Network Intrusion Detection

Omar Hatem

Mohamed Fekry

Problem: Detect malicious network actions that are considered as intrusions/attacks to be able to stop them and secure the data under attack. In the past, network engineers used signatures which were basically human made patterns that were designed through knowledge of previous malicious attacks. We aim to use Deep Learning to create a NIDS that detects malicious traffic.

Dataset Description

Dataset: The dataset chosen was the UNSW-NB15 dataset. This dataset was collected by the Australian Center for Cyber Security. It provides about two million records divided into nine classes: Shellcode, Worms, Port Scans, Backdoor, Generic, Reconnaissance, Fuzzers, Exploits, and DoS. it is about 100Mb, and it can be downloaded from here. We chose the UNSW-NB15 as it is more recent and contains more records. Furthermore, it has a more diverse set of attacks such as Worms, Shellcode, and Reconnaissance for example.

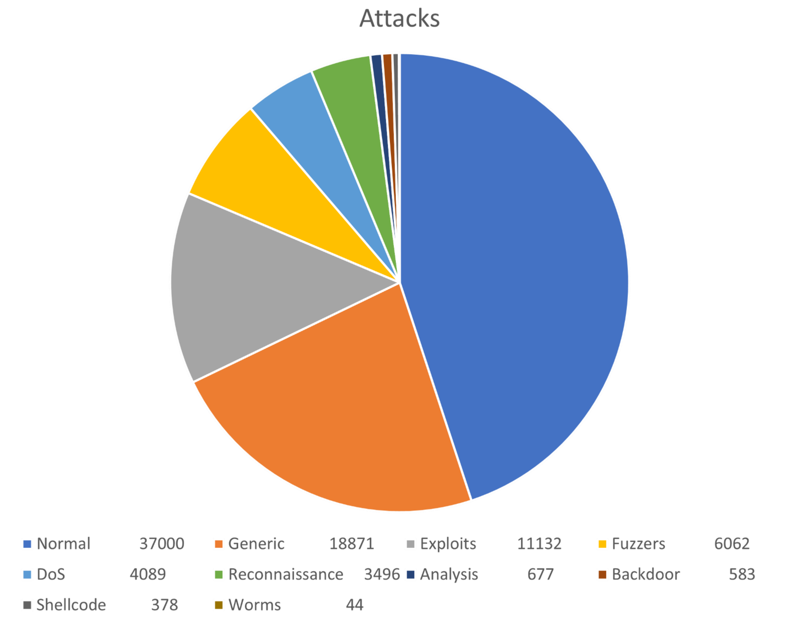
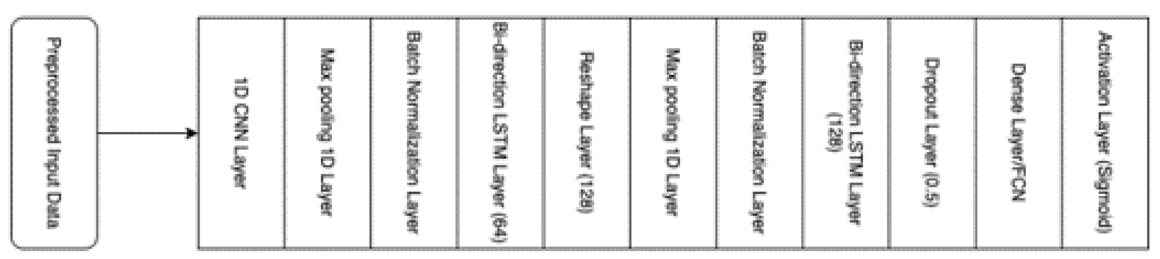


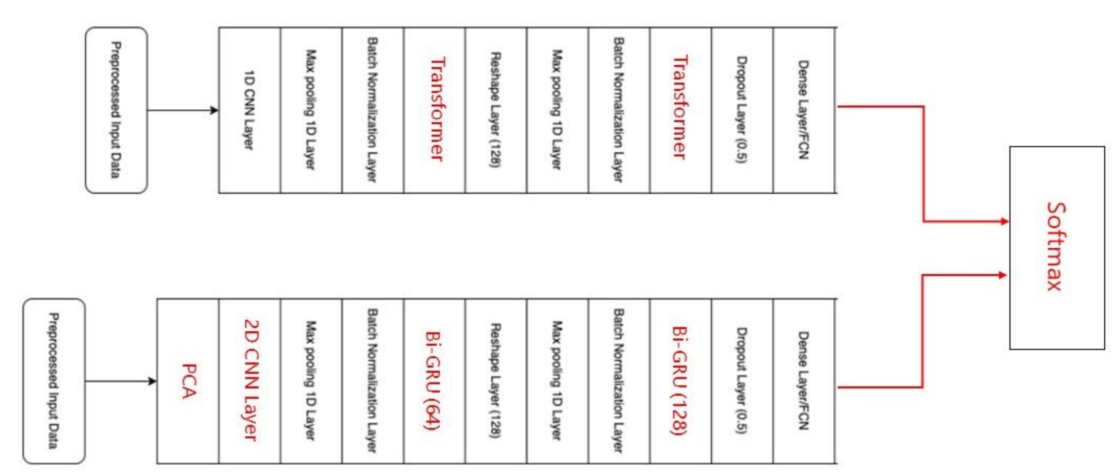
Fig. 1. Class Distribution of UNSW-NB15 Dataset

Different Models

Original Model by Sinha et al.



Final Proposed Model



Final Model Description

- An Ensemble Model consists of two models
  - CNN-Transformer
  - 2D CNN with PCA
- Loss Function used was Categorical Cross entropy
- Output is Softmax with 10 nodes.

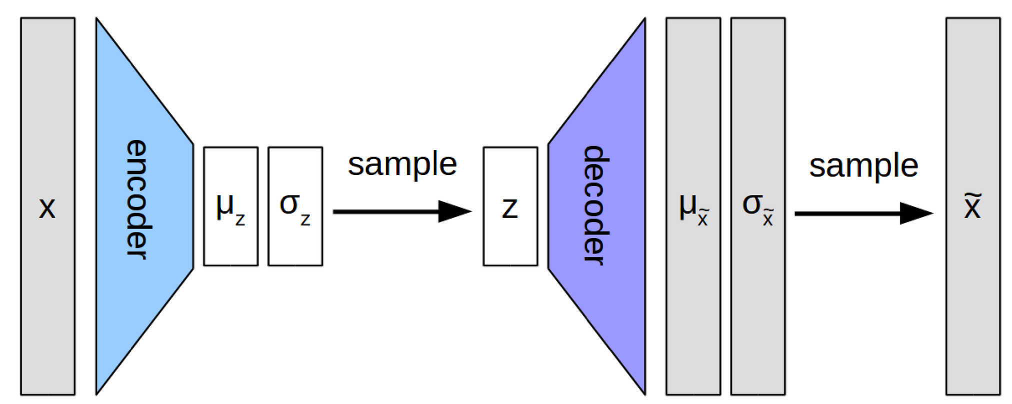
Discussion and Data Preprocessing

We encountered a limit for the training accuracy in our experiments at 86%.

We suspected this had to do with the uneven distribution of the dataset.

To solve this problem, we used:

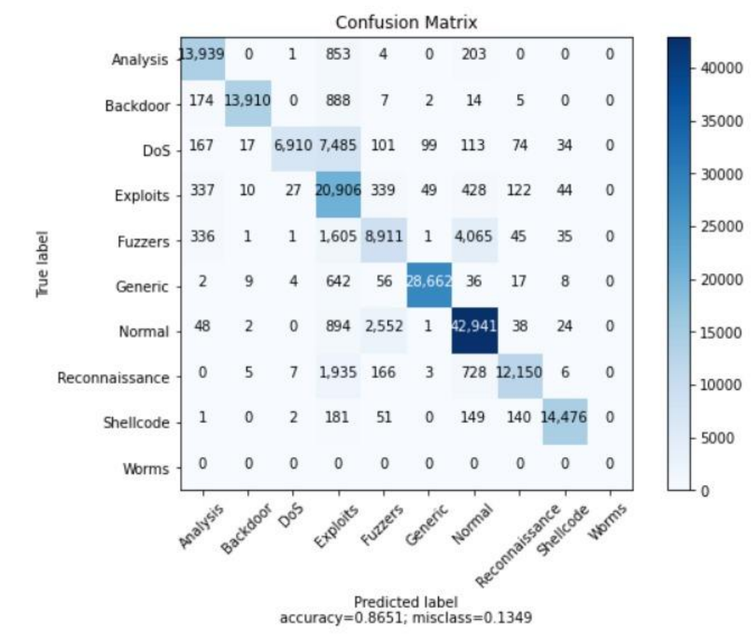
- Oversampling
- Variational AutoEncoders (VAE)



Results

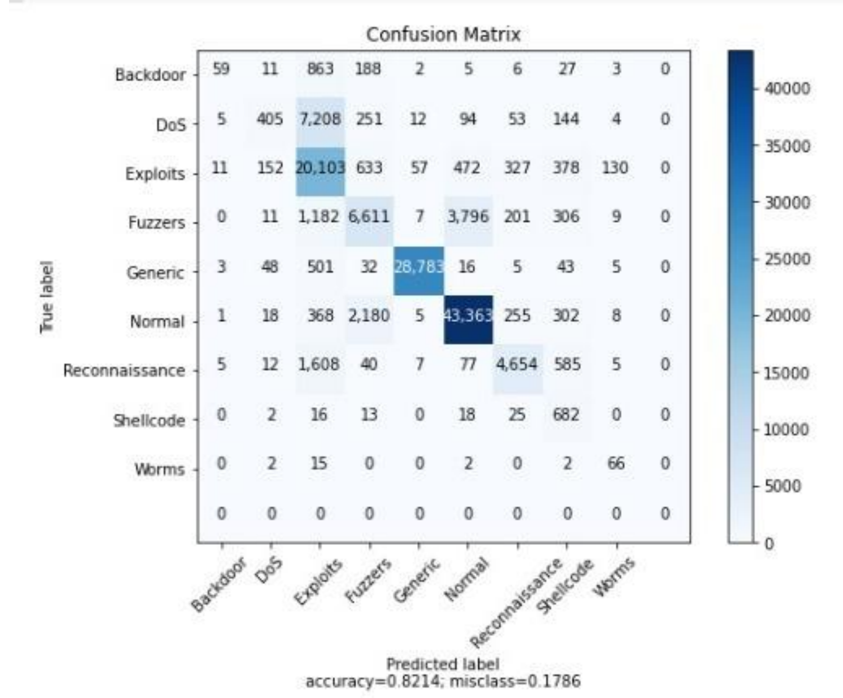
The Original Results with only the basic modification of GRU units:

- Loss: 0.3459
- Training Accuracy: 87.31%
- Validation Accuracy: 86.51%
- Confusion Matrix:



Results with Oversampling method

- Loss: 0.2486
- Training Accuracy: 89.83%
- Validation Accuracy: 82.16%
- Confusion Matrix:



The Results with VAEs

- Loss: Same as Proposed
- Training Accuracy: Same as Proposed
- Validation Accuracy: Same as Proposed

Conclusions

- 2D CNNs seemed to lose the temporal features
- PCA led to overfitting in training
- The data distribution was a real issue that needed a lot more investigation than what we did.
- Oversampling turned out to be an effective solution to classes with low frequency in the dataset (i.e. worms)
- With the skewness of the dataset, measures like recall and precision might be better indicators than accuracy.
- However, accuracy still remains to be the main issue with the UNSW-NB15 dataset, and any improvement will be based on it.

References

Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2020). Network intrusion detection system: A systematic study of machine learning and Deep Learning Approaches. Transactions on Emerging Telecommunications Technologies, 32(1). https://doi.org/10.1002/ett.4150

J. Sinha and M. Manollas, “Efficient deep CNN-BILSTM model for network intrusion detection,” Proceedings of the 2020 3rd International Conference on Artificial Intelligence and Pattern Recognition, 2020.

K. Jiang, W. Wang, A. Wang, and H. Wu, “Network intrusion detection combined hybrid sampling with deep hierarchical network,” IEEE Access, vol. 8, pp. 32464–32476, 2020.

S. Naseer, Y. Saleem, S. Khalid, M. K. Bashir, J. Han, M. M. Iqbal, and K. Han, “Enhanced network anomaly detection based on Deep Neural Networks,” IEEE Access, vol. 6, pp. 48231–48246, 2018.

Y. Xiao, C. Xing, T. Zhang, and Z. Zhao, “An intrusion detection model based on feature reduction and Convolutional Neural Networks,” IEEE Access, vol. 7, pp. 42210–42219, 2019.

Acknowledgments

We would like to thank Prof. Moustafa Youssef and Eng. Sherif Mostafa for their constant support and engagement with us in the project