Network Based Intrusion Detection

Rahul Yadav
Department of Computer Science and Engineering University at Buffalo, Buffalo, NY 14260
rahulyad@buffalo.edu

1. Intrusion Detection

Intrusion detection is the process of monitoring computer systems, networks, and other digital assets to identify unauthorized access or activity. The goal of intrusion detection is to detect and respond to security threats as quickly as possible, to minimize the potential damage and protect valuable data. There are two main types of intrusion detection:

1. Host-based intrusion detection (HIDS): This type of intrusion detection focuses on monitoring individual devices, such as servers or workstations, to identify suspicious activity that could indicate an intrusion. HIDS systems typically work by analyzing system logs, file integrity, and other indicators of unusual activity.
2. Network-based intrusion detection (NIDS): This type of intrusion detection monitors network traffic to identify suspicious patterns or anomalies that could indicate an intrusion. NIDS systems typically work by analyzing network packets and other network traffic data.

In our experimentation we talk about Network-based intrusion detection (NIDS) on 4 different types of intrusion datasets:

a) NSL-KDD
b) CICIDS2017
c) UNSW_NB15
d) Kitsune Network Attack

2. NSL-KDD Dataset Detector Comparison

Number of records = 125973
Number of features = 122
Percentage of two classes representation in the data:
1-class = 46%
0-class = 54%

Detector	Recall Score	Precision Score	F1 Score
SVM	0.98	0.98	0.98
MLP	0.987	0.976	0.981
LSTM	0.991	0.980	0.968
AE	0.987	0.864	0.921

3. CICIDS2017 Dataset Detector Comparison

Number of records = 566148
Number of features = 79
Percentage of two classes representation in the data:
1-class = 80%
0-class = 20%

Detector	Recall Score	Precision Score	F1 Score
SVM			
MLP	**0.984**	**0.811**	**0.889**

LSTM	**0.997**	**0.894**	**0.810**
AE	**0.889**	**0.870**	**0.852**

4. UNSW_NB15 Dataset Detector Comparison

Number of records = 257673
Number of features = 56
Percentage of two classes representation in the data:
1-class = 63%
0-class = 37%

Detector	Recall Score	Precision Score	F1 Score
SVM	**0.37**	**0.32**	**0.36**
MLP	**0.99**	**0.69**	**0.81**
LSTM	**0.149**	**0.56**	**0.236**
AE	**0.77**	**0.66**	**0.71**

5. Kitsune Network Attack Dataset Detector Comparison

Number of records = 99999
Number of features = 115
Percentage of two classes representation in the data:
1-class = 63%
0-class = 37%

Detector	Recall Score	Precision Score	F1 Score
SVM	**0.47**	**0.78**	**0.39**
MLP	**0.26**	**0.99**	**0.41**
LSTM	**0.55**	**0.99**	**0.75**
AE	**0.98**	**0.99**	**0.985**

6. Conclusion:

Results compassion is above.

7. References:

[1] "NSL-KDD | Datasets | Research | Canadian Institute for Cybersecurity | UNB." *NSL-KDD | Datasets | Research | Canadian Institute for Cybersecurity | UNB*, www.unb.ca/cic/datasets/nsl.html.

[2] abhinav-bhardwaj. "GitHub - Abhinav-bhardwaj/Network-Intrusion-Detection-Using-Machine-Learning: A Novel Statistical Analysis and Autoencoder Driven Intelligent Intrusion Detection Approach." *GitHub*, 12 Oct. 2021

[3] Asharf, J.; Moustafa, N.; Khurshid, H.; Debie, E.; Haider, W.; Wahab, A. A Review of Intrusion Detection Systems Using Machine and Deep Learning in Internet of Things: Challenges, Solutions and Future Directions. *Electronics* **2020**, *9*, 1177. https://doi.org/10.3390/electronics9071177

[4] Ferriyan, A.; Thamrin, A.H.; Takeda, K.; Murai, J. Generating Network Intrusion Detection Dataset Based on Real and Encrypted Synthetic Attack Traffic. *Appl. Sci.* **2021**, *11*, 7868. https://doi.org/10.3390/app11177868

[5] Chalapathy, Raghavendra, and Sanjay Chawla. "Deep Learning for Anomaly Detection: A Survey." arXiv.org, 10 Jan. 2019, https://doi.org/10.48550/arXiv.1901.03407.

[6] "Intro to Autoencoders | TensorFlow Core." *TensorFlow*, www.tensorflow.org/tutorials/generative/autoencoder.