

Achieving High-Speed and Robust Encrypted Traffic Anomaly Detection with Programmable Switches

Han Zhang¹, Guyue Liu³, Xingang Shi¹, Yahui Li¹, Dongbiao He⁵, Jilong Wang¹, Zhiliang Wang¹,
Yongqing Zhu⁴, Ke Ruan⁴, Weihua Cao⁴, Xia Yin²

¹Institute for Network Sciences and Cyberspace, Tsinghua University

²Department of Computer Science and Technology, Tsinghua University

³School of Computer Science, Peking University

⁴China telecom

⁵Sangfor Technologies Inc

ABSTRACT

Attacks against data centers are becoming more common as a result of the fast expansion of applications. In order to keep pace with the growing amount of data centers connected to their networks, internet service providers must offer comprehensive security services. However, existing network intrusion detection systems (NIDS) are either ineffective or inefficient for the high-speed encrypted network traffic. In this paper, we design and implement Mazu, an inline network intrusion detection system with programmable switches specifically developed to protect data centers connecting to the internet service provider. Mazu proposes a dual-plane feature extraction model to extract extensive traffic features at near line-speed. Mazu also proposes a lightweight one-class classification model that trains the best parameters exclusively on benign traffic to identify the malicious traffic. In addition, Mazu introduces an online update mechanism aimed at dynamically adjusting the detection model in response to environmental changes. Mazu has been in production for two years, during which time it has identified over 10 critical attack events and protect more than 10 million servers for two ISPs. Our production and testbed evaluations demonstrate that Mazu can detect malicious traffic entering the data center sites with approximately 90% accuracy within minutes.

CCS CONCEPTS

• **Networks** → **Network monitoring**; **Network measurement**; **Network security**;

KEYWORDS

Security; Anomaly Detection; Network Intrusion Detection ; Programmable Switches

ACM Reference Format:

Han Zhang¹, Guyue Liu³, Xingang Shi¹, Yahui Li¹, Dongbiao He⁵, Jilong Wang¹, Zhiliang Wang¹, Yongqing Zhu⁴, Ke Ruan⁴, Weihua Cao⁴, Xia Yin².

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

SIGCOMM '25, September 8–11, 2025, Coimbra, Portugal

© 2025 Copyright held by the owner/author(s). Publication rights licensed to the Association for Computing Machinery.

ACM ISBN 979-8-4007-1524-2/25/09...\$15.00

<https://doi.org/10.1145/3718958.3750493>

2025. Achieving High-Speed and Robust Encrypted Traffic Anomaly Detection with Programmable Switches. In *ACM SIGCOMM 2025 Conference (SIGCOMM '25)*, September 8–11, 2025, Coimbra, Portugal. ACM, New York, NY, USA, 3 pages. <https://doi.org/10.1145/3718958.3750493>

1 INTRODUCTION

With the rapid development of big data, artificial intelligence [6], especially language models [5, 7, 11], the demand for data centers has increased significantly [9, 10]. In this trend, the economic losses caused by data center attacks [2–4, 8] are also steadily rising.

The network intrusion detection system (NIDS) is an essential device for monitoring network traffic, detecting anomalous activities, and reporting alerts upon their identification. The current NIDS frameworks can be categorized into out-of-band and inline based on their deployment strategies. Although most of them have already shown high performance in malicious traffic detection, they are still inadequate in providing high-speed encrypted traffic.

To address these challenges, we present Mazu, an inline NIDS specifically designed to safeguard data center security at ISPs, leveraging the capabilities of programmable switches. Mazu achieves both *efficient* and *robust* malicious traffic detection with the following designs:

Dual-plane feature extraction model. We propose a new dual-plane detection model: basic operations (e.g., packet counting, lookups) are offloaded to programmable data plane engines for high performance, while complex computations (e.g., division, exponential operations) are delegated to CPU engines to fully utilize their general computing capabilities.

Lightweight one-class classification model. Mazu advocates to perform anomaly detection in a lightweight manner. The extraction of valuable information concealed within encrypted traffic in a resource-constrained environment is challenging. Therefore, we propose a 2D Discrete Fourier Transform (2DDFT) to transform the traffic representation to model the spatiotemporal relationship within and between the feature sequences.

An online update mechanism. Mazu employs an online update mechanism for parameter update. When a high false alarm rate is detected, Mazu enters the update phase, during which the detection model is refined using samples provided by the data center users based on the current parameters. Our results demonstrate that Mazu is capable of adjusting the parameters to environment changes.

Contributions. Mazu has been in production for two years, handling thousands of TB traffic daily. Over the past two years, it has

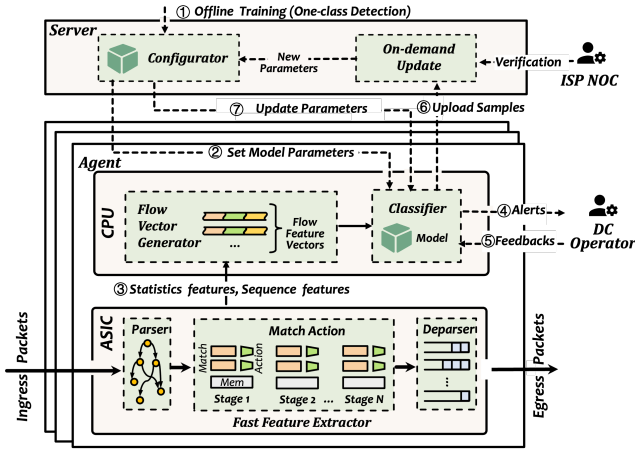


Figure 1: Mazu framework overview.

identified over 10 critical attack events and protect more than 10 million servers for the two ISPs.

2 MAZU DESIGN

This part presents the design and implementation of Mazu, an inline intrusion detection system that is designed with programmable switches to provide precise and effective malicious traffic detection service for data center sites on the ISP side.

The architecture in Figure 1 depicts the structure of Mazu, demonstrating its capability to identify and analyze harmful network activity from the ISP to the data centers. In general, Mazu consists of two high-level components: **Agent** and **Server**. The FTP component extracts flow statistics features (e.g., average flow length) and packet sequence features (e.g., packet size sequence) at the data plane. The FVG component forms the feature vector at the control plane. The Classifier component runs the malicious traffic detection algorithm. The Mazu server works at the ISP network operator center (NOC) and it is responsible for configuring and updating the model. Mazu involves the operational phase and the update phase.

Operational phase: Since the system developers are hard to attain the production labeled attack events, therefore, Mazu offline trains the one-class malicious traffic detection model just by the benign traffic patterns (①). Then Mazu server configures the agent (②). By generating flow vectors through an adjustable detection window ϵ (e.g., two to three minutes), the FVG component can effectively balance detection latency with cost efficiency (③). Upon identifying malicious behavior, the classifier promptly reports alarms to the data center operators (④). In turn, the data center operators are accountable for reporting any false alarms or missed attack events that have been verified by data center users back to the classifier (⑤).

Update phase: In practice, the fundamental characteristics of the network, such as bandwidth, packet interval, and connection duration, can exhibit significant variability. This variability may cause the training environment to diverge from the conditions observed in the real deployment environment. When the false positive rate of traffic analysis exceeds a pre-defined threshold after deployment, it indicates that the current parameters are no longer adequately aligned with the network conditions, prompting the system to enter

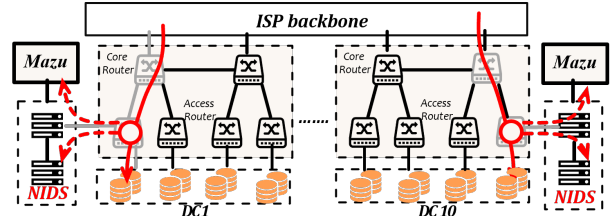


Figure 2: Production topology.

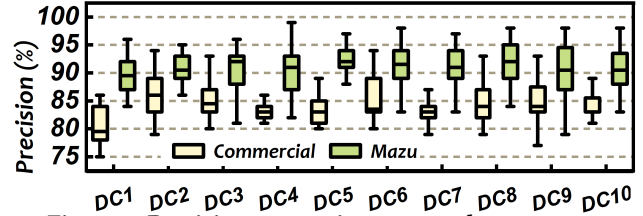


Figure 3: Precision comparison across data centers.

the update phase. During this phase, the classifier component of Mazu agent reports the extracted flow features and the corresponding detection results to Mazu server (⑥). The ISP network operation center (NOC) operators may participate in verifying the feedback on the updated samples. The Mazu server then utilizes the provided traffic samples to execute a model update algorithm designed to adapt to these environmental changes. The updated parameters are subsequently configured to the corresponding agents. Once the observed false positive rate falls below the threshold, Mazu transitions back to the operational phase (⑦).

3 MAZU IN PRODUCTION

We begin our evaluation of Mazu by first performing experiments on a real production ISP network. We selected 10 data centers to perform the evaluations. As shown in Figure 2, each site connects to the core routers through two access routers. The capacity between each access router and the core router link is 100 Gbps. Each data center operates over 20,000 applications across 100,000 servers.

Setup. We have implemented Mazu agent on the Tofino switch [1] with 3.2 Tbps bandwidth. To conduct testing without affecting the business, we configured the traffic mirrored to Mazu. As shown in Figure 2, all the traffic from the Internet to the data center will be mirrored to Mazu agent. Mazu server is deployed at the ISP network operator center. The experiment lasted 6 months. In comparison, we also deployed a commercial out-of-band rule based NIDS¹ to analyze the traffic. The product manual indicates that the commercial NIDS is implemented utilizing 20 general-purpose servers proficient in rapidly sampling and detecting malicious traffic according to pre-established rules.

Ground truth. Upon detecting malicious behaviors, the systems will notify the data center operators. The data center operators will verify the accuracy of the detection results with the data center users. Furthermore, data center users also reported their attack incidents to the data center operators to inform them of undetected events.

Results. Figure 3 demonstrates that the overall precision accuracy of Mazu is over 90% over the 10 data centers. Mazu has stable performance, and it is up to 30% better than the commercial NIDS.

¹We do not disclose its specific name due to the commercial privacy.

The performance of Mazu is superior to commercial NIDS due to its ability to manage all traffic and adapt to changes in the environment, whereas the commercial NIDS are limited to managing partial traffic with strict rules.

ACKNOWLEDGMENTS

The research is supported by the National Natural Science Foundation of China under Grant No. 62394322 and National Natural Science Fund for the Excellent Young Scientists Fund Program (Overseas). The corresponding authors are Guyue Liu and Yahui Li.

REFERENCES

- [1] Barefoot Networks. 2022. Tofino Switch. <https://www.barefootnetworks.com/products/brief-tofino/>. (2022).
- [2] Colonial Pipeline ransomware attack. 2012. Colonial Pipeline ransomware attack. <https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years>. (2012).
- [3] cyberark. 2024. Identity Security Threat Landscape Report. <https://www.cyberark.com/threat-landscape/>. (2024).
- [4] dyn. 2023. Dyd DDOS attack. https://en.wikipedia.org/wiki/DDoS_attacks_on_Dyn. (2023).
- [5] Qinghao Hu, Zhisheng Ye, Zerui Wang, Guoteng Wang, Meng Zhang, Qiaoling Chen, Peng Sun, Dahua Lin, Xiaolin Wang, Yingwei Luo, et al. 2024. Characterization of large language model development in the datacenter. In *21st USENIX Symposium on Networked Systems Design and Implementation (NSDI 24)*. 709–729.
- [6] Haochen Hua, Yutong Li, Tonghe Wang, Nanqing Dong, Wei Li, and Junwei Cao. 2023. Edge computing with artificial intelligence: A machine learning perspective. *Comput. Surveys* 55, 9 (2023), 1–35.
- [7] Ziheng Jiang, Haibin Lin, Yinmin Zhong, Qi Huang, Yangrui Chen, Zhi Zhang, Yanghua Peng, Xiang Li, Cong Xie, Shibiao Nong, et al. 2024. {MegaScale}: Scaling large language model training to more than 10,000 {GPUs}. In *21st USENIX Symposium on Networked Systems Design and Implementation (NSDI 24)*. 745–760.
- [8] yahoo-hacks. 2012. A History of Yahoo Hacks. <https://www.technologyreview.com/2016/12/15/106901/a-history-of-yahoo-hacks/>. (2012).
- [9] Han Zhang, Xingang Shi, Xia Yin, Jilong Wang, Zhiliang Wang, Yingya Guo, and Tian Lan. 2021. Boosting bandwidth availability over inter-DC WAN. In *Proceedings of the 17th International Conference on emerging Networking EXperiments and Technologies*. 297–312.
- [10] Han Zhang, Xia Yin, Xingang Shi, Jilong Wang, Zhiliang Wang, Yingya Guo, Tian Lan, Yahui Li, Yongqing Zhu, Ke Ruan, and Haijun Geng. 2022. Achieving High Availability in Inter-DC WAN Traffic Engineering. *IEEE/ACM Trans. Netw.* 31, 6 (Dec. 2022), 2406–2421. <https://doi.org/10.1109/TNET.2022.3216592>
- [11] Pei Zhang, Fangzhou He, Han Zhang, Jiankun Hu, Xiaohong Huang, Jilong Wang, Xia Yin, Huahong Zhu, and Yahui Li. 2023. Real-Time Malicious Traffic Detection With Online Isolation Forest Over SD-WAN. *Trans. Info. For. Sec.* 18 (Jan. 2023), 2076–2090. <https://doi.org/10.1109/TIFS.2023.3262121>