

パケットマーキングとロギングを用いたサイバー攻撃に対するトレースバック

李, 鵬飛

九州大学大学院システム情報科学府

馮, 堯鎔

九州大学大学院システム情報科学研究所 : 助教

川本, 淳平

九州大学大学院システム情報科学研究所

櫻井, 幸一

九州大学大学院システム情報科学研究所 : 教授

<https://hdl.handle.net/2324/1662066>

出版情報 : コンピュータセキュリティシンポジウム. 2015, pp.3E3-4-, 2015-10-21

バージョン :

権利関係 :

パケットマーキングとロギングを用いた サイバー攻撃に対するトレースバック

李鵬飛†, フォン ヤオカイ‡, 川本 淳平‡, 櫻井幸一‡

†九州大学大学院システム情報科学府

‡九州大学大学院システム情報科学研究院

819-0395 福岡市西区元岡 744 番地

あらまし インターネット技術の進歩と共にサイバー攻撃事件が多発している。サイバー攻撃への対策として、攻撃の検知・遮断技術と共に、攻撃者までのトレースバック（IP アドレスの同定）技術が不可欠である。既存のトレースバック技術には、特定の攻撃しか対応できないおよび通信経路再構成の計算量が大きくトレースバックに時間を要するという問題がある。本研究では早期に攻撃者を発見するために、通信経路再構成に要する計算量の小さい新しいトレースバック手法を提案する。シミュレーションにより作成したデータと既存研究で用いられている実験データを利用して、提案手法の性能を実証する。

キーワード：サイバー攻撃、追跡、トレースバック、パケットマーキング、ロギング

A Proposal for Cyber Attack Trace-back With Packet Marking and Logging

Li Pengfei†, Yaokai Feng‡, Junpei Kawamoto‡, Kouichi Sakurai‡

†Graduate School of Information Science and Electrical Engineering, Kyushu University

‡Faculty of Information Science and Electrical Engineering, Kyushu University

744 Motooka, Nishi-ku, Fukuoka 819-0395 Japan

Abstract Cyber-attack incidents have become more and more frequent and serious. As a countermeasure against cyber attacks, the technology of (IP address etc.) trace back to the attackers is essential. Although many methods have been proposed for this purpose, the existing trace-back techniques suffer from several problems, including that only the specific attacks can be traced back, the tracing back is too time-consuming and traffic-path reconfiguration cannot be guaranteed. In this study, to discover the attacker quickly and correctly, we propose a new method. Using simulation data, its performance is demonstrated.

Keyword: cyber attack, trace-back, packet marking, logging.

1. はじめに

サイバー攻撃に対して、有効な防御手段だけでは足りなくなっている。攻撃者を発見し、法的に責任を取らせることが求められている。IP トレースバックはこのために、作られた技術である。幾つの手法が提案された：パケットマーキング[1][2]、ロギング[2]、イングレスフィルタリング[3]、エントロピー変量[4]、ICMP トレースバック[5]等。更に、パケットマーキングとロギングを用いた HIT[6]と PPIT[7]という手法がある。手法[6][7]に最も重要な技術はパケットマーキングとロギングである。しかし、既存のトレースバック技術には特定の攻撃しか対応できないおよびトレースバックに長い時間を要する。実用できるシステムにとって正確的に追跡するだけではなく、早速にトレースバックするのも重要である。トレースバックが遅くなれば、他の被害も出ることや攻撃者が証拠を消すことなど考えられる。

本論文では早期に攻撃者を発見するために、通信経路再構成に要する計算量の小さい新しいトレースバック手法を提案する。

本論文の構成は次の通りである。2章では、関連する既存の技術を紹介する。3章では、提案手法の概要とメリットを説明する。4章では、提案手法に基づいて、シミュレーションを行った結果を説明する。5章はまとめである。6章では、結論と今後の課題である。

2. 既存の関連技術

攻撃者を追跡する為に、攻撃の証拠が必要である。攻撃の証拠を得る為に、通信経路の

記録を利用し、通信経路を再構成するのは最も代表的な方法である。しかし、ネットワークが匿名化アクセスと非国家的という特性があるので、パケットの通信経路に関する記録がない。従って、トレースの為に必要な情報を記録する手法は、パケット中の一部分領域を書き換えるとルーターに記録機能を追加する二種類が利用される。それぞれパケットマーキングとロギングと呼ばれる。本論文では、パケットマーキング技術とロギング技術が用いられる。

2.1 パケットマーキング技術

パケットマーキングとは通信パケットに経由したルーターの IP アドレスをマークする技術である。図 1 はその手法を示す。パケットマーキングとは通過するパケットの中

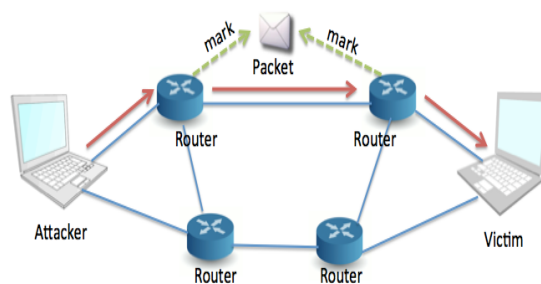


図 1 パケットマーキング

に、ルーターが情報（ルーターの IP アドレスなど）を書き込み、パケットを受信した端末が書き込まれた情報から攻撃ルートを推定する技術である。パケットマーキングは二種類があり、一定な確率でマークする確率的パケットマーキング PPM 法[8]と常にマークする確定的パケットマーキング DPM[9]法である。PPM では、一定な確率でパケットを

経由するルーターの必要な情報でマークする。PPM が低確率（一般的には、確率が 1/25 に設定される）を使うことにより、コストを低減することが注目されている。DPM では、パケットがエッジルーター[10]を経由する際に、ルーターの情報でパケットをマークする。

しかし、これらのパケットマーキング手法はそれぞれの問題がある。確率的パケットマーキング PPM は再構成の計算量が大きくてトレースバックが遅い[11]。パケットをマークする際、パケットにつけたマークが段々増加する。再構成する際、マークとしてのアドレス一つずつを計算しなければいけないからである。一方、確定的パケットマーキング DPM はエッジルーターの性能に依頼する。

2.2 ログ技術

ログ技術とは通信パケットの ID などの情報を経由したルーターに記録するものである[2]。ルーターに記録機能を追加し、パケットがルーターを通過する際、ルーターがパケットの情報を一定の形式で時系列に記録し、保存する。ログ技術は大量なパケットを送るフラッディング攻撃だけではなく、単一パケットを送る攻撃も追跡することができる。本手法の弱点としては大量なパケット情報が記録され、ルーターの負担が増大する。ルーターが全てのパケットを記録するならば、高性能のルーターが必要である。そのためコストは高い。それでも高速かつ大量の攻撃の場合では全てのパケットを記録・保存することも不可能である。従って、DDoS 攻

撃のような大量なパケットを送る攻撃に対応できない。

3. 本研究での提案

3.1 提案の詳細

本提案の基本アイデアは次のとおりである。ルーターが行う操作は二つがある：ルーターの IP アドレスをパケットにマークを書き込むこととパケットの一部分情報と二番目のマークを記録することである。図 2 に示

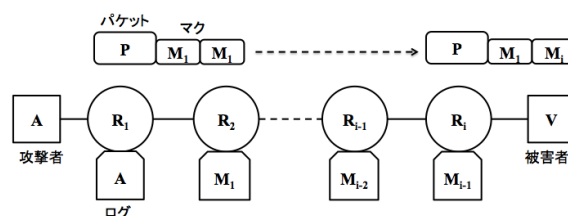


図 2 提案の基本アイデア

したように、各通信パケットに 2 つの領域（マーク領域）を追加する。2 つのルーターのアドレスを保存するためである。通信パケット (P とする) の最初に経由したルーター (R1 とする) では、一定な確率 p で R1 のアドレス (M1 とする) を P にマーキングすると共に、P の始点 IP を R1 にログする。次のルーター (R2 とする) を経由する際、R2 が P のマーク領域をチェックし、もし R1 が P にマーキングされていないならば、これから経由したルーターではマーキングもログもしない。もし R1 が P にマーキングされれば、R2 をもマーキングする。即ち、P のもう 1 つのマーク領域に R2 のアドレス (M2 とする) をマークする。これで、P の 2 つのマーク領域は M1M2 となる。同時に P の始点 IP アドレ

スなどの情報を R_2 にログする。そして、これから経由したルーター (R_i とする) では、 P にあるマーク M_{i-1} (ルーター R_{i-1} のアドレス) を R_i にログしてから、 R_{i-1} の代わりに R_i を P にマーキングする。即ち、 P にあるマーク M_{i-1} を消して、 R_i のアドレス M_i を入れる。これで、 P の2つのマーク領域は M_1M_i となる。このように、 P の2番目のマーク領域の内容が変更し続ける; 経由した各ルーターには一歩前のルーターのアドレスをログする。最後に各パケットの最初と最後のルーターアドレスおよび全経路 (ルーターリスト) の情報ログが残る。

R_1 で一定な確率 p マーキングするのは、攻撃者たち (特に DDoS 攻撃などの場合) は多くのパケットを送ると想定し、その中1つだけでもマーキングできれば十分に追跡できるので、各ルーターの負担を軽減するためである。想定した攻撃者の発送パケット数より確率 p を調整する。既存の確率的パケットマーキングと同じように、想定した攻撃者の発送パケット数が多いほど、確率 p が減らすことができる。想定した攻撃者からパケット数が少ない場合は、 $p=100\%$ とする。即ち、 R_1 は必ずマークキングされる。その場合、何かのトラブルで R_1 はマーキングされなくても、次のルーターはマーキングされるので、トレースバックする際に、無事にマーキングされた最初ルーターまでトレースバックできる。

3.2 提案手法のメリット

本提案手法は5つのメリットがある、

- 1) トレーシングが速い
パケットの1番目マークは経路を無視し、直接にパケットが最初に経由するルーターを探し出しでき、そのルーターのログに攻撃源の IP アドレスが記録されている、容疑者を見つけることができる。
- 2) アドレス偽造に強い
本提案は攻撃の全経路は各ルーターのログに分散的に記録されて、攻撃者が一歩偽造しても、PATH 全体偽装できないはずであるので、本提案はアドレス偽造にも強い。
- 3) ルート再構成の計算量が少ない
マークする際、複雑な計算しないので、ルート再構成する際、複雑な計算は必要がない。
- 4) パケットの負担が軽い
パケットに二つマークだけを付けるので、他の確率的パケットマーキングと比べ、マークが少ない。
- 5) 個々のルーターに依存しない
ルーターの役割を分担し、リスクを減らす。ルーターの役割は大体同じである。そして、一番重要なマークはルーター R_1 のマークであるが、不可欠ではない。他のマークも不可欠ではない。

4. シミュレーション

パケットをトレーシングするシミュレーションを設計して、ルーターを経由する際のパケットの特徴を抽出する。このように作成したシミュレーションデータと既存研究の

実験データを利用して、提案手法の性能を実証する。

本手法では、ロギングの確率はマーキングの確率と同じ、通信パケットがマークされるなら、ルーターにログする。パケットにログしないなら、ルーターにログしない。更に、1回の攻撃にたとえ一つの通信パケットだけが正確的にマークされた場合でも、攻撃元を追跡できる。即ち、1回の攻撃に対して、トレースバックの成功率は正確的にマークされた通信パケットが存在するかどうかにより決められる。

シミュレーションにより、通信パケットが少ない際、確率を100%に設定し、パケット数を増加すると、確率を下がるということを想定する。通信パケット数を100から10000まで増やせ、通信パケット数が100、300、500、1000、2000、3000、4000、5000、10000になる時のマーク数を監視し、各確率で10000回のシミュレーションを実行した。図2と図3に10000回のシミュレーションの実行結果を示した。確率は1/10の場合、通信パケット数が100から10000までふやせば、10000回のシミュレーションでは、追跡できる回数は10000回である。確率は1/20の場合、通信パケット数が100の時、トレースバックの成功率が下がって、99.37%になった。通信パケット数が300に増加した以後、成功率が100%に上がった。確率は1/50の場合、通信パケット数が1000になった以後は、成功率は100%になれる。更に、確率は1/500と1/1000の場合では、成功率が100%になれるのは、通信パケット数が10000になる時で

ある。

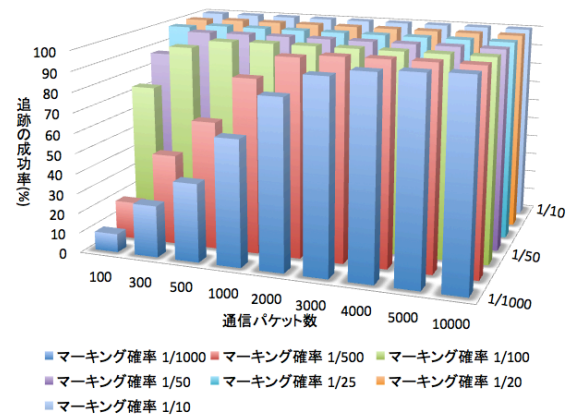


図2 シミュレーションの結果 (図示)

		マーキング確率						
		1/10	1/20	1/25	1/50	1/100	1/500	1/1000
通信 パ ケ ッ ト 数	100	10000	9937	9854	8733	7356	1867	918
	300	10000	10000	10000	9976	9544	4518	2579
	500	10000	10000	10000	9999	9955	6381	3907
	1000	10000	10000	10000	10000	10000	8673	6264
	2000	10000	10000	10000	10000	10000	9821	8398
	3000	10000	10000	10000	10000	10000	9981	9486
	4000	10000	10000	10000	10000	10000	9997	9817
	5000	10000	10000	10000	10000	10000	9998	9934
	10000	10000	10000	10000	10000	10000	10000	10000

図3 シミュレーションの結果 (数値)

図2と図3のシミュレーション結果から分かるように、各確率で通信パケット数が少ない方は成功率が低いである。

図4に各確率1/10、1/20、1/25、1/50で通信パケット数を100から500までを増加させ、シミュレーションをした結果を示した。図4の結果から分かるように、成功率を100%に維持するために、通信パケットが100の時に、マーキング確率が1/10以上にすべきである。通信パケット数が300の時、マーキング確率は1/25なら、まだ追跡できる。通信パケット数は500の時、マーキング確率は1/50は

下限になる。

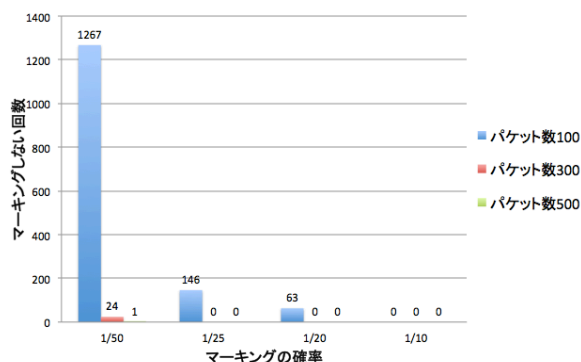


図4 各確率で追跡失敗した回数

各確率でマークされたパケット数のデータを収集し、ルーターにおける負担の大きさを分析するために、各確率が1/10、1/20、1/25、1/50の場合で一回のシミュレーションをした。図5に通信パケット数が100から10000まで増やし、各確率でパケットをマークしたシミュレーションの結果を示した。シミュレーションの結果から見ると、通信パケット数の増加と共に、ルーターの負担が大きくなる。更に、マーキング確率は大きくほど大きければ、ルーターにおける負担が著しくになる。

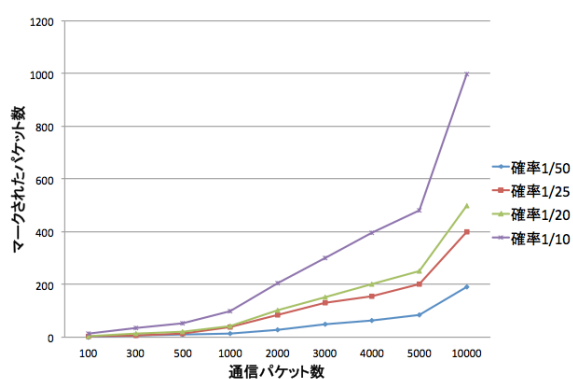


図5 各確率でマークされたパケット数

一方、シミュレーションにより、パケットのマーク数は二つ種類がある。図6にシミュ

レーションで一つ通信パケットのマーク数を示した。予想と同じで、マークされないならば、通信パケットのマーク数がいつも0である。マークされたならば、通信パケットのマーク数がいつも2である。PPMとPPITなど既存の手法と比べると、一つパケットにマークは最大二つしかないの、オーバーロード防止する対策は必要がない。

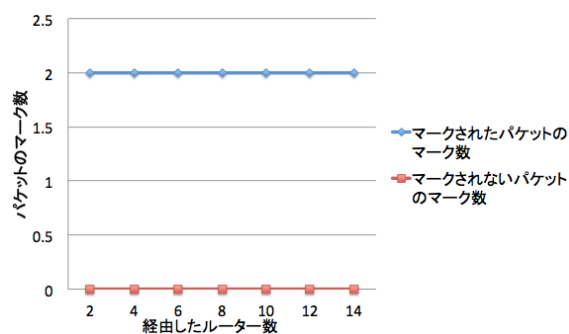


図6 一つ通信パケットのマーク数

以上のシミュレーションにより、トレースバックの成功率が通信パケット数とマーキング確率との二つパラメーターに決められる。通信パケット数が少ないなら、マーキング確率は上がる必要がある、逆に通信パケット数が一定程度増加したら、ルーターにおける負担を減少するために、マーキング確率は下がるべきである。一方、一つ通信パケットのマーク数はルーターにおける負担を増加しない。

5. まとめ

既存のトレースバック技術の、特定の攻撃しか対応できないおよび通信経路再構成の計算量が大きいためにトレースバックに時間を要するという問題を解決するために、新

しい手法を提案した。模擬実験で提案手法の有効性を確認した。

本手法ではトレースバックの時間が短い。更に、ルート再構成の計算量が少ない。ルーターの役割を分担する為、ルーターにおける負担を減少し、リスクも少なくなった。そして、マークが二つだけがあるので、オーバーロード防止する対策は必要がない。最後、結果としては、IP アドレス偽装攻撃の場合は、追跡の時間が多少影響されるが、基本的には、IP アドレス偽装攻撃にトレースバック能力が強い。

6. 今後の課題

マーキングする際、マークの数だけではなく、マークの大きさも考慮すべきである。よって、マークの内容と領域を選ぶことは重要である。既存の PPM がパケットのヘッダの識別子領域を利用する。更に、ルーターID を作って、IP アドレスの代わりに、ルーターID でパケットをマークするルーターID 領域[12]という研究がある。今後の課題として、より良いマーク内容と領域を決める。

もう一つ課題は IP アドレス偽装攻撃の場合では、本手法のトレースバック効率が下がると考えられる。そのために、本手法では、IP アドレス偽装攻撃の対策を追加することが必要である。

謝辞

この研究の一部は、科学研究費（基盤研究(C) No. 25330131)の支援を受けている。ここに記して謝意を表す。

参考文献

- [1] H. Burchand and B. Cheswick, “Tracing anonymous packets to their approximate source”, in Proceedings of the 14th USENIX Conference on System Administration, 2000.
- [2] R. Jain and A. Meshram, “A Survey on Packet Marking and Logging”, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (3), 2013.
- [3] P. Ferguson and D. Senie, “Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing”, RFC 2267, Jan. 1998.
- [4] S. Yu, W. L. Zhou, and W. J. Jia, “Traceback of DDoS attacks using entropy variations”, IEEE Transactions on Parallel and Distributed Systems, Vol. 22, 2011.
- [5] S. M. Bellovin, “ICMP traceback messages”, Network Working Group Internet Draft, March 2000.
- [6] C. Gong and K. Sarac, “A more practical approach for single-packet IP traceback using packet logging and marking”, IEEE Transactions on Parallel and Distributed Systems, Vol. 19, 2008.
- [7] Y. Dong, Y. Wang, S. Su, and F. Yang, “A Precise and Practical IP Traceback Technique Based on Packet Marking and Logging”, Journal of Information Science and Engineering March 2012.
- [8] S. Savage, D. Wetherall, A. Karlin and

- T. Anderson, "Network Support for IP Traceback", ACM/IEEE Trans. Networking, vol. 9, no. 3, pp. 226-237, 2001.
- [9] A. Belenky and N. Ansari, "IP Traceback With Deterministic Packet Marking", IEEE Communication Letters, Vol.7, No.4, Apr.2003.
- [10] F. Xue and S. J. Ben Yoo, "Self-similar traffic shaping at the edge router in optical packet-switched networks", Communications, 2002. ICC 2002. IEEE International Conference on. Vol. 4. IEEE, 2002.
- [11] X. Yang, W. Zhou and M. Guo, "Flexible Deterministic Packet Marking: An IP Traceback System to Find the Real Source of Attacks", IEEE Trans. on Parallel and Distributed Systems. Vol. 20, No. 4, Apr. 2009.
- [12] M. Muthuprasanna, G. Manimaran, M. Manzor and V. Kumar, "Coloring the internet: IP Traceback", in Proceedings of the 12th International Conference on Parallel and Distributed Systems, 2006.