Guaranteed Trade-Offs in Dynamic Information Flow Tracking Games

M. Weininger, **K. Grover**, S. Misra, J. Křetínský

Accepted in CDC’21

From the previous talk

Stochastic Games

Motivation

Motivation

Target, which averages 30 million customers a week, said Friday that an ongoing investigation found that "the stolen information includes names, mailing addresses, phone numbers or e-mail addresses for up to 70 million individuals."

"I know that it is frustrating for our guests to learn that this information was taken, and we are truly sorry they are having to endure this," Target CEO Gregg Steinhafel said in a press release.

In December, the retailer disclosed that data thieves hacked 40 million accounts, stealing encrypted PIN data, customer names, credit and debit card numbers, card expiration dates and the embedded code on the magnetic strip on the back of cards used at Target between Nov. 27 and Dec. 15.

Motivation

Compromised a third-party vendor

Motivation

Compromised a third-party vendor

Stayed there for 2 weeks

Motivation

Compromised a third-party vendor

Stayed there for 2 weeks

Defence

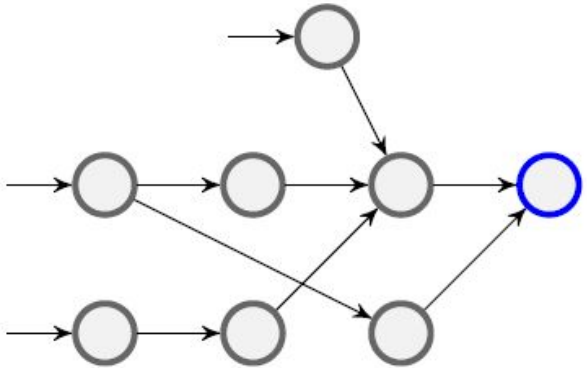
Defence

DIFT: Dynamic Information Flow Tracking

Defence

DIFT: Dynamic Information Flow Tracking

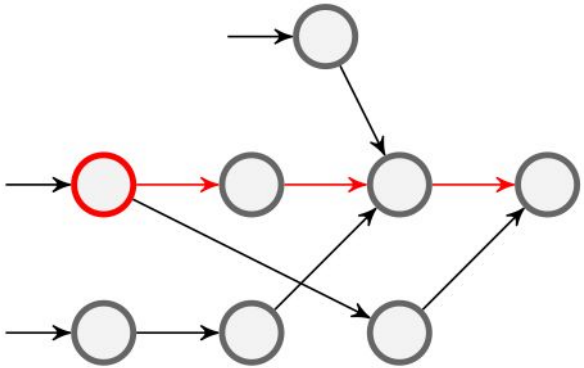
Track user’s movement in the system using information flow graph



Defence

DIFT: Dynamic Information Flow Tracking

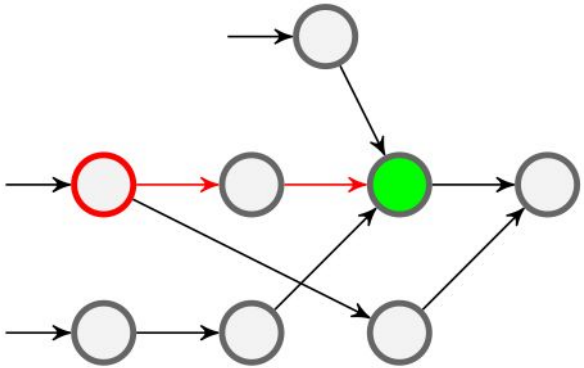
Tag suspicious data I/O channels.



Defence

DIFT: Dynamic Information Flow Tracking

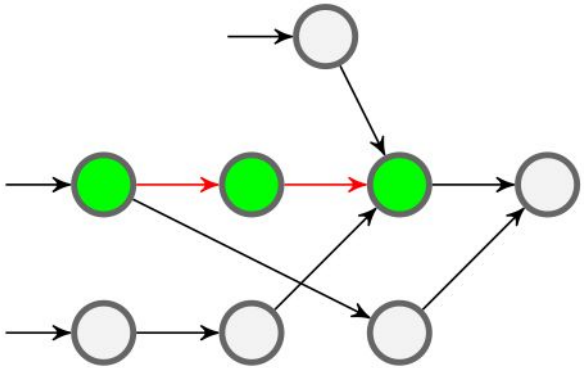
Perform security analysis on a node.



Defence

DIFT: Dynamic Information Flow Tracking

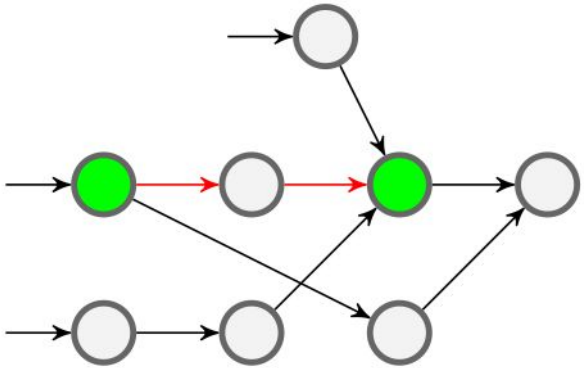
Tracking and analyzing information flow induces a memory and performance **cost**.



Defence

DIFT: Dynamic Information Flow Tracking

It is critical to optimally select, on which nodes to perform the security analysis.

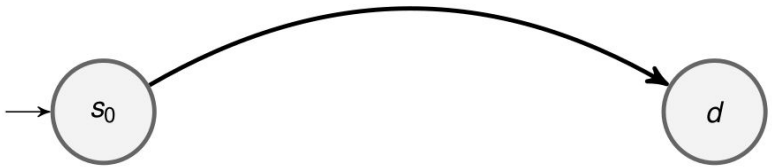


Previous Approach [Shruti CDC’19]

- Model the interaction as a concurrent stochastic game.

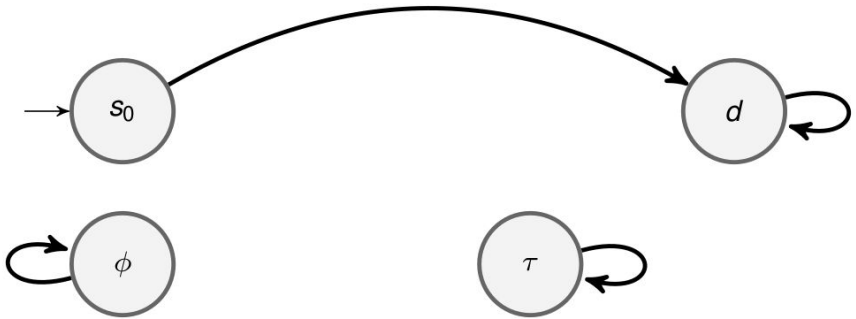
Previous Approach [Shruti CDC'19]

- Model the interaction as a concurrent stochastic game.



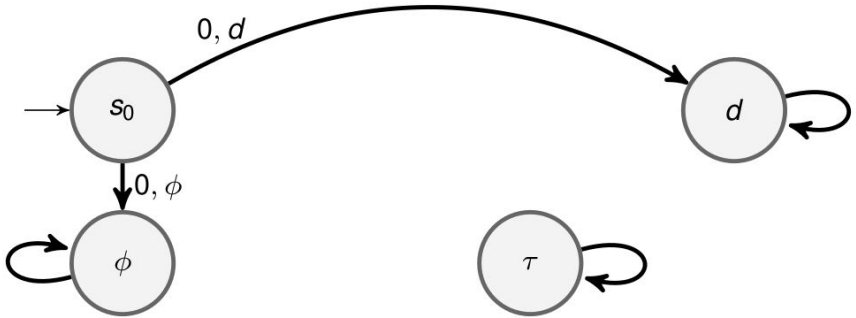
Previous Approach [Shruti CDC’19]

- Model the interaction as a concurrent stochastic game.



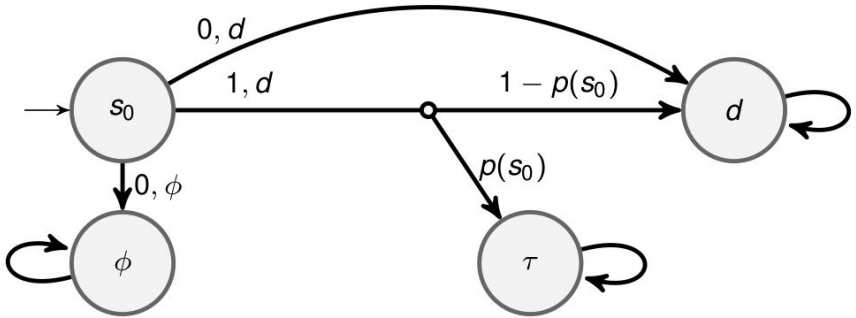
Previous Approach [Shruti CDC'19]

- Model the interaction as a concurrent stochastic game.



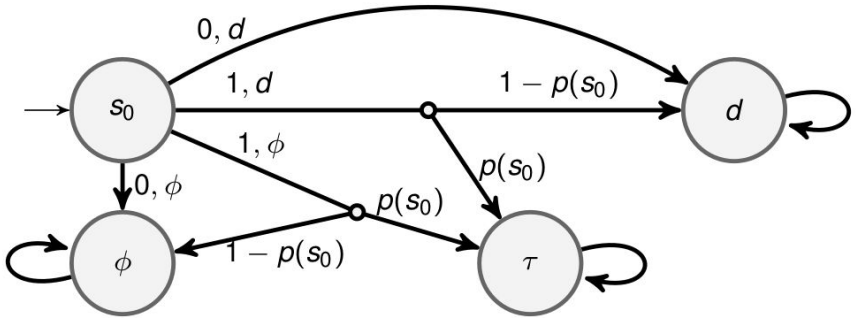
Previous Approach [Shruti CDC'19]

- Model the interaction as a concurrent stochastic game.



Previous Approach [Shruti CDC'19]

- Model the interaction as a concurrent stochastic game.



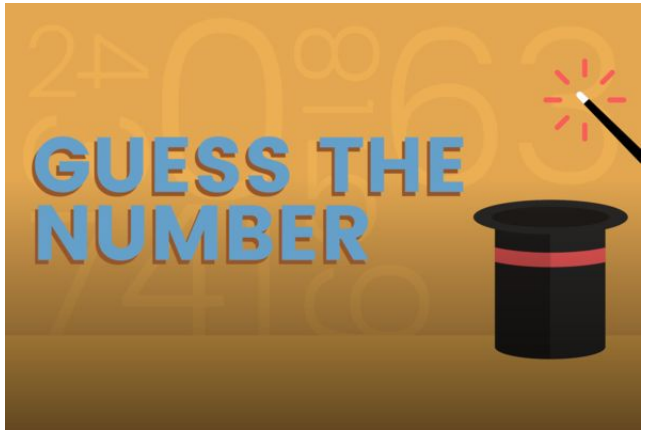
Previous Approach [Shruti CDC’19]

- Model the interaction as a concurrent stochastic game.
- Use reinforcement learning to find the optimal solution.

Previous Approach [Shruti CDC'19]

- Model the interaction as a concurrent stochastic game.
- Use reinforcement learning to find the optimal solution.

Guess the probabilities.



Previous Approach [Shruti CDC’19]

- Model the interaction as a concurrent stochastic game.
- Use reinforcement learning to find the optimal solution.

Guess the probabilities.

No cycles allowed.

Previous Approach [Shruti CDC'19]

- Model the interaction as a concurrent stochastic game.
- Use reinforcement learning to find the optimal solution.

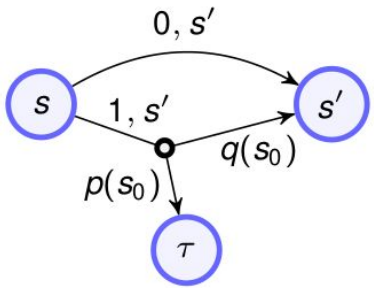
Guess the probabilities.

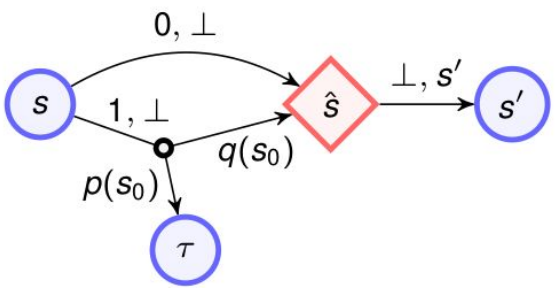
No cycles allowed.

1 reward for multiple objectives.

Our Approach

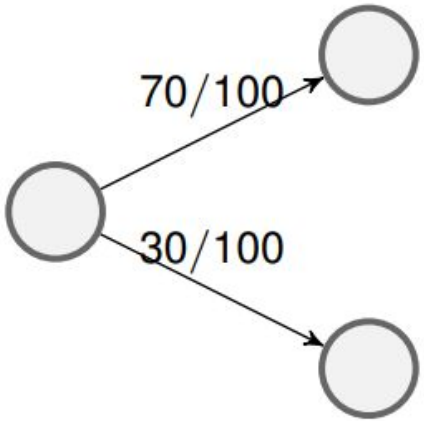
- Turn it into a turn-based game. [**Our**]





Our Approach

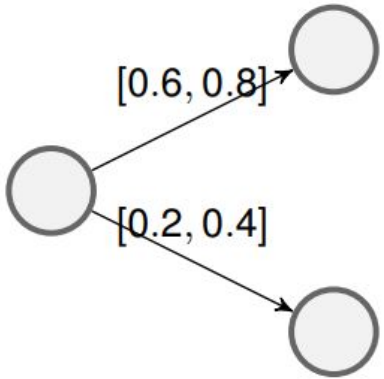
- Turn it into a turn-based game. [**Our**]
- Find probabilities using simulations. [Maxi et. al. CAV'19]



Our Approach

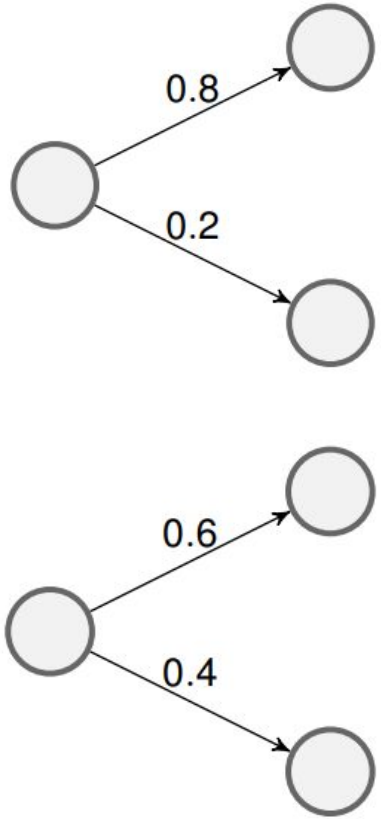
- Turn it into a turn-based game. [**Our**]
- Find probabilities using simulations. [Maxi et. al. CAV'19]

PAC



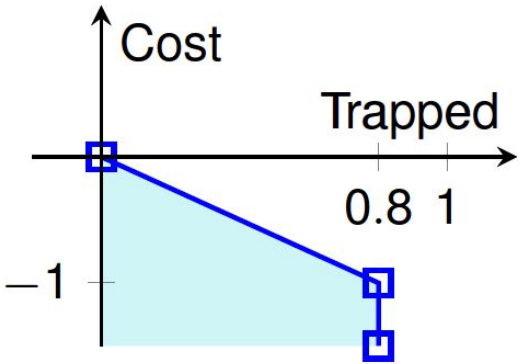
Our Approach

- Turn it into a turn-based game. [**Our**]
- Find probabilities using simulations. [Maxi et. al. CAV'19]
- Generate best and worst case games. [Maxi et. al. CDC'19 + **Our**]



Our Approach

- Turn it into a turn-based game. [**Our**]
- Find probabilities using simulations. [Maxi et. al. CAV'19]
- Generate best and worst case games. [Maxi et. al. CDC'19 + **Our**]
- Find Pareto frontiers for best and worst case games. [Kwiatkowska et. al. QEST'13]



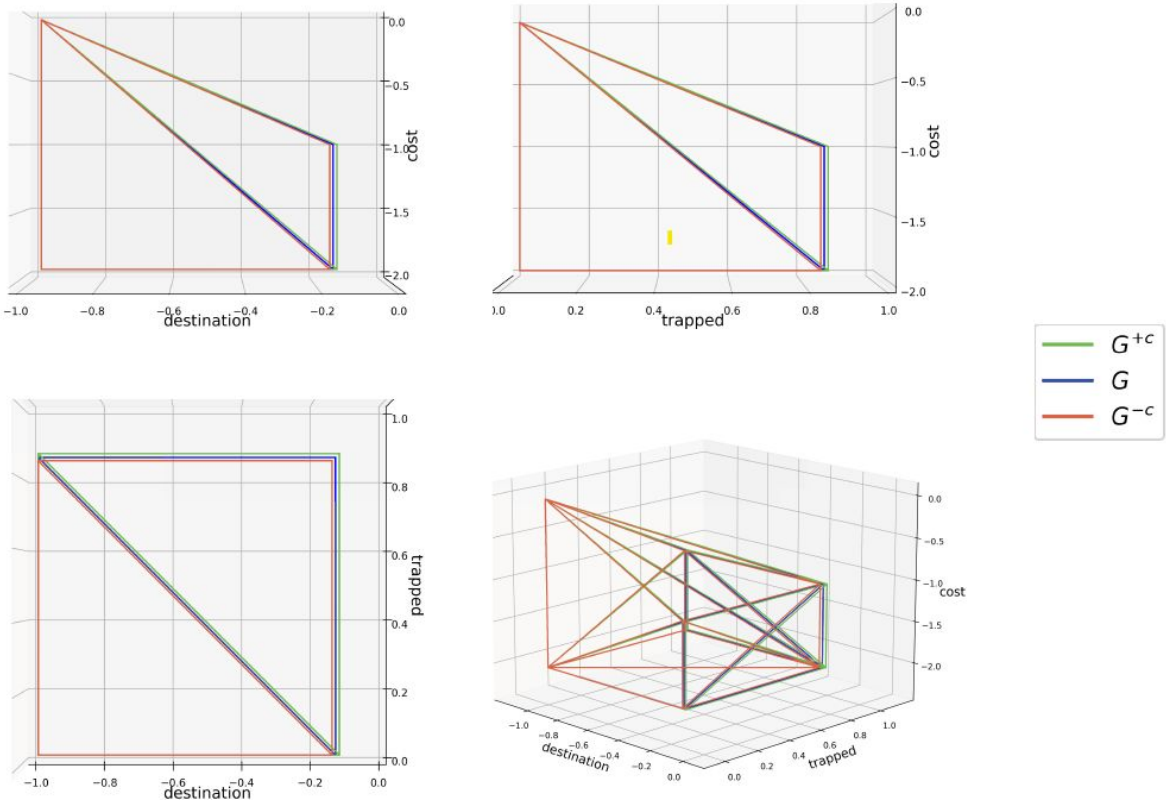
Our Approach

- Turn it into a turn-based game. [**Our**]
- Find probabilities using simulations. [Maxi et. al. CAV'19]
- Generate best and worst case games. [Maxi et. al. CDC'19 + **Our**]
- Find Pareto frontiers for best and worst case games. [Kwiatkowska et. al. QEST'13]

Solved all the problems.

Experiments

Experiments



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!