

Distributed Multi-Agent Decision Making Under Uncertain Communication

by

Cameron W. Pittman

M.A., Belmont University (2011)

B.A., Vanderbilt University (2009)

Submitted to the Department of Aeronautics and Astronautics
in partial fulfillment of the requirements for the degree of
Master of Science in Aeronautics and Astronautics
at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

September 2023

© 2023 Cameron W. Pittman. License: CC BY-NC 4.0,
<https://creativecommons.org/licenses/by-nc/4.0/>.

The author hereby grants to MIT a nonexclusive, worldwide,
irrevocable, royalty-free license to exercise any and all rights under
copyright, including to reproduce, preserve, distribute and publicly
display copies of the thesis, or release the thesis under an open-access
license.

Author
Department of Aeronautics and Astronautics
August 15, 2023

Certified by
Brian C. Williams
Professor of Aeronautics and Astronautics, MIT
Thesis Supervisor

Accepted by
Jonathan P. How
R.C Maclaurin Professor of Aeronautics and Astronautics, MIT
Chair, Graduate Program Committee

Distributed Multi-Agent Decision Making Under Uncertain Communication

by

Cameron W. Pittman

Submitted to the Department of Aeronautics and Astronautics
on August 15, 2023, in partial fulfillment of the
requirements for the degree of
Master of Science in Aeronautics and Astronautics

Abstract

As space exploration accelerates and the number of robots and humans working in extreme environments grows with it, we must enact autonomous multi-agent coordination in order to safely operate in environments that are inherently hostile to communication. To the best of our knowledge, there are no autonomous executives capable of coordinating with other agents while independently reasoning over communication delay to decide when to act. A key gap that must be addressed is a single-agent executive capable of deciding when to act given communication delay, which can form the basis for a multi-agent execution context. Existing research has provided insights into temporal reasoning, namely modeling observation delay and scheduling actions with temporal constraints, but there is both a need for deciding when to schedule events when there is uncertain observation delay, and a need to robustly coordinate between agents. Scheduling actions in the face of uncertainty is a challenge due to the compounding uncertainties of uncontrollable exogenous events, unknown observation delay, and uncertain communication between agents. This thesis puts forth a series of contributions that culminates in a robust single-agent executive demonstrated to run on real hardware with the ability to coordinate in a multi-agent context despite observation delay. Doing so required insights in checking variable-delay controllability, defining an execution strategy against temporal constraints with variable observation delay, and online coordination for multiple agents. We show that single agent online scheduler exhibits the expected performance characteristics, and demonstrate multi-agent execution with uncertain communication in the context of a simulated astronaut and robotic asset collaborating with communication delay.

Thesis Supervisor: Brian C. Williams
Title: Professor of Aeronautics and Astronautics, MIT

Acknowledgements

My journey to this SM thesis began eight years ago when I was a software engineer living in San Francisco. Two years prior, I had just wrapped four years of teaching high school science and didn't know how to code. I taught myself Python using MIT OpenCourseware on a whim because it was something I had always wanted to learn. Coding took over my life the first time I wrote a function. My first projects were physics demos and websites, but soon I learned I loved helping systems make decisions. And there is absolutely no system cooler than human spaceflight. So I sat there at my desk in SF and wondered, "I want to be a part of the next space race! What if I studied autonomy for human spaceflight? Where would I even go to learn autonomy?" (I didn't even know the field was called "autonomy" at the time.) Of course, MIT came up when I started searching. It took five more years of studying computer science, finding people to learn from, and integrating in the human spaceflight community, but eventually I found my way into AeroAstro and the MERS lab. It's been the journey of a lifetime and there's no way I would be here without the love and support from so many people.

First, I have to thank my amazing wife, Mo, who is the hardest working, most driven person I've ever met. She's been my biggest cheerleader and sounding board for my ideas (even when she has no idea what I'm talking about). Our newborn daughter, Catalina, is my inspiration. I think about her living in a world where there are thousands of people living and working in space. At the time of writing this, she's a month old and already making me work harder than I ever have. I never would have made it this far without a supportive family. My parents, Mark and Suzanne, and my brother, Max, have always been there for me.

My advisor, Brian Williams, has consistently surprised me with how much support he's freely given. Brian has been one of the most helpful people I've ever met, starting with the first time I introduced myself and blurted out, "hi, I'm taking your class and I think it's amazing and I want to use everything at work and can I please join your lab?" From academic mentoring, to brainstorming executive architectures, to

explaining basic concepts in temporal reasoning, to envisioning the next generation of online education, he's been open, honest, and eager to share ideas. Brian, you have had a profound impact on my life and career, and for that I'm forever grateful.

Next, I have to thank all my labmates. I can't really quantify the level of impact any single person has had, so I'll be doing these chronological order of when we met.

The first people I met were my 16.413 TAs, Simon Fang and Sungkweon Hong. I would go to office hours even when I didn't have questions just because I wanted to hang out and talk autonomy with people. Simon, thank you for being a supportive TA (and introducing me to *Aunty Donna*). Sungkweon, ...

Contents

1	Introduction	17
1.1	Summary of Contributions	21
1.2	Thesis Structure	22
2	Problem Statement	25
2.1	Extravehicular Activities as a Motivating Scenario	26
2.2	Motivating Scenario	27
3	Approach	29
3.1	Modeling and Controllability	30
3.1.1	Modeling Uncertain Observation Delay in STNUs	32
3.1.2	Modeling Observation Delay in RMPL	34
3.1.3	Explicitly Modeling Agents in RMPL	39
3.2	Scheduling Temporal Events	41
3.2.1	Defining a Valid Execution Strategy for STNUs with Variable Observation Delay	41
3.2.2	Online Dispatching for STNUs with Variable Observation Delay	42
3.3	Coordination	43
4	Consistency Checking of Temporal Constraint Networks with Uncertain Observation Delay	45
4.1	Temporal Networks	46
4.2	Fixed-Delay Controllability	50

4.3	Variable-Delay Controllability	53
4.3.1	Variable-Delay to Fixed-Delay Transformations	56
4.4	Discussion	65
4.5	Experimental Analysis	65
5	Single-Agent Execution with Delayed Event Monitoring	71
5.1	Dynamic Scheduling through Real-Time Execution Decisions	72
5.2	Delay Scheduling as an Extension to Dynamic Scheduling	75
5.2.1	Fixed-Delay Scheduling	76
5.2.2	Variable-Delay Scheduling	77
5.3	Dynamic Dispatching of STNUs with Observation Delay	81
5.3.1	Guaranteeing Agents Receive Actionable Events	82
5.3.2	Dynamic Event Dispatching	84
5.3.3	Observing Contingent Events	88
5.3.4	Optimistic Rescheduling	88
5.4	Experimental Analysis	94
6	Coordinating Multiple Agents under Uncertain Communication	97
6.1	Multi-Agent Control Programs	98
6.2	Event Propagation	101
6.3	Experimental Analysis	105
6.3.1	Distributed Kirk Simulation	105
6.3.2	Hardware Demonstration	111
7	Discussion and Future Work	123
7.1	Optimistic Rescheduling	123
7.1.1	Possible Improvements	129
7.2	Coordination	129
A	Comparison of Variable-Delay STNUs to Partially Observable STNUs	133
B	RMPL Control Programs and STNUs	139

List of Figures

4-1	We visualize the relationship between realized assignments across S and S' . In this example, each horizontal line is a timeline monotonically increasing from left to right. Dashed lines represent observation delays. We see how an assignment in S , $\xi(x_c)$, realized observation delay, $\Gamma(x_c)$, and an observation in S , $\text{obs}(x_c)$, contribute to an assignment in S' , $\xi(x'_c)$.	56
4-2	A visualization of the lemmas used to transform contingent links with variable observation delay and subsequent requirement links.	59
4-3	An STNU representing an EVA sampling task. The episode durations are representative of the bounds used in simulation. The depiction of this STNU with variable-delay is presented with rows representing actors to clarify the context of each event.	66
5-1	A high-level flow chart showing how we use variable-delay STNUs to generate scheduling decisions. The boxes represent the data structures involved in scheduling, while the arrows are the processes that are followed to eventually produce RTEDs.	75
5-2	Here, we show how the combination of $\xi(x_c)$ and $\bar{\gamma}(x_c)$ lead to an assignment of $\xi(x'_c)$ in S' . We see the range $\alpha \in [l, l + \bar{\gamma}^+(x_c) - \bar{\gamma}^-(x_c)]$ representing the earliest and latest assignments of $\xi(x_c)$ that could result in $\text{obs}(x_c) \in \xi(x'_c) \in [l^+(x_c), l^+(x_c)]\$$. The grey region represents the range of possible observation delays, $\bar{\gamma}(x_c)$, supporting $\xi(x'_c) \in [l^+(x_c), l^+(x_c)]$.	78

5-3 An STNU representing the installation and test of repeater antennas. Each row represents a single rover. The episode durations are representative of the bounds used in simulation.	95
6-1 The Kirk architecture used to generate event assignments for the centralized delay STNU. A single Kirk receives the VDC STNU that includes constraints for all agents, as well as contingent event observations. Kirk then performs delay scheduling, resulting in an assignment to all events.	106
6-2 The distributed architecture for the demonstration. The original centralized delay STNU is manually decoupled to three separate RMPL control programs, which are then used to initialize three Kirks. The Kirks receive appropriate event observations, which they then share to their peers. After delay scheduling, each Kirk produces an assignment to events that were under their control.	107
6-3 The two Kirks and two agents of the hardware demonstration. The Kirk executive running on the laptop is controlling the Barrett WAM arm in the background. Cameron Pittman is the second agent (acting as the astronaut) and interacting with a Kirk executive running on the Steam Deck handheld PC. This image was taken in the MERS lab on 20 May 2023.	113
6-4 The information flow between the two agents and two Kirks in the hardware demonstration. “SD” is short for Steam Deck.	113
6-5 The laptop screen at the end of the second hardware demo scenario. On the left is Kirk’s output, on the right is the ROS translation layer. Kirk is showing the schedule that it executed, while we can see logs from messages sent between Kirk and the ROS layer on the right. . .	114

THIS PAGE INTENTIONALLY LEFT BLANK

List of source codes

1	A sample control program composed of three constraints. <code>eat-breakfast</code> and <code>bike-to-lecture</code> designate controllable constraints, while the <code>main</code> control program enforces that the constraints are satisfied in series.	35
2	A student’s morning routine preparing for lecture as modeled in RMPL. This is a complete RMPL program that includes the required Lisp package definitions to run in Kirk.	37
3	An uncontrollable, or contingent, temporal constraint in a control program.	38
4	An RMPL control program describing a science data collection task with observation delay.	38
5	A snippet of an RMPL script that defines an agent and classical planning predicates and effects of a control program.	40
6	The control program the astronaut uses while collecting and downlinking scientific data.	117
7	The control program the robot uses to decide when to act with respect to learning the astronaut has finished collecting scientific data.	118

THIS PAGE INTENTIONALLY LEFT BLANK

List of Tables

3.1	The schedule produced by Kirk’s scheduler for the student’s routine before lecture as modeled in Listing 2. Note: Kirk’s output has been cleaned for readability purposes.	36
4.1	Edge generation rules for a labeled distance graph derived from a fixed-delay STNU.	53
4.2	Variable-delay vs. minimum, mean, and maximum fixed-delay controllability results with the parallel installation STNU from Figure 5-3. .	68
4.3	Variable-delay controllability vs. the controllability of a network that elongates its contingent links to account for observational uncertainty when using an exponential delay function with $\lambda = 3$	69
6.1	The schedule produced by a single Kirk against against the “multi-agent” variable-delay STNU.	109
6.2	The single agent schedule produced by <code>agent0</code> in the demonstration.	110
6.3	The single agent schedule produced by <code>agent1</code> in the d emonstration.	110
6.4	The single agent schedule produced by <code>agent0</code> in the demonstration. We added a <code>CLOSE-OUT</code> episode to end with a requirement event. . . .	111
6.5	The complete history of the delay scheduler for the astronaut in the first hardware demo scenario.	121
6.6	The complete history of the delay scheduler for the robot in the first hardware demo scenario.	121
6.7	The complete history of the delay scheduler for the astronaut in the second hardware demo scenario.	122

6.8 The complete history of the delay scheduler for the robot in the second hardware demo scenario.	122
---	-----

Chapter 1

Introduction

The United States, Europe, private companies, and new space agencies around the world are collectively urging humanity further into the cosmos with a never-before-seen zeal. We are witness to the great forces of political will, economics, and technological prowess launching our foothold beyond low Earth orbit and into planetary colonization. From every perspective, the scale of space exploration is staggering. It will take relentless effort from untold numbers of people, and our robotic partners, to usher us into the era where interplanetary travel and living off-world are commonplace. In every envisioned scenario for deep space exploration, there is a need to coordinate between agents, whether human or robotic, who must find a way to safely work together in the face of the communication challenges inherent to extreme environments.

There is good reason to design a system for coordination around the notion of uncertain communication. We take for granted that communication is easy in our civilized corners of the Earth’s surface. Cellular signals and WiFi are security blankets, tricking us into thinking it must be easy for *everyone* to communicate *everywhere*. The fact of the matter is that the communication is far from a given when you leave civilization. Consider low Earth orbit. The largest artificial satellite, the International Space Station (ISS), has been in orbit since 1998. Despite that, it still loses communication with the ground regularly. Satellites with much less robust infrastructure lose contact with the ground even more often. When astronauts set foot

on the South Pole of the Moon soon as part of the Artemis program [1], they will find uncertain satellite coverage and the need to contend against local topology that is hostile to radio signals. Any robots working near a habitat, or any astronauts on Extravehicular Activity (EVA), may be reliant on complicated systems of relays only to suffer unpredictable communications with other *in situ* agents, let alone Mission Control on Earth. Communications may be delayed due to passing through multiple relays and the speed of light. Or communications may drop out altogether when agents accidentally walk behind a big boulder between them and the closest relay.

The gap in our understanding of distributed collaboration and coordination that this thesis proposes to address is deciding how a collaborative agent should act, given a set of constraints between events, when there is uncertainty about when, *if ever*, communications and observations of exogenous events are received. To do so, we leverage and contribute to temporal reasoning research. We envision an executive capable of multi-agent coordination that can manage communication delay, which would be used by mission control to both plan and execute against a set of objectives. There are a range of multi-agent contexts that may realistically arise during near-term deep space missions. For instance, building a habitat on the lunar surface may require teams of astronauts and robots collaborating to construct facilities over a wide area. Spacewalks on the lunar surface for scientific exploration will inherently draw crews into locations with uncertain communication, such as craters.

An end-to-end approach would allow a human mission planner to construct a plan for all agents in the mission, separate actions for each agent, and then task agents to coordinate during the mission despite observation delay. An important stepping stone to the envisioned multi-agent planning and execution scenario is defining a single-agent executive that can decide when to act when the information it receives, i.e. observations or communications, has uncertain delay. Such a single-agent executive is useful in its own right, and can then form the basis for end-to-end multi-agent planning and coordination.

A mature corpus of research in the temporal reasoning community provides the foundation for such a single-agent task scheduling executive. We base our research

on the notion of events, which are discrete time points representing actions, and the timing constraints between events. Written in English, events and constraints might be stated as “samples must be stowed no more than five minutes after being collected.” In this case, “sample collecting” and “sample stowing” would be two events, with a constraint of < 5 minutes between them. It is the case that constraints between events we can control [2], events we cannot control [3], constraints between multiple agents [4], events that may not be observed [5], and events with variable observation delay [6] already give mission planners a robust set of modeling tools for creating schedules and guaranteeing that all constraints are satisfied during a mission.

What the state of the art lacks is an execution strategy when there is observation (or communication) delay. Existing execution strategies assume that events are either observed instantaneously as they happen or never. This is a challenge because, for events that are outside of our control, we no longer have a guarantee of knowing when they have occurred, yet the task scheduler must decide when to act such that all constraints are satisfied. To illustrate the challenge posed by uncertain communication on event scheduling, consider the following scenario.

There are two robots, **alpha** and **beta**, collaborating to perform a construction task on a planetary surface. The task involves uploading large video files documenting their progress back to engineers in Mission Control. There is limited bandwidth to the ground, so they need to coordinate their usage of the satellite uplink. At some point in the mission, there is a constraint that **alpha** should wait between three and five minutes after **beta** has finished uploading a video before uploading their own video. **alpha** knows exactly when **beta** started uploading because they were colocated at the time, but since then **alpha** has traversed to a distant location. The video will take eight to ten minutes to upload. **beta** will send a message to inform **alpha** the upload is complete, which **alpha** may receive instantaneously or after a delay of up to two minutes. Given when **alpha** learns that **beta** has finished their upload, how should **alpha** decide when to start their upload?

There are two constraints and two sources of uncertainty in the scenario, which we can associate with three events.

1. The event “**beta** finishes upload” will arrive in $[8, 10]$ (minutes) after “**beta** starts upload.” Neither **alpha** nor **beta** can control where in $[8, 10]$ the upload is finished.
2. **alpha** will decide where the event “**alpha** starts upload” should be scheduled in $[3, 5]$ after “**beta** finishes upload.”
3. The event “**beta** finishes upload” will be observed by **alpha** in $[0, 2]$ after it occurs. Neither **alpha** nor **beta** is guaranteed to know how long the delay is.

We can study a few scenarios to uncover the impact of observation uncertainty on **alpha**’s decision as to when to start uploading. We do so based on when **alpha** receives the observation that **beta** finished their upload. For simplicity’s sake, we assume that $t = 0$ when “**beta** starts upload” occurs.

- At $t = 8$, **alpha** knows there was no observation delay because the only way the observation could have come at $t = 8$ is if the video finished uploading at $t = 8$ and they received the message from **beta** instantaneously. They are safe to choose anywhere in $[3, 5]$ to start their upload. **alpha** chooses to upload as soon as possible at $t = 11$.
- At $t = 9$, the message from **beta** may have been delayed up to a minute (upload finishes at $t = 8 + \text{one minute delay}$), or it could have been sent as late as $t = 9$ and received instantaneously. **alpha** then must choose a time in $[3, 5]$ that is consistent with **beta** finishing anywhere in $[8, 9]$. **alpha** chooses to upload at $t = 12$.
- At $t = 10$, **beta** could have finished uploading as early as $t = 8$ (upload finishes at $t = 8 + \text{two minute delay}$) or as late as $t = 10$ if there was no communication delay. **alpha** must choose a time to start uploading that is consistent with the range of upload completion times in $[8, 10]$. **alpha**’s only option is to upload at $t = 13$.

This example demonstrates the type of online temporal reasoning over multiple sources of uncertainty required from the perspective of a single agent (`alpha` in this case). We could extend decision making to a multi-agent context by alternating our perspective to `beta`, who might then need to wait for `alpha` to send a message before its next action. With more constraints, compounding sources of uncertainty, and more agents cooperating, the decision as to when to act becomes increasingly difficult.

This thesis proposes to address the following high-level gaps that are required in order to define a single-agent task scheduling executive that can participate in a multi-agent context.

1. Defining and implementing an execution strategy that is applicable to all outcomes of uncertainty when there is variable observation delay.
2. Enacting online, multi-agent coordination through communication.

We take the view that the coordination of multiple agents with observation uncertainty requires that each agent must act independently without any assumption of a centralized authority dispatching plans. The first gap effectively defines a single-agent architecture that is useful in its own right for online scheduling in the face of observation delay. To do so, we build off existing temporal reasoning procedures for checking the controllability of temporal constraints to include uncertain observations of events. This procedure naturally informs the design of an execution strategy, or scheduling algorithm, for deciding when an agent should act given their knowledge of the history of events that have been scheduled so far. The second gap allows independent scheduling agents to coordinate their actions through communications, even when those communications may have uncertain delay. The result is a multi-agent execution architecture that is greater than the sum of its parts.

1.1 Summary of Contributions

Here we present the specific contributions of this thesis that are required to address the gaps presented above.

Safe Execution Strategy for Temporal Networks with Uncertain Observation Delay

Past work on the study of temporal networks with variable observation delay has provided a sound and complete method for proving the controllability given a set of constraints and uncertain observation delay [6]. We contribute an execution strategy that builds off the controllability checker and is valid for all resolutions of uncertainty realized during execution.

An Online Scheduler for Temporal Networks with Uncertain Observation Delay

Past work in temporal reasoning has provided a sound and complete online algorithm for dispatching controllable events given all other event assignments up to the current time [7]. We contribute an extension to online scheduling that implements the execution strategy for uncertain observation delay.

An Online Dispatcher for Dispatching Events to Hardware

State of the art schedulers are limited in that they output execution decisions, which act like instructions as to when to act rather than actions themselves [7]. We contribute a dispatching algorithm for enacting execution decisions on robotic hardware in the face of uncertain observations.

Distributed, Multi-Agent Coordination through Uncertain Communications

We contribute a coordination algorithm that allows multiple agents, each using the scheduling and dispatching contributions described above, to share knowledge of event observations. The result is a framework that enables safe scheduling and dispatching events when there are inter-agent constraints with uncertain communication.

1.2 Thesis Structure

The structure of this thesis is as follows. A more detailed problem statement, including descriptions of the scenarios used for testing distributed collaboration and coordination with uncertain communication, will be provided in Chapter 2. Our approach to addressing the problem statement will be outlined in Chapter 3. Chapter 4 will provide the first technical contributions of this thesis, first by addressing the

issue of modeling observation delay, then by providing a procedure that can be used to guarantee that temporal constraints with observation delay are satisfiable. Chapter 5 expands existing algorithms for deciding when to act given the resolution of constraints. There, we contribute a novel strategy for deciding when to act given observation delay. Additionally, we formalize and separate often confused components of scheduling, allowing us to design a more robust task scheduling executive that can be deployed to real hardware. Chapter 6 finally contributes a multi-agent coordination architecture for environments with uncertain communication. The discussion in Chapter 7 concludes this thesis by providing additional context for the decisions made during this research.

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 2

Problem Statement

There is a real-world need for coordinating multiple agents that are collaborating while facing uncertain inter-agent communication in uncertain environments. This thesis will focus on two motivating scenarios drawn from collaborative space operations, though this section will include a third example from the domain of military operations to further motivate the need for modeling uncertain delay in observations. The first scenario is based on an Artemis-like extravehicular activity (EVA), where an astronaut and a rover on the lunar surface are required to coordinate to share limited downlink bandwidth. The second scenario comes from the domain of satellite swarms, where many homogeneous agents coordinate operations with tight temporal constraints. The third scenario (which will not be modeled in experiments) is one where cooperative military agents are moving into and out of regions where immediate communication is purposefully halted in order to avoid detection by an enemy.

Delay temporal networks are essential to modeling space operations, where uncertainty is systemic to all aspects of planning, scheduling, and execution. As will be described in more detail for each motivating scenario below, uncertain observation delay is unavoidable due to imperfect communication infrastructure, uncertain timing with respect to knowledge transfer between agents, and finicky scientific equipment.

2.1 Extravehicular Activities as a Motivating Scenario

NASA is preparing to send astronauts back to the lunar surface as part of the Artemis program¹. The Artemis astronauts will continue a longstanding tradition in the U.S. space program of performing EVAs [8]. Like the Apollo astronauts of the 1960s and 1970s, Artemis astronauts will embark on EVAs wherein crews don spacesuits, egress landers, and conduct scientific expeditions on the lunar surface. There, they will survey surface features, collect samples, and in general perform field geology [9][11]. A small number of astronauts are Ph.D. geologists by trade, and NASA is training others in the principles of field geology up to a notional masters level of understanding [12]. NASA will support the lunar activities of these astronauts through a vast infrastructure of personnel on the ground, including teams of domain-relevant scientists. Together with flight controllers and engineers from various disciplines, a science team on the ground will provide real-time feedback to ensure that Artemis astronauts maximize the scientific return of their EVAs.

The relevant actors in an EVA include extravehicular (EV) crew members, who conduct all field activities outside the vehicles and habitats, and a ground-based Mission Control Center (MCC). Typically there are two EV crew members who often, but not always, work together to complete tasks. Life support imposes a temporal bound on the overall length of excursions. As an EVA progresses, EV crews consume four non-renewable resources, comprised of oxygen, battery power, water, and CO₂ scrubbers [13]. The duration of EVAs is limited by the consumable that is on track to be depleted first across the life support systems of both EV crew members, referred to as the limiting consumable.

Mission Control Center (MCC) is comprised of hundreds of flight controllers and engineers who monitor all aspects of EVAs. Its strict hierarchical structure ensures that all space-to-ground decisions pass through the Flight Director [14]. For the purposes of this example, we treat MCC as a single actor.

¹<https://www.nasa.gov/specials/artemis/>

When astronauts perform field science, another actor comes into play, called the ground-based Science Backroom Team (SBT). The SBT is comprised of multidisciplinary scientists who help astronauts prioritize and select scientific sample targets online [9], [15]. The science team reports their priorities to MCC, who then passes them along to the crew. The SBT behaves as a separate actor with limited communication, in that their messages may only pass directly to MCC, not the crew.

For EVAs, delay is manifested across three distinct categories: signal transmission, human operational delays, and instrument processing. Each category presents a source of delay that varies with uncertainty. For signal transmission, delay is sourced from the speed of light between planetary bodies and infrastructural deficiencies. Communication infrastructure outside of low-Earth orbit, including satellites and planetary surface signal repeaters [16], is not robust, and as such unpredictable delays and signal dropouts will be common [17]. For human operational delays, note that the primary goal of Mission Control is keeping the crew safe [18]. As such, communications from the science team to the crew may be delayed or dropped because Mission Control needs to prioritize communications and actions related to crew health and safety at the expense of science [19], [20]. Lastly, for instrument processing, there is uncertainty in the temporal relationships between the activation of complex scientific instruments and the return of useful information NO_ITEM_DATA:Sehlke2019. Scientific packages may generate high and low bandwidth data products, the uplink of which will be bottlenecked by limited bandwidth between space and ground, creating additional uncertainty between when a data product is ready and when it is available to the science team.

2.2 Motivating Scenario

A human and a rover are working together to perform scientific exploration on the lunar surface. The human is performing exploration of targets of opportunity that were identified during descent. The rover has a robotic arm, which it is using to perform sampling tasks collecting rocks in a predetermined location.

Both are in communication with mission control and scientists on Earth. Importantly, they share bandwidth on the relays and satellites used to transmit data between the Moon and Earth. CONOPS says only one agent may be using the bandwidth at a time (including uploads from Earth)

Both the human and the robot have their own schedules of events to perform and are aware of the other agent's events.

Chapter 3

Approach

For addressing our problem statement, we envision that a high-level executive should take responsibility for managing task planning and execution with respect to temporal constraints. For this thesis, we chose to extend an existing high-level task and motion planner, *Kirk* [22]. Kirk is a complete, end-to-end executive in that it can take human-friendly problem specifications as input and send commands to hardware as output.

To clarify terminology in this thesis, the term *executive* refers to Kirk and its subsystems, while *agent* refers to the combination of an executive and the system it controls that interacts with the outside world, e.g. robotic hardware.

At a high-level, Kirk works by first taking a description of the problem domain as written by domain experts, which should include the constraints, agent dynamics, environment, and starting and goal states of the problem at hand. Kirk then generates and checks plans using an optimal satisfiability (OpSAT) solver [23], elaborates temporal plan networks (TPNs) [24] to sub-executives when it encounters constraints and goals it cannot plan against directly, and eventually dispatches event schedules and motion plans to hardware. For the purpose of this thesis, we focus on Kirk's capability to dispatch events online after a plan has been generated.

Kirk operates on qualitative state plans, which consist of episodes that organize the occurrence of events as activities. Also includes causal links (:effects and :requires ala STRIPS/PDDL planning). All passed to OpSAT, which is like an SMT solver. Makes choices through causal links to decompose state constraints into a SAT problem

and then solve. Temporal constraints go to temporal-controllability. State plan gets turned into a SAT solver, with ordering from temporal constraints.

Some aspects of Kirk were already well-suited for coordinating multiple agents under observation delay, others were not. Specifically, our approach required research contributions in three key areas, which were then implemented in Kirk:

1. *Modeling and Controllability*: prior to execution, we must be able to model communication delay separate from temporal constraints, as well as guarantee that all temporal constraints can be satisfied
2. *Scheduling*: during execution, executives must be able to dynamically schedule and dispatch events respecting temporal constraints in spite of observation delay
3. *Coordination*: during execution, peer executives must be able to share event assignments and observations

Our approach to each research focus will be described below.

3.1 Modeling and Controllability

We take a model-based approach to deploying autonomous systems, that is, prior to a mission, we envision that engineers and domain experts work together to model the system at hand, then during the mission (though not necessarily online), the autonomous system then takes the models as input and decides how to act as output. There are three core challenges with modeling - the first being that we need formalisms that can be ingested by our algorithms and be used to guarantee safe execution. In other words, we need a data type to represent the phenomenon over which we want the algorithms comprising our system to reason. Next, the chosen formalism must allow us to guarantee the satisfiability of the system, i.e. the autonomous system must be able to act in a safe manner respecting all constraints to go from the starting state to the goal state. The third challenge is that we need a human-friendly form of said formalisms such that human domain experts, who are unlikely to also be experts in autonomy, can still model their domains accurately enough such that the desired

safe behavior is exhibited by the autonomous system. We address each challenge in our approach to modeling.

States and constraints can take on arbitrary forms, and how they are modeled depends entirely on the problem domain. Classical planning problems use boolean predicates and actions to model the world (e.g. STRIPS planning problems [25]). Scheduling problems involving time constraints will have continuous temporal bounds between discrete timepoints (e.g. in the form of temporal constraint graphs [2]). Other scenarios where motion planning is the focus will likely be modeled with vectors of continuous values in \mathbb{R} (e.g. often representing convex regions as in the case of the *Magellan* planner [26]). Hybrid domains combine states and constraints with mixed continuous and discrete values (e.g. using mixed-integer linear programs as demonstrated by Chen et al. [27]).

Given this thesis' emphasis on temporal scheduling, we choose to focus entirely on formalisms where states and constraints are temporal in nature. The starting state of the system is, by definition, one where time is set to 0 seconds, $t = 0$, and no events have been executed (i.e. no event assignments have been made). We then define controlled and uncontrolled set-bounded constraints between events. The goal state is one where times have been assigned to each controllable event such that all constraints are satisfied. To do so, we build our formalisms representing temporal constraints with set-bounded observation delay on top of simple temporal networks with uncertainty (STNUs) [3]. A brief explanation of our modeling strategy for temporal constraints with observation delay follows in Section 3.1.1, though we will elaborate on temporal reasoning and our chosen formalisms for it in much more detail in Chapter 4.

With a modeling formalism in hand, the second key challenge is to use the formalism to guarantee a property known as *controllability*, or that all controllable temporal constraints can be satisfied given the existing uncertainty in the STNU. There already exist a number of strategies for checking the controllability of STNUs. Examples of different strategies include the canonical work by Morris, Muscettola, and Vidal in checking for semi-reducible negative cycles (SRNCs) [28][31], as well as reframing

controllability as a Satisfiable Modulo Theory (SMT) problem [32]. In our approach to controllability under observation uncertainty, we build on top of checks for SRNCs as will be shown in 4.3.

For the third challenge, we choose to extend the Reactive Model-Based Programming Language (RMPL) [33], which provides to domain experts a means for describing the constraints and goal states of their domain without requiring additional expertise in autonomy. With RMPL, a human planner is capable of building control programs describing the constraints, agents, and states of the problem domain in a way that is human-readable yet highly programmable, and is independent of the underlying algorithms used by the autonomous system. As will be explained in Section 3.1.2 below, our approach was to add the ability for planners to model observation delay alongside temporal constraints in RMPL.

3.1.1 Modeling Uncertain Observation Delay in STNUs

In the case of observation delay, our model dictates that we reason over two time intervals. The first time interval represents the true length of time between two events, while the second interval represents the length of time between when an event occurs and when an executive observes the event. For ensuring that an executive takes safe actions in an uncertain environment, we assume worst-case scenario with respect to information gain. Our approach to modeling uncertain observation delay in STNUs is as follows.

1. The duration of time between two events is represented as a set-bounded interval
2. The duration of time between an event and its observation (observation delay) is represented as a set-bounded interval
3. Timestamps in event observations are ignored
4. The true duration of observation delay is not guaranteed to be learned

The first point comes directly from the STNU formalism (see Section 4.1). The second point allows for uncertainty in the amount of observation delay, e.g. in an uncertain environment, we could model observation delay for a given event as, say,

$[1, \infty]$, meaning an observation of an event could arrive one second after it occurs, or never arrive, or arrive at some arbitrary time, t , $1 < t \leq \infty$ later. The third point comes from assuming worst-case scenario and prevents us from “cheating” in our scheduling algorithm. For instance, imagine two agents coordinating. If agents passed timestamp information along with events to one another, they must also be able to synchronize their clocks, potentially to an arbitrary degree of precision. The challenge of synchronizing clocks between agents is outside the scope of this thesis and may not always be possible. As such, executives only trust their own clocks. Rather than backfill potentially erroneous times for event assignments as reported by exogenous sources, the executive we envision in this thesis records times that are internally consistent with its own clock. Doing so guarantees that the actions the executive takes as a result of temporal reasoning are consistent with its model.

The fourth point, that we are not guaranteed to learn event assignments, is a result of the first three. It stands to reason that an event observation is a function of the true assignment of an event and its observation delay. If there is uncertainty in both the event assignment and delay, then we have one equation with two unknowns. Thus, the term “uncertain” in uncertain observation delay means that we are forced to reason with deciding when to act even when we are not guaranteed to learn the true times assigned to events.

We call STNUs with variable observation delay *variable-delay STNUs*, which Bhargava first proposed as the underlying data structure for checking Variable-Delay Controllability (VDC) [6], [34]. We (Pittman) co-authored a journal article with Bhargava that was submitted to the Journal of AI Research presenting VDC and its chance constrained variant. We include VDC as a contribution of this thesis, given that we (Pittman) wrote or rewrote a significant portion of the VDC article, notably including a rewrite of key proofs with novel explanations. The new proofs will be presented in Section 4.3. Additionally, we rewrote the comparison of VDC to Partially Observable STNUs (POSTNUs) [5], including identifying and correcting a mistake in the same comparison as originally put forth by Bhargava in [34]. See Appendix A for an in-depth comparison to POSTNUs. We designed and ran the quantitative evaluation

of VDC in the article. The same experiments will be included at the end of Chapter

We formalize event observations and observation delay in Section 4.3.

3.1.2 Modeling Observation Delay in RMPL

RMPL is a key component of Kirk. This section steps through example RMPL control programs to describe their features and our modeling choices. The purpose of this section is three-fold:

1. A short walkthrough of the language is required in order to explain this thesis' contributions because an updated RMPL description in any form (e.g. manual, publication, or tutorial) has not been publicly released since 2003 [22]
2. We must describe the modeling choices of RMPL in sufficient detail to make concrete our approach to modeling temporal constraints in human-readable form
3. The above is used to demonstrate that modeling uncertain communication delay can be naturally modeled in RMPL

This section is not meant to be a complete documentation of RMPL, rather our goal is to motivate the strength of RMPL as a modeling language for human planners describing autonomous systems with observation uncertainty.

RMPL has undergone a number of rewrites since its inception, and is currently being developed as a superset of the Common Lisp language using the Metaobject Protocol [35]. The goal is that a human should have a comfortable means for accurately modeling sufficient detail about the problem domain such that an executive can perform model-based reasoning to decide how to act.

RMPL and Kirk can be used to achieve a number of different goals. These include but are not limited to temporal scheduling, classical planning, hybrid planning. For this thesis, we focus on temporal scheduling and the ability for a human to write *control programs*, or composable constraints and goals.

For this thesis, we take the assumption that each Kirk executive is responsible for a single agent. We also ignore vehicle dynamics given this thesis' focus on contributions

to temporal scheduling. However, RMPL is more flexible and allows multi-agent planning and motion planning using vehicle dynamics, which will be briefly described in Section 3.1.3.

An example of an RMPL control program for a single-agent without agent dynamics follows in Listing 1.

```
;; NOTE: we omitted Lisp package definitions here for simplicity's sake

(define-control-program eat-breakfast ()
  (declare (primitive)
    (duration (simple :lower-bound 15 :upper-bound 20)))

(define-control-program bike-to-lecture ()
  (declare (primitive)
    (duration (simple :lower-bound 15 :upper-bound 20)))

(define-control-program main ()
  (with-temporal-constraint (simple-temporal :upper-bound 40)
    (sequence (:slack nil)
      (eat-breakfast)
      (bike-to-lecture)))
```

Listing 1: A sample control program composed of three constraints. `eat-breakfast` and `bike-to-lecture` designate controllable constraints, while the `main` control program enforces that the constraints are satisfied in series.

Looking past the parentheses, we can see different options for defining temporal constraints. For example, the `(duration (simple ...))` form is used to define a set-bounded temporal constraint between a `:lower-bound` and an `:upper-bound`. The `main` control program uses a different form, `(with-temporal-constraint ...)` to place an `:upper-bound` on the overall deadline for scheduling all events in the control program.

The example control programs in Listing 1 are defined without agents in that there is an assumption that the Kirk instance that executes this control program must know what the semantics of `eat-breakfast` and `bike-to-lecture` mean and how to execute them.

It could also be the case that Kirk is simply being used to produce a schedule

of events offline that will be handed to an agent that knows how to execute them. As an example, perhaps a student wants some help planning their morning, so they write an RMPL control program with constraints representing everything they need to do between waking up and going to lecture, as seen in the more complex control program in Listing 2. The student could ask Kirk to produce a schedule of events that satisfies all the temporal constraints in this RMPL control program, which they would then use to plan their morning routine. See the resulting schedule produced by Kirk in Table 3.1. (Note that while normally times in RMPL are represented in seconds, we use minutes in Listing 2 and Table 3.1 for simplicity's sake.)

Table 3.1: The schedule produced by Kirk’s scheduler for the student’s routine before lecture as modeled in Listing 2. Note: Kirk’s output has been cleaned for readability purposes.

Event	Time (min)
START	0
Start shower	1
End shower	6
Start review-scheduling-notes	6
Start eat-breakfast	6
End review-scheduling-notes	16
Start review-planning-notes	16
End eat-breakfast	21
End review-planning-notes	26
Start pack-bag	26
End pack-bag	31
Start bike-to-lecture	32
End bike-to-lecture	46
END	46

Listing 2 introduces the notion of control programs that are allowed to be executed simultaneously, as modeled with the `(parallel ...)` form found in the `main` control program on line 48.

Kirk is able to simulate the RMPL script in Listing 2 and produce a schedule because there were no uncontrollable constraints, that is, all control programs are under the agent’s control. Say we replaced `bike-to-lecture` with `drive-to-lecture`. Due to traffic conditions, driving presents in an uncontrollable constraint. RMPL allows us to model uncontrollable constraints as in Listing 3.

```

1  ;; This file lives in the thesis code repo at:
2  ;;      kirk-v2/examples/morning-lecture/script.rmpl
3  ;;
4  ;; To execute this RMPL control program as-is and generate a schedule, go to the root
5  ;; of the thesis code repo and run the following command:
6  ;;
7  ;; kirk run kirk-v2/examples/morning-lecture/script.rmpl \
8  ;;      -P morning-lecture \
9  ;;      --simulate
10
11 (rmpl/lang:defpackage #:morning-lecture)
12
13 (in-package #:morning-lecture)
14
15 (define-control-program shower ()
16   (declare (primitive)
17            (duration (simple :lower-bound 5 :upper-bound 10))))
18
19 (define-control-program eat-breakfast ()
20   (declare (primitive)
21            (duration (simple :lower-bound 15 :upper-bound 20))))
22
23 (define-control-program review-scheduling-notes ()
24   (declare (primitive)
25            (duration (simple :lower-bound 10 :upper-bound 15))))
26
27 (define-control-program review-planning-notes ()
28   (declare (primitive)
29            (duration (simple :lower-bound 10 :upper-bound 15))))
30
31 (define-control-program pack-bag ()
32   (declare (primitive)
33            (duration (simple :lower-bound 5 :upper-bound 6))))
34
35 (define-control-program bike-to-lecture ()
36   (declare (primitive)
37            (duration (simple :lower-bound 15 :upper-bound 20))))
38
39 (define-control-program review-notes ()
40   (sequence (:slack t)
41             (review-scheduling-notes)
42             (review-planning-notes)))
43
44 (define-control-program main ()
45   (with-temporal-constraint (simple-temporal :upper-bound 60)
46     (sequence (:slack t)
47               (shower)                                37
48               (parallel (:slack t)
49                         (eat-breakfast)
50                         (review-notes)))

```

```
(define-control-program drive-to-lecture ()
  (declare (primitive)
    (duration (simple :lower-bound 15 :upper-bound 20
                      :contingent t)))
```

Listing 3: An uncontrollable, or contingent, temporal constraint in a control program.

The addition of `:contingent t` to the `(duration ...)` form tells Kirk that it does not have control over when the end of `drive-to-lecture` is scheduled, rather, Nature (i.e. traffic conditions) chooses a time. Despite the lack of control over `drive-to-lecture`, we do know the drive should take between 15 and 20 minutes, hence our model includes `:lower-bound 15` and `:upper-bound 20`.

With uncontrollable constraints in a control program, we are no longer guaranteed to be able to produce a schedule offline as we show in Table 3.1. Instead, as time passes, we may only choose to schedule controllable events based on the *partial history* of contingent event assignments so far, or, in other words, perform *dynamic scheduling*. Thus, we can no longer simulate a schedule with Kirk. We must connect Kirk to a source for receiving contingent event assignments in order to make valid controllable event assignments. Our approach to dynamic scheduling is the focus of Section 3.2.

As a contribution of this thesis, our existing approach to specifying durations in RMPL was expanded to model observation delay. An example follows in Listing 4 modeling a sample collection control program with observation delay.

```
(define-control-program collect-science-sample ()
  (declare (primitive)
    (duration (simple :lower-bound 15 :upper-bound 30
                      :min-observation-delay 5
                      :max-observation-delay 15)
              :contingent t)))
```

Listing 4: An RMPL control program describing a science data collection task with observation delay.

We can see in Listing 4 that representing set-bounded observation delay is as simple as adding `:min-` and `:max-observation-delay` to the `(duration (simple ...))` `:contingent t`) form. In full, this control program represents an uncontrollable

constraint with a contingent event that Nature will schedule [15, 30] time units after sample collection begins. The executive will then wait an additional [5, 15] time units before learning that `collect-science-sample` has been scheduled. As will be described in much greater detail in Section 4.3, the executive will only learn *that* the contingent event occurred - is not guaranteed to learn where in [15, 30] the contingent event was assigned, nor will it know how much observation delay was incurred.

3.1.3 Explicitly Modeling Agents in RMPL

This section is included to expand on the features of RMPL, though note that none of these features are required for controlling distributed agents, and were not a part of the experiments for this research.

If we wanted to specify agents in a multi-agent control program, or if we wanted to take vehicle dynamics into account, RMPL gives us a means for using the Common Lisp Object System (CLOS) for defining agents, agent dynamics, and the control programs agents may execute.

An example RMPL control program with an agent is provided in Listing 5 for completeness sake from the domain of underwater robotics.

In Listing 5, `glider` refers to a low-powered autonomous underwater vehicle that prefers to traverse by following ocean currents using a buoyancy engine.¹ We see that we model a `glider` agent and its properties using standard CLOS. The `move` control program then takes a `glider` and a `location` as arguments. The `(requires ...)` form is equivalent to the preconditions of a durative action in a PDDL 2.1 [36] domain. Likewise, the `(effect ...)` form is equivalent to PDDL effects. Finally, as we saw before, the durative action also includes a temporal constraint in its `(duration ...)` form.

Kirk is able to take RMPL as input to perform classical planning, though further discussion of it falls outside the scope of this thesis.

¹The Slocum Glider is an example: <https://www.whoi.edu/what-we-do/explore/underwater-vehicles/auvs/slocum-glider/>.

```

;; This code is a snippet from a file in the thesis code repo found at:
;;      kirk-v2/examples/glider/script.rmpl

(defclass glider ()
  ((id
    :initarg :id
    :finalp t
    :type integer
    :reader id
    :documentation
    "The ID of this glider.")
   (deployed-p
    :initform nil
    :type boolean
    :accessor deployed-p
    :documentaiton
    "A boolean stating if the glider is deployed at any point in time.")
   (destination
    :initform nil
    :type (member nil "start" "end" "science-1" "science-2")
    :accessor destination
    :documentation
    "The location to which the glider is currently heading, or NIL if it is not
     in transit.")
   (location
    :initarg :location
    :initform "start"
    :type (member nil "start" "end" "science-1" "science-2")
    :accessor location
    :documentation
    "The location where the glider is currently located, or NIL if it is not at
     a location (in transit)."))

(define-control-program move (glider to)
  (declare (primitive)
           (requires (and
                      (over :all (= (destination glider) to))))
           (effect (and
                     (at :start (= (destination glider) to))
                     (at :start (= (location glider) nil))
                     (at :end (= (destination glider) nil))
                     (at :end (= (location glider) to))))
           (duration (simple :lower-bound 10 :upper-bound 20))))
```

Listing 5: A snippet of an RMPL script that defines an agent and classical planning predicates and effects of a control program.

3.2 Scheduling Temporal Events

The bulk of the technical chapters of this thesis, namely Chapters 4 and 5, describe the algorithmic insights behind the *delay scheduler*. The delay scheduler dispatches controllable events online for dynamically controllable STNUs while reasoning over observation delay in the uncontrollable events it receives. There were two key contributions that enabled the delay scheduler.

Reasoning over the controllability of STNUs with variable-observation delay had been demonstrated to be possible in prior work [37], though an explicit, online execution strategy, let alone a valid execution strategy, was never defined for variable-delay STNUs. For our first contribution, we define an execution strategy for variable-delay controllable STNUs and prove its validity.

Likewise, dynamic schedulers have been established for dispatching events from STNUs, e.g. FAST-EX [7]. For our second contribution, we defined a novel delay scheduler built on FAST-EX capable of applying the execution strategy defined in our first contribution.

We elaborate further on our approach to each contribution below.

3.2.1 Defining a Valid Execution Strategy for STNUs with Variable Observation Delay

We cannot execute an STNU without first demonstrating that it is controllable. Our approach to checking the controllability of STNUs with observation delay is to apply Bhargava’s Variable-Delay Controllability checker (VDC) [6]. VDC is a procedure that takes place in two stages and is $O(N^5)$ in the number of events. In the first stage, we transform the STNU with variable observation delay to one with fixed observation delay in $O(N^2)$. In the second stage, we check the controllability of the fixed-delay STNU using Bhargava’s fixed-delay controllability checker (FDC) [34], [37], which is modified from Morris’ $O(N^3)$ dynamic controllability check [31] such that it accounts for fixed observation delay in contingent links.

In short, the first stage process is built around the idea of modeling a worst-

case scenario with respect to receiving observations. The resulting fixed-delay STNU reflects a situation where the executive learns as little as possible about the contingent events. If the fixed-delay STNU with minimal information is controllable, then so too must any situation be controllable when we learn more information.

We contribute the definition for an execution strategy for variable-delay STNUs, wherein we dispatch events according to the *dispatchable form* of the *fixed-delay* STNU, while respecting the constraints modeled in the *variable-delay* STNU. Existing controllability checks, like FDC, and execution strategies, like FAST-EX, depend on a dispatchable form, i.e. a *distance graph* representation of the STNU. The key challenge in defining an execution strategy for a variable-delay STNU is that unlike vanilla STNUs and fixed-delay STNUs, there is no dispatchable form for variable-delay STNUs. Hence why the VDC check first transforms the variable-delay STNU to a fixed-delay form. In Chapter 5, we formally define the execution strategy for variable-delay STNUs and prove its validity.

3.2.2 Online Dispatching for STNUs with Variable Observation Delay

We chose to build the delay scheduler as a modified variant of Hunsberger’s FAST-EX [7] because, to the best of our knowledge, FAST-EX is the fastest dynamic scheduler published to date.

FAST-EX maps partial histories, or schedules of events up to the current time, to Real-Time Execution Decisions (RTEDs). RTEDs contain a list of events to be executed and a time (that could be from now to point in the future) to execute them. When contingent events are observed or controllable events are scheduled, it updates the distance graph to capture the information gained. To improve the online performance of dynamic scheduling, Hunsberger’s insight was to reduce the space of the dispatchable form by removing edges as events are executed. It can do so by first iteratively updating the distances to and from the remaining events by performing Dijkstra’s Single Sink and Single Source Shortest Paths algorithms to and from the

zero point (start event) of the distance graph.

The delay scheduler differs from FAST-EX in the way it (1) records partial histories and (2) how it generates RTEDs. For both changes, we must address special cases related to a change in the *execution space* - the time ranges of possible event assignments - that result from the variable-delay to fixed-delay STNU transformation. We make two changes for (1). First, we remove the assumption that contingent events are instantaneously observed. Essentially, we use the known fixed observation delay to decide where in the past an observed contingent event was assigned. Second, to account for one special case due to the transformation, we use observations to optimistically rewrite the variable-delay STNU in an attempt to shorten the overall makespan (see Section 7.1). Key to (2) is that we are allowed to *imagine* that contingent events were assigned despite never observing them. Imagining contingent events is a result of the other special case from the variable-delay to fixed-delay transformation (see Section 5.2).

3.3 Coordination

To the best of our knowledge, this thesis contributes the first framework for, and demonstration of, online coordination between dynamic schedulers with inter-agent temporal constraints.

Our challenge is to allow multiple Kirk instances to dynamically schedule simultaneously while sharing events. At a high level, our approach is that inter-agent communications take the form of event observations. Each agent's ego controllable events are sent to peers, who receive them as exogenous, uncontrollable event observations. We allow (and expect) that communications have uncertain delay, thus we apply the modeling formalisms of variable-delay STNUs to inter-agent temporal constraints.

Our approach to online coordination is as follows:

1. Each instance of Kirk receives a unique, manually written control program
2. All control programs begin execution at the same time

3. Kirk executives broadcast scheduled events to a known set of peers
4. In their own schedules, Kirk executives record event observations from their peers as they are received

The challenge of manually writing control programs that enable MA execution is non-trivial. A modeler must consider both intra-agent and inter-agent constraints that, compounded by uncertain communication, frequently contain difficult to spot conflicts. (It is no surprise that temporal decoupling is incomplete!) Furthermore, we found that translating events between executives is challenging. When writing MA control programs, it is possible that the same event has different identifiers in different STNUs. Care must be taken to ensure different executives understand the event observations they receive from their peers. In our experiments, our strategy was to carefully write MA control programs to guarantee events shared names between executives. MA control programs under uncertain communication will be discussed in detail in Section 6.1.

The second point ensures that control programs share a temporal frame of reference. However, uncertain communication was able to partially mitigate executives with clocks that did not agree. In effect, communication delay can be used to mitigate the differences in executive clock times.

The third and fourth points encapsulate our contribution to the challenge of MA communication with respect to inter-agent temporal constraints. We imagined inter-agent communications as a simple directional graph between executives. In this structure, all event nodes are publishers. Outgoing edges represent subscribers that receive all scheduled events, including both controllable events and uncontrollable event observations that the publishing agent itself receives. Event observations are then naturally propagated through the graph. We assume that communication delay in the modeled system incorporates the time events spend propagating through the graph. Event propagation will be formally defined in Section 6.2.

Chapter 4

Consistency Checking of Temporal Constraint Networks with Uncertain Observation Delay

Our overarching aim in this Chapter is to architect the offline portions of a single-agent pipeline that takes a temporal network with uncertain observation delay of exogenous events as input in order to execute events in the real world within time windows that guarantee temporal consistency. Given everything we know and do not know about the temporal relationship between events within and outside of our control, this chapter will lay the groundwork that there exists an execution strategy that guarantees all constraints are satisfied despite the uncertainty. The next chapter, Chapter 5, will provide accompanying online procedures for acting on said execution strategy and dispatching events with real hardware (or by generally telling an agent what to do).

The three aims of this chapter are to

1. model temporal constraints with uncertain observation delay,
2. define a consistency (controllability) checking procedure for temporal networks with uncertain observation delay, and
3. prove that the execution strategy assumed by the controllability checking pro-

cedure is safe.

In Section 4.1, we address aim (1) by outlining the necessary definitions for modeling temporal networks. Sections 4.2 and 4.3 describe our chosen model for temporal constraints with uncertain observation delay, and address aim (2) by presenting a procedure for checking the consistency thereof. Sections 4.2 and 4.3 are largely based on the work originally put forth by Bhargava et. al., [6], [34], [37] with additional contributions by us as highlighted below. Notably, Section 4.3 addresses aim (3) by contributing novel proofs that the execution strategy assumed to exist by Bhargava et. al. is safe. We conclude with experimental analysis of our chosen consistency checking procedure in Section 4.5 using example temporal constraint networks inspired by lunar exploration.

4.1 Temporal Networks

Temporal networks form the backbone of our architecture for temporal reasoning under observation delay. Simple Temporal Networks (STNs) offer the basic building blocks for most expressive temporal network formalisms [2]. An STN is composed of a set of variables and a set of binary constraints, each of which limits the difference between a pair of these variables; for example, $B - A \in [10, 20]$. Each variable denotes a distinguished point in time, called an *event*. Constraints over events are binary *temporal constraints* that limit their temporal difference; for example, the aforementioned constraint specifies that event A must happen between 10 and 20 minutes before event B .

Definition 1. STN [2]

An *STN* is a pair $\langle X, R \rangle$, where:

- X is a set of variables, called events, each with a domain of the reals \mathbb{R} , and
- R is a set of simple temporal constraints. Each constraint $\langle x_r, y_r, l_r, u_r \rangle$ has scope $\{x_r, y_r\} \subseteq X$ and relation $x_r - y_r \in [l_r, u_r]$.

Definition 2. Schedule [28]

A *schedule*, ξ , is a mapping of events to times, $\xi : X \rightarrow \mathbb{R}$.

An STN is used to frame scheduling problems. A schedule is feasible if it satisfies each constraint in R . We use the notation $\xi(x)$ to represent a mapping from an event, x , to a time, $x \rightarrow \mathbb{R}$, in the schedule. A schedule is *complete* if all $x \in X$ are assigned times in ξ . An STN is *consistent* if it has at least one feasible schedule that assigns all events in X .

An STN is consistent if and only if there is no negative cycle in its equivalent distance graph [2]. Let n be the number of events in a temporal network and m to be the number of constraints. Then consistency of an STN can be checked in $O(mn)$ time using the Bellman-Ford Algorithm to check for negative cycles.

While an STN is useful for modeling problems in which an agent can control the exact time of all events, it does not let us model actions whose durations are uncertain. A Simple Temporal Network with Uncertainty (STNU) is an extension to an STN that allows us to model these types of uncertain actions [3].

Definition 3. STNU [3]

An *STNU* S is a quadruple $\langle X_e, X_c, R_r, R_c \rangle$, where:

- X_e is the set of executable events with domain \mathbb{R} ,
- X_c is the set of contingent events with domain \mathbb{R} ,
- R_r is the set of requirement constraints of the form $l_r \leq x_r - y_r \leq u_r$, where $x_r, y_r \in X_c \cup X_e$ and $l_r, u_r \in \mathbb{R}$, and
- R_c is the set of contingent constraints of the form $0 \leq l_r \leq c_r - e_r \leq u_r$, where $c_r \in X_c$, $e_r \in X_e$ and $l_r, u_r \in \mathbb{R}$.

An STNU divides its events into executable and contingent events and divides its constraints into requirement and contingent constraints. The times of executable events are under the control of an agent, and assigned by its scheduler. STNU executable events are equivalent to events in an STN. Contingent events are controlled by Nature. Contingent constraints model the temporal outcomes of uncertain actions and are enforced by Nature. Contingent constraints relate a starting executable event

and an ending contingent event. To ensure causality, the lower-bound of a contingent constraint is required to be non-negative; hence, the end event of the constraint follows its start event. Contingent constraints are not allowed to be immediately followed by additional contingent constraints. Requirement constraints specify constraints that the scheduler needs to satisfy and may relate any pair of events. An STNU requirement constraint is equivalent to an STN constraint.

To clarify terminology, we sometimes refer to contingent constraints as contingent links and requirement constraints as requirement links. We also sometimes use the term *free* instead of requirement to describe executable events and constraints. When we discuss contingent constraint or contingent link duration, we refer to the amount of time that actually elapses between a contingent link’s starting executable event and its ending contingent event. We sometimes refer to STNUs as defined in Definition 3 as *vanilla* STNUs (in contrast to the many “flavors” of STNUs, namely the variants with fixed and variable observation delay functions as will be defined in Sections 4.2 and 4.3 respectively).

With STNs, our goal is to construct a consistent schedule for all events such that all constraints are satisfied. In STNUs, however, contingent events cannot be scheduled directly. Instead, we are interested in determining whether there is a *controllable* execution strategy that guarantees that a schedule can be constructed such that all constraints are satisfied despite how uncertainty is resolved.

Definition 4. Situations [3]

For an STNU S with k contingent constraints $\langle e_1, c_1, l_1, u_1 \rangle, \dots, \langle e_k, c_k, l_k, u_k \rangle$, each *situation*, ω , represents a possible set of values for all links in S , $\omega = (\omega_1, \dots, \omega_k) \in \Omega$. The *space of situations* for S , Ω , is $\Omega = [e_1, c_1] \times \dots \times [e_k, c_k]$.

Each *situation* in the *space of situations*, $\omega \in \Omega$, represents a different assignment of contingent links in the schedule [3]. We may represent the situation for a specific constraint as ω_i for the i -th constraint in S , or $\omega(x_c)$ for contingent event x_c .

Situations may be applied to STNUs.

Definition 5. Projection [3], [28]

A *Projection* is an application of a situation, ω , on an STNU S , which collapses the durations of contingent links to specific durations resulting in an STN.

A *projection* is an STN that is the result of applying a situation to an STNU, and thus the contingent links have reduced from uncertain ranges to specific durations [3], [28].

Definition 6. Execution Strategy

An *execution strategy*, \mathcal{S} , is a mapping of situations to schedules, $\mathcal{S} : \Omega \rightarrow \Xi$.

An *execution strategy* then naturally maps a specific resolution of the uncertainty of the contingent constraints to a set of assignments for the events of an STNU. For an STNU, time monotonically increases and we only observe *activated* contingent events, or those contingent events at the tail of a contingent link whose free event predecessor has been executed. As such, we modify our definition of ξ .

Definition 7. Partial Schedule

A *partial schedule*, ξ , is a mapping from a proper subset of events in an STNU, $X' \subseteq X_e \cup X_c$, to times, $\xi : X' \rightarrow \mathbb{R}$.

As a proper subset, ξ represents an assignment of events *so far* during the execution of an STNU. From here on, ξ refers to a partial schedule. If $X' = X_e \cup X_c$, then the schedule is complete.

To determine whether an STNU is controllable, we determine whether there exists a *valid* execution strategy for it.

Definition 8. Valid Execution Strategy

A *valid* \mathcal{S} is one that enforces that, for any $\omega_f \in \Omega_f$, the outputted decision respects all existing temporal constraints and ensures the existence of a subsequent valid execution strategy following that action.

In the world of STNU literature, there are many forms of controllability that represent the ability of a scheduler to enact execution strategies that satisfy constraints under different conditions [3]. Three forms of controllability, *strong*, *weak*, and *dynamic* are studied most often, though in practice we omit weak controllability from

our analysis. A temporal network is *strongly controllable* (or exhibits strong controllability) (SC), if there exists a complete schedule that will satisfy all constraints for all projections of the STNU. A temporal network exhibits dynamic controllability (DC) if an execution strategy exists for a given partial schedule. As we will see below, variable-delay controllability, used to check the consistency of temporal networks with uncertain observation delay, will unify strong and dynamic controllability into a single theory. But first, we describe fixed-delay controllability, which introduces known observation delay to STNUs.

4.2 Fixed-Delay Controllability

Under fixed-delay controllability (FDC) [37], we consider the problem of scheduling execution decisions when the assignment of values to contingent events is learned after some time has passed from the initial assignment, if ever. Fixed-delay controllability uses a *fixed-delay function* to encode the delay between when an event occurs and when it is observed by a scheduling agent. We sometimes refer to an STNU with an associated fixed-delay function as a *fixed-delay STNU*.

Definition 9. Fixed-Delay Function [37]

A *fixed-delay function*, $\gamma : X_c \rightarrow \mathbb{R}^+ \cup \{\infty\}$, maps a contingent event to the amount of time that passes between when the event is assigned and when its value is observed.

As a matter of convention, we use $A \xrightarrow{[l,u]} B$ to represent requirement links between events A and B and use $A \xrightarrow{[l,u]} E$ to represent contingent links between A and E . When we refer to the fixed-delay function associated with a contingent event E of some contingent constraint $A \xrightarrow{[l,u]} E$, we use the notation $\gamma(E)$, or equivalently, γ_E . Without instantaneous observation of contingent events, we must clarify the relationship between when an event is assigned and when it is *observed*.

Definition 10. Contingent Event Observation

Observations, obs , are a mapping from contingent events to times when the agent receives knowledge the event has been assigned, $\text{obs} : X_c \rightarrow \mathbb{R}$. An observation of an event, x_c , follows the relationship, $\text{obs}(x_c) = \xi(x_c) + \gamma(x_c)$.

We also present a revised definition of situations, Ω_f , to reflect the impact of the delay function on event observations.

Definition 11. Fixed-Delay Situations

For an STNU S with k contingent constraints $\langle e_1, c_1, l_1, u_1 \rangle, \dots, \langle e_k, c_k, l_k, u_k \rangle$ and fixed-delay function γ , each *fixed-delay situation*, ω_f , represents a possible set of *observed* values for all links in S , $\omega_f = (\omega_{f1}, \dots, \omega_{fk})$. The $\{\text{space of situations}\}$ for S , Ω_f , is $\Omega_f = [e_1, c_1] + [\gamma_1, \gamma_1] \times \dots \times [e_k, c_k] + [\gamma_k, \gamma_k]$.

To emphasize that the *observed* value for an event is not the same as its assignment, we also use the term *observation space* as a synonym for the space of situations.

Definition 12. Valid, Fixed-Delay Execution Strategy

A *valid* \mathcal{S} for a fixed-delay STNU is one that enforces that, for any $\omega_f \in \Omega_f$, while receiving observations of contingent events after a known and fixed delay, the outputted decision respects all existing temporal constraints and ensures the existence of a subsequent valid execution strategy following that action.

With the semantics of delayed observations in hand, we can define what it means for a fixed-delay STNU to be controllable.

Definition 13. Fixed-Delay Controllability [37]

An STNU S is *fixed-delay controllable* with respect to a delay function, γ , if and only if for the space of situations, Ω_f , there exists a valid, fixed-delay execution strategy, \mathcal{S} , that will construct a satisfying schedule for all requirement constraints during execution.

Importantly, fixed-delay controllability (FDC) generalizes the two concepts of controllability that are central to STNUs, strong and dynamic controllability. In particular, by using a fixed-delay function where we observe all events instantaneously,

e.g. $\gamma(x_c) = 0 \forall x_c \in X_c$, checking fixed-delay controllability reduces to checking *dynamic controllability*. Similarly, a fixed-delay function that specifies we never observe any contingent events, e.g. $\gamma(x_c) = \infty \forall x_c \in X_c$, corresponds to checking *strong controllability* [3].

As is the case for a vanilla STNU, evaluating whether a valid execution strategy exists for a fixed-delay STNU reduces to checking for the presence of a *semi-reducible negative cycle* in a *labeled distance graph* derived from the fixed-delay STNU [30]. The key insight for checking fixed-delay controllability is the inclusion of a fixed-delay function in the constraint generation rules for building the labeled distance graph [37].

The labeled distance graph corresponds to the constraints of the STNU with each unlabeled edge from A to B with weight w (denoted $A \xrightarrow{w} B$) representing the inequality $B - A \leq w$. Labeled edges represent conditional constraints that apply depending on the realized value of contingent links in the graph. For example, a lower-case labeled edge from A to B with weight w and lower-case label c (denoted $A \xrightarrow{c:w} B$) indicates that $B - A \leq w$ whenever the contingent link ending at C takes on its lowest possible value. An upper-case labeled edge from A to B with weight w and upper-case label C (denoted $A \xrightarrow{C:w} B$) indicates that $B - A \leq w$ whenever the contingent link ending at C takes on its highest possible value. Given a labeled distance graph, there are several valid derivations we can apply to generate additional edges (see Table 4.2). If it is possible to derive a negative cycle that is free of lower-case edges, then the STNU has a *semi-reducible negative cycle* and the STNU is not controllable.

Note that with fixed-delay controllability, the lower-case and cross-case rules are modified from the Morris and Muscettola [29], accounting for γ . More specifically, we address the case where observation delay makes it impossible to receive information about a contingent event before its immediate successor. More detail can be found in [38].

We generalize fixed-delay to variable-delay controllability next.

Edge Generation Rules			
	Input edges	Conditions	Output edge
No-Case Rule	$A \xrightarrow{u} B, B \xrightarrow{v} C$	N/A	$A \xrightarrow{u+v} C$
Upper-Case Rule	$A \xrightarrow{u} D, D \xrightarrow{C:v} B$	N/A	$A \xrightarrow{C:u+v} B$
Lower-Case Rule	$A \xrightarrow{c:x} C, C \xrightarrow{w} D$	$w < \gamma(C), C \neq D$	$A \xrightarrow{x+w} D$
Cross-Case Rule	$A \xrightarrow{c:x} C, C \xrightarrow{B:w} D$	$w < \gamma(C), B \neq C \neq D$	$A \xrightarrow{B:x+w} D$
Label Removal Rule	$B \xrightarrow{C:u} A, A \xrightarrow{[x,y]} C$	$u > -x$	$B \xrightarrow{u} A$

Table 4.1: Edge generation rules for a labeled distance graph derived from a fixed-delay STNU.

4.3 Variable-Delay Controllability

While fixed-delay controllability is quite expressive, its fundamental limitation is that it assumes that contingent event assignments, even those made after a fixed delay, are always known. If uncertainty in observation delay, and thus uncertainty in contingent event assignment, is added to the model, then we are forced to decide when to act despite imperfect knowledge of the partial history.

We now introduce this model in terms of definitions for a *variable-delay function* and *variable-delay controllability* (VDC) checking as applied to *variable-delay STNUs*. Since variable-delay semantics generalizes the notion of fixed-delay, as a matter of convenience, we also use the simplified term *delay STNUs* to refer to STNUs with variable observation delay. VDC was originally presented by Nikhil Bhargava [6]. However, we contributed significant improvements of the lemmas and proofs herein, including the addition of novel visual depictions of VDC, in our role as a coauthor with Bhargava on a journal article on the topic of VDC that was submitted to the *Journal of AI Research*.

This section formalizes the definition of VDC, which is required to explain the procedure of checking VDC in Section 4.3.1.

Definition 14. Variable-Delay Function

A *variable-delay function*, $\bar{\gamma} : X_c \rightarrow (\mathbb{R}^+ \cup \{\infty\}) \times (\mathbb{R}^+ \cup \{\infty\})$, maps a contingent event, x_c , to an interval $[a, b]$, where $a \leq b$. The interval bounds the time that

passes after $\xi(x_c)$ before that value is observed to be assigned. No prior knowledge is assumed about the distribution associated with this interval.

Importantly, this model does not assume that an executing agent may be able to infer *when* a contingent event was executed. Instead, our model only infers *that* the event was executed. Like the resolution of contingent constraints, the resolved value of $\bar{\gamma}(x_c)$ will be selected by Nature during execution. Thus, the timing of when an agent receives an observation is a function of the independent resolutions of the contingent link and variable-delay function.

By convention, we use $\bar{\gamma}^-(x_c)$ and $\bar{\gamma}^+(x_c)$ to represent the lower-bound and upper-bound, respectively, of the range representing the possible delay in observation, i.e. $\bar{\gamma}(x_c) \in [\bar{\gamma}^-(x_c), \bar{\gamma}^+(x_c)]$.

Definition 15. Observation Projection

The *observation projection* Γ is a mapping from a contingent event to a fixed observation delay, $\Gamma : X_c \rightarrow \mathbb{R} \in [\bar{\gamma}^-(X_c), \bar{\gamma}^+(X_c)]$.

During execution, the *observation projection*, Γ , represents the resolution of observation delay. Much like how a projection collapses a vanilla STNU to an STN, the observed projection collapses a contingent link with variable-observation delay to one with fixed-observation delay. However, unlike the projection of an STNU, the observation projection is not guaranteed to be learned. We update our definitions of obs , ξ , and Ω accordingly.

Definition 16. Contingent Event Observation

Contingent event observations, obs , are a mapping from contingent events to times when the agent receives events, $\text{obs} : X_c \rightarrow \mathbb{R}$, based on the relationship, $\text{obs}(x_c) = \xi(x_c) + \Gamma(x_c)$.

Determining a real-valued mapping of a contingent event to the value of its assignment, i.e. its schedule or $\xi(x_c)$, is no longer guaranteed due to an interval bounded $\Gamma(x_c)$. We must use interval-bounded contingent event assignments instead.

Definition 17. Schedule

A *schedule*, ξ , when applied to contingent events, is a mapping of events to interval-bounded times, $\xi : X_c \rightarrow (\mathbb{R}^+ \cup \{\infty\}) \times (\mathbb{R}^{++} \cup \{\infty\})$, where, for any contingent constraint, $0 \leq l_r \leq c_r - e_r \leq u_r$, ending in contingent event x_c , $\xi(x_c) \in [l + \bar{\gamma}^-(x_c), u + \bar{\gamma}^+(x_c)]$.

We sometimes use interval bounded schedules for requirement events as well. For a requirement constraint $l_r \leq x_r - y_r \leq u_r$ ending in requirement event x_e , $\xi(x_e) = t \in [l_r, u_r]$ for some time t .

We once again revise our definition of situations, Ω_v , to reflect the impact of the variable-delay function on the space of observations.

Definition 18. Variable-Delay Situations

For an STNU S with k contingent constraints $\langle e_1, c_1, l_1, u_1 \rangle, \dots, \langle e_k, c_k, l_k, u_k \rangle$ and variable-delay function $\bar{\gamma}$, each *variable-delay situation*, ω_v , represents a possible set of *observed* values for all links in S , $\omega = (\omega_{v1}, \dots, \omega_{vk})$. The {space of situations} for S , Ω_v , is $\Omega_v = [e_1, c_1] + [\bar{\gamma}_1^-, \bar{\gamma}_1^+] \times \dots \times [e_k, c_k] + [\bar{\gamma}_k^-, \bar{\gamma}_k^+]$.

We see that the space of observations has likewise grown in the transition to variable observation delay. If $\bar{\gamma}^- < \bar{\gamma}^+$, Ω_v for variable observation delay is strictly larger than Ω_f for fixed-observation delay and Ω for vanilla STNUs.

Like the fixed-delay function for fixed-delay controllability, the variable-delay function relates an observation delay to a contingent event, independent of other events. We take a similar approach to defining variable-delay controllability, relative to fixed-delay controllability.

Definition 19. Variable-Delay Controllability

An STNU S is *variable-delay controllable* with respect to a variable-delay function, $\bar{\gamma}$, if and only if for the space of situations, Ω_v , there is an \mathcal{S} that produces a satisfying schedule for requirement events during execution, ξ .

Determining whether a given variable-delay STNU, S , is variable-delay controllable has two components [6]. The first is to derive a fixed-delay STNU, S' , with fixed-observation delay, γ , that is equivalent with respect to controllability. The second is to show that S' is fixed-delay controllable. Below, we reiterate the claims of

[6], demonstrating how to derive S' from S that is equivalent with respect to controllability. In Section 4.3.1, we first demonstrate how to transform the contingent links from S to S' , and demonstrate their correctness with respect to observation spaces, before following up with transformations to the requirement links to maintain the same scheduling semantics in S' .

4.3.1 Variable-Delay to Fixed-Delay Transformations

We now show how we transform a variable-delay STNU to a fixed-delay STNU in order to perform fixed-delay controllability checking.

For the following lemmas, let x_c be a contingent event in S and variable-delay function $\bar{\gamma}(x_c)$. Let x'_c be the transformed contingent event in S' with fixed-delay function, $\gamma(x'_c)$.

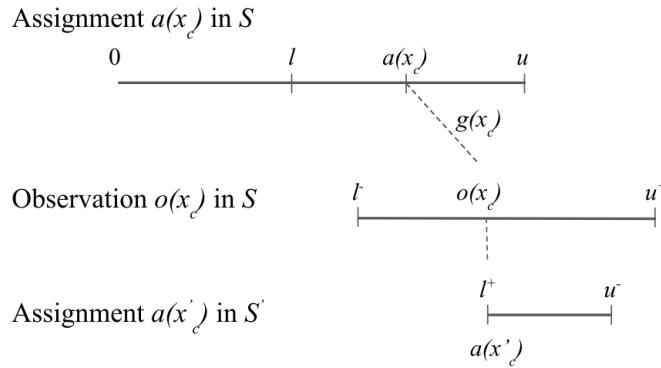


Figure 4-1: We visualize the relationship between realized assignments across S and S' . In this example, each horizontal line is a timeline monotonically increasing from left to right. Dashed lines represent observation delays. We see how an assignment in S , $\xi(x_c)$, realized observation delay, $\Gamma(x_c)$, and an observation in S , $\text{obs}(x_c)$, contribute to an assignment in S' , $\xi(x'_c)$.

Note that we receive $\text{obs}(x_c)$ from Nature, but make the assignment $\xi(x'_c)$ in the dispatchable form of S' . To be clear, while $\xi(x_c)$ is an interval, $(\mathbb{R} \cup \infty) \times (\mathbb{R} \cup \infty)$, $\xi(x'_c)$ is in \mathbb{R} . For a fixed interval, e.g. $\text{obs}(x_c) \in [t, t]$, we sometimes employ an equivalent representation, $\xi(x_c) = t$.

Additionally, we sometimes apply $-$ and $+$ superscripts to l and u to denote the earliest and latest times respectively that an assignment at those bounds could be

observed. For instance, the relationship in Definition 16 simplifies to,

$$\text{obs}(x_c) = [l + \bar{\gamma}^-(x_c), u + \bar{\gamma}^+(x_c)] \quad (4.1)$$

$$\text{obs}(x_c) = [l^-(x_c), u^+(x_c)] \quad (4.2)$$

Lastly, we need a means to compare observation spaces if we are to transform variable-delay to fixed-delay STNUs.

Definition 20. Observation Space Mapping

Let μ be a mapping from an assignment to a situation, $\mu : \xi \rightarrow \omega$. To say that $\mu(x'_c) \subseteq \omega_v(x_c)$ means that, for any assignment of x'_c in S' , there is an equivalent situation in S for x_c .

For the transitions below, it is a *valid observation space mapping*, if we can show that $\mu(x'_c) \subseteq \omega_v(x_c)$. If so, it is guaranteed that any assignment in the observation space of x'_c also has a valid assignment in the observation space of x_c .

We now have the necessary vocabulary and notation to step through the transformations from S to S' . These lemmas were first presented in [6], with some refinement by us for the aforementioned journal article submission.

Definition 21. Variable-Delay to Fixed-Delay Transformations

The *variable-delay to fixed-delay transformations* define a set of observation space mappings, where there are valid observation space mappings for all the contingent constraints in S' to S .

Thus, if there is a satisfying \mathcal{S} for the fixed-delay observation space of S' , it is guaranteed to simultaneously satisfy any situation in the variable-delay observation space, Ω_v , of S .

Lemma 1. *For any contingent event $x_c \in X_c$ in S , if $\bar{\gamma}^-(x_c) = \bar{\gamma}^+(x_c)$, we emulate $\bar{\gamma}(x_c)$ in S' using $\gamma(x'_c) = \bar{\gamma}^+(x_c)$.*

Proof. We translate an already fixed-bounded observation delay in the form of $\bar{\gamma}(x_c)$ to the equivalent fixed-delay function, $\gamma(x'_c)$, thus $\omega_f(x'_c) = \omega_v(x_c)$. \square

Lemma 2. For any contingent event $x_c \in X_c$, $\bar{\gamma}^+(x_c) = \infty$, we emulate $\bar{\gamma}(x_c)$ in S' as $\gamma(x'_c) = \infty$.

Proof. There are projections where we would not receive information about x_c , therefore we have to act as if we *never* receive an observation of x_c . Any \mathcal{S} that works when we do not receive information about x_c would also work when we receive an observation if we choose to ignore the observation.

None of our decisions depend on $\xi(x'_c)$, thus no observation space mapping to S is necessary. \square

Lemma 3. If $u - l \leq \bar{\gamma}^+(x_c) - \bar{\gamma}^-(x_c)$, we emulate $\bar{\gamma}(x_c)$ in S' using $\gamma(x'_c) = \infty$.

Proof. We can ignore observations of x_c because they are not guaranteed to narrow where $\xi(x_c)$ was assigned in the range $[l, u]$.

Let α be the range of $\text{obs}(x_c)$ when $\xi(x_c) \in [l, l]$. Let β be the range of $\text{obs}(x_c)$ when $\xi(x_c) \in [u, u]$. By Equation 4.1,

$$\alpha = [l^-(x_c), l^+(x_c)]$$

$$\beta = [u^-(x_c), u^+(x_c)]$$

We can show that $u^-(x_c) \leq l^+(x_c)$.

$$\begin{aligned} u - l &\leq \bar{\gamma}^+(x_c) - \bar{\gamma}^-(x_c) \\ u + \bar{\gamma}^-(x_c) &\leq l + \bar{\gamma}^+(x_c) \\ u^-(x_c) &\leq l^+(x_c) \end{aligned}$$

The lower bound of β is less than the upper bound of α , thus $\alpha \cap \beta$. An observation $\text{obs}(x_c) \in [u^-(x_c), l^+(x_c)]$ could be the result of $\xi(x_c) = [l, l]$, $\xi(x_c) = [u, u]$, or any value $\xi(x_c) \in [l, u]$. Observations provide no information about the underlying contingent constraint, therefore we ignore $\text{obs}(x_c)$.

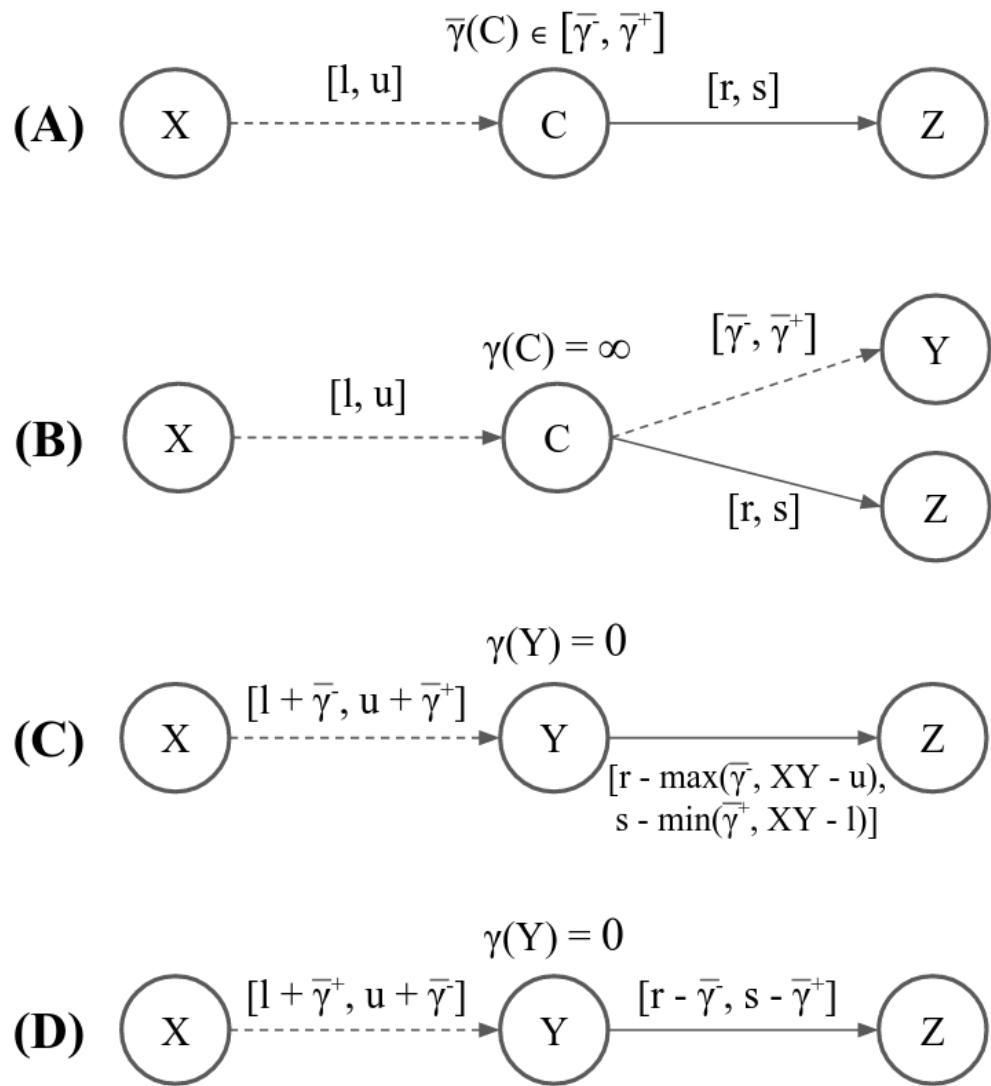


Figure 4-2: A visualization of the lemmas used to transform contingent links with variable observation delay and subsequent requirement links.

None of our decisions depend on $\xi(x'_c)$, thus no observation space mapping to S is necessary. \square

Lemma 4. *If $u - l > \bar{\gamma}^+(x_c) - \bar{\gamma}^-(x_c)$, we can emulate $\bar{\gamma}(x_c)$ under minimal information by replacing the bounds of x_c with $x'_c \in [l^+(x_c), u^-(x_c)]$ and letting $\gamma(x'_c) = 0$.*

Proof. Under Lemma 4, observations $\text{obs}(x_c)$ are guaranteed to narrow the range of $\xi(x_c)$.

We have the same ranges for α and β as in Lemma 3, however we can show that $u^-(x_c) \geq l^+(x_c)$ instead.

$$\begin{aligned} u - l &\geq \bar{\gamma}^+(x_c) - \bar{\gamma}^-(x_c) \\ u + \bar{\gamma}^-(x_c) &\geq l + \bar{\gamma}^+(x_c) \\ u^-(x_c) &\geq l^+(x_c) \end{aligned}$$

Thus, receiving an observation is guaranteed to narrow the derived range of $\xi(x_c)$. The transformation tightens the range of x'_c to one where there is maximum ambiguity of the assignment of x_c while guaranteeing an execution strategy for any assignment of $x_c \in [l, u]$. \square

After applying Lemma 4, despite the limited expected range of assignments in x'_c in S' compared to x_c in S , we can show that Lemma 7 guarantees a satisfying schedule for any $\text{obs}(x_c) \in [l^-(x_c), u^+(x_c)]$ using an \mathcal{S} that employs *buffering* and *imagining* contingent events.

Definition 22. Buffering

Buffering a contingent event x_c is an execution strategy where, if x_c is observed earlier than the lower bound of the observation space $\text{obs}(x_c) < \omega_f^-(x'_c)$, we assign $\xi(x'_c)$ to the lower bound of the observation space, $\xi(x'_c) = \omega_f^-(x'_c)$.

Definition 23. Imagining

Imagining a contingent event x_c is an execution strategy where, if x_c is observed later than the upper bound of the observation space, $\text{obs}(x_c) > \omega_f^+(x'_c)$, we assign $\xi(x'_c)$ to the upper bound of the observation space, $\xi(x'_c) = \omega_f^+(x'_c)$.

Lemma 5. *If S' is fixed-delay controllable after applying Lemmas 4, 6, and 7 to contingent event Y with following requirement event Z , there is a valid \mathcal{S} for any observation in the observation space of S , $\omega_v(Y) = [a^-(Y), b^+(Y)]$.*

Proof. We first note the observation space of S' is a subinterval of the original observation space of S , $\omega_f(Y') \subset \omega_v(Y)$, and there are two distinct ranges of observations that are not in $\omega_f(Y')$.

$$\begin{aligned}\omega_f(Y') &= [a + \bar{\gamma}^+(Y), b + \bar{\gamma}^-(Y)]; \quad \omega_v(Y) = [a + \bar{\gamma}^-(Y), b + \bar{\gamma}^+(Y)] \\ \omega_f(Y') &\not\supseteq [a + \bar{\gamma}^-(Y), a + \bar{\gamma}^+(Y)) \quad ("Early" \text{ observations}) \\ \omega_f(Y') &\not\supseteq (b + \bar{\gamma}^+(Y), b + \bar{\gamma}^-(Y)) \quad ("Late" \text{ observations})\end{aligned}$$

We address the early observations first. The range of early assignments of $\xi(Y)$ in S that we care about are the ones that could produce an observation $\text{obs}(Y) \leq a + \bar{\gamma}^+(Y)$, which is $\xi(Y) = [a, a + (\bar{\gamma}^+(Y) - \bar{\gamma}^-(Y))]$. We rewrite the range of early assignments as $\xi(Y) = a + (\bar{\gamma}^+(Y) - \bar{\gamma}^-(Y)) - \epsilon$, where $0 \leq \epsilon \leq (\bar{\gamma}^+(Y) - \bar{\gamma}^-(Y))$. By the semantics of S , the range of assignments of $\xi(Z)$ is then,

$$\begin{aligned}\xi(Z) &= [a + (\bar{\gamma}^+(Y) - \bar{\gamma}^-(Y)) - \epsilon, a + (\bar{\gamma}^+(Y) - \bar{\gamma}^-(Y)) - \epsilon] + [u, v] \\ \xi(Z) &= [a + u + (\bar{\gamma}^+(Y) - \bar{\gamma}^-(Y)) - \epsilon, a + v + (\bar{\gamma}^+(Y) - \bar{\gamma}^-(Y)) - \epsilon]\end{aligned}$$

The earliest assignment of Y' in S' is $\xi(Y') = a + \bar{\gamma}^+(Y)$. By the semantics of S' , the range of assignments of $\xi(Z')$ is then,

$$\xi(Z') = [a + \bar{\gamma}^+(Y), a + \bar{\gamma}^+(Y)] + [u - \bar{\gamma}^-(Y), v - \bar{\gamma}^+(Y)]$$

$$\xi(Z') = [a + u + (\bar{\gamma}^+(Y) - \bar{\gamma}^-(Y)), a + v]$$

We see that $\xi(Z') \subseteq \xi(Z)$ for any ϵ , meaning the execution strategy when $\xi(Y') = a + \bar{\gamma}^+(Y)$ results in a valid assignment of $\xi(Z)$ for all early observations of $\xi(Y)$. We are safe to buffer early observations to $\xi(Y') = a + \bar{\gamma}^+(Y)$.

We use the same argument for imagining late observations. The range of late assignments of $\xi(Y)$ in S that we care about are the ones that could produce an observation $\text{obs}(Y) \geq b + \bar{\gamma}^-(Y)$, which is $\xi(Y) = b - (\bar{\gamma}^+(Y) - \bar{\gamma}^-(Y)) + \epsilon$. By the semantics of S , the range of assignments of $\xi(Z)$ is then,

$$\xi(Z) = [b - (\bar{\gamma}^+(Y) - \bar{\gamma}^-(Y)) + \epsilon, b - (\bar{\gamma}^+(Y) - \bar{\gamma}^-(Y)) + \epsilon] + [u, v]$$

$$\xi(Z) = [b + u - (\bar{\gamma}^+(Y) - \bar{\gamma}^-(Y)) + \epsilon, b + v - (\bar{\gamma}^+(Y) - \bar{\gamma}^-(Y)) + \epsilon]$$

The last assignment of Y' in S' is $\xi(Y') = b + \bar{\gamma}^-(Y)$. By the semantics of S' , the range of assignments of $\xi(Z')$ is then,

$$\xi(Z') = [b + \bar{\gamma}^-(Y), b + \bar{\gamma}^+(Y)] + [u - \bar{\gamma}^-(Y), v - \bar{\gamma}^+(Y)]$$

$$\xi(Z') = [b + u, b + v - (\bar{\gamma}^+(Y) - \bar{\gamma}^-(Y))]$$

We see that $\xi(Z') \subseteq \xi(Z)$ for any ϵ , meaning the execution strategy when $\xi(Y') = b + \bar{\gamma}^-(Y)$ results in a valid assignment of $\xi(Z)$ for all late observations of $\xi(Y)$. In practice, there is no reason to wait until after $\text{obs}(Y) = b + \bar{\gamma}^-(Y)$ to receive a late observation. As soon as we see the clock has reached $b + \bar{\gamma}^-(Y)$, we are safe to imagine that $\text{obs}(Y)$ has been received. \square

This concludes the modifications required to transform a contingent event $x_c \in X_c$

in S to its equivalent $x'_c \in X_c$ in S' . What remains is to address the transformation of requirement links, $x_r \in X_r$, in S such that their transformed equivalents, $x'_r \in X_r$ in S' , express the same execution semantics in S' as they did in S . We will demonstrate the correctness of the transformations after Lemma 7.

Lemma 6. *If we have contingent link $X \Rightarrow C$ with duration $[l, u]$, outgoing requirement link $C \rightarrow Z$ with duration $[u, v]$ with an unobservable C , and contingent link $C \Rightarrow Y$ with range $[\bar{\gamma}^-(x_c), \bar{\gamma}^+(x_c)]$, we can emulate the role of the original requirement link during execution with a new link $Y \rightarrow Z$ with bounds $[u - \max(\bar{\gamma}^-(x_c), XY - l), v - \min(\bar{\gamma}^+(x_c), XY - l)]$, where XY is the true duration of $X \Rightarrow Y$.*

Proof. See Figure 4-2c for reference. From an execution perspective, X and Y are the only events that can give us any information that we can use to reason about when to execute Z (since C is wholly unobservable).

If we execute Z based on what we learn from Y , then we use our information from Y to make inferences about the true durations of $X \Rightarrow C$ and $C \Rightarrow Y$ based on $X \Rightarrow Y$. We know that the lower-bound of $C \Rightarrow Y$ is at least $XY - b$ and that its upper-bound is at most $XY - a$. But we also have the a priori bounds on the contingent link that limit its range to $[\bar{\gamma}^-, \bar{\gamma}^+]$. Taken together, during execution we can infer that the true bounds of $C \Rightarrow Y$ are $[\max(\bar{\gamma}^-, XY - b), \min(\bar{\gamma}^+, XY - a)]$. Since we have bounds only on Z 's execution in relation to C , we can then infer a requirement link $Y \rightarrow Z$ with bounds $[u - \max(\bar{\gamma}^-, XY - b), v - \min(\bar{\gamma}^-, XY - a)]$.

If we try to execute Z based on information we have about X , we must be robust to any possible value assigned to $X \Rightarrow C$. This means that we would be forced to draw a requirement link $X \rightarrow Z$ with bounds $[u + b, v + a]$. But we know that $u - \max(\bar{\gamma}^-, XY - b) \leq u + b - XY$ and $v - \min(\bar{\gamma}^-, XY - a) \geq v + a - XY$, which means that the bounds we derived from Y are at least as expressive as the bounds that we would derive from X . \square

Since we have a local execution strategy that depends on the real value of XY , we can try to apply this strategy to the contingent link that we restricted in Lemma 4, in order to repair the remaining requirement links.

Lemma 7. *If we have an outgoing requirement link $C \rightarrow Z$ with duration $[u, v]$, where C is a contingent event, we can emulate the role of the original requirement link by replacing its bounds with $[u - \bar{\gamma}^-(x_c), v - \bar{\gamma}^+(x_c)]$.*

Proof. See Figure 4-2d for reference. If we directly apply the transformation from Lemma 6 and Figure 4-2c to our original STNU, we introduce complexity through the need to reason over *min* and *max* operations in our link bounds. However, from Lemma 4, we know that in a controllability evaluation context, it is acceptable for us to simplify the $X \Rightarrow Y$ link to a stricter range of $[a + \bar{\gamma}^+, b + \bar{\gamma}^-]$, instead of $[a + \bar{\gamma}^-, b + \bar{\gamma}^+]$. This means that for the purpose of evaluating controllability, we can assume $a + \bar{\gamma}^+ \leq XY \leq b + \bar{\gamma}^-$. When we evaluate the requirement link $Y \rightarrow Z$, we see $\max(\bar{\gamma}^-, XY - b) = \bar{\gamma}^-$ and $\min(\bar{\gamma}^+, XY - a) = \bar{\gamma}^+$. This gives us bounds of $[u - \bar{\gamma}^-, v - \bar{\gamma}^+]$ for the $Y \rightarrow Z$ requirement link as seen in Figure 4-2d. \square

Lemma 7 handles outgoing requirement edges connected to contingent events. In addition, we must handle incoming edges.

Corollary 7.1. *If we have an incoming requirement link $Z \rightarrow C$ with duration $[u, v]$, where C is a contingent event, we can replace the bounds of the original requirement link with $[u + \bar{\gamma}^+(x_c), v + \bar{\gamma}^-(x_c)]$.*

Proof. A requirement link $Z \rightarrow C$ with bounds $[u, v]$ can be immediately rewritten as its reverse $C \rightarrow Z$ with bounds $[-v, -u]$. After reversing the edge, we can apply Lemma 7 to get $Y \rightarrow Z$ with bounds $[-v - \bar{\gamma}^-, -u - \bar{\gamma}^+]$, which we can reverse again to get $Z \rightarrow Y$ with bounds $[u + \bar{\gamma}^+, v + \bar{\gamma}^-]$. \square

We can examine a concrete example of Lemmas 4, 6, and 7 to show equivalence in the transformation from Figure 4-2a to 4-2d. We start by building an example of 4-2a. Let $X \xrightarrow{[2,5]} C$ with $\bar{\gamma}(C) \in [1, 2]$ and $C \xrightarrow{[11,20]} Z$. If we learn of event C at time 4, then one possibility is that the realized duration of C could have been 2 with an observation delay of 2. In this case, event Z must be executed in $[13, 22]$. However, if the realized duration of C were 3 with an observation delay of 1, then Z would fall in $[14, 23]$. Given we cannot distinguish between the possibilities, we

take the intersection of the intervals, yielding $Z \in [14, 22]$. Likewise, if we learn of C at time 6, then C could have been realized at time 5 with an observation delay of 1 or it could have been realized at time 4 with an observation delay of 2. In the first case, Z must then fall in $[16, 25]$, while in the second, Z would fall in $[15, 24]$. The intersection yields $[16, 24]$.

By the semantics represented in Figure 4-2d, we can build an equivalent network with $\gamma(Y) = 0$ by setting $X \xrightarrow{[4,6]} Y$ and $Y \xrightarrow{[10,18]} Z$. If Y is observed at time 4, Z must be executed in $[14, 22]$. If Y is observed at time 6, Z then must be executed in $[16, 24]$. The execution semantics for both cases match the equivalent networks from 4-2a described above.

4.4 Discussion

We have demonstrated a modeling formalism to describe temporal networks with uncertain observation delay, along with a sound and complete procedure for checking controllability of said temporal networks. VDC is sound because if it finds that S' has a valid execution strategy, then it must also be the case that S has an execution strategy. VDC is complete because if it finds that S' is not controllable, then there exists a projection of S that is uncontrollable, thus S is not variable-delay controllable.

4.5 Experimental Analysis

In this section, we provide empirical evaluations of our variable-delay controllability checking algorithms, showing that variable-delay controllability gives us a level of modeling expressiveness that cannot be captured by approximations that use delay controllability alone. We do so by constructing examples of variable-delay STNUs for realistic multi-agent coordination scenarios that are taken from the domain of planetary exploration, inspired by the real decision-making processes during Apollo EVAs and modern day EVA operations research. First, we briefly describe the operational environment, relevant actors, and decisions in EVAs. We then provide a selection of

STNUs that reflect the activities and temporal constraints of planetary exploration. Using these building blocks, we make a case for the expressivity of VDC in modeling uncertain communication, then generate larger STNUs to demonstrate the soundness of variable-delay controllability checking.¹

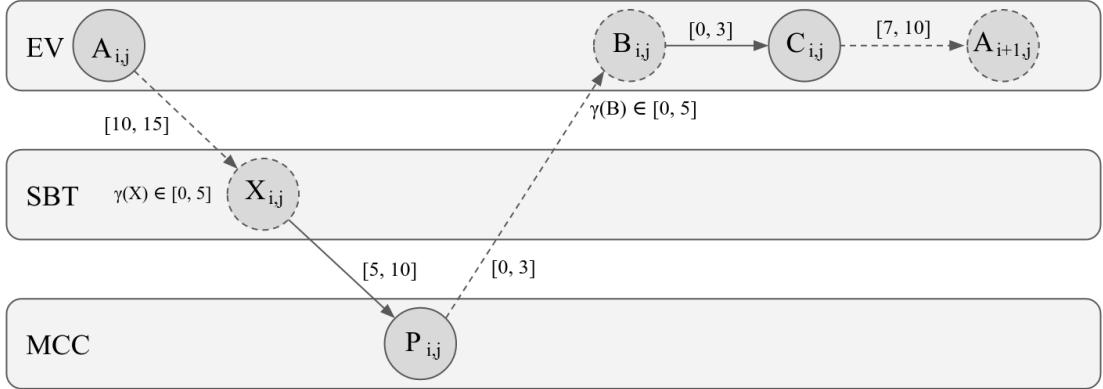


Figure 4-3: An STNU representing an EVA sampling task. The episode durations are representative of the bounds used in simulation. The depiction of this STNU with variable-delay is presented with rows representing actors to clarify the context of each event.

Now, we present a sample collection communication scenario in Figure 4-3 that is representative of the types of activities performed during exploration and requires uncertain communication delay to faithfully model.

At a high level, in this activity a crew of i astronauts perform j activities of scanning potential samples and receiving feedback from the science team as to whether they should store or discard those sample. Scanning requires liberating, that is chipping away, a piece of rock from an outcrop, $A_{i,j}$, and performing a scan of the newly exposed surface with a handheld spectrometer. Spectroscopy data is eventually received at $X_{i,j}$; we model this duration of this process with the contingent link $A_{i,j} \Rightarrow X_{i,j}$ where $X_{i,j}$ is uncontrollable because the time to liberate and scan is a function of the environment (eg. how hard the sample is to access), not the crew. The processing completion time of the handheld spectrometer is highly variable, and as such we have

¹The implementation of the experiments herein can be found at [<https://gitlab.com/mitmers/delay-stnu-benchmarks>].

$\bar{\gamma}(X_{i,j})$ represent a variable delay in receiving the results of the scan. Interestingly, note that the general time of $A_{i,j}$ will be known immediately through the use of audio and video communications - the variability of $X_{i,j}$ refers to the delay of receiving the spectroscopy data itself.

During a narrow window of opportunity between the receipt of the sample information and a deadline imposed by Mission Control, $P_{i,j}$, the science team must confer and decide on a sample collection priority list to send to Mission Control, $X_{i,j} \rightarrow P_{i,j}$. Even once Mission Control has a sample priority list in hand, $P_{i,j}$, due to health and safety concerns, they may prioritize other messages before they send the science team's sampling priority decision to the crew. As such, the message passing process, $P_{i,j} \Rightarrow B_{i,j}$, is modeled as uncontrolled with a variable communication delay. Once the crew receives the priority list, B , they then stow the requested amount of samples at $C_{i,j}$. Then the astronaut traverses to the next location and the procedure repeats anew. We use $C_{i,j} \Rightarrow A_{i,j+1}$ to model the time needed to traverse to the site of the next activity. We apply a requirement link with a lower-bound of 0 and an upper bound of the limiting consumable from the overall start of each STNU to its overall end after each astronaut has completed all activities.

With realistic STNUs in hand, we can now evaluate the performance of our variable-delay formulations. For the simulations presented in subsequent sections, we generated STNUs that follow the form of Figure 4-3 with randomized bounds on the links and delay functions, as will be described below.

We now will evaluate the comparative quality of variable-delay formulations against fixed-delay approximations by using the repeater installation scenario seen in Figure 5-3. We generate STNUs with four astronauts each performing five installations. We set the lower bounds of $A_{i,j} \Rightarrow B_{i,j}$ to 0 and choose the upper bounds from a uniform distribution of integers between 0 and 20, $\mathcal{U}_{[0,20]}$. There is no delay function for $B_{i,j}$. Likewise, for $B_{i,j} \rightarrow C_{i,j}$, we set the lower bounds to 0 and choose an integer upper bound in $\mathcal{U}_{[0,15]}$. $C_{i,j} \Rightarrow D_{i,j}$ has a lower bound of 0 and an upper bound integer chosen in $\mathcal{U}_{[0,20]}$. The variable-delay function $\gamma(D_{i,j})$ has a lower bound of 0 and upper-bound chosen from the exponential distribution $f(t) = \lambda e^{-\lambda t}$ with $\lambda = 3$. $D_{i,j} \Rightarrow A_{i,j+1}$ takes

	Variable-delay controllable	Variable-delay uncontrollable
Min-fixed controllable	222	619
Min-fixed uncontrollable	0	159
Mean-fixed controllable	222	583
Mean-fixed uncontrollable	0	195
Max-fixed controllable	222	355
Max-fixed uncontrollable	0	423

Table 4.2: Variable-delay vs. minimum, mean, and maximum fixed-delay controllability results with the parallel installation STNU from Figure 5-3.

a lower bound integer, a , from $\mathcal{U}_{[10,20]}$ and its upper bound in $a + \mathcal{U}_{[4,10]}$. Lastly, we pick a random limiting consumable as the multiple of the number of activities and an integer from $\mathcal{U}_{[50,60]}$.

We employ three different strategies for each $\gamma(x_c)$ in S for our fixed-delay approximations: $\gamma(x_c) = \bar{\gamma}^-(x_c)$, $\gamma(x_c) = \frac{\bar{\gamma}^- + \bar{\gamma}^+}{2}$, and $\gamma(x_c) = \bar{\gamma}^+(x_c)$. For each strategy, we know that whenever the original STNU is variable-delay controllable with respect to $\bar{\gamma}$, it is also fixed-delay controllable with respect to γ . Each choice of γ represents a potential realization of the delays offered by $\bar{\gamma}$, and the fixed-delay approximation has the added benefit of eliminating uncertainty in observation.

We generate 1000 different STNUs and compare the variable-delay controllability results to the different fixed-delay controllability approaches (Table 4.2). Note that our randomly generated variables, notably the choice of $\gamma(C_{i,j})$ and the width of the following $C_{i,j} \rightarrow D_{i,j}$ link, were selected such that the STNUs generated could be variable-delay, fixed-delay, dynamic, or strong controllable, or uncontrollable. The instances that are of greatest interest are those where the STNU is not variable-delay controllable but the fixed-delay approximations determine it to be controllable.

This false positive rate of the minimum fixed-delay controllability approximation is quite high at 80.0%. The mean and maximum fixed-delay approximations have more reasonable false positive rates at 74.9% and 45.6% respectively. Since all approximations yield the correct answer when the original STNU is variable-delay controllable,

	Variable-delay controllable	Variable-delay uncontrollable
Elongated controllable	36	0
Elongated uncontrollable	186	778

Table 4.3: Variable-delay controllability vs. the controllability of a network that elongates its contingent links to account for observational uncertainty when using an exponential delay function with $\lambda = 3$.

it follows that the maximum fixed-delay approximation has the lowest false positive rate, as it is the most demanding of the three.

We note that these results are dependent on the width of the variable-delay ranges found in the network. We can increase the likelihood that a delay takes longer by increasing the choice of λ in our exponential delay function. When we vary our delay function using $\lambda = 4.5, 6, 7.5$, and 9 , the false positives of the max-delay approximation are 27.9%, 12.9%, 7.0%, and 3.1%, respectively.

In addition to simulating the network using fixed-delays, we also consider the effect of combining the two sources of uncertainty, the duration of the action and the delay in observation, into one new source of uncertainty. Unlike the fixed-delay approximations, we know that if a network under this transformation is controllable, then so too is the original network, as this approach discards any existing knowledge about the difference in uncertainties between the original event and the observation of that event.

As seen in Table 4.3, this approach yields no false positives, but still presents a modestly high false negative rate of 19.3%. An appropriate approximation strategy can be adopted to prevent either false positives or false negatives; however, such a wide disparity in results strongly reinforces the value of modeling observational uncertainty directly.

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 5

Single-Agent Execution with Delayed Event Monitoring

Now that we have shown there exists a valid execution strategy for variable-delay controllable STNUs, we contribute a novel scheduling and dispatching architecture for online, dynamic execution. In this Chapter, our aim is to describe the single-agent form of a new instantiation of Kirk, *Delay Kirk*, that can reason over uncertain observation delay to decide when to execute requirement events on real hardware. There are two main components to Delay Kirk: (1) a *delay scheduler*, and (2) a *delay dispatcher*. As will be shown in Section 5.2, scheduling variable-delay controllable STNUs is an extension to existing dynamic scheduling algorithms with modifications for the execution strategy shown to be sound and complete in Chapter 4.

Additionally, to the best of our knowledge, scheduling fixed-delay STNUs has not been presented in the literature. Fixed-delay scheduling is required for addressing (1). As such, we contribute a fixed-delay scheduler in Section 5.2. The execution strategy from Chapter 4 will be shown to be a small extension to the fixed-delay scheduler. As to (2), to the best of our knowledge, there are no other formalized dispatching algorithms in the literature. In the development of Delay Kirk, we found it to be extremely useful to formalize dispatching as part of creating a clear interface boundary between scheduling and dispatching. The dispatching algorithms we put forth in Section 5.3.2 represent novel contributions to temporal reasoning.

This Chapter makes additional contributions to scheduling and dispatching. Safely executing events on real hardware requires modifications to generating decisions in dynamic scheduling. We include said modifications, with confluent interfaces in dynamic dispatching, to suit our intended use cases for Delay Kirk.

In Section 7.1, we extend our approach to scheduling variable-delay STNUs by introducing an optional procedure that addresses a shortcoming in the semantics of scheduling a variable-delay STNU. The shortcoming takes the form of potentially unnecessary wait times that are added after receiving contingent event assignments, extending the makespan of procedures. We present a generate-and-test algorithm to partially mitigate said shortcomings.

Finally, Section 5.4 provides a series of benchmarks of the scheduling and dispatching algorithms described in this Chapter.

5.1 Dynamic Scheduling through Real-Time Execution Decisions

We first provide a necessary overview of dynamic scheduling of vanilla STNUs, which we will extend for STNUs with observation delay in Section 5.2.

An STNU, S , that exhibits dynamic controllability can be *scheduled* dynamically (or *online*). At a high-level, dynamic scheduling is the process of mapping the history of event assignments to the execution time of future free events. We will build off of the scheduling work by Hunsberger [7], [39], which describes an $O(N^3)$ online procedure, FAST-EX, for dynamic scheduling of STNUs. We chose FAST-EX because, to the best of our knowledge, this is the fastest dynamic scheduling algorithm in the literature today. At its core is the notion of *Real-Time Execution Decisions* (RTEDs), which map a timepoint to a set of requirement events to be executed and are generated based on *partial schedules* of STNUs being executed. WAIT decisions may also be produced, reflecting the need to wait for the assignment of a contingent event before continuing. RTED-based scheduling applies a dynamic programming

paradigm in three steps:

1. creating a dispatchable form of temporal constraints offline in the form of a distance graph,
2. updating the dispatchable form as the partial schedule is updated online through event assignments, and
3. querying the dispatchable form online to quickly find the next RTED [40].

The dispatchable form employed by FAST-EX is the *AllMax* distance graph, which is produced by the Morris $O(N^4)$ DC-checking procedure [30].

Definition 24. AllMax Distance Graph [29]

The *AllMax* distance graph is a distance graph exclusively consisting of unlabeled and upper-case edges.

The key idea of FAST-EX is maintaining accurate distances from an artificial zero point, Z , of the distance graph to all events. At the outset of execution, all events from S are present as nodes in *AllMax*. As events are assigned, *AllMax* performs update steps using Dijkstra Single Source/Sink Shortest Path (SSSP) to maintain distances to unexecuted events, while also collapsing executed events to Z . We include pseudo-code of the real-time update step in Figure 1.

With an up-to-date distance graph in hand, we can perform an online query for the current RTED.

Definition 25. Real-Time Execution Decisions [40]

A *Real-Time Execution Decision* is a two-tuple $\langle t, \chi \rangle$, where:

- t is a time with domain \mathbb{R} ,
- χ is a set of $x_r \in X_r$ to be executed at time t

Let U_x be the set of unexecuted free timepoints. If U_x is empty, then the RTED is to **WAIT**. Otherwise, we find the lower bound of the earliest executable time point and the set of executable events associated with it.

Input: Time t ; Set of newly executed events $\text{Exec} \subseteq X_e \cup X_r$; AllMax Graph G ;
 Distance matrix D , where $D(A, B)$ is the distance from A to B

Output: Updated D

FAST-EX Update:

```

1   for each contingent event  $C \in \text{Exec}$  do
2     Remove each upper-case edge,  $Y \xrightarrow{C:-w} A$ , labeled by  $C$ ;
3     Replace each edge from  $Y$  to  $Z$  with the strongest replacement edge;
4   end
5   for each event  $E \in \text{Exec}$  do
6     Add lower-bound edge  $E \xrightarrow{-t} Z$ ;
7   end
8   For each event  $X$ , update  $D(X, Z)$  using Dijkstra Single-Sink Shortest
    Paths;
9   for each event  $E \in \text{Exec}$  do
10    Add upper-bound edge  $Z \xrightarrow{t} E$ ;
11  end
12  For each event  $X$ , update  $D(Z, X)$  using Dijkstra Single-Source Shortest
    Paths;
```

Algorithm 1: Algorithm for updating distances for all events in relation to Z upon the execution of an event. Adapted from [3], Fig. 19.

$$t = \min\{-D(X, Z) \mid X \in U_x\} \quad (5.1)$$

$$\chi = \{X \in U_x \mid -D(X, Z) = t\} \quad (5.2)$$

We cannot execute events in the past. Let `now` be the current time, i.e. the last timepoint captured in the event assignments. It is possible that $t \leq \text{now}$, in which case we must reassign t to guarantee that $t > \text{now}$. To do so, we update t as follows, where t^+ is earliest upper bound of the executable timepoints,

$$t^+ = \min\{D(Z, X) \mid X \in U_x\} \quad (5.3)$$

$$t = \frac{\text{now} + t^+}{2} \quad (5.4)$$

So long as $t^+ > \text{now}$, we know that the reassignment of t ensures $t > \text{now}$.

5.2 Delay Scheduling as an Extension to Dynamic Scheduling

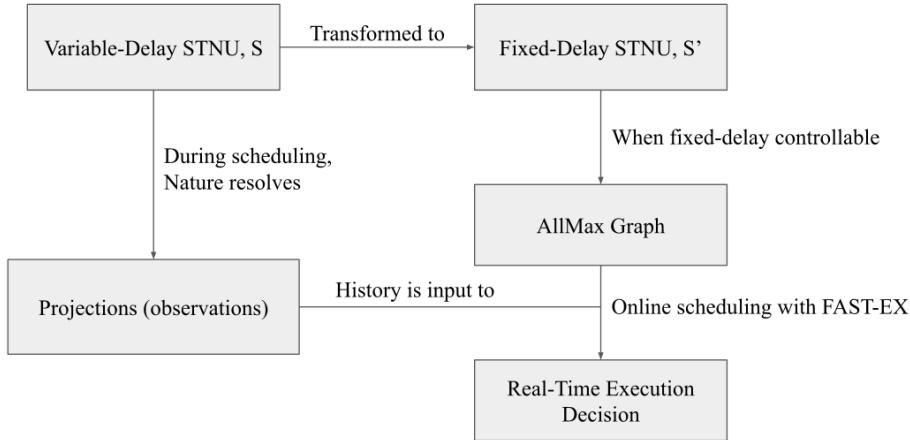


Figure 5-1: A high-level flow chart showing how we use variable-delay STNUs to generate scheduling decisions. The boxes represent the data structures involved in scheduling, while the arrows are the processes that are followed to eventually produce RTEDs.

Figure 5-1 presents a high-level overview of the information flow in the scheduling process.

In order to schedule a variable-delay STNU, the core problem we must address is that, to date, there is no means to directly create a corresponding dispatchable form that accounts for uncertain assignments resulting from variable observation delay. We encountered this same problem when describing the process of checking VDC in Section 4.3. We overcame this limitation by first transforming the variable-delay STNU to a fixed-delay STNU before checking FDC. A similar strategy will be followed for scheduling in that we will transform the variable-delay to a fixed-delay STNU, then dispatch events using the dispatchable form of the fixed-delay STNU instead. However, doing so creates a second problem. While we will be performing FAST-EX against the fixed-delay STNU, the contingent event observations we receive will adhere to the constraints and variable-delay function of the variable-delay STNU. Hence, we must modify our real-time update and RTED generation algorithms to account for early and late contingent event observations.

We start by providing an explanation of fixed-delay scheduling, before expanding it to address the execution strategies of variable-delay scheduling.

5.2.1 Fixed-Delay Scheduling

We first establish the algebra of receiving observations.

Lemma 8. *For any contingent event, $x_c \in S$ or $x'_c \in S'$, observing x_c at time $t \in [l^-(x_c), u^+(x_c)]$ fixes the observation to $\text{obs}(x_c) = [t, t]$.*

Proof. Prior to execution, an observation of x_c may fall anywhere within the set-bounded interval from the earliest possible observation at $l^-(x_c)$ to the last possible observation at $u^+(x_c)$. Receiving an observation $\text{obs}(x_c) = t$ during execution eliminates all possible observations outside the interval $[t, t]$. \square

Lemma 9. *For any temporal constraint, x , with bounds $x \in [l, u]$ for some l and u , and timepoint $t \in [l, u]$, if information reduces the bounds of x to $x \in [t, t]$, we may assert $x = t$.*

Proof. When the bounds of an interval, $x \in [l, u]$ are fixed such that $t = l = u$, we can assert that x must have resolved to t . \square

Lemma 10. *For any contingent event $x'_c \in X_c$ in fixed-delay controllable S' , if $\gamma(x'_c) \in \mathbb{R}$, we assign $\xi(x'_c) = \text{obs}(x_c) - \gamma(x'_c)$ in the dispatchable form of S' .*

Proof. The central challenge of checking fixed-delay controllability is determining that an execution strategy exists that allows an agent to wait an additional $\gamma(x'_c)$ time units after a contingent event has been assigned to learn its outcome. Importantly, the γ function is not used to modify the edges of the labeled distance graph, which are derived from the constraints $r \in R_e \cup R_c$ in S' .

As $\gamma(x'_c)$ resolves to a known and finite value, we can derive the true value of $\xi(x'_c)$ to be assigned in the labeled distance graph. Contingent event assignments are recorded in the labeled distance graph as follows, where $\text{obs}(x_c)$ is the resolved observation,

$$\xi(x'_c) = \text{obs}(x_c) - \gamma(x'_c) \quad (5.5)$$

□

The FAST-EX real-time update algorithm, Algorithm 1, then becomes Algorithm 2.

Input: Time t ; Set of newly observed events $\text{Exec} \subseteq X_e \cup X_r$; AllMax Graph G ; Distance matrix D , where $D(A, B)$ is the distance from A to B ; Fixed-delay function γ ;

Output: Updated D

FAST-EX Update with Fixed Observation Delay:

```

1   for each contingent event  $C \in \text{Exec}$  do
2      $\xi(C) \leftarrow \text{obs}(C) - \gamma(C);$ 
3     Remove each upper-case edge,  $Y \xrightarrow{C:-w} A$ , labeled by  $C$ ;
4     Replace each edge from  $Y$  to  $Z$  with the strongest replacement edge;
5   end
6   for each event  $E \in \text{Exec}$  do
7     Add lower-bound edge  $E \xrightarrow{-t} Z$ ;
8   end
9   For each event  $X$ , update  $D(X, Z)$  using Dijkstra Single-Sink Shortest
  Paths;
10  for each event  $E \in \text{Exec}$  do
11    Add upper-bound edge  $Z \xrightarrow{t} E$ ;
12  end
13  For each event  $X$ , update  $D(Z, X)$  using Dijkstra Single-Source Shortest
  Paths;
```

Algorithm 2: Algorithm for updating distances for all events in relation to Z upon the execution or observation of an event.

No other modifications to FAST-EX are required to schedule a fixed-delay STNU.

5.2.2 Variable-Delay Scheduling

Our execution strategy must address each of the following special categories of contingent event observations:

1. contingent events with infinite observation delay,

2. contingent events that are observed outside $[l^+(x_c), u^-(x_c)]$ in S' .

The first category is a requirement for dispatching the fixed-delay equivalent of a variable-delay STNU. If the constraints of a problem domain are modeled directly in a fixed-delay STNU and the modeler gives a contingent event, x_c , infinite delay, e.g. $\gamma(x_c) = \infty$, the event will never be observed and thus a fixed-delay scheduler has no need for an execution strategy in the event that x_c is observed. However, by Lemmas 2 and 3 there are some contingent events with potentially finite observation delay in S that are transformed to infinite observation delay in S' , making it possible that the scheduler receives observations of them.

Lemma 11. *For any contingent event $x'_c \in X_c$ in fixed-delay controllable S' , if $\gamma(x'_c) = \infty$, we mark the event executed but do not assign $\xi(x'_c)$ in the dispatchable form of S' .*

Proof. If we are scheduling a fixed-delay STNU, S' , that is already known to be fixed-delay controllable, an execution strategy must exist that is independent of the assignment of $\xi(x'_c)$ when $\gamma(x'_c) = 0$. We are not required to record $\xi(x'_c)$ when $\gamma(x'_c) = \infty$ to guarantee controllability and may safely ignore it.

We mark the event executed to prevent it from appearing in future RTEDs. \square

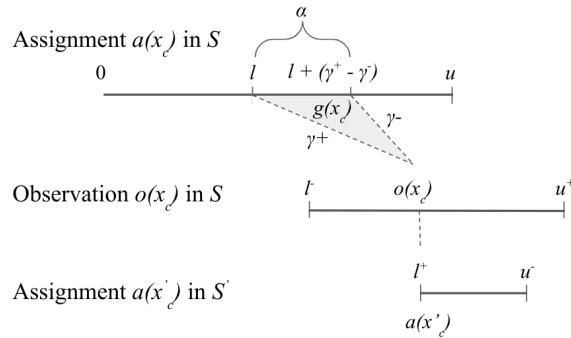


Figure 5-2: Here, we show how the combination of $\xi(x_c)$ and $\bar{\gamma}(x_c)$ lead to an assignment of $\xi(x'_c)$ in S' . We see the range $\alpha \in [l, l + \bar{\gamma}^+(x_c) - \bar{\gamma}^-(x_c)]$ representing the earliest and latest assignments of $\xi(x_c)$ that could result in $\text{obs}(x_c) \in \xi(x'_c) \in [l^+(x_c), l^+(x_c)]$. The grey region represents the range of possible observation delays, $\bar{\gamma}(x_c)$, supporting $\xi(x'_c) \in [l^+(x_c), l^+(x_c)]$.

The second category refers to the need for buffering and imagining events as a result of Lemma 4 using the execution strategy proven to be valid in Lemma 5. There are three regimes of contingent event observations to address.

1. $\text{obs}(x_c) \in [l^-(x_c), l^+(x_c))$, ie. strictly earlier than the range of $\xi(x'_c)$,
2. $\text{obs}(x_c) \in [l^+(x_c), u^-(x_c)]$, ie. the range equivalent to x'_c , and
3. $\text{obs}(x_c) \in (u^-(x_c), u^+(x_c)]$, ie. strictly later than the range of $\xi(x'_c)$.

Note that we omit the $-\gamma(x'_c)$ term from Equation 5.5 in this analysis due to the fact that $\gamma(x'_c) = 0$ after applying Lemma 4.

Our execution strategy is to then make the following assignments during the FAST-EX real-time update.

$$\xi(x'_c) = \begin{cases} & \\ & \end{cases} \quad (5.6)$$

In the first case, we cannot immediately schedule buffered events. It may be the case that there are other unexecuted timepoints between $\text{obs}(x_c)$ and $l^+(x_c)$. If we make an assignment at $l^+(x_c)$, we would be preempting later timepoints, which would cause us to later make assignments in the past, which invalidates our assumptions of partial history. Thus, we buffer x'_c in the sense that we wait until $l^+(x_c)$ to assign $\xi(x'_c) = l^+(x_c)$.

In the last case, late observations are assigned to an earlier time. During execution, time is always increasing. There is no need to wait to make an observation after $u^-(x_c)$. Instead, we modify RTED generation, namely Equation 5.1, such that we dispatch x'_c at $u^-(x_c)$ if it is not been observed before $u^-(x_c)$. Let U_c be the set of unobserved contingent timepoints.

$$t_x = \min\{-D(X, Z) \mid X \in U_x\} \quad (5.7)$$

$$t_c = \min\{D(Z, X) \mid X \in U_c\} \quad (5.8)$$

$$t = \min\{t_x, t_c\} \quad (5.9)$$

$$\chi_x = \{X \in U_x \mid -D(X, Z) = t\} \quad (5.10)$$

$$\chi_c = \{X \in U_c \mid D(Z, X) = t\} \quad (5.11)$$

$$\chi = \chi_x \cup \chi_c \quad (5.12)$$

We see that RTEDs may now include unobserved (or unexecuted) contingent timepoints at their upper bounds. Note that there is no need to distinguish between contingent events that are the result of tightening during the fixed-delay transformation by applying Lemma 4 and others. We assume that the contingent constraints of the variable-delay STNU accurately reflect Nature. The latest any other contingent event should be observed is their upper bound in S' and thus should never be in the set of events, χ , of an executed RTED.

We have defined variable-delay execution strategies for when contingent events have infinite delay and tightened constraints. The remaining category of contingent events is when a contingent event has a finite, non-zero $\gamma(x'_c)$ in S' . If that is the case, x'_c must have had fixed observation delay in S , Lemma 1, and can be scheduled normally after backing out the observation delay with Equation 5.5.

We have addressed the key issue of reconciling observations from S with the dispatchable form from S' . We now present a dispatcher and wrapper algorithms on top of FAST-EX that combine to add robustness for variable observation delay.

5.3 Dynamic Dispatching of STNUs with Observation Delay

The terms “scheduling” and “dispatching” are often used interchangeably in temporal reasoning literature. However, we distinguish the goals of a scheduler, as described above, and a dispatcher, described here.

- **Scheduling:** Generating RTEDs based on a partial schedule.
- **Dispatching:** Reasoning over a clock and RTEDs to guarantee that requirement events are safely executed (w.r.t. controllability).

We assume that events in an STNU map 1:1 to actions in the real world. To put the design of the dispatcher in context, it is worth considering what events may look like. In the case of a robotic agent, requirement events may represent the instantaneous timepoints when motion plans begin, while contingent events could be anything from the completion of said motion plans to the receipt of `PROCEED` messages from a third party. For a human, requirement events could be presented in a mission timeline as the start of planned actions such as the collection of scientific samples. The end of a sampling activity would then be a contingent event. Or contingent events could be the actions performed by other agents, like say another astronaut on an EVA, with whom temporal constraints are shared. In both the case of the robot and the human, a robust dispatcher should take into consideration that passing a message to the agent telling it to execute a requirement event does not cause the event to occur instantaneously. Put in other words, dispatching is not the same as assignment. A robot may require offline processing before it executes the motion plan. Or a human may need to acknowledge that they have started the activity their mission timeline has told them to perform. Neither is a problem, though, for our chosen formalism for temporal reasoning so long as each requirement event is assigned at some point within their constraints in the STNU. In our view, the dispatcher is responsible for ensuring requirement constraints are met by both monitoring the real-world and interfacing with hardware to cause actions to be performed.

We finally introduce a third component, the *driver*, that can interpret dispatched events and cause some action to be performed in an exogenous system. For instance, if Delay Kirk is controlling a robotic arm, the driver might be responsible for forming and publishing ROS messages when the dispatcher dispatches an event. If Delay Kirk is managing an astronaut’s EVA schedule, the driver might be responsible for causing a heads up display to alert the astronaut to start their sample collection procedure.

In this Section, we contribute a set of algorithms for building the dispatcher for a robust executive that can reason over observation delay and safely enact the actions symbolized in requirement events in the real world. Dynamic dispatching is designed around the two interfaces of scheduling - the input of partial schedules and output of RTEDs. As such, we focus on the interpretation, management, and flow of RTEDs in Section 5.3.2 and observing events in Section 5.3.3. But first, we present a novel view on RTEDs that is required for dispatching events to real hardware in Section 5.3.1.

5.3.1 Guaranteeing Agents Receive Actionable Events

We take the view that events in an STNU may be interpreted as commands by the driver. It is improper to knowingly send an invalid command. Accordingly, the driver must never receive a dispatched event that cannot be mapped to a corresponding action in its exogenous system. As such, it is the dispatcher’s responsibility to filter events in order to only dispatch valid commands to the driver.

In a variable-delay STNU, there are events that need to be executed by the driver and there are events that do not. We call these *real* and *noop* (“no operation”) events. Both contingent *and* requirement events may fall into either category. Below, we present our rationale for the distinction between real and no-op events, and how we modify real-time execution decisions accordingly.

To start, imagined contingent events are no-ops. They are assignments we artificially perform with no corresponding real-world action, and solely exist to maintain the controllability of the fixed-delay dispatchable form. Imagined events should never be dispatched to a driver.

There are requirement events that are also no-ops. Consider the process of nor-

malization of an STNU [30]. While building the labeled distance graph during a DC check, we rewrite contingent links such that their lower bounds are always 0. For instance, for a contingent event C and free event E , $C - E \in [l, u]$, during normalization we create a new requirement event, C' , fixed at the lower bound of the contingent link, and then shift the bounds of the contingent link to start at 0 while maintaining the original range, $u - l$. This results in two constraints: $E - C' \in [l, l]$ and $C - C' \in [0, u - l]$ that still reflect the original contingent link's semantics.

Importantly, the requirement events representing the normalized lower bounds of contingent events are in the dispatchable form for dynamic scheduling because we draw the AllMax graph directly from the DC check. To a scheduler, there is no distinction between the semantics of a real event, as modeled by a human planner writing an STNU for an agent to execute, and C' , an artifact of checking controllability. Both are modeled in the AllMax distance graph forming the basis of RTED generation. However, an agent does not need to execute any task in the outside world to satisfy $E - C'$. Thus, we make the following addendum to the definition of RTEDs.

Definition 26. Event-No-op Pair

An *Event-No-op Pair*, *event-noop*, is a two-tuple, $\langle x, noop \rangle$, where:

- x is an event in $X_e \cup X_c$,
- $noop$ is a boolean, where if true, the event cannot be interpreted by the driver, else the event is a valid command.

Definition 27. RTED with Operational Distinction

A *Real-Time Execution Decision with Operational Distinction* is a two-tuple $\langle t, event\text{-}noops \rangle$, where:

- t is a time with domain \mathbb{R} ,
- *event-noops* is a set of *event-noop* pairs to be executed at time t .

For convenience and simplicity, and given the similarities between RTED and RTED with Operational Distinction, future references to RTEDs will always refer to RTEDs with Operational Distinctions.

5.3.2 Dynamic Event Dispatching

The dynamic dispatcher runs the main loop of the executive’s temporal reasoning routine. It consists of a dispatching routine and some type of outer loop monitoring it. The dispatching routine, Algorithm 4, is responsible for retrieving the latest RTEDs and firing driver commands when the clock indicates that the agent has reached time t corresponding to the latest RTED. The outer loop allows the dispatching routine to run until the scheduler reports there are no requirement events remaining.

The dispatcher requests RTEDs with blocking synchronous calls, while the dispatcher and driver communicate asynchronously. The dispatcher spawns a thread to make non-blocking calls to the driver’s interface to execute events. The dispatcher and driver also share a FIFO queue that the driver can append messages to indicating the successful execution of events.

We now provide a walkthrough of the dynamic dispatching algorithm. For simplicity’s sake, the term *schedule* here is shorthand for whatever data structures the scheduler uses to generate RTEDs. *Updating the schedule* refers to running the fixed-delay FAST-EX update, Algorithm 2, using the variable-delay execution strategy from Section 5.2.

The interaction between the dispatching routine and monitoring loop is limited. Algorithm 4 returns a Boolean indicating whether there are executable events remaining. Here, the monitoring loop is a simple `while` that repeats until it receives `false` from the inner loop. Otherwise, the only communication between the dispatching routine and outer loop is a variable containing the last RTED that was generated but not executed. The outer loop creates the variable and passes it by reference to the dispatching routine, which is free to use or modify the variable as it sees fit.

We break the dispatching routine into three distinct phases.

1. Receive execution confirmation from the driver.
2. Collect an RTED and confirm the clock time matches RTED time t .
3. If there is an RTED:
 - (a) send executable events to the driver, else

- (b) immediately assign all *no-op* events to the current time.

Our goal in the dispatching routine is to dispatch events to the driver only after updating the schedule, collecting an up-to-date RTED, and confirming we are within the time window of the RTED. The routine will exit before reaching the dispatch step if any conditions are not met.

For the first step, we ask the scheduler if there are any remaining executable events. If there are none, we return `false` to signal the loop's termination, otherwise we continue.

Next, we check the FIFO queue for any event execution messages returned from the driver. The presence of a message would indicate that the driver has successfully executed a free event. We iteratively pop messages off the queue and update the schedule with the events and execution time contained in each message. Note that the scheduler update is a blocking operation because we need an up-to-date schedule to guarantee future RTEDs are consistent. We then invalidate the last RTED generated.

The second step starts once we have popped all messages from the driver off the queue. If we do not have a valid RTED from the last iteration of the routine, we ask the scheduler for one and save it to the referenced variable from the outer loop. Given that we interact with the driver asynchronously, it is possible that the current RTED is one that has already been sent to the driver but we have yet to receive an acknowledgment message confirming its execution. If so, there is nothing to do so we return `true`.

Lastly, we compare the suggested time in the RTED against the clock's elapsed time. Given the relationship between the scheduler, routine, and driver, we do not assume that dispatched events are executed instantaneously by the driver. We know that execution contends against delays such as the computational time in simply calling a function, to network latency, to robotic hardware that takes a moment to interpolate a motion plan from waypoints. In some contexts, it may make sense to preempt execution by dispatching events some small amount of time *before* the clock time reaches the RTED execution window. We call this preemption time ϵ , where $\epsilon \in \mathbb{R}^{\geq 0}$. Thus, we dispatch events, signaled by `dispatch-p`, when `dispatch - p =`

$(t_{RTED} - t_{clock} \leq \epsilon)$. If $\epsilon = 0$, the dispatcher is not allowed to preemptively dispatch events before the RTED time. We allow the human operator to choose an ϵ that is consistent with the operational context for the driver.

If `dispatch-p` is `false`, we are too early to execute the RTED and so the loop returns `true`. Otherwise we continue.

Once we reach the third stage, we are guaranteed to be able to safely dispatch events because (1) we have confirmed that the RTED we have in hand has unexecuted events that have never been dispatched, and (2) that we are in a time window that the scheduler has told us is consistent with the STNU's constraints. Going forward, we take advantage of the operational distinction we added to Hunsberger's RTEDs in Definition 27. Using the *no-op* property of each *event-noop* pair in the RTED, we filter the *event-noop* pairs into a set of *no-op* events and a set of real events. In the event that a contingent event and its normalized lower bound are to be scheduled at the same time, we schedule the *no-op* events first. The real events are then asynchronously sent to the driver.

Finally, because events were dispatched, the dispatching routine returns `true`.

Initialization: $RTED_{last} \leftarrow \emptyset$

Dynamic Dispatching Outer Loop:

```

1   while Calling inner loop with  $RTED_{last}$  returns true do
2     |   continue
3   end

```

Algorithm 3: The outer loop of the dynamic dispatching algorithm.

The biggest contributor to the performance of the dispatching routine, Algorithm 4, is updating the schedule. Assuming the *Scheduler* is the Delay Scheduler described in Section 5.3, then performing an assignment of an event will trigger the FAST-EX update that runs in $O(N^3)$ [7, p. 144] with the number of events in the STNU. In the worst case, the dispatcher confirms that all events in the STNU have arrived at the same time, whether as messages from the driver in the FIFO queue, or RTED *noop* events. Each event would trigger a schedule update. Thus, the dynamic dispatching routine runs in $O(N^4)$ in the worst case.

Input: Scheduler; Driver; FIFO queue, Queue; RTED_{last}; ϵ ;

Output: Boolean whether the outer loop should continue

Initialization: events_{real} $\leftarrow \{\}$; events_{noop} $\leftarrow \{\}$;

Dynamic Dispatching Routine:

```
1   if Scheduler has no more unexecuted events then
2   |   return false;
3   |   endif
4   |   for message in Queue do
5   |   |   Pop message;
6   |   |   for event, texecution in message do
7   |   |   |   Set  $\xi(\text{event}) = t_{\text{execution}}$  in Scheduler;
8   |   |   end
9   |   |   RTEDlast  $\leftarrow \emptyset$ ;
10  |   end
11  |   RTED  $\leftarrow$  a new RTED from Scheduler; //Equations 5.2 and 5.4
12  |   if RTED = RTEDlast then
13  |   |   return true;
14  |   |   endif
15  |   |   RTEDlast  $\leftarrow$  RTED =;
16  |   |   if tRTED - tcurrent >  $\epsilon$  then
17  |   |   |   return true;
18  |   |   endif
19  |   |   for event-noop pair in RTEDevent-noops do
20  |   |   |   if event-noop[noop] is true then
21  |   |   |   |   Add event-noop[x] to eventsnoop;
22  |   |   |   else
23  |   |   |   |   Add event-noop[x] to eventsreal;
24  |   |   |   endif
25  |   |   end
26  |   |   for event in eventsnoop do
27  |   |   |   Set  $\xi(\text{event}) = t_{\text{RTED}}$  in Scheduler;
28  |   |   end
29  |   Asynchronously send all eventsreal to the Driver;
30  |   return true;
```

Algorithm 4: The dynamic dispatching routine.

5.3.3 Observing Contingent Events

The dispatcher relays contingent event observations to the scheduler. In the base case, when a contingent event is observed, the dispatcher updates the schedule with the event and current clock time. If this were the only responsibility of the dispatcher when receiving a contingent event, we would end the section here. However, this interface is also where we implement an *Optimistic Rescheduling* technique to address a problem inherent to the buffering performed by the Delay Scheduler.

We describe Optimistic Rescheduling below and present the full contingent event observation algorithm.

5.3.4 Optimistic Rescheduling

We return to problem of potentially unnecessary wait time created by the buffering execution strategy described in Lemma 5. First, we use an example to demonstrate how buffering early contingent events results in a reduction of the execution space. Then we contribute a technique for managing event observations that circumvents the loss of execution space.

Consider the following variable-delay controllable STNU, which we will refer to as *Bufferable*.

$$A \xrightarrow{[1,7]} B \xrightarrow{\bar{\gamma} \in [1,3]} C$$

Following the semantics of the delay scheduler, we would first transform *Bufferable* to its fixed-delay equivalent, *Bufferable'* by applying Lemma 4.

$$A' \xrightarrow{[4,8]} B' \xrightarrow{\gamma=0} C'$$

If we assume A is executed at $t = 0$, the only question is when to schedule C (or its fixed-delay equivalent, C'). According to the semantics of *Buffering*, if B is observed at $t = 2$, we know that B was assigned at $t = 1$. Thus, we only need to wait until $t = 6$ to schedule C . However, the delay scheduler would schedule according the

constraints found in *Buffering'*, wherein $\xi(B') = 2$ falls earlier than the lower bound of $A' \xrightarrow{[4,8]} B'$, triggering Lemma 5. As a result, we act as if $\xi(B') = 4$ and then wait for the lower bound of $B' \xrightarrow{[4,6]} C'$. The end result is that C' is assigned to a later time of $t = 8$.

From a human mission manager perspective, this wait appears to be a waste. Time is money. And in the case of planetary exploration, time is safety. If a NASA flight controller were to ask why your software is telling astronauts on Moon to just stand there doing nothing, responding that your algorithm *does not know* if it is safe to act, would be unacceptable. Therefore, we contribute a generate-and-test approach that looks for opportunities to avoid buffering when contingent events arrive before their expected windows in the fixed-delay STNU. The goal of this method is to dispatch future events earlier if possible.

At its core, optimistic rescheduling consists of copying the original variable-delay STNU then rewriting it to reflect the resolution of uncertainty so far. Key to rewriting the variable-delay STNU is narrowing the constraint and observation delay to match what was observed. We then re-perform controllability checks. If controllable, we have a new schedule that removes the need to buffer this contingent event. If not controllable, we do nothing, buffer the contingent event as planned, and continue dispatching against the original schedule.

We now step through the Event Observations with optimistic rescheduling algorithm (Algorithm 8) in detail.

We cannot know if an event is buffered if we do not attempt to schedule it. Our first step is to schedule an event like normal. If scheduling is possible without buffering, we simply return whether scheduling was successful.

If the event was buffered, then we begin to optimistically reschedule. We do so by tightening the bounds of the original VDC STNU, $S_{original}$, based on the observation we received, which is the responsibility of Algorithm 9, implementing Lemma 13.

If the rewritten STNU, S^* , is found to be VDC, we prepare to schedule it. First we iterate through all the assignments in the partial schedule and make the same assignments against the new STNU. When assignments are made, we subtract out

Input: Original VDC STNU S ; Equivalent fixed-delay function γ ;
 Partial history ξ ; Executed events map $Ex(S, x)$; Observed contingent event x ;
 Normalized lower bound \hat{x} ; Current time t ;
Output: Boolean whether x was successfully scheduled, VDC STNU

Event Observations with Optimistic Rescheduling:

```

1   successp, bufferedp ← updateSchedule(S, x, t);
2   if  $\neg$ bufferedp then
3   |   return successp, S;
4   endif
5    $S^* \leftarrow \text{rewriteSTNU}(S, x, t)$ ;
6   if  $S^*$  is not variable-delay controllable then
7   |   return successp, S;
8   endif
9   for  $a$  in  $\xi$  // $a$  is an assignment
10  do
11  |   if  $\gamma(a[\text{event}]) \neq \infty$  then
12  |   |   updateSchedule( $S^*$ ,  $a[\text{event}]$ ,  $a[\text{time}] + \gamma(a[\text{event}])$ );
13  |   endif
14  end
15  for  $event$  in  $Ex(S)$  do
16  |    $Ex(S^*, x) \leftarrow Ex(S, x)$ 
17  end
18  updateSchedule( $S^*$ ,  $\hat{x}$ ,  $t$ );
19
20  return true,  $S^*$ ;
```

Algorithm 5: An Algorithm for observing contingent events with optimistic rescheduling.

the fixed observation delay. In this loop, we add the observation delay back, lest it be subtracted from the original observation twice.

If any contingent events with infinite delay were observed, they would have been marked executed but not assigned. We iterate through the executed events of S and mark the same events executed in S^* .

The distance graph, partial schedule, and executed events of S^* now match that of S before x_c was received. We are almost safe to record a new observation. Lastly, we must address the executable event representing the normalized lower bound of x_c , \hat{x}_c . During scheduling, we would have received an RTED consisting of $\langle l + \bar{\gamma}^+(x_c), \hat{x}_c \rangle$. Given that x_c arrived before $l + \bar{\gamma}^+(x_c)$, we never would have assigned \hat{x}_c , so we assign $\xi(\hat{x}_c) = t$ now. We finally update the schedule with the contingent event that arrived.

Lemma 12. *If a contingent event, $x_c \in X_c$, where $u - l > \bar{\gamma}^+(x_c) - \bar{\gamma}^-(x_c)$, is observed at time t and when $t < l + \bar{\gamma}^+(x_c)$, we may replace x_c and $\bar{\gamma}(x_c)$ with a constraint, x_c^* , and variable-delay function, $\bar{\gamma}(x_c^*)$, with narrower bounds as follows.*

$$\begin{aligned} x_c^* &= [l^*, u^*] \\ x_c^* &= [\max(l, t - \bar{\gamma}^+(x_c)), \min(u, t - \bar{\gamma}^-(x_c))] \\ \bar{\gamma}(x_c^*) &= [\max(\bar{\gamma}^-(x_c), t - u), \min(\bar{\gamma}^+(x_c), t - l)] \end{aligned}$$

Proof. Buffering is only possible if the conditions of Lemmas 4 and 5 are triggered. By Lemma 4, we are guaranteed to be able to narrow where in the range $[l, u]$ x_c was scheduled. By Lemma 5, we know that rewritten bounds will lead to an assignment of x_c that is no later than $l + \bar{\gamma}^+(x_c)$. Our tool for narrowing the bounds is Equation 5.5, which allows us to use the observation to reason over the assignment and observation delay. Our strategy is to look at the extreme cases leading to an observation.

We start by reasoning over the earliest and latest assignments respectively. In order for x_c to be assigned as early as possible, l^* , we assume the delay has taken on its maximum value, $\bar{\gamma}^+(x_c)$.

$$\xi(x_c) = \text{obs}(x_c) - \gamma(x_c) \quad (5.13)$$

$$l^* = t - \bar{\gamma}^+(x_c) \quad (5.14)$$

Likewise, to find the last possible assignment leading to an observation, we subtract the smallest observation delay, $\bar{\gamma}^-(x_c)$.

$$u^* = t - \bar{\gamma}^-(x_c) \quad (5.15)$$

Given that Nature will adhere to the constraints originally put forth in S , the bounds of x_c^* must remain within the bounds of x_c . Hence, we guarantee the lower bound is at least l while the upper bound is at most u .

$$l^* = \max(l, t - \bar{\gamma}^+(x_c))$$

$$u^* = \min(u, t - \bar{\gamma}^-(x_c))$$

We use the same logic for narrowing the observation delay. If x_c was assigned as late as possible, u , then the observation delay would be minimized, $\bar{\gamma}^-(x_c^*)$. Likewise, if x_c was assigned as early as possible, l , the observation delay would be maximized, $\bar{\gamma}^+(x_c^*)$. The narrowed lower and upper bounds of $\bar{\gamma}(x_c)^*$ are as follows.

$$\gamma = \text{obs}(x_c) - \xi(x_c)$$

$$\bar{\gamma}^-(x_c^*) = t - u$$

$$\bar{\gamma}^+(x_c^*) = t - l$$

As before, the bounds of $\bar{\gamma}(x_c^*)$ must stay within the original bounds of $\bar{\gamma}(x_c)$,

leaving us with the following narrowed observation delay.

$$\bar{\gamma}^-(x_c^*) = \max(\bar{\gamma}^-(x_c), t - u) \quad (5.16)$$

$$\bar{\gamma}^+(x_c^*) = \min(\bar{\gamma}^+(x_c), t - l) \quad (5.17)$$

□

We revisit the example from the beginning of this section to see Lemma 13 in action. As we saw before, any $\text{obs}(B)$ before $t = 4$ will result in buffered assignments.

$$A \xrightarrow{[1,7]} B \xrightarrow{\bar{\gamma} \in [1,3]} C$$

Let $t = 3$. We will step through the reasoning for narrowing the bounds of x_c accordingly.

$$x_c^* \in [\max(l, t - \bar{\gamma}^+(x_c)), \min(u, t - \bar{\gamma}^-(x_c))]$$

$$x_c^* \in [\max(1, 3 - 3), \min(7, 3 - 1)]$$

$$x_c^* \in [1, 2]$$

$$\bar{\gamma}(x_c^*) \in [\max(\bar{\gamma}^-(x_c), t - u), \min(\bar{\gamma}^+(x_c), t - l)]$$

$$\bar{\gamma}(x_c^*) \in [\max(1, 3 - 7), \min(3, 3 - 1)]$$

$$\bar{\gamma}(x_c^*) \in [1, 2]$$

We find that $\xi(x_c)$ must have fallen somewhere in the range of $[1, 2]$, while $\bar{\gamma}(x_c)$ was resolved somewhere in $[1, 2]$. Looking at the extremes, it is clear that there are multiple combinations of the assignment and observation delay that could lead to an observation at $t = 3$. While the narrowed range allows for observations other than $t = 3$, for instance, if $\xi(x_c) = 2$ and $\text{obs}(x_c) = 2$ yielding an observation at $t = 4$, there are no other ranges of assignments or observation delay outside of $\xi(x_c) \in [1, 2]$

and $\bar{\gamma}(x_c) \in [1, 2]$ that would allow an observation at $t = 3$.

Input: VDC STNU $S_{original}$; Variable-delay function $\bar{\gamma}$;

Observed contingent event x ; Observation time t ;

Output: VDC STNU

Initialization: $S_{new} \leftarrow \text{copy}(S_{original})$

Rewrite STNU:

```

1   for constraint in  $S_{new}$  do
2       if constraint ends in  $x$  then
3           constraint[lower]  $\leftarrow \max(\text{constraint}[lower], t - \bar{\gamma}^+(x))$ ;
4           constraint[upper]  $\leftarrow \min(\text{constraint}[upper], t - \bar{\gamma}^-(x))$ ;
5            $\bar{\gamma}^-(x) \leftarrow \max(\bar{\gamma}^-(x), t - \text{constraint}[upper])$ ;
6            $\bar{\gamma}^+(x) \leftarrow \max(\bar{\gamma}^+(x), t - \text{constraint}[lower])$ ;
7       endif
8   end
9   return  $S_{new}$ ;
```

Algorithm 6: An Algorithm for rewriting an STNU given the resolution of uncertainty of a contingent link.

The complexity of Algorithm 8 is dominated by the loop over `updateSchedule`. Each call to `updateSchedule` is $O(N^3)$ in the number of events. In the worst case scenario, every event up to the last contingent event has been scheduled, giving us a complexity of $O(N^4)$. We discuss potential means for improving optimistic rescheduling in Section 7.1.1.

5.4 Experimental Analysis

We first introduce an example which models a construction task on the lunar surface that will be used to randomly generate STNUs with realistic constraints for benchmarking purposes. We then describe benchmarks against the performance of the real-time FAST-EX update with the variable-delay execution strategy, the dispatching routine, real-time observations, and optimistic rescheduling. All benchmark code can be found at <https://gitlab.com/enterprise/enterprise> in the `kirk-v2/benchmarks` directory.

It is possible that, before NASA is ready to grow the population of a lunar base, there is a need to prepare a communications infrastructure near a habitat with a

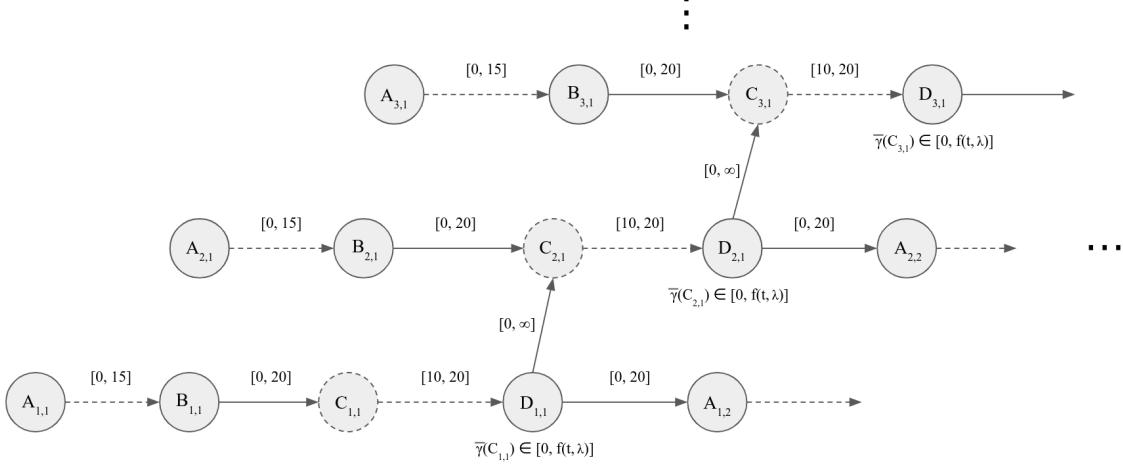


Figure 5-3: An STNU representing the installation and test of repeater antennas. Each row represents a single rover. The episode durations are representative of the bounds used in simulation.

large grid of repeater antennas. This scenario depicted with the STNU in Figure 5-3 represents an installation task wherein i rovers (mobile robot) are each installing j surface signal repeater antennas. During the activity, every rover is responsible for installing one repeater. Each event, X , is represented for the i -th rover and j -th repeater as $X_{i,j}$. All numbers in the figure are representative of the minimum and maximum of the randomly generated constraints in the benchmarks.

The rovers work in parallel, with a $[0, \infty)$ requirement link from the start of the STNU to each $A_{i,1}$ (not shown). The first episode, $A_{i,j} \Rightarrow B_{i,j}$, represents traversing to the site of the installation. We model traverses as uncontrollable due to the fact that crews are embarking across unknown terrain. Once at the site, an antenna is installed as represented by $B_{i,j} \rightarrow C_{i,j}$. Each repeater needs to have its configuration tested and confirmed working by $D_{i,j}$, represented by the edge $C_{i,j} \Rightarrow D_{i,j}$. Confirmation takes the form of a request-response cycle to the ground. We model $D_{i,j}$ as uncontrolled and with variable delay because each antenna takes an unknown time to self-configure and the crew does not know when they will receive a response from Earth that the repeater installation has been verified due to uncertainty in communication. Bandwidth is limited, so we limit the number of repeaters simultaneously

sending requests to their configuration. We use the $D_{i,j} \rightarrow C_{i+1,j}$ links to enforce that the start of the confirmation of the next repeater does not begin until after the previous repeater's confirmation. Confirmations are required until we reach the last crew member or the last activity. Once testing is complete, the rovers clean up their workstations, $D_{i,j} \rightarrow A_{i,j+1}$ and then repeat the cycle until all antennas have been installed.

To perform the benchmarks, we generated variable-delay STNUs with randomly generated constraints as previously described of increasing sizes. We immediately checked VDC of each STNU, and would generate new STNUs of a given size until we found one that was confirmed to be VDC. We then simulated scheduling and dispatching of the STNU with a faster-than-realtime clock. No driver was present, so all real events were scheduled immediately.

Our results for scheduling were as follows.

TODO

- average, max (+ stdev) runtime of schedule updates by num of events
- average, max (+ stdev) runtime of observations by num of events
- average... of schedule updates mid-execution by num of executed and unexecuted events

Chapter 6

Coordinating Multiple Agents under Uncertain Communication

In this chapter, we present a novel MA framework for dynamic event scheduling with inter-agent temporal constraints. Our framework adheres to the variable observation delay modeling framework presented in Chapter 4, making it robust to uncertain communication.

Online MA coordination of event dispatching allows executives to dynamically decide when to act given the resolution of inter- and intra-agent temporal constraints. In our formulation, each executive has its own STNU with contingent events it expects to observe and free events it is responsible for monitoring. We do not distinguish between contingent events that are the free events scheduled by peer agents and contingent events from any other source in Nature. There are no restrictions on inter-agent constraints, though they must avoid chained contingencies the same way that vanilla, single-agent STNUs do [28].

Executives are *not* required to have perfect knowledge of the complete state of the world with respect to event assignments, nor are they required to even *agree* on the state of the world. Rather, their knowledge should be consistent with the temporal constraints and observation delay modeled in their individual delay STNUs. This requirement stands in opposition to the communication challenge that is commonly addressed in problems involving distributed agents, e.g. distributed consensus

approaches [41], [42], where it is crucial that all agents agree on the state of the world. In our framework, each agent acts according to their given constraints. Due to scheduling uncertainty from observation delay, it is impossible to expect agents to agree on partial histories, nor is it necessary because each agent is capable of scheduling events with observation uncertainty.

To our knowledge, no such online scheduler for MA coordination with this requirement has been proposed. In this chapter, we first present a grounded Artemis-like scenario to motivate coordination. Next, we describe a modeling framework for MA control programs that is necessary for establishing coordination between agents. Then we define an event propagation algorithm used to guarantee that event observations match individual agent STNUs. We finish by presenting experimental analysis of our event propagation algorithms, and the results of hardware demonstrations of Delay Kirk using a robotic arm and a simulated astronaut.

6.1 Multi-Agent Control Programs

This thesis introduces challenges in writing control programs for multiple agents who need to coordinate. We do not claim to solve all aspects of coordination, rather we present a framework for simple scenarios with the key feature being that agents need to agree on the *order* of a subset of events. We start by presenting an example of inter-agent temporal constraints, followed by defining a modeling technique for guaranteeing that agents agree about the order of events in their respective partial histories. To the best of our knowledge, we are unaware of any other MA framework for coordinating the order of event histories.

Consider two agents, `agent1` and `agent2`, that are scheduling STNUs S_1 and S_2 respectively. S_1 and S_2 share a subset of semantically similar episodes, e_1 and e_2 . `agent1` “owns” e_1 , meaning it is responsible for scheduling the free event $e_1\text{-start}$ and observing the contingent event $e_1\text{-end}$, while `agent2` owns e_2 . It is the case that e_1 must precede e_2 in S_1 and S_2 . A simplified MA view of the constraints is as follows.

$$e_1\text{-start} \xrightarrow{[15,30]} e_1\text{-end} \xrightarrow{[0,\infty]} e_2\text{-start} \xrightarrow{[22,26]} e_2\text{-end}$$

From **agent1**'s perspective, S_1 models the following constraints. We add a **noop** start event, Z , to simplify coordination. For now, we allow chained contingencies, though in a moment they will need to be addressed.

$$Z \xrightarrow{[0,0]} e_1\text{-start} \xrightarrow{[15,30]} e_1\text{-end} \xrightarrow{[0,\infty]} e_2\text{-start} \xrightarrow{[22,26]} e_2\text{-end}$$

We assume that **agent1** models e_2 in S_1 because other events under their control depend on e_2 . S_2 is then modeled as follows. Note the change to the controllability of $Z \xrightarrow{[0,0]} e_1\text{-start}$.

$$Z \xrightarrow{[0,0]} e_1\text{-start} \xrightarrow{[15,30]} e_1\text{-end} \xrightarrow{[0,\infty]} e_2\text{-start} \xrightarrow{[22,26]} e_2\text{-end}$$

For the sake of controllability of S_1 and S_2 , we would simply add $[0, 0]$ free constraints between consecutive contingent constraints. Also note that from a scheduling standpoint, there is no difference between $a \xrightarrow{[0,0]} b$ and $a \xrightarrow{[0,0]} b$ - both indicate a and b should be scheduled simultaneously.

We will walk through scheduling this scenario from the perspective of both agents. First, we describe their actions in the case that there is no communication delay, then we introduce communication, and finally we add delay to communications. This scenario will motivate our analysis of the challenges that arise in MA control programs.

If both agents have perfect knowledge of the world (instantaneous knowledge of events), scheduling is trivial. **agent1** and **agent2** execute Z simultaneously. **agent1** schedules $e_1\text{-start}$ and **agent2** instantaneously receives an observation of $e_1\text{-start}$. $e_1\text{-end}$ arrives in $[15, 30]$ later, which again, both agents observe simultaneously. Now **agent2** is free to act. It schedules $e_2\text{-start}$, which **agent1** observes instantaneously. $e_2\text{-end}$ arrives $[22, 26]$ later and is observed simultaneously by both agents.

Now, we enforce that **agent1** “owns” e_1 and is the only agent that can observe it directly. Likewise, **agent2** owns e_2 . In order for an agent to learn about an episode they do not own, they must receive a communication from the agent who does. After

`agent1` schedules e_1 -start, it must send a message to `agent2`. `agent2` receives said message, which it interprets as an observation of e_1 -start. If communications are instantaneous, the partial histories of both agents agree on the assignment of e_1 -start. Later e_1 -end is observed by `agent1`, who is then responsible for relaying a communication to `agent2` indicating that it is safe to assign e_1 -end. `agent2` is now free to schedule e_2 -start, which it does instantaneously. The same pattern of sending messages that events have been scheduled repeats and `agent1` learns that e_2 -start was scheduled simultaneously with e_1 -end. After all events have been scheduled, the histories of `agent1` and `agent2` still agree on the times assigned to each event.

We now show that adding delay to the communications between agents forces us to add *synchronization* episodes to S_1 and S_2 to maintain event ownership. First, we must address the chained contingencies. Note that we have freedom in how we model the constraints of this scenario. The following example will motivate the need for a synchronization episode while remaining as close to the semantics of the original STNU as possible.

From the perspective of `agent1`, S_1 , we cannot escape the fact that there are two uncontrollable events in sequence - the end of e_1 and the start of e_2 , if we try to separate the events with a synthetic requirement episode, σ , with a $[0, \infty]$ constraint, the semantics no longer respect the original scenario.

$$Z \xrightarrow{[0,0]} e_1\text{-start} \xrightleftharpoons{[15,30]} e_1\text{-end} \xrightarrow{[0,0]} \sigma\text{-start} \xrightarrow{[0,\infty]} \sigma\text{-end} \xrightleftharpoons{[0,0]} e_2\text{-start} \xrightleftharpoons{[22,26]} e_2\text{-end}$$

The delay scheduler will choose to schedule σ -end simultaneously with σ -start, also leading to e_2 -start being immediately scheduled. However, e_2 is not under `agent1`'s control, and thus it has no authority to schedule e_2 -start. Instead, our synthetic constraint also needs to be contingent.

$$Z \xrightarrow{[0,0]} e_1\text{-start} \xrightleftharpoons{[15,30]} e_1\text{-end} \xrightarrow{[0,0]} \sigma\text{-start} \xrightleftharpoons{[0,\infty]} \sigma\text{-end} \xrightarrow{[0,0]} e_2\text{-start} \xrightleftharpoons{[22,26]} e_2\text{-end}$$

Now, the issue is that S_1 is uncontrollable due to $\sigma\text{-start} \xrightarrow{[0,\infty]} \sigma\text{-end}$. We know the `agent2` will receive $e_1\text{-end}$ somewhere in $\bar{\gamma}'(e_1\text{-end})$, where the $\bar{\gamma}'$ function represents observation delay in S_2 . `agent2` will then immediately schedule $e_2\text{-start}$. Finally, S_1 becomes

$$Z \xrightarrow{[0,0]} e_1\text{-start} \xrightarrow{[15,30]} e_1\text{-end} \xrightarrow{[0,0]} \sigma\text{-start} \xrightarrow{[\bar{\gamma}'^-(e_1\text{-start}), \bar{\gamma}'^-(e_1\text{-end})]} \sigma\text{-end} \xrightarrow{[0,0]} e_2\text{-start} \xrightarrow{[22,26]} e_2\text{-end}$$

In practice, an agent may choose to schedule other events while waiting for $\sigma\text{-end}$ to arrive.

In S_2 , we may choose to give `agent2` the same synchronization episode without changing the execution semantics. We know that $e_1\text{-end}$ will be observed somewhere in $\bar{\gamma}'(e_1\text{-end})$. When $e_1\text{-end}$ arrives, we are guaranteed to have waited somewhere in the lower and upper bounds σ . Assuming `agent2` knows that $e_1\text{-end}$ and $\sigma\text{-end}$ semantically represent the same point in time, $\sigma\text{-end}$ can be safely scheduled as soon as $e_1\text{-end}$ arrives.

Synchronization episodes allow inter-agent constraints with observation delay to be modeled without impacting the ordering of events. They are used to separate control programs in the hardware demonstration in Section 6.3.2.

6.2 Event Propagation

At a high level, scheduled events propagate through a simple directed graph of connected executives. We put checks in place to ensure that cycles do not cause infinitely recursed event observations.

Definition 28. Communication Graph

A *communication graph* C is a tuple $\langle V, E \rangle$, where:

- V is a set of vertices representing peer executives,
- E is a set of directed edges between $v \in V$ representing the path of event observation propagation,

- Each edge $e_i \in E$ is a pair (o, t) , where $o, t \in V$ represent the origin and termination of the edge respectively.

Self-loops, or self-edges, are not allowed, i.e. for any vertex $v_i \in V$, no single edge $e_i \in E$ may both originate and terminate at v_i .

For some executive $v_i \in V$ with outgoing edges in E , $(v_i, v_j), \dots, (v_i, v_k)$, any scheduled events that v_i assigns, whether free or contingent, are propagated to all peer executives v_j, \dots, v_k . Likewise, all contingent events received from Nature are propagated to peers. Finally, any events v_i receives from other agents are also relayed to peers.

Definition 29. Event Propagation Messages

An *event propagation message* m is a tuple $\langle x, P \rangle$, where:

- x is a set of one or more events scheduled simultaneously,
- $P \subseteq V$ is a set of executives who have already received the message.

Recognize that Definition 29 is vague in defining x . Event propagation messages are passed between agents, and each agent has its own STNU. In some cases, x will be free events, in others x will be contingent events. The type of event makes no difference to the algorithm so we do not distinguish between them here.

Events that are received in m , $m[x]$, are handled the same as observations of contingent events during scheduling. Lemmas 8, 11, and 10 are applied as appropriate when the observation of $m[x]$ arrives.

For an edge $(v_i, v_j) \in E$, it is possible that v_j receives events that are not present in its STNU.

Because we have not defined a temporal decoupling-like algorithm wherein an STNU for multiple-agents is programmatically separated into individual STNUs (see the discussion of multi-agent STNUs [4] in Section 7.2), we are reliant on human planners to write STNUs for each agent by hand. As a result, there is no guarantee that x is meaningful to a given agent.

To be more specific, there is no guarantee that any event $x_i \in x$ in the event propagation message has an equivalent event in X_c of the STNU being executed by

any receiving agent $v_j \in V$. If agent v_j cannot find x_i in their X_c , then x_i can be ignored. As will be discussed in Algorithm 7, we represent x using a type that can be compared for equivalence with the events in an agent's STNUs, e.g. a list of strings.

We use P to avoid cycles in event propagation. As will be shown in Algorithm 7, agent v_i will avoid propagating x to any agents in P . Agent v_i will also grow P when it relays m to other agents by appending to P itself and all outgoing agents v_j, \dots, v_k .

Timing information, e.g. timestamps, is explicitly excluded from m . Dynamic scheduling and the variable-delay STNU and event observation, **obs**, formalisms do not account for timestamps. Instead, we expect that passing messages for event propagation between executives takes an amount of time in the domain \mathbb{R}^+ . Thus, when v_j expects to receive an event, $x_i \in x$, from v_i , the time delay can be naturally modeled in the variable-delay function, $\bar{\gamma}(x_i)$, in the STNU that v_j will execute.

If event propagation messages were to include accurate timestamps, we would need to modify the way events are recorded during scheduling, impacting scheduling Lemmas 8, 11, and 10. Scheduling events in the past could also impact controllability. For these reasons, we avoid the inclusion of timestamps in event propagation messages.

By Definition 29, events received from other agents are no different than events received from Nature, and no special considerations are required for scheduling.

We now walk through the process of passing messages between agents as shown in Algorithm 7. We use the same *Event Propagation* algorithm in three cases:

1. When an agent v_i schedules free events x ,
2. When v_i receives an observation from Nature of contingent events x ,
3. When v_i receives an incoming message m_i with contingent events $m_i[x]$ from another agent in V .

Let **peers** be a mutable set initialized to the terminal vertices for all $e \in E$ originating at v_i .

In the first case, agent v_i fulfills its responsibilities as defined in C by broadcasting x to its **peers**, who will receive x as exogenous contingent events. The outgoing

message m_o that will be passed to `peers` will include enough information such that no agent should receive a given x more than once. To do so, we let P be a set of all agents that will have observed x when m_o is received by `peers`, $P = \{v_i, p \mid p \in \text{peers}\}$. We finalize $m_o = \langle x, P \rangle$, which we simultaneously transmit to each p in `peers`. Transmission is a “fire and forget” operation, where v_i does not wait for acknowledgment from any p that m_o was received.

The second case plays out the same as the first, the only difference being that x is itself observed from Nature. Once again, we let P be a list of v_i and all `peers`, and then transmit m_o simultaneously to all `peers`.

The third case is a relay operation. Agent v_i is responsible for propagating events $m_i[x]$ that it has just observed, but we want to avoid sending the events to `peers` who have already observed them. We remove those agents from `peers` accordingly with a set difference operation: $\text{peers} = \text{peers} - m_i[P]$. Likewise, we grow the list of agents who have received x , which is now $P = P \cup \text{peers}$. Agent v_i composes a new $m_o = \langle m_i[x], P \rangle$ and transmits it to `peers`.

Ideally, the Event Propagation algorithm should run on a separate thread from the main scheduling loop, else we run the risk of incurring unnecessary delays in observing and dispatching events.

Input: Incoming message m_i ; Scheduled events x ; Self $v_i \in V$; Set of outgoing $\text{peers} \subset V$

Event Propagation:

```

1   peers ← peers −  $m_i[P]$ ;
2    $P \leftarrow m_i[P] \cup \{v_i\} \cup \text{peers}$ ;
3    $x \leftarrow x \text{ or } m_i[x]$ ;
4    $m_o \leftarrow \langle x, P \rangle$ ;
5   for each  $p$  in peers do
6   |   Perform a non-blocking transmission of  $m_o$  to  $p$ ;
7   end
```

Algorithm 7: An event propagation algorithm that avoids recursive message passing.

The complexity of Algorithm 7 is trivially $O(N)$, where N is the number of executives in $V - 1$. The limiting factor to the performance of Event Propagation will be the time it takes to transmit messages between agents, which, to reiterate, should be

modeled in the delay functions for any inter-agent temporal constraints.

6.3 Experimental Analysis

We performed two demonstrations of the Event Propagation algorithm. The first was a hardware demonstration performed on a Barrett WAM manipulator in the MERS lab. The second is a multi-agent simulation showcasing inter-agent constraints. Both will be described below.

6.3.1 Distributed Kirk Simulation

To demonstrate multi-agent communication, we built a simulation of an end-to-end mission with three independent Kirks, `agent0`, `agent1`, and `agent2`. We will show that distributed Kirks can successfully dispatch events within temporal bounds in the face of multiple sources of communication uncertainty. The Kirks are responsible for executing an installation procedure with the same randomly generated constraints as used in the validation of the delay scheduler in Section 5.4. In this scenario, each agent is responsible for installing two satellite dishes with staggered confirmations so as to limit uplink bandwidth usage. As Kirks receive confirmation that installation has been completed, they then share the confirmations with their peers.

To simplify comparing schedules, we used a standardized format for event names. Repeated event names are given as `Event:[agent]:[iteration]`, where `[agent]` and `[iteration]` are zero-indexed. For instance, `Install:4:3` would be the start of an installation episode for a hypothetical `agent4` (of at least five agents) in its fourth iteration.

There is one modification from the original constraints from Section 5.4 in that we separate the communication delay inherent to the confirmation task with the observation delay inherent to sharing observations with peers. There may be a delay waiting for confirmation from ground, and the *in situ* communication infrastructure may add an additional delay to communications between agents. We assume the sources of delay compound. For instance, `agent1` will need to know when `agent0` has

confirmed its installation task, `Confirm:0:0` before beginning their own installation, `Install:1:0`. If `agent0` expects to receive `Confirm:0:0` with an observation delay of $\bar{\gamma}(\text{Confirm}:0:0) = [0, 10]$, we increase $\bar{\gamma}^+(\text{Confirm}:0:0)$ by one for any peers that receive the observation broadcasted from `agent0`. In other words, from the perspective of `agent1` or `agent2`, $\bar{\gamma}(\text{Confirm}:0:0) = [0, 11]$ instead.

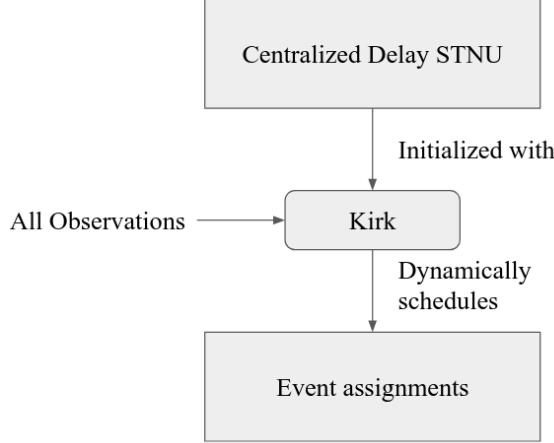


Figure 6-1: The Kirk architecture used to generate event assignments for the centralized delay STNU. A single Kirk receives the VDC STNU that includes constraints for all agents, as well as contingent event observations. Kirk then performs delay scheduling, resulting in an assignment to all events.

At a high-level, our procedure for creating this demonstration is as follows. We randomly generated a variable-delay STNU for three agents and two installation procedures (using the same generator code that was used in Section 5.4) and confirmed it to be VDC. We call this STNU the *centralized delay STNU* in that it includes all constraints for all three agents in a multi-agent mission with observation delay. We then acted like a mission planner in that we manually decoupled the centralized delay STNU into three single-agent RMPL control programs. Each control program contained the subset of the constraints from the centralized delay STNU required for a single agent to maintain the semantics of the original constraints. We call the variable-delay STNUs represented by the collection of the three RMPL control programs the *distributed variable-delay STNUs*. We finally pre-determined when observations would arrive for each agent to simplify running the demonstration. Both the centralized and

distributed scenarios received observations of the same events at the same times.

The architecture for the centralized scenario is shown in Figure 6-1, while the distributed scenario is represented in Figure 6-2. Figure 6-2 presents a simplified view in order to keep the diagram readable. In reality, each Kirk broadcasts all events to all peers.

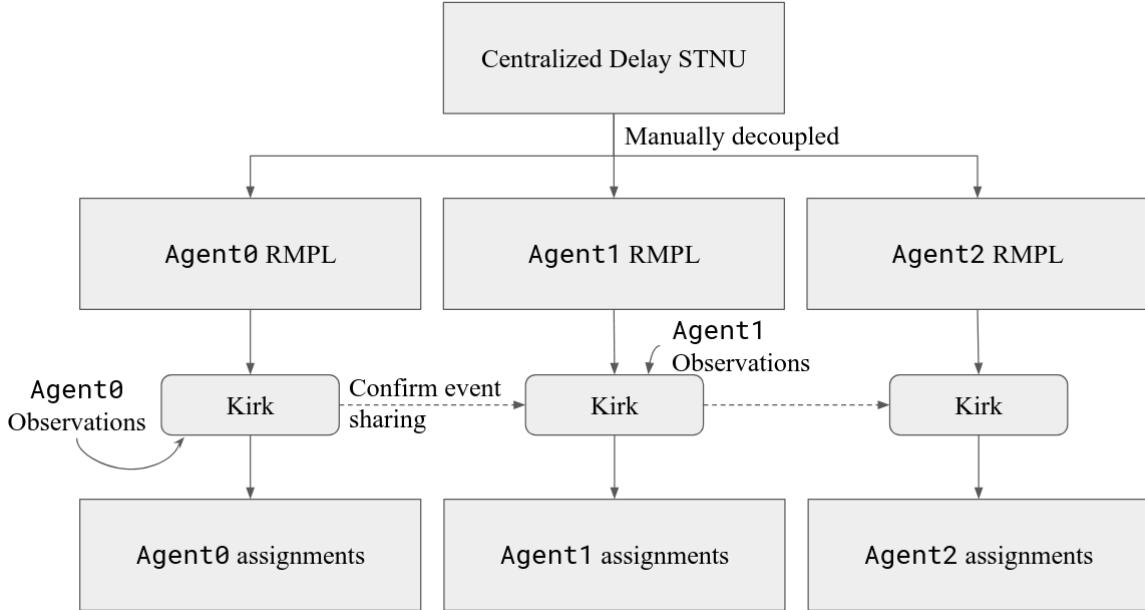


Figure 6-2: The distributed architecture for the demonstration. The original centralized delay STNU is manually decoupled to three separate RMPL control programs, which are then used to initialize three Kirks. The Kirks receive appropriate event observations, which they then share to their peers. After delay scheduling, each Kirk produces an assignment to events that were under their control.

Event observations were arranged as follows. In the centralized case, the single Kirk received all contingent event observations. Any observations that were not explicitly provided as an observation was assumed to be assigned at its upper bound. In the distributed case, Kirks were only given event observations for events that belong to them. For instance, only `agent0` received an observation of `Confirm:0:0`, the event signifying that they have completed installation of the first satellite. It was then the responsibility of `agent0` to broadcast the event observation to its peers.

To evaluate the ability of a distributed Kirk architecture to perform scheduling

with communication uncertainty, we focus on the schedules produced. To do so, we compare the schedule created by a Kirk running against centralized delay STNU (Table 6.1) against the combined schedules of the three single agents (Tables 6.2-6.4). If observations arrive at the same time, both scenarios should yield the same schedules. Importantly, the inter-agent constraint between overlapping installation tasks should hold in the distributed scenario. The confirmation events are highlighted in gray in each table for ease of identification.

Running the demonstration was then a matter of running three networked instances of Kirk simultaneously against three different control programs. We did so using a `Makefile` with three targets, running `make` with the `-j3` flag, and setting up communications to take place over HTTP.

From the root of the thesis repository, execute `make kirk && make -j3 demo` to run the demonstration. The resulting schedules will be written to `agent{0,1,2}.txt`. Note that the STNU was generated directly for the centralized delay STNU, but the STNUs were compiled from RMPL control programs for the distributed delay STNUs. There are naming differences between the events of the different schedules due to way control programs receive names in RMPL and the way RMPL control programs are compiled to STNUs. The event names in schedules in Tables 6.1-6.4 have been manually altered such that they match here. See Appendix B for a description of the resulting STNUs from RMPL control programs.

Here, we show `Confirm:0:1` as the last event, but In the RMPL control program, we used a `close-out` episode with bounds $[0, \infty]$ to end the mission. Given that it follows a `Confirm` episode, It is semantically the same as the confirmation (again, see Appendix B for an explanation of how control programs translate to STNUs).

We can see in Tables 6.1-6.4 that the three Kirks are able to avoid overlapping installation tasks using a communication architecture that assume uncertain communication.

Table 6.1: The schedule produced by a single Kirk against against the “multi-agent” variable-delay STNU.

Event	Time (s)
ALL:START	0
Start:0:0	0
Start:1:0	0
Normalized Lower for Traverse:0:0	1
Normalized Lower for Traverse:1:0	1
Traverse:0:0	10
Install:0:0	11
Normalized Lower for Confirm:0:0	15
Traverse:1:0	15
Confirm:0:0	17
Install:1:0	17
Start:2:0	17
Normalized Lower for Traverse:2:0	18
Start:0:1	19
Normalized Lower for Traverse:0:1	20
Normalized Lower for Confirm:1:0	22
Confirm:1:0	30
Start:1:1	31
Normalized Lower for Traverse:1:1	32
Traverse:2:0	32
Install:2:0	33
Traverse:0:1	38
Install:0:1	39
Normalized Lower for Confirm:2:0	40
Confirm:2:0	41
Normalized Lower for Confirm:0:1	42
Start:2:1	43
Normalized Lower for Traverse:2:1	44
Traverse:1:1	44
Install:1:1	45
Confirm:0:1	48
Normalized Lower for Confirm:1:1	52
Confirm:1:1	55
Traverse:2:1	60
Install:2:1	61
Normalized Lower for Confirm:2:1	62
Confirm:2:1	63
ALL:END	63

Table 6.2: The single agent schedule produced by `agent0` in the demonstration.

Event	Time (s)
Start:0:0	0
Normalized Lower for Traverse:0:0	1
Traverse:0:0	10
Install:0:0	11
Normalized Lower for Confirm:0:0	15
Confirm:0:0	17
Start:0:1	19
Normalized Lower for Traverse:0:1	20
Traverse:0:1	38
Install:0:1	39
Normalized Lower for Confirm:0:1	42
Confirm:0:1	48

Table 6.3: The single agent schedule produced by `agent1` in the d emonstration.

Event	*Time (s)
Start:1:0	0
Start:0:0	0
Normalized Lower for Confirm:0:0	6
Confirm:0:0	17
Traverse:1:0	17
Install:1:0	18
Normalized Lower for Confirm:1:0	23
Confirm:1:0	30
Start:1:1	31
Normalized Lower for Traverse:1:1	32
Traverse:1:1	44
Install:1:1	45
Normalized Lower for Confirm:1:1	52
Confirm:1:1	55

Table 6.4: The single agent schedule produced by `agent0` in the demonstration. We added a `CLOSE-OUT` episode to end with a requirement event.

Event	Time (s)
Start:2:0	17
Normalized Lower for Confirm:1:1	22
Confirm:1:1	30
Traverse:2:0	32
Install:2:0	33
Normalized Lower for Confirm:2:1	40
Confirm:2:1	41
Start:2:1	43
Normalized Lower for Traverse:2:1	44
Traverse:2:1	60
Install:2:1	61
Normalized Lower for Confirm:2:1	62
Confirm:2:1	63

6.3.2 Hardware Demonstration

We envision a scenario with an astronaut and a robot coordinating on the lunar surface. The astronaut is performing scientific exploration while the robot performs remote construction tasks. The concept of operations allows for the astronaut to use a rover to traverse away from the robot in search of promising scientific samples. Due to the position of surface relays and general uncertainty in lunar topology, there is an uncertain time delay between agents.

Bandwidth between Mission Control on Earth and the Moon is limited. There are low and high bandwidth communications available to both agents. Low bandwidth is responsible for transmitting critical data (e.g. suit telemetry), while high bandwidth communications are reserved for purposes such as video calls and large dumps of scientific data. It is not possible for both the astronaut and the robot to use high bandwidth communications simultaneously. Thus, there is a need for the agents to coordinate such that they make effective use of high bandwidth communications without stepping on each others toes, so to speak.

We hone in on a point in an EVA where there is substantial time delay between the astronaut and robot. The astronaut has set out far from the robot in search of scientifically interesting rock samples. Meanwhile, the robot is preparing to perform

a drilling operation. The astronaut’s sample collection work involves spectroscopy and video imagery, which is being sent to Mission Control using the high bandwidth connection. It will take between 15 and 30 minutes to downlink all the data. As soon as sample collection is over, the robot can use the high bandwidth connection to stream video back to scientists and engineers on earth while performing a drilling operation.

We say that the astronaut “owns,” or is responsible for sharing observations of, the start and end of the experiment, while the robot similarly owns the drilling operation.

We built a physical demonstration of this scenario of this thesis in our laboratory using a Barrett WAM manipulator and a simulated astronaut. In this scenario, the astronaut and robot are collaborating on the lunar surface with uncertain communication delay between them. Throughout this mission, agents must coordinate with respect to their usage of uplink bandwidth. We choose to focus on a moment in time where the robot is waiting for the human to finish their use of the uplink before beginning a bandwidth-heavy task of their own. We assume the agents are moving on the lunar surface during execution, and as such the observation delay between them changes as well. See Figure 6-3 for the laboratory setup.

The architecture of the hardware demonstration is as shown in Figure 6-4. We ran two Kirks on the same network. One Kirk was responsible for driving the Barrett WAM, while the other acted as the decision making logic behind an interface on the astronaut’s person (say a tablet, heads-up-display, or portable computer of some kind).

The laptop ran the Kirk that controls the WAM. It did so by dispatching requirement events to a separate driver that could translate event names to pre-built trajectories for the WAM. The trajectories were then published to the WAM’s controller as ROS messages. As trajectories were completed, ROS messages were received by the ROS driver layer, which then sent contingent event observations back to Kirk.

The Valve Steam Deck (SD), a handheld PC, ran the astronaut’s Kirk. The Kirk command line tool allows users to press a number to trigger the observation of a contingent event. We modified the output of the video game controller buttons of

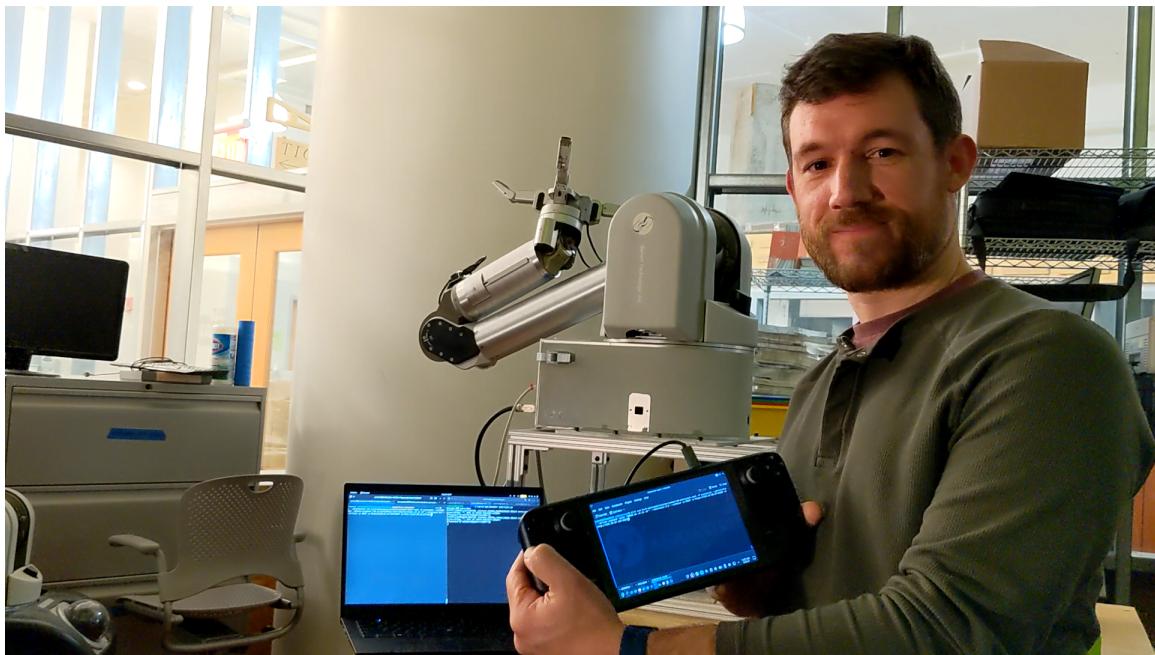


Figure 6-3: The two Kirks and two agents of the hardware demonstration. The Kirk executive running on the laptop is controlling the Barrett WAM arm in the background. Cameron Pittman is the second agent (acting as the astronaut) and interacting with a Kirk executive running on the Steam Deck handheld PC. This image was taken in the MERS lab on 20 May 2023.

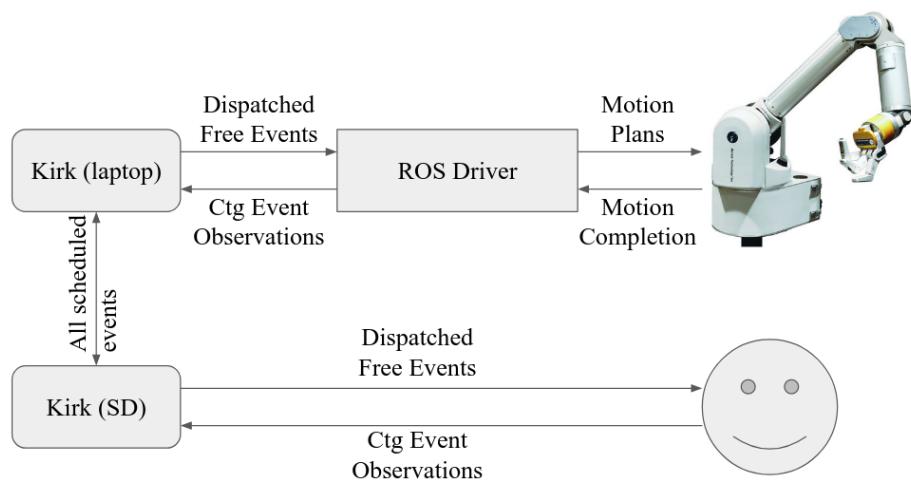


Figure 6-4: The information flow between the two agents and two Kirks in the hardware demonstration. “SD” is short for Steam Deck.

The screenshot shows a laptop screen with two terminal windows side-by-side.

Left Terminal Window:

```

Activities Terminal May 20 01:49
cameron@workstation:~/mtk/workspaces/primary/enterprise... /home/robot/ROS/catkin_ws/src/mers/ros-wam-joint...
cameron@xenial:~/catkin_ws$ rostest wam_listener subscriber.py
Running WAM subscriber
[INFO] [1684561513.718448]: /Listener_588724-1684561391882 RESULT error_code: 0
error_string: ''
GOAL ID: #ROVER-POWEROFF::START+
["recorded":["#ROVER-POWEROFF::START+"]]
[INFO] [1684561620.354879]: /Listener_588724-1684561391882 RESULT error_code: 0
error_string: ''
GOAL ID: #ROVER-POWEROFF::START+
["recorded":["#ROVER-POWEROFF::START+"]]
[INFO] [1684561732.473901]: /Listener_588724-1684561391882 RESULT error_code: 0
error_string: ''
GOAL ID: #ROVER-POWEROFF::START+
["recorded":["#ROVER-POWEROFF::START+"]]

```

Kirk's Output (Left Window):

```

SCHED: Scheduling EV1426 (free) at 69.905485d0
SCHED: Success scheduling EV1426
DISP: t=70: EV1426 execution confirmed
SCHED: Trying to update-schedule! EV1101 at 69.905485d0
SCHED: Scheduling EV1101 (free) at 69.905485d0
SCHED: Success scheduling EV1101
DISP: t=70: EV1101 execution confirmed
SCHED: Trying to update-schedule! #ROVER-POWEROFF::END+ at 69.905485d0
SCHED: Success scheduling #ROVER-POWEROFF::END+
DISP: Success scheduling #ROVER-POWEROFF::END+
DISP: t=70: #ROVER-POWEROFF::END+ execution confirmed
DISP: t=70: Next Decision: at #.DOUBLE-FLOAT-POSITIVE-INFINITY
DISP: t=70: We already tried to dispatch #5(RTED
:TIME #.DOUBLE-FLOAT-POSITIVE-INFINITY
:EVENTS NIL)
Confirmed execution: #End-Execution+ at t=71
Confirmed execution: NIL at t=71
+-----+-----+
|What |When (s)|
+-----+-----+
|+HUMAN-SETUP-SCIENCE::START+ |0 |
+-----+-----+
|EV1499 |0 |
+-----+-----+
|+LOWER--SYNC::START++REWOL++ |30 |
+-----+-----+
|+ROVER-DRILLING::START+ |35 |
+-----+-----+
|+SYNC::START+ |35 |
+-----+-----+
|+LOWER--ROVER-POWEROFF::START++REWOL++ |58 |
+-----+-----+
|+ROVER-POWEROFF::START+ |60 |
+-----+-----+
|+ROVER-POWEROFF::END+ |70 |
+-----+-----+
|EV1101 |70 |
+-----+-----+
|EV1426 |70 |
+-----+-----+

```

Right Terminal Window:

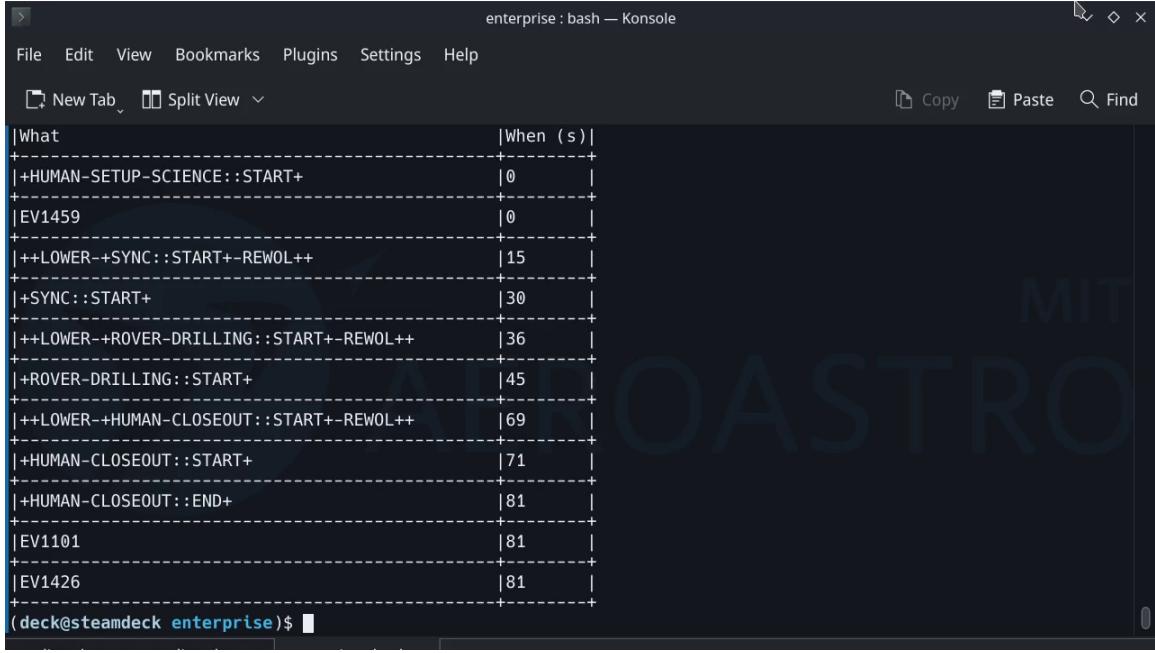
```

cameron@xenial:~/catkin_ws$ rostest wam_listener subscriber.py
Running WAM subscriber
[INFO] [1684561513.718448]: /Listener_588724-1684561391882 RESULT error_code: 0
error_string: ''
GOAL ID: #ROVER-POWEROFF::START+
["recorded":["#ROVER-POWEROFF::START+"]]
[INFO] [1684561620.354879]: /Listener_588724-1684561391882 RESULT error_code: 0
error_string: ''
GOAL ID: #ROVER-POWEROFF::START+
["recorded":["#ROVER-POWEROFF::START+"]]
[INFO] [1684561732.473901]: /Listener_588724-1684561391882 RESULT error_code: 0
error_string: ''
GOAL ID: #ROVER-POWEROFF::START+
["recorded":["#ROVER-POWEROFF::START+"]]

```

Figure 6-5: The laptop screen at the end of the second hardware demo scenario. On the left is Kirk's output, on the right is the ROS translation layer. Kirk is showing the schedule that it executed, while we can see logs from messages sent between Kirk and the ROS layer on the right.

the Steam Deck such that they would automatically input the number corresponding to the observation of a contingent event. As the astronaut, Cameron only needed to press one button (mapped to left on the d-pad) during the run to trigger the observation.



The screenshot shows a terminal window titled "enterprise : bash — Konsole". The window has a menu bar with "File", "Edit", "View", "Bookmarks", "Plugins", "Settings", and "Help". Below the menu is a toolbar with "New Tab", "Split View", "Copy", "Paste", and "Find". The main area of the terminal displays two columns of data. The left column, labeled "What", lists various events and their start times. The right column, labeled "When (s)", lists the corresponding time values. The data is as follows:

What	When (s)
+HUMAN-SETUP-SCIENCE::START+	0
EV1459	0
++LOWER+SYNC::START+-REWOL++	15
+SYNC::START+	30
++LOWER+ROVER-DRILLING::START+-REWOL++	36
+ROVER-DRILLING::START+	45
++LOWER+HUMAN-CLOSEOUT::START+-REWOL++	69
+HUMAN-CLOSEOUT::START+	71
+HUMAN-CLOSEOUT::END+	81
EV1101	81
EV1426	81

At the bottom of the terminal, the prompt "(deck@steamdeck enterprise)\$" is visible.

Figure 6-6: The Steam Deck screen at the end of the second hardware demo scenario. On the left is Kirk’s output, on the right is the ROS translation layer. Kirk is showing the schedule that it executed, while we can see logs from messages sent between Kirk and the ROS layer on the right.

The laptop and the Steam Deck were on the same local network. Note the cable dangling from the Steam Deck in Figure 6-3, which is a USB-C to Ethernet adapter. The Steam Deck was hardwired to the network for demonstration purposes. Communications occurred over HTTP. To simulate uncertain communication, a sleep call with a time in the range of $\bar{\gamma}(x_c)$ was injected into Kirk’s function responsible for broadcasting event observations to peers, where $\bar{\gamma}(x_c)$ was drawn from any contingent event $x_c \in X_c$ of the receiving agent.

To start a run of the demonstration, we would start both Kirks simultaneously. Each Kirk had their own RMPL control program, which we include in Listings 6 and 7. Note that the control programs are nearly identical. The control programs

related to the high bandwidth handoff, `human-downlink-science`, `sync`, and `robot-drilling`, differ only in observation delay and whether the `sync` event is controllable. Adding observation delay reflects uncertain communication between the agents.

The `sync` control programs were included as synchronization episodes between `human-downlink-science` and `robot-drilling`. Note that the robot also has a `sync` episode, which ensures that both agents agree on the naming of events.

We can see the modeling power of variable observation delay in Listings 6 and 7. It is natural that the observation delay between agents may change due to the evolution of resources during a mission. The variable-delay modeling framework allows us to model uncertain delay for each temporal constraint independently. For instance, if we know that, say, agents will be distant during a given constraint, then we may add uncertain delay accordingly. If agents are collocated during other constraints, then we can safely decrease the observation delay (absent other sources of delay).

According to the constraints and variable delay of the `human-downlink-science` control program from the perspective of the robot, the transformed fixed-delay STNU the robot is executing will reflect constraints of `human-downlink-science:start` $\xrightarrow{[30,35]}$ `human-downlink-science:end` with $\gamma(\text{human-downlink-science:end}) = 0$ after applying Lemma 4.

We performed two demonstrations. In the first, the astronaut would observe the end of the science downlink, the end event of `human-downlink-science:end`, which would trigger a delayed observation being passed to the robot. Once the robot received the command, it would begin its `robot-drilling` activity. It passed observations of its scheduled events back to the astronaut.

The second demonstration focused on the behavior of the delay scheduler when communications are not received in time. After starting both Kirks at the same time, we unplugged the astronaut’s Kirk from the network. While, in reality, a disconnection should be modeled as $\bar{\gamma}^+(x_c) = \infty$, we did it to emphasize the fact that the robot’s Kirk would not receive an observation within the fixed bounds it was expecting. The delay scheduler would then imagine `human-downlink-science:end` and dispatch its drilling activity accordingly.

```

(defpackage #:scenario1)

(in-package #:scenario1)

(define-control-program human-downlink-science ()
  (declare (primitive)
    (duration (simple :lower-bound 15 :upper-bound 30)
              :contingent t)))

(define-control-program sync ()
  (declare (primitive)
    (duration (simple :lower-bound 5 :upper-bound 15
                      :min-observation-delay 0
                      :max-observation-delay 1)
              :contingent t)))

(define-control-program robot-drilling ()
  (declare (primitive)
    (duration (simple :lower-bound 22 :upper-bound 26
                      :min-observation-delay 0
                      :max-observation-delay 2)
              :contingent t)))

(define-control-program human-closeout ()
  (declare (primitive)
    (duration (simple :lower-bound 10 :upper-bound 30)))))

(define-control-program main ()
  (with-temporal-constraint (simple-temporal :upper-bound 480)
    (sequence (:slack nil)
              (human-downlink-science)
              (sync)
              (robot-drilling)
              (human-closeout))))

```

Listing 6: The control program the astronaut uses while collecting and downlinking scientific data.

```

(defpackage #:scenario1)

(in-package #:scenario1)

(define-control-program human-downlink-science ()
  (declare (primitive)
    (duration (simple :lower-bound 15 :upper-bound 30
                      :min-observation-delay 5
                      :max-observation-delay 15)
              :contingent t)))

(define-control-program sync ()
  (declare (primitive)
    (duration (simple :lower-bound 5 :upper-bound 15)))))

(define-control-program robot-drilling ()
  (declare (primitive)
    (duration (simple :lower-bound 22 :upper-bound 26
                      :min-observation-delay 0
                      :max-observation-delay 1)
              :contingent t)))

(define-control-program robot-poweroff ()
  (declare (primitive)
    (duration (simple :lower-bound 10 :upper-bound 30)))))

(define-control-program main ()
  (with-temporal-constraint (simple-temporal :upper-bound 480)
    (sequence (:slack nil)
              (human-downlink-science)
              (sync)
              (robot-drilling)
              (robot-poweroff))))

```

Listing 7: The control program the robot uses to decide when to act with respect to learning the astronaut has finished collecting scientific data.

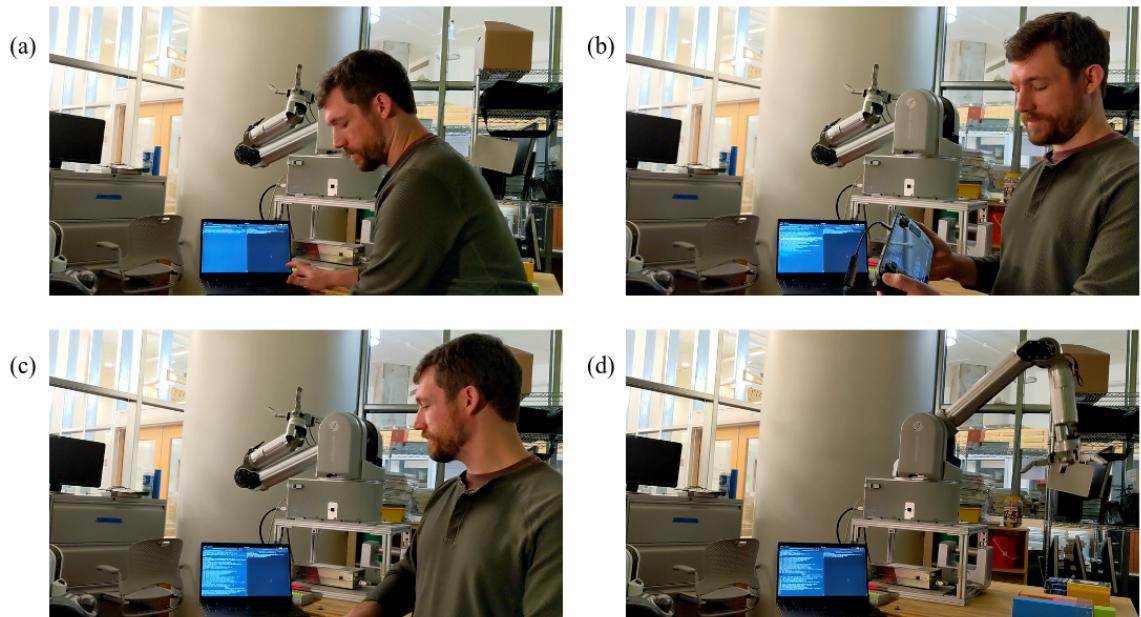


Figure 6-7: The first demonstration in four parts. (a) $t = 0$, when the two Kirks are started at the same time (unfortunately, the SD is below the image frame). (b) $t = 16$, when the astronaut observed that the science experiment was setup. (c) $t = 23$, when the robot received a delayed observation from the astronaut indicating they had completed science setup. (d) $t > 23$, as the robot performed the drilling task.

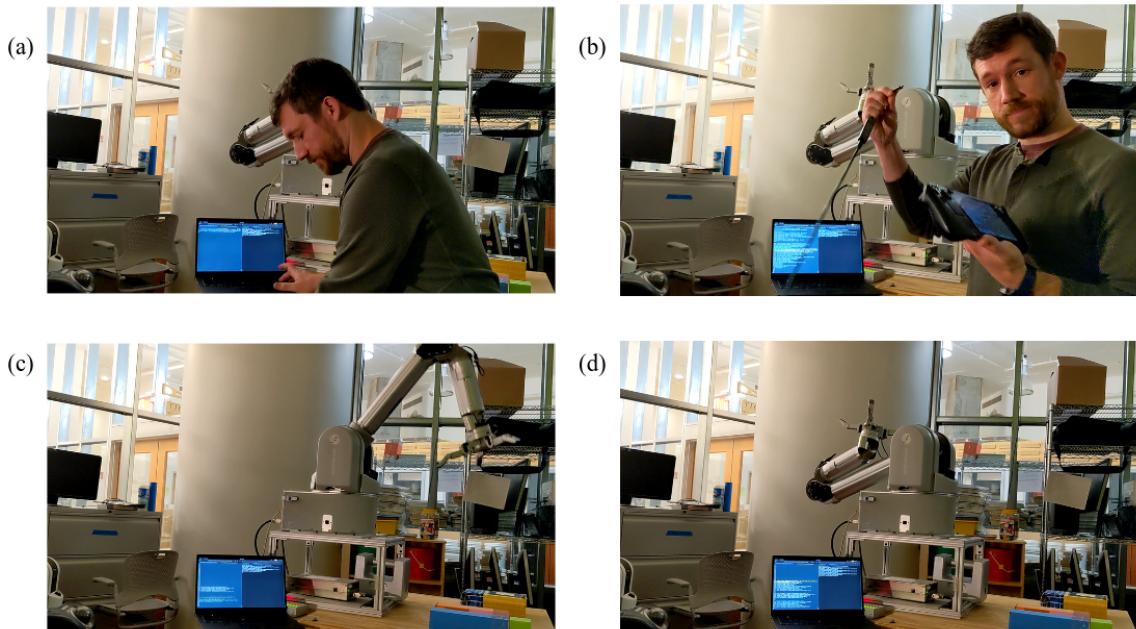


Figure 6-8: The second demonstration in four parts. (a) $t = 0$, when the two Kirks are started at the same time (unfortunately, the SD is below the image frame again). (b) $t = 3$, when the SD is removed from the network. (c) $t = 38$, after the robot imagined an observation from the astronaut and began the drilling task. (d) $t = 60$, when Kirk has observed the end of the drilling task.

We present the schedules of the agents for both scenarios in Tables 6.5-6.8. The schedule has been cleaned and the event names have been modified to better reflect the intent of the RMPL control programs. See Appendix B for an explanation of how RMPL and the STNUs compiled from it are related. We also removed anonymous (non-named) events that were added in the process of translating RMPL to variable-delay STNU.

Table 6.5: The complete history of the delay scheduler for the astronaut in the first hardware demo scenario.

Event	Time (s)
Start Human Setup Science	0
Normalized Lower for End Human Setup Science	15
End Human Setup Science	16
Start Sync	16
Normalized Lower for Sync	22
End Sync	23
Start Robot Drilling	23
Normalized Lower for Robot Drilling	47
End Robot Drilling	49
Start Close Out	49
End Close Out	59

Table 6.6: The complete history of the delay scheduler for the robot in the first hardware demo scenario.

Event	Time (s)
Start Human Setup Science	0
Normalized Lower for Human Setup Science	15
End Human Setup Science	22
Start Sync	22
End Sync	22
Start Robot Drilling	22
Normalized Lower for Robot Drilling	45
End Robot Drilling	46
Start Robot Poweroff	46
End Robot Poweroff	56

We can see variable observation delay at work by comparing the assigned end times for `human-setup-science` between the astronaut and robot in Tables 6.5 and 6.6. The human knows that science setup was completed at $t = 16$, but the robot received an observation of the same event after an apparently delay of six seconds.

Note that the robot was running an experimental *optimistic* version of the delay scheduler in the demonstration. The difference between the delay scheduler as described in Chapter 5 and the optimistic version is that the optimistic version will attempt to avoid buffering early contingent events by rewriting the delay STNU based on the early observation and checking VDC. It will be discussed in more depth in Section 7.1.

Table 6.7: The complete history of the delay scheduler for the astronaut in the second hardware demo scenario.

Event	Time (s)
Start Human Setup Science	0
Normalized Lower for End Human Setup Science	15
End Human Setup Science	30
Start Sync	30
Normalized Lower for Sync	36
End Sync	45
Start Robot Drilling (imagined)	45
Normalized Lower for Robot Drilling	69
End Robot Drilling (imagined)	71
Start Close Out	71
End Close Out	81

Table 6.8: The complete history of the delay scheduler for the robot in the second hardware demo scenario.

Event	Time (s)
Start Human Setup Science	0
Normalized Lower for Human Setup Science	30
End Human Setup Science (imagined)	35
Start Sync	35
End Sync	35
Start Robot Drilling	35
Normalized Lower for Robot Drilling	58
End Robot Drilling	60
Start Robot Poweroff	60
End Robot Poweroff	70

Finally, we see in the second experiment that the robot was forced to imagine contingent events due to communication delay. The robot was able to satisfy all constraints with its drilling episode despite not receiving communication from the astronaut about the end of the astronaut setting up the science experiment.

Chapter 7

Discussion and Future Work

7.1 Optimistic Rescheduling

We return to problem of potentially unnecessary wait time created by the buffering execution strategy described in Lemma 5. First, we use an example to demonstrate how buffering early contingent events results in a reduction of the execution space. Then we contribute a technique for managing event observations that circumvents the loss of execution space.

Consider the following variable-delay controllable STNU, which we will refer to as *Bufferable*.

$$A \xrightarrow{[1,7]} B \xrightarrow{\bar{\gamma} \in [1,3]} C$$

Following the semantics of the delay scheduler, we would first transform *Bufferable* to its fixed-delay equivalent, *Bufferable'* by applying Lemma 4.

$$A' \xrightarrow{[4,8]} B' \xrightarrow{\gamma=0} C'$$

If we assume A is executed at $t = 0$, the only question is when to schedule C (or its fixed-delay equivalent, C'). According to the semantics of *Buffering*, if B is observed at $t = 2$, we know that B was assigned at $t = 1$. Thus, we only need to wait until $t = 6$ to schedule C . However, the delay scheduler would schedule according the

constraints found in *Buffering'*, wherein $\xi(B') = 2$ falls earlier than the lower bound of $A' \xrightarrow{[4,8]} B'$, triggering Lemma 5. As a result, we act as if $\xi(B') = 4$ and then wait for the lower bound of $B' \xrightarrow{[4,6]} C'$. The end result is that C' is assigned to a later time of $t = 8$.

From a human mission manager perspective, this wait appears to be a waste. Time is money. And in the case of planetary exploration, time is safety. If a NASA flight controller were to ask why your software is telling astronauts on Moon to just stand there doing nothing, responding that your algorithm *does not know* if it is safe to act, would be unacceptable. Therefore, we contribute a generate-and-test approach that looks for opportunities to avoid buffering when contingent events arrive before their expected windows in the fixed-delay STNU. The goal of this method is to dispatch future events earlier if possible.

At its core, optimistic rescheduling consists of copying the original variable-delay STNU then rewriting it to reflect the resolution of uncertainty so far. Key to rewriting the variable-delay STNU is narrowing the constraint and observation delay to match what was observed. We then re-perform controllability checks. If controllable, we have a new schedule that removes the need to buffer this contingent event. If not controllable, we do nothing, buffer the contingent event as planned, and continue dispatching against the original schedule.

We now step through the Event Observations with optimistic rescheduling algorithm (Algorithm 8) in detail.

We cannot know if an event is buffered if we do not attempt to schedule it. Our first step is to schedule an event like normal. If scheduling is possible without buffering, we simply return whether scheduling was successful.

If the event was buffered, then we begin to optimistically reschedule. We do so by tightening the bounds of the original VDC STNU, $S_{original}$, based on the observation we received, which is the responsibility of Algorithm 9, implementing Lemma 13.

If the rewritten STNU, S^* , is found to be VDC, we prepare to schedule it. First we iterate through all the assignments in the partial schedule and make the same assignments against the new STNU. When assignments are made, we subtract out

Input: Original VDC STNU S ; Equivalent fixed-delay function γ ;
 Partial history ξ ; Executed events map $Ex(S, x)$; Observed contingent event x ;
 Normalized lower bound \hat{x} ; Current time t ;
Output: Boolean whether x was successfully scheduled, VDC STNU

Event Observations with Optimistic Rescheduling:

```

1   successp, bufferedp ← updateSchedule(S, x, t);
2   if  $\neg$ bufferedp then
3   |   return successp, S;
4   endif
5    $S^* \leftarrow \text{rewriteSTNU}(S, x, t)$ ;
6   if  $S^*$  is not variable-delay controllable then
7   |   return successp, S;
8   endif
9   for  $a$  in  $\xi$  // $a$  is an assignment
10  do
11  |   if  $\gamma(a[\text{event}]) \neq \infty$  then
12  |   |   updateSchedule( $S^*$ ,  $a[\text{event}]$ ,  $a[\text{time}] + \gamma(a[\text{event}])$ );
13  |   endif
14  end
15  for  $event$  in  $Ex(S)$  do
16  |    $Ex(S^*, x) \leftarrow Ex(S, x)$ 
17  end
18  updateSchedule( $S^*$ ,  $\hat{x}$ ,  $t$ );
19
20  return true,  $S^*$ ;
```

Algorithm 8: An Algorithm for observing contingent events with optimistic rescheduling.

the fixed observation delay. In this loop, we add the observation delay back, lest it be subtracted from the original observation twice.

If any contingent events with infinite delay were observed, they would have been marked executed but not assigned. We iterate through the executed events of S and mark the same events executed in S^* .

The distance graph, partial schedule, and executed events of S^* now match that of S before x_c was received. We are almost safe to record a new observation. Lastly, we must address the executable event representing the normalized lower bound of x_c , \hat{x}_c . During scheduling, we would have received an RTED consisting of $\langle l + \bar{\gamma}^+(x_c), \hat{x}_c \rangle$. Given that x_c arrived before $l + \bar{\gamma}^+(x_c)$, we never would have assigned \hat{x}_c , so we assign $\xi(\hat{x}_c) = t$ now. We finally update the schedule with the contingent event that arrived.

Lemma 13. *If a contingent event, $x_c \in X_c$, where $u - l > \bar{\gamma}^+(x_c) - \bar{\gamma}^-(x_c)$, is observed at time t and when $t < l + \bar{\gamma}^+(x_c)$, we may replace x_c and $\bar{\gamma}(x_c)$ with a constraint, x_c^* , and variable-delay function, $\bar{\gamma}(x_c^*)$, with narrower bounds as follows.*

$$\begin{aligned} x_c^* &= [l^*, u^*] \\ x_c^* &= [\max(l, t - \bar{\gamma}^+(x_c)), \min(u, t - \bar{\gamma}^-(x_c))] \\ \bar{\gamma}(x_c^*) &= [\max(\bar{\gamma}^-(x_c), t - u), \min(\bar{\gamma}^+(x_c), t - l)] \end{aligned}$$

Proof. Buffering is only possible if the conditions of Lemmas 4 and 5 are triggered. By Lemma 4, we are guaranteed to be able to narrow where in the range $[l, u]$ x_c was scheduled. By Lemma 5, we know that rewritten bounds will lead to an assignment of x_c that is no later than $l + \bar{\gamma}^+(x_c)$. Our tool for narrowing the bounds is Equation 5.5, which allows us to use the observation to reason over the assignment and observation delay. Our strategy is to look at the extreme cases leading to an observation.

We start by reasoning over the earliest and latest assignments respectively. In order for x_c to be assigned as early as possible, l^* , we assume the delay has taken on its maximum value, $\bar{\gamma}^+(x_c)$.

$$\xi(x_c) = \text{obs}(x_c) - \gamma(x_c) \quad (7.1)$$

$$l^* = t - \bar{\gamma}^+(x_c) \quad (7.2)$$

Likewise, to find the last possible assignment leading to an observation, we subtract the smallest observation delay, $\bar{\gamma}^-(x_c)$.

$$u^* = t - \bar{\gamma}^-(x_c) \quad (7.3)$$

Given that Nature will adhere to the constraints originally put forth in S , the bounds of x_c^* must remain within the bounds of x_c . Hence, we guarantee the lower bound is at least l while the upper bound is at most u .

$$l^* = \max(l, t - \bar{\gamma}^+(x_c))$$

$$u^* = \min(u, t - \bar{\gamma}^-(x_c))$$

We use the same logic for narrowing the observation delay. If x_c was assigned as late as possible, u , then the observation delay would be minimized, $\bar{\gamma}^-(x_c^*)$. Likewise, if x_c was assigned as early as possible, l , the observation delay would be maximized, $\bar{\gamma}^+(x_c^*)$. The narrowed lower and upper bounds of $\bar{\gamma}(x_c)^*$ are as follows.

$$\gamma = \text{obs}(x_c) - \xi(x_c)$$

$$\bar{\gamma}^-(x_c^*) = t - u$$

$$\bar{\gamma}^+(x_c^*) = t - l$$

As before, the bounds of $\bar{\gamma}(x_c^*)$ must stay within the original bounds of $\bar{\gamma}(x_c)$,

leaving us with the following narrowed observation delay.

$$\bar{\gamma}^-(x_c^*) = \max(\bar{\gamma}^-(x_c), t - u) \quad (7.4)$$

$$\bar{\gamma}^+(x_c^*) = \min(\bar{\gamma}^+(x_c), t - l) \quad (7.5)$$

□

We revisit the example from the beginning of this section to see Lemma 13 in action. As we saw before, any $\text{obs}(B)$ before $t = 4$ will result in buffered assignments.

$$A \xrightarrow{[1,7]} B \xrightarrow{\bar{\gamma} \in [1,3]} C$$

Let $t = 3$. We will step through the reasoning for narrowing the bounds of x_c accordingly.

$$x_c^* \in [\max(l, t - \bar{\gamma}^+(x_c)), \min(u, t - \bar{\gamma}^-(x_c))]$$

$$x_c^* \in [\max(1, 3 - 3), \min(7, 3 - 1)]$$

$$x_c^* \in [1, 2]$$

$$\bar{\gamma}(x_c^*) \in [\max(\bar{\gamma}^-(x_c), t - u), \min(\bar{\gamma}^+(x_c), t - l)]$$

$$\bar{\gamma}(x_c^*) \in [\max(1, 3 - 7), \min(3, 3 - 1)]$$

$$\bar{\gamma}(x_c^*) \in [1, 2]$$

We find that $\xi(x_c)$ must have fallen somewhere in the range of $[1, 2]$, while $\bar{\gamma}(x_c)$ was resolved somewhere in $[1, 2]$. Looking at the extremes, it is clear that there are multiple combinations of the assignment and observation delay that could lead to an observation at $t = 3$. While the narrowed range allows for observations other than $t = 3$, for instance, if $\xi(x_c) = 2$ and $\text{obs}(x_c) = 2$ yielding an observation at $t = 4$, there are no other ranges of assignments or observation delay outside of $\xi(x_c) \in [1, 2]$

and $\bar{\gamma}(x_c) \in [1, 2]$ that would allow an observation at $t = 3$.

Input: VDC STNU $S_{original}$; Variable-delay function $\bar{\gamma}$;

Observed contingent event x ; Observation time t ;

Output: VDC STNU

Initialization: $S_{new} \leftarrow \text{copy}(S_{original})$

Rewrite STNU:

```

1   for constraint in  $S_{new}$  do
2       if constraint ends in  $x$  then
3           constraint[lower]  $\leftarrow \max(\text{constraint}[lower], t - \bar{\gamma}^+(x))$ ;
4           constraint[upper]  $\leftarrow \min(\text{constraint}[upper], t - \bar{\gamma}^-(x))$ ;
5            $\bar{\gamma}^-(x) \leftarrow \max(\bar{\gamma}^-(x), t - \text{constraint}[upper])$ ;
6            $\bar{\gamma}^+(x) \leftarrow \max(\bar{\gamma}^+(x), t - \text{constraint}[lower])$ ;
7       endif
8   end
9   return  $S_{new}$ ;
```

Algorithm 9: An Algorithm for rewriting an STNU given the resolution of uncertainty of a contingent link.

The complexity of Algorithm 8 is dominated by the loop over `updateSchedule`. Each call to `updateSchedule` is $O(N^3)$ in the number of events. In the worst case scenario, every event up to the last contingent event has been scheduled, giving us a complexity of $O(N^4)$. We discuss potential means for improving optimistic rescheduling in Section 7.1.1.

7.1.1 Possible Improvements

What if we looked for conflicts? Could we possibly search for a time to dispatch early in the buffered execution space?

Smarter rewriting STNU. Could we update the existing d-graph directly and check it for SRNCs? maybe?

7.2 Coordination

We were focused on addressing the multi-agent (MA) online scheduling problem. Before scheduling, we must contend with planning, e.g. building variable-delay STNUs

for each agent. We considered extending the two existing planning approaches described below to model variable observation delay between agents. We ultimately decided neither were fit for the motivating scenarios of this thesis. Instead, we used a manual planning approach more akin to the ISS EVA planning process.

The first planning approach we considered was to model the system as a Multi-Agent STNU (MASTNU) [4]. MASTNUs allow modelers to describe temporal constraints between multiple agents, then check the overall dynamic controllability of the system. To check the controllability of a MASTNU, the first step is to perform temporal decoupling with the goal of producing individual dynamically controllable STNUs for each agent that can be dynamically scheduled per usual. While superficially promising, there is a considerable drawback to this approach, namely that temporal decoupling is sound but not complete, i.e. temporal decoupling may report failure even when the MASTNU is dynamically controllable. This limits the utility of MASTNUs as a planning tool.

The other approach to this problem we are aware of is Stedl’s Hierarchical Reformulation (HR) algorithm [43]. HR begins with a MA temporal plan network (TPN), which is similar to a MASTNU (though HR pre-dates MASTNUs). Stedl’s key insight is to avoid inter-agent communication altogether by reformulating constraints between groups of agents such that they are strongly controllable. As such, no communication between agents is required. A centralized dispatcher is then responsible for then handing events to agents. We also assume that there is no central authority, making HR a poor fit for our problem domain.

Both MASTNUs and HR assume communications between agents are either instantaneous or impossible, i.e. with an infinite delay. As we will see in Section 4.3, our formalism for variable observation delay allows a *spectrum* of communication delay. While we felt it was possible to shoehorn uncertain observation delay into MASTNUs or HR, we felt both were a poor choice because of their pre-existing expectations with respect to communication. In combination with our focus on online scheduling, we decided to forgo extending either formalism to account for observation delay. Instead our planning process simply consists of manually writing variable-delay STNUs with

intra-agent and inter-agent temporal constraints by hand.

We believe it may be possible for MASTNUs or HR to be expanded to include variable observation delay, though we leave that problem for future research.

We considered framing our approach to inter-agent communication as a distributed consensus problem because we believed we needed a means for disparate agents to agree on the state of the world. Existing distributed consensus algorithms like Paxos [42] or Raft [41] would then be integrated into the communication layer of Kirk and take responsibility for ensuring that agents agree on which events have been scheduled.

Ultimately the drawbacks of a distributed consensus approach outweighed the benefits. Chiefly, both Paxos and Raft assume that communications are either instantaneous and freely available or that agents have gone dark (i.e. can no longer communicate). This communication model is incongruous with the explicitly modeled communications of the VDC formalism. Furthermore, the VDC formalism allows us to model that agents never receive communications, negating the requirement for distributed consensus.

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix A

Comparison of Variable-Delay STNUs to Partially Observable STNUs

The delay scheduler is flexible in that so long as it receives a variable-delay STNU, it is capable of scheduling. Human modelers have flexibility in how they represent temporal constraints in that there are many flavors of STNUs, each with their own advantages and disadvantages. Earlier, we presented RMPL as a modeling language that is compiled to variable-delay STNUs. There are other choices for modeling frameworks. Here, we present a comparison of variable-delay STNUs to POSTNUs [5], a flavor that is similar in many respects. This section presents a comparison of variable-delay STNUs and POSTNUs, including transformations that allow some classes of POSTNUs to be represented as variable-delay STNUs.

One of the strengths of the variable-delay controllability model is its ability to generalize the concepts of strong and dynamic controllability. This technique was first seen in greater depth in the context of POSTNUs. In an STNU, all contingent events are either instantaneously observable under a dynamic controllability model or entirely unobservable under a strong controllability model. In POSTNUs, contingent events can be marked observable and unobservable. To say that a POSTNU is dynamically controllable equates to asserting that it is possible to construct a schedule

during execution that respects all constraints if the scheduler only receives information about observable contingent events.

While, superficially, POSTNUs and delay STNUs appear to model distinct problems in temporal reasoning, all delay STNUs can be accurately represented as POSTNUs. While the converse is not true, there is a subset of POSTNUs that delay STNUs are able to model. It is advantageous to translate POSTNUs to delay STNUs when possible because we are guaranteed to finish controllability checks for delay STNUs in polynomial time, while evaluating the controllability of POSTNUs in general is harder [5]. Furthermore, the sub-class of POSTNUs that can be checked efficiently and accurately, those without chained contingent links [44], are members of the subset of POSTNUs that can be expressed directly as STNUs with fixed-delay, and likewise variable-delay, functions , [34, p. 59]. The converse is also true - we may emulate STNUs with variable-delay functions as POSTNUs without chained contingent links. Below, we elaborate on translations from delay STNUs to POSTNUs, before describing how we can express POSTNUs without chained contingent links as STNUs with fixed-delay functions. Note that this is not a comprehensive list of transformations between delay STNUs and POSTNUs - our aim is to describe the minimum set of transformations required to model POSTNUs without chained contingent links as delay STNUs. For the following discussion, let S be a delay STNU and P be an equivalent POSTNU.

We present these transformations to demonstrate that the delay scheduler is capable of scheduling POSTNUs without chained contingencies. So long as it receives a variable-delay STNU, the fact that POSTNUs can be scheduled allows modelers additional flexibility in their means of representing the problem domain.

We start with an S that consists of the links $A \Rightarrow B$ and $B \rightarrow D$ with delay function $\bar{\gamma}(B)$. See Figure A for an example translation between a fixed-delay STNU and a POSTNU.

Lemma 14. *For contingent link $A \Rightarrow B$ in S with observation delay $\bar{\gamma}(B) = [l, u]$, where $0 \leq l \leq u < \infty$, and outgoing requirement link $B \rightarrow D$, we may emulate observation delay in P by copying $A \Rightarrow B$ and $B \rightarrow D$ to P , enforcing that B is*

unobservable, and adding a new observable contingent event, B' with $B \xrightarrow{[l,u]} B'$.

Proof. In both S and P , we do not observe B directly, yet we define an outgoing requirement link, $B \rightarrow D$, that depends entirely on the resolution of B . The only information available to reason about the assignment of B comes in the form of an indirect observation, B' or $\bar{\gamma}(B)$, received after a delay in $\mathbb{R}^{\geq 0}$. If P was not equivalent to S , we would be able to learn the assignment of B without waiting $\bar{\gamma}(B)$ time units after its true assignment. Thus, because we must wait $B' - B \in [l, u]$ time units to learn the assignment of B , and $B \rightarrow D$ has equivalent constraints between S and P , P must model the same semantics as S . \square

Lemma 15. *For a contingent event B with variable-delay function $\bar{\gamma}(B) = [0, 0]$ in S , we may emulate the same constraints with an observable contingent event, B in P .*

Proof. The variable-delay function enforces instantaneous observation. By the definition of observable contingent events in the POSTNU model, we will observe B instantaneously. \square

A POSTNU with a chained contingency is defined as follows. Consider a chain of contingent events, $A \Rightarrow B$ and $B \Rightarrow C$. If B has one or more outgoing links to free or contingent events other than C , it is a chained contingency. Lemma 14 results in a POSTNU without chained contingencies, hence variable-delay STNUs fall into the subclass of POSTNUs that can be checked efficiently [44].

In the other direction, to transform a POSTNU without chained contingencies into an STNU with variable-delay functions, we need to address three cases of contingent constraints: (1) unobservable contingent events not immediately followed by other contingent constraints, (2) unobservable contingent events immediately followed by other contingent constraints, and (3) observable contingent constraints.

Lemma 16. *For an unobservable event B in P , with no outgoing contingent links, we can emulate it in S with a contingent event B and upper bound of its variable-delay function set to $\bar{\gamma}^+(B) = \infty$.*

Proof. We will not observe B nor will outgoing contingent links provide information about B . As such we define $\bar{\gamma}^+(B) = \infty$ in S .¹ From a controllability standpoint for both S and P , we know the *a priori* bounds of B but will not learn its true assignment. \square

Lemma 17. *For an unobservable contingent link $A \xrightarrow{[m,n]} B$ in P , with a single outgoing link, $B \xrightarrow{[w,z]} C$, we replace the two constraints from P in S with a concatenated constraint, $A \xrightarrow{[m+w,n+z]} C$.*

Proof. The only information we may receive is the observation of C . Given there are no other outgoing links from B , folding B into the successive contingent constraint can not affect the semantics of the network. The bounds of the new link, $A \xrightarrow{[m+w,n+z]} C$ is the result of summing the intervals of $A \xrightarrow{[m,n]} B$ and $B \xrightarrow{[w,z]} C$: $[m, n] + [w, z] = [m + w, n + z]$. \square

Note that we did not specify whether C is observable in P . After applying Lemma 17, we then apply either Lemma 15 or 16 to C .

Lemma 18. *For an observable contingent event $A \xrightarrow{[m,n]} B$ in P , with a single outgoing link to an observable contingent event, C , $B \xrightarrow{[w,z]} C$, we create three constraints in S : $A \xrightarrow{[m,n]} B$, $B \xrightarrow{[0,0]} B'$, and $B' \xrightarrow{[w,z]} C$ where $\bar{\gamma}(B) = [0, 0]$.*

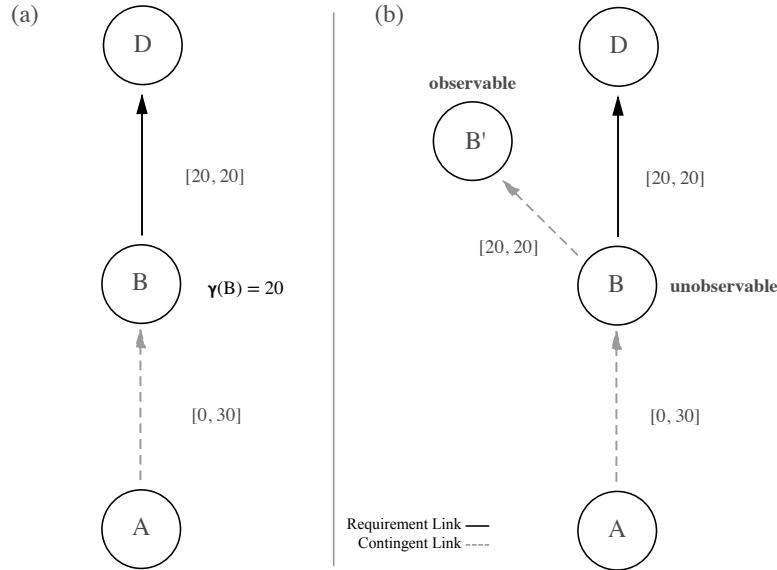
Proof. Given C is observable in P , a simulated free event, B' in S , can be scheduled simultaneously with B . Any contingent constraints following B now start at an executable event and are thus valid constraints in S . B is observable, so we need no observation delay according to Lemma 15. \square

Thus, delay STNUs are sufficiently capable of expressing all POSTNUs that can efficiently be checked for controllability using today's tractable POSTNU algorithms.

It is not clear if controllability can be checked more efficiently across a greater subset of POSTNUs beyond those without chained contingencies. However, it is worth highlighting that variable-delay controllability can be leveraged to construct improved

¹Note: ,p. [34, p. 60] erroneously claims that we should define $\gamma(B) = 0$ for unobservable events.

Figure A-1: (a) An STNU with a contingent constraint that has a certain delay. (b) One possible way of rewriting the STNU as an equivalent POSTNU. This particular POSTNU exhibits a chained contingency, as B is a contingent event that starts a contingent constraint and is connected to B' via a contingent constraint.



algorithms with respect to scheduling and controllability of POSTNUs. The model for observation delay proposed by variable-delay controllability can be expressed exactly as a POSTNU with a “single-headed” chained contingency² as shown in Figure Ab; the main difference is that we represent the contingent link between B and B' with our variable-delay function $\bar{\gamma}(B)$. Hence, the algorithm we present for variable-delay controllability can be used to both solve POSTNUs without chained contingencies, as described above, as well as those POSTNUs with single-headed chained contingencies. Approaches inspired by variable-delay controllability have been used to further expand POSTNU dynamic controllability checking in more expressive chained instances [45]. We hope that insights from variable-delay controllability will continue to expand the subset of POSTNUs that can be controllability checked, and as such we advocate for continued development of the theory of variable-delay controllability as a relevant framework for modelers.

²To borrow the term “single-headed” from [45].

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix B

RMPL Control Programs and STNUs

Key to the challenge of being a mission planner is to understand the constraints between events. RMPL is an abstraction layer, meaning that it will interpret RMPL and produce a delay STNU reflecting its own interpretation, which may not align with the mission planner’s intention. We have seen students in the lab be surprised by the temporal constraints generated by RMPL, and, through the experiments involved in this thesis, have also found RMPL to be less-than-intuitive on occasion. The chief cause of confusion is a disjoint between the fundamental unit of temporal reasoning, the temporal event, and the fundamental unit of RMPL control programs, the episode, which consists of a start and an end event. This is not a limitation of the semantics of RMPL, rather, it is a naming issue.

To elaborate, temporal reasoning literature emphasizes events as meaningful time-points. For instance, we used numbered `Confirm:0:0` events to represent the end of an installation task in Sections 5.4 and 6.3.1, while the start of the task was an `Install:0:0` event, e.g. $\text{Install}:0:0 \xrightarrow{[l,u]} \text{Confirm}:0:0$. Depending on the size of the generated STNU, the `Confirm:0:` event then had outgoing edges to events such as `Start:0:1`, `Install:1:0`, or `ALL:END`. In RMPL, however, a representation of this constraint between events with these names is impossible.

Consider the following control program.

```
(define-control-program take-pictures ()
  (declare (primitive)
    (duration (simple :lower-bound 1 :upper-bound 5))))
```

We have defined an episode named `take-pictures`. It represents a requirement constraint in the form of `take-pictures:start` $\xrightarrow{[1,5]}$ `take-pictures:end`. Note that the one episode led to the creation of two events. We now add a second episode and show the two options RMPL gives us for joining them in series.

```
(define-control-program eat-snack ()
  (declare (primitive)
    (duration (simple :lower-bound 3 :upper-bound 7))))
```

;; Sequence option 1

```
(define-control-program with-slack ()
  (with-temporal-constraint (simple-temporal :lower-bound 6 :upper-bound 10)
    (sequence (:slack t)
      (take-pictures)
      (eat-snack))))
```

;; Sequence option 2

```
(define-control-program no-slack ()
  (with-temporal-constraint (simple-temporal :lower-bound 6 :upper-bound 10)
    (sequence (:slack nil)
      (take-pictures)
      (eat-snack))))
```

We have two commonly used options for `:slack` in the sequence, `(:slack nil)` and `(:slack t)`. If slack is applied, episodes are connected with $[0, \infty]$ constraints, effectively guaranteeing episode ordering without enforcing that the latter episode must start immediately after the first. Ignoring the overall constraint, the two control programs are connected like so.

$$\text{take-pictures:start} \xrightarrow{[3,7]} \text{take-pictures:end} \xrightarrow{[0,\infty]} \text{eat-snack:start} \xrightarrow{[3,7]} \text{eat-snack:end}$$

Without slack, the constraints are arranged as follows.

$$\text{take-pictures:start} \xrightarrow{[3,7]} \text{take-pictures:end} \xrightarrow{[0,0]} \text{eat-snack:start} \xrightarrow{[3,7]} \text{eat-snack:end}$$

The RMPL compiler takes it a step further. A constraint of the form $A \xrightarrow{[0,0]} B$ enforces simultaneous execution of A and B , making one of the events redundant from a scheduling perspective. In this example, RMPL removes `take-pictures:end`, leaving us with three events for the two constraints.

$$\text{take-pictures:start} \xrightarrow{[3,7]} \text{eat-snack:start} \xrightarrow{[3,7]} \text{eat-snack:end}$$

From an execution perspective, `eat-snack:start` both signifies the end of taking pictures and the beginning of snacking.

Going back to the installation example, we want the execution semantics of deciding when to start, traversing to an installation location, performing the installation, waiting for the response, and then moving to the next installation. As described in Section 5.4, the delay STNU takes the form as follows, with $\bar{\gamma}(\text{confirm}:0:0) = [0, 3]$.

$$\text{start}:0:0 \xrightarrow{[1,15]} \text{traverse}:0:0 \xrightarrow{[1,14]} \text{install}:0:0 \xrightarrow{[1,6]} \text{confirm}:0:0 \xrightarrow{[2,12]} \text{start}:0:1$$

In RMPL, we model each iteration of the procedure like so. (We use the /0-0 numbering instead of the :0:0 scheme in RMPL because : causes errors related to lisp package exports.)

```
(define-control-program traverse/0-0 ()
  (declare (primitive))
```

```

(duration (simple :lower-bound 1 :upper-bound 15)
          :contingent t)))

(define-control-program install/0-0 ()
  (declare (primitive)
    (duration (simple :lower-bound 1 :upper-bound 14)))))

(define-control-program confirm/0-0 ()
  (declare (primitive)
    (duration (simple :lower-bound 1 :upper-bound 6
                      :min-observation-delay 0 :max-observation-delay 3)
              :contingent t)))

(define-control-program start/0-1 ()
  (declare (primitive)
    (duration (simple :lower-bound 2 :upper-bound 12)))))

(define-control-program main ()
  (with-temporal-constraint (simple-temporal :upper-bound 108)
    (sequence (:slack nil)
      (traverse/0-0)
      (install/0-0)
      (confirm/0-0)
      (start/0-1))))
```

This results in a delay STNU of the form below (ignoring the overall upper-bound for simplicity's sake).

$$\begin{array}{c}
 \text{traverse/0-0:start} \xrightarrow{[1,15]} \text{install/0-0:start} \xrightarrow{[1,14]} \text{confirm/0-0:start} \xrightarrow{[1,6]} \\
 \text{start/0-1:start} \xrightarrow{[2,12]} \text{start/0-1:end}
 \end{array}$$

If we need to translate events between the two forms, we simply note that event names are shifted by one place earlier in the delay STNU generated by RMPL.

THIS PAGE INTENTIONALLY LEFT BLANK

Bibliography

- [1] D. A. Coan, Exploration EVA System Concept of Operations, National Aeronautics and Space Administration, Houston, TX, EVA-EXP-0042 Revision B, 2020.
- [2] R. Dechter, I. Meiri, and J. Pearl, Temporal constraint networks, *Artificial intelligence*, vol. 49, no. 1-3, pp. 6195, 1991, doi: 10.1016/0004-3702(91)90006-6.
- [3] T. Vidal and H. Fargier, Handling Contingency in Temporal Constraint Networks: From Consistency to Controllabilities, *Journal of experimental and theoretical artificial intelligence*, vol. 11, no. 1, pp. 2345, 1999, doi: 10.1080/095281399146607.
- [4] G. Casanova, C. Pralet, C. Lesire, and T. Vidal, Solving dynamic controllability problem of multi-agent plans with uncertainty using mixed integer linear programming, *Frontiers in artificial intelligence and applications*, vol. 285, pp. 930938, 2016, doi: 10.3233/978-1-61499-672-9-930.
- [5] M. D. Moffitt, On the partial observability of temporal uncertainty, *Proceedings of the national conference on artificial intelligence*, vol. 2, pp. 10311037, 2007.
- [6] N. Bhargava, C. Muise, and B. C. Williams, Variable-delay controllability, in *IJCAI International Joint Conference on Artificial Intelligence*, 2018, vol. 2018-July, pp. 46604666. doi: 10.24963/ijcai.2018/648.
- [7] L. Hunsberger, Efficient execution of dynamically controllable simple temporal networks with uncertainty, *Acta informatica*, vol. 53, no. 2, pp. 89147, 2016, doi: 10.1007/s00236-015-0227-0.
- [8] J. W. McBarron, Past, present, and future: The U.S. EVA Program, *Acta astronautica*, vol. 32, no. 1, pp. 514, 1994, doi: 10.1016/0094-5765(94)90143-0.
- [9] C. P. Sonnett, REPORT of the AD HOC WORKING GROUP ON APOLLO EXPERIMENTS AND TRAINING on the SCIENTIFIC ASPECTS OF THE APOLLO PROGRAM, NASA, 1963.
- [10] J. M. Hurtado, K. Young, J. E. Bleacher, W. B. Garry, and J. W. Rice, Field geologic observation and sample collection strategies for planetary surface

- exploration: Insights from the 2010 Desert RATS geologist crewmembers, *Acta astronautica*, vol. 90, no. 2, pp. 344355, 2013, doi: 10.1016/j.actaastro.2011.10.015.
- [11] K. Young and T. Graff, Planetary Science Context for EVA, in *NASA EVA Exploration Workshop*, 2020, p. 40.
 - [12] A. Kanelakos, Artemis EVA Flight Operations - Preparing for Lunar EVA Training & Execution, in *NASA EVA Exploration Workshop*, 2020, p. 47.
 - [13] C. Campbell, Advanced EMU Portable Life Support System (PLSS) and Shuttle/ISS EMU Schematics, a Comparison, *42nd international conference on environmental systems*, pp. 118, 2012, doi: 10.2514/6.2012-3411.
 - [14] E. S. Patterson and D. D. Woods, Shift changes, updates, and the on-call architecture in space shuttle mission control, *Computer supported cooperative work*, vol. 10, no. 3-4, p. 27, 2001, doi: 10.1023/A:1012705926828.
 - [15] S. J. Payler *et al.*, Developing Intra-EVA Science Support Team Practices for a Human Mission to Mars, *Astrobiology*, vol. 19, no. 3, pp. 387400, 2019, doi: 10.1089/ast.2018.1846.
 - [16] D. A. Coan, Exploration EVA System Concept of Operations Summary for Artemis Phase 1 Lunar Surface Mission, NASA, Houston, TX, 2020.
 - [17] M. A. Seibert, D. S. Lim, M. J. Miller, D. Santiago-Materese, and M. T. Downs, Developing Future Deep-Space Telecommunication Architectures: A Historical Look at the Benefits of Analog Research on the Development of Solar System Internetworking for Future Human Spaceflight, *Astrobiology*, vol. 19, no. 3, pp. 462477, Mar. 2019, doi: 10.1089/ast.2018.1915.
 - [18] M. J. Miller and K. M. Feigh, *Addressing the envisioned world problem: A case study in human spaceflight operations*, vol. 5. Cambridge University Press, 2019. doi: 10.1017/dsj.2019.2.
 - [19] M. J. Miller, K. M. McGuire, and K. M. Feigh, Information flow model of human extravehicular activity operations, *Ieee aerospace conference proceedings*, vol. 2015-June, 2015, doi: 10.1109/AERO.2015.7118942.
 - [20] M. J. Miller, K. M. McGuire, and K. M. Feigh, Decision Support System Requirements Definition for Human Extravehicular Activity Based on Cognitive Work Analysis, *Journal of cognitive engineering and decision making*, vol. 11, no. 2, pp. 136165, 2017, doi: 10.1177/1555343416672112.

NO_ITEM_DATA:Sehlke2019

- [22] B. C. Williams, M. D. Ingham, S. H. Chung, and P. H. Elliott, Model-based programming of intelligent embedded systems and robotic space explorers, *Proceedings of the ieee*, vol. 91, no. 1, pp. 212236, 2003, doi: 10.1109/JPROC.2002.805828.
- [23] B. C. Williams and R. J. Ragno, Conflict-directed A* and its role in model-based embedded systems, *Discrete applied mathematics*, vol. 155, no. 12, pp. 15621595, 2007, doi: 10.1016/j.dam.2005.10.022.
- [24] P. Kim, B. C. Williams, and M. Abramson, Executing reactive, model-based programs through graph-based temporal planning, *Ijcai international joint conference on artificial intelligence*, pp. 487493, 2001.
- [25] R. E. Fikes and N. J. Nilsson, Strips: A new approach to the application of theorem proving to problem solving, *Artificial intelligence*, vol. 2, no. 3-4, pp. 189208, 1971, doi: 10.1016/0004-3702(71)90010-5.
- [26] E. Fernández González, Generative Multi-Robot Task and Motion Planning Over Long Horizons, Massachusetts Institute of Technology, 2018.
- [27] J. Chen, B. C. Williams, and C. Fan, Optimal mixed discrete-continuous planning for linear hybrid systems, in *HSCC 2021 - Proceedings of the 24th International Conference on Hybrid Systems: Computation and Control (part of CPS-IoT Week)*, 2021, vol. 1. doi: 10.1145/3447928.3456654.
- [28] P. H. Morris, N. Muscettola, and T. Vidal, Dynamic Control Of Plans With Temporal Uncertainty, 2001.
- [29] P. Morris and N. Muscettola, Temporal dynamic controllability revisited, *Proceedings of the national conference on artificial intelligence*, vol. 3, pp. 11931198, 2005.
- [30] P. Morris, A structural characterization of temporal dynamic controllability, *Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics)*, vol. 4204 LNCS, pp. 375389, 2006, doi: 10.1007/11889205
28.
- [31] P. Morris, Dynamic controllability and dispatchability relationships, *Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics)*, vol. 8451 LNCS, no. Dc, pp. 464479, 2014, doi: 10.1007/978-3-319-07046-9
33.
- [32] A. Cimatti, A. Micheli, and M. Roveri, Solving temporal problems with uncertainty using SMT: Strong Controllability, *Constraints*, vol. 20, no. 1, pp.

129, 2012, doi: 10.1007/s10601-014-9167-5.

- [33] M. Ingham, R. Ragno, A. Wehowsky, and B. Williams, The Reactive Model-based Programming Language, MIT Space Systems and Artificial Intelligence Laboratories, 2002.
- [34] N. Bhargava, Multi-Agent Coordination under Limited Communication, Massachusetts Institute of Technology, 2020.
- [35] G. Kiczales, J. Des Rivières, and D. G. Bobrow, *The art of the metaobject protocol*. Cambridge, Mass: MIT Press, 1991.
- [36] M. Fox and D. Long, PDDL2.1: An extension to PDDL for expressing temporal planning domains, *Journal of artificial intelligence research*, vol. 20, pp. 61124, 2003, doi: 10.1613/jair.1129.
- [37] N. Bhargava, C. Muise, T. Vaquero, and B. Williams, Delay Controllability : Multi-Agent Coordination under Communication Delay, Massachusetts Institute of Technology, Cambridge, MA, 2018.
- [38] N. Bhargava, C. Muise, T. Vaquero, and B. Williams, Managing communication costs under temporal uncertainty, in *IJCAI International Joint Conference on Artificial Intelligence*, 2018, vol. 2018-July, pp. 8490. doi: 10.24963/ijcai.2018/12.
- [39] L. Hunsberger, A faster execution algorithm for dynamically controllable STNUs, *Proceedings of the 20th international symposium on temporal representation and reasoning*, pp. 2633, 2013, doi: 10.1109/TIME.2013.13.
- [40] L. Hunsberger, Fixing the semantics for dynamic controllability and providing a more practical characterization of dynamic execution strategies, *Time 2009 - 16th international symposium on temporal representation and reasoning*, pp. 155162, 2009, doi: 10.1109/TIME.2009.25.
- [41] D. Ongaro and J. Ousterhout, In search of an understandable consensus algorithm, *Proceedings of the 2014 usenix annual technical conference, usenix atc 2014*, pp. 305319, 2014.
- [42] L. Lamport *et al.*, The Part-Time Parliment, *Acm transactions on computer systems*, vol. 16, no. 2, pp. 373386, 1998, doi: 10.1145/568425.568433.
- [43] J. L. Stedl, Managing Temporal Uncertainty Under Limited Communication: A Formal Model of Tight and Loose Team Coordination, Massachusetts Institute of Technology, 2004.

- [44] A. Bit-Monnnot, M. Ghallab, and F. Ingrand, Which contingent events to observe for the dynamic controllability of a plan, *Ijcai international joint conference on artificial intelligence*, vol. IJCAI-16, no. July, pp. 30383044, 2016.
- [45] P. H. Morris and A. Bit-monnot, Dynamic Controllability with Single and Multiple Indirect Observations, in *ICAPS 2019 - Proceedings of the 29th International Conference on Automated Planning and Scheduling*, 2019, p. 9.