社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2005－DPS－122（59）
2005－CSEC－28（59）
2005／3／23

DDoS 攻撃に対する AS 間発信源探査方式の提案

甲斐 俊文*　長嶋 昭人*　中谷 浩茂*　清水 弘*　高橋 輝壮**　鈴木 彩子***
*松下電工株式会社 システム技術研究所　**工学院大学 情報工学科
*** NTT アドバンステクノロジ株式会社 コアネットワーク事業本部 システム開発ユニット

あらまし インターネットの普及に伴って，不正アクセスによる被害が増加傾向にある．特に，送信元アドレスを偽装した DoS（Denial of Service）攻撃や DDoS（Distributed DoS）攻撃は，システムを停止に追いやることもあり，社会生活への影響が出始めている．その対策のために，幾つかの発信源探査方式（トレースバック方式）が提案されている．本稿では異なる探査方式が導入されたネットワーク（AS）間での探査を可能にするための AS 間発信源探査方式を提案する。また、探査に要する時間についてテストベッドでの実験により評価する。

Inter AS Traceback Method for Detecting DDoS Attacks

Toshifumi KAI*　Akito NAGASHIMA*　Hiroshige NAKATANI*　Hiroshi SHIMIZU*
Teruaki TAKAHASHI**　Ayako SUZUKI***

*Matsusita Electric Works, Ltd.　Systems Technology Research Laboratory
**Kogakuin University　Dept. of Computer Engineering
***NTT Advanced Technology Corp, Core Networks Bussiness Headquarters System Development Unit

Abstract　The amount of damage by illegal access is increasing with the spread of the Internet. Especially the DoS (Denial of Service) and DDoS (Distributed DoS) attacks cause system down and often have serious impacts on the society. Various attacker detection techniques have been proposed until now.　We propose inter AS(Autonomous System) traceback method for detecting attackers on large scale network. Performance of this proposed scheme was clarified by some numerical models and experiment.

1.　はじめに

ネットワークが社会的インフラとして定着した今日、これを用いたサービスの提供は当然のものと認識されている。一方で、それを停止させようとする妨害も増加の一途を辿っている。このような「攻撃」と呼ばれる妨害行為の代表的なものに DoS（Denial of Service）攻撃や DDoS（Distributed DoS）攻撃がある。これらの攻撃は一般的に送信元 IP アドレスを偽装したパケットを用いていることが多く、被害者側には真の発信源が特定できないため対策が困難なものとなっている。

攻撃の発信源を探査する手法として、不正パケットの経路を基に探査を行うトレースバック（図１）がある。ただし、インターネットは、プロバイダネット、行政ネットなど固有のポリシーによって管理され AS（Autonomous System）の集合体で構成されているため、複数の AS にわたって同じ方法で探査することは不可能に近い。そこで、AS 間のトレースバックと AS 内のトレースバックを階層的に行う必要があると言われている[1]。

我々はすでに AS 内トレースバックに関して、高速かつ高精度なハイブリッドトレースバック方式を提案しているが[2]、AS 間のトレースバックについても並行して研究を進めてきた [3]。我々はまず、MIT の Moriarty が提案している RID(Real-Time Inter-Network Defense)[4]を参考にして、AS 間で

トレースバック情報を交換するプロトコルを規定した。その後、このプロトコルを用いて異なる AS 同士で AS 内トレースバックシステムを連動させることによりインターネットのような複数の AS から構成される大規模ネットワークに適用可能な AS 間発信源探査システムを考案した。本稿では、考案した AS 間トレースバックプロトコルと AS 間発信源探査システムの説明を行い、実装したシステムの性能評価の結果を示す。

なお、同様の研究として国立天文台の大江らにより IP トレースバックシステムの相互接続アーキテクチャが提案されている [5]。しかしその実現性が実環境で実証されてはいない。

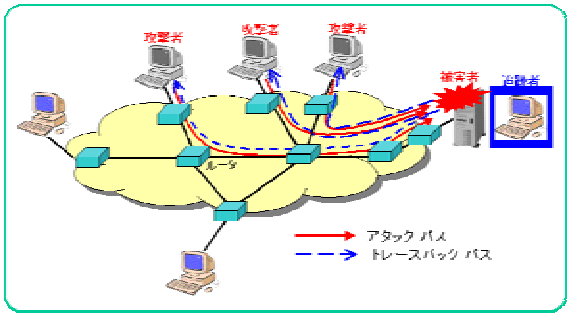

図 1　トレースバック

2.　関連研究

2.1.　AS 内トレースバック

パケットやトラフィックの発信源および通過経路をルータ単位で探査する IP トレースバック方式が数多く提案されている。我々はこれらの方式を AS 内トレースバックと呼んでいる。探査対象がトラフィックであるか単一のパケットであるかによって、AS 内トレースバックは複数パケット探査型と単一パケット探査型に分類できる。複数パケット探査型としては ICMP 方式[6]、マーキング方式[7]、UDP 方式[2]などがあり、単一パケット探査型としては Hash 方式[8]がある。

2.2.　AS 間トレースバック

異なる AS 内トレースバック方式を導入した AS 同士で連携して発信源探査を行うためには、AS 内トレースバックから独立して、探査要求や探査情報をやり取りするための仕組みが必要になる。この仕組みを我々は AS 間トレースバックと呼んでいる。AS 間トレースバックに相当するものとして、以下に挙げる RID と IP トレースバックシステムの相互接続アーキテクチャが提案されている。

2.2.1.　RID

RID は IETF(Internet Engineering Task Force)の inch ワーキンググループにおいて提案されている、複数 AS を経由する攻撃の追跡を目的としたインシデント情報交換プロトコルである。

各 AS には NMS(Network Management System)が設置され隣接 AS の NMS と接続される。NMS 間でやり取りされるメッセージとして Trace Request、Trace Authorization、Source Found 等が規定されている。

攻撃追跡の手順は図 2 の通りである。(1)被害者のいる AS の NMS で攻撃を転送してきている隣接 AS を調べ Trace Request を送信する。(2) Trace Request を受信した NMS は、追跡を実行するかどうか判断した結果を Trace Authorization によって送り返す。(3)追跡を実行する場合は(1)と同様、攻撃を転送してきている隣接 AS を調べ、Trace Request を送信する。(4)もし攻撃源を発見したら、Source Found を被害 AS に送信する。

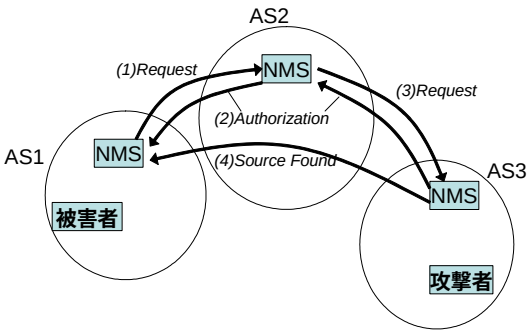

図 2　RID による追跡手順

RID では NMS 間の情報交換に焦点を当てており、内部トレースバックとの連携方法（インターフェースや詳細な手順）に関しては言及されていない。

2.2.2.　IP トレースバックシステムの相互接続ア

ーキテクチャ

IP トレースバックシステムの相互接続アーキテクチャは文献[5]で大江らにより提案されている AS 間トレースバックの仕組みであり、次の３つの要素から構成される。

-AS 内で攻撃が通過したルータを特定するための TS(Traceback System)

-AS の境界で攻撃フローの流入元を特定するための BTS(Border Traceback System)

-AS 間でトレースバック情報交換および TS/BTS の統括を行う ITM(Internet Traceback Manager)

動作手順を図 3 に示す。(1)被害者のいる AS 内で BTS により攻撃フローの流入元を特定し、トレースバック要求を送信する。(2) トレースバック要求を受信した ITM は同様に BTS により攻撃フローの流入元を調べ、トレースバック要求を送信する。(3) BTS により自 AS 内に攻撃フローの送信元があることが判明した場合、TS により AS 内トレースバックを行い、結果を要求元に返す。(4)結果を受け取った ITM は要求元に転送する。

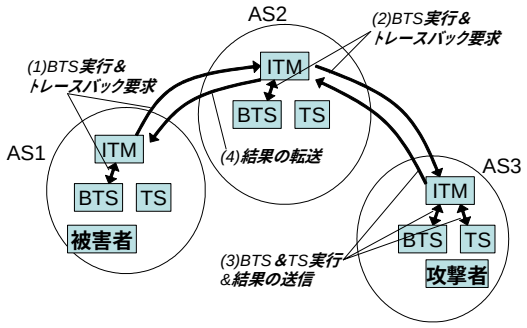

図 3　IP トレースバックシステムの相互接続アーキテクチャの動作

3.　提案方式

我々は管理単位の異なる AS 間での追跡を実現するためのシステムを実現するにあたり、RID に着目して研究を進めてきた。RID は前述のように内部トレースバックとの連携方法に関しては触れられておらず、NMS 間でやり取りされるメッセージフォーマットの規定に留まっている。そこで我々は AS 間発信源探査システムとして、RID の仕組みをベースに、様々な AS 内トレースバック方式に対応したメッセージフォーマット、効率的な追跡手順、および AS 内トレースバックとの連携手順を考案した。

我々の提案方式は IP トレースバックシステムの相互接続アーキテクチャと、追跡手順がほぼ同じであるが、実環境での適用を可能とするために、次の機能を実現した。

-攻撃のタイプに適した AS 内トレースバック方式の選択実行

-AS 毎の追跡実行ポリシー設定

-AS への部分的なシステム導入

3.1.　システム構成

各 AS は NMS、境界探査システム、内部探査システムの３つの構成要素を持つ。

(1) NMS(Network Management System)

NMS は AS 間発信源探査機能を実装した装置で、AS 毎に一台設置される。図 4 に示すように、NMS は AS 間発信源探査プロトコルを処理するモジュール(RIS)を持ち、隣接 AS 間の NMS が相互に接続された NMS ネットワークを構成する。また、NMS は追跡する攻撃の種類や AS 管理者によって設定されたポリシーなどに基づいて、追跡要求に応じるかどうかや実行する境界／内部探査システムを決定するモジュール(DM)を持ち、他 AS からの追跡要求に応じてこれらのシステムに探査を行わせる。また、様々な境界探査システムや内部探査システムに応じて、DM モジュールとのインターフェースとなるモジュール(TM)を持つ。

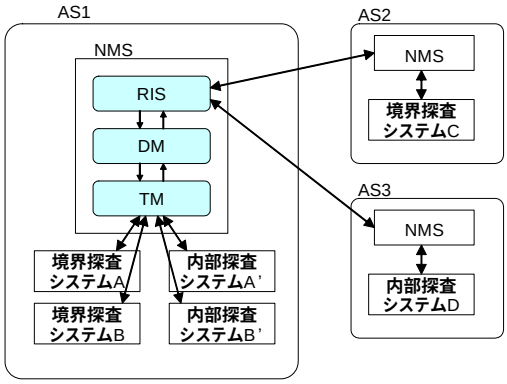

図 4　AS 間発信源探査システムの構成図

(2) 境界探査システム

境界探査システムは、NMS から指定された攻撃パケットや攻撃トラフィックがどの隣接 AS から流入してきているかを探査し、その結果を NMS に返す。

(3) 内部探査システム

内部探査システムは NMS から指定された攻撃パケットや攻撃トラフィックについて、AS 内のルータ単位での発信源探査を行い、結果を NMS に返す。

境界探査と内部探査は他の AS から独立して動作するため AS 毎に異なる方式のシステムを導入することが可能である。また、大量パケット攻撃探査用や単一パケット探査用など複数のシステムを導入し、攻撃によって使い分けることも可能である。

内部探査を実現するトレースバック方式としては、ICMP 方式、マーキング方式、Hash 方式、我々の提案している UDP 方式などがある。これらの方式を境界ルータだけに適用することで、境界探査システムを実現できる。CenterTrack[9]のように境界探査を主目的とした方式も提案されている。

3.2. AS 間発信源探査プロトコルのメッセージ

AS 間発信源探査プロトコルでやり取りされるメッセージは、Trace Request、Trace Authorization、Trace Result の 3 種類である。以降の説明ではそれぞれ Request、Auth、Result と略記する。

Request は追跡要求メッセージであり、攻撃パケットや攻撃フローを特定するための情報や被害ノードの IP アドレスなどを持つ。Auth は追跡要求に対する応答メッセージであり、要求された追跡を実行するか拒否するかを示す情報を持つ。Result は追跡結果メッセージであり、攻撃経路や攻撃ノードの IP アドレスのリストを持つ。これらのメッセージのフォーマットは、AS 内トレースバックとして ICMP 方式、マーキング方式、UDP 方式、Hash 方式など様々な方式が導入されていても必要な情報が交換できるように規定した。

3.3. 動作概要

各 AS に配置された NMS の動作を図 5 に示す。

(1) Request の受信

Request を受け取ると、DM により探査を行うかどうかを決定する。

(2) Auth の送信

Request 送信元の NMS に Auth を返信する。探査しない場合は直後に処理を終了する。

(3) 境界探査の実行

DM は攻撃の情報やポリシー設定に従って適切な境界探査システムを選択し探査を行う。

(4) Request の送信

境界探査により攻撃の流入元 AS を発見した場合、それらの NMS に Request を送信する。

(4') 応答待ち

送信した Request 毎に Auth の返信を待つスレッドを立てる。Auth を受信し、要求が受け入れられていた場合は Result を待つ。また、受け取った Auth／Result は追跡の起点となっている AS まで転送する。

(5) 内部探査の実行

DM は攻撃の情報やポリシー設定に従って適切な内部探査システムを選択し探査を行う。

(6) Result の送信

Request 送信元の NMS に Result を返信する。

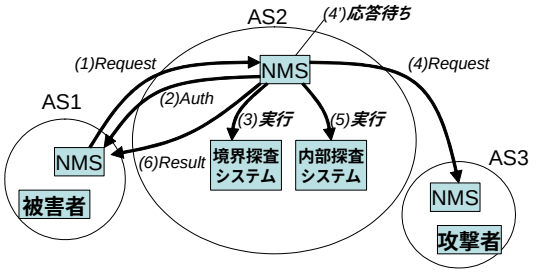

図 5 AS 間発信源探査システムの動作図

以上の動作は、AS 内に攻撃の種類に対応した境界探査システムと内部探査システムが導入されている場合である。境界探査システムしか導入されていない場合、内部探査は実行せず境界探査の結果を Result として返信する。逆に、内部探査システムのみが実行可能である場合は、境界探査の処理を行わない。ただし、内部探査の結果、流入元 AS が見つかった場合には、その AS に(4)の処理同様、Request を送信する。

4. 評価

4.1. プロトタイプシステムの実装

提案するAS間発信源探査システムの動作検証と性能評価を行うため、プロトタイプシステムを実装した。プロトタイプシステムでは、複数パケット探査型AS内トレースバック方式としてUDP方式、単一パケット探査型AS内トレースバック方式としてHash方式を選択した。UDP方式の実装は我々が開発した uTrace を用いた。Hash 方式に関してはBBN Technology 社がフリーソフトとして公開しているSPIEを用いた。また、uTraceには若干の修正を加え、境界探査用uTraceを作成した。

NMSはLinuxマシンとし、RIS, DM, TMなどのモジュールはすべて C++で開発した。また、AS 間発信源探査プロトコルのメッセージ交換には、RIDで提案されている通りSOAPを用いた。

4.2. 性能予測

ある一箇所の攻撃者について、被害者までの攻撃経路上にある AS の数を AS ホップ数と呼び、記号Nで表す。攻撃者と被害者が同一AS内にいる場合はN=１である。また、攻撃経路上のｉ番目のASでの境界探査システムの探査時間を Bi、内部探査システムの探査時間を Ii とする。このとき、攻撃経路上の全てのASで境界探査と内部探査の両方を実行した場合の探査時間は式１になる。

$$I_{n-1}+\Sigma Bi \quad (i=0..n-1) \quad \text{— 式１}$$

DDoS攻撃の場合、AS間発信源探査システムの探査時間は、通常、被害者のいる AS から AS ホップ数が最も遠いASにいる攻撃者が見つかるまでの時間である。被害者に近い場所にいる攻撃者の方が遅く見つかるケースも考えられるが、簡単のためにそうしたケースは考慮しないことにする。このためDDoS攻撃の場合も、探査時間は式１となる。

4.3. テストベッドでの実験

4.3.1. 実験環境

実験に用いたテストベッドは７つのASから構成されており、各AS内ではOSPF、AS間ではBGPを用いて経路情報を交換している。各ASにはNMS１台、BGPルータ３台が存在する。OSPFルータはASによって台数が違い、それぞれの AS に 10～30 台程度存在する。なおNMS、ルータ、サーバ、端末はすべてLinux PCである。また、全てのASにAS内トレースバックとして uTrace と SPIE をインストールし、BGPピア接続しているAS間でNMS同士の接続を行った。

4.3.2. 実験方法

テストベッドで行った実験のうち、ここでは次の２つについて説明する。

(１)ASを直列に並べた場合の探査速度実験
　攻撃者のいる AS から被害者のいる AS までを直列に接続する。AS ホップ数を２から７まで変化させ、探査速度を測定した。

(２)ASをスター型に配置した場合の探査速度実験
　被害者のいるASに、攻撃者のいる複数のASを隣接させる。攻撃者のいるAS数を１、２、３と変化させ、探査速度を測定した。

攻撃は10packet/secのsyn floodである。これは複数パケット攻撃であるため、各NMSではuTraceが選択されて探査が行われる。また、この実験では全てのASにおいて境界探査と内部探査を実行するものとした。また、各々の試験は50回程度繰り返し測定し、実験結果としてその平均値を求めた。

4.3.3. 実験結果

図6、図7に実験結果を示す。予測値は、式１によって求めた値である。式１のパラメータであるBiは、ここでは1.0secondである。この値はuTraceの境界探査が、探査を諦めて結果を返すまでのタイムアウト値である。I_{n-1}はAS内でのuTrace探査時間＋タイムアウト値（1.0second）である。uTrace 探査時間は攻撃パケット送信頻度（単位 packet/sec）の逆数と経路上のルータ数の掛け算で求めることができる。今回の実験では攻撃者のいるASでの攻撃経路上のルータ数が６台で、

攻撃パケット送信頻度は10packet/secであるため、uTrace探査時間は0.6secである。(注：スター型１対１試験だけはルータ数４台である)

実験結果から、ほぼ予測通りの時間で探査が行われていると言える。4. 2節の式１では通信や処理遅延を無視しており、測定値の方がこれらのオーバヘッドの分だけ探査に時間が掛かっている。このオーバヘッドはASホップ数に比例して増加していく傾向にあることも実験結果から確認できる。

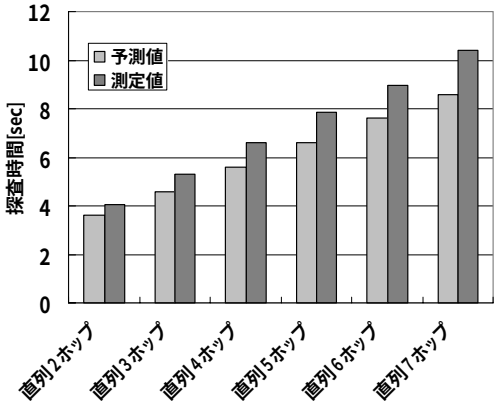

図6 直列試験における探査時間

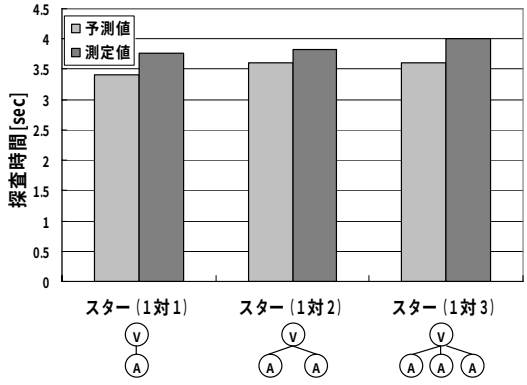

図7 スター型試験における探査時間

5. おわりに

RIDを参考にして、管理単位の異なるAS間でトレースバックを行うためのAS間発信源探査システムを考案し、AS内トレースバックとして我々の提案しているハイブリッド方式と組み合わせた場合の性能試験を行った。その結果、攻撃経路上にあるAS数がそれほど多くない場合には、処理や通信のオーバヘッドが小さく、予想通りの結果が得られることを確認できた。今後は、さらにAS数が多い場合にオーバヘッドがどれだけ大きくなるかを、シミュレーションにより確認する予定である。

(注)本研究は独立行政法人 情報通信研究機構からの委託(H14～H16年度)による。

参考文献

[1] 塚本他”AS間のトレースバックに関する一考察”,電子情報通信学会2004総合大会,Mar.2004

[2] 甲斐他”DDoS攻撃に対する高性能発信源探査方式の提案”, 第27回 コンピュータセキュリティ研究会,情報処理学会研究報告 vol.2004, no.129,2004-CSEC-27, Dec. 2004.

[3] 清水他”大規模ネットワークセキュリティの確保に向けた研究開発”, 情報通信研究機構 平成15年度成果報告書(要約版), http://www2.nict.go.jp/ns/s802/seika/h15/seika/71/7101_matsushita-denko.pdf

[4] Kathleen M. Moriarty, “Real-Time Inter-Network Defense”, InternetDraft: draft-ietf-inch-rid-01.txt, submitted Oct 2004.

[5]大江他,”IPトレースバックシステムの相互接続アーキテクチャの提案”,IEICE-SCIS2005 予稿集 3B4-3, pp.1549-1454, Jan 2005.

[6] Steven M. Bellovin, "ICMP Traceback Message",InternetDraft:draft-bellovin-itrace-00.txt, submitted Mar. 2000.

[7] D. Song and A. Perrig, “Advanced and Authenticated Marking Schemes for IP Traceback,” Proc. IEEE INFO-COM, April 2001.

[8] Snoeren AC, Partridge C, Sanchez LA, Jones CE, Tchakountio F, Kent ST, Strayer T, "Hash-Based IP Traceback", Proc. of the ACM SIGCOMM 2001 Conf. San Diego, Aug 2001.

[9]R. Stone. “CenterTrack: An IP Overlay Network for Tracking DoSFloods." 9th UsenixSecurity Symposium, August 2000.