RSTPを使った透過型PPMシステムの耐障害性向上

後藤成聡† 金岡晃‡ 岡田雅之§ 岡本栄司†

†筑波大学
305-8577 茨城県つくば市天王台 1-1-1
{goto@cipher.,okamoto@}risk.tsukuba.ac.jp

‡東邦大学
274-8510 千葉県船橋市三山 2-2-1
akira.kanaoka@is.sci.toho-u.ac.jp

§一般社団法人日本ネットワークインフォメーションセンター
101-0047 東京都千代田区内神田 3-6-2 アーバンネット神田ビル 4F
okadams@nic.ad.jp

あらまし DoS 攻撃などのデータ送信元を追跡する技術に確率的パケットマーキング（PPM）がある．著者らはこれまでに PPM を現実的に適用するためのシステムとして透過型 PPM 装置を提案・開発してきた．透過型 PPM 装置は既存ルータの設定を変更することなくルータを PPM 対応とすることが可能であるが，透過型 PPM 装置自身が単一障害点となってしまうため，システムの故障率に大きな影響を及ぼす．そこで本論文では，Rapid Spanning Tree Protocol（RSTP）を利用し透過型 PPM 装置設置による故障率増加を抑えるシステムを提案し，提案システムによる故障率の評価とシステム実装による実証実験の評価を行う．

Tolerant Transparent Probabilistic Packet Marking System using RSTP

Nasato Goto† Akira Kanaoka‡ Masayuki Okada§ Eiji Okamoto†

†University of Tsukuba
Tennoudai1-1-1, Tsukuba-city, Ibaraki 305-8577 Japan
{goto@cipher.,okamoto@}risk.tsukuba.ac.jp
‡Toho University
Miyama2-2-1, Funabashi-city, Chiba 274-8510 Japan
akira.kanaoka@is.sci.toho-u.ac.jp

§Japan Network Information Center
Uchikanda 3-6-2, Chiyoda, Tokyo 101-0047 Japan
okadams@nic.ad.jp

Abstract Probabilistic Packet Marking (PPM) is one of the technique for IP Traceback. We have proposed and developed the Transparent PPM device for practical use of PPM. However, Transparent PPM device that achieves existing routers to be ready for PPM by deploying between routers, can be Single Point of Failure (SPOF) in the system. In this paper, we propose Tolerant Transparent PPM system using Rapid Spanning Tree Protocol. Then, we show evaluation of the proposed system from two point of view: improvement of availability and performance.

1　はじめに

IP（Internet Protocol）ネットワーク上で通信を行う際，パケットは送信元ホストから宛先ホストへと転送される．しかし多くのホスト間は異なるネットワークセグメントに属し IP 層で直接通信を行うことができないため，IP 層の中継器であるルータを介して通信を行う．

パケットの経路を知る要求はいくつかのケースが存在する．代表的な例として，分散型サービス妨害（Distributed Denial of Service，以後 DDoS）攻撃における攻撃側から攻撃対象（被害者）への大量のパケットが転送されてきた経路を知り，経路上で攻撃への対策を講じることが挙げられる．

IP トレースバックは，パケットが中継されてきた経路情報を与える技術であり，さまざまなアプローチで研究開発が行なわれてきた．確率的パケットマーキング（Probabilistic Pac-ket Marking，以後 PPM）手法は，IP トレースバック手法の 1 つであり，パケットが中継されるルータの情報をパケットに確率的に書き込む手法である．中継するルータは確率的に自身の情報をマークするため，受信者側では受信までに中継された様々なルータの情報を集めることができ，それらの情報をもとに経路情報を構築することが可能になる．

PPM 手法は 2000 年に Savage らにより提案された後 [1]，様々なアプローチが研究されてきた [2]〜[17] ．最近の研究では実装面での成果をもとに最適なマーキング確率を求めることを可能にするなど [9]，基礎研究を超えて応用研究や実際の展開・運用といった問題を考える段階に進みつつある．

実際の展開や運用を検討すると PPM には依然多くの課題が残る [11]．その 1 つに既存ルータへの適用がある．既存のルータを PPM 対応させるには，ルータの OS やソフトウェアの入れ替え・更新，またはルータ機器自身の入れ替えなどが必要になるが，そういった作業は基幹に近いルータになるほど，パフォーマンスの低下や高いコストがかかるなど問題が大きく，容易ではない．

著者らはこの問題を解決するために透過型 PPM 装置を提案･開発してきた [17]．PPM 未対応ルータに代わって透過型 PPM 装置が PPM に必要なマーキング，距離情報の追加作業を行うことで，既存ルータの機能更新や機器入れ替えをせずに PPM 対応が可能となる．また透過型 PPM 装置の実装実験により，当装置を用いて PPM を行った場合の packet per second（pps）は PPM を行わない場合とほぼ同様であることが示された．一方で透過型 PPM 装置をネットワークシステムに導入することで，当装置自体が単一障害点となるという新たな問題点が挙げられる．

そこで本論文では，Rapid Spanning Tree Protocol（RSTP）に対応したスイッチを用いることで，透過型 PPM 装置設置による故障率増加を抑え，障害から迅速に復旧できるシステムの提案を行う．本システムに用いる RSTP 対応のスイッチは 2 万円程度と安価で購入することができる．これらの装置を元に実際に本システムを構築し，故障率による評価，pps や障害からの復旧時間の計測による評価を行う．

本論文の構成は以下の通りである．第 2 章で IP トレースバックと PPM について解説し，第 3 章で透過型 PPM 装置の概要と課題について述べる．第 4 章で提案手法の説明を行い，第 5 章で提案システムの評価を行う．最後に第 6 章でまとめる．

2　確率的パケットマーキング

IP トレースバックにはロギング手法，ICMP 手法，リンクテスト手法，パケットマーキング手法など様々な手法があり，またそれらを複合的に使うハイブリッド手法も存在する．PPM はパケットマーキング手法に属し，パケットへ経路情報を付与する手法の中でその付与を確率的に行なう手法である．

2.1　確率的パケットマーキング手法

パケットマーキング手法は，攻撃元から攻撃対象へ至る途中経路のルータにおいて，通過するパケットの IP ヘッダの特定部位を利用して，

攻撃経路の再構成が可能となる情報を書き込む．攻撃対象となった被害者や通信経路上のルータは，受信したパケットのヘッダ情報から書き込まれたマーキング情報を取り出し攻撃経路を再構成する．パケットマーキング型手法の提案当初，マーキング情報はルータ自身の IP アドレスと付随する情報とされた．その後，パケットマーキング手法は一般化され IP アドレス情報だけではなく様々な情報を通知することが可能となっている．

パケットマーキング型の長所としては，中央管理システムが不要であることや，余計なトラフィックを生成しないこと，IP トレースバックシステム全体の自動化の実現性が比較的高いと予想できるなど複数の長所が知られている．

2.2 Savage らによる PPM 手法

Savage らが提案した手法は，パケットが中継される経路上においてルータが確率的に自身の情報をマーキングする手法である．確率的にマーキングを付与する方法としては最初のものである．

Savage らの手法では，ある確率を持つルータ A は自身の IP アドレス情報を IPv4 パケットのヘッダにある Identification フィールドに書き込む．32 ビットの IP アドレスに対し 16 ビットしかない Identification フィールドに書き込むために，32 ビット IP アドレスと，32 ビット長の IP アドレスのハッシュ値を 1 ビットずつ交互に並べ（ビットインタリーブ），64 ビットのデータを 8 ビットずつの 8 ブロックに分解する．16 ビットの Identification フィールドのうち，3 ビットをどのブロックのデータが記入されているかを示すオフセット，5 ビットをマークされたルータまでの距離情報を示すデータ，そして 8 ビットを分割されたブロックデータとして使う．マーキングを行なわないルータは，距離情報に 1 を加えて転送する．

Savage らの手法の特徴は，マーキングしたルータだけの情報を記載するだけでなく，マーキングしたルータの隣のルータの情報も排他的論理和により書き込むことで，どの 2 ルータ間を

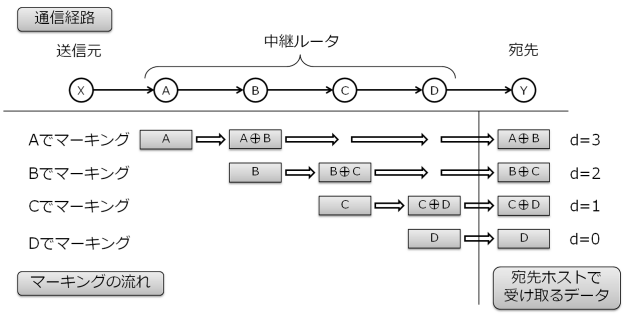

図 1: Savage らの手法でのマークパケットの受信

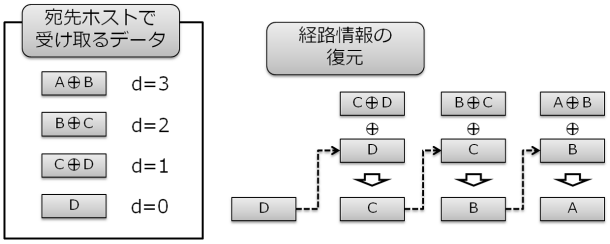

図 2: Savage らの手法での経路情報の再構成

通ったかの情報を運ぶことにある．これを Savage らは Edge Sampling と呼んでいる（図 1）．

経路再構成を行なうホストでは，マーキングされたパケットを収集し，距離情報を元に再構成を行なう．まず距離情報が 0 のマークは，排他的論理和が行なわれていないために，直近のルータそのものの情報となる．そのルータ情報を元に，距離情報 1 のマークと再度排他的論理和を取ることで，距離 1 のルータの IP アドレスを取得することができる．この作業を繰り返すことで，経路上にあるルータ群の IP アドレスを取得することができる（図 2）．

3 透過型 PPM 装置

3.1 透過型 PPM 装置提案の背景

多くの研究で攻撃経路の再構成に必要な収集パケット数の効率化が図られ，さらに実装や最適確率の議論がされるなど，PPM 手法自体の

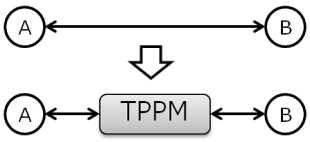

図 3: 透過型 PPM 装置の配置

研究は進んでいるが，実用化を検討する場合にはまだ多くのことを検討しなければならない．

金岡らが整理した PPM の実用化への要件としては非マークパケットの被害者側での処理，対応ノードの増減に対する動的対応，攻撃直近ノード検出後の対応，法的対応などがある [11]．

上記要件に加え，PPM 対応ルータを展開するにあたって解決すべき課題はまだ多く存在し，その 1 つに既存ルータへの適用がある．既存のルータを PPM 対応させるにはルータの OS やソフトウェアの入れ替えや更新，またはルータ機器自身を入れ替えることなどが必要になる．そういった作業は基幹に近いルータになるほどパフォーマンスの低下や高いコストがかかることなど問題が大きく，ルータを PPM 対応させるのは容易ではない．

3.2 透過型 PPM 装置の概要

既存ルータの PPM 対応化の問題に対し，著者らはこれまでに透過型 PPM（Transparent PPM，以後 TPPM）装置を提案してきた [17]．

PPM は各ルータにおいてパケット転送時にマーキングや距離情報の追加を行う．透過型 PPM 装置は図 3 のようにルータ間に接続され，マーキングと距離情報の追加作業を代行することで，既存ルータの機能更新や機器入れ替えを必要とせずに PPM 対応を可能にする．IP 上のルーティングを行なわいため，IP 層ではその存在を確認することなく透過的に見える．

TPPM 装置の具体的な実現方法は，ethernet フレーム自身も変更することなく中継をおこなうリピータ形式と，ethernet によるフレーム交換により実現するブリッジ・スイッチ形式がある．

さらに TPPM 機器によるマーキングの代行は 2 つに分けられる．1 つは接続された 1 台のルータのマーキングのみを代行するケースであり，もう 1 つは接続されたうち複数台のルータのマーキングを代行するケースである．特に後者の場合には，ルータ上でパケットが出力されるポートに注目してマーキング情報の設定を行う必要があり，技術的な困難性が増す．

しかし，特に Savage らの手法の場合，複数台のルータのマーキング代行を行なうことで 2 回行なわれなければならなかったマーキング作業（マーキングされたルータでのマークと，その隣接ルータによる排他的論理和によるマーキング上書き）が 1 回の作業ですむこととなり，効率化が図れるという利点がある．

3.2.1 透過型 PPM 装置の性能評価

TPPM 装置の実装について，岡田らは Linux のカーネル部分に PPM 機能を適用することでこれを実現した [17]．そしてリピータ形式の TPPM 装置を含む実験環境において，PPM カーネルを利用せず単なるリピータとした場合 (non-PPM) と複数のマーキング確率を設定し PPM カーネルを利用した場合 (PPM with $p = 0, 0.082, 0.5$) の pps を計測し評価を行った．

その結果，non-PPM と $p = 0$ の pps には有意な差は見られず，PPM の実行に大きな負荷がないことが示された．また $p = 0.082$，$p = 0.5$ では前述の 2 つの pps をわずかに下回る場合があるものの，マーキングを行った場合でも十分な通信性能が確保されていることが示された．

3.3 透過型 PPM 装置利用における課題

TPPM 装置を導入することで得られる利点がある一方，当装置の導入がシステムの故障率の上昇をもたらす問題が考えられる．

1 本のケーブルで結ばれた 2 台のルータで構成されたシステムの故障率は，各ルータとケーブルの故障率に依存する．しかし，ここに TPPM 装置を導入することで，当装置自体が単一障害点（Single Point of Failure）となり，システム全体の故障率に影響を及ぼす可能性がある．

詳しく見るため，図 3 においてルータ A の故障率を α_A, ルータ B の故障率を α_B，2 つの

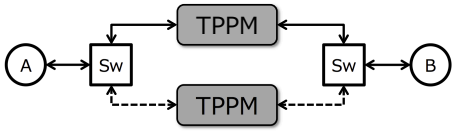

図 4: R-TPPM システム：両側

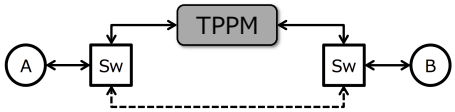

図 5: R-TPPM システム：片側

ルータを結ぶケーブルの故障率を α_{Ca}，そして TPPM 装置の故障率を α_{TPPM} とする．この時，図 3 の上の TPPM 装置を含まない構成のシステム全体の故障率は $1-(1-\alpha_A)(1-\alpha_B)(1-\alpha_{Ca})$ となる．この式を γ とし，同様に下の TPPM 装置を含む構成の場合を考えると，システム全体の故障率は $1-(1-\gamma)(1-\alpha_{Ca})(1-\alpha_{TPPM})$ となる．これより，TPPM 装置の故障率がシステム全体の故障率に大きく影響することが分かり，故障率の上昇を抑える仕組みが必要であると言える．故障率の式に具体的な値を当てはめた場合の比較結果は 5.1 節にて詳述する．

4　提案システム

本研究では 3.3 節で述べた課題に対し，RSTP に対応したスイッチを利用することで TPPM 装置設置による故障率増加を抑え，迅速に復旧できるシステムの提案 (以後 R-TPPM システム) を行う．

今回用いた RSTP は OSI 参照モデルの第 2 層における通信のループの防止や障害耐性向上のために使われる STP（Spanning Tree Protocol）を高速に実現したプロトコルである．STP では障害発生時の経路切り替えに約 50 秒ほどの時間を要していたのに対し，RSTP では数秒程度で切り替えが可能である．

R-TPPM システムの構成は図 4 または図 5 のようになる．ここで Sw は RSTP に対応したスイッチを表している．本システムにおいて

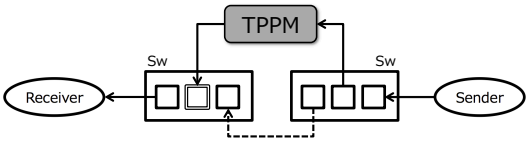

図 6: 実験環境の概要図

通常の通信は実線の経路を通して行われ，上の TPPM 装置に障害が発生し通信が遮断された場合に，RSTP により自動的に点線の経路を通して通信が再開する．切り替えた経路にも TPPM 装置を設置する場合 (図 4)，設置しない場合 (図 5) の選択は使用者のポリシーに依存する．

5　提案システムの評価

本研究で提案した耐障害性向上を目的とした R-TPPM システムの評価を行うため，数式による故障率の算出と実験環境での pps によるパケット処理能力測定，障害からの復旧時間測定を行った．

実験環境は図 6 の構成とした．Sender の OS は Mac OS X，Receiver の OS は Linux（CentOS）であり，共に 1 Gbps の Network Interface Card（NIC）をもつ．TPPM 装置は FUJITSU ESPRIMO D750/A（Dual Core of Intel Core i5（3.20Ghz），4GB RAM, Intel PRO/1000 NIC（1Gbps）, BUFFALO LGY-PCI-GT（1Gbps））で OS は Linux（Debian GNU/Linux 6.0.1）を利用した．スイッチは NETGEAR GS 108T（8 ports, 1Gbps）を 2 台用いる (図 6 では利用した 3port のみを示している)．スイッチ間をまたいで VLAN-ID の設定を行い，実線の経路が途切れた場合に RSTP によって自動的に点線の経路に切り替わるよう設定を行った．

5.1　故障率による評価

3.3 節と同様の方法で提案システムの故障率を算出する．スイッチ（Sw）の故障率を α_{Sw} とし，その他の機器の故障率は 3.3 節と同様である．

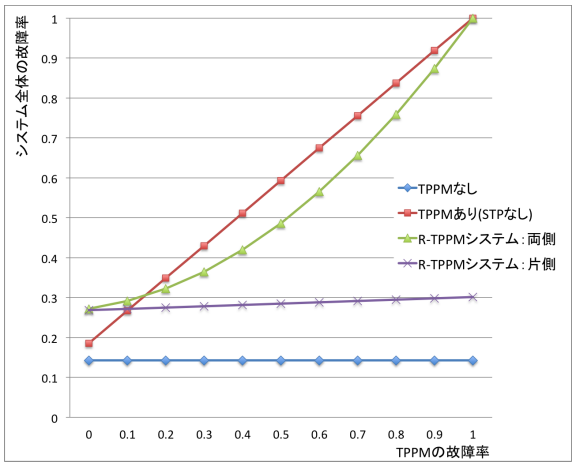

図 7: TPPM の故障率とシステム全体の故障率の関係

図 4 に示した R-TPPM システム：両側の全体の故障率は $1-(1-\alpha_A)(1-\alpha_B)(1-\alpha_{Ca})^2(1-\alpha_{Sw})^2(1-(1-(1-\alpha_{Ca})^2(1-\alpha_{TPPM})^2)$ となる．また図 5 に示した R-TTPM システム：片側の全体の故障率は $1-(1-\alpha_A)(1-\alpha_B)(1-\alpha_{Ca})^2(1-(1-(1-(1-\alpha_{Ca})^2(1-\alpha_{TPPM})))\alpha_{Ca})$ となる．

上記 2 式と 3.3 節で示した 2 つの式をグラフに表したのが図 7 であり，TPPM 装置の故障率の変化に対するシステム全体の故障率を表している．ここでは具体的なパラメータとしてルータ A,B，ケーブル，スイッチの故障率 $(\alpha_A, \alpha_B, \alpha_{Ca}, \alpha_{Sw})$ を全て 0.05 とした．

結果を見ると TPPM を利用しない場合のシステム全体の故障率は一定であるのに対し，STP なしで TPPM を利用した場合の全体の故障率は TPPM の故障率に比例している．また両経路にて TPPM を用いた R-TPPM システムでは TPPM の故障率増加に対し 2 次関数的に全体の故障率が増加しているが，大部分において STP なしの TPPM 利用の故障率を下回っている．これに対し一方の経路にて TPPM を用いた R-TPPM システムは全体の故障率も一定となる傾向があり，STP なしの TPPM 利用，両経路の R-TTPM システムに対し全体の故障率は十分に小さいと言える．

5.2 パケット処理能力による評価

図 6 の実験環境における送受信者間のパケットの処理能力の計測を行った．

PPM のマーキングの有無や確率が異なる以下の 5 つのパラメータに対して測定を行った．

- only-Switch（説明は後述）
- non-PPM（未 PPM 化の通常カーネル）
- $p = 0$（マーキングせず距離の可算のみ）
- $p = 0.082$
- $p = 0.5$

only-Switch は図 6 において TPPM 装置を通さず，1 つのスイッチを介して Sender と Receiver が直接接続された状態を意味する．$p = 0.082$ は岡田らによって算出された PPM の理想的なマーキング確率である [9]．

測定は netperf によって UDP パケットのサイズを変えながら送信し，各パケットサイズにつき 10 回の計測を行った．その平均値についてそれぞれのパケットサイズから pps を算出した．

結果を図 8 に示す．パケットサイズが 1000Byte を超えるまで only-Switch，non-PPM，p=0.5 と p=0，p=0.082 との間にわずかながら差が生じているが，全体としてマーキング確率を設定し PPM を行った場合でも only-Switch や non-PPM と同程度の pps を得ることができている．1000Byte 以降，only-Switch に比べ他のパラメータの pps が低いが，この原因は TPPM 装置のマーキングを行う NIC がボトルネックになっているものと考える．

5.3 障害からの復旧時間による評価

TPPM 装置を含むシステムに障害が発生した場合を想定し，そこから RSTP によって経路が切り替わり通信が継続されるまでにどのくらい時間がかかるか計測を行った．

測定には netperf を用いて UDP パケットを流し，それを受信側で tcpdump で観測した．パケットが流れている最中に図 6 の左のスイッチの 2 重線のポートから LAN ケーブルを抜き，

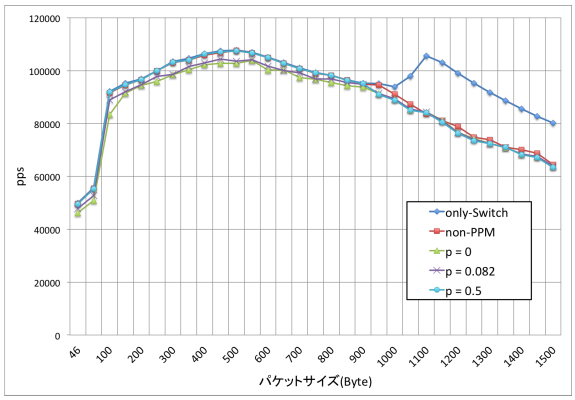

図 8: パケットサイズごとの pps

TPPM 装置を含む実線の経路が点線の経路に切り替わり通信が行われるまでの時間を受信側でキャプチャした結果から求めた．TPPM で設定したマーキング確率は $p = 0.082$，送信したパケットサイズは 1500Byte とした．

10 回計測し平均値をとったところ，結果 0.91 秒であった．これにより RSTP 機能をもつスイッチを利用することで，TPPM 装置に障害が発生した場合でも，1 秒以内という非常に短時間で通信が復旧できることが分かった．

また図 9 は 10 回の計測のうちの 1 回を Wireshark に入力し，時間経過ごとのパケット流量を表したグラフである．Y 軸は netperf により転送されたデータの転送量 (Byte) を表す．時系列順に見ていくと開始から 5 秒後，LAN ケーブルを抜いた箇所で転送量が 0 になっている．ここから約 1 秒で経路が切り替わり，TPPM を経由しない経路になると先ほどよりも転送量が増加している．これは図 5.2 で見たように Switch のみを経由することで TPPM 装置を経由するよりも高い pps が得られるためである．開始から 10 秒後に LAN ケーブルを元のポートに再び差し込み，そこから約 18 秒後に転送量が最初の値に戻っていることから，この段階で再び TPPM 装置への経路に戻ったと考えられる．

6　まとめ

本論文では確率的パケットマーキング (PPM) 手法の実用化へ向けた課題の 1 つである，既存

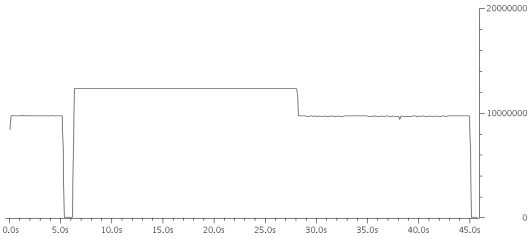

図 9: 時間経過に伴うパケット流量の変化

ルータの PPM 対応化について，透過型 PPM 装置を導入することで当装置自体が単一障害点となる可能性について議論し，その解決を図った．透過型 PPM 装置は 2 つの PPM 未対応ルータに挟まれ，代理でマーキングを行う装置であるが，当機器がネットワークシステムに加わることによりシステムの故障率に大きな影響を及ぼす．

そこで RSTP に対応した安価なスイッチを用いることで，障害が発生した際に迅速・かつ自動的に経路を切り替え通信を継続するシステムを提案し，故障率による評価と実際の実験による評価を行った．その結果，RSTP 対応のスイッチを用いることで単に透過型 PPM 装置をルータ間に挟んだだけの場合に比べシステム全体の故障率を大幅に抑えることが可能であることが分かった．また TPPM 装置を含む通信経路に障害が発生した場合でも，1 秒以内に経路を切り替え通信を再開できることが確認された．

参考文献

[1] S. Savage, D. Wetherall, A. R. Karlin, and T. Anderson, ”Practical Network Support for IP Traceback”, in Proc of ACM SIGCOMM, pp.205-306, 2000.

[2] D. Song and A. Perrig, “Advanced and Authenticated Marking Schemes for IP Traceback”, in Proc. IEEE INFOCOM, pp. 876-886, 2001.

[3] D. Dean, M. Franklin, and A. Stubblefield, “An Algebraic Approach to IP

Traceback,", in Proc. Network and Distributed System Security Symp. (NDSS), pp. 3-12, 2001.

[4] 岡崎直宣, 河村栄寿, 林美娘,“ サービス不能攻撃の経路追跡手法の効率化に関する検討”, 情報処理学会論文誌, vol. 44, no. 12, 3197-3201, 2003.

[5] T. K. T. Law, D. K. Y. Yau, and J. C. S. Lui,“An Effective Statistical Methodology to Traceback DDoS attackers“, IEEE Trans. Parallel Distrib. Syst., Vol. 16, No. 9, pp. 799-813, Sep. 2005.

[6] M. T. Goodrich, “Probabilistic Packet Marking for Large-scale IP Traceback“, IEEE/ACM TRANSACTIONS ON NETWORkING, Vol. 16, No. 1, pp. 15-24, 2008.

[7] A. Durresi, V. Paruchnri, L. Barolli, R. Kannan, and S. S. Lyengar,“Efficient and Secure Autonomous System Based Traceback”, Journal of Interconnection Networks, 5(2): 151–164, 2004.

[8] V. Paruchnri, A. Durresi, and L. Barolli, “FAST: Fast Autonomous System Traceback”, 21st International Conference on Advanced Networking and Applications (AINA ’ 07), pp. 498-505, 2007.

[9] 岡田 雅之, 金岡 晃, 勝野 恭治, 岡本 栄司, ”確率的パケットマーキングにおける最適マーキング確率の推定”, 情報処理学会論文誌, Vol.52, No.3, pp.929-939, 2011.

[10] 金岡晃, 岡田雅之, 勝野恭治, 岡本栄司, ”攻撃経路を効率的に再構築するためのトポロジ特性を利用した確率的パケットマーキング手法”, 情報処理学会論文誌 Vol.52, No.3, 2011

[11] 金岡 晃, 岡田 雅之, 岡本 栄司, ”確率的パケットマーキングの実用化検討”, コンピュータセキュリティシンポジウム 2011 年論文集, Vol.2011, No.3, pp.618-623, 2011.

[12] M. Okada, A. Kanaoka, Y. Katsuno, E. Okamoto, ”32-bit AS Number Based IP Traceback”, in Proc. of the Fifth International Workshop on Advances in Information Security (WAIS-2011), pp.628-633, 2011.

[13] J. Liu, Z-J. Lee, Y-C. Chung, ”Dynamic probabilistic packet marking for efficient IP traceback”, The International Journal of Computer and Telecommunications Networking, vol. 51, Issue 3, 2007.

[14] H. Tian, J. Bi, X. Jiang, W. Zhang, ”A Probabilistic Marking Scheme for Fast Traceback”, in Proc. of the the 2010 2nd International Conference on Evolving Internet, 2010.

[15] W. Yen, J-S. Sung, ”Dynamic Probabilistic Packet Marking with Partial Non-Preemption”, in Proc. of the 5th international conference on Ubiquitous Intelligence and Computing (UIC ’08), 2008.

[16] L. Lu, M-C. Chan, E-C. Chang, ”A general model of probabilistic packet marking for IP traceback”, in Proc. of the 2008 ACM symposium on Information, computer and communications security (ASIACCS ’08), 2008.

[17] M. Okada, N. Goto, A. Kanaoka, E. Okamoto, ”A Device for Transparent Probabilistic Packet Marking”, in Proc. of the 4th IEEE International Workshop on Network Technologies for Security, Administration and Protection (NETSAP2013) , 2013.