Resilience Of Multi-robot Systems To Physical Masquerade Attacks

Hello!

I'm Kacper

SafeThings Workshop
May 23rd, 2019

Kacper Wardega

Roberto Tron

Wenchao Li

BOSTON UNIVERSITY

IEEE SECURITY & PRIVACY

Exposé! Security of Industrial Robots

(Quarta et. al. S&P'17)

- Easy to hack
- Easy to cause damage
- Many different settings

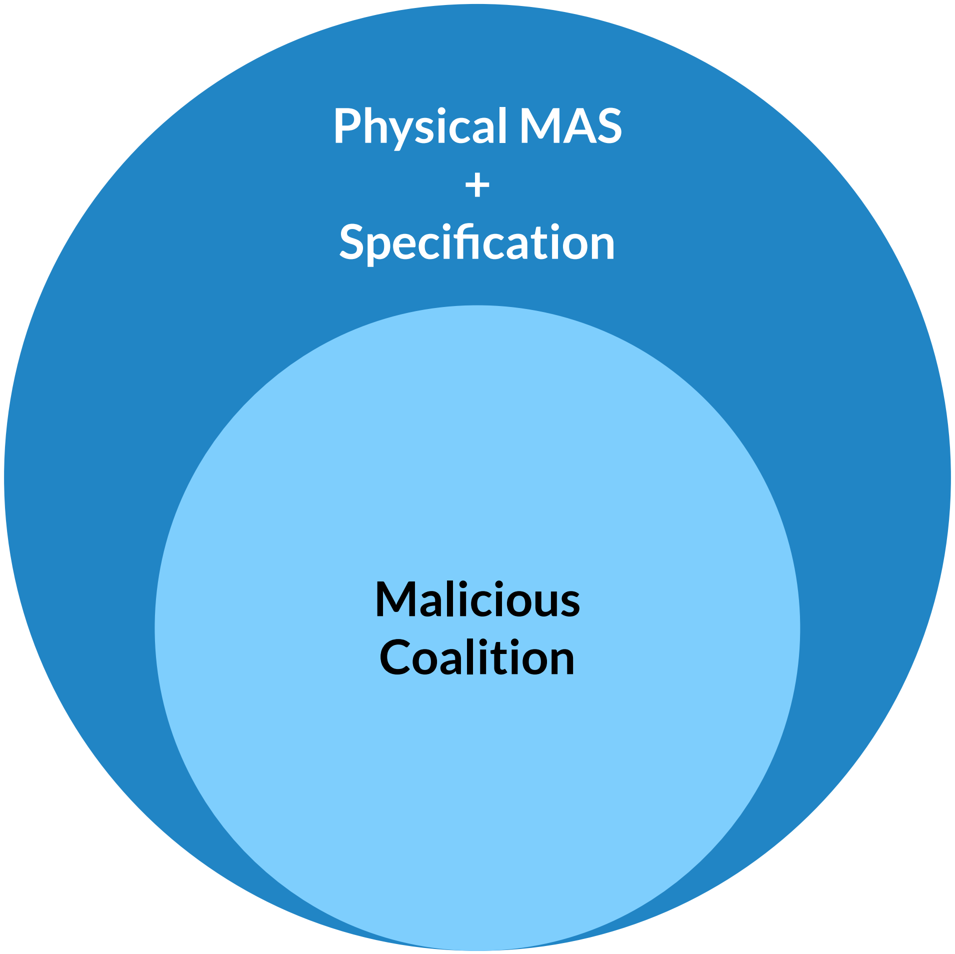
Illustration designed by macrovector / Freepi

Sybil attacks

(Gil et. al. Aut. Rob.'17)

- Spoofing location can also cause harm!

Physical Masquerade Attack



MAPF problem

Robots, reach, avoid.

+

Single malicious agent

Reach a secure location.

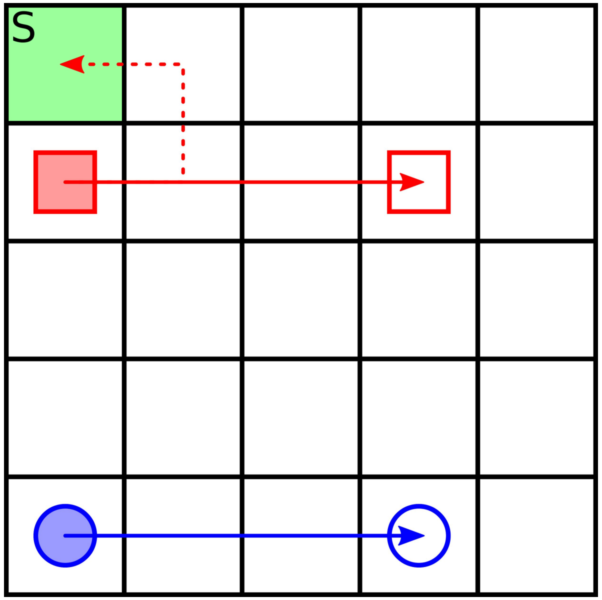
+

Stealth!

Inter-agent observations.

A new, unstudied problem!

Other domains include UAV patrolling and unstructured monitoring.



Vulnerable

Threat Model

Power

The attacker has full control of a single robot.

Limitations

The attacker inherits the control-actions of non-compromised robots.

Information

Sensor capabilities and planned routes are common knowledge.

Questions

How much of a concern are physical masquerade attacks?
How can designers defend against these attacks?

Two cases:

Discrete space

Discrete actions

Adjacent observations

Continuous space

Displacement dynamics

Radius-based observation

>90%

Of all conventionally-obtained plans are vulnerable to physical masquerade attack.

OBSERVATION PLANNING

By leveraging inter-agent observations, designers can implement monitoring for physical masquerade attacks.

Observation Planning: Example

FROM	TO	TIME
A	B	3
B	A	3
…	…	…
F	A	24

Monitoring Guarantee

Plan	Observe	Report
Plan the set of expected observations.	Run the system, following the motion & observation plan.	Issue an alarm on unexpected or missing observations.

Challenges

Enhanced Conflict-Based Search

Complete & optimal decentralized planner.

How can I speed the discovery of plans with monitoring guarantees using conflicts?

A*-esque

Heuristic-guided centralized planner.

What heuristics even make sense to use? What are the properties of plans with monitoring guarantees?

Discrete Space

EF-SMT

(Z3)

Continuous Space

MIQCP

(GUROBI)

“

$$\left(\forall t \in \mathbb{N}_T, j \in \mathbb{N}_R \setminus i^*\right)$$
$$\left(\phi\left(x_j^t, x_{i^*}^t\right) \iff \phi\left(x_j^t, y^t\right)\right)$$

The attacking agent must not violate the observation plan

Optimal & complete planning with monitoring guarantees!

4-connected grid

EF-SMT

(Z3)

Continuous Space

MIQCP

(GUROBI)

Optimal & complete planning with monitoring guarantees!

4-connected grid

EF-SMT

(Z3)

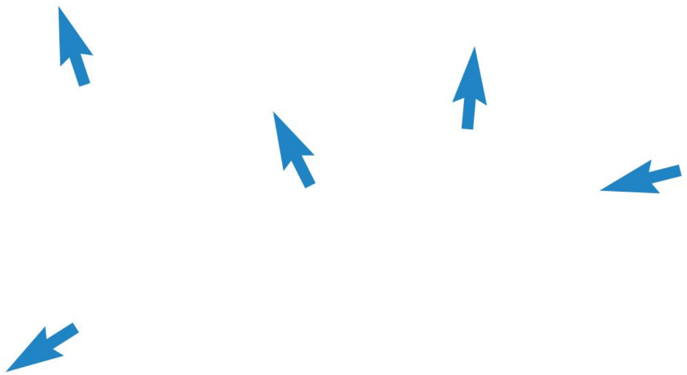
Continuous Space

MIQCP

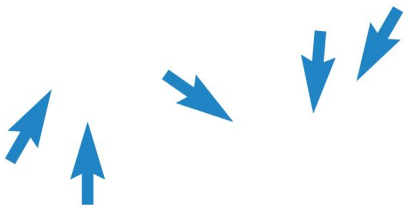
(GUROBI)

Check vulnerability of existing plans.

Observation



Sparse



Dense

Traditional MAPF algorithms leverage sparsity.
Planning with monitoring guarantees is **achieved through dense solutions**.

Scalability

How can I efficiently handle large environments and many agents?

Collusion

How can I handle situations with multiple compromised agents? Are there logics to reason about unknown coalitions?

Thanks!

Questions?

Q1: Efficient planning & impact on performance?

Q2: How to model collusion?