MAC アドレスを用いた IP トレースバックの提案

播磨　宏和*，渡邊　晃（名城大学）

The proposal of IP trace back using MAC Address

Hirokazu Harima, Akira Watanabe (Meijo University)

1.　はじめに

インターネット人口の増大に伴い、セキュリティにかかわる被害規模が拡大している。その中でもサービス不能攻撃（DoS 攻撃）は防御が難しく、巧妙に身元を隠してシステムを機能不全にしてしまう。この攻撃に対して身元を探索するのが IP トレースバック技術である[1]。しかし、IP アドレスの送信元は多くの場合偽造されており、攻撃パケットの発信源を即座に特定するのは困難である。

本研究では攻撃パケットの MAC アドレス情報から上位ルータを特定し、発信源までの経路を追跡するトレースバック方式を提案する。

2.　既存の IP トレースバックとその課題

現在、DoS 攻撃を阻止する有効な手段は確立されていない。一般の攻撃に対してはファイヤウォールやルータのフィルタリング等により阻止できるが、DoS,DDoS 攻撃は正常な攻撃を装うため防止困難である。また、アドレスが偽造されているため犯人の特定は容易ではない。

Input-debugging 方式はルータのデバッグ機能を利用したものであるが、被害者は攻撃を受けた時点で DoS パケットを分析しなければならないことから、パケットの特徴抽出が難しいとされている。

逆探知パケットおよび、マーキング方式は各ルータにおいて、通過するパケットについてある確率で経路情報の一部をのせるが、攻撃パケット数が少ない場合には、発信源を特定できない。

また､Hash トレースバック方式はパケットのダイジェストを利用するので、攻撃パケットが 1 個あれば発信源を特定できるが、大きな記憶容量や高いハッシュ処理能力が必要とされるため、コスト面において不利になる。

3.　提案方式

図 1 に MAC アドレスを用いた IP トレースバックを示す。各ホスト、ルータの MAC アドレス、IP アドレスは図中に示すように構成されているものとする。図 1 には攻撃パケットの MAC アドレスがルータを通過するたびに入れ替わっていく様子が示されている。ホスト又はルータは受信バッファに残されている MAC アドレスを見ることにより上流のノードを知ることができる。

被害ホストは自分が攻撃を受けていることを検知すると攻撃ホストまでの経路を特定するため、受信したパケットの送信元 MAC アドレス y_mc を持つ上流ノードに対して問合せパケットを送信する。問合せを受けたルータ Y は受信バッファ内の攻撃パケットを検索し、パケットの送信元 MAC アドレスへ次の問合せを行う。これを順に繰り返すことで発信源までの経路情報を調べることができる。

提案方式では大量の攻撃パケット数を必要とせず、コスト面においても有効なトレースバックが可能である。

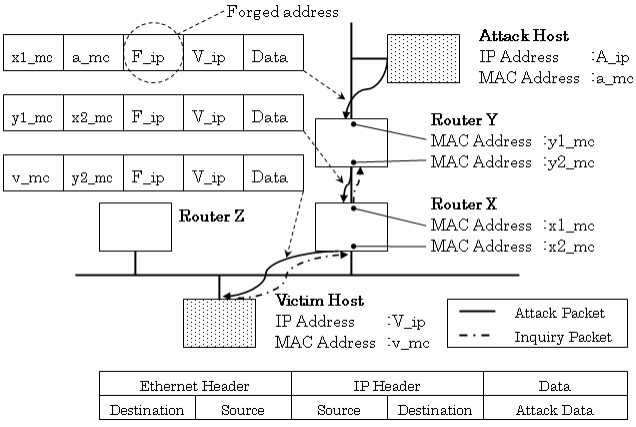


Fig.1 MAC アドレスを用いた IP トレースバック

4.　まとめ

本研究では、MAC アドレスを用いた IP トレースバックの提案を行った。本方式を実装することにより本方式のオーバーヘッドやルータにかかる負荷などについて既存技術と比較していく。

文献

[1]門森 雄基, 大江 将史：IP トレースバック技術, IPSJ Magazine Vol.42(Dec.2001)

[2]岡崎 直宣, 河村 栄寿, 朴 美娘：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, 情報処理学会論文誌 Vol.44,No12(Dec.2003)

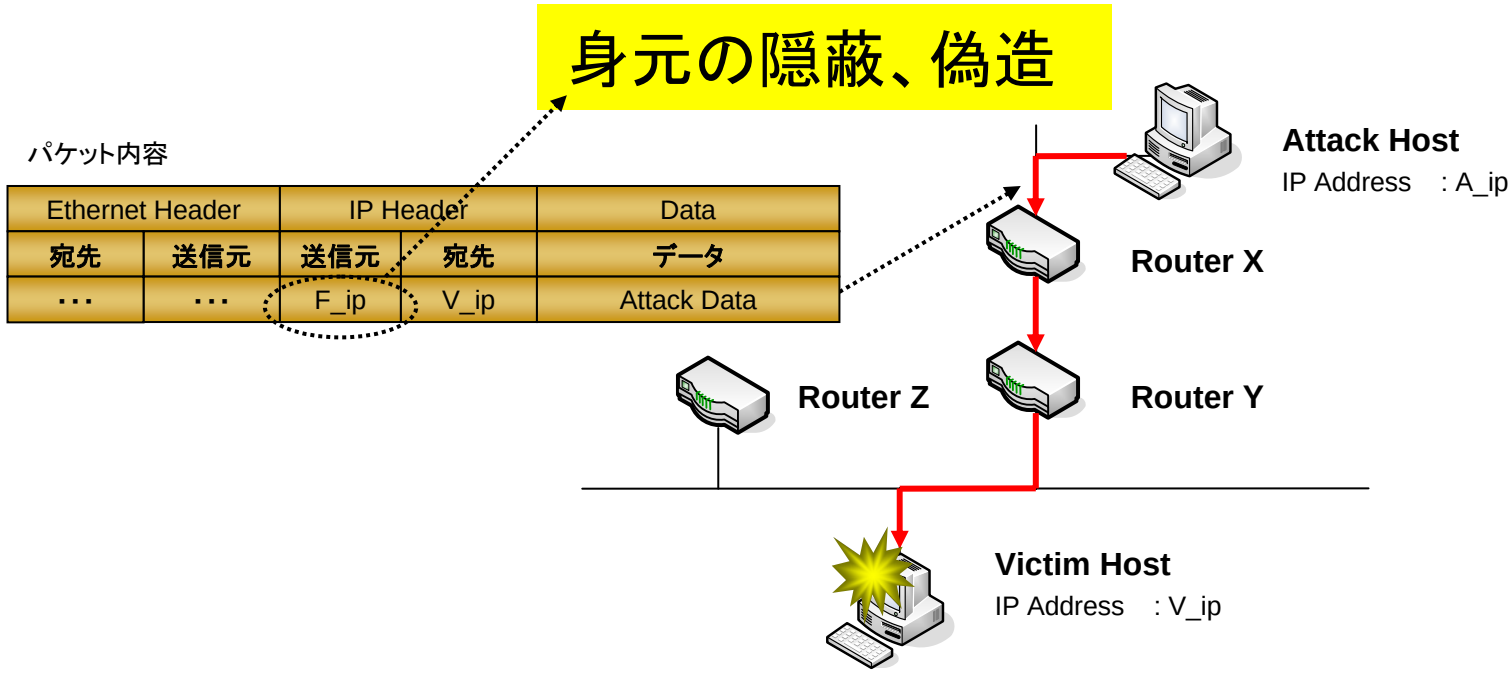
MACアドレスを用いた IPトレースバックの提案

The proposal of IP trace back using MAC Address

名城大学理工学部
播磨　宏和　渡邊　晃

研究の背景

- セキュリティにかかわる被害規模の拡大
  - サービス不能攻撃（DoS攻撃）の巧妙な機能



- 攻撃パケットの発信源を特定する手段が必要

IPトレースバック技術

既存技術

IPトレースバック技術

- Input-debugging方式
  - ルータのデバッグ機能を利用
  - フィルタ設定から隣接ルータを特定
- マーキング方式
  - 逆探知情報の追加
  - IPv4ヘッダ内の未使用ビットIP identification
- Hashトレースバック方式
  - パケットから計算したハッシュ値を利用
    （IPヘッダのうち経路中で不変である値、ペイロードの先頭）

既存技術の問題点

IPトレースバック技術の問題点

- Input-debugging方式
  - 特徴抽出の困難
  - 管理主体（ISP）をまたいでのアクセスが難しい
- マーキング方式
  - 発信源の特定ができない可能性
    （断片化の再考慮）
- Hashトレースバック方式
  - 大きな記憶容量や高いハッシュ処理能力
  - コスト面の不利

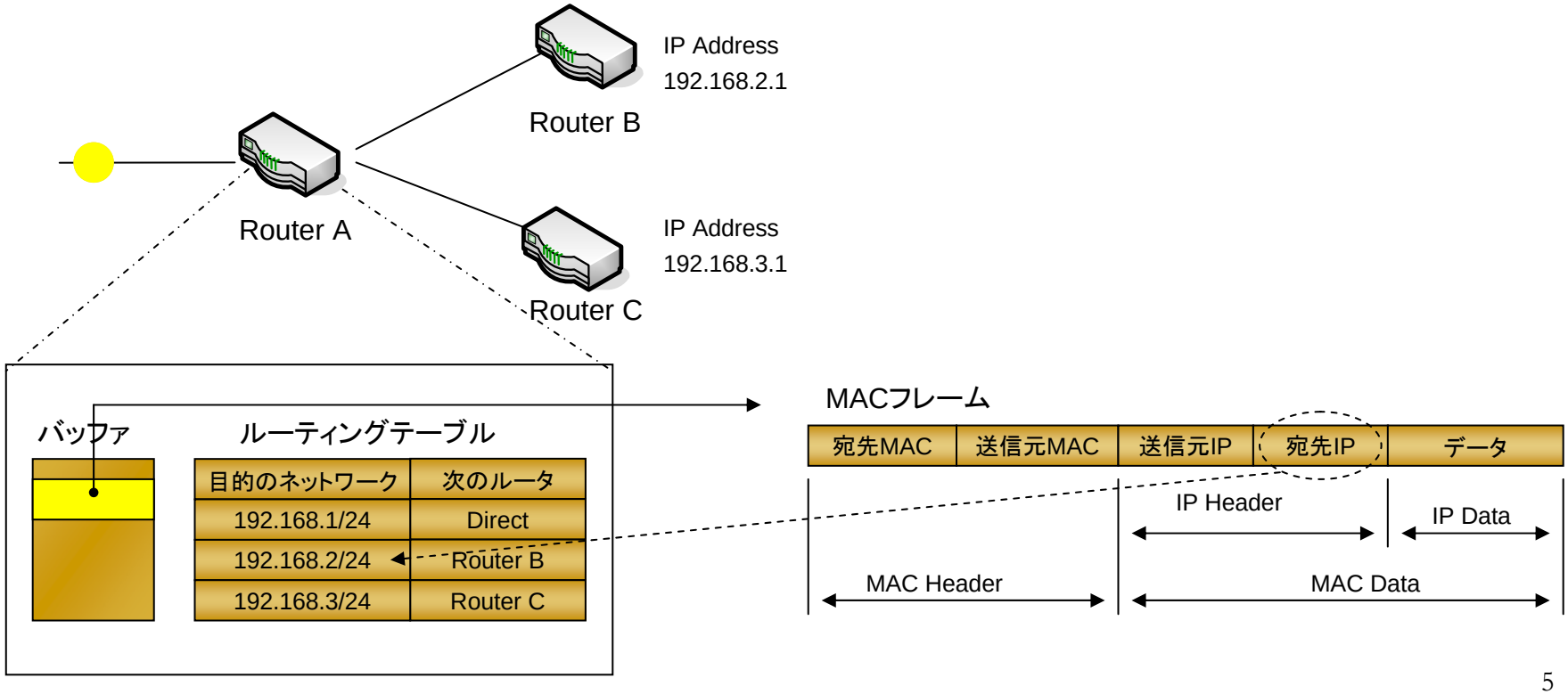
提案方式

- ルータの受信バッファに残されているMACアドレスを見つけ、発信源までの経路を追跡するIPトレースバック環境を提案する

ルータにおけるバッファリング

経路制御の際にルータが行う処理

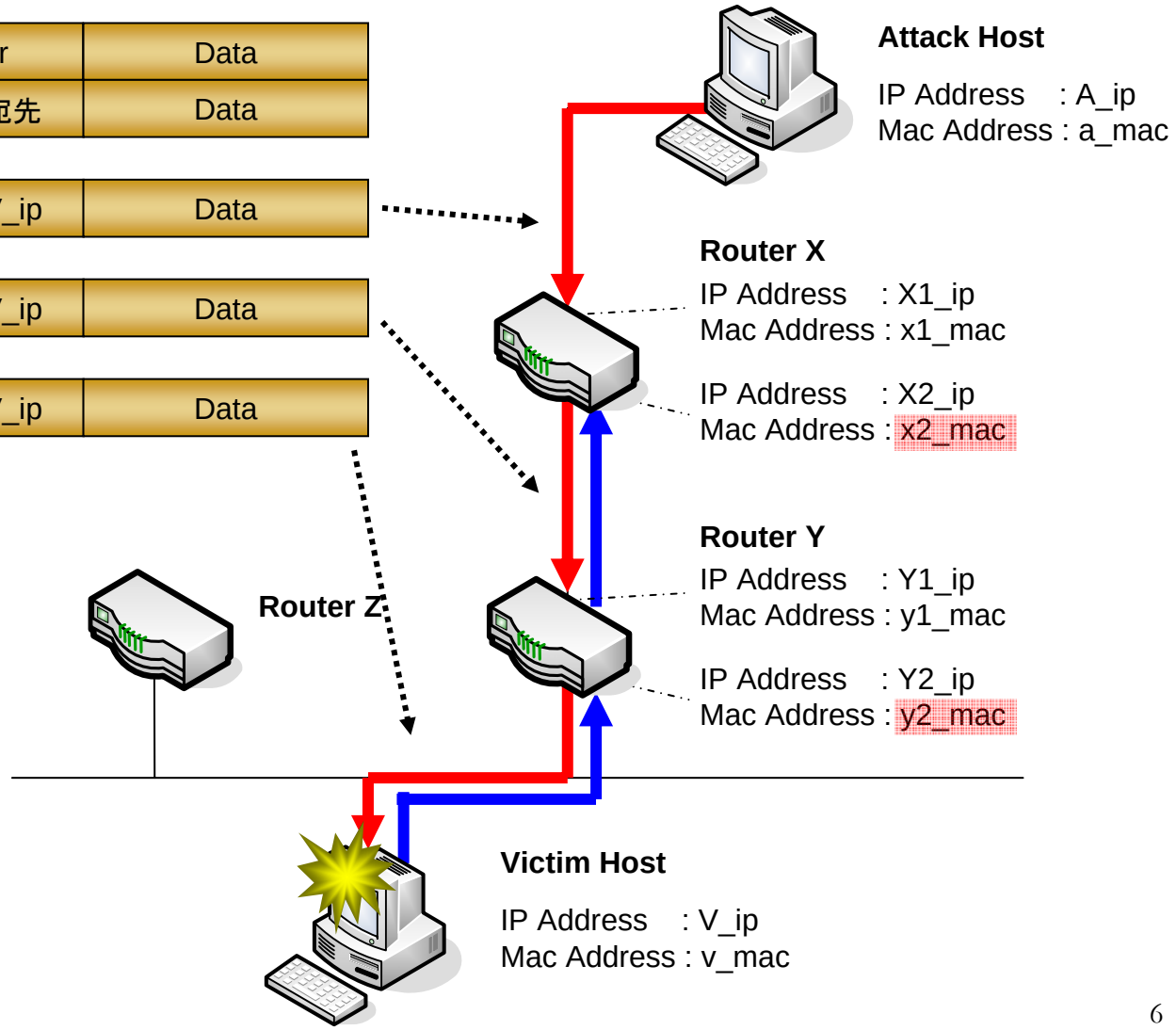
1. MACフレームからIPパケットを取り出す
2. IPパケットの中から送信先IPアドレスを取り出す
3. IPアドレスとルーティングテーブルから次のルータを決定する



提案方式の動作原理

パケット内容

Ethernet Header		IP Header		Data
宛先	送信元	送信元	宛先	Data
x1_mac	a_mac	F_ip	V_ip	Data
y1_mac	x2_mac	F_ip	V_ip	Data
v_mac	y2_mac	F_ip	V_ip	Data



問合せパケットとは

攻撃経路の探査依頼

被害ホストへ連絡

攻撃パケット

問合せ

提案方式の利点

- 大量の攻撃パケットを必要としない
- 高い処理能力が不要
- 低コストによる構築環境

まとめと今後の課題

- 問題点
  - 受信バッファにおけるパケットの生存保持時間
- 課題の検討
  - 提案システムの実装
  - 既存技術との比較

終わり