L-003

パケットフィルタリング機能を搭載した NIC による DoS 攻撃対策
A Proposal of Preventing DoS Attacks using a Packet Filtering NIC

長尾 宗胤† 遠山 宏明† 冨澤 眞樹†
Toshitsugu Nagao† Hiroaki Toyama† Masaki Tomisawa†

1. はじめに

サイバー攻撃の一つである DoS 攻撃は，攻撃対象のシステムに対し過大な負荷をかけ，その正常な稼働を妨害する行為である．近年，DoS 攻撃が企業恐喝の手段として利用されるなど悪質化が進んでおり，対策が急務となっている[1].

DoS 攻撃の手法の一つに HTTP-GET flood 攻撃がある．この攻撃手法は，攻撃対象の Web サーバに対して短時間に大量のアクセスを行うことで攻撃対象サーバの正常な運用を妨害する攻撃手法である．

HTTP-GET flood 攻撃の対策として広く行われているのは，サーバに DoS 攻撃対策モジュールをインストールし，攻撃ホストからの接続を遮断する方法である．この対策手法は手軽である反面，アプリケーション層で処理が行われるためオーバーヘッドが大きく，大規模な DoS 攻撃に対処できないおそれがある．

本研究では，パケットフィルタリング機能を搭載した NIC[2]を使用し，ソフトウェアとの連携により，低いレイヤで攻撃ホストからのパケットを遮断することで DoS 攻撃への耐性を高める手法“*S-NIC*”について提案する．

2. HTTP-GET flood 攻撃とその対策

2.1 HTTP-GET flood 攻撃

HTTP-GET flood 攻撃は，攻撃対象の Web サーバに対して短時間に大量の HTTP-GET Request を送信することで攻撃対象サーバのリソースを消費させ，正常な運用を妨害する手法である．

この攻撃は，特別な攻撃ツールを必要とせず，ブラウザのリロードボタンを連打することにより簡単に実行できるという特徴がある．また，ボットネットの機能としてこの攻撃が実装されることも多く，大きな脅威になっている．

2.2 HTTP-GET flood 攻撃の対策

HTTP-GET flood 攻撃のパケットは，正規の HTTP プロトコルに則って送信されるため，攻撃と正当なアクセスとを判別することが困難である．しかしながら，HTTP-GET flood 攻撃は TCP のコネクションが確立した状態で行われるため，IP アドレスの偽装ができないという特徴がある．そのため，攻撃元ホストを IP アドレスにより識別可能であり，特定のホストから単位時間当たりに設定した数（しきい値）を超える HTTP-GET Request を受信した場合，そのホストを攻撃ホストと判定し，パケットを遮断することで対策が可能である．

† 前橋工科大学大学院工学研究科
† Graduate School of Engineering
Maebashi Institute of Technology

2.3 Apache での HTTP-GET flood 攻撃対策

ここでは Web サーバとして大きなシェアを持つ Apache を例に挙げ，サーバサイドでの HTTP-GET flood 攻撃対策の現状とその問題点について述べる．

Apache は，モジュールと呼ばれるコンポーネントを追加することで機能拡張が可能である．Apache には，DoS 攻撃対策を目的としたモジュールがいくつか提供されている．代表的な DoS 攻撃対策モジュールに“mod_evasive” [3]がある．mod_evasive は，図 1 に示すように Apache の一部として動作し，攻撃の検出と攻撃トラヒックのフィルタリングを行う．mod_evasive は，接続元ホストの IP アドレスを内部のテーブルに保持しており，ホストごとの単位時間当たりのアクセス回数を記録する．同じ URL に対して，あらかじめ設定した閾値を超えるアクセス行うホストを攻撃ホストと判定し，当該ホストからのアクセスを拒否する．

この対策手法は，特別なハードウェアを必要とせず，容易に導入が可能である．また，Apache 上で攻撃の検出とフィルタリングを行うため，アクセス制限を行う条件を細かく設定できるというメリットがある．その反面，次の問題点が存在する．

(1) Apache のプロセスにパケットが渡された後でフィルタリングが行われるため，オーバーヘッドが大きく，大規模な攻撃が行われた際にパフォーマンスが低下するおそれがある．

(2) DDoS 攻撃が行われた際，対策モジュールが保持している IP アドレステーブルのサイズが大きくなり，検索に時間がかかるおそれがある．

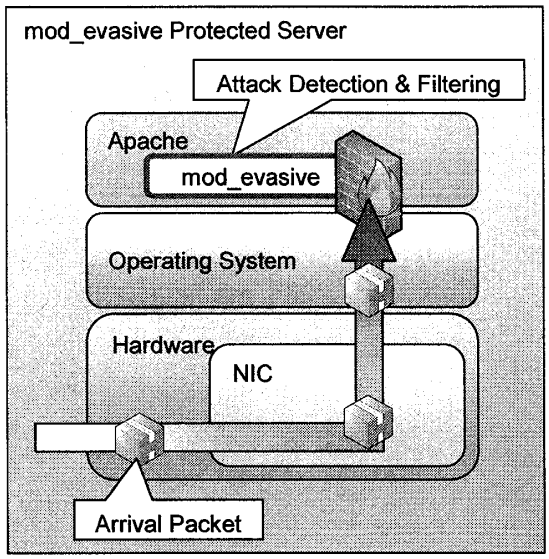

図1 Apache での DoS 攻撃対策

3. S-NIC による DoS 攻撃対策

S-NIC の特徴は，攻撃パケットのフィルタリングを NIC 側で行うという点にある．S-NIC のアーキテクチャは図 2 に示すように，攻撃検出及び攻撃ホストの IP アドレスを NIC に通知する“*Attack Detection Module(ADM)*”と，攻撃ホストからのパケットをフィルタリングする“*Filter Engine(FE)*”の 2 層構造を持つ．攻撃パケットのフィルタリングをハードウェアにオフロードすることにより，攻撃パケットがハードウェア側で遮断され，OS やサーバソフトウェアが DoS 攻撃の影響を受けにくくなり，Web サーバの DoS 攻撃への耐性が向上する．

3.1 Attack Detection Module(ADM)

ADM は Apache のモジュールとして実装されるソフトウェアである．mod_evasive が攻撃の検出とフィルタリングを行うのに対し，ADM は攻撃の検出と攻撃ホストの IP アドレスを NIC に通知する処理を行う．Apache が HTTP-GET Request を受信すると，接続元ホストの IP アドレスが ADM に通知される．ADM は接続元ホストの IP アドレスを内部の Access Frequency Table(AFT)に保持しており，ホストごとの単位時間当たりのアクセス回数を記録する．あらかじめ設定したしきい値を超えるアクセス行うホストを検出すると，FE にデバイスドライバを通じて当該ホストの IP アドレスを通知し，フィルタリングを行うよう指示する．フィルタリングを指示したホストの IP アドレスは AFT から削除される．

3.2 Filter Engine(FE)

FE は FPGA(Field Programmable Gate Array)により構成され NIC に実装されるハードウェアで，ネットワーク層でパケットフィルタリングを行う．ADM から通知された攻撃ホストの IP アドレスは，FE 内部の Blacklist に記録される．FE は入力されたパケットの送信元 IP アドレスが Blacklist に存在するか否か検査し，入力パケットが攻撃ホストから送信されたものである場合は，当該パケットを破棄する．

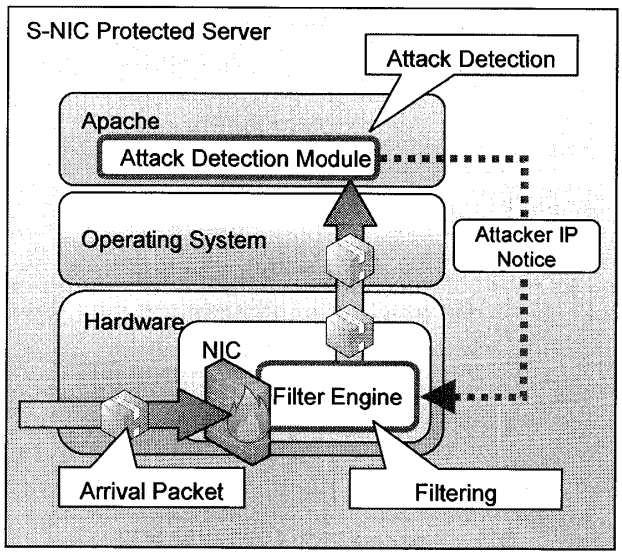

図2　S-NIC のアーキテクチャ

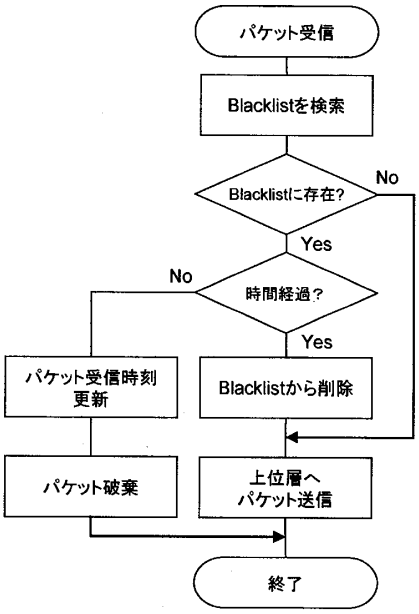

図3　Filter Engine の動作

FE では，攻撃の終了を判定する必要がある．FE は攻撃ホストからパケットを受信した時刻を Blacklist に記録しておき，あらかじめ設定した時間を経過しないうちに受信したパケットを破棄する．一方，設定時間を経過した後に受信したパケットについては上位層に送信するとともに，Blacklist からエントリを削除する(図 3)．

4. まとめ

本研究では，Web サーバにおける DoS 攻撃対策の現状と問題点について述べると共に，パケットフィルタリング機能を搭載した NIC を用いた DoS 攻撃対策について提案した．

S-NIC のアーキテクチャは攻撃検出を行うソフトウェアと，攻撃パケットのフィルタリングを行うハードウェアとの 2 層構造を持つ．攻撃パケットのフィルタリングをハードウェアにオフロードすることにより，攻撃パケットがハードウェア側で遮断され，OS やサーバソフトウェアが DoS 攻撃の影響を受けにくくなり，Web サーバの DoS 攻撃への耐性が向上する．

S-NIC の課題として，Blacklist のサイズの問題がある．DDoS 攻撃では，一度に多くの攻撃ホストからのパケットを受信することとなり，Blacklist のオーバーフローが懸念される．このため S-NIC の実現に当たっては，メモリ使用効率のよい実装方法を検討する必要がある．

今後は S-NIC の実現に向け詳細設計を行い，プロトタイプを製作するとともに，実証実験により提案手法の有効性を検証する予定である．

参考文献

[1]警察庁情報通信局情報技術解析課, “インターネットにおけるボットネットの現状と対策について”, ハイテク犯罪対策協議(2007).http://www.cyberpolice.go.jp/material/pdf/20070522_kouen.pdf

[2]長尾 宗胤, 冨澤 眞樹, “FPGA によるパケットフィルタリング処理の高速化”, 情報処理学会第 70 回全国大会(2008)

[3]Jonathan Zdziarski, “What is mod_evasive?”, ZDZIARSKI.com (2003).http://www.zdziarski.com/projects/mod_evasive/