3T-4

MACアドレスを用いたIPトレースバック技術の提案

播磨　宏和†　　竹尾　大輔‡　　渡邊　晃†
名城大学理工学部†　　名城大学大学院理工学研究科‡

1. はじめに

近年, インターネット人口の増大や常時接続環境の普及から, ネットワークセキュリティに対する問題が多発している．中でもサービス不能攻撃（DoS 攻撃）は大量の IP パケットを送りつけてサーバを動作不能にする悪質な行為である. 正当な動作を装うためファイアウォールによる防止が難しく, 攻撃パケットの送信元は偽造されていることが多いので攻撃者の身元を確認することはできない.

そこで DoS 攻撃のパケットから送信元を特定する技術として IP トレースバック技術が研究されている．既存の IP トレースバック技術には，input debugging 方式，ICMP Traceback 方式，マーキング方式，Hash-based IP トレースバック方式などが存在する.

本研究ではルータに残されたパケットのMACアドレス情報からトレースバックが可能となる方式を提案する.

2. 既存技術とその課題

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. 被害ホストは攻撃を受けた時点で攻撃パケット群を分析し, 攻撃パケットの特徴を抽出する．次にネットワーク管理者がルータの出力ポートにおいて攻撃パケットを判別するフィルタを設定することで入力ポートに接続しているノードを特定し, そのノードに対しても同様の操作を行うことで攻撃経路を再構築することができる．しかし, 攻撃ツールの発達により攻撃パケットの特徴抽出が困難になりつつあり, 複数の管理主体をまたがって隣接ルータのアクセスを繰り返すことが難しい.

ICMP Traceback 方式は ICMP に新たなメッセージ種別 traceback メッセージを定義し, ルータを通過するパケットに攻撃経路を特定するための情報を付与する．各ルータにおいて 2 万分の 1 という低い確率で ICMP traceback メッセージを生成することで通信量のオーバーヘッドを抑えている. 被害ホストは受け取った ICMP traceback メッセージから, 攻撃パケットが通過したリンク情報等を知ることが可能である. この手法では攻撃パケットの数が少ない場合，ICMP traceback メッセージを生成できないので発信源を特定できない可能性がある.

マーキング方式は逆探知のための情報を IPv4 ヘッダ内の未使用ビットを用いて被害ホストに伝える方式である. 細分化された隣接ルータの IP アドレスを IP ヘッダ内の IP identification フィールドに書き込むことによって，被害ホストに攻撃経路の情報を通知する. これらの情報を復元することで攻撃経路が構築できる. 問題点としては経路情報を IP identification フィールドに書き込むため，IPsec などの新しいアプリケーションとの親和性が低い. ルータ自身がある確率でパケットにマーキングを行うため，ICMP Traceback 方式と同様に攻撃パケットの数が少ない場合は発信源を特定できない可能性がある.

Hash-based IP トレースバック方式はすべてのパケットにおいて先頭部分から計算した複数のハッシュ値を記録する方式である．IP ヘッダの中で，経路中で不変な部分とペイロード（パケットシグニチャ）についてハッシュ関数を適用した結果をビットマップとして保存する. ビットマップは一定の時間間隔でゼロクリアされ, そのときに使用したハッシュ関数と共にダイジェストテーブルに保管する. 追跡時においては攻撃パケットのパケットシグニチャをダイジェストテーブルのハッシュ関数に通し, 記録されているかどうかを調査することで攻撃経路を再構成し追跡を行う. この方式では攻撃パケットが 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, ルータに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, 他の方式よりもコスト面で不利になる.

3. 提案方式

提案方式は既存のトレースバック技術とは異なり, ルータに残された攻撃パケットの送信元MACアドレスを手がかりとして攻撃側のエッジルータまでを追跡する.

DoS 攻撃では大量の攻撃パケットが攻撃ホストから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．ことのき，上流ルータから受信した攻撃パケットの送信元 MAC アドレスと宛先 IP アドレスの組をルータに記録しておくことで, 攻撃対象ホストに対する攻撃の経路を推測する手がかりを得る．以降，パケット

The proposal of IP trace back using MAC Address
† Hirokazu Harima
Faculty of Science and Technology，Meijo University
† Akira Watanabe
Faculty of Science and Technology，Meijo University
‡ Daisuke Takeo
Graduate School of Science and Technology，Meijo University

の送信元 MAC アドレスと宛先 IP アドレスを組アドレスと呼ぶ.

提案方式では図 1 のように情報を記録するテーブル 1, テーブル 2 を保持しており, それぞれカウント値が設けられている. ルータはパケット転送時にパケットの宛先 IP アドレスとその転送回数をテーブル 1 に記録し, その内容は一定間隔で消去する. 転送回数のカウント値にはある閾値を設けておき, カウント値が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, その時のパケットの組アドレスをテーブル 2 へと記録する正常なパケットがたまたま記録されることがあるので, このテーブルにもカウント値が設けられており, 記録されるごとに値は増加する. テーブル 2 の保持時間は短期間ではなく, 攻撃経路の判断材料となるため長期的に保持する.

テーブル1

Destination IP Address	COUNT値
……	……
……	……
M_ip	73
V_ip	1015
……	……
N_ip	28

テーブル2

Destination IP Address	Source MAC Address	COUNT値
……	……	……
V_ip	V_mac	25
V_ip	N_mac	43
……	……	……
……	……	……
V_ip	M_mac	7

図 1 記録テーブル

Fig.1 Record table

追跡時においては, 被害ホストは攻撃を受けた時点で上流ルータに対して逆探知のための問合せパケットを送信する. 問合せパケットには被害ホストの IP アドレスが含まれており, 受信した上流ルータは自身のテーブル 2 を用いて被害ホストの IP アドレスから組アドレスの送信元 MAC アドレスすべてを割り出す. 次にルータは自分自身の IP アドレス情報を加え, 割り出した MAC アドレスを持つ更に上流のルータに対して問合せパケットを送信する. 各ルータが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まで問合わせていく（図 2）.

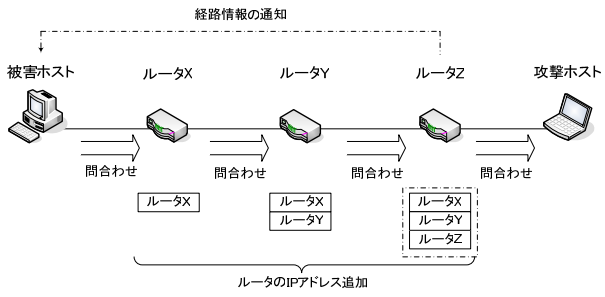

図 2 提案技術の概念

Fig.2 The concept of proposal technology

次に問合せパケットとその応答について述べる（図 3）. 問合せパケットを受信したルータが持つテーブル 2 に被害ホストの IP アドレスを含む組アドレスが存在しない場合は, その旨の応答を下流ルータへ返すことで, この経路は攻撃経路でないとわかる. 一方, エッジルータが攻撃ホストに最も近いルータは問合せを行っても応答は返ってこない. この場合は, 自身がエッジルータである可能性が高い. 問合せパケットには, 最終的に被害ホストからエッジルータまでの IP アドレスが書き込まれることから, このルータまでが発信源までの攻撃経路となる.

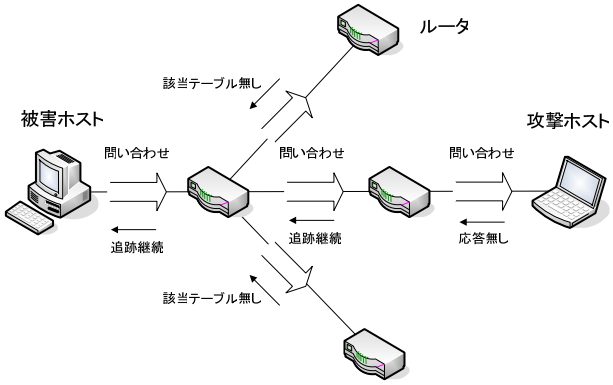

図 3 問合わせとその応答

Fig.3 An inquiry and its response

4. 評価

提案方式では, マーキング方式のようにパケットに新たな改良を加えないことからアプリケーションの親和性に影響を与えない. Hash-based IP トレースバック方式と比べ, ルータが行う処理は限られたものであり高い処理能力は必要としないと考えられる.

5. むすび

本研究では MAC アドレスを用いた IP トレースバック技術の提案について検討した. 今後は提案方式を実装し, 動作確認および検証を行う.

また, 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を確認する. 実装環境は FreeBSD とし IP 層に実装する予定である.

参考文献

[1] 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

[2] 門林雄基, 大江将史; "IP トレースバック技術", 情報処理 Vol.12 No.42, 2001

[3] Steve Bellovin, et al, "ICMP Traceback Messages", Internet-Draft, Expires August 2003