M-002

パケット認証を用いたDoS攻撃に起因するトラフィック問題の回避手法の提案

A Proposal for Avoiding Traffic Problems Attributed to DoS Attack using Packet Data Authentication

今野 裕太 † **市田 智也** ‡ **佐藤 健哉** ‡
Yuta Konno Tomoya Ichida Kenya Sato

1 はじめに

現在，我々の生活にインターネットは欠かせないものとなっている．今日のスマートフォンの普及などを始めとして，通信のトラフィック量は増加の一途をたどっており，今後もこの傾向は継続していくものと思われる．一方使用できる帯域には限りがあるために，今後ネットワーク設備の輻輳が頻繁に起こってしまう問題が考えられる．そしてこの問題に拍車をかける代表例として DoS（Deny of Service）攻撃がある．

DoS 攻撃により，大量のデータや不正パケットを送りつけることによって，攻撃対象のシステムがサービスを提供できないようにしたり，システムそのものがダウンさせられる．その際に大量のパケットが流れるため，帯域幅のリソースを消費してしまい，通常の通信サービスの享受が困難になるといったトラフィックの問題が発生する．

そこで本研究では，パケットのヘッダ部に認証値を付加することで認証されたパケットと判断し，その認証されたパケットを優先的にルータで通すことによって，DoS 攻撃に起因する現在のネットワークトラフィックの問題点を回避するシステムを提案する．

2 関連研究

DoS 攻撃に対する対策として第一に，DoS パケットの発信元 IP アドレス情報を元にパケットフィルタリングを行う手法がある．この手法の利点としては対策が容易に行うことができるという点であるが，今日の DoS 攻撃は発信元 IP を偽装する IP スプーフィングが一般的に行われているために単に発信元 IP アドレスの情報のみでのフィルタリングの効果は期待できない．

この IP スプーフィングを考慮した対策としては IP トレースバックが挙げられる．DoS 攻撃に用いられたパケットの情報より攻撃に用いられた真の経路を割り出す手法であり，方式として提案されているものは様々ある [1][2]．例としてロギング方式ではルータを通過するパケットのログを記録しておくことで，上位ルータから再起的に発信元の探索を行う．これによりパケットの発信元 IP アドレスの情報が偽造されている場合でも攻撃経路の割り出しが可能となるが，問題点としては通過パケットのログを記録するために大きな記憶容量がルータに要求される点，また本質上，この IP トレースバック技術は「誰と誰が通信しているのか」という点を調べるために情報の発信源の特定の過程で，通信の秘密の保護に抵触してしまう可能性がある．

3 提案システム

3.1 概要

認証サーバより得た認証値をパケットヘッダに付加し，ルータで認証値が付加されたパケットを優先的に転送するパケット認証システムを提案する．

提案システムではすべてのパケットを DoS 攻撃によるものと仮定し，ルータで認証された認証パケットを優先的に転送することで，挙動を感知することが困難な DoS 攻撃自体を防ぐのではなく，DoS 攻撃に起因する被害を回避，軽減させるかを目的とする．

3.2 システムの構成と条件

- **認証サーバ**
  ルータでパケットの優先制御を受けるために必要な認証値をユーザに発行する．認証値を利用可能なユーザと発行時に必要なパスワードの組み合わせを登録，またその組み合わせデータを照合する機能を持つ．
- **認証パケット**
  パケットヘッダに認証サーバ発行の認証値が格納されたものを認証パケットと見なす．
- **ルータ**
  転送されてきたパケットヘッダを確認し，その値が認証サーバが発行した認証値ではない場合，未認証パケットと見なし一度バッファに格納することで，認証パケットを優先的に転送する．なおバッファに格納しきれなかったパケットについては破棄する処理を行う．また事前条件として認証サーバとルータの間で認証値は共有しているものとする．

3.3 認証の手順

(1) ユーザ端末は認証サーバに問い合わせ，認証値を要求．
(2) 認証サーバは入力情報を元にユーザ認証を行う，認証ユーザであれば認証値をユーザに送信．
(3) ユーザ端末は認証値をパケットヘッダに格納し，ルータに向けて送信．
(4) パケットを受けとったルータでヘッダ部の認証値を確認．
(5) ヘッダの認証値がルータの保持する認証値と一致した場合，ルータで対象パケットの優先転送処理

† 同志社大学 理工学部 情報システムデザイン学科
‡ 同志社大学大学院 工学研究科 情報工学専攻

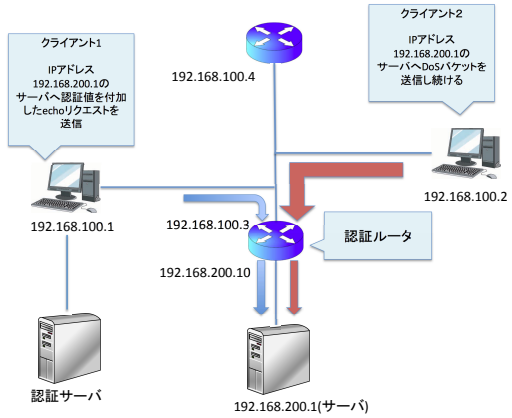

図 1　評価環境

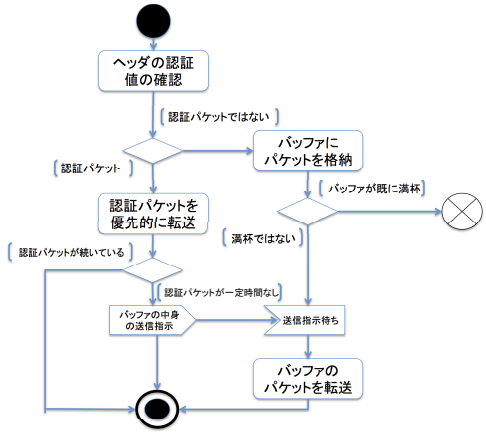

図 2　ルータにおけるパケット転送手順

を行う．

4　評価

次のような 2 種類の評価項目を用いる．ICMP の echo 要求メッセージ 100 回による平均到達時間，到達率により比較する．評価環境は図 1 のように作成し，クライアント 1 より認証パケットを，クライアント 2 より DoS パケット発生環境を作成した．ルータのパケット転送手順は図 2 のように行う．また今回は認証値の格納場所としてパケットヘッダの ToS フィールドを用いる．

(1) 提案システムの有無での比較
ルータにおいて認証値を用いた優先制御を行った場合と行わない場合を比較．
(2) 提案システムと既存の対策との比較
提案手法を用いて，ルータにおいて優先パケットの識別を認証値で行う場合と，IP アドレスで行う場合を比較．

各比較結果を表 1，表 2 に示す．

表 1　提案システムの有無による比較

提案手法の使用	平均到達時間（ms）	到達率（%）
使用する	7.280	54
使用しない	14.704	48

表 2　提案システムと既存の対策との比較

認証に用いる値	平均到達時間（ms）	到達率（%）
認証値	7.280	54
IP アドレス	8.450	56

5　考察

提案システムにより，DoS 攻撃に起因するパケット転送時間の遅延の改善を確認することができた．一方，認証値と IP アドレスとの認証方法の比較では大きな差は見られなかった．しかしユーザ認証に IP アドレスではなく，認証サーバより発行される認証値を用いることで，ルータでの複数の認証 IP アドレスを保管，照合をする負荷の減少にも効果がある．

またルータでバッファに格納しきれない未認証パケットについては，破棄する処理を行うことで DoS パケットによるサーバのリソース占有といった問題も軽減できる．

提案システムより以下の既存対策の問題点についても解消できる．

- **IP スプーフィング**
  偽装が可能である IP アドレスの代わりに認証値を用いているため第三者によるなりすましを防止することができる．
- **通信の秘密保護**
  提案システムによる DoS 攻撃対策として発信元の調査が必要がないため，通信秘密の保護に抵触することはない．

6　まとめ

本稿ではパケットヘッダに格納された認証値をルータで識別，優先制御をすることで DoS 攻撃に起因するトラフィック問題の回避手法を提案した．DoS 攻撃の発信元を特定して攻撃自体を遮断するのではなく，事前に認証されたユーザのパケットを優先的に転送することで発信元特定に労力をかけず，認証ユーザは DoS 攻撃の影響を回避することが可能である．

今後は今回の提案システムを IPv6 でも利用可能なように拡張を目指す．

参考文献

[1] 桂井友輝，中村嘉隆，高橋修:DoS 攻撃を対象とした IP トレースバックにおけるルータ負荷削減手法，マルチメディア・分散・協調とモバイル（DICOMO2014）シンポジウム，pp.530-536，2014
[2] 井上伸一郎，石井方邦，笹瀬巌:DDoS 攻撃に対して排他的論理和と確率的 Marking 方式を用いることでルータへの負荷分散を実現する IP Traceback，情報処理学会論文誌，pp.795-804，2012