Batu Burgu 0402010098 – Javad Ibrahimli 040210932– Kerem Karadeniz 0402110049

Project Title:

Anomaly Detection in Networks Traffic Scenarios Using ML Based Algorithms

Project Overview:

This research focuses on developing machine learning based algorithms to detect anomalies in different network traffic scenarios. In modern networks, identifying malicious behavior or unusual patterns is critical to maintaining security and operational efficiency. Traditional anomaly detection methods often struggle with accuracy and adaptability due to the complexity of network environments and detecting abnormal behaviors in networks are known to be challenging for humans. This project aims to utilize ML-based algorithms like supervised learning models such as logistic regression, random forest, and regression to accurately detect traffic anomalies in various network scenarios. OMNeT++ or Sionna will be used to simulate realistic network traffic, and machine learning models will be integrated to identify and classify abnormal behavior.

Objectives:

1. Obtain the suitable data necessary to train machine learning models to be used for detecting anomalies in the network traffic scenarios from the simulations deployed in OMNeT++ and pre-existing datasets (data augmentation methods are planned to be used).
2. Develop and implement machine learning algorithms for detecting network anomalies.
3. Simulate various network traffic scenarios in OMNeT++ or Sionna and apply the developed ML models to detect abnormal patterns (the simulation environment will be decided according to the algorithm's deployment complexity in OMNeT++ and Sionna).
4. Evaluate the performance of the anomaly detection system based on detection accuracy, false positive rates, and computational efficiency.

Methodology:

1. **Literature Review**
2. **Simulation Environment**: OMNeT++ or Sionna will be used to simulate normal and anomalous network traffic patterns, including real-world scenarios such as Distributed Denial of Service (DDoS) attacks, spoofing, and network congestion.
3. **Data Collection**: Necessary traffic features, such as packet size, flow duration, and throughput, will be collected and fed into the ML models for training and validation. The data will be collected from pre-existing datasets and will be manually gathered from simulation environments.
4. **ML-Based Algorithms**: Supervised learning models (e.g., decision trees, SVM) will be explored to identify anomalies in the simulated traffic data.

5. **Performance Evaluation**: The simulation will measure performance indicators like packet delivery ratio, delay, throughput, and efficiency in adapting to real-time network conditions.

Tools and Technologies:

- **OMNeT++**: Simulation platform for network traffic scenarios.
- **Sionna**: Simulation platform for network traffic scenarios.
- **Python**: For AI algorithm development and integration into chosen simulation environments.
- **AI Frameworks**: For AI-based routing model training and deployment.

Expected Outcomes:

- A robust anomaly detection system integrated into OMNeT++ or Sionna using ML-based algorithms.
- Accurate detection of network traffic anomalies with minimal false positives, high precision and minimal algorithm delays.
- Comprehensive evaluation metrics comparing the performance of different machine learning models for anomaly detection.

References:

- OMNeT++ Discrete Event Simulator. (2023). Retrieved from https://omnetpp.org
- Perez, A., Morán-Fernández, D., Marnerides, A., & García-Teodoro, P. (2021). Deep Learning for Network Traffic Anomaly Detection. IEEE Access, 9, 18895-18909. https://doi.org/10.1109/ACCESS.2021.3052369
- Sionna: Open-Source Library for Machine Learning Research in Wireless Communications. (2023). Retrieved from https://nvlabs.github.io/sionna/
- Mohammed, R., Akay, M.F. (2023). Anomaly Detection in Network Traffic Using Machine Learning, Cukurova University Journal of Natural & Applied Sciences 2(3): 5-12
- Fosić, I., Žagar, D., Grgić, K., & Križanović, V. (2023). Anomaly detection in NetFlow network traffic using supervised machine learning algorithms
- ComNetsHH. (n.d.). omnetpp-ml [GitHub repository]. GitHub. Retrieved October 14, 2024, from https://github.com/ComNetsHH/omnetpp-ml
- Younis, O., & Fahmy, S. (2004). HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications, 366-379. https://doi.org/10.1145/1030194.1015492
- Varga, A., & Rudolf, C. (n.d.). *OMNeT++ simulation manual* (Version 6.0). OMNeT++. Retrieved October 14, 2024, from https://doc.omnetpp.org/omnetpp/SimulationManual.pdf