Trusted AI Challenge
Phase II: Architectures and Approach

SERC Trusted Artificial Intelligence Systems Engineering Challenge,
Fall 2024

Dec 11, 2024

Athul C. Dharmarajan, Vikranth Gadi, Zichong Yang, Bradley Feng, Jitesh H. Panchal

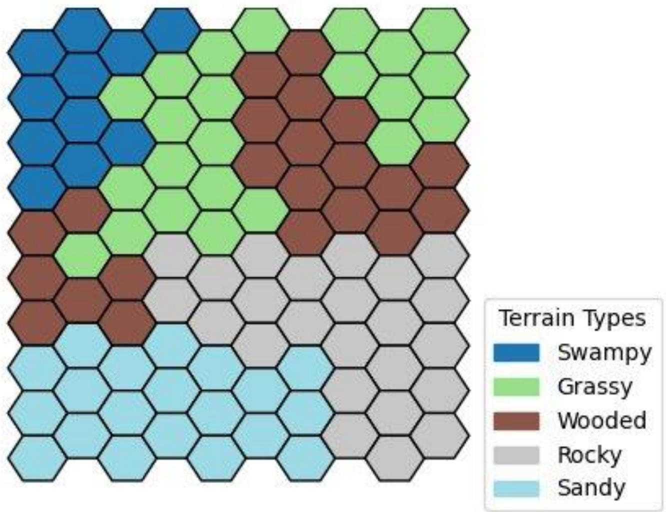
School of Mechanical Engineering, Purdue University

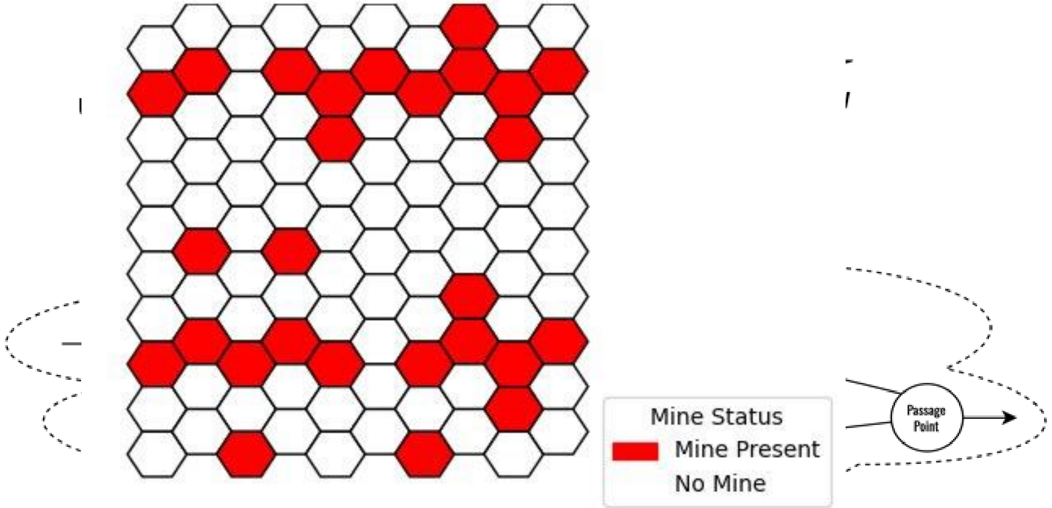
Design Engineering Laboratory @ Purdue
http://engineering.purdue.edu/DELP

Problem Statement

Objectives:

- Ensure safe passage from start node to terminus node along a defined network
- Develop the notion of trust between Artificial intelligence (AI) models and human operators
- Develop architectures to use human operators in conjunction with AI
- Identify the roles humans and AI should play in different architectures
- Compare different architectures across measures of performance





Characterizing Architectures

- We describe the architecture as the decision-making architecture for the task of navigating the network
- Each architecture is characterized by the flow of information and control instructions between the different stakeholders – who makes what decision? In which sequence?
- Communication between agents are of two types: information or control input

Images Captured

Updated Route

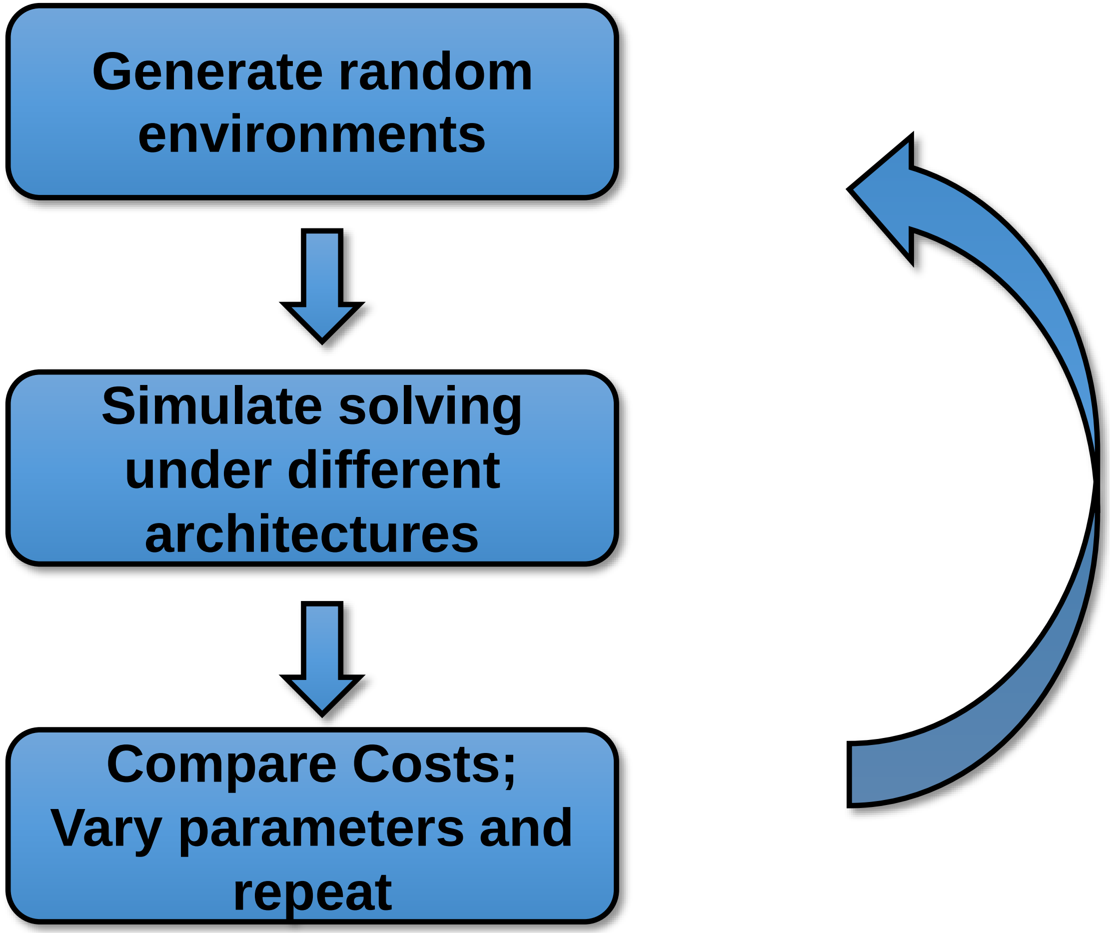
AI Confidence

Actual Terrain Info

Overall method

<u>Architectures</u>
A1: Centralized, Human
A2: Centralized, AI
A3: Centralized, Human-AI Teaming

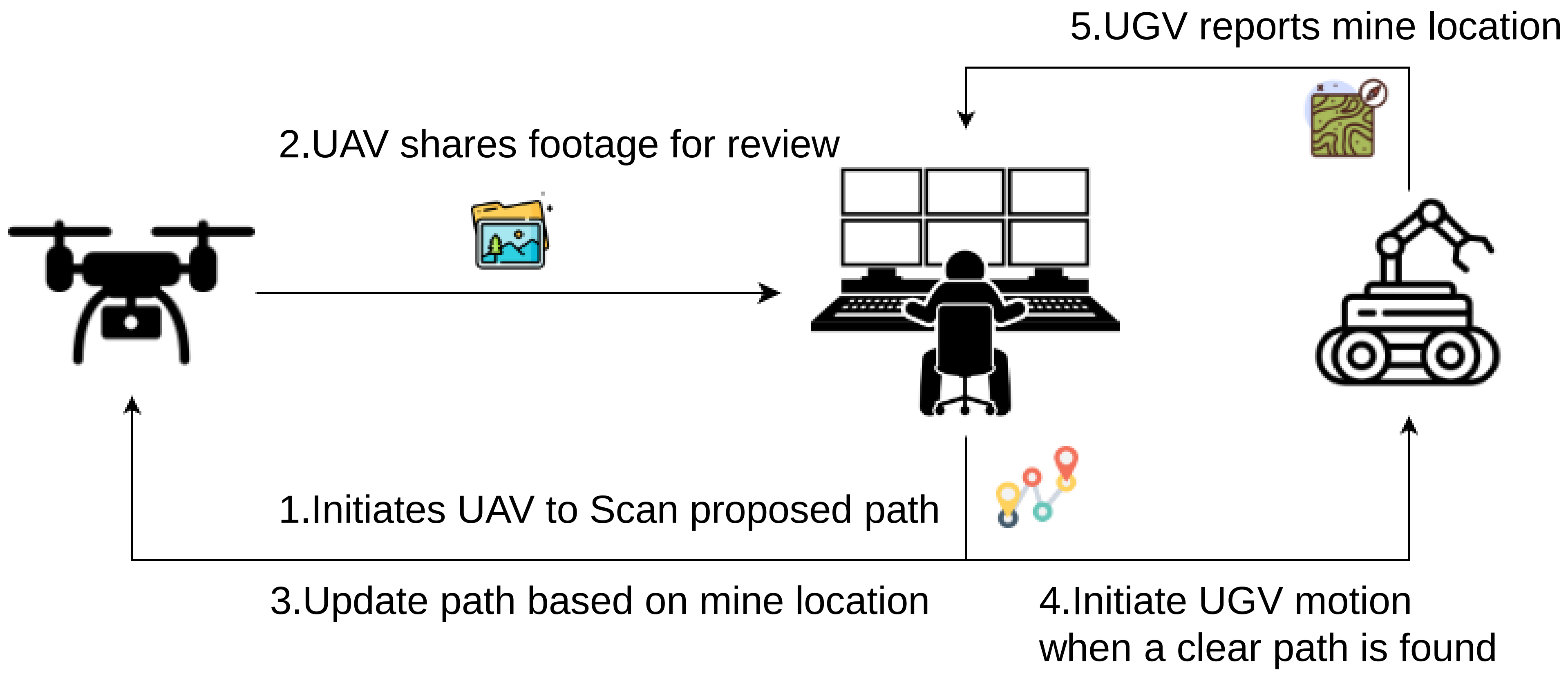
Architectures characterize the decision-
making
involved in navigating the terrain



How do we simulate and compare architectures?

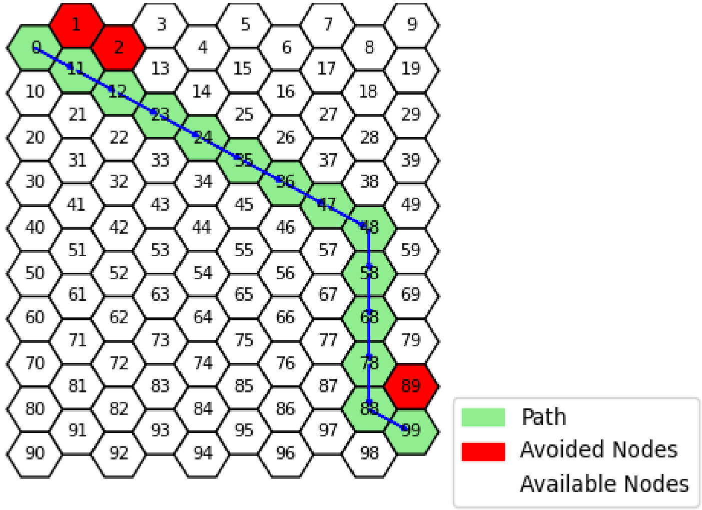
- Environment nodes are initialized with random terrain type, mine placement, start and end locations.
- Formalizing it as Markov Decision Process (MDP):
  - **States**
    - Final position (100x1)
    - Terrain classes (100x5)
    - UAV position (100x1)
    - UGV position (100x1)
    - UGV Trace (100x1)
    - Human responses (100x1)
    - AI responses (100x1)
  - **Actions**
    - 0-5: Move UAV
    - 6-11: Move UGV
    - 12: AI query
    - 13: Human query
  - **Reward**
    - UAV movement: -1
    - AI query: -5
    - Human query: -30
    - UGV movement: -20
    - UGV clearance: -60

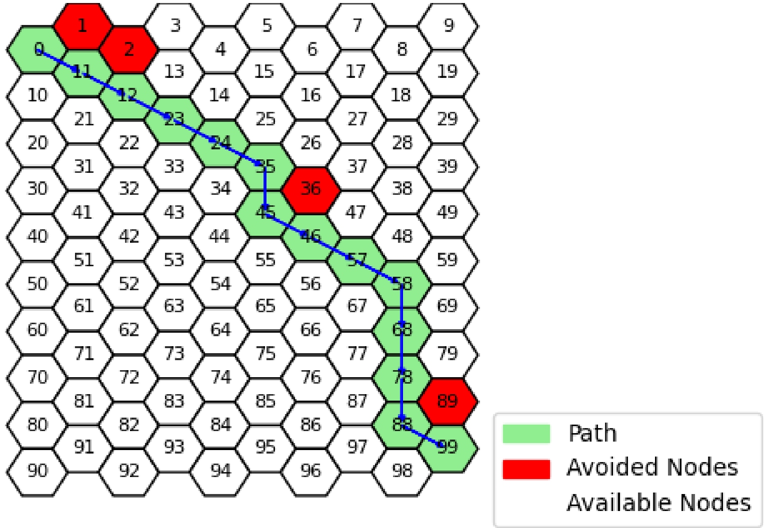
Architecture A1: Centralized, Human

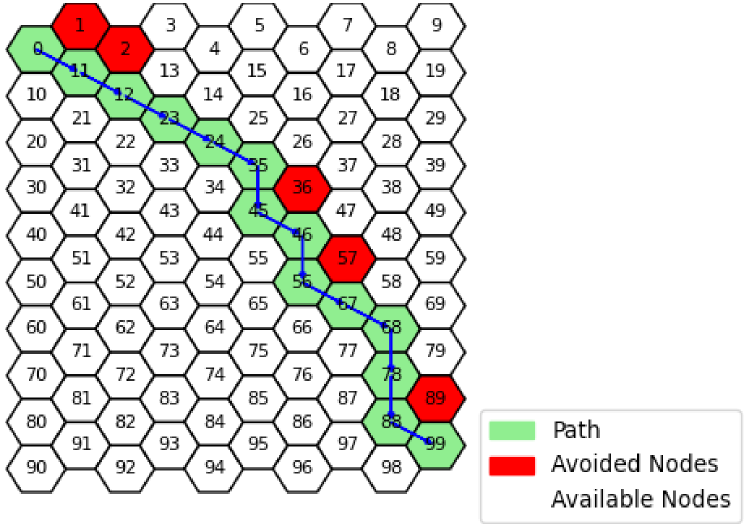


Path Planning Scheme

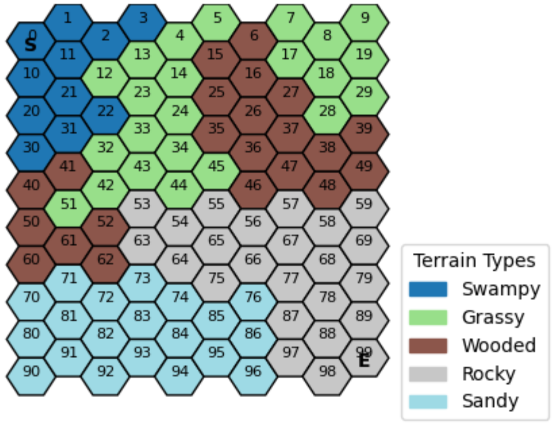
A* search algorithm is used to determine the path based on start node (current node), end node (final node) and a list of nodes to avoid (mines)

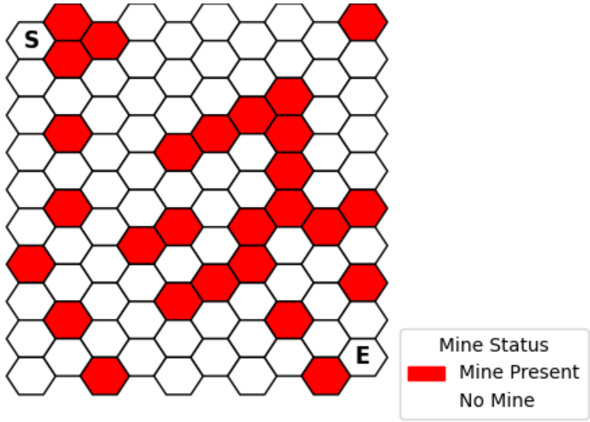


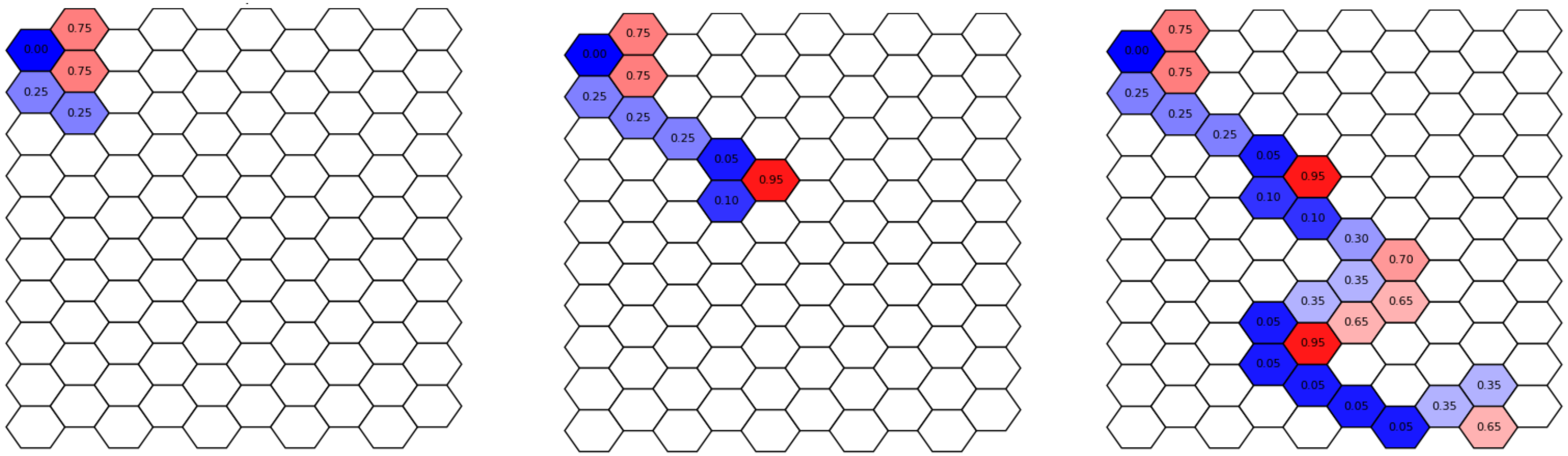




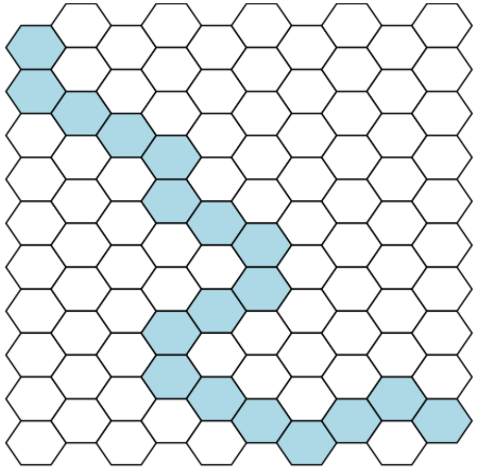
Architecture A1 – Centralized, Human





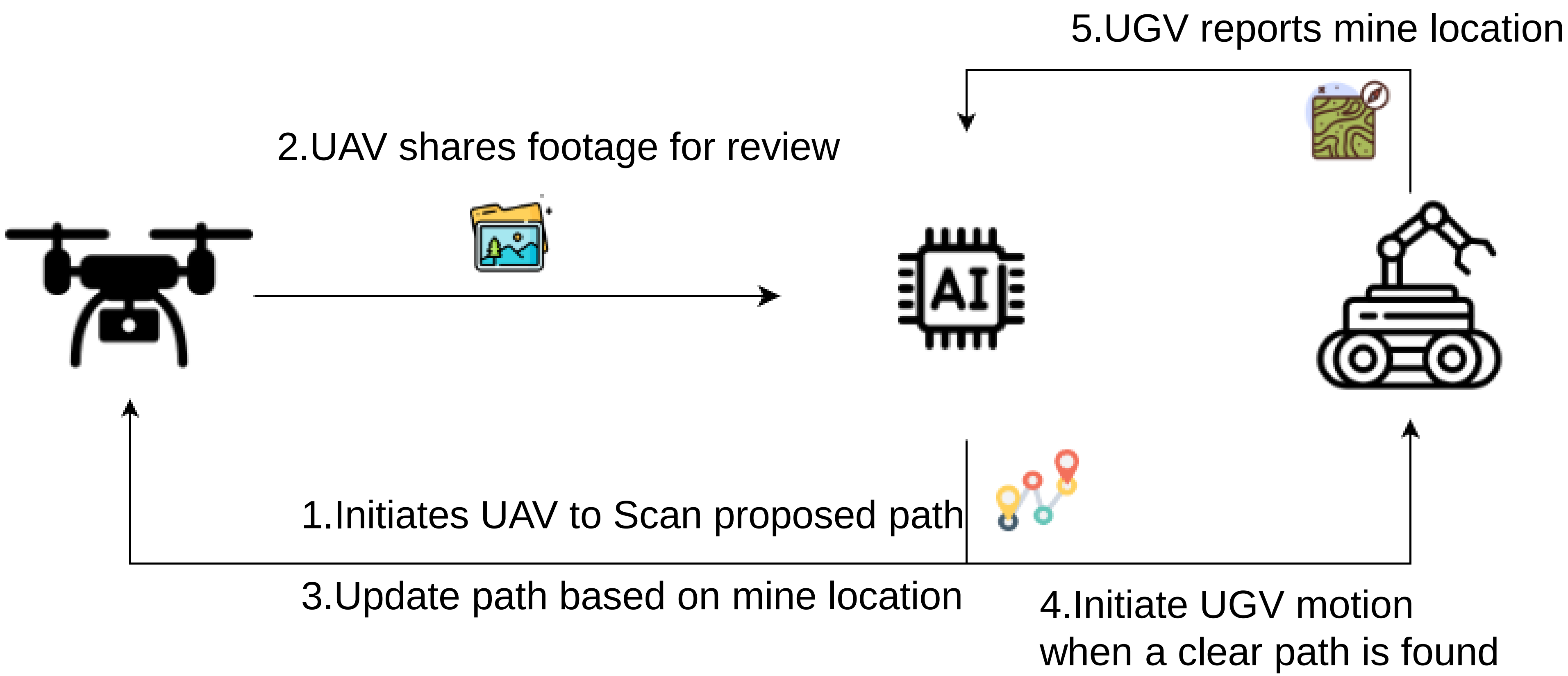


UAV Estimates

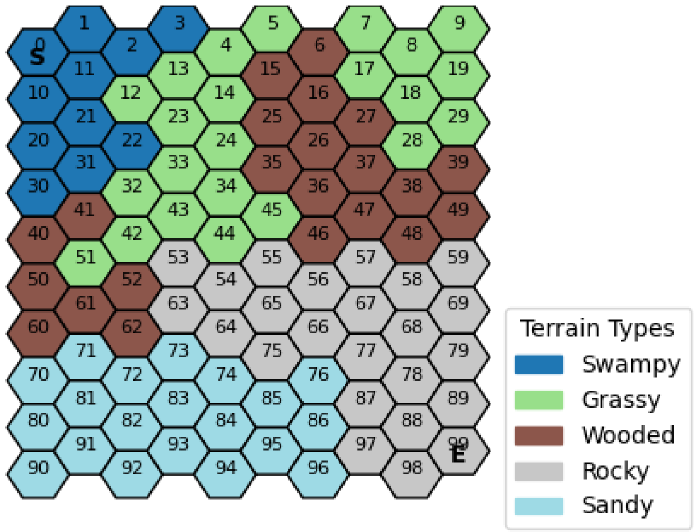


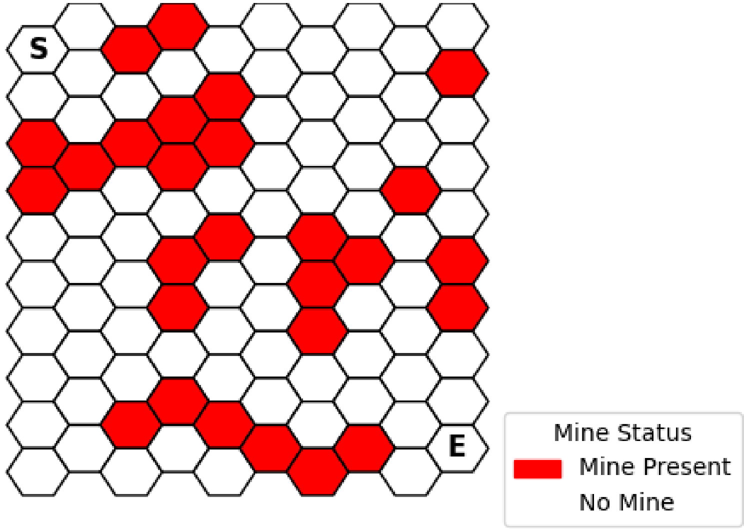
UGV Path

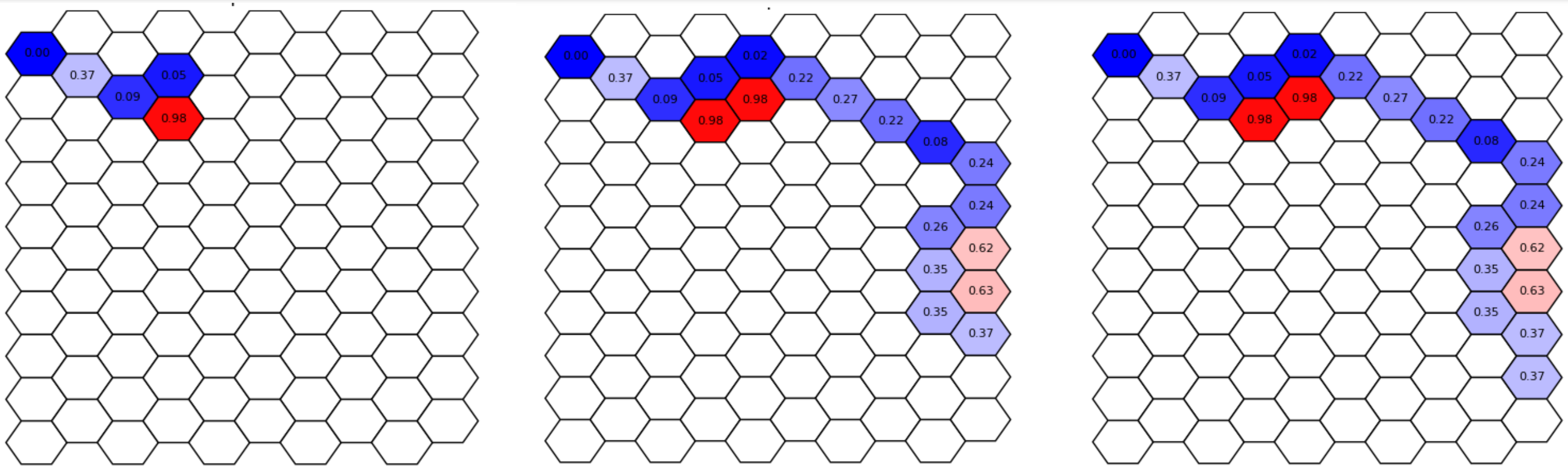
Architecture A2: Centralized, AI



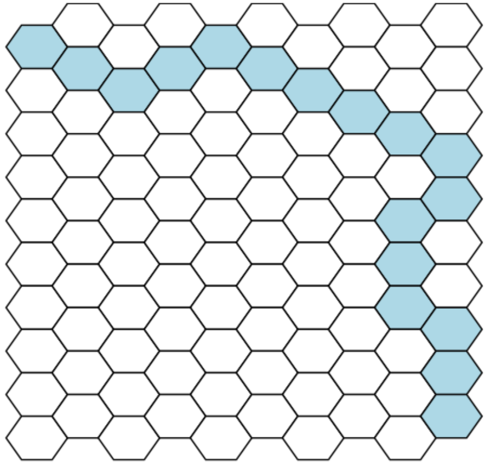
Architecture A2: Centralized, AI







UAV Estimates

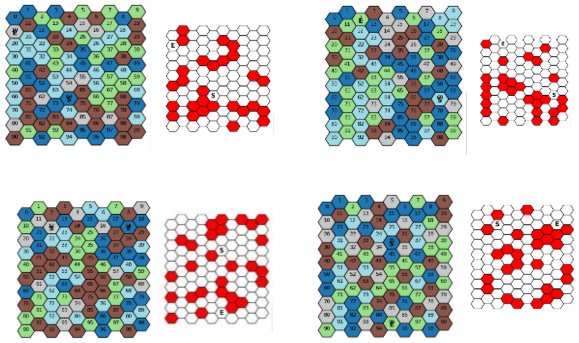


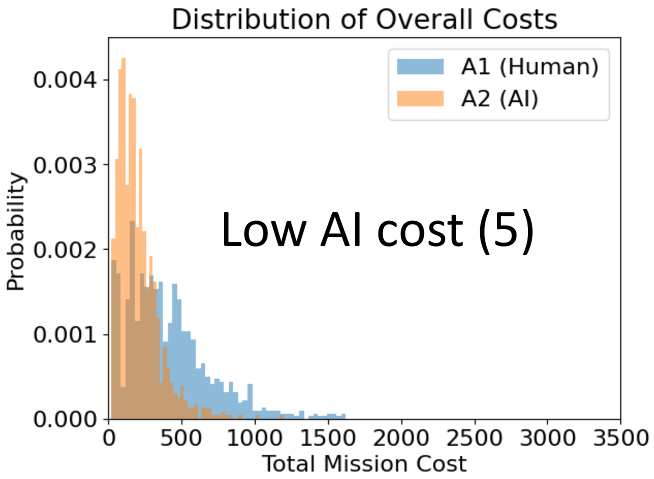
UGV Path

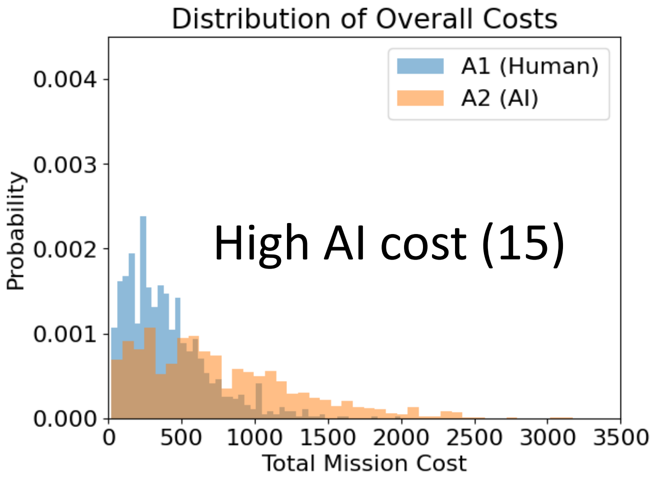
Comparison of A1 and A2

A1 is better when AI cost is high and A2 is better when AI cost is low.

Test A1 and A2 on 10,000 randomly initialized missions



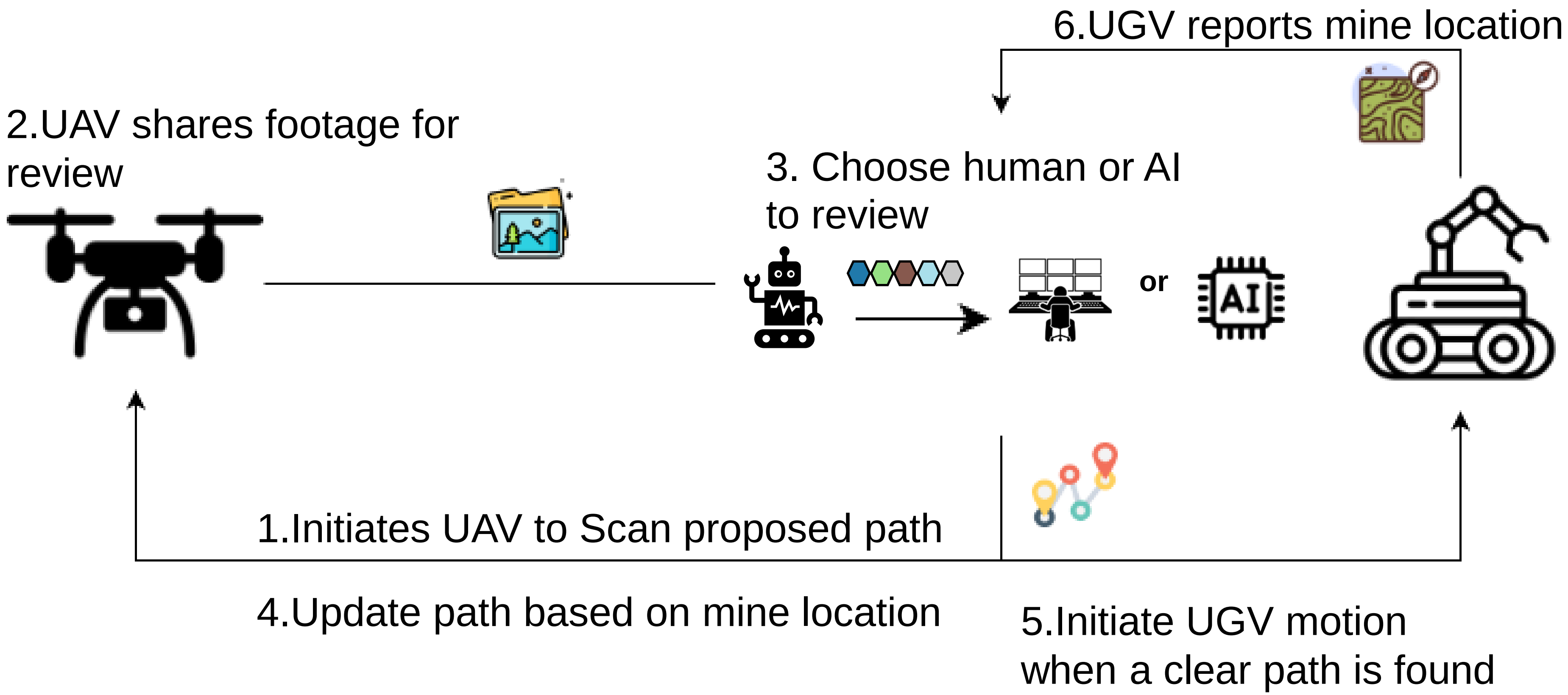




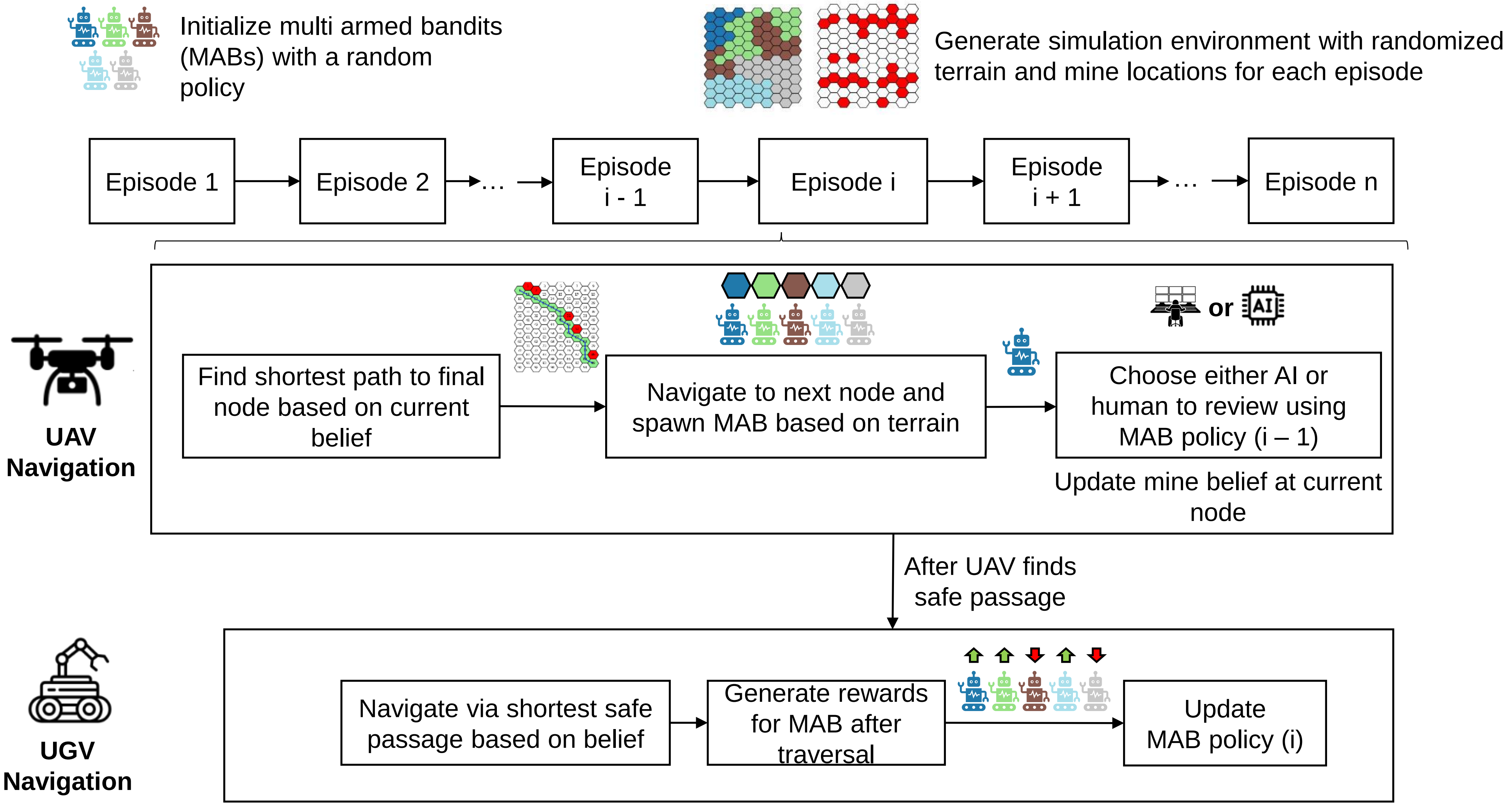
Can we learn when to trust AI or human based on the **terrain information** and **cost**?

Approach A3: Actions for querying are made by 5 multi-armed bandits (MAB) with two arms corresponding to AI and human

Architecture A3: Centralized, Human-AI Teaming

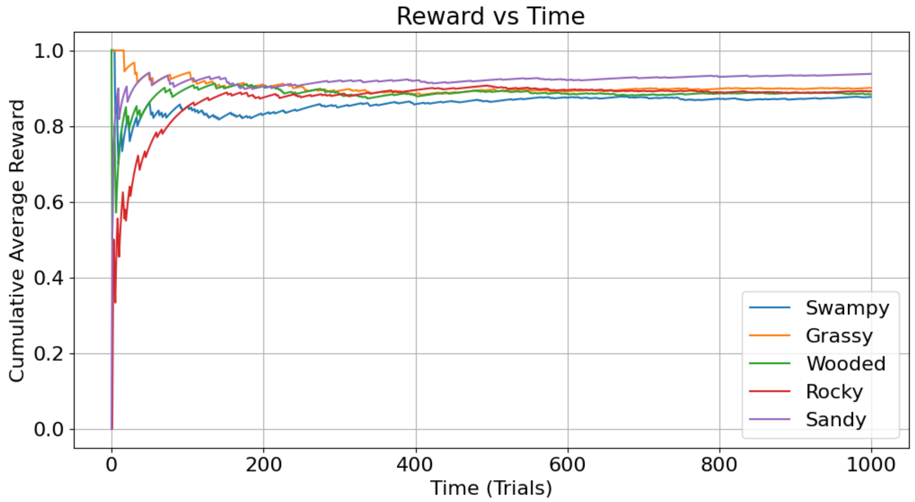


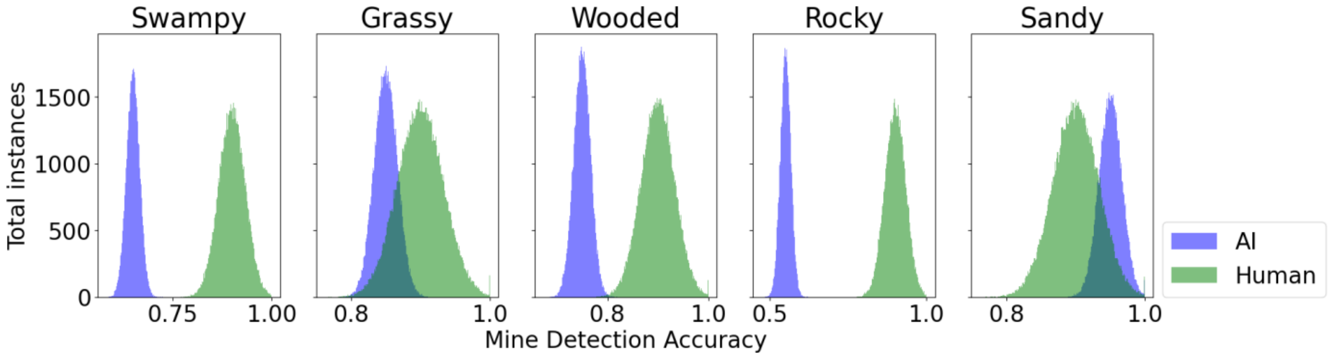
A3: Using AI4SE for SE4AI

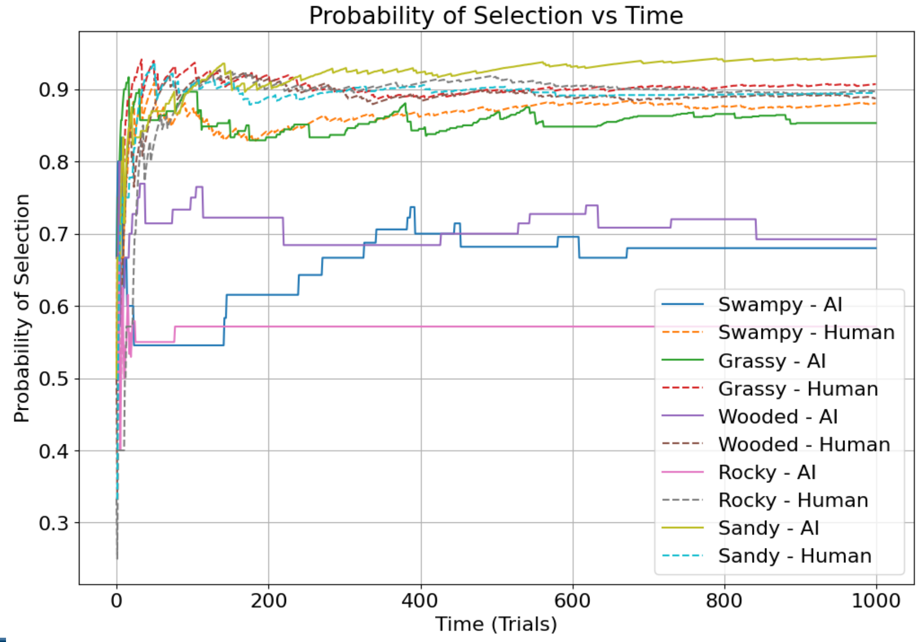


A3: Centralized, Human-AI Teaming

- Actions for movement are predetermined by pathfinding algorithm (A*)
- Actions for querying are made by multi-armed bandits (using UCB policy)
  - Total bandits: terrain types (5)
  - Arms corresponding to AI and human query (2)
  - Reward = (1– λ) × accuracy + λ × (-normalised_cost)
- Environment is sampled for 1000 episodes (λ=0)







A3: Heuristics for terrains

Prioritize Accuracy ← → Prioritize Cost

	λ = 0	λ = 0.33	λ = 0.67	λ = 1
Rocky	Human	Human	Human	AI
Swampy	Human	Human	AI	AI
Wooded	Human	AI	AI	AI
Grassy	Human	AI	AI	AI
Sandy	AI	AI	AI	AI

MAB reward = $(1 - \lambda) \times \text{accuracy} + \lambda \times (\text{-normalised\_cost})$

Results

- Successfully generated multiple simulations to test and validated three approaches
- **Centralized Human (A1):**
  - Effective for high AI costs
- **Centralized AI (A2):**
  - Superior when AI costs are low
- **Human-AI Teaming (A3):**
  - Leveraged reinforcement learning (RL) using multi armed bandits
  - Balanced accuracy and cost
  - Learnt heuristics for trust based on the terrain

Possible Extensions

- Account for changes in the operational environment during the task, limited bandwidth and errors/loss of information during communication
- Expand to decentralized architecture with a UAV AI
- Consider Lethality while making decisions
- Expand strategy to leverage multiple UAVs/UGVs and human movement along with UGVs
- Hardware implementation plan:
  - Set up a test network structure with obstacles simulating mines
  - Use UAVs to scan the network, with view obfuscated in parts
  - Benchmark the architectures in terms of expected time, computational power, bandwidth required
- Hardware
  - Turtle Bots
  - Drones
- Leverage existing facilities at Purdue for test and evaluation
  - Purdue UAS Research and Test Facility (PURT)

Acknowledgements

SERC WRT-1085: Trusted Artificial Intelligence (AI) Systems Engineering (SE) Challenge: Seed Funding

Prime contract number: *HQ003419D0003, DO HQ003423F0495*

Subcontract Number 2103596-05

SYSTEMS ENGINEERING RESEARCH CENTER