

サービス不能攻撃の経路追跡手法の効率化に関する検討

岡崎 直宣[†] 河村 栄寿[†] 朴 美娘^{††}

近年、インターネットの安全性を脅かすサービス不能 (DoS: Denial of Service) 攻撃が大きな問題となっている。本稿では、DoS 攻撃パケットの送信元を追跡する技術の 1 つであるマーキング方式について検討し、そこで課題となる攻撃経路を特定する際の追跡のために必要となる情報量を削減し、攻撃者を特定するまでにかかる時間を改善する手法を提案する。

A Study of an Efficient Method for Re-construction of Path in the DoS Attacks

NAONOBU OKAZAKI,[†] SHIGEHISA KAWAMURA[†] and MIRANG PARK^{††}

Recently, frequency of Denial of Service attacks are increased, and it is difficult to trace packets with incorrect, or "spoofed", source address. This paper discuss a method to trace flooding attacks by marking packets, and proposes an extended method to reduce the computation time for reconstruction of a path back to the attacker.

1. はじめに

インターネットへの常時接続環境が整ってくるとともに、その安全性を脅かす様々な脅威、なかでも DoS (Denial of Service) やその分散型である DDoS (Distributed DoS) と呼ばれるサービス不能攻撃が大きな問題となっている。DoS 攻撃などで送信されるパケットの送信元アドレスは偽装されていることも多く、攻撃の送信元の特定は困難となっている。

送信元アドレスが偽造されている DoS や DDoS 攻撃の送信元を追跡するための手法としては IP トレースバックと呼ばれる技術があり、リンク検査手法、ログ解析手法、ICMP トレースバック、マーキング手法などいくつかの手法が提案されている¹⁾。このうち、マーキング手法は流れているパケットそのものに追跡のための情報を付与する方法である。この代表的なものとして、Savage らの方法²⁾ (以下、マーキング法) がある。マーキング法では IP ヘッダの特定のエリアに追跡のための情報を分割して挿入し、攻撃対象へ送

り届ける。マーキングされたパケット (以下、マーキングパケット) を受け取った攻撃対象は、複数のマーキングパケットから分割される前の情報を元どりに復元し、攻撃パケットが送られてくる経路 (攻撃経路) を再構築する。この攻撃経路は、DDoS 攻撃のように複数の送信元から攻撃パケットが送られてくる場合を考慮すると、一般には攻撃対象を根とするツリーを形成する。

マーキング法では、複数の攻撃経路を再構築する際に分割されたデータを復元する過程において莫大な計算量を要するという課題がある。これに対し、Song らは攻撃対象がネットワーク構成を知りうる場合において、効率的に攻撃経路を推定する手法を提案している³⁾。本稿では、特にこのような限定を必要としない場合について考える。ここでは、マーキング法において課題となる攻撃経路を特定する際の計算量を削減し、攻撃者を特定するまでにかかる時間を改善するための検討について報告する。

以下、まず 2 章でマーキング法の概要について紹介する。3 章では既存手法の課題と、それを解決するために本稿が提案するマーキング法の拡張について述べる。4 章では攻撃経路を特定する際の計算量の観点からの評価を示し、マーキング法と提案する手法とを比較する。5 章はまとめと今後の課題である。

[†] 宮崎大学工学部
Faculty of Engineering, University of Miyazaki

^{††} 三菱電機株式会社情報技術総合研究所
Information Technology R&D Center, Mitsubishi Electric Corporation

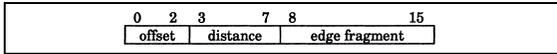


図1 識別子フィールド
Fig.1 Identification field.

2. マーキング法

2.1 マーキングの手順

流れているパケットにマーキングをするためには IP パケットのいずれかの部分に追跡のための情報を格納するフィールドが必要になる。IP ヘッダのうち 16 ビットの識別子 (identification) フィールドはフラグメント化されたパケットを結合する際の識別子として用いられる。マーキング法では、フラグメント化されたパケットはインターネットを流れるトラフィック全体からみてもごくわずかな量である¹⁾との前提のもとで、この識別子フィールドを追跡のための情報を格納するために利用している。そして、図 1 のように識別子フィールドを 3 つに分割し、これらのフィールドに追跡のための情報を格納する。分割後の各フィールドに追跡情報を格納する手順を以下に示す。

【マーキング手順】

- (1) 準備
 - (a) ルータは起動時に自分自身の IP アドレスのハッシュ値を計算しておく。
 - (b) ルータは IP アドレスとハッシュ値をビットインタリーブする。このとき、IP アドレスは奇数ビットに、またハッシュ値は偶数ビットに挿入するものとする。
 - (c) ビットインタリーブした 64 ビットの値 (以下、インタリーブ値) を k 分割する ($k = 2^i, i = 1, \dots, 5$)。マーキング法では $k = 8$ である。以下、分割した値をフラグメントと呼ぶ。
- (2) 初期マーキング
 - (a) ルータは、自分自身を通過するパケットのうち確率 p でマーキングをするものを選ぶ。
 - (b) 選んだパケットについて以下を行う。
 - 0 から $k - 1$ までの整数 j をランダムに選び、 j 番目のフラグメントをパケットの識別子フィールドのエッジフラグメント (edge fragment) フィールドに書く。
 - j をオフセット (offset) フィールドに書く。
 - マーキングしたルータから攻撃対象まで何個のルータを通過したかを示すディスタンス (distance)

初期マーキングの手順では、すでにマーキングされているパケットであるかどうかにかかわらず、一定の確率 p でマーキングされることに注意。

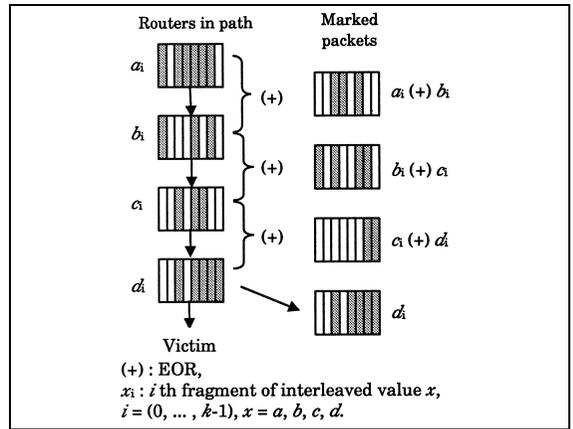


図2 マーキングの手順
Fig.2 Marking procedure.

フィールドの値を 0 として下流のルータに送る。
(c) 選ばれなかったパケットについては、以下の (3) または (4) を行う。

(3) 終端マーキング

ディスタンスフィールド値が 0 であるパケットを受け取ったルータ (初期マーキングを行ったルータの次ホップのルータ) は、以下を行ってそのパケットを下流のルータに転送する。

- 自分自身のインタリーブ値のフラグメントのうち、パケットのオフセットフィールド値と同じ部分 (j 番目) のものと、パケットのエッジフラグメントフィールド値との EOR (排他的論理和) を求める (図 2)。この値をエッジ ID と呼ぶ。
- エッジフラグメントフィールドの値をエッジ ID に書き換える。
- ディスタンスフィールドを 1 増加させる。

(4) 転送ルータによる処理

ディスタンスフィールド値が 0 でないパケットを受け取ったルータ (攻撃対象までの間でマーキングされたパケットが通過するルータ) では、ディスタンスフィールド値を 1 ずつ増やしていく。

2.2 攻撃経路の再構築

攻撃対象に集められたマーキングパケットを再構築する過程において、攻撃経路が一直線である場合には、各ルータどうしのマーキングパケットのディスタンスフィールド値が重複することはないため、攻撃経路は一意に決まる。しかし複数の攻撃者が存在し各攻撃経路が部分的にでも独立していると、他のルータが

複数の攻撃パケットの送信元があり、それらが攻撃対象への経路上にたまたま一列に並んでいた場合には、一番遠い送信元からの経路が 1 つ求まる。

送ったマーキングパケットと同じディスタンスフィールド値とオフセットフィールド値を持つ場合がありうる。そのため、同じディスタンスフィールド値の任意のフラグメントを結合してインタリーブ値を復元し、その奇数ビットに割り当てられた IP アドレスから求められたハッシュ値と偶数ビットに割り当てられたハッシュ値とが同じ値になれば復元されたインタリーブ値は正当なものであると判断する。同じ値にならなかった場合は、フラグメントの違う組合せを試し、正当なインタリーブ値と認められるまで同じことを繰り返す（このようにして正しいインタリーブ値を求める手順を以下では復元手順と呼ぶことにする）。

以下に、攻撃経路を再構築するための手順を示す。ここでは、ディスタンスフィールド値が i のエッジ ID から復元手順により求められたインタリーブ値をディスタンス (i) のインタリーブ値と呼ぶ。

【再構築手順】

- (1) 攻撃対象はディスタンスフィールド値が 0 のマーキングパケットを集め、復元手順によりディスタンス (0) のインタリーブ値を導出する。
- (2) ディスタンス (i) のインタリーブ値が求められているものとする。ディスタンスフィールド値が $i+1$ のエッジ ID を集め、それぞれのオフセットフィールド値に対応するディスタンス (i) のインタリーブ値の部分との EOR を求める。
- (3) これらの値から復元手順によりディスタンス ($i+1$) のインタリーブ値を求める。
- (4) 攻撃パケットの送信元に最も近いルータのインタリーブ値を導出するまで (2), (3) を繰り返し、1 ホップずつ上流のルータに遡って順次計算する。

3. マーキング法の拡張

3.1 既存方式の課題

従来のマーキング法では、IP ヘッダに追跡のための情報を格納する領域が十分でないため、インタリーブ値をフラグメントに分割して送る。そのため攻撃対象は攻撃経路を再構築するために多数のマーキングパケットを集め、これから復元手順により元のインタリーブ値を復元する。このとき、攻撃パケットのうちそれがマーキングパケットであるかどうかを識別することができないため、マーキングパケットのフラグメントだけでなくマーキングされていない攻撃パケットのフラグメントとの組合せも調べなければならない。したがって、復元手順の際にフラグメントの組合せ数が爆発するという問題が生じた。そのために攻撃経路の再構築に時間がかかり、実用上の課題となっている。

```

Marking procedure at router R:
let  $R' = \text{Bitinterleave}(R, \text{Hash}(R))$ ;
let  $k$  be the number of non-overlapping fragment in  $R'$ ;
for each packet  $w$ 
  let  $x$  be a random number from  $[0..1]$ ;
  let  $M$  be a number from  $[0,1]$ ; //(*1)
  if  $x < p$  then
    let  $n$  be random integer from  $[0..k-1]$ ;
    let  $f$  be the fragment of  $R'$  at offset  $n$ ;
    write  $f$  into  $w.\text{frag}$ ;
    write 0 into  $w.\text{distance}$ ;
    write  $n$  into  $w.\text{offset}$ ;
  else
    if  $w.\text{distance} = 0$  then //(*2)
      let  $f$  be the fragment of  $R'$  at offset  $w.\text{offset}$ ; //(*3)
      write  $f(+)$   $w.\text{frag}$  into  $w.\text{frag}$ ; //(*4)
      write 1 into  $w.M$ ; //(*5)
      increment  $w.\text{distance}$ ;
    else
      let  $FlagTbl$  be a table of tuples (frag, offset, distance, M);
      let  $G$  be a tree with root  $v$ ;
      let edges in  $G$  be tuples (start, end, distance);
      let  $maxd := 0$ ;
      let  $last := v$ ;
      for each packet  $w$  from attacker
         $FlagTbl.Insert(w.\text{frag}, w.\text{offset}, w.\text{distance}, w.M)$ ;
        if  $w.M = 0$ 
          continue; //(*6)
        if  $w.\text{distance} > maxd$  then
           $maxd := w.\text{distance}$ ;
      for  $d := 0$  to  $maxd$ 
        for all ordered combinations of fragments at distance  $d$ 
          construct edge  $z$ ; //(*7)
          if  $d != 0$  then
             $z := z (+) lastz$ ;
            if  $\text{Hash}(\text{OddBits}(z)) = \text{EvenBits}(z)$  then
              insert edge ( $last, \text{OddBits}(z), d$ ) into  $G$ ;
               $last := \text{OddBits}(z)$ ;
               $lastz := z$ ;
          remove any edge  $(x, y, d)$  with  $d != \text{distance from } x \text{ to } v$  in  $G$ ;
          extract path  $(R_1 \dots R_k)$  by enumerating acyclic paths in  $G$ ;

```

図 3 識別マーキング法のアルゴリズム

Fig. 3 Proposed algorithm.

3.2 識別マーキング法

ここではマーキング法の課題である、攻撃経路再構築時におけるフラグメントの組合せ数の爆発問題を緩和し、攻撃経路の再構築にかかる時間を短縮できるように拡張した手法（以下、識別マーキング法）を提案する。

図 3 に識別マーキング法の提案アルゴリズムを示す。識別マーキング法では、IP ヘッダ内の識別子フィールドに設けたオフセットフィールド（図 1）の上位 1 ビット分について、マーキングパケットかそれ以外のパケットかを識別するために用いることとする（このビットを以下では M ビットと呼ぶ）（図 3 (*1), 以下同様）。そして、ディスタンスフィールドが 0 であるパケットを受け取ったルータがマーキングを行う際（終端マーキング）(*2) に、オフセットフィールドの値を参照してエッジ ID をエッジフラグメントフィールドに書いた (*4) 後に、このビットに $M = 1$ の値を設定 (*5) する。さらに、インタリーブ値の復元手順の際には、集められた攻撃パケットから $M = 1$ であるパケットのみを対象としてフラグメントの組合せを試す (*6) ようにする。これらのことにより、復元手順の際にフラグメントの組合せ数が爆発する問題を緩和することができる。

なお、オフセットフィールド値はマーキング手順の終端マーキングにおいてエッジ ID を求める際(*3)と、攻撃経路の再構築の手順においてインタリーブ値を復元する際(*7)に用いられる。M ビットは終端マーキングの際に、初期マーキングで設定されたオフセットフィールドを参照してエッジ ID を求めた後に設定されるため、エッジ ID の値そのものには影響しない。ただし、インタリーブ値の復元においては、候補となるフラグメントの組合せを考える際に、各フラグメントの位置について 2 通りの可能性がある点に注意が必要である。

4. 評価

ここでは、攻撃経路を再構築するために必要な時間の観点から評価を行う。以下では、すべてのルータは確率 p で通過するパケットにマーキングを行うものとし、攻撃対象から d ホップ離れたルータ R_d から攻撃対象 V までの経路

$$R_d, R_{d-1}, \dots, R_1, V$$

を再構築する場合について考える。

攻撃経路を再構築するためのアルゴリズムの収束時間は、攻撃対象が観察しなくてはならない攻撃パケットを集めるのにかかる時間と、インタリーブ値の復元手順にかかる時間である。このうち、前者は攻撃経路を再構築するために収集しなければならないパケット数に比例すると考えられる。この収集パケット数の期待値 $E(X)$ は、

$$E(X) < \ln(kd)/p(1-p)^{d-1} \quad (1)$$

で与えられる²⁾。式(1)はマーキング法、識別マーキング法ともに成り立つ。たとえば $p = \frac{1}{25}$, $d = 10$ の場合、攻撃対象は平均して 1,300 以下の攻撃パケットを受け取るにより攻撃経路を再構築することができる。

一方、後者については、復元手順において調べるフラグメントの組合せ数に依存し、これは識別マーキング法とマーキング法は異なる値となる。以下では、フラグメントの組合せ数について検討し、両者の比較を行う。

まず、各ルータが通過するパケットにマーキングをする確率は p であるため、ルータ R_d によりマーキングされたパケットが下流のルータ R_{d-1}, \dots, R_1 によって上書きされない確率は $p(1-p)^{d-1}$ である。したがって、ルータ R_d から 1 つのマーキングパケットを受け取るために観察しなければならない攻撃パケット数の期待値 Q は $Q = 1/p(1-p)^{d-1}$ となる。こ

で、一般に識別子フィールドの値は実装に依存して不定であるため、その値だけからそのパケットがマーキングパケットであるかどうかを判断することができない。すなわち、マーキング法ではルータ R_d が実際にマークしたパケットを、集めた Q 個のパケットの中から識別することができない。したがって、復元手順において各フラグメントについて Q 通りすべての組合せについて試みる必要がある。たとえば、 d ホップ離れたルータが m 個あるとすると、組合せの候補となるフラグメントの種類が Qm あることになる。このとき、これらの k 個の組合せは $(Qm)^k$ 通りである。ただし、ここでは 1 つのフラグメントのビット数は $64/k$ であるので、 Qm の上限は $2^{\frac{64}{k}}$ である。

一方、識別マーキング法では、同様にルータ R_d によるマーキングパケットを得るために必要なパケットは平均 Q 個であるが、そのうち M ビットの値によりルータによって実際にマークされたパケットであることを識別できる。したがって、 d の距離に m 個のルータがある場合のフラグメントの組合せは、オフセットフィールドの上位 1 ビットを M ビットと使用していることを考慮して、たかだか $(2m)^k$ 通りである。

以上より、たとえば $p = \frac{1}{25}$, $d = 10$, $m = 10$ の場合、マーキング法では Qm の値が上限の 256^8 となり、約 1.8×10^{19} 通りもの組合せがある。一方、識別マーキング法では 2.56×10^{10} 通りの組合せである。これらのことより、識別マーキング法では、攻撃経路の再計算がマーキング法に比十分少なくなると考えられる。

5. まとめ

本稿では、IP トレースバック技術のうち、ネットワークに対する負荷が低いなどの利点を持つマーキング手法に関して検討した。そして、そこで課題となっている、攻撃経路の再構築に時間がかかるという問題に着目し、これを解決するための拡張手法を提案した。ここでは特に、マーキングパケットであることを識別するための情報を付加することにより、フラグメントを結合する際の組合せ爆発の問題を緩和し、実用的な計算量で攻撃経路の再構築を行うことができる可能性を示した。

今後の課題としては、各ルータがマーキングを行う確率を変化させることにより、集めなければならないパケットの数とフラグメントを結合する際の組合せ数が変わってくるため、その値をどのように設定すればよいかを検討する必要がある。また、マーキングパケットであることを識別するための情報を偽って付加され

たパケットが大量に送られるような攻撃に対する対処や、IP ヘッダの特定の領域に情報を埋め込むことによる既存の通信への影響についても今後検討していきたい。さらに、提案した手法の実装を行い、実用的なパフォーマンスを得られるかどうかを検証することも必要と考える。

参 考 文 献

- 1) 門林雄基, 大江将史: IP トレースバック技術, 情報処理, Vol.42, No.12, pp.1175–1180 (2000).
- 2) Savage, S., Wetherall, D., Karlin, A. and Anderson, T.: Practical Network Support for IP Traceback, *Proc. SIGCOMM '00*, pp.295–306 (2000).
- 3) Song, D. and Perrig, A.: Advanced and Authenticated Marking Schemes for IP Traceback, *Proc. IEEE INFOCOM 2001*, pp.878–886 (2001).
- 4) 河村栄寿, 岡崎直宣, 中谷直司, 厚井裕司, 朴美娘: ネットワークサービス不能攻撃の追跡手法に関する一検討, 情報処理学会夏の国情報シンポジウム 2003 予稿集, pp.168–175 (2003).

(平成 15 年 8 月 11 日受付)

(平成 15 年 10 月 16 日採録)



岡崎 直宣 (正会員)

昭和 61 年東北大学工学部通信工学科卒業。平成 3 年東北大学大学院工学研究科電気及通信工学専攻博士後期課程修了。同年三菱電機(株)入社。平成 14 年より宮崎大学工学部助教授。通信プロトコルの形式仕様記述, ネットワークセキュリティ等の研究に従事。博士(工学)。電子情報通信学会, 電気学会, IEEE 各会員。



河村 栄寿 (学生会員)

平成 15 年宮崎大学工学部情報システム工学科卒業。現在, 宮崎大学大学院工学研究科博士前期課程在学中。ネットワークセキュリティの研究に従事。



朴 美娘 (正会員)

昭和 58 年漢陽大学工学部電子工学科卒業。同年漢陽大学工学部助手。平成 5 年東北大学大学院工学研究科情報工学専攻博士後期課程修了。同年東北大学電気通信研究所助手。平成 6 年三菱電機(株)入社。通信プロトコルの試験系列生成法, ネットワークセキュリティ等の研究に従事。博士(工学)。電気学会会員。