School of Computer Science & Mathematics
Marist University

Summer Research Fellowship Project Proposal

Goal-Oriented Response Planning (GORP): Adaptive cyber-defense inspired by video game AI

Cayleigh Goberman
Honors student

Matthew A. Johnson
Faculty sponsor

Melissa Chodziutko
Faculty co-sponsor

April 25, 2025

1 Abstract

There exist various prevention and mitigation tactics for defending a host system from cyber threats. Implementing a comprehensive cyber-defense strategy involves a carefully chosen subset of these, and a responsive strategy may need to change tactics over time as the threat profile changes. In many video games, it is similarly desirable for computer-controlled non-player characters (NPCs) to behave in interesting ways that change in response to the player's actions or even to the actions of other NPCs. Goal-Oriented Action Planning (GOAP) is a classical AI technique developed for use in video games. GOAP enables the creation of complex, emergent behavior for NPCs in video games. We propose a new design for an adaptive cyber-defense software agent based on a modified version of the GOAP algorithm, which we call GORP (Goal-Oriented Response Planning). We then provide a reference implementation of our design and examine the results of deploying and testing the agent in a simulated threat environment.

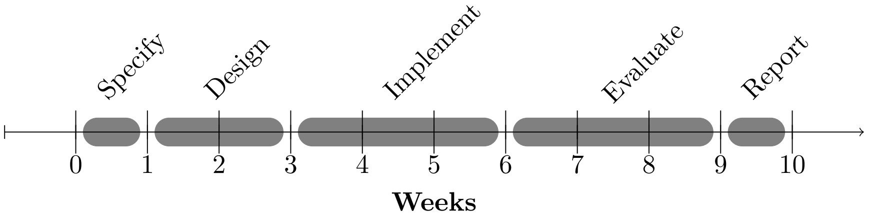
Keywords: GOAP, planning systems, video game AI, emergent behavior, cybersecurity, threat mitigation, intrusion detection, cyber-defense

2 External affiliations

This research is not associated with any outside agency.

3 Proposed timeline

We plan to conduct our research over a 10-week period in five distinct phases.



3.1 Formal problem specification (1 week)

Initially, we will define precise security goals (e.g., ”prevent unauthorized access to resource X”), determine specific actions that can be automated in pursuit of those goals, and identify real-time data sources that can serve to measure ”distance” from our defined goals. We will also outline resource and configuration requirements for a sandbox test environment.

3.2 Agent design & architecture (2 weeks)

Next, we will design the software architecture for an adaptive security agent capable of executing any of the previously-identified defensive actions. The foundation of our design will be the GOAP algorithm, with modifications as needed to tailor the agent to our target domain of defensive cybersecurity operations.

3.3 Reference implementation (3 weeks)

We will then develop a proof-of-concept implementation of our agent design using an appropriate coding language (e.g., C++ or Java). We will conduct preliminary unit and integration testing to validate the desired operational capabilities on an appropriate host system.

3.4 Deployment & evaluation (3 weeks)

In order to assess the feasibility of our approach, we will prepare a simulated threat environment in which to deploy our proof-of-concept agent. Within this sandbox environment, we will examine the behavior of our agent in the presence of simulated attacks and collect data regarding the performance of the agent relative to its prescribed goals.

3.5 Final report (1 week)

Finally, we will assemble a comprehensive report that details each phase of the project and summarizes our test results and conclusions.

4 Personal impact

My ultimate goal for my career is to become a programmer in the video game industry. As such, I will need to have an in-depth understanding of NPC qualities and behavior. This research project will give me an opportunity to develop a program with a unique spin on NPC artificial intelligence. While the project details a type of NPC AI that will be utilized for cybersecurity rather than video games, it will still employ techniques that are universally shared across NPC categorizations, such as goal-oriented action planning.

Additionally, this project will allow me to gain insight into the cybersecurity side of computer science. My main academic focuses are in general computer science and video game programming; as such, it would be incredibly valuable to have insight into another aspect of programming that could intersect with my career goals in the future. Cybersecurity is extremely important in the modern day; as such, it will be beneficial to have an understanding of how cybersecurity functions.

While this project would be undoubtedly useful in preparing for my career after college, I still have a few more years before I leave Marist. I am currently a junior enrolled in the Computer Science five-year Master's program with a concentration in artificial intelligence. As such, the project would be incredibly useful in furthering my understanding of artificial intelligence as I prepare to begin my graduate courses in the fall. It would be refreshing to have a launching point like this for these difficult classes. If the project goes well, I might even attempt to improve upon it through my Honors Thesis. The ten-to-twelve-week period allocated for this project provides an excellent starting point, but there will always be room for improvement, especially with a project as complex as this.