(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3560552号
(P3560552)
(45)発行日　平成16年9月2日(2004.9.2)　(24)登録日　平成16年6月4日(2004.6.4)

(51)Int.Cl.[7]　F I
G06F 13/00　G06F 13/00　３５１Ｚ
G06F 13/00　３５３Ｒ

請求項の数 2　(全 5 頁)

(21)出願番号　特願2001-26567(P2001-26567)
(22)出願日　平成13年2月2日(2001.2.2)
(65)公開番号　特開2001-265678(P2001-265678A)
(43)公開日　平成13年9月28日(2001.9.28)
審査請求日　平成13年2月2日(2001.2.2)
(31)優先権主張番号　09/503608
(32)優先日　平成12年2月11日(2000.2.11)
(33)優先権主張国　米国(US)

(73)特許権者　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国１０５０４　ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
(74)代理人　100086243
弁理士　坂口　博
(74)代理人　100091568
弁理士　市位　嘉宏

最終頁に続く

(54)【発明の名称】サーバへのフラッド攻撃を防止する方法及び装置

(57)【特許請求の範囲】
【請求項１】
ネットワーク・サーバ上の一のポート番号に対するキューに配置するため多数のコネクションレス・データグラムが受信されるという形態の前記サーバへのフラッド攻撃を防止する方法であって、
前記ポート番号に対する一のホストからの一のデータグラムが前記サーバに着信したことに応答して、当該ポート番号に使用可能なキュー・スロットの数をポート番号毎に設定された値である割合Ｐにかけることによってしきい値を計算するステップと、
前記ポート番号へのキューにすでに配置されている前記ホストからのデータグラムの数が前記しきい値を超えるかどうかを判定し、超える場合は、前記着信したデータグラムを破棄するステップと
を含む、方法。
【請求項２】
ネットワーク・サーバ上の一のポート番号に対するキューに配置するため多数のデータグラムが受信されるという形態の前記サーバへのフラッド攻撃を防止する装置であって、
前記ポート番号に対する一のホストからの一のホストからのデータグラムが前記サーバに着信したことに応答して、当該ポート番号に使用可能なキュー・スロットの数をポート番号毎に設定された値である割合Ｐにかけることによってしきい値を計算する手段と、
前記ポート番号へのキューにすでに配置されている前記ホストからのデータグラムの数が前記しきい値を超えるかどうかを判定し、超える場合は、前記着信したデータグラムを破

棄する手段と、
を含む、装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、一般にはネットワークの分野に関し、特にコネクションレス・データグラムをサーバに溢れさせることによってサーバを使用不能にしようとする悪意あるユーザからの攻撃を防ぐ方法に関する。
【０００２】
【従来の技術】
最近、インターネットのサーバを標的にしてサーバを使用不能にするフラッド攻撃が増加している。フラッド攻撃は、サーバを過負荷にし、よって使用不能にする意図を持って比較的短い時間にユーザが大量のリクエストを送ることをいう。悪意あるユーザからのパケットの洪水は、構成ミスのあるシステムからのパケットの洪水と同様、サーバを過負荷にすることがある。しかし結果は同じである。サーバはリクエストを処理しようとして過負荷になる。そのため、正当なリクエストを適時に処理できなくなり、サーバが使用不能になったりクラッシュしたりすることもある。最近のニュースでは、有名なＷｅｂサイトに対する複数のフラッド攻撃が報告されている。こうした攻撃の特徴は、初期通信を確立する個々の接続リクエストのフラッドにある。関連する他の特許出願は、そのような接続リクエスト攻撃を防ぐアルゴリズムを開示している。しかし、ＵＤＰ（ユーザ・データグラム）プロトコルのように、コネクションレス・データグラムを溢れさせることによってサーバを攻撃することも可能である。その効果は、基本的には同じである。サーバは多数のデータグラムを処理しようとして過負荷になり、完全に使用不能になることもある。フラッド攻撃は、従来の侵入検出システムで防止するのは難しい。トラフィックが正当かどうか判定するのが困難だからである。
【０００３】
【発明が解決しようとする課題】
データグラムの意図的フラッド攻撃と、データグラムのバーストにより生じる意図的ではない過負荷の状況は、正当なトラフィックと不当なトラフィックを区別しようとする従来の考え方をなくすことによって軽減できると本発明では考える。本発明では、フラッドの原因が正当なデータグラム・トラフィックか不当なデータグラム・トラフィックかにかかわらず、正当な操作が実行され、フラッド状況でもサーバがクラッシュしないことを保証しようとするポリシーの対象として、全てのデータグラム・トラフィックを想定する。本発明により、過負荷によるサーバのクラッシュを防ぎやすくなり、攻撃者が全サーバ・リソースを消費するのを防ぐことができる。
【０００４】
【課題を解決するための手段】
サーバの指定ポートに宛てられたデータグラムの着信に応答して、転送側ホストが確認され、同じホスト及び同じポートにすでに待機しているデータグラムの数が確認される。この数が第１しきい値を超える場合、接続リクエストは拒否される。
【０００５】
第１しきい値は、好適な実施例では動的に決定される。サーバ所有者は、データグラム・フラッド・チェックの対象になるポート毎に、どの時点でもポートに可能な最大待機データグラム数（Ｍ）とポートに残っている使用可能なキュー・スロットの支配的割合（Ｐ）を指定する。本発明では、待機データグラム数を最大データグラム数からマイナスすることによって、ポートの待機データグラムの数（Ａ）が追跡され、使用可能なキュー・スロット数（Ｉ）が計算される（Ｉ＝Ｍ－Ａ）。転送側ホストですでに待機しているデータグラムの数が、Ｐ×（残存キュー・スロット数）（≧Ｐ×Ｉ）に等しいかより大きい場合、現在のデータグラムは拒否される。他の場合、データグラムはキューに置かれ、ポートの待機データグラム数（Ａ）が１つ増分される。

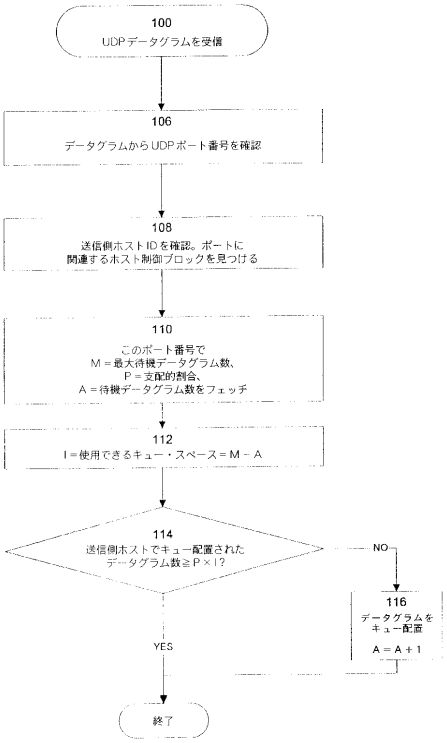
【０００６】
ほとんどの所有者にとって、最大データグラム数としきい値割合Ｐを設定するのは難しい。そこで、複数のサーバの通常のトラフィック負荷を測定し、類似の正当なトラフィック負荷を妨げることのない適切な最大値としきい値を提案する統計モードが提供される。
【０００７】
【発明の実施の形態】
本発明では、サーバの所有者が、特定のパラメータでサーバを設定する必要がある。例えば所有者は、好適な実施例では、データグラム・フラッド・チェックの対象になるポート番号毎に、どの時点でもポートへのキューに置ける最大データグラム数（Ｍ）と、ポートに残っている使用可能なキュー・スロットの支配的割合（Ｐ）を指定する必要がある。割合Ｐは、データグラム処理拒否をトリガするしきい値を設定するため用いられる。データグラムがキューに置かれ処理されるとき、サーバは、フラッド・チェックの対象になるポート毎に、使用できるキュー・スロットの数を動的に維持する。
【０００８】
図１のステップ１００で、ネットワーク・サーバでデータグラムが受信される。最初のステップ１０６では、データグラムの宛先であるポート番号がデータグラムから確認される。データグラムに含まれるポート番号は、データグラムが送信される所定のホスト・コンピュータ内の宛先を表す。標準サービスに予約されているポートもある。例えばネットワーク・ファイル・システム（ＮＦＳ）は、ＵＤＰデータグラムを受信する標準サービスの１例である。
【０００９】
送信側ホストのＩＤ（ＩＰアドレス）もデータグラムから確認される。ポート番号は、ステップ１０８で、ポートのメモリ制御ブロックを見つけるか、またはポート制御ブロックが現在存在しない場合に１つ作成するため用いられる。ポート制御ブロックには、キューに現在データグラムを持つホスト用の複数のホスト制御ブロックが付加される。送信側ホストにホスト制御ブロックがない場合は１つ作成される。ホスト制御ブロックは、特に、ホストに現在割当てられているポート接続のカウントを格納する。
【００１０】
ステップ１０８で、データグラムを開始した送信側ホストのＩＤがデータグラムから確認され、ポート番号とホストＩＤによりメモリ制御ブロックが見つけられるか、または現在存在しない場合はメモリ制御ブロックが作成される。既存メモリ制御ブロックは、特に、ホストにより現在キューに置かれたデータグラム数のカウントを格納する。ステップ１０８でこのデータグラムが送られるポート番号が確認される。
【００１１】
ステップ１１０でサーバが、メモリ制御ブロックから、このポート番号に指定された最大待機データグラム数Ｍ、支配的割合Ｐ、及び待機データグラム数Ａをフェッチする。ステップ１１２で、使用できるキュー・スロット数ＩがＭ－Ａとして計算される。ステップ１１４で、送信側ホストへのキューにすでに入ったデータグラム数がＰ×Ｉに等しいかより大きいかどうかが判定される。等しいかより大きい場合、データグラムは破棄され、キュー・アルゴリズムは１１８で終了する。一方、送信側ホストによりすでに開始された待機データグラム数がＰ×Ｉより少ない場合、データグラムはステップ１１６で処理のためキューに置かれ、Ａが１つ増分されてこのポート番号に対するキューのデータグラム数が更新される。
【００１２】
ここで説明しているコンピュータ・プログラムは、パーソナル・コンピュータからＩＢＭのＳｙｓｔｅｍ　３９０マシン等の大型メインフレームまで、事実上、あらゆる種類のコンピュータで実行することができる。唯一の要件は、コンピュータをネットワーク通信ソフトウェアで構成し、ネットワークを通してコンピュータをサーバとしてアクセスできることである。
【００１３】

当業者には明らかなように、ここに開示した実施例には、本発明の主旨と範囲から逸脱することなく、様々な変更を加えることができる。

【図面の簡単な説明】

【図１】フラッド状況により他の操作の完了が妨げられることがなく、サーバがクラッシュすることのないよう、データグラムの受信に応答してサーバ側で実行される操作のフローチャートである。

【図１】



フロントページの続き

(72)発明者　キラ・スターリング・アトウッド
アメリカ合衆国２７５１６、ノース・カロライナ州チャペル・ヒル、プルピット・ヒル・ロード　１３１１
(72)発明者　リンウッド・ヒュー・オバーベイ・ジュニア
アメリカ合衆国２７６１５、ノース・カロライナ州ローリー、ベンスレー・コート　８６０５
(72)発明者　チエン－エン・スン
アメリカ合衆国２７５１４、ノース・カロライナ州チャペル・ヒル、チッポークス・ドライブ　１０３

審査官　須藤　竜也

(56)参考文献　特開平０９－２１８８３７（ＪＰ，Ａ）
特開２０００－０３２０５６（ＪＰ，Ａ）
国際公開第０１／０１３５８９（WO，Ａ１）
国際公開第９９／０４８３０３（WO，Ａ１）
白井健宏，いまなぜ帯域制御技術が求められるのか？，コンピュータ＆ネットワークＬＡＮ，日本，株式会社オーム社，１９９９年　5月　1日，第１７巻　第5号，ｐ．８５－９２

(58)調査した分野(Int.Cl.^{7}，ＤＢ名)
G06F 13/00
G06F 15/00
H04L 12/56