MAC-based トレースバック方式の提案

播磨　宏和　　渡邊　晃

名城大学大学院理工学研究科

A proposal of MAC-based Traceback method

Hirokazu Harima　　Akira Watanabe

Graduate School of Science and Technology, Meijo University

1.　はじめに

CATV や ADSL といった常時接続環境が整うにつれ，多くの企業や個人が手軽にサーバを構築できるようになってきた．それに伴い，悪意ある第三者からの攻撃数は年々増加し，ウイルスの感染や外部からの不正侵入等の脅威が多発している．中でもサービス不能攻撃（DoS 攻撃）は，ターゲットコンピュータに対して大量の接続要求や不正なデータを送りつけることで機能不全に陥らせたり，ネットワークのトラヒックを増大させるなどしてネットワークの機能を麻痺させる攻撃である．現在，DoS 攻撃に対して有効な処置の一つとして攻撃者の最寄のルータを特定し，帯域制御やフィルタリングを行うことが一般的だが，DoS 攻撃で送信されるパケットの送信元アドレスは偽造されていることがほとんどであり，攻撃者の特定は非常に困難とされている．　このような問題に対し，送信元アドレスが詐称されていても発信源を特定する IP トレースバック技術[1]が提案されている．

既存の IP トレースバック技術としては，ルータのデバッグ機能を利用する Input-debugging 方式，逆探知パケットを使用する ICMP 方式[2]，ある確率でパケット中継時にマークをつけるマーキング方式[3][4]，パケットのダイジェストを記憶する Hash-based 方式[5][6]などが有名である．多くの研究は IP レイヤの情報を利用するが MAC(Media Access Control)の情報を利用する方式も一部に見られるようになった[7][8].

本研究では詐称が困難な MAC アドレスに注目し，効率的にパケット情報を記録する MAC-based トレースバックを提案する．DoS 攻撃では大量の攻撃パケットが攻撃対象ホストへと送信されることから，ルータは特定の上位ルータから同じ宛先 IP アドレスのパケットを大量に受信することになる．このとき，DoS 攻撃を転送した上流ルータの MAC アドレスを記憶しておくことにより，攻撃の経路を推測する手がかりを得る．試作の結果，本方式ではルータにほとんど負荷を与えず，性能劣化が無いことを確認した．

2 章で既存技術と課題を述べ，3 章で MAC-based トレースバック，4 章で実装，5 章で評価を述べ．6 章でまとめを行う．

2.　既存技術とその課題

パケットがどのような振る舞いをして，どのような経路を通過したかということを順にたどっていく行為をトレーシングと表現する．トレーシングの中でも攻撃の発信元までさかのぼるシステムを自動化したものをトレースバックシステムと呼び，それらの技術を総称して IP トレースバックという．IP トレースバック技術とは，IP パケットの送信元アドレスが詐称されたとしても，発信源を特定できる手法の総称である．ルータに機能を追加することにより，パケットが通過した手がかりを調べることによって発信源の特定を行う．以下に代表的な IP トレースバック技術であるマーキング方式と Hash-based 方式，本研究と関連のある MAC の情報を利用する方式について概要と指摘されている課題を述べる．

(1)　マーキング方式

マーキング方式は，ルータがパケット転送時にある確率で逆探知が可能となる情報をパケットの特定のフィールドに挿入する方式である．被害ホストは，マーキング情報から攻撃経路を再構築する．追跡のための追加パケットを必要としないことから，ネットワークに負荷をかけずに追跡を実行できる利点がある．しかし，攻撃経路を再構築する際に大量のマーキングパケットが必要で，莫大な計算量を要するという課題がある．またマーキングデータが詐称された場合においても経路を構築できない．

(2) Hash-based 方式

Hash-based 方式は，ルータがすべてのパケットに対してログを記録する方式である．記録に関しては，ハッシュ計算を用いて記録量を削減する．追跡においては攻撃パケットからハッシュ値を計算し，この値が記録されているルータを探し出す．攻撃パケットが 1 個さえあれば発信源を特定できるという利点があるが，大きな記憶容量や高いハッシュ処理能力などが要求されるため，コスト面で不利になる．

(3) MAC の情報を利用する方式

[8]では，パケットのログを記録する際に MAC の情報を含める．AS 内に追跡のためのマネージャとルータ内のトレーサの連携で追跡作業を行うモデルで構成されており，各ルータは転送した全てのパケットに対して, それに対応した MAC アドレスを記録する. MAC 情報を含めたことにより上流ルータの特定が容易になるという利点がある．この方式をここでは Hash-based with MAC と呼ぶ．追跡においては，マネージャの指示で攻撃パケットと一致する転送パケットを検索することで隣接ルータを特定し, その IP アドレスをマネージャに報告する．しかし，追跡に必要な情報を記録するには大きな記憶容量を必要とする．また，あらかじめトレーサは接続されている装置の IP アドレスや MAC アドレスといったネットワークインタフェース情報を調査し，それらを記憶装置に保存する必要がある．

3.　MAC-based トレースバック

3.1.　概要

攻撃ホストから被害ホストに DoS 攻撃が仕掛けられた場合におけるパケットの MAC アドレスが変化する様子を図 1 に示す. 攻撃ホストから送信されたパケットの送信元 IP アドレスは一般に詐称されており，送信元 MAC アドレスも詐称

されている可能性が大きい．攻撃パケットの内容は図1のように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．宛先IPアドレスは被害ホストのアドレスであり，ルータを通過してもその内容は変わることがない．つまり，攻撃パケットには被害ホストのIPアドレスと上流ルータの正しい送信元MACアドレスが必ず含まれている．

MAC-basedトレースバックは,攻撃パケットの送信元MACアドレスからパケット転送した上流の送信元IPアドレスを割り出し,宛先である被害ホストのIPアドレスをペアにして記録させておき，この情報を元にトレースバックを行う．

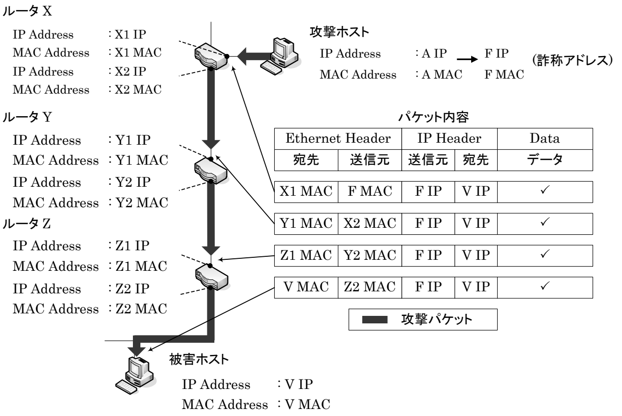


図1.　パケットのアドレスが変化する様子

3.2.　システムの構成

MAC-basedトレースバックは図2のようなネットワーク構成を想定する．攻撃ホストと被害ホストはプロバイダの外部ネットワークに存在し，プロバイダが提供するルータには本提案方式の機能が搭載されているものとする．プロバイダ内には管理ホストが存在し，DoS攻撃が発生したときは管理ホストの指示に従いトレースバックを開始する．点線内がプロバイダに相当し，被害ホストは特殊な機能を持たない一般端末である．

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に対して電話等により攻撃ホスト特定の依頼を行う．依頼を受けたプロバイダ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問合せパケットを送信する．問合せ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のIPアドレスを管理ホストへ返答する. 管理ホストは上流ルータに対して問合せを行う．同様の操作を繰り返し行うことにより，攻撃ホスト側のエッジルータまでさかのぼることができる．

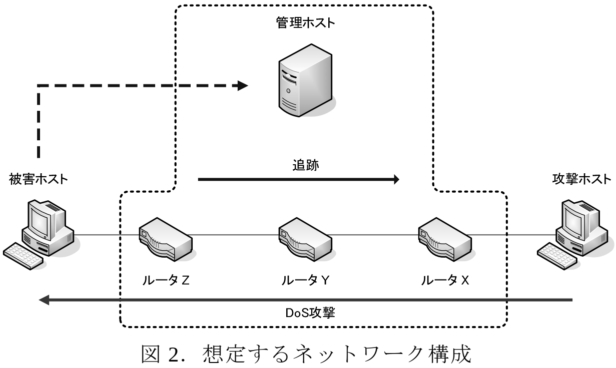


図2．想定するネットワーク構成

3.3.　アドレス情報の記録

MAC-basedトレースバックに対応したルータでは，一般パケットと攻撃パケットの判別を行うために，単位時間におけるパケット転送回数をリアルタイムで計測している．ある宛先に対するパケットの転送回数が，設けられた閾値を超えるとDoS攻撃の可能性があると判断する．

ルータは追跡のための情報を記録する一時テーブル（temporary table），及び記録テーブル（record table）の2つを保持している（図3）．パケット転送時にパケットの宛先IPアドレスとポート番号,転送回数を一時テーブルに記録する．ポート番号別に記録するのは次に述べる閾値がポート番号により異なる可能性があるためである．一時テーブルの内容は短い一定間隔で消去する．カウント値にはある閾値が設けられており，カウント値が上記一定時間内にこの閾値を超えた場合,その宛先を攻撃対象としたDoS攻撃が行われている可能性があると判断し，この時のパケットの送信元MACアドレスを利用してARPキャッシュテーブルから上位ルータのIPアドレスを取得する．宛先IPアドレスと上位ルータのIPアドレスの2つのアドレスを記録テーブルへ記録する．記録テーブルは攻撃の可能性があった場合のみ生成されるものであり長期的に保持する．

このように上位ルータを特定するためにMACアドレスを利用するが,上流ルータを記憶するときはIPアドレスを用いる.これは,管理ホストからの追跡を行いやすくするためと，レイヤ2を抽象化するためである．プロバイダネットワークのレイヤ2はLANとは限らず，ATMや専用線のこともありMACアドレスが存在しない場合もあるため,そのような場合にも対応できるように考慮している．

3.4　閾値の変更

カウント値に設けられる閾値は，ルータの起動時に管理ホストの管理者によって決定されるが，手動または管理ホストからの指示によって変更することができる．IKEのように処理の重いプロトコルでは，少量のパケットでもシステムを機能不全にする．これらの攻撃にも対応させるため，特定のプロトコルタイプやポート番号ごとに閾値を変更することを可能とする．ルータは閾値制御リスト(threshold control list)を保持しており，このリストの閾値に従い一時テーブルの内容を検査する．

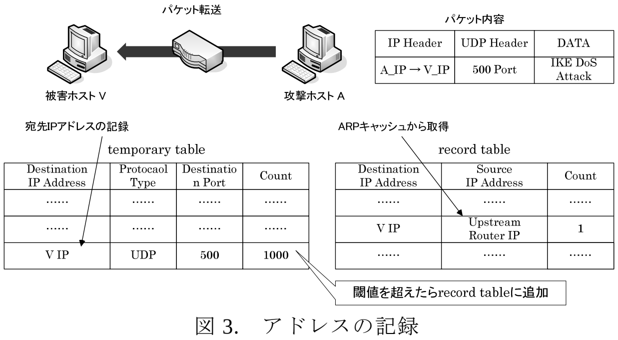


図3.　アドレスの記録

3.5.　追跡動作

追跡時においては，管理ホストがルータに対して問合せを行い，ルータはこれに順次返答することにより，攻撃経路を構築していく．

管理ホストは被害ホストのIPアドレスを格納した問合せパケットを被害ホスト側のエッジルータに対して送信する．問合せパケットを受信したルータは自身の記録テーブルから

被害ホストの IP アドレスをキーに上位ルータの IP アドレスをすべて割り出す．次にルータは，割り出した IP アドレスを管理ホストに返答する．管理ホストは返答結果から，次の上流ルータに問合せを行う．これらの操作を同様に行うことで，攻撃ホストのエッジルータ側まで問合わせを行うことができる．最終的に管理ホストは攻撃側のエッジルータまでの IP アドレスを割り出し，攻撃経路を構築することができる．

4.　提案方式の実装

4.1　モジュール構成

MAC-based トレースバックを実行するルータはデータリンク層においてテーブルを生成する．OS には FreeBSD を選択した．図 4 にルータのモジュール構成を示す．データリンク層の入力関数である ether_input()から MAC-based モジュールを呼び出し，入力パケットの内容を参照してテーブルを更新する．処理されたパケットはデータリンク層の元の場所に戻すため，既存の通信処理に一切影響を与えない．

応答デーモンは，MAC-based モジュールで生成した記録テーブルをシステムコールで呼び出し，Socket を利用して返答パケットを生成する．なお，管理ホスト側の処理は全てアプリケーション層にて実装した．

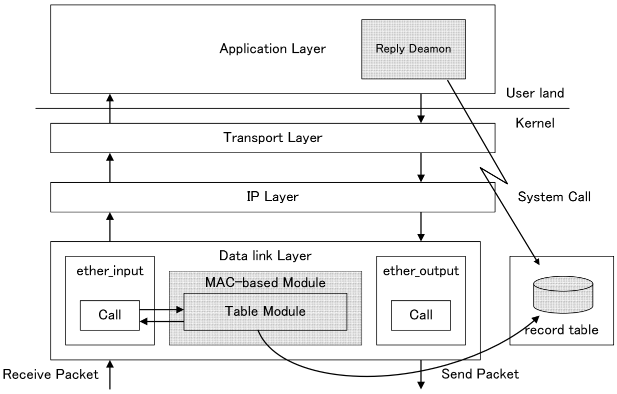


図 4.　ルータのモジュール構成

4.2.　パケットフォーマット

追跡のための問合せパケットは UDP パケットをベースに定義されている．パケットフォーマットを図 5 に示す．

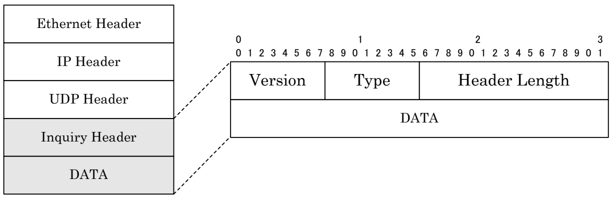


図 5.　パケットフォーマット

追跡パケットには以下の 2 通りがあり，Inquiry ヘッダの Type フィールドで分類される．

① 追跡要求（Trace Request）
管理ホストからルータへの問合せ．

② 追跡応答（Trace Reply）
上記問合せに対する応答．該当する被害ホストの IP アドレスが記録テーブルに存在した場合に，上位ルータの IP アドレスとともに報告する．報告をする上位ルータが複数の場合もありうる．

5.　評価

上記機能をルータ及び管理ホストに実装し，トレース実験を行った結果，正確な攻撃経路の構築が行えることを確認した．以下に性能測定の結果を示す．

5.1.　パケット転送時間

MAC-based トレースバックを実装した場合に，ルータの中継処理に与える影響がどの程度あるのか，1 パケットの転送時間を比較した．ルータは CPU Pentium4 2.4GHz，メモリ 256MB，OS FreeBSD 5.3 の PC を使用した．提案方式を実装した状態と実装していない状態で UDP パケットを中継させて測定し，500 パケットごとの処理時間の平均を測定した結果を表 1 に示す．MAC-based モジュールを実装した場合は，実装していない場合に比べパケット転送時間の増加は 3.41% 程度となった．パケット長の違いによる有意差は認められなかった．

表 1.　パケット転送時間

	64 [Byte]	256 [Byte]	1472 [Byte]
未実装時	361.5 [μsec]	355.3 [μsec]	366.5 [μsec]
実装時	367.3 [μsec]	371.9 [μsec]	382.4 [μsec]

5.2.　FTP によるスループット測定

FTP を利用したスループットの測定を行った結果を表 2 に示す．FTP サーバと FTP クライアントの 2 台が本システムを実装したルータを介して接続し，その間でファイルの転送を 100 回試行した．転送したファイルのサイズは 100M バイトのバイナリファイルを使用した．その結果，スループットの減少は 3.6%であった．

表 2. FTP スループット測定結果

	所要時間 [sec]	スループット[Kbyte/sec]
未実装時	16.38	6251.52
実装時	16.97	6034.17

測定結果から分かるようにルータに MAC-based トレースバック機能を実装させてもオーバーヘッドや通信処理に影響はほとんどないと考えられる．

5.3.　既存技術との比較

既存方式と MAC-based トレースバックを比較した結果を表 3 に示す．

ハードウェアコストの面においては， Hash-based 方式と Hash-based with MAC はルータにログを記録するための大きな記憶容量が求められる．MAC-based 方式は DoS 攻撃とみなされるパケットを転送した場合にのみ攻撃情報を記録するので，大きな記憶容量を必要としない．解析量の面においては，マーキング方式は膨大なマーキングパケットから攻撃経路の情報を確かめなければならないことから攻撃ホスト特定に時間がかかる．パケットへの影響に関しては，マーキング方式はパケットそのものを書き換えるため，マーキングフィールドを使用した既存の通信に影響を与えるといった問題がある．新規プロトコルの必要性に関しては，独自の追跡シーケンスを適用する Hash-based 方式と Hash-based with MAC，MAC-based 方式はルータ間の連携が必要になることからエラーの発生を考慮した設計が必要である．

MAC-based 方式では，与えられた閾値によってはトレースが行われない場合の出ることが考えられる．小規模なネット

ワークとISPや企業などの大規模なネットワークでは，ルータが転送するパケット量は大きく異なってくる．閾値の設定によっては通常のパケットが攻撃パケットととられてしまう可能性があり，この誤認知をさけるためには各テーブルに設ける閾値の決定が特に重要であり，今後の検討課題である．

表3．既存方式とMAC-based方式の比較

	ハードウェアコスト	解析量	パケットへの影響	新規プロトコルの必要性
マーキング方式	○	×	×	○
Hash-based方式	×	○	○	×
Hash-based with MAC	×	○	○	×
提案方式	○	○	○	×

6.　まとめ

本研究ではIPアドレスが偽造されても，パケットのMACアドレスをたどることにより上位ノードを特定し，攻撃経路を構築できるMAC-basedトレースバックについて検討した．本方式はパケット転送回数に設けられた閾値からDoS攻撃を判別するので，ルータに記録する容量が少ない．閾値をプロトコル，ポートに関して設定できるため，処理負荷の高いプロトコルに対しても対応可能である．MAC-based方式を実装し，動作検証と性能測定を実施した．その結果，ルータにはほとんど負荷がかからないことを示した．

今後は，さまざまなネットワークトポロジ環境において，どの程度まで正確に攻撃経路をさかのぼることが可能か，実用性を確認するとともに，追跡時間を測定する．同時に，経路を撹乱させる分散型DoS攻撃（DDoS攻撃）においても正確にトレースできるのか検討を行う予定である．また，本方式を専用線やATMといった異なる媒体にも対応させるように拡張する予定である．

参考文献

[1] 門森雄基，大江将史“IP トレースバック技術”情報処理 Vol. 12，No. 42，Aug，2001

[2] Steve Bellovin，et al，“ICMP Traceback Messages”，Internet-Draft，Expires August，2003

[3] S. Savege, D. Wetherall, A. Karlin, T. Anderson, “Practical Network Support for IP Traceback”，In Proceedings of SIGCOMM ‘00，pp. 295-306，2000

[4] 岡崎直宣，河村栄寿，朴美娘，“サービス不能攻撃の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，No. 12，Dec. 2003

[5] A. C. Snoeren，C. Partridge，L. A. Sanchez，C. E. Jones，F. Tchakountio，S. T. Kent，and W. T. Strayer，“HashBased IP Traceback”，Proceedings of ACM SIGCOMM 2001，San Diego，CA，USA，August 2001

[6] Snoeren, C. Partridge, L. Sanchez, C. Jones, F. Tchakountio, B. Schwartz, S. Kent, and W. Strayer. Single-Packet IP Traceback. In ACM/IEEE Transactions on Networking, vol.10, no.6, December 2002.

[7] 竹爪慎治，松田栄之，渡辺英俊，柳田正博，小久保勝俊“不正アクセス発信源追跡アーキテクチャの検討”情報処理学会第60回全国大会，3-287，Mar. 2000

[8] Shigeyuki Matsuda, Tatsuya Baba, Akihiro Hayakawa, and Taichi Nakamura, "Design and Implementation of Unauthorized Access Tracing System", in Proceedings of the 2002 Symposium on Applications and the Internet (SAINT 2002), IEEE Computer Society, pp.74-81, January 2002.

[9] 三輪信雄，白井雄一郎，白濱直哉，又江原恭彦，柳岡裕美，「不正アクセスの手法と防御」，ソフトバンクパブリッシング株式会社，2001年

[10] Stephen Northcutt，Mark Cooper，Matt Fearnow，Karen Frederik，クイープ，ネットワーク侵入解析ガイド 侵入検知のためのトラフィック解析法，株式会社ピアソン・エデュケーシ

[11] Stefan Savage，David Watcherall，Anna Karlin，and Tom Anderson，“Network Support for IP Traceback，IEEE/ACM TRANSACTIONS ON NETWORKING, VOL.9，NO.3 JUNE，2001

[12] 池田竜朗，山田竜也，“発信源追跡のためのハイブリッドトレースバック方式”東芝レビュー，Vol.58，No.8，2003

[13] Stefan Savage，David Wetherall，Anna Karlin and Tom Anderson，“Network support for IP traceback”，IEEE/ACM Transactions on Net- working，Vol.9，No.3，pp.226-237，(2001)

MAC-basedトレースバック方式の提案

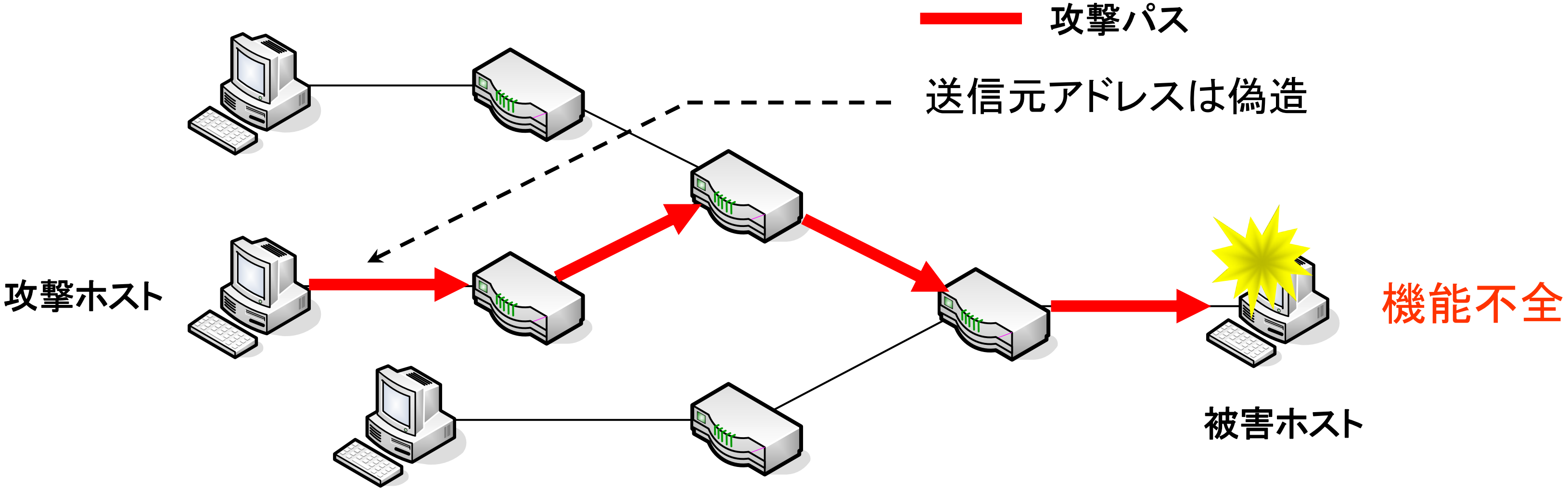
A proposal of MAC-based Traceback method

名城大学大学院理工学研究科

播磨　宏和，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

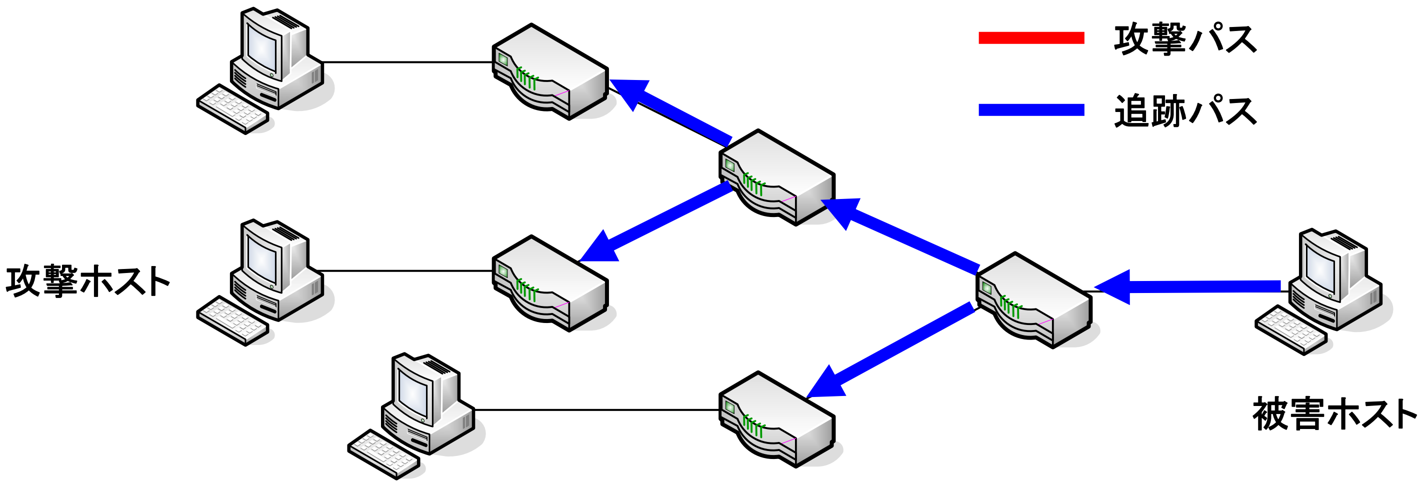


- 攻撃パケットの発信源を特定する必要性が高まってきている

IPトレースバック技術

IPトレースバック技術とは

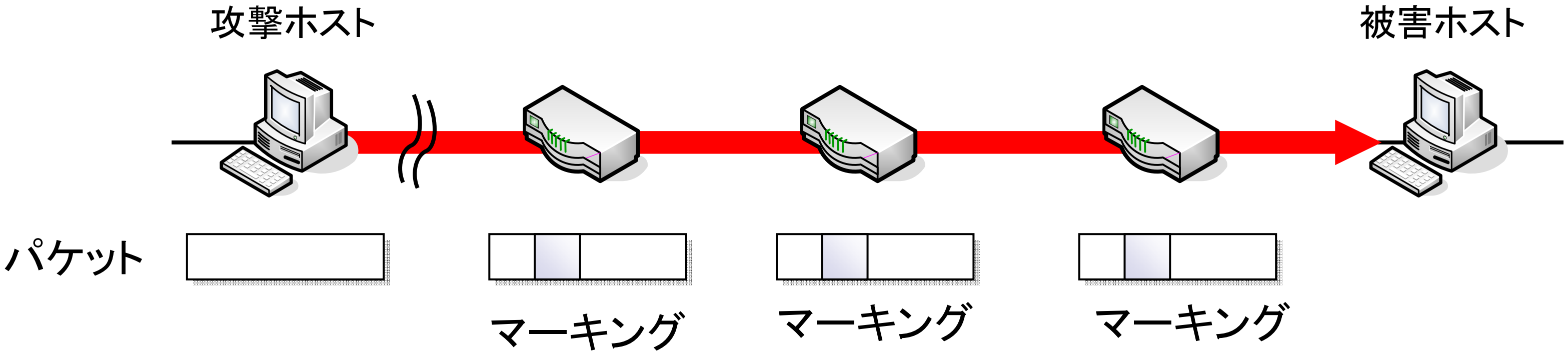
- IPトレースバック技術
  - ルータ機能の追加



- 既存技術
  - マーキング方式
  - Hash-based方式

既存技術
マーキング方式

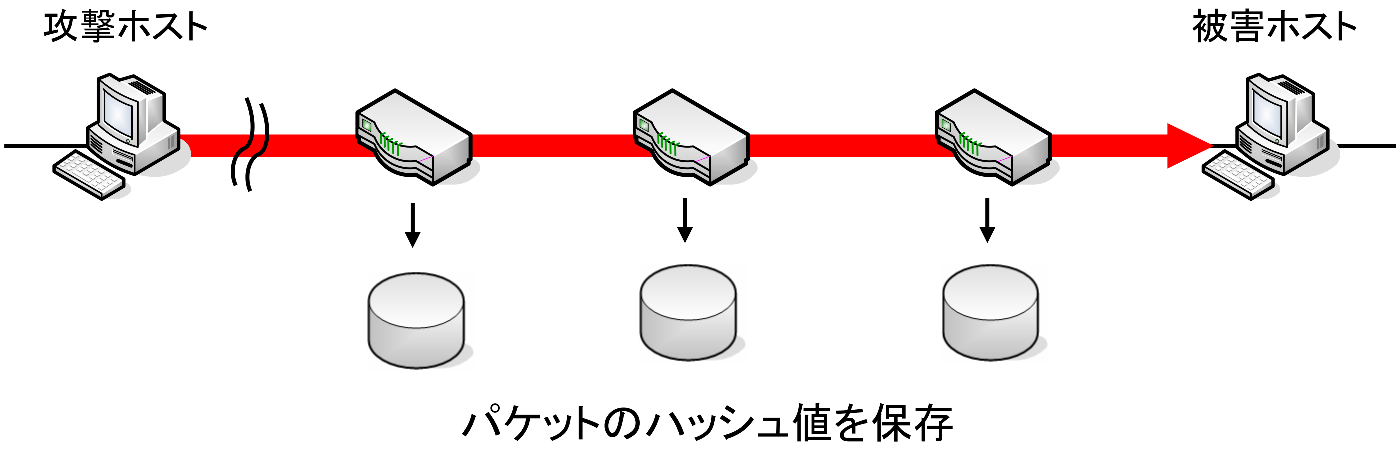
- IPヘッダ内の未使用ビットにマーキング
  - IPヘッダ（Identificationフィールド）
  - ルータのIPアドレスを分割して挿入
- 収集したマーキングパケットから攻撃経路を再構築



- 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パケットのログ（通過記録）を保存
  - IPヘッダの不変な部分
- ログ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
- 上位ルータの特定を容易化
  - MACアドレスを利用

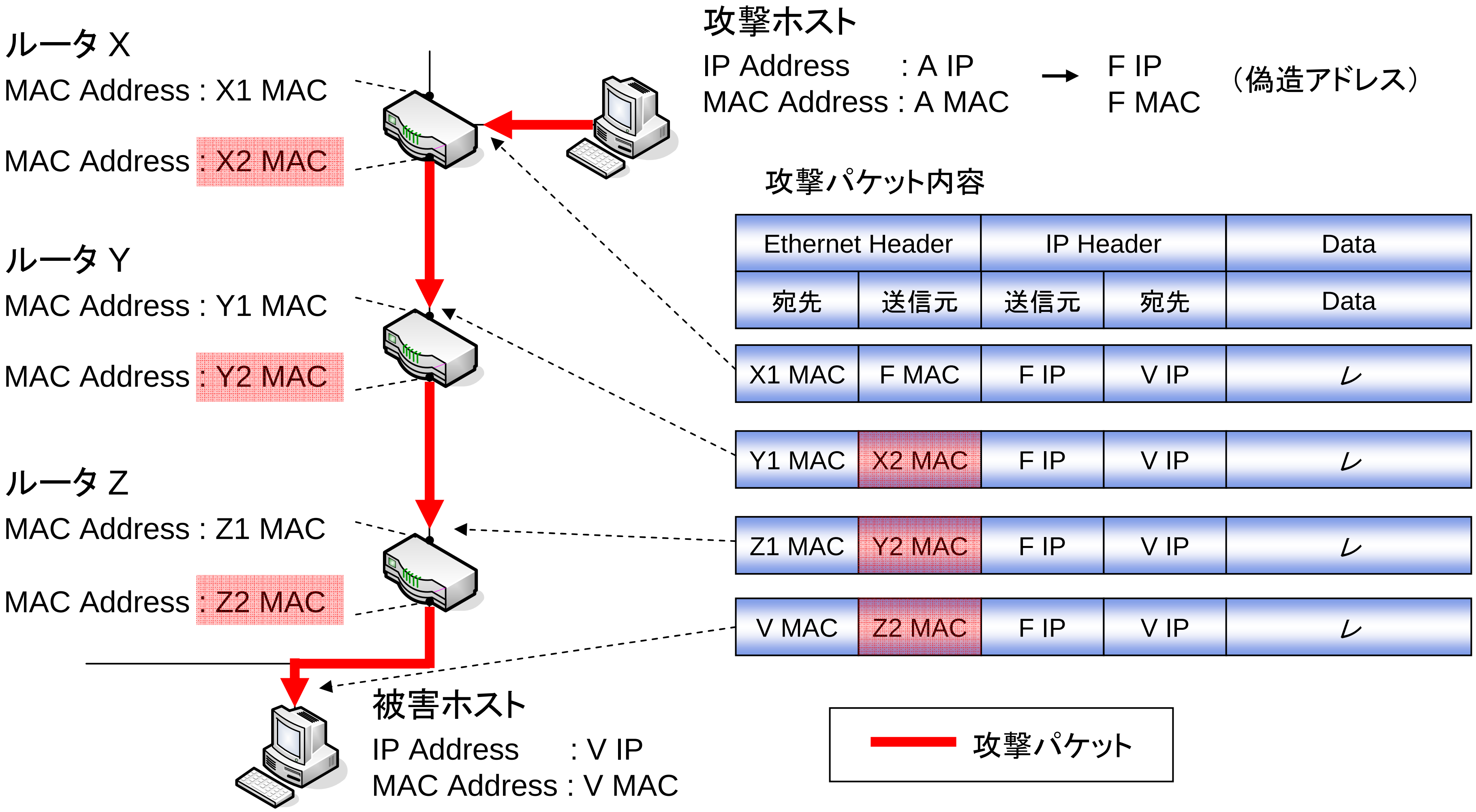


- 欠点
  - 大きな記憶容量や高いハッシュ処理能力が必要
  - あらかじめMAC情報を保持している必要がある

提案方式
MAC-based方式の特徴

- 詐称が困難なMACアドレスに注目
- 記憶容量・処理負荷の少ないトレースバック
- 下位レイヤに依存しないシステム

概要



ルータ X

MAC Address : X1 MAC

MAC Address : X2 MAC

ルータ Y

MAC Address : Y1 MAC

MAC Address : Y2 MAC

ルータ Z

MAC Address : Z1 MAC

MAC Address : Z2 MAC

攻撃ホスト

IP Address : A IP → F IP

MAC Address : A MAC → 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	F MAC	F IP	V IP	レ
Y1 MAC	X2 MAC	F IP	V IP	レ
Z1 MAC	Y2 MAC	F IP	V IP	レ
V MAC	Z2 MAC	F IP	V IP	レ

被害ホスト

IP Address : V IP

MAC Address : V MAC

攻撃パケット

レイヤ2の抽象化

- 上位ルータの特定
  - MACの情報を利用
- 上位ルータのアドレス記憶
  - IPアドレスを利用

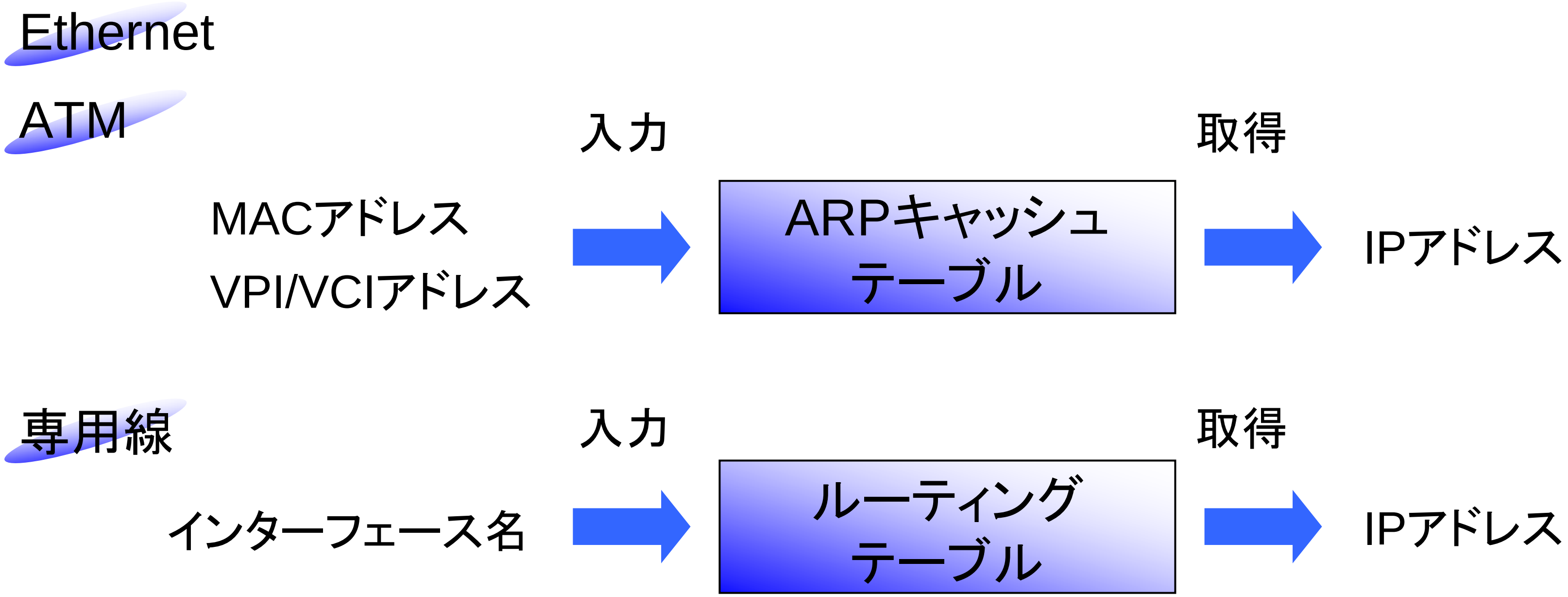
↓

- ISPは様々な通信媒体で構成
  - イーサネット、ATM、専用線等

レイヤ2を抽象化

抽象化の方法

- IPアドレスの取得
  - ARPキャッシュテーブル
  - ルーティングテーブル



Ethernet

ATM

入力

取得

MACアドレス

VPI/VCIアドレス

ARPキャッシュテーブル

IPアドレス

専用線

入力

取得

インターフェース名

ルーティングテーブル

IPアドレス

ルータの動作

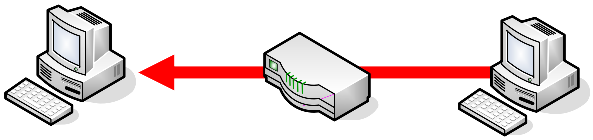
Temporary Table

1. 宛先IPアドレスとシグニチャごとにカウント値を加算
2. 時間単位（1秒）で消去
3. 特定の閾値を超えたらRecord Tableに保存*1

*1攻撃経路の判断材料

Record Table

1. 送信元MACアドレスから上位ルータのIPを取得
2. 宛先IPと上位ルータのIPを記録
3. 長期保存



宛先IPアドレスの記録

Temporary Table

Destination IP Address	Signature	Count
……..	……..	……..
V IP	……..	250
……..	……..	……..

閾値：250

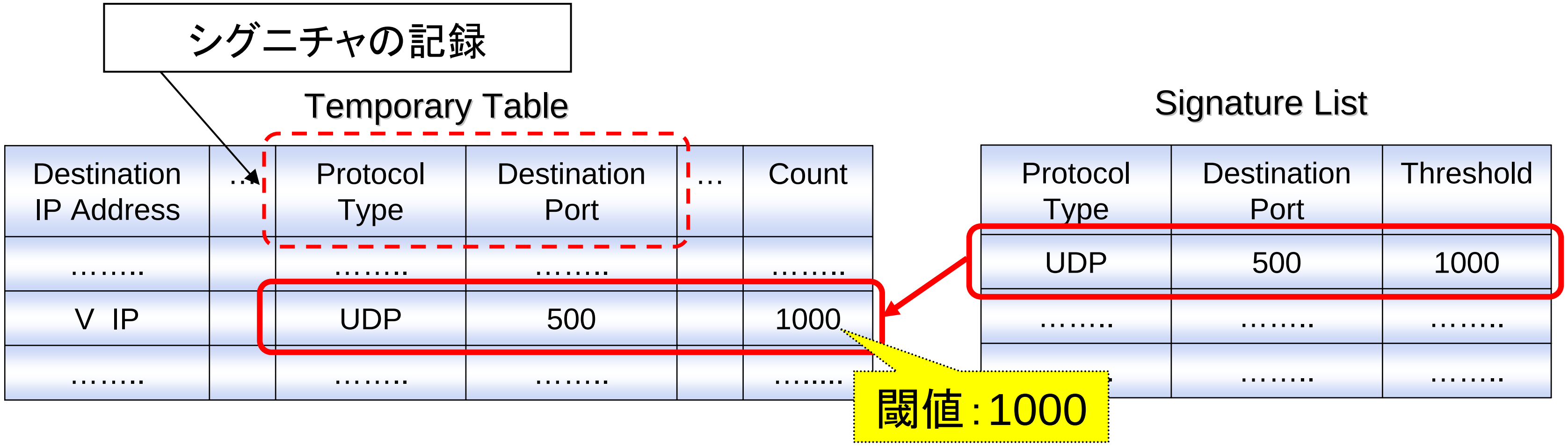
ARPキャッシュテーブルから取得

Record Table

Destination IP Address	Signature	Source IP Address
V IP	……..	Upstream Router
……..	……..	……..
……..	……..	……..

閾値の設定

- Temporary Tableの閾値
  - ルータの起動時に管理者によって決定
  - 手動または管理ホストからの指示で変更可能
- DoSの種類で閾値は異なる
  - DoS攻撃ごとにシグニチャが定義されているリストを保持
  - シグネチャリストに従い、Temporary Tableの内容を記録
  - シグニチャごとに閾値を設定



シグニチャの記録

Temporary Table

Destination IP Address	…	Protocol Type	Destination Port	…	Count
……..		……..	……..		……..
V IP		UDP	500		1000
……..		……..	……..		……..

閾値：1000

Signature List

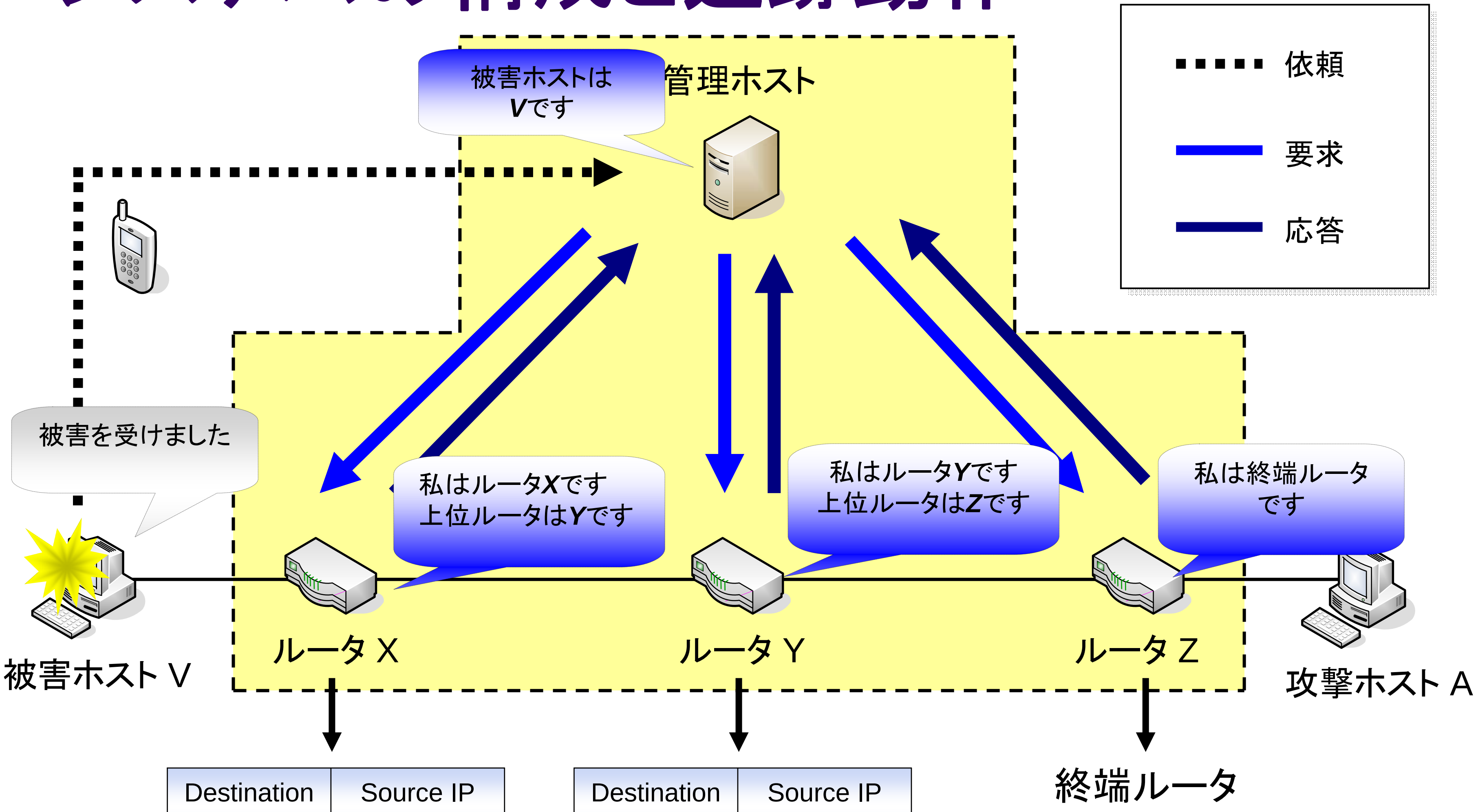
Protocol Type	Destination Port	Threshold
UDP	500	1000
……..	……..	……..
……..	……..	……..

DoS攻撃を判別するシグニチャ

- 少量パケットのDoS攻撃（IKE DoS）に対応
  - 計算処理の問題を突いた攻撃
- 単発パケットのDoS攻撃に対応
  - TCP/IPのセキュリティホールを突いた攻撃

DoS攻撃種類	シグニチャ
UDP Flood	プロトコルタイプ：UDP
SYN Flood	プロトコルタイプ：TCP、TCPフラグ：SYN
IKE DoS	プロトコルタイプ：UDP、宛先ポート番号：500、IPデータ長：＞800
Land Attack	プロトコルタイプ：TCP、 IPアドレス：宛先＝送信元、ポート番号：宛先＝送信元
Ping of Death	プロトコルタイプ：ICMP、 IPフラグメント：IPオフセット*8+IPデータ長>65535
WinNUKE	プロトコルタイプ：TCP、宛先ポート番号：139、TCPフラグ：URG
Reload Attack (F5 Attack)	プロトコルタイプ：TCP、宛先ポート番号：80、ペイロード：GET

システムの構成と追跡動作

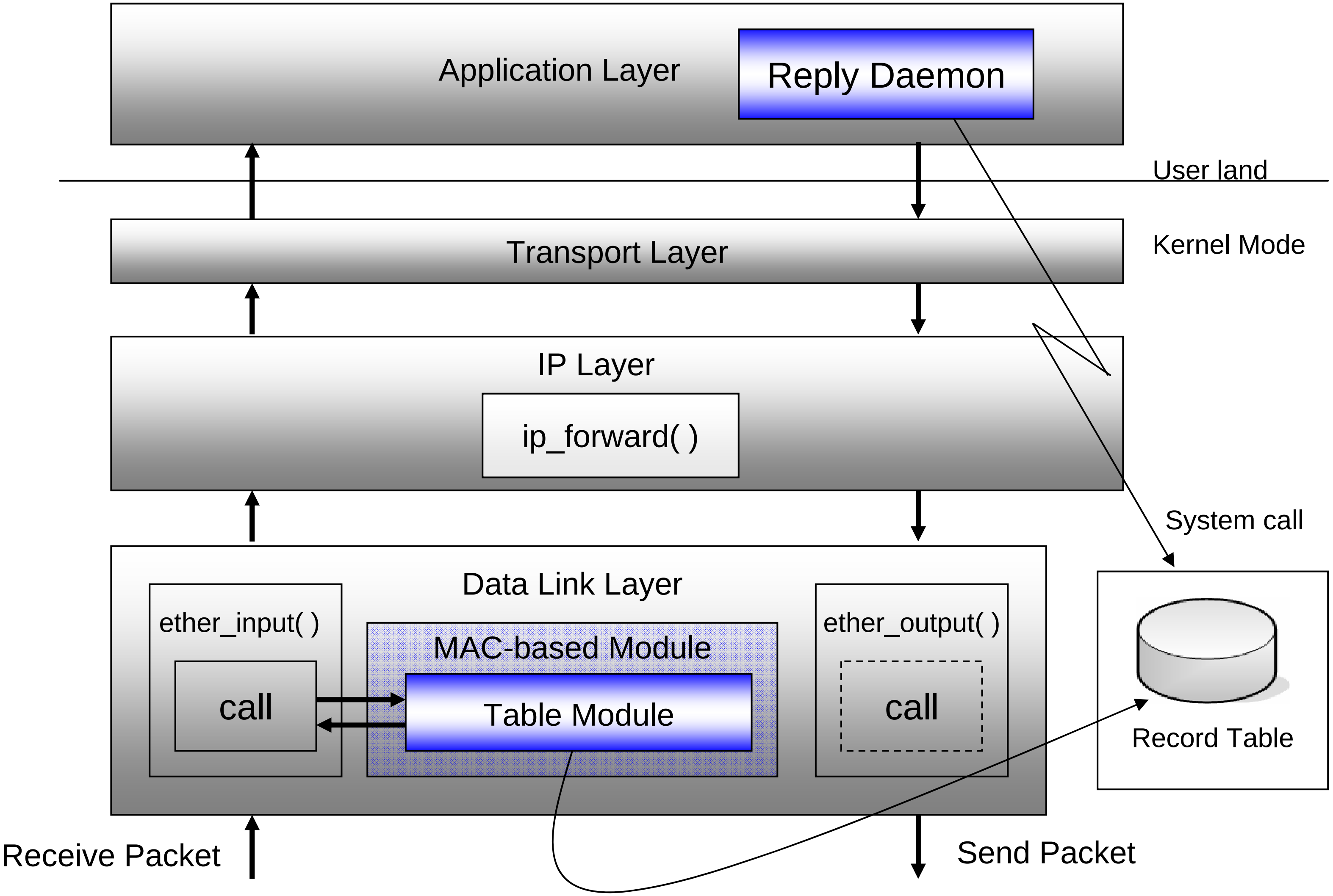


Destination IP Address	Source IP Address
V IP	Y IP
……..	……..
……..	……..

Destination IP Address	Source IP Address
……..	……..
V IP	Z IP
……..	……..

MAC-Basedプログラムの実装

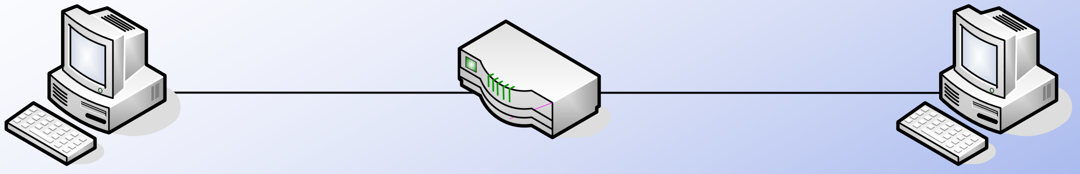
- FreeBSD 5.3に実装



性能測定

- ルータの中継処理に与える影響
  - FTPを利用したスループット測定
  - 1GBのバイナリファイル

測定環境



FTPクライアント

FTPサーバ

CPU	Pentium4 2.4Ghz
メモリ	256MB
NIC	Gigabit Ethernet
OS	FreeBSD 5.3

性能測定結果

	所要時間 [sec]	スループット [Mbyte/sec]	CPU負荷 [%]
未実装時	31.70	32.30	25.28
実装時	**31.87**	**32.14**	**25.88**

- 性能劣化は1%未満
- MAC-basedシステムを実装させても、性能の低下きわめて小さい

既存技術と提案方式との比較

	検出の確実性	解析量	パケットへの影響	ルータ性能への影響
マーキング方式	△	×	×	○
Hash-based方式	○	○	○	×
提案方式	△	○	○	○

- **検出の確実性**
  - Hash-based方式：確実にDoS攻撃パケットを検出可能
- **解析量**
  - マーキング方式：攻撃者の数が増えるほど増大
- **パケットへの影響**
  - マーキング方式：既存の通信への影響
- **ルータ性能への影響**
  - Hash-based方式：スループットの低下

むすび

- まとめ
  - MAC-basedトレースバック方式について提案した
    - MAC情報を利用して上位ルータを特定
    - テーブルを操作するだけの単純な動作
  - MAC-basedを実装し、性能測定を行った
    - MAC-basedによる性能劣化はきわめて小さい

- 今後の課題
  - DoS攻撃と具体的な閾値の決定
  - DDoS攻撃の対応について検討

おわり