uOttawa

Faculty of Engineering

A Literature Review toward Building Model to Detect Intrusions and Malicious Activity on the Network

Authors:

Hosam Mahmoud[a], Kareem Waly[a], Mohamed Elesawy [a], Sondos Ali [a]

[a]University of Ottawa School of Electrical Engineering and Computer Science

Abstract

There are several uses for Artificial Intelligence(AI), especially in the area of Cybersecurity, Nowadays Cybersecurity is important due to the increasing internet usage, apps, and websites more security solutions are needed to keep the system aware of malicious activities, Intrusion Detection Systems (IDS) is an indispensable part in the security framework in communication systems and networked computing, it's a software app that examines what occurs to the network or has occurred during the performance of a task and seeks to identify or locate signs that a certain region of a computer has been improperly utilized, any illegal activity or violation is often alarmed to the administrator, traditional methods suffer from low detection rate, high false alarm rate, difficulty in dealing efficiently with the huge amount of data due to time changing network environments, and according to the development of deep learning technologies, deep learning performs more accurately than machine learning algorithms when learning large amounts of data, especially in case of learning from imbalanced data. So, in this project, we are going to investigate the recent and state-of-the-art GAN architectures and their different classification methods for identifying and analyzing various intrusions. We will apply our models' experiments on the benchmark datasets KDD 99 and discuss why we choose GAN architectures to build our model.

Keywords

Artificial Intelligence (AI); Network security; Generative Adversarial Network (GAN); Intrusion Detection System (IDS); Machine Learning (ML); Deep Learning (DL); Deep Convolutional Generative Adversarial Networks (DCGAN); KDD 99.

1. Problem Statement

With the emergence of new Internet technologies such as data sharing, online payment, and the spread of the Internet of Things (IoT), network security has become more complex, and the need to secure personal data has increased. As different systems are constantly facing the risk of trying to steal their data and trace and track their critical information from cyber attackers using many methods. One of which is spreading malware in the network to extract its data, Therefore, solutions like Intrusion Detection Systems (IDSs) have become essential for spotting and defending against network attacks brought on by malicious network traffic. the IDSs are used on the basis of two fundamental approaches as shown in **fig.1**: first, the identification of anomalous activities as they typically occur when normal or abnormal behavior turns, and second, the misuse detection by looking for unauthorized "signatures" of those identified malicious assaults and classification vulnerabilities. The main objective of IDS is to distinguish between Normal and malicious network records.

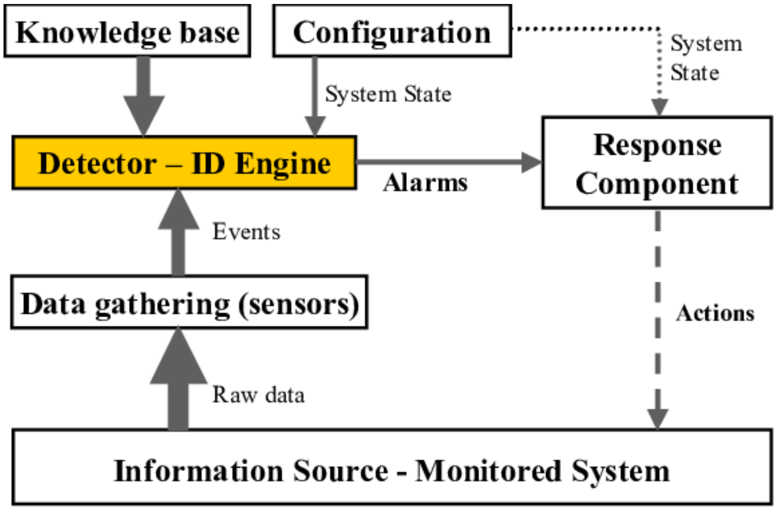

Figure 1. The basic architecture of the Intrusion Detection System [3]

2. State-of-the-art review

2.1. Our Baseline Paper [1]

2.1.1. Summary

- The **problem** that the authors of that research paper [1] tried to solve is to find a new way to detect cyber-intrusions that can endanger the security of enterprise systems and devices.

  The problem is that traditional ways like SVM and Decision trees (statistical learning models) don’t give good results with imbalanced data, while anomaly detection algorithms like Local Outlier Factor, Robust Covariance, and Isolation Forest is handling imbalanced data better but these algorithms will face some difficulties when dealing with high dimensional data.

- The authors **solved** this problem by developing a model that is derived from Bi-GAN architecture, with some modifications.
- The **experiments** that the authors of this research paper did Are:
    - The authors have trained different models on the KDD-99 dataset which is used for the testing of cyber-intrusions detectors.
    - The authors tuned and evaluated their model, and the authors also did some comparisons between the models.
- **The main conclusion**: the authors have developed a model that outperforms any of the previous GAN-based models on cyber-intrusion detection problems, and also their model is faster than the previous GAN-based models on this problem.

2.1.2. Research Goal

- This paper [1] aims to develop a model that is able to detect cyber-intrusions and give a better performance than the previous models in terms of speed and accuracy.
- The authors have achieved their goal by developing a model that is derived from Bi-GAN, and this model not only transforms the latent samples into real in the generator but also simultaneously transforms the real into their latent status via an encoder, and also, the authors have added intermediate layers in the discriminator to optimize the feature extraction. and this helps a lot in increasing the speed of their model.
- This model helped them achieve the best performance from the previously proposed models in terms of accuracy and speed.
- Before proposing their model, the authors mentioned a review of different previous works and what is the problems for each method.
- The authors have mentioned their goal for future work, and they plan to look into how timing affects intrusion detection.

2.1.3. Description of the solutions

➢ Methodology

- The authors in paper [1] used a model which is derived from Bi-GAN that uses the encoder to reflect the real samples into their latent state. Then they used different approaches which helped in enhancing the GAN's training and they found that the minimax objective is the most often utilized. Then, they did Anomaly Assessment to detect the anomalies and evaluate the level of the produced output.
- Anomaly score has been defined in several ways, but they are all essentially the same. The authors suggested two criteria to select the abnormal sample based on its anomaly score:
- The first method is appropriate for online detection since all that is required is a threshold that may be determined by experience; there is no need to understand the ratio of normal samples to abnormal samples.

- The second method, which is based on the ratio of normal samples to aberrant samples, is typically used to test datasets and assess the model's performance.

➢ The Experiments and Results

- The author’s experiment is based on the KDD-99 dataset which is used to test cyber-intrusion detectors. Each sample in this dataset contains 41 features. The authors did a preprocessing on the dataset, then they applied many models, including typical anomaly detection techniques like Isolation Forest, BiGANFM and OC-SVM to detect the abnormal samples. They did a comparison between these traditional methods and their model and found that their model achieved **results** higher than the other methods.

Model	Precision	Recall	F1
Isolation Forest	0.4415	0.3260	0.3750
OC-SVM	0.7457	0.8523	0.7954
DSEBM-r	0.8521	0.6472	0.7328
DSEBM-e	0.8619	0.6446	0.7399
AnoGANFM	0.8786	0.8297	0.8865
BiGANFM	0.6578	0.7253	0.6899
This paper Model	0.9324	0.9473	0.9398

Table 1. Performance on the KDD-99 dataset

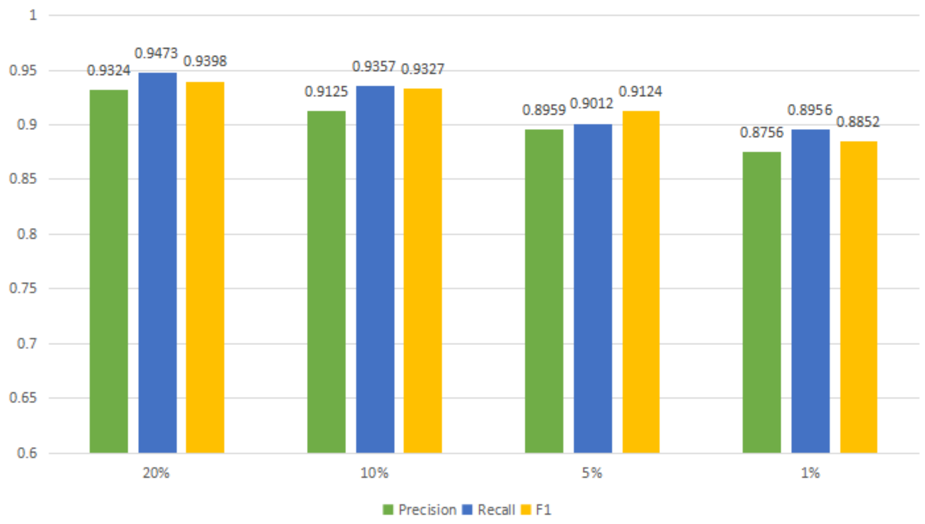

Figure 2. Performance of paper model on KDD-99 with 20%, 10%, 5%, 1% contaminate rate respectively.

2.1.4. Strengths and Weaknesses

- **Strengths**

  - They have overcome the problem of working with imbalanced data by not using traditional statistical learning models.
  - The other problem that the authors have overcome is working with high dimensional data by not using anomaly detection algorithms like Local Outlier Factor, Robust Covariance, and Isolation Forest, instead they used Generative Adversarial Network (GAN) to overcome this problem.
  - The third problem is the speed of the model and to overcome this problem they used an encoder that inverse the mapping from real space to latent space.
  - They have discussed and explained these problems clearly and efficiently.
  - They have conducted different experiments and tried different models and made good comparisons between these models in terms of accuracy and speed, and they provided the results of these comparisons on tables and graphs.

- **Weaknesses**

  - We think that the authors of paper [1] have done pretty good work with a perfect number of mentioned details.

2.2. Paper [2]

2.2.1. Summary

- The **problem** authors of that research paper [3] tried to solve the weaknesses in the traditional machine learning model by finding a model that can deal with high-dimensional data samples and efficiently detect intrusion in the network.
- The authors **solved** this problem by developing a model that used NIDS which provides protection from Internet-based attacks, and long short-term memory (LSTM) to automatically learn the features of network intrusion behaviors, recurrent unit based to enable intrusion detection in real time
- **The main conclusion**: authors have developed six popular learning models (including SVM, Random-Tree, Random Forest, NB Tree, Naive, Bayes, and J48) and all of these models can only achieve maximum accuracy 94% on KDD-99 and 83% on NSL-KDD wherever the SRU-DCGAN get 99.73% on KDD-99 and 99.62% on NSL-KDD

2.2.2. Research Goal

- The authors aim to generate a network intrusion detection model based on simple recurrent unit-based (SRU) and DCGAN which can detect cyber-intrusions and give a better performance compared to any Machine learning model.

2.2.3. Description of the solutions

- **Methodology**

  - The authors in paper [2] used an SRU-DCGAN model and six other methods to detect the intrusions in the network
  - An SRU-based multichannel network intrusion detection model is applied. It beats the LSTM algorithm in terms of classification speedup and automatically extracts the features through repeated multi-level learning. Additionally, this approach increases the effectiveness of categorization and the precision of detection of network danger behaviors.
  - The generation of cyber threat samples using a generative adversarial model is suggested. New training samples are produced using this technique. It addresses the issue of inadequate and imbalanced samples that standard intrusion perception methods frequently confront. Additionally, it lowers the number of false alarms and increases system detection rates.
  - To guarantee that the data can be processed by our model with great efficiency, a preprocessing approach of mapping the network data using Mahalanobis Distance is recommended. This method provides high-quality data input for the proposed deep learning model.

- **The Experiments and Results**

  - They used 3 datasets in the experiment: the KDD'99 dataset, the NSL-KDD dataset
  - Firstly, in the experiments of the SRU-DCGAN model on the KDD-99, The Hyper-parameter settings were hidden units = [30, 70, 30, 30], steps = 400000, batch-size = 20000, epoch = 500, Learning Rate η = 0.001 as shown in **fig.3** and the SRU-DCGAN model was the highest accuracy model compared to all other methods.
  - Secondly, in the experiments of the SRU-DCGAN model on the NSL-KDD, as shown in **fig.4** and the SRU-DCGAN model was the highest accuracy model compared to all other methods.
  - We only illustrate a sample from their experiments, they really tried a lot of experiments to be sure that their model doing great on different datasets.

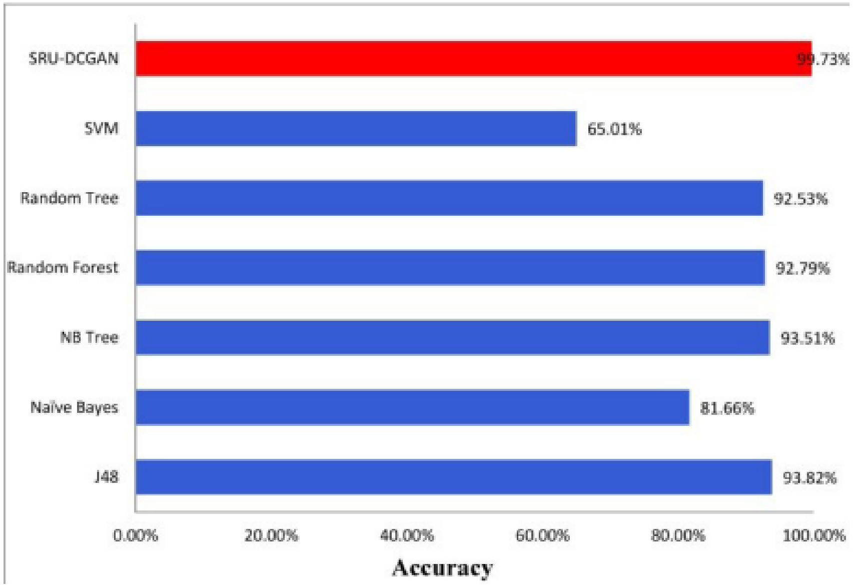

Figure 3. Comparing experiment with SRU-DCGAN model and the classical algorithm on KDD-99.

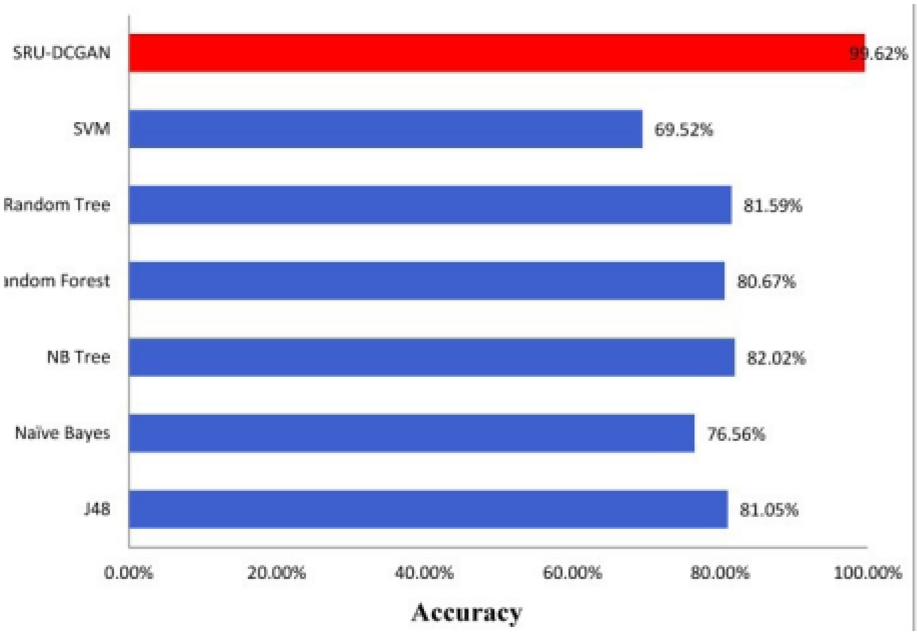

FIGURE 4. Comparing experiment with SRU-DCGAN model and the classical algorithm based on NSL-KDD dataset.

2.2.4. Strengths and Weaknesses

- **Strengths**

  - The whole paper was well-written and very clear.
  - Anyone without any domain knowledge can understand it, not only the specialist
  - They use graphs and tables to illustrate their results

- **Weaknesses**

It was difficult for us to find a weak point in this paper [2] They have already covered all aspects of this project and have tried many models on many datasets, and they plot their results in comparison forms.

3. Our Solutions

Our problem can be considered as an anomaly detection problem, and our solution is to implement different GAN architectures such as DCGAN and (SRU-DCGAN) with long short-term memory (LSTM) to speed up the classification process and with the suitable distance metric as a preprocessing, then choose the best model. Also, we will consider the evaluation metrics during the implementation, and compare our results to the results we presented above in this paper. The dataset we will be dealing with during our experiments will be the KDD-99 10 percent dataset which is a benchmark used to test cyber-intrusion detectors.

BIBLIOGRAPHY

[1] Chen, Hongyu & Jiang, Li. (2019). GAN-based method for cyber-intrusion detection.

[2] Yang, J., Li, T., Liang, G., He, W., & Zhao, Y. (2019). A Simple Recurrent Unit Model Based Intrusion Detection System With DCGAN. In IEEE Access (Vol. 7, pp. 83286–83296). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/access.2019.2922692

[3] Meena, G., & Choudhary, R. R. (2017). A review paper on IDS classification using KDD 99 and NSL KDD dataset in WEKA. In 2017 International Conference on Computer, Communications and Electronics (Comptelix). 2017 International Conference on Computer, Communications and Electronics (Comptelix). IEEE. https://doi.org/10.1109/comptelix.2017.8004032