

DRDoS 攻撃回避のためのマルチエージェント強化学習に基づく 増幅トラフィックフィルタリング戦略学習機構の試作

川添 智貴[†][†] 静岡大学情報学部行動情報学科福田 直樹[‡][‡] 静岡大学 学術院情報学領域

1 はじめに

DRDoS 攻撃は攻撃対象の通信回線を圧迫する手法としてよく用いられるものである。DRDoS 攻撃に対する回避速度向上は多くのネットワーク利用者にとって利益となる。リアルタイムの応答を要求されるネットワークの課題に対し、マルチエージェント強化学習を用いて解決を試みる研究が行われている [1]。

本論文では、DRDoS 攻撃回避のための、マルチエージェント強化学習に基づく、増幅トラフィックフィルタリング戦略学習機構の試作について述べる。この機構では、DRDoS 攻撃を検知するハニーポットを複数用いてそれらを自立協調させる。これによりハニーポットが単独動作であるときよりも効率よくフィルタリングルールを導き出すことを可能にする。

2 DRDoS 攻撃回避機構の試作

2.1 DRDoS 攻撃回避機構の構成

図 1 に、本研究における DRDoS 攻撃回避機構のシミュレータのスクリーンショットを示す。1 が攻撃者、2 が SDN 転送デバイス、3 が ISP ネットワーク、4 が脆弱性のあるサーバ、5 が強化学習機構を備えたハニーポット、6 がファイアウォールアプリケーション、7 が SDN コントローラ、8 が攻撃対象である。本試作は JavaScript を用いて作成した。

図 2 に、本研究における DRDoS 攻撃回避機構のシミュレータ上での動作可視化部分のスクリーンショットを示す。攻撃がどこからどこに移動しているかを分かるようにするために半透明の残像が表示されるようになっている。本フィルタリング戦略学習機構では、異なる ISP ネットワーク (鼠色、緑色、赤色のエリア) それぞれで独立して強化学

習を用いて戦略を学習し、それぞれの学習結果をほかの強化学習機構に渡すことで、協調的なフィルタリング戦略の獲得を試みる。たとえばその方法の一例としては、シミュレーション上最も性能の優れた学習手法を基準として戦略をさらに改良するという方法がある。右側の ISP ネットワークに示される SDN forwarding device の上にある盾は、戦略に基づいて攻撃をフィルタリングし始めたことを示している。

図 3 において、中央に示される ISP ネットワークにある雲のように見える部分が強化学習した結果を示しており、図 3 では、これが他の ISP ネットワーク内のハニーポット (オレンジ色のサーバのアイコンで表示された部分) に送られる様子を表現している。

3 まとめ

本論文では、DNS や NTP などの仕組みを悪用し、攻撃対象にデータを大量に送りつけて過負荷状態に陥らせる DRDoS 攻撃を回避する方法として、異なる ISP ネットワークそれぞれで独立して強化学習を用いて学習した戦略を他の学習機構に渡すことで、協調的なフィルタリング戦略の獲得を試みるシミュレータの試作について述べた。

参考文献

- [1] K. Sugiyama, and N. Fukuta, “A Multiagent Learning Approach for Distributed Control of Address Randomization in Communication Destination Anonymization”, Proc. of IEEE/IIAI International Congress on Applied Information Technology (IEEE/IIAI AIT2019), 2019.

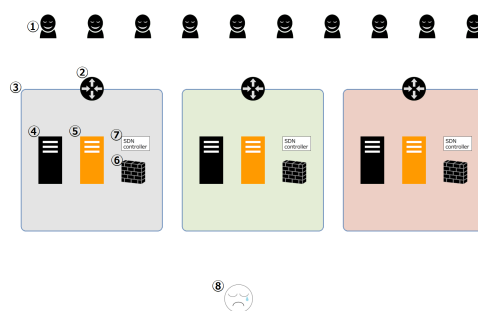


図 1: 試作した DRDoS 攻撃回避機構のシミュレータ

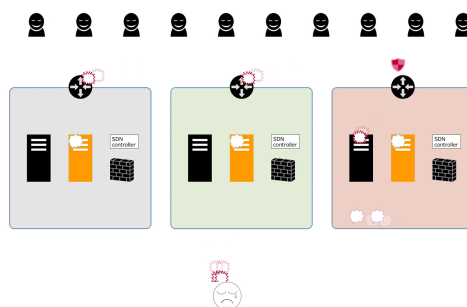


図 2: 試作した DRDoS 攻撃回避機構シミュレータ動作例

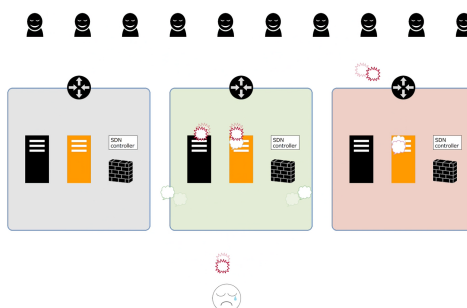


図 3: 中央の ISP ネットワークから両側の ISP ネットワークに強化学習した結果が送られる例