Secure Connectivity Determination Under the Risk of Adversarial Model

郭洪一 516030910306

陈纪坤 516030910303

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

问题描述

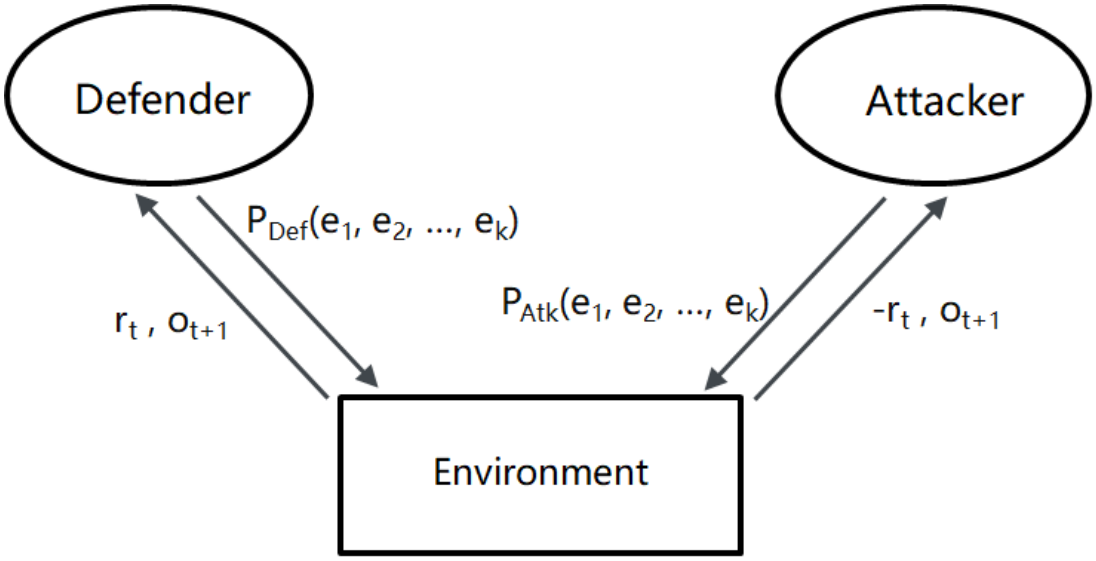
- 在一个网络中，攻击者在试图破坏网络的连边，而防御者试图选择容易被攻击者选中破坏的边进行事先的保护。在这种攻防对抗的情况下，分析防御者怎么做更容易维护整个网络的连通性。

主要思路

- 我们通过强化学习同时优化防御者网络和攻击者网络，通过对抗学习，最终：
- 防御者网络 f(o)
  - 在每个epoch开始的时候，防御者得到一个输入o，包含了当前网络的状态（可能需要做图的embedding，保证这时的网络可以连通），网络输出每条边需要防御的概率。最后取出概率前k_f大的边进行防御。防御过的边可以不受攻击影响。
  - 如果受到攻击之后的图仍然是连通的，那么防御者得到+1的reward；否则得到-1的reward
- 攻击者网络 g(o)
  - 在每个epoch开始的时候，攻击者得到一个输入o，与防御者得到的输入是相同的。网络输出攻击每条边的概率，最后取概率前k_g大的边进行攻击。被攻击的边如果没有受到防御则被认为将不能连通。
  - 如果攻击之后的图不再连通，那么攻击者得到+1的reward；否则得到-1的reward。
- 可以认为，攻击者与防御者在进行一个零和博弈。我们希望，通过强化学习训练过的防御者网络可以在随机攻击的场景下获得比基于规则的防御更好的效果，而攻击者网络可以在面对随机防御时达到比随机攻击更佳的效果。我们将采用一系列的baseline进行对比验证。

模型架构

- o_t：t 时刻攻击者、防御者网络得到的网络
- $P_{Def}(e_i)$：防御网络给出的边 e_i 需要防御的概率;
- $P_{Atk}(e_i)$：攻击网络攻击边 e_i 的概率
- r_t：由图的连通性给出的 reward 值



拓展问题

- 怎样对图进行表示，怎样建立攻击、防御网络结构能达到最佳的效果？
- 若同时存在多个攻击者，分别使用不同的攻击策略，如何设计合适的防御方法？
- 如何利用相关领域的模型和算法（如GAN、对抗样本）进行改进？

文章总结

- Adversarial resilience of matchings in bipartite random graphs
- 研究了对于给定的（起点，终点）对，维护最短路径（与时间有关）的问题。介绍了多种攻击策略。

- Adversarial Deletion in a Scale Free Random Graph Process
- 提出了一种名为 “follow the perturbed optimistic policy” 的算法，该算法结合了 “ollow the perturbed leader” 方法，用于在线学习任意序列和 “上层自信强化学习” 。

文章总结

- Near Optimal Adaptive Shortest Path Routing with Stochastic Links States under Adversarial Attack
- 研究了在一张随机二分图中寻找最大匹配的问题，对手每次会删除掉一些边。提出的理论：
  - 二分图由A、B两部分组成，大小分别为n, (1+ε)*n
  - A中的每个点会独立地在B中按照均匀分布随机地选择d个点作为邻居（连线）
  - 对手：对A中的每个点，删掉不超过r条相连的边，r是≥1的常数，在d固定且足够大的情况下，对任意的η>0
  - 如果，那么对手不可能销毁掉所有大小为n的匹配
  - 如果，那么对手几乎一定可以销毁掉所有大小为n的匹配

文章总结

- The adversarial stochastic shortest path problem with unknown transition probabilities
- 研究了一个动态演化的随机图，它使用 “preferential attachment” 添加点和边，并受到攻击者的攻击。在 t 时刻，加入一个新的点 x_t，和 m 条与 x_t 相邻的边（m为常数）。某一个点被选择与 x_t 相邻的概率与这个结点的度成正比。这一步完成之后，一个（自适应的）攻击者可以决定删去一些点，约束条件为：到 n 时刻为止，总共删除的点数不得超过 δ*n（δ为常数）。
- 论文证明了：若 δ 足够小，m 足够大，则在 n 时刻，图大概率会存在一个规模不低于 n/30 的连通分量。