

# Synthesis of Surveillance Strategies via Belief Abstraction

Suda Bharadwaj<sup>1</sup> and Rayna Dimitrova<sup>2</sup> and Ufuk Topcu<sup>1</sup>

**Abstract**—We study the problem of synthesizing a controller for a robot with a *surveillance objective*, that is, the robot is required to maintain knowledge of the location of a moving, possibly adversarial target. We formulate this problem as a one-sided partial-information game in which the winning condition for the agent is specified as a temporal logic formula. The specification formalizes the surveillance requirement given by the user, including additional non-surveillance tasks. In order to synthesize a surveillance strategy that meets the specification, we transform the partial-information game into a perfect-information one, using abstraction to mitigate the exponential blow-up typically incurred by such transformations. This enables the use of off-the-shelf tools for reactive synthesis. We use counterexample-guided refinement to automatically achieve abstraction precision that is sufficient to synthesize a surveillance strategy. We evaluate the proposed method on two case-studies, demonstrating its applicability to large state-spaces and diverse requirements.

## I. INTRODUCTION

Performing surveillance, that is, tracking the location of a target, has many applications. If the target is adversarial, these applications include patrolling and defense, especially in combination with other objectives, such as providing certain services or accomplishing a mission. Techniques for tracking non-adversarial but unpredictable targets have been proposed in settings like surgery to control cameras to keep a patient’s organs under observation despite unpredictable motion of occluding obstacles [?]. Mobile robots in airports have also been proposed to carry luggage for clients, requiring the robots to follow the human despite unpredictable motion and possibly sporadically losing sight of the target [?].

When dealing with a possibly adversarial target, a strategy for the surveying agent for achieving its objective can be seen as a strategy in a two-player game between the agent and the target. Since the agent may not always observe, or even know, the exact location of the target, surveillance is, by its very nature, a partial-information problem. It is thus natural to reduce surveillance strategy synthesis to computing a winning strategy for the agent in a two-player partial-information game. Game-based models for related problems have been extensively studied in the literature. Notable examples include pursuit-evasion games [?], patrolling games [?], and graph-searching games [?], where the problem is formulated as enforcing eventual detection, which is, in its essence a search problem – once the target is detected, the game ends. For many applications, this formulation is too restrictive.

Often, the goal is not to detect or capture the target, but to maintain certain level of information about its location over an unbounded (or infinite) time duration, or, alternatively, be able to obtain sufficiently precise information over and over again. In other cases, the agent has an additional objective, such as performing certain task, which might prevent him from capturing the target, but allow for satisfying a more relaxed surveillance objective.

In this paper, we study the problem of synthesizing strategies for enforcing *temporal surveillance objectives*, such as the requirement to never let the agent’s uncertainty about the target’s location exceed a given threshold, or recapturing the target every time it escapes. To this end, we consider surveillance objectives specified in linear temporal logic (LTL), equipped with basic surveillance predicates. This formulation also allows for a seamless combination with other task specifications. Our computational model is that of a two-player game played on a finite graph, whose nodes represent the possible locations of the agent and the target, and whose edges model the possible (deterministic) moves between locations. The agent plays the game with partial information, as it can only observe the target when it is in its area of sight. The target, on the other hand, always has full information about the agent’s location, even when the agent is not in sight. In that way, we consider a model with one-sided partial information, making the computed strategy for the agent robust against a potentially more powerful adversary.

We formulate surveillance strategy synthesis as the problem of computing a winning strategy for the agent in a partial-information game with a surveillance objective. There is a rich theory on partial-information games with LTL objectives [?], [?], and it is well known that even for very simple objectives the synthesis problem is EXPTIME-hard [?], [?]. Moreover, all the standard algorithmic solutions to the problem are based on some form of *belief set construction*, which transforms the imperfect-information game into a perfect-information game and this may be exponentially larger, since the new set of states is the powerset of the original one. Thus, such approaches scale poorly in general, and are not applicable in most practical situations.

We address this problem by using *abstraction*. We introduce an *abstract belief set construction*, which underapproximates the information-tracking abilities of the agent (or, alternatively, overapproximates its belief, i.e., the set of positions it knows the target could be in). Using this construction we reduce surveillance synthesis to a two-player perfect-information game with LTL objective, which we then solve using off-the shelf reactive synthesis tools [?]. Our construction guarantees that the abstraction is sound, that is,

<sup>1</sup>Suda Bharadwaj and Ufuk Topcu are with the University of Texas at Austin

<sup>2</sup>Rayna Dimitrova is with the University of Leicester, UK. Most of this work was done while Rayna Dimitrova was a postdoctoral researcher at UT Austin.

if a surveillance strategy is found in the abstract game, it corresponds to a surveillance strategy for the original game. If, on the other hand, such a strategy is not found, then the method automatically checks if this is due to the coarseness of the abstraction, in which case the abstract belief space is automatically refined. Thus, our method follows the general counterexample guided abstraction refinement (CEGAR) [?] scheme, which has successfully demonstrated its potential in formal verification and reactive synthesis.

**Contributions.** We make the following contributions:

- (1) We propose a *formalization of surveillance objectives* as temporal logic specifications, and frame surveillance strategy synthesis as a partial-information reactive synthesis problem.
- (2) We develop an *abstraction method that soundly approximates* surveillance strategy synthesis, thus enabling the application of efficient techniques for reactive synthesis.
- (3) We design procedures that *automatically refine a given abstraction* in order to improve its precision when no surveillance strategy exists due to coarseness of the approximation.
- (4) We evaluate our approach on different surveillance objectives (e.g, safety, and liveness) combined with task specifications, and discuss the qualitatively different behaviour of the synthesized strategies for the different kinds of specifications.

**Related work.** While closely related to the surveillance problem we consider, pursuit-evasion games with partial information [?], [?], [?] formulate the problem as eventual detection, and do not consider combinations with other mission specifications. Other work, such as [?] and [?], additionally incorporates map building during pursuit in an unknown environment, but again solely for target detection.

Synthesis from LTL specifications [?], especially from formulae in the efficient GR(1) fragment [?], has been extensively used in robotic planning (e.g. [?], [?]), but surveillance-type objectives, such as the ones we study here, have not been considered so far. Epistemic logic specifications [?] can refer to the knowledge of the agent about the truth-value of logical formulas, but, contrary to our surveillance specifications, are not capable of expressing requirements on the size of the agent’s uncertainty.

CEGAR has been developed for verification [?], and later for control [?], of LTL specifications. It has also been extended to infinite-state partial-information games [?], and used for sensor design [?], both in the context of safety specifications. In addition to being focused on safety objectives, the refinement method in [?] is designed to provide the agent with just enough information to achieve safety, and is thus not applicable to surveillance properties whose satisfaction depends on the size of the belief sets.

## II. GAMES WITH SURVEILLANCE OBJECTIVES

We begin by defining a formal model for describing surveillance strategy synthesis problems, in the form of a two-player game between an agent and a target, in which the agent has only partial information about the target’s location.

### A. Surveillance Game Structures

We define a *surveillance game structure* to be a tuple  $G = (S, s^{\text{init}}, T, \text{vis})$ , with the following components:

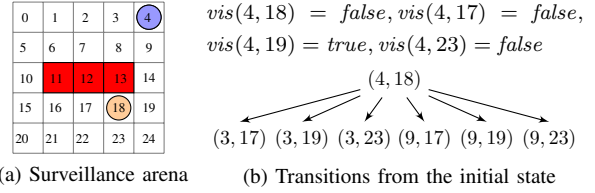


Fig. 1: A simple surveillance game on a grid arena. Obstacles are shown in red, the agent (at location 4) and the target (at location 18) are coloured in blue and orange respectively.

- $S = L_a \times L_t$  is the set of states, with  $L_a$  the set of locations of the agent, and  $L_t$  the locations of the target;
- $s^{\text{init}} = (l_a^{\text{init}}, l_t^{\text{init}})$  is the initial state;
- $T \subseteq S \times S$  is the transition relation describing the possible moves of the agent and the target; and
- $\text{vis} : S \rightarrow \mathbb{B}$  is a function that maps a state  $(l_a, l_t)$  to *true* iff position  $l_t$  is in the area of sight of  $l_a$ .

The transition relation  $T$  encodes the one-step move of both the target and the agent, where the target moves first and the agent moves second. For a state  $(l_a, l_t)$  we denote  $\text{succ}_t(l_a, l_t)$  as the set of successor locations of the target:

$$\text{succ}_t(l_a, l_t) = \{l'_t \in L_t \mid \exists l'_a. ((l_a, l_t), (l'_a, l'_t)) \in T\}.$$

We extend  $\text{succ}_t$  to sets of locations of the target by stipulating that the set  $\text{succ}_t(l_a, L)$  consists of all possible successor locations of the target for states in  $\{l_a\} \times L$ . Formally, let  $\text{succ}_t(l_a, L) = \bigcup_{l_t \in L} \text{succ}_t(l_a, l_t)$ .

For a state  $(l_a, l_t)$  and a successor location of the target  $l'_t$ , we denote with  $\text{succ}_a(l_a, l_t, l'_t)$  the set of successor locations of the agent, given that the target moves to  $l'_t$ :

$$\text{succ}_a(l_a, l_t, l'_t) = \{l'_a \in L_a \mid ((l_a, l_t), (l'_a, l'_t)) \in T\}.$$

We assume that, for every  $s \in S$ , there exists  $s' \in S$  such that  $(s, s') \in T$ , that is, from every state there is at least one move possible (this might be staying in the same state). We also assume that when the target moves to an invisible location, its position does not influence the possible one-step moves of the agent. Formally, we require that if  $\text{vis}(l_a, l_t''') = \text{vis}(l_a, l_t''''') = \text{false}$ , then  $\text{succ}_a(l_a, l_t'', l_t''''') = \text{succ}_a(l_a, l_t'', l_t''''')$  for all  $l_t'', l_t''', l_t''''', l_t'''''' \in L_t$ . This assumption is natural in the setting when the agent can move in one step only to locations that are in its sight.

*Example 1:* Figure 1 shows an example of a surveillance game on a grid. The sets of possible locations  $L_a$  and  $L_t$  for the agent and the target consist of the squares of the grid. The transition relation  $T$  encodes the possible one-step moves of both the agent and the target on the grid, and incorporates all desired constraints. For example, moving to an occupied location, or an obstacle, is not allowed. Figure 1b shows the possible transitions from the initial state  $(4, 18)$ .

The function  $\text{vis}$  encodes straight-line visibility: a location  $l_t$  is visible from a location  $l_a$  if there is no obstacle on the straight line between them. Initially the target is not in the area of sight of the agent, but the agent knows the initial position of the target. However, once the target moves to one of the locations reachable in one step, in this case, locations  $\{17, 19, 23\}$ , this might no longer be the case. More precisely, if the target moves to location 19, then the agent observes its location, but if it moves to one of the others, then the agent no longer knows its exact location. ■

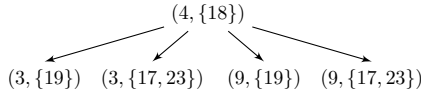


Fig. 2: Transitions from the initial state in the belief-set game from Example 2 where  $\text{vis}(4, 17) = \text{vis}(4, 23) = \text{false}$ .

### B. Belief-Set Game Structures

In surveillance strategy synthesis we need to state properties of, and reason about, the information which the agent has, i.e. its *belief* about the location of the target. To this end, we can employ a powerset construction which is commonly used to transform a partial-information game into a perfect-information one, by explicitly tracking the knowledge one player has as a set of possible states of the other player.

Given a set  $B$ , we denote with  $\mathcal{P}(B) = \{B' \mid B' \subseteq B\}$  the powerset (set of all subsets) of  $B$ .

For a surveillance game structure  $G = (S, s^{\text{init}}, T, \text{vis})$  we define the corresponding *belief-set game structure*  $G_{\text{belief}} = (S_{\text{belief}}, s_{\text{belief}}^{\text{init}}, T_{\text{belief}})$  with the following components:

- $S_{\text{belief}} = L_a \times \mathcal{P}(L_t)$  is the set of states, with  $L_a$  the set of locations of the agent, and  $\mathcal{P}(L_t)$  the set of *belief sets* describing information about the location of the target;
- $s_{\text{belief}}^{\text{init}} = (l_a^{\text{init}}, \{l_t^{\text{init}}\})$  is the initial state;
- $T_{\text{belief}} \subseteq S_{\text{belief}} \times S_{\text{belief}}$  is the transition relation where  $((l_a, B_t), (l'_a, B'_t)) \in T_{\text{belief}}$  iff  $l'_a \in \text{succ}_a(l_a, l_t, l'_t)$  for some  $l_t \in B_t$  and  $l'_t \in B'_t$  and one of these holds:
  - (1)  $B'_t = \{l'_t\}$ ,  $l'_t \in \text{succ}_t(l_a, B_t)$ ,  $\text{vis}(l_a, l'_t) = \text{true}$ ;
  - (2)  $B'_t = \{l'_t \in \text{succ}_t(l_a, B_t) \mid \text{vis}(l_a, l'_t) = \text{false}\}$ .

Condition (1) captures the successor locations of the target that can be observed from the agent's current position  $l_a$ . Condition (2) corresponds to the belief set consisting of *all possible successor locations of the target not visible from  $l_a$* .

*Example 2:* Consider the surveillance game structure from Example 1. The initial belief set is  $\{18\}$ , consisting of the target's initial position. After the first move of the target, there are two possible belief sets: the set  $\{19\}$  resulting from the move to a location in the area of sight of the agent, and  $\{17, 23\}$  consisting of the two invisible locations reachable in one step from location 18. Figure 2 shows the successor states of the initial state  $(4, \{18\})$  in  $G_{\text{belief}}$ . ■

Based on  $T_{\text{belief}}$ , we can define the functions  $\text{succ}_t : S_{\text{belief}} \rightarrow \mathcal{P}(\mathcal{P}(L_t))$  and  $\text{succ}_a : S_{\text{belief}} \times \mathcal{P}(L_t) \rightarrow \mathcal{P}(L_a)$  similarly to the corresponding functions defined for  $G$ .

A *run* in  $G_{\text{belief}}$  is an infinite sequence  $s_0, s_1, \dots$  of states in  $S_{\text{belief}}$ , where  $s_0 = s_{\text{belief}}^{\text{init}}$ ,  $(s_i, s_{i+1}) \in T_{\text{belief}}$  for all  $i$ .

A *strategy for the target* in  $G_{\text{belief}}$  is a function  $f_t : S_{\text{belief}}^+ \rightarrow \mathcal{P}(L_t)$  such that  $f_t(\pi \cdot s) = B_t$  implies  $B_t \in \text{succ}_t(s)$  for every  $\pi \in S_{\text{belief}}^*$  and  $s \in S_{\text{belief}}$ . That is, a strategy for the target suggests a move resulting in some belief set reachable from some location in the current belief.

A *strategy for the agent* in  $G_{\text{belief}}$  is a function  $f_a : S^+ \times \mathcal{P}(L_t) \rightarrow S$  such that  $f_a(\pi \cdot s, B_t) = (l'_a, B'_t)$  implies  $B'_t = B_t$  and  $l'_a \in \text{succ}_a(s, B_t)$  for every  $\pi \in S_{\text{belief}}^*$ ,  $s \in S_{\text{belief}}$  and  $B_t \in \mathcal{P}(L_t)$ . Intuitively, a strategy for the agent suggests a move based on the observed history of the play and the current belief about the target's position.

The outcome of given strategies  $f_a$  and  $f_t$  for the agent and the target in  $G_{\text{belief}}$ , denoted  $\text{outcome}(G_{\text{belief}}, f_a, f_t)$ , is a run  $s_0, s_1, \dots$  of  $G_{\text{belief}}$  such that for every  $i \geq 0$ , we have  $s_{i+1} = f_a(s_0, \dots, s_i, B_t^i)$ , where  $B_t^i = f_t(s_0, \dots, s_i)$ .

### C. Temporal Surveillance Objectives

Since the states of a belief-set game structure track the information that the agent has, we can state and interpret surveillance objectives over its runs. We now formally define the surveillance properties in which we are interested.

We consider a set of *surveillance predicates*  $\mathcal{SP} = \{p_k \mid k \in \mathbb{N}_{>0}\}$ , where for  $k \in \mathbb{N}_{>0}$  we say that a state  $(l_a, B_t)$  in the belief game structure satisfies  $p_k$  (denoted  $(l_a, B_t) \models p_k$ ) iff  $|\{l_t \in B_t \mid \text{vis}(l_a, l_t) = \text{false}\}| \leq k$ . Intuitively,  $p_k$  is satisfied by the states in the belief game structure where the size of the belief set does not exceed the threshold  $k \in \mathbb{N}_{>0}$ .

We study surveillance objectives expressed by formulas of linear temporal logic (LTL) over surveillance predicates. The LTL surveillance formulas are generated by the grammar  $\varphi := p \mid \text{true} \mid \text{false} \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \bigcirc \varphi \mid \varphi \mathcal{U} \varphi \mid \varphi \mathcal{R} \varphi$ , where  $p \in \mathcal{SP}$  is a surveillance predicate,  $\bigcirc$  is the *next* operator,  $\mathcal{U}$  is the *until* operator, and  $\mathcal{R}$  is the *release* operator. We also define the derived operators *finally*:  $\Diamond \varphi = \text{true} \mathcal{U} \varphi$  and *globally*:  $\Box \varphi = \text{false} \mathcal{R} \varphi$ .

LTL formulas are interpreted over (infinite) runs. If a run  $\rho$  satisfies an LTL formula  $\varphi$ , we write  $\rho \models \varphi$ . The formal definition of LTL semantics can be found in [?]. Here we informally explain the meaning of the formulas we use.

Of special interest will be surveillance formulas of the form  $\Box p_k$ , termed *safety surveillance objective*, and  $\Box \Diamond p_k$ , called *liveness surveillance objective*. Intuitively, the safety surveillance formula  $\Box p_k$  is satisfied if at each point in time the size of the belief set does not exceed  $k$ . The liveness surveillance objective  $\Box \Diamond p_k$ , on the other hand, requires that infinitely often this size is below or equal to  $k$ .

*Example 3:* We can specify that the agent is required to always know with certainty the location of the target as  $\Box p_1$ . A more relaxed requirement is that the agent's uncertainty never grows above 5 locations, and it infinitely often reduces this uncertainty to at most 2 locations:  $\Box p_5 \wedge \Box \Diamond p_2$ . ■

### D. Incorporating Task Specifications

We can integrate LTL objectives not related to surveillance, i.e., *task specifications*, by considering, in addition to  $\mathcal{SP}$ , a set  $\mathcal{AP}$  of atomic predicates interpreted over states of  $G$ . In order to define the semantics of  $p \in \mathcal{AP}$  over states of  $G_{\text{belief}}$ , we restrict ourselves to predicates observable by the agent. Formally, we require that for  $p \in \mathcal{AP}$ , and states  $(l_a, l'_t)$  and  $(l_a, l''_t)$  with  $\text{vis}(l_a, l'_t) = \text{vis}(l_a, l''_t) = \text{false}$  it holds that  $(l_a, l'_t) \models p$  iff  $(l_a, l''_t) \models p$ . One class of such predicates are those that depend only on the agent's position.

*Example 4:* Suppose that  $\text{at\_goal}$  is a predicate true exactly when the agent is at some designated goal location. We can then state that the agent visits the goal infinitely often while always maintaining belief uncertainty of at most 10 locations using the LTL formula  $\Box \Diamond \text{at\_goal} \wedge \Box p_{10}$ . ■

### E. Surveillance Synthesis Problem

A *surveillance game* is a pair  $(G, \varphi)$ , where  $G$  is a surveillance game structure and  $\varphi$  is a surveillance objective. A *winning strategy for the agent* for  $(G, \varphi)$  is a strategy  $f_a$  for the agent in the corresponding belief-set game structure  $G_{\text{belief}}$  such that for every strategy  $f_t$  for the target in  $G_{\text{belief}}$  it holds that  $\text{outcome}(G_{\text{belief}}, f_a, f_t) \models \varphi$ . Analogously, a *winning strategy for the target* for  $(G, \varphi)$  is a strategy  $f_t$  such that, for every strategy  $f_a$  for the agent in  $G_{\text{belief}}$ , it holds that  $\text{outcome}(G_{\text{belief}}, f_a, f_t) \not\models \varphi$ .

**Surveillance synthesis problem:** Given a surveillance game  $(G, \varphi)$ , compute a winning strategy for the agent for  $(G, \varphi)$ , or determine that such a strategy does not exist.

It is well-known that two-player perfect-information games with LTL objectives over finite-state game structures are determined, that is exactly one of the players has a winning strategy. This means that the agent does not have a winning strategy for a given surveillance game, if and only if the target has a winning strategy for this game. We refer to winning strategies of the target as *counterexamples*.

### III. BELIEF SET ABSTRACTION

We used the belief-set game structure in order to state the surveillance objective of the agent. While in principle it is possible to solve the surveillance strategy synthesis problem on this game, this is in most cases computationally infeasible, since the size of this game is exponential in the size of the original game. To circumvent this construction when possible, we propose an abstraction-based method, that given a surveillance game structure and a partition of the set of the target's locations, yields an approximation that is sound with respect to surveillance objectives for the agent.

An *abstraction partition* is a family  $\mathcal{Q} = \{Q_i\}_{i=1}^n$  of subsets of  $L_t$ ,  $Q_i \subseteq L_t$  such that the following hold:

- $\bigcup_{i=1}^n Q_i = L_t$  and  $Q_i \cap Q_j = \emptyset$  for all  $i \neq j$ ;
- For each  $p \in \mathcal{AP}$ ,  $Q \in \mathcal{Q}$  and  $l_a \in L_a$ , it holds that  $(l_a, l'_t) \models p$  iff  $(l_a, l''_t) \models p$  for every  $l'_t, l''_t \in Q$ .

Intuitively, these conditions mean that  $\mathcal{Q}$  partitions the set of locations of the target, and the concrete locations in each of the sets in  $\mathcal{Q}$  agree on the value of the propositions in  $\mathcal{AP}$ .

If  $\mathcal{Q}' = \{Q'_i\}_{i=1}^m$  is a family of subsets of  $L_t$  such that  $\bigcup_{i=1}^m Q'_i = L_t$  and for each  $Q'_i \in \mathcal{Q}'$  there exists  $Q_j \in \mathcal{Q}$  such that  $Q'_i \subseteq Q_j$ , then  $\mathcal{Q}'$  is also an abstraction partition, and we say that  $\mathcal{Q}'$  *refines*  $\mathcal{Q}$ , denoted  $\mathcal{Q}' \preceq \mathcal{Q}$ .

For  $\mathcal{Q} = \{Q_i\}_{i=1}^n$ , we define a function  $\alpha_{\mathcal{Q}} : L_t \rightarrow \mathcal{Q}$  by  $\alpha_{\mathcal{Q}}(l_t) = Q$  for the unique  $Q \in \mathcal{Q}$  with  $l_t \in Q$ . We denote also with  $\alpha_{\mathcal{Q}} : \mathcal{P}(L_t) \rightarrow \mathcal{P}(\mathcal{Q})$  the *abstraction function* defined by  $\alpha_{\mathcal{Q}}(L) = \{\alpha_{\mathcal{Q}}(l) \mid l \in L\}$ . We define a *concretization function*  $\gamma : \mathcal{P}(\mathcal{Q}) \cup L_t \rightarrow \mathcal{P}(L_t)$  such that  $\gamma(A) = \{l_t\}$  if  $A = l_t \in L_t$ , and  $\gamma(A) = \bigcup_{Q \in A} Q$  if  $A \in \mathcal{P}(\mathcal{Q})$ .

Given a surveillance game structure  $G = (S, s^{\text{init}}, T, \text{vis})$  and an abstraction partition  $\mathcal{Q} = \{Q_i\}_{i=1}^n$  of the set  $L_t$ , we define the *abstraction of  $G$  w.r.t.  $\mathcal{Q}$*  to be the game structure  $G_{\text{abstract}} = \alpha_{\mathcal{Q}}(G) = (S_{\text{abstract}}, s_{\text{abstract}}^{\text{init}}, T_{\text{abstract}})$ , where

- $S_{\text{abstract}} = (L_a \times \mathcal{P}(\mathcal{Q})) \cup (L_a \times L_t)$  is the set of *abstract states*, consisting of states approximating the belief sets in the game structure  $G_{\text{belief}}$ , as well as the states  $S$ ;

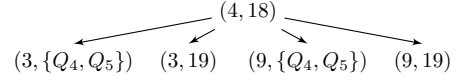


Fig. 3: Transitions from the initial state in the abstract game from Example 5 where  $\alpha_{\mathcal{Q}}(17) = Q_4$  and  $\alpha_{\mathcal{Q}}(23) = Q_5$ .

- $s_{\text{abstract}}^{\text{init}} = (l_a^{\text{init}}, l_t^{\text{init}})$  is the *initial abstract state*;
- $T_{\text{abstract}} \subseteq S_{\text{abstract}} \times S_{\text{abstract}}$  is the transition relation such that  $((l_a, A_t), (l'_a, A'_t)) \in T_{\text{abstract}}$  if and only if one of the following two conditions is satisfied:
  - (1)  $A'_t = l'_t$ ,  $l'_t \in \text{succ}_t(\gamma(A_t))$  and  $\text{vis}(l_a, l'_t) = \text{true}$ , and  $l'_a \in \text{succ}_a(l_a, l_t, l'_t)$  for some  $l_t \in \gamma(A_t)$ .
  - (2)  $A'_t = \alpha_{\mathcal{Q}}(\{l'_t \in \text{succ}_t(\gamma(A_t)) \mid \text{vis}(l_a, l'_t) = \text{false}\})$ , and  $l'_a \in \text{succ}_a(l_a, l_t, l'_t)$  for some  $l_t \in \gamma(A_t)$  and some  $l'_t \in \text{succ}_t(\gamma(A_t))$  with  $\text{vis}(l_a, l'_t) = \text{false}$ .

As for the belief-set game structure, the first condition captures the successor locations of the target, which can be observed from the agent's current location  $l_a$ . Condition (2) corresponds to the *abstract belief set* whose concretization consists of all possible successors of all positions in  $\gamma(A_t)$ , which are not visible from  $l_a$ . Since the belief abstraction overapproximates the agent's belief, that is,  $\gamma(\alpha_{\mathcal{Q}}(B)) \supseteq B$ , the next-state abstract belief  $\gamma(A'_t)$  may include positions in  $L_t$  that are not successors of positions in  $\gamma(A_t)$ .

*Example 5:* Consider again the surveillance game from Example 1, and the abstraction partition  $\mathcal{Q} = \{Q_1, \dots, Q_5\}$ , where the set  $Q_i$  corresponds to the  $i$ -th row of the grid. For location 17 of the target we have  $\alpha_{\mathcal{Q}}(17) = Q_4$ , and for 23 we have  $\alpha_{\mathcal{Q}}(23) = Q_5$ . Thus, the belief set  $B = \{17, 23\}$  is covered by the abstract belief set  $\alpha_{\mathcal{Q}}(B) = \{Q_4, Q_5\}$ . Figure 3 shows the successors of the initial state  $(4, 18)$  of the abstract belief-set game structure. The concretization of the abstract belief set  $\{Q_4, Q_5\}$  is the set  $\{15, 16, 17, 18, 19, 20, 21, 22, 23, 24\}$  of target locations. ■

An abstract state  $(l_a, A_t)$  *satisfies a surveillance predicate*  $p_k$ , denoted  $(l_a, A_t) \models p_k$ , iff  $|\{l_t \in \gamma(A_t) \mid \text{vis}(l_a, l_t) = \text{false}\}| \leq k$ . Simply, the number of states in the concretized belief set has to be less than or equal to  $k$ . Similarly, for a predicate  $p \in \mathcal{AP}$ , we define  $(l_a, A_t) \models p$  iff for every  $l_t \in \gamma(A_t)$  it holds that  $(l_a, l_t) \models p$ . With these definitions, we can interpret surveillance objectives over runs of  $G_{\text{abstract}}$ .

Strategies (and winning strategies) for the agent and the target in an abstract belief-set game  $(\alpha_{\mathcal{Q}}(G), \varphi)$  are defined analogously to strategies (and winning strategies) in  $G_{\text{belief}}$ .

In the construction of the abstract game structure, we overapproximate the belief-set of the agent at each step. Since we consider surveillance predicates that impose upper bounds on the size of the belief, such an abstraction gives more power to the target (and, dually less power to the agent). This construction guarantees that the abstraction is *sound*, meaning that an abstract strategy for the agent that achieves a surveillance objective corresponds to a winning strategy in the concrete game. This is stated in the following theorem.

**Theorem 1:** Let  $G$  be a surveillance game structure,  $\mathcal{Q} = \{Q_i\}_{i=1}^n$  be an abstraction partition, and  $G_{\text{abstract}} = \alpha_{\mathcal{Q}}(G)$ . For every surveillance objective  $\varphi$ , if there exists a winning strategy for the agent in the abstract belief-set game

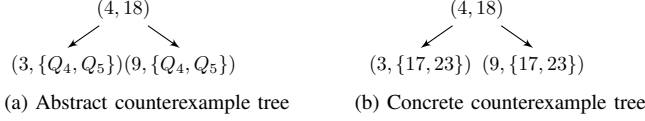


Fig. 4: Abstract and corresponding concrete counterexample trees for the surveillance game in Example 6.

$(\alpha_Q(G), \varphi)$ , then there exists a winning strategy for the agent in the concrete surveillance game  $(G, \varphi)$ .

#### IV. BELIEF REFINEMENT FOR SAFETY

##### A. Counterexample Tree

A winning strategy for the target in a game with safety surveillance objective can be represented as a tree. An *abstract counterexample tree*  $\mathcal{C}_{\text{abstract}}$  for  $(G_{\text{abstract}}, \square p_k)$  is a finite tree, whose nodes are labelled with states in  $S_{\text{abstract}}$  such that the following conditions are satisfied:

- The root node is labelled with the initial state  $s_{\text{abstract}}^{\text{init}}$ .
- A node is labelled with an abstract state which violates  $p_k$  (that is,  $s_{\text{abstract}}$  where  $s_{\text{abstract}} \not\models p_k$ ) iff it is a leaf.
- The tree branches according to all possible transition choices of the agent. Formally, if an internal node  $v$  is labelled with  $(l_a, A_t)$ , then there is unique  $A'_t$  such that:
  - (1)  $((l_a, A_t), (l'_a, A'_t)) \in T_{\text{abstract}}$  for some  $l'_a \in L_a$ , and
  - (2) for every  $l'_a \in L_a$  such that  $((l_a, A_t), (l'_a, A'_t)) \in T_{\text{abstract}}$ , there is a child  $v'$  of  $v$  labelled with  $(l'_a, A'_t)$ .

A *concrete counterexample tree*  $\mathcal{C}_{\text{belief}}$  for  $(G_{\text{belief}}, \square p_k)$  is a finite tree defined analogously to an abstract counterexample tree with nodes labelled with states in  $S_{\text{belief}}$ .

Due to the overapproximation of the belief sets, not every counterexample in the abstract game corresponds to a winning strategy for the target in the original game.

An abstract counterexample  $\mathcal{C}_{\text{abstract}}$  in  $(G_{\text{abstract}}, \square p_k)$  is *concretizable* if there exists a concrete counterexample tree  $\mathcal{C}_{\text{belief}}$  in  $(G_{\text{belief}}, \square p_k)$ , that differs from  $\mathcal{C}_{\text{abstract}}$  only in the node labels, and each node labelled with  $(l_a, A_t)$  in  $\mathcal{C}_{\text{abstract}}$  has label  $(l_a, B_t)$  in  $\mathcal{C}_{\text{belief}}$  for which  $B_t \subseteq \gamma(A_t)$ .

*Example 6:* Figure 4a shows an abstract counterexample tree  $\mathcal{C}_{\text{abstract}}$  for the game  $(\alpha_Q(G), \square p_1)$ , where  $G$  is the surveillance game structure from Example 1 and  $Q$  is the abstraction partition from Example 5. The counterexample corresponds to the choice of the target to move to one of the locations 17 or 23, which, for every possible move of the agent, results in an abstract state with abstract belief  $B = \{Q_4, Q_5\}$  violating  $p_1$ . A concrete counterexample tree  $\mathcal{C}_{\text{belief}}$  concretizing  $\mathcal{C}_{\text{abstract}}$  is shown in Figure 4b. ■

##### B. Counterexample-Guided Refinement

We now describe a procedure that determines whether an abstract counterexample for a safety surveillance objective is concretizable. This procedure essentially constructs the precise belief sets corresponding to the abstract moves of the target that constitute the abstract counterexample.

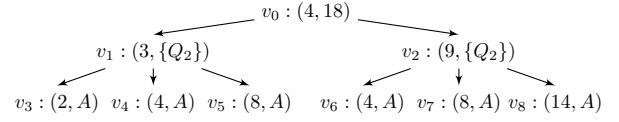


Fig. 5: Abstract counterexample in Example 7. The leaf nodes are labelled with the abstract belief set  $A = \{Q_1, Q_2\}$ .

1) *Forward belief-set propagation:* Given an abstract counterexample tree  $\mathcal{C}_{\text{abstract}}$ , we annotate its nodes with states in  $S_{\text{belief}}$  in a top-down manner as follows. The root node is labelled with  $s_{\text{belief}}^{\text{init}}$ . If  $v$  is a node annotated with the belief set  $(l_a, B_t) \in S_{\text{belief}}$ , and  $v'$  is a child of  $v$  in  $\mathcal{C}_{\text{abstract}}$  labelled with an abstract state  $(l'_a, A'_t)$ , then we annotate  $v'$  with the belief set  $(l'_a, B'_t)$ , where  $B'_t = \text{succ}_t(l_a, B_t) \cap \gamma(A'_t)$ . The counterexample analysis procedure based on this annotation is given in Algorithm 1. If each of the leaf nodes of the tree is annotated with a belief set  $(l_a, B_t)$  for which  $(l_a, B_t) \not\models p_k$ , then the new annotation gives us a concrete counterexample tree  $\mathcal{C}_{\text{belief}}$ , which by construction concretizes  $\mathcal{C}_{\text{abstract}}$ . Conversely, if there exists a leaf node annotated with  $(l_a, B_t)$  such that  $(l_a, B_t) \models p_k$ , then we can conclude that the abstract counterexample tree  $\mathcal{C}_{\text{abstract}}$  is not concretizable and use the path from the root of the tree to this leaf node to refine the partition  $Q$ .

*Theorem 2:* If Algorithm 1 returns a path  $\pi_{\text{abstract}}$  in  $\mathcal{C}_{\text{abstract}}$ , then  $\mathcal{C}_{\text{abstract}}$  is not concretizable, and  $\pi_{\text{abstract}}$  is a non-concretizable path, otherwise  $\mathcal{C}_{\text{abstract}}$  is concretizable.

*Example 7:* Let  $G$  be the surveillance game structure from Example 1, and consider the surveillance game  $(G, \square p_5)$ . Let  $Q = \{Q_1, Q_2\}$  consist of the set  $Q_1$ , corresponding to the first two columns of the grid in Figure 1a and the set  $Q_2$  containing the locations from the other three columns of the grid. Figure 5 shows a counterexample tree  $\mathcal{C}_{\text{abstract}}$  in the abstract game  $(\alpha_Q(G), \square p_5)$ . The analysis in Algorithm 1 annotates node  $v_1$  with the concrete belief set  $\{17, 23\}$ , and the leaf node  $v_3$  with the set  $B = \{16, 18, 22, 24\}$ . Thus, this counterexample tree  $\mathcal{C}_{\text{abstract}}$  is determined to be unconcretizable and the partition  $Q$  should be refined. ■

When the analysis procedure determines that an abstract counterexample tree is unconcretizable, it returns a path in the tree that corresponds to a sequence of moves ensuring that the size of the belief-set does not actually exceed the threshold, given that the target behaves in a way consistent with the abstract counterexample. Based on this path, we can

**Input:** surveillance game  $(G, \square p_k)$ ,  
 abstract counterexample tree  $\mathcal{C}_{\text{abstract}}$   
**Output:** a path  $\pi$  in  $\mathcal{C}_{\text{abstract}}$  or CONCRETIZABLE  
**while** there is a node  $v$  in  $\mathcal{C}_{\text{abstract}}$  whose children  
 are not annotated with states in  $S_{\text{belief}}$  **do**  
   let  $(l_a, B_t)$  be the state with which  $v$  is annotated;  
   **foreach** child  $v'$  of  $v$  labelled with  $(l'_a, A'_t)$  **do**  
     └ annotate  $v'$  with  $(l'_a, \text{succ}_t(l_a, B_t) \cap \gamma(A'_t))$ ;  
**if** there is a path  $\pi$  in  $\mathcal{C}_{\text{abstract}}$  from the root to a leaf  
 annotated with a state  $s_{\text{belief}}$  where  $s_{\text{belief}} \models p_k$   
**then return**  $\pi$ ; **else return** CONCRETIZABLE;

**Algorithm 1:** Analysis of abstract counterexample trees for games with safety surveillance objectives.

then refine the abstraction in order to precisely capture this information and thus eliminate this abstract counterexample.

2) *Backward partition splitting*: Let  $\pi_{\text{abstract}} = v_0, \dots, v_n$  be a path in  $\mathcal{C}_{\text{abstract}}$  where  $v_0$  is the root node and  $v_n$  is a leaf. For each node  $v_i$ , let  $(l_a^i, A_t^i)$  be the abstract state labelling  $v_i$  in  $\mathcal{C}_{\text{abstract}}$ , and let  $(l_a^i, B_t^i)$  be the belief set with which the node was annotated by the counterexample analysis procedure. We consider the case when  $(l_a^n, B_t^n) \models p_k$ , that is,  $|\{l_t \in B_t^n \mid \text{vis}(l_a, l_t) = \text{false}\}| \leq k$ . Note that since  $\mathcal{C}_{\text{abstract}}$  is a counterexample we have  $(l_a^n, A_t^n) \not\models p_k$ , and since  $k > 0$ , this means  $A_t \in \mathcal{P}(\mathcal{Q})$ .

We now describe a procedure to compute a partition  $\mathcal{Q}'$  that refines the current partition  $\mathcal{Q}$  based on the path  $\pi_{\text{abstract}}$ . Intuitively, we split the sets that appear in  $A_t^n$  in order to ensure that in the refined abstract game the corresponding abstract state satisfies the surveillance predicate  $p_k$ . We may have to also split sets appearing in abstract states on the path to  $v_n$ , as we have to ensure that earlier imprecisions on this path do not propagate, thus including more than the desired newly split sets, and leading to the same violation of  $p_k$ .

Formally, if  $A_t^n = (l_a^n, \{B_{n,1}, \dots, B_{n,m_n}\})$ , then we split some of the sets  $B_{n,1}, \dots, B_{n,m_n}$  to obtain from  $A_t^n$  a set  $A'_n = \{B'_{n,1}, \dots, B'_{n,m'_n}\}$  such that  $|\{l_t \in \gamma(C^n) \mid \text{vis}(l_a, l_t) = \text{false}\}| \leq k$ , where  $C^n = \{B'_{n,i} \in A'_n \mid B'_{n,i} \cap B_t^n \neq \emptyset\}$ .

This property intuitively means that if we consider the sets in  $A'_n$  that have non-empty intersection with  $B_t^n$ , an abstract state composed of those sets will satisfy  $p_k$ . Since  $(l_a^n, B_t^n)$  satisfies  $p_k$ , we can find a partition  $\mathcal{Q}^n \preceq \mathcal{Q}$  that guarantees this property, as shown in Algorithm 2.

What remains, in order to eliminate this counterexample, is to ensure that only these sets are reachable via the considered path, by propagating this split backwards, obtaining a sequence of partitions  $\mathcal{Q} \succeq \mathcal{Q}^n \succeq \dots \succeq \mathcal{Q}^0$  refining  $\mathcal{Q}$ .

Given  $\mathcal{Q}^{j+1}$ , we compute  $\mathcal{Q}^j$  as follows. For each  $j$ , we define a set  $C^j \subseteq \mathcal{P}(L_t)$  (for  $j = n$ , the set  $C^n$  was defined above). Suppose we have defined  $C^{j+1}$  for some  $j \geq 0$ , and  $A_t^j = (l_a^j, \{B_{j,1}, \dots, B_{j,m_j}\})$ . We split some of the sets  $B_{j,1}, \dots, B_{j,m_j}$  to obtain from  $A_t^j$  a set  $A'_j = \{B'_{j,1}, \dots, B'_{j,m'_j}\}$  where there exists  $C^j \subseteq A'_j$  with

$$\gamma(C^j) = \{l_t \in \gamma(A_t^j) \mid \text{succ}_t(l_a^j, \{l_t\}) \cap \gamma(A_t^{j+1}) \subseteq \gamma(C^{j+1})\}.$$

This means that using the new partition we can express precisely the set of states that do not lead to sets in  $A'_{j+1}$  that we are trying to avoid. The fact that an appropriate partition  $\mathcal{Q}$  can be computed, follows from the choice of the leaf node  $v_n$ . The procedure for computing the partition  $\mathcal{Q}' = \mathcal{Q}^0$  that refines  $\mathcal{Q}$  based on  $\pi_{\text{abstract}}$  is formalized in Algorithm 2.

*Example 8*: We continue with the unconcretizable abstract counterexample tree from Example 7. We illustrate the refinement procedure for the path  $v_0, v_1, v_3$ . For node  $v_3$ , we split  $Q_1$  and  $Q_2$  using the set  $B = \{16, 18, 22, 24\}$ , obtaining the sets  $Q'_1 = Q_1 \cap \{16, 18, 22, 24\} = \{16\}$ ,  $Q'_2 = Q_1 \setminus \{16\}$ ,  $Q'_3 = Q_2 \cap \{16, 18, 22\} = \{18, 22, 24\}$  and  $Q'_4 = Q_2 \setminus \{18, 22, 24\}$ . We thus obtain a new partition  $\mathcal{Q}_{v_3} \preceq \mathcal{Q}$ . In order to propagate the refinement backwards (to

ensure eliminating  $\mathcal{C}_{\text{abstract}}$ ) we compute the set of locations in  $Q_2$  from which the target can move to a location in  $Q'_2$  or  $Q'_4$  that is not visible from location 3. In this case, these are just the locations 18, 22 and 24, which have already been separated from  $Q_2$ , so here backward propagation does not require further splitting. ■

Let  $\mathcal{Q}$  and  $\mathcal{Q}'$  be two counterexample partitions such that  $\mathcal{Q}' \preceq \mathcal{Q}$ . Let  $\mathcal{C}_{\text{abstract}}$  be an abstract counterexample tree in  $(\alpha_{\mathcal{Q}}(G), \square p_k)$ . We define  $\gamma_{\mathcal{Q}'}(\mathcal{C}_{\text{abstract}})$  to be the set of abstract counterexample trees in  $(\alpha_{\mathcal{Q}'}(G), \square p_k)$  such that  $C'_{\text{abstract}} \in \gamma_{\mathcal{Q}'}(\mathcal{C}_{\text{abstract}})$  iff  $C'_{\text{abstract}}$  differs from  $\mathcal{C}_{\text{abstract}}$  only in the node labels and for every node in  $\mathcal{C}_{\text{abstract}}$  labelled with  $(l_a, A_t)$ , the corresponding node in  $C'_{\text{abstract}}$  is labelled with an abstract state  $(l_a, A'_t)$  such that  $\gamma(A'_t) \subseteq \gamma(A_t)$ .

The theorem below states the progress property (eliminating the considered counterexample) of Algorithm 2.

*Theorem 3*: If  $\mathcal{Q}'$  is the partition returned by Algorithm 2 for an unconcretizable abstract counterexample  $\mathcal{C}_{\text{abstract}}$  in  $(\alpha_{\mathcal{Q}}(G), \square p_k)$ , then  $\gamma_{\mathcal{Q}'}(\mathcal{C}_{\text{abstract}}) = \emptyset$ , and also  $\gamma_{\mathcal{Q}''}(\mathcal{C}_{\text{abstract}}) = \emptyset$  for every partition  $\mathcal{Q}''$  where  $\mathcal{Q}'' \preceq \mathcal{Q}'$ .

*Example 9*: In the surveillance game  $(G, \square p_5)$ , where  $G$  is the surveillance game structure from Example 1, the agent has a winning strategy. After 6 iterations of the refinement loop we arrive at an abstract game  $(\alpha_{\mathcal{Q}^*}(G), \square p_5)$ , where the partition  $\mathcal{Q}^*$  consists of 11 automatically computed sets (as opposed to the 22 locations reachable by the target in  $G$ ), which in terms of the belief-set construction means  $2^{11}$  versus  $2^{22}$  possible belief sets in the respective games.

In the game  $(G, \square p_2)$ , on the other hand, the agent does not have a winning strategy, and our algorithm establishes this after one refinement, after which, using a partition of size 4, it finds a concretizable abstract counterexample. ■

## V. BELIEF REFINEMENT FOR LIVENESS

### A. Counterexample Graph

The counterexamples for general surveillance properties are directed graphs, which may contain cycles. In particular, for a liveness surveillance property of the form  $\square \Diamond p_k$  each

**Input**: surveillance game  $(G, \square p_k)$ , abstraction partition  $\mathcal{Q}$ ,

unconcretizable path  $\pi = v_0, \dots, v_n$  in  $\mathcal{C}_{\text{abstract}}$

**Output**: an abstraction partition  $\mathcal{Q}'$  such that  $\mathcal{Q}' \preceq \mathcal{Q}$   
let  $(l_a^j, A_t^j)$  be the label of  $v_j$ , and  $(l_a^j, B_t^j)$  its annotation;

$$A := \{Q \cap B_t^n \mid Q \in A_t^n, Q \cap B_t^n \neq \emptyset\} \cup \{Q \setminus B_t^n \mid Q \in A_t^n, Q \setminus B_t^n \neq \emptyset\};$$

$$\mathcal{Q}' := (\mathcal{Q} \setminus A_t^n) \cup A; C := \{Q \in A \mid Q \cap B_t^n \neq \emptyset\}$$

**for**  $j = n-1, \dots, 0$  **do**

**if**  $A_t^j \in L_t$  **then break**;

$$B := \{l_t \in \gamma(A_t^j) \mid \text{succ}_t(l_a, \{l_t\}) \subseteq \gamma(C)\};$$

$$A := \{Q \cap B \mid Q \in A_t^j, Q \cap B \neq \emptyset\} \cup$$

$$\{Q \setminus B \mid Q \in A_t^j, Q \setminus B \neq \emptyset\};$$

$$\mathcal{Q}' := (\mathcal{Q}' \setminus A_t^j) \cup A; C := \{Q \in A \mid Q \cap B \neq \emptyset\}$$

**return**  $\mathcal{Q}'$

**Algorithm 2**: Abstraction partition refinement given an unconcretizable path in an abstract counterexample tree.



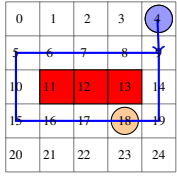


Fig. 6: Agent locations on an (infinite) path in the abstract counterexample graph from Example 10. In the graph, the first node is labelled with  $(4, 18)$ , the second with  $(9, \{Q_2\})$ , and all other nodes with some  $(l_a, \{Q_1, Q_2\})$ .

infinite path in the graph has a position such that, from this position on, each state on the path violates  $p_k$ . An *abstract counterexample graph* in the game  $(G_{\text{abstract}}, \square \Diamond p_k)$  is a finite graph  $\mathcal{C}_{\text{abstract}}$  defined analogously to the abstract counterexample tree. The difference being that there are no leaves, and that for each cycle  $\rho = v_1, v_2, \dots, v_n$  with  $v_1 = v_n$  in  $\mathcal{C}_{\text{abstract}}$  that is reachable from  $v_0$ , every node  $v_i$  in  $\rho$  is labelled with state  $s_{\text{abstract}}^i$  where  $s_{\text{abstract}}^i \not\models p_k$ .

*Example 10:* We saw in Example 9 that in the safety surveillance game  $(G, \square \Diamond p_2)$  the agent does not have a winning strategy. We now consider a relaxed requirement, namely, that the uncertainty drops to at most 2 infinitely often. We consider the liveness surveillance game  $(G, \square \Diamond p_2)$ .

Let  $\mathcal{Q} = \{Q_1, Q_2\}$  be the partition from Example 7. Figure 6 shows an infinite path (in lasso form) in the abstract game  $(\alpha_{\mathcal{Q}}(G), \square \Diamond p_2)$ . The figure depicts only the corresponding trajectory (sequence of positions) of the agent. The initial abstract state is  $(4, 18)$ , the second node on the path is labeled with the abstract state  $(9, \{Q_2\})$ , and all other nodes on the path are labeled with abstract states of the form  $(l_a, \{Q_1, Q_2\})$ . As each abstract state in the cycle violates  $p_2$ , the path violates  $\square \Diamond p_2$ . The same holds for all infinite paths in the existing abstract counterexample graph. ■

A *concrete counterexample graph*  $\mathcal{C}_{\text{belief}}$  for the belief game  $(G_{\text{belief}}, \square \Diamond p_k)$  is defined analogously.

An abstract counterexample graph  $\mathcal{C}_{\text{abstract}}$  for the game  $(G_{\text{abstract}}, \square \Diamond p_k)$  is *concretizable* if there exists a counterexample  $\mathcal{C}_{\text{belief}}$  in  $(G_{\text{belief}}, \square \Diamond p_k)$ , such that for each infinite path  $\pi_{\text{abstract}} = v_{\text{abstract}}^0, v_{\text{abstract}}^1, \dots$  starting from the initial node of  $\mathcal{C}_{\text{abstract}}$  there exists an infinite path  $\pi_{\text{belief}} = v_{\text{belief}}^0, v_{\text{belief}}^1, \dots$  in  $\mathcal{C}_{\text{belief}}$  starting from its initial node such that if  $v_{\text{abstract}}^i$  is labelled with  $(l_a, A_t)$  in  $\mathcal{C}_{\text{abstract}}$ , then the corresponding node  $v_{\text{belief}}^i$  in  $\mathcal{C}_{\text{belief}}$  is labelled with  $(l_a, B_t)$  for some  $B_t \in \mathcal{P}(L_t)$  for which  $B_t \subseteq \gamma(A_t)$ .

## B. Counterexample-Guided Refinement

*1) Forward belief-set propagation:* To check if an abstract counterexample graph  $\mathcal{C}_{\text{abstract}}$  is concretizable, we construct a finite graph  $\mathcal{D}$  whose nodes are labelled with elements of  $S_{\text{belief}}$  and with nodes of  $\mathcal{C}_{\text{abstract}}$ . By construction we will ensure that if a node  $d$  in  $\mathcal{D}$  is labelled with  $\langle (l_a, B_t), v \rangle$ , where  $(l_a, B_t)$  is a belief state, and  $v$  is a node in  $\mathcal{C}_{\text{abstract}}$ , then  $v$  is labelled with  $(l_a, A_t)$  in  $\mathcal{C}_{\text{abstract}}$ , and  $B_t \subseteq \gamma(A_t)$ .

Initially  $\mathcal{D}$  contains a single node  $d_0$  labelled with  $\langle s_{\text{belief}}^{\text{init}}, v_0 \rangle$ , where  $v_0$  is initial node of  $\mathcal{C}_{\text{abstract}}$ . Consider a node  $d$  in  $\mathcal{D}$  labelled with  $\langle (l_a, B_t), v \rangle$ . For every child  $v'$  of  $v$  in  $\mathcal{C}_{\text{abstract}}$ , labelled with an abstract state  $(l'_a, A'_t)$  we proceed as follows. We let  $B'_t = \text{succ}_t(l_a, B_t) \cap \gamma(A'_t)$ . If there exists a node  $d'$  in  $\mathcal{D}$  labelled with  $\langle (l'_a, B'_t), v' \rangle$ , then we add an edge from  $d$  to  $d'$  in  $\mathcal{D}$ . Otherwise, we create such a node and add the edge. We continue until no more nodes

and edges can be added to  $\mathcal{D}$ . The procedure is guaranteed to terminate, since both the graph  $\mathcal{C}_{\text{belief}}$ , and  $S_{\text{belief}}$  are finite, and we add a node labelled  $\langle s_{\text{belief}}, v \rangle$  to  $\mathcal{D}$  at most once.

If the graph  $\mathcal{D}$  contains a reachable cycle (it suffices to consider simple cycles, i.e., without repeating intermediate nodes)  $\rho = d_0, \dots, d_n$  with  $d_0 = d_n$  such that some  $d_i$  is labelled with  $(l_a, B_t)$  where  $(l_a, B_t) \models p_k$ , then we conclude that the abstract counterexample  $\mathcal{C}_{\text{abstract}}$  is not concretizable. If no such cycle exists, then  $\mathcal{D}$  is a concrete counterexample graph for the belief game  $(G_{\text{belief}}, \square \Diamond p_k)$ .

*Example 11:* The abstract counterexample graph in the game  $(\alpha_{\mathcal{Q}}(G), \square \Diamond p_2)$  discussed in Example 10 is not concretizable, since for the path in the abstract graph depicted in Figure 6 there exists a corresponding path in the graph  $\mathcal{D}$  with a node in the cycle labelled with a set in  $G_{\text{belief}}$  that satisfies  $p_2$ . More precisely, the cycle in the graph  $\mathcal{D}$  contains a node labelled with  $(19, \{10\})$ . Intuitively, as the agent moves from the upper to the lower part of the grid along this path, upon not observing the target, it can infer from the sequence of observations that the only possible location of the target is 10. Thus, this path is winning for the agent. ■

*Theorem 4:* If Algorithm 3 returns a path  $\pi$  in the graph  $\mathcal{D}$  constructed for  $\mathcal{C}_{\text{abstract}}$ , then  $\mathcal{C}_{\text{abstract}}$  is not concretizable, and the infinite run in  $G_{\text{belief}}$  corresponding to  $\pi$  satisfies  $\square \Diamond p_k$ , otherwise  $\mathcal{C}_{\text{abstract}}$  is concretizable.

*2) Backward partition splitting:* Consider a path in the graph  $\mathcal{D}$  of the form  $\pi = d_0, \dots, d_n, d'_0, \dots, d'_m$  where  $d_n = d'_m$ , and where for some  $0 \leq i \leq m$  for the label  $(l'_a, B'_t)$  it holds that  $(l'_a, B'_t) \models p_k$ . Let  $\pi_{\text{abstract}} = v_0, \dots, v_n, v'_0, \dots, v'_m$  be the sequence of nodes in  $\mathcal{C}_{\text{abstract}}$  corresponding to the labels in  $\pi$ . By construction of  $\mathcal{D}$ ,  $\pi_{\text{abstract}}$  is a path in  $\mathcal{C}_{\text{abstract}}$  and  $v_n = v'_m$ . We apply the refinement procedure from the previous section to the whole

**Input:** surveillance game  $(G, \square \Diamond p_k)$ , abstract counterexample graph  $\mathcal{C}_{\text{abstract}}$  with initial node  $v_0$   
**Output:** a path  $\pi$  in a graph  $\mathcal{D}$  or CONCRETIZABLE  
graph  $\mathcal{D} = (D, E)$  with nodes  $D := \{d_0\}$  and edges  $E := \emptyset$ ;  
annotate  $d_0$  with  $\langle s_{\text{belief}}^{\text{init}}, v_0 \rangle$ ;

```

do
   $\mathcal{D}' := \mathcal{D}$ ;
  foreach node  $d$  in  $\mathcal{D}$  labelled with  $\langle (l_a, B_t), v \rangle$  do
    foreach child  $v'$  of  $v$  in  $\mathcal{C}_{\text{abstract}}$  labelled  $(l'_a, A'_t)$ 
      do
         $B'_t := \text{succ}_t(l_a, B_t) \cap \gamma(A'_t)$ ;
        if there is a node  $d'$  in  $\mathcal{D}$  labelled with
           $\langle (l'_a, B'_t), v' \rangle$  then
          | add an edge  $(d, d')$  to  $E$ 
        else
          | add a node  $d'$  labelled  $\langle (l'_a, B'_t), v' \rangle$  to  $D$ ;
          | add an edge  $(d, d')$  to  $E$ 
  while  $\mathcal{D} \neq \mathcal{D}'$ ;
  if there is a lasso path  $\pi$  in  $\mathcal{D}$  starting from  $d_0$  such that
    some node in the cycle is annotated with  $\langle s_{\text{belief}}, v \rangle$  and
     $s_{\text{belief}} \models p_k$ 
  then return  $\pi$ ; else return CONCRETIZABLE;
```

**Algorithm 3:** Analysis of abstract counterexample graphs for games with liveness surveillance objectives.

path  $\pi_{\text{abstract}}$ , as well as to the path-prefix  $v_0, \dots, v_n$ .

Let  $\mathcal{Q}$  and  $\mathcal{Q}'$  be two counterexample partitions such that  $\mathcal{Q}' \preceq \mathcal{Q}$ . Let  $\mathcal{C}_{\text{abstract}}$  be an abstract counterexample graph in  $(\alpha_{\mathcal{Q}}(G), \square \Diamond p_k)$ . We define  $\gamma_{\mathcal{Q}'}(\mathcal{C}_{\text{abstract}})$  to be the set of abstract counterexample graphs in  $(\alpha_{\mathcal{Q}'}(G), \square \Diamond p_k)$  such that for every infinite path  $\pi$  in  $\mathcal{C}'_{\text{abstract}}$  there exists an infinite path  $\pi'$  in  $\mathcal{C}_{\text{abstract}}$  such that for every node in  $\pi'$  labelled with  $(l_a, A'_t)$  the corresponding node in  $\mathcal{C}_{\text{abstract}}$  is labelled with an abstract state  $(l_a, A_t)$  such that  $\gamma(A'_t) \subseteq \gamma(A_t)$ .

*Theorem 5:* If  $\mathcal{Q}'$  is the partition obtained by refining  $\mathcal{Q}$  with respect to an uncretizable abstract counterexample  $\mathcal{C}_{\text{abstract}}$  in  $(\alpha_{\mathcal{Q}}(G), \square \Diamond p_k)$ , then  $\gamma_{\mathcal{Q}'}(\mathcal{C}_{\text{abstract}}) = \emptyset$ , and also  $\gamma_{\mathcal{Q}''}(\mathcal{C}_{\text{abstract}}) = \emptyset$  for every partition  $\mathcal{Q}''$  with  $\mathcal{Q}'' \preceq \mathcal{Q}'$ .

*Example 12:* We refine the abstraction partition  $\mathcal{Q}$  from Example 6 using the path identified there, in order to eliminate the abstract counterexample. For this, following the refinement algorithm, we first split the set  $Q_1$  into sets  $Q'_1 = \{10\}$  and  $Q'_2 = Q_1 \setminus \{10\}$ , and let  $Q'_3 = Q_2$ . However, since from some locations in  $Q'_2$  and in  $Q'_3$  the target can reach locations in  $Q'_2$  and  $Q'_3$  that are not visible from the agent's position 19, in order to eliminate the counterexample, we need to propagate the refinement backwards along the path and split  $Q'_2$  and  $Q'_3$  further. With that, we obtain an abstraction partition with 10 sets, which is guaranteed to eliminate this abstract counterexample. In fact, in this example this abstraction turns out to be sufficiently precise to obtain a winning strategy for the agent. ■

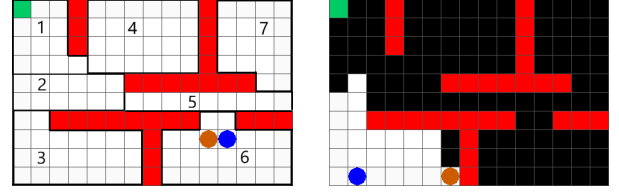
### C. General surveillance and task specifications

We have described refinement procedures for safety and liveness surveillance objectives. If we are given a conjunction of such objectives, we first apply the refinement procedure for safety, and if no path for which we can refine is found, we then apply the refinement procedure for liveness.

In the general case, we check if the counterexample contains a state for which the concrete belief is a strict subset of the abstract one. If this is not the case, then the counterexample is concretizable, otherwise we refine the abstraction to make this belief precise. In the special case when we have a conjunction of a surveillance and task specifications, we first refine with respect to the surveillance objective as described above, and if this is not possible, with respect to such a node. Since the set of states in the game is finite, the iterative refinement will terminate, either with a concretizable counterexample, or with a surveillance strategy.

## VI. EXPERIMENTAL EVALUATION

We report on the application of our method for surveillance synthesis in two case studies. We have implemented the simulation in Python, using the `slugs` reactive synthesis tool [?]. The experiments were performed on an Intel i5-5300U 2.30 GHz CPU with 8 GB of RAM. In both cases, the target is being controlled by a human while the agent responds using the synthesized surveillance strategy.



(a) Gridworld with a user provided abstraction partition with 7 sets, marked by black lines.. (b) Gridworld showing visibility of the agent. All locations shown in black are invisible to the agent.

Fig. 7: 10x15 gridworld with a surveillance liveness specification. The agent is blue, and the target to be surveilled is orange. Red states are obstacles.

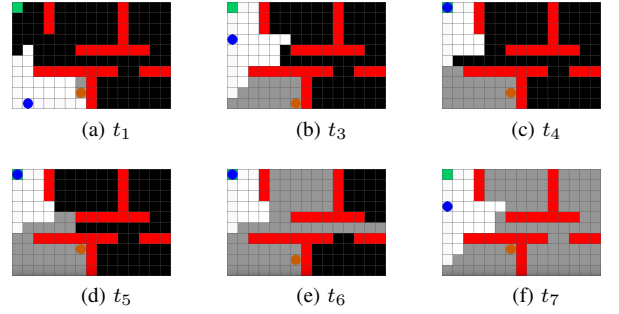


Fig. 8: Evolution of the agent's belief about the target's location as it moves to the goal and loses sight of the target. Grey cells represent the locations the agent believes the target could be in. We show the belief at different timesteps  $t_1, \dots, t_7$  (note that  $t_2$  is excluded for space concerns)

### A. Liveness Surveillance Specification + Task Specification

Figure 7a shows a gridworld divided into regions. The surveillance objective requires the agent to infinitely often know precisely the location of the target (either see it, or have a belief consisting of one cell). Additionally, it has to perform the task of patrolling (visiting infinitely often) the green 'goal' cell. Formally, the specification is  $\square \Diamond p_1 \wedge \square \Diamond goal$ . The agent can move up to 3 grid cells away at each step. The sensor mode, that is, the visibility function, used here is 'line-of-sight' with a range of 5 cells. The agent cannot see through obstacles (shown in red) and cannot see farther than 5 cells away.

Using the abstraction partition of size 7 shown in Figure 7a, the overall number of states in the two-player game is  $15 \times 10 + 2^7 = 278$  states. In contrast, solving the full abstract game will have in the order of  $2^{150}$  states, which is a state-space size that state-of-the-art synthesis tools cannot handle.

Figure 8 shows how the belief of the agent (shown in grey) can grow quickly when it cannot see the target. This growth occurs due to the coarseness of the abstraction, which overapproximates the target's true position. In 7 steps, the agent believes the target can be anywhere in the grid that is not in its vision. It has to then find the target in order to satisfy the surveillance requirement. Figure 9 illustrates the searching behaviour of the agent when it is trying to lower



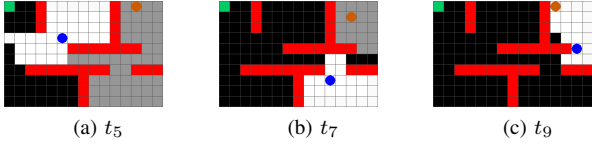


Fig. 9: The agent has to search for the target in order to lower its belief below the surveillance liveness specification.

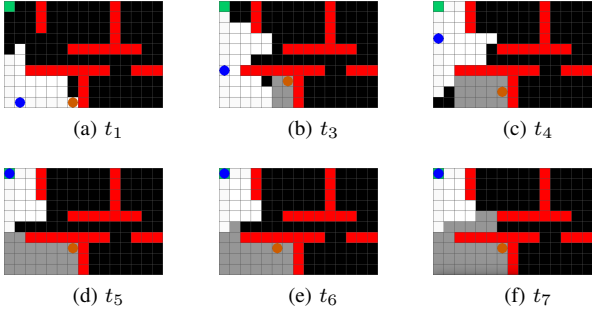


Fig. 10: Evolution of the agent's belief about the target's location in a game with an abstraction partition of size 12.

the belief below the threshold in order to satisfy the liveness specification. The behaviour of the agent shown here will contrast with the behaviour under safety surveillance which will we look at next.

In this example, an abstraction partition of size 7 was enough to guarantee the satisfaction surveillance specification. For the purpose of comparison, we also solve the game with an abstraction partition of size 12 to illustrate the change in belief growth. Figure 10 shows the belief states growing much more slowly as the abstract belief states are smaller, and thus they more closely approximate the true belief of the agent.

The additional abstraction partitions result in a much larger game as the state space grows exponentially in the size of the abstraction partition. Table I compares the sizes of the corresponding abstract games, and the time it takes to synthesize a surveillance controller in each case.

Size of abstraction partition	Size of abstract game	Synthesis time
7	278	237s
12	4346	810s

TABLE I: Comparison of synthesis times for the two cases

A video simulation can be found at <http://goo.gl/YkFuxr>.

### B. Safety surveillance specification + task specification

Figure 11 depicts an environment created in *Gazebo* where the red blocks model buildings. The drone is given full line of sight vision - it can detect the target if there is no obstacle in the way. In this setting, we enforce the safety surveillance objective  $\Box p_{30}$  (the belief size should never exceed 30) in addition to infinitely often reaching the green cell. The formal specification is  $\Box \Diamond p_{30} \wedge \Box \Diamond goal$ . Additionally, the

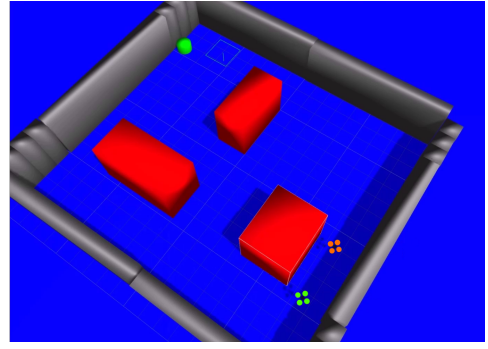


Fig. 11: A Gazebo environment where the red blocks are obstacles that the drones cannot see past. The green drone is the agent and the orange drone is the target.

target itself is trying to reach the goal cell infinitely often as well, which is known to the agent.

We used an abstraction generated by a partition of size 6, which was sufficiently precise to compute a surveillance strategy in 210 s. Again, note that the precise belief-set game would have in the order of  $2^{200}$  states.

We simulated the environment and the synthesized surveillance strategy for the agent in Gazebo and ROS. A video of the simulation can be found at <http://goo.gl/LyC1gQ>. This simulation presents a qualitative difference in behaviour compared to the previous example. There, in the case of liveness surveillance, the agent had more leeway to completely lose the target in order to reach its goal location, even though the requirement of reducing the size of the belief to 1 is quite strict. Here, on the other hand, the safety surveillance objective, even with a large threshold of 30, forces the agent to follow the target more closely, in order to prevent its belief from getting too large. The synthesis algorithm thus provides the ability to obtain qualitatively different behaviour as necessary for specific applications by combining different objectives.

### C. Discussion

The difference in the behaviour in the case studies highlights the different use cases of the surveillance objectives. Depending on the domain, the user can specify a combination of safety and liveness specification to tune the behaviour of the agent. In a critical surveillance situation (typical in defense or security situations), the safety specification will guarantee to the user that the belief will never grow too large. However, in less critical situations (such as luggage carrying robots in airports), the robot has more flexibility in allowing the belief to grow as long as it can guarantee its reduction in the future.

## VII. CONCLUSIONS

We have presented a novel approach to solving a surveillance problem with information guarantees. We provided a framework that enables the formalization of the surveillance synthesis problem as a two-player, partial-information game. We then presented a method to reason over the belief that the agent has over the target's location and specify formal

surveillance requirements. The user can tailor the behaviour to their specific application by using a combination of safety and liveness surveillance objectives.

The benefit of the proposed framework is that it allows it leverages techniques successfully used in verification and reactive synthesis to develop efficient methods for solving the surveillance problem. There are several promising avenues of future work using and extending this framework. Some of which currently being explored are the following;

- Synthesizing distributed strategies for multi-agent surveillance in a decentralized manner. These compositional synthesis methods avoid the blow up of the state space that occurs in centralized synthesis procedures as the number of surveillance agents grow.
- Incorporating static sensors or alarm triggers for the mobile agent(s) to coordinate with.
- Allowing for sensor models to include uncertainty and detection errors while still providing surveillance guarantees.

**Acknowledgement:** This work was supported in part by grant Sandia National Lab 801KOB, grant ARO W911NF-15-1-0592, and grant DARPA W911NF-16-1-0001.