Brett Luskin

Data 606 - Deliverable 3

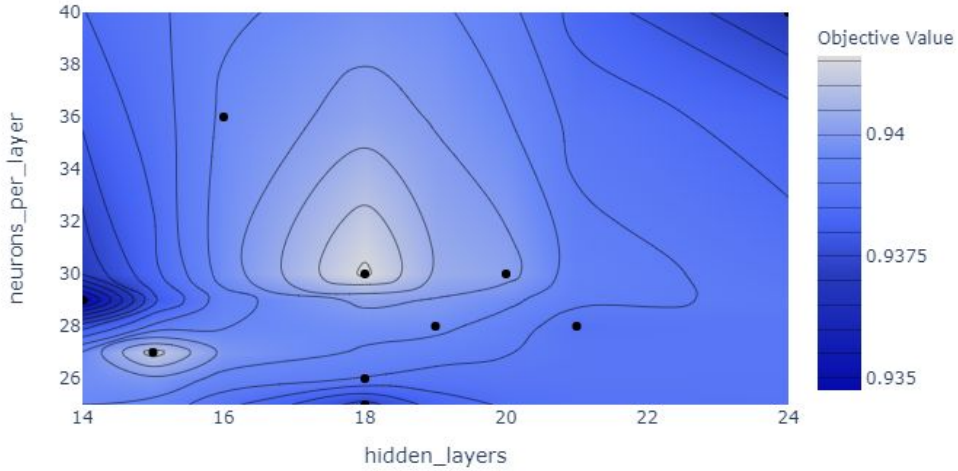
Malware Detection with Machine Learning

My third presentation discusses the progress I have made in creating a Network Intrusion Detection System (NIDS) with the UNSW-NB15 data set. I have focused on creating an Anomaly Based detection system, which means that it will classify network traffic into two classes: Normal network traffic and Malicious network traffic. I think this makes sense because I am not concerned about classifying an attack as a worm, exploit, etc., I am only concerned with identifying that it has bad intent. I did, however, make it possible in my notebooks to switch from a binary classifier to a multiclass classifier with relative simplicity.

I tried five algorithms in the machine learning space of my project so far. Logistic Regression, SVM, PCA, Random Forests, and ADABoost. As I explain in the presentation, my intuition was that decision tree based models would work best because of the existence of a few information rich features in the data set, and also because the decision boundary could be unusual in a high dimensional space. Random Forests and ADABoost outperformed the other models by a wide margin. I benchmarked the performance against the research paper, "Important Complexity Reduction of Random Forest in Multi-Classification Problem," which achieved an accuracy score using a multiclass classifier of 75%. I achieved an accuracy score of 76%, right in line with the paper. By switching to a binary classifier, the accuracy score jumps to 85% because it is only trying to categorize by Normal or Malicious instead of into ten different categories. SVM and PCA both performed poorly, and I was surprised by SVM not doing better than a coin flip. I thought that using the kernel trick to create a non-linear decision boundary that it might be able to classify with a higher degree of accuracy. Logistic Regression was surprising in that I thought it would be terrible but ended up being between a coin flip and decision trees.

The Neural Network paper that I researched, "Modeling Network Intrusion Detection System Using Feed-Forward Neural Network Using UNSW-NB15 Dataset," described a neural network that was able to achieve 99.5% accuracy on the dataset. This is amazing! The only problem is that the authors don’t list all the hyperparameters they used in setting up their network and also that they don’t provide any code for their network. This makes reproducing what they did very frustrating because I am guessing what will work best to achieve this benchmark, but there is a lot to tune and it takes a long time for the network to run every time I want to make a change.

I went ahead and created a neural network using as much information as was available in the paper. I filled in the blanks as best as I could. On my first pass, my network achieved a 93% accuracy rating. This is better than any machine learning method that I used, but still not the 99.5% that the authors achieved. I then used Optuna to try to optimize the layers and nodes in each layer.



Tuning through Optuna took over ten hours worth of run time! It suggested that I might be able to get an extra 1.5% of accuracy by changing the layers to 18 and nodes to 30. However, when I tried this on the validation set, it still only achieved 93% accuracy.

Going forward, I will be trying to tune this model with different activation functions and optimizers. I will also do some research to see if using an unsupervised neural network such as an autoencoder or GAN makes sense for this data.

References

1. K. Hassine, A. Erbad and R. Hamila, "Important Complexity Reduction of Random Forest in Multi-Classification Problem," 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), Tangier, Morocco, 2019, pp. 226-231.
2. L. Zhiqiang, G. Mohi-Ud-Din, L. Bing, L. Jianchao, Z. Ye and L. Zhijun, "Modeling Network Intrusion Detection System Using Feed-Forward Neural Network Using UNSW-NB15 Dataset," 2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE), Oshawa, ON, Canada, 2019, pp. 299-303.