2025년도 한국통신학회 하계종합학술발표회

Leveraging AutoML for Enabling Zero-Touch Intrusion Detection in Future Generation Wireless Networks

Md. Monirul Islam and Seong Ho Jeong*
Hankuk University of Foreign Studies
monirul@hufs.ac.kr, shjeong@hufs.ac.kr*

차세대 무선 네트워크에서 제로터치 침입 탐지를 활성화하기 위한 AutoML 활용

모니룰, 정성호
한국외국어대학교 정보통신공학과

Abstract

As next generation wireless networks such as 6G networks strive for ultra-reliable, low-latency, and extremely scalable connectivity, controlling network operations with minimal human interaction becomes crucial. Automated Machine Learning (AutoML) can manage complex processes like resource allocation, anomaly detection, and predictive maintenance more efficiently. This paper proposes a way to leverage AutoML to enhance intrusion detection systems (IDS) in future generation wireless networks. Specifically, the paper shows an architecture of AutoML to enable Zero-Touch Intrusion Detection (ZT-ID) where the processes of model selection, training, and hyperparameter optimization are automatically handled for intrusion detection tasks to minimize manual intervention and enhance the system's ability to detect evolving threats. By automating the IDS process using AutoML, the ZT-ID can increase detection accuracy, scalability, and resource efficiency in future wireless networks without human intervention or with minimal human intervention.

Ⅰ. Introduction

ZT-ID minimizes or eliminates human intervention in intrusion detection. As the network technology rapidly advances with the advent of 6G, ensuring security and performance across complex infrastructures becomes increasingly challenging. Intrusion detection systems (IDSs) are essential for identifying malicious activities such as Denial of Service (DoS), probe attacks, and unauthorized access. Traditional IDSs require manual model selection, tuning, and adaptation to evolving attack patterns, making them inefficient for dynamic networks. This paper proposes a way to leverage AutoML to automate the intrusion detection process, specifically focusing on optimizing machine learning models for future wireless environments. AutoML simplifies model selection, training, and hyperparameter tuning, enabling non-experts to build effective models [1]. This approach enhances ZT-ID by reducing human oversight while improving the detection of emerging attack patterns.

Ⅱ. Method

The proposed approach applies AutoML to intrusion detection tasks in network security. The methodology is shown in Figure 1.

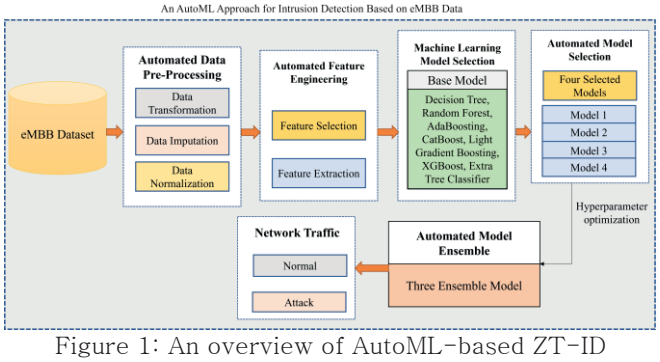

Figure 1: An overview of AutoML-based ZT-ID framework

Data preprocessing improves model quality by addressing outliers, missing values, and class imbalance. Automated preprocessing converts categorical data, imputes missing values, balances classes, and normalizes data. Automated Feature Engineering (AutoFE) enhances models by generating, selecting, and extracting key features, reducing redundancy and speeding intrusion detection. The AutoML framework can be used for the model and training process automatically to improve intrusion detection performance. AutoML's hyperparameter optimization techniques find the optimal settings for each selected model, ensuring that the intrusion detection system achieves maximum performance in detecting attacks. Once the model is trained, the system autonomously classifies network traffic in real-time, detecting intrusions with minimal human intervention.

Table 1 shows the comparison results based on eMBB dataset. Three ensemble strategies based on AutoML—OCSE (Optimized Confidence-Based Stacking), OTSE (Optimized Traditional Stacking), and OHSE (Optimized Hybrid Stacking)—are evaluated for classification performance. Among them, OCSE achieved the highest accuracy of 99.66%, along with the best precision, recall, and F1-score, indicating superior model performance. Both OTSE and OHSE followed closely, each with 99.57% accuracy, showing consistent and highly reliable results across all metrics. Figure 2 shows the confusion matrix for OCSE model.

Table 1: Model Performance Comparison on eMBB dataset.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
OCSE	99.6558	99.6563	99.6557	99.6557
OTSE	99.5697	99.5709	99.5697	99.5697
OHSE	99.5697	99.5709	99.5697	99.5696

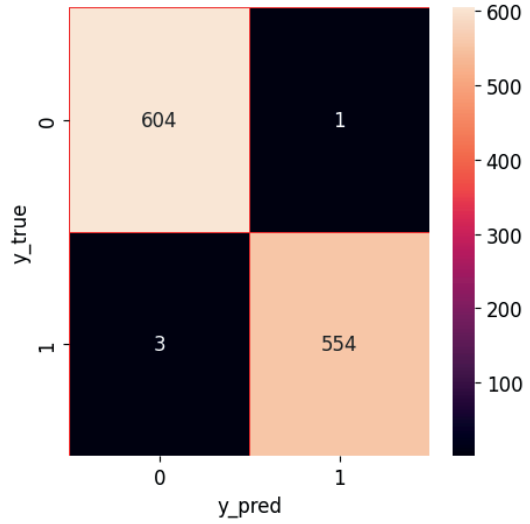

Figure 2. Confusion matrix of OCSE

Ⅲ. Conclusion

In this paper, we proposed an AutoML-based framework for a zero-touch intrusion detection system applicable to real-world scenarios.

ACKNOWLEDGMENT

This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (RS-2022-00156353) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation).

REFERENCES

[1] Yang, Li, et al. "Enabling AutoML for Zero-Touch Network Security: Use-Case Driven Analysis." IEEE Transactions on Network and Service Management (2024).