Intelligent Prevention of DDoS Attacks using Reinforcement Learning and Smart Contracts

Emily Struble and **Maikel Leon Espinosa** and **Erotokritos Skordilis**
Miami Herbert Business School
5250 University Dr, Coral Gables, FL 33146

Abstract

(Distributed) Denial-of-Service (DoS/DDoS) attacks are among the most dangerous cybersecurity threats to computer networks. Lately, blockchain and artificial intelligence (AI) cyberdefense applications have successfully been implemented to identify attack patterns. This paper proposes a novel collaborative, blockchain-based multi-agent reinforcement learning (RL) cyberdefense method using smart contracts. Initial numerical experiments have shown that the agents quickly learn to predict attacks, which can lead to mitigating network-wide service disruptions.

Introduction

According to (Das and Mao 2020), the number of IoT devices installed worldwide will surge to approximately 75 billion by 2025 and 160 billion by 2030. Strong security measures are essential to ensure uninterrupted operations with this growing interconnectivity. Although permissions, sureties, and firewalls play a significant role in network protection, attacks can easily overload connected devices and disrupt everyday operations. Due to their severity, predicting such attacks is essential to the normal operations of sensitive residential, industrial, and military assets.

Literature Review

Applications of RL in DDoS prevention have appeared in the literature recently. The authors in (Javadpour et al. 2023) developed a Slice Isolation-based Reinforcement Learning (SIRL) model that allowed for a compromised slice in a 5G network to be isolated from the other slices, leading to harm mitigation. In (He et al. 2024), the authors proposed an RL-based transferable network intrusion system to detect network traffic outliers. Smart contracts have also been successfully applied to DDoS prevention studies. (Yakubu et al. 2023) focused on DDoS attack prevention by utilizing innovative contracts over the Ethereum blockchain network to create an authentication system. This was combined with a single server queuing system that managed to service requests and mitigate attacks.

Apart from stand-alone methods, recent works in the literature combine blockchain applications and machine learning for cyberdefense. In (Jawahar et al. 2024), the authors initially used an artificial neural network to develop a DDoS attack detection algorithm among network traffic. Then, smart contracts were used to store the verified malicious IP addresses, which were subsequently blocked from future access. In another paper, the authors focused on protecting IoT environments by utilizing AI and smart contracts (Shah et al. 2023). The proposed method used random forests and recurrent neural networks to detect malicious users using a binary classification problem. Then, they utilized smart contracts to authenticate benign data and prevent exploitation by malicious actors. The authors in (Gadallah, Ibrahim, and Omar 2024) developed a model to detect attacks based on network traffic. This led to an increase in the network's trust value and blocked any suspicious activity based on that.

This paper presents a new approach to preventing DDoS attacks that combines the advantages of smart contracts and RL. While previous works have utilized blockchain applications, AI, or combinations of both, none have specifically combined smart contracts with collaborative multi-agent reinforcement learning. By doing so, we propose an innovative solution that has the potential to help protect the nation's largest and most vulnerable networks from malicious attacks.

Methodologies

Blockchain: A blockchain network is an immutable, distributed, public ledger that records transactions. One example of these peer-to-peer systems is the Ethereum blockchain. Ethereum can be used to deploy smart contracts and important blockchain applications. These smart contracts are programs on a blockchain that automatically execute based on certain conditions. They are written in Solidity, an object-oriented, high-level programming language designed to write smart contracts on the Ethereum blockchain.

Reinforcement Learning: A branch of machine learning, RL utilizes agents that, through continuous interaction with their environment, learn policies aiming to maximize an expected cumulative discounted reward or, equivalently, an ex-

pected return G_t (1).

$$G_t = \sum_{k=0}^{\infty} \gamma^k R_{t+k+1}, \tag{1}$$

where R_{t+k+1} is the reward received at time step $t+k+1$, and γ is the discount factor, with $0 \leq \gamma < 1$. The policy maps environment states to actions. Real-world systems' state spaces are vast, so modern RL algorithms adhere to parameterized policies via function approximators such as deep neural networks (Mnih et al. 2013). RL algorithms can generally be classified into value-function, policy gradient, and actor-critic categories. The proposed framework uses Proximal Policy Optimization (PPO), an actor-critic method that is highly effective for optimizing extensive, non-linear policies (Schulman et al. 2017).

Proposed Approach: We utilize a multi-agent RL method where each agent represents a node in a collaborative computer network. During agent training, each agent scans the incoming network traffic to their respective computing node at regular intervals, and all agents collaboratively learn to optimize the shared policy using the reward given in (2), which raises the alarm when an agent considers an attack imminent in the next time interval:

$$z = \begin{cases} -100 & \text{if attack \& no alarm} \\ 0 & \text{if no attack \& no alarm} \\ -1 & \text{if no attack \& alarm} \\ 10 & \text{if attack \& alarm} \end{cases} \tag{2}$$

The procedure punishes agents that do not raise an alarm while an attack happens and less severely when they raise an alarm while no attack happens. No cost occurs when nothing happens, while a positive reward is given when the agents raise the alarm when the attack is about to happen. Agent training occurs over a blockchain network, and network traffic is logged using a smart contract. The proposed framework is displayed in Fig. 1.

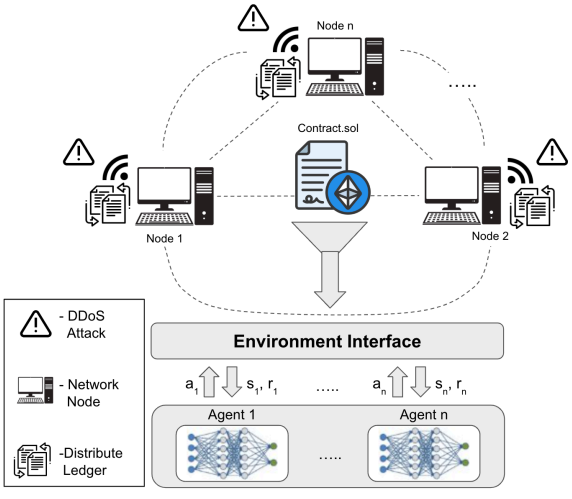

Figure 1: Proposed framework.

Preliminary Results

We utilized a synthetic DDoS attack dataset provided in (Hekmati, Grippo, and Krishnamachari 2021) for agent training. The authors used traffic data from a real-world IoT network and injected it with simulated attacks with duration intervals from 1 minute to 24 hours. In our empirical study, we used 8-hour-long attacks. Figure 2 shows how the reward increases during agent training, demonstrating that the agents quickly learn the optimal policy and anticipate DDoS attacks on the network. We show the mean reward as well as its confidence intervals. Furthermore, the loss reduction shown in Figure 3 demonstrates that the policy network learns to adequately map environment states to actions.

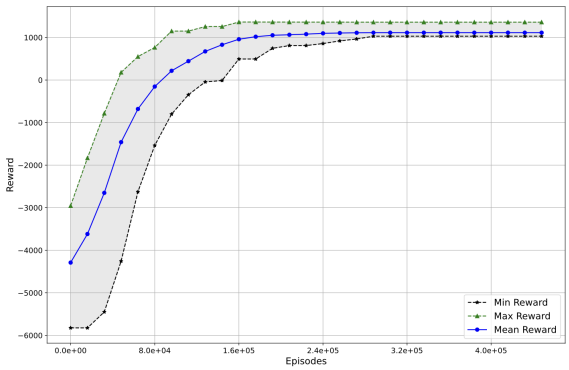

Figure 2: Cumulative reward evolution during training.

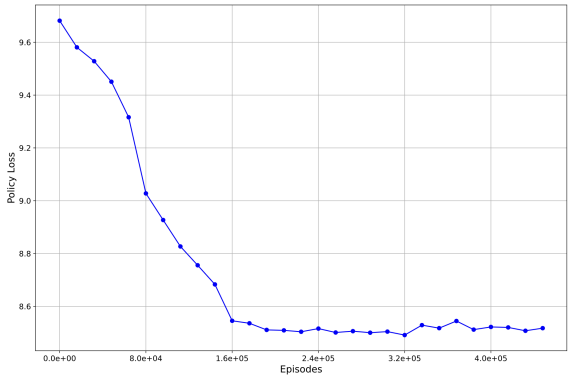

Figure 3: Policy loss.

Conclusions and Future Work

We proposed a first-of-its-kind DDoS attack prediction method utilizing smart contracts and multi-agent reinforcement learning. The technique offers a unique, viable solution to one of the most challenging contemporary cyber-attack problems. In future work, we aim to train the agents to capture DDoS attacks of different time durations. We also plan to evaluate the trained policy in new, unseen data.

References

Das, S., and Mao, E. 2020. The global energy footprint of information and communication technology electronics in connected internet-of-things devices. *Sustainable Energy, Grids and Networks* 24:100408.

Gadallah, W. G.; Ibrahim, H. M.; and Omar, N. M. 2024. A deep learning technique to detect distributed denial of service attacks in software-defined networks. *Computers & Security* 137:103588.

He, M.; Wang, X.; Wei, P.; Yang, L.; Teng, Y.; and Lyu, R. 2024. Reinforcement learning meets network intrusion detection: A transferable and adaptable framework for anomaly behavior identification. *IEEE Transactions on Network and Service Management*.

Hekmati, A.; Grippo, E.; and Krishnamachari, B. 2021. Dataset: Large-scale urban iot activity data for ddos attack emulation. *arXiv preprint arXiv:2110.01842*.

Javadpour, A.; Ja'fari, F.; Taleb, T.; and Benzaïd, C. 2023. Reinforcement learning-based slice isolation against ddos attacks in beyond 5g networks. *IEEE Transactions on Network and Service Management*.

Jawahar, A.; Kaythry, P.; Kumar, V. C.; Vinu, R.; Amrish, R.; Bavapriyan, K.; and Gopinaath, V. 2024. Ddos mitigation using blockchain and machine learning techniques. *MULTIMEDIA TOOLS AND APPLICATIONS*.

Mnih, V.; Kavukcuoglu, K.; Silver, D.; Graves, A.; Antonoglou, I.; Wierstra, D.; and Riedmiller, M. 2013. Playing atari with deep reinforcement learning. *arXiv preprint arXiv:1312.5602*.

Schulman, J.; Wolski, F.; Dhariwal, P.; Radford, A.; and Klimov, O. 2017. Proximal policy optimization algorithms. *arXiv preprint arXiv:1707.06347*.

Shah, H.; Shah, D.; Jadav, N. K.; Gupta, R.; Tanwar, S.; Alfarraj, O.; Tolba, A.; Raboaca, M. S.; and Marina, V. 2023. Deep learning-based malicious smart contract and intrusion detection system for iot environment. *Mathematics* 11(2):418.

Yakubu, B. M.; Khan, M. I.; Khan, A.; Jabeen, F.; and Jeon, G. 2023. Blockchain-based ddos attack mitigation protocol for device-to-device interaction in smart home. *Digital Communications and Networks* 9(2):383–392.