RADemics

Multi-Agent AI Systems for Coordinated Threat Response Using Deep Q-Networks (DQN) and Swarm Intelligence

Shantha Visalakshi Upendran, M R Mohanraj, Shiny Malar F. R.
ETHIRAJ COLLEGE FOR WOMEN (AUTONOMOUS,
JKKN COLLEGE OF ENGINEERING AND TECHNOLOGY,
STELLA MARY'S COLLEGE OF ENGINEERING

Multi-Agent AI Systems for Coordinated Threat Response Using Deep Q-Networks (DQN) and Swarm Intelligence

[1]Shantha Visalakshi Upendran, Associate Professor, MCA, Ethiraj College for Women (Autonomous), Chennai, profdrusv@gmail.com

[2]M R Mohanraj, Associate Professor, Electrical and Electronics Engineering, J K K N College of Engineering and Technology, Komarapalayam, Namakkal Dist -638183, mohanraj.mr86@gmail.com

[3]Shiny Malar F. R. (Francis Rosy), Professor & Head, CSE, Stella Mary's College of Engineering, Aruthenganvilai, Azhikkal. Pin 629202. headcse@stellamaryscoe.edu.in

Abstract

The increasing sophistication of cyber threats has made traditional defense mechanisms insufficient for addressing complex, large-scale attacks. Multi-Agent AI systems, particularly those utilizing Deep Q-Networks (DQN) and Swarm Intelligence (SI), have emerged as promising solutions for coordinated threat response in dynamic and distributed environments. These systems allow multiple agents to autonomously detect, assess, and mitigate threats through decentralized decision-making, enhancing scalability and efficiency in cybersecurity. However, ensuring the robustness and adversarial resilience of these systems remains a critical challenge. This chapter explores the integration of reinforcement learning and bio-inspired algorithms to develop a resilient multi-agent defense framework capable of adapting to both known and unknown cyber threats. The study examines the potential of DQN for adaptive learning in cyber defense, the role of SI in facilitating cooperative agent behavior, and strategies for improving system resilience against adversarial manipulations. Performance evaluations demonstrate the effectiveness of the proposed approach in real-world threat scenarios, offering a new paradigm for autonomous and scalable cyber defense systems. The chapter provides insights into optimizing multi-agent AI systems for proactive, robust, and efficient cybersecurity in large-scale networks.

Keywords: Multi-Agent Systems, Deep Q-Networks (DQN), Swarm Intelligence, Cybersecurity, Adversarial Resilience, Reinforcement Learning.

Introduction

The landscape of cybersecurity has shifted dramatically with the growing sophistication and frequency of cyber-attacks. Traditional defense mechanisms, such as signature-based detection and static rule-based systems, have become increasingly inadequate in the face of advanced and dynamic threats, such as Advanced Persistent Threats (APTs) and zero-day exploits. These attacks, which evolve rapidly and often involve multiple coordinated stages, require security systems that can not only detect but also anticipate and respond to threats in real time. As cyber environments become more complex and distributed, leveraging autonomous decision-making through multi-agent AI systems becomes a viable solution to counteract these challenges. By utilizing multiple

agents that can collaborate and learn, these systems offer a new paradigm for addressing security vulnerabilities at scale.

In particular, the combination of Deep Q-Networks (DQN) and Swarm Intelligence (SI) has shown promise in enhancing the effectiveness of multi-agent cybersecurity systems. DQN, a deep reinforcement learning algorithm, enables agents to learn optimal strategies through a process of trial-and-error interactions with the environment. This learning technique allows agents to continuously adapt to changing threat patterns, without relying on predefined rules or signatures. However, the challenge remains that in a multi-agent setting, DQN-based models often face issues such as non-stationarity, where the environment is constantly changing due to the actions of multiple agents. This makes it difficult for individual agents to optimize their strategies independently, resulting in suboptimal performance.

Swarm Intelligence, which draws inspiration from natural systems like ant colonies and bird flocks, offers a solution to the coordination challenges in multi-agent systems. Swarm-based algorithms allow agents to self-organize, share information, and adjust their behavior dynamically, without requiring a central controller. This decentralized coordination enables agents to adapt quickly to emerging threats and collaborate effectively to respond to complex attack scenarios. By integrating DQN with SI, multi-agent systems can combine the strengths of adaptive learning and decentralized coordination, offering enhanced scalability and resilience in cybersecurity applications. This hybrid approach not only helps in responding to known threats but also in predicting and neutralizing novel, previously unseen attack strategies.

One of the critical aspects of any AI-driven cybersecurity system is its ability to withstand adversarial attacks aimed at manipulating or bypassing the defense mechanisms. In multi-agent systems, adversarial threats can take many forms, including data poisoning, where attackers deliberately inject misleading information into the system, and reward manipulation, where attackers attempt to mislead the reinforcement learning process by exploiting vulnerabilities in the reward structure. For multi-agent DQN systems to be truly effective, they must be resilient to such adversarial interference. This requires the development of strategies that enhance the robustness of the learning algorithms, enabling agents to continue functioning effectively even under malicious conditions. One promising approach is adversarial training, which involves training the agents to recognize and respond to adversarial inputs, making them more resistant to manipulation.