DoS 攻撃を対象とした IP トレースバックにおける ルータ負荷削減手法

桂井友輝[†1]　中村嘉隆[†2]　高橋修[†2]

近年のネットワーク技術の発達，普及によって，DoS 攻撃をはじめとしたネットワークを利用した攻撃の規模は年々拡大している．DoS 攻撃は大量のデータや通信要求を送りつけることで，対象のサービスの処理能力やトラフィックに過負荷を与える攻撃の総称である．DoS 攻撃は攻撃パケットの送信元アドレスが偽装されており，被害を受けたホストが攻撃元を容易に特定できないという大きな特徴があり,その対策として存在する技術が IP トレースバックである．IP トレースバックには様々な手法が存在し，それぞれにネットワークへの影響，トレースバックに要する時間，機器にかかる負荷などの面において利点，欠点が存在する．本研究では，ネットワーク上のルータにログを保存することで攻撃元を特定するロギング方式を改良する．ロギング方式は攻撃パケットの数が少なくとも攻撃元を特定できる方式であるが，欠点としてルータに多大な負荷がかかる点が存在する．そこで本研究ではロギング方式を改良し，被害を受けたホストが攻撃を検知した後に各ルータがログの保存を開始することで，同方式におけるルータの負荷を削減する手法を提案する．

A router load reduction technique in the IP traceback for a DoS attack

YUKI　KATSURAI[†1]
YOSHITAKA　NAKAMURA[†2]　OSAMU　TAKAHASHI[†2]

1. はじめに

近年，インターネットを利用する人口の増加や常時接続可能な環境の普及により，人々の生活にとってネットワークは身近なものとなった．しかし同時に，ネットワークセキュリティに関する問題も多発している．ネットワーク上で特定の国家，企業，団体，個人に対して行われるクラッキング行為であるサイバー攻撃もまたその一つである．サイバー攻撃は標的のコンピュータやネットワークのデータの詐取や破壊，改竄を行うことでシステムを機能不全に陥らせるものであり，例として，対象の処理能力やトラフィックサービスに過負荷を与える DoS 攻撃(Denial of Service attack), またその分散型である DDoS 攻撃などが存在する．

DoS 攻撃に用いられるパケットは通信プロトコル上正当な動作を装っており既存のファイアウォールによる防止が難しい．また DoS 攻撃の最大の特徴として，攻撃パケットの送信元アドレスが偽装されていることが多い. そのため，被害ノードによる攻撃元の特定が困難であるということが問題になっている．

この送信元偽装の対策として，IP トレースバック技術が存在する. IP トレースバックとは DoS 攻撃に用いられた攻撃パケットの情報を用いて攻撃に用いられた経路を検出する技術である．これまで Input Debugging 方式[1], 確率的マーキング方式[2], ロギング方式など様々な IP トレースバック方式が提案されている．本研究が着目したロギング方式では，ネットワークを構成するルータが常にパケットを保存しておき，被害ノードが受信した攻撃パケットと特徴情報を照合する．この方式はルータに大きな記憶容量，処理能力が要求され，他方式よりもコストの面で不利になっているが，攻撃パケットが非常に少ない場合にも攻撃元を特定できるという利点がある．

本研究では，パケットを常に保存することによってルータへかかる負担を可能な限り軽減させるため，被害ノードが設置する不正アクセス監視システムである IDS(Intrusion Detection System)などによる DoS 攻撃の検知をトリガーとして各ルータがパケットの保存を開始する方式を提案する．

2. 関連研究

IP トレースバックにおけるロギング方式は，ルータにログを記録する機能を追加する手法である．ネットワークを通過するパケットのログを記録し，攻撃パケットのログを上位ルータから再帰的に探索することで発信源の探知を行う．しかしルータが全てのパケットをログに記録することはディスク空間などの都合上不可能なため，ハッシュテーブルを用いたダイジェスト方式[3], マーキング方式と併用したハイブリッド方式[4]などが提案されている．この方式では，IP ヘッダの中で，TTL, TOS, ID フィールドを除く経路中で不変の部分と，宛先アドレスや発信元アドレスなどの管理情報を除いた正味のデータであるペイロードの先頭 8 バイトについて, k 個の独立なハッシュ関数を適用した結果を 2n ビットのビットマップとして保持する. このビットマップは一定の間隔で初期化され，その期間中に使用したハッシュ関数とともにダイジェストテーブルに保管される．

†1 公立はこだて未来大学大学院 システム情報科学研究科
Graduate School of Systems Information Science, Future University Hakodate
†2 公立はこだて未来大学 システム情報科学部
Systems Information Sciences, Future University Hakodate

この方式を用いることで，探査端末は各ルータに対し能動的に攻撃パケットの通過の有無を問い合わせることができる．

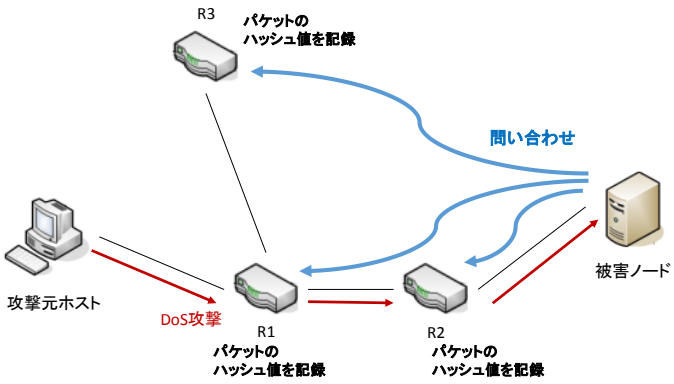

図 1: ロギング方式

この方式には，攻撃パケットの数が少なくとも攻撃元ホストに最も近いルータ(エッジルータ)を特定することができるという利点がある．問題点としては，大きな記憶容量や高いハッシュ処理能力などが要求される点，常にログを保存し続けるということからルータへかかる負荷が大きい点などが挙げられる[5].

3. 提案方式

3.1 アプローチ

本提案方式では，IDS などの不正アクセス監視システムが DoS 攻撃を発見した際に，その情報をトリガーとして各ルータに通知を送信，ルータがログの収集を開始するといった手順を取る．その後被害ノードがエッジルータの位置を特定した段階で，IP トレースバックが完了したとする．また本提案方式では，攻撃が短時間で終了した場合に，誤って攻撃経路の途中に存在するルータをエッジルータと特定する場合が存在する．そういった事例を回避するため，攻撃の継続時間に応じてエッジルータと通知を送受信し，特定したルータが真のエッジルータかどうか検証を行う．

3.2 提案方式の前提条件

本提案方式の前提条件として以下の 2 つを挙げる．

(1) 想定環境

本研究では通常の通信がランダムに行われているネットワーク環境において不特定のタイミングで DoS 攻撃が開始されたことを想定する．また被害ノード，ネットワークを構成する全ルータは隣接するルータの情報を保持しているものとし，全ルータに提案方式に必要な機能が追加されていると仮定する．

(2) ルータへの機能追加

ルータの標準的な機能として，以下を追加する．

i. ルータを通過するパケットのログを保存する機能
ii. ログの保存に必要なディスク空間
iii. 各種通知の送信，受信を行う機能

3.3 トレースバックの手順

本提案方式におけるトレースバックの手順を，通知を拡散し各ルータがログの保存を開始するまで，攻撃経路を確定しエッジルータを特定するまで，特定したルータが真のエッジルータかどうか検証するまでの 3 フェーズに分けて述べる．

フェーズ 1: 各ルータのログ保存・照合開始

IDS が DoS 攻撃を検知した際，被害ノードは，最も近いルータに対し，ログの保存命令と攻撃に用いられたパケットの特徴を通知する．通知を受け取ったルータはログの保存を開始し，同時に通知の送信元ルータ以外の隣接するルータに対し通知を行う．以下同様に通知の拡散を行い，最終的にネットワークを構成するルータそれぞれに通知が行き渡ることになる．この際，自身に対し通知を送信したことのあるルータには通知を送信しない．また，各ルータが隣接ルータに通知を送信する際には通知に含まれる被害ノードからのホップカウントを増加させる．通知を重複して受け取った場合は，ホップカウントが最も小さいもののみを残し，他の通知を破棄する．図 2，図 3 に通知の拡散，ホップカウントの比較による重複通知の破棄の様子を示す．

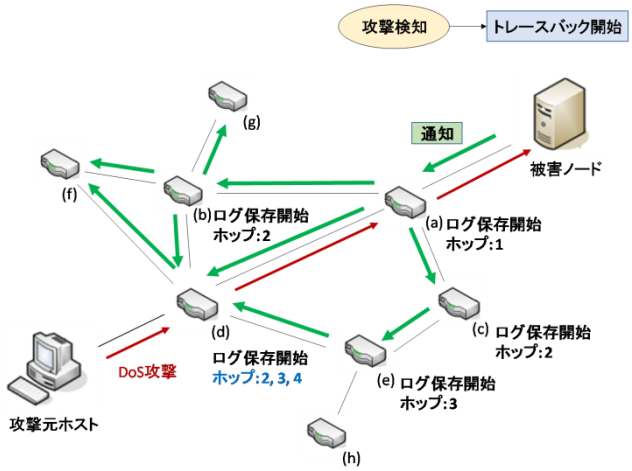

図 2: 通知の拡散

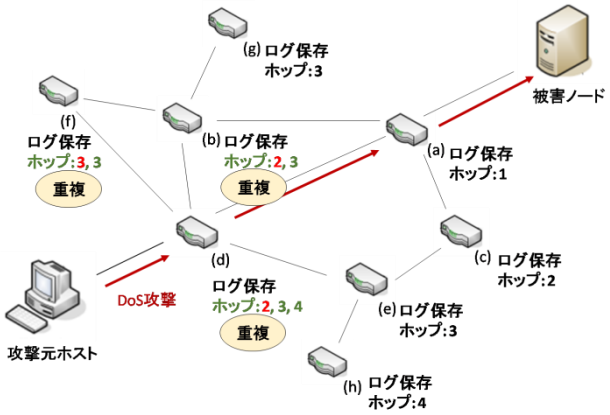

図 3: 通知が重複した時

フェーズ 2: 攻撃経路確定，エッジルータの特定

各ルータは通知のやり取りを行った後に，自身が保存を開始したパケットのログ内から攻撃パケットの検索を行う．攻撃パケットを発見したルータは，トレースバック動作開始時に通知を受け取ったときと同様，隣接するルータに自身のホップカウントを記した発見通知を送信する．発見通知を受け取ったルータが自身も攻撃パケットを発見した場合は，受け取った通知に記されたホップカウントと自身のホップカウントを比較し，差が 1 であれば正しい経路として保存し，経路確定の通知を隣接ルータに送信する．発見通知を受け取ったルータが攻撃パケットを発見していない場合は，受け取った通知のホップカウントと自身の保持するホップカウントを比較する．通知のホップカウントが自身のホップカウント以上であれば，ログの保存を終了し，最後に保存したログまで攻撃パケットとの照合を行う．攻撃パケットを発見できなければ動作を終了する．以後，全てのルータが同様の操作を行うことで，攻撃経路を確定させる．

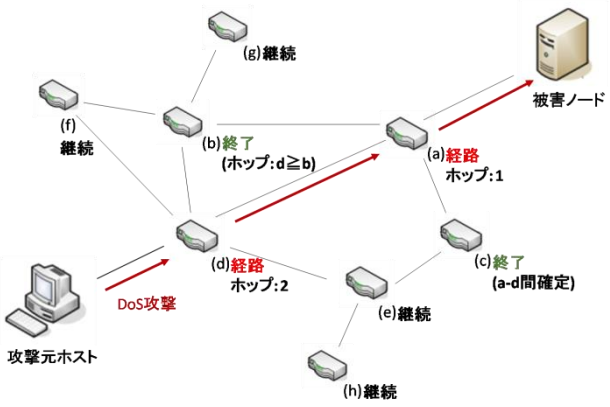

図 4: 経路確定時

図 4 が示すように，これまでの動作を終え経路が確定した時，ルータ(e)，ルータ(f)，ルータ(g)，ルータ(h)はログの保存，攻撃パケットの照合を継続したままである．これは被害ノード，各ルータ自身が，経路が確定したことを知る術が無いためである．これらのルータはある一定の時間が経過した後，ログの保存，攻撃パケットの照合を終了し平常の動作に戻る．またそれと並行して，被害ノード側は攻撃パケットを発見した中で最もホップカウントの大きいルータをエッジルータと特定する．

フェーズ 3: エッジルータの検証

フェーズ 1，フェーズ 2 の操作によってエッジルータを特定したが，攻撃の継続時間やパケットロスの関係によって，攻撃経路の途中に存在するルータをエッジルータと誤って特定する場合が存在する．そのため，エッジルータを特定した際，エッジルータ側から自身の位置と攻撃パケットを受信した時のタイムスタンプを被害ノードに対し送信する．被害ノードはエッジルータからの通知を受信すると，エッジルータに対し現在時刻の送信を要求する．そしてエッジルータから現在時刻を被害ノードに対し送信する．この際，被害ノードが現在時刻の送信を要求してからエッジルータから現在時刻を受け取るまでの時間の半分と，攻撃パケットのタイムスタンプと被害ノードが最後に攻撃を受けた時間の差を比較する．ここで，後者が前者を上回っていた場合は，攻撃の継続時間に依らずエッジルータの特定を行えたと判断する．前者が後者を上回る場合は，攻撃継続時間が短い場合に，最後の攻撃パケットが通過した後にログの保存を開始したルータが存在する可能性を否定できないとして，トレースバック不可能と判断する．またエッジルータの現在時刻の送信を要求することで，攻撃パケットを発見した時点でのタイムスタンプがずれていた場合に矯正を行うことができるという利点がある．このエッジルータの検証を行うかどうかは，エッジルータが確定するまでに攻撃が終了しているか否かで判断する．

3.4 動作シーケンス

フェーズ 1，フェーズ 2 の動作シーケンス

フェーズ 2 までに例として用いたルータの中から，被害ノード，ルータ(a)，ルータ(b)，ルータ(d)，ルータ(f)に着目し，フェーズ 1 とフェーズ 2，すなわちトレースバック開始からエッジルータ特定に至るまでの動作について，シーケンス図を図 5 に示す．

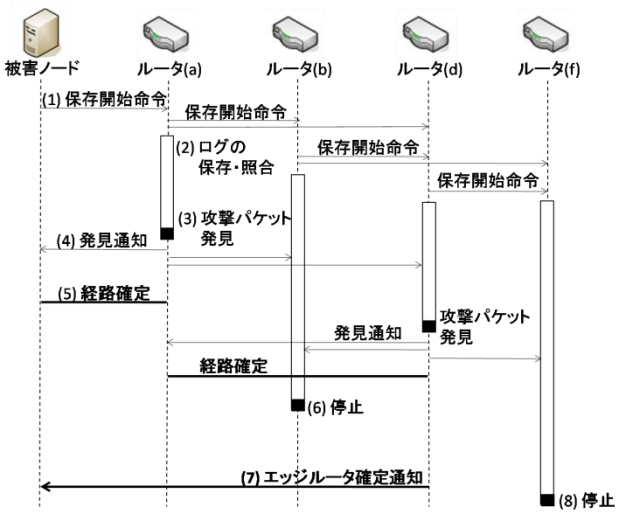

図 5: フェーズ 1，フェーズ 2 の動作シーケンス図

それぞれの動作について，(1)～(8)に類別する．(1)，(2)がフェーズ 1 の動作，(3)～(8)がフェーズ 2 の動作である．

(1) 被害ノードからルータ(a)に対し，攻撃パケットの特徴と共に，通過するパケットのログの保存を開始する旨の通知が送信される．その後ルータ(a)からルータ(b)，ルータ(d)に，ルータ(b)からルータ(d)，ルータ(f)に，ルータ(d)からルータ(f)に，それぞれ隣接するルータに対し同様に通知を送信する．送信の際には，通知に記されたホップカウントを増加させる．また自身に対して通知を送信したルータには通知を送信しない．

(2) 保存開始命令を隣接するルータに送信したルータが，ログの保存・照合を開始する．またこの際，1.の動作で複数受け取った通知のホップカウントが競合していたならば，最もホップカウントが小さいものを被害ノードから見た自身のホップ数とする．

(3) 保存しているログの中から攻撃パケットを発見する．

(4) ログ内に攻撃パケットを発見した旨，被害ノードから見た自身のホップ数を記した発見通知を，隣接するルータに対し送信する．またこの際，1.の動作とは異なり，自身に対し通知を送信したルータにも通知を送信する．

(5) 発見通知を互いに送信し，ホップ数の差が 1 であった場合は, その 2 ルータを攻撃に用いられた経路とする．

(6) 隣接するルータから発見通知を 2 通以上受け取ったルータは，通知に記されたホップ数と自身のホップ数を比較する．2 通に記されたホップ数の内どちらかが自身のホップ数よりも大きかった場合，自身が攻撃経路に含まれていないとして，ログの保存・照合を終了する．

(7) 経路が確定したルータの内最もホップ数の大きいルータが，自身が発見通知を送信してから一定時間経過したとき自身をエッジルータと判断し，被害ノードに対して自身の位置を送信する．またその際，エッジルータの検証に必要となる発見した攻撃パケットのタイムスタンプを同時に送信する．

(8) ログの保存・攻撃パケットとの照合を行い，5. の動作終了判断を行えず攻撃パケットを発見できなかったルータが，一定時間経過後に動作を終了する．

フェーズ 3 の動作シーケンス

フェーズ 1，フェーズ 2 の動作によって，エッジルータを特定した．このエッジルータ特定に至るまでに DoS 攻撃が終了していた場合，フェーズ 3，すなわちエッジルータの検証動作を行う．シーケンス図を図 6 に示す．

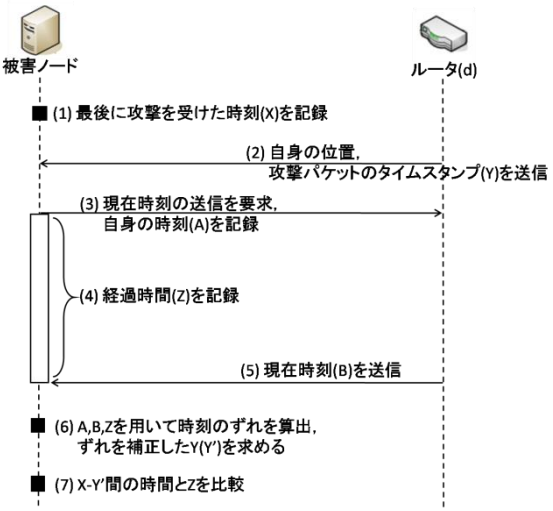

図 6: フェーズ 3 の動作シーケンス図

それぞれの動作について，(1)～(7)に類別する．

(1) エッジルータの特定動作を行っている最中に攻撃が終了した場合, 最後に攻撃パケットを受け取った時刻(以後 X)を記録しておく．

(2) フェーズ 2 の動作によって自身をエッジルータと判断したルータが，自身の位置と同時に攻撃パケットをログに保存したタイムスタンプ(以後 Y)を被害ノードに対し送信する．

(3) 被害ノードがエッジルータに対し現在時刻の送信を要求する．また送信する際に時刻(A)を記録する．

(4) 被害ノードがエッジルータに現在時刻の送信要求を行ってからエッジルータの現在時刻を受け取るまでの時間(以後 Z)を記録する．

(5) エッジルータが被害ノードに対し，自身の時計から現在時刻(B)を送信する．

(6) A + Z/2 と B を比較する．ずれが存在した場合は，Y の値をずれに応じて増減させ，エッジルータが送信した攻撃パケットのタイムスタンプを被害ノードからみた正しい値(Y')に変更する．

(7) Y'-X と Z/2 を比較する．Y'-X ≧ Z/2 となる場合は，正しいエッジルータであると判断する．対して Y'-X

＜ Z/2 となる場合は，エッジルータと特定したルータが単に攻撃経路の途中に存在するルータであるとして，正しいエッジルータを特定できなかったということでトレースバックを終了する．

4. 実験および評価

4.1 実験の概要

本実験では，常にログを保存し続ける従来のロギング方式を用いる場合と，各ルータが通知を受け取ってからログの保存を開始する提案手法の内エッジルータの検証を行わない場合において，それぞれのエッジルータ特定に要する時間と特定精度を比較し，本提案手法の優位性を示す．またその後，提案手法におけるエッジルータの検証を行う場合，行わない場合のエッジルータ特定に要する時間，特定精度の比較を行い，同操作の意義を示す．

4.2 実験環境

本実験ではネットワークシミュレータである NS-2（Network Simulator version 2）[6]を用いる．NS-2 上にネットワークを構成し，シミュレーションを行った．ネットワーク上では，DoS 攻撃に加えて，平常の通信も行われているものとする．

表 1: 実験の設定

ルータ設置数	100
各ルータの伝送速度	100Mbps
通常の通信プロトコル	TCP
DoS攻撃の種類	SYN Flood
通知の通信プロトコル	UDP

4.3 特定に要する時間，特定精度に関する実験

提案手法の実験として，ハッシュ関数を適用しない場合における DoS 攻撃検知後の攻撃元ホストの位置特定に要する時間，特定精度を調べるため，ns-2 上で評価実験を行った．評価方法は，ルータが常にログを保存し続ける既存方式の場合と提案方式の場合，すなわち被害ノードの攻撃検知後，各ルータが通知を受け取ってからログの保存を開始する場合についてそれぞれ，DoS 攻撃が開始してからの経過時間 100ms ごとにトレースバックを行い，検出に要する時間，特定精度を比較した．この際，DoS 攻撃に関わらない通信パケットはネットワークに影響を与えない程度にランダムに送受信されているものとする．また，被害ノード側は DoS 攻撃を検知するのは攻撃開始から 1000ms 後と仮定し，そこからトレースバックを行うものとする．

4.4 エッジルータの検証に関する実験

4.5 実験結果

本実験における，従来のロギング方式と提案手法の内エッジルータの検証を行わないものの比較実験の結果を示す．

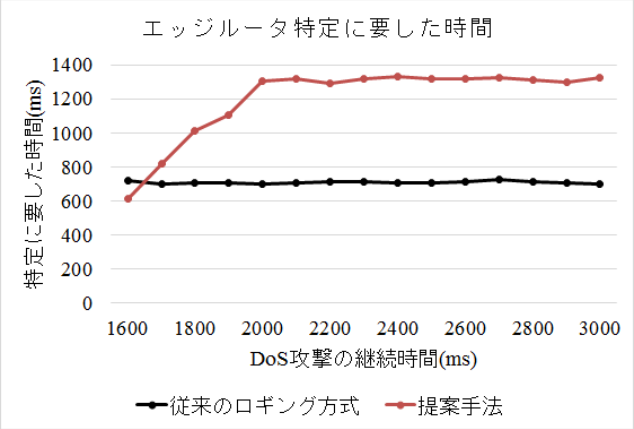

図 7: 特定に要する時間比較(従来の方式と提案手法)

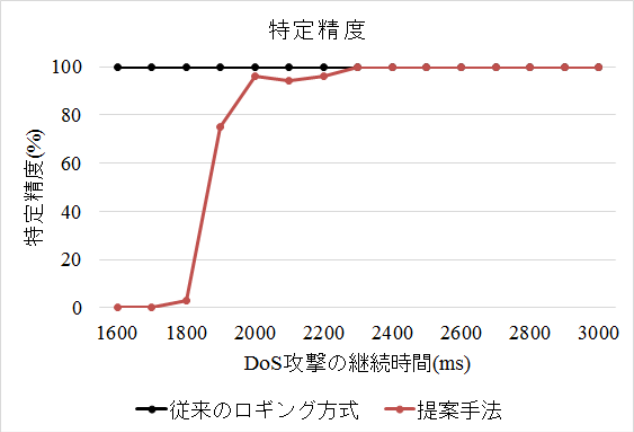

図 8: 特定精度比較(従来の方式と提案手法)

特定に要する時間を示すグラフにおいては，縦軸がエッジルータの特定に要した時間，横軸が DoS 攻撃の継続時間を表す．この実験では，精度を問わず，エッジルータと思わしきルータを特定するまでの時間を示している．従来のロギング方式に対して提案手法を用いた場合，特定に要する時間が大きく長引くことになった．攻撃の継続時間が 1600ms の辺りでは従来のロギング方式よりも短時間で特定している．特定精度を示すグラフでは，縦軸がエッジルータの特定成功率，横軸が DoS 攻撃を開始してからの経過時間を表す．DoS 攻撃の継続時間を問わず常に 100%の特定精度を示す従来のロギング方式に対し，DoS 攻撃の検知をトリガーとしてトレースバックを開始する提案手法では，一定時間が経過するまでは精度が著しく低下した．また，この精度が低下している時間帯は，特定に要した時間のグラフにおいて従来のロギング方式よりも短時間で特定した場合であることがわかる．しかしその後は既存方式と同様，100%の特定精度を維持したことが読み取れる．特定に要した時間のグラフと照らし合わせると，従来のロギング方式を用いた場合は常に同じような値を維持し，提案手法を用いる場合は 2000ms ほど経過した段階で最大値に到達し，その後は大きな変化が無いことがわかる．

続いて提案手法においてエッジルータの検証を行う場

合，行わない場合の特定に要する時間，特定精度を示す．

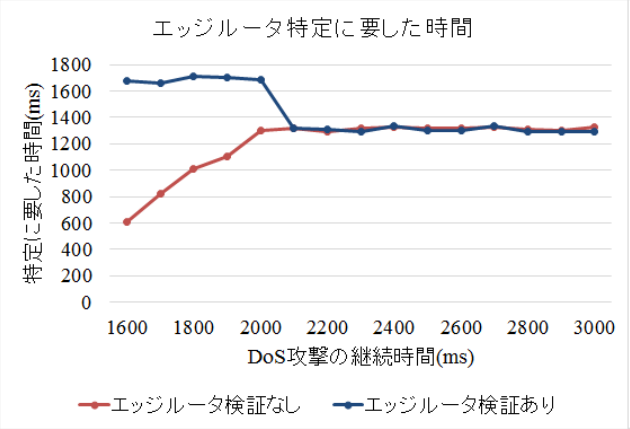

図 9: 特定に要する時間比較(エッジルータ検証の有無)

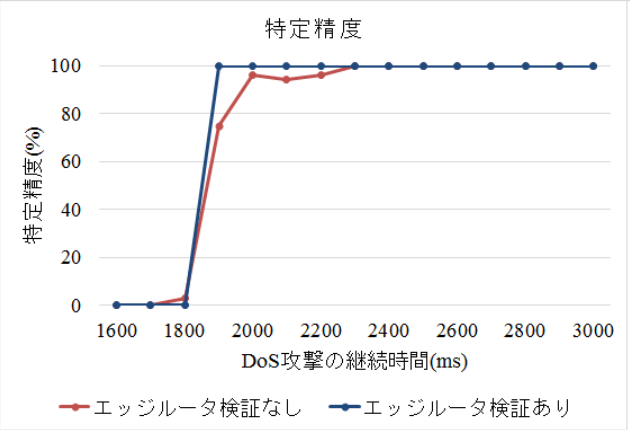

図 10: 特定精度比較(エッジルータ検証の有無)

精度に関しては，検証を行わない場合は 100%に到達するまでにわずかに上下幅が存在したが，それに対し検証を行う場合は攻撃の継続時間が一定を過ぎてからは常に 100%を維持している．

5. 考察

5.1 実験の考察

実験の結果から，従来のロギング方式を用いる場合は総じて特定に要する時間，特定精度が高水準を保っているということが読み取れる．これはルータが常にログを保存し続けるために攻撃パケットが 1 つでも通過していれば攻撃経路であると判断できるためである．対して本提案手法を用いる場合は，被害ノードの攻撃発見をトリガーとし，また各ルータに対しログの保存命令を拡散する必要があることから，特定に要する時間が長くなる．図 7 より，実験の設定では，精度が安定している場合にはおよそ 500ms の差が生じている．また図 8 から，特定精度が 100%になる直前にわずかなぶれが生じてしまうことが読み取れる．これは攻撃が終了した後にログの保存命令を受け取った際，経路途中のルータをエッジルータと誤って認識してしまう可能性が存在するためである．対策として，エッジルータの検証を行う機能を追加した．図 9 より，エッジルータの検証を行う場合，すなわちエッジルータと思わしきルータが発見されるまでに攻撃が終了している場合は，検証の動作を挟むために特定に要した時間が検証を行わない場合と比較して長くなる．しかし図 10 より，特定に成功した場合．その精度が常に 100%を維持していることがわかる．

5.2 提案方式の考察

実験の考察から，提案手法は従来のロギング方式と比較して特定に要する時間が長くなってしまうが，特定精度に関しては問題が無いといえる．また提案手法では，従来のロギング方式の最大の問題点であるルータの負荷を，常時ログの保存を行わせないことで大きく削減している．提案手法の欠点である攻撃継続が特定の値をとるときの精度のぶれに関しても，DoS 攻撃の継続時間の長短を判別し，特定精度を保証するためのエッジルータの検証機能を追加したことで，信頼度を高めることが可能となった．各手法における特定に要する時間，特定の精度，ルータの負荷に関してまとめたものを表 2 に示す．

表 2: 各手法の特徴まとめ

	特定に要する時間	特定精度	ルータの負荷
従来のロギング方式	○	○	×
提案手法 (エッジルータの検証なし)	△	△	○
提案手法 (エッジルータの検証あり)	△	○	○

ルータ負荷を削減できていることは自明であるが，今後ルータの負荷に関して定量的な処理量の差を計測する必要があると考えられる．

提案手法の問題点である特定に要する時間が長くなってしまうという点に関して，今後はネットワーク内部に DoS 攻撃検知機能をおいた状況下での研究を行う．攻撃経路の途中からトレースバックを開始できるようにすることで，現在被害ノードからのみ拡散している動作開始命令を攻撃経路の途中から拡散させる．これによって，全体の処理時間の減少が見込めると考えられる．

6. おわりに

本稿では，IP トレースバックにおいて従来のロギング方式で問題となっていたルータへかかる負荷を軽減し，かつ特定精度を維持することを目的とする手法を提案した．DoS 攻撃を受けた際，攻撃を検知した後に各ルータへとトレースバック開始命令を通知し，ログの保存と攻撃パケットとの照合を行う手法について提案を行った．また，ns-2

を用いて環境を構築し，エッジルータを検出する実験を行うことで，結果から提案手法を用いることで各ルータの処理量が減少し，特定精度は高水準を維持することが証明できた．また DoS 攻撃が途中で終了してしまう場合に関しても，エッジルータと特定したルータと被害ノード間で通知のやり取りを行うことで対応した．既存の方式と比較した場合に，特定に要する時間を長く取ることで全体のルータの処理を減らすことに成功したといえる．

今後は，ルータの負荷を定量的に計測すると共に，ネットワーク内部に DoS 攻撃検知機能を導入し，攻撃の道中で DoS 攻撃を検知した場合にトレースバックを開始できるようにすることで，全体動作の短時間化を目指し，提案方式の有用性を示す．

参考文献

[1] R. Stone. “CenterTrack: An IP overlay network for tracking DoS floods,” Proceedings of the 9th conference on USENIX Security Symposium (SSYM ’00), Vol.9, p.15, 2000.

[2] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, “Network support for IP trace-back.” IEEE/ACM Transactions on Networking, Vol. 9, No. 3, pp. 226–237, 2001.

[3] A.C. Snoeren, C. Partridge, L.A. Sanchez, C.E. Jones, F. Tchakountio, S.T. Kent, and W.T. Strayer, "Hash-based IP traceback," Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM '01), pp.3-14, 2001.

[4] C.K. Singh, S. Koppu, and V.M. Viswanatham,“E-RIHT: Enhanced Hybrid IP Traceback Scheme with 16-bit marking field”, International Journal of Engineering & Technology (0975-4024), Vol. 5 Issue 3, p.2594, 2013.

[5] 井上慎一郎, 石井方邦, 笹瀬巌, “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,” 情報処理学会論文誌 Vol.53, No.2, pp.795-804. 2012.