不正アクセス発信源追跡システムの実装と検証

1G－5

早川 晃弘　馬場 達也　小久保 勝敏　松田 栄之
(株)NTT データ 開発本部
e-mail: {aki, baba, kokubo, matu }@rd.nttdata.co.jp

1. はじめに

筆者らは、インターネットにおける不正アクセスの発信源を追跡し特定するための研究開発を進め、これまでに、基本アーキテクチャを提案し、アーキテクチャに基づく机上シミュレーションの結果を示した[1][2][3]。

本稿では、提案した基本アーキテクチャに基づき開発したプロトタイプシステムの実装内容と、パケット列の違いにより分類選択した不正アクセスを用いて、発信源追跡動作を検証した結果を示す。

2. システムの実装

筆者らは、提案したアーキテクチャの動作を実機で検証するために、プロトタイプシステムを開発した。

提案したアーキテクチャは、追跡動作を管理する追跡マネージャと、追跡対象パケットの転送元上流ノードを特定するトレーサとで構成した[1]。各構成要素が有するべき機能を考慮し、機能構成を検討し各機能を実装した。それぞれの実装機器の構成を表 1 に、機能構成図を、図 1 と図 2 に示す。

2.1. 追跡マネージャの実装

追跡マネージャは、同時に複数の追跡を実現するため、追跡依頼を受信する追跡依頼受信機能と、制御を行う追跡制御機能の二つの機能によって構成した。

追跡依頼受信機能は、追跡依頼を受信すると、追跡制御機能を新しいプロセスとして生成することとした。

生成された追跡制御機能は、トレーサ等の応答から上流ノードの IP アドレスと種別を取得し、種別に従って追跡動作を制御することとした。追跡が完了したら、追跡結果を不正アクセスセンサに送信することとした。

2.2. トレーサの実装

トレーサは、パケットフィーチャを蓄積するパケット変換蓄積機能と、蓄積された情報を用いて追跡対象パケットを転送してきた上流ノードを特定する追跡検索機能の二つの機能を有する。

パケット変換蓄積機能では、ノードを通過するパケットから追跡に必要なパケットフィーチャと転送元のデータリンク層識別子(発信元 MAC アドレス等)、及び通過時間を 1 レコードとし、時系列順にリングバッファに蓄積することとした。

追跡検索機能については、パケット検索機能と上流インタフェース決定機能の二つに分けて検討した。

パケット検索機能では、蓄積エリアから対象パケットのパケットフィーチャを検索する。パケットフィーチャは、時系列に規則正しく蓄積されているため、新しいものから古いものへと順に線形逐次検索を行うこととした。

上流インタフェース決定機能では、データリンク層識別子と各情報を対応させた静的なテーブル(トレーステーブル)を用いて、合致したレコードのデータリンク層識別子から、上流ノードの IP アドレスと、追跡マネージャの追跡制御機能に必要な上流ノードの種別と所属 AMN の情報を求めることとした。

表 1 実装機器の構成

構成機器	構成
追跡マネージャ	Sun Enterprise 250 CPU: UltraSPARC-II 400MHz メモリ: 512MBytes OS: Solaris 2.7
トレーサ	川崎製鉄 A2DIS SV-1000 CPU: MC68360 25MHz メモリ: 16MBytes OS: 独自 OS

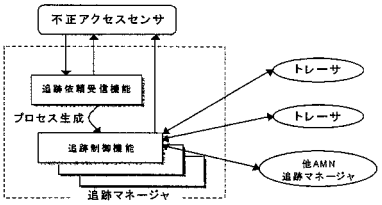

図 1 追跡マネージャの機能構成図

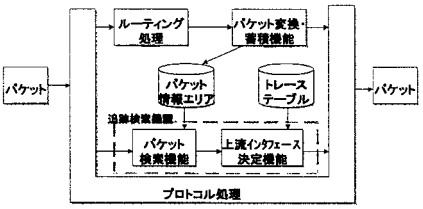

図 2 トレーサの機能構成図

3. 追跡動作の検証

実装した機器を用いて、実際に不正アクセスが追跡できるか検証した。分類した不正アクセスから選択する代表例を実際に発生させ追跡の成否を検証し、結果から不正アクセス全体に対するの追跡の成否を考察した。

Implementation and verification of unauthorized access tracing system
Akihiro HAYAKAWA,Tatsuya BABA,
Katsutoshi KOKUBO, Shigeyuki MATSUDA,
†Department of Information Technology,
NTT DATA CORPORATION

3.1. 検証に用いる不正アクセスの分類

本システムは、蓄積したパケットフィーチャと追跡対象のパケットフィーチャを単純に比較し、合致した情報から上流ノードを決定し追跡を実行する[2]。すなわち、本システムでは、不正アクセスのパケット内容によって追跡動作が左右されないため、不正アクセスも通常のパケット列とみなすことが可能である。

そこで、不正アクセスをパケット列の種別によって分類し、各分類の代表例を検証用のデータとして用いることで、全体の不正アクセスに対する追跡動作について考察できると考えた。以下に、パケット列の種別をまとめる。

(分類 1) 1 パケットによる不正アクセス
一個の不正パケットを送信することで成立する不正アクセス。ヘッダのフィールドに不正な値を設定した不正アクセス等が該当する。

(分類 2) 複数パケットによる不正アクセス
一連の複数の不正パケットを送信することで成立する不正なアクセス。複数パケットにわたる巨大なサイズのデータを送信し、バッファーオーバーフローを意図した不正アクセス等が該当する。

(分類 3) Flood 系の不正アクセス
一箇所から短時間で大量のパケットを送信することで成立する不正アクセス。

(分類 4) DDoS 系の不正アクセス
複数個所から一箇所に対して送信する Flood 系の不正アクセス。

3.2. 追跡動作の検証

検証を行う実験ネットワークの構成を図 3 に示す。検証に利用する不正アクセスは、3.1 節の分類に基づき決定した。一覧を、表 2 に示す。

発信源端末からターゲットに対して、各不正アクセスを発生させ、発信源の真の IP アドレスが求められるかどうかを確認した。DDoS 系の不正アクセスを行う場合は、複数の発信源端末から同時に不正アクセスパケットを発生させた。検証結果を、表 3 に示す。

3.3. 考察

検証結果から、選択した不正アクセスに対して発信源を追跡可能であることが判明した。

検証に用いなかった不正アクセスで、分類 1、分類 2、分類 3 の各分類に属するものは、検証に用いたそれぞれの不正アクセスと比較しても、パケットフィーチャの内容が異なるだけであり、追跡動作への影響がないため、同様の追跡動作が期待できる。従って、分類 1、分類 2、分類 3 の各分類に属する不正アクセスは、検証結果と同様に追跡可能であると考えられる。

ただし、複数の発信源からの不正アクセスである分類 4 に属する不正アクセスに対しては、一つの発信源を特定することには成功したが、全ての発信源を特定することはできなかった。トレーサ内の検索処理で、複数箇所から追跡対象パケットが転送されていて、複数の合致レコードがある場合でも、合致レコードは一つであるとして処理することが原因である。結果として、転送元の一箇所を選択して追跡を継続するため、全ての発信源を特定することができない。同時に複数経路を追跡する仕組みを、今後の検討課題とする。

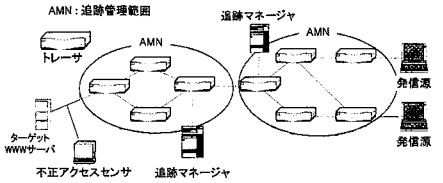

図 3 実験ネットワーク

表 2 検証に利用した不正アクセス

不正アクセス手法	利用不正アクセス
1 パケットによる不正アクセス	Land アタック
複数パケットによる不正アクセス	Long URL クラッシュ
Flood 系の不正アクセス	ping Flood
DDoS 系の不正アクセス	DDoS(分散 SYN Flood)

表 3 検証結果

手法	不正アクセス	結果
1 パケット	Land アタック	成功
複数パケット	Long URL クラッシュ	成功
Flood 系	ping Flood	成功
DDoS 系	分散 SYN Flood	一部成功

4. まとめ

本稿では、提案した基本アーキテクチャに基づき開発したプロトタイプシステムの実装内容を示すとともに、追跡動作を踏まえ、パケット列の違いにより分類選択した代表的な不正アクセスを用いて、発信源特定動作を検証した結果を示した。検証の結果、提案した基本アーキテクチャを実装した実機を用いて、不正アクセスの発信源の特定が可能であることが確かめられた。

今後は、適用するネットワーク構成と、本アーキテクチャの構成要素の機器に必要なリソースとの関係を明らかにし、追跡成功のための条件を考察する。

謝辞

本研究は、通信・放送機構（TAO）の委託研究テーマ「不正アクセス発信源追跡技術に関する研究開発」の一環として行われているものである。

参考文献

[1] 竹爪他：不正アクセス発信源追跡アーキテクチャの一検討,情処 60 全大,pp287-288,Mar.2000.

[2] 渡辺他：不正アクセス発信源追跡のためのパケット識別情報の検討、情処 60 全大，pp289-290, Mar.2000

[3] 池田他：不正アクセス発信源追跡システムのアーキテクチャの有効性検証、情処 62 全大，pp285-286, Mar.2001