DDoS攻撃に対応したIP TracebackのためのHop Label based Probablistic Packet Marking手法の提案

Hop Label based Probablistic Packet Marking for IP Traceback addressing DDoS Attacks

M-99

小川　敏明† 中村　文隆†‡ 若原　恭†‡
Toshiaki Ogawa Fumitaka Nakamura Yasushi Wakahara

1. まえがき

近年，多数の攻撃者が同時に大量のトラフィックを特定のホストに送りダウンさせる攻撃が社会問題になっている．このような攻撃をDDoS(Distributed Denial of Service)攻撃と呼ぶ．現在，DDoS攻撃の有効な対処法の一つは，攻撃者の最寄のルータでフィルタリングを行うことであると言われている．

しかし，DDoS攻撃において攻撃者は送信元IPアドレスを偽装している[1]ことが多いため，現在受信パケットからは攻撃者の最寄のルータを特定することはできない．そのため，攻撃者の最寄のルータを検出することを目的とするTraceback手法が重要となってきている．[3]

その中で最も効果的な手法は，Edge Sampleを利用したProbablistic Packet Marking手法である．しかし，Edge Sample手法は，攻撃者に最寄のルータを検出するのに完全な経路を再構成する必要があるためにその検出効率が低いという問題がある．本稿ではその問題点を解決するために，新たにHop Labelに基づくProbablistic Packet Marking手法を提案する．

2. Edge Sample手法の問題点

Edge Sample手法の動作原理は次の通りである．まず，一部の機能拡張ルータ（以下，CN:Co-operatingと呼ぶ）で，経由するパケットに対して次に示すマーキング処理を行う．ただし，そのパケットには，隣接する2つのCNのIPアドレス(Address Label，Next Address Label)と，それらのうち先にマークしたCNと犠牲者との間の距離(step数）を記録するフィールドが定義されている．ここでstep数とは，あるCNから別のCNに到達するのに通過するCN又は犠牲者の数を表す．

1. 各CNは確率pで自分のIPアドレスをAddress Labelに上書きしてマークする．
2. CNが上書きした場合，step数の値を0として，Next Address Labelを空にする．
3. CNが上書きしなかった場合，step数の値を1だけ増加する．もし，Next Address Labelが空であれば，自分のIPアドレスを書き込む．

次に，犠牲者はマーキングされたパケットを受信して，犠牲者から攻撃者に向けて，CNのリンクを逐次的に連結して経路を再構成していく．最後に，経路が完全に再構成されたときのリーフにあたるCNを攻撃者に最寄のCN（NCN:Nearest CN）と判定する．

†東京大学大学院新領域創成科学研究科
‡東京大学情報基盤センター

Edge Sample手法は，すべてのCNのリンク情報を収集すれば完全に経路を再構成できるという点で優れているが，大きく以下の2つの問題がある．

1. すべてのCNのリンク情報を収集しなければ，経路を再構成できずにNCNを特定できないため，検出効率が低い．
2. NCNを検出するのに必要なパケット数が，NCNと犠牲者との間のstep数に依存して増加する割合が大きい．

3. Hop Label手法の提案

2. で指摘した問題点を解決するために，あるCNを基点として，そのCNから犠牲者までの経路上に存在するCNの位置を記録した情報（以下，Hop Labelと呼ぶ）を用いることで，完全な経路の再構成を必要とせずにNCNの検出を可能とするHop Label手法を提案する．本手法では，IPv4パケットのIP Optionフィールドに，新たにAddress Label(32bit)，Hop Label(32bit)，Previous TTL(8bit)を定義する．

Hop Label手法の処理は，Packet Marking Process(PMP)とPath Reconstruction Process(PRP)に大別される．図1は，攻撃経路の具体例を表しており，以下の説明で利用する．

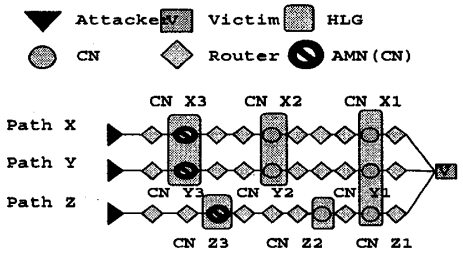

図1: Hop Label手法における攻撃経路の一例

3.1 Packet Marking Process

PMPでは，次のような動作原理で各フィールドに処理を行う．

Address Label

Address Labelの値が空なら，CNは確率pでこのフィールドに自分のIPアドレスを記録する．このアドレスを記録したCNをAddress Marking Node(AMN)と呼ぶ．

Previous TTL

Address Label が書き込まれているなら，CN はパケットの現在の TTL の値を Previous TTL に上書きする．

Hop Label

ここでは，Hop Label の値を，AMN と犠牲者との間に存在する CN の位置に対応した bit 値を 1 とする 32bit のビットパターンで表している．Address Label が書き込まれているなら，CN は Previous TTL の値とパケットの現在の TTL 値との差分から直前の CN との Hop 数を求めて，Hop Label に記録する．CN が Address Label を書き込んだときも，Hop Label に自分が基点であることを記録する．

図 1 では，X,Y,Z の 3 つの経路でそれぞれ一つずつ攻撃パケットが生成され，CNX3,CNY3,CNZ3 が AMN となっている場合を表している．犠牲者が受信した各パケットの Hop Label 値は図 2 に示す通りである．経路 X，Y は AMN と犠牲者との間の CN の配置が等しいので，HLX3 と HLY3 の値は等しいが，経路 Z はそれらと異なる配置をしているので，HLZ3 の値も異なる．

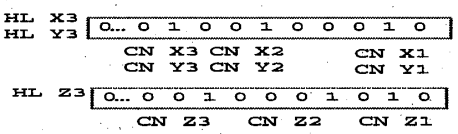

図 2: PMP 処理後の Hop Label の一例

3.2 Path Reconstructing Process

自分を基点としたときの Hop Label 値が等しい CN をまとめて Hop Label Group(HLG) と呼ぶ．犠牲者は，マークされたパケットを一つ受信すると，AMN とそれ以降に経由した CN が属する HLG を知ることができるので，HLG をノードとし，その中に AMN が存在する経路を一つ生成できる．そのような経路を連結して最終的にツリーを構成する．そして，そのツリーのリーフにあたる AMN を NCN とみなす．図 3 は，CNX3，CNY3，CNZ3 でマークされた 3 つのパケットを受信した際に再構成される経路を表しており，3 つの NCN を検出した結果を示している．

4. Edge Sample 手法との比較評価

Edge sample 手法と Hop Label 手法の本質的な違いは，前者は必要なパケット数は多少多くても犠牲者から NCN に向かって完全に経路を再構成していくことに主眼をおいているが，後者は厳密に途中の経路を再構成することなく少ないパケットで高速に NCN を検出することに主眼をおいている点である．両者の比較評価は次の通りである．

NCN の検出効率

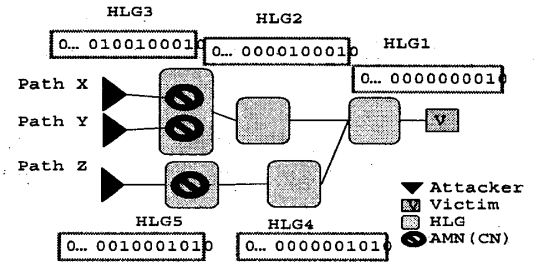

図 3: PRP 処理後の Hop Label Model の一例

Hop Label 手法の方が Edge Sample 手法に比べて，受信したパケット数が少ない場合における NCN の検出率は高いと期待できる．これは，冒頭で述べた NCN の検出方法の違いによる．一攻撃経路において Hop Label 手法では NCN の検出に必要なパケット数が NCN の step 数に依存せず一定であるのに対して，Edge Sample 手法では，NCN の step 数の増加関数となっている．[3]

オーバーヘッド

IPv4 では，両者で計算負荷と必要な情報量のサイズは大きな違いはない．ただし，アドレス空間が拡大すると（IPv6），Hop Label 手法では簡単な bit 演算で済むのでオーバーヘッドが少ないが，Edge Sample 手法ではハッシュ演算などの複雑な処理をするためにオーバーヘッドが大きくなる．また，必要な情報量のサイズも Edge Sample の方が大きくなる．

5. まとめと今後の展望

本稿では，DDoS 攻撃における IP Spoofing の対策として，Edge Sample 手法に代わり高速に NCN を検出することが期待できる Hop Label 手法を提案した．セキュリティに関しては，現状では攻撃者は容易にマーキングするアドレスを偽装できるので，今後それに対する検討が必要がある．また，PRP で再構成された経路において，リーフ以外の AMN が NCN である場合に関しても検出可能にすることが今後の課題である．

参考文献

[1] R. T. Morris, "A weakness in the 4.2BSD Unix TCP/IP Software," AT&T Bell Labs, Tech. Rep. Comput. Sci. 117, 1985.

[2] Paul J. Criscuolo, "Distributed Denial of Service", CIAC-2319, Feb. 2000.

[3] Stefan Savage, David Wetherall, Member, IEEE, Anna, Karlin, and Tom Anderson, "Network Support for IP Traceback," IEEE/ACM transaction on networking, vol. 9, no.3, JUN. 2001.