確率的パケットマーキング手法の実用化検討

金岡 晃 †　　岡田 雅之 ‡　　岡本 栄司 †

† 筑波大学
305-8573　茨城県つくば市天王台 1-1-1
kanaoka@risk.tsukuba.ac.jp, okamoto@risk.tsukuba.ac.jp

‡ 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 2-3-4　国際興業神田ビル 6F
okadamas@nic.ad.jp

あらまし サービス妨害（DoS）攻撃における対策の 1 つである確率的パケットマーキング（PPM）手法は、実用化にあたっては多くの課題を残している。本論文では実用化の要件を整理し、要件のいくつかを解決する手法の提案を行なった。

Toward Practical Probabilistic Packet Marking

Akira KANAOKA†　　Masayuki OKADA‡　　Eiji OKAMOTO†

†University of Tsukuba
1-1-1, Ten-nodai, Tsukuba, Ibaraki, 305-8573, Japan
kanaoka@risk.tsukuba.ac.jp, okamoto@risk.tsukuba.ac.jp

‡Japan Network Information Center (JPNIC)
16F Kokusai-Kougyou-Kanda Bldg. 2-3-4 Uchikanda, Chiyodaku, Tokyo 101-0047, Japan
okadams@nic.ad.jp

Abstract Probabilistic Packet Marking (PPM) which is a defense method for Denial of Service (DoS) attack, has many subjects to practical use. Requirements for practical use and some solutions are presented in this paper.

1　はじめに

サービス妨害（Denial of Service、以後 DoS）攻撃や分散型 DoS（Distributed DoS、以後 DDoS）攻撃はインターネット上で非常に大きな脅威となっている。DoS/DDoS 対策はさまざまなアプローチで研究が行なわれており、その中でも被害者から攻撃元までの攻撃経路をもとめることができる確率的パケットマーキング（Probabilistic Packet Marking、以後 PPM）は実装や最適マーキング確率の計算などが行なわれ、現実的な配置に向けた応用の段階に来ている。

手法として成熟してきる一方で、実用化に向けてはまだ数々の課題が残っている。例えば、多くの PPM 研究ではネットワーク上の全てのノードが PPM に対応していることを前提としているが、実用上はその前提は非現実的であり、PPM 非対応ノードが混在する環境を十分に考慮した方式や運用が重要となってくる。

本論文では PPM の実用化に向けた要件の整理を行ない、そしてその要件のうちいくつかについて解決方法を提案する。

2 関連研究

DoS 攻撃に対する防御手法の研究は多岐にわたる。Peng らは DoS 攻撃と防御手法の整理を行なっておりその広さを一端を知ることができる [1]。

攻撃元や攻撃経路の特定手法であるトレースバックも DoS 攻撃に対する防御手法の 1 つとして多く研究されている。トレースバックに関しては高橋らがその分類を試みている [2]。

PPM はトレースバック技術の 1 つであり、ロギング手法や ICMP（Internet Control Message Protocol）手法と比較してストレージや追加の通信の必要性がない利点を持つ。Savage らにより提案された PPM[3] は、その後様々なアプローチにより改良が加えられており、PPM の欠点とされている攻撃元までの経路を判別するまでに必要な取得パケット数の短縮や DDoS 時の誤検出の改善が図られている [4, 5, 6, 7, 8, 10, 9, 11, 12, 13]。

Savage らが提案した PPM はルータごとにマーキングを行なうものだったが、Durresi らや岡田らは AS（Autonomous System）単位で PPM を行なう手法を提案している [6, 7]。また多くの PPM 手法は各ルータ/AS におけるマーキング確率を等しくしているが、近年ではマーキング確率を動的に変化させる手法も提案されている [8, 9, 10]。

従来では PPM のマーキング負荷を考慮して数式評価が行なわれていたが、2011 年に岡田らは Linux カーネルに PPM 機能を搭載し実験を行ない、マーキング負荷が無視できるほどであることを示した [13]。この結果により、PPM の最適確率を議論することが可能となった。

2.1 Savege らの確率的パケットマーキング手法

Savage らが提案した PPM は、攻撃者から被害者にいたる経路上のルータが確率的に自身の情報を IPv4 のヘッダに書き込むものであった。マーキングするルータの IP アドレス（32bit）とそのハッシュ値（32bit）を合わせたデータを 8 分割し、IPv4 ヘッダ中の Identificatin フィールド（16bit）に書き込む。フィールド中には分割データの他に、オフセット情報と距離情報がマークされる。

被害者側は経路上のルータのマーキングを収集し、距離情報とオフセットの組を揃える。その後距離情報の少ないものから IP アドレスを復元し、攻撃経路上のルータ IP アドレス群を得る。経路構築に必要なパケット数の期待値を攻撃者までの距離ごとに算出し、評価が行なわれた。この評価手法は他の PPM 論文でも一般的に用いられている。複数攻撃者が存在する DDoS 環境では、経路復元時にハッシュ値の衝突による誤検知（False Positive）が発生するため、誤検知の発生率も評価されている。

2.2 金岡、岡田らによる PPM の Linux ルータ実装と最適確率計算

Savage らの手法ではマーキング確率を 1/25 として評価が行なわれており、他の論文でも同様の確率が利用されていた。しかし確率の設定に関してはルータの負荷も考慮されるべきとされる一方で、確率の最適性に関しては深く議論されてこなかった。

金岡らは距離の要因を排除するために、インターネット上のルータトポロジ情報を利用しルータの 2 点間距離の分布を求め、分布情報を基に距離に依存しない必要パケット数を求めた。また実際に Linux カーネルに PPM 機能を実装することでその負荷を測った。その結果、PPM の負荷は無視できるものであることがわかり、確率の最適性は必要パケット数の最小化を実現することで得られることを示した。

3 確率的パケットマーキングの実用化要件

多くの研究で攻撃経路構築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。

3.1 PPM 非対応ルータ/AS の考慮

これまでの研究では、インターネット全体など、対象とするネットワーク全体のルータや AS（以下ノード）が ppm 対応ノードであることが前提だった。しかしこの前提は非現実的である。現実適用を考えた場合には、未対応ノードが混在することを含めた方式を考慮しなければならない。混在環境で考慮すべき事項は以下のことがある。

- 対応ノード状況の把握
- マーキング確率の設定方法
- マーキングフィールドの構成方法
- 非マークパケットの被害者側での処理
- 攻撃者に最も近いのノード検出後の対応

非対応ノードが混在する環境では、マーキング確率とマーキングフィールド構成を最適にする場合、どのノードが対応しているかといった対応ノード状況の把握が必要となる。マーキング確率やマーキングフィールドの構成は、ネットワーク上の対応ノード状況を知ることが可能であれば最適な構成を導出することが可能である。マーキングフィールド構成方法については 4 章で提案する。

混在環境では、マーキングされていないパケットが被害者により多く届く。しかしマーキングの有無を被害者側で判断するのは困難であり、その処理方法が検討されなければいけない。

また厳密な最適性を追求せず、柔軟性を持った対応手法も考えられる。確率やフィールド構成といった構成の柔軟性は対応ノード数の動的変化にも関わるため、3.1.2 で議論する

3.1.1 非マーキングパケットの被害者側での処理

非対応ノードが混在する環境では、被害者のもとに全くマーキングがされていないパケットが増えることが考えられる。これまでの PPM 研究ではマーキングの有無に関する判断材料をマーキング自身に与えることはされていないため、被害者側では受信パケットがマーキングされたものかの判断はできない。混在環境では非マーキングパケットの対応も考慮しなければならない。

手法としてマーキングパケットにマーキング有無の情報を載せることも考えられるが、非マーキングパケットに「マーキング無し」という情報を載せることは困難であろう。

マーキングの有無を問わず、すべてのパケットをマーキングパケットと仮定してパケット再構築を行なうことも考えられる。Savege らの手法やその改良手法は IP アドレスの再構成のためにハッシュ値を付与しているため、再構築時のハッシュ値検証である程度の非マーキングパケットは排除されるが、同時にハッシュ値の衝突可能性が高まるおそれがあることに注意しなければならない。

3.1.2 対応ノードの増減に対する動的対応

新たに対応ノードがネットワークに追加されることや、非対応ノードの PPM 対応移行、あるいは PPM 対応ルータの非対応化等、対応ノードの状況は動的に変化することが考えられる。実用化においてはこのような動的変化に対する対応も考慮しなければならない。

対応を手法として行なうか、あるいは運用で担保するかなどアプローチは複数考えられる。マーキング確率やマーキングフィールドの構成も厳密性を捨ててより柔軟性を持ったものにすることは、対応の 1 つであろう。柔軟なマーキング対応におけるネットワーク上の対応ノード群の把握必要性やその方法も議論されるであろう。

増減に対する動的対応として、フィールド構成を逐次変化させることも考えられるが、その場合は各ノードの変化タイミングの非同期性を考慮しなければならない。途中経路での判断や、被害者側でのパケット排除などが考えられよう。

3.1.3 攻撃直近ノード検出後の対応

PPM による攻撃経路構成により直近のノードは判明するが、非対応ノードが混在する環境では攻撃者がそのノードの管理下にいることを

示すとは言えず、あくまで対応ノード中で攻撃者の直近ノードが判明しただけとなる。攻撃者の追跡、あるいは攻撃の遮断・緩和にあたっては判明後の対応が必要となる。

3.2 マーキング確率の均一性

Dynamic PPM などで一部実現されているが、マーキング確率が均一でない場合の議論もされる必要がある。例えば、ネットワークの中心近くに位置し、各末端ネットワークに対するハブ機能を持つノードがより高い確率でマーキングすることや、逆に低い確率でマーキングすることによる効率の差が考慮される必要がある。このことは対応ノードのネットワーク上の適切な配置を議論することを可能にする。

3.3 PPM 手法の相互運用性

PPM の手法は標準化されておらず、複数の手法が存在する。あるノード群 X は方式 A を採用し、別のノード群 Y は方式 B を採用しているケースも考えられる。同一の方式を採用しているノード群やその方式をドメインと呼ぶとした場合、他のドメインのことを考慮しない場合は、ドメイン外のノードをすべて「非対応ノード」として扱えば良いが、ネットワーク全体でより効果的な DoS 攻撃対策を考慮する場合、ドメイン間での相互運用性も考慮されるべきであろう。

さらに言えば、PPM 手法の相互運用性だけでなく、ロギング方式や ICMP 方式など他のトレースバック手法を含めた相互運用性が保たれることが望ましい。

3.4 法的対応

PPM に限らずトレースバック技術の中には電気通信事業者法第 4 条に規定される「通信の秘密」を侵害する恐れがある。実用化にあたっては十分に考慮されなければならない。

電気通信事業者法の通信の秘密については、PPM 手法ではないが、2009 年に日本データ通信協会がパケットヘッダのハッシュを用いたトレースバック手法についての法的問題点の整理を行なっており [14]、参考にすべき情報である。

また日本以外の他国のノードにおける法的対応も考慮されなければならないケースも十分考えられる。

4 提案手法

本章では、3 章であげた実用化要件のうち、いくつかを解決するための以下の提案を行なう。

- マーキングデータフィールドの算出手法
- 確率的パケットマーキング手法の統一評価手法
- 中央管理機関による管理アーキテクチャ

4.1 マーキングデータフィールドの算出手法

実用化にあたっての要件では IP のバージョンは特定していないが、本提案では Version 4 と Version 6 の双方に対応したフィールド算出手法を提案する。本手法では、IP アドレスなどのマーキング対象データに対し衝突回避のためのハッシュ値を合わせてマーキングすることと、マーキング情報にマーキングしたノードから受信者までの距離情報を含むことを前提とする。

まずマーキングするノードと受信者の距離をどの程度まで考慮するかを決定する。たとえばインターネット上のルータトポロジの場合、任意の 2 点間の 99.964%が 15 ホップ以内であることが知られている。決定した想定最大距離（ルータホップ数）を $d_{\max}$ と置く。

次にパケットのどこにマーキングを行なうかの設定を行なう。IPv4 で Savage らの手法を踏襲する場合は Identification フィールド（16bit）、あるいは Goodrich らの手法のような Identification フィールドと Type Of Service フィールドの計 24bit の利用などがある。IPv6 の場合は独自のヘッダ拡張として利用することも可能である。設定したフィールドのデータ長（ビット）を L_{Field} とする。

続いて IP アドレスや AS 番号など書き込むデータを設定する。設定したデータの長さ（ビット）を L_{ID} とする。

データ分割数 l を決定する。ただし、$l > \frac{L_{\mathrm{ID}}}{L_{\mathrm{Field}}}$ である。

上記の設定情報をもとにハッシュ長を計算する

$$h = l\left(L_{\mathrm{Field}} - \lfloor \log_2 d_{\max} \rfloor - \lfloor \log_2 l \rfloor\right) - L_{\mathrm{ID}}$$

これにより、データフィールドに距離情報と分割された ID とハッシュ値、分割のオフセット値が適切に設定することが可能になる。

4.2 確率的パケットマーキング手法の統一評価手法

PPM の評価は、攻撃経路構築に必要なパケット数の期待値 E と、ハッシュ値衝突による経路復元時の誤検出の 2 つによって行なわれてきた。これらの評価は分かれて行なわれていたため、これら 2 つの評価を合わせた統一評価値 V を提案する。V は、経路構築に必要なパケット数期待値 E と衝突確率 P_{col} より

$$V = \frac{E}{1 - P_{\mathrm{col}}}$$

で与えられる。

4.2.1 Savage らの手法における V の計算

Savege らの手法では、ルータの IP アドレスとハッシュ値を合わせたデータを分割し、パケットにマーキングを行なう。マーキングの際には、データだけでなく、距離情報も記載する。これらを踏まえて V を計算する。

まず必要なパケット数の期待値 E は

$$E = \sum_{d=1}^{\infty} f_d E_d$$

で与えられる。ここで f_d は対応ノード同士により実ネットワーク上に構成される仮想ネットワークの 2 ノード間距離の頻度（割合）である。また E_d は距離 d のときの経路構築に必要なパケット数期待値であり、以下で与えられる。

$$E_d = \frac{ml\ln(ml) + \gamma ml + 1/2}{P_d}$$

ここで m は攻撃者数、l はマーキング時のデータ分割数、γ はオイラーの定数である。また P_d は距離 d でマーキングされたパケットが受信者に届く確率であり、以下で与えられる。

$$P_d = p(1-p)^{d-1}\sum_{i=d}^{\infty} f_i$$

次に、ハッシュ値の衝突確率 P_{col} を計算する。P_{col} はハッシュ長 h と m, l より以下で与えられる。

$$P_{\mathrm{col}} = 1 - \left(1 - \frac{1}{2^h}\right)^{m^l}$$

4.3 中央管理機関による管理アーキテクチャ

ネットワーク内に PPM 非対応ノードが存在し PPM 利用可能ノードが動的に変化する状況を想定する。ノード変化に従ってマーキングの確率とマーキングフィールドの構成を動的変化させる場合には、動的な変化を捕捉し、変化に従った確率とフィールド構成の計算を行ない、更新情報を対応ノードに通知し適用させる必要がある。そこで、ネットワーク上に PPM の中央管理機関を設け、各対応ノードは中央管理機関と定期的に通信を行なうことで、PPM 対応ノードのネットワークへの参加や離脱、また他のノード参加によるネットワークの動的変化に対応する。

ネットワークの動的変化に従ってマーキング確率とフィールド構成を変更するにあたって、中央管理機関は新しいマーキング確率とフィールド構成情報を各参加ノードに通知すると同時に、移行の猶予期間情報も通知する。

各参加ノードは猶予期間中に新しい確率とフィールド構成に移行を行なう。猶予期間中に攻撃経路構築を行なう必要が生じた場合、移行前の構成を前提に経路構築を行ない経路復元を試み、猶予期間後に再度経路構築を行ない比較する。

5 まとめ

PPM 手法は Savege らにより提案されて以来さまざまな改良が提案されてきたが実用化に対してはまだ多くの課題を持っている。本論文では実用化に向けた要件の整理を行ない、PPM 非対応ノードの考慮や PPM 手法の相互運用性、法的対応などを挙げた。

さらに要件のうちいくつかを解決する手法として、マーキングデータフィールドの算出方法と、PPM 手法の評価手法、さらに中央管理機関による管理アーキテクチャを提案した。

参考文献

[1] Peng, C. Leckie, and K. Ramamohanarao, “ Survey of Network-based Defense Mechanisms Countering the DoS and DDoS Problems, ”ACM Computing Surveys, Vol. 39, Issue 1, 2007.

[2] T. Takahashi, H. Hazeyama, D. Miyamoto, Y. Kadobayashi, ”Taxonomical Approach to the Deployment of Traceback Mechanisms”, in Proc. 2011 BCFIC Riga , 2011

[3] S. Savage, D. Wetherall, A. R. Karlin, and T. Anderson, ”Practical Network Support for IP Traceback, ” in Proc. ACM SIGCOMM, pp. 295-306, 2000.

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

[6] 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.

[7] 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) , 2011

[8] 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

[9] 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

[10] 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

[11] 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

[12] 金岡 晃, 岡田雅之, 勝野恭治, 岡本栄司, ”DoS 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

[13] 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. 9, 2011

[14] 財団法人日本データ通信協会, ”本トレースバック手法の導入に関する法的問題点の整理”, 2009