社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2007－ＱＡ１－22（５）
2007／1／19

PPM方式IPｖ６パケットトレースの情報収集と経路構築

原山 美知子† 岩田 竜一† 岩井 孝広† 山田 真貴† 田中 昌二†

†岐阜大学工学部 〒501-1193 岐阜市柳戸１－１

E-mail: †harayama@gifu-u.ac.jp,

あらまし IPトレースバックは，行われたIP通信の情報からパケットの送信経路および送信元を解析する手法であり，DoS（サービス妨害）攻撃対策およびネットワーク管理ツールとして期待されている．ここでは，経路情報をパケット内にもつPPM(確率的パケットマーキング方式）に着目する．ノード情報の収集と経路構築を行うため，IPｖ６の中継点オプションを利用した実装方法を提案し，小規模ネットワークでの実験結果を示す．

キーワード IPパケットトレース，PPM，IPv6，DoS，ネットワークセキュリティ

Collection of Node Information and Construction of Route For PPM IPv6 Packet Trace.

Michiko HARAYAMA† Ryuichi IWATA† Takahiro IWAI† Maki YAMADA and Akiji TANAKA†

† Faculty of Engineering, Gifu University 1-1 Yanagi-to, Gifu, Gifu, 501-1193 Japan

E-mail: †harayama@gifu-u.ac.jp

Abstract IP trace back is a group of methods that analyze packets of Internet Protocol(IP) to obtain their trace and source IP. It is expected to be available as a remedy against DoS (Deniable of Service) attacks and also as a tool for network administration. Here, Probabilistic Packet Marking (PPM), one of the IP trace back is focused. It is proposed that collection of the node information using hop-by-hop option of IPv6 and trace construction. Implementation and experimental results with an experimental network are reported.

Keyword IP Packet Trace, PPM, IPv6, DoS, Network Security

1. はじめに

標的に対して大量のパケットを送りつけてサービスを妨害するネットワーク攻撃 DoS（Denial of Services；サービス妨害）は，決定的な解決策がないまま，今や日常的に行われるようになっている．送信元IP詐称，コンピュータウィルスとの連携による分散DoSも常套化し，さらに反射型DDoSと悪質化している．

IPトレースバックは，DoS攻撃の対策として受信パケットの通信経路を特定する技術であり[1]，手法としては，ICMPを利用する方式，パケットに経路の情報を記録するパケットマーキング方式，ルータでパケットの記録をとるダイジェスト方式などがある．IPトレースバックでは，大量のパケットを前提としているため，確率的な手法を用いるのが一般的である．中でもパケットマーキング方式[2]は，受信側だけで情報を収集し経路構築ができること，ルータに負荷をかけないという点で実用性が高いと考えられ，IPv4を中心に様々な研究がなされている[3-6]．しかしながら，IPｖ４に実装する場合，逆探知に必要な情報を埋込む場所が小さいないなど，いくつかの問題点が指摘されている．

一方，IPv6では拡張ヘッダが定義されより柔軟な情報埋込みが可能となっている[7]．そこで，IPv6へのPPM（Probabilistic Packet Marking; 確率的パケットマーキング）方式の実装を検討してきた[8]．

ここでは，IPｖ６の中継点オプションをもちい，PPMの情報を記録するための新しいオプションとしてトレースオプションを定義し，逆探知情報の収集と経路構築を行うことを提案する．

本報告では，FreeBSD への実装方法と小規模ネットワークでの実験結果を報告し，情報収集と経路構築について議論する．

2. PPM の概要

PPM では，IP パケットがルータを通過する際，経路を再構成するために必要な情報を確率的にパケット内に埋めこむ．パケットを受信した各ルータは，パケットにマークするかどうかを確率的に判定する．1 つのパケットにマークされるのは高々1 つの辺やノードの情報である．目的ノードに到達したパケット群から経路構築に必要なパケットを集め，情報をつなぎあわせて経路を構築する．なお，マーキング確率については，固定値 4%が推奨されている．

これまでに提案されている辺サンプリング方式では，各ルータは，パケットへのマークする場合，直前に送信されたルータの IP アドレスと，自分自身の IP アドレスの XOR をとり，その値を辺の情報としてパケット内に格納する．また，その地点からの距離を計測しはじめる．最終的に目的地で受信されたパケットには辺の情報と目的地から辺までの距離が書込まれている．

パケットの目的地ノードでは，パケットの中から，同種の送信パケットを選ぶ．さらにパケット群の中から，辺の情報をすべて集める．目的地ノードの IP アドレスと距離 1 の辺の XOR 情報から，直前のルータの IP アドレスを得る．距離を増やしながら，次々と辺情報との XOR をとることによって逆順に通過 IP アドレスリストすなわちトレースを構成する．

3. 中継点オプションを用いた辺情報のマーキング（A）

これまでの研究で提案されている PPM の実装を試みた．以下にマーキングのデータ構成とアルゴリズムを示す．

3.1. トレースオプションの構成

RFC2460 により、IP v 6 では，6 種類の拡張ヘッダが定義されている．パケットマーキングはルータで処理されるため，中継点オプション（Hop by hop オプション）を用いた．中継点オプションに格納されるオプションは複数でもよく格納されるデータ形式は TVL フォーマットに従う．ここで用いたトレースオプションの構成を Fig.1(A)に示す．アライメント要求は 8n+5，トレースオプション番号（Trace Type）は 39，Trace Length 9,である．辺の情報を格納するためのデータ構成として，先頭 1 オクテットを Distance フィールドとし，それにつづく 8 オクテットを Edge - ID フィールドとした．Edge-ID フィールドには IPv6 アドレスのプレフィックス（上位 64 ビット）を格納する．

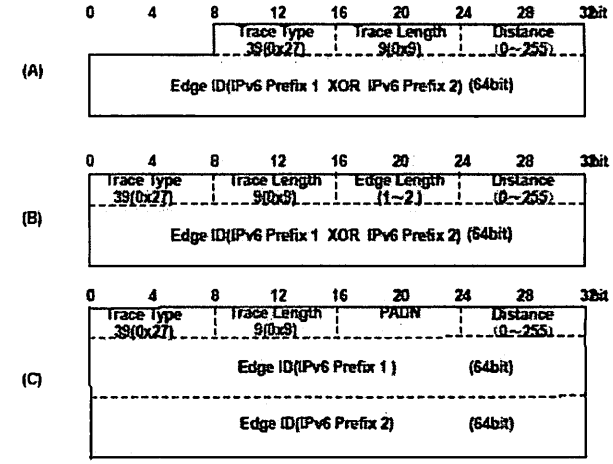

Fig.1 トレースオプションヘッダ．

4. 1 マーキングアルゴリズム

1. 各ルータは確率 p でマークするかどうか判定する．
2. マークする場合，自身の IPv6 アドレスのうちプレフィックス（上位 64 ビット）を Edge-ID フィールドに書込み，Distance フィールドを 0 クリアする．
3. マークしない場合，
   3.1. Distance フィールドが 0 なら，自身のアドレスと Edge-ID の XOR をとり，その値を Edge-ID フィールドに書込む．
   3.2. Distance が 0 でなければその値をインクリメントする．

このアルゴリズムでは，確率 p でマークすると決定した場合，データのあるなしに係わらず辺情報が新しく書込まれる．

5. 複数の送信元に対する IP トレースバック（B）

PPM の辺サンプリングで，辺情報として 2 つの IP アドレスの XOR を格納するのは，情報量をなるべく少なくするためである．しかしながら，DDoS 攻撃を想定した場合，複数の経路から同じ内容のパケットが送信される可能性がある．Fig. 1(A)に示すような経路で複数の送信元からの同種のパケットが届き，距離だけのデータでは異なる経路のパケットを分離することができない場合，正しく経路が構成できないケースがあ

る．それに対処するために，隣接ノード間の情報および1ノードをはさんだ2ノード間の情報を用いるマーキングを検討した．

5.1. トレースオプションの構成

Fig.1 (B) では，データ構成として Distance フィールドと Edge-ID フィールドの他に，Edge Length フィールドを追加した．このフィールドは辺の長さを示す．隣接ノード間の辺情報では1である．1ノードをはさんで接続されたノード間の情報の場合は，2が選択される．

5.2. マーキングアルゴリズム

1. 各ルータは確率 p でマークするかどうか判定する．
2. マークする場合，自身の IPv6 アドレスのうちプレフィックス（上位 64 ビット）を Edge-ID に書込み，Distance フィールドを 0 クリアする．Edge Length フィールドを 1 とする．
3. マークしない場合，
   3.1.Distance フィールドが 0 の場合，確率 q でスキップするかどうかを判定する．
   3.1.1 スキップする場合は，Edge Length フィールドをインクリメントする．
   3.1.2 スキップしない場合は，自身のアドレスと Edge-ID の XOR をとり，その値を Edge-ID フィールドに書込む．Distance をインクリメントする．
   3.2 Distance フィールドが 0 でなければ，その値をインクリメントする．

5.3. 経路構築アルゴリズム

経路構築は，基本的には目的地ノードから送信元に向かって Distance 0 から Edge-ID の XOR をといてゆくのであるが，ノードをさかのぼるとき，次のアルゴリズムを用いる．

1. Distance N のノードの IP アドレスがわかったものとする．Distance N+1, Edge-Length 1 のパケットの Edge-ID を用いて 隣接ノードの候補を得る．
2. 隣接ノードの候補に対し，Distance N+2 のパケットの辺情報を適用し，1 ホップ手前のノードを得る．
3. Distance N の Edge-ID と Distance N+1 かつ Edge Length 2 のパケットの Edge-ID を用いて 1 ホップ手前のノードを得る．2，3の結果が一致する場合，2の隣接ノード候補を Distance N+1 のノードとして確定する．

6. XOR を用いない場合（C）

しかしながら，辺情報として，XOR をとる場合，ルータのプレフィックスが近い値である場合，（B）のアルゴリズムでも間違った経路が構築されるケースがあり，厳密には回避することはできない．実際，組織内でルータを設置する場合や，広域ネットワークでも集約アドレスを想定すると，ルータのプレフィックスは連番となる可能性が高い．すると，ノードの XOR を辺情報とする限り，正しい経路の構築を保障できない．そこで，辺情報として2つのノードのプレフィックスを格納する必要があると考えられる．この場合の，トレースオプションは Fig.1(C)に示す．また，マーキングのアルゴリズムは下記の通りである．経路構築アルゴリズムは省略する．

5.1 マーキングのアルゴリズム

1. 各ルータは確率 p でマークするかどうか判定する．
2. マークする場合，自身の IPv6 アドレスのうちプレフィックス(上位 64 ビット)を 1st Edge-ID フィールドに書込み，Distance フィールドを 0 クリアする．
3. マークしない場合，
   3.1. Distance フィールドが 0 なら，自身の IP アドレスのプレフィックスを 2nd Edge-ID フィールドに書込む．
   3.2. Distance が 0 でなければその値をインクリメントする．

7. 実験

7.1. 実装方法

本研究では，FREEBSD 4.10 を用いた．kame-2005131-freebsd410-snap.tgz パッチをあてし，kame/sys/netinet6 ディレクトリ内のファイルに着目した．追跡情報の格納はパケットの入力時と出力時に行うため，ip-input.c: ip6-input () および ip-output.c: ip6-output ()に追加した．3つのケース(A),(B),(C)を実装した．マーキング確率，スキップ確率ともに，固定値 4%とした．

7.2. 実験環境

10台の PC を用い，Fig.2のような実験ネットワークを構築した．PC 性能は Pentium4 1.5-3.2GHz, メモリは RIMM256MB-DIMM 512MB である．ノード N1 に対し，N8,N9,N10 の，3点のエンドノードから,それぞれ 10000 パケットの ICMPv6Echo Request を送信する．N1 が受信したパケットを tcpdump で記録した．内容を観測するとともに，負荷を調べるためターンアラウンドタイムを測定した．さらに，受信したパケットの情報に基づき経路を構築した．

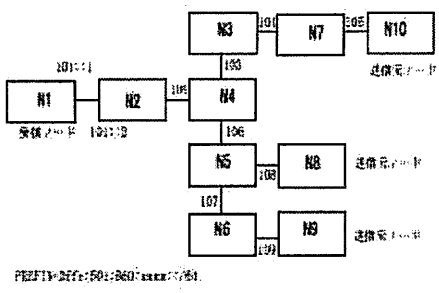

Fig.2 実験ネットワークのトポロジー.

7.3. 実験結果

各アルゴリズムとも，経路構築に十分なパケットが収集されていることを確認した．実装した場合と実装しない場合のターンアラウンドタイムの比をとり，実装による負荷を調べた．その結果，実装による影響は，B,C ともに程度であることがわかる．

実験ネットワークにおいて、関して再構築を行ったところ，

N10-N7-N3-N4-N2-N1
N8-N6-N4-N2-N1
N9-N6-N5-N4-N2-N1
N9-N8-N5-N4-N2-N1

のルートが構築できた．このうち，３つの経路は正しい経路であるが，4 番目のケースは正しくない．このケースは間違った経路を出力した例であるが，架空のノードを再構築する可能性も確認している．

8. 辺情報と経路構築について

これまでの IP トレースバックの研究は，IP v 4 を扱ったものが多く，IP v 4 の制約にそった提案となっている．たとえば，IP v 4 では，ヘッダに余裕がないため，IP トレースのための情報を格納する場所が限られている．そこで，XOR エンコーディングは格納すべき辺情報の情報量を節約するよい方法と考えられる．ところが，DDoS 攻撃のように同種のパケットが複数の発信元から送信されてくるため，距離の情報だけでは異なる経路のパケットを分類することができず，IP アドレスリストを正しく展開できない．

IP アドレスがランダムに存在する場合には，隣接ノードだけでなく，隣接していないノード間の情報を収集し利用することによって，回避できるケースも多いが，連続した IP アドレスが経路上で集中している場合には，やはり正しく経路構築ができない．

XOR などで辺情報を集約せず，２つの IP アドレスを両方格納した場合，情報量の増大によるパケットの送信遅延への影響を考慮する必要がある．さらに IP v 6 は IP v 4 に比べアドレス空間が大きいため，IP アドレスのうちプレフィックスのみ（上位 64 ビット）をトレースすべき IP 情報とし，ホストアドレスは除外した．IP v 4 XOR エンコーディングの 4 倍となるが，計測結果では，著しいターンアラウンドの低下はみられなかった．

9. まとめ

PPM 方式 IP トレースバックの IP v 6 の実装手法について提案した．小規模な実験ネットワークにおいて実験した結果から，ルータの負荷は軽微と思われるが，XOR エンコーディングの辺情報では，複数経路からパケットを受信した場合，正しく経路を構築することできない．XOR を用いず両端の IP 情報を格納すれば，複数経路を正しく構成できる．その場合も処理性能への負荷は少ないと考えられる．

また，今回の報告では固定的な確率値を用いたが，今後は，可変値を含めた確率値の付与に関する検討を行う予定である．

文　献

[1] 門林雄基，大江将史，“IP トレースバック技術”,情報処理,vol.42,no.12,pp.1175-118,2001.

[2] S. Savage, D. Wetherall, A. Karlin and T. Anderson, “Practical Network Support for IP Traceback”, In Proceedings of SIGCOMM'00,pp.295-306,2000.

[3] M.Oe,”IP traceback mechanism using IPv6 Flowlabel”, In Proceegdings of 50th IETF itrace WG, 2001.

[4] C.Shannon, D.Moore and K.Claffy,”Characteristics of Fragmented IP Traffic in Internet links”, In Proceegins of Networking 2002, pp.697-708,2002.

[5] N.Nishio, N.Harashima and H.Tokuda,”Reflective Probabilistic Packet Marking Scheme for IP Traceback,” In Proceedings of ISPJ JOURNAL vol.44.,no.8, pp.1848-1860,2003.

[6] 山名正人，平田勝久，清水弘，中谷浩茂，甲斐俊文，塚本克治，“DoS 攻撃に対する IP トレースバック手法のシミュレーション－IP マーキングトレースバック方式のシミュレーション—”,情報処理学会研究報告，2004-QAI-13, pp.1-6,2004.

[7] S. Hagen,”IPv6 エッセンシャルズ”,オライリー・ジャパン，2003.

[8] M. Harayama, N. Kakehi, and D. Takeuchi, “Implementation of Probabilistic Packet Marking for IPv6 Traceback”, IEEE IPSI2005 Journal, pp. 54-58, 2005.