2008－CSEC－43 (2)
2008／12／5

帯域制御を利用した能動的 DoS 攻撃対策

武藤 展敬 佐藤 直

情報セキュリティ大学院大学
〒221-0835 神奈川県横浜市神奈川区鶴屋町 2-14-1
Email:{mgs075503,sato}@iisec.ac.jp

あらまし ネットワークサービスが日常生活に身近になるにつれて，悪意のある利用者が正常な利用者のサービス利用を妨害する，サービス拒否攻撃や分散型サービス拒否攻撃が与える影響はより深刻化しており早急な対応が望まれる．しかし，サーバに対し過剰な量のデータを流す輻輳型 DoS 攻撃について決定的な対策は研究されていない．一方 TCP の通信プロトコル上では輻輳回避の手法が実装されている．攻撃者はサーバ側を輻輳させることが目的であるため，輻輳回避手法に正常に従ってこないことが予想される．このことからサーバ側からクライアントに対し，故意に輻輳しているとの情報を流し輻輳回避の行動を確認する．ここで従ってこないクライアントを DoS 源として判定し正常な利用者と DoS 源を区別して対応する手法を評価する．

キーワード DoS 攻撃，フロー制御，輻輳制御，プロービング

Active DoS attack measures by bandwidth control.

Hiroyuki Muto Naoshi Sato

Institute of Information Security
2-14-1 Tsuruya-cho Kanagawa-ku Yokohama, 221-0835,Japan

Abstract This study highlights the DoS attacks which send excessive amounts of data to uploading servers, that is, congestion-type DoS attacks. In most cases, the uploading services use TCP on the transport layer. TCP has a function to manage the congestion. This study focuses the control function of TCP and proposes a method(measures) against the congestion-type DoS attacks, where the server intentionally executes the flow control and promotes congestion control of corresponding clients, and then distinguishes source of the attacks by monitoring the response of clients, and further allocates prioritized bandwidth to related TCP connections. The study simulates the proposed method and demonstrates its effectiveness.

Keyword DoS attacks, Flow control, Congestion control, Probing

1 はじめに

近年，インターネットの急速な普及に伴い，様々なネットワークサービスが提供されている．ネットワークサービスが日常生活に身近になるにつれて，悪意のある利用者が、正常な利用者のサービス利用を妨害するサービス妨害攻撃（DoS 攻撃）や複数のホストから同時に DoS 攻撃を行う分散型サービス妨害攻撃（DDoS 攻撃）が与える影響はより深刻化している．たとえば，通信販売サイトを運用しているサーバが DoS 攻撃にあえばサーバ側，利用者双方に直接的な被害を与えることが簡単に実行できる．

近年金銭目的の犯罪事例の報道[1]，botnet の流行から DoS 攻撃が容易に実施できる環境が整いつつあること．DoS 攻撃単体での攻撃ではなく，他の攻撃のログ解析を困難にするツール，サーバをダウンさせた後にフィッシングサイトへ誘導する等の他攻撃の補助として選択される可能性等から再度 DoS 攻撃が注目を集める可能性がある．

2 DoS/DDoS 攻撃について

2.1 DoS 攻撃概要

DoS 攻撃とは，サーバやルータなどのネットワーク

を構成する機器・ネットワーク回線自体に対して攻撃を行い，サービスの提供を不能な状態にする攻撃である．主な攻撃方法として下記に挙げられるようなものが存在する．

2.2 DoS 攻撃の分類

DoS 攻撃は確認されているものにいくつか種類があるが，タイミングで分類した場合に通信コネクション確立時のものと確立後の 2 つタイミングで実施されている．また，攻撃者側が有利な条件で攻撃をしやすいことから攻撃ツール等が複数配布されている．

2.2.1. コネクション確立時の攻撃

コネクション確立時の攻撃として有名なのは SYN Flood 攻撃がある．この攻撃は主として TCP 通信の 3 ウェイ・ハンドシェイク時に返事をしない等の通常通信とは違う通信が確認できることが特徴である．

2.2.2. コネクション確立後の攻撃

コネクション確立後の攻撃としては，F5attack や，MailBomb，輻輳型攻撃等が考えられる．3 ウェイ・ハンドシェイク後に正規通信ではあるが，通信量（通信要求回数・データ量）が対象機器やネットワークが処理できない量を送信してくることが特徴である．

2.3 DDoS 攻撃

DDoS 攻撃とは DoS 攻撃を複数の端末にて同時に実行することで，より大規模に攻撃を行うものである．DoS 攻撃では，単体 PC もしくはごく少数の PC により攻撃が実施されていたが，サーバのハード性能向上により単体 PC では十分な効果が上がりにくくなってきていること・botnet により多数端末から攻撃が容易であること・攻撃者の特定が困難になることなどから，DDoS 攻撃が盛んに行われるようになってきている．最近では，2 ちゃんねるが 2008 年 4 月 DDoS 攻撃により一時的にサービス停止に陥った．サーバでは最終的に韓国から 4000 以上の IP アドレスからの攻撃を確認していると発表している[2]．このように攻撃はより大規模化してきている．

3 関連研究

DoS 攻撃として有名なものとして Flooding 型攻撃がある．この Flooding 型攻撃対策として先行研究が実施されておりいくつかを紹介する．

Flooding 型攻撃として大量のパケットを送る攻撃が確認されている．この攻撃手法に対して原田らはトラフィックパターンを観測し，周期性を考え異常トラフィックを検出する方法を提案した[3]．この方法では過去のトラフィックデータから，未来に起こりうるトラフィック量を予測し閾値を超えた場合に異常トラフィックとして対応しようというものである．ただしこの手法では，単純に予想されるトラフィックが閾値を超えるかを監視しているため，判断方法はあくまで機械的である．

Flooding 型攻撃の中でも SYN Flood 攻撃はコネクションを張る前に攻撃ができるものとして猛威を振るっている．この攻撃に対しては赤池らが，輻輳具合によってハーフオープン状態の待機時間を最適化することで対策することを提案している[4]．この方法では，ハーフオープンのパケットの到着数に着目し多量に到着する場合に輻輳状態と判断,タイマ値を短くするというものである．この手法においても送信者側が正常な利用者か攻撃者かの判断をしておらず，正常な利用者の増加に対して優れた性能が発揮できないことが予想される．

本提案では，従来手法では実施していなかった正常な利用者と攻撃者を能動的に判断することが，DoS 攻撃に対して有効であるのではないかと考え，DoS 源に対する差別化も遮断ではなく，優先制御・帯域制御による対策を実施することで誤検知した場合に対する配慮も含めた提案をするものである．

4 提案法の概要

4.1 対象とする攻撃および手法概要

手法の対応する DoS 攻撃として輻輳型 DoS 攻撃とを考える．輻輳型 DoS 攻撃とは，特定のサーバに対して大量のデータを送ることにより帯域幅を消費させる攻撃をいう．既存対策では，サーバは，過剰な量のトラフィックを検知するとその該当 IP アドレスからの通信を遮断していたが，正常な利用者と攻撃者の区別がされていないため，正常な利用者も影響がある．

TCP には輻輳回避のためフロー制御とび再送・輻輳制御が RFC に規定されている．しかし攻撃者はサーバに多量のデータを送ることを目的としているため，TCP 通信プロトコルを違反して多量のデータを送ることを試みるであろうことが考えられる．通信プロトコルに従ってくる攻撃者については，輻輳発生時には輻輳回避手法により送信レートは自動的に抑えられるため攻撃とはならない．

本手法では，本当の輻輳が発生する前にサーバから送信者に故意に輻輳が発生したと通知し，その後通信プロトコルに正しく従って送信レートを変化させるかを確認する．通信プロトコルに従ってくるものを正常な送信者（正常者），従ってこないものを攻撃者（DoS 源）と判断する．この確認により，誤検知が少なく DoS 源と区別できると考える．また万が一のことを考え，DoS 源に対しては通信遮断でなく，帯域割り当ての低

下という差別化による対策を実施する．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”と呼ぶこととする．

サーバから実行されるプロービングにより，正常者と 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・帯域制御することで輻輳型 DoS 攻撃に対応できる．対策制御全体の流れを図 1 に示す．

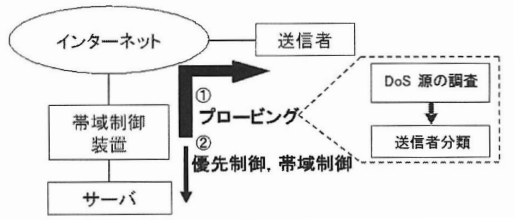

図 1 対策制御の流れ

5 DoS 源の能動的判別手法

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，本手法で利用する TCP の通信プロトコルのフロー制御及び再送・輻輳制御について記載し，次に各々の適用する場合の考え方を示す．最後にプロービングアルゴリズムを提示する．

5.1 フロープロービング

TCP のフロー制御に着目し，「送信者が正常であれば送信者は広告ウィンドウサイズ以下のデータサイズを送信する」というアルゴリズムから，受信側で指定した広告ウィンドウサイズに基づいてデータサイズを決定し送信してきたかで，送信者の正常性の識別する．この識別のため，サーバは故意にフロー制御を実施する．具体的には通信のある段階で故意に広告ウィンドウサイズを小さく指示し、送信者側の送信レートが指示どおりに下がることを確認する．この作業を以下”フロープロービング”と呼ぶ．

フロープロービングを実施すると，正常者であればサーバ側が指定した広告ウィンドウサイズ以下にしてくるが，攻撃者は広告ウィンドウサイズに従っていてはデータを多量に送ることができないことから，指示に従って送信レートを変化させてこないことが予想される．このことからフロープロービングを実施すれば能動的に正常者と DoS 源を判断することが可能となる．

5.2 ACK プロービング

TCP では，何らかの原因で送信データが到達せず，次のシーケンス番号のデータが到達すると，重複 ACK と呼ばれる ACK を返し未受信データの再送依頼をかける．送信者は，重複 ACK を受信すると，重複 ACK を受けたシーケンス番号のデータから送信を再度実行する．またサーバからの再送要求依頼を 3 回受信すると中継網上でパケットの破棄が起こっていると能動的に判断を下し，送信レートを低下させる．この制御に着目し，サーバから故意に重複 ACK を送信することで送信者側の通信レートの減少量を確認しようというものである．

ここで，正常者であれば重複 ACK を受信した時点で，前のデータサイズの半分以下に送信レートを下げてくる．しかし攻撃者は，輻輳制御のように送信レートを半分以下に下げてしまっては攻撃にならないため，TCP の仕様を守らず半分を超えるサイズを送ってくることが予想される．この重複 ACK に対する送信レートの違いを利用して能動的に正常者と DoS 源を判別する．またこの確認作業を”ACK プロービング”と呼ぶこととする．

5.3 フロープロービングと ACK プロービングの実施方針

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フィック量への影響の点から比較して次のように決定した．

(1) プロービングの実行タイミング

フロー制御：送信者がサーバからの広告ウィンドウサイズに基づいて行う．

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される．

(2) プロービングによるトラフィックへの影響

フロープロービング：トラフィック増加はない．

ACK プロービング：重複 ACK が流れる分トラフィック量が増加する．

以上のことから，ACK プロービングのみが通常通信では送信しないパケットを送信していることから，ACK プロービングを実施する場合のみ，トラフィックへの影響を考慮すればよいことがわかる．トラフィックへの影響を考慮して，ACK プロービングはぎりぎりまで実施しないほうがネットワークに余分なパケットが流れないため，下記のような方針で両制御を実施する．

- フロープロービング実施タイミング：すべての新規コネクションに対して実行する．
- ACK プロービング実施タイミング：軽輻輳時（輻輳予兆時）にフロープロービングで非優先となったコネクションに対して ACK プロービングを実行する．

5.4　プロービング及び優先度の分類

具体的なプロービングの実施タイミングとコネクション分類アルゴリズムを図 2 に示す．アルゴリズムは以下のⅠ～Ⅶを実施する．アルゴリズムの結果から正常者と DoS 源に分類される．

新規コネクションにフロープロービングの実施

Ⅰ：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，コネクション毎に広告ウィンドウサイズを故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：各コネクションが前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確かめる．

Ⅲ：指定通りの送信レートを変えてきたコネクションは，正常者とみなす．レートを下げてこないコネクションを DoS 源とする．

ACK プロービングの実施

Ⅳ：帯域制御装置に対してあるタイミングでの受信トラフィック量が予め設定した閾値を超えた場合，軽い輻輳状態と判断しⅤを実行する．

Ⅴ：サーバからⅢで DoS 源としたコネクションに故意に重複 ACK を送信する．

Ⅵ：送信レートが下がったコネクションと低下しなかったコネクションに分類する．
（送信レートが重複 ACK 送信前の 50%以下になったとき低下したと判断する）

Ⅶ：送信レートが下がったコネクションに対して，以降そのコネクションのトラフィックは正常者とする．送信レートが下がらなかったコネクションは DoS 源とみなす．

6　優先制御・帯域制御

送信者の分類結果に基づき帯域制御装置で優先制御を実行する．プロービングの結果，正常者として判断したコネクションを高優先とする．逆に DoS 源を低優先とする．

優先制御方式は正常者を確実に優先したいことから帯域制御装置で受けたパケットをサーバに対して PQ（Priority Queuing）にて実施する．これにより正常者のトラフィックに対しては優先的に帯域を割り当てられる．逆に，DoS 源とみなした送信者のトラフィックに対しては，非 DoS 源とみなした送信者のトラフィックが使用していない余剰帯域が割り当てられる（図 3）．

7　期待する効果

以上の方法から期待している効果は次のように考えている．

(1) 能動的なDoS源の判定による，誤検知によって発生する被害の低減

攻撃者の行動に着目したDoS源判定を実施することにより，従来のDoS源判定方法よりも誤検知率が低下するものと考えられる．また同一IPアドレスから通信がきた場合にも，コネクション単位でDoS源判定が出来る．

(2) 誤検知に対する配慮

判定においてはDoS攻撃パケットだと断定するわけではなくあくまでもみなすだけであり，パケットを廃棄するわけではないので、ある程度の誤検知が許されると考える．その結果，誤検知により正常者のトラフィックが破棄され，全く通信出来ないといった可用性侵害が低減できる．

(3) 正常トラフィックの可用性の確保

DoS攻撃とみなしたコネクションと正常者のコネクションを優先制御により差別化することにより，正常者に対する可用性が確保できる．

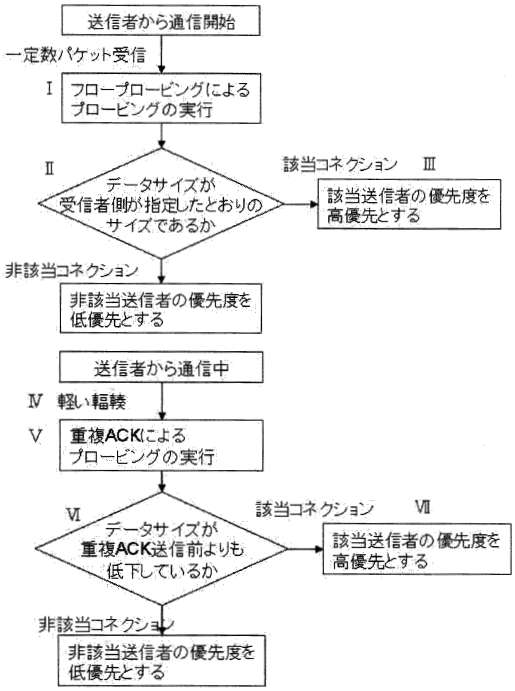

図2 プロービングおよび送信者の優先度分類

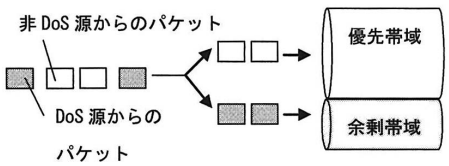

図3 優先制御・帯域制御のイメージ

8 シミュレーション

輻輳型 DoS 攻撃により http によるファイルアップデートサービスが困難になる場合．手法の効果を確認する．シミュレーションを実施するネットワーク構成を図 4 のように設定した．

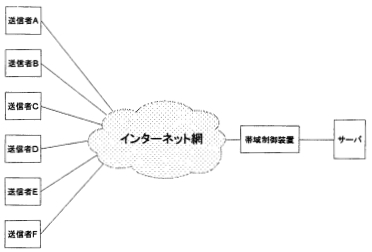

図 4 ネットワーク構成図

またネットワークの条件を次のように設定した．

- 送信データサイズについては，正常端末は 1Mbyte, DoS 源端末は 5Mbyte とする．
- 帯域制御装置でプロービング，優先制御，帯域制御を行う．
- 帯域制御装置の LAN 側の帯域幅を 1Mbps とし WAN 側はそれよりも十分大きいとする．
- サーバを 1 台とし、全端末がサーバにデータをアップロードする．
- 伝送遅延は送信者から帯域制御装置への送信時のみとし，50m 秒とし，送信者，帯域制御装置，サーバにおける処理遅延については無視する．
- 全送信者の送信タイミングは同時とする．
- 同一コネクションから 2 パケット目を受信した時にフロープロービングを実施する．回数については 1 回フロープロービング実行につき 2 回連続広告ウィンドウサイズを抑えたパケットを送信する．
- フロープロービングを実施時の広告ウィンドウサイズはフロープロービング実施前の送信レートと同じサイズを指定する．
- ACK プロービングについては 1 回の実行につき 3 回連続で重複 ACK パケットを送信する．
- ACK プロービングの実施タイミングとして帯域制御装置のサーバ側インタフェースのバッファ使用率が 50%以上のタイミングで通信中の送信者に対して実行する．
- ACK プロービングを実行した後に送信者からの送信レートが重複 ACK 送信前と比較して 50%以下にならない場合は，DoS 源とみなす．
- TCP の送信レートの決定方法については TCP/Reno で規定されている方法を採用した．

実施にシミュレーションをする環境として Linux 上 C 言語にて TCP 上の通信を再現した．

なお以下シミュレーション結果として全正常端末が合計で利用している帯域使用率，全 DoS 源が合計で利用している帯域使用率をまとめたグラフを表示する．また図の X 軸は通信開始からの通信経過時間（単位：秒），Y 軸は帯域盛業装置とサーバ間の帯域使用率（単位：%）を示す．

8.1 手法未実施：正常端末 3 台 DoS 源 3 台

提案手法の効果を明確にするため，未実施時の結果を提示する．正常端末と DoS 源端末の帯域使用率を比較すると DoS 源端末の帯域利用率が正常端末の帯域利用率より上回り，正常端末の通信を妨害していることがわかる（図 5）．

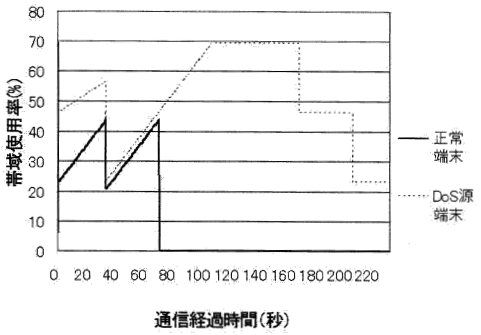

図 5 手法未適用（正常端末 3 台 DoS 源 3 台）

8.2 手法適用：正常端末 3 台 DoS 源 3 台

提案手法を実施した結果を図 6 に示す．比較すると、DoS 源の帯域利用率は対策により大幅に減少し，正常端末に優先的に帯域を割り当てられていることが確認できる．このことから DoS 攻撃中であっても正常端末は問題なく通信できることがわかる．

また DoS 源と検知した場合についても帯域は絞られているものの通信そのものを遮断していないため通信は継続され帯域に余裕が出た後に正常に終了できることも確認できる．

8.3 手法適用：正常端末 1 台 DoS 源 5 台

最後のケースとして端末構成比率を変えた結果を図 7 に表した．結果から考察すると比率を変えても正常端末に優先的に帯域が割り振られることがわかる．このことから端末台数の比率が変わり，台数が増えたとしても正常者が優先され，DoS 源が余剰帯域にて実施されることがわかる．

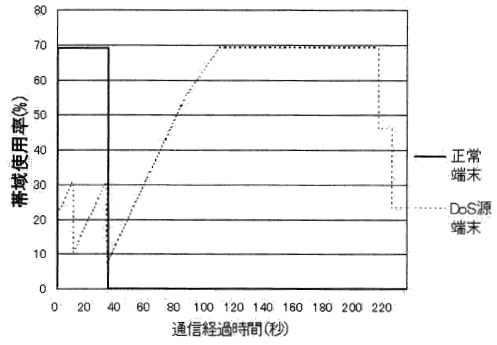

図 6 手法適用（正常端末 3 台 DoS 源 3 台）

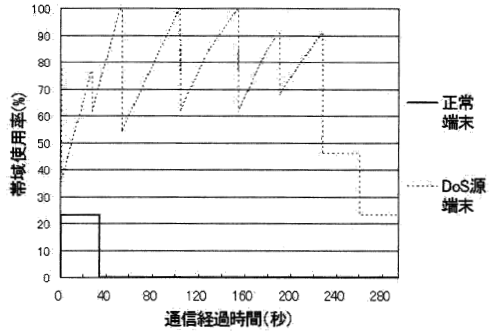

図 7 手法適用（正常端末 1 台 DoS 源 5 台）

8.4 シミュレーション考察

以上のシミュレーション結果から提案手法の効果について考察する．

提案手法は従来の手法に比べて以下の部分が優れているということが確認できた．

- 能動的な正常者と DoS 源の判別
  コネクション毎にプロービングを実施するため，クライアント単位で正常者（非 DoS 源）か DoS 源かの判別が能動的に可能である．
- 誤検知に対する配慮
  DoS 源と判断されても余剰帯域があれば，通信は可能である．このことは従来 DoS 源と判断すると通信が遮断していたことから，DoS 源と判断する閾値に配慮が必要だった点を解決している．
- 正常者への可用性の確保
  正常者であれば正常な端末のみの時と変わらない通信帯域が割り当てられるので DoS 攻撃中であっても正常な端末の可用性が確保される．

以上の点は期待する効果として挙げていた部分と合致し，輻輳型 DoS 攻撃に対する対策としてプロービングは有効である．

9 おわりに

本稿では TCP 環境での輻輳型 DoS 攻撃対策について，プロービングによる正常者と DoS 源との判別アルゴリズムの説明及びシミュレーションによる効果の確認を実施した．既存の TCP の通信仕様を利用し能動的に DoS 源を判断することができることから誤検知が少なく，優先制御・帯域制御を活用するため DoS 源であっても通信を遮断されない，しかも対策も容易に展開が可能な手法である．

今後ネットワークを使ったファイルやデータのやり取りは，ますます盛んになると思われる．ここでファイルのやり取り時の通信仕様は TCP を利用することが予想されることから，攻撃者が DoS 攻撃を実施し，サービスを妨害する可能性は大きくなり，提案手法はますます有効性が増してくると考えられる．

ただし，提案手法についても，まだフロープロービングや ACK プロービングの実施タイミングなどの調査は必要であるため，引き続きシミュレーション等で最適値の調査を続けていく必要がある．またクライアント台数が著しく増え DDoS 攻撃のような状態になった場合にも本当に効果があるかを調査する必要がある．

なお，本研究は，電気通信普及財団の助成を受けたものである．

参考文献

[1]. 日経ニュース,急増する DoS 攻撃にラックが警鐘,"http://itpro.nikkeibp.co.jp/article/NEWS/20070619/275227/" ,Jun.2007.

[2].Big-server.com ニュースリリース，“【公式見解】2ちゃんねるへの DDoS 攻撃および PIE データセンターの障害について”，http://www.maido3.com/server/news/release/2008/20080418_2.html

[3] 原田　薫明,川原　亮一,森　達哉,上山　憲昭,吉野秀明,“周期性を考慮した異常トラヒックの検知手法”,2007 年電子情報通信学会通信ソサイエティ大会 BS-8-5 S-86-87.

[4] 赤池　大史,会田　雅樹,村田　正幸,今瀬　真,“ネットワーク状態適応タイマを用いた SYN Flood Attack 防御技術の検討”,信学技法 IEICE Techical Report IN2007-26 p91-96.