Coordinating Heterogeneous Teams for Urban Search and Rescue

Zongyue Zhao
CMU-RI-TR-22-44
August 11, 2022

The Robotics Institute
School of Computer Science
Carnegie Mellon University
Pittsburgh, PA

Thesis Committee:
Dr. Katia Sycara, chair
Dr. Changliu Liu
Tejus Gupta

Submitted in partial fulfillment of the requirements for the degree of Master of Science in Robotics.

Copyright © 2022 Zongyue Zhao. All rights reserved.
To my family.
Abstract

The mission of Urban Search and Rescue (USAR) is a fight against time. Victim survival depends on whether they can be found and attended to in a critical time frame. However, rescuers face severe visibility issues in the complex environment shortly after structural collapse catastrophes. This brings the need to study effective schemes of team coordination. In this thesis, we present methods to coordinate a rescue team of members with different domain knowledge and capabilities. We first formalize a framework for modeling agents-environment interaction that allows for arbitrary origins of heterogeneity, from which we identify two configuration instances generalizable to common real-world tasks. We use them to develop a series of USAR environment simulators with regard to the trade-off between fidelity and sample efficiency. Under these preparations, we propose a multi-agent reinforcement learning algorithm to tackle USAR. We adopt graph attention, in a novel manner, to fuse information perceived across agents and exploit structural priors of the environment. We apply action-dominant agent indexing to benefit from the power of parameter sharing, while still allowing agents to have different behavioral traits. We show that our proposed approach outperforms previous state-of-the-art literature by 40% to 120% in terms of victim evacuation. In addition, we develop hierarchical planning-based agents that mimic human behavior. We conduct imitation learning over faux human trajectories and demonstrate the improvement over purely online reinforcement learning. Ultimately, we show that the feature distributions of artificial and real data are sufficiently close, so that the former can be used to forecast human performance. We observe that the inference error can be reduced by half when transformer-based predictors are augmented with a synthetic dataset.
Acknowledgments

I would like to express gratitude to my research advisor, Professor Katia Sycara, for her precious insights, guidance, and support. I had an amazing time over the last two years in the lab, in which she created a caring and collaborative atmosphere. I am also thankful to my thesis committee members, Professor Changliu Liu and Tejus Gupta, who have patiently devoted their time to providing valuable feedback and comments.

I also want to say thank you to my collaborators: Professor Michael Lewis, Dr. Dana Hughes, Dr. Joseph Campbell, Dr. Simon Stepputtis, Sophie Yue Guo, Max Chris, Ini Oguntola, Huao Li, Keyang Zheng, Noel Chen, Akshay Dharmavaram, Ying Chen, Ruiyu Li, and Renos Zabounidis, for all the sparkling ideas and comments they kindly shared in our meetings. Special thanks to Joe and Simon for how they put an extensive amount of effort into helping me refine my thesis.

It has been a fantastic journey at CMU. I appreciate the friends I made along the way.
Funding

This work was supported by DARPA Award HR001120C0036. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Defense Advanced Research Projects Agency (DARPA).
## Contents

1 Introduction .......................................................... 1

2 Background ............................................................ 7  
   2.1 Markov Decision Process ........................................ 7  
   2.2 Markov Games .................................................... 8  
      2.2.1 Heterogeneity in Multi-Agent Systems .................... 8  
      2.2.2 Information Structure ...................................... 9  
   2.3 Reinforcement Learning Algorithms .............................. 10  
      2.3.1 Value-based ............................................... 11  
      2.3.2 Policy Gradient and Actor-Critic ......................... 12  
   2.4 RL over Graph Environments .................................... 13

3 Task Formulation ..................................................... 15  
   3.1 Heterogeneous Teamwork ........................................ 15  
   3.2 USAR Mission Design .......................................... 17

4 Marcomanagement ..................................................... 21  
   4.1 Graph-based Environment Simulator .............................. 21  
      4.1.1 State Space ............................................... 21  
      4.1.2 Observation Space ......................................... 22  
      4.1.3 Action Space and Dynamics ................................ 22  
   4.2 Algorithms ........................................................ 23  
   4.3 Experiments ....................................................... 27  
      4.3.1 Baselines .................................................... 27  
      4.3.2 Results and Discussions .................................... 28

5 Micromanagement ....................................................... 33  
   5.1 Grid-based Environment Simulator .............................. 33  
      5.1.1 State and Observation Space ............................... 33  
      5.1.2 Action Space and Dynamics ................................. 33  
      5.1.3 Optional Features .......................................... 35  
   5.2 Algorithms ....................................................... 36  
   5.3 Experiments ....................................................... 38  
      5.3.1 Decision-Making ............................................. 38
5.3.2 Forecasting Human Performance .............................. 41

6 Conclusion .......................................................... 45

A Acquiring Human Data ............................................. 47

B Implementation and Future Work ................................. 51
   B.1 Marcomanagement ............................................. 51
   B.2 Micromanagement ............................................. 52
   B.3 Predicting Human Performance ............................. 53
   B.4 Future Work ................................................. 53

Bibliography .......................................................... 55
# List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Study Outline</td>
</tr>
<tr>
<td>3.1</td>
<td>Saturn map for the USAR mission.</td>
</tr>
<tr>
<td>4.1</td>
<td>Model architecture.</td>
</tr>
<tr>
<td>4.2</td>
<td>Graph-based environments.</td>
</tr>
<tr>
<td>4.3</td>
<td>Performance in the marcomanagement task.</td>
</tr>
<tr>
<td>4.4</td>
<td>Impact of partial observability on MAVEN.</td>
</tr>
<tr>
<td>4.5</td>
<td>Performance in preconditions - Middle Map.</td>
</tr>
<tr>
<td>4.6</td>
<td>Ablation studies - Communication</td>
</tr>
<tr>
<td>4.7</td>
<td>Ablation studies: Agent-indexing schemes.</td>
</tr>
<tr>
<td>4.8</td>
<td>Attention to feature dimensions. Weights are extracted from the model trained for 100 million steps in the Saturn-right map.</td>
</tr>
<tr>
<td>5.1</td>
<td>Visibility masks that overlay the global map. Light Grey indicate that the block is within an agent’s field of view.</td>
</tr>
<tr>
<td>5.2</td>
<td>Hierarchical planning agents.</td>
</tr>
<tr>
<td>5.3</td>
<td>Four randomization levels in the top-left region of Saturn. The initial agent locations are always randomized. Environment dimension: $17 \times 28 \times 6$. Maximum M1: 120.</td>
</tr>
<tr>
<td>5.4</td>
<td>Details regarding online RL.</td>
</tr>
<tr>
<td>5.5</td>
<td>Comparison between online RL and IL over end-of-episode performance, in the environment shown in Figure 5.3.</td>
</tr>
<tr>
<td>5.6</td>
<td>Long-term prediction model: $D_h</td>
</tr>
<tr>
<td>5.7</td>
<td>Short-term prediction model: $D_h</td>
</tr>
<tr>
<td>5.8</td>
<td>Long-term prediction model: $D_{vh}</td>
</tr>
<tr>
<td>5.9</td>
<td>Short-term prediction model: $D_{vh}</td>
</tr>
<tr>
<td>5.10</td>
<td>Comparison between MLP and Transformer for long-term prediction.</td>
</tr>
<tr>
<td>A.1</td>
<td>Minecraft Environment</td>
</tr>
<tr>
<td>A.2</td>
<td>The layout of a participant’s interface.</td>
</tr>
<tr>
<td>A.3</td>
<td>Marker Blocks</td>
</tr>
</tbody>
</table>
List of Tables

3.1  Reward signals. ............................................................... 19
5.1  Traveling speed [m/s] of each role. The environment operates at 4Hz. 34
B.1  Hyperparameters for marcomanagement. .......................... 51
B.2  Hyperparameters for micromanagement. ............................ 52
Chapter 1

Introduction

Earthquakes claimed more than 700,000 lives in the first two decades of this century [28]. Urban areas, in particular, are severely impacted due to extended building structures [97]. Victims under the collapsed ruins must be attended to in a critical time frame for successful evacuation [91]. However, the rescue team, often limited in human resources, faces an unknown, complex environment with hazards associated with secondary disasters [54, 59]. Thus, it is crucial to search for effective schemes of team coordination in urban search and rescue (USAR) scenarios.

We first consider the goal of finding the optimal team policy, i.e., what the rescuers should do. For this purpose, we adopt the paradigm of cooperative multi-agent reinforcement learning (MARL), which aims to maximize cumulative reward signals from the interaction between a group of agents and the environment. However, two challenges arise when applying MARL to USAR. Firstly, a typical USAR mission involves intrinsically different operations, such as search, locate, on-site medical support, and extrication [97]. Entities specialized in one domain may not have the knowledge or ability to execute other operations. Thus, the team is heterogeneous. Meanwhile, USAR rescuers often encounter severe visibility limitations [87, 121, 126], highlighting the importance of information sharing among teammates [16, 22, 44, 64, 93]. This raises the question of role-adaptive communication: agents need to identify and communicate transferable knowledge while preserving their own behavioral traits.

Recent advances in cooperative MARL realize information sharing by averaging recurrent communication channels [93, 98] or applying the attention mechanism over
the agent relationship graph [10, 55, 58, 70, 90]. However, we observed that the former approach had trouble distinguishing transferable knowledge from domain knowledge only applicable to the sender. The latter approach, on the other hand, is only applicable for tasks involving a great number of agents. Identifying which agent pairs carry more weight in communication becomes of less significance for a small rescue team with only a few agents.

In addition to the methodology of explicit communication, recent literature also adopted the parameter sharing (PS) paradigm that reuses policy or value networks for multiple agents. While PS have been increasingly popular, they are often proposed for homogeneous teams [9, 34, 114]. Work that aims to address this limitation generally relies on agent indexing [26, 63, 83]. However, plain agent indexing fails to utilize the prior knowledge of an agent’s capabilities, which are available in various high-level decision-making tasks. Another approach to address issues associated with partial observability is to assume that global states are available for the agents during training [63, 83, 94, 123]. This is known as a variant of centralized training decentralized execution (CTDE). While such global information can be exploited to stabilize learning, acquiring true states is often only feasible in simulated games like StarCraft II [86]. For USAR missions, even if we make simulators where global states are available, agents trained with the state-based CTDE paradigm cannot be further fine-tuned in real-world testbeds, eventually harming the performance in execution [21, 125].

In this thesis, we propose a novel MARL architecture to address the aforementioned drawbacks. Unlike previous literature that operates on the agent relationship graph, we apply attention over the environment graph structure. From a USAR perspective, this corresponds to the case where participants are equipped with a map describing the building structure before the catastrophe, and hope to use outdated priors to expedite the search process. We use a graph attention network [106] to fuse observations shared across agents, without the need to depend on global states. We also improve agent indexing with action availability indicators, so that actor inputs have a higher similarity when the optimal joint action is more homogeneous. Furthermore, we develop a graph-based USAR environment simulator optimized for sample and learning efficiency. We use it to evaluate the performance of the proposed algorithm against state-of-the-art literature in MARL, and show that we outperform methods that use
1. Introduction

agent-relationship graphs or demand global information.

While it is beneficial to exploit heterogeneity explicitly presented to the policy network, there exist another series of decision-making tasks in which such extra information is unavailable. For low-level control tasks, it is typical for the action space to appear identical for all agents despite their intrinsic differences. These implicit diversities can be modeled with role-specific environment dynamics. To study the practices applicable to this setup, we develop a grid-based environment also for USAR scenarios. This environment comes with a resolution that maps to $1m \times 1m$ squares in the real world, effectively allowing for in-room navigation.

As the nature of the grid-based environment demands agents to conquer ambiguity in the action space, we observed that online MARL failed to properly comprehend true short-term objectives that differ for each role. For such a complex and unstructured task, imitation learning (IL) and offline RL serve as two natural replacements for online RL [73, 78, 115]. Compared to IL, offline RL demands a diverse, uniformly distributed dataset that covers the entire state-action space, and poses a higher requirement for the amount of samples [25, 31]. This makes offline RL a less preferable solution in our grid-based environment with high fidelity but low sample efficiency. Meanwhile, (purely offline) IL requires high-performing expert demonstrations to learn from [41, 85]. Because acquiring human data for USAR tasks is costly and time-intensive [19, 29, 32, 77], we develop planning-based faux human agents, a practice adopted by modern literature in complex tasks like autonomous driving [56, 111, 122]. We demonstrate the empirical advantages of imitating experts over online RL.

In addition to the study on optimal coordination, we also hope to comprehend human behavior in USAR, i.e., what the rescuers currently do. Understanding so allows assistive robots to cope with human behavior or issue adequate intervention at an early stage, eventually improving the mission outcome. In the field of human-robot collaboration, it is common to build cognitive models that predict human intent [12, 81, 120] or performance [13, 18, 36]. Deep neural networks are progressively assuming a crucial role for these purposes [89]. For example, recent literature has adopted sequential models like RNNs [61, 112] and transformers [43, 52, 69]. These architectures are known to demand a vast amount of training data [80, 110], sometimes more than $10^{10}$ annotated data points [46]. As it is almost impossible to collect such an amount of human data for USAR missions, we consider the application of using
1. Introduction

Figure 1.1: Study Outline

artificial trajectories for inference tasks in USAR. We tune our planning-based agents to show behavioral traits similar to real humans, and use faux-human trajectories to help train a transformer-based prediction model. We demonstrate advantages, in terms of inference accuracy over unseen human data, against training without synthetic data. We also show how such a data-intensive architecture is proper for the task by showing improvements against simpler models.

To conclude, the outline of our study is summarized in Figure 1.1. The rest of this thesis is organized correspondingly as follows:

- In Chapter 2, we review the key concepts in multi-agent reinforcement learning and provide preliminaries for our work.
- In Chapter 3, we formalize a universal framework to model heterogeneity in cooperative MARL and identify two representative configurations. We also provide an overview of the USAR mission we aim to address.
- In Chapter 4, we present a graph-based environment to simulate USAR at a high level. We propose an online MARL architecture and show improvement against previous state-of-the-art algorithms designed for generic setups.
- In Chapter 5, we present a grid-based environment to simulate USAR at a low level. We show the limitation of online MARL towards action ambiguity. We demonstrate how imitating vivid faux humans may improve decision-making...
given the same network architecture. We also show that synthetic trajectories can be used to augment cognitive models that aim to infer human performance.

- In Chapter 6, we conclude the findings in this thesis.
- In Appendix A, we describe our collaborators’ methodology when acquiring human data.
- In Appendix B, we present implementation details and acknowledge aspects for future work.
1. Introduction
Chapter 2

Background

2.1 Markov Decision Process

In fully-observable, single-agent reinforcement learning, the interaction between the agent and the environment is formalized as a Markov decision process (MDP) [101], which is represented by the Markov tuple \((S, A, T, R, \gamma)\):

- The state space \(S\) is the set of possible states of the environment.
- The action space \(A\) consists of the possible actions the agent may take.
- The transition function \(T : S \times A \times S \rightarrow [0, 1]\) determines the probability \(T(s, a, s')\) of the environment arriving in the state \(s'\) after the agent executed the action \(a\) given state \(s\). The one-step Markov property is attained, as the entire dynamics of the environment are described with the triplet \((s, a, s')\) but not history.
- The reward function \(R : S \times A \times S \rightarrow \mathbb{R}\) maps the state \(s\), action \(a\), and the resulting state \(s'\) to an reward signal \(R(s, a, s')\) known by the agent after reaching \(s'\).
- The discount factor \(\gamma \in [0, 1]\) weights the importance of future rewards over immediate rewards.

Under MDP, a policy \(\pi(a|s)\) is considered optimal if it maximizes the expected discounted cumulative rewards \(G = \mathbb{E}_\pi[\sum_{t=0}^{T} \gamma^t r_t]\) [79]. If the transition dynamics \(T\)
and reward function $R$ are fully known, the optimal policy can be solved via dynamic programming [6]. Otherwise, RL algorithms need to learn from agent-environment interaction experiences in an error-and-trial manner. Furthermore, MDP assumes complete access to the environment states. If the inception capabilities of the agent are limited, decision-making can be modeled as a partially observable Markov decision process (POMDP) by introducing the observation space $\Omega = \{o\}$ and the observation function $O: S \times A \times \Omega \rightarrow [0, 1]$ [96]. As the probability $p(o'|o,a)$ does not represent the environment dynamics, algorithms designed for POMDP commonly hold a belief regarding the unseen environment states [68, 96] or use dynamic models [39, 95].

2.2 Markov Games

In this section, we discuss how to model the interaction between multiple agents and the environment. Among the various formulations proposed to extend (PO)MDPs to a multi-agent setting, the two key differences are a) which elements in the Markov tuple are agent-sensitive, and b) the paradigms that regularize and reflect the information structure among agents.

2.2.1 Heterogeneity in Multi-Agent Systems

Consider the partially observable Markov tuple. A generalizable adaptation for the multi-agent setting is to replace selected elements $(X, Y, ...) \subseteq (S, A, \Omega, T, R, O, \gamma)$ with sets of those elements ($\{X^{(i)}\}, \{Y^{(i)}\}, ...$) to address heterogeneity between agents. For example, the Markov Games model [57, 92] allows for a set of action spaces $\{A^{(i)}\}$ and reward functions $\{R^{(i)}\}$. Under this formulation, it is possible to define whether a task is cooperative based on the reward structure: either a) the same reward function applies to all agents ($\forall i, j, R^{(i)} = R^{(j)}$, also known as the MMDP model [8]), or b) the overall optimization target is the average of agent-specific returns $(\max \sum_i G^{(i)})$ [47, 118]. Furthermore, there exists work that considered heterogeneity in Markov elements other than $A$ and $R$. The POSG model [35] supports disjoint observation spaces $\{\Omega^{(i)}\}, \{O^{(i)}\}$ in addition to action space and rewards variations. As discussed by the authors of [35], when the reward function is uniform across agents, POSG regresses to DEC-POMDP [7], which is a widely adopted framework in recent
work on deep cooperative MARL [11, 23, 27, 83]. Moreover, the MAH-POMDP [90] model extended DEC-POMDP with state spaces \( \mathcal{S}^{(i)} \) that are unique to the agent’s corresponding class.

### 2.2.2 Information Structure

The second thing to consider when formalizing cooperative MARL tasks is how agents are allowed, in both explicit regulations and feasibility constraints, to share information among themselves [119]. Certain real-world scenarios, e.g., when agents are geometrically sparse [76] or facing adversarial attacks [99], constrain or even prohibit timely information exchange. Under the most strict limitation, MARL can be realized in a fully decentralized setting [7, 118], where each agent corresponds to an independent policy that only considers its own observation. Algorithms in this setup scale linearly with the number of agents. However, for any arbitrary agent \( i \), because the environment evolves due to not only its own action but also other agents’ actions unknown to \( i \), the transition dynamics perceived by \( i \) is non-stationary [71]. This violation to the Markov property means agent \( i \)’s value estimate may not approximate the status quo of the environment as other agents’ learning progresses.

Meanwhile, suppose the task scenario can be separated into distinct training and execution stages, where information exchange is only prohibited during execution. In that case, it is possible to mitigate the aforementioned deficiencies via the paradigm of centralized training with decentralized execution (CTDE). This paradigm has been popular in recent advances [14, 53, 60, 63, 83, 84, 94] in cooperative MARL. The problem setup is similar to DEC-POMDP, where agents make decisions under their own observation/action space rather than joint spaces. However, during the training stages, participants are allowed to freely share information with each other [34, 60] or access global states [83, 86]. Such extra information is often only used to train the critic in the actor-critic setting (Section 2.3.2), so that the actor heads face the same input distribution in both stages. Nonetheless, the environment under this paradigm would appear more stationary to the agents, leading to performance improvements against non-CTDE baselines in certain tasks [15] that allow for a training playground.

Parameter sharing (PS) [103] is the technique where multiple agents reuse a policy and/or value network. This mechanism abides by the same constraints regarding
2. Background

information flow as CTDE. So long as there exists a centralized playground at the training stage, trajectories from all agents can be gathered to update the agent models, whether they share weights (PS) or not (Non-PS CTDE). The trained models can be deployed separately to each agent prior to the execution stage, thus fulfilling the requirement of decentralized execution. For cooperative settings, it has been observed that this mechanism facilitates training speed by reducing the total amount of trainable parameters and improves converged returns by utilizing instantaneous peer information and learned knowledge [15, 48]. Unfortunately, a fully shared model encounters issues adapting to multiple coherently distinct tasks when used naively. Thus, it is common to condition the network with a one-hot vector indicating the agent’s identity [26, 34, 63, 83, 104]. This method is known as agent indexing or agent identification. An alternative solution is to share partially, e.g., sharing the critic but keeping actor heads separated in an actor-critic framework [17, 117]. For tasks that involve a large number of agents, it is also possible to use more than one shared network. Agents who most closely resemble each other can be grouped together and assigned with the same model [15, 107].

In scenarios that pose no constraints on the information flow, MARL can be realized by adopting a single policy that maps the joint observation \( o \in \prod^n_i O^{(i)} \) of all agents to a joint action \( a \in \prod^n_i A^{(i)} \) [2]. This method allows for reusing existing single-agent RL algorithms, and is immune to non-stationarity resulted from independent learners with partial observability. However, it suffers from scalability issues, as the observation and action space of the joint controller scale exponentially with respect to the number of agents [34]. This calls for a representation of semi-independent learners that corresponds to agent-specific spaces. In addition to the CTDE/PS paradigms that are still applicable, agents here may adopt explicit communication mechanisms via recurrent channels [58, 74], attention [42, 45, 90], or shared memories [75]. There is also a series of works that aim to factorize value networks of the centralized controller, which is discussed in detail in Section 2.3.1.

2.3 Reinforcement Learning Algorithms

In this section, we briefly review key reinforcement learning algorithms and the special considerations when multiple agents are involved.


2.3.1 Value-based

Action-value methods maintain value estimates for state-action pairs and use them to select actions. For example, Q-Learning [108] estimate the optimal state-action value function $Q$ from rollouts $(s, a \sim \pi(\cdot|s), r, s')$ by any policy $\pi$, commonly a $\varepsilon$-soft variant of the greedy policy represented by $Q$:

$$Q(s, a) \leftarrow Q(s, a) + \alpha \left[ r + \gamma \max_{a'} Q(s', a') - Q(s, a) \right]$$  \hspace{1cm} (2.1)

For tasks with high-dimensional or continuous state/action spaces, neural networks can be used as function approximators for the Q-value. With the trainable parameters in the network denoted as $\theta$, the loss function to be minimized can be expressed as:

$$L(\theta) = \mathbb{E}_\pi \left[ (r + \gamma \max_{a'} Q(s', a'|\theta) - Q(s, a|\theta))^2 \right]$$  \hspace{1cm} (2.2)

To address instability issues from a long and correlated decision sequence, a popular architecture, DQN [66] introduced the replay buffer $D_t = \{e_1, ..., e_t\}$, where $e_t = (s_t, a_t, r_t, s_{t+1})$ is the Markov tuple of the past experience at $t$. During training, gradient descent is conducted on minibatches sampled from the uniform distribution of the replay buffer: $\{(s, a, r, s')\} \sim U(D_t)$, instead of the current Markov tuple $(s_t, a_t, r_t, s_{t+1})$ only. It was observed that replay buffers, together with periodical updates of the target Q function, helped DQN to achieve human-equivalent performance in Atari [5].

DQN and other off-policy algorithms with a replay buffer encounter issues when extended to the multi-agent setup. As discussed in Section 2.2.2, the joint state and action space would scale exponentially when trained with a centralized controller, challenging the expression power of the Q-network. Meanwhile, Q-networks in the fully decentralized approach (independent Q-learning [103]) would face a non-stationary environment, so optimal convergence cannot be guaranteed. The non-stationarity introduced by independent agents also invalidates the use of a replay buffer [60]. As discussed in Section 2.2.2, the transition dynamics $T(s'|s, a)$ for an agent $i$ depends on the policy of all other agents $\forall j \neq i$. As the policies $\pi_j$ progress independently over time, even for a replay buffer $D^i$ that only contains experience from the current...
agent, the dynamics reflected by the sampled batch \( \{(s, a, r, s')\} \) no longer match the current environment.

For cooperative tasks that issue a uniform reward signal for the entire team, even when the number of agents is small and centralized learning can be adopted to mitigate the non-stationarity issue, value-based algorithms still encounter the "lazy-learner" problem. After the centralized value network is learned such that it performs well for one agent, the exploration of other agents will be suppressed because doing so would worsen the team reward \([100]\). Thus, VDN \([100]\) has been proposed to decompose the centralized Q-value estimation \( Q_{\text{tot}} \) into a sum of individual value functions \( \{Q_a\} : \sum_a Q_a = Q_{\text{tot}} \), each corresponding to an individual agent. QMix \([83]\) improved the art of factorization by introducing a mixing network instead of simple summation. As long as monotonicity is preserved between \( Q_{\text{tot}} \) and \( \{Q_a\} \), greedy actions based on each individual value network would still be equivalent to the greedy joint action based on \( Q_{\text{tot}} \). Meanwhile, the mixing network allows for learnable non-linear factorization, resulting in a significant performance boost in the StarCraft II Environment \([86]\).

### 2.3.2 Policy Gradient and Actor-Critic

*Policy gradient* algorithms directly optimize the parametrized policy \( \pi(a|s, \theta) \) to maximize the discounted return \( J(\theta) = \mathbb{E}_{\pi(\theta)} \left[ \sum_{t=0}^{T} \gamma^t r_t \right] \), by stepping \( \theta \) into the direction of the gradient \( \nabla_{\theta} J(\theta) \), which can be approximated \([102]\) as:

\[
\nabla_{\theta} J(\theta) = \mathbb{E}_{s \sim \rho^\pi, a \sim \pi(\theta)} \left[ (\nabla_{\theta} \log \pi(a|s, \theta)) Q^\pi(s, a) \right] \tag{2.3}
\]

where \( \rho^\pi(s) = \lim_{t \to \infty} Pr(s_t = s|s_0, \pi) \) (provided that it exists) is the stationary distribution of states given policy \( \pi \). Under a differentiable representation of the policy network \( \pi(a|s, \theta) \), the problem becomes estimating the action-value \( Q^\pi(s, a) \). For example, REINFORCE \([109]\) uses the Monte-Carlo estimate \( G_t = \sum_{t=t_0}^{T} \gamma^{t-t_0} r_t \), which is a unbiased estimation of the true action value. Unfortunately, the Monte-Carlo estimation suffers from high variance \([51]\). The authors of \([109]\) suggested reducing the variance by subtracting \( G_t \) with a learned function \( b(s_t|\omega) \) known as the
The estimate of the policy gradient at time $s$ now becomes:

$$
\nabla_\theta \log \pi(a_t|s_t, \theta_t) \left( G_t - b(s_t|\omega_t) \right)
$$

(2.4)

A natural placement for the baseline function is the state-value estimate $V^\pi(s)$. In this case, the scaling factor $G_t - V(s_t|\omega_t)$ can be seen as an estimate of the advantage of action $a_t$ at state $s_t$, because $G_t$ estimates the action-value $Q(s_t, a_t)$ [101]. In general, mechanisms that involve approximations to both the policy and value functions belong to the family of actor-critic, where the actor refers to the policy model and the critic refers to the value estimation. In a stricter definition, actor-critic frameworks use TD-learning to estimate a state-action value model $Q(s, a|\omega)$ in place of the Monte-Carlo estimate $G_t$, thereby enabling step-wise updates and facilities training [117]. The use of a baseline function $V^\pi(s)$ still applies, leading to the advantage actor-critic (A2C) method [67]. Furthermore, bootstrapping can be applied to the estimation of $V^\pi(s)$, leading to a generalized advantage estimator (GAE) [88].

Actor-critic algorithms have been widely applied in multi-agent tasks. They have a particularly strong presence in tasks that limit information flow during execution and benefit from implicit coordination paradigms (Section 2.2.2). Since the critic is only used during training, they can be designed to take extra information from peer agents as input (MADDPG [60], COMA [27]), or be shared across multiple agents [62, 117]. Meanwhile, tasks that allow explicit communication during the execution stage also commonly adopt policy gradient algorithms. In this aspect, IC3Net [93] uses LSTM units as communication channels that persist across timestamps. G2ANet [58], HetNet [90], MAGAT [55], GAMA [10], and MAGIC [70] form relationship graphs over agents to apply attention-based communication.

## 2.4 RL over Graph Environments

Our main contributions in Chapter 4 involve applying MARL over a graph-based environment simulator. Thus, we hope to review literature in this domain and discuss the similarities and differences.

The work that most closely resembled ours is [127], which applied a graph attention network (GAT) to solve graph navigation. While we also adopted GAT to examine
2. Background

neighborhood features, the main differences are as follows:

- The scope of [127] is single-agent RL that aim to one-shot navigate unseen graph structures. The agent’s sole purpose is to cover more graph nodes within the given time budget. On the contrary, we focus on coordinating a team of multiple agents. Rapid graph navigation would not necessarily lead to desirable teamwork.

- In [127], a graph node contains no feature other than its identity. Meanwhile, nodes in our graph differ from each other by their content (victims, rubbles, etc.). Our graph is thus heterogeneous [116], such that it can be used to study USAR missions that involve not only graph navigation but also how agents interact with the node they reside in.

- We adopted different network architectures and gradient estimation methods. Recent advances applied RL in other graph-related problems, such as minimum vertex cover, traveling salesman, and maximum cut [4, 40, 49]. These tasks reduce to combinatorial optimization [65], and like the problem investigated in [127], they focus on how identical nodes are connected to each other. On the contrary, our problem statement primarily focus on how graph nodes host information about different types of entities. We argue that this distinction separates our work in Chapter 4, i.e., coordinating heterogeneous agents in a heterogeneous graph, from previous literature.
Chapter 3

Task Formulation

3.1 Heterogeneous Teamwork

The problem of coordinating a heterogeneous team including $N$ agents with $C \leq N$ distinct roles can be formalized by the tuple:

$$(C, S, \{A^{(c)}\}, \{M^{(c)}\}, \{\Omega^{(c)}\}, \{O^{(c)}\}, \{T^{(c)}\}, \{R^{(c)}\}, \gamma) \quad (3.1)$$

- $C = \{1, \ldots, N\} \rightarrow \{1, \ldots, C\}$, where $C(i)$ indicates the role of agent $i$. Given the current state, agents with the same role are interchangeable with respect to all other Markov elements.

- $S$, which is the space of global states. The entire environment is uniquely determined given $C$ and $S$, i.e., we do not consider information describing an agent (other than its role) to be separated from $S$. For example, $s \in S$ contain information on the location of any arbitrary agent $i$.

- $A = \cup A^{(c)} = \{a\}$ is the union of all agent-wise actions, where $A^{C(i)}$ is the action space for the $i$-th agent. This is different from the joint action space $U = \prod A^{C(i)} = \{A\}$.

- $M^{(c)} : S \times A \rightarrow \{0, 1\}$, where the action mask $M^{(c)}(s, a) = 1$ indicates that the action $a$ is available for an agent with role $c$ given the global state $s$. Note how the separation of $C$ from $S$ makes $M$ conditional to $c$ as well.
3. Task Formulation

- \( \Omega = \cup \Omega^{(c)} = \{ o \} \), which is the union of all role-specific observation spaces. \( \Omega \subset \mathcal{S} \cup \mathcal{C} \) is a proper subset of the union of the state space and the set of role mappings.

- \( \mathcal{O}^{(c)} : \mathcal{S} \times \Omega \rightarrow [0,1] \) is the observation function, where \( \mathcal{O}^{(c)}(s,o) \) is the probability of an agent with role \( c \) observing \( o \) given the global state \( c \). Compared to the DEC-POMDP setting that requires a state-action pair \((s,a)\), this marginalized formalization indicates that agents may observe the environment without the need to execute an action. This is common for modern environments [86] with a high observation rate asynchronous to action selection.

- \( \mathcal{T}^{(c)} : \mathcal{S} \times \mathcal{A} \times \mathcal{S} \rightarrow [0,1] \) is the transition dynamics, where \( \mathcal{T}^{(c)}(s,a,s') \) is the probability of the environment arriving at \( s' \) after an agent with type \( c \) executed action \( a \) given the previous global state \( s \). Note that this allows for role-specific dynamics on top of the possible constraints on the action space. We find this useful for real-world scenarios where the action space can be decomposed to task-irrelevant atomic actions. Moreover, this assumes sequential action execution, i.e., the environment immediately transits after a single agent calls for action. This allows for a simplified representation of role-specific environment dynamics because it no longer depends on the agents' joint action.

- \( \mathcal{R}^{(c)} : \mathcal{S} \times \mathcal{A} \times \mathcal{S} \rightarrow \mathbb{R} \), where \( \mathcal{R}^{(c)}(s,a,s') \) is the reward received by an agent of type \( c \) executed the action \( a \) from state \( s \) resulting in state \( s' \).

- \( \gamma \in [0,1] \) is the discount factor uniform to all agents. We do not consider role-specific discount factors to simplify advantage estimation under parameter sharing.

In this thesis, we consider cooperative tasks only, where the end goal is to maximize the average expected discounted return from all agents:

\[
\max_{\pi_1,\ldots,\pi_N} \mathbb{E}_{\pi_1,\ldots,\pi_N} \left[ \sum_{i=1}^{N} \sum_{t=0}^{T} \gamma^t R_{t} \right] \tag{3.2}
\]

Within this framework, we focus on two configurations that have a significant presence in real-world tasks. The first one, which we will refer to as micromanagement, has a uniform action space \( \mathcal{A}^{(c)} = \mathcal{A}, \forall c \). In this case, agents differ by the structure of their corresponding transition dynamics \( \mathcal{T}^{(c)} \). We call this micromanagement because
3. Task Formulation

this setting is often found in low-level control problems. Consider a set of 6-DOF open-chain manipulators with different dimensions and end-effectors. The action space for each manipulator is the same Cartesian product of six individual joint spaces ranging from zero to two pi. However, the outcome from the interaction between the manipulators and the environment will differ subject to their intrinsic properties (dimensions, tools, etc.). This form of heterogeneity can be modeled with either role-specific transition dynamics or states. Here, we adopt the former method to better indicate that the aforementioned intrinsic is stationary over time and episodes.

The second configuration that we consider often corresponds to high-level decision-making tasks, which we will refer to as *macromanagement*. In this case, heterogeneity primarily comes from well-defined disjoint sub-action spaces. For each role, we can decompose its corresponding action space as follows:

\[
A^{(c)} = A^{(c)}_e + A_o \tag{3.3}
\]

where \(A^{(c)}_e \cap A_o = \emptyset\) and \(A^{(m)}_e \cap A^{(n)}_e = \emptyset, \forall m \neq n\). \(A_o\) represents role-invariant actions, e.g., navigation, and depends on the state \(s\) only. On the other hand, the role-specific disjoint subspaces \(A^{(c)}_e\) often correspond to explainable agent capabilities declared by the task and environment. Consider a USAR setting, for example. In a rescue team consisting of people from different backgrounds, it is common that only licensed medical practitioners have sufficient knowledge to diagnose and stabilize a victim’s condition properly. This stabilization action belongs to \(A_e\) for the medical role. As demonstrated in Section 4.3, information regarding an agent’s action space can be used as a strong indicator of the essence of that agent; and should be taken into account of designing heterogeneous autonomous systems. Furthermore, although this configuration does not rule out heterogeneous reward structures \(R^{(c)}\), for the sake of simplicity, we assume all roles perform an action equivalently well, provided that the action is in its current action space.

### 3.2 USAR Mission Design

We consider a USAR mission involving a team of three participants. The end goal of this mission is to evacuate injured victims out of a partially collapsed building. As
3. Task Formulation

the locations of victims are unknown to the rescue team in advance, the team must learn to efficiently explore the building in a limited amount of time. However, certain hallways and rooms are blocked by rubbles that have collapsed from the building structure. This issue can be mitigated by the engineer in the team. After victims are found, their condition needs to be treated on-site before they can be carried out of the building. This requires the presence of the medic, the only member with sufficient medical expertise. It is also worth noting that victims require different treatment according to their injury types, either abrasions (A), bone damage (B), or critical condition (C). Victims that suffered the former two types of injury are also referred to as regular victims, as their condition can be treated by the medic alone. On the contrary, stabilizing a critical victim requires both the medic and another team member to be present. After the pre-condition of stabilization is met, it is the transporter’s job to move fast and carry the victim to the correct evacuation zones.

Figure 3.1 shows a grid-world representation of the map, which we will refer to as the Saturn map, used for this mission.

From the perspective of a USAR mission, the performance of the team should be evaluated by the weighted sum of the number of victims evacuated to the correct zone. The team is rewarded with 10 points for each regular victim it evacuated. Meanwhile, as evacuating a critical victim demands more close collaboration between
the teammates, they are worth 50 points each. For the reinforcement learning agents, these scores are only reflected in the reward function of the participant who is directly responsible for transportation. Thus, we also issue intermediate rewards to help other participants identify desirable behavior, as shown Table 3.1. To distinguish between the RL-reward function and the actual task performance, we will refer to the team score as the M1 metric.

<table>
<thead>
<tr>
<th>Event</th>
<th>Reward</th>
</tr>
</thead>
<tbody>
<tr>
<td>The engineer cleaned a rubble block.</td>
<td>1.0</td>
</tr>
<tr>
<td>The medic stabilized a regular victim</td>
<td>1.0</td>
</tr>
<tr>
<td>A participant picked up a stabilized regular victim</td>
<td>1.0</td>
</tr>
<tr>
<td>The medic stabilized a critical victim</td>
<td>1.0</td>
</tr>
<tr>
<td>A participant picked up a stabilized critical victim</td>
<td>5.0</td>
</tr>
<tr>
<td>A participant evacuated a regular victim.</td>
<td>10.0</td>
</tr>
<tr>
<td>A participant evacuated a critical victim.</td>
<td>50.0</td>
</tr>
</tbody>
</table>

Table 3.1: Reward signals.

Furthermore, we investigate several variants of the general mission context discussed above. For example, in Chapter 4 only the transporter is allowed to carry an victim. In Chapter 5, all roles may carry an victim, but the maximum moving speed of a participant varies based on their roles: the transporter moves significantly faster than the other participants, whereas the engineer moves the slowest. These variations will be discussed in more detail in the following chapters.

At the end, we make the assumption that communication infrastructure remains functional following the disaster, such that MARL agents may freely share knowledge as they please. Thus, we compare our proposed architecture with previous literature equipped with both implicit and explicit communication mechanisms (in Section 4.3). Moreover, partial observability heavily applies in our task setting. As discussed in the introduction, we provide global states (during training) only for our benchmarking literature, in the manner they see fit.
3. Task Formulation
Chapter 4

Marcomanagement

4.1 Graph-based Environment Simulator

The graph-based environment\(^1\) aims to simulate the USAR task at the room level. Each room or corridor segment is represented with a node in the graph, whereas (non-directional) graph edges show connectivity.

4.1.1 State Space

The global state \(s \in S\) and agent-role mapping \(C\) are represented with a dictionary with entry sizes:

- **graph**: \(s_g \in \mathbb{R}^{G \times (f_n + N)}\)
- **agent**: \(s_a \in \mathbb{R}^{N \times (f_a)}\)

where \(G\) is the number of nodes, \(N\) is the number of agents, and \(f_n\) is the dimension encoding a node. \(f_a = f_i + C\) where \(C\) is the number of roles and \(f_i\) is the number of injury types. The **graph** entry encodes the content of each node, including the number of stabilized and unstabilized victims, evacuation zones of each injury type, the number of rubbles, and the whether a certain player is on this node. The **agent** entry encodes information that suffices to describe each agent, including its role and (if applicable) the victim’s injury type it is carrying. One-hot encoding is used in these features when appropriate.

\(^1\)https://gitlab.com/cmu_asist/gym_graph
4.1.2 Observation Space

Upon calling the step function of the environment, a dictionary with the following optional keys is returned for each agent, e.g., agent $i$:

- $\text{obs: } o^{(i)} \in \Omega$ is a dictionary in the same fashion as $s$:
  - $\text{graph: } o^{(i)}_g \in \mathbb{R}^{G \times f_g}$
  - $\text{agent: } o^{(i)}_a \in \mathbb{R}^{f_a}$

where $f_g = f_n + 1$ is notion of the encoding dimension of each node. The additional dimension indicates whether agent $i$ is in this room. In addition, the agent entry only contains information regarding the corresponding agent and thus is one-dimensional. Furthermore, the visibility mask $O(s, \cdot)$ is constructed in a way to mimic the challenging limitations encountered in real-world USAR tasks. All information in the graph entry will be masked to zeros except for the agent’s current room, effectively making it one-hot along the rows.

- $\text{agent_id}$, which is a one-hot vector $i^{(i)}$ encoding the agent’s identity $i$. This is not used by our model but provided for benchmarking literature that adopt plain agent indexing.

- $\text{action mask}$, which is the multi-hot vector $M^{C(i)}(s, \cdot)$ indicating the agent’s current action space. We will use $m^{(i)} \in \{0, 1\}^{|A|}$ to denote this vector.

Both the states and observations are normalized to $[0, 1]$ channel-wise.

4.1.3 Action Space and Dynamics

The size of the action space is $|A| = |A_0| + |A_e|$, where $|A_0| = G + 1$ is the number of actions available to all roles and $|A_e| = \bigcup_c |A_c^{(c)}|$ is the total number of role-specific actions. Among the $G$ navigational actions, only the nodes adjacent to the current room are available. As a node is not considered as its neighbor, an agent must explicitly call the still action to keep waiting in the current location. The role-specific actions, which describe interactions between the agent and room contents, include clean, stabilize, pick and evacuate. clean is unique to the engineer, stabilize is unique to the medic, and the last two actions are unique to the transporter. Note that if rubbles exist in a room, they must be cleaned by the engineer before any other
interactions with the room content.

We study the USAR problem where the building structure prior to the disaster is known and fixed, but agents will encounter path-blocking rubbles that have collapsed to random locations. The locations of victims and evacuation zones are also unknown to the agents in advance. These variables, along with the initial locations of agents, will be randomized for each episode to avoid memorization.

4.2 Algorithms

Figure 4.1 shows the proposed actor-critic algorithm. The network is shared among all agents. Superscripts that indicate timestamp or agent identity are omitted where obvious.

At each timestamp $t$, the environment returns the dictionary:

$$\{i : (o_g^{(t,i)}, o_a^{(t,i)}, m^{(t,i)}) \forall i\} \tag{4.1}$$

An arbitrary agent $i$ first receives communication $\{o_g^{(t,j)} \forall j \neq i\}$ from all other agents, then merge them with its own observation with max pooling:

$$\bar{o}_g^{(t,i)} = \max_{1 \leq j \leq N} \{o_g^{(t,j)}\} \tag{4.2}$$
The observation scheme described in Section 4.1 ensures that agents will not suffer from outdated knowledge from a peer that failed to comprehend this non-stationary environment, as opposed to memory-based communication like [75]. However, the merged observation is still highly sparse: only \( N \) out of \( G \) entries in \( \bar{o}_{g}^{(t,i)} \) are non-trivial. This is an undesirable behavior, as the contents \( \bar{o}_{g}^{(t,i)}(p) \in \mathbb{R}^{f_{g}} \) of an arbitrary node \( p \) should correlate with the value of not only itself but also its neighborhood \( \mathcal{N}(p) \). Therefore, we apply a graph attention network [106] to integrate features over the environment graph.

For node \( p \), the corresponding output feature from the attention layer is:

\[
\bar{o}_{g}^{(t,i)}(p) = \sum_{q \in \mathcal{N}(p) \cup \{p\}} \alpha_{p,q} W \bar{o}_{g}^{(t,i)}(q)
\]  

(4.3)

where \( W \in \mathbb{R}^{f_{g} \times f_{g}} \) is a weight matrix shared across this graph attention layer, and the normalized attention coefficient \( \alpha_{p,q} \in \mathbb{R} \) between node \( p \) and \( q \) is computed as:

\[
\alpha_{p,q} = \frac{\exp(e_{pq})}{\sum_{r \in \mathcal{N}(p) \cup \{p\}} \exp(e_{pr})}
\]  

(4.4)

where the raw attention coefficient \( e_{p,q} \in \mathbb{R} \) is computed with linear weights \( a \in \mathbb{R}^{2f_{g} \times 1} \):

\[
e_{p,q} = \text{LeakyReLU} \left( a \cdot [W \bar{o}_{g}^{(t,i)}(p) \Vert W \bar{o}_{g}^{(t,i)}(q)] \right)
\]  

(4.5)

which indicate the importance of node \( q \)’s contents to node \( p \). As adopted by [106], attention is conducted over the first-order neighborhood of \( p \) including the node itself, which corresponds to graph-navigation action space \( A_{o}(s^{(t)}) \). Compared to literature that compute agent-wise importance scores [42, 58], such a room-wise importance fits better to our task involving merely three agents but a large graph structure.

We also improve plain agent-indexing to attentively identify transferable knowledge. Under the scheme of agent indexing, the policy model is guaranteed to perceive unequal input \( \{o, i\} \) for different agents, even though the raw observation \( [o^{(i)}, ...] \) from the environment could be similar. The benefit of doing so is that it causes agent-specific hidden states to be deduced within a fully shared policy network, thus allowing for heterogeneous behavioral traits. However, sub-optimality exists in this approach. Suppose an optimal joint policy \( \Pi^{*}(A | \prod_{i} o^{(i)}) \) exists for our setup. The goal of
training a shared and indexed policy model $\pi_{\theta}(a|o,i)$ is to satisfy:

$$\prod_i \pi_{\theta}(\cdot|o^{(i)},i^{(i)}) = \Pi^*(\cdot|\prod_i o^{(i)}) \quad (4.6)$$

Consider the case where agents share similar optimal behavior:

$$\exists s \in \mathcal{S}, o \in \bigcap_i \Omega^{C(i)}(s), a \in \bigcap_i \mathcal{A}^{C(i)}(s) : \left\{ \forall i, o^{(i)} \in \Omega^{C(i)} \implies o = \prod_i a \right\} \quad (4.7)$$

In this case, despite the joint optimal controller’s input consisting of identical components $o$, the input to the parameterized shared model $\pi_{\theta}$ still differs for each agent.

$$\forall 1 \leq i, j \leq N : i \neq j, \{o^{(i)}, i^{(i)}\} \neq \{o^{(j)}, i^{(j)}\} \quad (4.8)$$

Furthermore, the component that causes such a difference are agent-wise orthogonal: $i^{(i)} \perp i^{(j)}$, which requires the shared model to find adequate weights $\theta$ that deactivates $\forall i$ for all observations-action pairs $(o, a)$ that satisfy Equation 4.7. While it is possible to approximately do so with a sufficiently large neural network, we argue that this learning paradigm can be improved by conditioning the model with action mask $m^{(i)}$ that denotes $A^{C(i)}(s)$. This is because the optimal joint policy may only appear homogeneous at the intersection of role-specific action spaces $\cap_i A^{C(i)}(s)$. For all cases that satisfy Equation 4.7, inputs to the new model have a greater similarity:

$$[o^{(i)}(s), m^{(i)}(s)] \cdot [o^{(j)}(s), m^{(j)}(s)] = o \cdot o + m^{(i)}(s) \cdot m^{(j)}(s)$$

$$\geq \|o\|^2 + \frac{\big|\cap_i A^{(c)}(s)\big|}{|A|}$$

$$> \|o\|^2 - [o^{(i)}(s), i^{(i)}(s)] \cdot [o^{(j)}(s), i^{(j)}(s)] \quad (4.9)$$

Without loss of generality, this argument of similarity improvement can be extended to cases where $o^{(i)} \neq o^{(j)}$, but the desired action are still the same for all agents. This fits into our environment that contains agent-specific states $o_a^{(i)}$.

As such, outputs of the GAT layer will be concatenated with the transformed agent-wise observation and the current action space availability indicator:

$$x^{(t,i)} = \text{MLP}_g \left(o_g^{(t,i)} \right) \| \text{MLP}_m \left(m^{(t,i)} \right) \| \text{MLP}_{a_1} \left(o_a^{(t,i)} \right) \quad (4.10)$$
4. Marcomanagement

We use the traditional [3] and effective practice of using Long Short Term Memory (LSTM) to capture history dependency. For the current timestamp, the output feature is the hidden state $h^{(t,i)}$ where:

$$h^{(t,i)}, c^{(t,i)} = \text{LSTM} (x^{(t,i)}, h^{(t-1,i)}, c^{(t-1,i)})  \quad (4.11)$$

All layers up to now are reused between the actor and the critic. It has been empirically observed that parameter sharing in this way helps deep models learn at early stages [1]. We apply two final linear layers to obtain the scalar value estimate and the current action distribution, from which we sample an action to execute:

$$\begin{cases} V^{(t,i)} = \text{MLP}_q(h^{(t,i)}) \\ a^{(t,i)} \sim \pi_\theta^{(t,i)} = \text{MLP}_{a2}(h^{(t,i)}) \end{cases}  \quad (4.12)$$

The method we use to obtain the policy gradient falls in the framework of advantage actor-critic [67], in which we adopt the generalized advantage estimator (GAE) [88]. At each timestamp $t$, the TD residual of $V$ is defined as:

$$\delta^{(t,i)} = r^{(t,i)} + \gamma V^{(t+1,i)} - V^{(t,i)}  \quad (4.13)$$

and the generalized advantage is:

$$A^{(t,i)} = \sum_{l=0}^{T-t} (\gamma \lambda)^l \delta^{(t+l,i)}  \quad (4.14)$$

where $T$ is the length of the episode and $\lambda = 1$ for unbiased estimation. The policy gradient can be thus calculated as:

$$\nabla_\theta J(\theta)^{(i)} = \sum_{t=0}^{T} \nabla_\theta \log \pi_\theta^{(t,i)} A^{(t,i)}  \quad (4.15)$$

where $\theta$ denotes trainable parameters in Figure 4.1.
4.3 Experiments

4.3.1 Baselines

We compare the performance of our algorithm against four baselines:

- **CommNet [98]**, where communication to agent $i$ is the mean of hidden states from all other agents $\forall j \neq i$. The averaged message will be used as additional input channels to the agent’s policy network.

- **G2ANet [58]**, where the interaction relationship between an arbitrary agent pair $i$ and $j$ is modeled with a bi-directional recurrent layer following Gumbel softmax. The output will then be used as scaling factors in dot-product attention between the hidden states of $i$ and $j$. Thus, their approach can be seen as applying attention over the graph of agents, where edges are weighted by the bi-directional GRU/LSTM that inputs features from corresponding agent nodes.

- **QMix [83]**. As discussed in Section 2.3.1, this method learns a monotonic mixer network to link agent-specific Q-value estimates with the centralized estimation. It also adopts the state-based CTDE paradigm that assumes access to true global states during training.

- **Maven [63]** improves QMix by introducing a latent variable $z$ that conditions individual action-value estimators, where different $z$ values map to different exploration traits. Global states are also required for the $z$-generator and the discriminator that models the variational distribution $q_v(z|\sigma(\tau))$.

As discussed above, the first two baselines rely on explicit communication. We choose them to demonstrate the benefits of utilizing attention-based communication over the environmental structure. Meanwhile, we selected the other two baselines to show that our algorithm may outperform methods that exploit training-stage global states. Moreover, all four baselines adopt the parameter sharing paradigm with plain agent-indexing; as opposed to our proposed action-dominant identification mechanism. We will benchmark our proposed approach against the baselines and conduct ablation studies to show the effect of each sub-module.
4. Marcomanagement

4.3.2 Results and Discussions

In this section, we quantify team performance using the final M1 score discussed in Section 3.2. We split the Saturn map in Figure 3.1 into three subdivisions with different graph structures, as shown in Figure 4.2:

- The left region with 28 nodes (12 of which are blocked by a total of 19 rubbles) and 33 edges. This environment has 12 victims, resulting a total M1 of 320.
- The middle region with 29 nodes (13 of which are blocked by a total of 22 rubbles) and 29 edges. This environment is the most sparse in terms of victim distribution, containing 9 victims and a total M1 of 210.
- The right region with 23 nodes (13 of which are blocked by a total of 15 rubbles) and 24 edges. 14 victims are trapped in this environment, including a room with three critical victims worth 150 M1 scores. The total M1 available in this environment is 420.

The same discount factor $\gamma = 0.7$ is used in all environments. Each episode contains 400 steps, and room contents are randomly permuted across episodes. In addition, shades in the following result plots indicate the 95% confidence interval.

Figure 4.3 demonstrates that our method outperformed baselines in all three map settings. Our model performed particularly well in the right-most region that bias
4. Marcomanagement

We observed that MAVEN, which has a theoretical advantage over QMix, outperformed the latter approach in all scenarios. However, they still performed significantly worse than communication-based architectures. The main reason behind this phenomenon is not insufficient replay buffer size or poor choices of other hyperparameters, but the fact that observations are highly sparse. We demonstrate so by providing global states to MAVEN as additional inputs during both training and evacuation. The model architectures remain the same except for the number of input channels. As shown in Figure 4.4, the (mostly) identical architecture and hyperparameter choices could effectively learn a good mapping from \((s, o)\) to \(a\), but were unable to address the strong partial observability in USAR tasks. Thus, we argue that explicit communication schemes should be applied when the task setup allows execution-stage information exchange.

We also notice that G2ANet outperformed CommNet in all environments, and the difference is most significant in the middle one. As successful victim evacuation relies on multiple preconditions, we plot the performance of individual tasks in Figure 4.5. All three algorithms were able to clean almost all rubbles, as shown in Figure 4.5a. However, CommNet failed to effectively accomplish secondary tasks that require more team collaboration. Figure 4.5c shows how the ability to stabilize critical victims is strongly correlated with the eventual task performance.

Figure 4.3: Performance in the marcomanagement task.

Figure 4.4: Impact of partial observability on MAVEN.
4. Marcomanagement

- (a) Rubble Cleaning.
- (b) Regular Victim Stabilization.
- (c) Critical Victim Stabilization.

Figure 4.5: Performance in preconditions - Middle Map.

Moreover, we conduct ablation studies regarding the communication mechanism to see how it contributes to the overall excellence of the proposed architecture. As shown in Figure 4.6, communication between agents reduced variance because the learner now perceives a more stationary environment. This effect is more significant in the left and middle maps, leading to not only variance reduction but also more optimal convergence. This is because their underlying graph structures are more complex and victims are more sparsely distributed. Meanwhile, Figure 4.7 shows how information regarding an agent’s action space can be used as a strong indicator of the essence of that agent, which greatly stabilized training.

Figure 4.6: Ablation studies - Communication

Figure 4.7: Ablation studies: Agent-indexing schemes.
We also show how the attention mechanism helps coordination. Let us revisit the notation in Section 4.2 where \( p \) denotes an arbitrary node and \( q \in Q_p = \mathcal{N}(p) \cup \{p\} \) belongs to its neighborhood; \( W \in \mathbb{R}^{f_g \times f_g} \) denotes the linear weights that encodes graph features, and \( a = [a_P; a_Q] \in \mathbb{R}^{2f_g \times 1} \) is the attention layer’s weights shared for all pairs \((p, q)\). From Equation 4.5, we can construct the vectors:

\[
\begin{align*}
W_P &= W^\top a_P \in \mathbb{R}^{f_g \times 1} \\
W_Q &= W^\top a_Q \in \mathbb{R}^{f_g \times 1}
\end{align*}
\]  

(4.16)

such that the raw attention coefficients \( e_{p,q} \) indicating the importance of node \( q \)'s contents to the current node \( p \) can be computed as:

\[
e_{p,q} = \text{LeakyReLU} \left( W_P^\top \bar{o}_g(p) + W_Q^\top \bar{o}_g(q) \right), \quad \forall q \in Q_p
\]  

(4.17)

Here, \( W_Q \) explains how any node values its neighbors by feature dimensions. Meanwhile, note that \( W_P^\top \bar{o}_g(p) \) only encodes contents of the current node \( p \), thus serves as a bias term uniform to all neighbors of \( p \). Because of the structure of the LeakyReLU activation, \( W_P \) declares what node \( p \) should contain so that the attention mechanism will examine the neighborhood of \( p \) more precisely. Given \( W_Q \bar{o}_g(q) \), if the feature distribution of node \( p \) has a (sufficiently) higher similarity with \( W_P \), the resulting greater dot-product \( W_P^\top \bar{o}_g(p) \) will cause more \( z_q \equiv W_P^\top \bar{o}_g(p) + W_Q^\top \bar{o}_g(q) \) to be greater than 0. Because more \( z_q \) values will be activated (by a unit tangential \( 1 > \alpha \)), the pairwise distances between \( e_{p,q} \) will be greater, leading to greater pairwise distances between \( \alpha_{p,q} \) and closer discrimination upon the neighborhood. Also, note that higher overall \( e_{p,q} \) caused by an increase \( W_P^\top \bar{o}_g(p) \) would not cause the network to put uniformly more attention to all neighbors, as the actual attention coefficients \( \alpha_{p,q} \) are subject to the SoftMax normalization with translation invariance.

We plot \( W_P, W_Q \), each independently normalized, with feature labels in Figure 4.8. It is immediately observed that the network cares to closely examine the neighborhood only when unstabilized critical victims are present in the current room \( p \). This phenomenon matches our intuition, as stabilizing a critical victim is the only atomic action that demands collaboration (Section 3.2). The network, upon seeing an unstabilized critical victim, will try to search for agents in adjacent rooms and instruct them to come and help. This is also reflected in \( W_Q \), as the model cares
4. Marcomanagement

Figure 4.8: Attention to feature dimensions. Weights are extracted from the model trained for 100 million steps in the Saturn-right map.

whether an arbitrary agent resides in the neighboring rooms. In addition, we observed that rubbles in the neighboring rooms are also closely attended to. We hypothesize that this is because rubble cleaning is a task valuable in both the short-term (easy rewards that can be achieved at the cost of only one agent-step) and the long run (cleaning is essential to allow for future task execution).
Chapter 5

Micromanagement

5.1 Grid-based Environment Simulator

For the task of micromanagement, we developed a testbed\(^1\) that provides observation spaces with a 1m × 1m resolution and action spaces transferable across participants.

5.1.1 State and Observation Space

The global state \(s \in S\) and agent-role mapping \(C\) are represented together with an array in shape \((\text{ROW}, \text{COL}, 6)\). The observation \(o^{(t,i)} \in \Omega\) is filtered from \(S \cup C\) by a Boolean visibility mask with a 51° field of view. Walls and rubbles that are at least two meters tall would cause occlusion, as shown in Figure 5.1. For RL-based agents, they are normalized to \([0, 1]\) channel-wise, whereas planning-based agents perceive the raw uint8 encoding.

5.1.2 Action Space and Dynamics

The action space \(A\), which contains \text{still}, \text{forward}_1, \text{forward}_2, \text{forward}_3, \text{turn}_\text{left}, \text{turn}_\text{right}, \text{toggle}, \text{pick}_\text{up},\) is uniform to all agents. The purposes of the first six navigational actions are self-explanatory. In addition, all agents in the grid-based environment may pick up a stabilized victim and carry it to the

\(^1\)https://gitlab.com/cmu_asist/multigrid-with-3-roles
5. Micromanagement

![Image](image_url)

Figure 5.1: Visibility masks that overlay the global map. Light Grey indicate that the block is within an agent’s field of view.

Evacuation zone; or relocate a regular victim for the convenience of other agents. Heterogeneity regarding evacuation is modeled with role-specific speeds described in Table 5.1. Furthermore, in order to decouple heterogeneous behavior from the action space, every role has the permission to call for any of the forward actions. The environment will ensure that the expected value of an agent’s speed is consistent with its corresponding fractional speed limit.

<table>
<thead>
<tr>
<th>Role</th>
<th>Carrying a victim</th>
<th>Not carrying a victim</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medic</td>
<td>2.374</td>
<td>4.317</td>
</tr>
<tr>
<td>Engineer</td>
<td>2.374</td>
<td>3.669</td>
</tr>
<tr>
<td>Transporter</td>
<td>5.180</td>
<td>5.180</td>
</tr>
</tbody>
</table>

Table 5.1: Traveling speed [m/s] of each role. The environment operates at 4Hz.

The **toggle** action is used as the main interaction method with the facing block, and should be called for a medic to stabilize an injured victim, for an engineer to clean a rubble block, or for a transporter to evacuate a stabilized victim being carried. If an agent with a role incompatible with the current facing block calls **toggle**, the environment will ignore its behavior or optionally return a small negative reward. This deliberately ambiguous **toggle** action lead to role-specific dynamics:

\[
\forall 1 \leq c_1, c_2 \leq C : c_1 \neq c_2, \exists s, s' \in S : T^{(c_1)}(s, \text{toggle}, s') \neq T^{(c_2)}(s, \text{toggle}, s') \quad (5.1)
\]

Meanwhile, such ambiguity can be handled by the environment without collision.
5. Micromanagement

A separate action, pick up, is introduced in case a medic hopes to move a regular victim that has yet been stabilized. In addition, note that the reward structure stays homogeneous over roles, given any tuple \((s, a, s')\).

5.1.3 Optional Features

The grid-based simulator has the capability to mimic the 3D Minecraft testbed for human trials (Appendix A) to the fullest extent possible. These optional features are only used for planning-based agents. Below is a non-comprehensive list:

- Enlarged Action Space: A swap action is introduced to address the issue with a discretized 2D testbed, which can be called when a participant, who is already carrying a victim, finds its path blocked by a movable victim. The action would swap the location of this participant with the movable victim, which can be done in a few steps in the 3D testbed. Also, a forced drop action can be called when a participant chooses to drop a victim at the evacuation location, with no regard for the injury types. On the contrary, calling toggle when facing a wrong-typed evacuation block would prevent the participant from dropping the victim, as if the participant noticed the no-change in the scoreboard in the 3D testbed.

- Collapse during the mission: as the building structure is unstable following the earthquake, agents may accidentally trigger secondary collapse while attempting the rescue. When enabled, new rubbles would fall and block the agent’s path out, trapping it until the engineer came to help. This calls for closer collaboration between team members.

- Task-based visibility mask: non-medic participants cannot differentiate between abrasion and bone damage victims, and they will have no access to any injury types after a victim has been stabilized. Moreover, collapse traps (not common rubbles) cannot be seen by any participants once the task has started, although the engineer has room-level prior knowledge regarding these traps.

- Marker blocks: to address the constraint discussed above, a medic may place marker blocks indicating injury types. These markers are globally visible (independent of the visibility masks), in order to mimic the dynamic map in
5. Micromanagement

the 3D testbed.

- Beep signals: the transporter may request for extra information when stepping on a trigger block. The environment would then return whether non-stabilized regular or critical victims are in the corresponding room.

5.2 Algorithms

For decision-making in the micromanagement scenario, we first adopt the paradigm of online reinforcement learning, like what we did in Chapter 4. We use a CNN shared between the actor and the critic to extract features from image-like observations. We then feed the features to two MLP branches separated for the value function and the actor head. The entire network is shared among all agents with no additional regard to their identity. Furthermore, we use the same mechanism discussed in Section 4.2 to estimate advantages and calculate the policy gradient.

In order to use imitation learning for our USAR mission, we develop a hierarchical controller equipped with structured communication protocols [72]. A priority queue is maintained to host communication instances. Agents may request each other to gather, clean rubbles, move victims, query for information, or respond to previous requests. An agent, upon receiving an action-related request, will compare it with the current task in-execution and decide accordingly. Meanwhile, an agent at ease would search in its internal belief system for the most valuable room-level action with exponential exploration. The room-level action would be translated to a Boolean mask of target grid-level locations, from which A* planning [38] is applied for navigation. In addition, in order to address the non-stationarity encountered with independent execution with insufficient knowledge sharing, agents will have an increasing tendency to revisit states that deemed invaluable according to its memory. Figure 5.2 shows the structure of the proposed planning-based agents.

The non-Markov experts that rely on a shared communication queue can be modeled with a joint policy \( b(A|O, h) \), where \( O \in \prod_i \Omega^{C(i)} \), \( A \in \prod_i \mathcal{A}^{C(i)} \) are joint observations and actions. We use the expert policy to roll out episodes with observation-action pairs \( \{(O(t), A(t))\} \), and decompose them back to the individual representation of \( \{(o^{(t,i)}, a^{(t,i)})\} \). Using the expert trajectories as ground truth, we apply supervised
learning to optimize for the IL-agent’s policy network:

$$\min_{\theta} - \sum_{i,t} \log \pi_{\theta} (a^{(t,i)} | o^{(t,i)})$$

(5.2)

where $\pi_{\theta}$ has an identical network architecture as the actor used in online RL, for the sake of a fair comparison.

We also consider the goal of forecasting human performance, in terms of the M1 metric introduced in Section 3.2, in two time scales. Let $m^{(t)}$ denote the cumulative M1 score at timestamp $t$. Given the sequence $\{m^{(0)}, ..., m^{(t)}\}$, we are to infer either the short-term progression $m^{(t+\Delta t)}$ or the eventual outcome $m^{(T)}$. We address this sequence modeling problem with a transformer encoder [105] exploiting multi-head self-attention. The transformer is fed with aggregated features of the trajectory to reduce the demand for computational resources. Moreover, we consider a baseline step-wise MLP model that does not consider time dependency. We use this baseline to evaluate the necessity of using the data-intensive transformer architecture.

Figure 5.2: Hierarchical planning agents.
5. Micromanagement

5.3 Experiments

5.3.1 Decision-Making

Experiment Design

The grid-based environment simulator supports multiple randomization levels. More stochasticity, \textit{e.g.}, to permute the location of all elements except for the building structure, leads to a higher requirement for the expressivity of the network. Meanwhile, a less randomized environment may require the engineer to clean rubbles prior to victim stabilization, posing a stricter requirement for team collaboration. In this section, we select four representative configurations, as shown in Figure 5.3, and see how randomization levels affect the performance of RL and IL models. We generated 2000 expert trajectories for each of these environment configurations.

Results and Discussions

Figure 5.4a shows how the online RL paradigm learns to improve episodic rewards. However, such improvements were mainly contributed by the engineer’s increasing ability to clean rubbles, as shown in Figure 5.4b. As rubble-cleaning is a task that can be accomplished by the engineer alone without any pre-conditions, limited team collaboration was achieved in the online RL setup. This is reflected in Figure 5.4c and 5.4d. The shared policy never learned to stabilize victims exceeding the extent of random walking, let alone to evacuate them afterward. One explanation for this phenomenon is action space ambiguity. The \texttt{toggle} action presented to the policy network corresponds to two unbalanced underlying tasks: rubble cleaning and victim stabilization. As the number of rubbles greatly exceeds the number of victims, the shared policy network perceived the sparse occasions of victim stabilization as noise, thus failing to optimize in that direction meaningfully. A potential solution within online RL is carefully handcrafting the reward structure and reducing the rewards associated with rubble cleaning.

Figure 5.5 demonstrates the benefits of imitating faux-human trajectories over purely online RL. It is shown that IL managed to accomplish the entire decision sequence of cleaning-stabilizing-evacuation, despite the same network architecture
5. Micromanagement

Figure 5.3: Four randomization levels in the top-left region of Saturn. The initial agent locations are always randomized. Environment dimension: $17 \times 28 \times 6$. Maximum $M1: 120$.

being used by both learning schemes. Meanwhile, the agents’ performance was subject to environment configurations. As shown in Figure 5.5b, posing a hard constraint on team collaboration would decrease the cumulative $M1$ metric by a minor margin. Regarding the topic of randomization, it is shown that agents were able to mitigate challenges associated with randomized victim locations. However, when the locations of rubbles and evacuation zones were permuted across episodes as well, a significant performance reduction was observed. This could be explained by two hypotheses. Either a) the representation power of the policy network or b) the size and variance of the expert dataset were insufficient for the more sparsely distributed observation space. As issues caused by insufficient expert demonstrations and distribution shifts
5. Micromanagement

(a) Rewards received.

(b) Rubbles cleaned.

(c) Regular victims stabilized.

(d) Critical victims stabilized.

Figure 5.4: Details regarding online RL.

(a) Online RL.

(b) IL.

Figure 5.5: Comparison between online RL and IL over end-of-episode performance, in the environment shown in Figure 5.3.
5. Micromanagement

were commonly observed in behavior cloning applications, the latter hypothesis is more likely to have played a more significant role.

5.3.2 Forecasting Human Performance

Experiment Design

In this section, we use the full-sized Saturn Map as shown in Figure 3.1 with optional features in Section 5.1.3 enabled. The duration of the mission is 15 minutes, which translates to 3600 steps in the environment. Our collaborators [19] first conducted 12 human trials in an equivalent environment, which will be referred to as $D_h$. We use the observations and statistics from $D_h$ to configure our faux-human agents, and roll out 3000 episodes denoted as $D_f$. After the faux-human dataset was collected, our collaborators collected 32 human trials, denoted as $D_{vh}$, with the same condition as $D_h$. They collected more 184 human trials, denoted as $D_{vi}$, where participants receive external guidance. Thus, $D_h$ and $D_{vh}$ should follow a similar distribution, where $D_h$ and $D_{vi}$ are likely to follow different distributions. The rationale of such a data split is discussed in Appendix A.

Under these preparations, we consider two experimental designs. Firstly, we study the effect of adopting synthetic data at an early stage of design iterations. For this purpose, we train the prediction models with either $D_h$ or $D_f$, and evaluate the models with $D_{vh}$ that is made available after the training sets. Secondly, we investigate whether synthetic data effectively span the policy space, such that they can be used to bridge the gap in human data caused by assistive robots or human advisors. In this case, we train the predictors with either $D_{vh}$ or $D_{vh} \cup D_f$, and evaluate the models with $D_{vi}$. Furthermore, each of these two settings involves both the short-term ($\Delta t = 60s$) and long-term prediction tasks.

To measure the performance of prediction models, we report the root mean square error (RMSE) between prediction and ground truth as the y-axis in the following figures. Because the synthetic dataset is significantly larger in size than human datasets, plotting errors against trained epochs would exaggerate the advantages of using synthetic data. Thus, we trained the models concurrently on the same devices and use training time as the x-axis.
5. Micromanagement

Figure 5.6: Long-term prediction model: $D_h | D_f \rightarrow D_v h$.

Figure 5.7: Short-term prediction model: $D_h | D_f \rightarrow D_{vh}$.

Results and Discussions

Figure 5.6 and 5.7 compare training with synthetic data vs. training with limited human data collected for early design choices. Figure 5.8 and 5.9 demonstrate the impact of augmenting the non-advisor human datasets with synthetic data. While introducing the faux-human dataset reduced validation error in all four configurations, we observed that performance improvement is more significant in long-term prediction tasks. This is because long-term prediction is modeled as a (simpler) sequence-to-one problem, leading to a higher chance of overfitting. As shown in Figure 5.6, when trained on the limited human dataset $D_h$, the model would quickly overfit after 30
5. Micromanagement

Figure 5.8: Long-term prediction model: $D_{vh} | D_f \cup D_{vh} \rightarrow D_{vi}$.

Figure 5.9: Short-term prediction model: $D_{vh} | D_f \cup D_{vh} \rightarrow D_{vi}$.

minutes of training. Meanwhile, as the tendency of overfitting is insignificant in the sequence-to-sequence problem of short-term prediction, the main benefit of adopting the synthetic dataset is that it helps stabilizes the transformer. Figure 5.7 and 5.9 show how training with human data only leads to a higher variance in training RMSE.

Figure 5.10 presents the comparison between the transformer and the baseline MLP model, where the latter one holds 65% less trainable parameters. Whether synthetic data is used or not, it is shown that the ability to consider time dependency is vital for the long-term task, resulting in lower training and validation RMSE. This invalidates the counterargument that relatively worse performance from training on
5. Micromanagement

Figure 5.10: Comparison between MLP and Transformer for long-term prediction.

human data alone can be addressed by plainly switching to a simpler model. Thus, we argue that applying data-intensive sequential models together with synthetic data is an adequate approach for human performance forecasting.
Chapter 6

Conclusion

In this thesis, we studied the task of coordinating a heterogeneous team in urban search and rescue (USAR) missions. For this purpose, we developed two USAR environment simulators that support role-specific action spaces or transition dynamics. We applied the graph attention mechanism to exploit environment structures and achieve effective communication among a small group of rescue workers. We showed that the proposed approach outperformed previous state-of-the-art literature that also rely on graph attention by a significant margin. In addition, we designed a series of faux-human agents that vividly mimic human behavior in USAR. We demonstrated how they could be used as experts in imitation learning to address action-space ambiguity. In the end, we showed that our artificial datasets addressed human data scarcity. We reduced the inference error of human cognitive models by half via this method of data augmentation.
6. Conclusion
Appendix A

Acquiring Human Data

Our collaborators [19, 29] developed a 3D synthetic environment for USAR using Minecraft. Figure A.1 shows the bird’s eye view of the environment, whose map structure and transition dynamics are equivalent to those of our 2D grid-based simulator in Figure 3.1.

Participants are recruited from Arizona State University and social platforms, e.g., Reddit. They are physically located in the US, have reliable internet connections,
A. Acquiring Human Data

have experience playing Minecraft with a standalone mouse and keyboard, speak English, and have normal color vision. The recruitment excludes minors and prisoners. Furthermore, participants are asked to team with people who they do not know in advance, so as to control the variance in collaboration level.

Prior to a human trial, participants are subject to a 10-minute screening session to check their capability to play Minecraft. Following the screening session, teams of three qualified participants will receive training videos that introduce the rules of the task and provide hands-on experience with the environment. Each team will then participate in two seventeen-minute trials in the Minecraft simulator, where participants use the first two minutes to discuss strategy and the following fifteen minutes to execute the mission. Each participant perceives the partially observable interface as shown in Figure A.2. The right 60% of the screen shows the corresponding agent’s field of view, whereas the left 40% of the screen reflects the map structure of the environment.

A participant sees their own location on the dynamic map, but not the location of their teammates. To mitigate this visibility constraint and share other information, a participant may place marker blocks on the ground, which are also rendered in
A. Acquiring Human Data

Figure A.3: Marker Blocks

all teammates’ dynamic maps. These marker blocks can be used to indicate the injury type of a victim nearby, that the room is blocked by rubbles, that the room contains collapse threats, or if the room is empty. As shown in Figure A.3, they also reflect the identity of the marker-placer, where blue corresponds to Engineer, green corresponds to Transporter, and red corresponds to Medic. In addition to the marker blocks, participants may verbally communicate over zoom audio and use Minecraft chat channels.

One purpose of acquiring human trajectories is to support the development of assistive robots that issue reasonable interventions to improve human teamwork. Thus, as discussed in Section 5.3.2, human data are collected under different conditions:

- \( D_h \), which includes 12 trials collected at a pilot stage. This dataset is used to guide the early development of assistive robots (intervention modules).

- \( D_v \), which includes 184 trials collected after the development of assistive robots. The robotic advisors are deployed into the environment during these trials, where they issue interventions to human participants as they see fit.

- \( D_{vh} \), which includes 32 trials also collected after the development of assistive robots. However, the robots are deactivated during these trials, thus \( D_{vh} \) serves as the comparison group.
A. Acquiring Human Data
Appendix B

Implementation and Future Work

The Adam optimizer [50] is used to train all our models. In addition, the random seeds for the environment and MARL/MAIL/Inference algorithms are selected randomly from OS-provided system entropy, so as to avoid cherry-picked results.

B.1 Marcomanagement

The network architecture\(^1\) and hyperparameters used to obtain the main results are shown in Table B.1.

<table>
<thead>
<tr>
<th>Optimization &amp; Env.</th>
<th>Value</th>
<th>Network Architecture</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discount Factor (\gamma)</td>
<td>0.7</td>
<td>Attention Layers</td>
<td>2</td>
</tr>
<tr>
<td>Learning Rate</td>
<td>(10^{-4})</td>
<td>Attention Heads</td>
<td>1</td>
</tr>
<tr>
<td>Batch Size</td>
<td>200</td>
<td>LeakyReLU (\alpha)</td>
<td>0.2</td>
</tr>
<tr>
<td>Graph Channels (F_g)</td>
<td>14</td>
<td>Attention Output (F'_g)</td>
<td>14</td>
</tr>
<tr>
<td>Agent Channels (F_a)</td>
<td>6</td>
<td>LSTM Channels (F_h = F_c)</td>
<td>256</td>
</tr>
</tbody>
</table>

Table B.1: Hyperparameters for marcomanagement.

Moreover, the feature-embedding MLPs in Figure 4.1 following \(o'_g, o_a, m\) contain two consecutive linear layers with 256 output channels each. The value branch to estimate \(V\) is a linear layer (which has one output channel), and the policy branch to calculate the distribution of \(\pi(\cdot|\sim)\) is also a single linear layer.

\(^1\) Implemented at https://gitlab.com/cmu_asist/MARL-Heterogeneous
B. Implementation and Future Work

We conducted hyperparameter searches for $\gamma \in [0.5, 0.6, 0.7, 0.8, 0.9, 0.95, 0.99]$, the learning rate in $[10^{-3}, 10^{-4}, 10^{-5}]$, the training batch size in $[20, 200, 2000]$, the number of attention layers in $[1, 2, 3]$, and the number of attention heads in $[1, 2, 4, 8, 16]$. We observed that changing the order of the learning rate and batch size would cause the model to diverge or converge to local maxima. Among the rest hyperparameters, we observed that the discount factor $\gamma$ was the most important. Thus, we use the same discount factor $\gamma = 0.7$ for our baseline methods\(^2\) for a fair comparison.

Results in Chapter 4 are reported based on 10 evaluation episodes at each plotted point. The dense curves indicate the mean of evaluation episodes, whereas the shades represent the 95-th confidence interval bootstrapped from 20 up-samples.

### B.2 Micromanagement

The hyperparameters used to obtain the main results are shown in Table B.2.

<table>
<thead>
<tr>
<th>Optimization &amp; Env.</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discount Factor $\gamma$</td>
<td>0.7</td>
</tr>
<tr>
<td>Learning Rate</td>
<td>$10^{-4}$</td>
</tr>
<tr>
<td>Batch Size</td>
<td>200</td>
</tr>
<tr>
<td>Grid Width ROW</td>
<td>28</td>
</tr>
<tr>
<td>Grid Height COL</td>
<td>17</td>
</tr>
<tr>
<td>Input Channels</td>
<td>6</td>
</tr>
</tbody>
</table>

Table B.2: Hyperparameters for micromanagement.

The network\(^3\) contains four consecutive convolutional layers (with ReLU activations in between). The first one has a $3 \times 3$ filter and 16 output channels; the second one also has a $3 \times 3$ filter and 32 output channels; and the third one uses a filter, which has the same size as the input 2D grid, to map the image-like features to a $1 \times 1 \times 32$ output. The output is then fed into the final convolutional layer with a $1 \times 1$ filter to obtain the action probability distribution. As mentioned in Chapter 5, this architecture is used across both online RL and imitation learning.

\(^2\)The baseline methods were originally implemented by https://github.com/starry-sky6688/MARL-Algorithms. We applied necessary adaptions and bug fixes at our forked repository https://github.com/andromeda-0/StarCraft/releases/tag/v1.0.

\(^3\)Implemented at https://gitlab.com/cmu_asist/MAIL-Heterogeneous
B. Implementation and Future Work

We put careful consideration into the faux-human trajectories’ reproducibility. For each trial, a parent seed sequence is generated from OS-provided system entropy, then spawned into two child seed sequences to initialize the independent random number generators used by the grid-world environment and agents, respectively. This practice is known to avoid seed collision [37]. These seed sequences are saved together with environment and agent configurations, which fully suffice to reproduce any trial.

B.3 Predicting Human Performance

Both human data and synthetic data are parsed to time sequences with a frequency of 4 Hz. We consider the following input features at every timestamp:

- **positions** is a $3 \times 2$ array indicating the $x - y$ location of each agent.
- **ratio_unvisited** is the ratio of rooms that are yet visited by any agent.
- **time_in_seconds** is self-explanatory.
- **$\langle A \cup B \mid C \rangle\langle\text{discovered}|\text{moved}|\text{stabilized}|\text{signaled}|\text{evacuated}\rangle$$
  contains ten integers that indicate the task progress. Note that victim discovery is defined as the union of victim stabilization and signaling.

The network architecture$^4$ is as follows: the input features are flattened, concatenated, and fed into a linear layer with 64 output channels. The output, activated by a ReLU layer, is fed into a transformer encoder with dual-head attention and 256 output channels. In the end, the 256-dim vector is mapped to a scalar prediction with a linear layer. Meanwhile, the baseline MLP model replaced the transformer encoder with a linear layer (that has the same output channels) and a ReLU activation function.

B.4 Future Work

We acknowledge two aspects of future work:

- To outperform planning-based experts in the micromanagement task. A potential solution is to consider IL or offline RL as pre-training, where the models

$^4$Implemented at [https://gitlab.com/cmu_asist/Inference_Artificial_Trajectories](https://gitlab.com/cmu_asist/Inference_Artificial_Trajectories)
B. Implementation and Future Work

trained from offline demonstrations are further fine-tuned with online interactions with the environment \([30, 33, 82]\).

• To investigate the generalization capability in the macromanagement task. The graphs on which we experimented in Chapter 4 are sparse \((E \approx G)\) and contain at most thirty nodes. Can our proposed architecture demonstrate a similarly significant improvement over the baselines, in a larger or denser graph? In order to do so, we may need to increase the model capacity, \(e.g.,\), to use more attention heads to attend to different features in neighboring nodes. However, preliminary results suggested that the benefit of using plain dot-product multi-head attention is limited in our setup, despite its success in various domains \([24, 105]\). A potential solution is to regularize the model for higher diversity and sparsity among the attention heads \([20, 113, 124]\).
Bibliography


[17] Xiangxiang Chu and Hangjun Ye. Parameter sharing deep deterministic policy


[83] Tabish Rashid, Mikayel Samvelyan, Christian Schroeder, Gregory Farquhar, Jakob Foerster, and Shimon Whiteson. Qmix: Monotonic value function factorisation for deep multi-agent reinforcement learning. In International Conference on Machine Learning, pages 4295–4304. PMLR, 2018. 1, 2.2.1, 2.2.2, 2.3.1, 4.3.1


[126] Vittorio Amos Ziparo, Alexander Kleiner, Alessandro Farinelli, Luca Marchetti, and Daniele Nardi. Cooperative exploration for USAR robots with indirect