Artificial Intelligence Course Project Assignment

This document presents an in-depth exploration of search and optimization algorithms applied within multiple computer science problem domains. It covers password guessing, secure pathfinding in network graphs, and firewall rule optimization using classical and evolutionary algorithms. Execution time measurements are included to assess algorithm efficiency. The structure follows a clear thematic progression from fundamental search concepts to applied network security optimization. Each section introduces problem context, algorithmic approaches, and outcomes, aiming to provide comprehensive insights suitable for computer science students and cybersecurity enthusiasts.

Password Guessing using Search Algorithms

This module examines various algorithms to guess a target password "Sal" through search and heuristic optimization strategies. The Genetic Algorithm (GA) evolves populations of guesses by applying a fitness function counting correctly matched characters and using mutation to explore variations. A* Search constructs guesses character-by-character, prioritizing paths with fewer mismatched characters according to a heuristic. Uniform Cost Search (UCS), Breadth-First Search (BFS), and Depth-First Search (DFS) explore guesses systematically, differing in exploration order and depth prioritization.

The comparative study highlights how heuristic-driven methods like GA and A* can outperform uninformed searches (BFS, DFS) in small-scale problems by efficiently guiding the search toward the solution. The mutation rate in GA introduces diversity to avoid premature convergence. This exercise provides a practical understanding of search techniques fundamental to AI and cybersecurity tasks involving combinatorial search spaces.

Secure Pathfinding in Network Graph

This section addresses the challenge of identifying the most secure and efficient path in a network graph with edges weighted by both distance and security level. The graph includes nodes A through D with bi-dimensional edge attributes. Algorithms implemented include Genetic Algorithm (GA), which evolves path candidates optimizing security aggregation, and A* Search, which balances physical distance and inverted security in its cost function.

Uniform Cost Search (UCS) prioritizes minimal distance ignoring security, while BFS and DFS explore all possible paths without heuristic guidance. Valid path checks ensure only existing edges are traversed. This comparative approach underscores the importance of multi-criteria optimization in cybersecurity network routing, demonstrating how advanced search methods can reconcile conflicting objectives like efficiency and security.

Firewall Rule Optimization

This component focuses on optimizing firewall rule sets to eliminate conflicts and minimize the number of rules. Each firewall rule is represented as a tuple specifying an action (e.g., ALLOW), a source IP pattern, and a port number. The objective is to produce a conflict-free, minimal rule set that ensures consistent security policies.

Algorithms employed include a Genetic Algorithm using a fitness function inversely proportional to the sum of conflicts and rule set size. Mutation operations randomly add or remove rules to explore diverse configurations. A* Search and Uniform Cost Search attempt to build rule sets incrementally while avoiding conflicts. BFS and DFS exhaustively traverse the search space. This study models practical network firewall management scenarios, illustrating how AI can automate and optimize complex policy configurations in cybersecurity infrastructures.

Malware Behavior Analysis

This section analyzes suspicious or malicious software behavior to detect threats by observing command patterns, system interactions, and resource access.

- Behavioral analysis combines dynamic monitoring and static code inspection to identify malicious activity patterns.
- Genetic Algorithms evolve behavioral features for classification.
- Search methods (A*, BFS, DFS, UCS) explore event sequences weighted by threat levels.

This approach enables detection of novel malware variants and supports adaptive, intelligent analysis tools essential for evolving cybersecurity challenges.

Network Intrusion Detection

This part focuses on identifying unauthorized or malicious network activity by analyzing traffic patterns and anomaly detection.

- Uses machine learning and heuristic search techniques to detect intrusions in real-time.
- Employs algorithms to scan network packets, model normal behavior, and flag deviations.
- Combines evolutionary algorithms and traditional searches to enhance detection accuracy and reduce false positives.

Effective intrusion detection is critical for maintaining network integrity and preventing cyber-attacks in dynamic environments.

Performance Measurement

Each project module incorporates execution time tracking to evaluate algorithm efficiency under controlled conditions. Timed measurements facilitate quantitative performance comparisons across diverse algorithms and problem domains, such as password guessing, pathfinding, firewall optimization, malware analysis, and intrusion detection.

These metrics provide insights into computational cost relative to accuracy, convergence speed, and heuristic effectiveness. Performance benchmarking is critical in assessing algorithm suitability for real-world applications where rapid and reliable solutions are necessary, particularly in cybersecurity contexts where time-sensitive decisions impact system safety and responsiveness.

Additional Formats and Deliverables

This final section offers support for delivering the project assignment in alternative formats like PDF, formatted Word documents, or LaTeX reports. Customization options include integrating detailed figures, tables, and algorithmic comparisons to enhance clarity and presentation quality.

Such professionally formatted documents cater to academic or professional requirements, facilitating easier dissemination and review. Please advise if you would like to obtain these enhanced report files or any specific visual additions tailored to your presentation or publication needs.