平成19年度 修士論文

低レートDoS攻撃と反射型DoS攻撃に対応した改良型ICMP Traceback

An Enhanced ICMP Traceback against Low Rate DoS Attack and Reflector based DoS Attack

東京大学大学院 新領域創成科学研究科 基盤情報学専攻

学籍番号: 47-66331

高田　友則

指導教官　中山　雅哉　准教授

平成 20 年 1 月 29 日 提出

目次

図 目 次

概要

今日のインターネットにおいて，サービス妨害攻撃 (DoS 攻撃) は非常に深刻な問題となっている．サービス妨害攻撃 (DoS 攻撃) とは，攻撃者が標的ホストに対して，大量にパケットを送り，そのホストが行っているサービスを妨害する攻撃である．

ICMP Traceback (iTrace) は，送信元 IP アドレスを偽装したパケットによる DoS 攻撃の攻撃元を，被害者が特定するのに有効な手法である．しかし，iTrace パケットがネットワークに与える負荷を考慮し，iTrace パケットの生成確率を小さな値としているため，攻撃パケットの発生レートが低い DoS 攻撃には適さないという問題があった．また，反射型の DoS 攻撃に対応するためには，数多くのルータに追加機能を持たせなければ有効に機能しないという問題がある．

本論文では，これらの問題を解決すべく，ICMP Traceback を改良した ICMP Traceback with Periodical Transmission (iTrace-PT) を提案する．iTrace-PT は，各ルータで一度 iTrace パケットを送ったあて先には，一定時間は再送しないことで，iTrace パケットの生成確率を上げながらネットワークに与える負荷を低く抑えられる．また，攻撃元の特定を通信の持続時間に基づいて行うことで，攻撃者だけの攻撃元特定を可能にしている．そして，iTrace パケットをリフレクタで反射させることで，対応ルータの数が少ない場合でも反射型の DoS 攻撃に対応できる．シミュレーションにより，iTrace-PT の有効性を示した．

第 1 章

序論

1.1 研究の背景と目的

今日のインターネットにおいて，サービス妨害攻撃 (DoS 攻撃) は非常に深刻な問題となっている．サービス妨害攻撃 (DoS 攻撃) とは，攻撃者が標的ホストに対して，大量にパケットを送り，そのホストが行っているサービスを妨害する攻撃である．攻撃者が複数であるとき，Distributed DoS (DDoS) 攻撃という．また，インターネット上でサーバ機能を持つ通常のホストを踏み台（リフレクタ）に利用し，送信元 IP アドレスを標的ホストに偽装したパケットを用いて，サーバからの応答パケットで標的ホストを攻撃する反射型の DoS 攻撃を，DRDoS (Distributed Reflective DoS) 攻撃 [1] という．

シマンテック社によると，DoS 攻撃の発生件数は年々増加し，2006 年 7 月 1 日から 12 月 31 日の間には一日平均 5213 件が記録されている [2]．特に近年は，インターネットに常時接続する初心者の PC ユーザが増加しているため，利用者が気が付かないうちに，攻撃者から遠隔操作されて DDoS 攻撃の一端として悪用されるケースが急増している．

DoS 攻撃は，一般的に送信元 IP アドレスを偽装したパケットによって行われるため，被害者は受け取った攻撃パケットから攻撃元を特定することは困難である．IP Traceback 手法は，偽装したパケットを送出する攻撃元を特定する技術であり，これまでにマーキング方式 [3] やロギング方式 [4]，ICMP Traceback (iTrace) [5] といった手法が提案されてきた．

しかし，これらの手法は，通常の DoS 攻撃の攻撃元を特定するための手法であるため，DRDoS 攻撃にそのまま適用すると，リフレクタの特定はできても，真の攻撃元を特定することができない．そのため，DRDoS 攻撃の真の攻撃元を特定するため，iTrace 手法を改良した手法 [6] や，マーキング方式を改良した手法 [7] 等が提案されてきた．しかし，これらの手法は数多くのリフレクタやルータに追加機能を持たせなければ有効に機能しないという問題がある．

ICMP Traceback (iTrace) [5] は，ルータがパケットを中継する際，一定の確率で中継パケットと同じあて先に ICMP パケットを新たに生成して送る．この ICMP パケットのデータ部には，ルータのアドレス等が記述される．この ICMP パケットを iTrace パケットと呼ぶ．iTrace パケットを受け取った被害者は，iTrace パケット内のデータ部から，生成したルータ

のアドレス情報を得ることができ，攻撃元までの経路を特定できる．iTrace 手法は，他手法に比べ実装がしやすく，DRDoS 攻撃 に対しても比較的容易に適用できるため，有効性が高い方式だと考えられている．

iTrace 手法では，iTrace パケットがネットワークに与える負荷を考慮し，iTrace パケットの生成確率を小さな値 (1/20000) とするように提案されている．このため，個々の攻撃レートを低く設定した DDoS 攻撃や，Low-Rate attack [8] では，各ルータが iTrace パケットを生成するのに非常に長い時間を要することになる．また，正当ユーザの通信にまぎれるほど低い攻撃レートの場合は，攻撃者だけの攻撃元特定が難しいという問題がある．

本論文では，上記の問題を解決すべく，ICMP Traceback を改良した ICMP Traceback with Periodical Transmission (iTrace-PT) を提案し，その有効性をシミュレーションによって評価する．iTrace-PT は，ルータで iTrace パケットを生成したり，中継する際に，そのあて先 IP アドレスを一定時間記憶し，当該時間帯において，そのあて先に対しては新たな iTrace パケットを生成しない．この変更により，ネットワークに与える負荷を低く抑えながら，各ルータの iTrace パケット生成確率を高めることを可能とし，低レートの攻撃者の特定が可能になることが期待される．また，iTrace-PT は，攻撃元の特定を通信の持続時間に基づいて行う．この特定法により，正当ユーザの通信にまぎれるほど低い攻撃レートであったとしても，攻撃時間が長ければ攻撃者だけの攻撃元特定が可能になる．さらに，iTrace パケットをリフレクタで反射させることにより，リフレクタに新たな追加機能を持たせる必要がなく，対応ルータの数が少ない場合でも DRDoS 攻撃の攻撃元を特定できる．

1.2　本論文の構成

本論文は以下のように構成される．

第 2 章「DoS 攻撃の概要」では，DoS, DDoS 攻撃の概要と，近年新たな脅威となってきている DRDoS 攻撃の概要を述べる．

第 3 章「関連研究」では，現在，DoS 攻撃の対策として提案されている手法の概要とその問題点を述べる．

第 4 章「iTrace-PT について」では，iTrace 手法が持つ問題を解決する提案手法である iTrace-PT について述べる．

第 5 章「シミュレーションによる評価」では，シミュレーションにより，iTrace-PT の有効性を示す．

第 6 章「考察」では，偽装 iTrace パケットが与える影響とその対策手法，また iTrace-PT の実用性について述べる．

第 7 章「結論」では，まとめと今後の課題を述べる．

第 2 章

DoS 攻撃の概要

今日のインターネットにおいて，サービス妨害攻撃 (DoS 攻撃) は非常に深刻な問題となっている．サービス妨害攻撃 (DoS 攻撃) とは，攻撃者が標的ホストに対して，大量にパケットを送り，そのホストが行っているサービスを妨害する攻撃の総称である．シマンテック社によると，DoS 攻撃の発生件数は年々増加し，2006 年 7 月 1 日から 12 月 31 日の間には一日平均 5213 件が記録されている [2].

DoS 攻撃は，攻撃者が直接標的ホストを攻撃するタイプと，インターネット上でサーバ機能を持つ通常のホストを踏み台（リフレクタ）に利用し，リフレクタからの応答パケットで標的ホストを攻撃する反射型のタイプがある．以下，それぞれについて述べる．

2.1 DoS, DDoS 攻撃

攻撃者が直接標的ホストを攻撃するタイプとして，攻撃者が単独である DoS 攻撃と，攻撃者が複数である Distributed DoS (DDoS) 攻撃がある．

DDoS 攻撃では，セキュリティに脆弱性を持つコンピュータを DoS 攻撃の Slave として利用し，遠隔操作を通じて Slave に攻撃を行わせる．(図 2.1).

特に近年は，インターネットに常時接続する初心者の PC ユーザが増加しているため，利用者が気が付かないうちに，Slave として利用され DDoS 攻撃の一端として悪用されるケースが急増している．

このタイプの DoS 攻撃は，一般的に送信元 IP アドレスを偽装したパケットによって行われるため，被害者は受け取った攻撃パケットから攻撃元を特定することは困難である．この攻撃元を特定するために，IP Traceback 手法が提案された．

以下で，DoS，DDoS 攻撃の詳細を，最も一般的な攻撃である Syn flooding を例にとって説明する．

Syn flooding は，TCP でコネクションを確立するための手順である，3 ウェイハンドシェイクを悪用した DoS 攻撃である．TCP の 3 ウェイハンドシェイクでは，クライアントから送られてきた Syn パケットをサーバが受け取ると，そのパケットの送信元 IP アドレスなどを一定時間そのサーバにおいて記憶する．攻撃者が，このサーバに対して大量に Syn パケッ

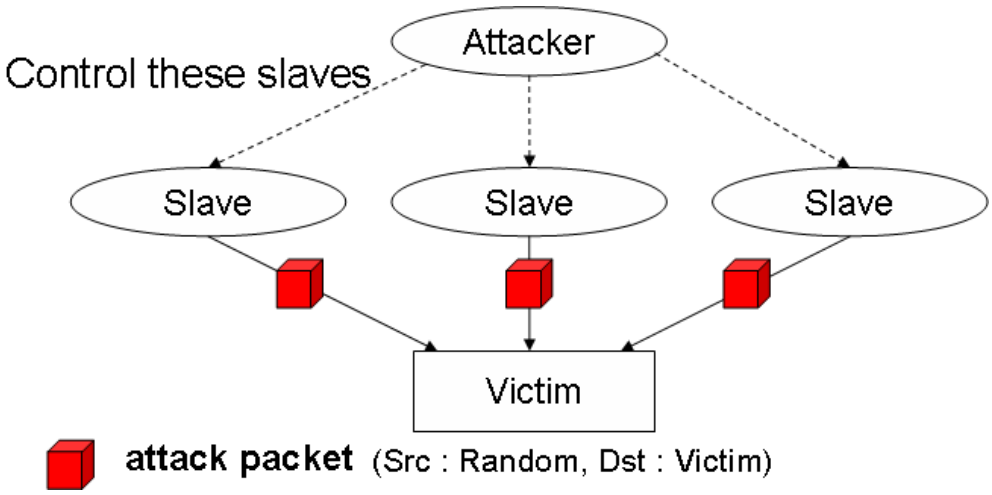

図 2.1 DDoS attack

トを送るとサーバの記憶領域を使い果たし，これ以上他の通信を受け付けることが出来なくなり，そのサーバの行うサービスが妨害される．これは，被害者のリソースを使い果たすタイプの DoS 攻撃であり，単独の攻撃者または少数の攻撃者によって行われる．

一方，攻撃者が複数である DDoS 攻撃では，被害者に届くパケットの数が大量であるため，攻撃者と被害者の間のルータにおいて，全パケットの処理が出来なくなり，パケットの廃棄が行われる．このとき，攻撃パケットと正当パケットの区別は非常に困難であるため，正当パケットも破棄されてしまう．その結果標的ホストの行うサービスが妨害される．これは，ネットワークのリソースを使い果たすタイプの攻撃に分類される．

2.2　反射型 DoS 攻撃

インターネット上でサーバ機能を持つ通常のホストを踏み台（リフレクタ）に利用し，送信元 IP アドレスを標的ホストに偽装したパケットを用いて，サーバからの応答パケットで標的ホストを攻撃する反射型の DoS 攻撃を，DRDoS (Distributed Reflective DoS) 攻撃 [1] という．

DRDoS 攻撃の概要を，以下で説明する．

図 2.2 のように，DRDoS 攻撃の攻撃者は，リフレクタと呼ばれるインターネット上でサーバ機能を持つホストに，送信元 IP アドレスを標的ホストの IP アドレスに偽装したパケットを送る．このパケットを受け取ったリフレクタは，その送信元 IP アドレス，つまり標的ホストに対して応答パケットを返信する．このように被害者が，攻撃者からではなく，リフレクタからの応答パケットにより攻撃を受けるということが，DRDoS 攻撃の最大の特徴である．この特徴のため，通常の IP Traceback を用いても，被害者はリフレクタまでしか攻撃元を特定できず，その後ろにいる真の攻撃元を特定できない．

この攻撃で利用されるリフレクタは，パケットを受け取り応答パケットを返すホストであれば何でも良いので，インターネット上には無数のリフレクタが存在することになる．

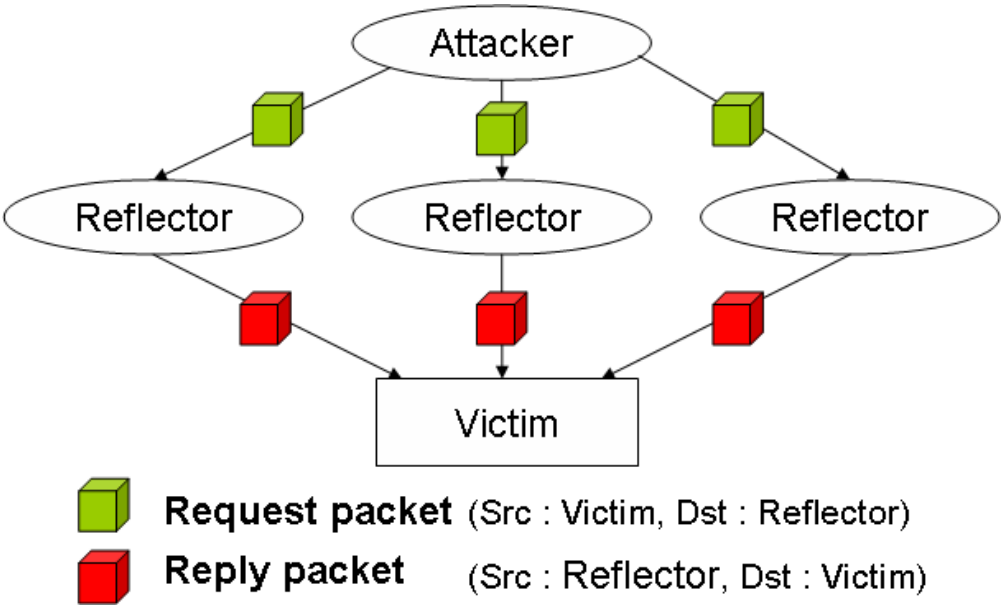

図 2.2 DRDoS attack

実際に，DRDoS 攻撃は 2002 年，Gibson Research Corporation [9] に対して行われ，この攻撃の脅威が示された．また，近年リフレクタに DNS サーバを用いて，DNS の Reply パケットによって攻撃を行う DRDoS 攻撃が増えてきており [10]，インターネット上の新たな脅威となってきた．

DRDoS 攻撃の脅威な点をまとめると以下のような 3 点が挙げられる．

- インターネット上のほとんどのホストがリフレクタになりえる．
- パケットの増幅作用が生じる．
- 攻撃者から直接パケットを受け取らない．

第一に，インターネット上のほとんどのホストがリフレクタになりえることにより，被害者が特定のリフレクタからの通信を拒否するだけでは，この攻撃を防ぐことはできない．

第二に，DRDoS 攻撃では，受信パケット数よりも多くの応答パケットを返したり，受信パケットのサイズよりも大きな応答パケットを返すリフレクタを用いることにより，攻撃者が送出したパケットの数やサイズを数倍から数十倍に増幅することが可能である [10, 11]．これはつまり，攻撃者が送出するパケット数が少なくても，非常に大きな攻撃を行えるということである．

第三に，DRDoS 攻撃の被害者は，攻撃者からのパケットではなく，リフレクタからの応答パケットによって攻撃を受けるため，通常の IP Traceback を用いても，リフレクタまでしか攻撃元を特定できず，その後ろにいる真の攻撃元を特定できない．

第 3 章

関連研究

DoS 攻撃の対策としては，攻撃を事前に防ぐ Proactive 型と，攻撃を受けた後に対策を行う Reactive 型がある．Proactive 型としては，攻撃パケットのフィルタリングを行う Ingress Filtering [12] があり，Reactive 型には，攻撃元の特定を行う IP Traceback がある．

3.1 Ingress Filtering

Ingress Filtering [12] は，ネットワークの境界となるエッジルータにおいて，送信元 IP アドレスが自ネットワーク以外のアドレスに偽装しているパケットをフィルタリングする手法である．DoS 攻撃は，一般的に送信元 IP アドレスを偽装したパケットによって行われるため，この手法が導入されれば，攻撃パケットは攻撃者のいるネットワークでフィルタリングされるため，DoS 攻撃を未然に防ぐことが出来る．

しかし，攻撃者が送信元 IP アドレスを，同一 AS 内の別のホストに偽装した場合は，フィルタリングすることが出来ず，DoS 攻撃を防ぐことが出来ない．さらに，この手法を導入していないネットワークからの攻撃は，防ぐことが出来ないため，全ての ISP が導入しなければ，有効に機能しないという欠点がある．

3.2 IP Traceback

IP Traceback 手法は，偽装したパケットを送出する攻撃元を特定する技術であり，大きく分類して，マーキング方式 [3]，ロギング方式 [4]，ICMP Traceback (iTrace) [5] がある．

3.2.1 マーキング方式

マーキング方式 [3] は，ルータがパケットを中継する際，ある確率で当該ルータのアドレス情報等を IP ヘッダに埋め込む．被害者は，この情報を集めることにより攻撃元を特定することができる．

この手法は，攻撃元の特定のために必要な情報を，新たにパケットを生成して送るのではなく，直接パケットに埋め込むため，ネットワークに負荷を与えることはない．しかし，IP ヘッダ中にマーキング専用のフィールドは存在しないため，ID フィールドを用いている．ID フィールドは，パケットのフラグメントが行われたとき，そのパケットの再構築のために使われるフィールドである．そのため，本方式を導入すると，パケットのフラグメントが出来なくなるという問題が生じる．

また，DRDoS 攻撃の真の攻撃元を特定するためには，リフレクタにおいてマーク情報を維持してもらう必要がある [7]．しかし，前章で述べたようにインターネット上には，無数のリフレクタが存在するため，それら全ての協力を得ることは困難であり，実用的ではないと考えられる．

3.2.2　ロギング方式

ロギング方式 [4] は，ルータを通過した全てのパケットを当該ルータにおいて記憶する．被害者は，受け取った攻撃パケットがどのルータを経由してきたかを，各ルータに問い合わせることにより，特定することができる．

この方式は，中継する全てのパケットに対し処理を行わなければならないため，ルータの処理負荷が大きいという問題がある．また，DRDoS 攻撃への適用が困難である．

3.2.3　ICMP Traceback

ICMP Traceback (iTrace) [5] は，パケットがルータに到着すると，そのルータの IP アドレス等をデータ部に記載した iTrace パケットを一定の確率で生成し，中継したパケットと同じあて先に対して送る．被害者は，受信した iTrace パケットのデータを基にして，攻撃元までの経路を特定できる．

iTrace 手法では，攻撃元を特定するために，被害者から攻撃者までの経路上の全ルータからの iTrace パケットを収集する必要がある．また，iTrace パケットがネットワークに与える負荷を考慮し，iTrace パケットの生成確率を低く設定しているため，攻撃元の特定に長く時間を要する場合がある．そのため，iTrace 手法を改良した提案が幾つかなされている [13, 14, 15, 16]．例えば，ICMP Traceback with Cumulative Path (iTrace-CP) [13] は，iTrace パケットを生成したルータから被害者までの経路情報を一度にデータ部に記載して送るため，攻撃者の直近ルータからの iTrace パケットを受信するだけで，攻撃元までの経路を特定できる．

iTrace 手法は，他手法に比べ実装がしやすく，DRDoS 攻撃に対しても比較的容易に適用できるため，有効性が高い方式だと考えられている．

以下に，iTrace 手法を DRDoS 攻撃に適用した手法である，Reverse iTrace と ICMP Caddie message を紹介する．

Reverse iTrace (r-iTrace)

Reverse iTrace (r-iTrace) は，iTrace 手法を DRDoS 攻撃に対応させた手法である．iTrace 手法では，中継パケットと同じあて先だけに，iTrace パケットを送っていたが，r-iTrace では，中継パケットの送信元に対しても送る．

例えば，図 3.1 において，R2 が攻撃パケットに対して iTrace パケットを生成するとき，攻撃パケットのあて先であるリフレクタと，送信元である被害者あての 2 パケット生成し，送信する．この改良により DRDoS 攻撃の被害者は，攻撃者-リフレクタ間の経路情報を得ることができ，受信した iTrace パケットのデータを基にして，DRDoS 攻撃の攻撃元を特定できる．

しかし，被害者から攻撃者の最寄りの対応ルータまでの経路上の全ルータが，対応ルータでなければ攻撃元を特定できないという問題がある．

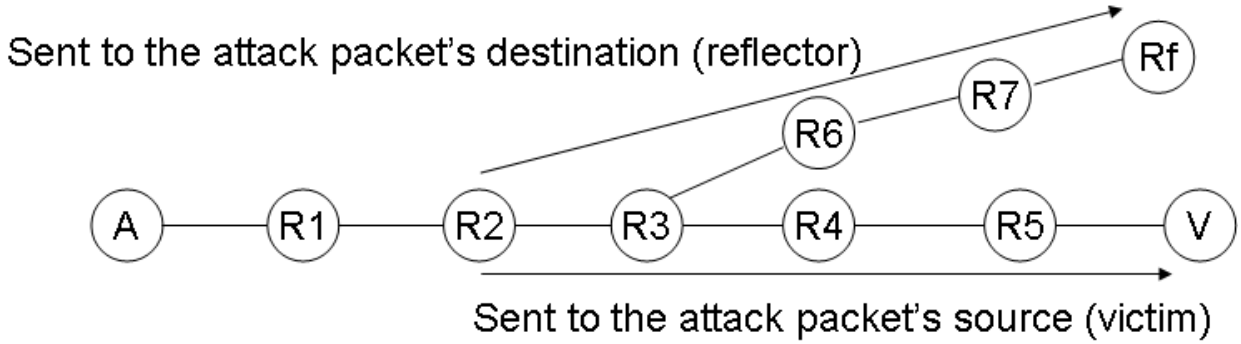

図 3.1 When R2 generates iTrace packets

ICMP Caddie messages (iCaddie)

ICMP Caddie messages (iCaddie) [6] における，DRDoS 攻撃への IP Traceback は，2 段階で行われる．

一段階目で，被害者が受け取ったリフレクタ-被害者間の経路情報を持った iTrace パケットにより，リフレクタの最寄りルータを特定し，二段階目で，特定したそのルータに対して Traceback Request を送り，Request を受けたルータが真の攻撃元まで特定する (図 3.2)．

iCaddie は，Traceback Request を受けたルータが，攻撃者-リフレクタ間の経路情報を持った iTrace パケットを受け取っていなければ，真の攻撃元を特定することができない．例えば，図 3.2 において，R3, R6, R7 が対応ルータでなければ，被害者は R4 までしか特定できず，R4 は攻撃者-リフレクタ間の経路情報を持った iTrace パケットを受け取れないため，リフレクタの後ろの真の攻撃者を特定できない．

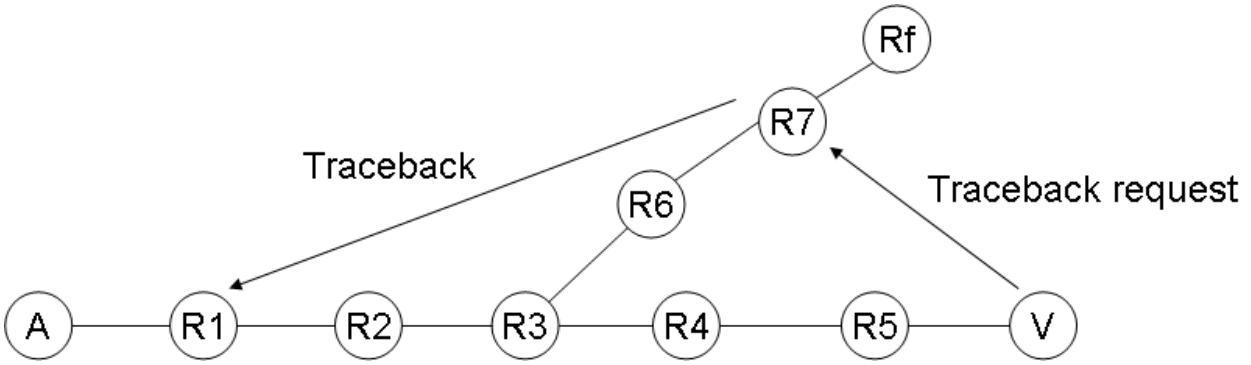

図 3.2 ICMP Caddie messages (iCaddie)

3.3　本章のまとめ

本章では，DoS 攻撃の対策として，現在提案されている手法である Ingress Filtering と IP Traceback に関して説明した．

攻撃パケットのフィルタリングを行うことにより，DoS 攻撃を対策する Ingress Filtering は，全ての ISP がこの手法を導入しなければ，有効に機能しないという欠点がある．

攻撃元の特定を行うことによって，DoS 攻撃の対策を行う IP Traceback には，マーキング方式，ロギング方式，iTrace といった手法があるが，既存のネットワークに与える影響やルータに与える処理負荷，また，DRDoS 攻撃への適用性を考慮すると，iTrace 手法が最も実用的であり，有効な手法であると考えられる．

しかし，iTrace 手法は，ネットワークに与える負荷を 0.1% 以下に抑えるために，各ルータが生成する iTrace パケットの生成確率を 1/20000 に定めている．このため，個々の攻撃パケットの生成レートを低く設定した DDoS 攻撃や，Low-Rate attack [8] では，各ルータが iTrace パケットを生成するのに長い時間を要し，短時間での攻撃元の特定が出来ないという問題がある．

また，正当ユーザの通信にまぎれるほどの低い攻撃レートで攻撃が行われた場合，攻撃者だけの攻撃元特定が困難になり，正当ユーザを攻撃者と誤検出する可能性が高くなる．

さらに，DRDoS 攻撃に適用するためには，多くのルータが対応ルータでなければ，有効に機能しないという問題もある．

本論文では，DoS 攻撃の対策として，iTrace 手法に焦点を当て，上記の問題を解決する手法を提案する．

第 4 章

iTrace-PTについて

前章で述べた様に iTrace 手法は，他手法に比べ有効な手法であるが，低レートでの DoS 攻撃に対する脆弱性を有する．主な問題点は，以下の二つである．

- iTrace パケットの受信に時間を要する
- 攻撃者だけを特定することが困難

また，DRDoS 攻撃に適用するためには，多くのルータが対応ルータでなければ，有効に機能しないという問題もある．

本論文では，上記の問題を解決すべく，ICMP Traceback を改良した ICMP Traceback with Periodical Transmission (iTrace-PT) を提案する．

上記の 1 つ目の問題は，iTrace パケットがネットワークに与える負荷を 0.1%以下に抑えるために，各ルータの iTrace パケット生成確率を 1/20000 に設定している点にある．そこで，iTrace-PT では，iTrace パケットの生成確率を上げながらネットワークに与える負荷を低く抑えるため，各ルータが一度 iTrace パケットを送ったあて先には，一定時間は再送しないという生成方式をとる．

上記の 2 つ目の問題は，既存手法が攻撃元の特定を，被害者が受け取った iTrace パケット数に基づいて行っている点にある．そのため，正当ユーザの通信にまぎれるほどの低い攻撃レートで攻撃が行われると攻撃者だけの特定が困難になる．iTrace-PT では，通信の持続時間に基づいた攻撃元の特定を行うことで，正当ユーザの通信にまぎれるほど低い攻撃レートであったとしても，攻撃時間の方が長ければ攻撃者だけの攻撃元特定が可能になる．

また，iTrace-PT は，iTrace パケット自体も攻撃パケットと同様にリフレクタに反射させる手法をとることで，対応ルータの数が少ない場合でも，DRDoS 攻撃の攻撃元を特定できる．

以下，それぞれについて詳細を述べる．

4.1 iTrace パケット生成アルゴリズム

iTrace-PT では，一度送った iTrace パケットのあて先 IP アドレスをルータで一定時間記憶する．ただし，単純にあて先 IP アドレスを記憶すると搭載するメモリ量が膨大に必要と

なる場合があるため，Bloom Filter を用いて一定のメモリ量で実現する機構を用いることとする．

Bloom Filter は，ある要素が集合のメンバーであるかどうかの判定を一定のメモリ量で実現するための手法であり，以下の様にする．Bloom Filter のデータ構造は，m ビットのビット配列であり，最初は，全てのビットを 0 にしておく．ある要素 P を Bloom Filter に追加するときは，k 種類のハッシュ関数を用いて，k 個のキー値を求め，対応する配列のビットを 1 に変更する (図 4.1)．ある要素 P が Bloom Filter に記憶されているかどうかを確認するときは，要素 P に対する k 個のキー値を求め，対応したビット配列の要素が全て 1 になっている場合には，要素 P が記憶されていると判定する．

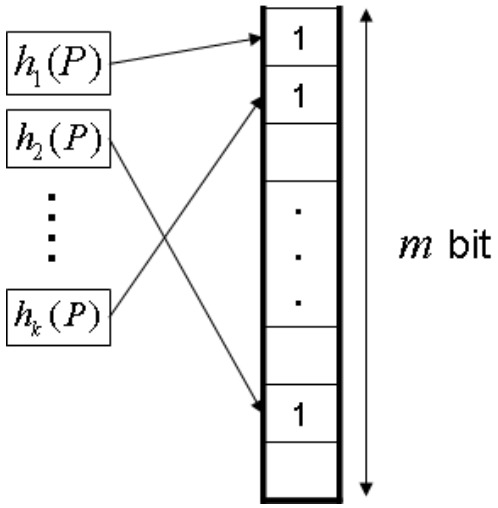

図 4.1 Bloom Filter の概要

また，提案する iTrace-PT における iTrace パケットの生成アルゴリズムを図 4.2 に示す．

ルータ R が，パケット a を受信すると，まず，iTrace パケットかどうか判定する．もし，iTrace パケットならば，a のあて先 IP アドレスを Bloom Filter に追加し，iTrace パケット a のデータ部に，ルータの IP アドレス R を追加し，送信する．

iTrace パケットでない場合は，$[0, 1]$ の乱数 x と iTrace パケットの生成確率 p の値とを比較して，$x \leq p$ となり，かつパケット a のあて先 IP アドレスが Bloom Filter に記録されていない場合，a に対応した iTrace パケットを生成し，a のあて先 IP アドレスを Bloom Filter に追加する．

一定時間 t 経ったら，Bloom Filter のビット配列の全ビットを 0 にクリアするとともに，タイマー j を 0 に戻す．今後，Bloom Filter のビット配列の全ビットを 0 にクリアする処理をハッシュクリアすると呼ぶ．この様に，定期的にハッシュクリアを行うことで，ルータ R から定期的な iTrace パケットの送信を実現している．

```
let BF be a hashtable of Bloom Filter
let p be a generation probability of iTrace packet
let t be a hash clear interval
let j be a timer
at Router R
for each received packet a
  if isiTrace(a) = true then
   set(a.dest,BF)
   append(a, R)

  let x be a random number from [0,1]
  if x ≤ p then
   if isset(a.dest,BF) = false then
    generate_iTrace(a)
    set(a.dest,BF)

  if j ≥ t then
   clear(BF)
   j = 0
```

図 4.2 iTrace パケットの生成アルゴリズム

4.2　攻撃元の特定方式

iTrace-PT は，攻撃者だけの特定を可能にするために，通信の持続時間に基づいた攻撃元の特定を行う．以下，iTrace-PT の攻撃元特定方式に関する基本アイデアとその詳細を述べる．

4.2.1　基本アイデア

図 4.3 に示すように，攻撃者 A と被害者 V 間に n 個の中継ルータ $R_i(1 \leq i \leq n)$ があるとき，攻撃者 A から k 番目のルータ R_k がハッシュクリア間隔内に iTrace パケットを被害者 V あてに生成する確率 $P(k)$ は，(4.1) 式で表せる．ただし，iTrace パケットの生成確率を p，攻撃レートを f(pps)，ハッシュクリア間隔を t(秒) とする．

$$P(k) = \frac{p(1-p)^{k-1}\{1-(1-p)^{kft}\}}{1-(1-p)^{k}} \tag{4.1}$$

図 4.4 に，(4.1) 式のグラフを示す．各種パラメータは，生成確率 1/1000，ハッシュクリア間隔 60 秒，攻撃レート 10, 20, 100pps とした．

この図より，生成確率を 1/1000，ハッシュクリア間隔を 60 秒と設定したとき，攻撃レート

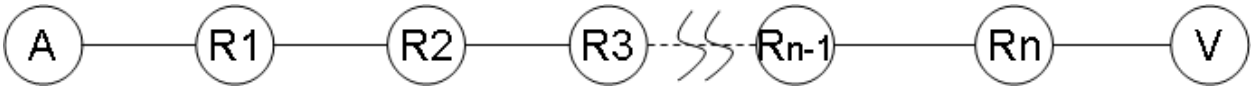

図 4.3 線形トポロジ

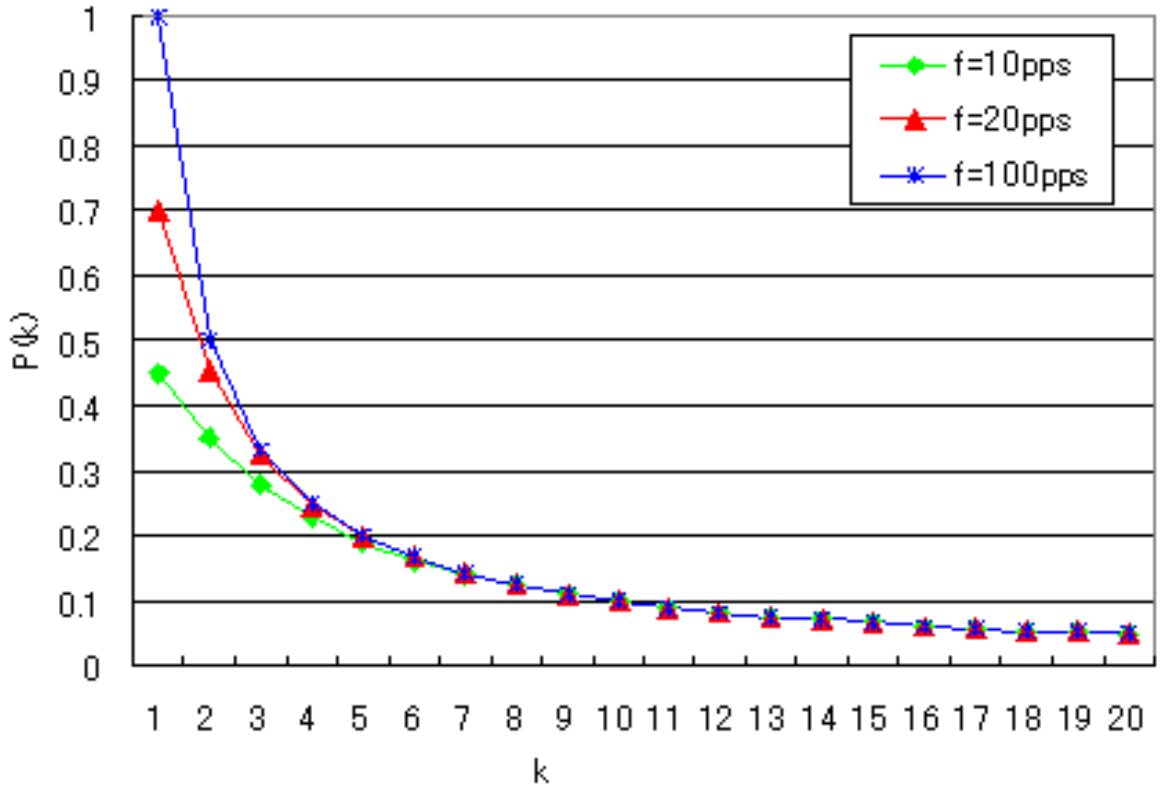

図 4.4 $P(k)$ のグラフ

によって，攻撃者の最寄りルータ ($k = 1$) において $P(k)$ の値が大きく異なることが分かる．

iTrace-PT における攻撃元の特定は，通信の持続時間に注目し，以下のように行う．m 回のハッシュクリアが行われたとき，閾値を α として，$\lceil m\alpha \rceil$ 個以上の iTrace パケットを発生させたルータを，攻撃者の直近ルータであると特定する．ここで $\lceil x \rceil$ は x 以上の最小整数である．ここで，同一パス上の 2 つ以上のルータが iTrace パケットを $\lceil m\alpha \rceil$ 個以上生成していた場合は，一番上流のルータを攻撃元と判定する．iTrace-PT のデータ部には経路情報が含まれているため，被害者は，最も上流のルータを認識することが出来る．

この方式において，図 4.4 の状況を想定すると，攻撃レート 10, 20, 100pps のとき，攻撃者の最寄りルータを特定するためには，$k = 1$ の点を見て，閾値 α をそれぞれ 0.45, 0.69, 0.99 以下に設定する必要がある．

以下で，この攻撃元特定手法を用いることで，上記の 2 つ目の問題点である「攻撃者だけの特定が困難」が解決される理由を述べる．iTrace-PT による攻撃元特定手法は，既存手法

とは異なり，被害者が受け取った iTrace パケット数に基づいた攻撃元の特定ではなく，通信の持続時間に基づいて攻撃元の特定が行われていることになる．

つまり，ある攻撃レートの攻撃が，m 回のハッシュクリアの時間だけ継続している場合，攻撃者の最寄りルータからの iTrace パケットは，(4.1) 式を使って，$mP(1)$ 個届くことが期待される．

一方，正当ユーザの通信レートが攻撃レートより高かったとしても，正当ユーザの最寄りルータから生成される iTrace パケットは，その通信時間に対応した個数となるため，通信が攻撃時間より短く終了すれば，複数回のハッシュクリア後に攻撃元の特定を行うことにより，その正当ユーザを攻撃元と誤検出する確率を低く抑えることができる．

ここでは，DDoS 攻撃の様な比較的長期間に及ぶ攻撃を前提としているため，本提案方式は有効に機能するはずである．このように，iTrace-PT では，攻撃者の通信が正当ユーザの通信にまぎれるほど小さくても，攻撃時間が長ければ，攻撃者だけを特定することができる．

4.2.2　特定方式の詳細

正当ユーザと攻撃者が混在している状況における，攻撃元特定法式の詳細に関して述べる．

ある被害者に対して行う正当ユーザの最大通信時間が T_n(秒) であったとすると，ハッシュクリア間隔を t(秒) として，正当ユーザの最寄りルータから生成される iTrace パケットの個数 N の最大値は，(4.2) 式で表される．

$$N = \left\lceil \frac{T_n}{t} \right\rceil + 1 \tag{4.2}$$

つまり，閾値を α としたとき，(4.3) 式に示した S 回目以降のハッシュクリア時に，攻撃元の特定を行えば，正当ユーザを攻撃元と誤検出することがなくなる．閾値 α を小さな値とすればするほど，より低レートの DoS 攻撃の攻撃者を特定できるが，(4.3) 式を見て分かるように，閾値 α を小さな値にすると，攻撃者だけの特定を行うためには長い時間を要する．

$$S = \left\lfloor \frac{N}{\alpha} + 1 \right\rfloor \tag{4.3}$$

続いて，閾値 α の設定方法について述べる．一回のハッシュクリア内に，攻撃者の最寄りルータが iTrace パケットを生成する確率 q は，(4.1) 式に $k = 1$ を代入して，以下のようになる．

$$q = P(1) = 1 - (1 - p)^{ft} \tag{4.4}$$

次に，m 回のハッシュクリアが行われたとき，攻撃者の最寄りルータが r 個の iTrace パケットを生成する確率 $f(m, r)$ は，(4.5) 式で表せる．

$$f(m, r) = {}_mC_r q^r (1 - q)^{m-r} \tag{4.5}$$

ここで，$\beta = \lceil m\alpha \rceil$ とすると，m 回のハッシュクリア時，攻撃者の最寄りルータを攻撃元と特定できる確率 Pr は，(4.6) 式で表せる．

$$Pr = \sum_{i=\beta}^{m} f(m, i) \tag{4.6}$$

被害者は，何 pps 以上の攻撃者 (f に相当) を，どれくらいの時間 (m に相当) で，どの程度特定したいか (Pr に相当) を決めることで，(4.6) 式を用いて，閾値 α を設定することが出来る．

ここで，閾値設定の例を示す．ただし，iTrace パケットの生成確率を 1/1000，ハッシュクリア間隔を 60 秒とする．今，攻撃を受けている被害者が，次の 2 通りの条件を設定したとする．

- 条件 1：
  50pps 以上で攻撃を行っている攻撃者を，10 回目のハッシュクリア時に，90%以上特定したい．
- 条件 2：
  10pps 以上で攻撃を行っている攻撃者を，15 回目のハッシュクリア時に，90%以上特定したい．

図 4.5 は，それぞれの条件において (4.6) 式を図示している．この図よりそれぞれの条件を満たす閾値を設定することができ，その値は，条件 1 では 0.9 以下に，条件 2 では 0.25 以下にすればよいことが分かる．

また，この被害者と正当ユーザの最大通信時間 T_n が，被害者が攻撃を受けていない平常時に測定した結果，100 秒であったとする．このとき，(4.3) 式より，正当ユーザを攻撃元と誤検出しないためには，閾値 0.9 のとき 4 回目以降，閾値 0.25 のとき 13 回目以降に攻撃元の特定をしなくてはならない．条件 1 で設定した値は 10 回目，条件 2 で設定した値は 15 回目であるからこの条件を満たしている．

よって，この被害者は，条件 1 ならば閾値 α を 0.9 とし，10 回目のハッシュクリア時 (10 分後) に，条件 2 ならば閾値 α を 0.25 とし，15 回目のハッシュクリア時 (15 分後) に，攻撃元の特定を行えば，誤検出がなく攻撃者の 90%以上を特定することが出来ると期待される．

このように，iTrace-PT では，被害者が自身の行っているサービスやリソースを考慮し，各種パラメータを設定することで，被害者の望んだ攻撃元の特定が出来る．

4.3　DRDoS 攻撃への適用

iTrace-PT は，対応ルータの数が少ない場合でも，DRDoS 攻撃の攻撃元を特定できるようにするため，iTrace パケットを攻撃パケットと同様にリフレクタに反射させる手法をとる．

iTrace-PT は，生成する iTrace パケットの送信元 IP アドレスとあて先 IP アドレスの組を，中継パケットと同一にし，ICMP の型を Traceback 用に新たに定義するのではなく，現在広

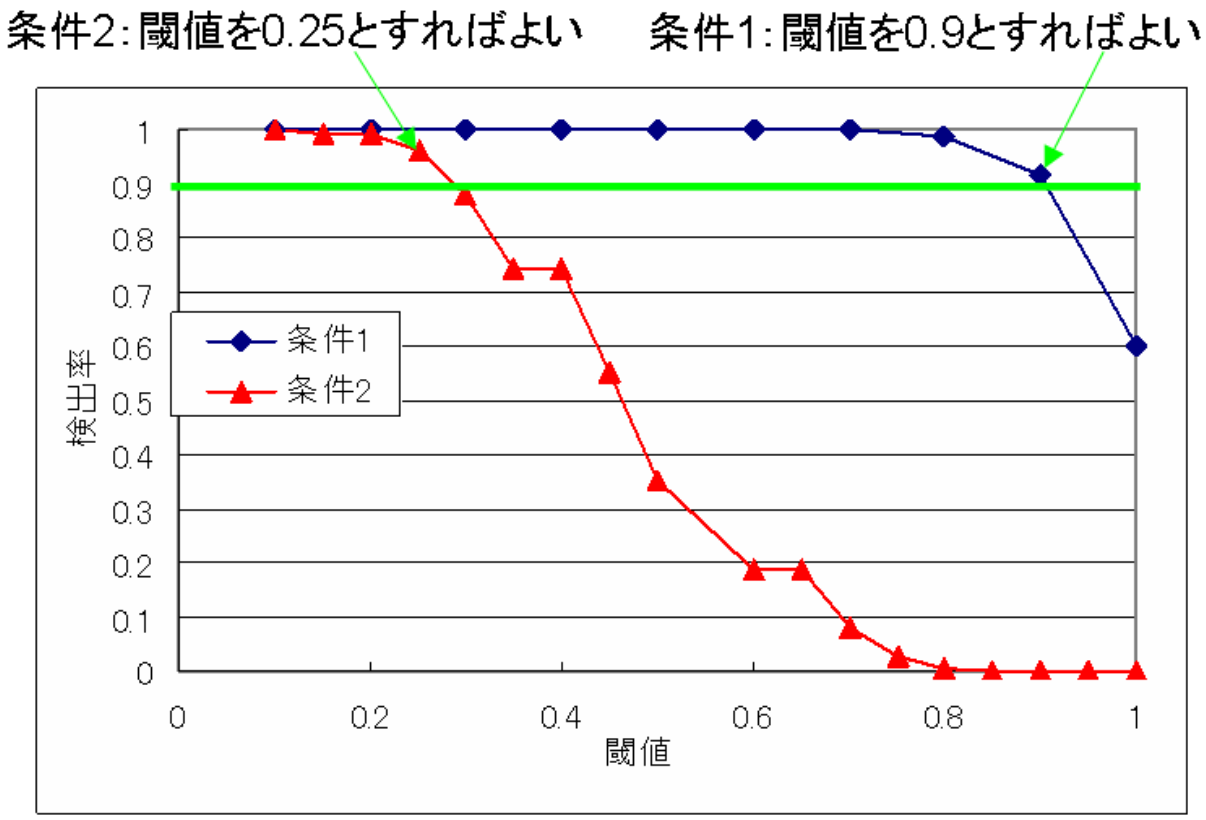
条件2:閾値を0.25とすればよい
条件1:閾値を0.9とすればよい
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
検出率
条件1
条件2
0
0.2
0.4
0.6
0.8
1
閾値

図 4.5 閾値の設定

く使われている ICMP echo (Ping) を用いることとする．ICMP echo Request に含まれているデータは，Reply に含まれなければならない [17]．そのため，ICMP echo Request のデータ部に記載された，攻撃者-リフレクタ間の経路情報が，リフレクタにおいて反射された後の ICMP echo Reply に維持される．

図 4.6 を用いて iTrace-PT の DRDoS 攻撃への適用法について説明する．

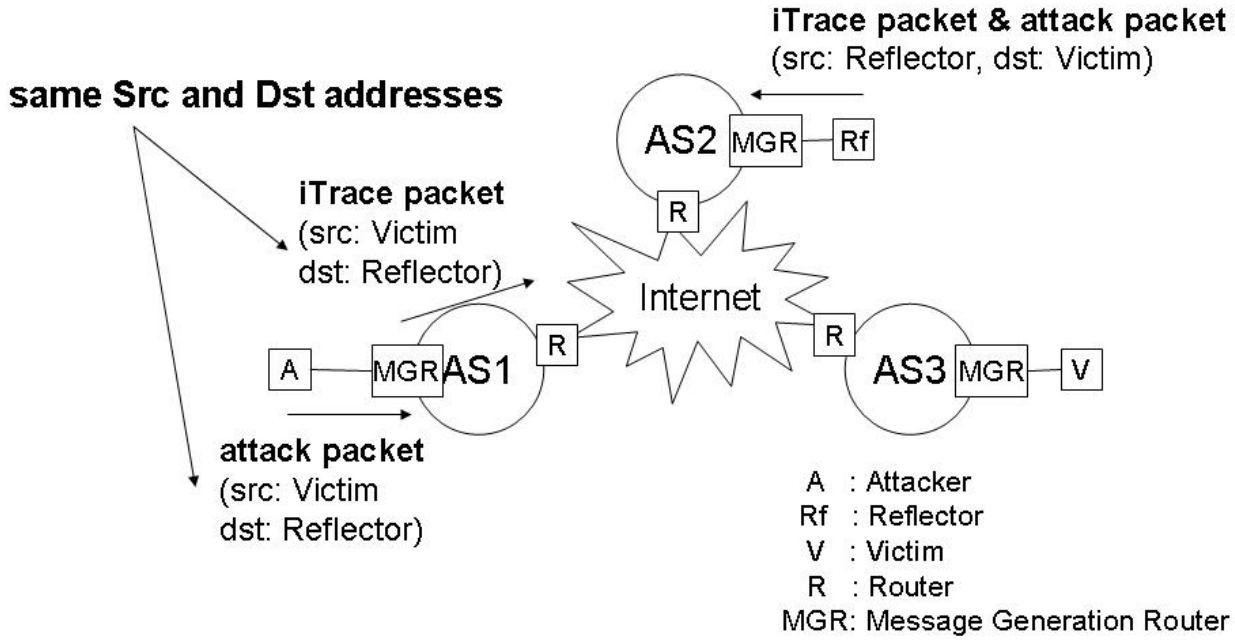

図 4.6 DRDoS 攻撃への適用

パケットが対応ルータである Message Generation Router (MGR) に到着すると，そのパケットと送信元・あて先 IP アドレスが同じである iTrace パケットを確率的に生成し送信する．こうすることにより，攻撃パケットと iTrace パケットは，同じ経路を通り被害者に届くことが期待される．この時，被害者が受け取った iTrace パケットのデータ部には，攻撃者－リフレクタ間とリフレクター被害者間の経路情報が含まれているため，被害者はこの情報により DRDoS 攻撃の真の攻撃元まで特定することができる．

本手法におけるリフレクタの役割は，ICMP echo Request に対して，ICMP echo Reply を返すという通常処理であるため，新たな機能を持つ必要はない．つまり，現時点においても大部分のリフレクタが協力してくれている状態であるといえる．

また，本手法は，攻撃経路中に一つでも対応ルータがあれば，攻撃者の最寄りの対応ルータを特定することが可能なので，対応ルータの数が少ない場合でも有効に機能することが期待される．例えば，図 4.6 において AS1 のみが対応ルータを設置しており，他 AS が設置していない状況でも，AS1 で生成された AS1 の経路情報を持った iTrace パケットのデータは，リフレクタからの応答パケットにおいても維持されるため，被害者は AS1 の攻撃元を特定することが可能である．

第 5 章

シミュレーションによる評価

本章では，前章で提案した iTrace-PT によるネットワークに与える負荷，攻撃元の特定能力，DRDoS 攻撃への適用性に関して，シミュレーションを行った評価結果についてまとめる．なお，本シミュレーションは Bloom Filter のメモリサイズが十分に大きく，衝突は起きないものとして行った．

5.1 ネットワークに与える負荷

本節では，iTrace-PT がネットワークに与える負荷を図 4.3 に示した線形トポロジを用いて，シミュレーション評価を行う．評価値は，攻撃パケットに対する iTrace パケットの割合とする．例えば，攻撃パケット 100 パケットに対して，iTrace パケットが 1 パケット生成されたなら，ネットワークに与える負荷は，1%となる．

図 4.3 に示した線形トポロジにおいて，$n = 20$ とし，iTrace パケットの生成確率を変化させたときの，iTrace-PT がネットワークに与える負荷の変化を図 5.1 に示す．本シミュレーションは，攻撃レートを 100pps，ハッシュクリア間隔を 60 秒とし，1000 回行った．

図 5.1 は iTrace パケットの生成確率を大きくしても，ネットワークに与える負荷はほとんど変わらないということが示されている．これは，iTrace-PT では，iTrace パケットを一度送ったあて先にはハッシュクリアされるまでは再送されないためである．生成確率が 1/5000 以下になると，ハッシュクリア間隔内に，R1 が iTrace パケットを一度も生成しない状況が発生するため，ネットワークへの負荷が低い値となっている．

図 5.2 は，図 4.3 の線形トポロジにおいて中継ルータ数 n を変化させたときのネットワークに対する負荷の変化を理論値とシミュレーションの結果で示している．シミュレーションは，生成確率 1/1000，攻撃レート 100pps，ハッシュクリア間隔 60 秒とし 1000 回行った．

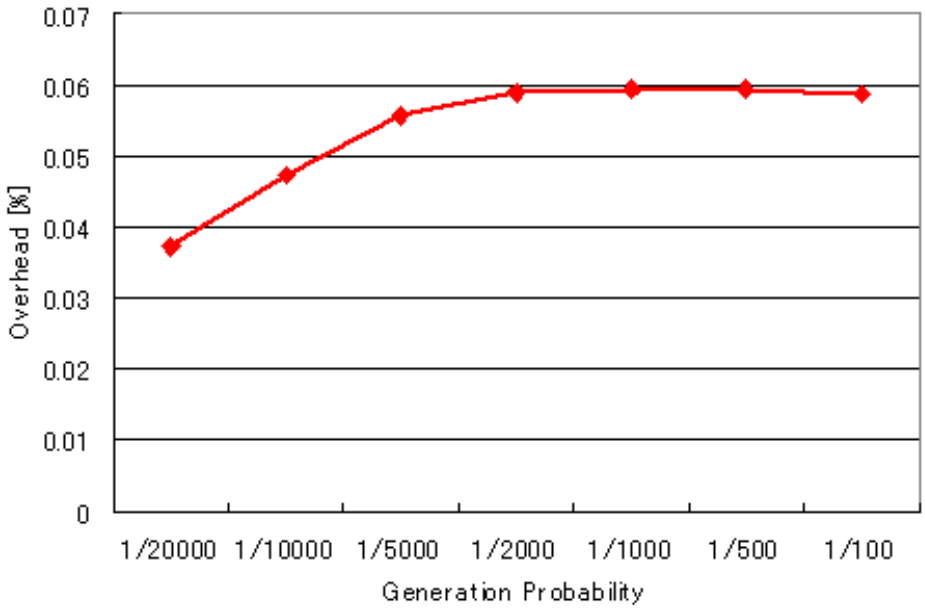

図 5.1 生成確率とネットワークに与える負荷との関係

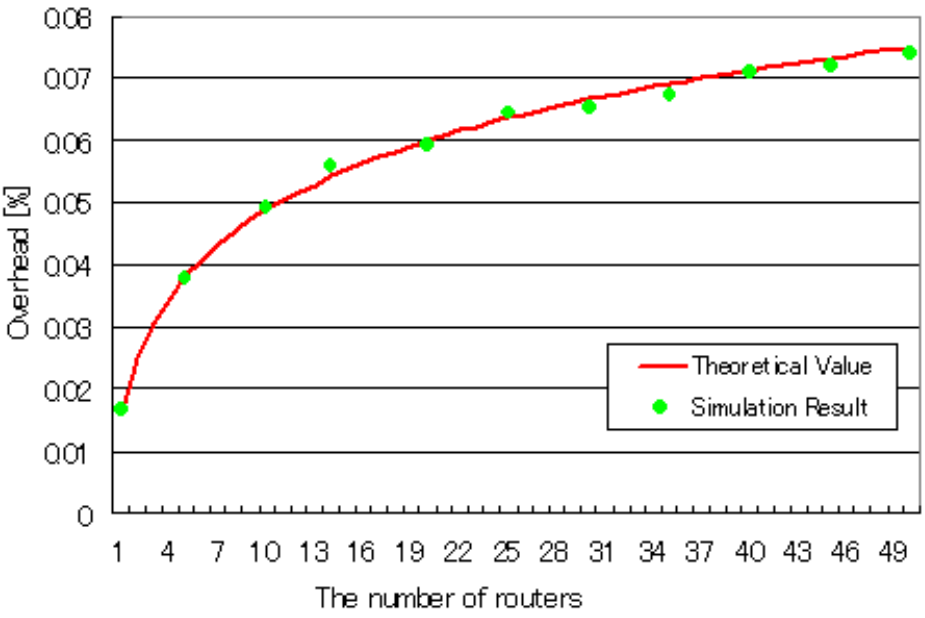

図 5.2 中継ルータ数とネットワークに与える負荷との関係

理論値は，以下のようにして求められる．中継ルータ数 n のとき発生する iTrace パケットの総数の期待値 $A(n)$ は，被害者側から k 番目のルータが最初に iTrace パケットを送ったとすると，iTrace パケットの総数の期待値が，$A(n-k)+1$ となるため，(5.1) 式のように表せる．

$$A(n) = \frac{1}{n}\sum_{k=1}^{n}\{A(n-k)+1\} \tag{5.1}$$

これより，(5.2) 式が導かれる．

$$A(n) = A(n-1) + \frac{1}{n}, \quad A(0) = 0 \tag{5.2}$$

ゆえに，生成確率を p，攻撃レートを f(pps)，ハッシュクリア間隔を t(秒) とすれば，$t > \frac{1}{pf}$ のとき，ネットワークに与える負荷は，$\frac{A(n)}{ft}$ となる．

図 5.2 より，iTrace-PT のネットワークに与える負荷は中継ルータ数に比例することがなく，中継ルータ数が増えても，ネットワークに与える負荷を低く抑えられていることが分かる．

図 5.3 に，図 4.3 に示した線形トポロジにおいて，$n = 20$ とし，攻撃レート f を変化させたときのネットワークに対する負荷の変化をシミュレーションした結果を示す．シミュレーションは，生成確率 1/1000，ハッシュクリア間隔 60 秒とし 1000 回行った．

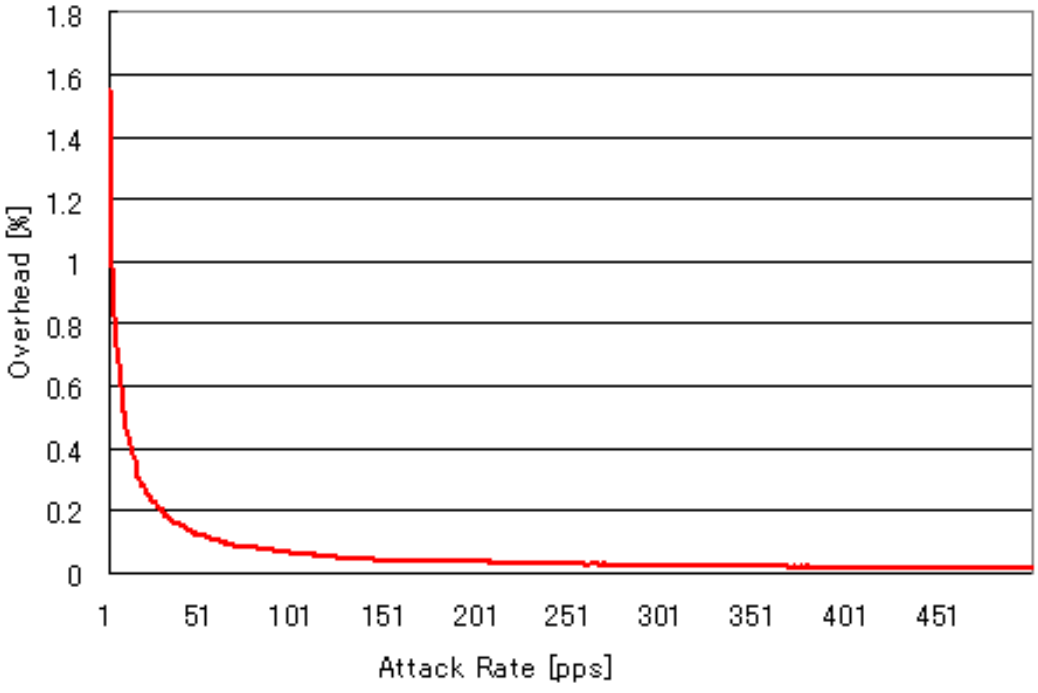

図 5.3 攻撃レートとネットワークに与える負荷との関係

iTrace-PT は，ネットワークに与える負荷を低く抑えるために，各ルータが一度 iTrace パケットを送ったあて先には，一定時間は再送しないという生成方式をとっているが，攻撃レートが低いと，この利点を活かせないため，負荷が高くなっている．負荷の最大値は，生成確

率を p，中継ルータ数を n としたとき，$pn \times 100[\%]$ となる．一方，攻撃レートが高くなると，iTrace-PT の利点が活きてくるため，ネットワークに与える負荷は，低い値で抑えられる．

図 5.4 は，図 4.3 に示した線形トポロジにおいて，$n = 20$ とし，ハッシュクリア間隔 t を変化させたときのネットワークに対する負荷の変化をシミュレーションした結果である．シミュレーションは，攻撃レート 100pps，生成確率 1/1000 とし 1000 回行った．

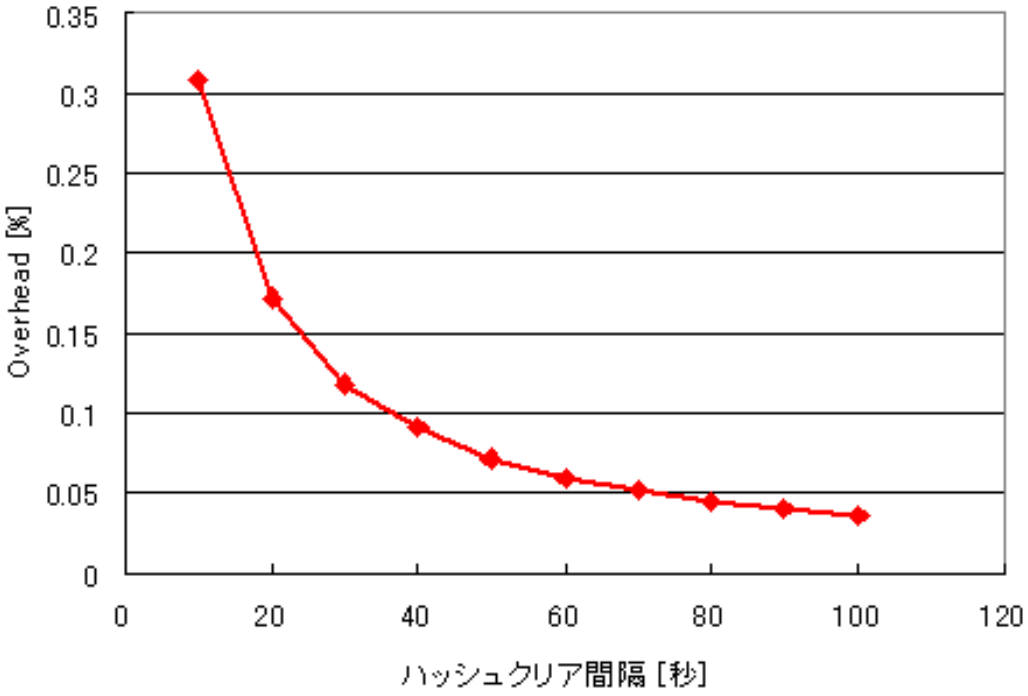

図 5.4 生成クリア間隔とネットワークに与える負荷との関係

先ほどの結果と同様に，ハッシュクリア間隔が短いと，iTrace-PT の利点を活かせないため，負荷が高くなっているが，ハッシュクリア間隔が長くなるにつれ，負荷は低くなっている．

本節では，iTrace-PT によるネットワークに与える負荷をシミュレーションにより評価した．図 5.1 より，iTrace-PT は生成確率を大きくしても，ネットワークに与える負荷を低く抑えることが可能であるが，図 5.3 より，低攻撃レート時の負荷は大きくなるため，適切な値を設定する必要がある．

5.2　攻撃元の特定能力

iTrace-PT の攻撃元特定能力を図 5.5 に示す実ネットワークである，SINET [18] のトポロジを用いて，シミュレーション評価を行う．

評価値は，以下の式で表される False Positive と False Negative である．攻撃者の最寄りルータを攻撃元とし，それ以外は攻撃元でないとする．False Positive は，攻撃元でない場所を攻撃元と判断してしまう誤検出を表し，False Negative は，攻撃者の検出漏れを表す．

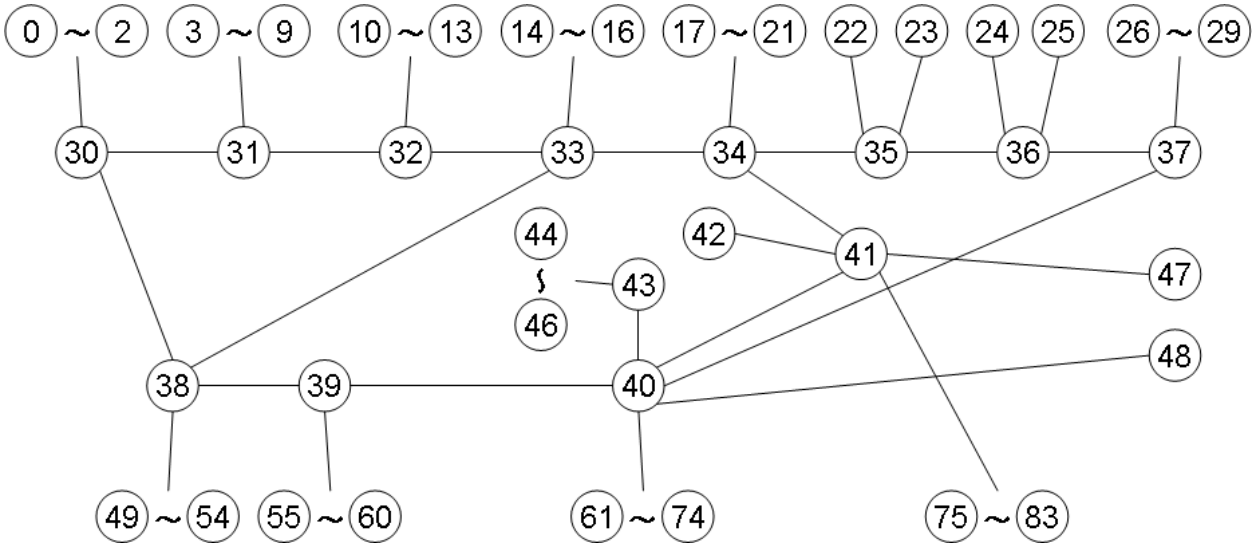

図 5.5 SINET

$$FalsePositive = \frac{\text{特定した中で攻撃元でないノード数}}{\text{攻撃元と特定したノード数}}$$

$$FalseNegative = \frac{\text{特定できなかった攻撃元の数}}{\text{検出すべき攻撃元の数}}$$

以降，シミュレーションは，生成確率を 1/1000，ハッシュクリア間隔を 60 秒として，100 回行っている．

まず最初に，被害者が攻撃レートを知っており，正当な通信者がいないという理想環境において，図 5.5 のトポロジで，攻撃者が広く分散しているワーストケースを考え，0, 14, 29, 44, 49 に 5 人配置し，被害者を 83 に配置し以下のシミュレーションを行う．

シミュレーション 1：

全攻撃者は，50pps で攻撃を行っており，被害者が次の条件を設定し，前章の閾値設定法を基に，閾値を 0.9 とした．

- 条件：50pps 以上で攻撃を行っている攻撃者を，10 回目のハッシュクリア時に，90%以上特定したい．

シミュレーション 2：

全攻撃者は，10pps で攻撃を行っており，被害者が次の条件を設定し，前章の閾値設定法を基に，閾値を 0.25 とした．

- 条件：10pps 以上で攻撃を行っている攻撃者を，15 回目のハッシュクリア時に，90%以上特定したい．

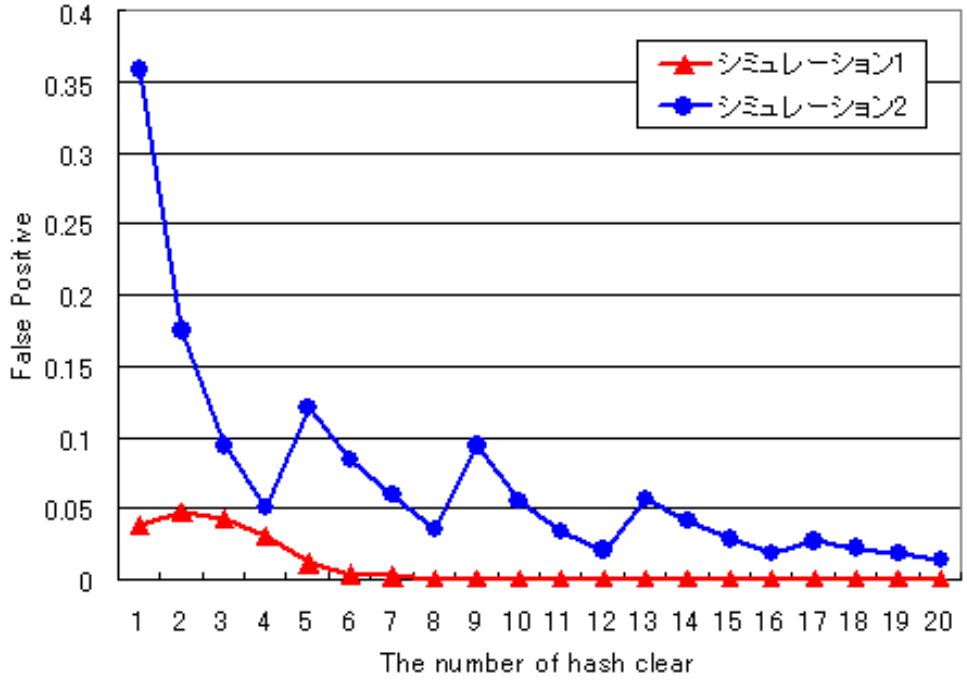

図 5.6 理想環境における False Positive

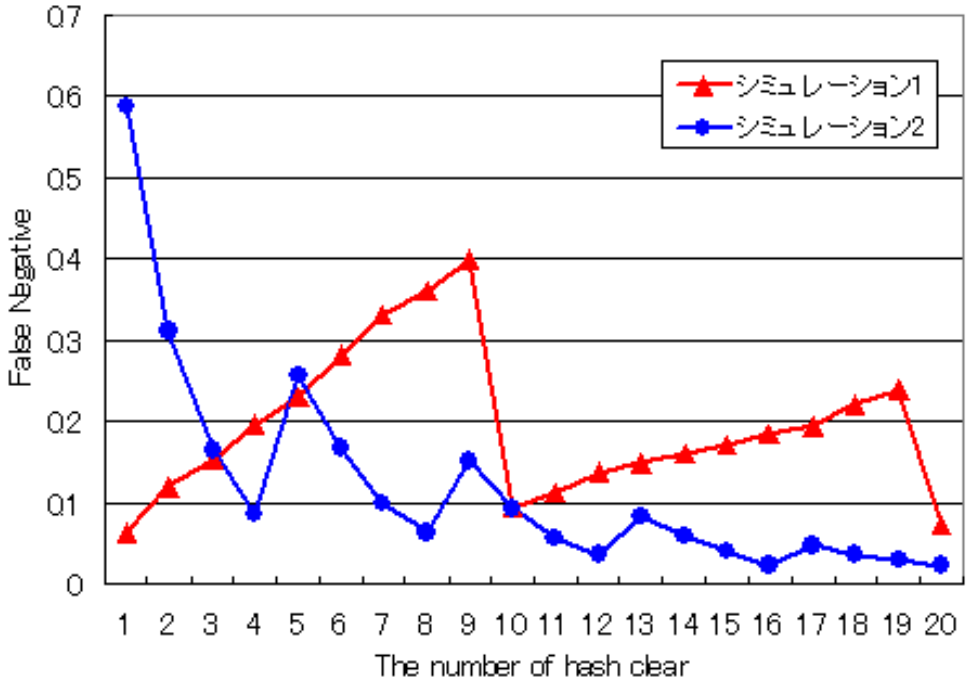

図 5.7 理想環境における False Negative

図 5.6，図 5.7 にそれぞれのシミュレーション結果を示す．

図 5.6，図 5.7 において，シミュレーション 1 の結果を見ると，被害者の希望通り，10 回目のハッシュクリア時に，90%以上の攻撃者を特定できており，誤検出がないことが分かる．

一方，シミュレーション 2 の結果では，被害者の希望通り，15 回目のハッシュクリア時に，90%以上の攻撃者を特定できているが，誤検出が 3%ほどあることが分かる．これは，シミュレーション 2 では，攻撃レートが 10pps と低いため，ハッシュクリア間隔内に，攻撃者の最寄りルータが iTrace パケットを生成する確率が低いためである．

続いて，正当な通信者がいないという環境は残し，被害者が攻撃レートを知らないという状況であるシミュレーション 3 を行う．攻撃者，被害者の配置場所は同じとする．

シミュレーション 3：

攻撃者は，攻撃開始時，1pps〜100pps の範囲でランダムに攻撃レートを設定する．被害者は次の条件を設定し，前章の閾値設定法を基に，閾値を 0.25 とした．

- 条件：10pps 以上で攻撃を行っている攻撃者を，15 回目のハッシュクリア時に，90%以上特定したい．

図 5.8，図 5.9 にシミュレーション 3 の結果を示す．

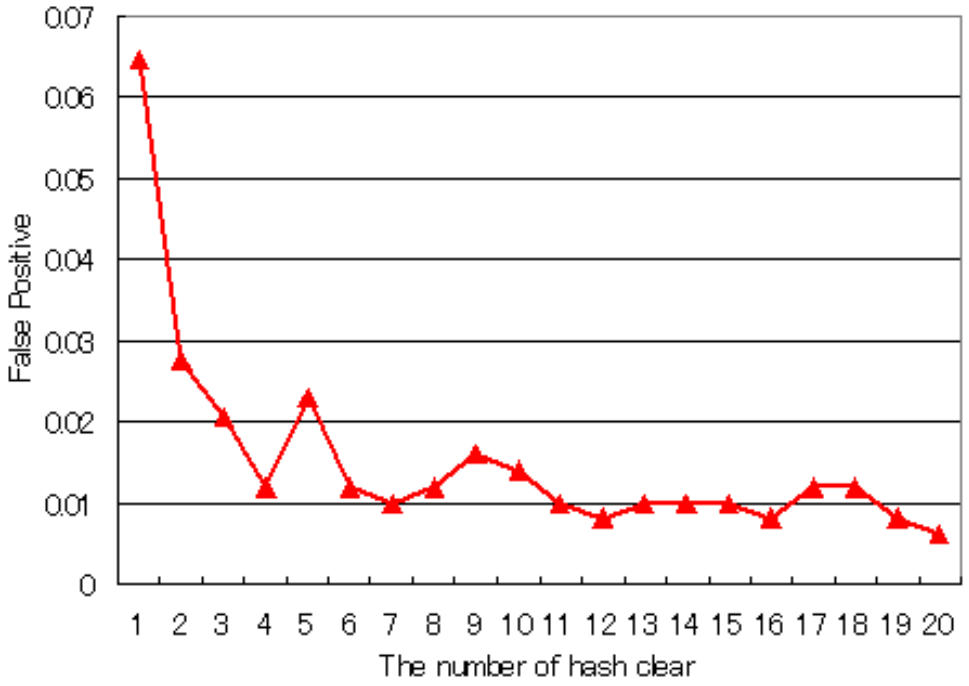

図 5.8 攻撃レートがランダム時の False Positive

図 5.9 において，ハッシュクリア 15 回目を見ると，0.05 となっており，被害者の希望通り，90%以上の攻撃者を特定できている．一方，図 5.8 の誤検出を見ると 1%程度であることが分

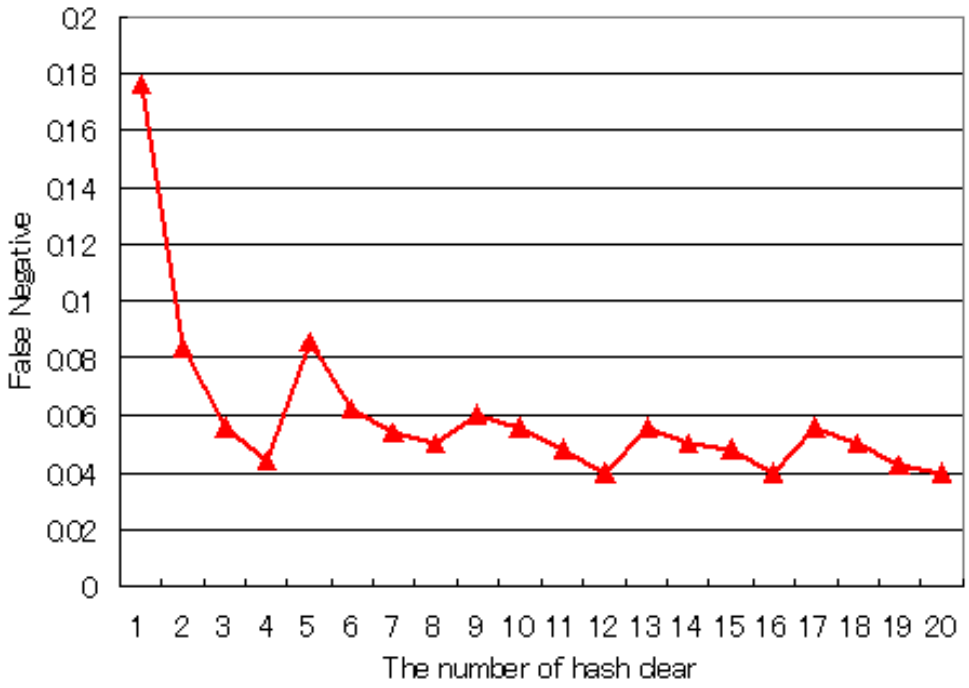

図 5.9 攻撃レートがランダム時の False Negative

かる．この誤検出は，シミュレーション 2 の理由に加えて，攻撃者が 10pps よりも低い攻撃レートを設定したときに生じたものだと考えられる．これらの図より，被害者が攻撃レートを知らない状況においても，提案手法が有効に機能することが示せた．

次に，正当な通信者が存在する現実的な環境においてシミュレーションを行う．攻撃者は，シミュレーション 3 と同様に，攻撃開始時，1pps〜100pps の範囲でランダムに攻撃レートを設定する．ここで正当な通信者の定義を行う．

正当な通信者は，平均到着率 λ (人/s) のポアソン分布に従って現れ，通信レート f_N (pps) で最大 T_N 秒間の通信を行う．現れる場所は，リーフノードからランダムに選ぶ．

シミュレーション 4，5，6 では，平均到着率 λ をハッシュクリア間隔に平均一人来ることを想定して，1/60 (人/s)，最大通信時間 T_N を 100 秒とし，通信レート f_N の変化が提案手法に与える影響をシミュレーションする．

シミュレーション 4：

正当ユーザの通信レート f_N を，50pps とする．被害者は次の条件を設定し，前章の閾値設定法を基に，閾値を 0.25 とした．

- 条件：10pps 以上で攻撃を行っている攻撃者を，15 回目のハッシュクリア時に，90%以上特定したい．

シミュレーション 5：
正当ユーザの通信レート f_N を，100pps とする．被害者は次の条件を設定し，前章の閾値設定法を基に，閾値を 0.25 とした．

- 条件：10pps 以上で攻撃を行っている攻撃者を，15 回目のハッシュクリア時に，90%以上特定したい．

シミュレーション 6：
正当ユーザの通信レート f_N を，150pps とする．この値は，攻撃者の通信が正当ユーザの通信にまぎれるワーストケースである．被害者は次の条件を設定し，前章の閾値設定法を基に，閾値を 0.25 とした．

- 条件：10pps 以上で攻撃を行っている攻撃者を，15 回目のハッシュクリア時に，90%以上特定したい．

図 5.10，図 5.11 にそれぞれのシミュレーション結果を示す．

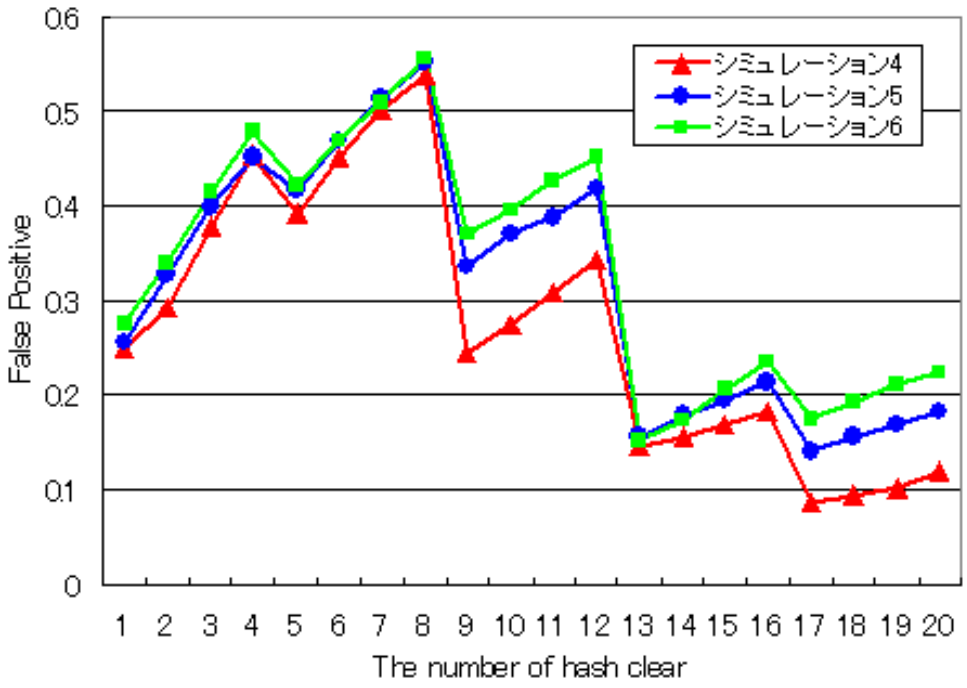

図 5.10 通信レートの変化の影響 (False Positive)

図 5.11 より，どのシミュレーションも 15 回目のハッシュクリア時に，90%以上の攻撃元を特定できている．一方，図 5.10 より，誤検出は 15 から 20%ほど生じ，正当ユーザの存在が影響していることが分かる．これは，同じルータ配下に，複数の正当ユーザが到着し，そこからの通信が長くなってしまっていることによると考えられる．正当ユーザの通信レートが低いほうが，誤検出が低い値となっているが，これは，通信レートが低ければ，生成される iTrace パケットの数が少なくなるためである．

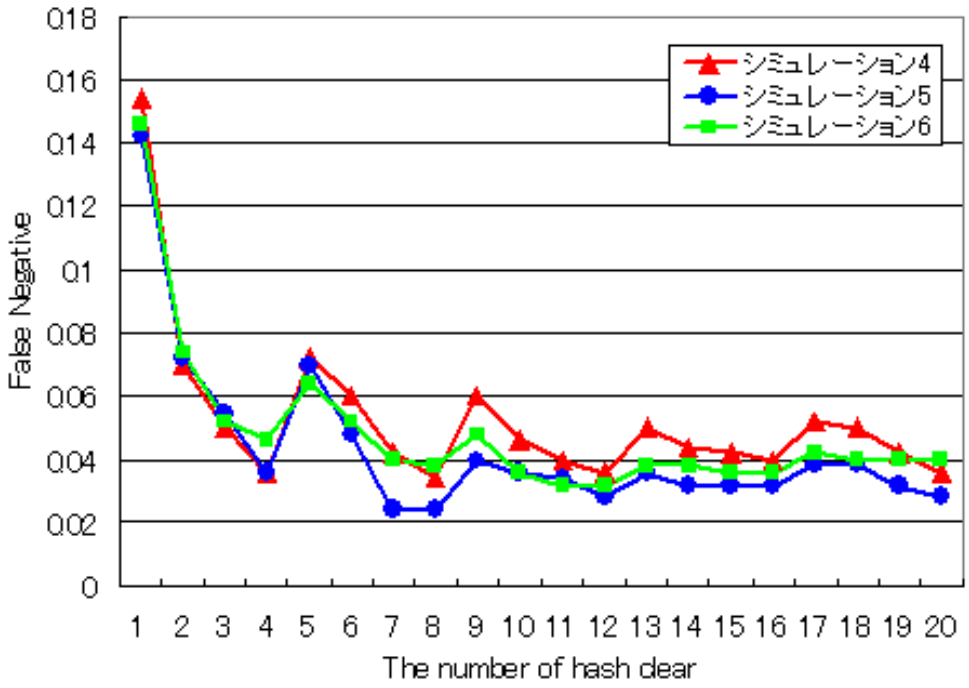

図 5.11 通信レートの変化の影響 (False Negative)

図 5.10，図 5.11 より，正当ユーザの通信レートの変化は，結果にあまり大きく影響しないことが分かる．これは，iTrace-PT は，通信の持続時間に基づいて攻撃元の特定を行っているためである．

シミュレーション 7，8，9 では，最大通信時間 T_N を 100 秒，通信レート f_N を攻撃者の通信が正当ユーザの通信にまぎれるワーストケースである 150pps とし，平均到着率 λ の変化が提案手法に与える影響をシミュレーションする．

シミュレーション 7：
正当ユーザの平均到着率 λ を 1/120 (人/s) とする．被害者は次の条件を設定し，前章の閾値設定法を基に，閾値を 0.25 とした．

- 条件：10pps 以上で攻撃を行っている攻撃者を，15 回目のハッシュクリア時に，90%以上特定したい．

シミュレーション 8：
正当ユーザの平均到着率 λ を 1/30 (人/s) とする．被害者は次の条件を設定し，前章の閾値設定法を基に，閾値を 0.25 とした．

- 条件：10pps 以上で攻撃を行っている攻撃者を，15 回目のハッシュクリア時に，90%以上特定したい．

シミュレーション 9：
正当ユーザの平均到着率 λ を 1/10 (人/s) とする．被害者は次の条件を設定し，前章の閾値設定法を基に，閾値を 0.25 とした．

- 条件：10pps 以上で攻撃を行っている攻撃者を，15 回目のハッシュクリア時に，90%以上特定したい．

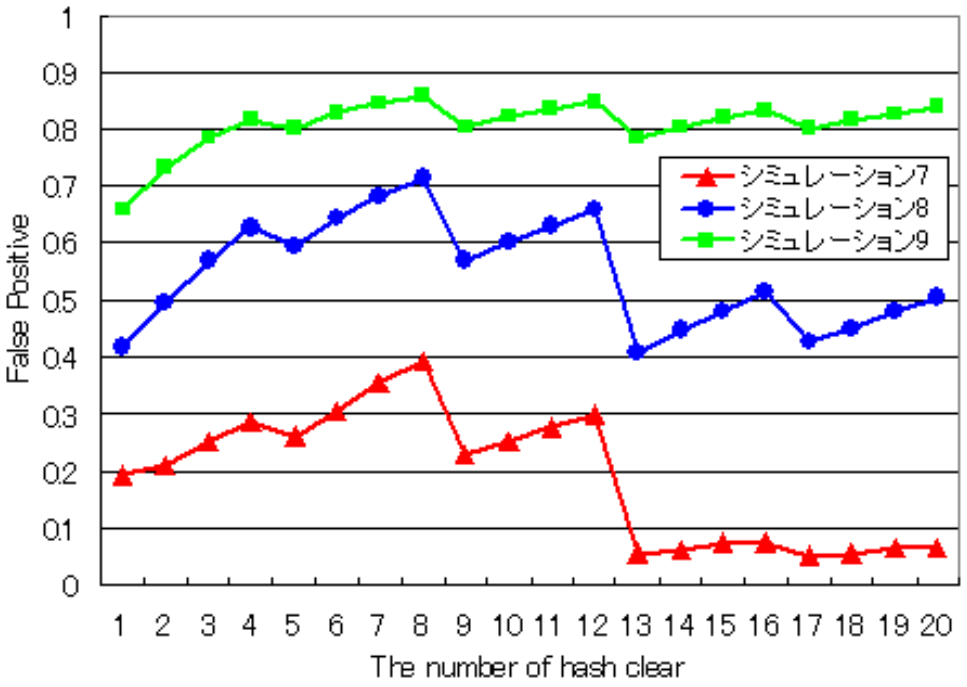

図 5.12 平均到着率の変化の影響 (False Positive)

図 5.13 より，すべて 15 回目のハッシュクリア時に，90%以上の攻撃元を特定できている．しかし，図 5.12 の結果を見ると，平均到着率が高いシミュレーション 8, 9 では，15 回目のハッシュクリア時，それぞれ 48%, 82%の誤検出を生じており，多くの正当ユーザを誤検出してしまっている．これは，平均到着率が高いために，同じルータ配下に，複数の正当ユーザが到着する事態が多く発生し，そこからの通信が長くなってしまっていることによると考えられる．

シミュレーション 10〜15 では，平均到着率 λ を 1/60 (人/s)，通信レート f_N を攻撃者の通信が正当ユーザの通信にまぎれるワーストケースである 150pps とし，誤った閾値の設定が与える影響と最大通信時間 T_N の変化が提案手法に与える影響をシミュレーションする．

シミュレーション 10：
正当ユーザの最大通信時間 T_N を 100 秒とする．被害者は次の条件を設定し，前章の閾値設定法を基に，閾値を 0.53 とした．

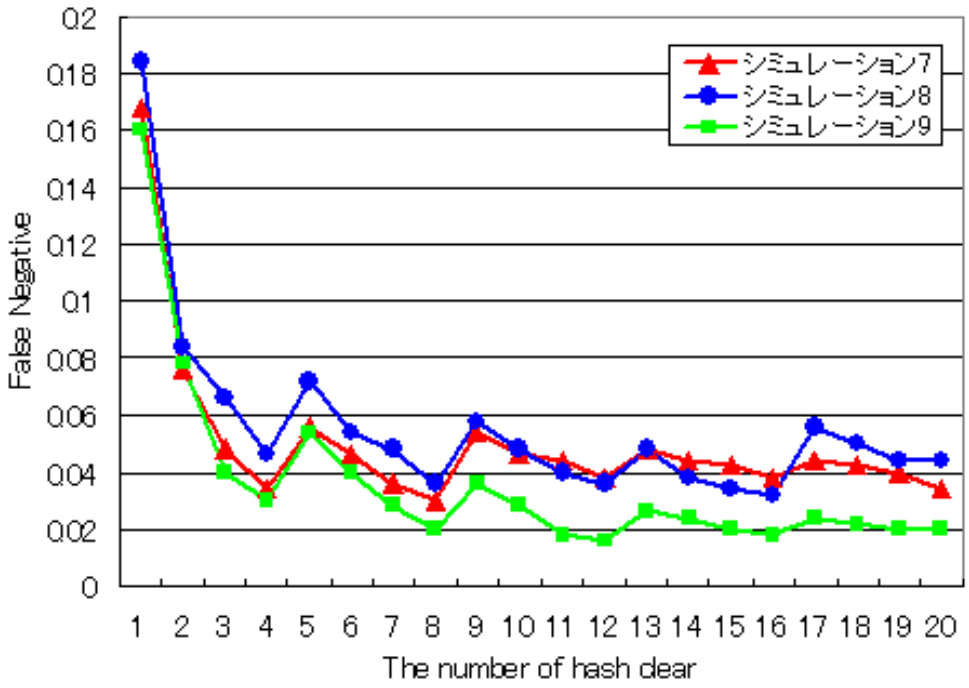

図 5.13 平均到着率の変化の影響 (False Negative)

- 条件：20pps 以上で攻撃を行っている攻撃者を，15 回目のハッシュクリア時に，90%以上特定したい．

シミュレーション 11：

正当ユーザの最大通信時間 T_N を 300 秒とする．被害者は次の条件を設定し，前章の閾値設定法を基に，閾値を 0.53 とした．

- 条件：20pps 以上で攻撃を行っている攻撃者を，15 回目のハッシュクリア時に，90%以上特定したい．

シミュレーション 12：

正当ユーザの最大通信時間 T_N を 600 秒とする．被害者は次の条件を設定し，前章の閾値設定法を基に，閾値を 0.53 とした．この値を用いると，前章で示した (4.3) 式から，ハッシュクリア 21 回目以降に特定を行わなければならないため，適切な値ではないが，その影響を調べるために用いる．

- 条件：20pps 以上で攻撃を行っている攻撃者を，15 回目のハッシュクリア時に，90%以上特定したい．

図 5.15 より，15 回目のハッシュクリア時を見ると，若干ではあるが，90%以上の攻撃元の特定ができていない．これは，20pps よりも低い攻撃レートを設定した攻撃者の特定ができなかったことによると考えられる．また，シミュレーション 11, 12 では，攻撃者と同じルー

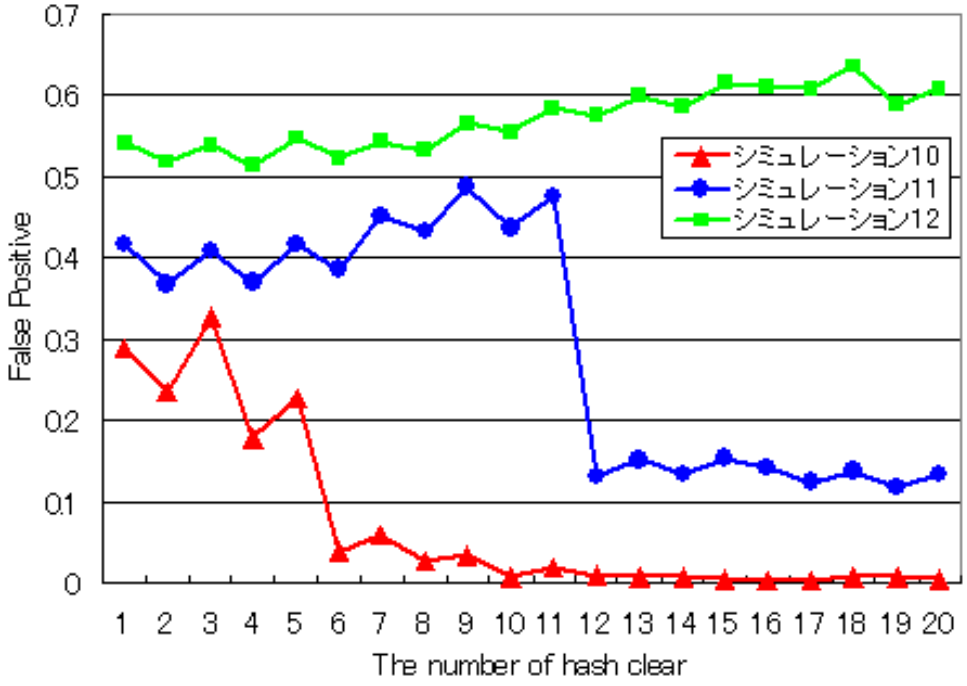

図 5.14 誤った閾値の設定が与える影響 (False Positive)

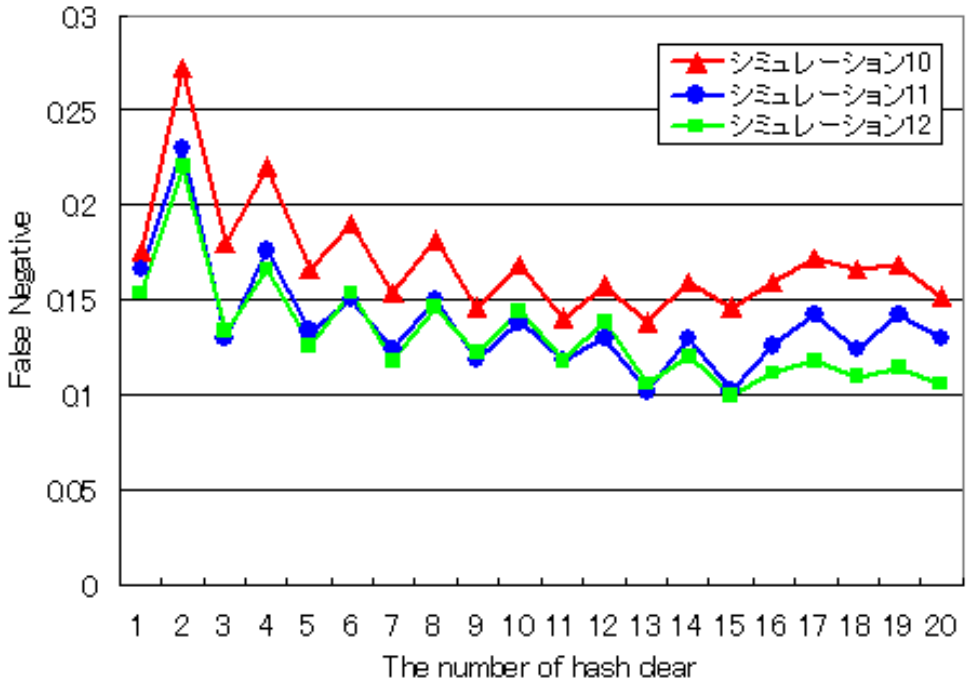

図 5.15 誤った閾値の設定が与える影響 (False Negative)

タ配下から正当ユーザの通信が始まり，見かけ上，攻撃レートが大きくなったため，検出漏れが少なくなっているのだと考えられる．

また，図 5.14 の結果を見ると，最大通信時間が長いシミュレーション 11, 12 では，15 回目のハッシュクリア時，それぞれ 15%, 61%の誤検出を生じている．シミュレーション 11 においては，同じルータ配下に，複数の正当ユーザが到着する事態が発生し，そこからの通信が長くなってしまったことによる誤検出であると考えられる．シミュレーション 12 では，この原因にあわせて，閾値の設定を誤っていることにより，誤検出が多く生じている．そこで，シミュレーション 13, 14, 15 では，正しい閾値を設定して，シミュレーションを行う．

シミュレーション 13, 14, 15：

被害者は次の条件を設定し，前章の閾値設定法を基に，閾値を 0.8 とした．他の条件は，それぞれシミュレーション 10, 11, 12 と同様である．

- 条件：40pps 以上で攻撃を行っている攻撃者を，15 回目のハッシュクリア時に，90%以上特定したい．

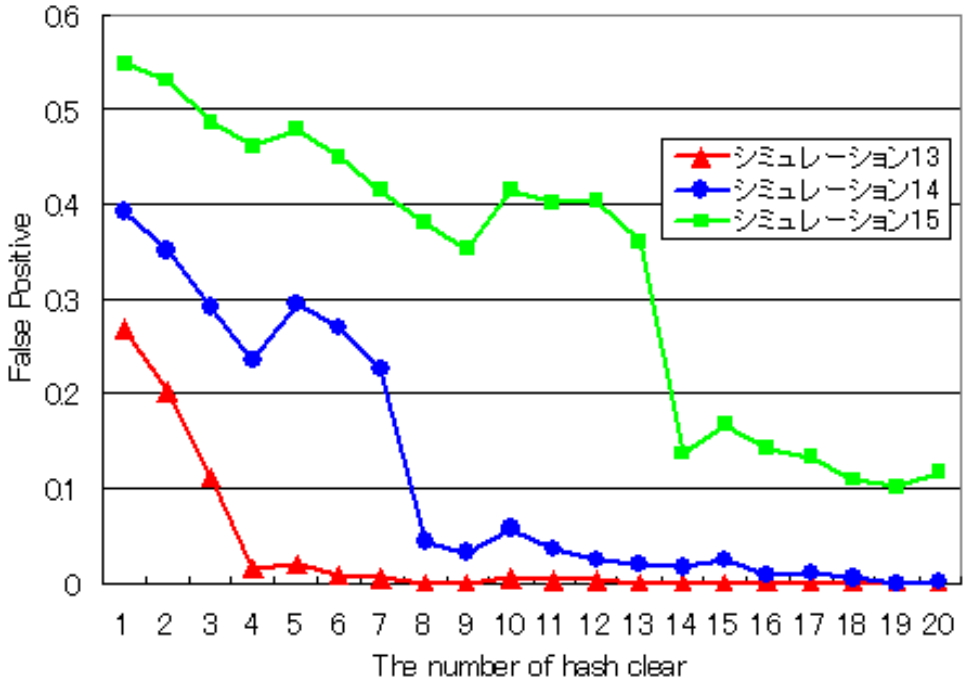

図 5.16 最大通信時間の変化の影響 (False Positive)

図 5.17 の 15 回目のハッシュクリア時を見ると，22%ほどの検出漏れが生じていることが分かる．これは，40pps よりも低い攻撃レートを設定した攻撃者の特定ができなかったことによると考えられる．

一方，図 5.16 の結果を見ると，15 回目のハッシュクリア時，シミュレーション 15 では，17%ほどの誤検出を生じている．この原因は前と同様で，同じルータ配下に，複数の正当ユー

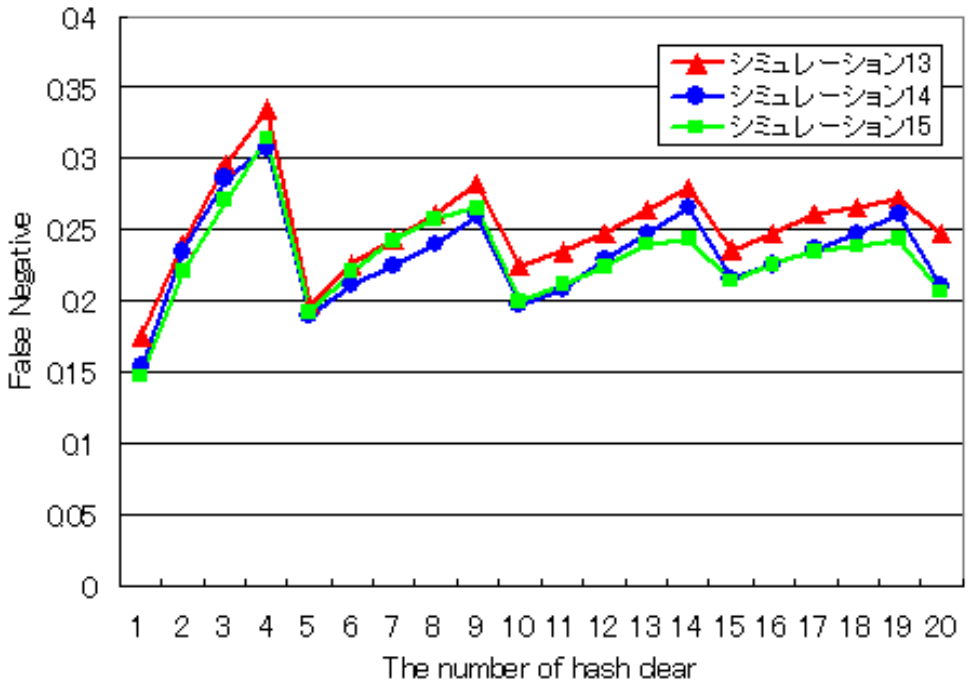

図 5.17 最大通信時間の変化の影響 (False Negative)

ザが到着する事態が発生し，そこからの通信が長くなってしまったことによると考えられる．

今までのシミュレーションで見てきたように，iTrace-PT は，平均到着率が高いときと最大通信時間が長いときに性能が落ちている．その原因は，同じルータ配下に，複数の正当ユーザが到着する事態が発生し，そこからの通信が長くなってしまったことにあると考えられる．

この考えの正当性を示すために，同じルータ配下に複数の正当ユーザが到着する確率が低くなるよう，ネットワークの規模を大きくしたトポロジで，同様のシミュレーションを行う．トポロジは，トポロジー生成ツール BRITE [19] で作成し，ルータ数を 1000 とした．

シミュレーション 16, 17, 18：

シミュレーション 7, 8, 9 を，BRITE によって生成したトポロジ上でシミュレーションを行う．

図 5.18 の結果を見ると，シミュレーション 17, 18 では，15 回目のハッシュクリア時，それぞれ 17%, 64%の誤検出となっており，シミュレーション 8, 9 における誤検出の値から大きく改善していることが分かる．しかし，シミュレーション 18 では，いまだに誤検出が 64%と非常に大きいため，閾値を高くし，誤検出を低く抑える必要がある．

また，図 5.19 より，BRITE によるトポロジにおいても，15 回目のハッシュクリア時に，90%以上の攻撃元を特定できていることが分かる．

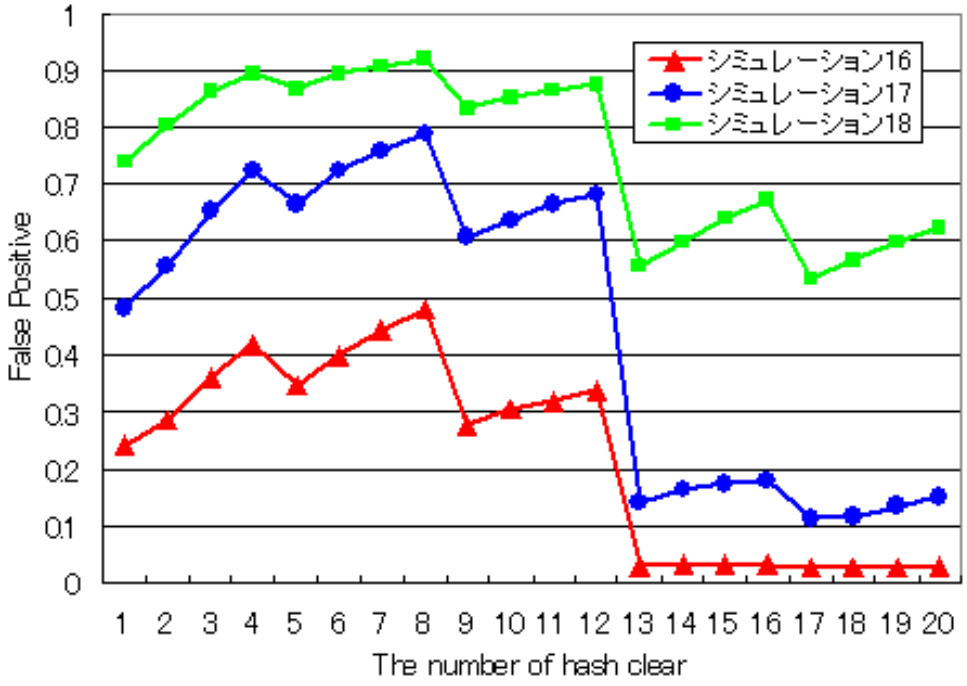

図 5.18 BRITE によるトポロジでの平均到着率の変化の影響 (False Positive)

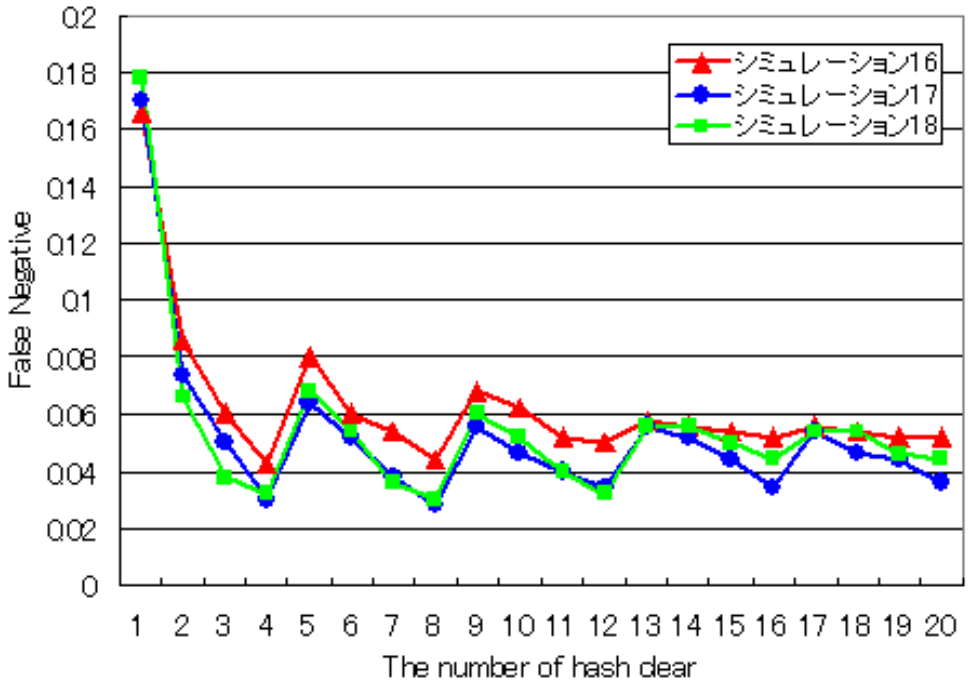

図 5.19 BRITE によるトポロジでの平均到着率の変化の影響 (False Negative)

シミュレーション 19, 20, 21：
シミュレーション 13, 14, 15 を，BRITE によって生成したトポロジ上でシミュレーションを行う．

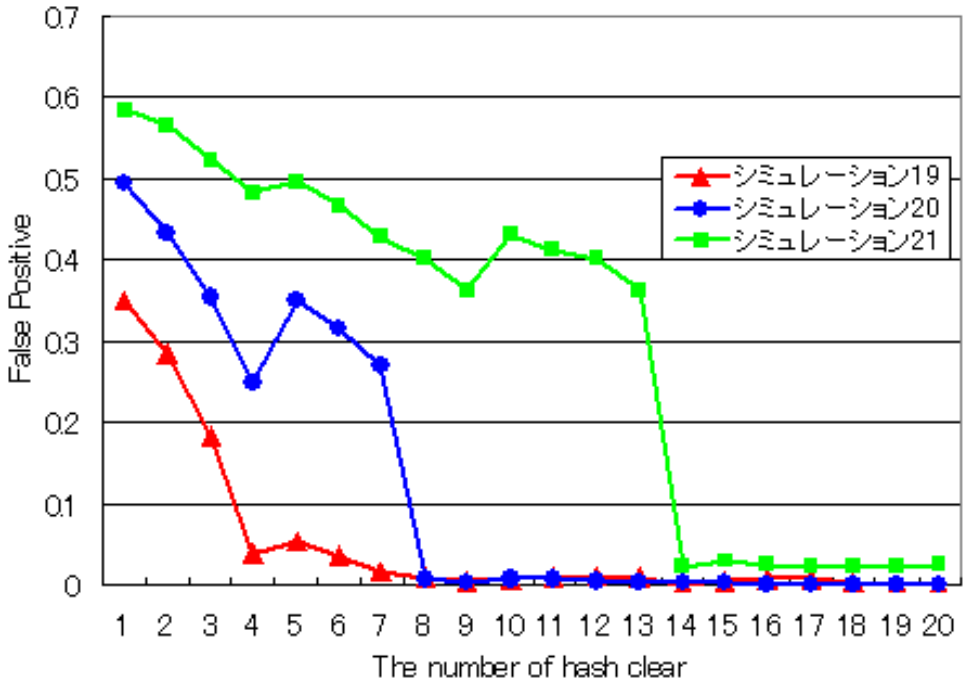

図 5.20 BRITE によるトポロジでの最大通信時間の変化の影響 (False Positive)

図 5.20 の結果を見ると，全てのシミュレーションにおいて，15 回目のハッシュクリア時，誤検出を低く抑えることができており，シミュレーション 15 における誤検出の値を大きく改善していることが分かる．また，図 5.21 より，BRITE によるトポロジにおいても，False Negative の値はシミュレーション 13, 14, 15 と同等の値となっていることが分かる．

シミュレーション 22, 23, 24 では，シミュレーション 16, 17, 18 における誤検出を低く抑えるために，閾値を高く設定してシミュレーションする．

シミュレーション 22, 23, 24：
被害者は次の条件を設定し，前章の閾値設定法を基に，閾値を 0.53 とした．他の条件は，それぞれシミュレーション 16, 17, 18 と同様である．

- 条件：20pps 以上で攻撃を行っている攻撃者を，15 回目のハッシュクリア時に，90%以上特定したい．

図 5.22 の結果を見ると，全てのシミュレーションにおいて，15 回目のハッシュクリア時，誤検出を低く抑えることができている．しかし，閾値をシミュレーション 16, 17, 18 よりも

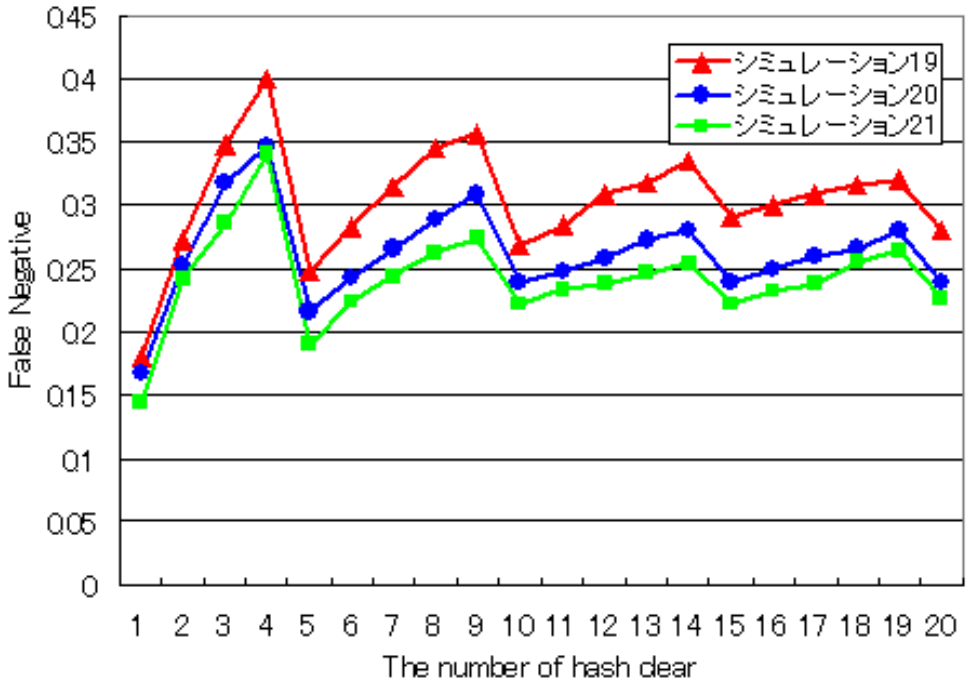

図 5.21 BRITE によるトポロジでの最大通信時間の変化の影響 (False Negative)

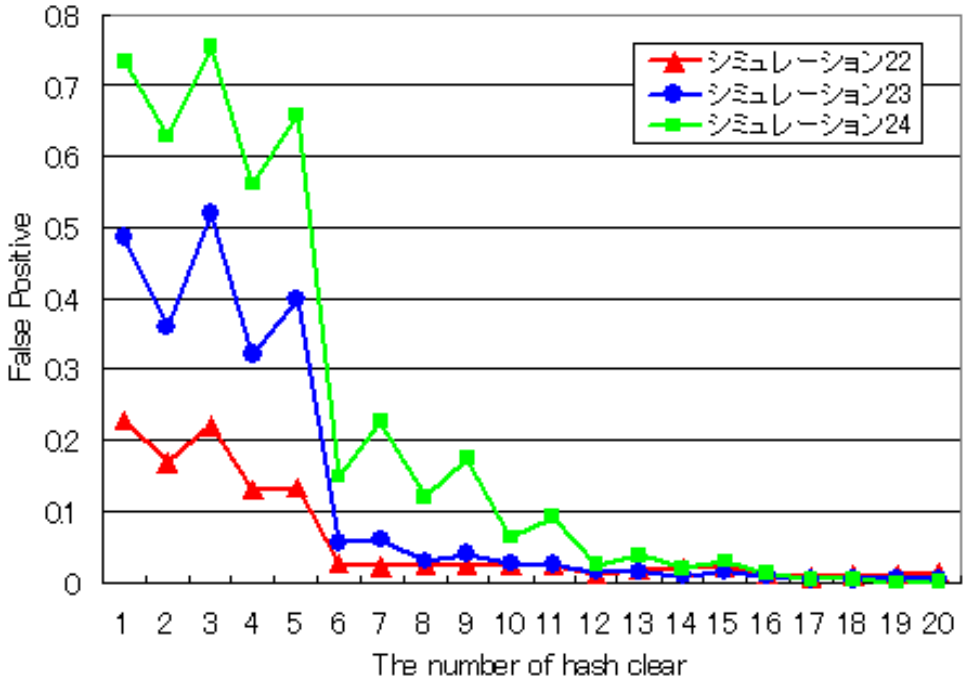

図 5.22 閾値を高く設定することによる効果 (False Positive)

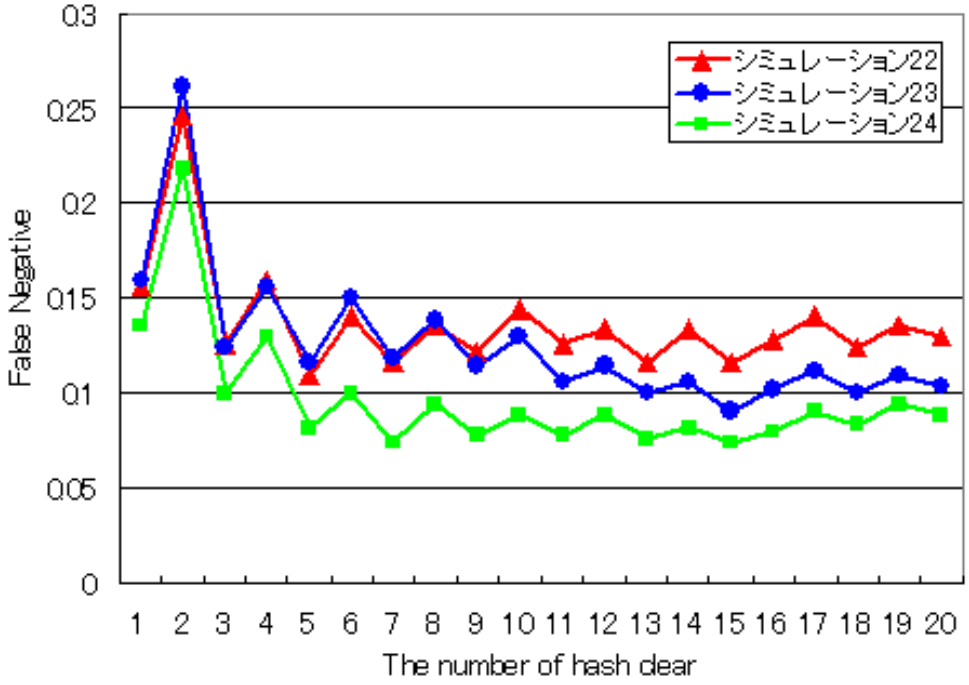

図 5.23 閾値を高く設定することによる効果 (False Negative)

高く設定したため，図 5.23 にあるように，False Negative の値は大きくなっている．

本節では，iTrace-PT の攻撃元特定能力をシミュレーションにより評価した．同じルータ配下に，複数の正当ユーザが到着する事態が発生しないような状況において，提案手法は，攻撃者の通信が正当ユーザにまぎれるほど低い通信レートであっても，攻撃者のみの特定が可能であることを明らかにした．

5.3　DRDoS 攻撃への効果

r-iTrace, iCaddie, iTrace-PT の 3 手法に関して，ルータの対応率が攻撃元の特定能力に与える影響を，シミュレーションによって評価した．

ルータの総数を M，対応率を γ $(0 \leq \gamma \leq 1)$ としたとき，$\lfloor \gamma M \rfloor$ 個を対応ルータとして，ランダムに配置する．評価値は，攻撃元の特定能力を調べるため，False Negative (検出漏れ) とした．ここでの検出すべき攻撃元は，攻撃者に最も近い対応ルータとする．例えば，図 5.24 では，R2 が検出すべき攻撃元である．

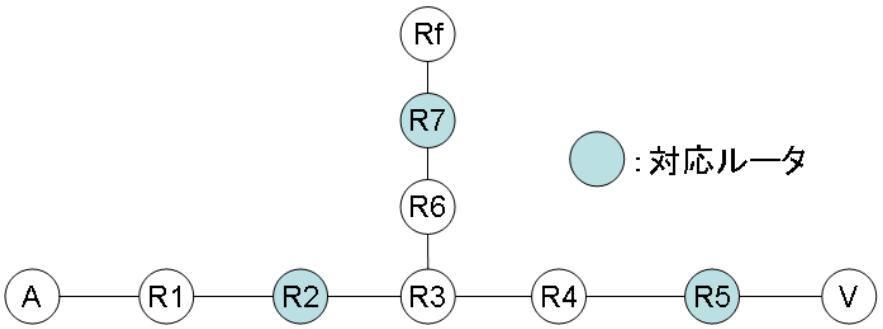

図 5.24 検出すべき攻撃元

図 5.26 は，図 5.25 の単純なトポロジで行ったシミュレーション結果と r-iTrace, iCaddie の理論値を示している．シミュレーションは，各 γ 毎に 1000 回行い，1 回ごとに対応ルータの配置を変えた．

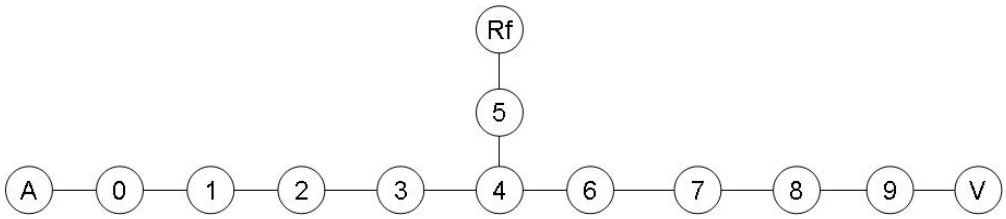

図 5.25 単純なトポロジ

r-iTrace では，被害者から攻撃元までの全ルータが対応ルータの時に攻撃元を特定できる．よって，y を対応ルータの数として，図 5.25 のトポロジにおける r-iTrace の False Negative の理論値 $FN_1(y)$ は，以下のように表せる．

$$FN_1(y) = \begin{cases} 1 & (y = 0) \\ 1 - \frac{1}{{}_{10}C_y} & (y \geq 1) \end{cases} \tag{5.3}$$

iCaddie は，Traceback Request を受けたルータが，攻撃者-リフレクタ間の経路情報を持った iTrace パケットを受け取ることができれば，攻撃元を特定できる．図 5.25 のトポロジでは，ルータ 4 またはルータ 5 が対応ルータであれば攻撃元を特定できる．y を対応ルータの

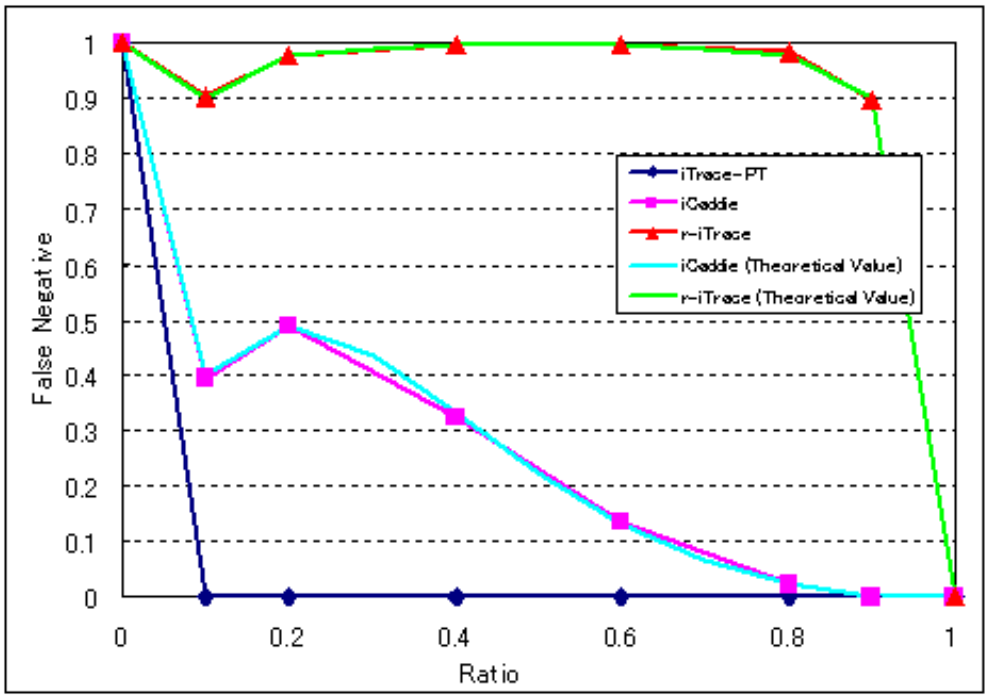

図 5.26 単純なトポロジにおける False Negative

数として，図 5.25 のトポロジにおける iCaddie の False Negative の理論値 $FN_2(y)$ は，以下のように表せる．

$$FN_2(y) = \begin{cases} 1 & (y = 0) \\ \frac{2}{5} & (y = 1) \\ 1 - \frac{{}_4C_y + 2 \cdot {}_8C_{y-1} + {}_8C_{y-2}}{{}_{10}C_y} & (2 \leq y \leq 4) \\ 1 - \frac{2 \cdot {}_8C_{y-1} + {}_8C_{y-2}}{{}_{10}C_y} & (5 \leq y \leq 9) \\ 0 & (y = 10) \end{cases} \tag{5.4}$$

図 5.26 より，提案手法は $\gamma = 0.1$，つまり攻撃経路中にひとつでも対応ルータがあれば攻撃元を特定できることが示されている．一方 r-iTrace は，90%のルータが対応していたとしても，ほとんど攻撃元を特定できない．また，iCaddie は，対応率が 0.8 以下になると性能が落ちている．これは，図 5.25 のトポロジにおいて，ルータ 4, 5 に対応ルータが配置されなかったことによる．

続いて実ネットワークにおいて，提案手法が有効に機能するか調べるため，図 5.5 で示した SINET をトポロジに用いてシミュレーションを行った．

攻撃者をルータ 0，被害者をルータ 29 の下に配置し，攻撃者が 1 つのリフレクタ (ルータ 83 の下に配置) を使ったときの，ルータの対応率と False Negative の関係グラフを図 5.27 に示す．

図 5.27 は，ルータの対応率が 0.4 以下になると提案手法においても，攻撃元を特定できないケースがあることが示されている．これは，攻撃経路中に一つも対応ルータが存在しない

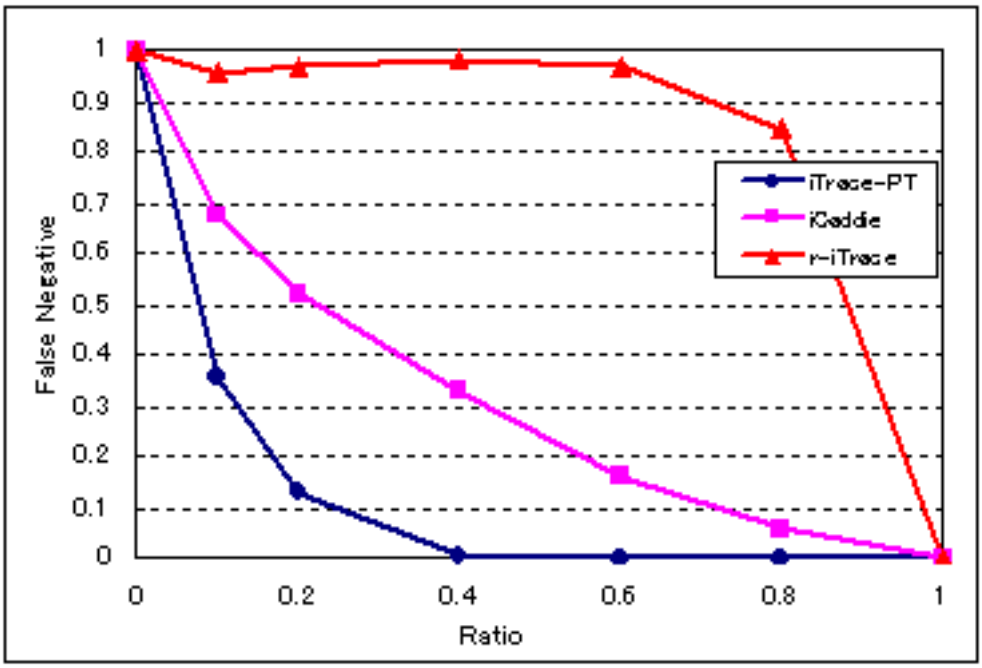

図 5.27 SINET における False Negative (1 つのリフレクタ)

ケースがあることを意味している．しかし，対応率が 0.4 以上になると攻撃経路中に少なくとも一つは対応ルータが配置されるようになり，攻撃元を特定できている．

続いて，図 5.28，図 5.29 に攻撃者が 3 つのリフレクタ (ルータ 83, 22, 42 の下に配置) を使ったとき，攻撃者が 5 つのリフレクタ (ルータ 83, 22, 42, 44, 49 の下に配置) を使ったときの結果をそれぞれ示す．

これらの図より，提案手法は，攻撃者が用いるリフレクタの数に依存せず，SINET において，ルータの対応率が 0.4 以上であれば攻撃元を特定できていることが分かる．一方，r-iTrace と iCaddie は，攻撃者が用いるリフレクタの数が増えると，False Negative の値が減少していることが見て取れる．これは，攻撃経路が分散することで，攻撃元を特定できる経路が含まれる確率が上がることによる．

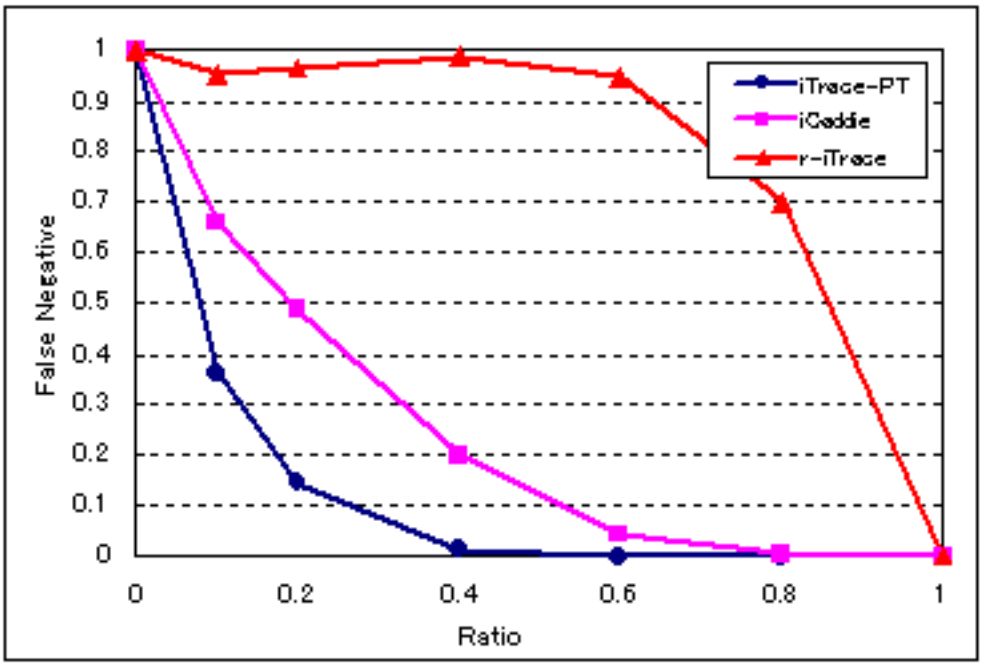

図 5.28 SINET における False Negative (3 つのリフレクタ)

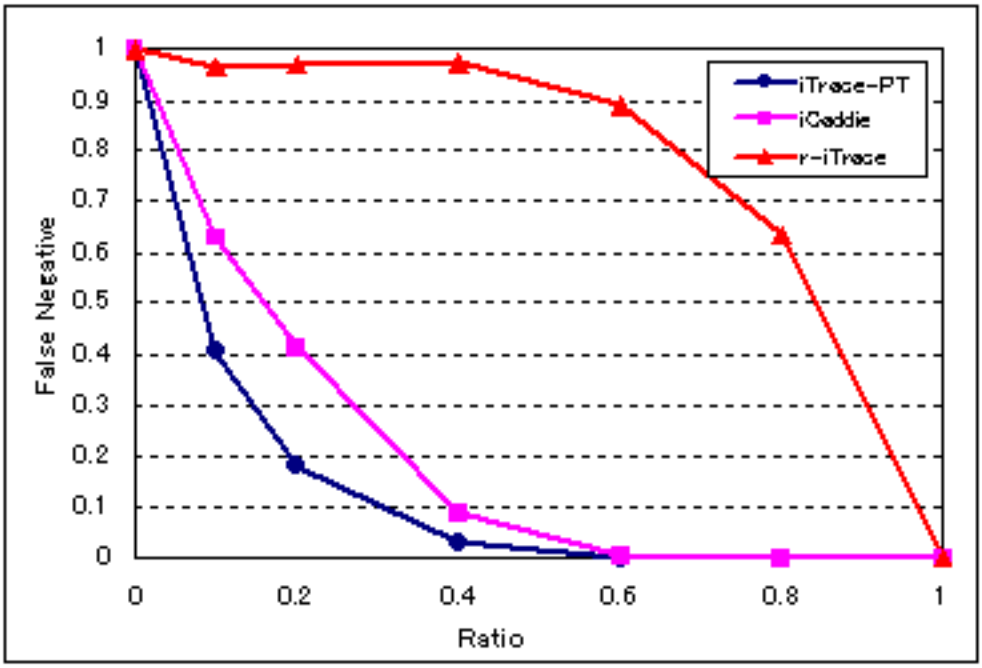

図 5.29 SINET における False Negative (5 つのリフレクタ)

第 6 章

考察

本章では，偽装 iTrace パケットへの対策と iTrace-PT の実用性に関して考察する．

6.1 偽装 iTrace パケットへの対策

本節では，偽装 iTrace パケットが iTrace-PT に与える影響を示し，その対策法を述べる．

6.1.1 偽装 iTrace パケットが与える影響

偽装 iTrace パケットとは，被害者の Traceback を妨害するために，攻撃者が生成した iTrace パケットのことである．この偽装 iTrace パケットのデータ部には，攻撃者が偽の経路情報を入れているため，被害者は，攻撃元の特定を誤ってしまう．さらに，iTrace-PT は，一度 iTrace パケットを送ったあて先にはハッシュクリアされるまで再送しないため，偽装 iTrace パケットが被害者に送られると，攻撃者－被害者間の中継ルータから正当な iTrace パケットが生成されなくなるという問題が生じる

偽装 iTrace パケットが iTrace-PT に与える影響をシミュレーションにより調べる．偽装 iTrace パケットの影響を調べる事が目的なので，前章のシミュレーション 1 の理想環境を用いた．攻撃者は，ハッシュクリアが起きる時刻を知っており，ハッシュクリアと同時に偽装 iTrace パケットを被害者に送る．偽装 iTrace パケットは，攻撃者と被害者間の中継ルータ以外のルータが生成したものであると偽装している．

図 6.1，図 6.2 にシミュレーション結果を示す．図 6.1，図 6.2 より，攻撃者を全く特定できず，完全に誤った場所を特定していることが分かる．このことから，偽装 iTrace パケットへの対策が必要であることが分かる．

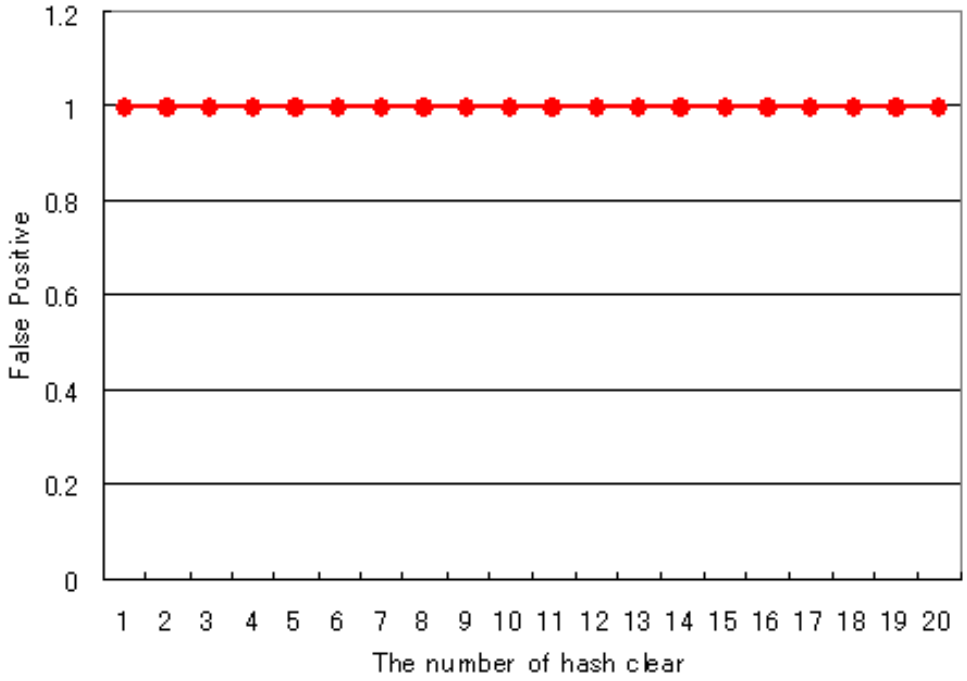

図 6.1 偽装 iTrace パケットが与える影響 (False Positive)

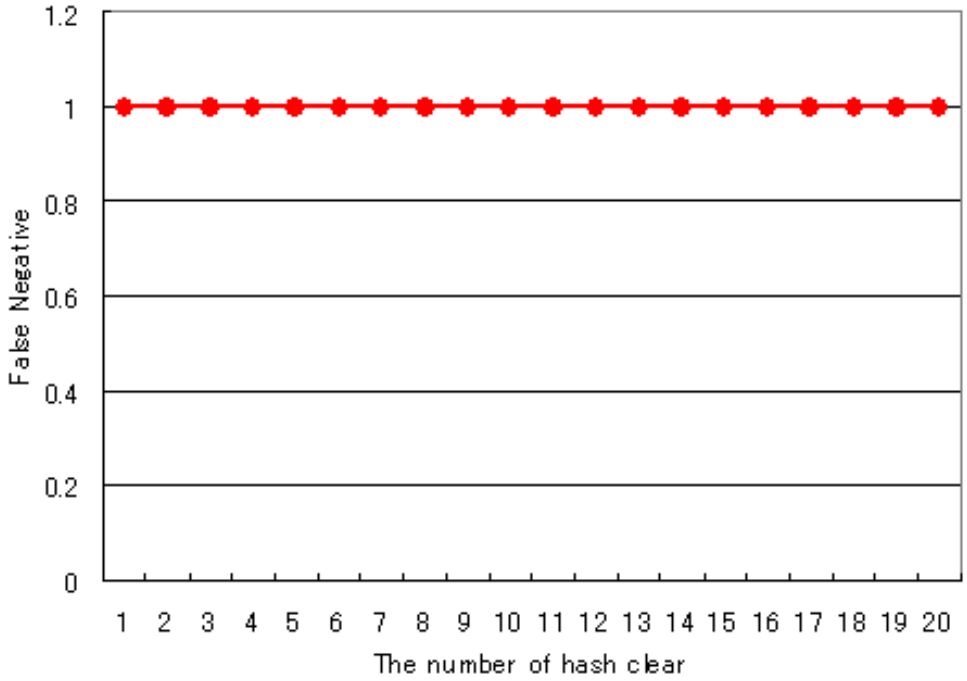

図 6.2 偽装 iTrace パケットが与える影響 (False Negative)

6.1.2　対策手法

偽装 iTrace パケットへの対策として，一般的な手法は，公開鍵認証である．公開鍵認証による偽装 iTrace パケットへの対策は，iTrace パケットを生成したルータが，自身の秘密鍵を用いて，Authentication Code を iTrace パケットに付加する．iTrace パケットを受け取った受信者は，対応した公開鍵を用いて，この Authentication Code の正当性を確認し，正当性が確認できなければ偽装 iTrace パケットと判定し，破棄する．

しかし，iTrace-PT は前節で述べたように，偽装 iTrace パケットの影響で正当な iTrace パケットが生成されなくなるため，この手法は，iTrace-PT には有効ではない．つまり，誤検出はなくなるが，結局攻撃元は特定できないということである．

iTrace-PT では，経路情報を iTrace パケットのデータ部に含むため，偽装 iTrace パケットにも正しい経路情報が含まれている．そこで，偽装 iTrace パケットからこの正しい経路情報だけを取り出す手法を提案する．

提案手法では，通常の公開鍵認証に加え，iTrace パケットの生成時刻に注目する．以下，詳細を述べる．

iTrace パケットを生成または中継するルータは，以下の 3 つを iTrace パケットのデータ部に入れる．

- ルータの IP アドレス
- iTrace パケットの生成 (中継) 時刻
- Authentication Code

Authentication Code は，中継パケットの送信元・あて先 IP アドレス，iTrace パケットの生成 (中継) 時刻の 3 つを秘密鍵で暗号化したものとし，$K_i(S, D, T_i)$ で表す．ただし，K_i は，ルータ i の秘密鍵，S，D は，それぞれ中継パケットの送信元・あて先 IP アドレス，T_i は，ルータ i が iTrace パケットを生成 (中継) した時刻である．

被害者は，各ルータが最後に iTrace パケットを生成 (中継) した時刻を記憶する Time Table を持ち，新しい正当な iTrace パケットを受け取ったら Time Table を更新する (図 6.3)．

受け取った iTrace パケットの各ルータの生成 (中継) 時刻が Time Table に記憶している時刻と等しい，または，記憶している時刻よりも前，または，Authentication Code が正しくないならば，その部分を iTrace パケットから取り除き，残りを正当パケットとして取り扱う．この手法によって，偽装 iTrace パケットから正しい経路情報だけが取り出せる．

以下の二つの例において，提案手法が有効に機能することを示す．

- 例 1：攻撃者が偽の経路情報を入れた iTrace パケットを被害者に送る
- 例 2：攻撃者が Replay Attack を行う

Replay Attack とは，暗号化された後のデータを盗聴し，そのまま再利用する攻撃のことである．

図 6.3 Time Table の更新

図 6.4 は，例 1 の対策を表した図である．色の付いている部分が，攻撃者が入れた偽の経路情報である．攻撃者は，R1, R2, R3 の秘密鍵を持っていないので，Authentication Code に正しい値を入れることはできない．よって，被害者は公開鍵認証により，色の付いた部分を取り除くことができ，正しい経路情報だけが取り出せる．

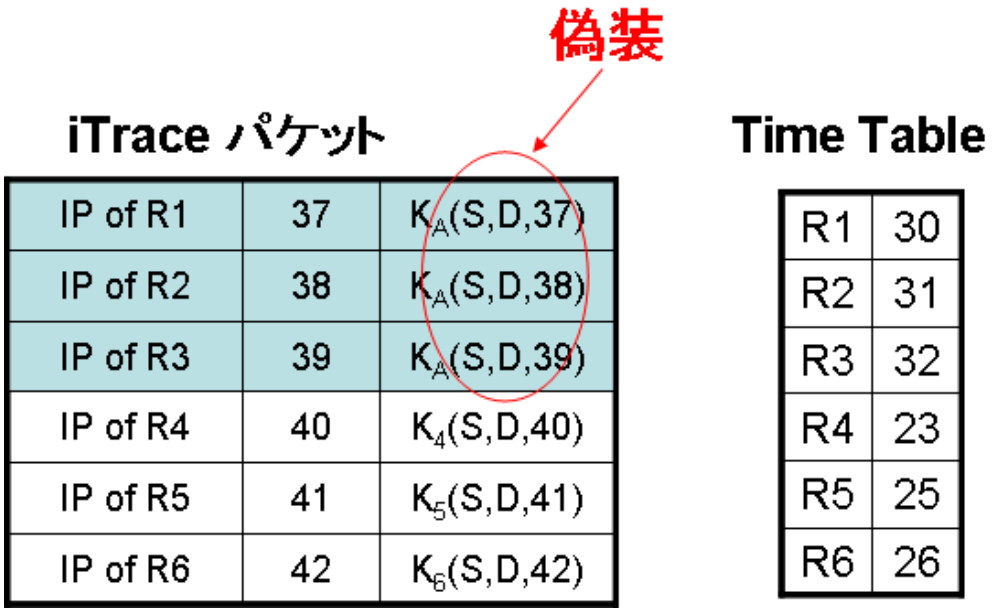

図 6.4 例 1 の対策

図 6.5 は，例 2 の対策を表した図である．Replay Attack なので，Authentication Code は正当なものとなっているが，R1, R2, R3 において iTrace パケットと Time Table に記憶されている時刻が等しくなっている．よって，この部分を取り除くことができ，正しい経路情報だけを取り出すことができる．

この対策手法を取り入れ，偽装 iTrace パケットが iTrace-PT に与える影響をシミュレー

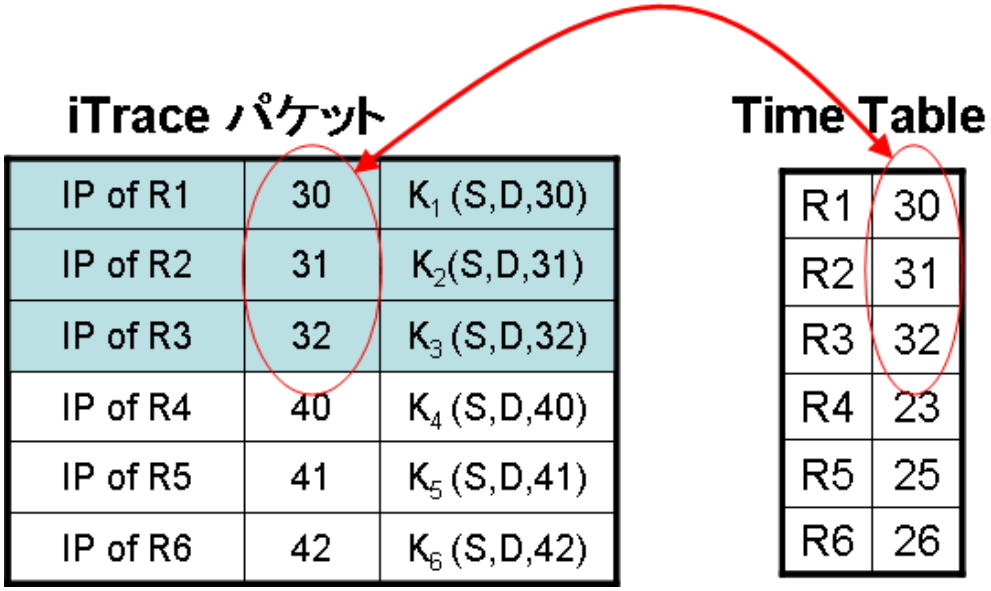

図 6.5 例 2 の対策

ションにより調べた．シミュレーション環境は，前節と同じである．

図 6.6，図 6.7 にシミュレーション結果を示す．図 6.6，図 6.7 より，対策手法が有効に働き，偽装 iTrace パケットから正しい経路情報を取り出せていることが分かる．

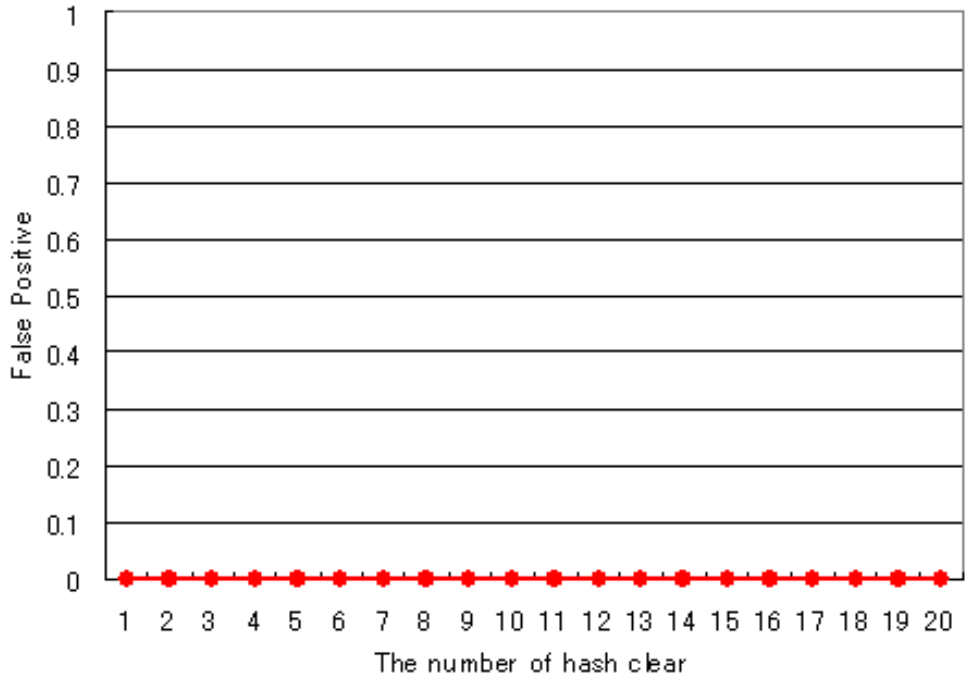

図 6.6 対策手法の効果 (False Positive)

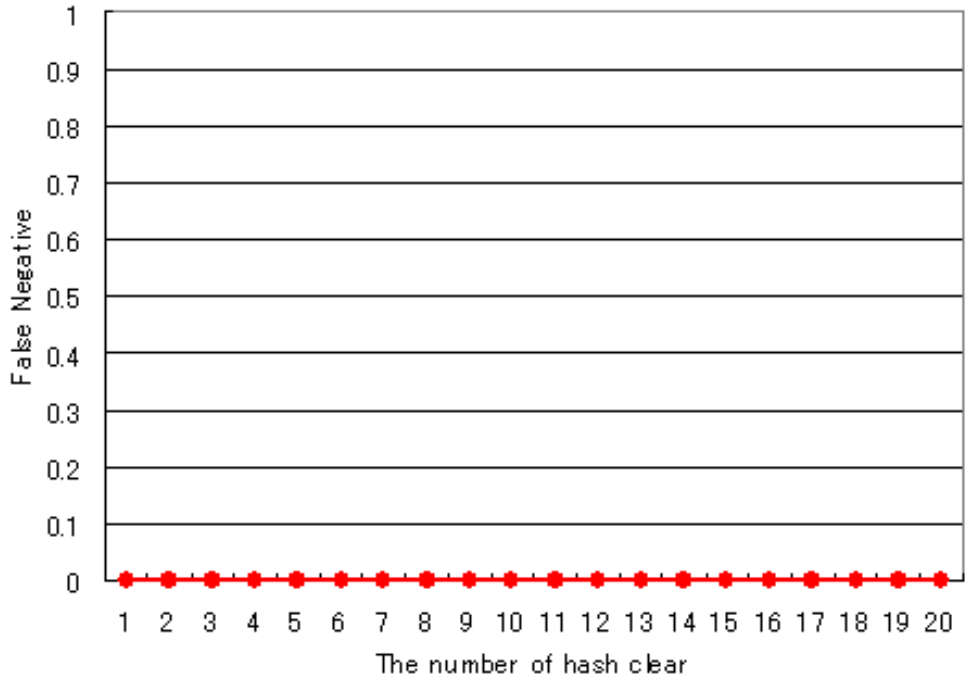

図 6.7 対策手法の効果 (False Negative)

6.2　iTrace-PT の実用性について

iTrace-PT は，ルータにおいてあて先 IP アドレスを記憶するためにメモリを必要としたり，偽装 iTrace パケットの対策のために，秘密鍵による暗号化処理が必要であり，ルータに負荷を与えることが欠点といえる．

しかし，図 6.8 のように iTrace-PT を実装することで，ルータの負荷を減らすことができる．図 6.8 の場合，ルータの仕事は iTrace パケットと，確率的に中継パケットを iTrace サーバに送るだけである．そして，iTrace サーバで iTrace-PT のパケット生成アルゴリズムを働かせればよい．

このように，iTrace-PT は十分に実用性があると考えられる．

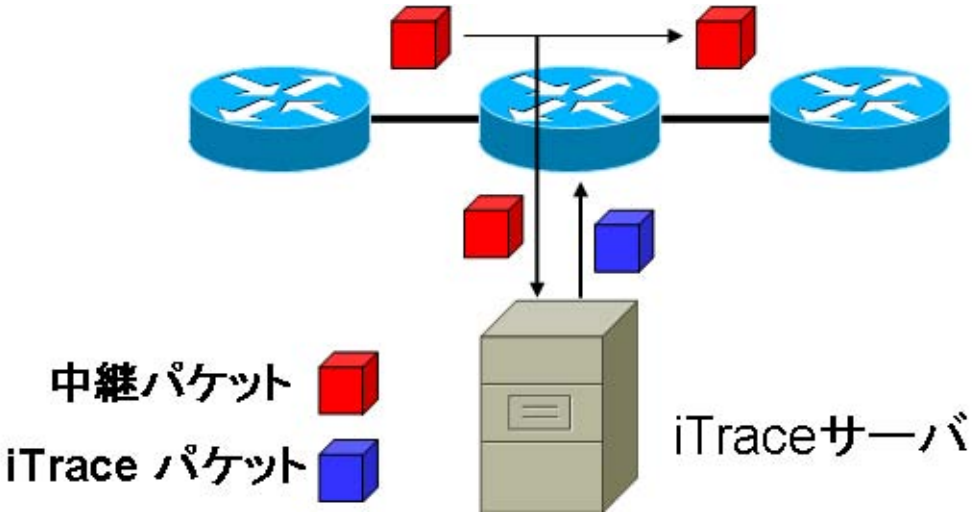

図 6.8 iTrace-PT の実装例

第 7 章

結論

本論文では，iTrace を改良した手法，ICMP Traceback with Periodical Transmission (iTrace-PT) を提案した．iTrace-PT は，一度 iTrace パケットを送ったあて先には，ハッシュクリアするまで再送しないことで，iTrace パケットの生成確率を上げながらネットワークに与える負荷を低く抑えることが出来る．また，攻撃元の特定を通信の持続時間に基づいて行うことで，攻撃者の通信が正当ユーザの通信にまぎれていたとしても，攻撃者だけの特定が可能である．そして，iTrace パケットをリフレクタで反射させることで，対応ルータの数が少ない場合でも反射型の DoS 攻撃に対応できる．

iTrace-PT は，被害者が自身の行っているサービスやリソースを考慮し，各種パラメータを設定することにより，それぞれの被害者に適した攻撃元の特定が行える．

シミュレーションにより，iTrace-PT は，生成確率を上げてもネットワークに与える負荷を低く抑えられることを示した．また，同じルータ配下に，複数の正当ユーザが到着する事態が発生しないような状況では，攻撃者の通信が正当ユーザにまぎれるほど低い通信レートであっても，攻撃者のみの特定が可能であることを示した．しかし，同じルータ配下に，複数の正当ユーザが到着する事態が発生する状況では，被害者の望んだ攻撃元の特定ができず，誤検出が多く出てしまうことがあることが示された．このような事態が発生する環境では，閾値を高く設定することで，誤検出なく攻撃元の特定ができることを示した．そして，対応ルータの数が少ない場合でも，DRDoS 攻撃の攻撃元特定に有効に機能することを示し，SINET においてはルータの対応率が 0.4 以上であれば，攻撃元を特定できることを示した．

公開鍵認証に加え，iTrace パケットの生成時刻に注目することで，偽装 iTrace パケットから正しい経路情報だけを取り出すことが可能であることを示した．

今後の課題としては，iTrace-PT を前章で示したような実装例で実装し，実際のネットワークで有効に機能するか検証する必要がある．

謝辞

本研究を進めるにあたって，終始御指導して頂いた，中山雅哉准教授に心から感謝致します．また，研究に関する貴重な御指摘をして頂いた，若原恭教授，中村文隆先生，関谷勇司先生に深く感謝致します．

また，研究に関する議論をし，貴重な御意見を下さった若原・中山研究室の皆様に厚く御礼申し上げます．

参考文献

[1] V. Paxson, "An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks", Computer Communication Review 31(3), July 2001.

[2] Symantec Corporation, "Symantec Internet Security Threat Report", p.24, September 2006. http://www.symantec.com/region/jp/istr/

[3] D. Song, A. Perrig, "Advanced and Authenticated Marking Schemes for IP Traceback", Proc. IEEE INFOCOM, 2001.

[4] A.C. Snoeren et al, "Hash-Based IP Traceback", ACM SIGCOMM 2001, August 2001.

[5] S.M. Bellovin, "ICMP Traceback Messages", Internet draft: draft-vellovin-itrace-00.txt, March 2000.

[6] B. Wang, H. Schulzrinne, "An IP Traceback Mechanism for Reflective DoS Attacks", IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), pp. 901-904, May 2004.

[7] N. Nishio, N. Harashima, H. Tokuda, "Reflective Probabilistic Packet Marking Scheme for IP Traceback", IPSJ Journal, vol.44, no.8, pp.1848-1860, August 2003.

[8] A. Kuzmanovic, E. Knightly, "Low-Rate TCP-Targeted Denial of Service Attacks (The Shrew vs. the Mice and Elephants)", Proc. ACM SIGCOMM 2003, August 2003.

[9] S. Gibson, "Distributed Reflection Denial of Service", 2002.
http://www.grc.com/dos/drdos.htm

[10] 警察庁, "DNS の再帰的な問い合わせを悪用した DDoS 攻撃手法の検証について", July 2006.

[11] 警察庁技術対策課, "DoS/DDoS 対策について　(検証) ", March 2004.

[12] P. Ferguson, D. Seine, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", RFC2827, May 2000.

[13] H.C.J. Lee, V.L.L. Thing, Y. Xu, M. Ma, "ICMP Traceback with Cumulative Path, An Efficient Solution for IP Traceback", Proc. 5th International Conference on Information and Communications Security (ICICS '03), pp.124-135, October 2003.

[14] V.L.L. Thing, H.C.J. Lee, M. Sloman, J. Zhou, "Enhanced ICMP Traceback with Cumulative Path", Proc. 61st IEEE Vehicular Technology Conference, May 2005.

[15] A. Mankin et al, "On Design and Evaluation of "intention-driven " ICMP Traceback", Proc. IEEE International Conference on Computer Communications and Networks, April 2001.

[16] B. Wang, H. Schulzrinne, "Multifunctional ICMP Messages for e-Commerce", Proc. IEEE EEE, Mar 2004.

[17] R. Braden, "Requirements for Internet Hosts – Communication Layers", October 1989. http://www.ietf.org/rfc/rfc1122.txt

[18] SINET3, "SINET3 (学術情報ネットワーク)", http://www.sinet.ad.jp/

[19] BRITE: Boston university Representative Internet Topology gEnerator, http://www.cs.bu.edu/brite/