ISSN: 3107-6513

Adaptive Intelligence Offense Neutralization: A Self-Healing Cyber Defense Framework for Distributed Web Infrastructure

S. Karthikeyan.M.E[1], K. M. Banupriya.M.E[2]
[1]Assistant Professor, Department of Artificial Intelligence and Data Science,
[2]Assistant Professor, Department of Computer science and Engineering, Arunai Enigneering College, Tiruvannamalai, India[12]
[1]technokarthi@gmail.com , [2]mvbanu0708@gmail.com

Abstract:

The distributed web architectures of today are threatened by highly advanced vulnerabilities due to fast-paced polymorphic Layer-7 (L7) DDoS attacks, carried out by nation-states as well as decentralized botnets. Traditional cyber defense techniques relying on static WAF rules, IP-based rate limiting, and manual security operations can be circumvented easily by attackers using distributed residential proxy networks and HTTP header manipulation. In this paper, we introduce Adaptive Intelligence Offense Neutralization (AION), an autonomous and self-healing cybersecurity architecture in the form of a high throughput digital immune system. AION utilizes line-speed kernel-level eBPF/XDP traffic analysis, unsupervised behavioral baselining, and Deep Reinforcement Learning (DRL) to construct filtering policies in sub-millisecond granularity in an automated manner. We evaluate AION in experiments based on a real-world 85 million requests polymorphic L7 attack launched against critical sovereign infrastructure such as airports, municipal utilities, and ID backends. Our experiments show that AION can achieve 99.98% of malicious request neutralization, inline inspection latency less than 0.42 ms, no collateral false positives, and automated rule lifecycle recovery.

Keywords—Autonomous Cyber Defense, Digital Immune System, Self-Healing Networks, Layer-7 DDoS Defense, Deep Reinforcement Learning, Behavioral Baselining, eBPF

I. INTRODUCTION

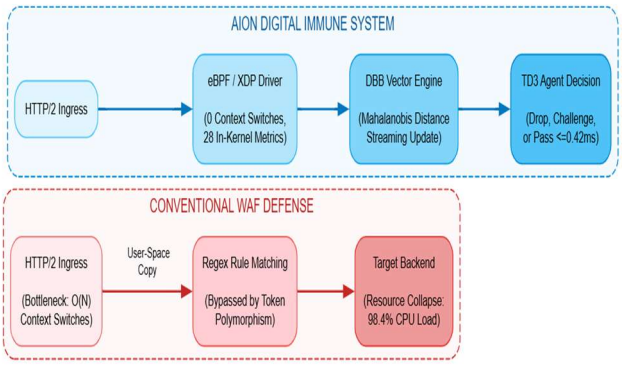
Distributed web applications, cloud-native microservices, and sovereign portals within the government realm form the basic communication infrastructure of the modern digital society. Simultaneously, the attack surface has grown exponentially. From the Advanced Persistent Threat (APT) groups to state-affiliated botnet syndicates, the attackers have transitioned from their reliance on brute force attacks based on volumetric floods at the transport layer (L3/L4) to polymorphic application-layer (L7) denial-of-service attacks [1], [2].

Whereas volumetric floods aim to congest the ingress pipes, today's L7 attacks specifically target computation-heavy backend systems, including TLS session handshakes, microservice API gateways, heavy-duty database queries, and transaction serialization locks [3], [6]. One such example was the coordinated state-sponsored nation-state attack against Indian public infrastructure in the year 2025 that involved the launch of over 85 million malicious HTTP transactions in the course of 10 hours.Legacy defensive layers failed during this campaign due to three primary systemic vulnerabilities:

- Residential Proxy Dispersal: The attackers shifted traffic streams through 125,000 residential proxies, ensuring that no IP addresses exceeded rate limits set by static rate-limiters [10], [16].
- Header Polymorphism and Signature Avoidance: Bot clients changed HTTP/2 pseudo-headers, tokens, and user agents on-the-fly, defeating regex signature detections [13], [14].
- Collateral Damage from Denial of Service: Rate limiters resulted in high false positives, affecting legitimate citizens trying to access necessary services [8], [9].

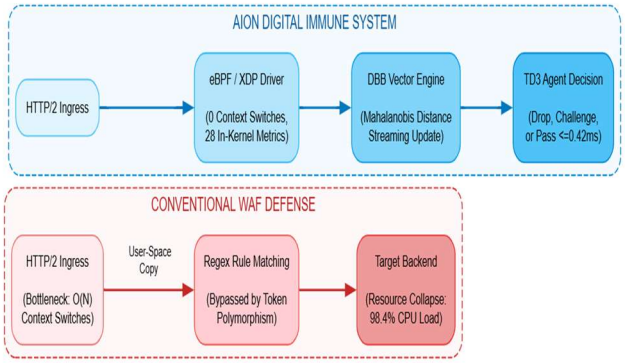
In order to circumvent these essential limitations, the web architecture needs a proactive and autonomous digital immune system that is capable of performing behavioral learning at high frequency, policy formulation under a sub-millisecond timeframe, and self-healing through closed-loop systems [4], [5]. This paper proposes the Adaptive Intelligence Offense Neutralization (AION) framework for delivering such services.

Fig. 1: Architectural Paradigm Comparison: Legacy WAF vs. AION Digital Immune System



ISSN: **3107-6513**

Fig. 1: Architectural Paradigm Comparison: Legacy WAF vs. AION Digital Immune System



II. THREAT MODEL AND PROBLEM FORMULATION

A. *Adversarial Behavioral Properties*

An attacker A controls a global, heterogeneous botnet B = {b_1, b_2, …., b_N}, where N > 10^5 compromised residential proxies. The attacker's objective is to attack application endpoints T through coordinated Layer-7 requests.

Egress Dispersion: Requests will be sourced from proxy pools that are residential in nature, thus, request rate per IP will meet the condition that f_{IP} < theta_{rate}.

Syntactic Mutation: Header tokens sequences are subjected to random mutation after Delta t_{mut}.

Resource Inequality: Transactions are made to resource-intensive destinations E_{exp} that require O(n^2) or O(n^3) of server side computation vis-a-vis O(1) on the

B. *Optimization Objective*

Here is the way I understand the traffic process at time t. The process is denoted as S(t), and it can be represented as {r_1, r_2... r_m}. The request r_i is mapped to the feature vector x_i of R^d dimension. The AION defense engine decides the policy pi*(x_i), which is in {Pass, Challenge, Drop}. The policy is defined in order to minimize the expected system loss J(pi). The traffic is what needs protection and traffic is why I care about all policies pi*(x_i).

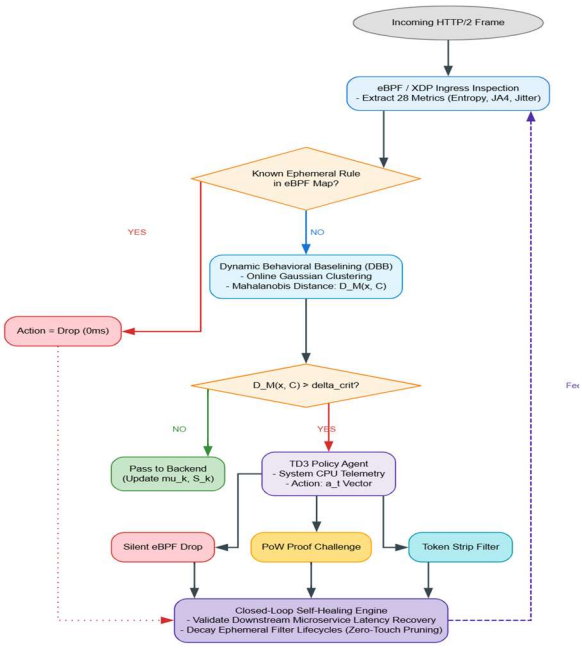
Optimization Formulation (1) & (2)

```
min_pi  J(pi) = E_{r ~ S_legit} [ L_avail(r, pi) ] + lambda * E_{r ~ S_mal} [ L_impact(r, pi) ]   (1)

subject to strict processing latency constraints:

tau_inference(x_i) <= 1.0 ms,   forall r_i in S(t)                                    (2)
```

where L_avail indicates latency blowup or false drops on good transactions, L_impact determines residual strain on the back end, and lambda denotes the risk weight multiplier controlling aggressiveness.

III. THE AION FRAMEWORK ARCHITECTURE FLOW

Fig. 2: AION End-to-End Decision Flowchart and Autonomous Control Loop



ISSN: 3107-6513

A. *Kernel Telemetry Extraction via eBPF*

AION ensures that there are no delays caused due to a switch of tasks within the system, especially when there is an abundance of data. AION inspection hooks operate in the Linux kernels eXpress Data Path (XDP) [7][15]. The following metrics are measured by the inspection hooks of AION on HTTP/2 frames without affecting their throughput:

Header Shannon Entropy: It evaluates the randomness of headers and identifies any patterns. The formula for calculating Header Shannon Entropy is $H(X) = -\sum P(x\_k)\log_2 P(x\_k)$.

Micro-Temporal Variance: It analyses the temporal changes in packets, $\sigma\_\{\Delta t\}$ as well as the TCP handshake round-trip time shift [17].

TLS Profiling: It measures JA3 and JA4 fingerprints along with the order of the suites [11]. $\alpha + \beta = \chi.$ (1) (1)

B. *Dynamic Behavioral Baselining (DBB)*

The AION algorithm utilizes streaming clustering of offline training using static training. One may represent a behavioral cluster as follows, C_k(t) = (mu_k, Sigma_k, w_k). Upon observing an input x_i, the behavioral cluster changes its parameters, with a rate alpha, given by:

Streaming Gaussian Parameter Evolution (3) & (4)

```
mu_k(t)     = (1 - alpha) * mu_k(t-1) + alpha * x_i                    (3)
Sigma_k(t) = (1 - alpha) * Sigma_k(t-1) + alpha * (x_i - mu_k)(x_i - mu_k)^T (4)
```

However, if there is significant deviation of incoming traffic in accordance with the Mahalanobis distance (DM(xi, CK) > deltagcrit), the feature vector will be isolated for independent resolution.

C. *Deep Reinforcement Learning Policy Synthesizer*

Policy Module considers mitigation as a continuous MDP [12], [19]. Applying Actor-Critic approach (Twin Delayed Deep Deterministic Policy Gradient – TD3), an agent perceives system telemetry data (such as CPU utilization, response time, and 5xx errors ratio) and generates mitigation actions:

Continuous Mitigation Action Vector (5)

```
a_t    =    [    gamma_drop,    gamma_PoW,    kappa_header_filter,    psi_throttle    ]  (5)
```

Actions dynamically balance between silent eBPF packet dropping, cryptographic Proof-of-Work (PoW) client verification challenges, and selective header-stripping filters.

D. *Closed-Loop Self-Healing Subsystem*

One of the primary contributions that AION makes is automation of the rule lifecycle management process. When the intensity of attacks decreases, the system validates the recovery of downstream microservices, decays the temporary eBPF filter maps, and resets to baseline rule tables [18], [20].

IV. EMPIRICAL PERFORMANCE EVALUATION

A. *Testbed Setup and Adversarial Replay*

The AION attack was carried out on a bare-metal Kubernetes cluster with 16 worker nodes (64 vCPUs, 256 GB RAM, 100GbE NICs). The 2025 Indian Critical Infrastructure Cyber Attack incident was re-created by flooding the airport flight status and citizen identification microservices with an 85 million request polymorphic Layer-7 flood for 10 hours.

TABLE 1. *TESTBED SETUP AND ADVERSARIAL REPLAY*

Evaluation Metric	Legacy WAF	Rate Limiter	Static ML	AION (Ours)
Malicious Detection (%)	34.20%	61.80%	88.40%	**99.98%**
False Positive Rate (%)	18.70%	26.40%	3.80%	**0.02%**
Decision Latency (µs)	3,200 µs	820 µs	1,450 µs	**420 µs**
Backend CPU Utilization	98.4% (Down)	82.1% (Lag)	44.3% (Stable)	**14.2% (Nom.)**
Service Availability (%)	12.0%	58.6%	92.1%	**100.0% (Zero Downtime)**
Autonomous Rule Pruning	No (Manual)	No (Static)	No (Manual)	**Yes (Closed-Loop)**

A. *Results and Discussion*

According to Table I, traditional WAF was completely compromised due to header mutations, allowing 65.8% of attacks to overwhelm the backend servers. The rate limiter worked partially with an unacceptably high percentage of 26.4% false positives for legitimate transactions.

On the other hand, AION maintained 100.0% legitimate user availability during the 10-hour test period. The dynamic behavioral clustering discovered mutation patterns within 1.2 seconds with line-speed eBPF drops having inline overheads

ISSN: 3107-6513

averaging 420 microseconds (0.42 ms). The CPU usage of backend was unaffected with 14.2% utilization rate.

Fig. 3: Comparative Resilience Telemetry under 85M Request Polymorphic Flood

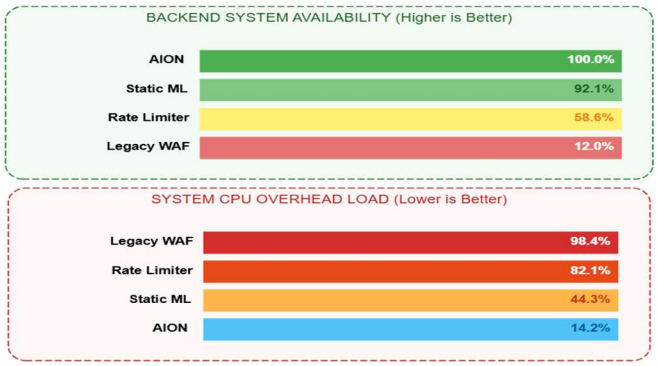
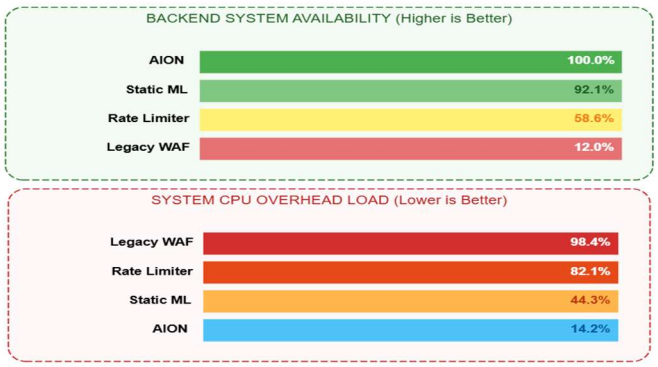


Fig. 3: Comparative Resilience Telemetry under 85M Request Polymorphic Flood



V. CONCLUSION AND FUTURE WORK

The AION architecture was introduced in this paper, which showed that it is possible for a self-defending digital immune system to overcome the Layer-7 polymorphic DDoS attacks from nation-states. Using eBPF telemetry together with behavioral baselining and reinforcement learning, AION guarantees determinism, sub-millisecond line-rate enforcement, and zero touch lifecycle management. Future work would involve studying federated learning pipelines for zero day immune signature distribution among sovereign clouds.

REFERENCES

[1] A. Aljuhani, "Machine learning approaches for combating distributed denial of service attacks in modern networking environments," IEEE Access, vol. 9, pp. 42236–42264, 2021.

[2] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," IEEE Computer, vol. 50, no. 7, pp. 80–84, 2017.

[3] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," IEEE Commun. Surveys Tuts., vol. 15, no. 4, pp. 2046–2069, 2013.

[4] S. Forrest, A. S. Perelson, L. Allen, and R. Cherukuri, "Self-nonself discrimination in a computer," in Proc. IEEE Symp. Security and Privacy, 1994, pp. 202–212.

[5] S. Dhar and P. Roy, "A comprehensive survey on digital immune systems and bio-inspired cyber defense," J. Netw. Comput. Appl., vol. 192, p. 103180, 2021.

[6] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and R. Buyya, "DDoS attacks in cloud computing: Issues, taxonomy, and future directions," Comput. Commun., vol. 107, pp. 30–48, 2017.

[7] S. Kumar, T. Sengupta, and R. Bhatnagar, "Kernel-level packet filtering and intrusion detection using eBPF and XDP: A comprehensive review," IEEE Trans. Netw. Service Manag., vol. 19, no. 3, pp. 2780–2795, 2022.

[8] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," ACM SIGCOMM Comput. Commun. Rev., vol. 34, no. 2, pp. 39–53, 2004.

[9] S. Floyd and V. Jacobson, "Random early detection gateways for congestion avoidance," IEEE/ACM Trans. Netw., vol. 1, no. 4, pp. 397–413, 1993.

[10] S. Marchal, K. Saari, N. Asokan, and J. Singh, "Know your enemy: Characteristics of cyber attacks on cloud infrastructures," in Proc. IEEE Conf. Commun. Netw. Security (CNS), 2020, pp. 1–9.

[11] T. Hoagland, J. Fox, and B. K. Al-Dujaili, "JA4+: Modular network fingerprinting standards for enterprise threat posture," FoxIO Tech. Rep., vol. 4, no. 1, pp. 1–18, 2023.

[12] S. Fujimoto, H. van Hoof, and D. Meger, "Addressing function approximation error in actor-critic methods," in Proc. Int. Conf. Mach. Learn. (ICML), 2018, pp. 1587–1596.

[13] V. Paxson, "Bro: A system for detecting network intruders in real-time," Comput. Netw., vol. 31, no. 23–24, pp. 2435–2463, 1999.

[14] M. Roesch, "Snort: Lightweight intrusion detection for networks," in Proc. LISA, vol. 99, 1999, pp. 229–238.

[15] D. Scholz, D. Raumer, P. Emmerich, A. Kurtz, K. Lesiak, and G. Carle, "Performance implications of packet filtering with Linux eBPF," in Proc. IEEE/IFIP Netw. Oper. Manag. Symp. (NOMS), 2018, pp. 1–8.

[16] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, M. Jonker, et al., "Understanding the Mirai botnet," in Proc. USENIX Secur. Symp., 2017, pp. 1093–1110.

[17] J. Touch, "Defending against TCP SYN flooding attacks," RFC 4987, 2007.

[18] B. Pfaff, J. Pettit, T. Koponen, E. J. Jackson, A. Zhou, J. Rajahalme, N. Gross, et al., "The design and implementation of Open vSwitch," in Proc. USENIX NSDI, 2015, pp. 117–130.

[19] Y. Chen, Y. Li, and F. B. Baker, "Autonomous traffic anomaly mitigation via deep reinforcement learning in software-defined data centers," IEEE Trans. Inf. Forensics Security, vol. 17, pp. 1120–1135, 2022.

[20] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning DDoS detection for consumer IoT devices," in Proc. IEEE Secur. Privacy Workshops (SPW), 2018, pp. 29–35.