Secure Connectivity Determination Under the Risk of Adversarial Model

Hongyi Guo, Jikun Chen

Jun. 10, 2019

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

Contents

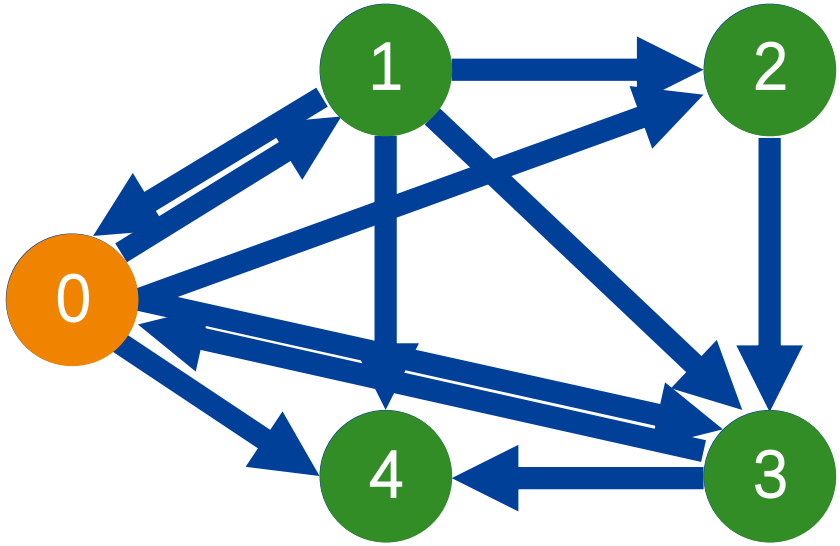
Contents

Introduction

- We consider the scene that in a network $G = (V, E)$:
  - Define $Connectivity$ as the number of points **reachable by the source point** divided by the total number of points other than the source.
    - $Connectivity \overset{\text{def}}{=} \sum_{v \in V, v \neq src} \frac{1_{connected(src,v)}}{|V|-1}$
  - **The attacker** is trying to reduce the connectivity by deleting K edges.
  - **The defender** can choose K edges and protect them from attacks.
  - The attack on the edge that has been protected will fail.
- We design a framework based on reinforcement learning, in which we simultaneously train an attacker model and a defender model. Our work is inspired by ***GAN***.
- Our experiments show that the RL-based model performs better than a rule-based algorithm and the stochastic algorithm.

Introduction

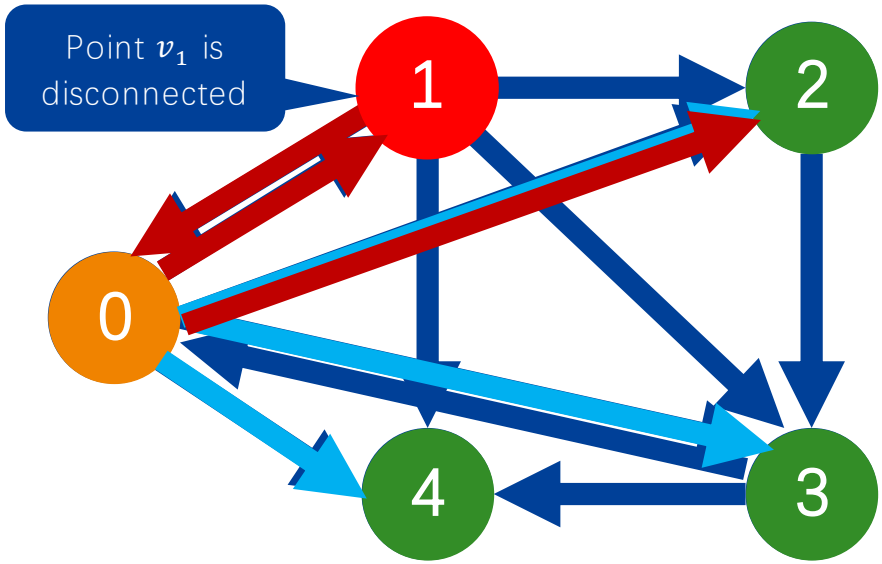
- First the network is represented by a directed graph G with N(=5) vertices and M(=11) edges. The source point is v_0 by default.



- Note that in this original graph, the source point is connected to all other four vertices.

Introduction

- Some edges are defended by the Defender.
- And some are under attack of the Attacker.



- Our goal is to develop stronger defender that can protect the connectivity.

Contents

Works on Connectivity Under Attack

- *Near Optimal Adaptive Shortest Path Routing with Stochastic Links States under Adversarial Attack (Pan Zhou, 2016)*
  - The shortest path routing of a network with stochastically time varying link metrics under potential adversarial attacks.
  - Formulating it as a multi-armed bandit (MAB) problem.

- *The adversarial stochastic shortest path problem with unknown transition probabilities (Gergely Neu, 2012)*
  - loop-free stochastic shortest path problems.
  - "follow the perturbed optimistic policy"

Works on Connectivity Under Attack

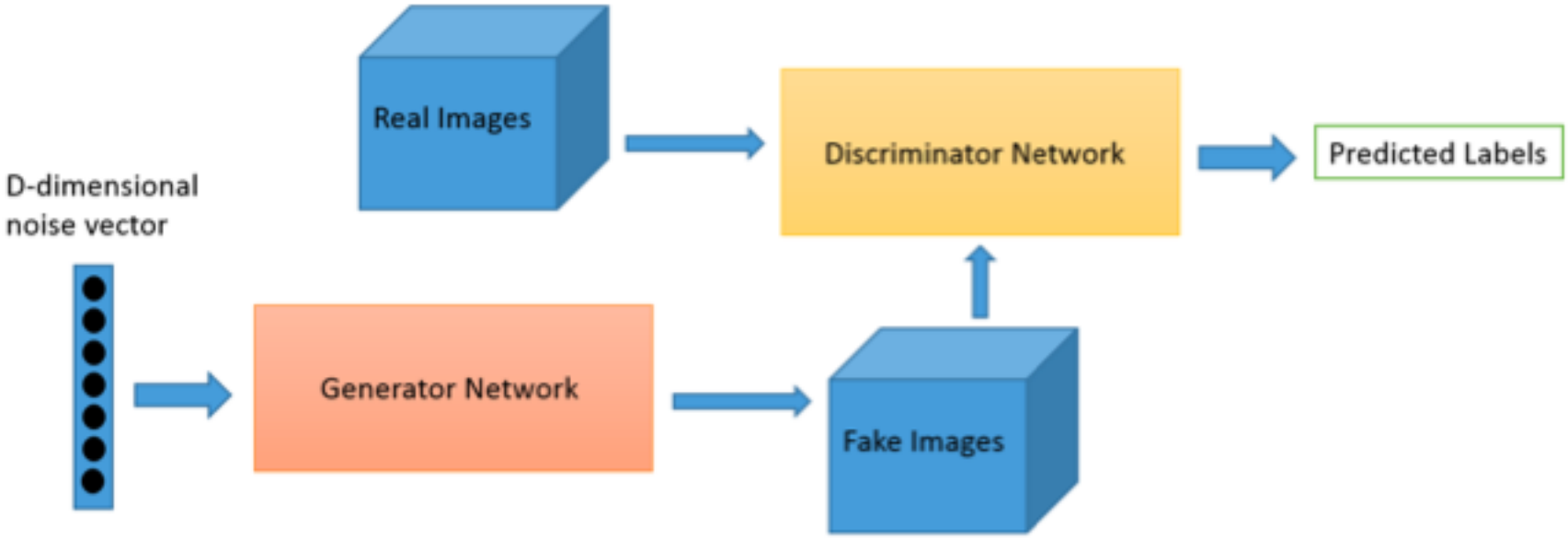
- *Adversarial resilience of matchings in bipartite random graphs (P. Balister, 2017)*
  - How to find the maximum matching in bipartite graphs after an adversary deleted some edges.

- *Adversarial Deletion in a Scale Free Random Graph Process (AD Flaxman, 2007)*
  - A property in a dynamically evolving random graph.

Contents

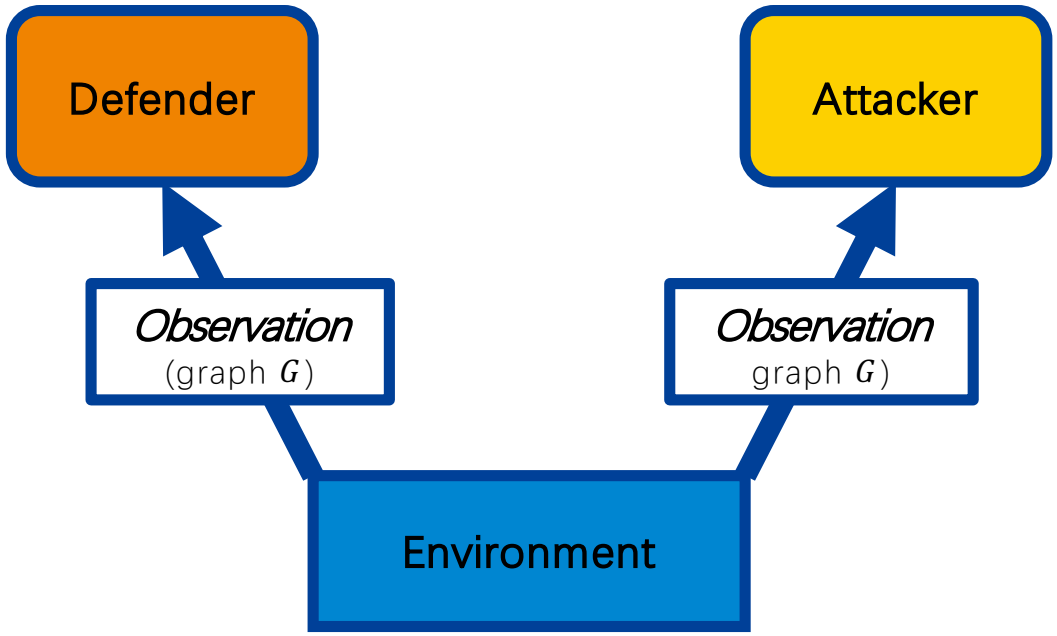
Review of GANs

- First, let us quickly review Generative Adversarial Networks (GAN).



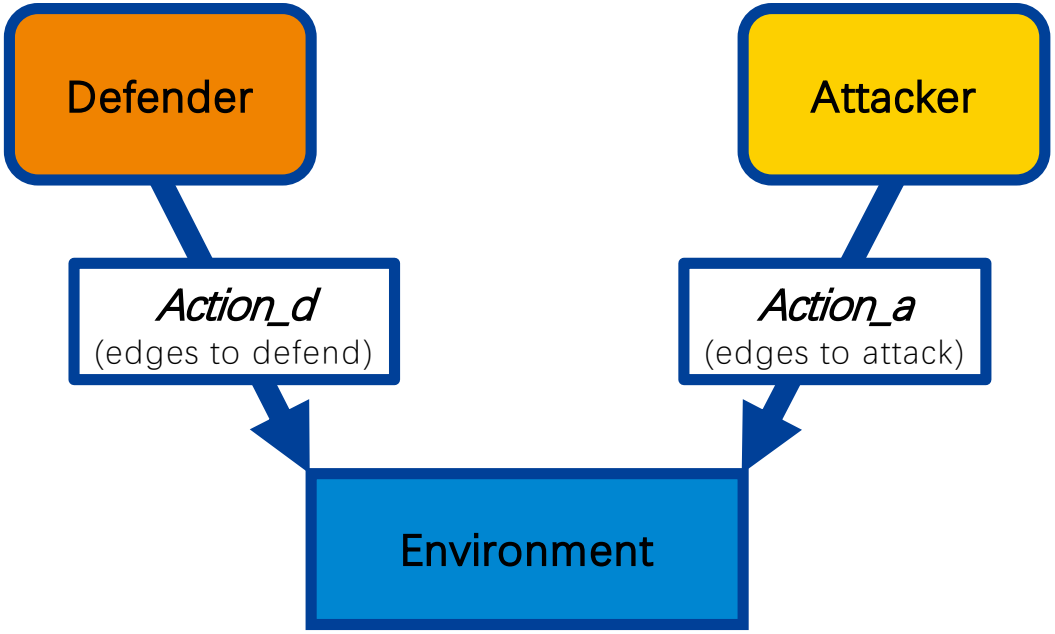
Proposed architecture

- We then propose our adversarial learning model.
- At the beginning of each time step:



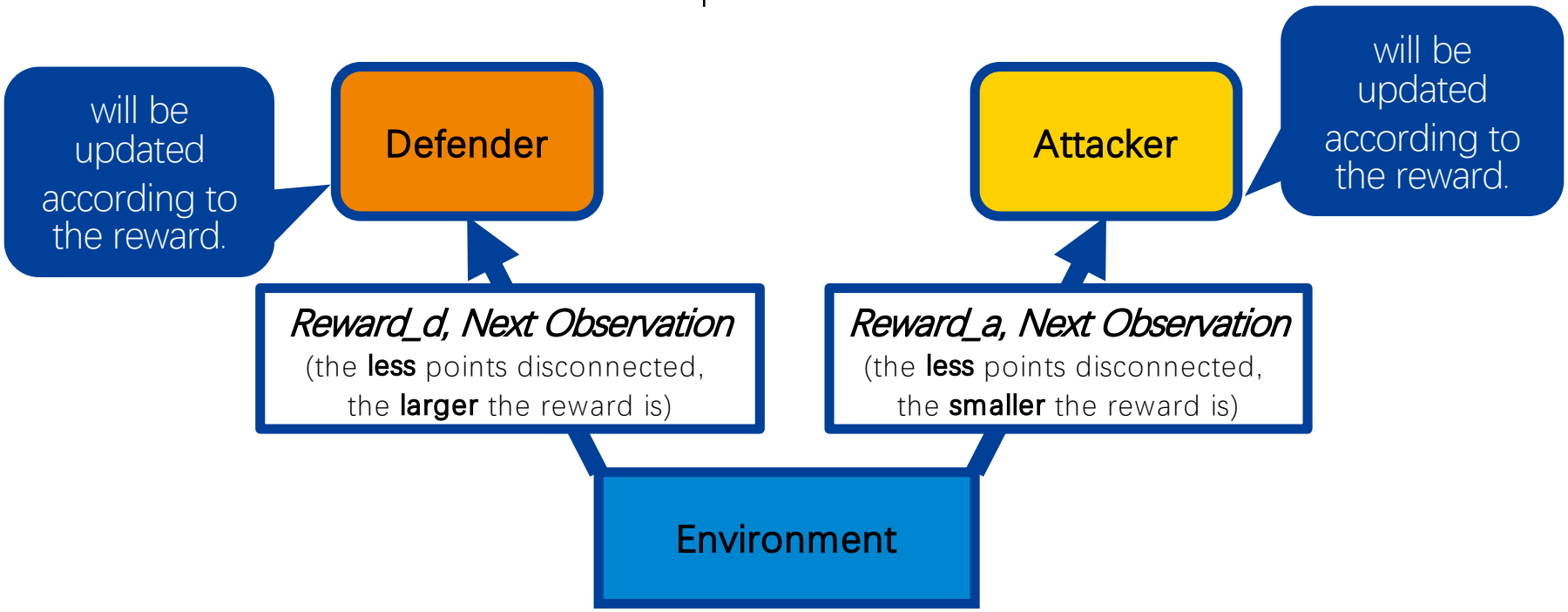
Proposed architecture

- We then propose our adversarial learning model.
- And then:



Proposed architecture

- We then propose our adversarial learning model.
- Then it enters the next time step:



- Assuming l points are disconnected from the source point after the attack, the defender gets $-\frac{l}{N-1}$ reward and the attacker gets $+\frac{l}{N-1}$ reward.

Models

RL(Reinforcement Learning)-based Model

- Based on **Advanced Actor Critic (A2C)**, one of the policy-based methods.
- Will be introduced later.

Stochastic Model

- Stochastically sample K edges among all.
- Do not update itself.
- Used as opponent when training single Attacker/Defender model.

Rule-based Model

- Stochastically sample K edges from edges outgoing from the source.
- Do not update itself.
- Used as baseline.

RL-based model

- *Observation:* s_t
  - The randomly generated directed graph G, as a flattened adjacent matrix.
- *Action:* $a_t^1, \ldots, a_t^k$
  - The action space of A2C is $1..N(N-1)$, representing each potential edge. The A2C algorithm we use will compute the policy (probability of taking each action). We take K actions with the largest K probabilities.
- *Reward*
  - $R_t^{Defender} = Connectivity_{t+1} - Connectivity_t$
  - $R_t^{Attacker} = -R_t^{defender}$
- *How to update*
  - The original update process of A2C is: $\nabla_\theta \log \pi(a_t|s_t;\theta)\, A(s_t, a_t;\theta)$
  - Our update process is: $\frac{1}{k}\sum_{k=1}^{K} \nabla_\theta \log \pi\left(a_t^k|s_t;\theta\right) A(s_t, a_t^k;\theta)$

Contents

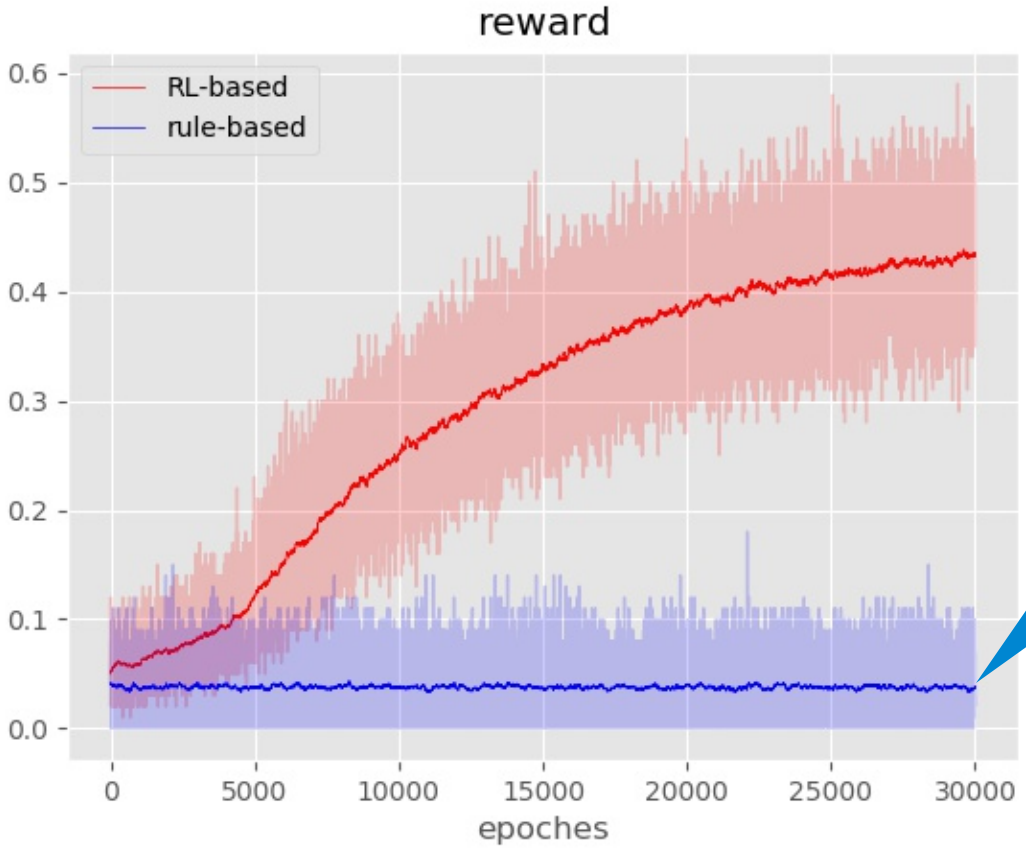
Experiment 1

- Train an **RL-based attacker** against a **stochastic-regime defender**.
  - Under setting: $\mathrm{N} = 5, M = 16, K = 3$

The baseline ***attacker*** model randomly choose edges connecting the ***source point*** to others to defend.

Experiment 2

- Train an **RL-based attacker** against a **rule-based defender**.
  - The rule-based defender is exploited.



The baseline ***attacker*** model randomly choose edges connecting the ***source point*** to others to defend.

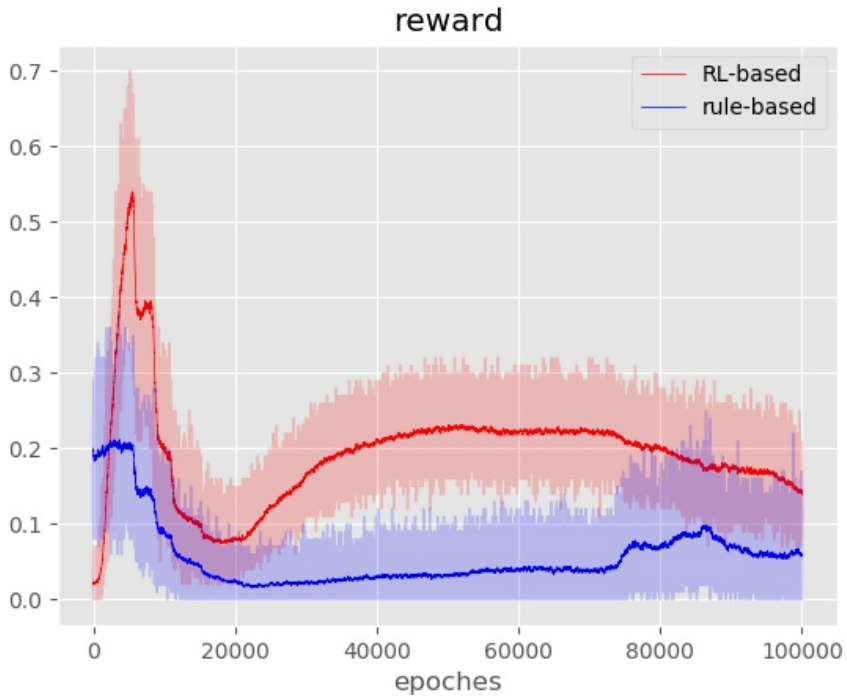
Experiment 3

- Then, we train an **RL-based defender** against the just trained RL-based attacker.

The baseline ***defender*** model randomly choose edges connecting the ***source point*** to others to defend.

Experiment 4

- What about training attacker and defender together, like **GAN**?



(a) RL-based Attacker

(b) RL-based Defender

Contents

Discussion

- *Contribution*
  - An adversarial learning architecture
  - RL-based model, together with stochastic model, rule-based model
  - Experiments
- *To be improved:*
  - Better representation of the graph?
  - Better designation of reward?
  - Stronger baseline model to compare?
  - Generalization?
  - Multiple attackers?
- *Maybe useful:*
  - GANs?
  - Adversarial Machine Learning?
    - https://aaai18adversarial.github.io/

Thank you!

Q&A

Group No.2

Hongyi Guo, Jikun Chen