輻輳型サービス不能攻撃に対する防御技術の高度化

代表研究者　佐藤　直　情報セキュリティ大学院大学情報セキュリティ研究科教授
共同研究者　武藤展敬　情報セキュリティ大学院大学情報セキュリティ研究科客員研究員

1 はじめに

インターネットを利用したネットワークサービスが普及するにしたがって，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，いわゆるサービス不能（Denial of Service；DoS）攻撃が深刻化している．特に，IP パケットを大量にサーバに送りつけるタイプの輻輳型 DoS 攻撃では，転送されるパケットの内容やその通信プロトコルは正常であることが多いため，DoS 攻撃の発生を検出することが難しく適切に防御することが困難となっている．

本検討はこのような輻輳型 DoS 攻撃に関する防御技術の高度化を目的として実施したものである．具体的には Web サービスや電子メールサービスのデータ転送プロトコルとして広く適用されている TCP を利用した輻輳型 DoS 攻撃に焦点をあてて検討を行った．TCP は，アプリケーションサービスデータを転送する前に送受信間の接続性を確認する，いわゆるコネクション型の転送プロトコルである．このような TCP に対する輻輳型 DoS 攻撃は，コネクションの確立過程における攻撃とコネクション確立後の攻撃に分けられる．従来の防御手法としては，コネクションの確立過程における攻撃として頻発している SYN フラッド攻撃を対象にしたものが多い[1]-[4]．一方，コネクション確立後の攻撃としてコネクションフラッド攻撃がある．これは多くの TCP コネクションコネクションを確立し,長い時間オープン状態を続けることによりソケットを独占し，サービス不能に陥らせる攻撃である．この攻撃に対しては，コネクションのアイドル接続時間の超過や多数のコネクションの同時確立を拒否する対策がとられるが，いずれも事後的な対策であり，コネクションの占拠を事前に回避する対策の検討例は見受けられない．

近年の Web サービスとして，クライアントが作成したコンテンツをアップロードさせ公開するものが普及している．今後この種の Web サービスへの攻撃として，コネクション確立後に無意味な大量コンテンツをアップロードすることで，他人のアップロードを妨害する DoS 攻撃が増加するもののと想定される．このような，コネクション確立後の輻輳型 DoS 攻撃に対する防御手法[5]-[7]の確立が重要となる．

上述したような従来の検討状況を踏まえ，コネクション確立後の輻輳型 DoS 攻撃に対する防御手法を検討した．具体的には，サーバからクライアントに対し送信レートの低減を要求し，クライアントの対応によって，クライアントが DoS 攻撃源であるか否かを判定し，攻撃源でない／あると判定したクライアントに対してサーバ側の受信帯域を高優先／低優先で割り当てる手法を提案した．さらに，シミュレーションによって提案手法の有効性を検証した．

２　研究の背景

コネクション確立後の DoS 攻撃としては，多くの TCP コネクションを確立し，長い時間オープン状態を続けることによりソケットを占拠するコネクション攻撃，Web サーバに HTTP リクエスト（再読み込み）を大量に送出してサーバをダウンさせる HTTP リクエストフラッド攻撃が代表的である.これらの攻撃はコネクションやデータ転送要求が膨大であることが特徴であるが，通信プロトコルは正常であるため，攻撃の通信と正常な通信を区別するのが難しい．当初，サーバ側では，受付可能なソケット数や HTTP リクエスト可能数等のリソースを増やすことで対処できた．しかし，最近では，ボット化した複数端末からより大規模に攻撃する，いわゆる DDoS 攻撃（Distributed DoS 攻撃）化する傾向があり，従来のリソース増加による対策は有効でなくなっている．このようなことから，現在では，受信トラヒック，すなわちコネクション数やデータ転送要求数について予めしきい値を設定しておき，このしきい値を超えるような状態になると，全ての TCP コネクションを強制的に遮断するのが一般的な対策として用いられている．この対策では，DoS 攻撃を確実に抑止できるが，正常トラヒックと攻撃トラヒックを識別しないため，DoS 攻撃を誤検出した場合は，正常トラヒックが大量に遮断されるという問題があった．

さらに，利用者がサーバからコンテンツをダウンロードするばかりではなく，最近では，利用者自らが作

成したコンテンツをサーバにアップロードして公開するサービスが普及している．このような，アップロードサービスをターゲットにした新しいタイプの DoS 攻撃として，大容量のデータを送り続けサーバ側の回線帯域を独占する攻撃，すなわちネットワーク輻輳型 DoS 攻撃（以下輻輳型 DoS 攻撃と呼ぶ）の発生が懸念される．この輻輳型 DoS 攻撃が発生すると，正常な利用者がアップロードできなくなるため，早急に対策を明らかにする必要がある．この輻輳型 DoS 攻撃への対策として，従来の DoS 攻撃対策と同様に，サーバ側で受信トラヒック量を測定し，受信トラヒック量が予め設定したしきい値を越えた場合，攻撃が発生したものとみなし，全てのコネクションを遮断することが考えられる．しかし，このようなコネクションを遮断する対策では，前節で述べたように，正常利用者もコネクションが遮断されため，正常利用者のサービス可用性が著しく損なわれる，という問題がある．

3　提案法の趣旨

本報告では，TCP により利用者がサーバへデータをアップロードするサービスを対象に，輻輳型 DoS 攻撃対策を検討する．TCP では，トラヒック制御として二つのタイプの方法が規定されている．一つはフロー制御と呼ばれるもので，受信データ量が多く，受信側に設けているバッファメモリの空き容量が少なくなったときに，受信側が送信側に送信レートの低減（もしくは送信停止）を要求する．もう一つは再送・輻輳制御と呼ばれるもので，受信側からの受信確認信号 ACK が所定時間を過ぎても送信側に返信されない（タイムアウトと呼ぶ），あるいは，同一の ACK が重複して返信される（重複 ACK と呼ぶ），といった状態が発生した場合，送信側はネットワークが輻輳しているものと判断し送信レートを低減する．これらの二つのトラヒック制御が行われた場合，正常な利用者（以下正常者と呼ぶ）であればいずれの制御の場合でも，輻輳状態を回避するため送信レートを低減することが期待できる．一方，攻撃者が輻輳型 DoS を行う場合，攻撃者は攻撃を遂行するためいずれのトラヒック制御にも対応しないことが想定される．すなわち，輻輳型 DoS 攻撃者が送信レートを低減することはないものと推定できる．本報告では，ネットワーク輻輳発生時のトラヒック制御に対する，正常者と攻撃者とのこのような対応の違いに基づき両者を識別（判定）して，ネットワーク帯域を制御する方法を検討する．具体的には，従来のような受信データ量の測定結果のみによる受動的判定でなく，コネクション毎に恣意的なフロー制御，あるいは，再送・輻輳制御を実施し，利用者が正常者（非 DoS 攻撃源）であるか攻撃者（DoS 攻撃源）であるかを能動的に分類する．この分類結果から，正常者と判定される利用者に対してはネットワーク帯域を優先的に割り当てる，逆に，攻撃者と判定される利用者に対してはネットワーク帯域を非優先的に，すなわち，正常者に割り当てた帯域以外の余剰帯域を割り当てることとする．本提案の特徴は，コネクション毎に正常者であるか攻撃者であるかをサービス不能状態となる前に判断し，割り当てるネットワーク帯域の量を差別化することによって，DoS 攻撃が発生しても，コネクションを遮断せずに正常者の利用帯域を確保して，サービスの可用性を維持することにある．

4　提案法の実施方針とアルゴリズム

本検討では，コンテンツのアップロードサービスの利用者がサーバとの間に TCP コネクションを確立したあと，コネクション毎にサーバから恣意的なフロー制御，あるいは，再送・輻輳制御を実施し，利用者に故意に送信レートの低減を要求し，利用者がこの要求に応じて送信レートを低減させるかどうかを調べる．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．このプロービング，すなわち，送信レート要求に従う利用者を正常者，従わない利用者を攻撃者と判定する．この判定結果を用いて，正常者に優先的に帯域を，攻撃者に非優先的に帯域を割り当てる．正常者にのみ帯域を割り当て，攻撃者に帯域を全く割り当てないことも考えられるが，プロービング用の IP パケットが輻輳等によって経路途中で廃棄された場合は，正常者であってもプロービングに対応しないため，攻撃者と誤判定される可能性がある．このような誤判定による正常者の可用性の劣化を避けるため，提案法では割り当て帯域の差別化を行う．提案法では攻撃者にも帯域を割り当てるため，攻撃トラヒックを全て遮断することはできないが，余剰帯域しか割り当てられないため実効的に輻輳型 DoS 攻撃が無害化される．

次に，提案手法で利用する TCP のフロー制御及び再送・輻輳制御の概要[8]を示し，各々をプロービングに適用する場合の方針を示す．さらに，この方針に基づく防御アルゴリズムを示す．

フロー制御では，受信側から利用者へ ACK パケットを送信する際， TCP ヘッダにある広告ウィンドウに受信処理可能なデータサイズを書き込み送信する．送信側はパケットのデータをこの広告ウィンドウサイズ以下にして送信する．提案法ではこの制御アルゴリズムを利用し，サーバ側で指定した広告ウィンドウサイズ

以下のサイズで送信してくるか否かで利用者の正常性を識別する．攻撃者は広告ウィンドウサイズの指定を無視することが予想されるため，従来のフロー制御のままで，正常者と攻撃者を識別することが考えられるが，より早くかつ確実に識別するため，提案法ではコネクション確立後早期に恣意的なフロー制御を実施する．具体的には，コネクション確立直後に広告ウィンドウサイズを小さく指示し、利用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．この動作を以下”フロープロービング”と呼ぶ．

次に，再送・輻輳制御では，ネットワークの輻輳状態を送信側で検出し，送信レートを低減することで，輻輳状態を改善する．一般に，受信側では ACK パケットを用いて送信側に未受信データの再送を要求する．ネットワークが輻輳し転送経路の途中で未受信データパケットが廃棄されると，受信側では同一の未受信データの再送を要求する ACK パケットを繰り返し送信側に送出する（これを重複 ACK と呼ぶ）．通常のコンピュータの実装では，重複 ACK を３回受信するとネットワークが輻輳していると判断し送信レートを低下する．送信側が正常者であれば，重複 ACK を受信した後，直前の送信したデータサイズの半分以下にデータサイズを変更する（送信レートを下げる）ことが期待できる．しかし，攻撃者は輻輳状態を維持するため，送信レートを低下させないものと推定される．そこで，提案法ではこの重複 ACK に対し，送信レートを下げるか否かで，利用者の正常性を識別する．この識別のため，サーバは恣意的に再送・輻輳制御を実施する．具体的には，コネクション確立後，故意に重複 ACK を送出し送信側が前述のように送信レートを下げることを確認する．この動作を以下”ACK プロービング”と呼ぶ．

次に，プロービングのトラヒックに与える影響を考察し，プロービングの実施方法について検討する．フロープロービングでは TCP ヘッダ内にある広告ウィンドウサイズを制御する．この広告ウィンドウサイズは受信側から送信側に送られる全てのパケットで通知されるため，フロープロービングのために新たにパケットを用いたり，情報を付加する必要はない．このためフロープロービングの実施に伴うトラヒックは発生しない．一方，ACK プロービングについては，故意に重複 ACK パケットを作成して送信側に転送するため，すなわち，通常の通信では発生しない ACK パケットを送信する必要があることから，故意に転送する ACK パケット分だけトラヒックが増加する．以上から，両プロービングをトラヒック量の点で比較すると，フロープロービングの方が望ましいことが分る．このため，全ての TCP コネクションに対して，コネクション確立後早期にフロープロービングを実施することにする．しかし，フロープロービングの実施タイミングが知られると，攻撃者は送信レート低減要求に一時的に従って，すなわち，正常者のように振舞ってサーバ側の判定を誤らせる,すなわち正常者になりすます，ことが想定される．このような，攻撃者の振る舞いを抑止するには，ランダムに複数回フロープロービングを実施すればよいが，逆に，正常者の送信レートも不必要に低下させることになり望ましくない．そこで ACK プロービングを補助的に適用することにする．すなわち，フロープロービングをかいくぐった攻撃者を検出する目的で ACK プロービングを実施する．ACK プロービングの実施タイミングについて，前述したように，ACK プロービングはトラヒックを増加することから，非輻輳状態で行うとその影響が比較的大きい．このため，ACK プロービングは輻輳状態で行うのが望ましい．しかし，実施タイミングが遅れると正常者の可用性の低下もより大きくなることから，輻輳が深刻になる前に，すなわち，軽度の輻輳状態で実施する．具体的には，サーバ側で受信トラヒック（コンテンツ）量を監視し，帯域の利用率があるしきい値を超えた場合，フロープロービングで正常と判定された利用者を対象に ACK プロービングを行う．両プロービングの実施方針をまとめると以下のようになる．

・フロープロービング：全てのコネクションに対してコネクション確立後早期に実施する．

・ACK プロービング：フロープロービングで正常と判定された利用者を対象に軽輻輳発生時に実施する．

両プロービングにより利用者が正常者か攻撃者を判定した後，前者に優先的に帯域を割り当て，後者に対して非優先的に帯域を割り当てる．この帯域制御法としては，優先コネクションでデータ転送が行われている場合は全ての帯域を優先コネクションが使用し，優先コネクションのデータ転送完了後に非優先コネクションのデータ転送が可能になる，優先度キューングˊ PQ（Priority Queuing）方式[9]を採用する．

以下，これまでに述べた提案法のアルゴリズムを図１のモデルで検討する．

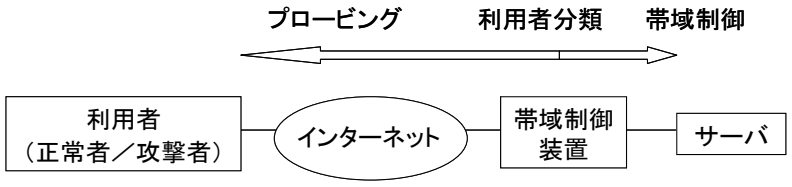


図1　検討モデル

具体的に,帯域制御置はインターネットを介したプロービング,プロービング結果に基づく利用者の分類,および帯域制御装置とサーバ間の帯域制御を実施する．図１の帯域制御装置は図２に示すようなフローで提案法を実施する．同フローはⅠからⅧのステップからなっており，前半のⅠからⅣではフロープロービングを行い，後半のⅤからⅧではACKプロービングを行い，利用者分類（判定）と帯域制御をそれぞれ実施する．以下，各ステップについて詳述する．

＜フロープロービングの実施＞

利用者のデータ受信開始時に実施する．

Ⅰ．フロープロービング

広告ウィンドウサイズを故意に小さく指定して利用者に転送する．具体的には，サーバが受信可能なデータサイズ（バッファ量）よりも十分小さい広告ウィンドウサイズを連続回設定して，データサイズ（送信レート）を抑制するように指示する．

Ⅱ．受信データサイズの確認

次に利用者から転送されるデータのサイズがⅠで指定したサイズ以下かどうかを判定する．

ⅢとⅣ．利用者分類と帯域制御

Ⅱで指定したとおりにデータサイズを変更した利用者を正常者と判定し,そうでない利用者を攻撃者と判定する．この判定結果から，正常者には帯域を優先的に割り当て，攻撃者には非優先的に割り当てる．

＜ACKプロービングの実施＞

帯域制御装置とサーバ間の帯域の利用率があらかじめ設定した閾値を超えた場合,軽い輻輳状態が発生したと判断し，Ⅱにおいて正常者と判定された利用者を対象に実施する．

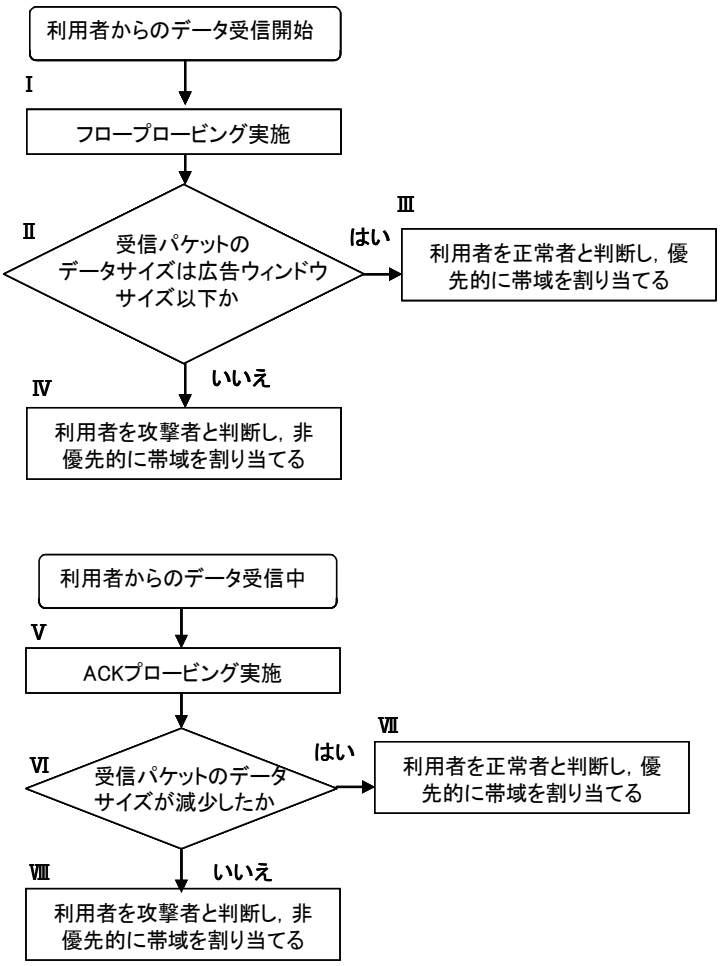


図2 提案法の実施フロー

Ⅴ．ACK プロービング

故意に同一の ACK を連続（３回以上）して利用者に転送する．

Ⅵ．受信データサイズの確認

次に利用者から転送されるデータのサイズが ACK プロービングの直前に転送されたデータのサイズの 50%以下かどうかを判定する．

ⅦとⅧ．利用者分類と帯域制御

Ⅵで，データサイズを 50%以下に変更した利用者を正常者と判定し，そうでない利用者を攻撃者と判定する．この判定結果から，正常者には帯域を優先的に割り当て，攻撃者には非優先的に割り当てる．

5　シミュレーション

データアップロードサービスを対象に，提案手法を模擬するプログラム（C 言語）を作成し，計算機シミュレーションを実施した．シミュレーション条件を次の(1)から(4)のように設定した．

(1)ネットワーク構成

図１の構成とする．同図には１台の HTTP サーバがあり，同サーバはインターネット側からのアップロードデータを受信する．帯域制御装置は双方向のプロキシとして機能し TCP コネクションを仲介するとともに提案手法のプロービング，利用者分類および帯域制御を行う．利用者は複数であり，各々正常者あるいは DoS 攻撃者のいずれか固定とする．

(2)シミュレーション諸量

帯域制御装置とサーバ間の帯域幅は 1Mbps としインターネット側はそれよりも十分に大きいとする．また， 伝送遅延は利用者から上り方向を 50m 秒とする．下り方向についてはトラヒック量が小さいため無視できるものとする．さらにサーバにおける処理遅延も無視できるものとする．正常者に比べ攻撃者は大きな容量のコンテンツをアップロードするものとし，正常者は 1M バイト，攻撃者は 5M バイトをアップロードするものとする．

(3)プロービング条件

①フロープロービング

最初に利用者からデータを受信した直後にフロープロービングを実施する．フロープロービングで指定する広告ウィンドウサイズは，受信バッファメモリの空き容量と直前に受信したデータサイズの小さい方とする．

②ACK プロービング

TCP の輻輳制御方式は最も使用されていると推定される TCP/Reno 方式[6]とする.ACK プロービングの実施タイミングは，帯域制御装置とサーバとの間の帯域（1Mbps）の利用率が 50%を越えた直後とする．1 回の実施につき 3 回連続で重複 ACK パケットを送信する．

(4)利用者判定と帯域制御

フロープロービングの場合，受信データが指定した広告ウィンドウサイズ以下ならば正常者，そうでない場合は攻撃者とみなす．ACK プロービングの場合，受信データサイズが ACK プロービング実施前の 50%以下ならば正常者，そうでない場合は攻撃者とみなす．帯域制御は PQ 方式とし，優先／非優先の二つのキューを設定する．正常者のパケットは優先キューで，攻撃者のパケットは非優先キューで転送処理する．

以下，提案法を実施しない場合１ケース，提案法を実施した場合３ケースについて，シミュレーション結果を示す．シミュレーションシ結果は複数の正常者が利用している合計の帯域，および複数の攻撃者が利用している合計の帯域を，帯域制御装置とサーバ間の帯域に対する割合（利用率）の特性として表し，提案法の有効性を評価する．以下シミュレーション結果例を図３に示す

＜ケース１：提案法を適用しなかった場合・・・正常者数３，攻撃者数３＞

提案法の適用効果を比較評価するため，正常者数３と攻撃者数３として，提案法を適用しない場合のシミュレーションを行った．正常者と攻撃者は時刻０から同時にアップロードを開始している（ケース２とケース３も同じく，正常者と攻撃者は時刻０から同時にアップロードを開始している）．図３において両者の帯域利用率を比較すると，利用開始時から 40 秒近傍まで攻撃者の帯域利用率が正常者の帯域利用率を上回り，正常者の通信を妨害していることがわかる．正常者がアップロードを完了するのに約 80 秒程度要している．

＜ケース２：提案法を適用した場合・・・正常者数３，攻撃者数３＞

ケース１と同じく,正常者数３と攻撃者数３として,提案法を適用した場合のシミュレーションを行った．

図３において，ケース１と比較すると，ケース２では攻撃者の帯域利用率が提案法により大幅に減少し，正常者に優先的に帯域が割り当てられていることが確認できる．正常者がアップロードを完了する時間はケース１に比べ短く，約 40 秒程度であることがわかる．さらに，攻撃中であっても未適用時と違い正常者の帯域利用率が一定に保たれていることも確認できる．一方，攻撃者の帯域は抑制されているものの遮断されていないため通信は継続されることも確認できる．

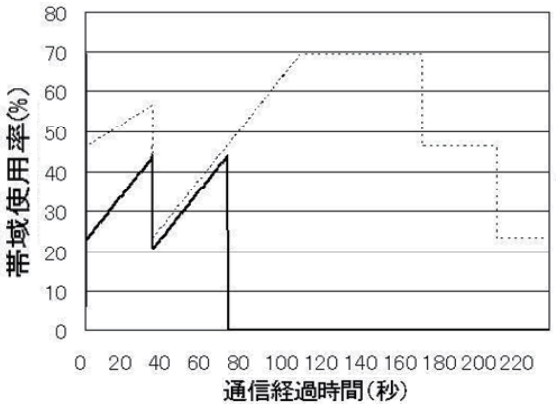
＜ケース３：提案法を適用した場合・・・正常者数１，攻撃者数５＞

ケース２における正常者と攻撃者の比率を変えシミュレーションを行った．図３から，比率を変えても正常者に優先的に帯域が割り振られることがわかる．正常者がアップロードを完了する時間はケース２と同じく約 40 秒程度であることがわかる．

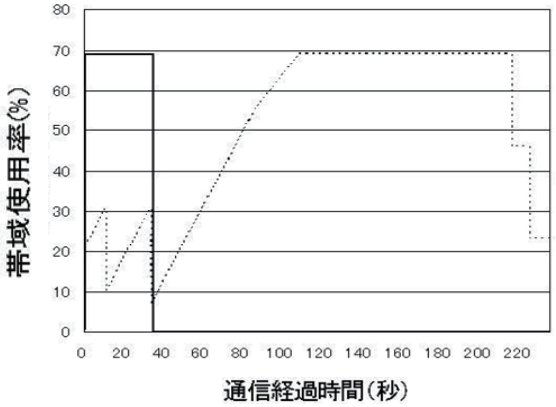
なお，本ケースの利用者数条件を変え，正常者数 1・攻撃者数 999 とした場合についてもシミュレーションを実施した．この場合であっても図 3 と同様の結果となった．このことから,DDoS のように攻撃者数が正常者より圧倒的に多いような状況であっても，提案法により正常者の可用性が確保されることが分かる．

＜ケース４：提案法を実施した場合・・・正常者数１，攻撃者数５＞

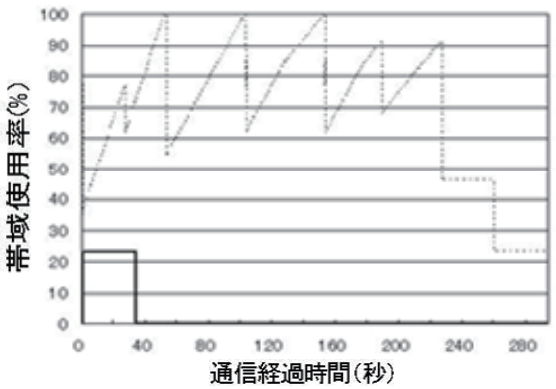
ケース３と同じ正常者数 1，攻撃者数 5 であるが，正常者の通信の開始を遅延させた場合，すなわち，輻輳型 DoS 攻撃を受けている途中から，正常者がデータ送信開始（送信開始時刻は 50 秒）した場合についてのシミュレーション結果である．この結果から，攻撃中に正常者の通信が開始された場合でも正常者の通信が優先されることが確認できる．以上のことから本提案法は，通信の開始タイミングによらず有効であることがわかる．



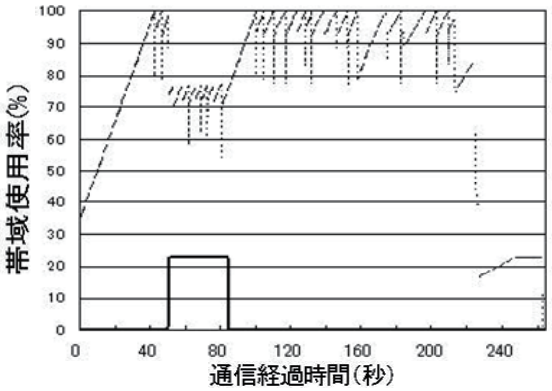
＜ケース1：提案法を適用しなかった場合
・・・正常者数3，攻撃者数3＞



＜ケース2：提案法を適用した場合
・・・正常者数3，攻撃者数3＞



＜ケース3：提案法を適用した場合
・・・正常者数1，攻撃者数5＞



＜ケース4：提案法を適用した場合
・・・正常者数1，攻撃者数5＞

——— 正常者　　--------- 攻撃者

図3　シミュレーション結果

6 考察

これまでの検討結果から提案手法の特徴と適用性について考察する.

(1)利用者の分類

提案法ではTCPコネクション毎にプロービングを実施するため,利用者(サーバのクライアント)単位で正常者か攻撃者かの分類(判別)を能動的に行うことが可能である.従来法ではこのような利用者分類を実施していなかったため,全ての利用者に対して一律の対応(全て通信を許可するかあるいは禁止する)で臨むしかなかったが,提案法により,正常者か攻撃者かを分類し,両者を差別化して防御することが可能となった.

(2)誤検知

利用者の反応に着目した攻撃者(DoS源)判定を実施することにより,従来法よりもDoS攻撃発生の誤検知率が低下するものと考えられる.また同一IPアドレスからの通信がきた場合にも,コネクション単位でDoS源判定を行うことができることからクライアント(ポート)単位での識別も可能になる.さらに,攻撃者と判断されても通信が遮断されるわけではなく,送信レートを抑えられるだけであるため,サーバ側に余剰帯域があれば,通信は可能であり,正常者が通信を終了した後に攻撃者も通信を行うことができる.従来法では,DoS攻撃が発生したと判断すると全てのコネクションを切断していたため,DoS攻撃の検知閾値を慎重に設定する必要があったが,提案法は攻撃者に対しても帯域を割り当てるため,この問題が緩和される.

(3)可用性

提案法により正常者と判別されれば,送信レートを落とすことなく通信が可能である.これは正常者のみの場合と変わらずに帯域が利用できることを意味する.また,前述のシミュレーション結果からも分かるように,DoS攻撃を受けている期間は,DoS攻撃者にも帯域を割り当てている分だけ,正常者の利用帯域は減少するが,正常者の可用性を確保することができる.このため,従来法に比べ,提案法はDoS攻撃に関する正常者の可用性が向上すると言える.

(4)拡張性

実際の輻輳型DoS攻撃では,本検討のシミュレーションで想定した数よりも非常に多くの攻撃者が攻撃を仕掛けることが考えられる.本攻撃はTCPコネクション確立後に実施されることから,対象となる攻撃者数の上限はサーバで受け入れ可能なコネクション数である.この受け入れ可能コネクション数は代表的なサーバの場合1000から2000程度である.従って,提案法の拡張性(スケーラビリティ)は,帯域制御装置がこの程度のコネクションについて個別にプロービングを実施してさらに帯域制御が可能かどうか,ということに依存する.現在市販されている帯域制御装置の対応コネクション数は数千から数十万程度であることから提案法を実装することが十分可能であると考えられる.

7 まとめ

本報告では,コンテンツアップロードサービスを対象にした輻輳型DoS攻撃について,防御技術の高度化を検討した.具体的には,プロービング(恣意的なフロー制御および再送・輻輳制御)による正常者と攻撃者との能動的判別と帯域制御による対策手法を提案し,計算機シミュレーションによってその効果を確認した.提案法は既存のTCPの仕様を利用し能動的に攻撃者を個別に検知することができ,正常者と攻撃者を差別して帯域を割り当てることができる.また,正常者と攻撃者の判別誤り,すなわち誤検知が生じても,正常者の可用性を確保することが可能であるという特徴を有する. 今後,インターネットを使ったアップロードサービスはますます盛んになると思われることから,提案手法の有効性が増すものと考えられる.今後の検討課題としては,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の最適化,実際の輻輳型DoS攻撃に対する提案法の有効性の検証,が挙げられる.

【参考文献】

[1] J. Lemon: Resisting SYN flood DoS attacks with a SYN cache, USENIX BSDCon2002,pp.89-98, Feb.2002.
[2] D.J.Bernstein: SYN cookies, http://cr.yp.to/syncookies.html (2009年6月現在).
[3] H. Wang, D. Zhang, and K.G. Shin : Detecting SYN flooding attacks, Proceedings of IEEE INFOCOM2002, pp.1530-1539, June 2002.
[4] Y. Ohsita, Shingo Ata,and Masayuki Murata : Detecting distributed Denial-of-Service attacks by analyzing TCP SYN packets statistically, IEICE Transactions on Communications, Vol.E89-B, No.10,

pp. 2868-2877, Oct. 2006.
[5]安齋孝志,佐藤直：輻輳型 DoS 攻撃を対象にした優先制御・帯域制御の提案，第 5 回情報科学技術フォーラム(FIT2006)，L-043，Sep. 2006.
[6]安齋孝志,佐藤直：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，情報処理学会平成 19 年（第 69 回）全国大会，4W-S，Mar. 2007.
[7]武藤展敬，安齋孝志，佐藤直：輻輳型 DoS 攻撃に対する能動的判別手法，2008 年暗号と情報セキュリティシンポジウム 1C2-3，Jan. 2008.
[8]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.
[9]P.Ferguson，G.Huston 著，戸田巌監訳：インターネット QoS，3 章，オーム社，2000.

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
A Study on Priority Control and Bandwidth Control against Congestion-type DoS Attacks	IEEE CQR 2008 International Workshop	2008. 4
帯域制御を利用した能動的 DoS 攻撃対策	情報処理学会コンピュータセキュリティ研究会 2008-CSEC-43	2008. 12
帯域制御を利用した輻輳型 DoS 攻撃対策の評価	2009 年暗号と情報セキュリティシンポジウム 3E3-2	2009.1