Improving Intrusion Detection and Prediction with Deep Learning

Sullivan Smith
Expecting to Graduate in Spring 2025
Pursuing Computer Science Degree
ssmith46@mail.umw.edu

Project Background

This semester, I was lucky enough to enroll in a deep learning course as well as a computer security course at UMW.

Computer security presents itself as an optimal use case for deep learning, as a network can be trained to classify various types of intrusion, which can help in quicker response times when systems are attacked.

Objective

Train a Neural Network to accurately classify different types of Denial of Service (DoS) attacks, given various sensor readings on a system.

The dataset used in this project includes five classes of intrusion:

- **Normal (no intrusion)**
- **Gray Hole**
- **Blackhole**
- **TDMA**
- **Flooding**

Dataset Overview

The dataset that the model was trained on was of Wireless Sensor Network (WSN) data. [1]

WSNs are essential for both military and civilian applications. [2]

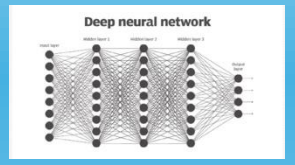
WSNs need an Intrusion Detection System (IDS), especially when in unattended environments. [2] This is where NN models can be extremely beneficial.

This dataset was collected using Network Simulator 2 (NS-2), with readings of 19 distinct features about the network. [1]

Sample Data

id	101000
Time	50
Is_CH	1
who CH	101000
Dist_To_CH	0.0
ADV_S	1
ADV_R	0
JOIN_S	0
JOIN_R	25
SCH_S	1
SCH_R	0
Rank	0
DATA_S	0
DATA_R	1200
Data_Sent_To_BS	48
dist_CH_To_BS	130.08535
send_code	0
Expaned Energy	2.4694
Attack type	Normal

Source: Kasasbeh, Bassam (2021)



Source: Yasar, Kinza (2024)

Deep Learning With Neural Networks

The model was built using a Keras Neural Network (NN).

This model has three hidden layers with 512, 1048, and 512 nodes, respectively.

The model was developed using a Jupyter notebook on Kaggle, the link to access this is given below:

https://www.Kaggle.com/code/sullivansmith12/cyber-security-poster

The Keras API allows users to quickly and easily train NNs on their own personal equipment. Keras optimizes much of the training process, meaning that this NN only took a couple of minutes to train on the data.

Results & Analysis

The model was able to reach an overall accuracy of 98.38%, with only a 3.73% loss over the data.

The specific precision for each class of intrusion the model achieved is listed below:

Normal	**100%**
Gray Hole	**78%**
Blackhole	**83%**
TDMA	**99%**
Flooding	**90%**

To achieve even higher precision in the future, a different number of hidden layers can be explored, as well as a variety of different nodes in each internal layer.

References

- [1] WSN-DS. (n.d.). Www.kaggle.com. https://www.kaggle.com/datasets/bassamkasasbeh1/wsnds
- [2] Almomani, Iman, Al-Kasasbeh, Bassam, AL-Akhras, Mousa, WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks, Journal of Sensors, 2016, 4731953, 16 pages, 2016. https://doi.org/10.1155/2016/4731953
- [3] Yasar, K. (2023, August). What is an Artificial Neural Network (ANN)? SearchEnterpriseAI. https://www.techtarget.com/searchenterpriseai/definition/neural-network