Synthesis of Surveillance Strategies for Mobile Sensors

Rayna Dimitrova

University of Leicester

joint work with

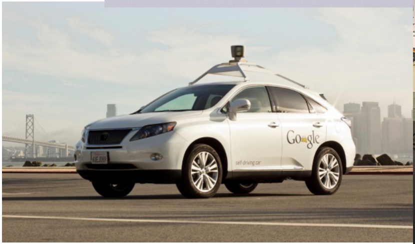
Suda Bharadwaj and Ufuk Topcu

University of Texas at Austin

S-REPLS 10

18th September 2018

Autonomous systems:
challenges and opportunities for formal methods

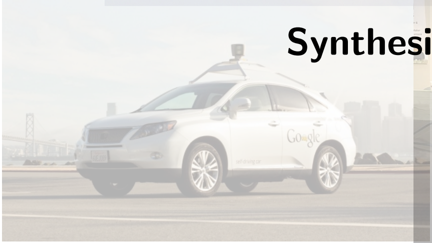


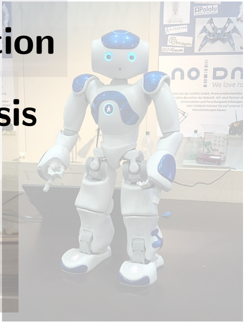
Autonomous systems: challenges and opportunities for formal methods

Specification

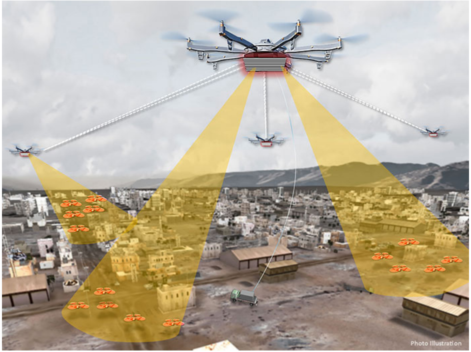
Verification

Synthesis





Reactive surveillance with mobile sensors



Goal: maintain knowledge of the location of a moving target

Example objectives

- always know (up to some precision) the location of the target
- eventually discover the target every time it gets out of sight

Reactive surveillance with mobile sensors

Specification φ: formulate surveillance objectives using LTL

Synthesis: solve a two player game between agent and target

agent (mobile sensor)
tries to satisfy φ

target
tries to violate φ

Compute a strategy for the agent to enforce φ.

Reactive surveillance with mobile sensors

Specification φ: formulate surveillance objectives using LTL

- introduce **surveillance predicates**

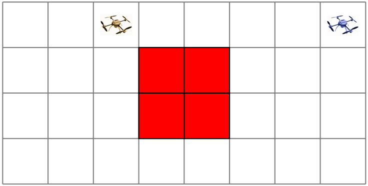
Synthesis: solve a two player game between agent and target

- tracking agent's **knowledge**
- handling **multiple sensors**

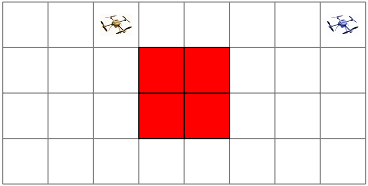
"Synthesis of Surveillance Strategies via Belief Abstraction"
S. Bharadwaj, **R. D.**,U. Topcu, CDC 2018

"Distributed Synthesis of Surveillance Strategies for Mobile Sensors"
S. Bharadwaj, **R. D.**,U. Topcu, CDC 2018

Surveillance game structures

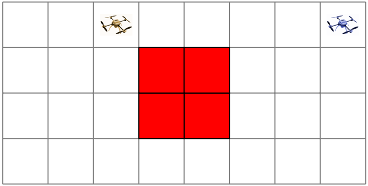


Surveillance game structures



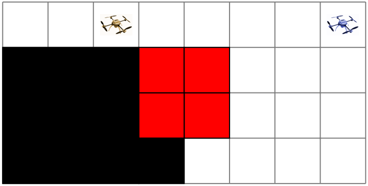
- set of locations L

Surveillance game structures



- set of locations L
- states $(l_a, l_t) \in L \times L$
  l_a: location of agent
  l_t: location of target

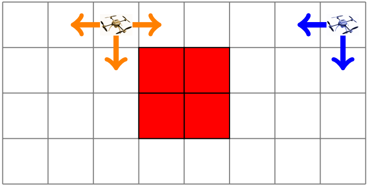
Surveillance game structures



- set of locations L
- states $(l_a, l_t) \in L \times L$
  l_a: location of agent
  l_t: location of target
- visibility $vis : L \times L \to \mathbb{B}$

visibility: $vis(l_a, l_t) = true$ iff l_t is in the line of sight of l_a

Surveillance game structures

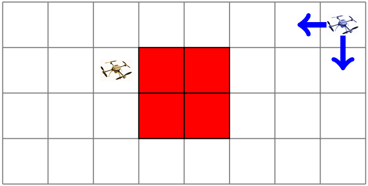


- set of locations L
- states $(l_a, l_t) \in L \times L$
  l_a: location of agent
  l_t: location of target
- visibility $vis : L \times L \to \mathbb{B}$
- transitions T, $(l_a, l_t) \rightsquigarrow (l'_a, l'_t)$

visibility: $vis(l_a, l_t) = true$ iff l_t is in the line of sight of l_a

transitions: move of target, followed by move of agent

Surveillance game structures

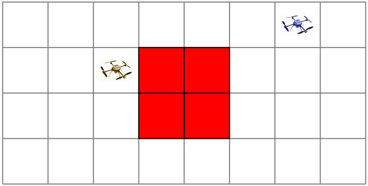


- set of locations L
- states $(l_a, l_t) \in L \times L$
  l_a: location of agent
  l_t: location of target
- visibility $vis : L \times L \to \mathbb{B}$
- transitions T, $(l_a, l_t) \rightsquigarrow (l'_a, l'_t)$

visibility: $vis(l_a, l_t) = true$ iff l_t is in the line of sight of l_a

transitions: move of target, followed by move of agent

Surveillance game structures



- set of locations L
- states $(l_a, l_t) \in L \times L$
  l_a: location of agent
  l_t: location of target
- visibility $vis : L \times L \to \mathbb{B}$
- transitions T, $(l_a, l_t) \rightsquigarrow (l'_a, l'_t)$

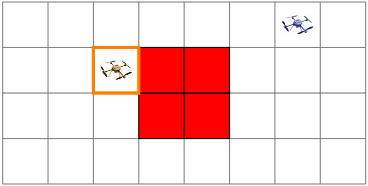
visibility: $vis(l_a, l_t) = true$ iff l_t is in the line of sight of l_a

transitions: move of target, followed by move of agent

Surveillance objectives

Belief game structure

belief: knowledge about the possible current locations of target

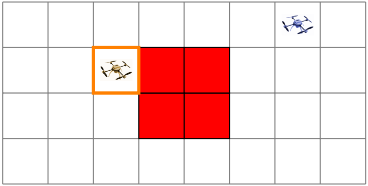


- set of beliefs 2^L
- belief states $(l_a, B_t) \in L \times 2^L$

Surveillance objectives

Belief game structure

belief: knowledge about the possible current locations of target



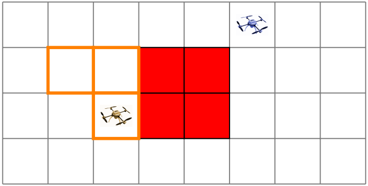
- set of beliefs 2^L
- belief states $(l_a, B_t) \in L \times 2^L$
- belief transitions
  $(l_a, B_t) \rightsquigarrow (l'_a, B'_t)$

belief transitions track the evolution of the agent's belief

Surveillance objectives

Belief game structure

belief: knowledge about the possible current locations of target



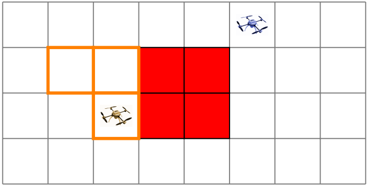
- set of beliefs 2^L
- belief states $(l_a, B_t) \in L \times 2^L$
- belief transitions $(l_a, B_t) \rightsquigarrow (l'_a, B'_t)$

belief transitions track the evolution of the agent's belief

Surveillance objectives

Belief game structure

belief: knowledge about the possible current locations of target



- set of beliefs 2^L
- belief states $(l_a, B_t) \in L \times 2^L$
- belief transitions $(l_a, B_t) \rightsquigarrow (l'_a, B'_t)$

belief transitions track the evolution of the agent's belief

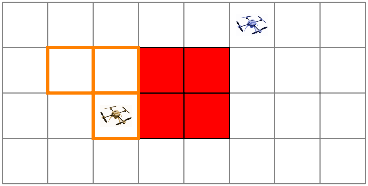
Specification

belief predicate $p_{\leq b}$, for $b \in \mathbb{N}_{>0}$: $(l_a, B_t) \models p_{\leq b}$ iff $|B_t| \leq b$

Surveillance objectives

Belief game structure

belief: knowledge about the possible current locations of target



- set of beliefs 2^L
- belief states $(l_a, B_t) \in L \times 2^L$
- belief transitions $(l_a, B_t) \rightsquigarrow (l'_a, B'_t)$

belief transitions track the evolution of the agent's belief

Specification

belief predicate $p_{\leq b}$, for $b \in \mathbb{N}_{>0}$: $(l_a, B_t) \models p_{\leq b}$ iff $|B_t| \leq b$

LTL surveillance formulas: LTL with belief predicates. Examples:

- **safety surveillance** $\Box p_{\leq b}$: "always" $p_{\leq b}$
- **liveness surveillance** $\Box\Diamond p_{\leq b}$: "infinitely often" $p_{\leq b}$

Surveillance games and strategies

surveillance game (G, φ), where

- $G = (L, vis, T)$ is a surveillance game structure,
- φ is a surveillance specification

strategy for the agent: function that maps sequences of belief states to moves that agree with T

A strategy for the agent is **winning** in (G, φ) if each sequence of belief states resulting from this strategy satisfies the specification φ.

Synthesis of surveillance strategies

Surveillance synthesis problem

Given: surveillance game (G, φ)

Compute: strategy for the agent wining in (G, φ)

A possible approach:

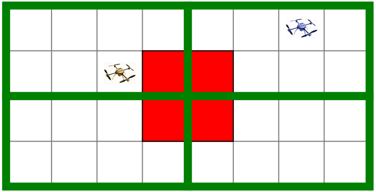
Solve game with LTL objective over belief game structure

Problem:

Size of belief game structure can be exponential in $|L|$

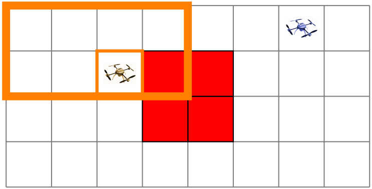
$\Rightarrow$ **Use abstraction!**

Belief abstraction



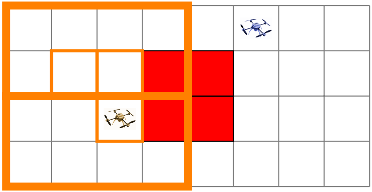
- $\mathcal{Q} = \{Q_i\}_{i=1}^{n}$ partition L
- abstract beliefs $2^{\mathcal{Q}}$

Belief abstraction



- $\mathcal{Q} = \{Q_i\}_{i=1}^n$ partition L
- abstract beliefs $2^{\mathcal{Q}}$
- abstract belief states $(l_a, A_t) \in L \times (2^{\mathcal{Q}} \cup L)$

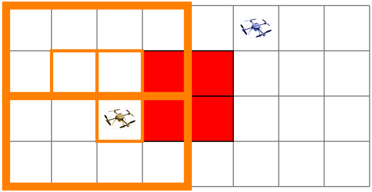
Belief abstraction



- $\mathcal{Q} = \{Q_i\}_{i=1}^{n}$ partition L
- abstract beliefs $2^{\mathcal{Q}}$
- abstract belief states $(l_a, A_t) \in L \times (2^{\mathcal{Q}} \cup L)$
- abstract belief transitions $(l_a, A_t) \rightsquigarrow (l'_a, A'_t)$

abstract belief transition: overapproximate belief at each step

Belief abstraction

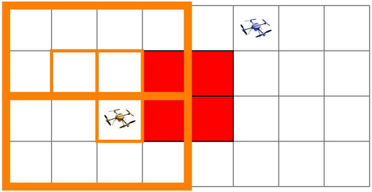


- $\mathcal{Q} = \{Q_i\}_{i=1}^{n}$ partition L
- abstract beliefs $2^{\mathcal{Q}}$
- abstract belief states $(l_a, A_t) \in L \times (2^{\mathcal{Q}} \cup L)$
- abstract belief transitions $(l_a, A_t) \rightsquigarrow (l'_a, A'_t)$

abstract belief transition: overapproximate belief at each step

Belief abstraction is sound for surveillance objectives.

Belief abstraction



- $\mathcal{Q} = \{Q_i\}_{i=1}^{n}$ partition L
- abstract beliefs $2^{\mathcal{Q}}$
- abstract belief states $(l_a, A_t) \in L \times (2^{\mathcal{Q}} \cup L)$
- abstract belief transitions $(l_a, A_t) \rightsquigarrow (l'_a, A'_t)$

abstract belief transition: overapproximate belief at each step

Belief abstraction is sound for surveillance objectives.

Worst case abstraction: each Q_i is singleton.

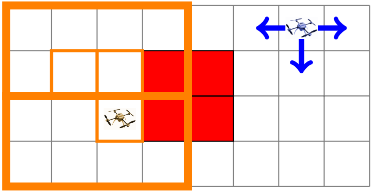
Abstraction-based synthesis of surveillance strategies

Abstract surveillance game: two-player game with LTL objective
$\Rightarrow$ use methods for synthesis of reactive systems

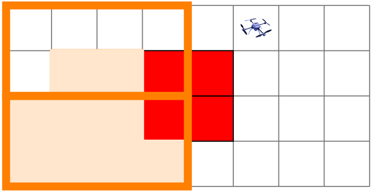
Restrict surveillance objectives to the efficient fragment GR(1)
$\Rightarrow$ use `slugs` [Ehlerers and Raman 2016]

Winning abstract strategy for agent $\mapsto$ surveillance strategy

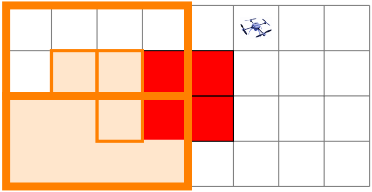
Abstract counterexamples



Abstract counterexamples

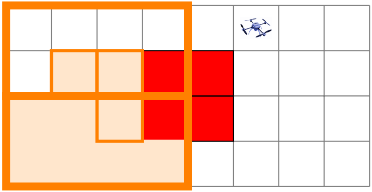


Abstract counterexamples



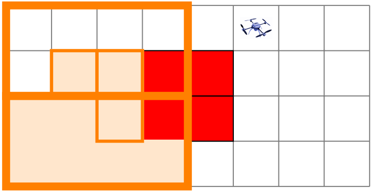
- specification $\Box p_{\leq 2}$
  $\Rightarrow$ concretizable

Abstract counterexamples



- specification $\Box p_{\leq 2}$
  $\Rightarrow$ concretizable
- specification $\Box p_{\leq 5}$
  $\Rightarrow$ spurious

Abstract counterexamples

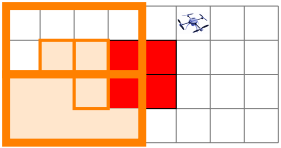


- specification $\Box p_{\leq 2}$
  $\Rightarrow$ concretizable
- specification $\Box p_{\leq 5}$
  $\Rightarrow$ spurious

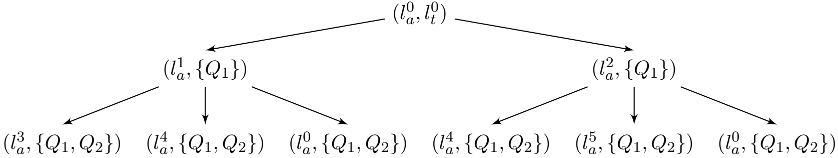
Analyse counterexample by computing concrete beliefs.

Determine which partitions to split, to refine the belief abstraction.

Counterexample-based belief refinement

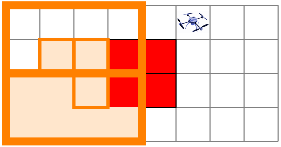


abstract counterexample for the surveillance specification $\Box p_{\leq 5}$



Annotate nodes of the tree with concrete belief sets.
Check if there is a leaf node where the bound is not exceeded.
If yes, then the counterexample is spurious. Refine to eliminate it.

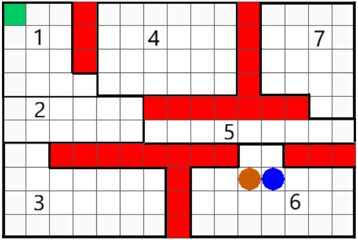
Counterexample-based belief refinement



Counterexamples for general surveillance properties are finite graphs.

- For a liveness property $\Box\Diamond p_{\leq b}$, check if there is a lasso path with a concrete belief in the loop with size not exceeding b.
- For general properties: refine some node with imprecise belief.

Example with liveness surveillance objective



specification

$\Box\Diamond p_{\leq 1} \wedge \Box\Diamond goal$

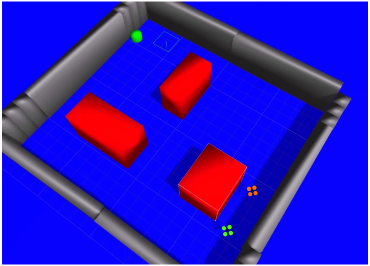
mobile sensor

straight-line visibility up to 5 cells

Number of abstract belief sets $15 \cdot 10 + 2^7$

Number of concrete belief sets 2^{150}

Example with safety surveillance objective



specification

$\Box p_{\leq 30} \wedge \Box \Diamond goal$

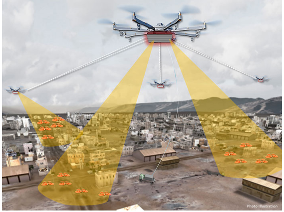
mobile sensor

unbounded straight-line visibility

Number of abstract belief sets $13 \cdot 18 + 2^6$

Number of concrete belief sets $\approx 2^{234}$

Multiple sensors

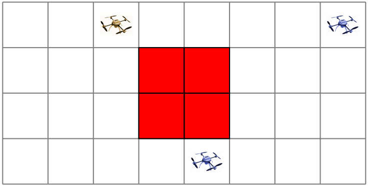


In practice: multiple sensors

+ better coverage, smaller abstractions should suffice

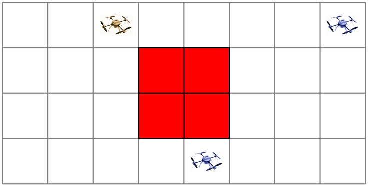
− the size of the state space of the concrete game increases

Multi-agent surveillance game structures



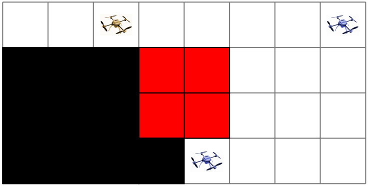
- set of locations L

Multi-agent surveillance game structures



- set of locations L
- states $(l_a^1, \ldots, l_a^m, l_t)$

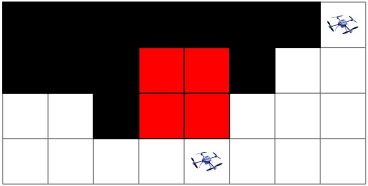
Multi-agent surveillance game structures



- set of locations L
- states $(l_a^1, \ldots, l_a^m, l_t)$
- visibility $vis_i : L \times L \to \mathbb{B}$

visibility: $vis_i(l_a^i, l_t) = true$ iff l_t is in the line of sight of l_i

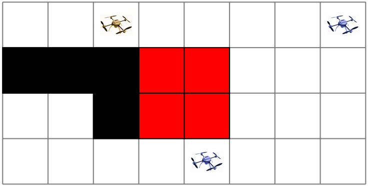
Multi-agent surveillance game structures



- set of locations L
- states $(l_a^1, \ldots, l_a^m, l_t)$
- visibility $vis_i : L \times L \to \mathbb{B}$

visibility: $vis_i(l_a^i, l_t) = true$ iff l_t is in the line of sight of l_i

Multi-agent surveillance game structures

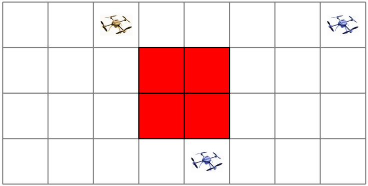


- set of locations L
- states $(l_a^1, \ldots, l_a^m, l_t)$
- visibility $vis_i : L \times L \to \mathbb{B}$
- joint visibility $vis : L^{m+1} \to \mathbb{B}$

visibility: $vis_i(l_a^i, l_t) = true$ iff l_t is in the line of sight of l_i

joint visibility: $vis(\bar{l}, l_t) = true$ iff l_t is visible to at least one agent

Multi-agent surveillance game structures



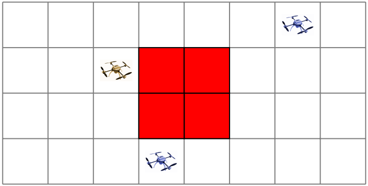
- set of locations L
- states $(l_a^1, \ldots, l_a^m, l_t)$
- visibility $vis_i : L \times L \to \mathbb{B}$
- joint visibility $vis : L^{m+1} \to \mathbb{B}$
- transitions $(l_a, l_t) \rightsquigarrow (l'_a, l'_t)$

visibility: $vis_i(l_a^i, l_t) = true$ iff l_t is in the line of sight of l_i

joint visibility: $vis(\bar{l}, l_t) = true$ iff l_t is visible to at least one agent

transitions: move of target, followed by agents' synchronous move

Multi-agent surveillance game structures



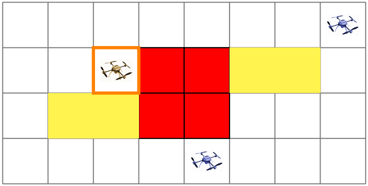
- set of locations L
- states $(l_a^1, \ldots, l_a^m, l_t)$
- visibility $vis_i : L \times L \to \mathbb{B}$
- joint visibility $vis : L^{m+1} \to \mathbb{B}$
- transitions $(l_a, l_t) \rightsquigarrow (l_a', l_t')$

visibility: $vis_i(l_a^i, l_t) = true$ iff l_t is in the line of sight of l_i

joint visibility: $vis(\bar{l}, l_t) = true$ iff l_t is visible to at least one agent

transitions: move of target, followed by agents' synchronous move

Multi-agent surveillance with static sensors

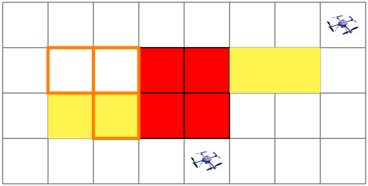


- static sensors $(R_1, \ldots, R_k)$

static sensor: defined by its range $R_i \subseteq L$

Static sensors do not exhibit false positives or false negatives.

Multi-agent surveillance with static sensors



- static sensors $(R_1, \ldots, R_k)$
- belief states $(l_a, B_t, C) \in L \times 2^Q \times 2^{\{1,\ldots,k\}}$

static sensor: defined by its range $R_i \subseteq L$

Static sensors do not exhibit false positives or false negatives.

B_t is contained in the ranges of the triggered sensors C.

Multi-agent surveillance strategies

multi-agent surveillance game $(G, \{R_1, \ldots, R_k\}, \varphi)$, where

- G is a multi-agent surveillance game structure,
- $R_1, \ldots, R_k$ are static sensors,
- φ is a surveillance specification

A **joint strategy** for the agents is **winning** in $(G, \{R_1, \ldots, R_k\}, \varphi)$ if each sequence of belief states resulting from the strategies for the agents satisfies the specification φ.

Multi-agent surveillance strategy synthesis

Multi-agent surveillance synthesis problem

Given: multi-agent surveillance game $(G, \{R_1, \ldots, R_k\}, \varphi)$

Compute: joint strategy for the agents that is wining

A possible approach:

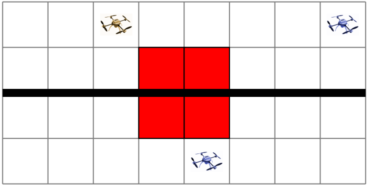
Compute a centralized strategy.

Problem:

Size of the state space is exponential in m.

$\Rightarrow$ **Decompose the synthesis problem!**

Game structure decomposition

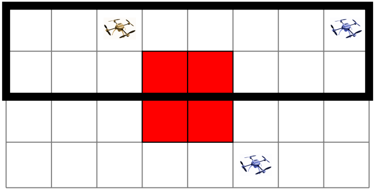


- partition $L = L_1 \uplus \ldots \uplus L_m$
- agent i cannot exit L_i
- agent i cannot observe $L \setminus L_i$

Synthesize individual surveillance strategies independently.

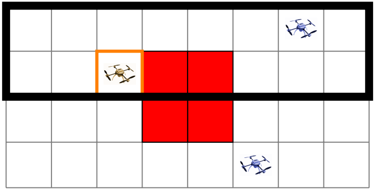
Define local specifications appropriately to ensure soundness.

Local surveillance game structures



- locations $L_i \uplus \{\widehat{l_i}\}$
- states (l_a, l_t)
- $\widehat{vis}_i(l_a, \widehat{l_i}) = false$
- static sensors $\widehat{R}_i$

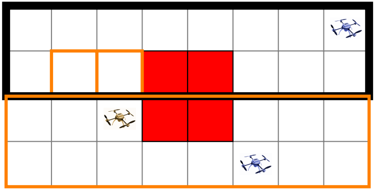
Local surveillance game structures



- locations $L_i \uplus \{\widehat{l_i}\}$
- states (l_a, l_t)
- $\widehat{vis}_i(l_a, \widehat{l_i}) = false$
- static sensors $\widehat{R}_i$

Agent 1: size of local belief set is 1

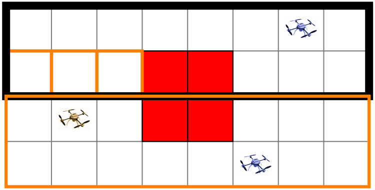
Local surveillance game structures



- locations $L_i \uplus \{\widehat{l_i}\}$
- states (l_a, l_t)
- $\widehat{vis}_i(l_a, \widehat{l_i}) = false$
- static sensors $\widehat{R}_i$

Agent 1: size of local belief set is 3, including $\widehat{l_1}$

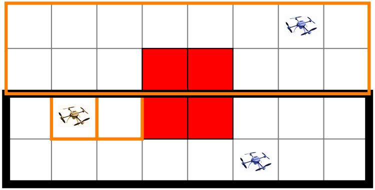
Local surveillance game structures



- locations $L_i \uplus \{\widehat{l_i}\}$
- states (l_a, l_t)
- $\widehat{vis}_i(l_a, \widehat{l_i}) = false$
- static sensors $\widehat{R}_i$

Agent 1: size of local belief set is 4, including $\widehat{l_1}$

Local surveillance game structures

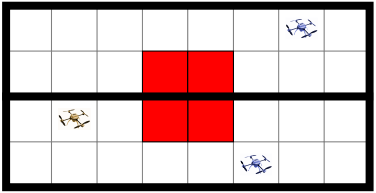


- locations $L_i \uplus \{\widehat{l_i}\}$
- states (l_a, l_t)
- $\widehat{vis}_i(l_a, \widehat{l_i}) = false$
- static sensors $\widehat{R}_i$

Agent 1: size of local belief set is 4, including $\widehat{l_1}$

Agent 2: size of local belief set is 3, including $\widehat{l_2}$

Local surveillance game structures

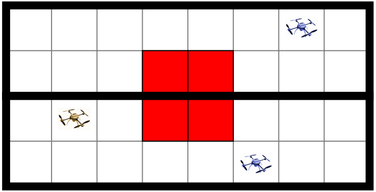


- locations $L_i \uplus \{\widehat{l_i}\}$
- states (l_a, l_t)
- $\widehat{vis}_i(l_a, \widehat{l_i}) = false$
- static sensors $\widehat{R}_i$

Agent 1: size of local belief set is 4, including $\widehat{l_1}$
Agent 2: size of local belief set is 3, including $\widehat{l_2}$

The size of the global belief set is 5.

Global belief sets



- locations $L_i \uplus \{\widehat{l_i}\}$
- states (l_a, l_t)
- $\widehat{vis}_i(l_a, \widehat{l_i}) = \mathit{false}$

local belief set of agent i**:** $\widehat{B}^i_t \subseteq (L_i \uplus \{\widehat{l_i}\})$

global belief set of agent i**:** $B^i_t = \begin{cases} \widehat{B}^i_t & \text{if } \widehat{l_i} \notin \widehat{B^i_t} \\ \widehat{B}^i_t \cup (L \setminus Li) & \text{otherwise} \end{cases}$

joint global belief set: $\bigcap_{i \in \{1,\ldots,m\}} B^i_t$

Specification decomposition

We want **local surveillance specifications** $\varphi_1, \ldots, \varphi_n$ such that

if $f_1, \ldots, f_n$ are wining strategies in the local games $(G_i, \widehat{R}_i, \varphi_i)$

then $f_1 \otimes \ldots \otimes f_n$ is a winning strategy in $(G, \{R_1, \ldots, R_k\}, \varphi)$.

Specification decomposition

We restrict to conjunctions of safety and liveness surveillance.

$$\begin{aligned} \square p_{\leq a} \wedge \square p_{\leq b} &\equiv \square p_{\leq \min(a,b)} \\ \square \diamond p_{\leq a} \wedge \square \diamond p_{\leq b} &\equiv \square \diamond p_{\leq \min(a,b)} \\ \square p_{\leq a} \wedge \square \diamond p_{\leq b} &\equiv \square p_{\leq a} \qquad \text{if } a \leq b \end{aligned}$$

It suffices to consider only specifications of the following forms

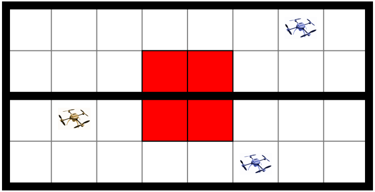
- safety $\square p_{\leq a}$, liveness $\square \diamond p_{\leq a}$,
- mixed $\square p_{\leq a} \wedge \square \diamond p_{\leq b}$ with $a > b$.

Safety surveillance objectives

For global specification $\Box p_{\leq b}$ and $n \geq 2$ agents, take local specifications

$$\Box p_{\leq c}, \text{ where } c = \lfloor \frac{b}{n} \rfloor + 1.$$

Example: specification $\Box p_{\leq 2}$



Each of the local specifications is $\Box p_{\leq 2}$ as well.

Conservative approximation due to the absence of coordination.

Liveness surveillance objectives

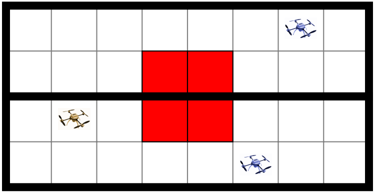
Require that each mobile sensor satisfies the liveness specification.

For global specification $\Box\Diamond p_{\leq 2}$ and n agents, take

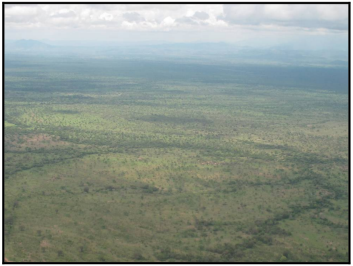
$$\big(\Box\Diamond(\mathit{belief} \neq \{\widehat{l_i}\})\big) \rightarrow \big(\Box\Diamond(p_{\leq b} \wedge (\widehat{l_i} \notin \mathit{belief}))\big),$$

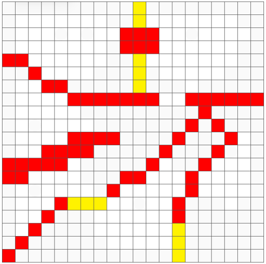
where $\mathit{belief} \neq \{\widehat{l_i}\}$ and $\widehat{l_i} \notin \mathit{belief}$ are surveillance predicates.

Example: specification $\Box\Diamond p_{\leq 1}$



Example





- model terrain by 20×20 grid
- red regions: impassable terrain
- yellow regions: range of static sensors

Surveillance specification: $\Box \Diamond p_{\leq 5}$

Example

	Subgame	Number of locations	Synthesis time (s)
3 sensors	Subgame 1	142	473
	Subgame 2	113	306
	Subgame 3	145	372
	Total	**400**	**1151**
6 sensors	Subgame 1	69	101
	Subgame 2	74	206
	Subgame 3	62	111
	Subgame 4	52	88
	Subgame 5	77	285
	Subgame 6	66	64
	Total	**400**	**855**

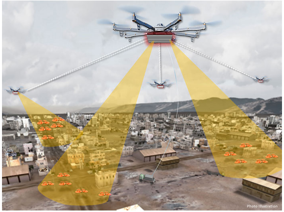
- model terrain by 20×20 grid
- red regions: impassable terrain
- yellow regions: range of static sensors

Surveillance specification: $\Box\Diamond p_{\leq 5}$

Current work and future directions

- Heuristics for constructing initial abstraction
- Improved abstraction refinement methods
- Less conservative specification decomposition
- Some coordination between mobile sensors
- Probabilistic detection errors by static sensors
- Noisy observations from mobile sensors

. . .



Conclusion

- Applying reactive synthesis to surveillance problems
- Domain specific formal specification languages
- Customized abstraction and refinement methods
- Compositional approaches key for achieving scalability

Thank you for your attention! 

 Questions?

Papers at 57th IEEE Conference on Decision and Control
preprints available at `raynadimitrova.github.io`