BSP Project Description: Unsupervised anomaly detection in network traffic with deep learning

Ivaylo Krumov
University of Luxembourg
Email: ivaylo.krumov.001@student.uni.lu

This report has been produced under the supervision of:
Salima Lamsiyah
University of Luxembourg
Email: salima.lamsiyah@uni.lu

Abstract

This document outlines the end of Phase I description of the project carried out by Ivaylo Krumov, under the guidance of Salima Lamsiyah, during his July-August Bachelor Semester Project. It is about the ability and application of deep learning models in assisting with the prevention of cyber attacks based on network intrusion by identifying anomalies in network traffic. The project will detail the scientific aspects, consisting of the acquisition of knowledge relevant to the scientific question at hand and to the development of the technical deliverable, and the technical aspects, which comprises the application of the gathered knowledge about the project's main topic.

1. Plagiarism statement

I declare that I am aware of the following facts:

- As a student at the University of Luxembourg I must respect the rules of intellectual honesty, in particular not to resort to plagiarism, fraud or any other method that is illegal or contrary to scientific integrity.
- My report will be checked for plagiarism and if the plagiarism check is positive, an internal procedure will be started by my tutor. I am advised to request a precheck by my tutor to avoid any issue.
- As declared in the assessment procedure of the University of Luxembourg, plagiarism is committed whenever the source of information used in an assignment, research report, paper or otherwise published/circulated piece of work is not properly acknowledged. In other words, plagiarism is the passing off as one's own the words, ideas or work of another person, without attribution to the author. The omission of such proper acknowledgement amounts to claiming authorship for the work of another person. Plagiarism is committed regardless of the language of the original work used. Plagiarism can be deliberate or accidental. Instances of plagiarism include, but are not limited to:
  1) Not putting quotation marks around a quote from another person's work
  2) Pretending to paraphrase while in fact quoting
  3) Citing incorrectly or incompletely
  4) Failing to cite the source of a quoted or paraphrased work
  5) Copying/reproducing sections of another person's work without acknowledging the source
  6) Paraphrasing another person's work without acknowledging the source
  7) Having another person write/author a work for oneself and submitting/publishing it (with permission, with or without compensation) in one's own name ('ghost-writing')
  8) Using another person's unpublished work without attribution and permission ('stealing')
  9) Presenting a piece of work as one's own that contains a high proportion of quoted/copied or paraphrased text (images, graphs, etc.), even if adequately referenced

  Auto- or self-plagiarism, that is the reproduction of (portions of a) text previously written by the author without citing that text, i.e. passing previously authored text as new, may be regarded as fraud if deemed sufficiently severe.

2. Main required competencies

The following is a description of the specific scientific and technical competencies, that are essential for the execution and success of this project:

2.1. Scientific main required competencies

The main scientific competencies required for this project include a good understanding of the cybersecurity field and the related process of network anomaly detection, specifically in the practical application of deep learning models for unsupervised anomaly detection. This primarily involves basic knowledge of deep learning techniques utilized in unsupervised learning approaches, including autoencoders and generative adversarial networks (GANs), and understanding the inner workings of neural network architectures as a whole, potentially knowing how to adapt them to challenges that arise from network security environments. Additionally, an essential aspect that provides a strong advantage is having some familiarity with existing research and methodologies for network traffic analysis and anomaly detection through deep learning.

2.2. Technical main required competencies

The main technical competencies required for the success of the project include fluency in Python, particularly in its application to the task of network traffic anomaly detection. This involves a practical understanding of deep learning techniques, including the implementation and hyperparameter fine-tuning of deep learning models like autoencoders and GANs. Moreover, it is vital to possess knowledge in data processing and analysis for working with the selected network traffic dataset and proficiency in data visualization skills is also essential to discover any patterns and outliers within the network traffic data. Finally, a comprehensive understanding of performance metrics is required to analyze and interpret the effectiveness of these deep learning models in the anomaly detection task.

3. Scientific Deliverable Description

As described in the above section, the main scientific aspect of this project consists of gaining a comprehensive understanding in the field of machine learning, with a particular focus on the fine-tuning of deep learning models like autoencoders and generative adversarial networks (GANs). The scientific deliverable will delve into an exploration of the utility that these models provide in the area of network anomaly detection through an in-depth study of machine learning principles, such as model architecture and hyperparameters, techniques for adapting these models to network traffic data through fine-tuning and the ability to perform effective model evaluation. The deliverable will also look into some of the theoretical basis of the relevant machine learning algorithms. The acquired knowledge will give a firm basis for the subsequent technical deliverable, while answering the scientific question: ”How can deep learning models be used to detect anomalies in network traffic?”. To that end, multiple scientific papers and articles will be utilized, which will be vital in providing the necessary knowledge to produce the final answer. The following is a list of referenced resources that will contribute towards this goal (may be potentially expanded later on during project development):

- ”Network traffic anomaly detection via deep learning” by [Fotiadou, K., Velivassaki, T. H., Voulkidis, A., Skias, D., Tsekeridou, S., & Zahariadis, T. (2021).]
- ”Deep learning approach for intelligent intrusion detection system” by [Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019).]
- ”Feature Extraction and Anomaly Detection Using Different Autoencoders for Modeling Intrusion Detection Systems” by [Sivasubramanian, A., Devisetty, M., & Bhavukam, P. (2024).]
- ”Deep autoencoding gaussian mixture model for unsupervised anomaly detection” by [Zong, B., Song, Q., Min, M. R., Cheng, W., Lumezanu, C., Cho, D., & Chen, H. (2018, February).]
- ”An empirical study on unsupervised network anomaly detection using generative adversarial networks” by [Truong-Huu, T., Dheenadhayalan, N., Pratim Kundu, P., Ramnath, V., Liao, J., Teo, S. G., & Praveen Kadiyala, S. (2020, October).]

The scientific deliverable will primarily focus on introducing key concepts of deep learning models and discussing the practical utility they provide in the context of network anomaly detection, which is essential in the formulation of an answer to the aforementioned scientific question.

First of all, the deliverable will provide a brief introduction to the current state of cybersecurity and network intrusion detection, as these fields are directly related to network traffic analysis. Following this, the deliverable will take a closer look at cases of utilizing deep learning models for detecting network anomalies, while highlighting the importance of anomaly detection in preventing network-related cyber attacks.

Next, the concept of using autoencoders and GANs for anomaly detection will be introduced, covering the theoretical foundations of these models and their applications in existing work in machine learning and cybersecurity. The deliverable will put focus on the process of fine-tuning the models to recognize patterns, deviations and outliers that would indicate anomalies in network traffic data.

In addition, an essential aspect is understanding how particular machine learning algorithms work, both in theory and in practice, which will be explored by the deliverable. This exploration will provide further insight into the possibilities for deep learning models to be fine-tuned for network anomaly detection.

Finally, once all these topics have been discussed, the scientific deliverable will conclude with a formulation of an answer to the scientific question. The answer will be based on the knowledge acquired in the previous sections, mostly leaning on information about relevant algorithms used for deep learning models and metric comparison between the different models. This technical aspect to the question's answer will further serve to justify the approach that will subsequently be used in the development of the technical deliverable.

4. Technical Deliverable Description

As mentioned earlier, the technical deliverable of this project will make use of the practical aspects explored in the scientific deliverable. In particular, it will be presented in the form of a Python implementation and evaluation of at least two deep learning models fine-tuned for network anomaly detection, each carrying some difference between training methods and/or parameters used. The selected coding environment for these tasks will be a Jupyter notebook, as this choice offers a lot of flexibility and code readability when it comes to dealing with machine learning problems.

The implemented models will all be trained and evaluated using the UNSW-NB15 dataset, which contains a large set of network traffic data collected from real scenarios ([https://research.unsw.edu.au/projects/unsw-nb15-dataset]). The selected dataset will be preprocessed accordingly with relevant libraries such as Pandas and Numpy, in order to accommodate unsupervised learning, which is the machine learning approach that the deliverable will aim to explore. For training GAN models specifically, generative adversarial training will be used by utilizing the GAN module within the PyOD library, as it provides a wide range of sophisticated algorithmic and optimization tools specialized for training GANs. A training of a variational autoencoder (VAE) is also considered due to the availability of the VAE module once again provided by PyOD. The evaluation part will analyze and compare the performance of the different models using multiple metrics such as accuracy, F1 score, and precision. Suitable visualizations will also be displayed by making use of the relevant utilities offered by the Scikit-learn and Matplotlib libraries.

The whole sequential process of implementing, training and testing the models will be described in detail in the final technical deliverable, justifying the principles used based on the knowledge acquired from the scientific deliverable. The UNSW-NB15 dataset and some of the selected libraries, such as the relevant utilities of PyOD, will also be explained, due to their crucial role in the overall process. Finally, the interpretation of the final results and their comparison will be documented, followed by a brief concluding discussion about their implications for the practicality of applying deep learning models in network anomaly detection.

References

[Fotiadou, K., Velivassaki, T. H., Voulkidis, A., Skias, D., Tsekeridou, S., & Zahariadis, T. (2021).] Network traffic anomaly detection via deep learning. Information, 12(5), 215.

[Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019).] Deep learning approach for intelligent intrusion detection system. Ieee Access, 7, 41525-41550.

[Sivasubramanian, A., Devisetty, M., & Bhavukam, P. (2024).] Feature Extraction and Anomaly Detection Using Different Autoencoders for Modeling Intrusion Detection Systems. Arabian Journal for Science and Engineering, 1-13.

[Zong, B., Song, Q., Min, M. R., Cheng, W., Lumezanu, C., Cho, D., & Chen, H. (2018, February).] Deep autoencoding gaussian mixture model for unsupervised anomaly detection. In International conference on learning representations.

[Truong-Huu, T., Dheenadhayalan, N., Pratim Kundu, P., Ramnath, V., Liao, J., Teo, S. G., & Praveen Kadiyala, S. (2020, October).] An empirical study on unsupervised network anomaly detection using generative adversarial networks. In Proceedings of the 1st ACM Workshop on Security and Privacy on Artificial Intelligence (pp. 20-29).

[https://research.unsw.edu.au/projects/unsw-nb15-dataset]