1Z-9

DoS攻撃の検知をトリガーとしたIPトレースバック手法の提案

桂井 友輝† 中村 嘉隆† 高橋 修†

公立はこだて未来大学 システム情報科学部†

1 はじめに

近年，ネットワークの普及・商用利用の規模は拡大の一途を辿っており，インターネットは人々の生活にとって不可欠な存在となった．しかしその反面，インターネットを利用した悪事の規模も年々拡大している．DoS 攻撃(Denial of Service attack)と呼ばれる，大量のデータや通信要求を対象のサービスに送りつけ，対象の処理能力やトラフィックサービスに過負荷を与える攻撃もまたその内の一つである．この DoS 攻撃に用いられるパケットは，通信プロトコル上は正当な動作を行うものであり，一般のファイアウォール機能による防御は難しい．また DoS 攻撃の大きな特徴として，パケットの送信元アドレスが偽装されていることが多く，攻撃元を簡単に特定できないようになっている．このアドレス偽装への対策の一つが，IP トレースバック[1]技術である．IP トレースバックを用いることで，攻撃経路や攻撃開始位置を特定し，攻撃元ホストをネットワークから遮断するための情報を得ることができる．IP トレースバックには様々な手法が存在するが，本研究ではその内ロギング方式と呼ばれる手法に着目した．ロギング方式の最大の問題点である各ルータの負担を，攻撃元の特定の速度，精度に可能な限り影響を与えないように減少させることを主目的とする．

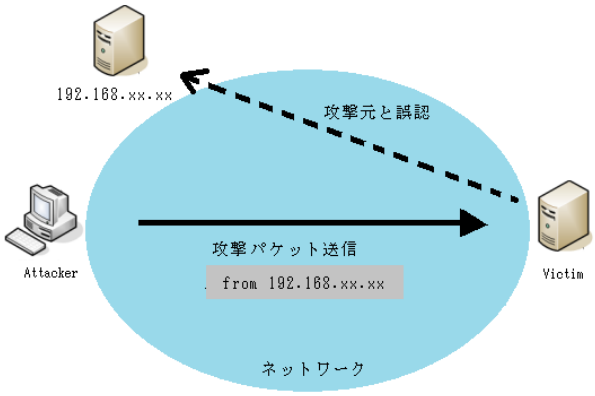

図 1: 攻撃元を詐称した DoS 攻撃

2 関連研究

ロギング方式は，ルータにログを記録する機能を追加する手法である．ネットワークを通過するパケットのログを記録し，攻撃パケットのログを上位ルータから再帰的に探索することで発信源の探知を行う．しかしルータが全てのパケットをログに記録することはディスク空間などの都合上不可能なため，ハッシュテーブルを用いたダイジェスト方式[2]などが提案されている．この方式では，パケットの内容の一部にハッシュ関数を適用し，その結果をビットマップとして保持する．このビットマップは一定の間隔で初期化され，その期間中に使用したハッシュ関数とともにダイジェストテーブルに保管される．この方式を用いることで，探査端末は各ルータに対し能動的に攻撃パケットの通過の有無を問い合わせることができる．この方式には，攻撃パケットの数が少なくとも攻撃元を特定することができるという利点がある．問題点としては，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点，随時パケットのログを記録し続けるということから，ルータへかかる負荷が大きい点などが挙げられる[3].

“A proposal of the IP traceback technique which detection of a DoS attack triggers off”
Yuuki Katsurai†, Yoshitaka Nakamura†, Osamu Takahashi†
† School of Systems Information Science, Future University Hakodate

3 提案方式

本提案方式では，IDS などの不正アクセス監視システムが DoS 攻撃を発見した際に，その情報をトリガーとして各ルータがログの収集を開始するといった手順を取る．

3.1 想定環境

本研究では通常の通信がランダムに行われているネットワーク環境において不特定のタイミングで DoS 攻撃が開始されたことを想定する．またネットワークを構成する全ルータに，提案方式に必要な機能が追加されていると仮定する．この機能に関しては次項で述べる．

3.2 ルータへの機能追加

提案方式を実現するためにネットワークを構成するルータに機能を 2 つ追加する．1 つ目に， ルータを通過するパケットのログを保存するための機能と，保存に必要なディスク空間を用意する．2 つ目に，各通知の送信，受信を行う機能を導入する．ログの保存に関する通知，攻撃に用いられたパケットの発見に関する通知を各ルータ間でやり取りする．

3.3 トレースバック開始の手順

IDS が DoS 攻撃を検知した際，被害ノードに最も近いルータに対し，ログの保存命令と攻撃に用いられたパケットの特徴を通知する．通知を受け取ったルータはログの保存を開始し，同時に隣接するルータに対し同様に通知を行う．その通知を受け取ったルータは更に隣接するルータに通知し，最終的にネットワークを構成するルータそれぞれに通知が行き渡る．また，各ルータが隣接ルータに通知を送信する際には通知に含まれる被害ノードからのホップカウントを増加させる．通知を重複して受け取った場合は，ホップカウントが最も小さいもののみを残し，他の通知を破棄する．各ルータは通知のやり取りを行った後に，自身が保存を開始したパケットのログ内から攻撃パケットの検索を行う．

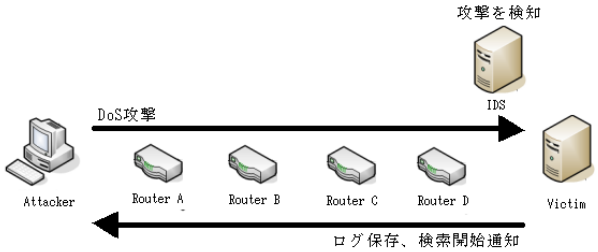

図 2: トレースバック開始時

3.4 攻撃パケットを発見した際の手順

ログ内に攻撃パケットを発見した際は，ログの収集，パケットの検索を終了する．同時に，ログの収集命令，攻撃パケットの特徴を通知した時と同様に，隣接ルータに対し

て自身の位置を記した発見通知を送信する．発見通知を受け取ったルータは，自身もパケットを発見していた場合は．ホップ数を比較して差が 1 であったならば正しい経路として保存．その旨を通知の送信元となるルータに送信する．またログの保存，検索を行っている各ルータは，隣接ルータから発見通知を受け取った際，その通知のホップカウントが自身の保持する通知のホップカウントよりも大きかった場合，動作を終了する．

全てのルータが検索を行い一定の時間が経過した後，攻撃パケットを発見したルータの内，被害ノードからのホップカウントが最も大きいルータを攻撃元ホストに最も近いルータ(エッジルータ)と判断し，被害ノードに対し自身の位置を通知する．またログから攻撃パケットを発見できなかったルータは通常の動作に戻る．

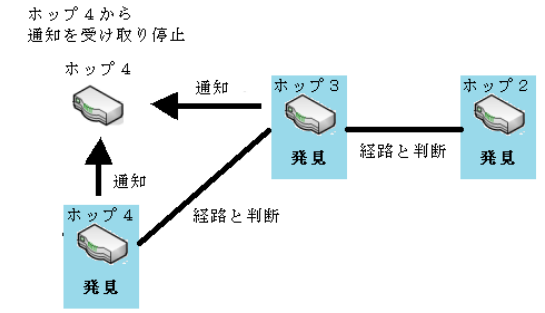

図 3 : 攻撃パケット発見時

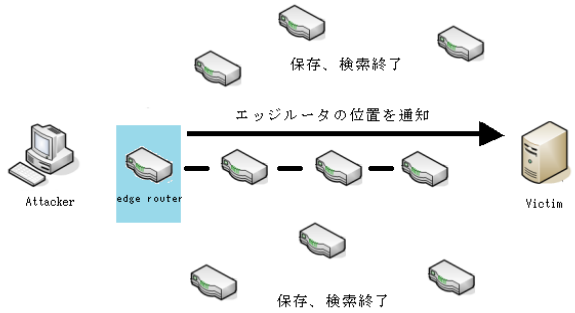

図 4: 動作終了時

4 予備実験

提案方式の予備実験として，ハッシュ関数を適用しない場合における DoS 攻撃検知後の攻撃元ホストの位置特定の精度を調べるため，ネットワークシミュレータである ns-2（Network Simulator version 2）[4]上で評価実験を行った．評価方法は，ルータが常にログを保存し続ける場合と本提案方式の場合，すなわち通知を受け取ってからログの保存を開始する場合についてそれぞれ，DoS 攻撃が開始してからの経過時間 100ms ごとに 100 回ずつトレースバックを行い，特定精度を比較した． またこの際，DoS 攻撃に関わらない通信パケットはランダムに送受信されているものとし，被害ノード側は DoS 攻撃を受けてから 1000ms 後に攻撃を検知すると仮定する．

表 1: ネットワークシミュレーションのパラメータ

各リンクの伝送速度	10Mbps, 100Mbps
通信プロトコル	TCP
DoS 攻撃の形式	SYN Flood

5 考察

図 5 の実験結果から，ルータが常にログを保存し続けている場合，本提案手法を用いる場合それぞれの攻撃元ホストの位置特定精度を比較した際，常にログを保存し続ける場合が常に 100%の精度を保っていたのに対し，経過時間が一定以下の場合は本提案手法を用いる場合の特定精度が著しく低下した．これは DoS 攻撃が開始されてから攻撃元ホストのエッジルータがログ保存を開始するまでの時間の差によるものであり，本提案手法を用いる場合は，エッジルータが通知を受け取るまで攻撃が継続していなければ特定が不可能であるということを示している．しかしある一定の経過時間からはどちらも精度が 100%であったことから，ある条件下での本提案手法の有用性を示すには十分であるといえる．このことから，本提案手法は短期間に行われる小規模の DoS 攻撃ではなく，長期にわたって行われる大規模な DoS 攻撃に対して効果を発揮するということが読み取れる．DoS 攻撃の規模を判別するため，また攻撃元ホストのエッジルータを誤検出することを防ぐためにも，ネットワーク環境別のトラフィックを考慮した追加機能の実装が求められる．今後の実験では，ハッシュ関数を適用した際の挙動，特に各ルータの処理量の評価，検出にかかる時間についても評価，検討を行う．

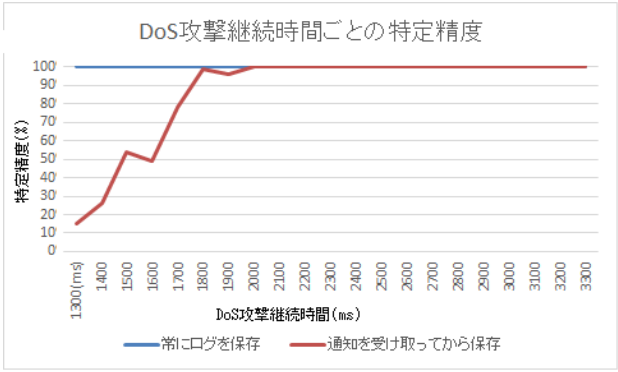

図 5: 実験結果

6 おわりに

本研究では IDS などによる DoS 攻撃の発見をトリガーとした IP トレースバックの手法を提案した．提案方式による予備実験によると，DoS 攻撃がある一定以上の時間にわたって継続された場合の特定精度は 100%を保った．

今後は，提案方式の有用性を裏付けるため，ns-2 上での提案方式の実装の拡張，評価を課題とする．提案方式を用いた場合の各ルータの処理量，ハッシュ関数を実装した場合の検知精度，速度について評価を行う予定である．

参考文献

[1] Japan Data Communication Association, “トレースバック研究ポータル”, https://www.telecom-isac.jp/tb/#.

[2] L.A. Sanchez C.E. Jones F. Tchakountio S.T. Kent A.C. Snoeren, C. Partridge and W.T. Strayer. Hash-based IP traceback. Proceedings of ACM SIGCOMM. 2001.

[3] 井上慎一郎, 石井方邦, 笹瀬巌. DDoS攻撃に対して排他的論理和と確率的Marking方式を用いることでルータへの負荷分散を実現するIP Traceback. 情報処理学会論文誌 Vol.53 No.2, pp.795-804. 2012..

[4] ns-2, “The Network Simulator version 2,” http://www.isi.edu/nsnam/ns/.