5E-5

管理対象ネットワークにおけるサービス被害の推定手法

伊豆 博聡† 佐藤 彰洋‡ 笹井 一人†† 高橋 秀幸†† 北形 元†† 木下 哲男††

†東北大学大学院情報科学研究科　‡九州工業大学　††東北大学電気通信研究所

1　はじめに

近年，大量のトラフィックによりサービスを提供不能にするDoS攻撃が大きな問題となっており，深刻な事態を回避するための様々な対策法が検討されている．DoS攻撃に対して対策を講じることは重要であるが，被害状況が不明なまま対策を講じると過剰反応となってしまう為，これらの調査が重要であると言える．しかしながら，実際のネットワークにおいて詳細な状況を調査する為には，ネットワーク機器やサーバの詳細なログを調査しなければならない為，対策に遅れが生じてしまうといった問題がある．

そこで本稿では，エッジネットワークの出入り口やそれよりも上位のルータで観測されたトラフィックに基づき，対象ネットワークの被害状況を推定することで，効率的かつ迅速な被害状況の推定を実現する，上位ルータにおけるサービス被害の推定手法を提案する．

2　関連研究と課題

DoS攻撃による被害状況を同定する評価値として既存研究で用いられているものに，PFT(Percentage of Failed Transactions)[1] がある．PFTはDoS攻撃へのネットワークの耐性を評価する為に用いられており，各サーバ上で収集したログからサービスに関するQoS要件（ユーザが許容可能なQoSの範囲）を満たさないトランザクションの数を元に算出される．既存研究におけるネットワーク耐性の評価は，テストベットネットワークやシミュレーションを用いて行われる為，詳細なログの収集にかかるコストは問題にならないが，実際のネットワークでは詳細なログが膨大な量となるため，既存研究をそのまま適応することは困難である．

上記の問題を解決するため，本研究では機器上から収集する詳細なログを元にする手法ではなく，エッジネットワークのゲートウェイやそれよりも上位のネットワークに位置するルータ（これを**上位ルータ**と呼ぶ）で観測されたトラフィックを元に対象の下位ネットワークで発生している被害状況（これを**サービス被害**と呼ぶ）を推定する手法を提案する．

Estimation of Service Damage in Target Network
Hiroaki Izu†,Akihiro Satoh‡,Kazuto Sasai††,
Hideyuki Takahashi††,Gen Kitagata††,Tetsuo Kinoshita††
†Graduate Scnool of Information Science, Tohoku University
‡Kyushu Institute of Technology
††Research Institute of Electrical Communication, Tohoku University

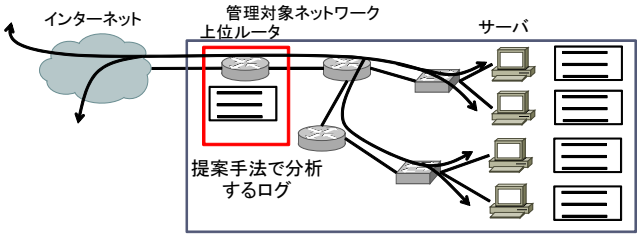

図1: 提案の概要

3　サービス被害の推定手法

図1に，提案手法の概要を示す．本研究では，前述した上位ルータで観測された一連のクライアント・サーバ間通信を集約して得られるフローを分析することでサービス被害を推定する．既存研究で用いられていたPFTに比べて，上位ルータで観測されるフローからは各サーバ上のログを必要とするRTT(Round Trip Time)やパケットロスが正確に計測できない為，本研究では，観測されるフローのパケット到着間隔に着目し，対象ネットワークのサービス被害を算出する．

3.1　妨害されたフローの検出

DoS攻撃の対象となっているネットワークでは，クライアント・サーバ間でやり取りされるフローにおいて，パケットの再送や遅延が発生し，その結果対象ネットワークが提供するサービスのQoSが著しく低下する．ここでは，DoS攻撃によってパケットの再送や遅延が発生しているフローを**妨害されたフロー**と定義し，上位ルータで観測されたトラフィックにおいて，妨害されたフローを推定する手法について説明する．

通常のTCPにおける再送処理は，やり取りされるパケットの到着間隔に基づいてRTO(Retransmission Time-Out)を調整し，現在のRTOが経過しても応答パケットが到着しない場合にパケットの再送を行う．本研究では，現在のパケット到着間隔から送信元によって調整されるRTOを推定し，それをRTOを超えたパケット到着間隔が発生した場合に，再送が発生したとみなす．

具体的には，一定の観測単位時間を用いて到着パケットの処理を行い，単位時間内に発生したフローに関して，連続して再送が発生したと見なされたフローは，妨害されたフローであるとして判定する．また，大規模なDoS攻撃によって深刻な被害を受けている場合には，観測単位時間内に最初に到着した1パケットのみしか

観測されなかったフローが存在する可能性がある．そのようなフローは，RTO を用いた到着パケットの分析では検出できないが，観測単位時間経過後に観測されたフローを検査することで判定を行う．

3.2 サービス被害の導出

本稿で推定するサービス被害の概念は，前述のように，ある DoS 攻撃によって，対象となるネットワークがどの程度深刻なサービス提供不能の状況に陥っているかを示す指標でなければならない．よって，ある観測単位時間内において観測された全フローのうち，3.1 節で示した手法によって妨害されたフローとみなされたフローの割合をサービス被害 SD(Service Damage) と定義する．ここで，SD $\in [0.0, 1.0]$ であり，0.0 に近ければ被害が非常に小さいの状態を示し，1.0 に近い場合は，ほとんどサービスが利用不可能である状態を示す．

既存研究で用いられている PFT は，末端の機器からログを収集することで算出しているため，サービスの利用者が感じる被害状況と一致しているといわれる．本稿で定義した SD は末端の詳細なログに基づいてはいないため，被害状況をよく反映しているかどうかは自明ではないため，実験を用いてこれを評価する．

4 実験と評価

本提案である SD の有効性について評価するため，NS-2[2] を用いたシミュレーション実験を行った．

まず，インターネットのトポロジーモデルである Transit-stub モデル [3] を用いて，計 100 ノードからなるトポロジーを構成した．実験では，stub-domain の一つを管理対象ネットワークとして想定し，当該ネットワーク内のノードはサービスを提供するサーバであると仮定する．また，それ以外の stub-domain にはクライアントが配置されているとし，そのうちのランダムに選択した 10 台を攻撃ノードとした．

実験開始後，クライアントは管理対象ネットワーク内のサーバをランダムに選択し，HTTP 通信を 360 秒間行う．攻撃ノードは，20-60，100-140，180-280[s] にそれぞれ，200, 100, 20Mbps のレートで管理対象ネットワークから選択した攻撃対象に対して DoS 攻撃を行う．

上記シナリオに対して，管理対象ネットワークとして選択した stub-domain がその他の stub-domain と接している境界を上位ルータとみなし，当該ルータを通過するフローを 3 章で示した手法で分析し，SD を算出する．また，比較対象とする PFT は，管理対象ネットワーク内の全ノードにおいて観測されるトラフィックデータを元に，文献 [1] と同様の方法で算出する．

図 2 に，ある試行における SD(提案手法) と PFT の時系列を示す．図 2 の横軸は時間 [s] であり，左の縦軸はそれぞれの手法で求めたサービス被害，右の縦軸は

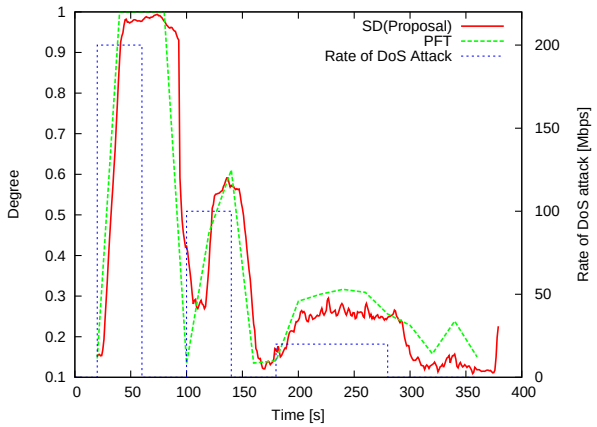

図 2: ある試行における SD(提案手法) と PFT の時系列

DoS 攻撃のレート [Mbps] である．PFT の方が滑らかでないのは，既存手法によって PFT を計算する際に，重複できない区間に分割するためである．結果から，提案手法で求めた SD と PFT の傾向がほぼ一致しており，提案手法がサービス被害を高い精度で推定できているといえる．DoS 攻撃のレートが大きい場合 (20-60[s]) は，既存手法と提案手法で求めた値がほぼ同じであり，DoS 攻撃のレートが小さい場合 (180-280[s]) は，誤差が 10-15%程度であった．また，サービス被害の度合いは，DoS 攻撃のレートにほぼ比例しているが，180-280[s] の DoS 攻撃のように小規模で長期間続く攻撃の場合は，レートに比べて被害が大きい場合等があった．

5 おわりに

本稿では，上位ルータで観測されたフローから，サービス被害の推定を行う手法を提案した．シミュレーション実験より，提案手法によって管理対象ネットワークのサービス被害が推定可能であることを確認した．今後は，さらに大規模なネットワークを対象に，提案手法の精度，および計算時間を評価する予定である．

参考文献

[1] J. Mirkovic, A. Hussain, S. Fahmy, P. Reiher, and R. K. Thomas, "Accurately Measuring Denial of Service in Simulation and Testbed Experiments," IEEE Trans. Dependable and Secure Computing, Vol. 6, 2009.

[2] Network Simulation version2, http://www.isi.edu/nsnam/ns/.

[3] K. Calvert, M. Doar, and E. W. Zegura, "Modeling Internet Topology," IEEE Communications Magazine, Vol. 35, 1997.