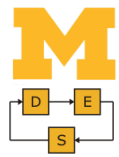
Resilience Against Sensor Deception Attacks at the Supervisory Control Layer of Cyber-Physical Systems

A discrete event systems approach

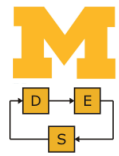
Stéphane Lafortune
Department of Electrical Engineering and Computer Science
The University of Michigan, Ann Arbor, USA

IFAC WC 2020 – Workshop on "Analysis and Control for Resilience of DES"

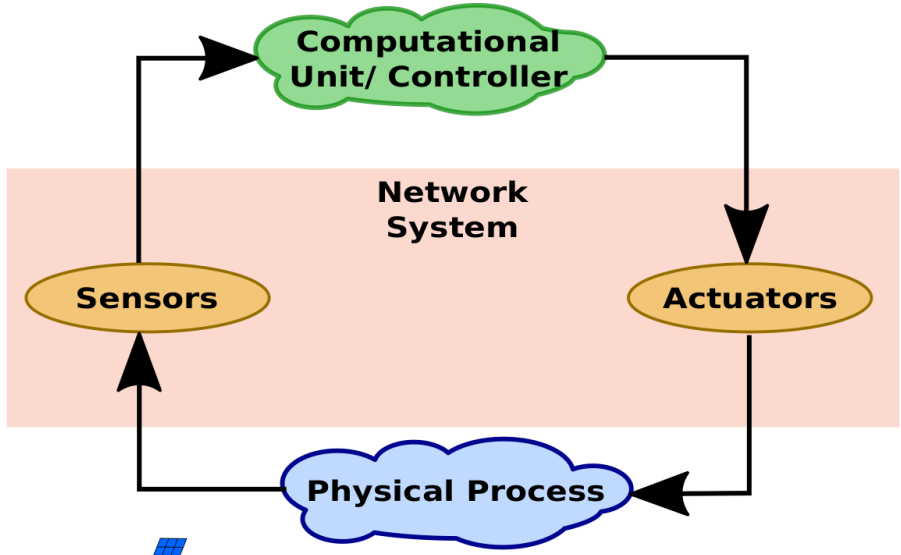


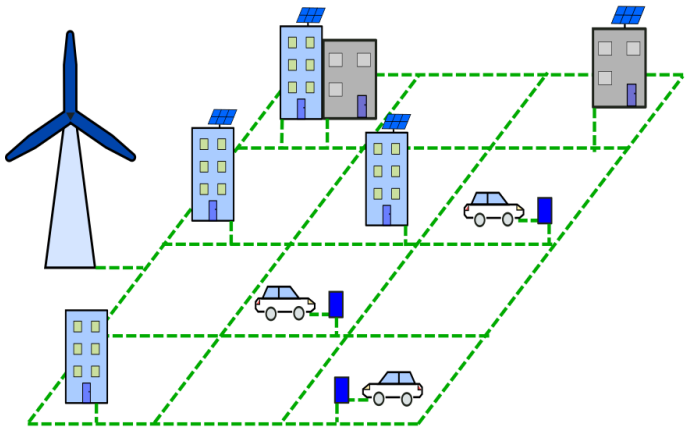
Acknowledgements

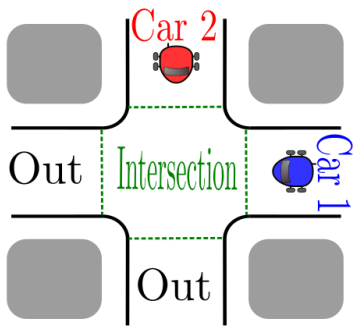
- **Rômulo Meira-Góes**
  PhD Candidate, EECS Dept., University of Michigan
- Collaborators
  - Eunsuk Kang, Carnegie-Mellon University, USA
  - Raymond Kwong, University of Toronto, Canada
  - Hervé Marchand, SUMO lab - INRIA-Rennes, France
- Financial Support: US National Science Foundation

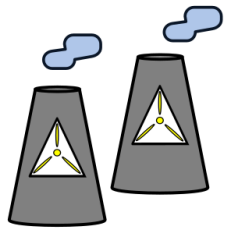


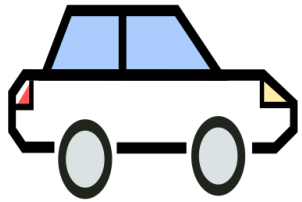
Cyber-physical systems

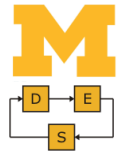




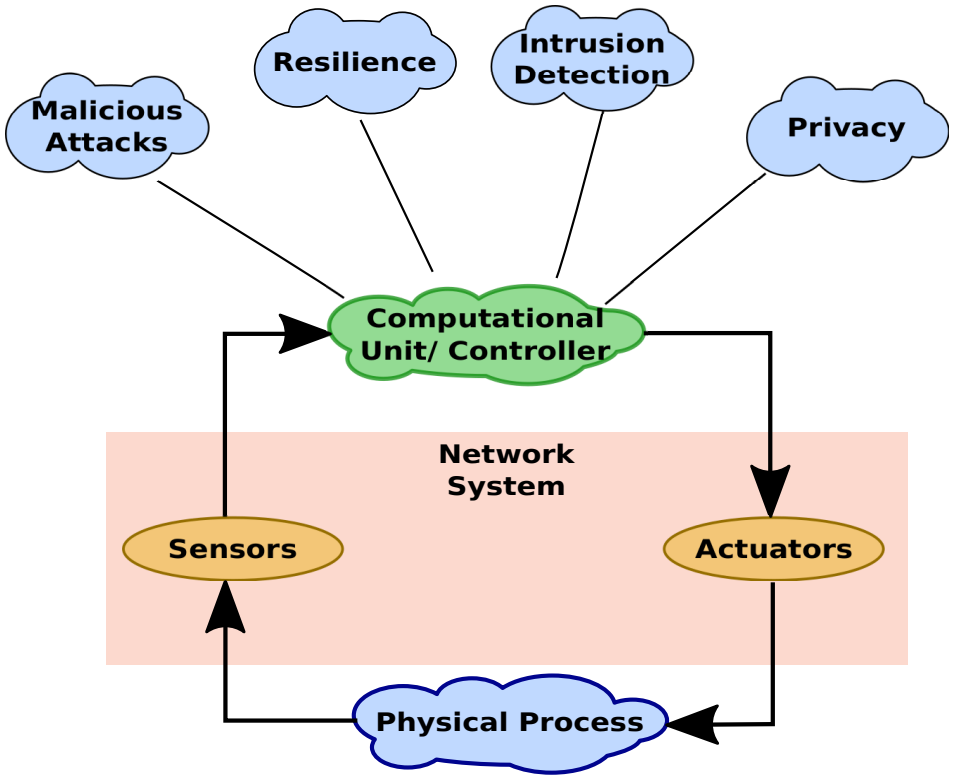


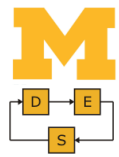




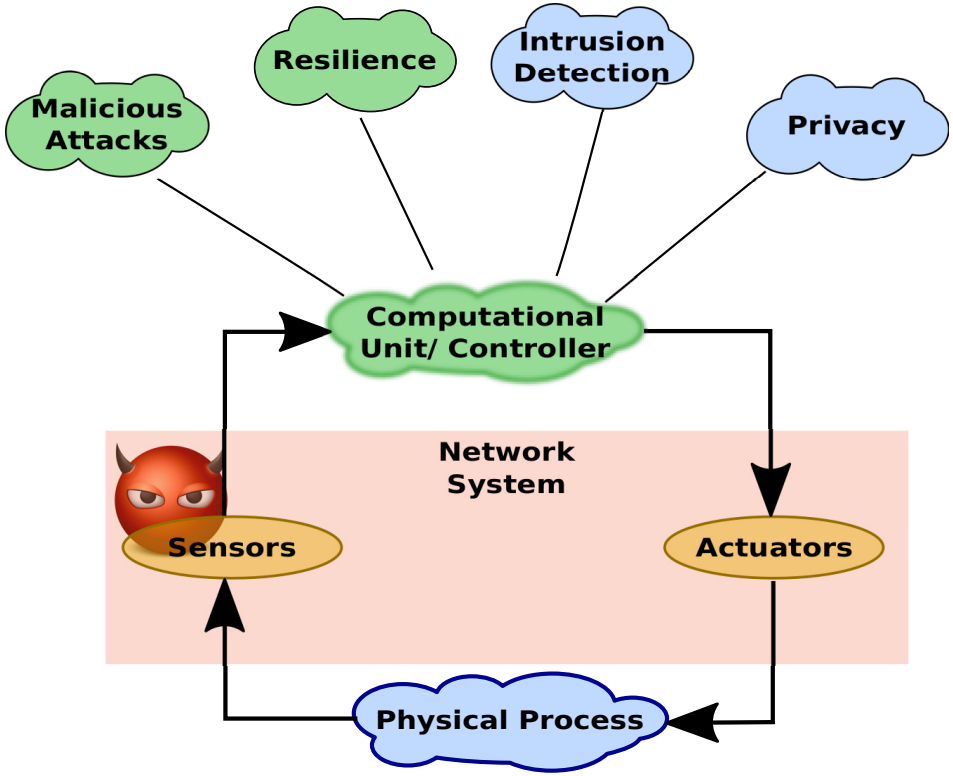


Cyber-security

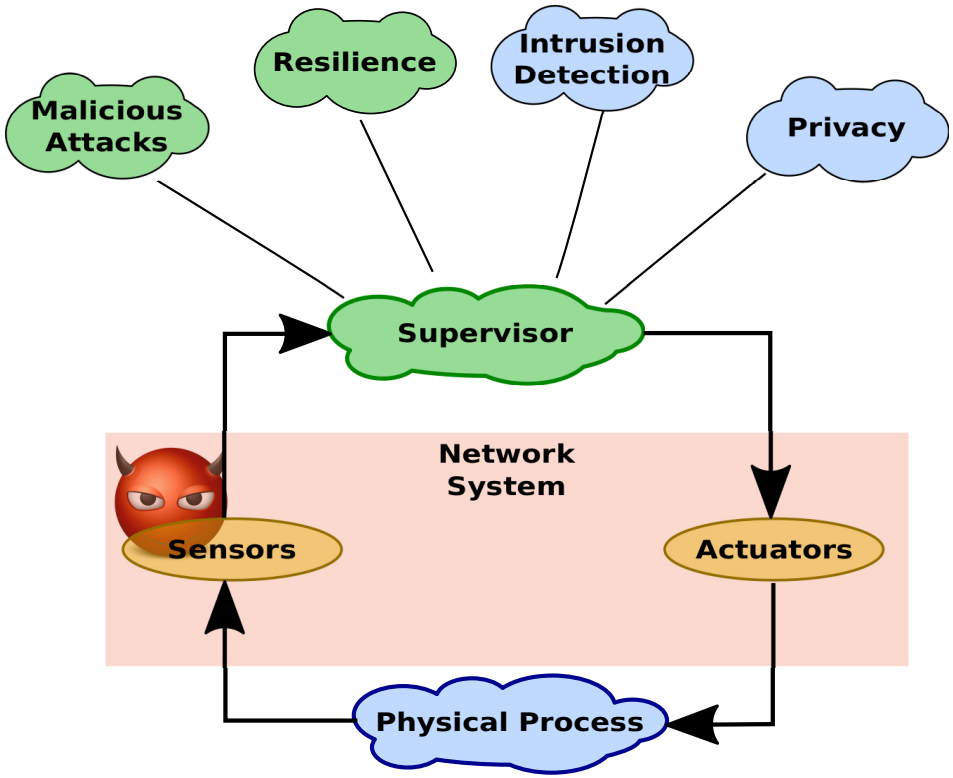


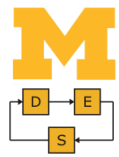


Cyber-security



Cyber-security





Discrete event systems

CPS already suitably abstracted as discrete transition system (at supervisory control layer)

DFA

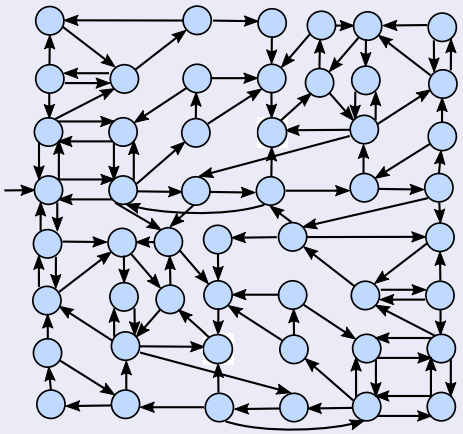
$G = (X_G, \Sigma, \delta_G, x_{0,G})$

- X_G is a finite set of states
- Σ is a finite set of events
- $\delta_G : X_G \times \Sigma \to X_G$
- $x_{0,G}$ is the initial state

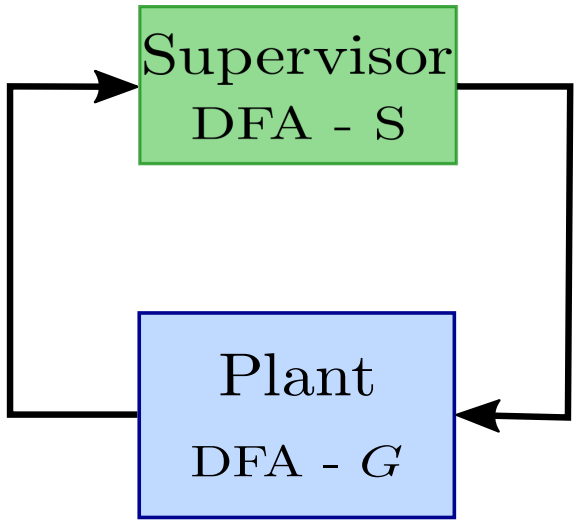
$\mathcal{L}(G)$ is the language generated by G

Example

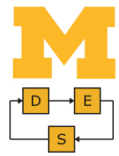
DFA - G



Supervisory control theory —SCT

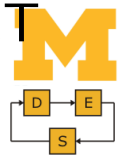


- $\Sigma = \Sigma_c \cup \Sigma_{uc}$
- Admissible Control Decisions
- $\Sigma = \Sigma_o \cup \Sigma_{uo}$
- Critical States $X_{crit} \subset X_G$
- S/G controlled system: $\mathcal{L}(S/G)$



Supervisory control theory

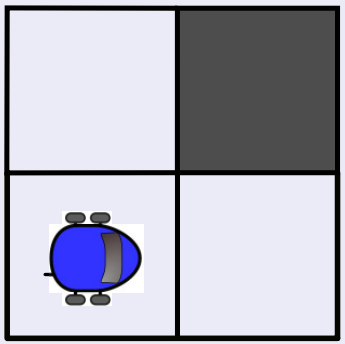
- Originally introduced by Ramadge & Wonham in the 1980s. Comprehensive theory now.
- Discrete-event system-theoretic properties for *necessary and sufficient* conditions for existence of solution
  - controllability (about *actuators*)
  - observability (about *sensors* and *actuators*)
- Effective computational algorithms for *supervisors* under regular language specifications (safety and non-blockingness)
  - Fix-point characterizations on languages: finitely-convergent iterative algorithms on automata
- This talk:
  - Supremal controllable sublanguage [customized]
  - Supremal controllable and normal sublanguage
  - Maximal controllable and observable sublanguage
- *Formal methods in control*: connection between reactive synthesis and SCT



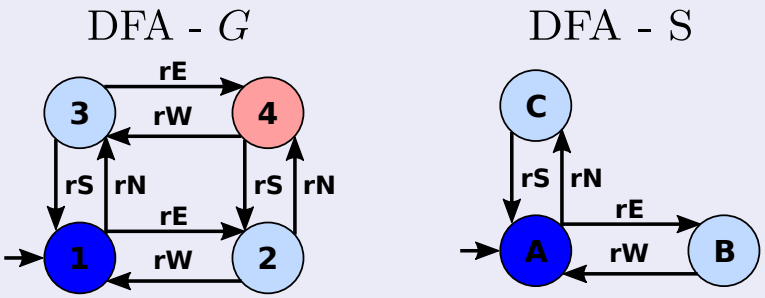
Supervisory control

Example: Robot in an $n \times n$ grid with obstacles

($n = 2$ to fit in one slide)



Model:

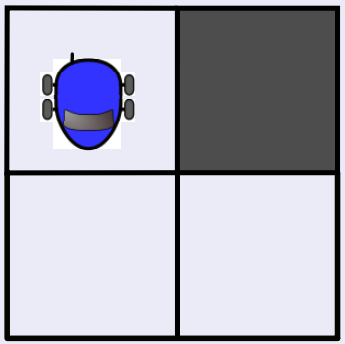


Current control decision: {rE, rN}

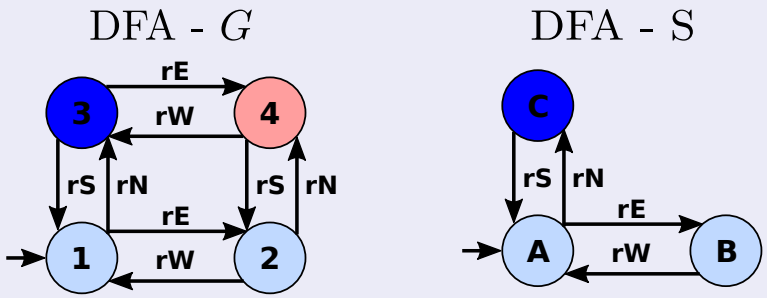
Supervisory control

Example: Robot in an $n \times n$ grid with obstacles

($n = 2$ to fit in one slide)



Model:

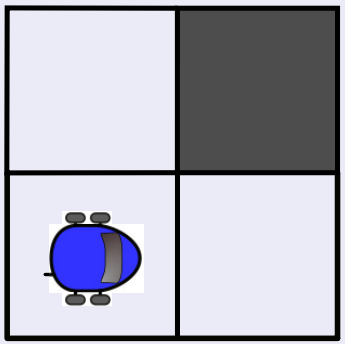


Current control decision: {rS}

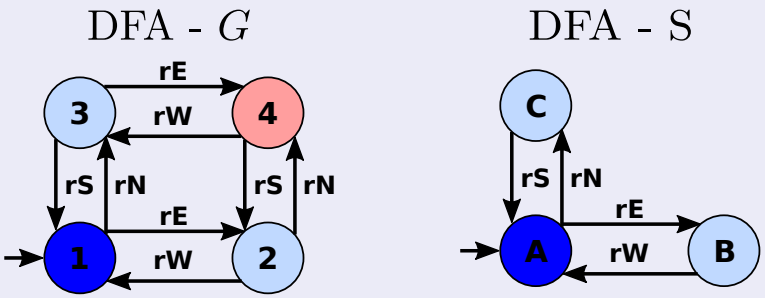
Supervisory control

Example: Robot in an $n \times n$ grid with obstacles

($n = 2$ to fit in one slide)



Model:

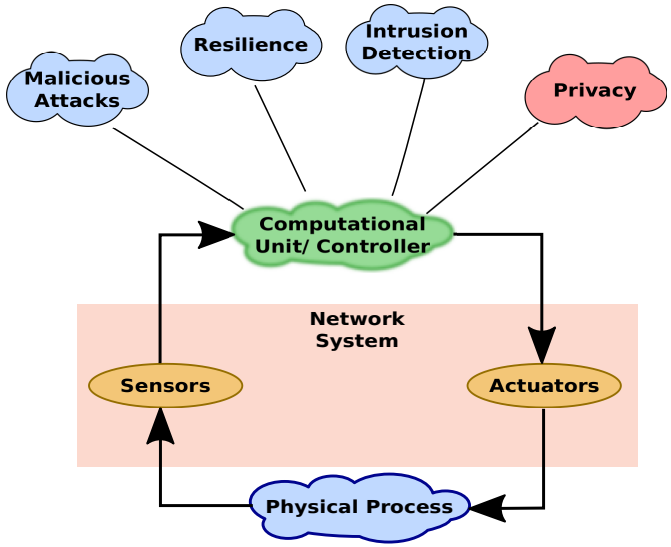


Current control decision: {rE, rN}

Security of CPS - Literature review in DES

Privacy:

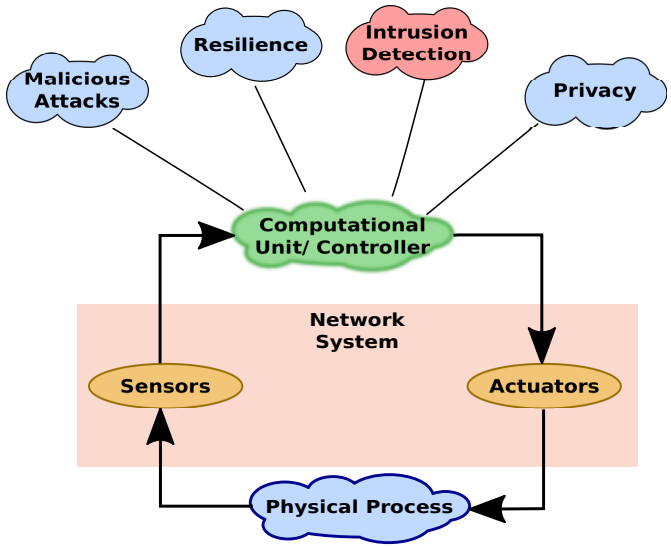
- **Saboori and Hadjicostis 2007**, *"Notions of security and opacity in discrete event systems"*
- **Dubreil, Darondeau, and Marchand 2010**, *"Supervisory control for opacity"*
- **Saboori and Hadjicostis 2012**, *"Opacity-Enforcing Supervisory Strategies via State Estimator Constructions"*
- **Cassez, Dubreil, and Marchand 2012**, *"Synthesis of opaque systems with static and dynamic masks"*
- **Jacob, Lesage, and Faure 2016**, *"Overview of discrete event systems opacity: Models, validation, and quantification"*
- **Wu et al. 2018**, *"Synthesis of Obfuscation Policies to Ensure Privacy and Utility"*



Security of CPS - Literature review in DES

Intrusion Detection:

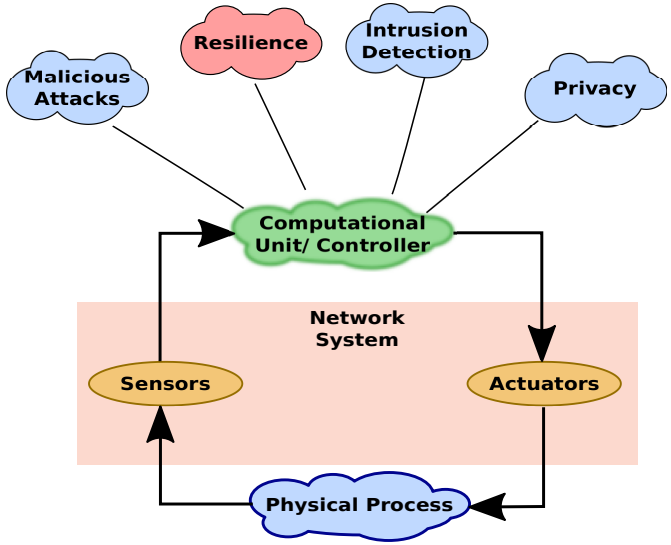
- **Thorsley and Teneketzis 2006**, *"Intrusion Detection in Controlled Discrete Event Systems"*
- **Carvalho et al. 2018**, *"Detection and mitigation of classes of attacks in supervisory control systems"*
- **Lima et al. 2019**, *"Security Against Communication Network Attacks of Cyber-Physical Systems"*
- **Wang et al. 2020**, *"Mitigation of Classes of Attacks using a Probabilistic Discrete Event System Framework"*
- **Meira-Góes, Keroglou, and Lafortune 2020**, *"Towards probabilistic intrusion detection in supervisory control of discrete event systems"*



Security of CPS - Literature review in DES

Resilience:

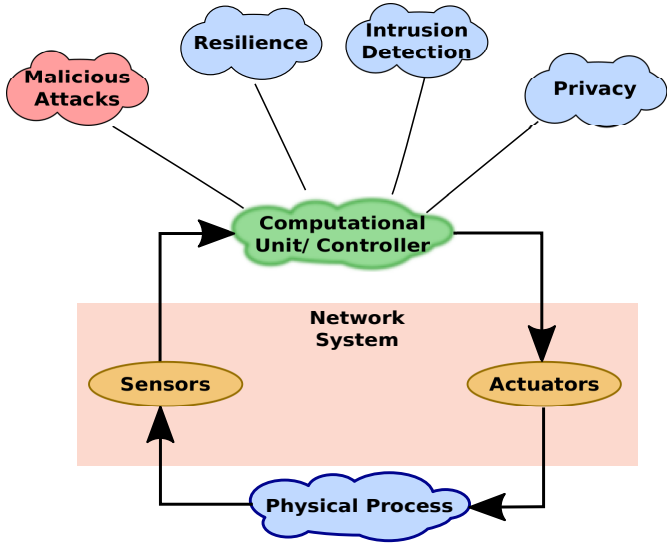
- **Moor 2016**, *"A discussion of fault-tolerant supervisory control in terms of formal languages"* FTC
- **Wakaiki, Tabuada, and Hespanha 2018**, *"Supervisory Control of Discrete-Event Systems Under Attacks"*
- **Su 2018**, *"Supervisor synthesis to thwart cyber attack with bounded sensor reading alterations"*
- **Zhu, Lin, and Su 2019**, *"Supervisor Obfuscation Against Actuator Enablement Attack"*
- **Wang and Pajic 2019a**, *"Attack-Resilient Supervisory Control with Intermittently Secure Communication"*
- **Meira-Góes and Lafortune 2020**, *"Moving Target Defense based on Switched Supervisory Control: A New Technique for Mitigating Sensor Deception Attacks"*



Security of CPS – Literature review in DES

Malicious Attacks:

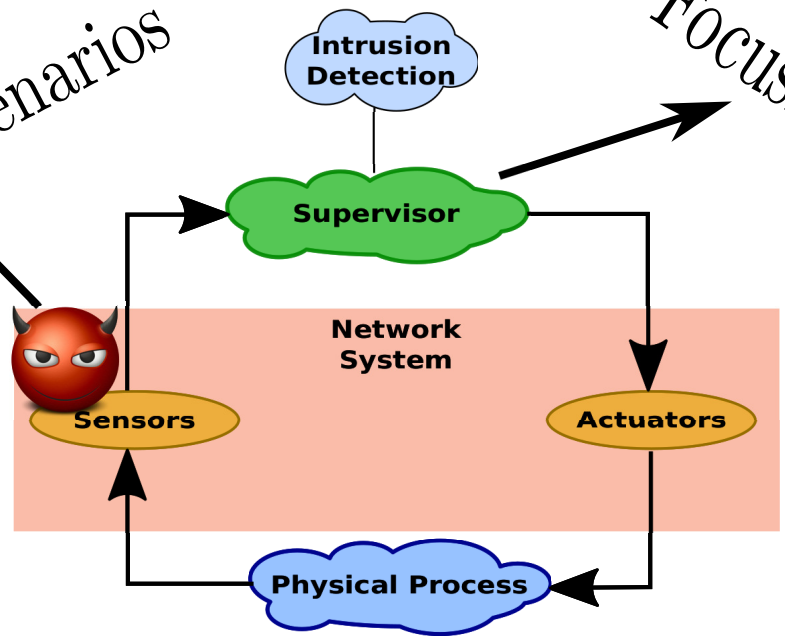
- **Su 2018**, *"Supervisor synthesis to thwart cyber attack with bounded sensor reading alterations"*
- **Zhang et al. 2018**, *"Stealthy Attacks for Partially-Observed Discrete Event Systems"*
- **Lin et al. 2019**, *"Synthesis of Supremal Successful Normal Actuator Attackers on Normal Supervisors"*
- **Wang and Pajic 2019b**, *"Supervisory Control of Discrete Event Systems in the Presence of Sensor and Actuator Attacks"*



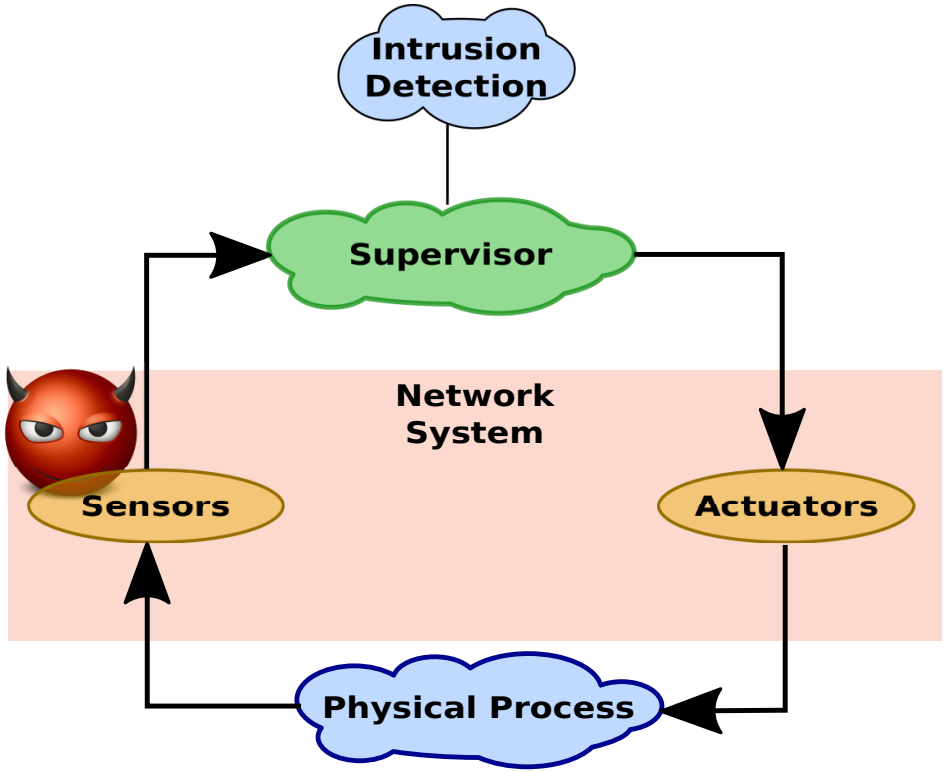
Overview of presentation

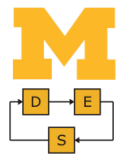
Part 1 - Focusing on the attacker
a) Basic scenario
b) Generalized scenarios

Part 2 - Focusing on the supervisor



Synthesis of sensor deception attacks





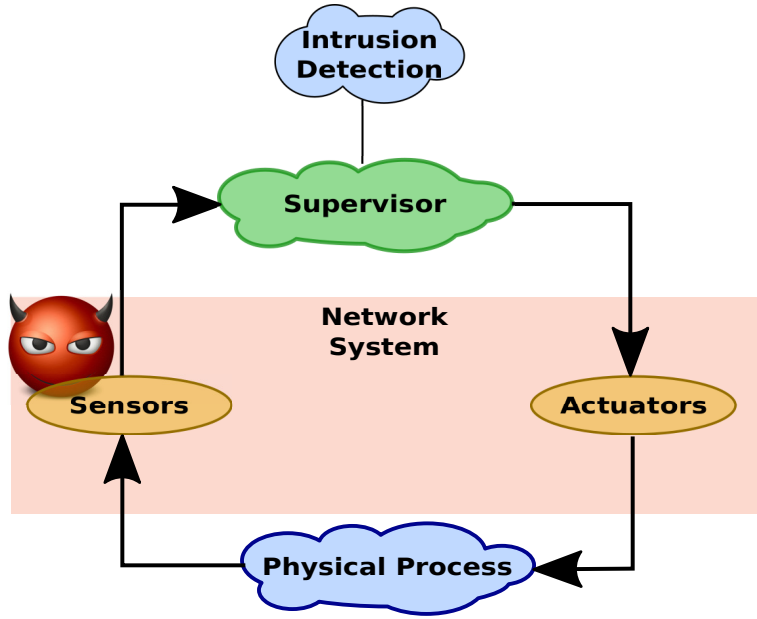
Synthesis of sensor deception attacks – Assumptions

Assumptions:

- Knows Supervisor and Plant models
- Observes same events as Supervisor
- Hijacks sensors $\Sigma_a \subseteq \Sigma$

Goals:

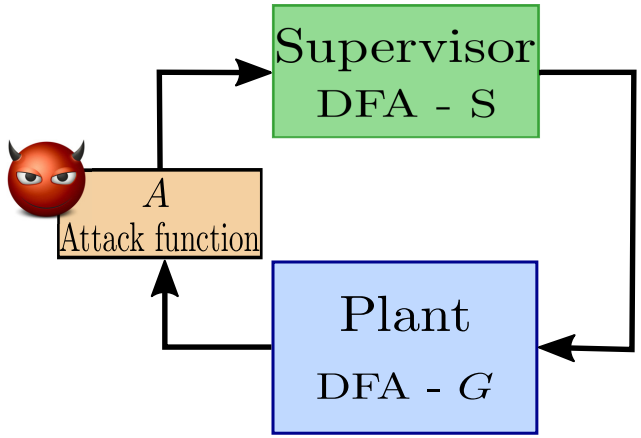
- Cause damage to Plant
- Do not trigger Intrusion Detection Module



Attack function

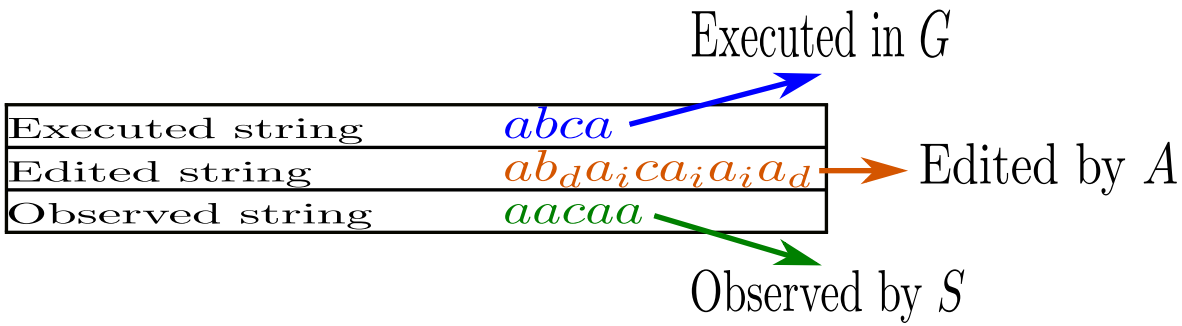
Attack function with $\Sigma_a \subseteq \Sigma$
A :(past edited string)$\times$(new executed event)$\rightarrow$(edited suffix)

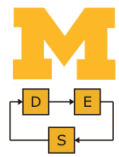
Executed string	$abca$
Edited string	$ab_d a_i c a_i a_i a_d$
Observed string	$aacaa$



Attack function

Attack function with $\Sigma_a \subseteq \Sigma$
A :(past edited string)$\times$(new executed event)$\rightarrow$(edited suffix)

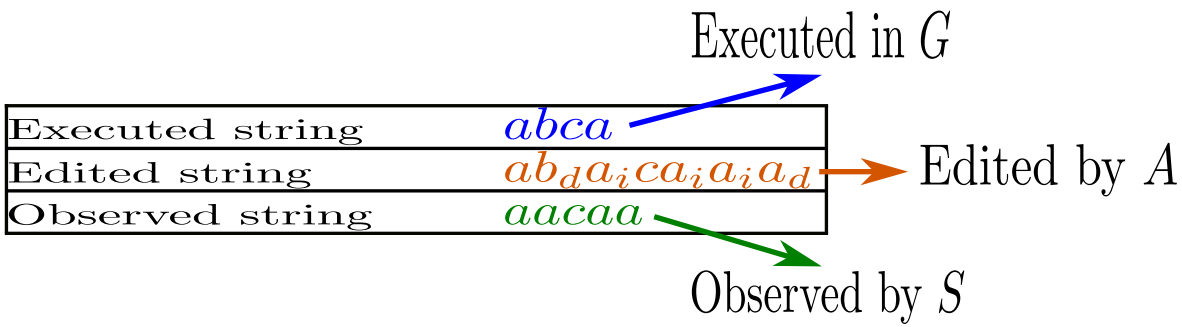


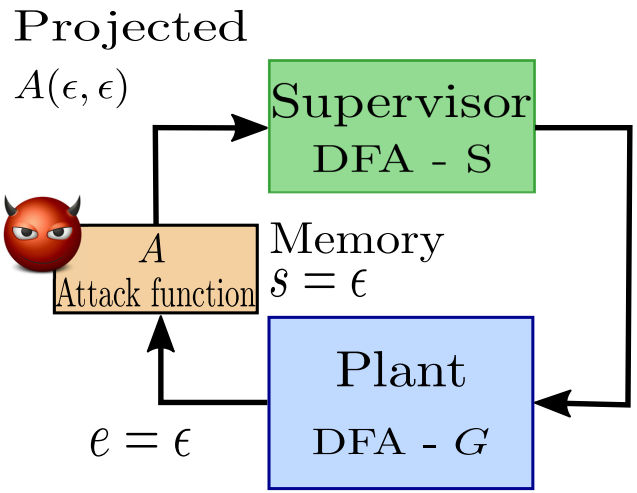


Attack function

Attack function with $\Sigma_a \subseteq \Sigma$

A :(past edited string)$\times$(new executed event)$\rightarrow$(edited suffix)





Initial condition: Insertions at system initialization

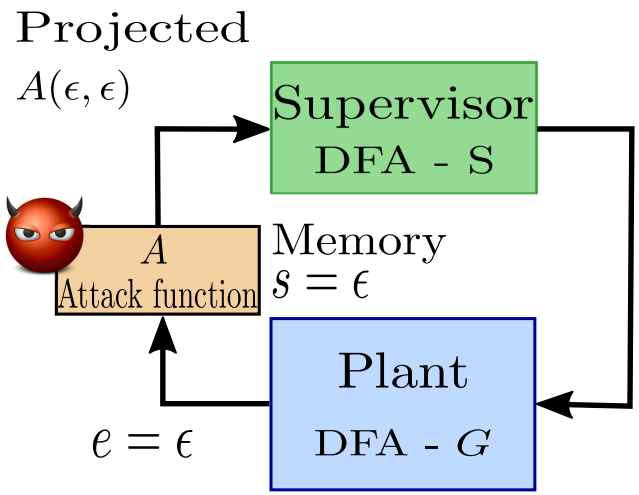
Attack function

Attack function with $\Sigma_a \subseteq \Sigma$

A :(past edited string)$\times$(new executed event)$\rightarrow$(edited suffix)

Initial condition: Insertions at system initialization

$$\mathbf{A}(\epsilon, \epsilon) \in \mathbf{\Sigma_a^*}$$



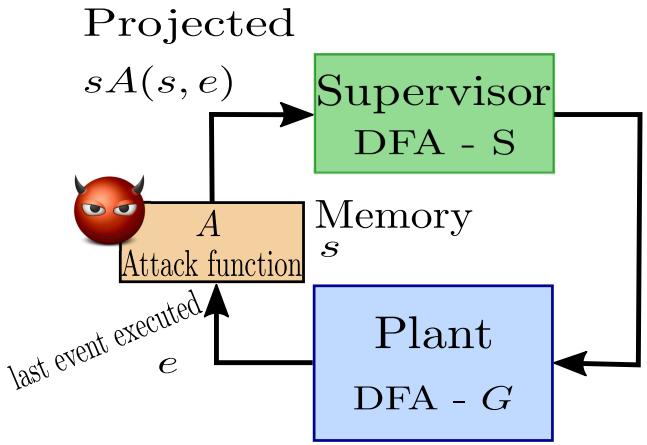
Attack function

Attack function with $\Sigma_a \subseteq \Sigma$
A :(past edited string)$\times$(new executed event)$\rightarrow$(edited suffix)

Initial condition: Insertions at system initialization
$\mathbf{A}(\epsilon, \epsilon) \in \mathbf{\Sigma_a^*}$

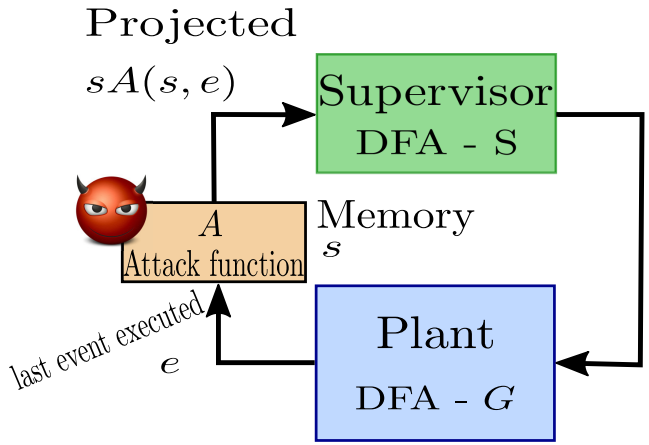
Compromised: Deletions/insertions

Not compromised: Insertions after event is reported unaltered



Attack function

Attack function with $\Sigma_a \subseteq \Sigma$
A :(past edited string)$\times$(new executed event)$\rightarrow$(edited suffix)



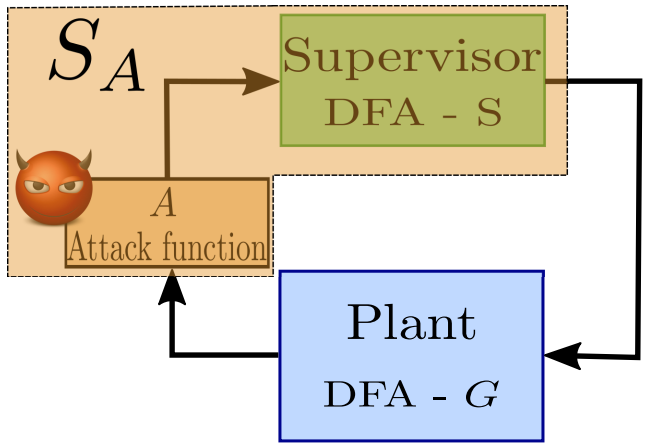
Initial condition: Insertions at system initialization
$\mathbf{A}(\epsilon, \epsilon) \in \mathbf{\Sigma_a^*}$

Compromised: Deletions/insertions
$\mathbf{e} \in \mathbf{\Sigma_a} \rightarrow \mathbf{A(s,e)} \in \mathbf{\Sigma_a^*}$

Not compromised: Insertions after event is reported unaltered
$\mathbf{e} \in \mathbf{\Sigma \backslash \Sigma_a} \rightarrow \mathbf{A(s,e)} \in \mathbf{\{e\}\Sigma_a^*}$

Attack function

Attack function with $\Sigma_a \subseteq \Sigma$
A :(past edited string)$\times$(new executed event)$\rightarrow$(edited suffix)

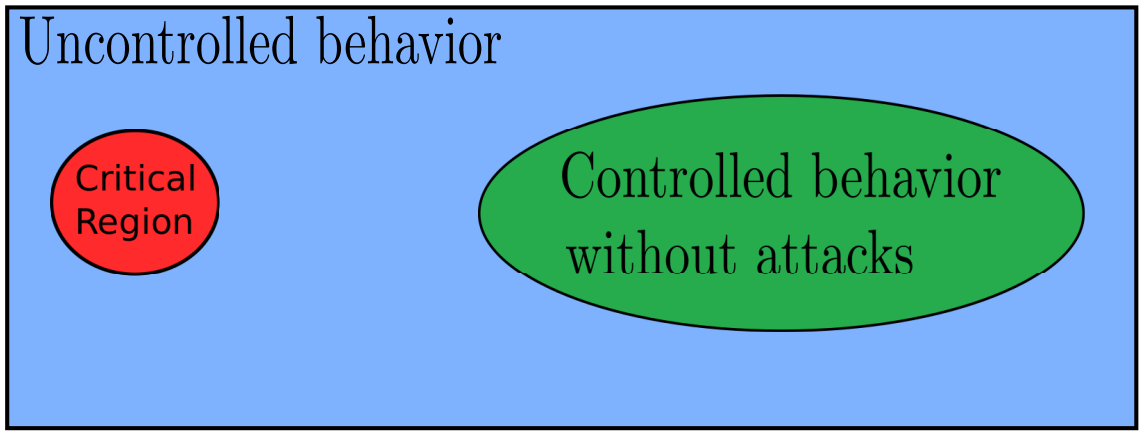


Initial condition: Insertions at system initialization
$\mathbf{A}(\epsilon, \epsilon) \in \mathbf{\Sigma_a^*}$

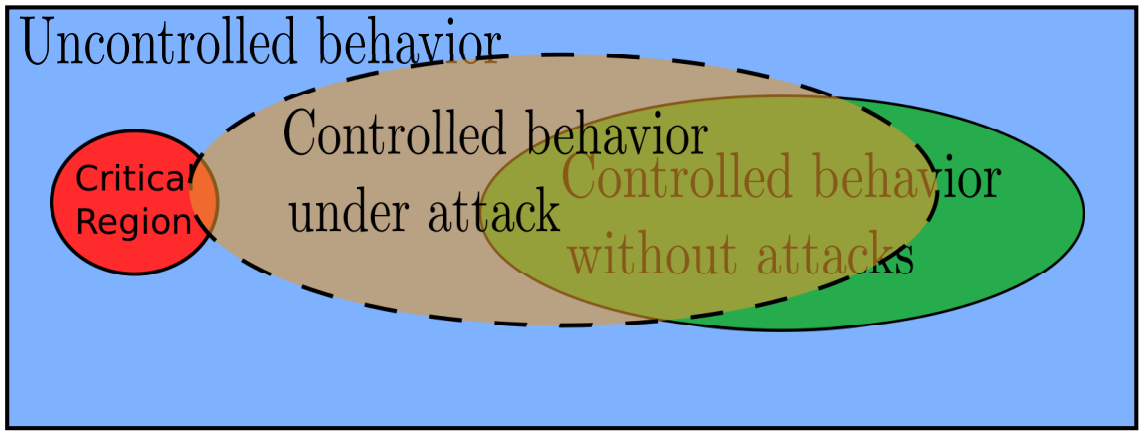
Compromised: Deletions/insertions
$\mathbf{e} \in \mathbf{\Sigma_a} \rightarrow \mathbf{A(s, e)} \in \mathbf{\Sigma_a^*}$

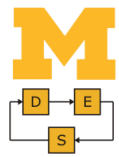
Not compromised: Insertions after event is reported unaltered
$\mathbf{e} \in \mathbf{\Sigma \backslash \Sigma_a} \rightarrow \mathbf{A(s, e)} \in \mathbf{\{e\}\Sigma_a^*}$

Influence of A on controlled system



Influence of A on controlled system





Problem formulation: Synthesis of attack functions

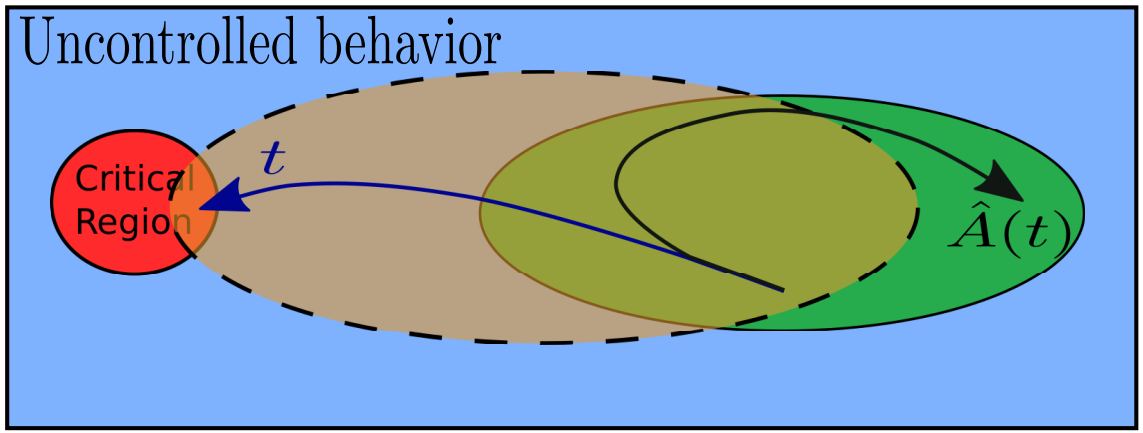
Synthesis of Attack Function

Given G, S and Σ_a. Synthesize an attacker A that generates $\mathcal{L}(S_A/G)$ satisfying:

Completeness: $\forall te \in \mathcal{L}(S_A/G) \rightarrow A(\hat{A}(t), e)$ is defined

Stealthiness: $\forall te \in \mathcal{L}(S_A/G) \rightarrow \hat{A}(t)A(\hat{A}(t), e) \in \mathcal{L}(S/G)$

Strong Attack: $\exists t \in \mathcal{L}(S_A/G) \rightarrow \delta_G(x_{0,G}, t) \in X_{crit}$

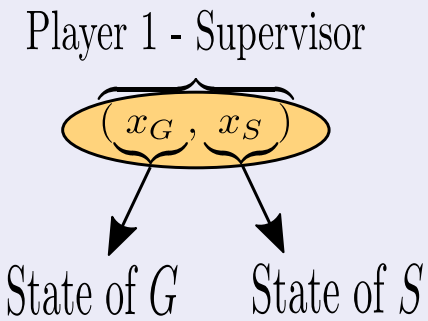


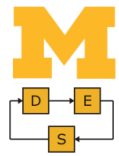
Note: $\hat{A}(t)$ is entire edited string for executed string t

Solution approach: Graph games

Information and Definition

Arena $\mathcal{A}$

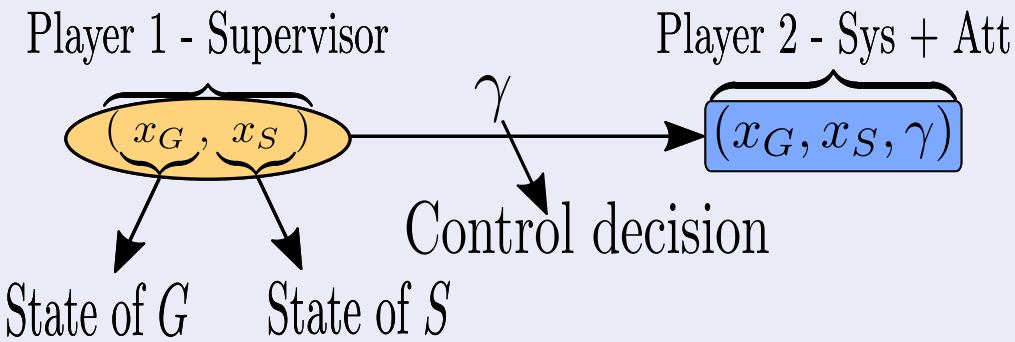




Solution approach: Graph games

Information and Definition

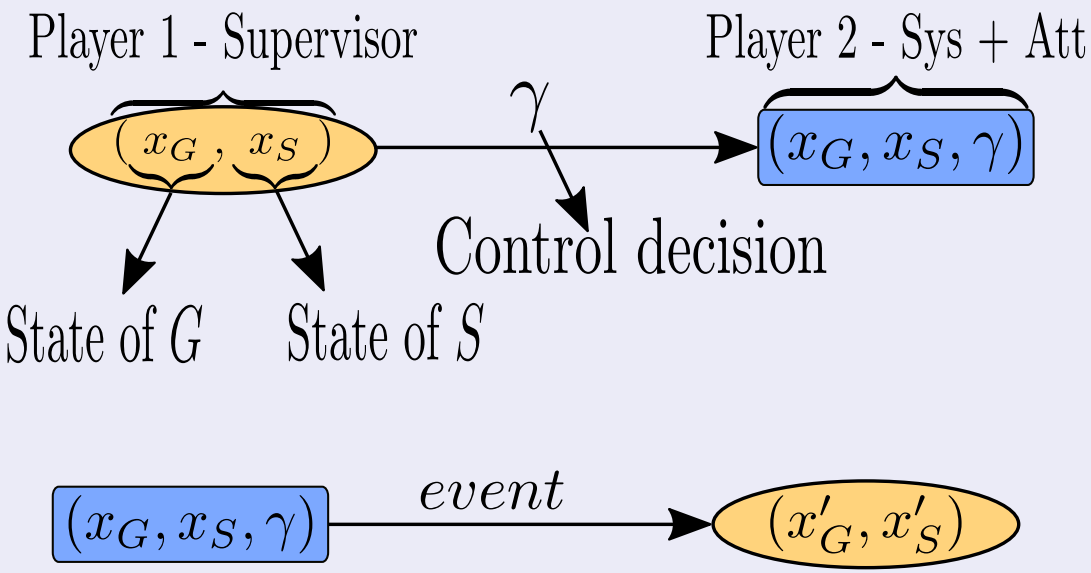
Arena $\mathcal{A}$



Solution approach: Graph games

Information and Definition

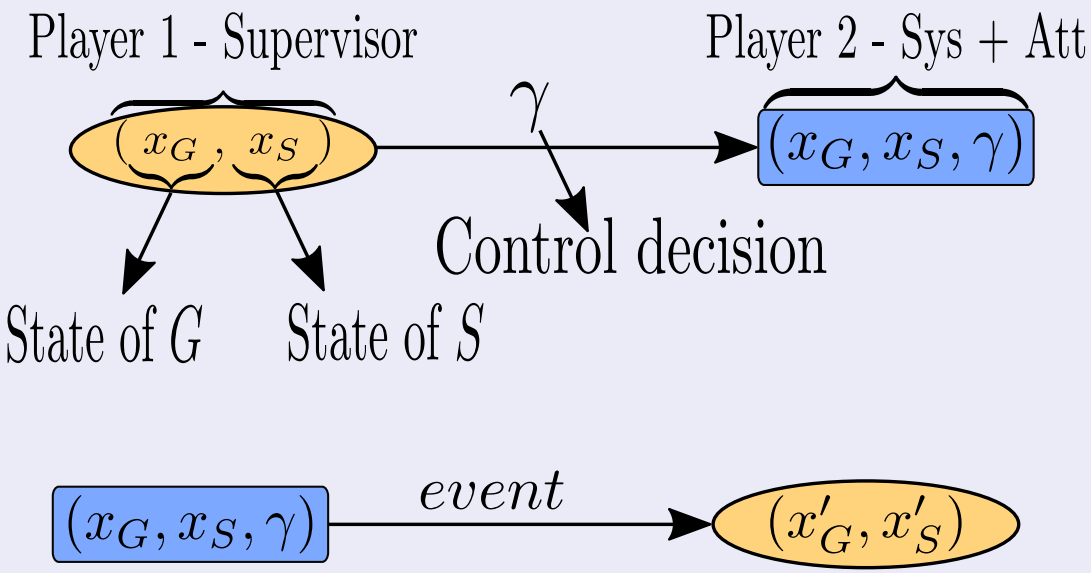
Arena $\mathcal{A}$



Solution approach: Graph games

Information and Definition

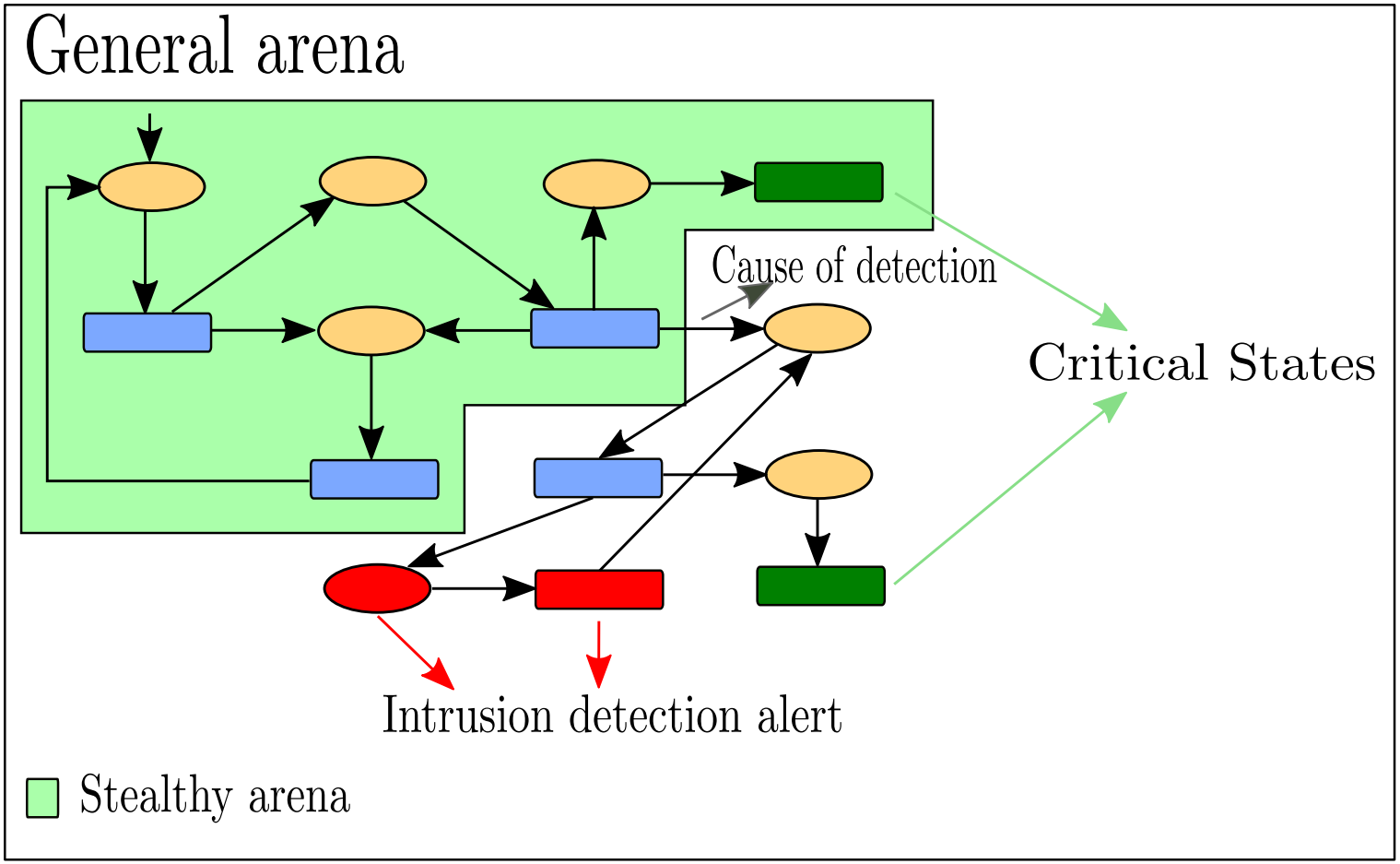
Arena $\mathcal{A}$



Construction and Pruning of Game Arena

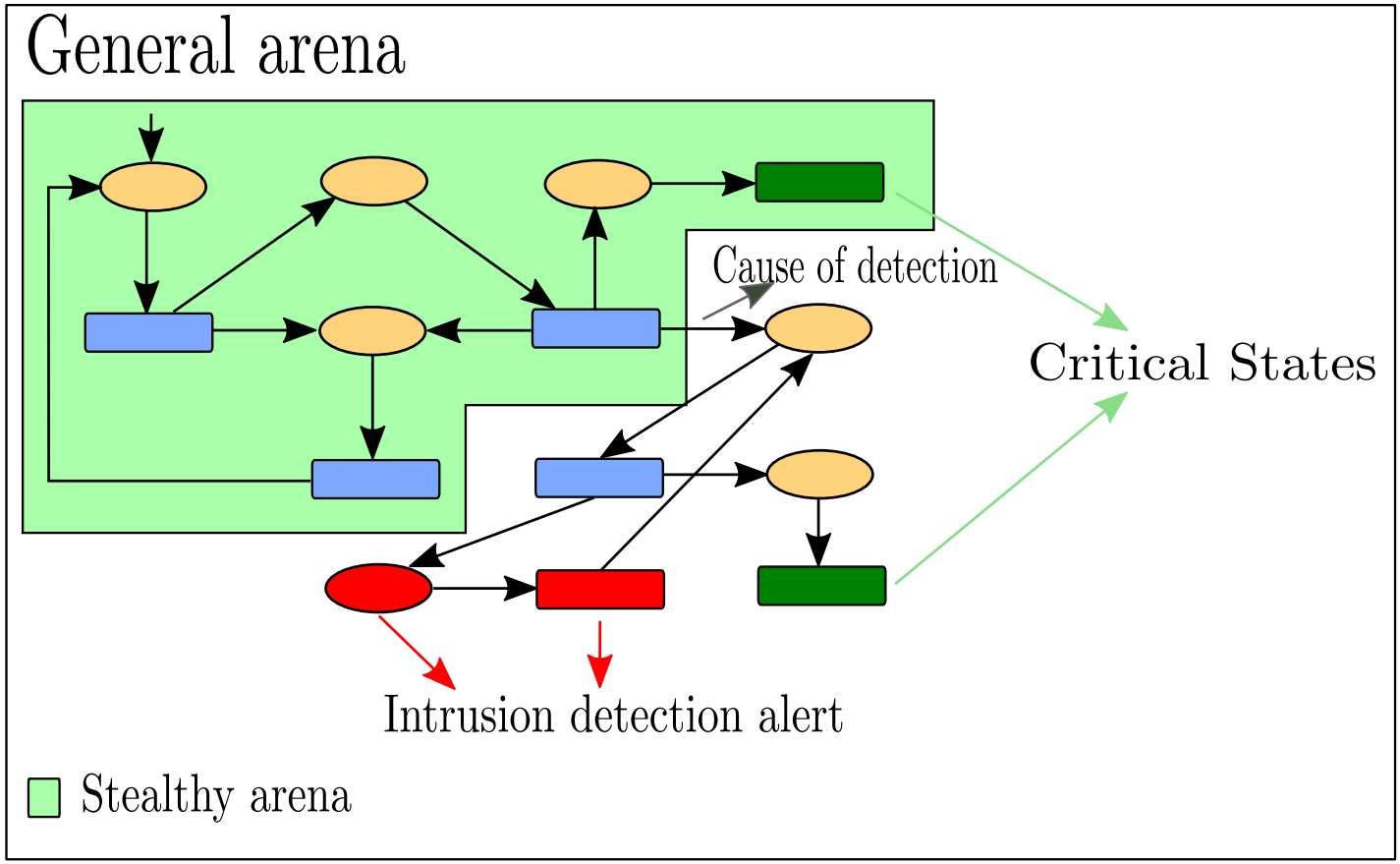
- BFS from y_0
- Prune non-stealthy attack strategies

Solution approach: Graph games pruning (iterative)



This can be formulated as *customized* computation of Supremal Controllable Sublanguage in SCT!

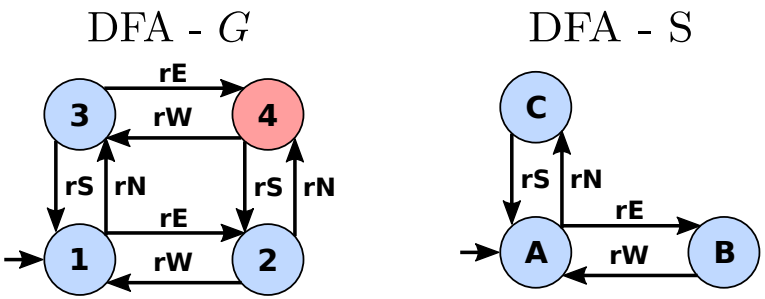
Solution approach: Graph games



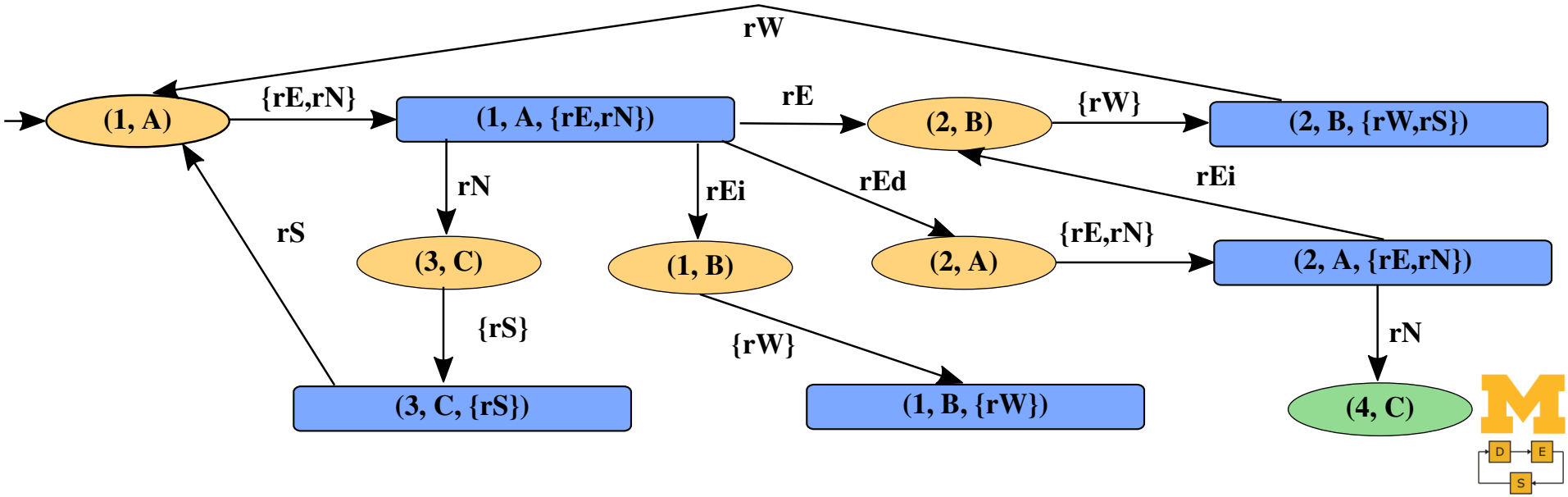
Theorem

- There exists an attack strategy if and only if there exists a critical state in the stealthy arena

Example



Compromised event set $\Sigma_a = \{rE\}$

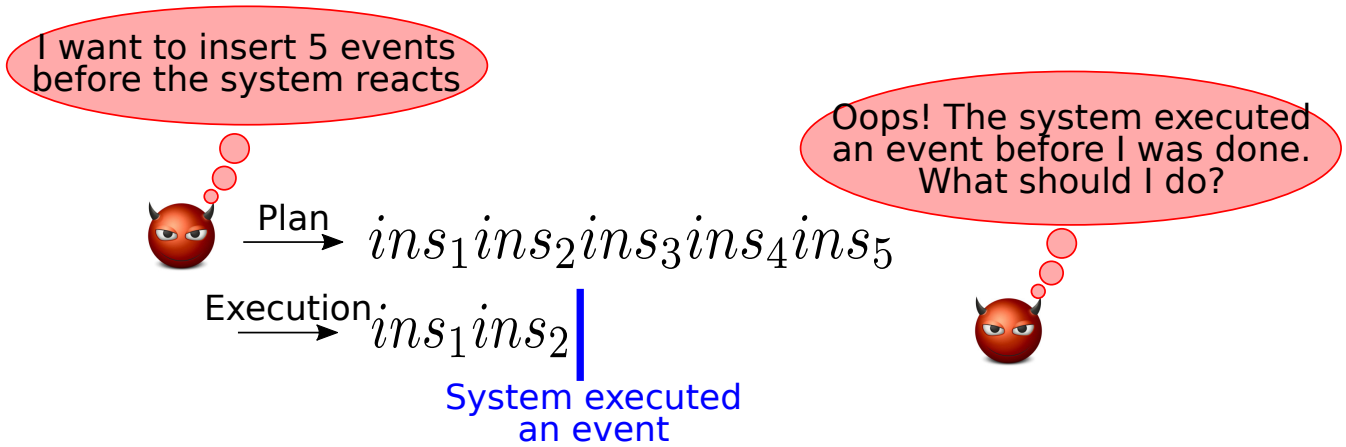


Synthesis of attack functions

- Logical constraints:
  - Deterministic
  - Bounded
  - Interruptability

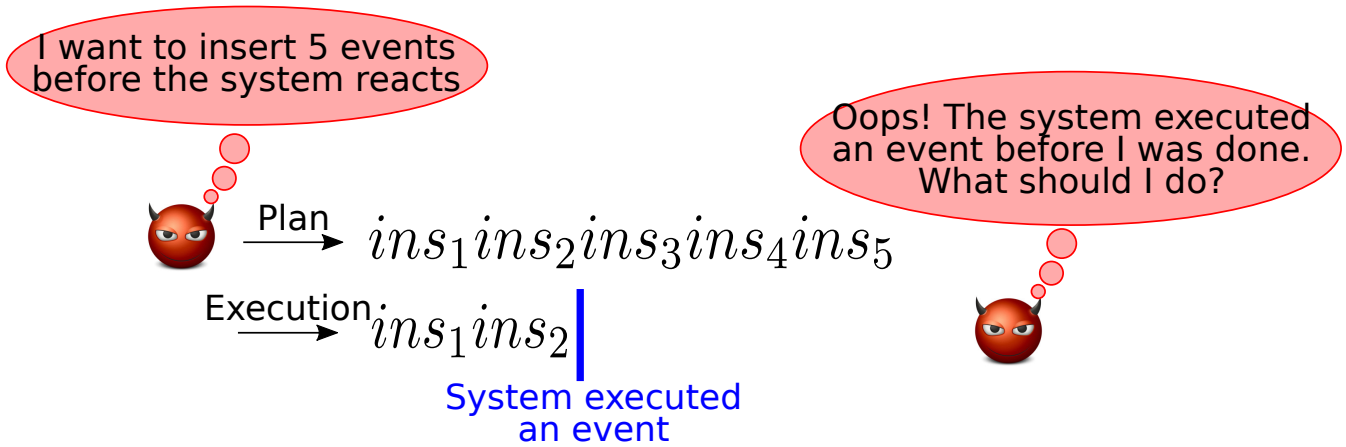
Synthesis of attack functions

- Logical constraints:
  - Deterministic
  - Bounded
  - Interruptability



Synthesis of attack functions

- Logical constraints:
  - Deterministic
  - Bounded
  - Interruptability

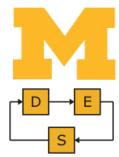


$\rightarrow$ Handled by customizing *construction* and *pruning* of game arena

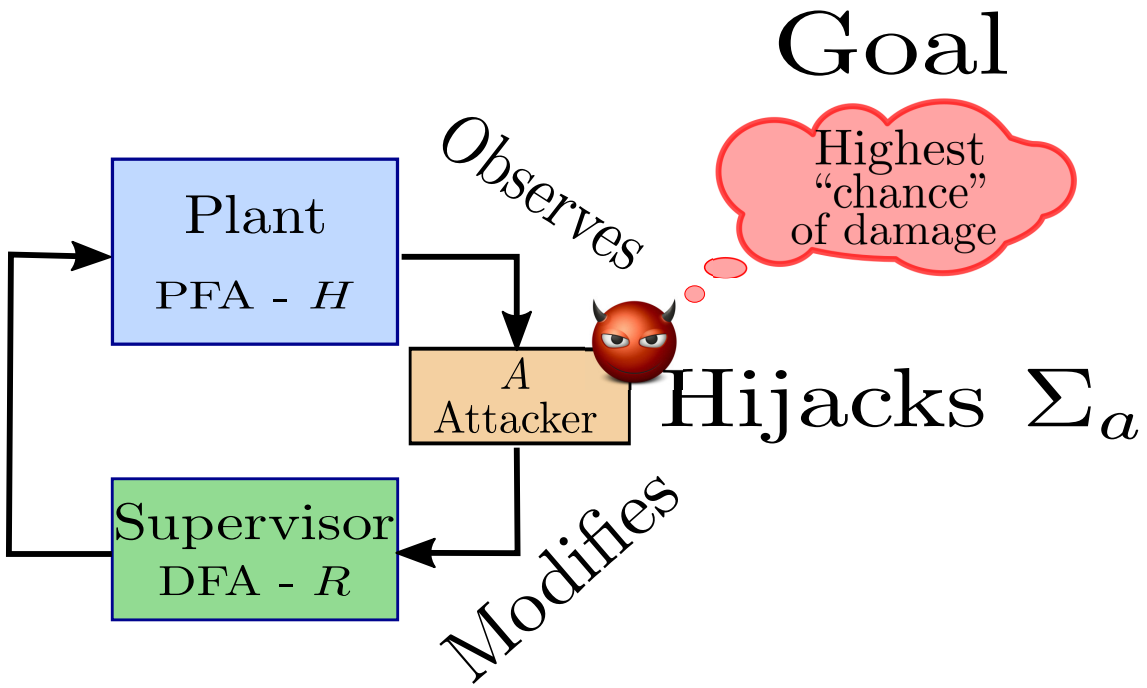
- Synthesis of attack function: based on paths to critical states in pruned arena

Problem variations

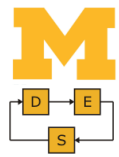
- Stochastic attack synthesis
- Partial observation case



Variation 1: Stochastic system

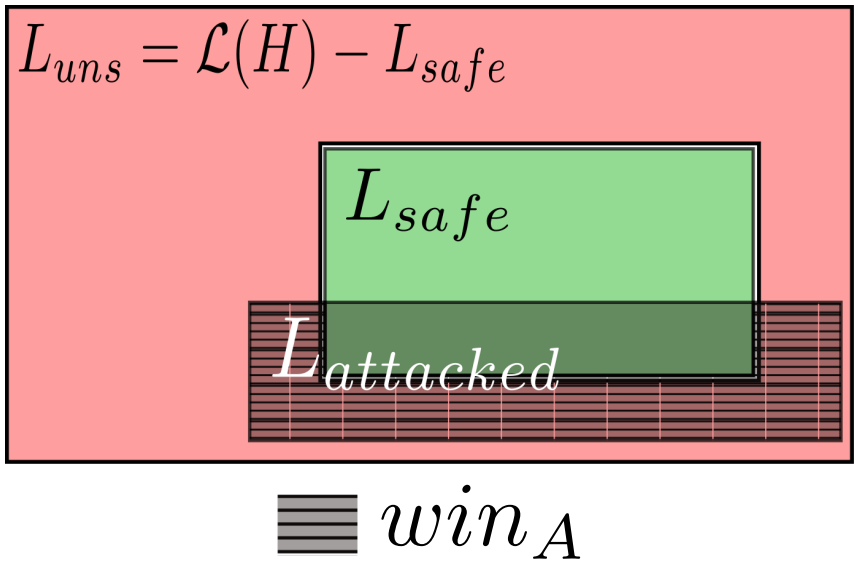


1. Maximize likelihood of damage (first hitting time)
2. Solution via 1-$\frac{1}{2}$ turn-based reachability stochastic game (MDP)
3. LP solution methodology from literature



Optimal Sensor Deception Attacks - Intuition

Suppose we have an attack strategy:



win_A - probability of reaching X_{crit} using attack function A

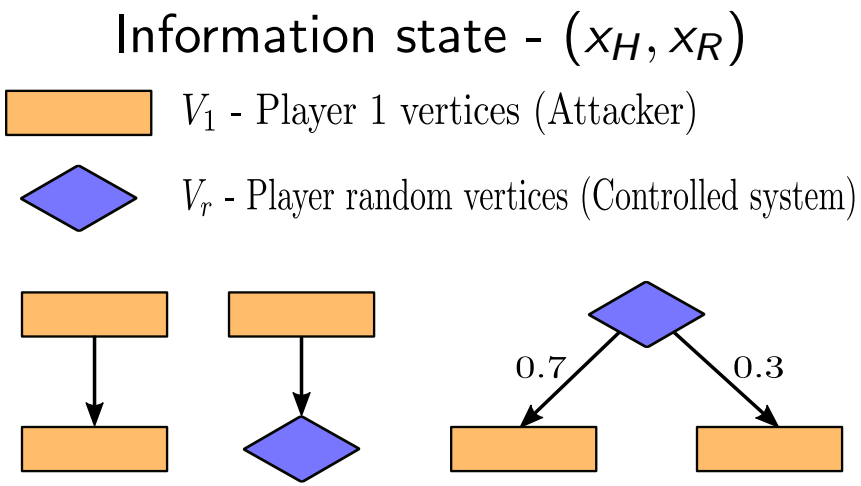
Stochastic system

Optimal Attack Function Synthesis Problem

Given the PFA H, a DFA R and $\Sigma_a \subseteq \Sigma$, **synthesize** $\mathbf{A}^*$, if one exists, s.t. $\forall A$:

$$\mathbf{win}_{\mathbf{A}^*} \geq \mathbf{win}_{\mathbf{A}} \tag{1}$$

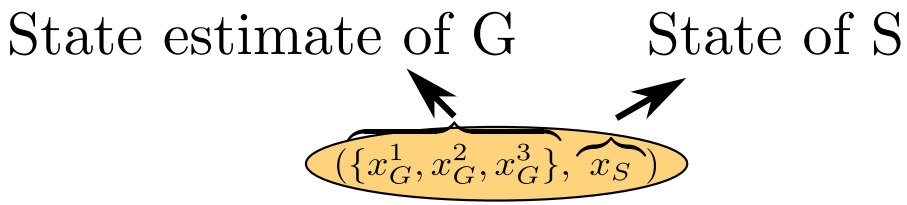
Solution via **1 and** $\frac{1}{2}$ **turn-based stochastic reachability game**[1] (Condon 1992)



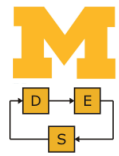
[1] Equivalent to MDP

Variation 2: System with partial observation

1. Same formulation as full observation case
2. $\Sigma_a \subseteq \Sigma_o$
3. State estimates



4. Two types of attack conditions:
   - Strong Attack:{Crit,Crit,Crit}
   - Weak Attack: {Good,Crit,Good}

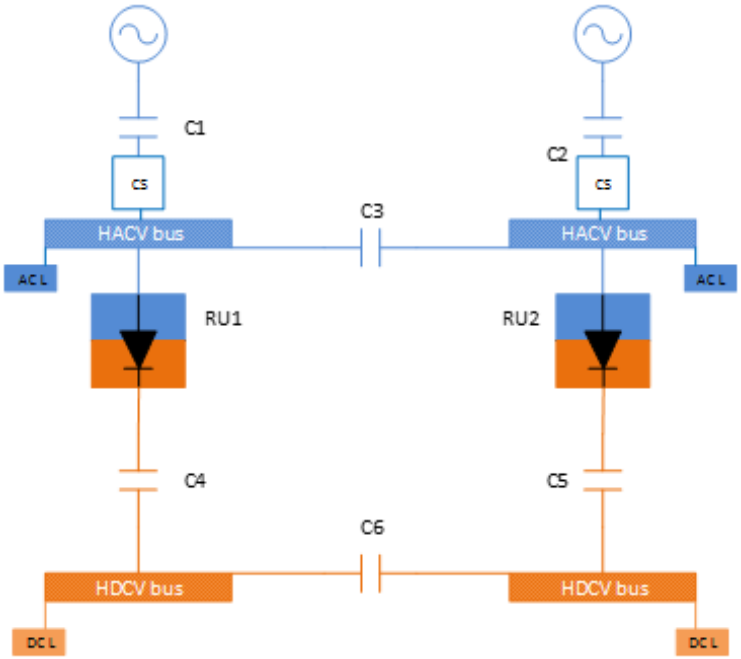


Application – Water treatment testbed


- Secure Water Treatment (SWaT) system[a] (*SWaT: Secure Water Treatment Testbed, 2015*; Kang et al. 2016)
- Scaled-down version of an industrial system
- Modeling: part of the plant
- Feasible sensor deception stealthy attack found

[a] Located at Singapore University of Technology and Design (SUTD)

Application – Aircraft power distribution system testbed

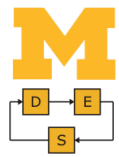


- Scaled-down version of an industrial system in Necmiye Ozay's lab at UMich (Benjumea 2015)
- Feasible sensor deception stealthy attack found

Conclusion - Part 1

Contribution

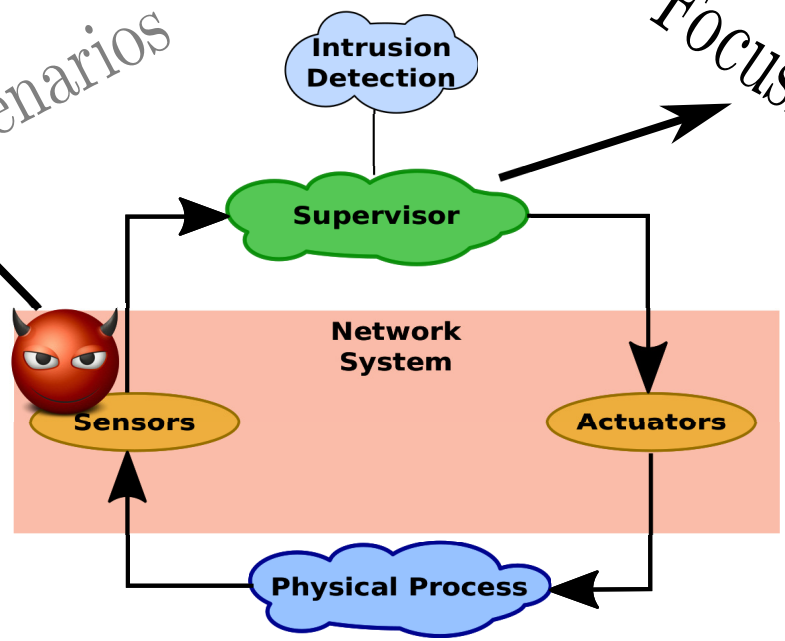
- Attacker's perspective
- Modeling an attacker as edit function for sensor reading modification
- Use of graph games techniques
  - Game arena states must be *information states*
- Existence and synthesis of two different types of attacks (strong/weak)
- Investigated different attack scenarios
- Optimal attack synthesis in context of probabilistic model



Overview of presentation

Part 1 - Focusing on the attacker
a) Basic scenario
b) Generalized scenarios

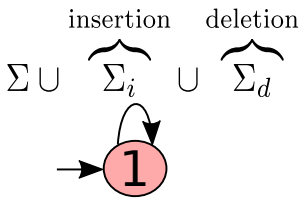
Part 2 - Focusing on the supervisor



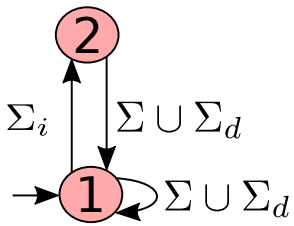
Attack function

Attack function with $\Sigma_a \subseteq \Sigma$ are encoded as a DFA A

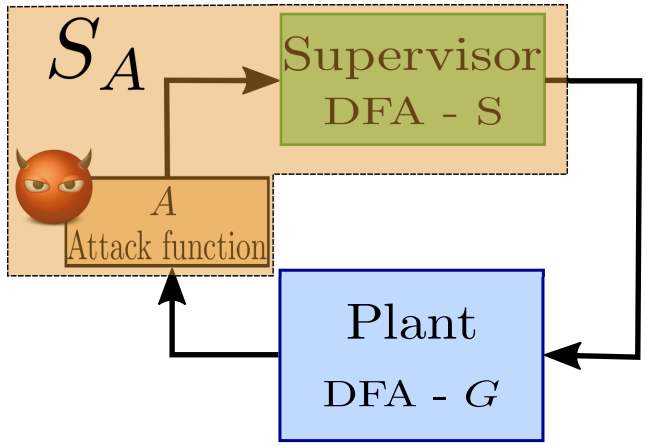
- All-out attack
- Prior knowledge, e.g., bounded, replacement, etc.



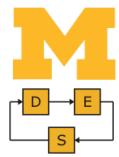
all-out



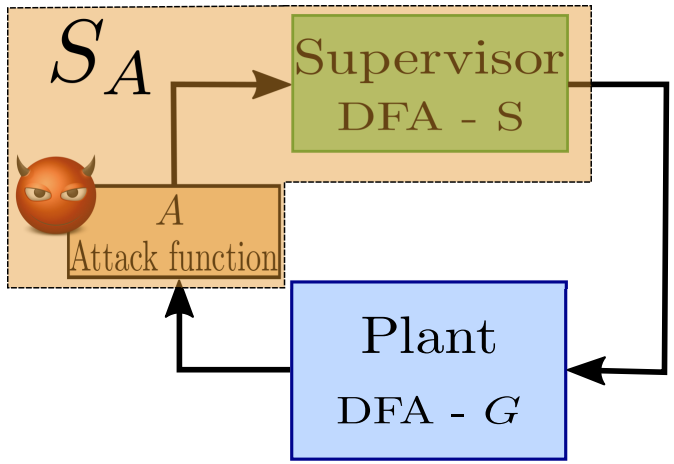
bounded insertion

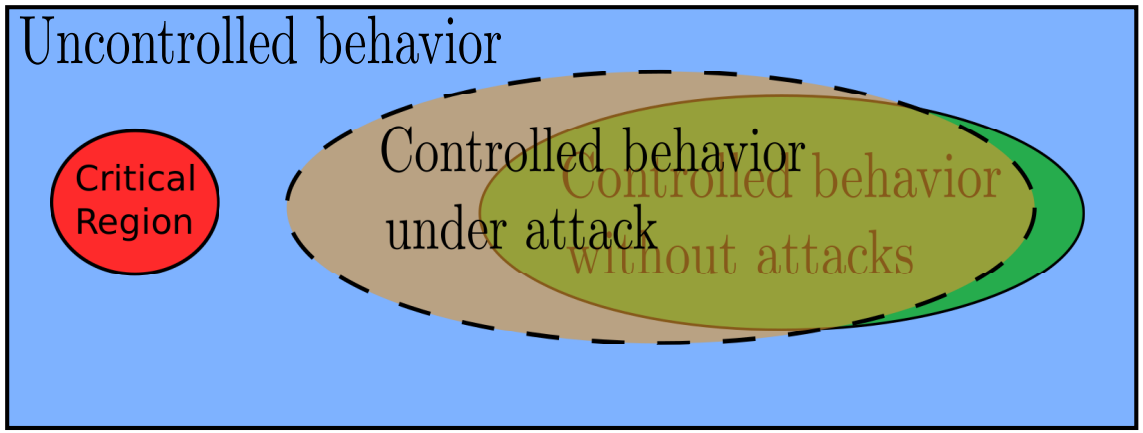


$\rightarrow$ Here, S is not fixed by must be synthesized



Influence of A on controlled system

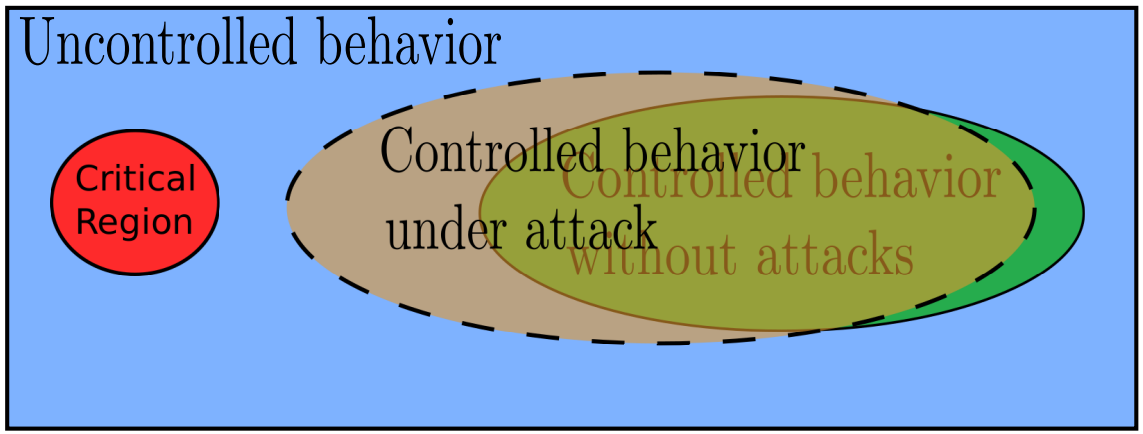




Synthesis of supervisors robust against sensor deception attacks

Synthesis of Supervisors

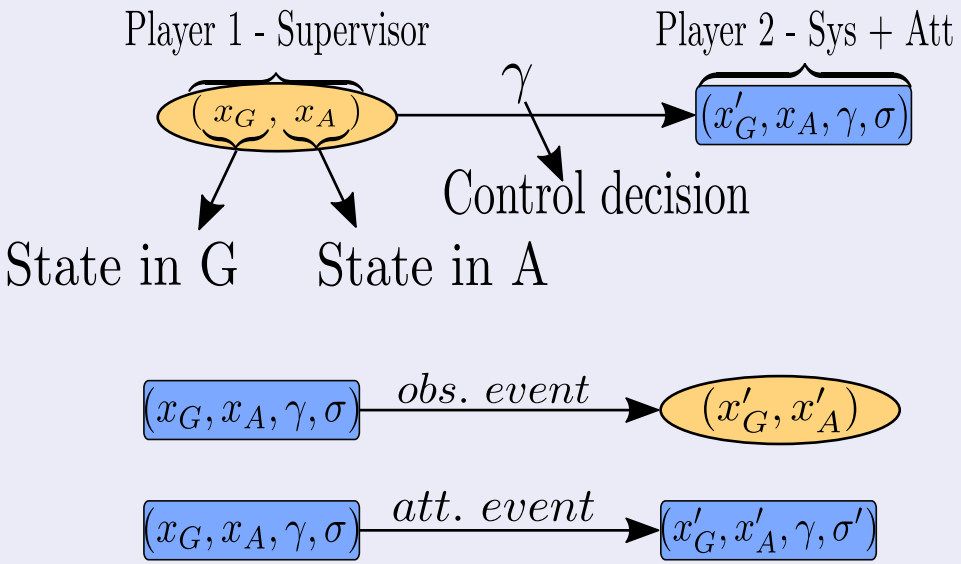
Given G, X_{crit} and A, synthesize a supervisor S such that it guarantees that S_A/G is safe.



Solution approach – Graph games

Definition

Arena $\mathcal{A}$ w.r.t to G, Σ_a is:

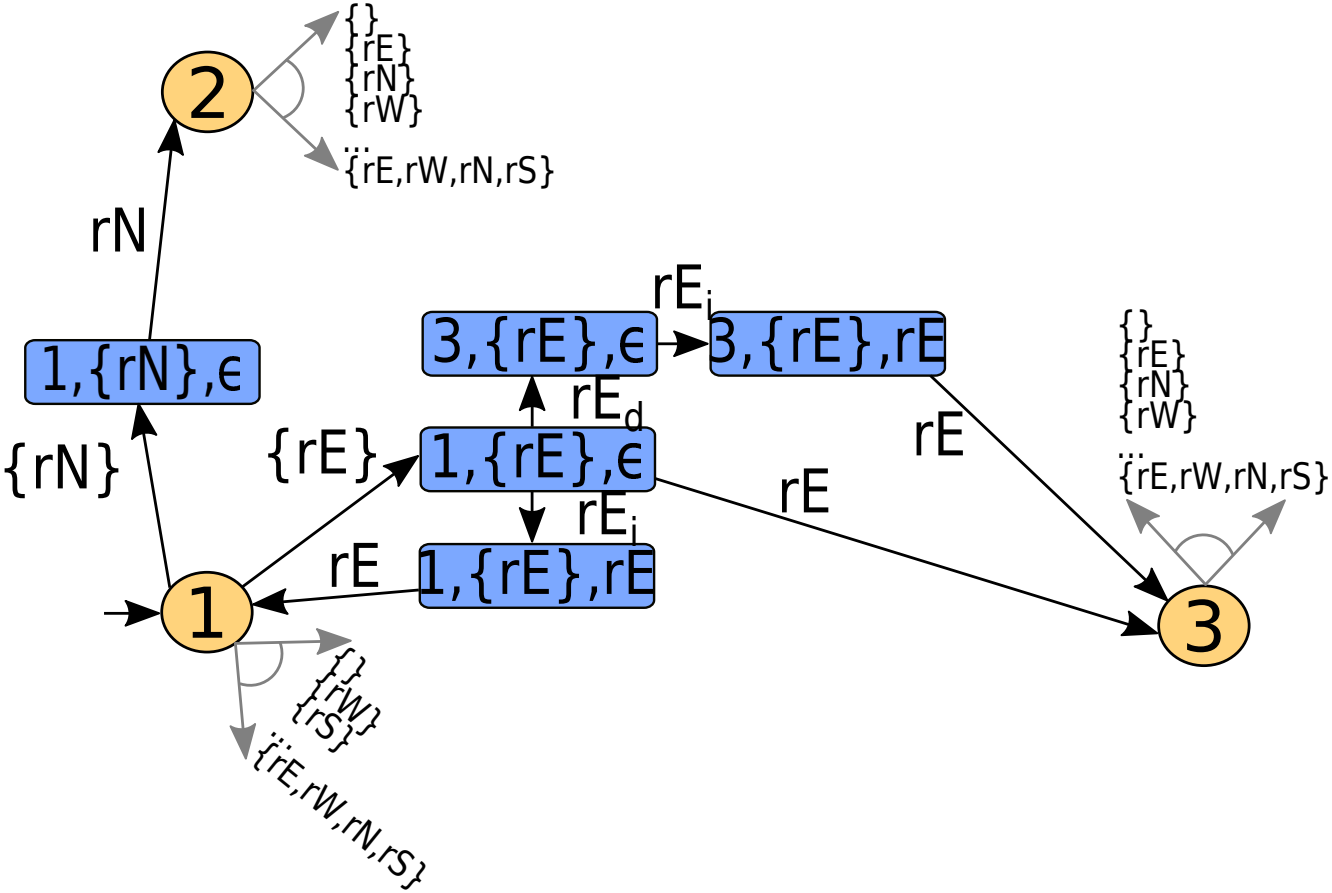


Comparison with previous game

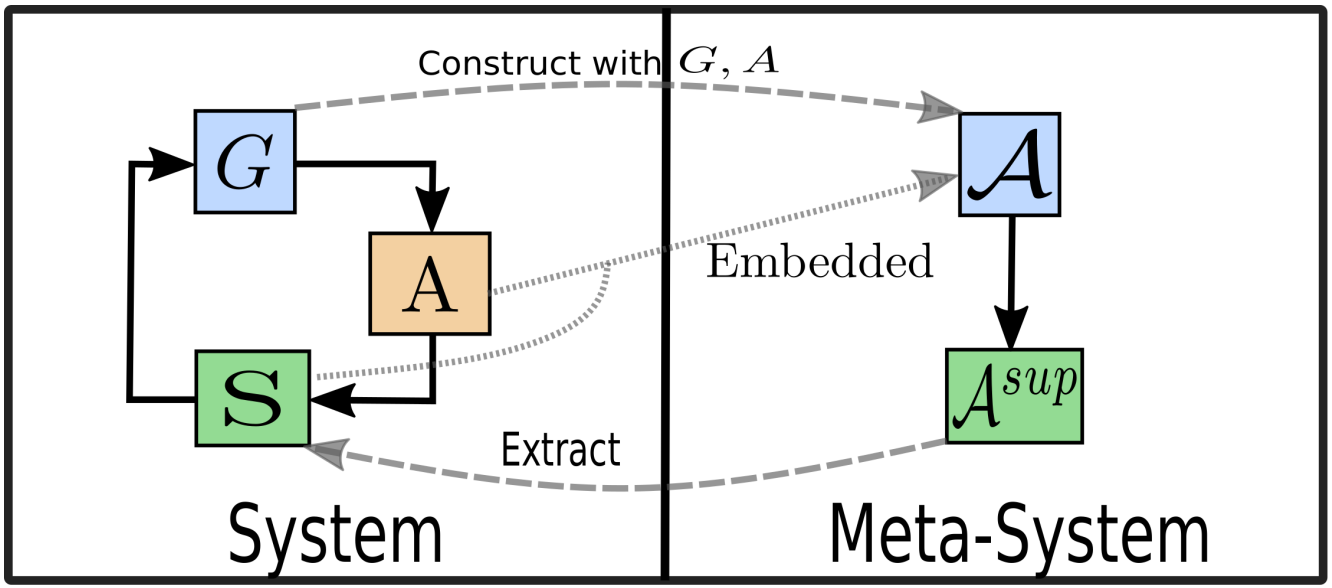
- Player 1 has actions
- Game is a partial information game (actions of attacker are not *observable*)

Example – Robot in a grid

Compromised event set: $\Sigma_a = \{rE\}$ - all-out attack

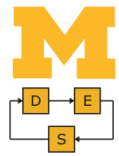


Meta-system

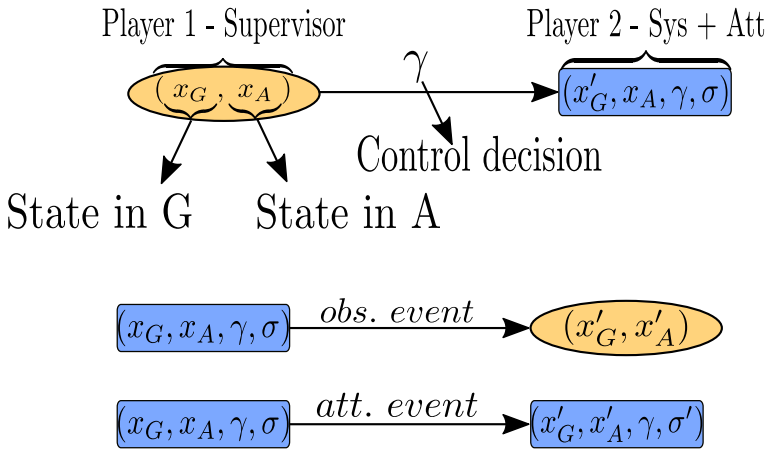


- Meta-system space has all possible supervisors of original control problem
- Pruning - Partially observed supervisory control problem
- Pruning - Partial information safety games

Theorem: All robust supervisors are embedded in $\mathcal{A}^{sup}$

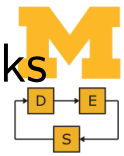


Meta-system



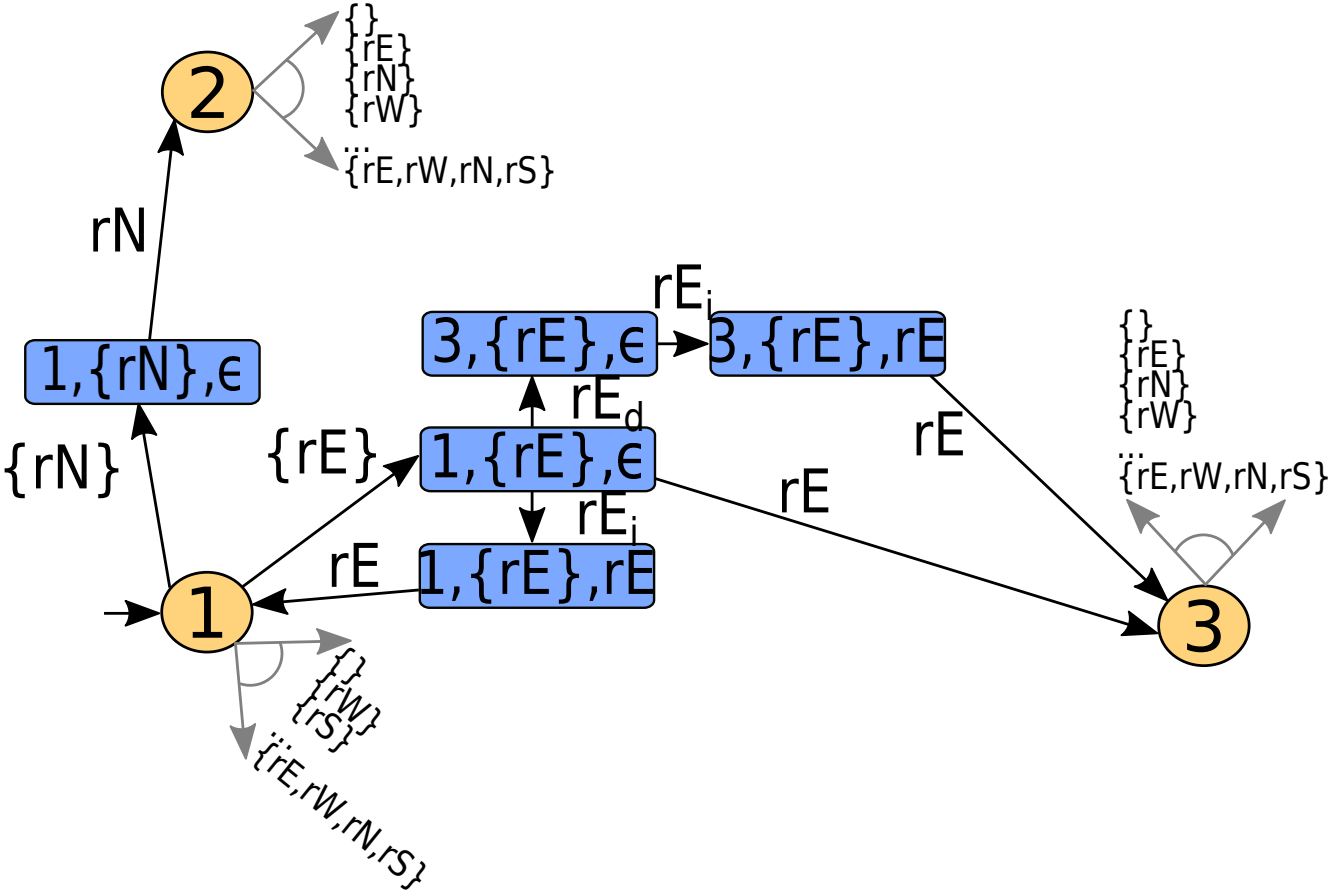
Some more details about solving (pruning) meta-system:

- Solve using SCT
- Arena is uncontrolled system: partially observed
- Specification involves safety
- All controllable events are observable
  - Supremal controllable and normal sublanguage is optimal solution
- That solutions embeds all supervisors that are robust against sensor attacks



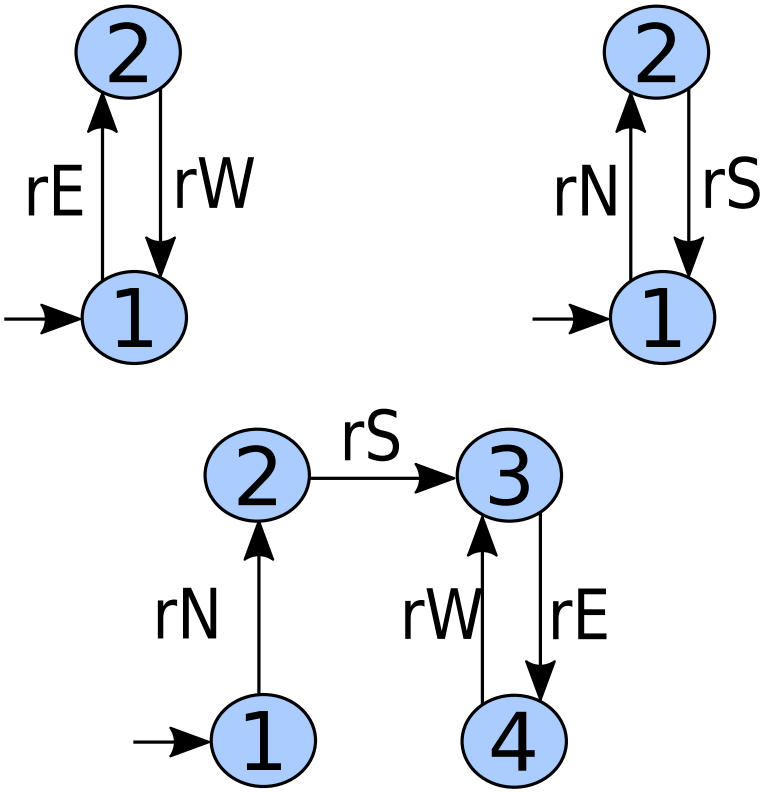
Example – Robot in a grid

Compromised event set: $\Sigma_a = \{rE\}$ - all-out attack

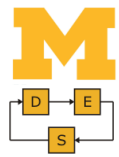


Example – Robust supervisors

Compromised event set: $\Sigma_a = \{rE\}$ - all-out attack

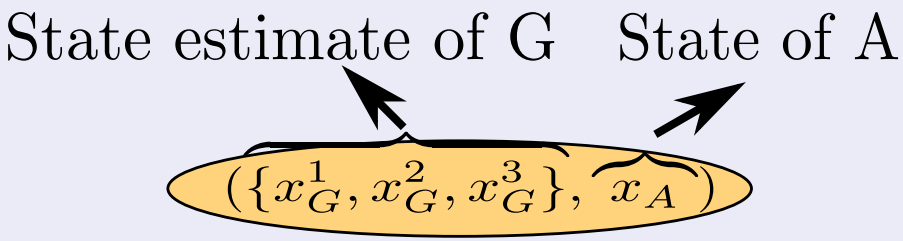


Note: Supervisor *ignores* [controllable] events not defined at its state (attacker not stealthy)

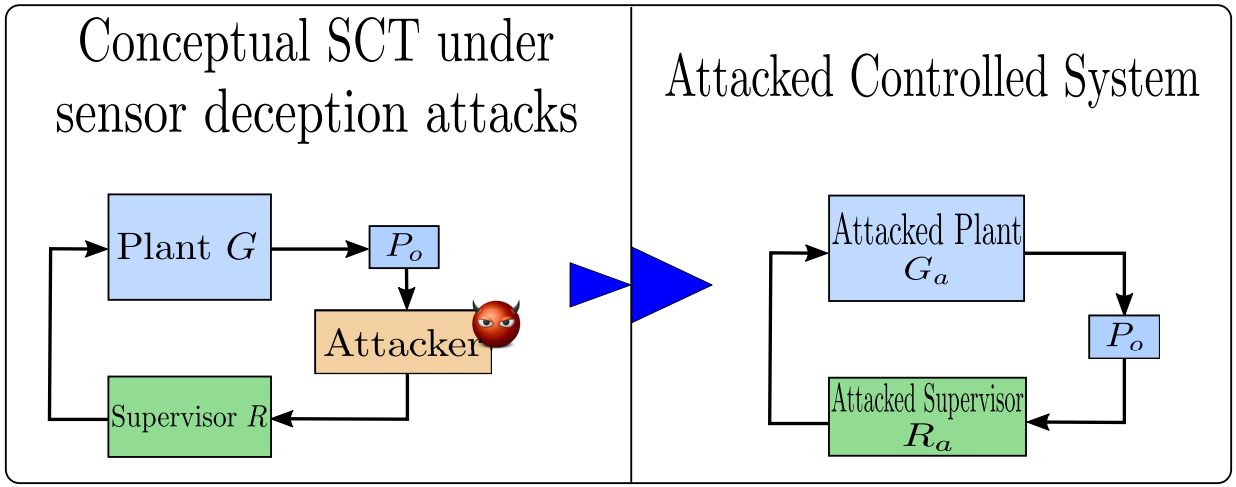


Extension

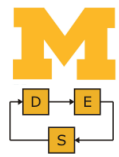
- Partially observed system: state estimates



Alternative approach: Robust supervisor via supervisory control theory (directly)



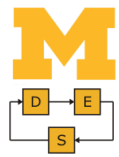
- Same problem formulation
- Attacked Controlled System embeds attack information
- Supervisory control theory with *arbitrary control patterns*
  $\rightarrow$ insertion and deletion events coupled with their legitimate counterpart
- No optimal solution here: maximal controllable and observable sublanguage(s)
  $\rightarrow$ adapted VLP-PO algorithm (has nice properties)
- Sound and Complete – but does *not* embed all solutions, as $\mathcal{A}^{sup}$ does
- Single exponential time complexity – even for partially observed system



Conclusion - Part 2

Contribution

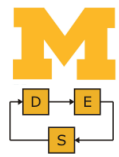
- Robust supervisors against sensor deception attacks
- Blending techniques from graph games with SCT
- Two methods to solve problem



Conclusion and Future Work

Conclusion

- Cyber-security with systems modeled as DES
- Sensor deception attacks from both perspectives: *attacker* and *defender*
- Use of graph games techniques blended with SCT

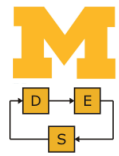


Conclusion and Future Work

Conclusion

- Cyber-security with systems modeled as DES
- Sensor deception attacks from both perspectives: *attacker* and *defender*
- Use of graph games techniques blended with SCT

Next talk: Alternative methodology to solve similar problems



Conclusion and Future Work

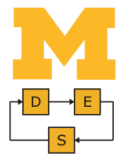
Conclusion

- Cyber-security with systems modeled as DES
- Sensor deception attacks from both perspectives: *attacker* and *defender*
- Use of graph games techniques blended with SCT

Next talk: Alternative methodology to solve similar problems

Future work

- Investigate case studies in CPS and in Cyber Control Systems
- Relax attacker assumptions
- Blend techniques of robust supervisors with intrusion detection modules
- Stochastic systems



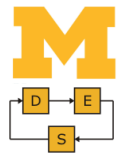
Selected papers

Journals

- **Meira-Góes et al. 2019**, *"Synthesis of Sensor Deception Attacks at the Supervisory Layer of Cyber-Physical Systems"*, conditionally accepted in Automatica
- **Meira-Góes, Lafortune, and Marchand 2019**, *"Synthesis of Supervisors Robust Against Sensor Deception Attacks"*, under review in IEEE Transactions on Automatic Control

Conferences

- **Meira-Góes, Marchand, and Lafortune 2019**, *"Stealthy deception attacks for cyber-physical systems"*, 2019 IEEE 58th Annual Conference on Decision and Control (CDC)
- **Meira-Góes, Kwong, and Lafortune 2019**, *"Synthesis of Sensor Deception Attacks for Systems Modeled as Probabilistic Automata"*, 2019 American Control Conference (ACC)
- **Meira-Góes et al. 2017**, *"Stealthy deception attacks for cyber-physical systems"*, 2017 IEEE 57th Annual Conference on Decision and Control (CDC)



References I

Benjumea, Mercedes Modet (2015). "Aircraft Electric Power System Testbed". MA thesis. Universidad Pontificia Comillas: Escuela Tecnica Superior de Ingeniaria.

Carvalho, Lilian Kawakami et al. (2018). "Detection and mitigation of classes of attacks in supervisory control systems". In: *Automatica* 97, pp. 121 –133.

Cassez, Franck, Jérémy Dubreil, and Hervé Marchand (2012). "Synthesis of opaque systems with static and dynamic masks". In: *Formal Methods in System Design* 40.1, pp. 88–115.

Condon, Anne (1992). "The complexity of stochastic games". In: *Information and Computation* 96.2, pp. 203 –224.

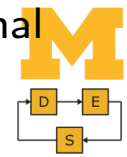
Dubreil, J., P. Darondeau, and H. Marchand (2010). "Supervisory control for opacity". In: *IEEE Transactions on Automatic Control* 55.5, pp. 1089–1100.

Jacob, Romain, Jean-Jacques Lesage, and Jean-Marc Faure (2016). "Overview of discrete event systems opacity: Models, validation, and quantification". In: *Annual Reviews in Control* 41, pp. 135–146.

Kang, Eunsuk et al. (2016). "Model-based security analysis of a water treatment system". In: *Proceedings of the 2nd International Workshop on Software Engineering for Smart Cyber-Physical Systems, SEsCPS@ICSE 2016, Austin, Texas, USA, May 14-22, 2016*, pp. 22–28.

Lima, Públio Macedo et al. (2019). "Security Against Communication Network Attacks of Cyber-Physical Systems". In: *Journal of Control, Automation and Electrical Systems* 30.1, pp. 125–135.

Lin, L. et al. (2019). "Synthesis of Supremal Successful Normal Actuator Attackers on Normal Supervisors". In: *2019 American Control Conference (ACC)*, pp. 5614–5619.



References II

Meira-Góes, R., C. Keroglou, and S. Lafortune (2020). "Towards probabilistic intrusion detection in supervisory control of discrete event systems". In: *to appear 21st IFAC World Congress*.

Meira-Góes, R., R. Kwong, and S. Lafortune (2019). "Synthesis of Sensor Deception Attacks for Systems Modeled as Probabilistic Automata". In: *2019 American Control Conference (ACC)*.

Meira-Góes, R. and S. Lafortune (2020). "Moving Target Defense based on Switched Supervisory Control: A New Technique for Mitigating Sensor Deception Attacks". In: *to appear 15th IFAC Workshop on Discrete Event Systems WODES 2018*.

Meira-Góes, R., S. Lafortune, and H. Marchand (2019). "Synthesis of Supervisors Robust Against Sensor Deception Attacks". In: *under review at IEEE Transactions on Automatic Control*.

Meira-Góes, R., H. Marchand, and S. Lafortune (2019). "Stealthy deception attacks for cyber-physical systems". In: *2019 IEEE 58th Annual Conference on Decision and Control (CDC)*.

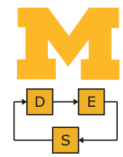
Meira-Góes, R. et al. (2017). "Stealthy deception attacks for cyber-physical systems". In: *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*, pp. 4224–4230.

– (2019). "Synthesis of Sensor Deception Attacks at the Supervisory Layer of Cyber-Physical Systems". In: *conditionally accepted in Automatica*.

Moor, Thomas (2016). "A discussion of fault-tolerant supervisory control in terms of formal languages". In: *Annual Reviews in Control* 41, pp. 159 –169.

SWaT: Secure Water Treatment Testbed, 2015. https://itrust.sutd.edu.sg/research/testbeds/secure-water-treatment-swat. Accessed: 2017-05-10.

Saboori, A. and C. N. Hadjicostis (2007). "Notions of security and opacity in discrete event systems". In: *46th IEEE Conference on Decision and Control*, pp. 5056–5061.



References III

Saboori, A. and C. N. Hadjicostis (2012). "Opacity-Enforcing Supervisory Strategies via State Estimator Constructions". In: *IEEE Transactions on Automatic Control* 57.5, pp. 1155–1165.

Su, Rong (2018). "Supervisor synthesis to thwart cyber attack with bounded sensor reading alterations". In: *Automatica* 94, pp. 35 –44.

Thorsley, D. and D. Teneketzis (2006). "Intrusion Detection in Controlled Discrete Event Systems". In: *Proceedings of the 45th IEEE Conference on Decision and Control*, pp. 6047–6054.

Wakaiki, Masashi, Paulo Tabuada, and João P. Hespanha (2018). "Supervisory Control of Discrete-Event Systems Under Attacks". In: *Dynamic Games and Applications*.

Wang, Y. and M. Pajic (2019a). "Attack-Resilient Supervisory Control with Intermittently Secure Communication". In: *2019 IEEE 58th Annual Conference on Decision and Control (CDC)*.

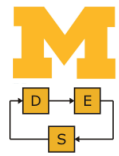
– (2019b). "Supervisory Control of Discrete Event Systems in the Presence of Sensor and Actuator Attacks". In: *2019 IEEE 58th Annual Conference on Decision and Control (CDC)*.

Wang, Z. et al. (2020). "Mitigation of Classes of Attacks using a Probabilistic Discrete Event System Framework". In: *to appear 15th IFAC Workshop on Discrete Event Systems WODES 2018*.

Wu, Yi-Chin et al. (2018). "Synthesis of Obfuscation Policies to Ensure Privacy and Utility". In: *Journal of Automated Reasoning* 60.1, pp. 107–131.

Zhang, Q. et al. (2018). "Stealthy Attacks for Partially-Observed Discrete Event Systems". In: *2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA)*. Vol. 1, pp. 1161–1164.

Zhu, Y., L. Lin, and R. Su (2019). "Supervisor Obfuscation Against Actuator Enablement Attack". In: *2019 18th European Control Conference (ECC)*, pp. 1760–1765.



Conclusion and Future Work

Conclusion

- Cyber-security with systems modeled as DES
- Sensor deception attacks from both perspectives: *attacker* and *defender*
- Use of graph games techniques blended with SCT

Future work

- Investigate case studies in CPS and in Cyber Control Systems
- Relax attacker assumptions
- Blend techniques of robust supervisor with intrusion detection modules
- Stochastic systems