(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4481780号
(P4481780)
(45)発行日　平成22年6月16日(2010.6.16)　(24)登録日　平成22年3月26日(2010.3.26)

(51)Int.Cl.　F I
H04L 12/56 (2006.01)　H04L 12/56　200Z

請求項の数 10　(全 11 頁)

(21)出願番号　特願2004-278606 (P2004-278606)
(22)出願日　平成16年9月27日 (2004.9.27)
(65)公開番号　特開2005-110255 (P2005-110255A)
(43)公開日　平成17年4月21日 (2005.4.21)
審査請求日　平成19年6月29日 (2007.6.29)
(31)優先権主張番号　10/674208
(32)優先日　平成15年9月29日 (2003.9.29)
(33)優先権主張国　米国(US)

(73)特許権者　596092698
アルカテル－ルーセント　ユーエスエー　インコーポレーテッド
アメリカ合衆国　０７９７４　ニュージャーシィ，マレイ　ヒル，マウンテン　アヴェニュー　６００－７００
(74)代理人　100094112
弁理士　岡部　讓
(74)代理人　100064447
弁理士　岡部　正夫
(74)代理人　100085176
弁理士　加藤　伸晃
(74)代理人　100106703
弁理士　産形　和央

最終頁に続く

(54)【発明の名称】ＴＣＰサーバへのＳＹＮパケット帯域幅攻撃から防御する方法および装置

(57)【特許請求の範囲】
【請求項１】
ゲートウェイの使用とともにネットワークにおけるＴＣＰパケットを分配する方法であって、前記ゲートウェイは、１つ以上の入力ポート、１つ以上の出力ポート、および複数のキューを備え、前記複数のキューの少なくとも１つが、ＳＹＮキューとして指定され、前記方法が、
前記入力ポートの１つからＴＣＰパケットを受信する工程と、
前記ＴＣＰパケットがＳＹＮパケットかどうかを決定する工程と、
それがＳＹＮパケットであるなら、前記ＴＣＰパケットを前記ＳＹＮキューの１つに挿入する工程と、
それがＳＹＮパケットでないなら、前記ＴＣＰパケットを、前記ＳＹＮキューの１つではない前記複数のキューの１つに挿入する工程と、
公正スケジューリング・アルゴリズムに基づき、前記出力ポートの１つを介して送信するために前記ＴＣＰパケットをスケジューリングする工程とを含む方法。
【請求項２】
前記公正スケジューリング・アルゴリズムは、ラウンド・ロビン・スケジューリング・アルゴリズムを含む請求項１に記載の方法。
【請求項３】
前記ＳＹＮキューの１つではない前記複数のキューは、パー・フロー・キューを含み、ＴＣＰパケットを格納する各パー・フロー・キューは、別個のＴＣＰ接続フローに関連す

る請求項１に記載の方法。
【請求項４】
前記ＳＹＮキューの１つではない前記複数のキューそれぞれは、それらに関連するキュー長さを有し、前記ＴＣＰパケットを前記ＳＹＮキューの１つではない前記複数のキューの１つに挿入する前記工程は、それらに関連する前記キュー長さにしたがって格納されたキューのサブリストのチェーンとして、前記ＳＹＮキューの１つではない前記複数のキューを維持する工程を含む請求項１に記載の方法。
【請求項５】
前記ＳＹＮキューの１つではない前記複数のキューそれぞれは、それらに関連するキュー長さを有する請求項１に記載の方法。
【請求項６】
前記ＴＣＰパケットがＳＹＮパケットであり、かつ前記ＳＹＮキューが一杯であれば、前記ＳＹＮキューの１つから前に挿入されたＳＹＮパケットを取り除く工程をさらに含む請求項１に記載の方法。
【請求項７】
前記ＴＣＰパケットがＳＹＮパケットではなく、かつＳＹＮキューではない前記複数のキューが一杯であれば、前記ＳＹＮキューの１つではない前記複数のキューの１つからＳＹＮパケットではない前に挿入されたＴＣＰパケットを取り除く工程をさらに含む請求項１に記載の方法。
【請求項８】
前記前に挿入されたＴＣＰパケットは、前記ＳＹＮキューの１つではない前記複数のキューの最大のキューから取り除かれる請求項７に記載の方法。
【請求項９】
前記ＳＹＮキューは、それに関連する容量を有し、前記容量は、許容される不完全な接続の最大数を提供し、ＳＹＮキューではない複数のキューは、それに関連する確立された数の接続を有し、許容される不完全な接続の前記最大数は、確立された接続の数に数学的に比例する請求項１に記載の方法。
【請求項１０】
ネットワークにおいてＴＣＰパケットを分配するネットワーク・ゲートウェイであって、前記ゲートウェイは、１つ以上の入力ポート、１つ以上の出力ポート、および複数のキューを備え、前記複数のキューの少なくとも１つが、ＳＹＮキューとして指定され、前記ゲートウェイはさらにプロセッサを備え、プロセッサが、
前記入力ポートの１つからＴＣＰパケットを受信し、
前記ＴＣＰパケットがＳＹＮパケットかどうかを決定し、
それがＳＹＮパケットであるなら、前記ＴＣＰパケットを前記ＳＹＮキューの１つに挿入し、
それがＳＹＮパケットでないなら、前記ＴＣＰパケットを、前記ＳＹＮキューの１つではない前記複数のキューの１つに挿入し、かつ
公正スケジューリング・アルゴリズムに基づき、前記出力ポートの１つを介して送信するために前記ＴＣＰパケットをスケジューリングするように構成されるネットワーク・ゲートウェイ。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般にインターネット・セキュリティの分野に関し、より詳細には、ＳＹＮ帯域幅攻撃として知られている、ある形態のサービス拒否（ＤＤｏＳ）攻撃から防御する問題に関する。
【０００２】
サービス拒否（ＤＤｏＳ）攻撃は、限定されたサーバ・リソースが、正当なユーザの代わりに攻撃に割り当てられるときに、サービスを混乱させる。分散されたサービス拒否（

ＤＤｏＳ）攻撃は、地理的に異なるインターネット・ノードから犠牲者へ向かう統合されたＤｏＳ攻撃を開始する。攻撃するマシンは、通常、遠隔マスタによって制御される損なわれたゾンビ・マシンである。通常攻撃の下のリソースは、リンク帯域幅、サーバ・メモリおよびＣＰＵ時間を含む。分散されたＤｏＳ攻撃は、特に攻撃者が、ネットワーク・トポロジの内部情報を有するときに、トラフィックを変換する集中効果のためにより強力である。ルート・ネーム・サWーバ上の「ＴＣＰ　ＳＹＰ　ｆｌｏｏｄ」、「ｓｍｕｒｆ　ＩＰ　ｇｏｉｎｇ」、および帯域幅攻撃は、全て以前に展開されたそのような攻撃の例である（各これらの攻撃は、当業者には良く知られている）。しかしながら、実際に、以前に知られているよりはるかに多くのそのような攻撃が存在することが報告されている。

【背景技術】

【０００３】

リソース枯渇に抵抗するためのサーバ動作システムを改善する多くのアプローチが存在する。いくつかのアプローチは、ステートフル・ハンドシェーク・プロトコル（当業者には良く知られている）上の攻撃からサーバを保護するために、より良好なネットワーク・プロトコル・デザイン原理を考慮していた。ＩＰトレース・バックは、他の良く知られているアプローチであり、攻撃するパケットをたどってその発信元に戻るネットワーク・ワイドの統合された努力である。しかしながら、そのようなアプローチは、明らかにネットワーク・ワイドの協働および調和を必要とする。

【０００４】

さらに、ＤＤｏＳ攻撃ツールは、時間にわたって突然変異しかつ進化する傾向があり得る。例えば、エグレス・フィルタリングのより広い展開とともに、攻撃者は、疑う余地もなく、ほぼ開いたままとされるドア（例えば、ＴＣＰ、ＤＮＳ）を利用する。攻撃のサインは、検出を回避するために変更しまたは消えることができる。したがって、高度な将来の攻撃は、正当なものとほとんど識別できなくなりそうである。したがって、問題に対するフィルタリングだけに基づくアプローチは、有効ではないだけではなく不十分でもある。多くの間違った確実性は、調査を、新たな発見的研究に関する画板に戻させる。

【０００５】

ＴＣＰサーバ上のある特定のタイプのＤＤｏＳ攻撃は、その限定されたリソースが枯渇されるまで、目標のサーバへの新たなＴＣＰ接続を連続して生成することによって開始されることができ、したがって、正当なユーザからのサービス要求を受けなくさせる。（当業者に良く知られているように、ＴＣＰは、良く知られている標準の伝送制御プロトコルの防御部門である。例えば、Ｉｎｆｏｒｍａｔｉｏｎ　Ｓｃｉｅｎｃｅｓ　ＩｎｓｔｉｔｕｔｅによるＤｅｆｅｎｃｅ　Ａｄｖａｎｃｅｄ　Ｒｅｓｅａｒｃｈ　Ｐｒｏｊｅｃｔｓ　Ａｇｅｎｃｙに関して準備された「Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｏｒｏｌ　Ｐｒｏｔｏｃｏｌ」、Ｊ．Ｐｏｓｔｅｌ、ｅｄｉｔｏｒ、Ｒｅｑｕｅｓｔ　ｆｏｒ　Ｃｏｍｍｅｎｔｓ（ＲＦＣ）７９３、１９８１年９月、「ｗｗｗ．ｆａｑｓ．ｏｒｇ／ｒｆｃｓ／ｒｆｃ７９３．ｈｔｍｌ」を参照されたい。ＲＦＣ７９３は、本明細書に完全に示されるように、参照によって本明細書に組み込まれる。）特に、そのような攻撃は、「ＳＹＮ攻撃」として知られる。なぜなら、それらは、新たなＴＣＰ接続を開始させるように送られる、膨大な初期ＳＹＮパケットのほんのフラリからなるからである。（ＳＹＮパケットは、当業者には完全に知られている接続要求パケットである。それらは、例えば、上記に参照されたＲＦＣ７９３のＴＣＰ標準に定義されかつ説明される。）

【０００６】

より詳細には、当業者には良く知られているように、各ＴＣＰ接続は、ＳＹＮパケットで開始する。ＴＣＰサーバは、各有効なＳＹＮ要求にＳＹＮ、ＡＣＫで応答しなければならず、必要であれば再送信しなければならない。（ＡＣＫパケットは、当業者には完全に知られ、同様にＲＦＣ７９３で定義されかつ説明される承認パケットである。）ＳＹＮパケットは、パケットにおける前の状態なしに、一時的なファイアウオールを貫通する。ＳＹＮパケットは、また、サーバおよびファイアウオールを、新たな接続に関する準備でリソースを割り当てさせる。結果として、それらは、サービス拒否攻撃を開始する第１の可

能性があるビークルである。
【特許文献１】特許仮出願第６０／４９７８８６号
【非特許文献１】Ｉｎｆｏｒｍａｔｉｏｎ Ｓｃｉｅｎｃｅｓ ＩｎｓｔｉｔｕｔｅによるＤｅｆｅｎｓｅ Ａｄｖａｎｃｅｄ Ｒｅｓｅａｒｃｈ Ｐｒｏｊｅｃｔｓ Ａｇｅｎｃｙに関して準備された「Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ」、Ｊ．Ｐｏｓｔｅｌ、ｅｄｉｔｏｒ、Ｒｅｑｕｅｓｔ ｆｏｒ Ｃｏｍｍｅｎｔｓ（ＲＦＣ）７９３、１９８１年９月、「ｗｗｗ．ｆａｒｓ．ｏｒｇ／ｒｆｃｓ／ｒｆｃ７９３．ｈｔｍｌ」
【発明の開示】
【発明が解決しようとする課題】
【０００７】
実際、２つの異なる形態のＳＹＮ攻撃が存在する。ＳＹＮ状態攻撃とＳＹＮ帯域幅攻撃である。ＳＹＮ状態攻撃は、ハンドシェークの残りを完了することなく、接続要求ＳＹＮパケットを送ることによってＴＣＰサーバを圧倒しようとし、サーバ上の「バックログ・キュー」を最終的にはオーバフローさせ、それによってサービス拒否を正当な要求にする。（当業者には良く知られているように、ＴＣＰ接続は、３方向ハンドシェークを介して確立され、不完全な接続は、一般にパー・リスナ・キューに保持される。バックログ・キューの制限は、通常はむしろ小さい。）しかしながら、ＴＣＰサーバが、自身によってＳＹＮ状態攻撃に対して防御することを可能にする少なくとも２つの解決方法が存在し、１つの解決方法は、不完全な接続に使用されるメモリ量を低減することであり、他方の解決方法は、任意のメモリ使用を完全に排除することである。
【０００８】
しかしながら、他の形態のＳＹＮ攻撃は、ＳＹＮ帯域幅攻撃である。ＳＹＮ帯域幅攻撃は、「下流側」（すなわち、攻撃下のＴＣＰサーバで）で扱うのがより困難である。一般的なＳＹＮパケットは、ただ６４バイト長であるにすぎないことに留意されたい。そのような最小サイズのパケットのバーストは、したがって、サーバ上でライブロックを引き起こす。（当業者には良く知られているように、「ライブロック」は、２つ以上のプロセスが、あらゆる有用な動作を行うことなく、他の１つまたは複数のプロセスにおける変化に応答してそれらの状態を連続して変化させるとき発生する状況である。）すなわち、デッドリー攻撃は、単にサーバのイングレス・リンクに多くのそのような小さなパケットでブラスティングすることからなり得る。多くの最適化が、受信器ライブロックを避けるために存在するが、一般に、帯域幅攻撃は、現在まで、さらに「上流側」だけで、すなわち損傷がサーバになされる前だけで扱われた。
【課題を解決するための手段】
【０００９】
本発明者は、ＳＹＮ帯域幅攻撃は、有利には保護されるべきネットワークのエッジに配置された（例えば、保護されたリンクからのある距離だけ上流側）「ＤＤｏＳゲートウェイ」におけるＳＹＮパケットをインターセプトしかつ識別し、かつ次に、本発明の原理にしたがって、他のＴＣＰパケットから別々にこれらのインターセプトされたＳＹＮパケットをキューイングすることによって、「下流側」で有効に扱われることができることを認識した。特に、本発明のある例示的な実施形態によれば、エッジ・パー・フロー・キューイングは、異なるプロトコル間の分離、およびリンクを共有する個別ＴＣＰ接続間の分離を提供するために、有利にはＤＤｏＳゲートウェイで用いられる。（パー・フロー・キューイング技術は、当業者には良く知られている。）
【００１０】
さらに、本発明の原理にしたがって、ＳＹＮパケットは、他のＴＣＰパケットから別々にキューイングされる。次に、ＤＤｏＳゲートウェイのエグレス・スケジューラは、有利にはそれぞれ空でないキューに公正な共有を与え（有利には、ＳＹＮパケットのための別々のキューを含む）、それによって、ＳＹＮパケット（例えば、ＳＹＮ帯域幅攻撃の一部として生成されたものなど）が、他のパケットの存在におけるエグレス・リンクを圧倒で

きないことを確実にする。さらに、そのようなスケジューリング・スキーマは、有利には、６４バイト・パケットを、一般より大きいデータ・パケットでインタリーブし、それによって下流側ＴＣＰサーバでライブロックを引き起こす尤度を低減する。

【発明を実施するための最良の形態】

【００１１】

図１は、本発明の例示的な実施形態による、ＳＹＮ帯域幅攻撃の防御メカニズムを組み込むＤＤｏＳゲートウェイの機能ブロック図を示す。例示的なＤＤｏＳゲートウェイは、有利には、ネットワーク・エッジ、すなわち保護されるべきリンクからある距離だけ上流側に配置される。例示的なゲートウェイの動作において、コアから到着するパケットは、他からＴＣＰパケットを分離するために、発送モジュール１１によってまず発送される。（ＴＣＰではないパケットは、ＴＣＰではないモジュール１２によって取り扱われる。）ゲートウェイにおいて前の状態を有するデータ・パケットは、検査モジュール１３によって決定されたように、あるバッファ管理ポリスを受ける様々なキューに格納されることができる。しかしながら、ＳＹＮパケットは、転送されるべき前の状態を必要とせず、したがって有利には、接続モジュール１４によって別々に取り扱われる。データ・パケット、ＳＹＮパケット、およびＴＣＰではないプロコトルからのパケットは、次に、ＦｌｏｗＱモジュール１５によって保護されたリンク上に現れるようにスケジュールされる。逆の方向に関して、ＴＣＰサーバからのパケットは、監視モジュール１６によって検査され、コアから到来するパケットのさらなる取り扱いのためにステートフル情報を提供する。本発明の例示的な実施形態による、以下の詳細に記載されるようなＳＹＮ帯域幅攻撃の防御メカニズムは、有利にはＦｌｏｗＱモジュール１５に組み込まれることができる。

【００１２】

本発明の例示的な実施形態によれば、ＳＹＮパケットを盲目的に格納しかつ通過させる代わりに、同一の接続からの隣接するＳＹＮパケット間の指数的な間隔が、有利に実施される。他の再送信と同様に、ＴＣＰプロトコルは、ＳＹＮパケットのための再送信が、データ・パケットに関する同一の指数関数的なバック・オフ時間間隔に従うことを特定する。例えば５００ミリ秒の初期間隔で、現在の間隔時間前に到着する以降のＳＹＮパケットは、有利にはドロップされる。延長された時間期間にわたって続いた不完全な接続は、それらが、次に新たな接続要求によって除かれないなら取り除かれる。例示的なシステムは、さらに、不完全な接続それぞれは、キューにおいて１つより多くないＳＹＮパケットを有することを確実にする。これは、エグレス・リンクが、わずかな数の不完全な接続によってあふれる可能性を取り除く。

【００１３】

ランダムに生成されたＳＹＮパケットが、ゲートウェイにおける多数の状態を生成し、かつエグレス・リンクをあふれることを防ぐために、例示的なシステムにおいて許容される不完全な接続の全数は、有利には、以下のように現在確立された接続の数に比例して設定され、

Ｐ＝Ｍ＋ｃ＊Ｎ　　（１）

ここで、Ｍおよびｃは定数であり、Ｎはシステムにおける確立された接続の数である。正当なＴＣＰ接続要求は、ほとんど確実に確立されたものになる。したがって、正当な要求の数および確立された接続の数は、一般に近く訂正される。定数ｃは、例えば値２に設定されることができる。Ｍは、ヘッド・スタートのためにシステムにおいてアクティブ接続を有さない許容された要求の数である。例示的にはＭ＝１００である。

【００１４】

本発明の例示的な実施形態によれば、新たなＳＹＮパケットが、前の状態なしに到着したときに、式（１）に特定された条件が保持されるなら、新たな状態が割り当てられる。代わりに、ランダムに選択された状態が除かれる。（本発明の他の例示的な実施形態によれば、エージングが、ランダムな選択の代わりに使用されることができることに留意されたい。しかしながら、ランダムな選択は、エージングにわたって好ましい、なぜなら、システムが実際に攻撃下であるときに、それは、長いラウンド・トリップ時間での接続に対

してよりフレンドリーであるからである。）接続は、有効な戻りＡＣＫパケットが通過するとき、不完全な状態から確立された状態に移動する。遷移にかかる時間は、サーバとクライアントとの間のラウンド・トリップ時間に主として依存することに留意されたい。再送信されたＳＹＮパケットが到着したなら、指数関数的な間隔が調べられる。受けられたパケットは、ＦＩＦＯバッファ内にキューイングされる。パケット・バッファが利用できないなら、パケット・バッファ・マネージャは、パケットをシステムから取り除く。バッファ管理に関する詳細に関しては、以下を参照されたい。

【００１５】

本発明の他の例示的な実施形態によれば、初期的なＳＹＮパケットおよび全てのサーバ応答を転送する、ＴＣＰハンドシェーク・プロキシが使用される。このプロキシは、クライアントが有効ＡＣＫを戻す、または接続タイム・アウトが発生するまで、必要であればクライアントに代わってＳＹＮ再送信を実行する。このプロキシ・アプローチは、良好に作用するが、ＳＹＮ再送信のためにゲートウェイで格納されるべきより多くの接続状態を必要とし、かつ実施により費用がかかる。

【００１６】

ネットワーク・エッジで、ネットワーク・コアからのイングレス・リンクは、通常最終顧客ネットワークに向かうエグレス・リンクより速いことに留意されたい。したがって、エグレス・リンクは、イングレス・パケット到着レートがリンク容量より高いなら、あふれることがある。しかしながら、当業者に良く知られるように、ＴＣＰは、輻輳の検出時にパケット・レートを抑圧して戻す、輻輳アウェア伝送プロコトルである。その結果、悪意のあるユーザは、リンクを大きくあふれることなく、他の正当なＴＣＰ接続をエグレス・リンク上でのそれらの利用を低減させることができる。この現象は、また悪意があってもなくても、集中したＴＣＰ実装によって駆動される接続の存在で起きる。

【００１７】

したがって、正当なＴＣＰの流れを保護するために、公正なスケジューリングおよび公正なバッファ管理メカニズムが、本発明の例示的な実施形態による有利に用いられる。特に、図１の例示的なＦｌｏｗＱモジュールは、有利に、公正なスケジューリングおよび公正なドロッピング・バッファ管理スキーマを実装する。

【００１８】

特に、本発明のこの例示的な実施形態によれば、コア・ネットワークから到着しかつ同一の出力インタフェース宛てであるＴＣＰデータ・パケットは、まずフロー・キューに格納される。この例示的な実施形態によれば、フローは、そのソース宛て先アドレスおよびポート数によって識別される単一のＴＣＰ接続として定義される。（本発明の他の例示的な実施形態によれば、フローは、定義されることができ、フロー・キューは、例えば単一のソースに属する各パケットのセットおよび宛て先ホスト対に関して、または単一のソース・ホストからの各パケットのセットまたはソース・ネットワークに関して実装される。）エグレス・パケット・スケジューラは、次に、命令されたパケット出発に関するこれらのフロー・キューを有利に操作する。パケットは、入力ポートに到着し、かつ出力ポートを出発する。本発明の例示的な実施形態のＤＤｏＳゲートウェイは、出力ポート・バッファリング・アーキテクチャを使用する。（用語「ポート」は、任意の物理的なネットワーク・インタフェースを表すために本明細書で使用されることに留意されたい。）

【００１９】

例示的な出力ポート・パー・フロー・キューイングおよびバッファ・シェアリング・アーキテクチャは、各出力ポート、すなわち到着サイドおよび出発サイドに２つのインタフェースを有する。到着サイドは、出力ポート・ライン速度より速いレートで入力ポートからのパケットを受信することができ、パケットをバッファさせかつ遅延させる。出発サイドは、キューイングされたパケットを有する複数のフローを提供する。結果として、本発明の例示的な実施形態により適合されたバッファ管理ポリシーは、有利には２つの個別の特性を示す。すなわち、

（１）出発での公正なスケジューリングは、全ての競合するフローが、同一の帯域幅リソ

ースに称されることを確実にする。
（２）到着での公正なドロッピングは、フローが、他を犠牲にしてより多くのバッファを使用するがないことを確実にする。
【００２０】
不正なスケジューリング・スキーマとともに、いくつかのフローは、たとえそれらが、他よりも多くのバッファを使用しなくとも、より高い帯域幅を得ることができることに留意されたい。また不正なバッファ割り当てとともに、フローは、たとえスケジューリング・スキーマが完全に公正であっても、送るパケットを有さないことがある。
【００２１】
パー・フロー・キューイングを考慮すれば、ラウンド・ロビン・スケジューリングは、「マックス・ミニ」公正であるとして当業者には知られている。ビット・バイ・ビット・ラウンド・ロビン・スケジューリングが、可変パケット長での作用に有効に近づくことができることにも留意されたい。パー・フロー・キューイングに関する典型的なパケット破棄アルゴリズムは、簡単である。フリーなバッファが存在する限り、全ての到来するパケットを受ける。任意のフリーなバッファなしに、パケットが到来するときに、最上位のバイトをバッファリングして、フローからパケットをドロップする。
【００２２】
不必要なパージング（受けられたパケットが、直ちに次に到着したもので置き換えられる）を避け、かつ小さなウインドウのために、ＴＣＰフローがタイム・アウトになることを防ぐために、到来するパケットが、最も長いキューがただ２つのパケットを有するとき、有利にはドロップされない。明らかに、これは、フローの最大数を、システムに収容される全体バッファ・サイズの１／２に制限する。
【００２３】
図２は、本発明の例示的な実施形態による、ＳＹＮ帯域幅攻撃に対する防御のための図１の例示的なＤＤｏＳゲートウェイの例示的（概念）構造ブロック図を示す。例示的なゲートウェイは、複数の入力（すなわちイングレス）ポート２１－１から２１－４と、複数の出力（「エグレス」）ポート２２－１から２２－３とを備える。さらに、ゲートウェイは、（多い）複数のＮパー・フロー・キュー２３－１から２３－Ｎ、ならびにキューイングＳＹＮパケットにおいて排他的な使用に関するＳＹＮシーケンス２３－０を備える。各フロー・キュー２３－１から２３－Ｎは、異なるＴＣＰ接続（すなわちフロー）に関連するＴＣＰをキューイングするために使用され、一方、ＳＹＮキュー２３－０は、ＳＹＮパケットだけを保持する。動作において、ラウンド・ロビン公正スケジューリング・アプローチが、有利に用いられ、各（Ｎ＋１）キューからのパケットが、次に処理される。このように、ＳＹＮキュー２３－０を満たすことがあるＳＹＮ帯域幅攻撃は、他（Ｎ）のキューからのパケットのスケジューリングおよび送信を有意には妨げない。
【００２４】
図３は、本発明の例示的な実施形態による、ＳＹＮ帯域幅攻撃に対する防御における使用に関する図１の例示的なゲートウェイの動作のフローチャートを示す。例示的なゲートウェイの動作は、１つの入力ポートからＴＣＰパケットを受信することによって開始し（ブロック３１）、それがＳＹＮパケットかどうかを決定する（決定ブロック３２）。ＳＹＮパケットであるなら、それは、有利にＳＹＮキューに挿入される（ブロック３３）。ＳＹＮパケットでないなら、それは、適切なフロー・キューに挿入される（ブロック３４）。次に、パケットは、例えばラウンド・ロビン・スケジューリングなどの公正スケジューリング・アルゴリズムに基づき、送信に関してスケジューリングされる（ブロック３５）。キューイングされる他の到来パケットが存在するなら（決定ブロック３６）、フローは、ブロック３１に戻る。そうでなければ、キューイングされたパケットは、転送されることを継続する。
【００２５】
上記で指摘されたように、ラウンド・ロビン・スケジューリングの実装は、当業者には良く知られている。さらに、最も長いフロー（例えば、キューイングされた最大のパケッ

ト、またはキューイングされた最大のバイトを有するフロー）から（必要なときに）、パケットをドロップすることが良く知られている。しかしながら、本発明の好ましい例示的な実施形態によれば、フローは、有利には、パケット毎に一定量の動作を使用して、パケット数に関してまたはバイト数に関して、例示的に測定されることができるそれらのキュー長さに基づき分類される。

【００２６】

特に、本発明のある例示的な実施形態によれば、全てのパケットが同一のサイズであると仮定される。換言すれば、キュー長さは、パケットのユニットで（バイトよりむしろ）測定されることを仮定する。例示的なシステムは、有利には、リストのチェーンを維持する。各サブリストは、同一のキュー長さを有する全てのフローを含む。これらのサブリストは、次に、下がる順番でキュー長さにしたがって格納される。全てのフローが空のキューを有するので、初期的に全てのリストが空であることに留意されたい。

【００２７】

フロー$_i$に関するパケットが、利用可能なフリー・バッファの状態で到着すると、それは受けられ、かつ長さQ_iを有するフロー$_i$・キューに付けられる。このように、キュー長さは、Q_i+1に増加する。システムは、現在のサブリストＳＬ（Q_i）からフロー$_i$を取り除き、サブリストＳＬ（Q_i+1）に付けられる。このサブリストは、それらがまさに１つのパケットによって異なるので、ＳＬ（Q_i）から離れるいずれかの１つのアイテムであるべきか、またはフローが、到着前にQ_i+1のキュー長さを有さないなら存在しない。後者の場合に、システムは、簡単にリストを作成し、かつＳＬ（Q_i）の前のそれを挿入する。両方の場合に、命令されたマスタ・リストを維持するために、全てのリストを走査する必要がないことに留意されたい。

【００２８】

図４は、本発明の例示的な実施形態による、そのようなキューイング動作の例示的な例を示す。図４Ａは、フロー$_2$に関する新たなパケットの到着前のキュー構造を示し、図４Ｂは、所定のパケットの到着後に修正されたキュー構造を示す。追加されたパケットの結果として、フロー$_2$は、有利にはＳＬ（Ｑ＝４）から取り除かれ、ＳＬ（Ｑ＝５）に挿入される。

【００２９】

フロー$_i$に関するパケットが、スケジュールされかつ出発したとき、それは、長さQ_iを有するフロー$_i$・キューから取り除かれる。それによって、キュー長さは、Q_i-1に低減される。例示的なシステムは、その現在のサブリストＳＬ（Q_i）からフロー$_i$を取り除き、次に、$Q_i>1$なら、サブリストＳＬ（Q_i-1）の開始でそれを攻撃する。必要であれば、ＳＬ（Q_i-1）が、有利に形成されることに留意されたい。古いサブリストＳＬ（Q_i）は、空であれば、有利に取り除かれかつ削除される。再び、線形走査は必要がない。

【００３０】

図５は、本発明の例示的な実施形態による、そのようなキュー・エントリ除去動作の例示的な例を示す。図５Ａは、フロー$_2$からスケジュールされたパケットの出発前のキュー構造を示し、図５Ｂは、所定のパケットの出発後に修正されたキュー構造を示す。パケット、すなわちフロー$_2$の取り除きは、有利にはＳＬ（Ｑ＝５）から取り除かれ、ＳＬ（Ｑ＝４）に挿入されることに留意されたい。

【００３１】

フロー$_i$に関するパケットが、満たされたバッファに到着するときに、最長のキュー長さを有するフロー$_j$は、格納されたマスタ・リスト内の第１のサブリストから見出されることができる。例示的なシステムは、$i\neq j$ならフロー$_j$からパケットをパージし、到来するパケットを受ける。代わりに、到着するパケットが有利にドロップされる。パケットをパージすることに関連する動作は、出発のためのパケットのスケジュールリングに使用される動作と同一であることに留意されたい。

【００３２】

パケットが可変長であることがある、本発明の他の例示的な実施形態によれば、シーケンス長さが、バイトのユニットを有し、各サブリストは、［Q_i／ＭＴＵ］の同じ値を有する全てのフローを含み、ここで、ＭＴＵは、最大パケット・サイズであり、［］は、数学的上限関数を表す。同様の動作が、到着および出発で実行される。Q_iを有するフロー$_i$が、ＳＬ［Q_i／ＭＴＵ］に追加されるときに、（Q_iモジュロＭＴＵ）＜ＭＴＵ／２であるなら、それは有利には付けられ、かつ代わりに開始に取り付けられる。これは、サブリスト内の誤りの分類が、ＭＴＵ／２より小さいことを確実にする。小さなパケットの到着または出発が、そのフローを隣接するサブリストに移動させないが、代わりに、更新されたキー長さが、ＭＴＵ／２境界を交差するかどうかに応じて、開始で取り付けられるかまたは同一のサブリストに付けられることが可能であることに留意されたい。

【００３３】

詳細な記載に対する追加

前述の全ての議論は、単に本発明の一般原理を示したものであることに留意すべきである。本明細書に明示して記載されかつ示されてはいないが、本発明の原理を具体化し、かつ本発明の精神および範囲に含まれる、様々な他の構成を考案することができることは理解される。さらに、本明細書で言及された全ての例および条件を表す言語は、本発明の原理および技術をさらに進めるために本発明者によって与えられた概念を、理解する助けにする教育的な目的のためだけに主として表現しようとするものであり、そのように特定して言及された例および条件を限定するものではないと解釈されるものである。さらに、本発明の原理、態様、および実施形態、ならびにその特定の例を言及する本明細書の全ての記述は、その構造的および機能的等価物を含むものである。そのような等価物は、現在知られている等価物、ならびに将来開発される等価物の両方、すなわち構造にかかわらず同様の機能を実行する開発された任意の要素を含むものでもある。

【００３４】

したがって、例えば、任意のフローチャート、フロー図、状態遷移図、擬似コードなどは、様々なプロセスを表し、それらは、そのようなコンピュータまたはプロセッサが明示的に示されていてもいなくとも、実質的にコンピュータ可読媒体に表されることができ、コンピュータまたはプロセッサによってそのように実行されることができることを当業者であれば認識するであろう。したがって、例えば、そのようなフローチャートに示されるブロックは、可能な物理的な要素を表すものとして理解されることができ、それらは、例えば、フローチャート・ブロックに記載されるなどの特別の機能を特定するための手段として現在の請求項に表現され得る。さらに、そのようなフローチャート・ブロックは、例えば、ディスクまたは半導体記憶デバイスなどの前述のコンピュータ可読媒体に含まれることができる、物理信号または格納された物理データを表すものとして理解されることもできる。

【図面の簡単な説明】

【００３５】

【図１】本発明の例示的な実施形態による、ＳＹＮ帯域幅攻撃の防御メカニズムを組み込むＤＤｏＳゲートウェイの機能ブロック図を示す。

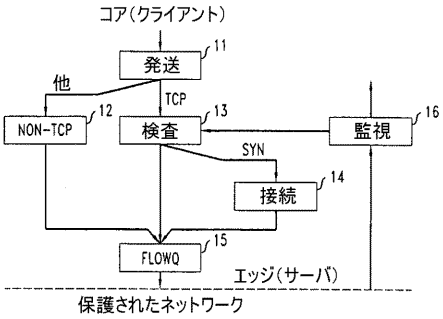
【図２】本発明の例示的な実施形態による、ＳＹＮ帯域幅攻撃に対する防御のための図１の例示的なＤＤｏＳゲートウェイの例示的（概念）構造ブロック図を示す。

【図３】本発明の例示的な実施形態による、ＳＹＮ帯域幅攻撃に対する防御における使用に関する図１の例示的なＤＤｏＳゲートウェイの動作のフローチャートを示す。

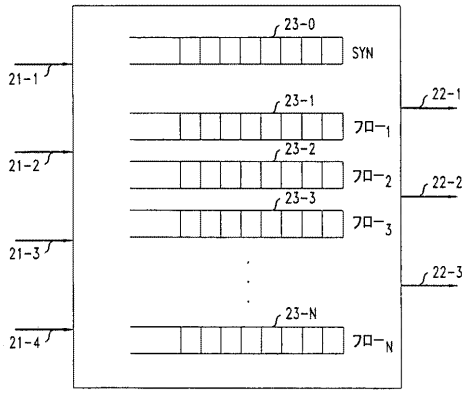
【図４】本発明の例示的な実施形態による、キューイング動作の例示的な例を示す。図４Ａは、新たなパケットの到着前のキュー構造を示し、図４Ｂは、所定のパケットの到着後に修正されたキュー構造を示す。

【図５】本発明の例示的な実施形態による、キュー・エントリ除去動作の例示的な例を示す。図５Ａは、スケジュールされたパケットの出発前のキュー構造を示し、図５Ｂは、所定のパケットの出発後に修正されたキュー構造を示す。

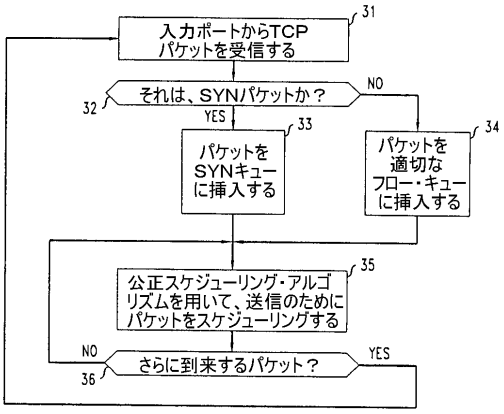
【図１】


コア(クライアント)
発送
11
他
TCP
NON-TCP
12
検査
13
監視
16
SYN
接続
14
FLOWQ
15
エッジ(サーバ)
保護されたネットワーク

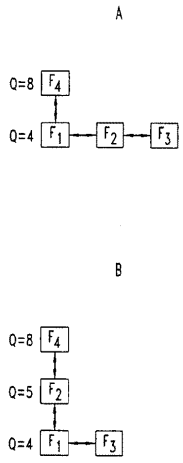
【図２】


23-0
SYN
21-1
23-1
フロー1
22-1
21-2
23-2
フロー2
22-2
23-3
フロー3
21-3
22-3
23-N
フローN
21-4

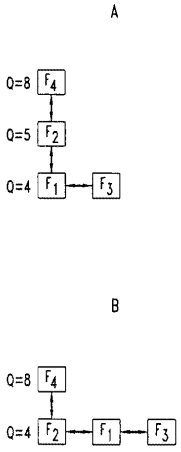
【図３】


入力ポートからTCP
パケットを受信する
31
それは、SYNパケットか？
32
NO
YES
パケットを
SYNキュー
に挿入する
33
パケットを
適切な
フロー・キュー
に挿入する
34
公正スケジューリング・アルゴ
リズムを用いて、送信のために
パケットをスケジューリングする
35
NO
さらに到来するパケット？
YES
36

【図４】


A
Q=8
F4
Q=4
F1
F2
F3
B
Q=8
F4
Q=5
F2
Q=4
F1
F3

【図５】


A
Q=8
F4
Q=5
F2
Q=4
F1
F3
B
Q=8
F4
Q=4
F2
F1
F3

フロントページの続き

(74)代理人 100096943
弁理士 臼井 伸一
(74)代理人 100101498
弁理士 越智 隆夫
(74)代理人 100096688
弁理士 本宮 照久
(74)代理人 100104352
弁理士 朝日 伸光
(74)代理人 100128657
弁理士 三山 勝巳
(72)発明者 ドング リン
アメリカ合衆国 ０７０２４ ニュージャーシィ，フォート リー，フィフティーンス ストリート １２６５，アパートメント １４イー

審査官 玉木 宏治

(56)参考文献 特開２００４－１６６０２９（ＪＰ，Ａ）
特開２００４－１２０４９８（ＪＰ，Ａ）
金子 斉，DDoS攻撃対策手法に関する一考察，2002年電子情報通信学会通信ソサイエティ大会 B-7-40，２００２年 8月２０日
田上 敦士 他，優先度付キューを用いたTCPコネクション接続性の向上手法，電子情報通信学会技術研究報告（信学技報） NS2001-231 IN2001-187，２００２年 3月 7日

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ １２／００－６６