既存手法を組み合わせたIPトレースバックの提案と評価

2002MT021 伊藤 健司　　2002MT38 川本 高弘
指導教員　後藤 邦夫

1 はじめに

不正アクセス“DoS/DDoS 攻撃”は, 直接的で単純な攻撃であるために, 確実な対策方法が少ない. さらにDoS/DDoS 攻撃パケットの発信元アドレスが詐称されており, 発信元を正確に特定できないことが対策を困難にしている. この DoS/DDoS 攻撃対策方法の一要素として, [3] で挙げられているように, 発信元アドレスの詐称パケットの発信元追跡技術 (IP トレースバック技術) が求められている. IP トレースバック技術とは IP アドレスが詐称されていたとしても, 目標のパケットが中継したルータからの報告を元にそのパケットの伝送経路を逆探知することによって発信源を突き止める技術である. 発信源を特定することができれば, パケットフィルタリングの設定や, 発信源の管理者へ通報するなどの対処が可能となる.

既存の手法には, リンク検査方式, 逆探知パケット方式, マーキング方式, ロギング方式などの方式が知られているが, どれも一長一短があるので, 複数の手法を組み合わせて欠点を補うような新たな手法を提案することが必要である. 本研究では逆探知パケット方式とロギング方式の 2 つの方式を組み合わせる. ロギング方式を用いて各ルータを経由するパケットのログを収集し, 各ホストは逆探知パケット方式を用い, 到着したパケットのログを隣接する追跡ホストへ通知し, 追跡する場合に攻撃パケットを特定する. この手法によって攻撃中に追跡を完了する必要はない, トラフィック増大の影響をあまり受けないなどの利点がある. 提案した手法は実験環境を構築し, 実際にプログラムを動かし追跡できるか評価する. なお, 伊藤は主に実験環境構築, 動作評価を担当し, 川本は主にプログラム作成を担当した.

2 既存の IP トレースバック方式

本研究で望ましいシステムを構築するため, [1][2] より, 既存手法を以下で説明する.

- リンク検査方式
  隣接ルータから攻撃の上流となるリンクを特定し, 隣接ルータへと順にたどっていくことで発信源を特定できる. しかし, 攻撃パケットを受信している間 (相手が攻撃中) しか追跡することができない.
- 逆探知パケット方式
  各ルータにおいて通過するパケットのうち, 逆探知するために必要な情報を, 別のパケットにおさめ, 被害者へ届ける. これを収集, 分析することによって発信源を特定する. しかし, 追跡パケットによるトラフィックの増大が発生する.
- マーキング方式
  各ルータが攻撃パケットのある部分へ特徴のある情報を埋め込み, その特徴を持つパケットを被害者が解析することによって発信源を特定する. しかし, 攻撃者が偽造マーキングを生成した場合, 伝送経路の逆探知が困難になる. だが, この方式によるトラフィックの増大は一切発生しない.
- ロギング方式
  ネットワーク上の要所にある記録装置がパケットを特定するための特徴情報を記録しておき, 被害者側で受信したパケットと記録した特徴情報を照合する. 特に通過するパケットの記録は, ハッシュ関数などを用いて効率よく記録する.

3 提案するシステム

この節では, 本研究で提案するシステムについて説明する.

3.1 システムの位置付け

インターネットはネットワークにより異なったルーティングポリシの元で管理, 運用されているため, 複数の AS を経由して攻撃パケットが流れて来た場合は**図 1** に示すように, まずどの AS から攻撃パケットが流れてくるのか特定する必要がある. 実際には AS 間の連携は難しく, 既存の研究は AS 間の連携を前提としている. 本研究では AS 境界ルータ付近に追跡装置を配置し, 攻撃パケットの発信源の AS を特定することを前提として, それによって特定された AS 内での IP トレースバックを実際に実装する.

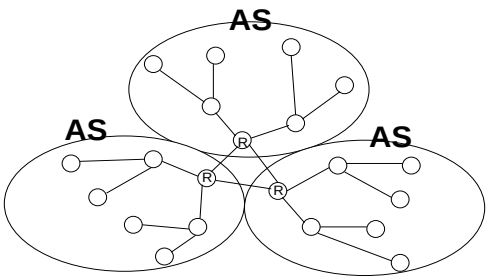

図 1: ネットワークの全体像

3.2 既存手法の組合せ

本研究では, ルータの設定を変えずにシステムを構築し, トラフィックが増大しないように提案する方式が逆探知パケット方式と, ロギング方式を組み合わせる. そこで, AS 内におけるネットワークに着目し, 実験環境を**図 2** のように構築した. IP アドレス詐称を伴った DoS

攻撃を考えているのでエンド側に, 攻撃ホスト, IP アドレス詐称されるホスト, 被害ホストの 3 台の PC を構成する．また, 同じスイッチ内に追跡ホストを設置する．トレーサは, 各ルータの横に配置し, IP アドレスも持つ．各トレーサ, ルータ, ホストの通信方法は, UDP とする．

この方法では, リンク検査方式のように攻撃パケット

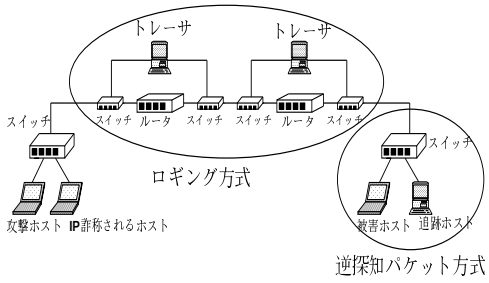

図 2: IP トレースバックのネットワークモデル

を受信している間しか追跡することができないという状況はなく, ネットワークに多大なトラフィックを引き起こすこともない．また, 通信データをハッシュ値で効率よく保存できる．このことから, この組み合わせは有効であると考える．

3.3 通常時における処理とデータの流れ

本研究でのシステムでは, 通常時と追跡時の 2 種類の場合に分けて考える．まず, パケットの情報を蓄積し追跡命令に備える通常時の処理とデータの流れを**図 3** で説明する．

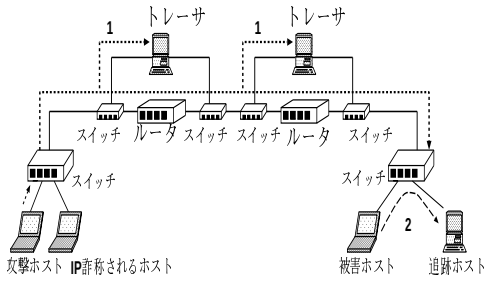

図 3: 通常時におけるネットワークモデル

通常時の処理とデータの流れは, **図 3** に示すように次の順となる．

1. 各ルータに流れ込むデータリンク層フレームは, スイッチのポートミラーリング機能を用いて, トレーサにも流し, それをハッシュ値として通信記録に保存させる．
2. 追跡ホストは, 被害ホストに届くデータリンク層フレームをハッシュ値として追跡ホストに一定の確率で送信し, 通信記録として保存する．

3.4 追跡時における処理とデータの流れ

次に, 追跡命令が発行されてから追跡完了までの追跡時の処理とデータの流れを**図 4** で説明する．

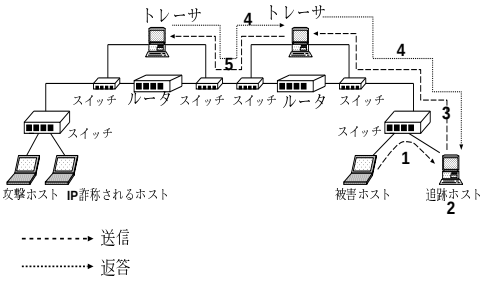

図 4: 追跡時におけるネットワークモデル

追跡時の処理とデータの流れは, **図 4** に示すように次の順となる．

1. 被害ホストが追跡ホストへ追跡命令を出し, 追跡を開始する．また, 被害ホストがダウンしていた場合は, 同じエンド側に接続している他のホストにより追跡命令を出す．
2. 追跡ホストでは, 同じ通信記録が多く保存してあるものを抽出する．
3. 同じ通信記録として保存されていたハッシュ値を追跡命令パケットとして隣接トレーサへ流す．
4. 隣接トレーサに流し, 受けとったら, 返答を返す．
5. トレーサに送られてきた追跡命令パケットを通信記録と比較して, 一致する通信記録が発見されたのなら, 次のトレーサへ追跡命令パケットを送信する．

   攻撃ホストまで検出成功した場合は, 命令を出したホスト宛に追跡結果を返す．

4 IP トレースバックの実装

この節では, IP トレースバックの構成要素であるトレーサ, 被害ホスト, 追跡ホストの処理内容を詳細に説明する．

4.1 通常時における詳細

最初に, 各装置の通常時における動作を説明する．

- 通常時のトレーサ

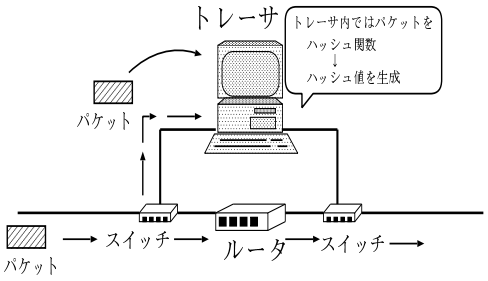

図 5: 通常時のトレーサ

左方からのパケットの流れの一部を**図 5** で示している．最初に, 通常時におけるトレーサを以下で説明する．

1. データリンク層フレームが, ルータへと中継される時, トレーサにも届くようにスイッチを用いて流す.
2. トレーサへ到着したパケットは, パケットキャプチャによってパケットを拾う.
3. パケットの特定の部分を取り出し, ハッシュ関数によって, ハッシュ値へと変換する.
4. 送信元 MAC アドレスもハッシュ値と一緒にハッシュテーブルに格納する.

- 通常時の被害ホストと追跡ホスト

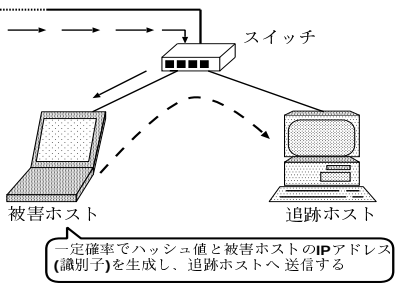

図 6: 通常時の被害ホストと追跡ホスト

通常時における被害ホストと追跡ホストの処理を**図 6** で示す. 以下の順に処理される.

1. 被害ホストまでデータがきたとき, 被害ホストは, ハッシュ関数でハッシュ値 (特定の部分をハッシュ値にするので, その部分を後で説明する) を生成し, 身分がわかる識別子 (IP アドレス) と一緒に, 一定の確率で追跡ホストへ送信する.
2. 受け取ったハッシュ値をハッシュテーブルで検索し, 同一のハッシュ値が存在するなら, そのカウントを更新する.
3. 同一のハッシュ値が存在しなれれば, そのハッシュ値と IP アドレスを保存する.

ハッシュ値

本研究では, データリンク層フレームを取り出しハッシュ値にする. そのさい, ルータで中継するときにパケット中で値が不変値であることが第一の条件である. 本研究では, **表 1** で示す部分を取り出し MD5 ハッシュ値に変換する.

表 1: ハッシュ値

IP ヘッダ	プロトコル, 送信元 IP アドレス, 送信先 IP アドレス, データ部分の 20Byte
TCP ヘッダ	送信元ポート, 送信先ポート
UDP ヘッダ	送信元ポート, 送信先ポート
ICMP ヘッダ	タイプ, コード

4.2 追跡時における詳細

最後に, 各装置の追跡時における詳細を説明をする. 追跡時の処理は, 通常時の処理と並行でしなければならないので, 本研究では別スレッドで実行する.

- 追跡時の追跡ホスト

追跡ホストの処理を以下の順に処理される.

1. 被害ホストから追跡命令が送られる. また, 被害ホストがダウンした時, 違うホストから追跡命令を送ることができる.
2. 追跡命令の中で, 被害ホストの IP アドレスが示されているので, その IP アドレスをもとに, 追跡ホストで保存しておいた最も数が多いハッシュ値を検索する.
3. 探し終えたら, そのハッシュ値と追跡命令を出したホストの IP アドレスをバッファに格納し, 隣接トレーサへと送信する.

- 追跡時のトレーサ

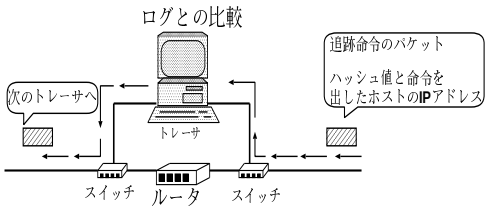

図 7: 追跡時のトレーサ

追跡ホストからの追跡命令のパケットがトレーサに届いた図を**図 7** で示し, 以下の順に処理される.

1. 追跡命令が届いたら, トレーサは, 通常時と共に追跡時のプログラムも起動させる.
2. 受け取り確認の返事を返す.
3. 現段階でハッシュテーブルに保存されているハッシュ値と, 送られてきたパケットのハッシュ値とを比較する.
4. 一致したハッシュ値が見つかれば, トレーサでハッシュ値と一緒に保存しておいた送信元 MAC アドレスを取り出す.
5. その MAC アドレス宛 (IP アドレスを調べて) に追跡命令のパケットを送信する. この操作については, 以下に示す.

トレーサへ追跡命令パケットが届いた場合, 上記に示したように, ハッシュ値から送信元 MAC アドレスを取り出す. 次に, 対応表を参照する. この対応表は, あらかじめ管理者がトレーサが置かれているルータの IP アドレスと, 隣接ルータの IP アドレスと, 隣接ルータの MAC アドレスを設定しておく. 対応表に検索した MAC ア

ドレスが存在すれば, 対応する IP アドレスを参照して, その IP アドレス宛に追跡命令パケットを送る．対応表に MAC アドレスが存在しなければ, 追跡先がないということで, 追跡完了とみなし, ハッシュ値と一緒に保存されている送信元 MAC アドレス (ここでいう攻撃者の MAC アドレス) を追跡完了メッセージとして, トレーサが置かれているルータの IP アドレスと共に, 追跡命令を出したホスト宛に結果を報告する．

5 実行結果

追跡命令を出してからの処理を**図 8** で示し, 本研究で試作したプログラムの実行結果を示す．

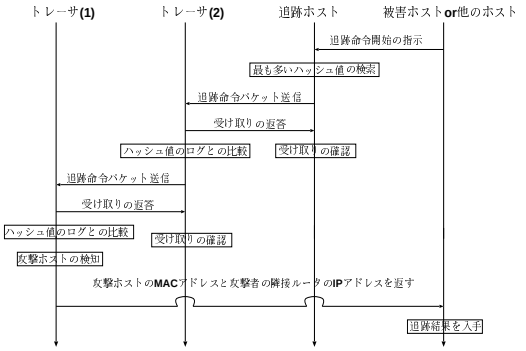

図 8: 追跡時におけるシーケンス例

1. 追跡結果
   追跡命令プログラムを実行した結果を示す．追跡が成功し攻撃ホストの MAC アドレスとその隣接ルータの IP アドレスを表示する．

   ```
   $ ./send 192.168.3.3
   ↑ 追跡命令を出したホストの IP アドレス
   IP trace SUCCEED!
   MAC: 00:00:0E:D8:6A:AA
   ↑ 攻撃者の MAC アドレス
   IP: 192.168.1.2
   ↑ 攻撃者の隣接ルータの IP アドレス
   ```

   追跡命令を出してから追跡結果を得るまでの処理を以下で示す．
2. 追跡ホストの処理
   全てのハッシュテーブルにおける最大カウントのハッシュ値を算出する．

   ```
   GETrecv!
   host 192.168.3.3   trace 192.168.3.3
   table:1  1 0 0 0 0 0 0
   table:2  1 7 1 2 1 4 1
   table:3  10 6 15 2 1 2 0
   hash :77838768fd27e7218ded1e6e199c6dc0
   ↑ 攻撃者の通信記録と思われるハッシュ値を算出
   ```

3. トレーサの処理
   対応表を用いて次のトレーサへ追跡命令を伝達する．

   ```
   send to recv message
   SRCH message recv!
   Hash: 98018e23cb376f762297f7cd1b1eeebe
   ↑ 追跡命令パケットのハッシュ値
   1:FIND! 2:FIND! 3:FIND!
   ↑ ハッシュ値がハッシュテーブルに存在
   reference_file match !!!
   ↑ 対応表に MAC アドレスが存在
   next tracer IP: 192.168.2.2
   ↑ 隣接トレーサの IP アドレス
   next router MAC:00:A0:DE:1E:25:CB
   ↑ 隣接ルータの MAC アドレス
   RECV message recv!
   ```

   追跡命令を受け取ったトレーサにおいて, 対応表中にこの MAC アドレスが存在しない場合, 次にメッセージを送信すべきトレーサが存在せず追跡完了とする．追跡命令を出したホストに対して追跡完了のメッセージと結果を送信する．

6 おわりに

既存手法のそれぞれの短所を補い長所を活かした IP トレースバック方式を検討した．そこで本研究では既存手法におけるロギング方式と逆探知パケット方式を組み合わせた IP トレースバック方式を提案した．実験ネットワーク環境において提案した手法を用いて実験をした結果, 攻撃者の MAC アドレスとその隣接するルータの IP アドレスを追跡することができた．本研究で提案した手法では,

1. ルータの設定を変えずに実装可能
2. トラフィック増大の影響をあまり受けない
3. 攻撃中に追跡を完了する必要はない

などの利点がある．本研究では, AS 内の IP トレースバック技術を扱ってきたが, 管理者の異なるネットワーク間での IP トレースバックを実現するためには, 管理者間の協力が必要となり, 課題が残る．

参考文献

[1] 池田 竜朗, 山田 竜也, 発信源追跡のためのハイブリットトレースバック方式, http://www.toshiba.co.jp/tech/review/2003/08/58_08pdf/a10.pdf, 2003

[2] 門林 雄基, 大江 将史, IP トレースバック技術, 情報処理学会論文誌, Vol.42, No.12, pp.1175–1180 (2001).

[3] 大谷 尚通, IP アドレス詐称パケットの追跡技術, http://www.bcm.co.jp/site/2003/2003Sep/techo-trend3/techo-trend3.htm, 2003