Deploying and analyzing classification algorithms for Intrusion Detection

by

Himanshu Pandey

Roll. No.: 2018IMT-038

Under the supervision of

Dr. Saumya Bhadauria

विश्वजीवनामृतं ज्ञानम्

ABV–INDIAN INSTITUTE OF INFORMATION TECHNOLOGY AND MANAGEMENT GWALIOR (M.P.), INDIA

Motivation

- Antiviruses or firewalls are no longer sufficient to ensure the security of the systems.
- Detecting known attacks through supervised intrusion detection and applying Deep Learning method LSTM that will recognise attacks and retain a long-term memory of them in order to prevent the emergence of new attacks while also treating all types of these attacks uniquely.
- New technologies to improve the time complexity and accuracy of the already existing algorithms.
    - Limitation:
        - New features increase the TPR score as the number of correct classification of “Normal” class points has increased, but that has also resulted in an increase in the FPR score for all the models which is not desirable.

Key related research

- A decision tree was utilized to develop a misuse detection model, which was then used to break down the normal training data into smaller groups.
    - A system for intrusion detection that incorporates a clustering technique, a basic feature selection algorithm, and the Support Vector Machine (SVM).
    - Work on feature reduction using the ADTree algorithm has also been done.

Objectives

- To analyse already implemented supervised learning algorithms for intrusion detection and applying new techniques to improve their time complexity and accuracy.
- To design and implement algorithms for unsupervised intrusion detection like ensemble learning, Autoencoder,the Multilayer Perceptron (MLP), the Long Short-Term Memory network (LSTM) algorithms), and Generative Adversarial Networks(GAN).
- To check the performance of supervised and unsupervised Machine Learning techniques in detecting intrusions by comparing their sensitivity, specificity, and accuracy. (Applying detection rate, Accuracy, Precision, F1-score and ROC Curve)

Methodology/System Design

- Feature normalization is done in Phase I by rescaling one or more attributes to have a mean of 0 and a standard deviation of 1.
- Machine Learning Classifiers such as Naive Bayes, Logistic Regression, SVM, Decision Tree, Random Forest, and GBDT/XGBoost are utilized in Phase II for training purposes.
- We used Clustering features, PCA transformed features, and Feature engineering employing existing features in Phase III to build some extra features to our dataset.

Methodology/System Design

- Classifying the dataset NSL-KDD into binary class and multi class algortihms using Linear SVM, Quadratic SVM, KNN, Linear Discriminant Analysis, Quadratic Discriminant Analysis and comparing their accuracy and sensitivity.
- Deploying LSTM method on NSL KDD dataset which prove to be an algorithm of better accuracy.

Implementation Details

- First Task is to identify the features that are used in the various classification models.

- To know the dependency of intrusions on different features.

- After the dataset has been imported, it is cleaned to remove/impute NULL values and duplicates. After that, we used Exploratory Data Analysis (EDA) to discover what the data could tell us in addition to the formal modelling.

- Confusion matrix is generated to know the number of False Positives, True Positives, False Negatives, and True Negatives acquired after classification.

Implementation Details

- Linear SVM, Quadratic SVM, KNN, Linear Discriminant Analysis, Quadratic Discriminant Analysis are implemented on binary and multi class classification and compared their accuracy and sensitivity.

- Demonstrating that the metrics of the detection of the LSTM method reach very high values more than the other classifiers which proves that our new proposed method is effective for NIDS.

Progress so far

- Intrusion detection was done using supervised machine learning algorithms like naive bayes, logistic regression, support vector machine, decision tree, random forest, XG Boost and their accuracy, sensitivity, specificity was calculated.
- Additional techniques like Clustering features (using MiniBatchKmeans), PCA features, and constructing new features from the data (such as adding two current features and deleting two existing features) were used to improve the accuracy and time complexity of the algorithms.
- From the research, it can be clearly noted that before applying the new techniques, the xgb classifier takes more than 3 hours which takes only 52mins after applying the new techniques.

Tasks completed

- Analyzed supervised machine learning techniques like Logistic Regression, Support Vector Machine(SVM), Decision Tree, Random Forest and GBDT / XGBoost.
- Analyzed and compared machine learning techniques like ensemble learning, Autoencoder,the Multilayer Perceptron (MLP), the Long Short-Term Memory network (LSTM) algorithms).
- To check the performance of supervised and unsupervised Machine Learning techniques in detecting intrusions by comparing their sensitivity, specificity, and accuracy. (Applying detection rate, Accuracy, Precision, F1-score and ROC Curve)

Research outcome

- The new feature engineering, clustering and PCA technologies applied on KDD Cup dataset used in supervised learning algorithms improves the accuracy as well as the time complexity of the algorithms.
- Compared binary and multi class classification algorithms like KNN, Linear SVM, Quadratic SVM, Multi Layer Perceptron, Linear Discriminant Analysis, Quadratic Discriminant Analysis
- Deployed LSTM method on NSL KDD dataset which prove to be an algorithm of better accuracy.

Research outcome

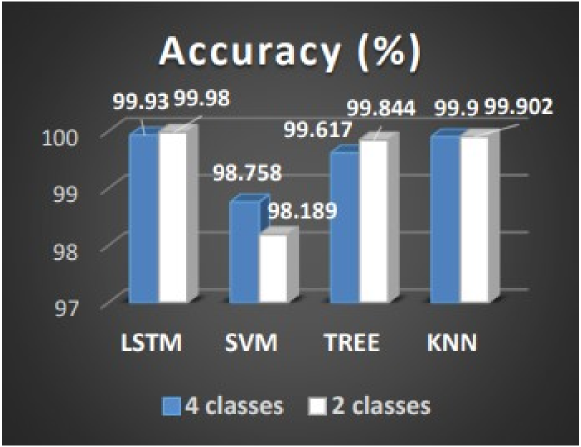

Figure: Accuracy for binary classification and multi-class classification

Research outcome

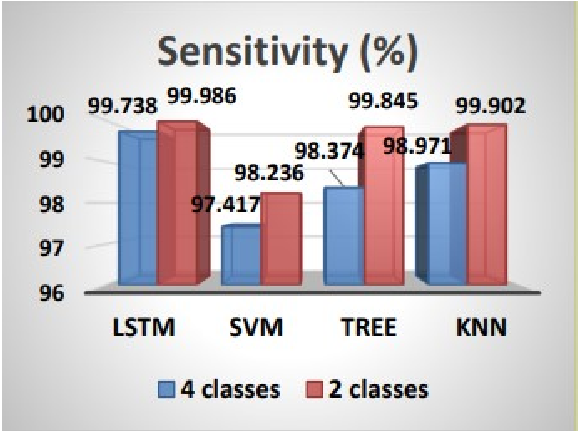

Figure: Average of Sensitivity for binary classification and multi-classification

Research outcome

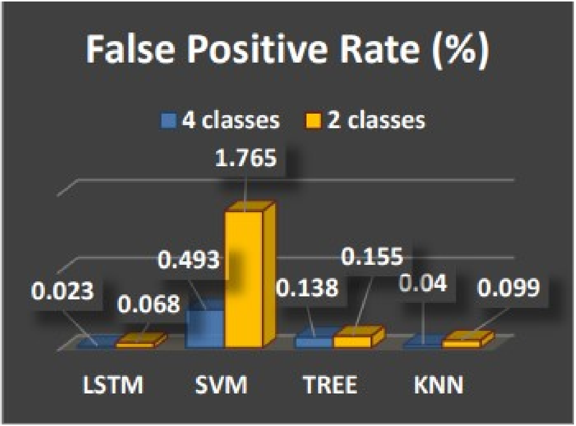

Figure: Average of false positive rate (FPR) for binary classification and multi-class classification

References I

- A. Paszke, S. G. and Lin, Z.: 2010, Automatic differentiation in pytorch, Computer Technology and Development (ICCTD), 2010 2nd International Conference on pp. 374 – 378. *IEEE Trans. NanoBioscience, vol. 4, no. 3, pp. 228-234,*, Sept. 2005.
- Axelsson, S.: 2000, The base-rate fallacy and the difficulty of intrusion detection, 3, 186–205. *IEEE/ACM Trans. Computational Biology and Bioinformatics, vol. 8, no. 6, pp. 1633-1641,*, Nov./Dec 2011.
- F. Amiri, M. Yousefi, C. L. A. S. and Yazdani, N.: 2011, Mutual informationbased feature selection for intrusion detection systems, Journal of Network and Computer Applications 34, 1184–1199.,"*J. Royal Statistical Soc.: Series B, vol. 67, no. 2, pp. 301-320*, 2005.

References II

F. Pedregosa, G. V. and Duchesnay, E.: 2011, Scikit-learn: Machine learning in python, Computer and Automation Engineering (ICCAE), Vol. 12, pp. 2825 – 2830. ", (*Computers and Chemistry, vol. 26,*, 2001.