4E-07

反射型DDoS攻撃を緩和するマルチエージェント学習機構構築のためのDRDoSシミュレータの試作

川添 智貴 †
† 静岡大学 総合科学技術研究科 情報学専攻

福田 直樹 ‡
‡ 静岡大学 学術院情報学領域

1 はじめに

反射型 DDoS(DRDoS) 攻撃は世界中に存在する膨大な数の botnet を起点に脆弱性を持つ多くのサーバを悪用した増幅攻撃を行う．我々はDRDoS攻撃に対処するための攻撃者の意思を加味したフィルタリング学習機構としてI-POMDP[1]を活用したものを検討し，その学習機構に対するより実証的な検証を行うための実験環境の試作および検討を行う．本稿で示すDRDoS攻撃シミュレータによる実験の目的は，検討している学習機構の動作および有効性を実際のケーブルやサーバ，スイッチ等のネットワーク機器における特性を加味しながら確認することである．ここでは主に，通信ケーブルやスイッチ，サーバの処理能力等に起因するパケットロスや情報伝達の遅延に焦点を当て，学習機構の精度を確認することができるようなシミュレータの実現を目指す．

2 DRDoS攻撃のモデル化

DRDoS 攻撃に対処する我々の以前の研究では攻撃者は攻撃の有効度合いを考慮しないと仮定していたが [2]，本シミュレータで取り扱う DRDoS 攻撃では，攻撃を行う botnet にトラフィックに応じて行動を変化させるような意思（intention）が組み込まれていると仮定する．この仮定のもとで，動作する botnet を再現可能とすることによりISPが攻撃者をそのモデルに基づいて認識し，その攻撃者モデルに応じたフィルタリングを学習するといった目的に使用することを検討している．

議論を簡潔にするために，本シミュレータにおける学習機構では，DRDoS 攻撃を，単一のフロー生成エージェント（botnet または正常なユーザ）と単一の防御者エージェント（ISP）が存在するコンテキストにおいて交互に意思決定が行われる問題としてモデル化するところから始める．DRDoS攻撃のモデル化にあたっては，他エージェントの内面までをフラットな構造で考慮することのできる部分観測マルコフ決定過程であるI-POMDP[1]を用いる．

3 シミュレータの構成

本稿で示すDRDoS攻撃シミュレータを構成する目的は，上記のように防御者側での学習機構の動作および有効性を実際のケーブルやサーバ，スイッチ等のネットワーク機器における特性を加味しながら確認することである．ここでは主に，通信ケーブルやスイッチ，サーバの処理能力等に起因するパケットロスや情報伝達の遅延に焦点を当て，学習機構の精度を確認することができるようなシミュレータの実現を目指す．これらは特に，フロー生成エージェントが観測値として取得するトラフィック状態に大きく影響すると考えられる．

DRDoS攻撃をシミュレーションするための方法としては，MATLAB などを用いて攻撃の強度などの数量的な時間変化をモデルに基づいて再現する方法，ネットワークシミュレータを用いてネットワーク上のパケットの流れの観測・再現が可能

A Preliminary Prototype Simulator for Building a Multi-Agent Learning Mechanism for Mitigating DRDoS Attacks

†Tomoki Kawazoe Department of Informatics, Graduate School of Integrated Science and Technology, Shizuoka University Email: kawazoe.tomoki.17@shizuoka.ac.jp

‡Naoki Fukuta College of Informatics, Academic Institute, Shizuoka University Email: fukuta@inf.shizuoka.ac.jp

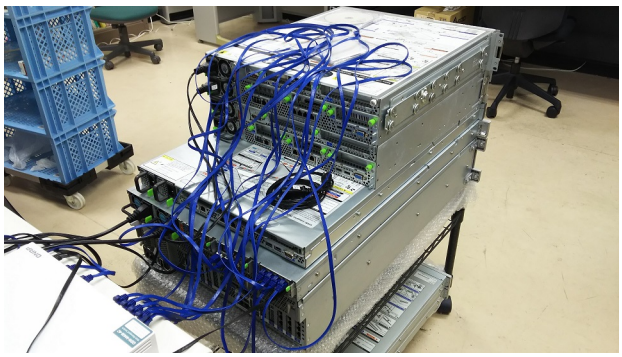

図 1: 本 DRDoS シミュレータで使用するサーバとスイッチ．Oracle Netra SPARC T4-1 Server(最上段，上から二段目)，SPARC S7-2 (上から四段目)，10GBASE-T をサポートする高速 Layer-2 スイッチ (左下，QSW-M408C)．

表 1: サーバの仕様

機種名	OS	CPU	memory
Oracle Netra SPARC T4-1	OpenBSD 7.0	4 コア 32 スレッド	32GB
Oracle Netra SPARC T4-1	OpenBSD 7.0	4 コア 32 スレッド	256GB
SPARC S7-2	OpenBSD 7.0	8 コア 64 スレッド	64GB

な範囲や条件を自由に拡張できるようにする方法，および，実際のネットワーク機器を物理的に用いてその実装に固有な詳細な挙動などを再現可能にする方法の 3 つが考えられる．ネットワークシミュレータとしては，dummynet[3] などがあることから，本稿では図 1 の機器を用いて DRDoS 攻撃のためのシミュレータを作成する．表 1 に使用する各サーバの仕様を示す．

本稿で検討しているシミュレータの作成に先立ち，上述した機器を用いたシミュレータを試作し，実際に DRDoS 攻撃シミュレーションを行った．本シミュレータでは，JDK1.8.0 を用いてコンパイルした Java プログラムを使用し，トリガーパケットの送信，トリガーパケットに対する増幅応答の生成を行った．図 2 は，本シミュレーション動作時のログの例を示す．同様に，本稿で検討しているシミュレータでも JDK1.8.0 でコンパイルした Java プログラムを使用して，トリガーパケットおよび脆弱なサーバによる増幅応答の生成および送信を行う．

DRDoS 攻撃の遮断方法の再現には，OpenBSD7.0 に実装されている PF（Packet-Filter）を使用する．具体的には pf.conf において anchor を設定し，対象とするフロー条件を記載したフィルタリングルールをプログラムを通して動的に追加していく．

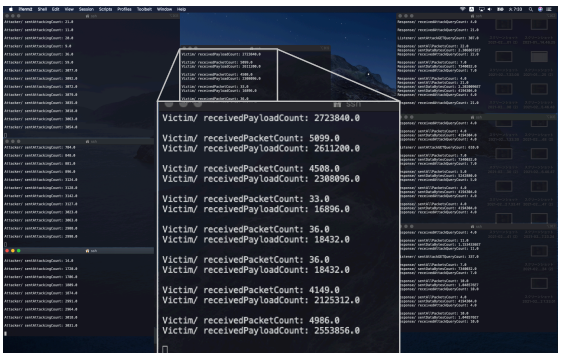

図 2: シミュレーション動作例

本シミュレータでは輻輳状態を容易に再現できるようにするために，必要に応じて特定の通信路上の帯域幅の制限を行えるようにする．これに対しては使用している L2 スイッチのポートにおける速度を調整できるようにするなどの実装が考えられる．

4 おわりに

本研究では DRDoS 攻撃に対処するための攻撃者の意思を加味した I-POMDP を活用したシミュレータの物理装置上での実現方法を検討し，そのシミュレータを用いて DRDoS 攻撃に対抗できる防御手段の学習機構の実証的な検証を行うための実験環境の試作および検討について述べた．

参考文献

[1] P. J. Gmytrasiewicz and P. Doshi, “A framework for sequential planning in multi-agent settings,” *J. Artif. Int. Res.*, vol. 24, no. 1, p. 4979, Jul 2005.

[2] T. Kawazoe and N. Fukuta, “A cooperative multi-agent learning approach for avoiding drdos attack,” in *Proc. 10th IIAI International Congress on Advanced Applied Informatics (IIAI AAI2021 / SCAI2021)*, 2021, pp. 518–523.

[3] L. Rizzo, “Dummynet: A simple approach to the evaluation of network protocols,” *SIGCOMM Comput. Commun. Rev.*, vol. 27, no. 1, p. 3141, Jan 1997.