パケットカウンタを用いた出国印方式による低負荷IP トレースバック

パケットカウンタを用いた 出国印方式による低負荷 IP トレースバック

山森　一人 a)・篠岡　祐太 b)　・相川　勝 c)

Low Load IP Trace Back Technique by Departure Stamp with Packet Counter in Edge router

Kunihito YAMAMORI,Yuta SHINOOKA,Masaru AIKAWA

Abstract

The number of illegal accesses and DoS（Denial of Service）or DDoS（Distributed DoS）attacks are increasing as popularization of Internet. In these attacks, the source IP address is sometimes manipulated, so it is difficult to identify the original source IP address. IP trace back technique by departure stamp in edge routers is a nice way to identify the original source IP address of attackers, and can reduce network load. However, it require high performance for edge router because it stamps all packets through the edge router. In this paper, we propose a method that stamps the limited number of packets that may participate DoS or DDoS attack. We implement proposed method and confirm that our method can reduce the load on edge router.

Keywords:　IP trace back,Departure stamp,Packet counter,Edge router

1.　はじめに

インターネットの普及に伴い、コンピュータウイルスへの感染や不正アクセスなどの被害が年々増加傾向にある[1]。

例えば、2015 年にはセブン銀行や毎日新聞社などが DoS（Denial of Service）攻撃、DDoS（Distribute DoS）攻撃の被害を受け、サービスの一時停止に追い込まれた[2]。

DoS 攻撃や DDoS 攻撃では送信元 IP アドレスが詐称されている場合があり、攻撃者の特定は難しい。この問題を解決するため、IP トレースバックが提案されている。播磨ら[3]は、L2-based IP トレースバック方式と名付けた、ハッシュ方式にパケットカウンタを組み合わせた方式の提案と実装を行っているが、ネットワーク内のすべてのルータの改造が必要であり、実現性に欠ける。藩ら[4]は、出国印方式と名付けた、エッジルータでマーキング処理を行う方式の提案と実装を行っている。出国印方式はエッジルータのみの改造で済むため実現性は高いものの、すべてのパケットにマーキング処理を行うのでエッジルータの負荷が増加してしまう。

本研究の目的は、出国印方式の改良を行い、エッジルータの負荷を低減することである。提案方式ではパケットカウンタを設け、攻撃パケットである可能性の高いパケットにのみマーキングを行う。さらに、提案方式を実装し、試作システムでエッジルータの負荷について評価を行う。

a)情報システム工学科教授
b)情報システム工学科
c)宮崎大学工学部教育研究支援技術センター技術職員

2.　出国印方式

図 1 に示すように、エッジルータは、企業や大学の LAN（Local Area Network）と WAN（Wide Area Network）の境界にあるルータを指す。出国印方式は、エッジルータが自身の IP アドレスを IP ヘッダの Identification フィールドに記録する方式である。

出国印方式以外の方式は WAN 内のルータの改造を伴ううえ、全プロバイダが同一方式を採用する必要がある。一方、出国印方式はエッジルータの改造のみで済み、企業など管理者が協力すれば実現が可能である。しかし、すべてのパケットにエッジルータがマーキング処理を行うことから、エッジルータに大きな負荷がかかる。

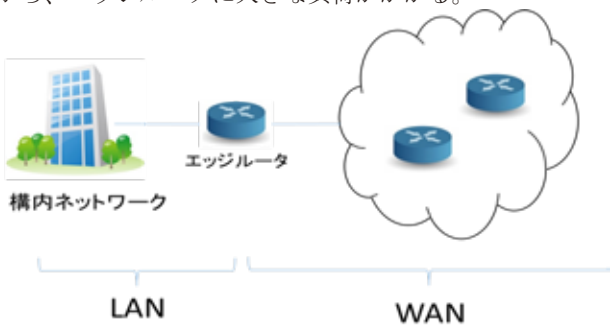


図 1. エッジルータのネットワーク上の位置.

3. 提案方式

本研究で提案する方式は、出国印方式と同様にエッジルータでルータ自身のIPアドレスをIPヘッダ中に記録する。このとき、エッジルータの負荷低減のためトラフィックを監視し、攻撃と判断した場合のみマーキング処理を行う。以下に提案方式について述べる。

3.1 マーキングするデータの検討

発信元側では、エッジルータが自身のIPアドレスやシーケンス番号などの情報をIPヘッダ中に書き込む。図2に示すIPv4ヘッダのうちIdentificationフィールドは、一度に送信することのできない大きなパケットをいくつかのフラグメントに分割して送信した際、パケットを再構成するための識別子として利用される。フラグメント化されたパケットは、インターネットを流れるトラフィック全体から見ても0.25%とごくわずかな量であることが知られている[5]。そこで、Identificationフィールドに、パケット追跡に必要な情報を格納する。

Identificationフィールドにエッジルータのの IPアドレスやシーケンス番号などの情報を格納する場合、IPアドレスが32ビットであるのに対し、Identificationフィールドは16ビットと短く、IPアドレスを1度に格納することができない。そこで、図3に示すように、発信元情報としてIPアドレスを8ビットごとに分割して4つのパケットにそれぞれ格納する。被害ホストがパケットを受け取った際に分割されたエッジルータのIPアドレスを復元するために、IPアドレス以外に2つの特徴情報を格納する。エッジルータのIPアドレスを復元するためには、同一エッジルータからのパケット4つが必要である。そこで、ルータ識別子を特徴情報として追加する。ルータ識別子には、認証やデジタル署名などに使用されるハッシュ関数であるsha-1により、エッジルータのIPアドレスから160ビットのハッシュ値を生成し、先頭の6ビットを使用する。また、パケットの到着が前後する可能性があるため、シーケンス番号を示すindex番号を追加する。このようにデータを格納することで、被害ホストはルータ識別子とindex番号からIPアドレスを復元することができる。

Version	IP Header Length	TOS	IP Packet Length
Identification		Flag	Fragment Off-set
TTL	Protocol	Header Check Sum	
Source Address			
Destination Address			
Option			
TCP/UDP Data			

図2. IPv4パケットの構造.

6 bit	2 bit	8bit
ルータ識別子	Index番号	発信元情報

図3. Identificationフィールドに書き込む情報.

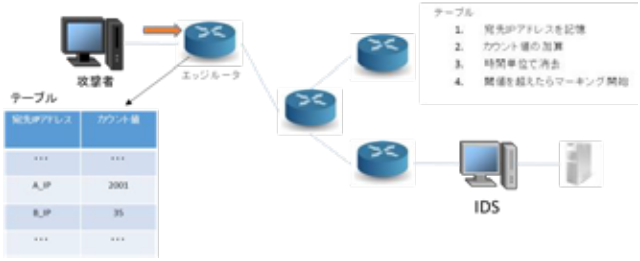


図4. エッジルータへのパケットカウンタの追加.

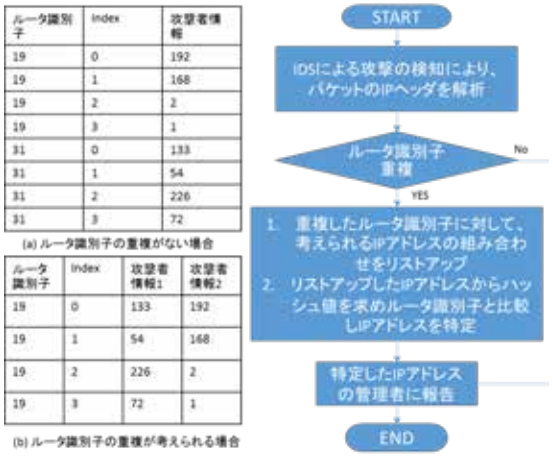
3.2 低負荷マーキング処理

提案方式では、エッジルータの負荷低減のためエッジルータにパケットカウンタを設け、同一IPアドレスへのパケットが一定数を超えた時からのみマーキング処理を開始する。図4に、攻撃ホストから被害ホストにDoS攻撃が仕掛けられた際の様子を示す。図4において、被害ホストのIPアドレスをA_IPとする。エッジルータは宛先IPアドレスと宛先IPアドレスごとのカウント値を保持する。宛先IPアドレスへのパケットを中継する度に、対象のIPアドレスのカウント値をインクリメントする。カウントテーブルのIPアドレスとカウント値は、一定時間更新がなければ消去する。カウント値がしきい値を超えた場合、DoS攻撃またはDDoS攻撃であると判断し、該当するパケットのIPヘッダ中にエッジルータ自身のIPアドレスやルータ識別子などのマーキング処理を開始する。被害ホストはマーキングされたパケットを解析し、エッジルータのIPアドレスを特定する。

3.2 被害ホストでの処理

被害ホストは、IDS（Intrusion Detection System）[6]を用いてパケットを監視し、DoS攻撃またはDDoS攻撃を検知した場合、受信パケットのヘッダ部分をデータベースに保存する。IDSからの通知後、被害ホストの管理者は攻撃の時間帯や攻撃を受けたインタフェース情報などにより、データベースから攻撃に関連すると思われるパケットのヘッダ部分を取り出し、図5に示す手順でパケットの解析を行う。図5での処理について以下で説明する。

1. 異なるエッジルータからのルータ識別子が偶然同じになる可能性があるので、ルータ識別子が重複しているか否かの判定を行う。
2. 同じルータ識別子の発信元情報をIndex番号順に並べ、同じIndex番号での発信元情報が同じ場合、同一エッジルータのルータ識別子であると判断する。図5の(a)のように、index番号順に発信元情報の8ビットを結合し、エッジルータのIPアドレスを復元する。
3. 同じルータ識別子の発信元情報をIndex番号順に並べ、同じIndex番号での発信元情報が異なって



ルータ識別子	Index	攻撃者情報
19	0	192
19	1	168
19	2	2
19	3	1
31	0	133
31	1	54
31	2	226
31	3	72

(a) ルータ識別子の重複がない場合

ルータ識別子	Index	攻撃者情報1	攻撃者情報2
19	0	133	192
19	1	54	168
19	2	226	2
19	3	72	1

(b) ルータ識別子の重複が考えられる場合

図 5. IP アドレス復元手順

いた場合は、異なるエッジルータで同じルータ識別子が使用されていると判断する。同じルータ識別子を持つパケットの発信元情報を Index 番号順に並べ、考えられるすべての IP アドレスの組み合わせをリストアップする。図 5 の(b)の場合は、192.168.2.1、もしくは 133.54.226.72、192.54.2.72、133.168.226.1 など 2 の 4 乗の組み合わせが考えられる。リストアップされた IP アドレスのそれぞれに対し sha-1 でハッシュを生成し、生成されたハッシュの先頭 6 ビットとルータ識別子を比較し、これらが等しければ発信元エッジルータの IP アドレスとして特定する。

4. 発信元エッジルータの IP アドレスを特定した後、当該エッジルータの管理者に被害を受けていることを報告し対処を要請する。

4. 提案方式の評価

4.1 しきい値の検討

提案方式では、しきい値を元にマーキング処理の開始を判断するため、このしきい値が重要なパラメータになる。DoS攻撃、DDoS攻撃には様々な種類があり、それぞれの攻撃に応じて適切なしきい値を設定しなければならない。そこで、最適なしきい値を得るために仮想環境上にWEBサーバを構築し、数種類のDDoS攻撃を行いサーバにかかる負荷を調査する。実験を行う環境を表1に、使用するツールを表2に示す。

WEBサーバのCPUを100%使用可能な場合と40%に制限した場合で、さらにメインメモリの容量により負荷が変わる可能性を考慮し、メインメモリを512MBの場合と640MBの場合について実験を行う。

DDoS攻撃には、主に過負荷をかけることを目的としたFlood攻撃タイプと、セキュリティホールを衝く脆弱性を狙った攻撃に分けられる。本研究ではFlood攻撃タイプに

表1. 実験環境

	攻撃者	WEBサーバ
CPU	Core i7 3820 3.8GHz	Core i7 3820 3.8GHz Corei7 3820の40%に制限 1.52GHz
メインメモリ	896MB	512MB/640MB
OS	Ubuntu14.04	

表2. 実験で使用したツール

目的	ツール名	バージョン
仮想環境ソフト	Oracle VM Virtualbox	5.0.10 Editon
DDoS攻撃	Hping	3.0.0-alpha-2
WEBサーバソフトウェア	Apache	2.4

焦点をあて、その中でも代表的な攻撃である ICMP Flood、SYN Flood、UDP Floodの３つの攻撃を実験に用いる。本稿では、一例としてSYN Flood攻撃について示す。１台の攻撃ホストからIPアドレスをランダムに詐称し、パケットレートを100[PPS]ずつ増加させSYN Flood攻撃を行う。

WEBサーバのCPUを40%に制限した場合の、SYN Flood攻撃におけるCPU負荷を図6に、アクセス応答時間を図7に示す。図6に示すように、パケットレートが200[PPS]を超えたあたりから急激にCPU負荷が増加し、400[PPS]では負荷が約62%になる。これ以降は緩やかに負荷が増加し、4,000[PPS]ではCPU負荷が100%になるという結果が得られた。図7のアクセス応答時間は、CPU負荷が100%になる4,000[PPS]を超えたあたりから徐々に増加しており、メインメモリが512MBの場合は10,000[PPS]で142.2[ms]という結果となった。このままパケットレートを上げていくと、サーバのCPU負荷は既に100%に達しているため処理能力が低下し、新たなTCP接続に対応できなくなる。その結果、他のクライアントからTCP接続要求を受信してもTCPコネクションがタイムアウトし、通常の通信要求に応答できない状態になることが予想される。以上の実験結果から、SYN Flood攻撃に対するしきい値は、200[PPS]から250[PPS]が適切であることが分かる。

3.2 試作システムの概要と環境

本研究では、OpenFlowフレームワークのTremaをエッジルータとして使用し、提案方式を実装する。OpenFlowとは、SDN（Software-Defined Networking）における、最初の標準化されたプロトコルである。表3に試作システムの環境を、使用したツールを表4に示す。

試作システムでは、既存方式と比べエッジルータの負荷が低減されているか確認することを目的とし、IDSは導入

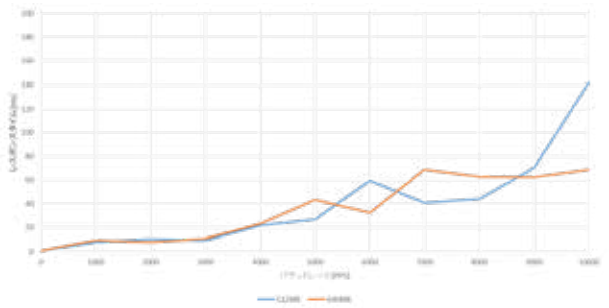


図6. SYN Flood攻撃におけるCPU負荷（CPU40%制限）.

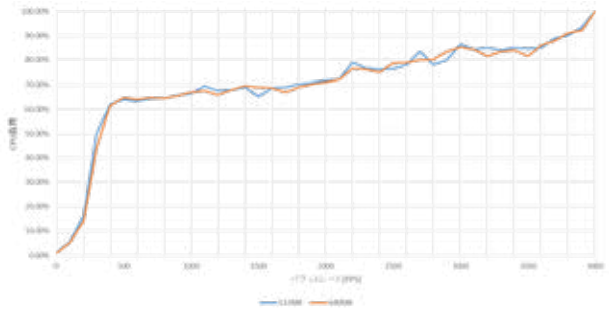


図7. SYN Flood攻撃におけるアクセス応答時間（CPU40%制限）.

せずシンプルなネットワーク構成とする。

3.3 エッジルータの負荷

SYN Flood攻撃を行い、既存方式と比較しエッジルータの負荷が改善されているか確認を行う。提案方式のしきい値は、パケットレートで200[PPS]と250[PPS]の2通りとし、比較を行う。参考までに既存方式だけでなく、マーキング処理を行わない一般的なルータとの比較も行う。しきい値を200[PPS]に設定したときの負荷を図8に示す。

図8から、しきい値を超えるまでは、エッジルータにかかる負荷が低減されていることが分かる。パケットレート150[PPS]では、既存方式と比べ約10%の低下となった。

5. おわりに

IPトレースバック方式の1つである出国印方式では、エッジルータですべてのパケットにマーキング処理を行うためエッジルータに大きな負荷がかかる。本研究では、エッジルータにカウントテーブルを設け、しきい値により、攻撃パケットである可能性の高いパケットにのみマーキング処理を行う方式を提案し、実装を行った。SYN Flood攻撃においてしきい値を200[PPS]にしたとき、150[PPS]ではエッジルータの負荷を約10%低減できた。

今後の課題は、しきい値を超えた後は既存方式の方が負荷が低いため、しきい値を超えた後の負荷を低減することが挙げられる。

表3. 試作システムの環境.

	攻撃者	ルータ	サーバ
CPU	Core i7 3820 3.8GHz		
メインメモリ	896MB	1024MB	896MB
OS	Ubuntu14.04		

表4. 試作システムで使用したツール.

目的	ツール名	バージョン
パケット書き換えツール	pkttools	1.8
エッジルータ	Trema	0.4.7

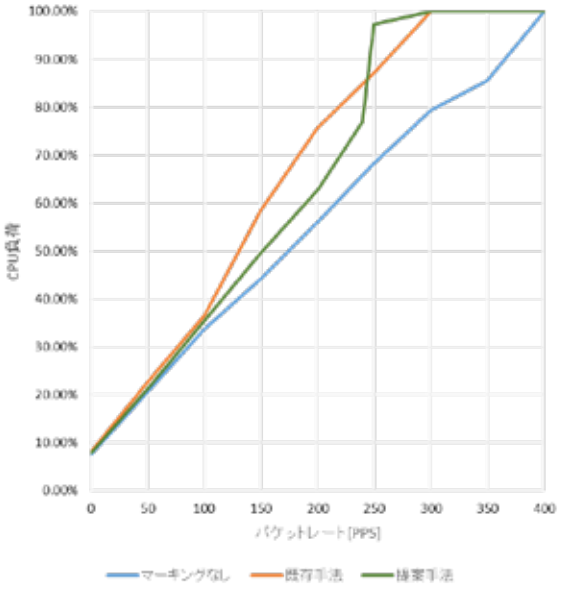


図8. しきい値を200[PPS]でマーキングを開始するように設定した際のルータの負荷.

参考文献

1)“@IT”http://www.atmarkit.co.jp/ait/articles/1508/19/news108.html.
2)“ボクシルマガジン”http://boxil.jp/magazine/20151113_cyber_attack_japan/.
3) 播磨宏和,伊藤将志,鈴木秀和,岡崎直宣,渡邊晃:“L2-based IP トレースバック方式の提案と実装”情報処理学会論文誌,vol.49,No.6,pp. 2200-2211,2008.
4) 潘博文,佐々木良一:”IP トレースバックのための出国印方式の試作と評価”,情報処理学会論文誌,vol49,No.9,pp. 81-94,2008.
5) Stoica, Ion and Zhang, Hui: “Providing Guaranteed Services Without Per Flow Management”,SIGCOMM Comput. Common . Rev.,Vol.29,No.4,pp.81-94,1999.
6) 竹森敬祐,三宅優,中尾康二: “IDS ログ分析支援システムの提案”,Technical Report 45(2003-CSEC-021),KDDI 研究所,2003.