Guaranteed Trade-Offs in Dynamic Information Flow Tracking Games

M. Weininger[1], K. Grover[1], S. Misra[2], J. Křetínský[1]

[1] Technical University of Munich, [2] University of Washington

ConVeY Retreat 2021

Outline

Motivating Example

Advanced Persistent Threats: An example

- In 2013, attack on Target Corporation's network.

Advanced Persistent Threats: An example

- In 2013, attack on Target Corporation's network.
- **40** million credit and debit cards.

Advanced Persistent Threats: An example

- In 2013, attack on Target Corporation's network.
- **40** million credit and debit cards.
- **70** million records of personal information.

Advanced Persistent Threats: An example

- In 2013, attack on Target Corporation's network.
- **40** million credit and debit cards.
- **70** million records of personal information.

How did they do it?

Advanced Persistent Threats: An example

- In 2013, attack on Target Corporation's network.
- **40** million credit and debit cards.
- **70** million records of personal information.

How did they do it?

- Entered in the system by compromising a third party vendor.

Advanced Persistent Threats: An example

- In 2013, attack on Target Corporation's network.
- **40** million credit and debit cards.
- **70** million records of personal information.

How did they do it?

- Entered in the system by compromising a third party vendor.
- Stayed there for 2 weeks.

Advanced Persistent Threats: An example

- In 2013, attack on Target Corporation's network.
- **40** million credit and debit cards.
- **70** million records of personal information.

How did they do it?

- Entered in the system by compromising a third party vendor.
- Stayed there for 2 weeks.

APTs: Gain illegitimate access to a system and remain there for a long time.

What can be done?

- Try to stop them from entering in the system.

What can be done?

- Try to stop them from entering in the system.
- Can we do something more?

What can be done?

- Try to stop them from entering in the system.
- Can we do something more?
- Add another layer of security to find the attacker if it's already in the system.

Problem formulation

Dynamic Information Flow Tracking

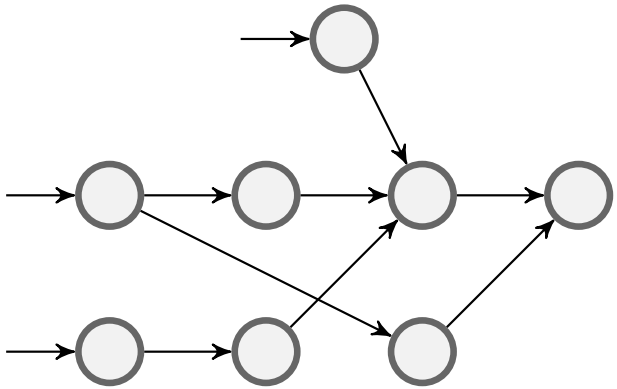
- APTs interaction with the system creates information flow.

Dynamic Information Flow Tracking

- APTs interaction with the system creates information flow.
- This results in an information flow graph.

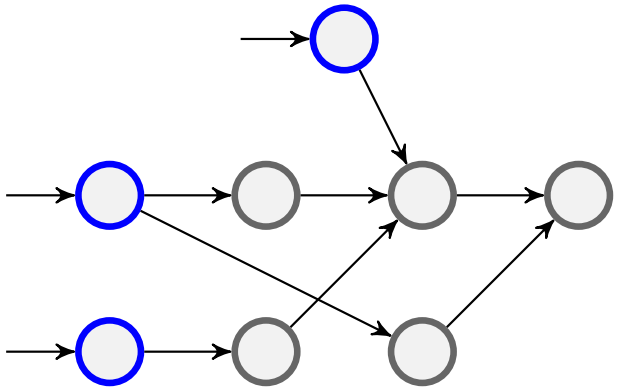
Dynamic Information Flow Tracking

- APTs interaction with the system creates information flow.
- This results in an information flow graph.



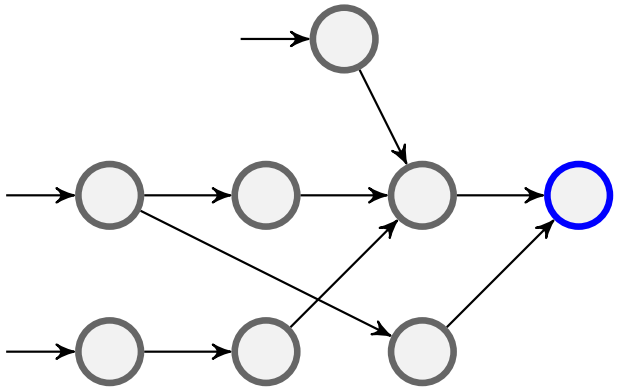
Dynamic Information Flow Tracking

- APTs interaction with the system creates information flow.
- This results in an information flow graph.



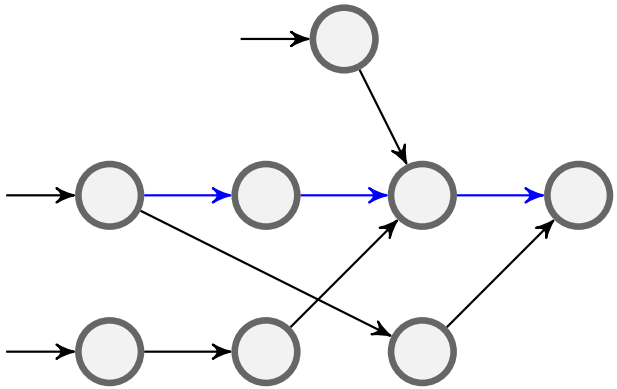
Dynamic Information Flow Tracking

- APTs interaction with the system creates information flow.
- This results in an information flow graph.



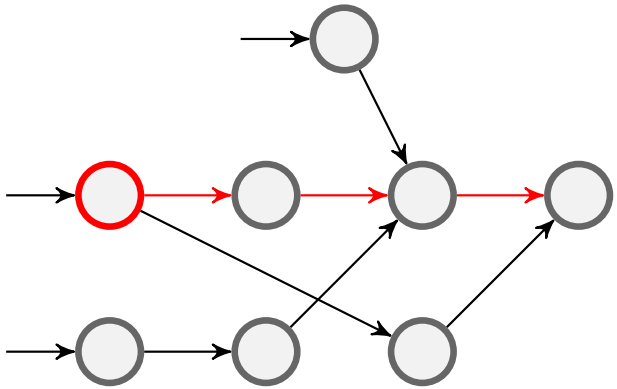
Dynamic Information Flow Tracking

- Try to find information flows which are APTs.



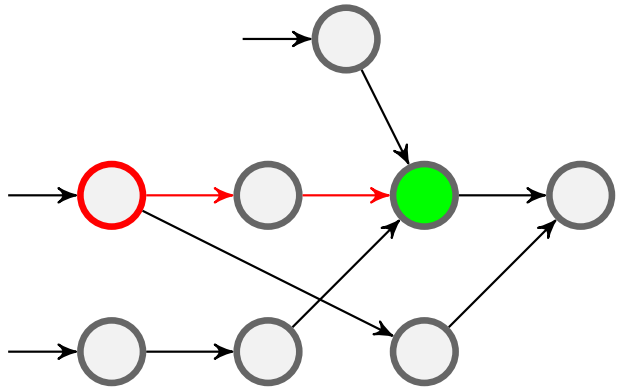
Dynamic Information Flow Tracking

- It operates by tagging "suspicious" data i/o channels.



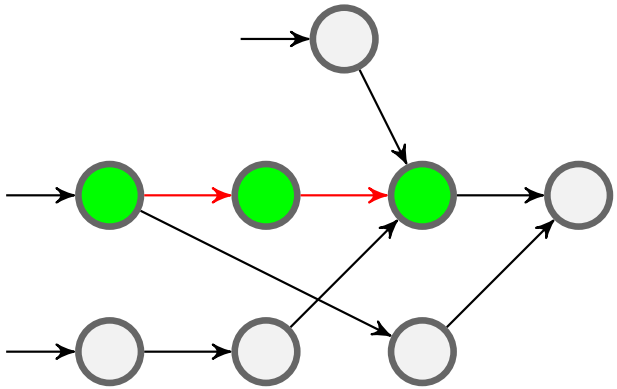
Dynamic Information Flow Tracking

- Perform security analysis on a node (a stochastic process).



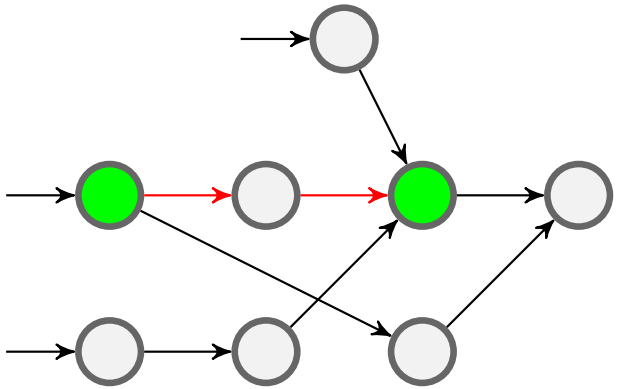
Dynamic Information Flow Tracking

- Tracking and analyzing information flow induces a memory and performance **cost** on the system.



Dynamic Information Flow Tracking

- It is critical to optimally select where to perform the security analysis.



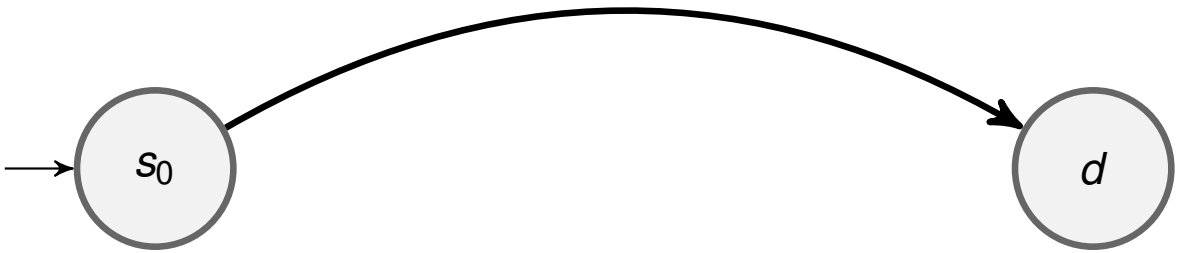
APT vs DIFT: A game

Model the interaction as a stochastic game on the information flow graph. [1]

[1] Shruti Misra, Shana Moothedath, Hossein Hosseini, Joey Allen, Linda Bushnell, Wenke Lee, and Radha Poovendran. Learning equilibria in stochastic information flow tracking games with partial knowledge. In CDC, pages 4053–4060. IEEE, 2019.

APT vs DIFT: A game

Model the interaction as a stochastic game on the information flow graph. [1]

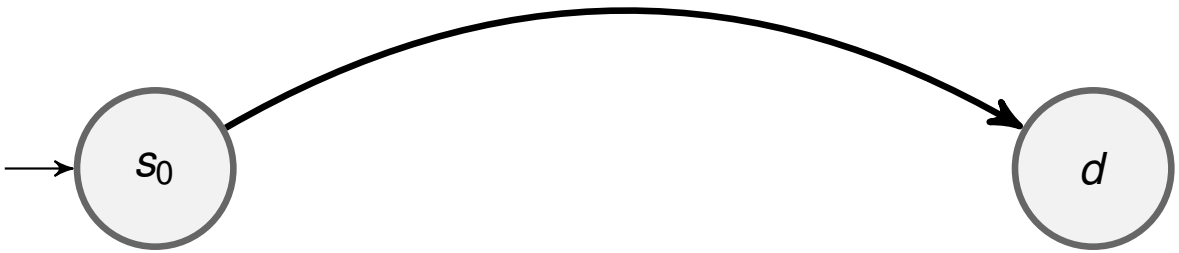


[1] Shruti Misra, Shana Moothedath, Hossein Hosseini, Joey Allen, Linda Bushnell, Wenke Lee, and Radha Poovendran. Learning equilibria in stochastic information flow tracking games with partial knowledge. In CDC, pages 4053–4060. IEEE, 2019.

APT vs DIFT: A game

Model the interaction as a stochastic game on the information flow graph. [1]

- Attacker: d (go to node d), ϕ (drop-out)
- Defender: 0 (don't trap), 1 (trap)

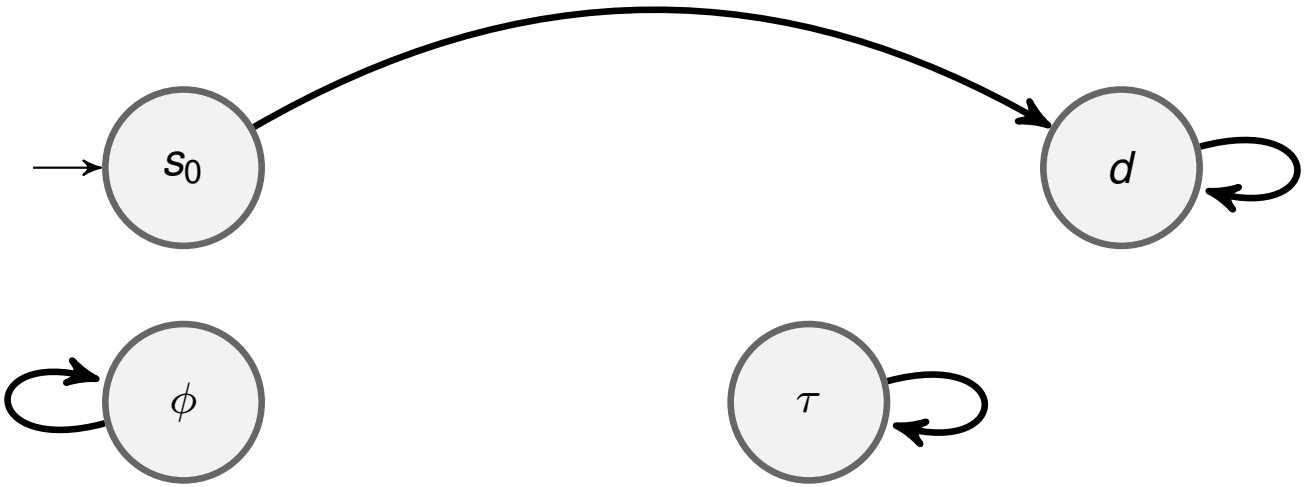


[1] Shruti Misra, Shana Moothedath, Hossein Hosseini, Joey Allen, Linda Bushnell, Wenke Lee, and Radha Poovendran. Learning equilibria in stochastic information flow tracking games with partial knowledge. In CDC, pages 4053–4060. IEEE, 2019.

APT vs DIFT: A game

Model the interaction as a stochastic game on the information flow graph. [1]

- Attacker: d (go to node d), ϕ (drop-out)
- Defender: 0 (don't trap), 1 (trap)

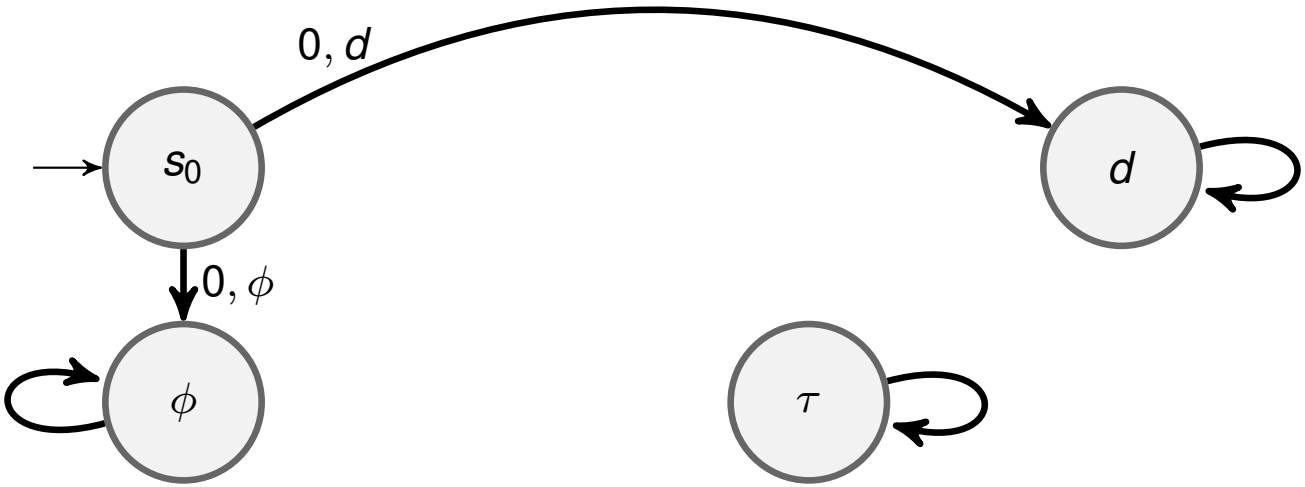


[1] Shruti Misra, Shana Moothedath, Hossein Hosseini, Joey Allen, Linda Bushnell, Wenke Lee, and Radha Poovendran. Learning equilibria in stochastic information flow tracking games with partial knowledge. In CDC, pages 4053–4060. IEEE, 2019.

APT vs DIFT: A game

Model the interaction as a stochastic game on the information flow graph. [1]

- Attacker: d (go to node d), ϕ (drop-out)
- Defender: 0 (don't trap), 1 (trap)

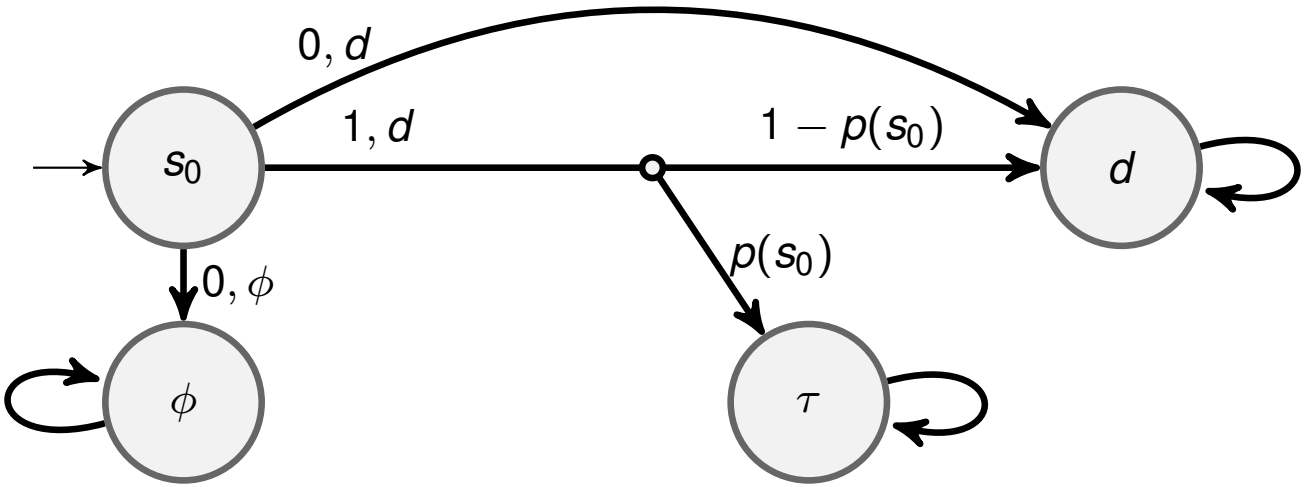


[1] Shruti Misra, Shana Moothedath, Hossein Hosseini, Joey Allen, Linda Bushnell, Wenke Lee, and Radha Poovendran. Learning equilibria in stochastic information flow tracking games with partial knowledge. In CDC, pages 4053–4060. IEEE, 2019.

APT vs DIFT: A game

Model the interaction as a stochastic game on the information flow graph. [1]

- Attacker: d (go to node d), ϕ (drop-out)
- Defender: 0 (don't trap), 1 (trap)

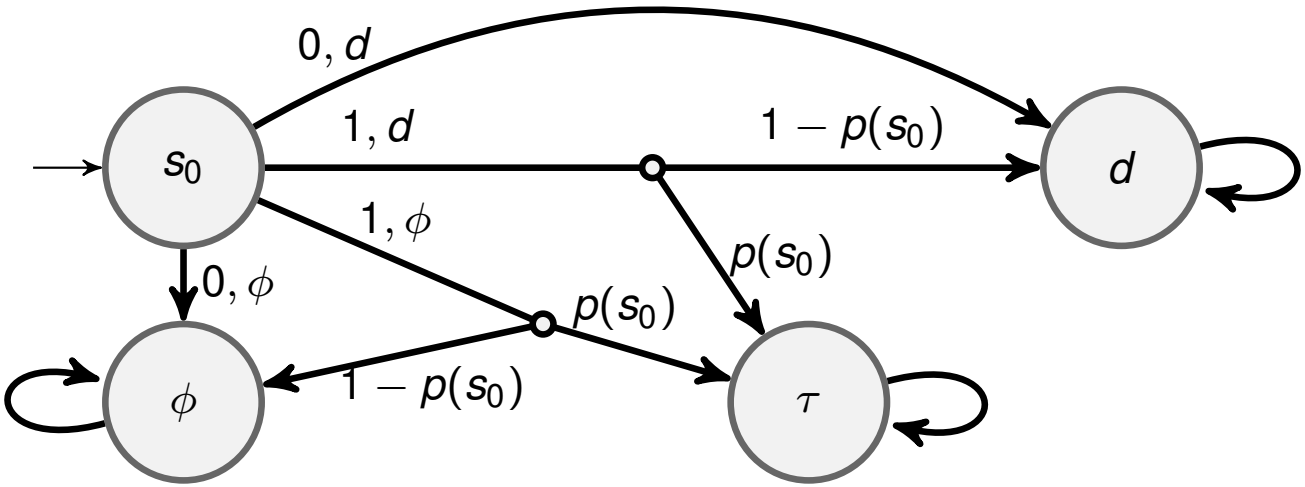


[1] Shruti Misra, Shana Moothedath, Hossein Hosseini, Joey Allen, Linda Bushnell, Wenke Lee, and Radha Poovendran. Learning equilibria in stochastic information flow tracking games with partial knowledge. In CDC, pages 4053–4060. IEEE, 2019.

APT vs DIFT: A game

Model the interaction as a stochastic game on the information flow graph. [1]

- Attacker: d (go to node d), ϕ (drop-out)
- Defender: 0 (don't trap), 1 (trap)

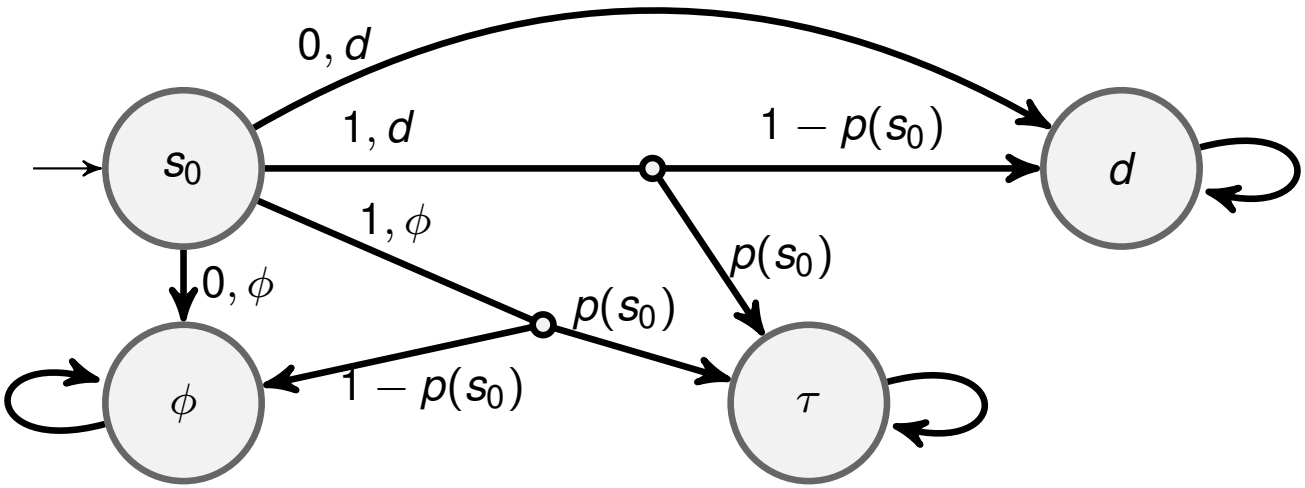


[1] Shruti Misra, Shana Moothedath, Hossein Hosseini, Joey Allen, Linda Bushnell, Wenke Lee, and Radha Poovendran. Learning equilibria in stochastic information flow tracking games with partial knowledge. In CDC, pages 4053–4060. IEEE, 2019.

APT vs DIFT: A game

Model the interaction as a stochastic game on the information flow graph. [1]

- Attacker: d (go to node d), ϕ (drop-out)
- Defender: 0 (don't trap), 1 (trap)

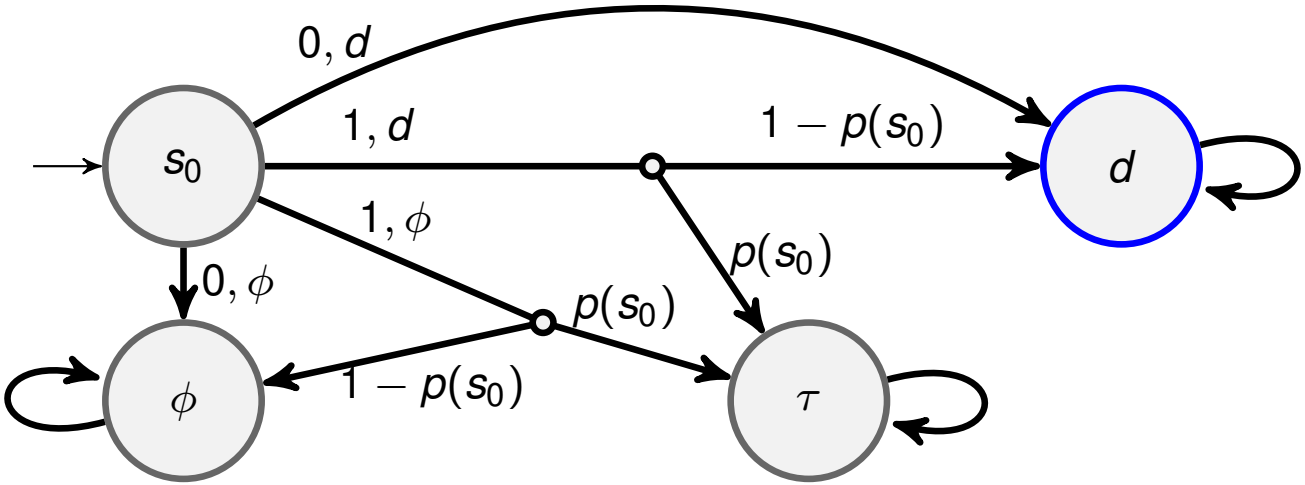


$p(s_0)$ is unknown.

[1] Shruti Misra, Shana Moothedath, Hossein Hosseini, Joey Allen, Linda Bushnell, Wenke Lee, and Radha Poovendran. Learning equilibria in stochastic information flow tracking games with partial knowledge. In CDC, pages 4053–4060. IEEE, 2019.

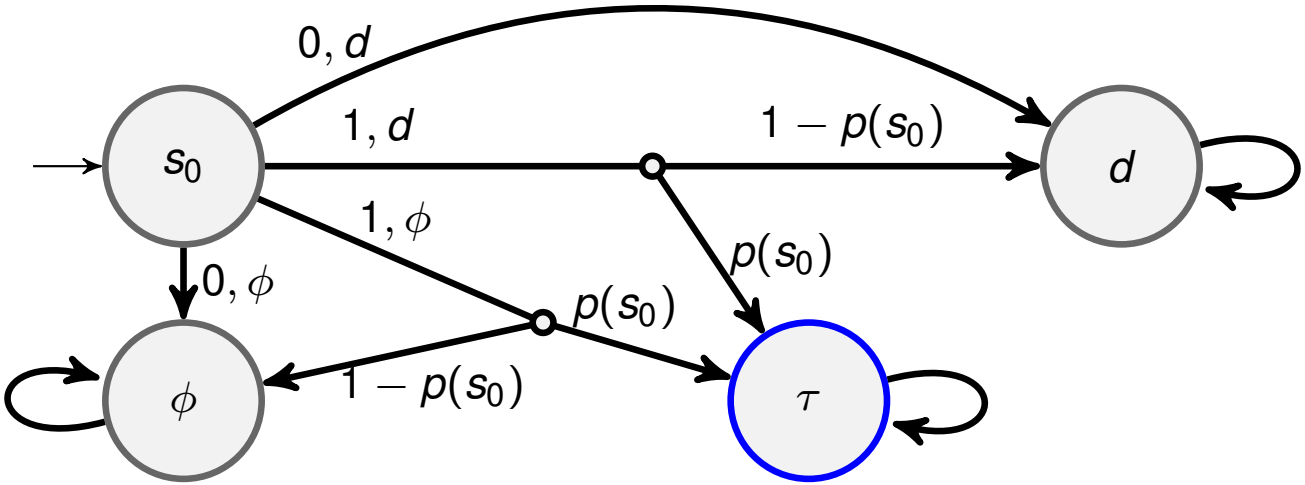
Objectives

- Minimize the probability of reaching the target.



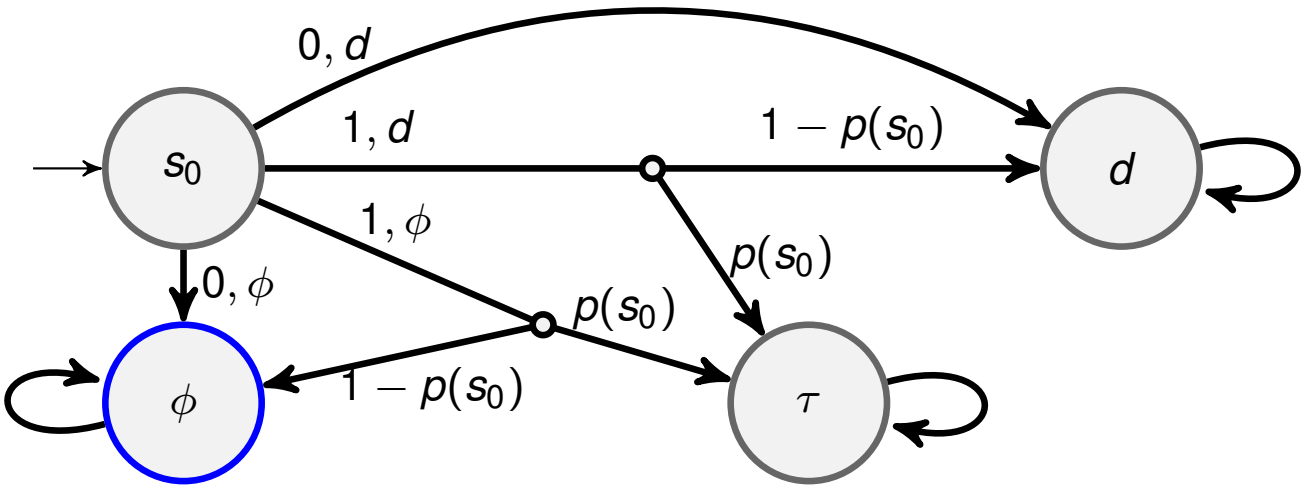
Objectives

- Minimize the probability of reaching the target.
- Maximize the probability of trapping.



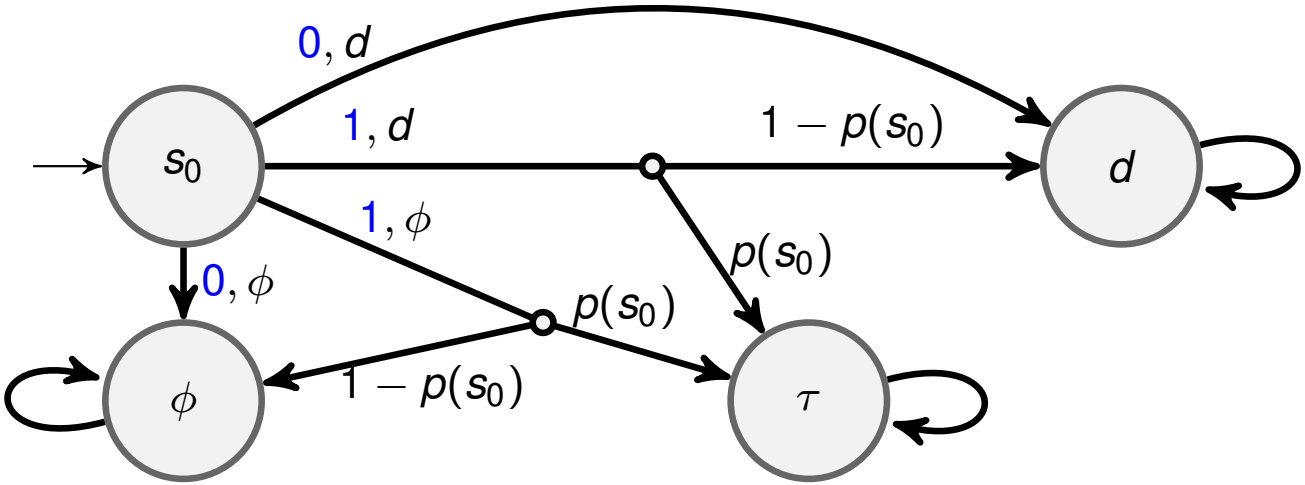
Objectives

- Minimize the probability of reaching the target.
- Maximize the probability of trapping.
- Maximize the probability of dropout.

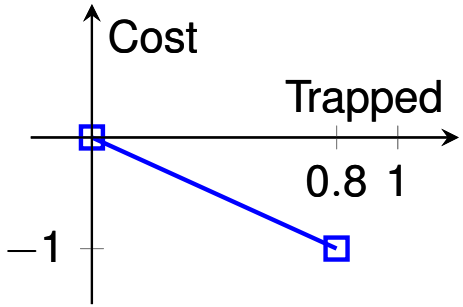


Objectives

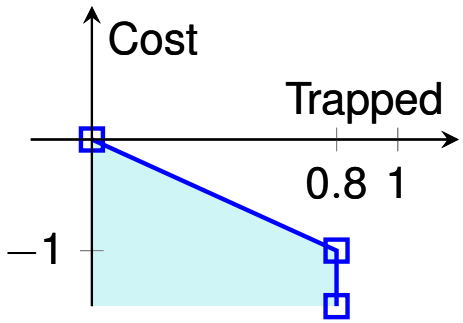
- Minimize the probability of reaching the target.
- Maximize the probability of trapping.
- Maximize the probability of dropout.
- Minimize cost.



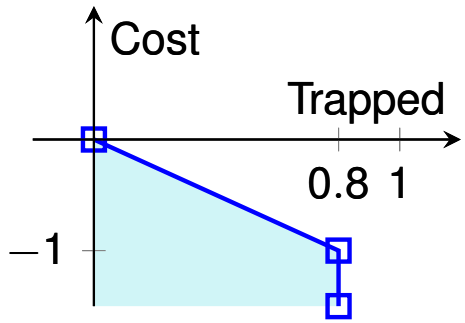
Trade-offs



Trade-offs



Trade-offs



Prism can compute these **Pareto frontiers** for turn-based games with known probabilities.

Our Solution

Turn-based Game

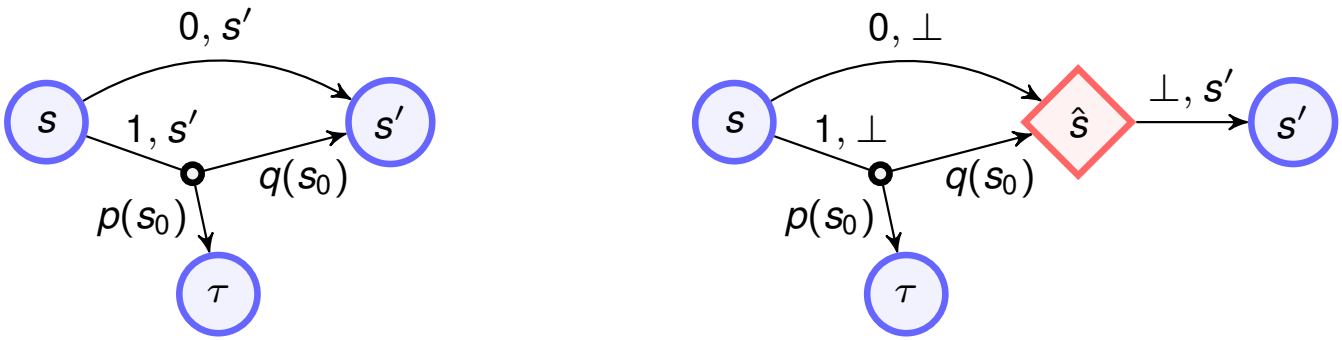
- This is a concurrent game.

Turn-based Game

- This is a concurrent game.
- We gave a transformation which makes it turn-based.

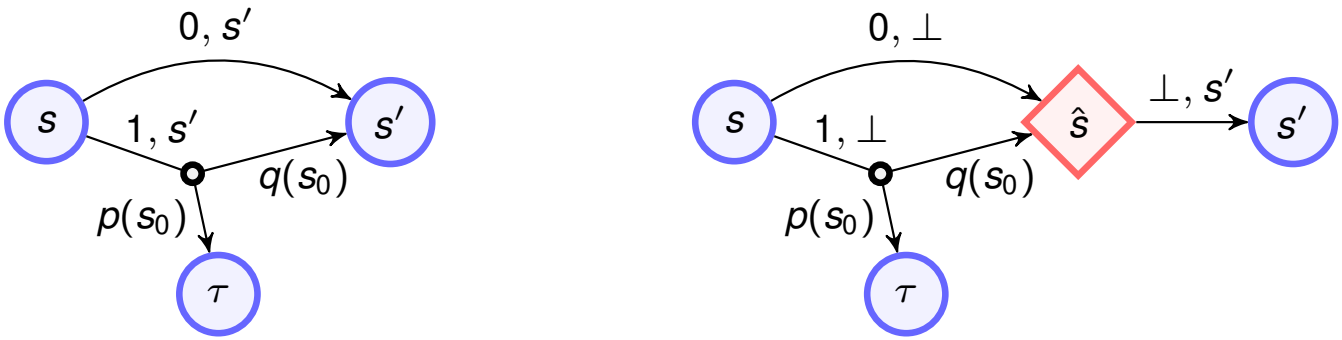
Turn-based Game

- This is a concurrent game.
- We gave a transformation which makes it turn-based.



Turn-based Game

- This is a concurrent game.
- We gave a transformation which makes it turn-based.



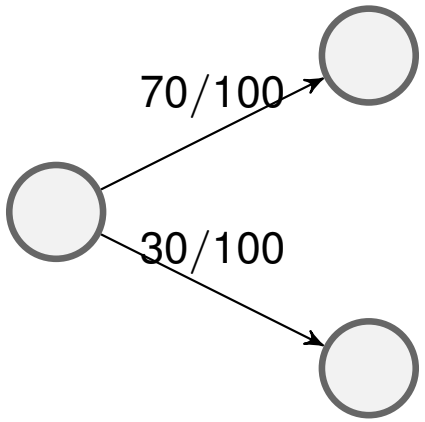
- Analyzing it becomes a lot easier now.

Where to get the probabilities?

- We modified PRISM code to generate probability intervals for each edge with PAC guarantees using simulations.

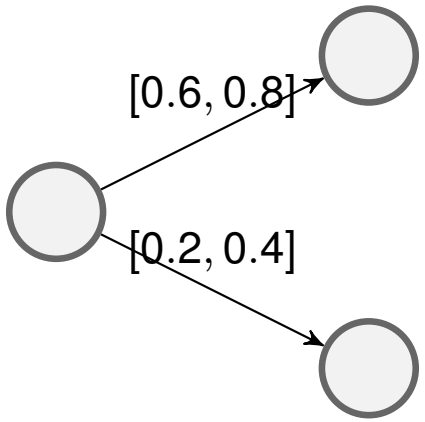
Where to get the probabilities?

- We modified PRISM code to generate probability intervals for each edge with PAC guarantees using simulations.



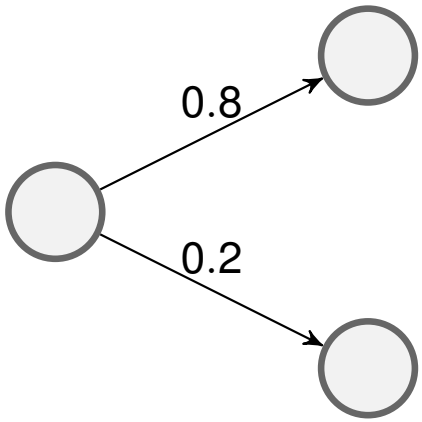
Where to get the probabilities?

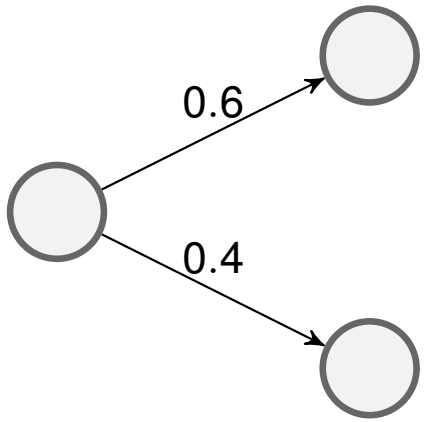
- We modified PRISM code to generate probability intervals for each edge with PAC guarantees using simulations.



Where to get the probabilities?

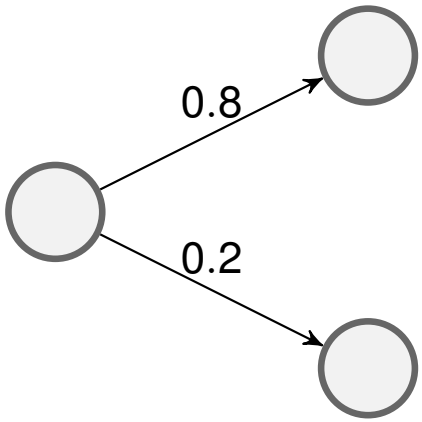
- We can construct best-case and worst-case games using these intervals.

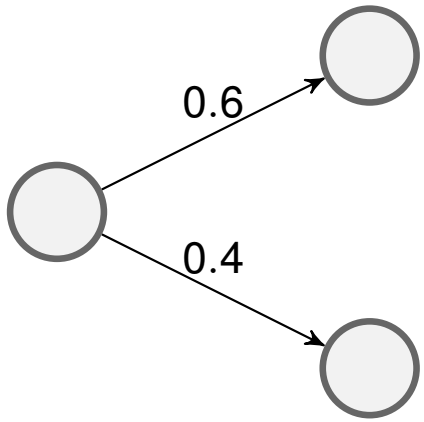




Where to get the probabilities?

- Generate Pareto frontiers for both games.





An overview

- Convert information flow graph to a *concurrent* stochastic game. [Shruti ’19]

An overview

- Convert information flow graph to a *concurrent* stochastic game. [Shruti ’19]
- Transform it to a *turn-based* stochastic game. [**Our contribution**]

An overview

- Convert information flow graph to a *concurrent* stochastic game. [Shruti ’19]
- Transform it to a *turn-based* stochastic game. [**Our contribution**]
- Compute probability intervals using simulations. [Pranav and Maxi ’19]

An overview

- Convert information flow graph to a *concurrent* stochastic game. [Shruti ’19]
- Transform it to a *turn-based* stochastic game. [**Our contribution**]
- Compute probability intervals using simulations. [Pranav and Maxi ’19]
- Generate best and worst case games. [Maxi and Tobi ’19 + **Our contribution**]

An overview

- Convert information flow graph to a *concurrent* stochastic game. [Shruti ’19]
- Transform it to a *turn-based* stochastic game. [**Our contribution**]
- Compute probability intervals using simulations. [Pranav and Maxi ’19]
- Generate best and worst case games. [Maxi and Tobi ’19 + **Our contribution**]
- Compute Pareto frontiers for these games. [Kwiatkowska ’13]

Experiments

Experiments

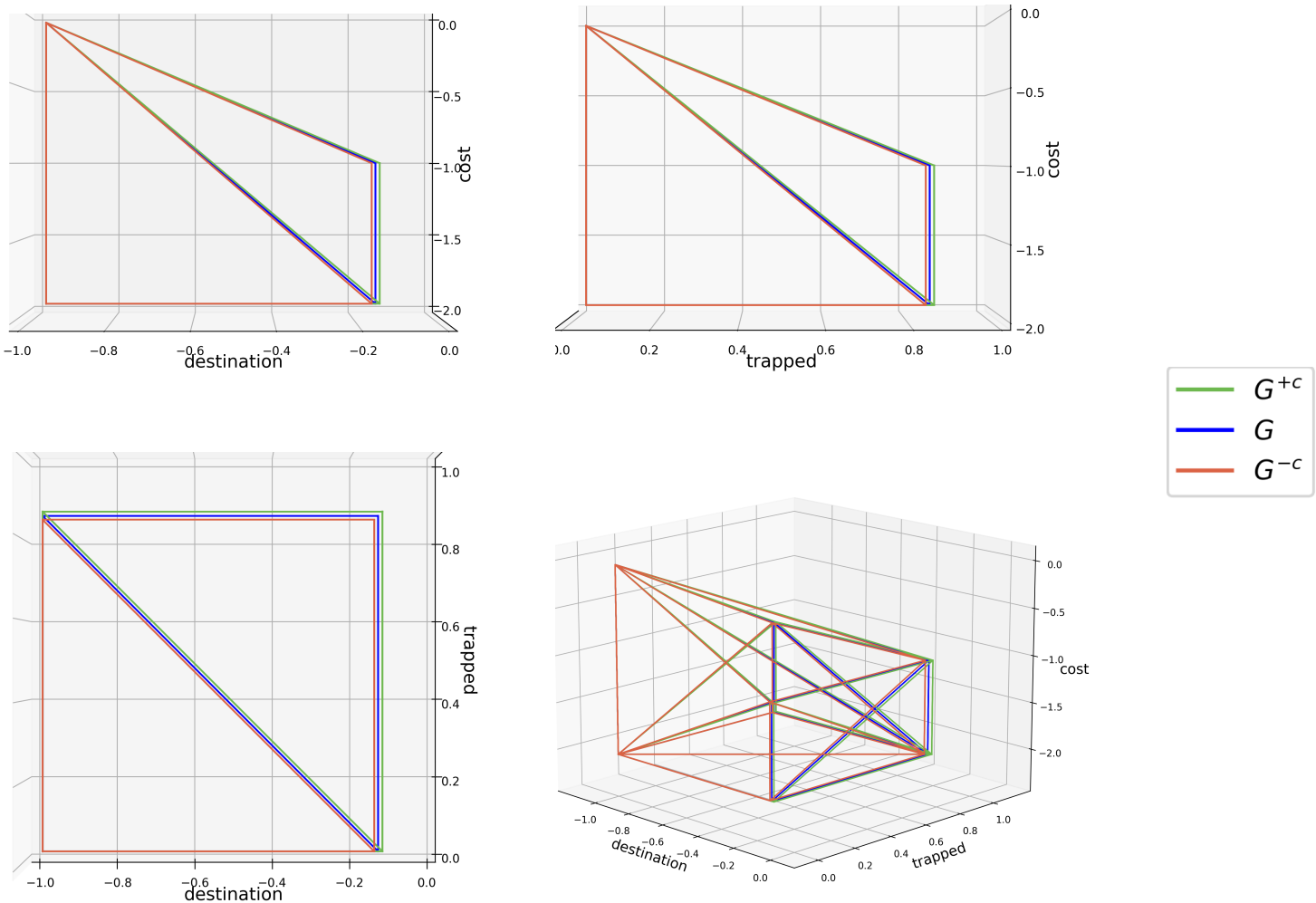


Figure: Achievable vectors of the NationState Attack case study.

Experiments

Example	Size	Cyclicity	Time taken (s)
Random	10	No	7.78
	100	No	11.90
Random	10	Yes	8.29
	100	Yes	17.63
ScreenGrab	9	No	7.95
NationState	30	Yes	8.40

Experiments

Example	Size	Cyclicity	Time taken (s)
Random	10	No	7.78
	100	No	11.90
Random	10	Yes	8.29
	100	Yes	17.63
ScreenGrab	9	No	7.95
NationState	30	Yes	8.40

Thank You!