UR-62

Deep Learning Approach to Network Anomaly Detection

Rene P. Lisasi, Jamia M. Jackson

Abstract

A series of network anomaly detection models capable of detecting a multitude of network attacks. These model are based on the hypothesis that by studying a system's network records for irregular patterns during system usage, network anomalies can be identified. These models should be used in any type of distributed environment. The general purpose of these models is to detect when an attack is or has happened.

Introduction

The job of analyzing network traffic up until this point has been very tedious and deterministic [18]. It has caused problems not only for network administrators but also for product managers who must optimize their product's distributed architecture performance. To mitigate this, we are developing a Network Anomaly Detection system (NADs). NADs identify events, which differ from the expected pattern in network data. Our NAD will be able to at least classify or identify anomalies of any kind on the network that might cause bottlenecks, impair performance, or identify security threat anomalies. Once that step is complete it would be possible to complete multiclass classification and further detect the specific types of anomalies. Once that step is complete it would be possible to complete multiclass classification and further detect the specific types of anomalies as part of the mitigation process [14].

Algorithms such as Logistic Regression (LR), Decision Trees (DTs), Naïve Bayes (NB), and Support Vector Machine (SVM) are widely used to identify various network-based attacks [2]. While these techniques are effective for detecting anomalies these techniques frequently had false positives [9]. Furthermore, these Machine Learning (ML) techniques are not efficient when there is huge network traffic data which makes these algorithms insufficient for network anomaly detection.

We decided to tackle this tasks because of the growing attacks on networks. We developed a series of models to detect network anomalies using a deep learning approach. These models accurately detect network anomalies and can be ran in the background of any distributed architecture.

Materials and Methods

Our thought process while creating these models was always to utilize a CNN but we did not just want to utilize a CNN we wanted a CNN and another architecture together to make it hybrid. As a result, we landed on CNN + Autoencoder hybrid and CNN + LSTM hybrid and a CNN + GRU hybrid.

Using these models the CNN layers were utilized for feature extraction as we had 42 features with most of that data being zeros and ones, we found it best to feed in all features and let the CNN pick the most relevant features for our task at hand.

Results

Our deep learning models experienced tremendous results when detecting network anomalies. The best model for network anomaly detection was found to be the CNN-Autoencoder hybrid. This model exhibited an accuracy of above ninety-nine percent. This model correctly predicted the instance of an attack on network data.

We recommend using either the proposed CNN-Autoencoder or the original CNN Autoencoder as both achieved over a 99% accuracy when detecting multiclass anomalies. We believe the CNN-Autoencoders performed the best because autoencoders can detect certain anomalies even when they are underrepresented in the network traffic. This is due to the autoencoders being trained in an unsupervised manner meaning labels are not needed for training.

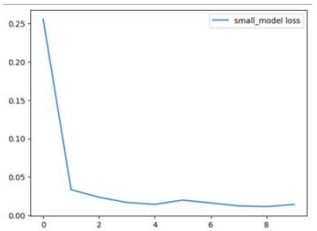

Figure 1: proposed CNN + Autoencoder loss

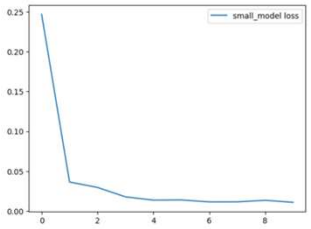

Figure 2: CNN + Autoencoder loss

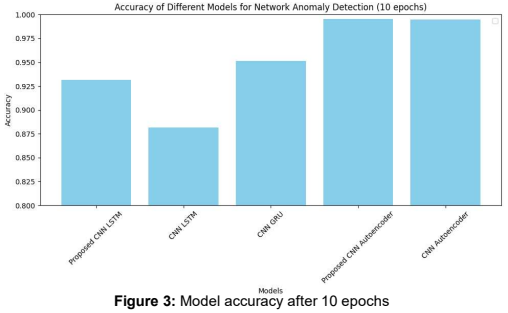

Figure 3: Model accuracy after 10 epochs

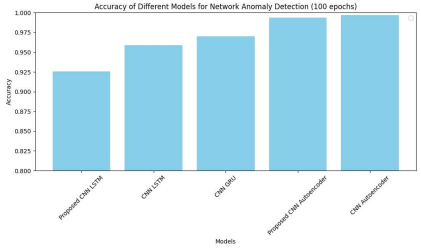

Figure 4: Model accuracy after 100 epochs

We decided to use the neural networks GRU, LSTM, and Autoencoder in companion with CNN. GRUs and LSTMs are good for anomaly detection because they utilize memory cells which helps them detect trends in network traffic. Autoencoders are also good for network anomaly detection because they can identify anomalies even when there are complex patterns or certain anomalies are underrepresented.

Conclusions

We have presented a series of models to detect anomalies, with CNN-Autoencoder hybrid being the most robust. Our model identifies anomalies in network data with a 99% accuracy. This significantly reduces the number of attacks a network may experience.

By designing these models, we have effectively made a way for networks to be safer from DoS, Probe, R2L and U2R attacks. Our results are very promising, and we expect these models to be very useful in detecting anomalies in network traffic.

Acknowledgments

Professor: Chen Zhao
Project Coordinator: Chen Zhao

Contact Information

Rene P Lisasi – rlisasi@students.kennesaw.edu
Jamia M Jackson – jjack528@students.kennesaw.edu

References

[1] Ren-Hung Hwang, Min-Chun Peng, Chien-Wei Huang. "Detecting IoT Malicious Traffic based on Autoencoder and Convolutional Neural Network." IEEE, 05 March 2020, https://ieeexplore.ieee.org/abstract/document/9024425

[2] Donghwoon Kwon, Kathiravan Natarajam, Sang C. Suh, Hyunjoo Kim, Jinoh Kim. "An Empirical Study on Network Anomaly Detection using Convolutional Neural Networks." IEEE, 23 July 2018, https://ieeexplore.ieee.org/document/8416441

[3] Abdallah Mahmoud, Nhien An Le Khae, Hamed Jahromi, Anca Delia Jurcut. "A Hybrid CNN-LSTM Based Approach for Anomaly Detection Systems in SDNs." ACM Digital Library, August 2021, https://dl.acm.org/doi/fullHtml/10.1145/3465481.3469190

KENNESAW STATE UNIVERSITY
COLLEGE OF COMPUTING AND SOFTWARE ENGINEERING