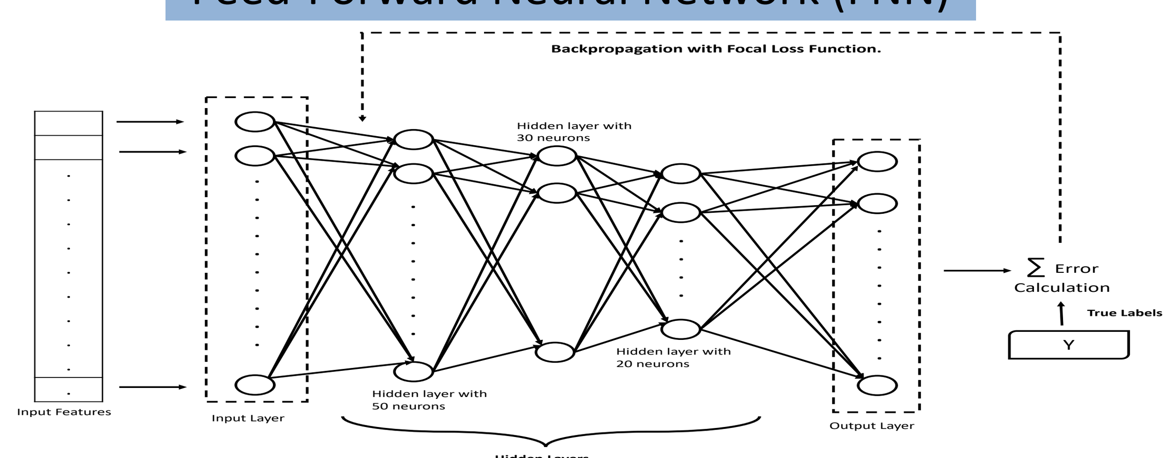
In academia and industry, researchers have used Machine Learning (ML) techniques to design and implement intrusion detection systems (IDSes) for computer networks; however, little has been done for IoT intrusion detection

Researchers trained ML models to predict intrusions using data collected by various organizations. The datasets used in such systems are often imbalanced (e.g., not all classes have the same number of samples).

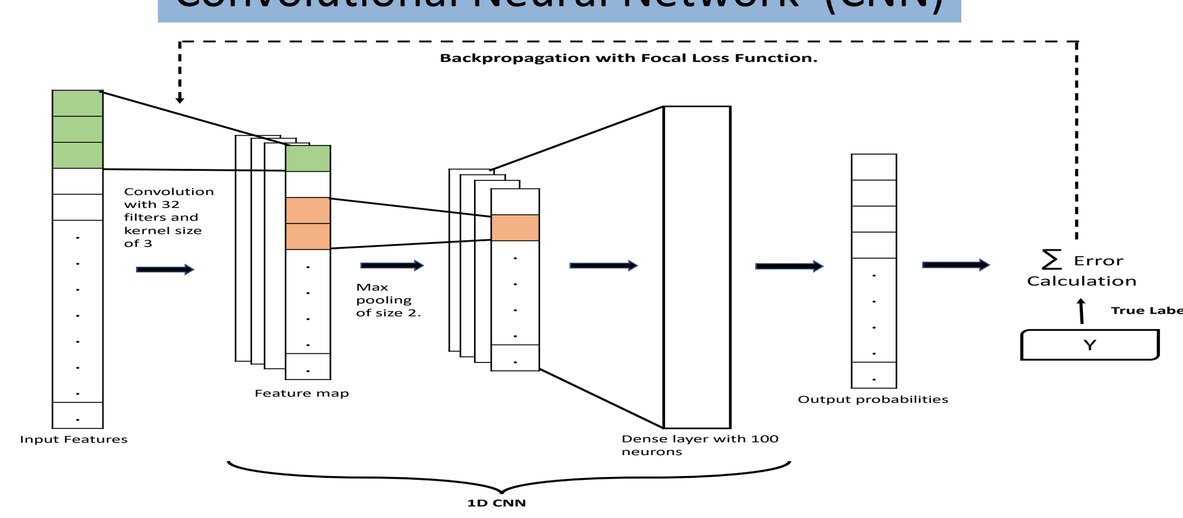
We implemented our approach using two well-known Deep Learning neural networks.. As compared to training them on datasets using cross-entropy loss functions, our approach (training DL models using focal loss function) performed better on accuracy, precision, F1 score, and MCC score by 24%, 39%, 39%, and 60% respectively.

Background

Feed-Forward Neural Network (FNN)



Convolutional Neural Network (CNN)



Methods

➤ Let us consider cross-entropy loss for binary classification

$$CE(p, y) = \begin{cases} -log(p), & \text{if } y = 1 \\ -log(1-p), & \text{otherwise} \end{cases}$$

➤ Focal loss function reshapes the loss function so that easy examples are down-weighted and training focuses on hard examples.

➤ A modulating factor $(1 - p_t)^{\gamma}$ is added to the cross-entropy loss function with a focusing parameter $\gamma \geq 0$. The focal loss defines as follows:

$$FL(p_t) = -(1 - p_t)^{\gamma} log(p_t)$$

Datasets

Data distribution in BoT-IoT

Class	Train	(%)
DDoS	1233052	52.52
DoS	1056118	44.98
Reconnaissance	58335	2.48
Normal	296	0.01
Theft	52	0.002

Data distribution in WUSTL-IIoT-2021

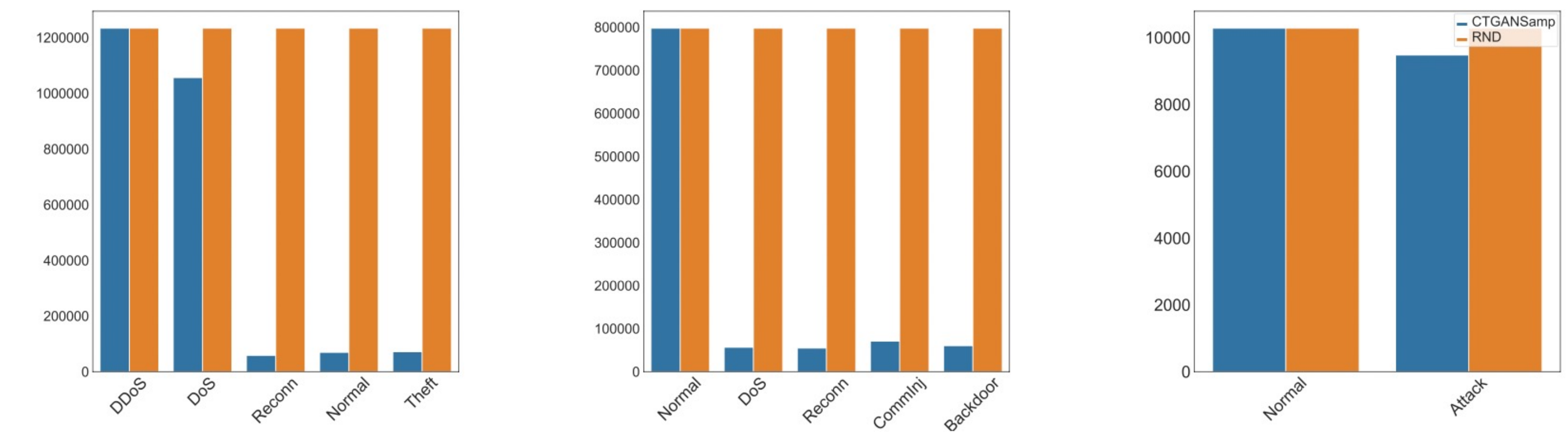
Class	Train	(%)
Normal	797261	92.71
DoS	56379	5.56
Reconnaissance	5932	0.69
Command Injection	185	0.02
Backdoor	152	0.02

Data distribution in WUSTL-EHMS-2020

Class	Train	(%)
Normal	10275	87.47
DoS	1472	12.53

Results

Adding synthetic data using random oversampling and CTGANSamp



(a) Bot-IoT (b) WUSTL-IIoT-2021 (c) WUSTL-EHMS-2020

Quantitative Analysis

Performance metrics used in evaluating ML-models

Metric	Formula for Calculating the Metric
Accuracy (Acc)	$\frac{TP+TN}{TP+TN+FP+FN}$
Precision (Pre)	$\frac{TP}{TP+FP}$
Recall (Rec)	$\frac{TP}{TP+FN}$
F_1 Score	$2 * \frac{Pre*Rec}{Pre+Rec}$
MCC Score	$\frac{TP*TN-FP*FN}{\sqrt{(TP+FP)*(TP+FN)*(TN+FP)*(TN+FN)}}$

- **True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN)**

Performance of the evaluated methods on Bot-IoT

DL Models	Classifier's Name	Acc	Pre	Rec	F_1	MCC
State-of-the-art	CNN-BiLSTM	0.1407	0.2477	0.2563	0.0778	-0.0246
	PB-DID	0.5252	0.1717	0.2037	0.1448	0.0009
FNN	FNN-ORG	0.8834	0.5073	0.6345	0.5436	0.7868
	FNN-RND	0.8614	0.4990	0.4990	0.5275	0.7623
	FNN-CTGANSamp	0.8808	0.4991	**0.8652**	0.5540	0.7885
	FNN-Dice	0.4499	0.0900	0.2000	0.1241	0.0000
	FNN-Focal (This work)	**0.9155**	**0.5559**	0.6380	**0.5784**	**0.8825**
CNN	CNN-ORG	0.6963	0.4434	0.5347	0.4211	0.4753
	CNN-RND	0.8084	0.5349	0.7843	0.5680	0.6550
	CNN-CTGANSamp	0.8168	0.4298	**0.7988**	0.4536	0.6878
	CNN-Dice	0.4499	0.0900	0.2000	0.1241	0.0000
	CNN-Focal (This work)	**0.8677**	**0.6165**	0.6325	**0.5853**	**0.7606**

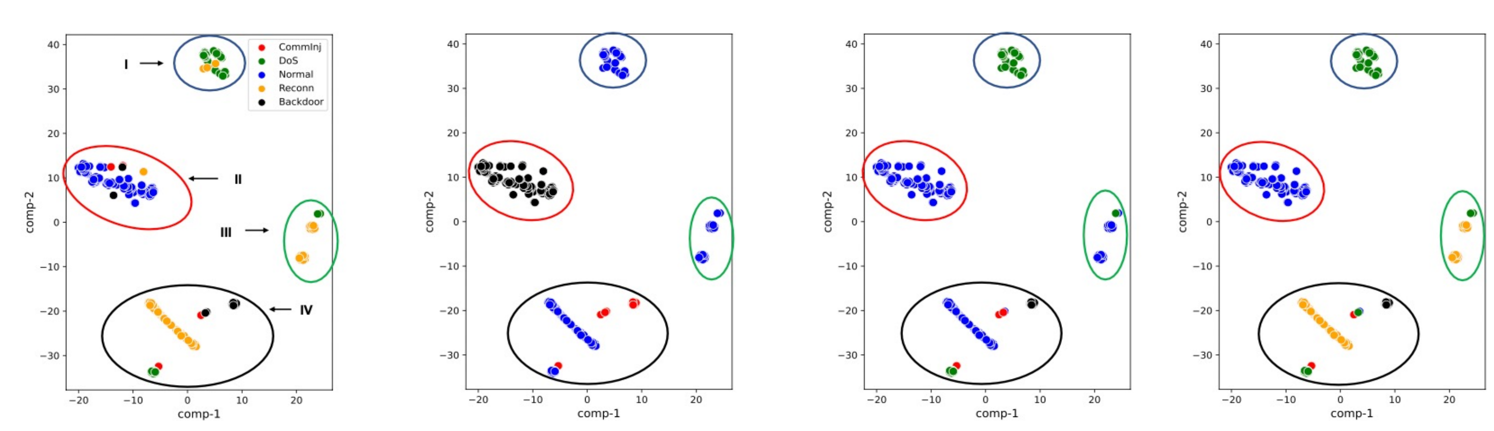
Performance of the evaluated methods on WUSTL-IIoT-2021

DL Models	Classifier's Name	Acc	Pre	Rec	F_1	MCC
State-of-the-art	CNN-BiLSTM	0.9624	0.7222	0.4349	0.5086	0.6829
	PB-DID	0.0356	0.2105	0.1110	0.0214	-0.6265
FNN	FNN-ORG	0.9620	0.7124	0.4338	0.5040	0.6798
	FNN-RND	0.5805	0.4243	**0.7708**	0.4185	0.3440
	FNN-CTGANSamp	0.7342	0.5953	0.5848	0.5057	0.3773
	FNN-Dice	0.9271	0.1854	0.2000	0.1924	0.0000
	FNN-Focal (This work)	**0.9895**	**0.7722**	0.6406	**0.6848**	**0.9232**
CNN	CNN-ORG	0.9799	0.7486	0.6142	0.6558	0.8596
	CNN-RND	0.9635	0.6059	**0.8126**	0.5800	0.7738
	CNN-CTGANSamp	0.9810	0.7939	0.6608	0.6940	0.8714
	CNN-Dice	0.9271	0.1854	0.2000	0.1924	0.0000
	CNN-Focal (This work)	**0.9821**	**0.8854**	0.6651	**0.7050**	**0.8792**

Performance of the evaluated methods on WUSTL-EHMS-2020.

DL Models	Classifier's Name	Acc	Pre	Rec	F_1	MCC
State-of-the-art	CNN-BiLSTM	0.9250	0.9010	0.7305	0.7851	0.6080
	PB-DID	0.8741	0.4372	0.4998	0.4664	-0.0066
FNN	FNN-ORG	0.9308	0.9382	0.7359	0.7975	0.6430
	FNN-RND	0.9305	0.9339	0.7367	0.7974	0.6410
	FNN-CTGANSamp	0.9299	0.9294	0.7364	0.7962	0.6372
	FNN-Dice	0.9302	0.9336	0.5000	0.4665	0.0000
	FNN-Focal (This work)	**0.9326**	**0.9524**	**0.7369**	**0.8011**	**0.6548**
CNN	CNN-ORG	0.9289	0.9284	0.7327	0.7927	0.6316
	CNN-RND	0.9296	0.9272	**0.7362**	0.7956	0.6354
	CNN-CTGANSamp	0.9274	0.9107	0.7360	0.7921	0.6227
	CNN-Dice	0.1256	0.0628	0.5000	0.1116	0.0000
	CNN-Focal (This work)	**0.9308**	**0.9423**	0.7338	**0.7963**	**0.6431**

Qualitative Analysis



(a) Ground Truth (b) FNN-ORG (c) CNN-BiLSTM (d) FNN-Focal

Qualitative analysis of FNN-ORG, CNN-BiLSTM, and FNN-Focal on WUSTL-IIoT-2021 dataset

Discussion & Conclusions

- Since the proposed system has not been tested for "In the Wild" deployments, its performance might differ in real-world deployments.
- Nonetheless, we want to emphasize that the proposed approach provides basis for building systems that might be deployed in the real-world.
- Last but not least, we observe that although our proposed approach out- performs state-of-the-art intrusion detection systems including many strong baseline models, it is far from being sufficient to be deployable in real-world.
- It highlights that there is need for more research in such an important research area and robust ML-based intrusion detection systems are needed that may be deployed in real-world without any manual and laborious handcrafting.

References

1. Insaf Ashrapov "Tabular GANs for uneven distribution", arXiv:2109.00666, 2021.
2. Lei Xu, Maria Skoularidou, Alfredo Cuesta-Infante, and Kalyan Veeramachaneni "Modeling tabular data using conditional GAN." , arXiv preprint arXiv:1907.00503, 2019.
3. Tsung-Yi Lin, Priya Goyal, Ross Girshick, Kaiming He, and Piotr Dollar "Focal loss for dense object detection." In Proceedings of the IEEE international conference on computer vision, pages 2980–2988, 2017
4. Ayesha S. Dina, A.B. Siddique, D. Manivannan "A Deep Learning Approach for Intrusion Detection in Internet of Things using Focal Loss Function." , Internet of Things journal, 2023.
5. Source Code: https://github.com/ayeshasdina/Intrusion-Detection-IoT