MAC-Based トレースバック方式の実装

播磨　宏和*，竹尾　大輔，渡邊　晃(名城大学)

Implementation of MAC-Based IP Traceback

Hirokazu Harima,　Akira Watanabe(Meijo University)

1.　はじめに

インターネットが普及し，安価で高速な常時接続環境の普及が進むにつれ，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）は大量のパケットをターゲットに送信し，システムを機能不全にする攻撃である．現在 DoS 攻撃を阻止する有効な手段は確立されていない．この攻撃に対して身元を特定する手法として IP トレースバック技術が存在する．我々はルータに記録されている MAC アドレスを基に上流のノードを特定し，攻撃経路を上流に向かってさかのぼることで攻撃者を特定する IP トレースバック技術「MAC-Based 方式」を提案している[1]. 本稿では MAC-Based 方式の実装について報告をする．

2.　MAC-Based 方式

図 1 に MAC-Based トレースバックの原理を示す．攻撃ホストが送信した攻撃パケットの送信元アドレスは一般に詐称されているが, ルータを通過するごとに MAC アドレスが入れ替わっていく様子が示されている．つまり，攻撃パケットには被害ホストの IP アドレスと中継ルータの正しい MAC アドレスが必ず含まれている．MAC-Based 方式ではこの情報を基に中継ルータをさかのぼることができる．

中継ルータは被害ホストの IP アドレスと上位ルータの MAC アドレスを対応付けた組アドレスをテーブルに保持する．このテーブルはルータがパケットを中継するごとにその MAC アドレスを精査し，生成しておく．各ルータは被害ホストの IP アドレスを基に関連付けられた MAC アドレスを探し出し，上位ルータを特定する．同様の操作を全ルータが実行することにより攻撃側のエッジルータまでさかのぼることができる．

被害ホストが DoS 攻撃を受けたと知ると，被害者側のユーザはプロバイダの管理者に対して攻撃ホスト特定の依頼を行う（①）．依頼を受けた管理者は管理ホストから被害ホスト側のエッジルータに攻撃経路追跡のための指示パケットを送信する（②）．指示パケットを受信したルータは記録されたアドレス情報から上位のルータを特定し，攻撃パケットが通過したルータを順にたどり攻撃経路を構築していく（③，④）．最後に攻撃ホスト側のエッジルータは管理ホストへ攻撃経路の情報を通知する（⑤）．なお，②，⑤は通常の IP パケット，③，④は MAC-Based 方式特有のイーサネットパケットにより追跡が行われる．

3.　実装と動作確認

試作システムでは，ルータとして Windows 2000 のサービス機能を使用し，MAC-Based 方式を実装させた．また，管理ホストに所定の機能を組み込んだ．

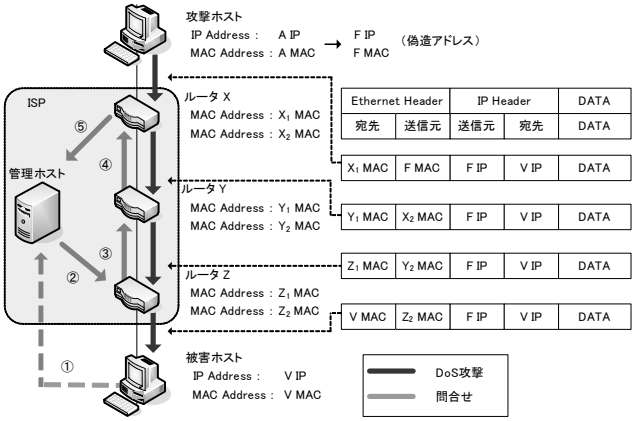


図 1. MAC-Based トレースバックの原理

パケットの精査及び追跡用パケット生成のために汎用パケットキャプチャライブラリ「Winpcap」を用いた．Winpcap はオープンソースであり，UNIX 用キャプチャライブラリ「libpcap」と互換性があるため，UNIX 係 OS へプログラムの移植が行いやすい．

図 2 にルータのモジュール構成を示す．トレースバック機能は Windows 上にユーザモードアプリケーションとして実現した. Wpcap.dll を利用して NPF デバイスドライバを操作することでイーサネットレベルでのパケットの送信が可能である．また，NIC が受信したパケットはその内容をコピーされてテーブルモジュール，トレースモジュールに渡される．テーブルモジュールは攻撃パケットから組アドレスを取り出してテーブルを生成し，トレースモジュールによりルータが自律的にトレースバックを行う．

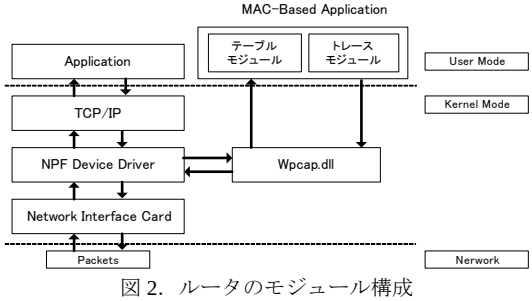


図 2. ルータのモジュール構成

4.　まとめ

本稿では MAC-Based トレースバック方式の実装について述べた．今回の実装ではルータのスループット低下の問題が大きいことから，今後は FreeBSD のカーネルに組み込むことを検討している．

文　献

[1]　播磨宏和，竹尾大輔，渡邊晃，“MAC アドレスを用いた IP トレースバック技術の提案”，情報処理学会，2005.3

MAC-Basedトレースバック方式の実装

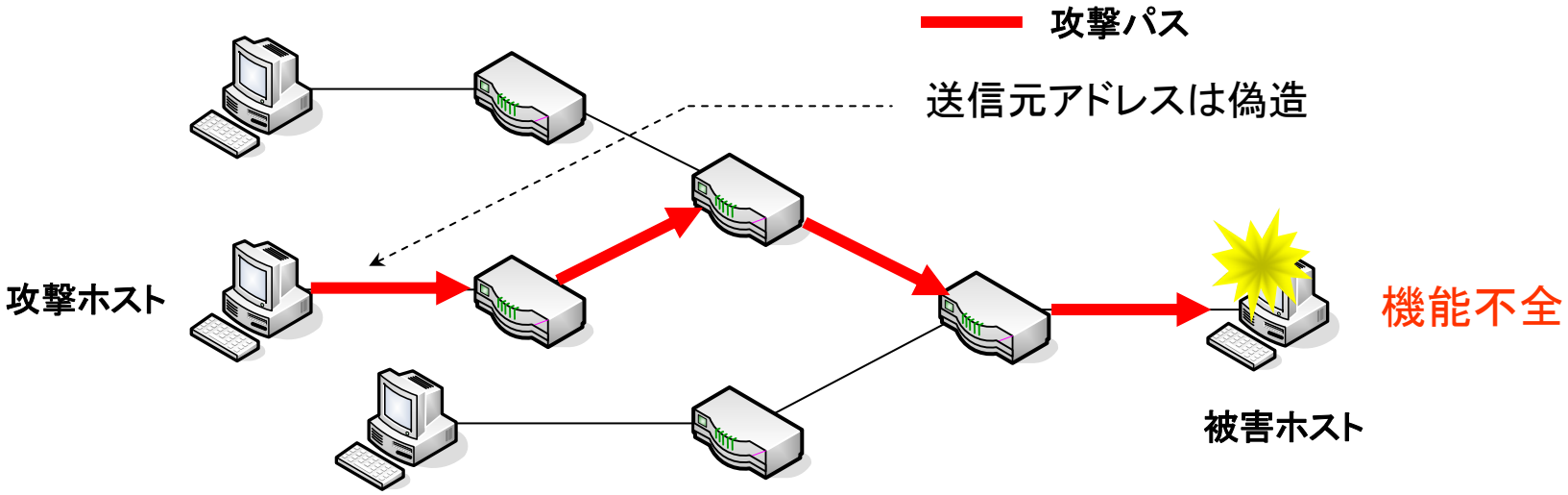
Implementation of MAC-Based IP Traceback

名城大学大学院理工学研究科

播磨　宏和，竹尾　大輔，渡邊　晃

研究の背景

- セキュリティに関わる被害規模の拡大
  - サービス不能攻撃（DoS攻撃）
    - 大量のパケットを送信
    - 身元の特定は困難

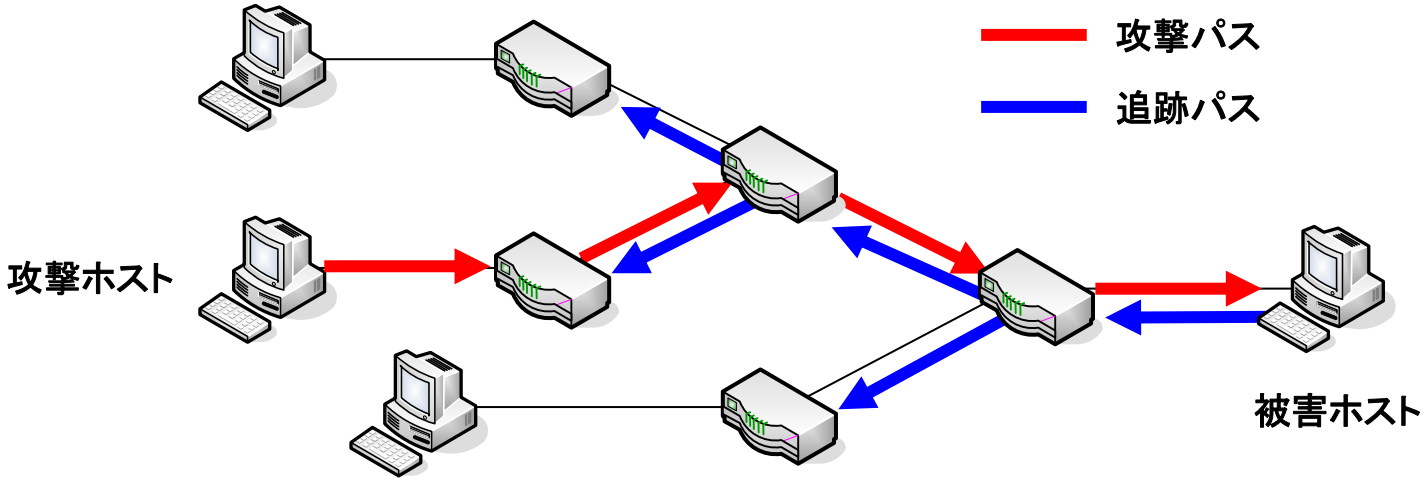


- 攻撃パケットの発信源を特定する手段が必要

IPトレースバック技術

IPトレースバック技術とは

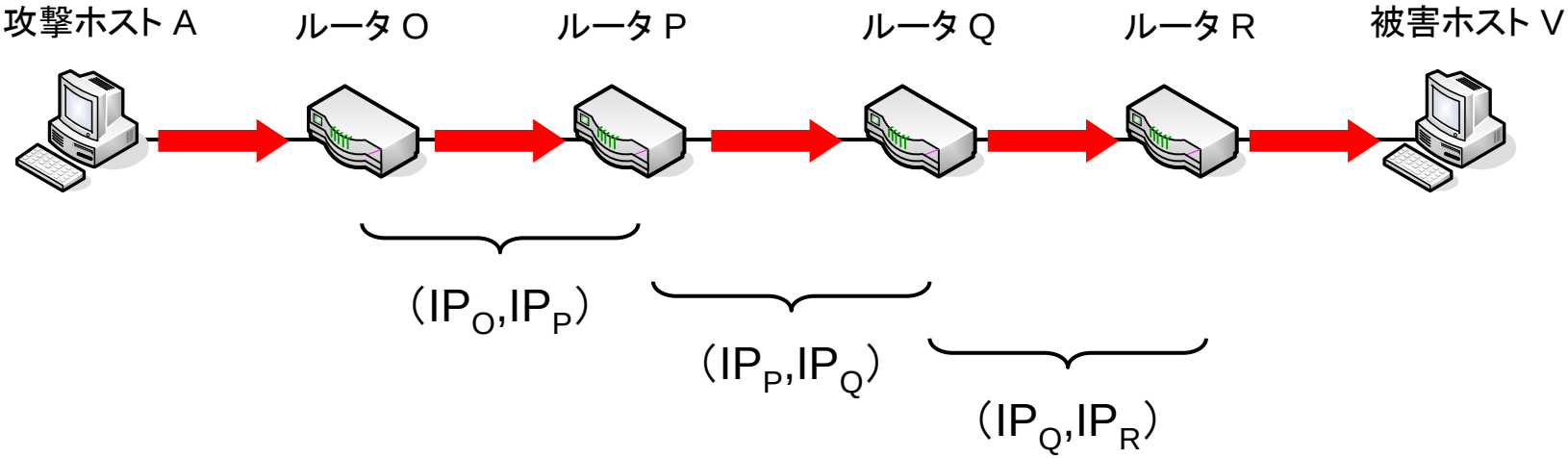
- IPトレースバック技術
  - ルータ機能の追加



- 既存技術
  - 受動型
    - マーキング方式
    - ICMP方式
  - 能動型
    - リンクテスト方式
    - Hash-based方式

既存技術
マーキング方式

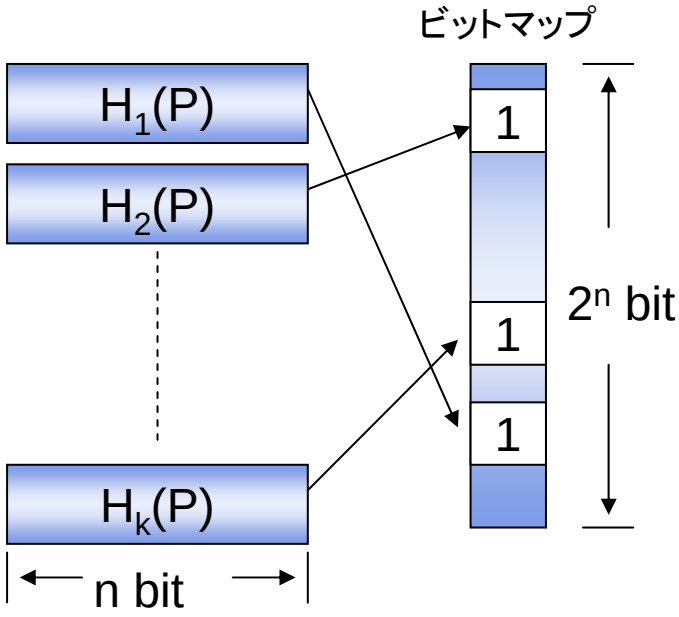
- IPヘッダ内の未使用ビットにマーキング
  - IPヘッダ（Identificationフィールド）
  - 2つのルータのアドレス
- 収集したマーキングパケットから攻撃経路を再構築



- 欠点
  - 攻撃経路の構築に膨大な時間が必要
  - 既存の通信に影響を及ぼす

既存技術
Hash-Based方式

- ハッシュ関数を用いてビットマップを生成、通過記録を保存
- ビットマップがルータに保存されているかを1ホップずつ検証することで攻撃経路を追跡



K個のハッシュ関数（$H_1,H_2,\ldots,H_k$）

IPヘッダ

不変な部分（P）

Ver	H L	TOS	Total Length
Identification			Fragment Offset
TTL		Protocol	Checksum
Source Address			
Destination Address			
Options			
Payload			

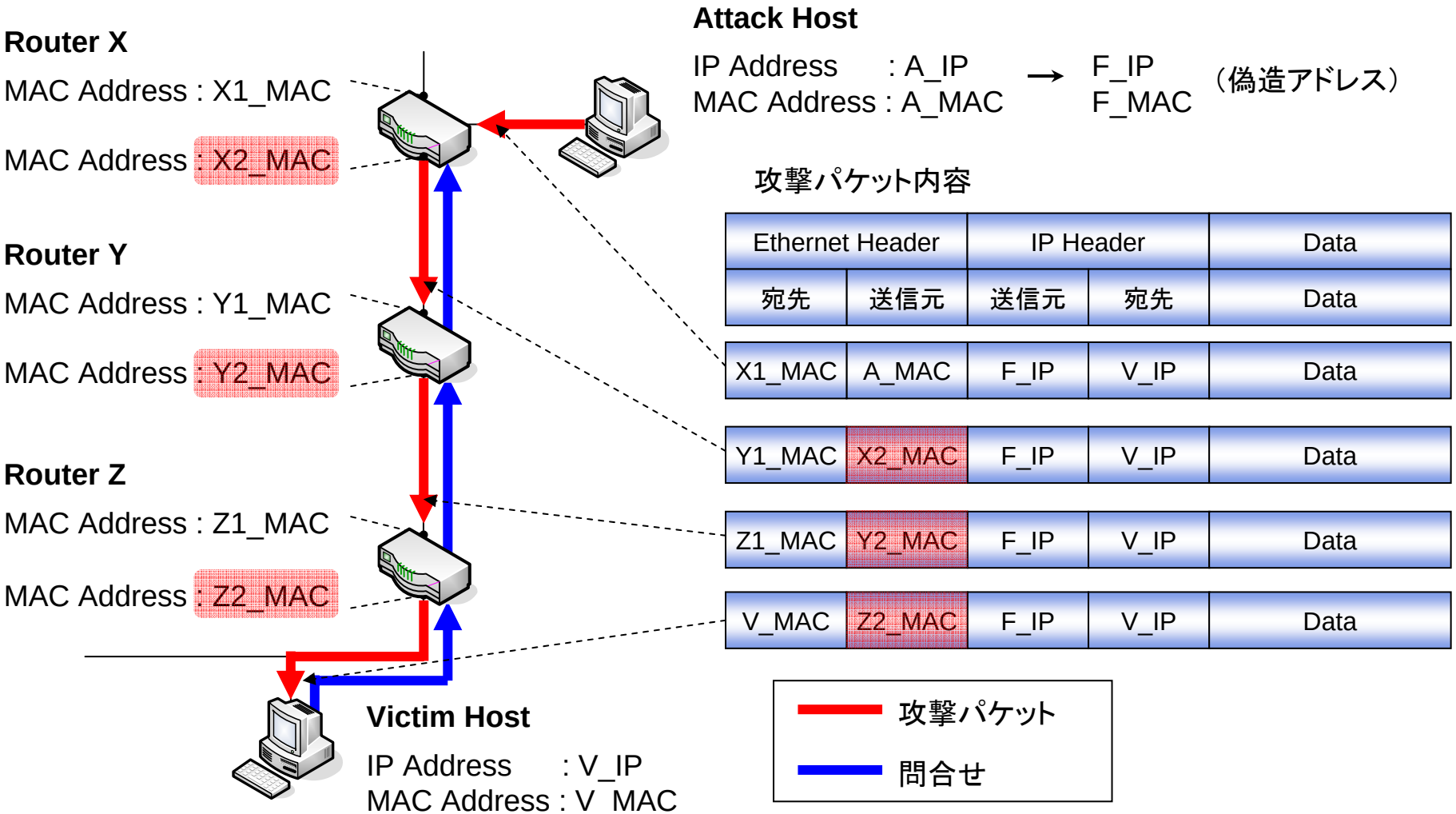
- 欠点
  - 大きな記憶容量や高いハッシュ処理能力が必要

提案方式
MAC-Based方式の概要

- DoS攻撃の可能性のあるパケットから
  送信元MACアドレスを記録

- 記録されたMACアドレスにより上位のノードを
  特定し発信元を追跡する

動作原理


Router X
MAC Address : X1_MAC
MAC Address : X2_MAC
Router Y
MAC Address : Y1_MAC
MAC Address : Y2_MAC
Router Z
MAC Address : Z1_MAC
MAC Address : Z2_MAC
Victim Host
IP Address : V_IP
MAC Address : V_MAC
Attack Host
IP Address : A_IP
MAC Address : A_MAC
→
F_IP
F_MAC
（偽造アドレス）
攻撃パケット内容
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
Z1_MAC
Y2_MAC
F_IP
V_IP
Data
V_MAC
Z2_MAC
F_IP
V_IP
Data
攻撃パケット
問合せ

上位MACアドレスの記録

テーブル1

Destination IP Address	COUNT値
・・・・・	・・・・・
V_IP	1000
・・・・・	・・・・・

閾値:1000

テーブル2

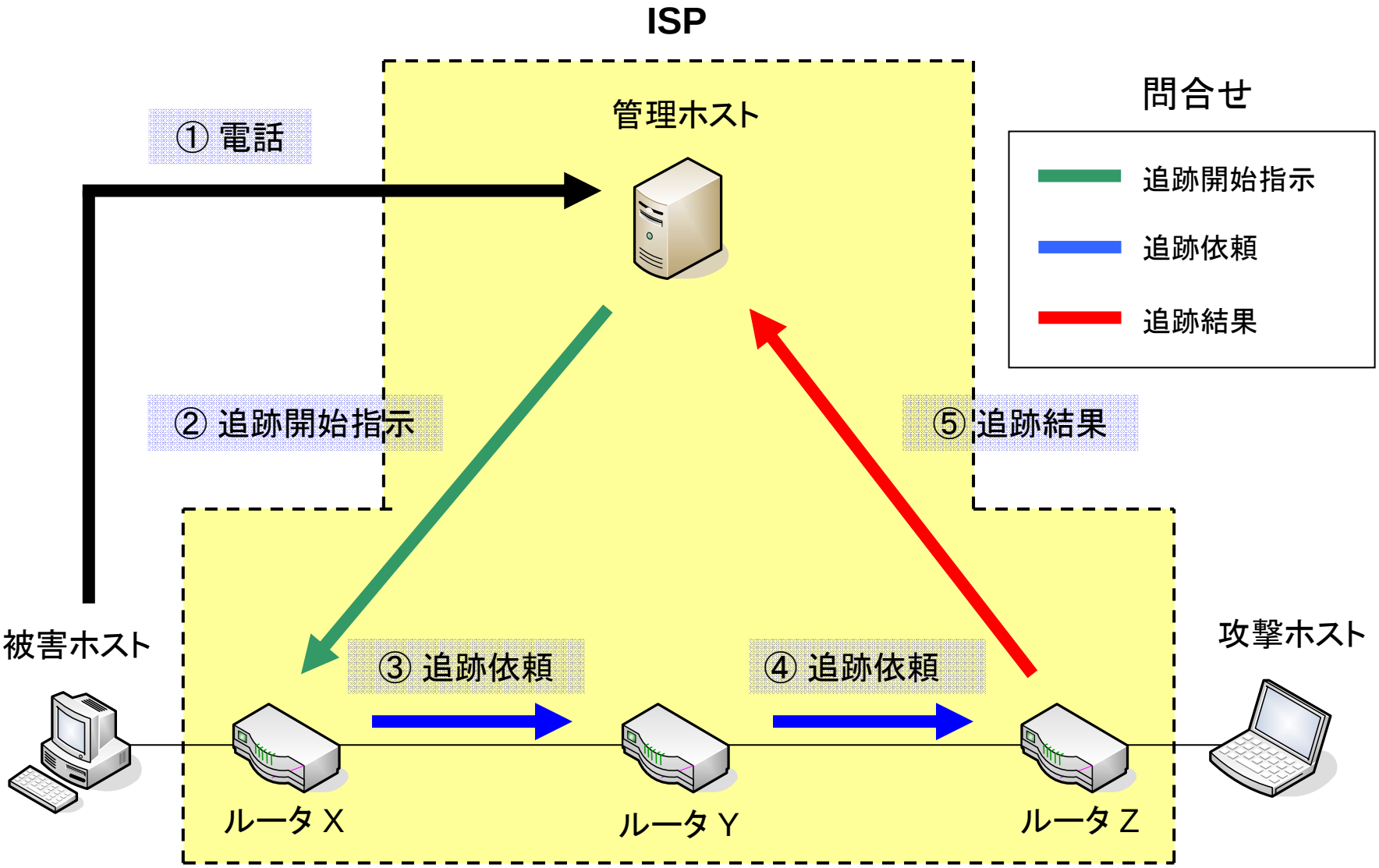
Destination IP Address	Source MAC Address
V_IP	Y_MAC
・・・・・	・・・・・
・・・・・	・・・・・

1. 宛先IPアドレスを記録
2. カウント値の加算
3. 単位時間で消去
4. 閾値を超えたらテーブル2に保存
   (攻撃経路の判断材料)

1. ・送信元MACアドレス
   ・宛先IPアドレス
   の2つを記録
2. 長期保存

追跡時　　：テーブル2を使用
テーブル2の内容　：DoS攻撃が発生した場合にしか記録されない

ネットワーク構成


ISP
管理ホスト
問合せ
追跡開始指示
追跡依頼
追跡結果
① 電話
② 追跡開始指示
③ 追跡依頼
④ 追跡依頼
⑤ 追跡結果
被害ホスト
攻撃ホスト
ルータ X
ルータ Y
ルータ Z

パケットフォーマット

MTC

Ethernet Header
IP Header
ICMP Header
Inquiry Header

MTI

Ethernet Header
Inquiry Header

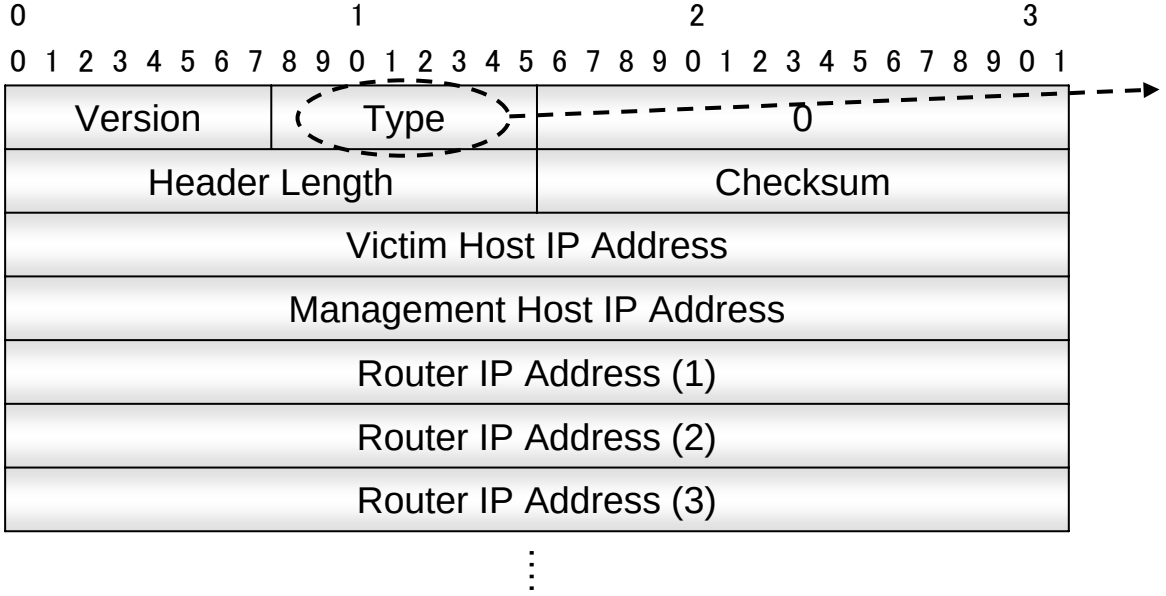
MTC（MAC Traceback Control）

管理ホスト - ルータ間

MTI（MAC Traceback Information）

ルータ - ルータ間

Inquiry Header

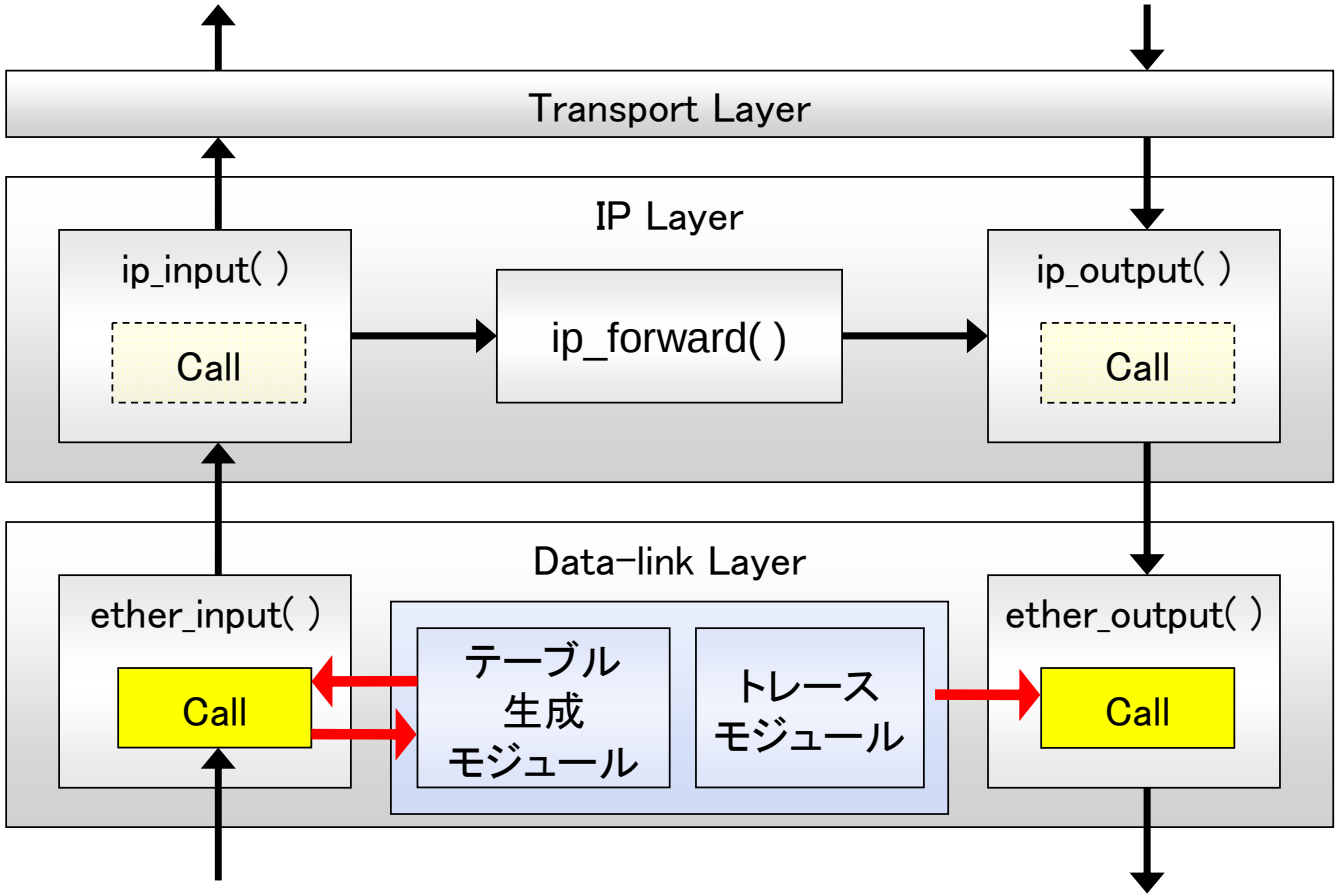


Type Field

- 追跡開始指示
- 追跡依頼
- 追跡結果

実装方式

- FreeBSD 5.3に実装



1パケットの転送時間

- ルータの中継処理に与える影響
  - 1つのUDPパケットの中継時間

CPU: Intel Pentium4 3.20Ghz
Memory: 256MB
NIC: 100Mbps

	実装なし [μsec]	実装あり [μsec]	割合 [%]	増加 [%]
32Byte	16.928994	17.061024	99.2	0.77
512Byte	17.440546	17.594433	99.1	0.87
1472Byte	18.226378	18.452242	98.7	1.22

MAC-Basedトレースバックの

導入によるスループットへの影響は無い

むすび

- まとめ
  - MACアドレスを用いたIPトレースバック技術の手法について提案した
- 現在の状況
  - MAC-BasedトレースバックをFreeBSD5.3のカーネルに実装
  - 管理ホストに追跡プログラムを導入
  - 攻撃者側のエッジルータの特定を確認
- 今後の課題
  - さまざまなネットワーク環境下において、最適な閾値決定方法を検討する

おわり