本資料について

本資料は下記論文を基にして作成されたものです。
文章の内容の正確さは保障できないため、正確な知識を求める方は原文を参照してください。

著　者：岡崎　直宣，河村　栄寿，朴　美娘
論文名：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
出　展：情報処理学会論文誌, Vol.44, No.12, pp.3197-3210
発表日：Dec. 2003

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

原文
岡崎　直宣，河村　栄寿，朴　美娘

発表
渡邊研究室　播磨　宏和

はじめに

- インターネットへの常時接続環境

  様々な脅威
  - DoS(Denial of Service)
  - DDoS(Ditributed DoS)

- 送信元アドレス
  - 偽造

  攻撃の送信元特定は困難

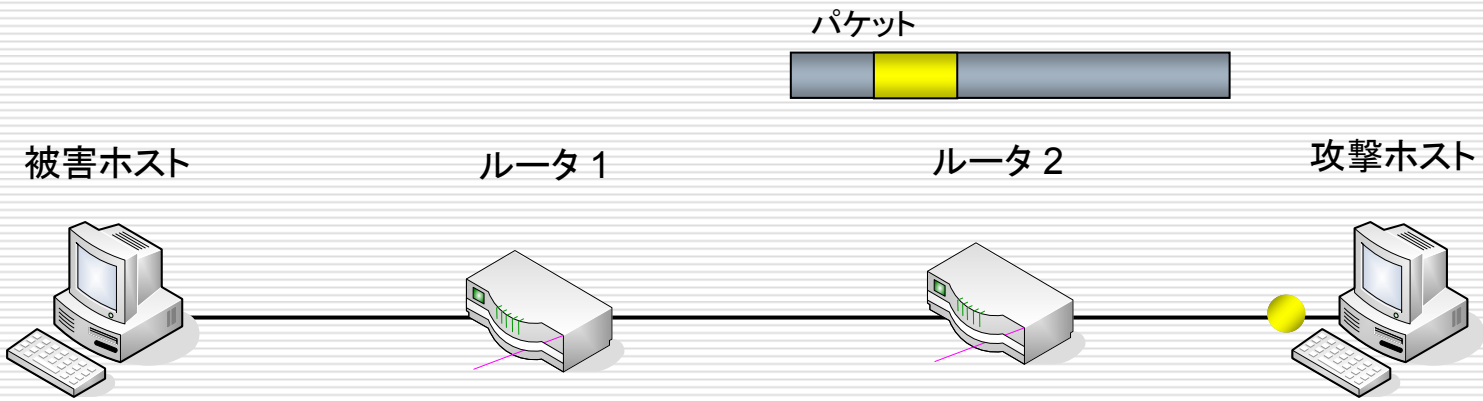
IPトレースバック技術

IPトレースバック

- 攻撃の発信元を追跡する手法
  - 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

- Savageらの手法
  - （Savage, S., Wetherall, D., Karlin ,A. and Anderson, T.:Practical Network Support for IP Traceback, Proc. SIGCOMM ’00 , pp.295-306 (2000).）

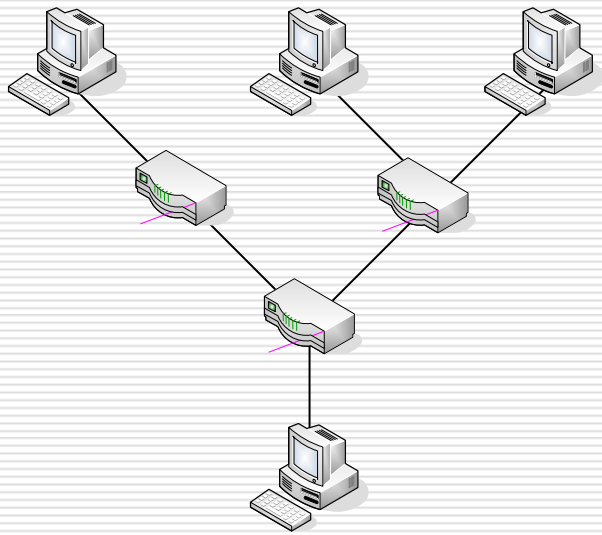
マーキング手法の概要



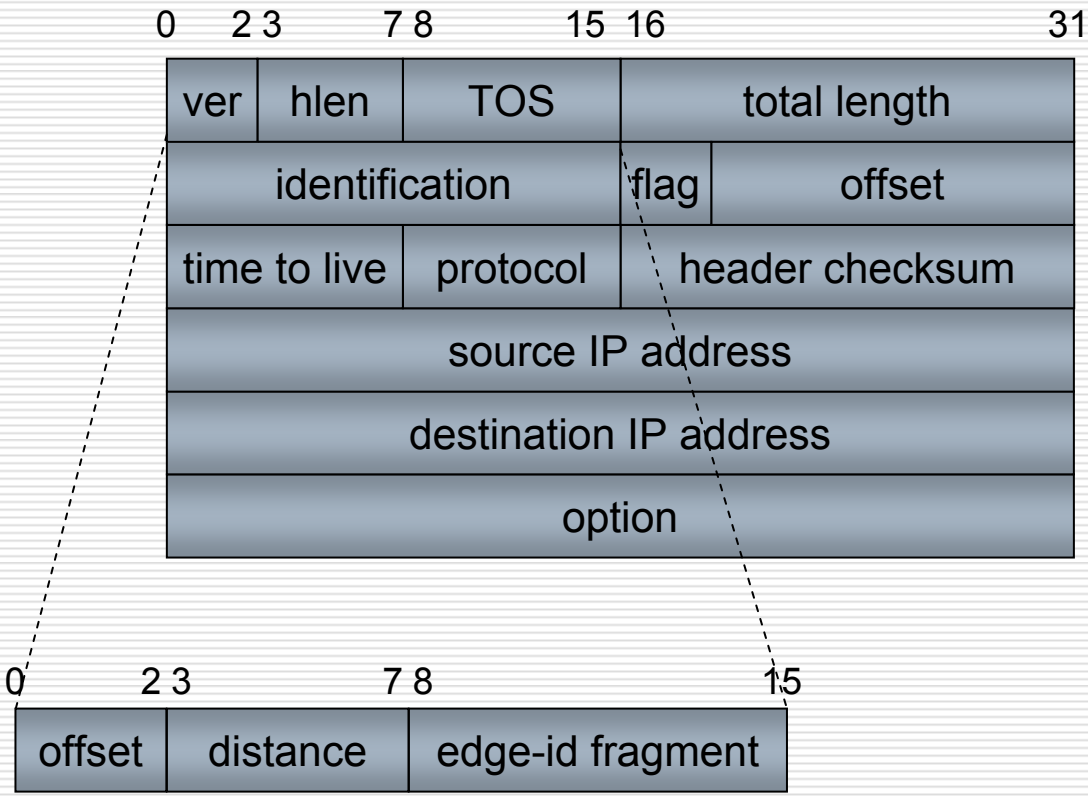
DDoS攻撃

複数の送信元からの攻撃パケット

攻撃対象を根とするツリーを形成



追跡情報の格納フィールド

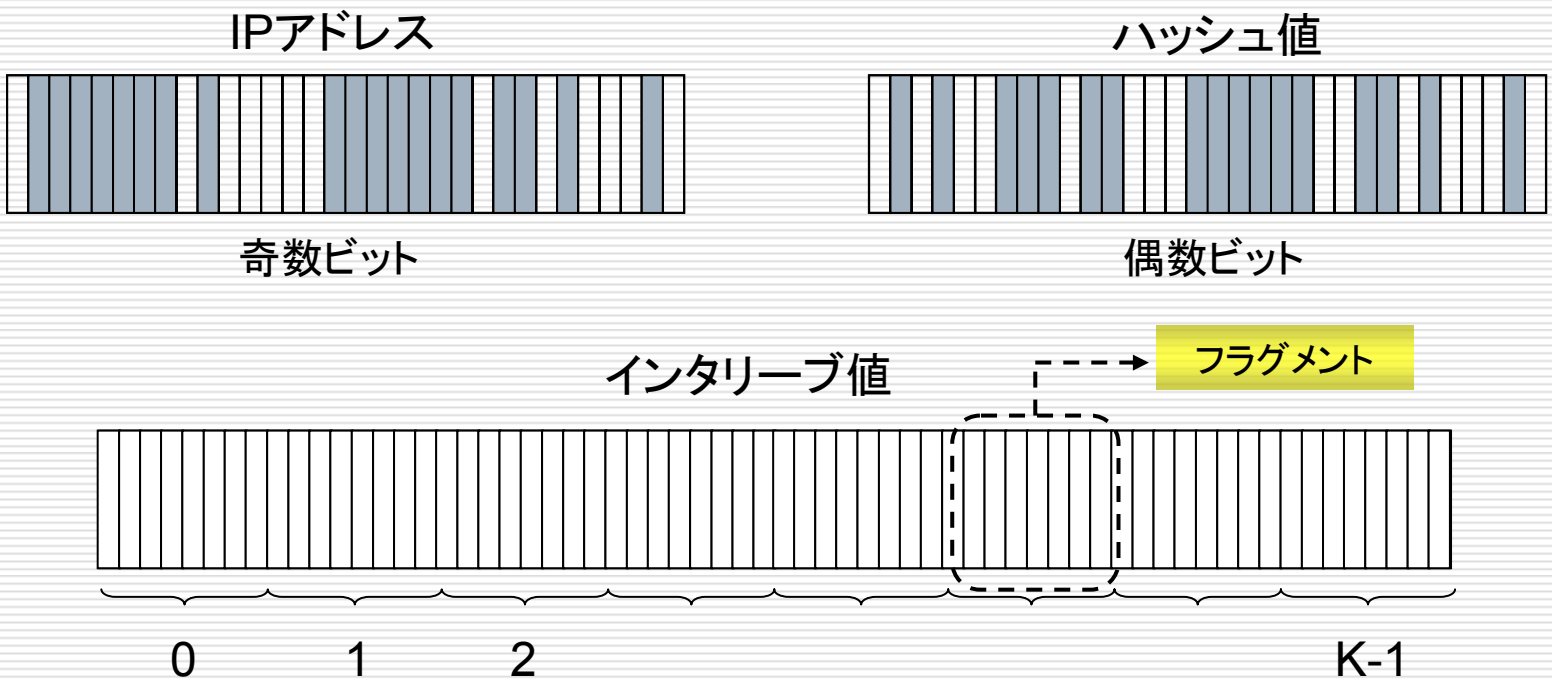


マーキング手順

1. 準備
2. 初期マーキング
3. 終端マーキング
4. 転送ルータによる処理

マーキング手順
1.準備

A) IPアドレスのハッシュ値を計算
B) IPアドレスとハッシュ値をビットインタリーブ（交互配置）する
C) ビットインタリーブ値をk分割する（マーキング法ではk=8）



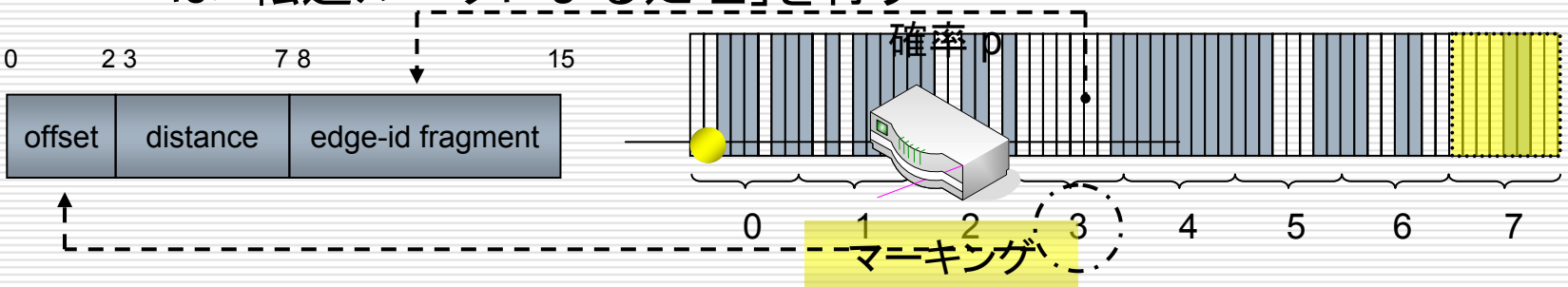
マーキング手順
2.初期マーキング

A) 確率pでマーキングするパケットを選ぶ

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
- ディスタンス(distance)フィールドの値を0として下流ルータに送る

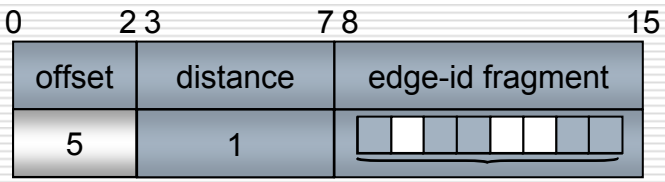
C) 選ばれなかったパケットはマーキング手順「終端マーキング」又は「転送ルータによる処理」を行う

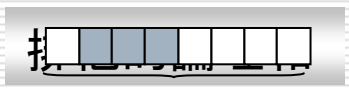


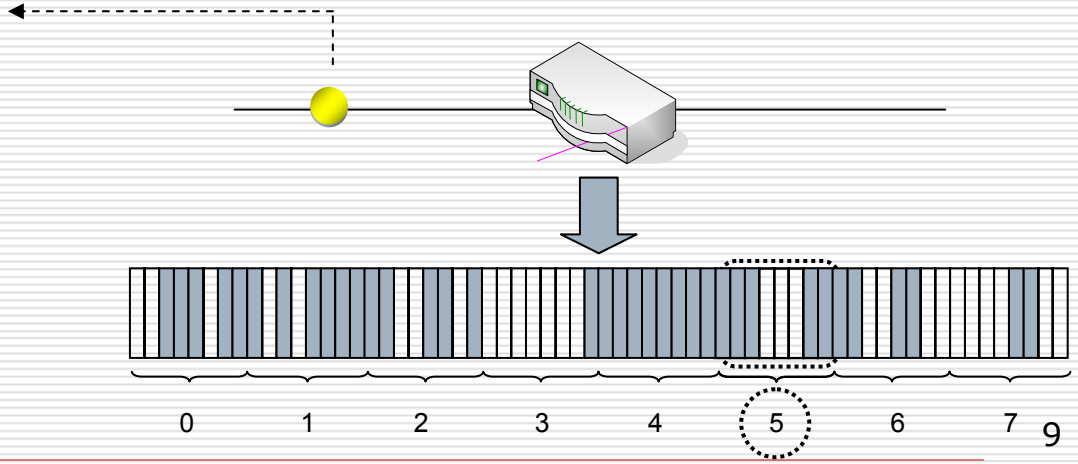
マーキング手順
3.終端マーキング

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※は以下を行ってパケットを下流ルータに転送する

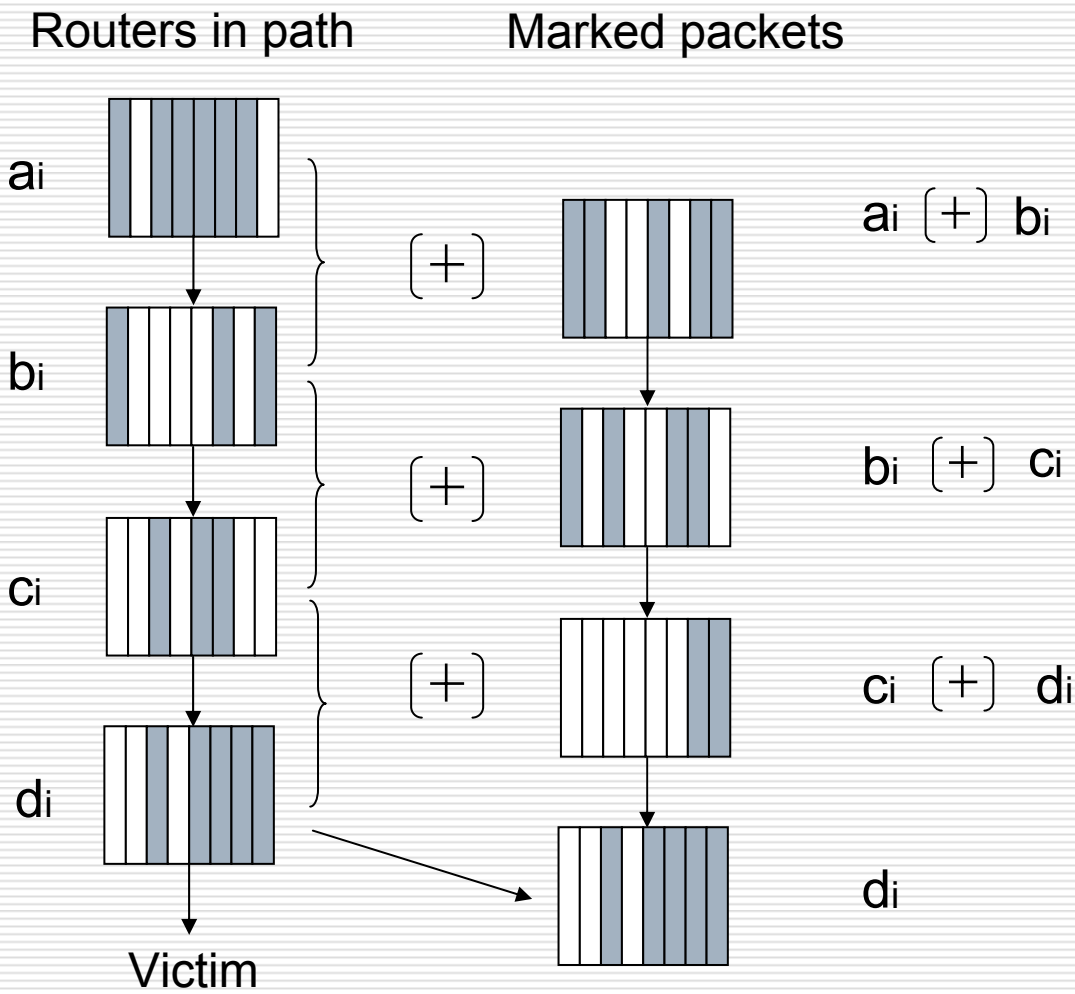
- 自分自身のインタリーブ値のフラグメントのうち、パケットのオフセットフィールド値と同じ部分（j番目）のものと、エッジフラグメントフィールド値との排他的論理和を求める（エッジID）
- エッジフラグメントフィールドの値をエッジIDに書き換える
- ディスタンスフィールドを1増加させる





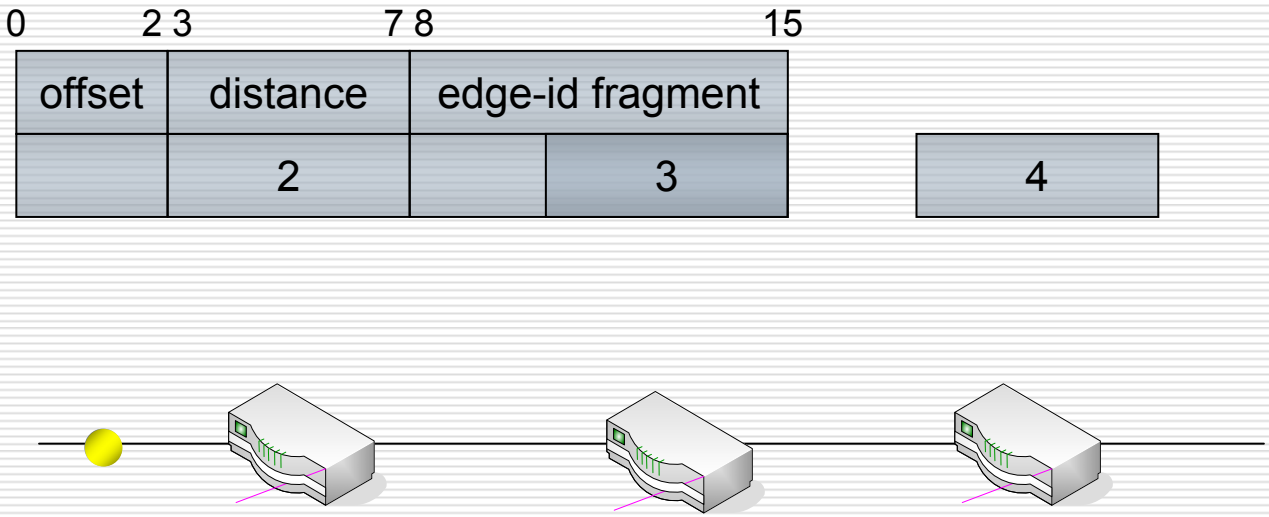


マーキングの手順
排他的論理和



マーキング手順
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※では、ディスタンスフィールド値を1ずつ増やしていく



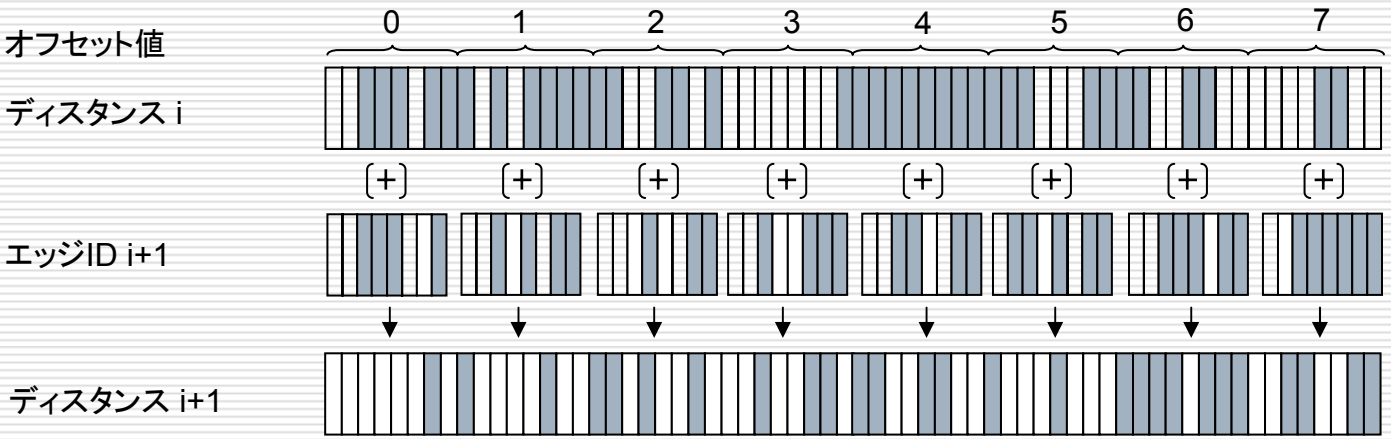
復元手順

1. 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
2. インタリーブ値を復元
3. 奇数ビットに割り当てられたIPアドレスがハッシュ値と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
4. 同じ値にならなかった場合は、フラグメントの違う組み合わせを試す

ディスタンス(i)のインタリーブ値:
復元手順により求められたインタリーブ値

再構築手順

1. ディスタンス(0)のインタリーブ値を導出
2. 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. ディスタンス(i+1)のインタリーブ値を求める
4. 2.、3.を繰り返し、1ホップずつ上流ルータを順次計算する



既存方式の課題

従来のマーキング法

攻撃パケットのうちマーキングパケットであるかを識別できない

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を調べなければならない

フラグメントの組合わせ数が多大

攻撃経路の再構築に多大な時間を要する

マーキング法の拡張

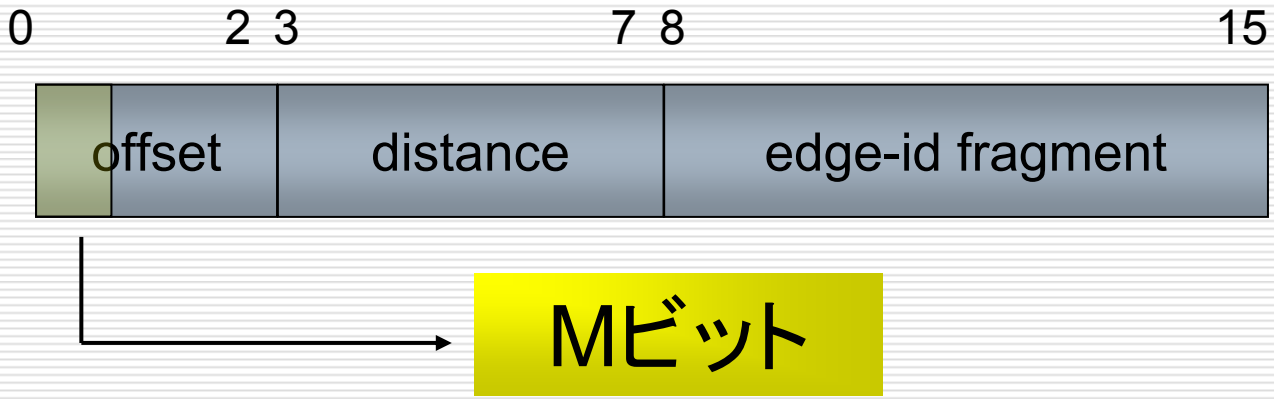
識別マーキング法

攻撃経路再構築時におけるフラグメントの組合せ数の増加問題を緩和し、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

識別マーキング法
拡張

- オフセットフィールド

  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



識別マーキング法
提案アルゴリズム

マーキング手順

終端マーキングにおいて

- オフセットフィールドの値を参照
- エッジIDをエッジフラグメントフィールドに記入
- オフセットフィールドのMビットをM＝1の値を設定

識別マーキング法
提案アルゴリズム

インタリーブ値復元手順

- 収集し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み合わせを試す

識別マーキング法
注意点

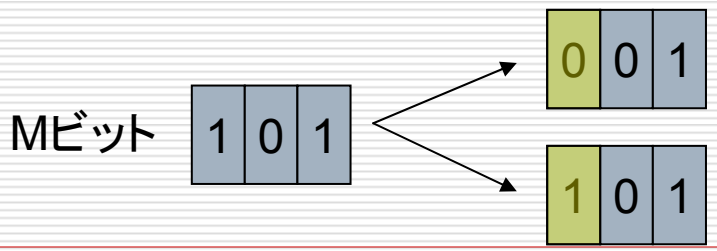
- 終端マーキングにおいて

  Mビット

  終端マーキングの際にはエッジIDの値そのものに影響しない

- インタリーブ値

  フラグメントの位置について2通りの可能性



まとめ

IPトレースバック技術のうち、攻撃経路の再構築に時間がかかるという問題を解決するための拡張手法を提案した

今後の課題

- 各ルータのマーキング確率
  - 収集するべきパケット数
  - フラグメント結合における組合せ数
- 識別情報の偽造
- 識別子（identificationフィールド）の考慮
  - パケットの断片化
  - 既存の通信への影響

評価

- 収集パケットの期待値
  - $E(X)<\ln(kd)/p(1-p)^{d-1}$
  - 1300以下の攻撃パケットで再構築可能
- マーキング法
  - $(Qm)^k$通り
- 識別マーキング法
  - $(2m)^k$通り