Traceroute の発生間隔に基づく Crossfire Attack の検知

Detecting Crossfire Attack Based on Interval of Traceroute

仲原 愛美　　上山 憲昭
Manami Nakahara　　Noriaki Kamiyama
福岡大学 工学部 電子情報工学科
Faculty of Engineering, Fukuoka University

1. はじめに

DDoS (distributed denial of service) と呼ばれる，特定のサーバに大量のパケットを送り付けてサーバを機能不全とする攻撃が頻繁に発生している．DDoS 攻撃は攻撃ターゲットとなるサーバで到着パケットを観測することで検知・防御が可能である．しかし近年，特定のサーバではなく，複数のターゲットホスト (TH) を含むターゲットエリア (TA) に至るネットワークのリンクを高負荷とすることで，TH へパケット到達不能とする Crossfire Attack (CFA) の問題が指摘されている [1][2]．CFA では攻撃対象がリンクであるためサーバにおける検知が困難であり，効率的・効果的な検知・防御方式の実現が課題である．CFA では攻撃対象リンクを選定するため攻撃に先立ち，攻撃に用いる大量のボットから TH に対し大量の traceroute が発生する特徴がある．そこで本稿では，traceroute の発生間隔から CFA の攻撃に用いるボットを特定する方式を提案する．

2. Crossfire Attack (CFA)

CFA では攻撃者はまず，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 内のホスト宛てのフローの多くが経由する少数のリンク (攻撃対象リンク) を発見する．次に多数のボットから 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．そして選定したボット・デコイサーバ間に，検知されない程度の少量の正常なトラヒックを発生させることで攻撃対象リンクを過負荷にする．

CFA の検知・防御は以下の理由から困難である．第一に，TA 内のサーバが直接攻撃されるわけではないため，従来の多くの DDoS 攻撃の検知に用いられるホストでの検知が困難である．第二に，攻撃リンクは TA とは異なる AS に属しているため，防御するには AS 間の協力が必要である．そして第三に，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．

3. CFA の提案検知・防御方式

CFA では攻撃に先立ち，攻撃者が攻撃に用いるボット・デコイサーバ組を選定するために，短い時間内に連続して大量のボットと TH/デコイサーバ間で traceroute を行う．そこで閾値時間 (T_s) 内に連続して traceroute を行ったホストをボットとして検知しブラックリスト (BL) 化する．BL 化されたホストに対し，traceroute の返信パケットを廃棄し攻撃リンクの選定を妨害，または攻撃トラヒックを妨害することで，CFA の防御が可能となる．

しかし正常なホストも T_s 以内に連続して traceroute を行う可能性があり，ボットとして誤検知される可能性がある．そこで TH が短い時間内に複数のボットからの traceroute のターゲットとなる特徴を利用して，閾値時間 (T_d) 内に連続して traceroute を受けたホストを TH として検出してターゲットホストリスト (THL) 化し，THL に含まれるホストに対して T_s 内に連続して traceroute を行ったホストをボットとして検知する．

任意のルータが発もしくは着 IP アドレスをキーとするハッシュテーブルを用いて BL と THL を作成する．ルータが traceroute の ICMP パケットで TTL が 0 となるパケットを受信すると，発ホスト (着ホスト)IP アドレスをキーとしてハッシュテーブルに現在時刻を記録する．その際に，既に記録された値と現在時刻との差分が $T_s(T_d)$ 以下である場合に，その発ホスト (着ホスト) をボット (TH) として検出し，BL(THL) に挿入する．ただし通常，1 回の traceroute において複数回の ICMP パケットが送信されることから，ハッシュテーブルには相手ホストの IP アドレスも記録し，相手が記録された IP アドレスと同じである場合にはボットや TH として検出しない．

4. 性能評価

単一ルータにおける ICMP パケットの到着を計算機シミュレーションにより再現し，提案方式の有効性を評価する．正常ホストの traceroute の発生時間間隔は，WIDE のバックボーンネットワークで取得された公開パケットトレースデータを分析して作成した時間分布を用いた．すなわち traceroute の戻りパケットを含む ICMP Type 11 パケットの中から宛先が同じで発アドレスを 2 つ以上含むものを traceroute の戻りパケットをみなして抽出し，同一の発ホストが異なる相手ホストに対して実施した traceroute の時間間隔の分布を作成した．同一ホストの traceroute の平均実施間隔は 2,069 秒だった．各ボットの traceroute の平均発生時間間隔は 1,000 秒に設定した．

ボットは検知を回避するため，各 TH に対して 1 回のみ traceroute を行い，確率 p で TH 以外のランダムに選択したホストにも traceroute を行った．今回は $p = 0.5$ に設定した．また一般ホストはパラメタ 0.2 の Zipf 分布に従いランダムに選択したホストに対し traceroute を行った．traceroute を行う正常ホスト数を 100，ボット数を 50，TH 数を 50，TH 以外の一般サーバを 5,000 に設定し，全ボットが全 TH に traceroute を打ち終わるのに要する時間以上となるよう 700,000 秒間，シミュレーションを行った．またボットの検知を回避するために，各ボットは平均 100 秒の指数分布に従う確率でランダムな間隔ごとに traceroute を開始した．

発着ホストの各々に対し 2 つの閾値を用いる提案方式 (Double Threshold 法) に加えて，比較方式として，発ホストごとの traceroute の時間間隔が T_s 内のホストをボットとして検知する場合 (Single Threshold 法) の，正常ホストをボットとして誤検知する確率 False Positive Ratio (FPR) と，ボットを見逃す確率 False Negative Ratio (FNR) を評価する．図??に $T_d = 50$ に設定し，T_s を変化させたときの各方式の FPR と FNR をプロットする．

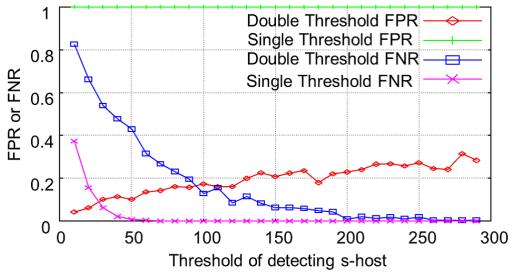

図 1: FPR and FNR of each method against T_s

着ホスト側は考慮しないで発ホストの検知閾値のみ考慮した Single Threshold 法では，正常ホストは 1 度でも T_s 時間内に連続して traceroute を行うとボットとして検知されるため，FPR は 1 となった．一方，着ホスト側においても検知閾値を設定して TH をも検知する提案 Double Threshold 法では，FPR を大幅に低減可能である．提案方式は T_s が小さい場合に FNR が大きいが，T_s を増加させることで FPR の増加を低く抑えながら FNR を大幅な抑制が可能である．

謝辞 本研究成果は，JSPS 科研費 18K11283 の助成を受けたものである．ここに記して謝意を表す．

参考文献

[1] W. Rafique, et al., CFADefense: A Security Solution to Detect and Mitigate Crossfire Attacks in Software-Defined IoT-Edge Infrastructure, HPCC 2019
[2] R. Rasool, et al., Cyberpulse: A Machine Learning Based Link Flooding Attack Mitigation System for Software Defined Networks, IEEE Access, 2019