Lightweight Hybrid Network Intrusion Detection Method based on AutoEncoder-XGBoost

Won Seok Choi
Research Institute for Computer and Information Communication
Chungbuk National University
Chungju, Republic of Korea
choiws@cbnu.ac.kr

Bum Su Kim
School of Information and Communication Engineering
Chungbuk National University
Chungju, Republic of Korea
bmori3@naver.com

Hyeon Ho Lee
School of Information and Communication Engineering
Chungbuk National University
Chungju, Republic of Korea
hhl9438@cbnu.ac.kr

Seong Gon Choi*
School of Information and Communication Engineering
Chungbuk National University
Chungju, Republic of Korea
choisg@cbnu.ac.kr

***Abstract*—We propose a lightweight hybrid network intrusion detection method based on AutoEncoder and XGBoost for use in resource-constrained environments such as small-scale networks, smartphones, and personal computers. Without relying on complex additional modules, the proposed system employs a lightweight pipeline consisting of a single AutoEncoder and XGBoost, enabling high-performance intrusion detection without the high memory and computational demands typically required for training and inference. In addition, to improve the learning rate for sparse attack traffic types, we apply Generative Adversarial Network (GAN)-based data augmentation for such traffic, thereby enhancing overall detection performance. To evaluate the effectiveness of the proposed method, we implemented the system and confirmed that it achieves high detection rates and practical applicability even in resource-limited environments.**

Keywords—Network Intrusion Detection, AutoEncoder, XGBoost, GAN, Lightweight

I. Introduction

Recent advances in artificial intelligence (AI), autonomous driving, and the Internet of Things (IoT) have been increasingly integrated with information and communication technologies (ICT). Along with the development of various ICT convergence technologies, intelligent cyberattacks have also become more sophisticated, making intrusion detection systems (IDS) an essential component of network security. In particular, recent years have seen active research on utilizing AI techniques, including machine learning and deep learning, to learn and detect abnormal behaviors [1][2].

AI-based network intrusion detection methods have attracted considerable attention in the field of network security because they can respond not only to known attack patterns but also to new and previously unseen types of attacks [3]-[5].

The XIDINTFL-VAE study applies Class-Wise Focal Loss to a variational AutoEncoder to synthesize data from sparse classes, thereby balancing the training data distribution, and then uses an XGBoost classifier to detect intrusions [3]. The Logarithmic AutoEncoder and XGBoost-based intrusion detection system replaces the conventional data normalization process with a logarithmic transformation layer, extracts features using an AutoEncoder, and classifies them with XGBoost [4]. The study by Kang et al. proposes an AutoEncoder–XGBoost-based intrusion detection model that mitigates data imbalance by upsampling normal samples, selecting key features using a random forest, and grouping features via the affinity propagation algorithm [5].

However, these existing studies improve detection rates by adding new algorithms or modifying the model, which increases model complexity and demands high memory and computational resources during training and inference. Such requirements make practical deployment difficult in hardware-constrained environments such as smartphones and personal computers.

Therefore, we propose a lightweight hybrid pipeline consisting of a single AutoEncoder and XGBoost. In addition, to enhance the learning capability for sparse attack traffic types, we apply Generative Adversarial Network (GAN)-based data augmentation for such traffic. The proposed method can perform training and inference with minimal memory and computational resources, and experiments demonstrate that it achieves high detection rates even in resource-constrained environments.

This paper is organized as follows. Section II reviews AI-based network intrusion detection techniques. Section III details the proposed lightweight hybrid network intrusion detection method. Section IV presents the experimental results, and Section V concludes the research and discusses future research directions.

II. Related Work

AI-based network intrusion detection techniques are actively being researched in the field of network security due to their ability to respond to not only known attack patterns but also new types of attacks. In particular, AutoEncoder (AE) and XGBoost have demonstrated excellent performance in anomalous traffic detection, leading to the proposal of various variants [3]-[5].

XIDINTFL-VAE uses a Variational AutoEncoder (VAE) with class-specific Focal Loss to generate and augment sparse class data to balance the training data distribution, then uses an XGBoost classifier to detect intrusions. It achieves high accuracies of 99.79% and 99.89% on the NSL-KDD and CSE-CIC-IDS2018 datasets, respectively, and maintains a precision of over 99%, resulting in a low false positive rate [3]. However, due to its structure combining Class-Wise Focal Loss, VAE, and XGBoost, it requires significant computation and memory during training and inference, and its execution time is longer than other techniques.

Studies on intrusion detection systems based on Logarithmic Autoencoder and XGBoost replace the data normalization process with a logarithmic transformation layer to reduce information loss during preprocessing. They then combine features extracted by AE with original data for classification using XGBoost. They achieve accuracies of 95.11% and 99.92% on the UNSW-NB15 and CICIDS2017 datasets, respectively, and a short execution time of 132 seconds, demonstrating their practicality [4]. However, the addition of the AE structure and data combination process increases model complexity.

Kang et al.'s study of an intrusion detection model based on AutoEncoder and XGBoost involves upsampling normal samples, selecting key features using Random Forest (RF), grouping features using Affinity Propagation, and then training AutoEncoder groups to extract root mean square errors as features and classifying them using XGBoost. This approach mitigates data imbalance issues, achieving an average accuracy of over 99% on the CSE-CIC-IDS2018 dataset [5]. However, its multiple AE structures and numerous preprocessing steps require high resource usage and long processing times during the training and inference processes.

Therefore, we propose a lightweight hybrid network intrusion detection method based on AutoEncoder and XGBoost for application in small-scale networks, smartphones and personal computers.

III. Proposed Lightweght Hybrid Network Intrusion Detection Method

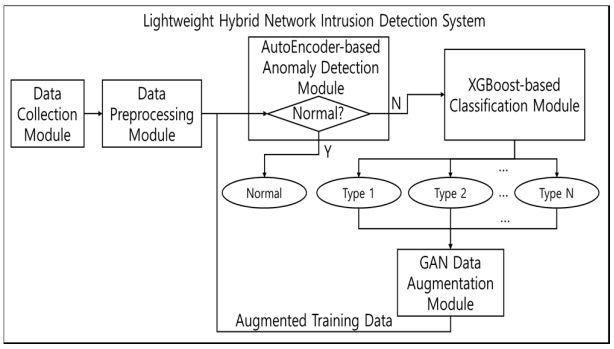

Fig. 1. Proposed Lightweight Hybid Netowrk Intrusion Detection System

We propose a lightweight hybrid network intrusion detection method based on AutoEncoder and XGBoost. Figure 1 illustrates the proposed lightweight hybrid network intrusion detection system. The proposed system consists of a data collection module, a data preprocessing module, an AutoEncoder-based anomaly detection module, an XGBoost-based classification module, and a GAN-based data augmentation module.

The data collection module provides either training datasets for model training or incoming packets for inference. Data collected during inference can also be stored and later utilized for retraining or fine-tuning of the model.

The data preprocessing module performs one-hot encoding of categorical variables and normalization of continuous variables for both training and inference. During training, it also separates normal and abnormal data.

The AutoEncoder-based anomaly detection module learns normal traffic patterns and detects anomalies by computing reconstruction error in the latent space.

The XGBoost-based classification module analyzes the feature importance of anomalous packets. During inference, the AutoEncoder first determines whether a packet is anomalous based on a predefined threshold. If classified as anomalous, the XGBoost classifier further identifies the attack type into categories such as DoS, Probe, R2L, and U2R.

The GAN-based data augmentation module generates synthetic samples for rare attack types, such as those with insufficient training data, to enhance classifier performance.

The operation of the proposed lightweight hybrid network intrusion detection system is as follows: once data is collected, it undergoes preprocessing, followed by anomaly detection through the AutoEncoder. If the packet is anomalous, the XGBoost-based classification module identifies the specific attack type. For attack categories with limited training data, the GAN-based augmentation module enriches the dataset with synthetic samples, which are then incorporated into training.

IV. Performance Evaluation

In this section, we evaluate the performance of the proposed lightweight hybrid network intrusion detection system.

For the experiments, we used the KDD99 dataset, which consists of 41 features and five main classes: Normal, DoS, Probe, R2L, and U2R. Preprocessing involved one-hot encoding of categorical variables (e.g., protocol type) and Min–Max normalization of continuous variables. The attack type labels were further consolidated into the five major categories mentioned above. The dataset was split into 70% for training and 30% for testing.

The AutoEncoder-based anomaly detection module was implemented with a four-layer encoder: Input (113), Dense (64), Dense (48), and Dense (32). The decoder mirrored this structure with four layers: Dense (32), Dense (48), Dense (64), and Output (113). Training was performed using only normal data to ensure identical input and output, enabling the detection of deviations through reconstruction error. An input was determined to be anomalous if its mean squared error (MSE) exceeded a predefined threshold, which was set at the 99th percentile of the normal data distribution (contamination = 0.01).

The XGBoost-based classification module was configured with a maximum decision tree depth of 6 and a learning rate of 0.3. The objective function was set to multi:softprob, which outputs a probability distribution over classes (e.g., [0.1, 0.3, 0.6, 0.0, 0.0]). The final prediction corresponds to the class with the highest probability. To mitigate overfitting, both the training data sample ratio and feature sample ratio were set to 0.8, meaning that 80% of the training samples and 80% of the features were randomly selected for training each tree.

The GAN-based data augmentation module was designed to generate synthetic samples for underrepresented attack classes. The generator network consisted of an input latent space vector of size 64, followed by Dense layers of 128 and 256 units, and an output layer producing attack feature vectors of size 113. The discriminator network was structured with an input feature vector of size 113, followed by Dense layers of

256 and 128 units, and a final output layer producing a one-dimensional probability indicating whether the input was real or synthetic.

TABLE I. HARDWARE AND SOFTWARE ENVIRONMENT

Component		Specification
Hardware	CPU	Ryzen 5900x 3.7GHz
	GPU	NVIDIA RTX 3090
	RAM	DDR4 48GB
Software	Python	Vserion 3.10
	TensorFlow	Vserion 2.12.0
	XGBoost	Vserion 1.7.5

Table I shows the hardware and software specifications used in the experiment. The main hardware components included a Ryzen 5900x CPU, an NVIDIA RTX 3090 GPU, and 48 GB of RAM. For software, Python 3.10 was used, along with the TensorFlow 2.12.0 and XGBoost 1.7.5 libraries. The proposed lightweight hybrid network intrusion detection method was tested on a personal computer level specification system.

TABLE II. AUGMENTED DATA FOR TRAINING

Class		Before Augmentation	After Augmentation	Increase
Normal Data		680,805	680,805	0
Abnormal Data	DoS	2,718,505	2,719,505	1,000
	Probe	28,759	29,759	1,000
	R2L	797	2,797	2,000
	U2R	35	535	500

Table II shows the augmented training data. Before augmentation, the training dataset consisted of 680,805 normal samples, 2,718,505 DoS samples, 28,759 Probe samples, 797 R2L samples, and 35 U2R samples. Using the GAN-based data augmentation module, the DoS data was augmented by 1,000 samples to 2,719,505, the Probe data by 1,000 to 29,759, the R2L data by 2,000 to 2,797, and the U2R data by 500 to 535.

The proposed hybrid network intrusion detection method was evaluated using both the pre-augmented and post-augmented datasets.

TABLE III. PERFORMANCE EVALUATION RESULTS BEFORE DATA AUGMENTATION

Class	Precision	Recall	F1-score	Support
Normal	0.99	0.99	0.99	291,976
Dos	1.00	1.00	1.00	1,164,865
Probe	0.92	0.94	0.93	12,343
R2L	0.06	0.16	0.08	329
U2R	0.11	0.76	0.20	17
Average	0.62	0.77	0.64	-

Table III summarizes the number of samples per class used for training. A total of 680,805 normal samples and 2,748,096 abnormal samples (DoS, Probe, R2L, and U2R) were used. Among the abnormal classes, R2L and U2R attacks have relatively few samples.

Table IV presents the class-specific performance of the proposed AutoEncoder and XGBoost-based lightweight hybrid network intrusion detection system, tested on the KDD99 dataset using PC-grade hardware. Anomalous packets were classified into DoS, Probe, R2L, and U2R attack types, and the evaluation metrics included Precision, Recall, F1-score, and Support.

TABLE IV. PERFORMANCE EVALUATION RESULTS AFTER DATA AUGMENTATION

Class	Precision	Recall	F1-score	Support
Normal	0.99	0.99	0.99	291,976
Dos	1.00	1.00	1.00	1,164,865
Probe	0.92	0.94	0.93	12,343
R2L	0.09	0.37	0.15	329
U2R	0.31	0.95	0.47	17
Average	0.67	0.85	0.71	-

Precision measures the proportion of packets predicted as positive that are true positives. Recall measures the proportion of actual positive packets correctly identified. F1-score is the harmonic mean of Precision and Recall, balancing the two metrics. Support indicates the number of samples per class.

DoS attacks accounted for the largest portion of all samples and achieved perfect detection performance with Precision, Recall, and F1-score of 1.00. Probe attacks, despite a smaller sample size, achieved high performance with Precision of 0.92, Recall of 0.94, and F1-score of 0.93. In contrast, R2L attacks showed low detection performance, with Precision of 0.06, Recall of 0.16, and F1-score of 0.08 based on only 329 samples. U2R attacks, with 17 samples, achieved a relatively high Recall of 0.76 but suffered from low Precision (0.11) and an F1-score of 0.20 due to false positives. Finally, normal packets were classified with high accuracy, achieving both Precision and Recall of 0.99, indicating that the model effectively distinguishes between normal and anomalous packets.

V. CONCLUSION

In this paper, we proposed a lightweight hybrid network intrusion detection method based on AutoEncoder and XGBoost. Experiments and performance analysis were conducted on the KDD99 dataset using a PC-grade hardware environment. To address classes with insufficient training data, we applied GAN-based data augmentation. The experimental results demonstrated improved detection performance, even for classes with small sample sizes and subtle features, such as R2L and U2R attacks.

Future work will focus on evaluating the proposed method on additional open datasets and further optimizing the system to enhance detection rates. Furthermore, we will measure computational cost and memory usage compared to existing AutoEncoder–XGBoost approaches, to more clearly demonstrate the lightweight advantages.

ACKNOWLEDGMENT

This work was supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No. RS-2024-00397979, Development of tera-level ultra-precision transmission network system technology, 50%) and by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (No. RS-2020-NR049604, 50%).

*Corresponding author: S.G. Choi(choisg@cbnu.ac.kr)

REFERENCES

[1] Truong, T. M., Choi, W. S., Hyeon, J. J., Choi, S. G. "The Development of a New System for Generating Training Data of AI-Based Anomaly Detection," In 2024 26th International Conference on Advanced Communications Technology (ICACT), Feb. 2024.

[2] Choi, W. S., Lee, S. Y., & Choi, S. G., "Implementation and Design of a Zero - Day Intrusion Detection and Response System for Responding to Network Security Blind Spots," Mobile Information Systems, 2022(1), 2022

[3] Abdulganiyu O. H., Ait Tchakoucht T., Saheed Y. K., Ahmed H. A. "XIDINTFL-VAE: XGBoost-based intrusion detection of imbalance network traffic via class-wise focal loss variational autoencoder," The Journal of Supercomputing, vol. 81, 2025.

[4] Xu W., Fan Y. "Intrusion Detection Systems Based on Logarithmic Autoencoder and XGBoost," Security and Communication Networks, vol. 2022.

[5] [4] Kang Y., Tan M., Lin D., Zhao Z. "Intrusion Detection Model Based on Autoencoder and XGBoost," Journal of Physics: Conference Series, vol. 2171, 2022.