# DDoS Attack Detection with Time-Series Predictions Using Empirical Dynamic Modeling

Wassapon Watanakeesuntorn, Keichi Takahashi, Junya Yamamoto, Kohei Taniguchi,
Hirotake Abe, Arata Endo, Chonho Lee, Susumu Date
D3 Center, Osaka University
Japan
wassapon.w@osaka-u.ac.jp

## 1. INTRODUCTION

Cloud-Edge Continuum Computing Infrastructure is an emerging infrastructure designed to unify cloud and edge clusters into a single computing system. Users can gain benefits to access geo-distributed sensors on edge devices with low latency and seamlessly execute high-performance applications on cloud clusters. However, this infrastructure can be susceptible to cyberattacks from unknown sources. Distributed Denial of Service (DDoS) is a common cyberattack in computer networks that floods large amounts of traffic from multiple sources to cause the victim's service becomes unavailable. DDoS detection is a challenging topic in the field of network security. Deep learning has been successfully applied to detect DDoS in previous studies. However, machine learning–based models typically require large amounts of data to train, making them unsuitable for real-time detection systems. In this research, we propose Empirical Dynamic Modeling (EDM) to detect DDoS attacks in computer networks. EDM is a mathematical framework for modeling nonlinear dynamical systems and can be used to predict future states of these systems. We assume that computer network traffic is a dynamical system that can be modeled and predicted using EDM. We can detect anomalies when the network metrics predicted by an EDM-based model (trained under normal conditions) significant deviate from actual measurements.

## 2. BACKGROUND

EDM has traditionally been used to model nonlinear dynamical systems in biology, neurology, oceanography, and other fields. Based on our previous works, mpEDM [1] and kEDM [2] were developed to execute EDM while fully utilizing supercomputer systems, including parallel computing and GPU acceleration. To the best of our knowledge, a few studies have applied EDM to problems in computer science. In computer science, time-series prediction is a popular research area, with many techniques, such as Autoregression and Long Short-Term Memory (LSTM), proposed to address it. This gap presents an opportunity for original research by introducing EDM into the computer science field. Thus, using EDM to model the dynamics of computer networking is a novel approach.

## 3. IMPLEMENTATION

We conducted an experiment to evaluate EDM for network traffic prediction tasks, comparing with AR and LSTM in terms of runtime and prediction accuracy. Figure 1 illustrates the overall process of applying EDM and machine learning for DDoS attack classification. First, we preprocess the dataset by selecting key features, such as the number of packets, average packet size, and packet flags. Then, we convert these features into multiple time series for training and prediction. During preprocessing, we created two separate datasets: one containing only normal traffic for training, and another containing a mix of normal and DDoS traffic for classification. Next, we test EDM, AR, and LSTM with various parameters to find the best results in terms of prediction runtime. After obtaining traffic predictions, we used the Root Mean Square Error (RMSE) to measure the difference between the actual observations and the predicted values for evaluating the prediction error. Finally, we employed a random forest classifier to distinguish between normal and DDoS attack traffic and evaluated the classification accuracy.

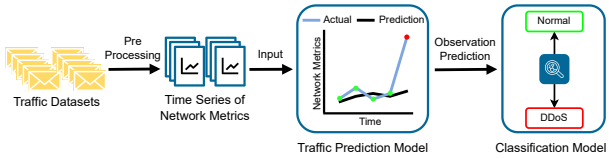


Figure 1: DDoS Attack Classification Process with EDM

## 4. RESULT AND CONCLUSION

In this experiment, we used EDM to individually predict 18 network traffic features and compared its performance with AR and LSTM. The preliminary results indicate that EDM predicts time series faster than LSTM-based model and achieves higher classification accuracy than the AR-based model. Our next step is to expand the dataset and fine-tune the parameters to achieve the best results from EDM.

## ACKNOWLEDGMENTS

This paper is based on results obtained from the project, "Research and Development Project of the Enhanced infrastructures for Post-5G Information and Communication Systems" (JPNP20017), commissioned by the New Energy and Industrial Technology Development Organization (NEDO).

## REFERENCES

[1] Watanakeesuntorn, Wassapon, et al. "Massively parallel causal inference of whole brain dynamics at single neuron resolution." 2020 IEEE 26th International Conference on Parallel and Distributed Systems (ICPADS). IEEE, 2020.

[2] Takahashi, Keichi, et al. "kEDM: a performance-portable implementation of empirical dynamic modeling using Kokkos." Practice and Experience in Advanced Research Computing. ACM, 2021.