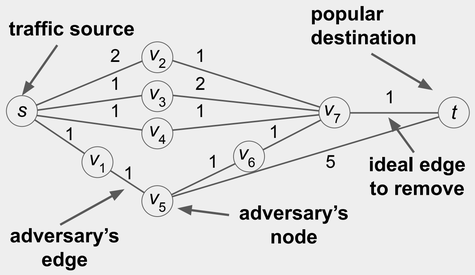
Optimizing Defense Against Shortest Path Attacks

Benjamin A. Miller[1], Zohair Shafi[1], Wheeler Ruml[2], Yevgeniy Vorobeychik[3], Tina Eliassi-Rad[1], and Scott Alfeld[4]

[1]Northeastern University, Boston, MA, USA
[2]University of New Hampshire, Durham, NH, USA
[3]Washington University in St. Louis, St. Louis, MO, USA
[4]Amherst College, Amherst, MA, USA

Problem Statement

Scenario: An adversary can divert traffic to specific parts of a graph by removing edges



***Goal*: Increase attacker's budget required to successfully attack**

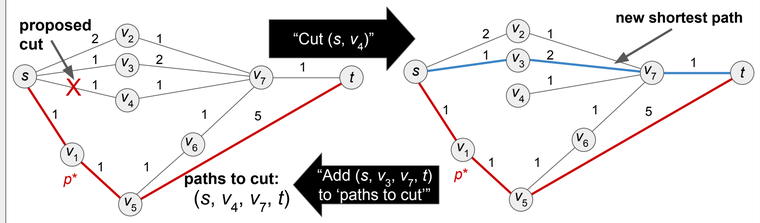
Assumed Context:

- We have a graph and know the true weights
- But we publish *approximate* weights
- Desired outcome: Adversary's required budget is increased
- Constraint: Minimize negative impact on legitimate users

Research Questions:

- What is the impact on legitimate network users when we stop an attack?
- Is it more costly to defend against an attack that targets a path that exits and returns to a community?

Attack: PATHATTACK*

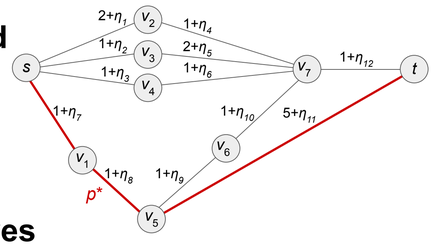


- **Algorithm to approximate optimal path cut cost**
- **Iteratively add constraints until *p** is shortest**

*B. A. Miller et al., "PATHATTACK: Attacking Shortest Paths in Complex Networks," in *ECML PKDD*, 2021

Defense: Modified Weights

- **Prior work† used noisy weights to increase adversarial uncertainty**
- **This work involves optimizing the defender's cost function with modified weights**

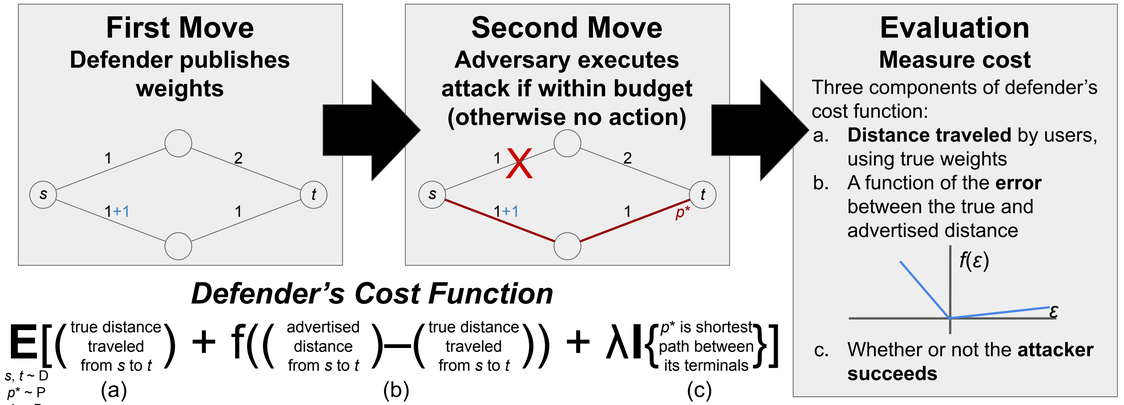


†B. A. Miller et al., "Defense Against Shortest Path Attacks," *GraphEx*, 2022

Optimization Approach

https://arxiv.org/abs/2305.19083

Stackelberg Game



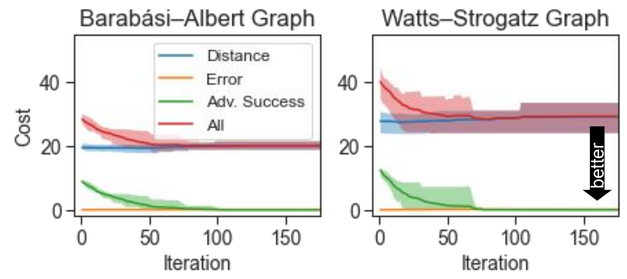
- ***Cut Defense* problem: Optimize defender's cost**
- ***Theorem*: Zero-sum Cut Defense with an attack oracle is NP-hard**

Algorithm: PATHDEFENSE

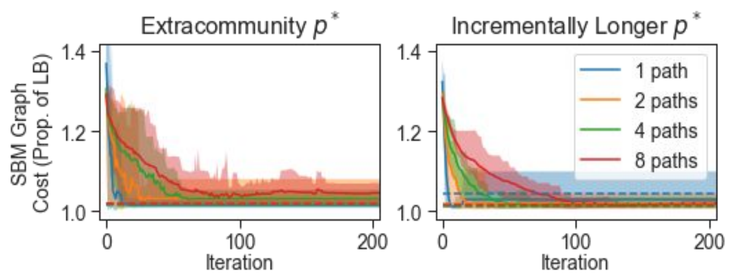
- **Heuristic algorithm to optimize defender cost**
- **Iteratively increment edges on *p** to decrease probability of attack**
- **After termination: Choose lowest-cost weights**

Results

- **Graphs with weights drawn from a Poisson distribution**
- **Edge removal costs are equal**
- **Randomly selected *s* and *t***
- **Defender uncertainty: distribution of target paths and adversary budgets**
- **Users are more likely to travel between nodes on potential target paths**



- **Attack probability becomes negligible with small increase in distance**
- **Cost due to error is extremely low**



Defense is more difficult and costly if it exits and returns to the community of *s* and *t*

This material is based upon work supported by the United States Air Force under Air Force Contract No. FA8702-15-D-0001 and the Combat Capabilities Development Command Army Research Laboratory (under Cooperative Agreement Number W911NF-13-2-0045). Any opinions, findings, conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the United States Air Force or Army Research Laboratory.