2008－CSEC－42（16）
2008 / 7 / 24

パケット生存時間を用いた確率的パケットマーキングによるIPトレースバック手法の提案

木内 忠司† 堀 良彰†† 櫻井 幸一††

†九州大学大学院システム情報科学府情報工学専攻
〒819-0395 福岡市西区元岡744
kiuchi@itslab.csce.kyushu-u.ac.jp

††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
{hori,sakurai}@csce.kyushu-u.ac.jp

あらまし 送信元IPアドレスを偽装されていても送信元を明らかにするため研究されているIPトレースバックの手法の一つに確率的パケットマーキング法というものがある．この手法はパケットが各ルータを通過する際に一定の確率でそのパケットが通過した経路の情報を書き込み攻撃パケットの経路を復元し攻撃者の場所を特定するものであるが書き込み時上書きが起きる可能性があるためトレースバックの復元に必要なパケット数が増えてしまう．そこで、本論文ではパケット生存時間（TTL）をマークする際の変数とした式で確率でマークを行い、各ルータでのマーク確率を変動させ問題の解決を図る．

Variable Probabilistic Packet Marking with TTL for IP Traceback

Tadashi Kiuchi† Yoshiaki Hori†† Kouichi Sakurai††

† † The Department of Computer Science and Communication Engineering, Kyushu University, 744 Motooka, Nishi-ku, Fukuoka 819-0395, Japan, kiuchi@itslab.csce.kyushu-u.ac.jp

‡Faculty of Information Science and Electrical Engineering, Kyushu University 744 Motooka, Nishi-ku, Fukuoka, 819-0395 Japan {hori,sakurai}@csce.kyushu-u.ac.jp

Abstract There are various kinds of menaces that exist within the network. There is a menace called the DoS attacks in the one of them. DoS attack sends a large amount of packets to a target server. The server received many packets uses all resources and can't continue to serve.There is a technique called the probabilistic packet marking method in one of the technique of the IP-traceback in technology to find the origin of transmission of a packet. When a packet passes each router, this technique writes in the information of the course that a packet passed for an unused field of the packet with constant probability. The possibility that the superscription occurs is suppressed. Therefore we suggest the probabilistic packet marking technique which used TTL for in this article. We aimed at holding down the possibility that overwrite by the marking happened in the router of the down stream by this method.

1. はじめに

近年、インターネットの普及によってネットワークは広がり企業から家庭まであらゆる場所からインターネットへと接続することが可能なった．だがネットワークを介したさまざま脅威も存在する．その一つにDoS（Denial of Service：サービス不能）攻撃という脅威がある．DoS攻撃とは図1に示したように大量のパケットを標的となるサーバに対して送信することで通信回線やサーバのリソースを過度に消費させることでそのサービスの提供を妨害する攻撃手法である．従来の単一箇所から発信されるDoS攻撃に加え複数地点から攻撃パケットが送信されるDDoS（Distributed Denial of Service：分散型サービス不能）攻撃もまた大きな問題となっている[1][2]．

これらのDoSやDDoS攻撃に対処するためには攻撃パケットの発信源をつきとめる必要があるが、DoS攻撃に用いられる攻撃パケットは通常、送信元のIPアドレスが偽装されているため発信源をつきとめ攻撃者を特定することが困難なものとなっている．そこで発信元のIPアドレスが偽装されていたとしてもそのパケットの発信元を特定するためIPトレースバック技術が研究されている[3]．IPトレースバック技術としてパケット内の未使用領域に逆探知の手がかりを各ルータにおいて書き込む確率的パケットマーキング、各ルータにストレージを用意しパケットの通過履歴をとるロギング法[4]、各ルータで低確率で逆探知の手がかりを書き込んだパケットを送信するICMPトレースバック法、ルータのデバッグ機能を用いたもの[5]などの方式が研究されている[6]．

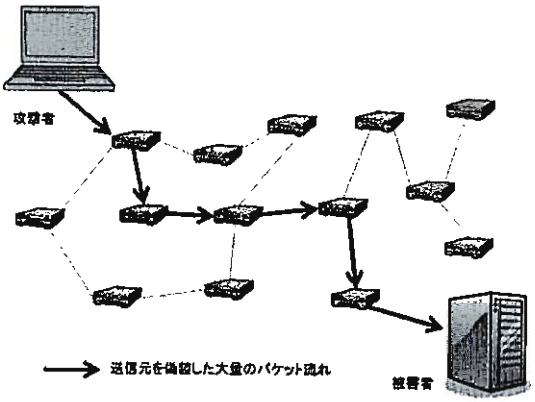

図 1 DoS 攻撃について

本研究では確率的パケットマーキングの問題点に注目した．既存の確率的パケットマーキングを用いたトレースバックは各ルータにおいて等しい確率でマーキングを行う．各ルータにおいて以前マークされたパケットに対してマークが行われ上書きされると当然マークされていた情報は失われてしまう．すると攻撃者近傍のルータの情報は被害者近傍のルータに比べて上書きされる機会が多くその情報は攻撃者に近ければ近いほど失われやすくなる．そこでTTL に依存する確率でのパケットマーキングを行うことで攻撃者に近いルータでは高く遠いルータでは低い確率でマークし、単一経路において一般的な TTL を初期値に持つパケットのトレースバックにおいて上書きによる必要パケット数の増加を抑えることを目指す方式を提案する．

本論文の構成は以下のようになっている．2 節では既存の IP トレースバックの手法のひとつである確率的パケットマーキングについて概説、3 節では提案方式の説明と既存手法の比較、4 節では今後の課題など、最後に 6 節で結びを述べる．

2. 確率的パケットマーキング方式

経路復元のための情報を ICMP トレースバック法のように別のパケットにおさめて送るのではなく、その情報をルータを通過する IPv4 パケットのヘッダ内の未使用ビットを使って被害者へと伝えようとする方式で、ネットワークへの余計な負担をかけないですむ利点がある．この手法では IP パケットのフラグメントの際に用いられるヘッダ情報である図 2 に示した IP identiffication フィールドを流用して、ルータにおいてパケットが通過した際に一定の確率でそこにマークを行う．この設計はフラグメント化したパケットはインターネットを流れるトラフィックに対しわずかな量であるため、IP identiffication フィールドの流用に問題はないはずであるという推測に基づき行われている．一般にルータを識別するための IPv4 のアドレスは 32 ビットであるのに対し IP identiffication フィールドは 16 ビットであるため符号化アルゴリズムにおいて何らかの工夫が必要となる．また受け取ったマークからもパケットの発信源の特定のため、複合化アルゴリズムにおいて何らかの知識を必要としたり、膨大な計算を必要としたりする場合がある．

- **Savage らの方式 [7]**

Savage らの発表した論文はマーキング方式に関する最初の論文で、隣接するルータの IP アドレスの組を (R_s, R_e) として各リンクを表現し、これを細分化して IP identiffication フィールドに埋め込み逆探知を実現しようとする方式である．

アドレスの排他的論理和 $(R_s \oplus R_e)$ によって (R_s, R_e) を簡潔に表現し、これを edge-id と呼ぶ．複数の edge-id からルータの IP アドレスを求めるにはそれぞれの edge-id が観測点からホップ数が既知であればよい．そこでホップ数 0 のルータの IP アドレス R_0 を元に隣接ルータのアドレス $\hat{R}$ は $\hat{R} = R_0 \oplus (R \oplus R_0)$ から求められる．よって、観測点からのホップ数を記録するため、マーク内の 5 ビットを割り当てさらに edge-id を 8 個の断片に分割し復元のため 3 ビットをオフセットとして割り当てる．

同一のホップ数に複数の edge-id が存在すると、復元の過程で異なる edge-id から生成された edge-id の断片と組み合わせてしまい IP アドレスを正しく復元できない危険性がある．そこで符号化の際に IP アドレスとそのアドレスのハッシュ値をビットインターリーブしこれを 8 個の断片にして分割し送信する．復元したアドレスが正しいかどうかはビット・インターリップから戻した値から検証できる．

3. TTL を変数として用いた確率的パケットマーキング手法の提案

確率的パケットマーキングによる手法では犠牲者から遠いルータの情報つまり攻撃者近傍のルータの情報であるほどパケットマーキングによる情報の上書きをされる可能性が高く、結果として犠牲者のもとにたどり着く可能性が犠牲者から遠いほどマークされた情報が低くなってしまう [8]．この問題を解決するため TTL を確率的パケットマーキングを行う際に参考にすることで、攻撃者に近いルータでは高い確率でパケットマーキングを行い攻撃者からホップ数が増加するにつれてマーキングする確率が低下する確率的パケットマーキング手法を提案する．TTL とは IP パケットのヘッダ情報の一つで IP パケットの寿命を表す生存時間を表す情報．パケットが各ルータを通過するたびに 1 ずつ値が減らされていき、値が 0 となったパケットは破棄される、これによりパケットが無限ループを起こし、延々とネットワークをさまよい続けることを防ぐ役割がある．

3.1 設　　計

本論文では Savage らの提案する確率的パケットマーキング手法においてマーキングを行う確率 p を一定にするのではなく各ルータで異なる確率でマークを行うことを提

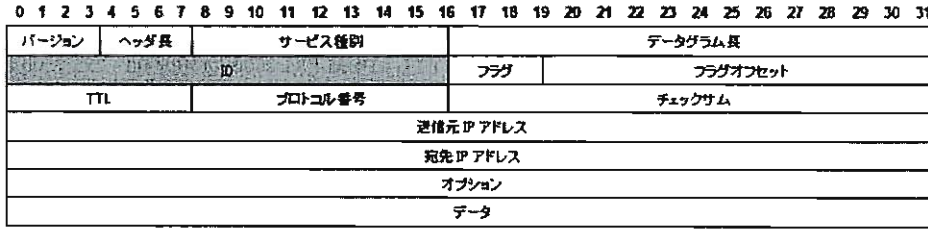

図 2　IPv4 パケットヘッダ情報の一つ ID フィールド

案する．

Savage らの提案した手法においては p=$\frac{1}{25}$ で検証された．すべてのルータにおいて同じ確率でパケットマーキングを行うと必然的に攻撃者に近いルータでマークされた情報であるほど後々パケットマーキングされる機会が多いことから犠牲者まで届きにくくなる．p の値は高すぎると上書きされる確率が増えてしまい、低すぎるとマークする確率自体が低くなりトレースバックに必要になるパケット数が増えてしまうため、Savage らの手法では p=$\frac{1}{25}$ でマークを行っている．そこで 1 ルータを通過するごとに 1 ずつ減っていく TTL を利用して攻撃者に近いほど高い確率でパケットマーキングが行われるように p を設定する．上書きが生じてしまうと、ホップ数が増えるほど指数関数的に攻撃者に近いルータから情報が届く確率が減りトレースバックのための必要パケット数が増えてしまうが、上書きによる影響を減らし各ルータから情報が届く確率をどのルータでも等しい値に近づけることでホップ数が増えても少ないパケット数でのトレースバックを行うことができる．攻撃者からのホップ数を hop とすると各ルータから被害者に対しパケットが等確率で届くためには、ホップ数が既知であれば

$p = \frac{1}{HOP}$

に設定する確率でマークを行うと実現できる．ところがこの式でマークを行うためにはマークする際にホップ数を知る必要があるがパケット受け取ったルータがそのパケットのホップ数を知る手段がないため、一般にはこの式の適用はできない．そこで各ルータで同じ確率でマークを行う既存方式と比べ、ホップ数が増えるほどマークする確率が減る点で理想の式に近い式として、線形に単調減少する以下の式を提案する．

$p = \frac{TTL+a}{L}$(TTL:TTL の値、a、L:定数)

$\frac{a}{L}$ はマークする確率の下限となる．$\frac{1}{L}$ はこの式の傾きとなり、L の値を大きくとると TTL が 1 減少した場合の TTL に依存した確率の変化があまり起きず、L を小さくとると変化が大きくなる．

3.2　パケットに記された TTL とその初期値の調査

IP の仕様により理論的には TTL の値は 0 から 255 の範囲での値をとるが、実際のネットワークにおいてパケットのヘッダに記されている TTL の値の分布について調査を行った．

パケットが送信されるとき、プログラマが陽に指定しない限りではその初期値は基本的に OS ごとに設定された値が使用されると考えられる．筆者らのサンプル調査では代表的な OS ごとの TTL の初期値は以下のようであった．

- TTL 32 windowsNT3.5、windows 95
- TTL 64 UNIX、freeBSD、windows 2000、2003
- TTL 128 windowsNT4.0、windows 98
- TTL 255 solaris

以上のことを考慮した上で実際にネットワーク上を流れるパケットの TTL の値の調査を行った．WIDE PROJECT が公開している MAWI(注1)の WIDE バックボーンの国際リンクから集めたパケット情報のアーカイブから 2007 年 1 月 9 日から同月 11 日までのパケットのヘッダ情報のデータから調べた 75520 個のパケットの TTL の値の分布を図 3 に示す TTL の値の分布からパケットの TTL は 64、

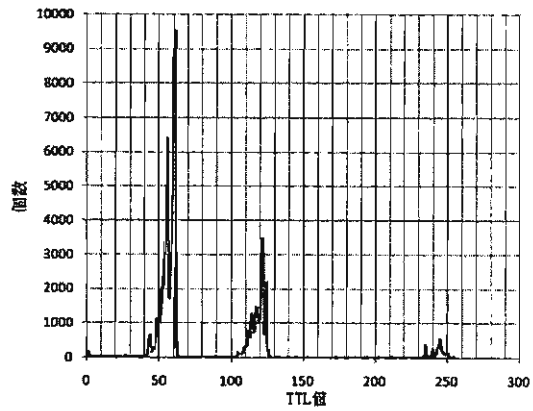

図 3　ネットワーク上のパケットの TTL 分布、横軸は TTL 値、縦軸はその数を示す

128、255 から 10 から 20、多くても 30 減った値の付近にほとんどのパケットが分布しているのがわかる．よって、提案方式と既存方式に対し TTL の初期値を 64、128、255 とした場合についてそれぞれの方式について攻撃経路のホップ数を 10 から 30 とし、構築に必要なパケット数を比べその性能の比較を行った．

(注1)：http://mawi.wide.ad.jp/mawi/

3.3 評　　価

図4のような単一の攻撃経路において、攻撃者と犠牲者のルータの数をNとし、N=10、20、30個の場合それぞれに対し、パケットの初期値に64、128、255を用いた時それぞれの場合において各ルータでのパケットマーキングが行われる確率を求め、そこからトレースバックに必要をなるパケット数の期待値を求め、Savageらの方式と本論文が提案する方式について比べてみる．なお期待値の計算に際し簡単のため各ルータから1以上のパケットの情報がもたらされれば経路構築ができるとした．Savageらの確率

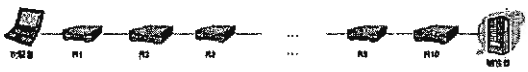

図4　攻撃経路が単一で攻撃者から被害者への間にルータが10個ある場合について

的パケットマーキングでは$p=0.04$,$p=0.05$,$p=0.06$としてトレースバックに必要となるパケット数の期待値を求めた．本論文での提案方式ではマーク確率の下限である$\frac{a}{L}$を0.03とし、$a=75$、$L=2500$、$a=150$、$L=5000$、$a=225$、$L=7500$、$a=300$、$L=10000$とおいてそれぞれの場合においてトレースバックに必要となるパケット数の期待値を求め最適なaとLの組み合わせを求め既存手法との比較を行った．まずSavageらの確率的パケットマーキングで経路構築に必要となるパケット数を表1に示す．なおSavageらの方式ではTTLの値はマークに無関係なので省いた．

表1　マーキング確率が一定である場合において経路構築に必要となるパケット数

N	p=0.04	p=0.05	p=0.06
10	302	254	223
20	757	680	638
30	1441	1390	1409

Savageらの方式で確率0.04、0.05、0.06でマークした場合の中継ルータ数ごとの必要パケット数の期待値

N=10の場合、上書きが起きる機会が少ないためマークする確率が高ければ必要パケット数は少なくなるが、N=30の場合では$p=0.06$でのマークより$p=0.05$のマークのほうが必要パケットが少ない．これはパケット情報の上書きにより攻撃者近傍の情報が届きにくくなったため必要なパケット数が増加したためである．

次に本論文の提案手法の確率的パケットマーキングで経路構築に必要となるパケット数をN=10、20、30の場合ごとに表2、3、4、図5、6、7に示す．図5，6，7において縦軸はトレースバックに必要なパケット数の期待値、横軸はパケット送信時のTTLの初期値をあらわしている．

$a=75$、$L=2500$の値に設定した場合マーキング確率pは、TTLの初期値に64が使われた際に$0.03<p<0.0552$の値をとる．このとき、パケットが30ホップ通過して届いた場合、各ルータでマークが行われる確率の平均値は

表2　提案方式による検証結果、N=10の場合

TTL	PPM	75;2500	150;5000	225;7500	300;10000
64	302	241	291	315	330
128	302	238	289	313	328
255	302	237	288	312	327

N=10の時、パケット送信時のTTLの初期値64、128、255の場合において、PPMは既存手法でp=0.04でのマークを行った場合について、数値1; 数値2はa=数値1、L=数値2とした場合についてそれぞれトレースバックに必要となるパケット数の期待値

表3　提案方式による検証結果、N=20の場合

TTL	PPM	75;2500	150;5000	225;7500	300;10000
64	757	655	740	783	808
128	757	653	735	778	803
255	757	653	733	776	801

N=20としに表2と同様の検証を行ったもの

表4　提案方式による検証結果、N=30の場合

TTL	PPM	75;2500	150;5000	225;7500	300;10000
64	1441	1315	1404	1455	1486
128	1441	1349	1409	1455	1485
255	1441	1370	1413	1456	1485

N=30の時に表2と同様の検証を行ったもの

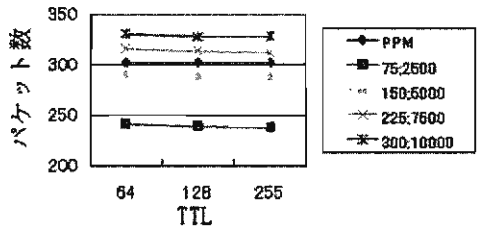

図5　N=10の時の提案手法の期待値

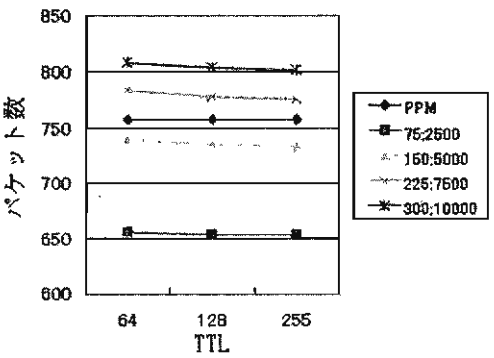

図6　N=20の時の提案手法の期待値

0.0492となる．この場合と既存手法で各ルータでのマーク確率の平均が$p=0.05$である場合とを比べると本手法の場合は1370個、既存手法の場合1390個となる．マークする確率の平均値は同程度であるが本手法の方が必要パ

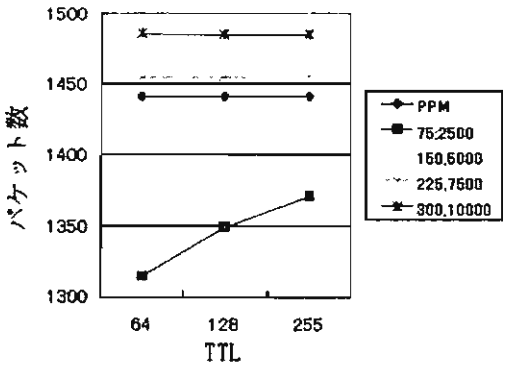

図 7 N=30 の時の提案手法の期待値

ケット数が少なくなり上書きによる影響を減らすことができた.

a と L の値を $a = 225$、$L = 7500$ や $a = 300$、$L = 10000$ とした場合は各ルータから情報が届く確率を TTL の初期値に 64 について計算してみると、$a = 225$、$L = 7500$ の場合は $0.03 < p < 0.0385$、$a = 300$、$L = 10000$ の場合は $0.03 < p < 0.0365$ それぞれの確率の変化が少ないことが分かった. これは L の値が大きかったため式の傾きが小さくなったためであるが、傾きが小さい場合においては攻撃者近傍でのマーク確率は低いままとなってしまい上書きによる影響を減らすことができない結果となった.

4. 課　　題

前章にて、本提案方式について各ルータの情報が被害者に到達する確率から性能評価を行った結果をもとに今後の課題などについての考察を行う.

- **評価内容について**

前章ではマークする確率がとりうる範囲の下限の値を 0.03 としたが下限の値を変えた別のケースでよりよいマークが行えないか、数式を二次式することや指数関数を用いることでよりよい形にならないか検討する.

$a = 75$、$L = 2500$ の N=10 の場合と N=30 の場合 TTL の初期値によってパケットマーキングに必要なパケット数の増減が大きいため、TTL の値によって場合分けし別の L や a の値を適用するなどできないか検討する.

- **評価方法について**

各ルータの情報が被害者に到達する確率から性能評価であったが、今後はトレースバックに必要なパケット数の期待値による評価や単一経路でない場合や攻撃者が複数いた場合についての挙動の評価など別の方法での評価も検討していくつもりである.

- **ルータの負担について**

従来方式よりもルータにおいて確率計算を行う処理が増えるため多少ルータのオーバーヘッドが増加することが考えられる.

- **TTL の初期値について**

本論文では既存手法との比較の際に初期値として OS ごとの標準の値を用いて性能の比較を行ったが、TTL の値が変えられた場合既存手法には影響はないが提案手法は影響が出ることが考えられるため OS 標準値以外での TTL の値を初期値に用いた場合の既存手法の比較について課題としてあげられる.

5. おわりに

近年、ネットワークの普及とともに増加しているインターネットにおける脅威の一つである DoS 攻撃が問題となってきている. DoS 攻撃は大量の不正なパケットを攻撃対象に送信することで対象のサービスの提供を妨害する. DoS 攻撃に対処するにはまずその攻撃の発信元を特定しなければならないが、DoS 攻撃に用いられる攻撃パケットは通常、送信元の IP アドレスが偽装されているため、その特定は困難である. そこで IP パケットの送信元アドレスが偽装されていたとしてもそのパケットの発信元まで辿って逆探知するための技術として IP トレースバック技術がある. 本論文ではまずネットワークの脅威である DoS 攻撃について解説し、それに対抗するための技術である IP トレースバック技術の既存の手法についての解説と比較を行った.

本論文では IP トレースバックの手法の一つである確率的パケットマーキングの手法を改良するための手法を提案した. 確率的パケットマーキングでは各ルータでマークを行う際にそのルータ以前でマークされていた情報がある場合は上書きされてしまう. 各ルータでは同じ確率でパケットマーキングが行われる場合、被害者近傍のルータよりも攻撃者近傍のルータの情報のほうが上書きされる機会多くその情報が失われやすい. そこでパケットのヘッダの情報の一つである TTL に依存した確率でパケットマーキングを行い攻撃者近傍のルータの情報が失われる確率を減らすことを目的とした. TTL はルータを通過するごとに 1 ずつ減っていくためこれを利用して攻撃者近くでのマークされる確率を上げ、被害者近傍でのマークの確率を減らすため TTL の値に依存しホップ数が増えるごとに線形的にマーク確率が減少していく方式を提案した. ホップ数と TTL の初期値を一定とした条件のもとで提案方式と既存方式の性能の比較を行い上書きによる必要パケット数の増加の影響を減らすことができた.

文　　献

[1] David R. Mirza Ahmad, "ハッキング対策マニュアル" ソフトバンククリエイティブ (2003/12)

[2] オンライン・コンピューター用語辞書 http://www2.nsknet.or.jp/ azuma/menu.htm

[3] 門林雄基, 大江将史, "I O トレースバック技術", 情報処理, Volume 42, Number 12, December 2001

[4] A. Snoeren, C. Partridge, L. Sanchez, C. Jones, F. Tchakountio, B. Schwartz, S. Kent, and W. Strayer, "Single-packet IP traceback," IEEE/ACM Trans. on Networking,

vol. 10, no. 6, pp. 721-734, 2002.

[5] S. Bellovin, et al. " ICMP Traceback Messages " , Internet-Draft. http://www.ietf.org/internet-drafts/draft-ietf-itrace-04.txt, (accessed 2003- 04-25) .

[6] Stone,R "An IP Overlay Network for Tracking DoS Floods", In Proceedings of USENIX Security Symposium'00.

[7] S Savage, D Wetherall, A Karlin, T Anderson "Network suport for IP traceback,"- IEEE/ACM Transactions on Networking, vol.9, no.3, pp.226-237, 2001.

[8] Basheer Al-Duwairi and Manimaran Govindarasu, "Novel Hybrid Schemes Employing Packet Marking and Logging for IP Traceback," IEEE Transactions on Parallel and Distributed Systems, Volume 17, Number 5, pp. 403-418, May 2006.