4W-8

輻輳型 DoS 攻撃を対象にした優先制御・帯域制御のシミュレーション

安齋　孝志†　佐藤　直†

情報セキュリティ大学院大学†

１．まえがき

インターネットにおいて DoS 攻撃が発生すると，トラヒック輻輳が生じ正常な通信の帯域が圧迫される場合がある．本稿では，web サーバへの攻撃を例に，恣意的なフロー制御と再送・輻輳制御を実施し，結果から DoS 攻撃を検知して，輻輳型 DoS 攻撃が発生した場合でも優先制御および帯域制度により正常な通信の帯域を確保する手法を提案し，計算機シミュレーションによりその有効性を検証する．

２．提案法の概要

対象とするネットワーク構成を図１に示す．同図において，輻輳型 DoS 攻撃により http によるアップデートサービスが困難になる場合を想定する．本稿では，サーバ（あるいは帯域制御装置）から実行されるフロー制御および再送・輻輳制御[1]に対する送信者（クライアント）の反応から，正常な送信者のセッションと DoS 源からのセッションを能動的に識別して，優先制御および帯域制御する方法を提案する．制御全体の流れを図２に示す．以下，フロー制御および再送・輻輳制御により DoS 源を判定することを “プロービング” と呼ぶ．

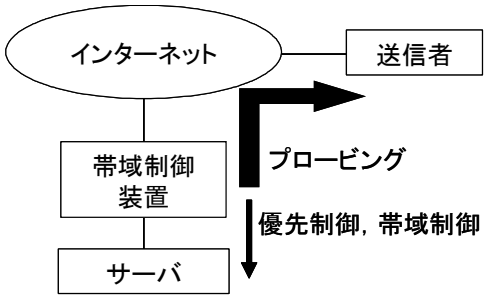

図１　輻輳型 DoS 攻撃に対する制御の概要

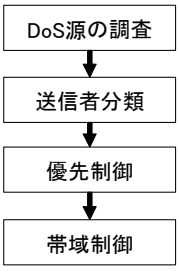

図２　制御の流れ

３．DoS 源の能動的判断方法

提案法の中心となるプロービングについて検討する．

A Simulation on Priority Control and Bandwidth Control against Congestion-type DoS Attacks

† Takashi Anzai , Naoshi Sato,
Institute of Information Security

最初に，フロー制御と再送・輻輳制御の適用方法を考察する．さらにプロービングアルゴリズムを検討する．

３．１　フロー制御と輻輳制御の利用方針

TCP におけるフロー制御と再送・輻輳制御を，実行タイミングとトラヒック量への影響の点から比較すると次のように整理される．

（１）実行タイミング

フロー制御：送信者がサーバから ACK パケットを受信する毎に実行する．

再送・輻輳制御：送信者がサーバから重複 ACK を数回（通常３回）受信した場合に実行する．

（２）トラヒック量への影響

フロー制御：トラヒック増加はない．

再送・輻輳制御：重複 ACK が流れる分トラヒック量が増加する．

以上により，トラヒック量への影響を考慮して，下記のような方針で両制御を利用する．

・通常時（輻輳発生前）；フロー制御を利用する．

・軽輻輳時（輻輳発生予兆時）：重複 ACK による再送・輻輳制御を利用する．

なお，輻輳状態ではさらなる輻輳を招くことから，両制御ともに実施しない．

３．２　プロービングおよび優先度分類

具体的なプロービングとセッション（送信者）分類アルゴリズムを図3に示す．本アルゴリズムでは以下のⅠ～Ⅷを実行する．

Ⅰ．通常時はフロー制御を利用する．図１の帯域制御装置からACKを送信する際，セッション毎広告ウィンドウサイズを恣意的に小さく指定し，送信レートを下げるように指示する．

Ⅱ．各セッションがⅠにより指定した通りのデータサイズで送信してきたかどうかを確かめる．

Ⅲ．指定通りのデータサイズで送信してきたセッションに対しては，以降その送信者からのトラヒックは高優先扱いとする（正常な送信者とみなす）．

Ⅳ．受信総トラヒック量が予め設定した閾値（例．全帯域の50%）を超えた場合，軽輻輳状態と判断しⅤを実行する．

Ⅴ．Ⅱで送信レートが下がらなかったセッションの送信者に対して能動的に（故意に）重複ACKを送信する．

Ⅵ．送信レートが下がったセッションと下がらなかったセッションを分類する．

Ⅶ．送信レートが下がったセッションに対しては，以降その送信者からのトラヒックは高優先扱いとする．

Ⅷ．Ⅵで送信レートが下がらなかったセッションの送信者からのトラヒックは低優先扱いとする（DoS源とみなす）．

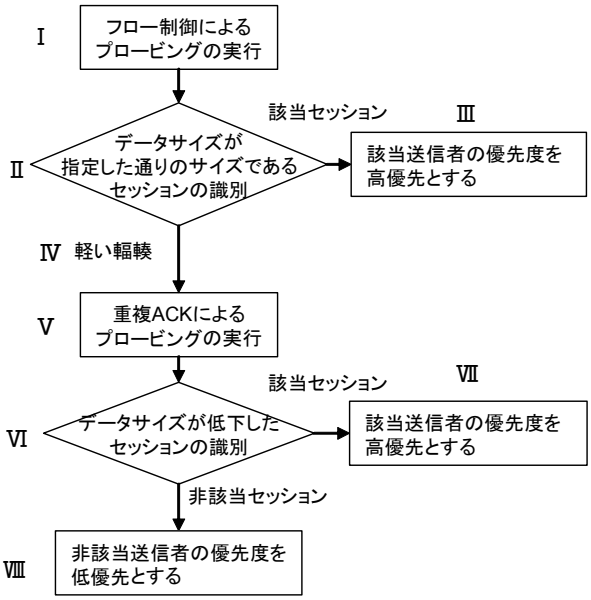

図3　プロービングおよび送信者の優先度分類

4．優先制御

送信者の分類結果に基づき優先制御を実行する．3．2で示したように，送信者がフロー制御および再送・輻輳制御で指示した通りに反応すれば高優先とする．逆に指示通りの反応をしなければDoS源とみなし低優先とする．優先制御方式としては非DoS源を確実に優先できることからPQとする．

5．帯域制御

4の結果，非DoS源とみなした送信者のトラヒックに対しては優先的に帯域を割り当てる．逆に，DoS源とみなした送信者のトラヒックに対しては非DoS源とみなした送信者のトラヒックが使用していない余剰帯域を割り当てる（図4）．

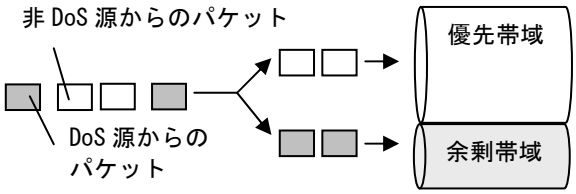

図４　帯域制御のイメージ

6．提案法の効果

提案法を適用することにより次のような効果が期待できる．

(1) 正常トラヒックの可用性の確保．

DoS攻撃とみなされるセッションと正常セッションの差別化により正常セッションの可用性が確保できる．

(2) 誤判定による可用性低下の軽減．

提案法では正常セッションの帯域が圧迫されている条件のもとで，DoS攻撃とみなされるセッションの帯域を制限する．この結果，DoS源の誤判定による可用性低下を軽減することができる．

7．シミュレーションの実施と考察

輻輳制御アルゴリズムとして TCP Reno 方式を想定し，提案法について計算機シミュレーションを実施した．シミュレーションにおけるネットワーク環境は，全送信者数が 6 台で，3 台は正常送信者，残り 3 台は DoS 源である．また，送信するデータサイズは，正常送信者の場合 1M バイト，DoS 源の場合 5M バイトとした．転送遅延については，全送信者から帯域制御装置までの伝送遅延を 50ms と固定に設定し，処理遅延は無視できるものとした．シミュレーションでは全送信者が一斉にデータ送信を開始するものとした．帯域については，帯域制御装置の LAN 側が 1Mbps，WAN 側はそれよりも非常に大きいものと仮定した．

提案法を適用しない場合／適用した場合のスループット特性を調べた．それぞれの結果を図５，図６に示す．なお，ここで，スループットとは，送信者からサーバへのアップロード時における，帯域制御装置 LAN 側の帯域使用率である．横軸は送信開始後の経過時間（秒）である．

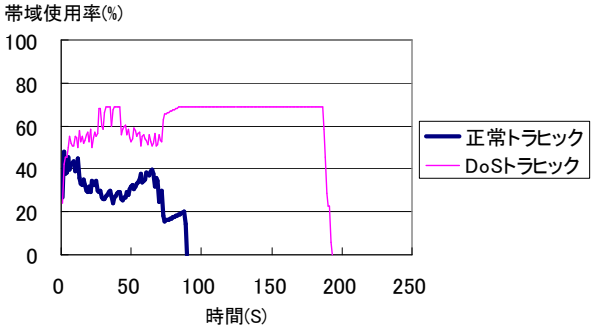

図５　提案法を適用しない場合のスループット特性

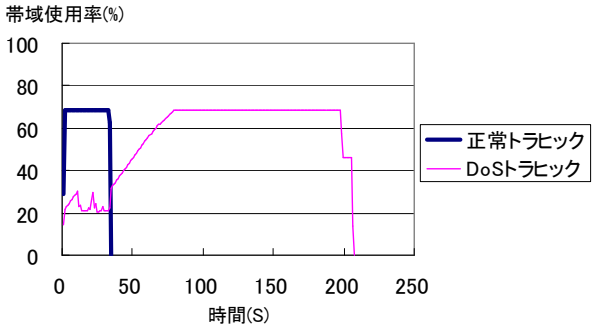

図６　提案法を適用した場合のスループット特性

提案法を適用しないと正常トラヒックが DoS トラヒックにより圧迫されるため可用性が低下することが分かる（図 5）．逆に，提案法を適用すると DoS 源が識別され，優先制御および帯域制御が有効に働くため，正常トラヒックの可用性が確保されることが確認できる（図 6）．

8．まとめ

本稿では，輻輳型 DoS 攻撃を対象にした優先制御・帯域制御法を提案し，計算機シミュレーションによりその有効性を検証した．実環境では送信者数の時間的な変動や遅延時間等が優先制御・帯域制御特性に大きく影響すると考えられる．今後このような実環境における提案法の適用領域を検討する．

文　献

[1]宮原秀夫，尾家祐二：コンピュータネットワーク，7 章，共立出版，1999.