Deploying and analyzing classification algorithms for Intrusion Detection

A project report,
submitted in partial fulfillment of the requirements for B. Tech project

by

Himanshu Pandey (2018IMT-038)

Under the Supervision of

Dr. Saumya Bhadauria

ABV INDIAN INSTITUTE OF INFORMATION TECHNOLOGY AND MANAGEMENT
GWALIOR-474 015
2021

Contents

List of Figures

1 Abstract

Hacking has grown in popularity in recent years, increasing in the quantity and variety of cyber-attacks. Malware, denial of service attacks, phishing, and social engineering are all examples of computer network threats. Antiviruses and firewalls are no longer sufficient for effective cybersecurity. To prevent these dangers, you can't only rely on antivirus and firewalls: you need multiple levels of defense. With the capacity to monitor packets from OSI layer 2 (Data link) through layer 7 (Application), network-based Intrusion Detection Systems (IDSs) offer a supplementary technique of increasing security. IDSs that use anomaly detection can detect unknown assaults, but they are less accurate, resulting in a high amount of false alarms. Machine learning methods are investigated in this thesis to develop IDSs that can be deployed in real-world computer networks. To begin, a three-step optimization strategy is given to increase detection quality: 1) data augmentation to rebalance the dataset, 2) model performance optimization, and 3) ensemble learning to integrate the findings of the best models. This method has the disadvantage of requiring labeled datasets, which are rarely available in real-life situations. As a result, transfer learning is explored to train machine learning models on huge labelled datasets and subsequently finetune them on innocuous network traffic. This method also has problems because the models are trained on previously known assaults and so do not do anomaly detection. As a result, an unsupervised learning-based method is provided. It takes advantage of network prototyping. When anomalies are discovered, they are grouped into attacks or disregarded if they are isolated. Finally, network congestion detection is investigated. The bandwidth usage of various links is forecasted to prevent problems from arising.

2 Introduction

Computers have become an inextricable aspect of our lives. They are widely employed in all government agencies, businesses, private organizations, hospitals, and private residences. Because of their importance in our lives, protecting them from invasions is a huge task for us. Intrusions are still the most persistent hazards in the cyber world, despite significant advancements in protection technologies. Many ways for analyzing intrusions have been developed to date. This process and the design of the machine learning models are usually managed by a framework such as scikit-learn [1], Tensorflow [2], PyTorch [3], Matlab or Weka [4].

3 Background

During the 1970s, the growth of computer networks created new problems related to the monitoring of user activities and access. Intrusion Detection Systems have two categories: signature-based detection (or “misuse detection”) and anomaly detection. In signature-based detection, the data monitored by the IDS is compared to known patterns of attacks and it can only detect known attacks while anomaly detection builds a model of the normal behaviour of the system and then looks for deviations in the monitored data. Anomaly detection has a wider aspect but it can also detect unknown attacks which can generate irrelevant alarms. Several machine learning techniques have come into the picture to detect the anomaly. Some of them can rely on algorithms with the ability to learn directly from the data, without being explicitly programmed. Despite so many advantages, these algorithms are rarely deployed just because of a higher false positivity rate. Indeed, even a false positive rate of 1% can create so many false alarms on a high traffic network that they become impossible for an administrator to process. [5]

4 Motivation

With the passage of time, several computer attacks are stretching their arms intending to harm the targeted system. For a company, antiviruses or firewalls are no longer sufficient to ensure the security of the systems of the company. Now we need multiple layers of security to ensure truly secured systems among which one of the most important layers is provided by the Intrusion Detection System (IDS) which is designed to protect its target against any potential attack through continuous monitoring of the system. In our thesis, we are going to deploy machine learning models which can detect known attacks through supervised intrusion detection and unknown attacks through unsupervised intrusion detection. Further, the thesis model will be deployed to predict bandwidth utilization and at last, all the machine learning techniques will be compared in detecting intrusions so that we can come up with better and efficient algorithms and others can have a knowledge to which algorithm is to be used in case of intrusion detection.

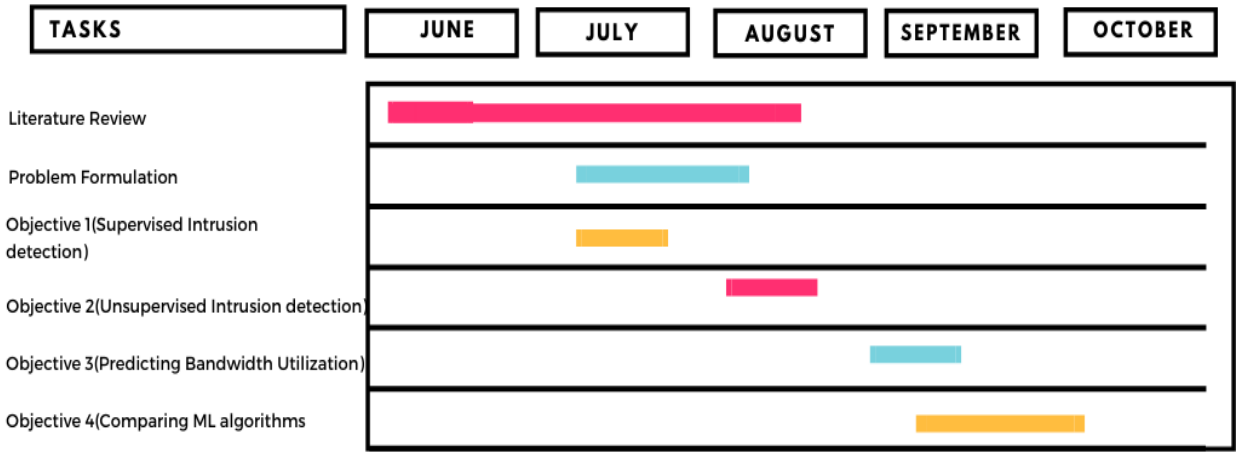
5 Problem Statement

To overcome the problems of unknown threats to the systems, we will be developing various classification algorithms like Gaussian Naive Bayes, KNN, MLP, decision tree, random forest, SVM, logistic regression, and then deploying ensemble and transfer learning algorithms that have better accuracy than the previous ones. We will be deploying the Autoregressive Integrated Moving Average (ARIMA), the Multilayer Perceptron (MLP), and the Long Short-Term Memory network (LSTM) [6] algorithms to predict Bandwidth utilization. We then use various methods to check the accuracy, specificity, and sensitivity of the algorithms.

5.1 Objectives

1. Techniques for Supervised Intrusion Detection (Using decision tree, random forest, extra tree, extra trees, k-Nearest Neighbors (KNN), SVM [7], logistic regression, Naive Bayes, gradient boosting, ensemble learning and multilayer perceptron (MLP), and transfer learning [8])
2. Techniques for Unsupervised Intrusion Detection (Using ensemble learning, Autoencoder [9], MLP, LSTM, and GAN)
3. Predicting Bandwidth Utilization (Using the Autoregressive Integrated Moving Average (ARIMA), the Multilayer Perceptron (MLP) and the Long Short-Term Memory network (LSTM) algorithms) [10]
4. To check the performance of Machine Learning techniques in detecting intrusions by comparing their sensitivity, specificity, and accuracy. (Applying detection rate, Accuracy, Precision, F1-score and ROC Curve) [11]

6 Gantt Chart



7 References

References

[1] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and E. Duchesnay, "Scikit-learn: Ma chine Learning in Python ," Journal of Machine Learning Research, vol. 12, pp. 2825–2830, 2011.
[2] M. Abadi, A. Agarwal, P. Barham, E. Brevdo, Z. Chen, C. Citro, G. S. Corrado, A. Davis, J. Dean, M. Devin, S. Ghemawat, I. Goodfellow, A. Harp, G. Irving, M. Isard, Y. Jia, R. Jozefowicz, L. Kaiser, M. Kudlur, J. Levenberg, D. Mane, R. Monga, S. Moore, D. Murray, C. Olah, M. Schuster, J. Shlens, B. Steiner, I. Sutskever, K. Talwar, P. Tucker, V. Vanhoucke, V. Vasudevan, F. Viegas, O. Vinyals, P. Warden, M. Wattenberg, M. Wicke, Y. Yu, and X. Zheng, "Ten sorflow: Large-scale machine learning on heterogeneous distributed systems," arXiv:1603.04467 [cs], 3 2016. arXiv: 1603.04467
[3] A. Paszke, S. Gross, S. Chintala, G. Chanan, E. Yang, Z. DeVito, and Z. Lin, "Automatic differentiation in pytorch," p. 4
[4] M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, and I. H. Wit ten, "The weka data mining software: an update," ACM SIGKDD Explorations Newsletter, vol. 11, p. 10, 11 2009.
[5] S. Axelsson, "The base-rate fallacy and the difficulty of intrusion detection," ACM Trans. Inf. Syst. Secur., vol. 3, p. 186–205, Aug. 2000.
[6] R. C. Staudemeyer, "Applying long short-term memory recurrent neural networks to intrusion detection," South African Computer Journal, vol. 56, no. 1, p. 136–154, 2015.
[7] M. S. Pervez and D. Farid, "Feature selection and intrusion classification in nsl kdd cup 99 dataset employing svms," SKIMA 2014 - 8th International Conference on Software, Knowledge, Information Management and Applications, 04 2015.
[8] C. Tan, F. Sun, T. Kong, W. Zhang, C. Yang, and C. Liu, "A survey on deep transfer learning," CoRR, vol. abs/1808.01974, 2018.
[9] A. Ng, "Sparse autoencoder," CS294A Lecture notes, vol. 72, no. 2011, p. 1–19, 2011.
[10] M. Labonne, C. Chatzinakis, and A. Olivereau 2020.
[11] G. Gu, P. Fogla, D. Dagon, W. Lee, and B. Skorić, "Measuring intrusion detection capability: An information-theoretic approach," in Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security, ASIACCS '06, (New York, NY, USA), pp. 90–101, ACM, 2006.