情報処理学会論文誌 Vol.53 No.2 795–804 (Feb. 2012)

DDoS攻撃に対して排他的論理和と確率的Marking方式を用いることでルータへの負荷分散を実現するIP Traceback

井上 慎一郎[1,a)] 石井 方邦[1] 笹瀬 巌[1]

受付日 2011年3月30日, 採録日 2011年11月7日

概要：DoS 攻撃や DDoS 攻撃に対し，その発信元を特定する IP トレースバックは重要な技術である．これまで，マーキング方式やロギング方式が個別に提案されてきたが，マーキング方式ではトレースバックのために大量の攻撃パケットの回収が必要であるという課題があり，またロギング方式ではすべての通過パケットのハッシュ値を保持するためルータへの負荷が増大するという課題がある．近年，2 つの方式の課題を補う HIT（Hybrid IP Traceback）方式が提案された．HIT 方式ではマーキングとロギングを交互に行うことでロギング回数を従来と比較し半分に低減させているが，すべての通過パケットに対して処理を行わなければならないという課題や，DDoS 攻撃において被害ホスト近傍のルータへ大きな負荷がかかるといった課題がある．そこで本論文では，DDoS 攻撃に対するトレースバックにおいて，95%以上の高いトレースバック成功率を達成しつつルータへの負荷を低減・分散するために，排他的論理和と確率的パケットマーキングを用いたトレースバック方式を提案する．排他的論理和を用いることで 2 つのルータの ID を 1 つにまとめることができ，ロギングの回数を低減させることが可能となる．また，DDoS 攻撃において攻撃パケットは大量に送信されてくるという特徴と被害ホスト近傍に攻撃パケットが集中するということを考慮して，すべての通過パケットではなく確率的に選択したパケットに対して 1 度のみ処理を行う．これにより，ルータへの負荷を低減させることが可能となる．計算機シミュレーションにより各方式におけるトレースバック成功率とパケット処理率，またパケット処理回数の評価を行い，高いトレースバック成功率を達成しつつルータへの負荷を低減・分散可能な提案方式の有効性を示す．

キーワード：トレースバック，負荷分散，DDoS

A Load-distributed IP Traceback by Using Exclusive-OR and Probabilistic Packet Marking for DDoS Attacks

Shinichiro Inoue[1,a)] Masakuni Ishii[1] Iwao Sasase[1]

Received: March 30, 2011, Accepted: November 7, 2011

Abstract: Tracing IP packets back to their origins is an important scheme to defend against denial-of-service (DoS) and distributed-Dos (DDoS) attacks. Mainly, two kinds of IP Traceback schemes have been proposed. One is a packet marking scheme which each routers marks their ID into packets. The other is a packet logging scheme which each router logs the digest of the forwarded packets. Recently, hybrid IP Traceback scheme, which makes up for shortcomings of above two schemes, has been proposed. By this hybrid scheme, the overhead on routers can be reduces compared to the conventional scheme. However, due to marking and logging for DDoS attacks, the hybrid scheme still causes much overhead and that router near victim server have a lots of burden. In this paper, we propose IP Traceback scheme which uses Exclusive-OR and probabilistic packet marking to reduce burden on routers with achieving high traceback success rate compared with conventional schemes. By computer simulation, we evaluate a traceback success rate, a ratio that how many each router does his job to forwarding packet and packet numbers to which each router does his job.

Keywords: Traceback, Load-distribution, DDoS

1. はじめに

インターネットは重要な社会インフラの1つとして定着しており，特に企業ではホームページ等が重要な情報発信手段として用いられている．一方，インターネットにおける様々な脅威も存在している．その脅威の1つとしてDoS（Denial of Service：サービス拒否）攻撃，DDoS（Distributed DoS：分散型サービス拒否）攻撃があげられる [1]．これらは，大量の攻撃パケットを標的サーバに送信することで通信回線やサーバリソースを浪費させ，サービス提供を妨害する攻撃である．しかしながら，攻撃パケットの送信元IPアドレスは偽装されている場合が多いため，発信元である攻撃ホストを特定することは困難となっている．

そこで，発信元IPアドレスが偽装されている場合においても攻撃パケットの発信元を特定することが可能な技術としてIPトレースバックが研究されている．代表的なIPトレースバックとして，各ルータが中継したパケットのハッシュ値を保持するロギング方式 [2] や中継時にルータがパケット内に自身のIDの記入を行うマーキング方式 [3]，また確率的にIDの記入を行う方式 [4], [5] が提案されている．ロギング方式は，トレースバックを行うためにたった1つの攻撃パケットで十分であるという特徴を有し，また2009年11月にロギング方式を用いて実証実験が行われ，ルータのメモリや資源を考慮しないのであれば実現可能な方式であることが証明された [6]．しかしながら，ロギング方式において各ルータは攻撃パケットに限らずすべての通過パケットのハッシュ値を算出し保持しなければならず，ルータへの負荷が大きいという課題が存在する．一方，マーキング方式は各ルータは通過パケットにIDを記入するのみであり，通過パケットの情報を保持することが不必要で負荷が小さいという特徴を有する．しかしながら，トレースバックを行うために大量の攻撃パケットを収集する必要 [7], [8] があるという課題や，マーキング情報が他のルータにより上書きされ以前のルータの情報が失われる [9] といった課題がある．

近年，それぞれの方式の課題を補うようにロギング方式とマーキング方式を組み合わせたHIT（Hybrid IP Traceback）方式 [10] が提案された．HIT方式は，マーキングとロギングを交互に行う方式である．それにより，各ルータは通過パケット2つのうち1つのパケットに対してのみロギング処理を行うため，ロギングによるルータへの負荷を方式 [2] と比較し約半分に低減させることが可能となっている．また，ロギング処理を行うため，以前のルータが記入した情報を上書きにより失うことなく保持することが可能であり，さらに通過するすべてのパケットに対してマーキングまたはロギングの処理を行うため，1つの攻撃パケットでトレースバックを行うことが可能となっている．

しかしながら，HIT方式には解決すべき3つの課題がある．1つ目の課題は，ロギング処理回数を低減させることである．HIT方式によってロギング処理回数は半減されたものの，ロギングはルータへの負荷が大きいため，さらにロギング処理回数を低減可能な方式が必要となる．2つ目の課題は，すべての通過パケットに対して処理を行うことによるルータへの負荷である．攻撃パケットではないパケットも流れるネットワークの中でルータを通過するすべてのパケットに対してマーキングやロギングの処理を行うことはルータへの負荷が非常に大きいと考えられる．HIT方式では1つの攻撃パケットでのトレースバックを可能とするために攻撃パケットに限らず通過するすべてのパケットに対して処理を行っているのであるが，攻撃パケットは攻撃ホストから大量に届く．そこで，複数個の攻撃パケットを用いてトレースバックを行えるようにすることで，ルータは通過するすべてのパケットに対して処理を行う必要がなくなり，結果ルータへの負荷を大きく低減させることができるものと考える．3つ目の課題は，DDoS攻撃において，被害ホスト近傍のルータへの負荷が増大するという課題である．被害ホスト近傍のルータへはあらゆる位置に存在する攻撃ホストからの攻撃パケットが集まる．そこで，被害ホスト近傍のルータへの負荷を低減させ，処理を全ルータにわたって分散させるために，被害ホストに近いルータほど，処理回数を抑制する方式が必要となる．トレースバックを行うためには，各ルータに対して通常の転送機能に加え新たな機能を付加しなければならい．したがって，高いトレースバック成功率を達成しつつも，ルータへの負荷を考慮した方式が重要となる．

そこで本論文では，DDoS攻撃に対するトレースバックにおいて，高いトレースバック成功率を達成しつつもルータへの負荷を低減・分散させるために，排他的論理和と確率的パケットマーキングを用いたトレースバック方式を提案する．排他的論理和を用いることで2つのルータのIDを1つにまとめることが可能となるため，ロギングの回数を低減させることが可能となる．また，DDoS攻撃において攻撃パケットは大量に送信されてくるという特徴と被害ホスト近傍に攻撃パケットが集中するということを考慮して，すべての通過パケットではなく確率的に選択したパケットに対して1度のみ処理を行う．これにより，被害ホスト近傍のルータの処理を行う確率は小さくなり，結果ルータへの負荷を低減することが可能となる．計算機シミュレーションにより各方式におけるトレースバック成功率とパケット処理率，またパケット処理回数の評価を行い，従来方式と同じ高いトレースバック成功率を達成しつ

[1] 慶應義塾大学理工学部情報工学科
Department of Information and Computer Science, Yokohama, Kanagawa 223–8522, Japan
[a)] inoue@sasase.ics.keio.ac.jp

つルータへの負荷を低減・分散可能な提案方式の有効性を示す．

以降，2 章では従来方式である HIT 方式とその課題について述べ，3 章では提案方式である DDoS 攻撃に対するトレースバックにおいて，ルータへの負荷を低減・分散する IP トレースバックについて述べる．4 章では提案方式の評価を行い，5 章で本論文をまとめる．

2. 従来方式

本章では，マーキング方式とロギング方式のハイブリッド型である HIT 方式とその課題について述べる．HIT 方式はマーキングとロギングを交互に行うためマーキング情報が失われず，ロギング回数を方式 [2] と比較し約半分に低減することが可能である．また，1 つの攻撃パケットに対してすべてのルータがマーキングまたはロギングの処理を行うため，1 つの攻撃パケットでトレースバックを行うことが可能であるという特徴を持つ．以下，HIT 方式を用いるネットワークにおいて，パケットが攻撃ホストから被害ホストに至るまでの処理方法を 2.1 節で述べ，トレースバック処理方法を 2.2 節で述べる．そして，HIT 方式の課題を 2.3 節で述べる．

2.1 パケットが攻撃ホストから被害ホストに至るまでの処理

本節では，パケットが攻撃ホストから被害ホストに至るまでのプロセスについて述べる．このステップにおいて，各ルータは主に 2 つの役割を担う．1 つは，マーキングであり，もう 1 つはロギングである．マーキングとは，各ルータが自身の ID（15 bit）をパケット内にある identification フィールド（16 bit）中の 15 bit に記入し，さらに残りの 1 bit にマーキングを行った証拠としてフラグを立てパケットの転送を行う処理である．一方，ロギングとは受信したパケットのハッシュ値を算出しダイジェストテーブルに保持し，さらにロギングを行った証拠としてフラグを立てパケットを転送する処理である．**図 1** にパケットが攻撃ホストから被害ホストに至るまでの例を示す．

初めに，攻撃ホストからパケットを受信したルータ R_1 は自身の ID を記入するマーキングを行い，パケットをルータ R_2 に転送する．次に，ルータ R_2 はルータ R_1 から受信したパケットのハッシュ値を算出し，それを自身のダイジェストテーブルに格納する．ここで**図 2** にルータ R_2 におけるダイジェストテーブルを示す．ルータ R_2 は近隣のルータに対するダイジェストテーブルを各々準備している．たとえば，ルータ R_1 から受信したパケットのハッシュ値はルータ R_1 用のダイジェストテーブルに，またルータ R_7 から受信したパケットのハッシュ値はルータ R_7 用のダイジェストテーブルに格納するという具合である．テーブルに格納することで，以前のルータの情報を上書きすることなく保持することが可能となる．以降も同様に，マーキングとロギングを交互に行い，パケットは被害ホストに届く．

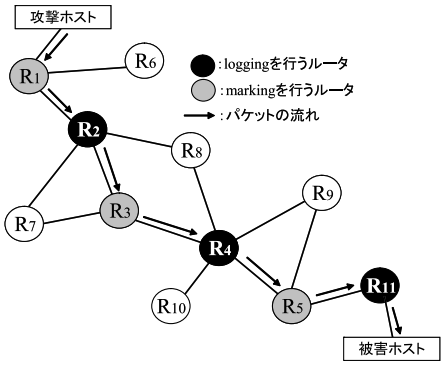

図 1 パケットが被害ホストに至るまでの処理
Fig. 1 Router's operation in HIT.

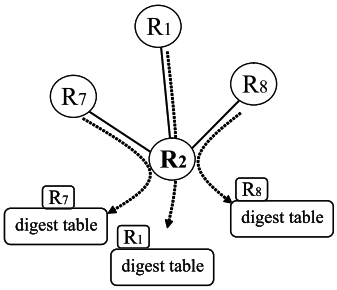

図 2 ルータ R_2 におけるダイジェストテーブル
Fig. 2 Digest table of router R_2.

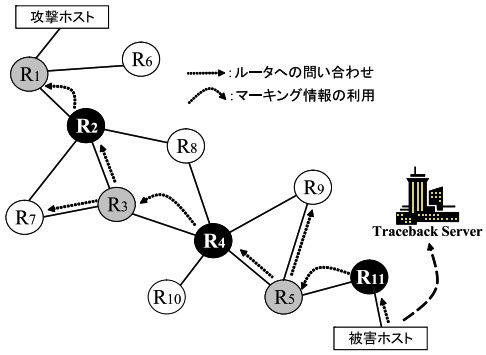

図 3 トレースバック処理
Fig. 3 Traceback process in HIT.

2.2 トレースバック処理

本節では，攻撃パケットの発信元を特定するトレースバック処理について述べる．トレースバックには主に 2 つのプロセスがある．1 つは，マーキング情報により通過ルータを特定するプロセスと，もう 1 つはロギングにより攻撃パケットのハッシュ値を保持するルータを発見することで通過ルータを見つけるプロセスである．**図 3** に HIT 方式におけるトレースバック処理を示す．ここで，図 3 におけるトレースバックサーバとはネットワークトポロジを把握する第 3 者機関であり，被害ホストから攻撃パケットを受け取り，実際にトレースバックを行う機関である．図 3 を

用いてトレースバック処理を述べる．

初めに，受信したパケットが攻撃パケットであると判断した被害ホストは，そのパケットをトレースバックサーバに送信し，トレースバック処理のリクエストを行う．

次に，トレースバックサーバは受信した攻撃パケット内のフラグより，被害ホストの直前のルータがマーキングを行ったか，またはロギングを行ったかを確認することが可能である．図 3 においては，直前のルータがロギングを行ったことが分かる．そこで，トレースバックサーバは被害ホストの直前ルータであるルータ R_{11} に対して攻撃パケットのハッシュ値を保持しているか，さらにその攻撃パケットはどのルータから受信したものであるかの問合せを行う．問合せを受けたルータ R_{11} は図 2 で示したルータ R_4 のダイジェストテーブルと同様の隣接ルータ用のダイジェストテーブルを保持しており，攻撃パケットのハッシュ値がどのルータ用のテーブルに格納されているかを探査する．ここでは，ルータ R_5 用のテーブルに入っていることから，攻撃パケットはルータ R_5 から受信したものであることが分かり，トレースバックサーバに対してルータ R_5 である情報を返信する．

ルータ R_5 が攻撃パケットの通過ルータであると確認したトレースバックサーバは，ルータ R_5 の全隣接ルータに対して攻撃パケットのハッシュ値を保持していないか問合せを行う．以降は，先に述べたプロセスと同様に，図 3 においては，ルータ R_4 が攻撃パケットのハッシュ値を保持していることと，さらにそのハッシュ値がルータ R_3 用のダイジェストテーブルに入っているという情報をトレースバックサーバに対して返信する．以上のプロセスを繰り返し，トレースバックサーバは最終的にルータ R_1 にまでたどり着き，トレースバック処理を終了する．

マーキング方式とロギング方式を組み合わせた HIT 方式は，トレースバックを行うために攻撃パケットが 1 つで十分であるという利点と，また，2 つに 1 つのルータがロギングを行うために，全ルータがロギングを行う方式 [2] と比較して問合せ回数を約半分に低減させることが可能であるという利点を有する方式である．

2.3 HIT 方式における課題

本節では，HIT 方式における 3 つの課題について述べる．

- **課題 1：ロギング処理によるルータへの負荷**
  1 つ目の課題は，ロギングを行うために生じるルータへの負荷である．ロギングは受信したパケットのハッシュ値を算出し，それを保持する必要があるためルータへの負荷も大きくなる．HIT 方式は方式 [2] と比較してロギング回数を半減させているが，トレースパスのホップ数や通過パケット数が多くなると，結果としてロギングを行うルータの数も増え，負荷が増加するという課題がある．そこで，さらにロギング処理回数を低減可能な方式が必要となる．
- **課題 2：すべての通過パケットに対して処理を行うことによるルータへの負荷**
  HIT 方式では，各ルータはすべての通過パケットに対して，マーキングまたはロギングの処理を行うように設定されている．そして，このルールによりたった 1 つの攻撃パケットでトレースバックを行うことが可能となっている．しかしながら，攻撃パケットでないパケットも流れるネットワークの中で，すべての通過パケットに対して処理を行うことはルータにとって非常に大きな負荷がかかると考えられる．また，攻撃ホストからは大量（10,000 個～）のパケットが送信されてくると思われる．そこで，1 つの攻撃パケットだけでなく複数の攻撃パケットを用いてトレースバックを行えるようにすることで，ルータへの負荷を低減させることができると考えられる．
- **課題 3：DDoS 攻撃における，被害ホスト近傍のルータへの負荷**
  DDoS 攻撃では，多数の攻撃ホストから 1 つの被害ホストに対して大量の攻撃パケットが送信されてくる．したがって，被害ホストに近いルータほど，通過する攻撃パケットの数が増加し，ルータへの負荷も増加すると考えれられる．そこで，被害ホストに近いルータほど処理回数を低減させる方式が必要となる．

3. 提案方式

本章では，DDoS 攻撃に対して高いトレースバック成功率を達成しつつルータへの負荷を低減・分散させるために，排他的論理和と確率的パケットマーキングを用いたトレースバック方式を提案する．提案方式における各ルータは従来方式と同様にマーキングとロギングを行ううえに，2 つのルータの ID を 1 つにまとめることによってロギングの回数を低減させるために排他的論理和も行う．2 つのルータの ID を 1 つにまとめる演算手法としては他にも 2 進数四則演算が考えられる．しかしながら，四則演算を用いることは，演算結果後に桁数の繰上げが発生する可能性があるということと，パケット内の ID を記入するためのスペースには限りがあり演算結果の桁数が繰り上がると正確な ID を記入できない可能性があるという理由から，不適切である．そこで，演算を行ったとしても桁数の増減が生じず，正確な ID を記入することが可能である演算方式として排他的論理和を用いる．

また，DDoS 攻撃において攻撃パケットは大量に送信されてくるという特徴と被害ホスト近傍に攻撃パケットが集中するということを考慮して，すべての通過パケットではなく確率的に選択したパケットに対して 1 度のみ処理を行う．これにより，被害ホストに近いルータほど処理を行う確率が小さくなり，結果ルータへの負荷を低減させること

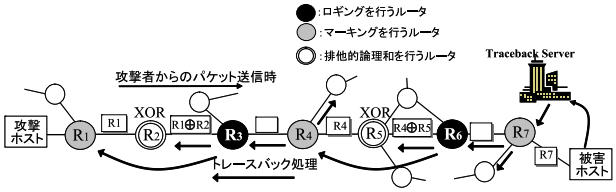

図 4 マーキング+排他的論理和（XOR）+ロギング
Fig. 4 Proposed Marking+XOR+Logging scheme.

ができる．初めに，2.3 節で述べた課題 1 を解決する排他的論理和を用いた方式を 3.1 節で述べ，課題 1 と課題 2 を解決する確率的にパケットに対して処理を行う方式を 3.2 節で述べる．最後に，すべての課題を解決する確率的かつ 1 度のみパケットに対して処理を行う方式を 3.3 節で述べる．

3.1 マーキング+排他的論理和（XOR）+ロギング

本節では，従来と比較しロギング回数をさらに低減させるために，排他的論理和を用いた方式について述べる．提案方式では，各ルータは従来方式と同様にマーキングとロギングを行ううえに，排他的論理和を行う．そこで，各ルータは以前のルータがどの処理を行ったかを知るために，3 つのパケット状態を判別しなければならず，フラグ用に 2 bit のスペースが必要となる．パケット内の identification は 16 bit であるため，残りの 14 bit をルータの ID スペースにしなければならない．従来方式では ID は 15 bit であるが，文献 [11] によると，各ルータが 2 ホップ先のルータを一意に識別するためには 12 bit で十分とされているため，14 bit でも十分であると考える．そこで，提案方式ではルータの ID 長は 14 bit とする．

初めに，パケットが攻撃ホストから被害ホストに至るまでのルータの処理を述べる．**図 4** に排他的論理和を用いたトレースバック方式を示す．図 4 において，初めにルータ R_1 は自身の ID（14 bit）を identification 内に記入するマーキングを行い転送する．そして，ルータ R_2 は自身の ID とルータ R_1 がすでに記入している ID との排他的論理輪（$R_1 \oplus R_2$）を identification 内に上書きし，転送する．次に，パケットを受信したルータ R_3 はパケットのハッシュ値を算出し，自身のダイジェストテーブルに格納する．ここで，提案方式において各ルータが保持するダイジェストテーブルは図 2 のように隣接するルータごとに準備されているものではなく，排他的論理和の値ごとに準備されている．図 4 におけるルータ R_3 には排他的論理輪（$R_1 \oplus R_2$）のためのダイジェストテーブルがある．以降，同様にしてパケット処理を行い，パケットは被害ホストに届く．

次に，実際にトレースバックを行う場合について述べる．初めに，被害ホストはトレースバックのリクエストを行うために，攻撃パケットをトレースバックサーバに送信する．図 4 において，トレースバックサーバはパケットのマーキング情報からルータ R_7 を通過ルータであると特定する．そして，トレースバックサーバはルータ R_7 に隣接するルータに対して攻撃パケットのハッシュ値を保持していないかの問合せを行う．図 4 では，ルータ R_6 は保持していることと，さらにそのハッシュ値が排他的論理輪（$R_4 \oplus R_5$）用のダイジェストテーブルに格納されていることから，攻撃パケットがルータ R_4 とルータ R_5 を通過して来たことが分かり，その情報をトレースバックサーバに返信する．各ルータの ID が 14 bit あるため，ルータ R_6 はルータ R_4 とルータ R_5 を一意に識別することが可能である．以降，同様の処理を繰り返し，ルータ R_1 にまでたどり着きトレースバック処理を終える．

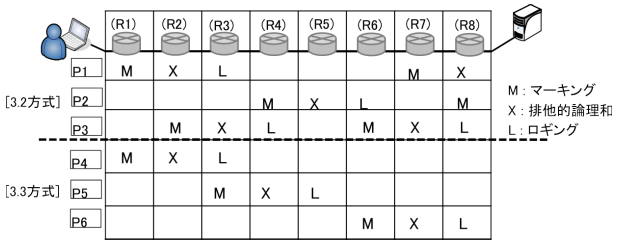

図 5 提案方式 3.2 と 3.3 におけるルータの処理
Fig. 5 Proposed scheme 3.2 and 3.3.

排他的論理和を用いることで，2 つのルータの ID を 1 つにまとめることができ，ロギング回数を低減させることが可能である．

3.2 確率的にマーキング+排他的論理和（XOR）+ロギングを繰り返す方式

本節では，提案方式 3.1 のマーキング（M）+排他的論理和（X）+ロギング（L）をベースにし，複数個の攻撃パケットを利用してトレースバックを行うようにすることで，ルータへの負荷を低減させる方式を提案する．1 つの攻撃パケットのみでのトレースバックは行えなくなるものの，ルータへの負荷を大きく低減可能な方式である．**図 5** の上段に確率的にマーキング（M）+排他的論理和（X）+ロギング（L）を行う方式を示す．各ルータはあらかじめ定められたサンプリング確率 P を保持しているものとする．ここで，サンプリング確率 P とは，各ルータが通過パケットに対して処理を行う確率である．サンプリング確率を用いて，各ルータはいまだ処理のされていない，または以前ロギング処理をされたパケットに対してマーキング処理を行う．以上のように，各パケットはルータによって一定の確率で処理されながら標的サーバへたどり着く．

次に，複数個の攻撃パケットを利用してトレースバックを行う場合について図 5 の上段を用いて述べる．初めに，トレースバックサーバは標的サーバが受信したパケット P1 内に記載されている値と，標的サーバの近隣ルータがルータ R_8 であることから，ルータ R_8 とルータ R_7 をパケット P1 の通過したルータとして特定する．次に，トレースバックサーバはルータ R_7 近傍のルータに対してパケット P1

のハッシュ値を保持していないか問合せを行う．しかしながら，パケット P1 はルータ R_6 において処理がなされていないため，この問合せは失敗する．そこで，トレースバックサーバはパケット P2 を用いて，ルータ R_6 やルータ R_7 の近傍のルータに対してパケット P2 のハッシュ値を保持していないか問合せを行う．すると，パケット P2 はルータ R_6 によってロギング処理がなされているため，問合せは成功し，さらにルータ R_6 は自身のダイジェストテーブルより，パケット P2 がルータ R_5 とルータ R_4 を通過したという情報をトレースバックサーバに対して返信する．これにより，トレースバックサーバは攻撃パケットに通過ルータとしてルータ R_6 とルータ R_5，ルータ R_4 を特定することができる．同様にして，トレースバックサーバはパケット P1 のハッシュ値を保持していないかルータ R_4 近傍のルータに対して問合せを行う．図 5 の上段の場合は，ルータ R_3 がハッシュ値を保持していることから，トレースバックサーバは問合せの返事を利用することで，ルータ R_3 とルータ R_2，ルータ R_1 をパケットの通過ルータとして特定し，トレースバックを終了する．

図 5 においては，パケット P1 のみ利用するとルータ R_6 とルータ R_5，ルータ R_4 が特定できず，またパケット P2 とパケット P3 のみを利用するとルータ R_1 が特定できず，トレースバックは失敗する．一方，パケット P1 とパケット P2 の 2 つのパケットを用いるとトレースバックを行うことが可能となり，この場合ルータ R_1 は従来と比較し処理回数を 1/3 に低減させることができることが分かる．DoS 攻撃や DDoS 攻撃では 1 つの攻撃ホストから 10,000 個以上の攻撃パケットが送信されてくると思われるため，1 個だけでなく複数個の攻撃パケットを用いてトレースバックが可能になるよう設定することで，各ルータへの負荷も低減させることができると考える．

3.3 確率的，かつ 1 度のみマーキング+排他的論理和（XOR）+ロギングを行う方式

本節では，コンピュータの発達とともに DoS 攻撃よりもさらに多発すると思われる DDoS 攻撃に対して，被害ホスト近傍のルータへの負荷を低減・分散させる方式を提案する．DDoS 攻撃においてはあらゆる端末から攻撃パケットが送信されてくるため，被害ホストに近いルータほど通過パケットが多く，提案方式 3.2 を用いると被害ホスト近傍のルータにおける処理回数が増加し負荷が大きくなると考えられる．そこで，通過パケットが増大する被害ホストに近いルータほど処理を行う確率を低くする必要がある．TTL を用いてパケットのホップ数を考慮する方式 [5] があるが，TTL の初期値は様々な値が考えられるため，被害ホストまでのホップ数をルータ自身が推測することは困難であると思われる．そこで，提案方式ではいずれかのルータにより 1 度処理をされたパケットに対してはそれ以上処理を行わないようにすることで，被害ホスト近傍のルータによる処理確率を小さくする．このことにより，各ルータは自身が被害ホストから遠いのか近いのかを推測することなく処理を行えるようになると考える．図 5 の下段に提案方式 3.3 を示す．図 5 に示すように，ルータは 1 度処理の行われたパケットに対しては処理を 2 度と行わない．また，トレースバックは 3.2 と同様に複数個の攻撃パケットを用いることで攻撃ホストの特定を可能とする．**表 1** に攻撃ホストから k+1 ホップ先にあるルータが初めて処理を行う確率 $P(1-P)^k$ について示す．表 1 において P の値は 0.5 である．表 1 で示すように，ルータ自身の被害ホストからの位置を考慮しなくても，通過パケットが少ない攻撃ホストに近いルータではサンプリング確率が高くなり，逆に多くの攻撃パケットが集まってくる被害ホストに近いルータには，小さいサンプリング確率が与えられる．これにより，処理を全ルータにわたって分散させることが可能であると考える．

表 1 k を変化させた場合の $P(1-P)^k$ の値
Table 1 The value of $P(1-P)^k$ as k changed.

1	0.5
2	0.25
3	0.125
4	0.0625
5	0.03125
6	0.015625
7	0.0078125
8	0.00390625

4. 特性評価

本章では提案方式の有効性を示すために，提案方式 3.2 と 3.3 におけるトレースバック成功率の評価とトレースバックが 95%以上成功する場合における各ルータの処理率や処理を行ったパケット数の評価を行う．

4.1 シミュレーション緒元

初めに，シミュレーション緒元について述べる．ネットワークトポロジは被害ホストを根とする深さ 20 以下の部分木を用いる．調査 [12] によると，90%以上のネットワークにおいてホップ数が 20 以内であるため，深さ 20 以下で十分であると考える．また，攻撃ホストの配置場所として，文献 [13], [14] では深さ 20 の位置に一様に攻撃ホストを設定しているが，同じ深さに攻撃ホストが均一に存在することは現実的ではない．そこで，本論文では深さ 2〜20 にランダムに攻撃ホストを 1,000 個配置する．また，攻撃ホストの位置に対して各方式がどのような特性をとるかを評価するため，深さ 2〜15 に攻撃ホストを配置した場合のシミュレーションも行う．そして，最後のシミュレーションにおいて攻撃端末の数を 5,000 個にし，提案方式が攻撃端末が大量に存在する場合においても負荷分散を行えること

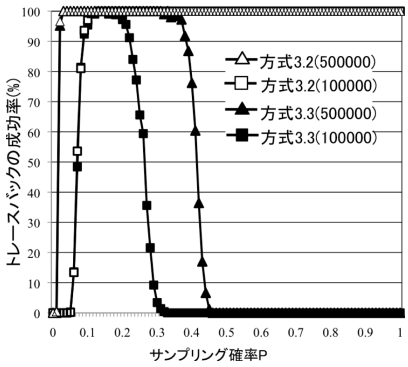

図 6 深さ 2〜20 に配置した場合のトレースバック成功率
Fig. 6 Traceback success rate for setting attackers in depth from 2 to 20.

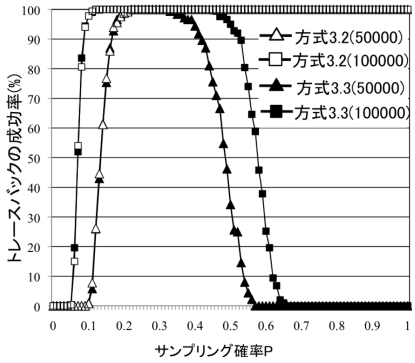

図 7 深さ 2〜15 に配置した場合のトレースバック成功率
Fig. 7 Traceback success rate for setting attackers in depth from 2 to 15.

を示す．またトレースバック成功率は，複数回シミュレーションを繰り返し，攻撃ホストから送信されたパケットが通過した全ルータを特定できた回数をシミュレーション回数で除算した値とする．

4.2 サンプリング確率 P におけるトレースバック成功率の評価

従来方式である HIT 方式と，提案方式 3.1 は 1 つのパケットに対してすべてのルータが処理を行う．したがって，トレースバック成功率は理論上，つねに 100%である．そこで，本節では提案方式 3.2 と 3.3 のトレースバック成功率について述べる．

図 6 に提案方式 3.2 と 3.3 においてサンプリング確率 P を変化させた場合におけるトレースバックの成功率を示す．ここで，図 6 の 500,000 と 100,000 は回収攻撃パケット数を示す．攻撃ホスト数を 1,000 個に設定しているため，500,000 は各攻撃ホストから攻撃パケットを 500 個，また 100,000 は各攻撃ホストから攻撃パケットを 100 個回収した場合であることを示す．両方式ともにサンプリング確率 P が小さい場合は，十分な数の処理がパケットに対して行われず，トレースバックが失敗している．そして，サンプリング確率 P が 0.1〜0.2 になるとすべてのルータがパケットに対して処理を行えるようになり，トレースバック成功率が約 100%に達している．この後，方式 3.2 ではすべてのルータが処理を行うことができるためつねに成功率 100%を達成しているが，方式 3.3 では成功率が急激に降下している．これは，サンプリング確率 P が高くなるとともに，攻撃ホスト近傍のルータが先にパケットに対して処理をしてしまい，被害ホスト近傍のルータは処理を行うことができず，成功率が低下していると考えられる．

また，**図 7** に攻撃ホスト 1,000 個を深さ 2〜15 に設定した場合におけるトレースバック成功率を示す．ここで，図 7 の 100,000 と 50,000 はそれぞれ，各攻撃ホストからパケットを 100 個と 50 個を回収した場合であることを示す．図 7 より深さが 2〜15 である場合は特に回収パケット数が少なくてもトレースバックを成功させることが可能であり，サンプリング確率 P の設定にある程度の幅を与えることができることが分かる．

4.3 トレースバック成功率が 95%の場合の，各ルータにおける処理率

本節では，各方式においてトレースバック成功率が 95%を達成する場合における，各ルータのパケットに対する処理率を評価する．ここで，処理率とは実際に処理を行ったパケット数を全通過パケット数で割った値である．処理率を評価することで，各階層のルータがどれくらい処理をしているかを相対的に知ることが可能となる．従来の HIT 方式と提案方式 3.1 は処理率がつねに 1.0 であるため，本節では提案方式 3.2 と 3.3 につい述べる．

表 2 に提案方式 3.2 と 3.3 における処理率を示す．ここで，表 2 における提案方式 3.3（左）と提案方式 3.3（右）とは，図 6 において提案方式 3.3 では 95%と交わる点が 2 点あり，それぞれその交点の左の交点と右の交点を示している．表 2 より，階層が 1〜10 の間において，他の方式と比較し提案方式 3.3（右）は処理率を低く抑えていることが分かる．特に，階層 1 では提案方式 3.2 と比較し，約 80%も処理率を低減させている．これは，DDoS 攻撃を考慮して確率的かつ 1 度のみ処理を行うことで，上層ルータが処理を行う確率が非常に小さくなるためである．したがって，処理率が低いにもかかわらず同じトレースバック成功率を達成できる提案方式 3.3（右）は有効な方式であると考えられる．

また，**表 3** に攻撃ホストを深さ 2〜15 に設置した場合における各ルータのパケットに対する処理率を示す．この場合においても階層が 1〜10 の間において，他の方式と比較し提案方式 3.3（右）は処理率を低く抑えられていることが分かり，被害ホストに近いルータほど処理回数を低減させるという課題を達成できていることが分かる．

一方，両方の場合において階層が 10〜20，また階層が 10〜15 の間では，共通して提案方式 3.3（右）は処理率が

表 2 深さ 2〜20 に配置した場合の処理率
Table 2 An actual probability for setting attackers in depth from 2 to 20.

	500000packets		
	方式3.2	方式3.3(左)	方式3.3(右)
確率P	0.02	0.02	0.374
階層1	0.0580	0.0427	0.0007
階層2	0.0580	0.0436	0.0010
階層3	0.0580	0.0445	0.0016
階層4	0.0580	0.0454	0.0026
階層5	0.0580	0.0464	0.0041
階層6	0.0580	0.0473	0.0065
階層7	0.0580	0.0482	0.0102
階層8	0.0579	0.0492	0.0161
階層9	0.0579	0.0502	0.0252
階層10	0.0579	0.0533	0.0392
階層12	0.0578	0.0549	0.0929
階層14	0.0574	0.0551	0.2085
階層16	0.0557	0.0480	0.4235
階層18	0.0480	0.0332	0.6582
階層20	0.0201	0.0201	0.3740

表 3 深さ 2〜15 に配置した場合の処理率
Table 3 An actual probability for setting attackers in depth from 2 to 15.

	100000packets		
	方式3.2	方式3.3(左)	方式3.3(右)
確率P	0.094	0.097	0.50
階層1	0.2376	0.0866	0.0011
階層2	0.2376	0.0961	0.0021
階層3	0.2376	0.1064	0.0043
階層4	0.2377	0.1178	0.0085
階層5	0.2377	0.1304	0.0161
階層6	0.2377	0.1442	0.0293
階層7	0.2375	0.1591	0.0520
階層8	0.2371	0.1749	0.0903
階層9	0.2363	0.1914	0.1537
階層10	0.2344	0.2077	0.2542
階層11	0.2314	0.2217	0.4033
階層12	0.2273	0.2285	0.5999
階層13	0.2111	0.2173	0.7857
階層14	0.1507	0.1554	0.6668
階層15	0.094	0.0970	0.5000

大きい．一方，提案方式 3.2 では処理率が均一であり，一見ルータへの負荷分散が実現できているように思われる．そこで，実際にルータが処理を行ったパケットの数を評価することで，提案方式 3.3（右）の有効性を次の 4.4 節で示す．

4.4 トレースバック成功率が 95%の場合の，各ルータにおける平均パケット処理数

本節では，各階層のルータが実際に処理を行ったパケット数についての評価を行う．処理を行ったパケット数を評価することで，通過パケット数に関係なくルータの処理回数を絶対的に見ることができる．

表 4 に攻撃ホストを 2〜20 に配置した場合の各階層ルータにおける平均パケット処理回数を示す．ここで，表 4 中の処理したルータ数とはその階層において実際に処理を行ったルータの数を示し，またパケ数はトレースバックが実際に成功した際に必要となる回収パケット数を示す．表 4 より，DDoS 攻撃を考慮していない提案方式 3.2 では上位の階層ほど処理回数が増加しており，負荷分散を実現できていないことが分かる．これは，通過するパケット数が少ない下層のルータと通過するパケット数が多い上層のルータとで同じ処理率で処理を行ってしまうためである．また，提案方式 3.3（左）はサンプリング確率 P が小さすぎるため，下層の全ルータが処理を行うまで時間がかかり，結果上層のルータでの処理回数が増加している．一方，提案方式 3.3（右）では全階層にわたって処理回数が多くても 200 回程度である．処理回数を大幅に低減させた理由として，階層 10 におけるパケット処理回数 28 を例にあげる．トレースバックが成功した場合において被害ホストが収集した攻撃パケットの平均値は表 4 より 313,201 個であり，また階層 10 において処理を行ったルータの数は 439 個である，つまり，1 つのルータあたり 713（≈313,201/439）個の攻撃パケットが通過していることとなる．表 2 より提案方式 3.3（右）における階層 10 の処理率は 0.0392 である．したがって，階層 10 の 1 つのルータが処理を行った攻撃パケットの数は 713×0.0392 より約 28 となる．同じ 95%というトレースバック成功率を達成しつつ，ルータによる処理回数を低減し負荷を分散できていることが分かる．

また，**表 5** に攻撃ホスト 1,000 個を深さ 2〜15 に設定した場合における平均パケット処理回数を示す．回収パケット数は 100,000 個である．この場合も 2〜20 に攻撃ホストを配置した場合と同様に，提案方式 3.3（右）において各ルータによるパケット処理回数を大きく低減させることができていることが分かる．特に，階層 1 における処理回数では提案方式 3.2 においては 17,404 であるのに対して，提案方式 3.3（右）では 63 と約 99.6%も処理回数を低減させていることが分かる．この理由も，大量の攻撃パケットが集まってくる被害ホストに近いルータに対して小さい処理率を与えているためであると考えられる．以上より，確率的かつ 1 度のみ処理を行うという提案方式が有効であることを示している．

4.5 提案方式 3.3 において確率 P を変化させた場合の各ルータの平均パケット処理回数

本節では，サンプリング確率 P とともに各階層のルータのパケット処理回数がどのように変化していくかを評価する．**図 8** に，いずれもトレースバックを 95%以上達成可能なサンプリング確率 0.02〜0.34 における各階層ごとのパケット処理回数を示す．攻撃端末は 1,000 個であり，回収攻撃パケット数は 500,000 個である．つまり，各端末は 500 個のパケットを送信したこととなる．サンプリング確率の値が小さい場合は，下層のルータの処理回数が小さく，処理が上層のルータに偏っている．しかしながら，サンプリング確率の値が大きくなるとともに，上層のルータによる処理回数は大きく低減され，下層のルータによる処理回数が増加している．そして，サンプリング確率が 0.34 あた

表 4 深さ 2〜20 に配置した場合のパケット処理回数
Table 4 The times of *job* for setting attackers in depth from 2 to 20.

	500000packets			処理したルータ数
	方式3.2	方式3.3(左)	方式3.3(右)	
確率P	0.02	0.02	0.374	
階層1	21461	15699	211	1
階層2	10728	8031	164	2
階層3	5363	4087	130	4
階層4	2682	2086	103	8
階層5	1341	1064	82	16
階層6	671	543	65	32
階層7	335	276	51	64
階層8	167	141	40	127
階層9	85	73	32	251
階層10	48	42	28	439
階層12	26	24	37	790
階層14	22	21	71	935
階層16	20	20	138	955
階層18	17	17	212	873
階層20	7	7	120	500
パケ数	363486	363014	313201	

りでは，全階層にわたって同程度の回数の処理が行われている．これは，サンプリング確率を 0.34 に設定することで表 2 よりパケット通過数が小さい下層のルータには約 0.4 の処理率を与え，逆にパケット通過数が大きい上層のルータには約 0.003 と小さな処理率を与えることとなるためである．したがって，図 8 のサンプリング確率が 0.34 の場合は全階層にわたって同程度の回数の処理が行われ，ルータ負荷の分散を実現できていると考えられる．

また，**図 9** に攻撃端末をランダムに 5,000 個配置した場合におけるパケット処理回数の変化を示す．回収攻撃パケット数は 2,500,000 個であり，各端末は 500 個のパケットを送信したこととなる．この場合においても，サンプリング確率の上昇とともにパケットの処理回数が徐々に全階層にわたって平均して行われるようになっていく様子が分かる．そして，特にサンプリング確率が 0.46 である場合は，各階層における攻撃パケットの数を考慮した処理率を各ルータに与えることができるため，全階層のルータが多くても 200 回程度の処理しか行っておらず，処理の分散が実現できていることが分かる．攻撃端末が大量に存在する場合においても，下層に位置するルータが先に処理を行うことにより，パケットが集中する上層のルータにおける処理回数を抑制している．

今後，ますます堅牢化されていくサーバをサービス不能状態にさせるためには，より多くのパケットを標的サーバに対して送信する必要がある．そして，そのような状況において攻撃ホストから攻撃パケットを 100 個，500 個と回収することは困難ではないと考える．したがって，上記の特性評価が示すように，攻撃パケットを 500,000 個（500 個/攻撃ホスト），100,000 個（100 個/攻撃ホスト）と回収することさえできれば，他の方式と比較し同じトレースバック成功率を達成しつつルータへの負荷を低減・分散可能な提案方式は非常に有効な方式である．

表 5 深さ 2〜15 に配置した場合のパケット処理回数
Table 5 The times of *job* for setting attackers in depth from 2 to 15.

	100000packets			処理したルータ数
	方式3.2	方式3.3(左)	方式3.3(右)	
確率P	0.094	0.097	0.50	
階層1	17404	6236	63	1
階層2	8703	3457	62	2
階層3	4351	1914	62	4
階層4	2176	1060	61	8
階層5	1088	586	58	16
階層6	543	324	53	32
階層7	271	178	47	64
階層8	135	98	41	127
階層9	68	54	35	251
階層10	38	33	33	438
階層11	25	24	36	633
階層12	20	20	43	762
階層13	16	17	50	799
階層14	11	11	40	727
階層15	6	6	29	500
パケ数	72021	70719	56506	

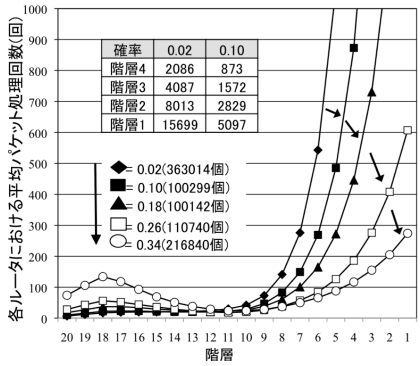

図 8 攻撃端末 1,000 個の場合における処理パケット数の変化
Fig. 8 The changes of numbers of jobbed packed in setting 1,000 attackers.

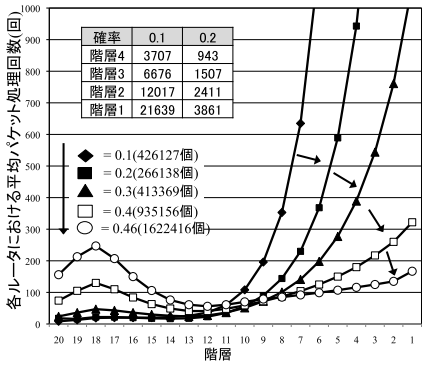

図 9 攻撃端末 5,000 個の場合における処理パケット数の変化
Fig. 9 The changes of numbers of jobbed packed in setting 5,000 attackers.

5. 結論

本論文では，DDoS 攻撃に対して高いトレースバック成功率を達成しつつルータへの負荷を低減・分散させるために，排他的論理和と確率的パケットマーキングを用いたトレースバック方式を提案した．提案方式では，各ルータは従来方式と同様にマーキングとロギングを行ううえに，排

他的論理和を行う．排他的論理和を用いることで2つのルータのIDを1つにまとめることが可能となるためにロギングの回数を低減させることができる．また，DDoS攻撃において攻撃パケットは大量に送信されてくるという特徴と被害ホスト近傍に攻撃パケットが集中するということを考慮して，すべての通過パケットではなく確率的に選択したパケットに対して1度のみ処理を行う．これにより，被害ホストに近いルータほど処理を行う確率が小さくなり，結果ルータへの負荷の低減が可能となる．計算機シミュレーションにより各方式におけるトレースバック成功率とパケット処理率，またパケット処理回数の評価を行い，従来方式と同じトレースバック成功率を達成しつつルータへの負荷を低減・分散可能な提案方式の有効性を示した．

謝辞 本研究の一部は文部科学省GlobalCOEプログラム「アクセス空間支援基盤技術の高度国際提携」，および富士通研究所の助成により行われた．関係者各位に深謝する．

参考文献

[1] Hussain, A., Heidemann, J. and Papadopoulos, C.: A Framework for Classifying Denial of Service Attacks, *Proc. ACM SIGCOMM* (2003).
[2] Snoeren, A., Partridge, C., Sanchez, L., Jones, C., Tchakountio, F., Schwartz, B., Kent, S. and Strayer, W.: Single-Packet IP Traceback, *IEEE/ACM Trans. Networking*, Vol.10, No.6, pp.721–734 (2002).
[3] Burch, H. and Cheswick, B.: Tracing Anonymous Packets to Their Approximate Source, *Proc. 14th Usenix System Administration Conf.* (*LISA '00*) (2000).
[4] Savage, S., Wetherall, D., Karlin, A.R. and Anderson, T.: Practical network support for IP traceback, *Proc. ACM SIGCOMM*, pp.295–306 (2000).
[5] 木内忠司，堀 良彰，櫻井幸一：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，電子情報通信学会技術研究報告，ISEC，情報セキュリティ，Vol.108, No.161, pp.109–114 (2008).
[6] サイバー攻撃源の逆探知システムの開発と実験に成功 (2009)，入手先 ⟨http://www.nec.co.jp/press/ja/0911/2602.html⟩.
[7] Goodrich, M.T.: Probabilistic Packet Marking for Large-Scale IP Traceback, *IEEE/ACM Trans. Networking*, Vol.16, No.1 (2008).
[8] Yaar, A., Perring, A. and Song, D.: FIT – Fast Internet Traceback, *Proc. IEEE INFOCOM* (2005).
[9] Paruchuri, V., Durresi, A. and Chellappan, S.: TTL based Packet Marking for IP Traceback, *IEEE GLOBECOM* (2008).
[10] Gong, C. and Sarac, K.: A More Practical Approach for Single-Packet IP Traceback Using Packet Logging and Marking, *IEEE Trans. Parallel and Distributed System*, Vol.19, No.10, pp.1310–1324 (2008).
[11] Muthuprasanna, M., Manimaran, G., Manzor, M. and Kumar, V.: Coloring the Internet: TP Traceback, *Proc. 12th Int'l Conf. Parallelel and Distributed System* (*ICPADS '06*) (2006).
[12] University of Oregon Router Views Project, available from ⟨http://www.routeviews.org/⟩.
[13] 磯崎裕臣，阿多信吾，岡 育男：履歴キャッシングを用いた確率的パケットマーキングの性能向上，電子情報通信学会信学技報，IEICE，pp.35–40 (Feb. 2005).
[14] Al-Duwairi, B.: Novel Hybrid Schemes Employing Packet Marking and Logging for IP Traceback, *IEEE Trans. Parallel and Distributed System*, Vol.17, No.5, pp.403–418 (2006).

井上 慎一郎 （正会員）

平成21年慶應義塾大学理工学部情報工学科卒業．平成23年同大学院修士課程修了．主として，インターネットセキュリティに関する研究に従事．

石井 方邦 （正会員）

平成23年慶應義塾大学大学院修士課程修了．主として，インターネットセキュリティに関する研究に従事．

笹瀬 巌 （正会員）

昭和54年慶應義塾大学工学部電気工学科卒業．昭和59年大学院博士課程修了．同年オタワ大学理工学部電気・ポストルドクトラルフェロー，昭和60年同大学講師，昭和61年慶應義塾大学理工学部電気工学科助手，昭和63年同大学専任講師，平成4年同助教授，平成11年同大学理工学部情報教授，現在に至る．主として，ディジタル通信，通信ネットワーク，光通信理論，マイクロ波通信，非線形通信システム，通信理論，符号理論に関する研究に従事し，これまで原著論文263編，国際会議論文385編を発表．工学博士．昭和59年度IEEEComSoc学生論文賞．昭和62年第3回井上研究奨励賞受賞．昭和63年第1回安藤博記学術奨励賞，昭和63年篠原記念学術奨励賞，平成8年度本会交換システム研究会優秀論文賞受賞．現在，IEEE Communications Society Board of Governors (Member-at-Large)，同Tokyo Section Chair．これまで，IEEE ComSoc AsiaPacific Regional Director，Satellite and Space Communications TechnicalCommittee Chair，電子情報通信学会通信ソサイエティ副会長，同ネットワークシステム研究専門委員長，同通信方式研究専門委員長等を歴任．IEEE Senior Member，電子情報通信学会フェロー．