037-ENGR

“Comparative Analysis of GAN-Based Anomaly Detection Techniques for 5G Networks”

The advancement of communication technology, especially the fifth generation of wireless cellular technology, 5G, has led to faster, more reliable and improved communication channels. However, the expansion of 5G networks introduces complex threats and challenges as the attack surface has increased with a wider range of anomalies and attacks still prevailing. The traditional methods used in detecting network anomalies such as Network Intrusion Detection Systems (NIDS) and machine learning models often face difficulty in handling the complex high dimensional traffic and dataset produced by 5G systems. These methods face the issue of data imbalance which is because of the limited data samples belonging to the network anomalies or threats.

Generative Adversarial Networks (GANs) has come out in recent research as a possible solution to these issues. GANs have the key ability to model data distributions and produce quality synthetic data to support the minority anomaly classes. It also adaptive and is suitable in detecting zero-day attacks or new threats.

By using insights from existing research, this poster provides a comparative review of GAN based anomaly detection techniques against traditional methods for 5G. The focus is on anomalies such as Distributed Denial of service (DDoS) attacks and datasets such as CIC-DDoS2019 are discussed. The advantages of GANs, challenges and computational requirements are highlighted in the poster. Furthermore, GANs have a high computational demand because they really on AI infrastructure to good training and deployment. Technological institutions have a role to play in ensuring efficient use of computational resources and successful GAN training and deployment and this is equally discussed.