L_043

輻輳型 DoS 攻撃を対象にした優先制御・帯域制御の提案

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 攻撃が実行されると，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，フロー制御と恣意的な再送・輻輳制御を実行して，輻輳型 DoS 攻撃が発生した場合でも正常な通信の帯域を確保する手法を提案する．

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例に検討する．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]に関する送信者（クライアント）の対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，その結果に基づいて優先制御，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・輻輳制御を利用して DoS 源を判定することを “プロービング”と呼ぶ．

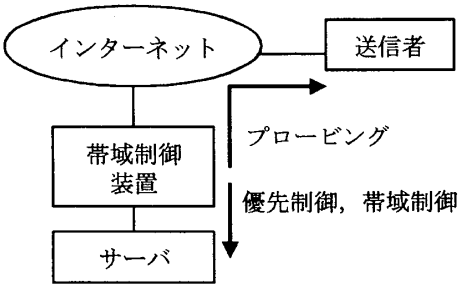

図１　輻輳型DoS攻撃に対する制御の概要

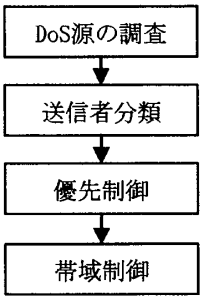

図２　制御の流れ

A Proposal on Priority Control and Bandwidth Control against Congestion-type DoS Attacks
† Takashi Anzai , Naoshi Sato,
Institute of Information Security

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．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適用方針

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なる．

（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 3 回受信した場合，または，再送タイマーが切れた場合に実行する．

（２）トラヒック量への影響

フロー制御：フロー制御による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両制御を使い分ける．具体的には，下記のような方針で適用することとする．

・通常時（輻輳発生前）；フロー制御を利用．
・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．
・重輻輳時：再送タイマーによる再送・輻輳制御を利用．

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～Ⅹ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を送信する際に受信ウィンドウサイズに小さな値を能動的に指定して送信レートの低下を指示する．

Ⅱ．Ⅰにより送信レートが下がったセッションがあるかどうか確かめる．

Ⅲ．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（正常な送信者とみなす）．

Ⅳ．受信総トラヒック量がある閾値（例．全帯域の50%）を超えた場合，軽輻輳状態だと判断する．

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図１の帯域制御装置から能動的に重複ACKを送信する．

Ⅵ．送信レートが下がったセッションがあるかどうか確かめる．

Ⅶ．Ⅵで受信総トラヒック量がある閾値（例．全帯域の80％）を超えた場合，または受信トラヒック量に変化がない場合，Ⅴで実行したセッションに対して図１の帯域制御装置からACKを送信しないようにする．その結果，送信者で再送タイマー切れによる輻輳制御を実行したかを確かめる．

Ⅷ．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．

Ⅸ．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．

Ⅹ．Ⅷ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）．

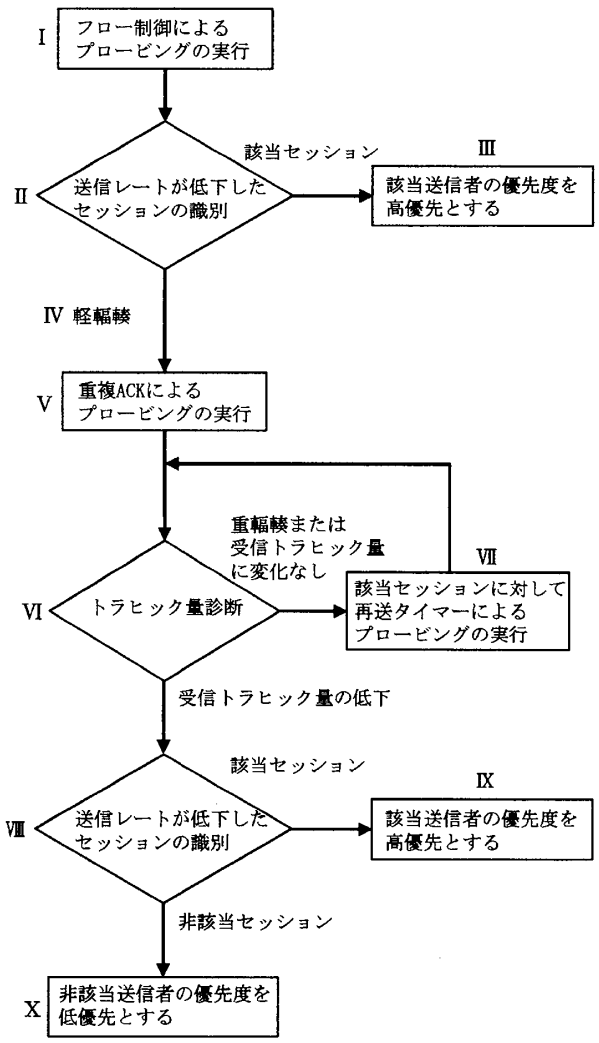

図3　プロービングおよび送信者優先度の分類

４．優先制御

フロー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，送信者が正しい反応をすれば高優先とする．逆に正しい反応をしなければDoS源からのパケットとみなし低優先とする．

５．帯域制御

４で優先度を設定されたセッションに対して帯域幅を設定する．すなわち，非DoS源とみなした送信者からのトラヒックに対しては優先的に帯域を割り当て，DoS源とみなした送信者からのトラヒックに対しては非DoS源とみなした送信者から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）．

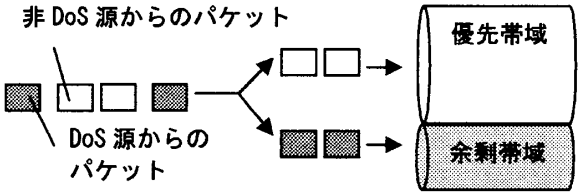

図４　帯域制御のイメージ

６．むすび

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．

本提案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．

今後，提案法の有効性を定量的に評価する予定である．

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.