NETWORK INTRUSION DETECTION USING TWO-TIER DISCRIMINATION OF GENERATIVE ADVERSARIAL NETWORK

Chih-Wei Lin, Institute of Information Management, National Yang Ming Chiao Tung University, Hsinchu City, Taiwan, ROC, t91121t91121@gmail.com
Cooper Cheng-Yuan Ku, Institute of Information Management, National Yang Ming Chiao Tung University, Hsinchu City, Taiwan, ROC, cooperku@nycu.edu.tw
Ting-Yu Chang, Institute of Information Management, National Yang Ming Chiao Tung University, Hsinchu City, Taiwan, ROC, lunken.hank@gmail.com

EXTENDED ABSTRACT

With the increasing number of internet users and the inherent vulnerabilities in the global network infrastructure, there are many imminent threats from malicious attackers. These attackers may disrupt networking services or steal unauthorized access, leading to potentially significant losses. While many defense tools were proposed, such as network intrusion detection systems (NIDS), firewalls, and network intrusion prevention systems (NIPS), there's still much room for improvement in their efficiency. This paper delves into applying deep learning techniques, specifically the Generative Adversarial Network (GAN), to enhance network intrusion detection capabilities. We introduce a unique two-tier discrimination framework of GAN for abnormal detection. This framework incorporates two tiers: the collaborative tier and the auxiliary tier, as shown in Figure 1. The individual model in both tiers is built upon the discriminators trained through GAN.

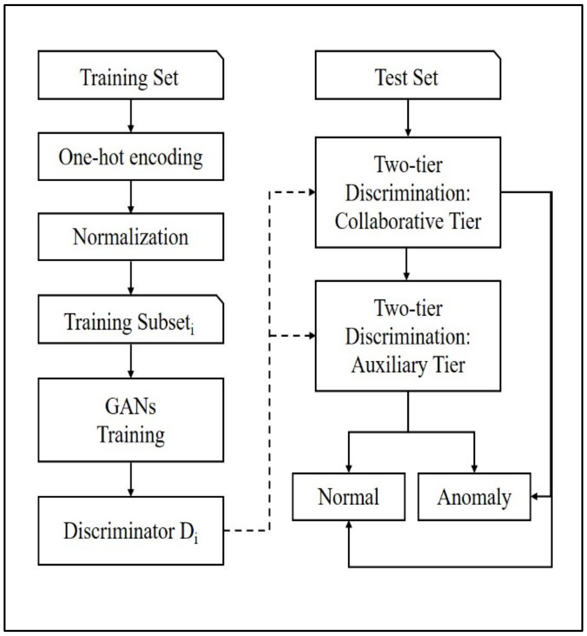

Figure 1 The workflow of the proposed framework

This GAN architecture comprises a generator synthesizing data and a discriminator that discerns between real and synthetic data. We harness the capability of the discriminator and train multiple variants using different types of data for enhanced detection capacity. The crux of our innovation lies in the two-tier discrimination framework. While previous literature predominantly focuses on GAN's data synthesis ability for NIDS, we employ GAN as a classification mechanism. The first tier, i.e., the collaborative tier, preliminarily classifies traffic as normal flow or malicious flow. Any ambiguous traffic is forwarded to the auxiliary level for further classification. This cascading mechanism ensures higher accuracy in malicious detection. The detailed procedure of this two-tier discrimination is illustrated in Figure 2. It is an enhanced proposal substantiated by the following experimental results. The NSL-KDD dataset, an enhancement over the KDD CUP 99 dataset, is utilized to implement the abovementioned experiments. It includes normal network traffic and four distinct attack types, i.e., DoS, U2R, R2L, and probing.

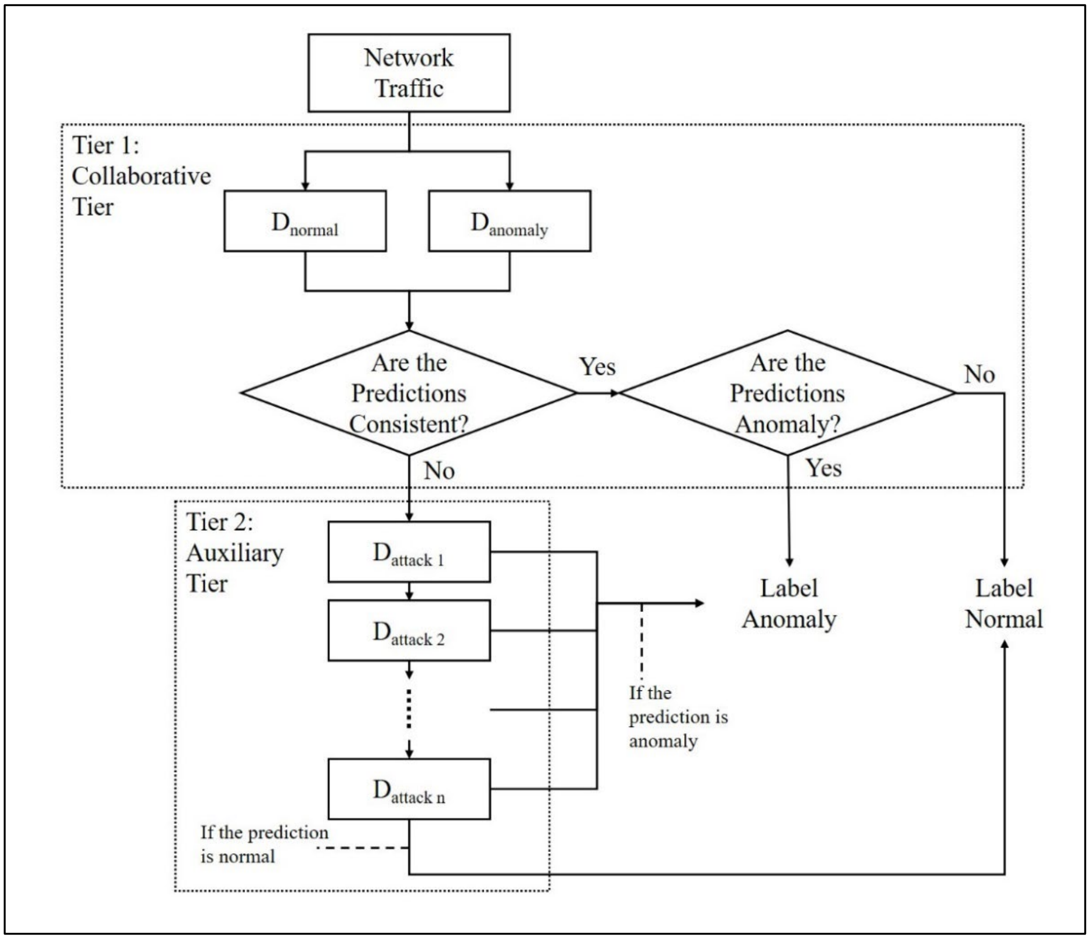
Network Traffic
Tier 1: Collaborative Tier
D_normal
D_anomaly
Are the Predictions Consistent?
Yes
Are the Predictions Anomaly?
No
No
Yes
Tier 2: Auxiliary Tier
D_attack 1
D_attack 2
D_attack n
Label Anomaly
Label Normal
If the prediction is anomaly
If the prediction is normal

Figure 2 The detailed procedure of the two-tier discrimination

This groundbreaking approach to network intrusion detection intertwines deep learning via GAN and a proprietary two-tier discrimination framework. The necessary data preprocessing involves one-hot encoding and min-max normalization for optimized gradient descent convergence. We then implement the discriminators derived from GAN using the NSL-KDD dataset. The collaborative tier undertakes primary classification, while the auxiliary tier handles more complex classifications. Our empirical evidence, based on the NSL-KDD dataset, substantiates the superior accuracy and F1 score of the proposed framework over other traditional methods. Consequently, our approach demonstrates enhanced accuracy in identifying benign and malicious network traffic types.

Keywords: Network Intrusion Detection, Anomaly Detection, Deep Learning, Two-tier Generative Adversarial Network, NSL-KDD.