クロスファイア攻撃の効率性分析・脆弱エリア推定

1. 研究背景

DDoS攻撃が社会に与える影響

- 近年、企業や組織を標的としたDDoS攻撃(分散型サービス拒否攻撃)による被害が深刻化しており、社会・経済活動に多大な影響を及ぼしている。
- Crossfire Attack(CFA)は通常のDDoS攻撃と異なり、攻撃対象がサーバではなくリンクであるといった特徴を持つ。
- 従来のDDoS攻撃の検知手法である、攻撃対象サーバでの検知や、異常なトラヒックを識別する手法では検知が困難である。

CFAは今後ネットワークに甚大な被害をもたらす可能性があり、CFAに脆弱なエリアの効果的・効率的な対策が必要である。

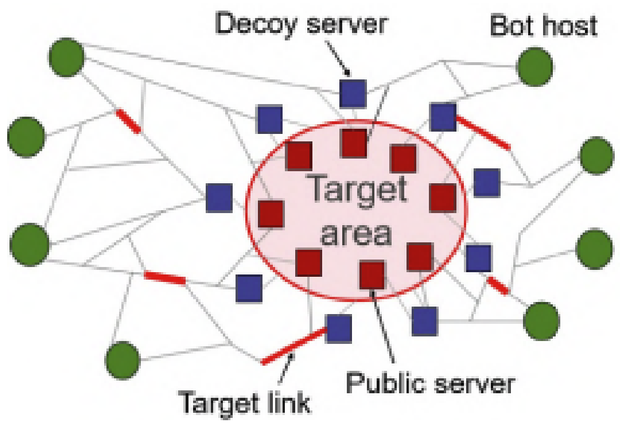
2. クロスファイア攻撃

Crossfire　Attack（CFA)とは？

- 攻撃者が攻撃対象とするエリア（TA)について、TA内のサーバやホストへ向かう外部の通信経路の内、特に多くのデータが流れる「重要なリンク」を意図的に混雑（過負荷）させることにより、TA内のホストが外部と通信できない状況に追い込む攻撃手法である。

CFAの攻撃ステップ：

- 多数のボットからTA内の多数の公開サーバ（Webサーバ等）に対しtracerouteを行うことで、TA内のホスト宛のフローの多くが経由する少数のリンク（攻撃リンク）を発見する。
- 多数のボットからTAの周囲に存在する多数の公開サーバ(デコイサーバ)に対しtracerouteを行い、攻撃対象リンクをフローが経由するボット・デコイサーバ組を選定する。
- 選定したボット・デコイサーバ組に対して、異常な通信であると検知されない程度の少量のトラヒック
  （通常のHTTP request/responseなど)を発生させる。



3. CFAの検知困難性

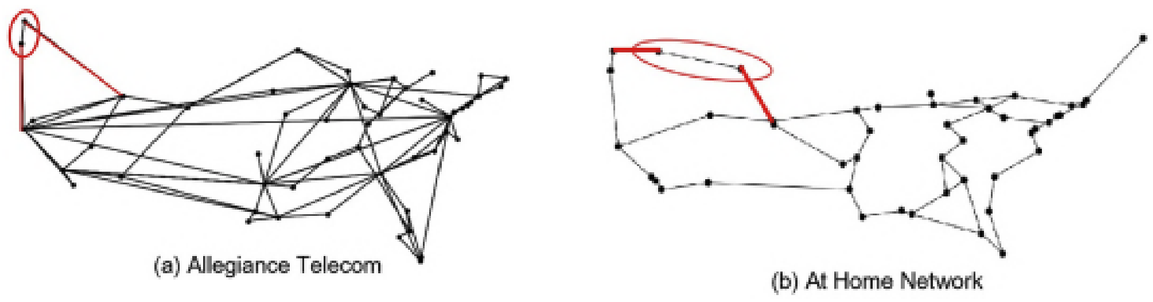
従来のDDoS攻撃との違い

- 従来のDDoS攻撃の検知手法は、攻撃対象サーバで検知を行うが、CFAはTA内のサーバが直接攻撃されないため、被攻撃サーバでの検知が困難である。
- 各ボットが各デコイサーバに対して送付するトラヒック量は少量で、かつ正常ユーザと区別がつかないため、トラヒック量やパケットのペイロードによる識別が困難である。

4. 研究目的

研究目標

- CFAの攻撃者にとっての費用対効果に基づく尺度を提案
- 上記尺度が高い、CFAに対して脆弱なエリアの推定法を提案
- CFAに脆弱なエリアのCFA効率性を、小コストで効果的に低減する技術を提案



5. 今後の予定

- 論文調査
  GCN(graph convolutional network)を用いた、CFAの脆弱エリア推定法に関する先行研究、論文を調査する。
- 定義式の詳細化
  攻撃者にとっての費用対効果である、CFA効率についての定義式を詳細化する。
- 性能評価
  上記定義式について、米国商用ISPバックボーンネットワークを用いた数値評価を行う。
- 国内学会での発表
  研究成果を原稿に執筆し、国内学会での発表を目指す