1S-02 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

池田 基† 田中 俊介‡ 早川 晃弘‡ 松田 栄之‡
(株)NTTデータ †公共地域ビジネス事業本部 ‡開発本部
e-mail: †ikedamtk@nttdata.co.jp, ‡{ shun, aki, matu }@rd.nttdata.co.jp

1. はじめに

近年インターネットが社会に浸透し、さまざまな分野で利用されている。それに伴い、ネットワーク経由の不正アクセスも急増しており、対策として発信源を特定する技術が注目されている[1]。そこで、筆者らはパケットの送信元IPアドレスの偽造に左右されない、不正アクセス発信源を追跡するアーキテクチャを提案した[2]。

筆者らが提案したアーキテクチャ(以下、本アーキテクチャ)は、発信源と不正アクセスセンサ間の中継装置の数(以下、ホップ数)に比例して追跡時間が増加する。一方、中継装置に蓄積し続けるパケット識別情報(以下、パケットフィーチャ)[3]を利用するため、追跡時間の増加によって発信源を特定できなくなる。

本稿では、ホップ数から追跡時間を求める計算式を導出し、机上において追跡可能なホップ数を求めることで、インターネットで想定されるホップ数であっても本アーキテクチャによって発信源を追跡できることを示す。

2. 発信源追跡アーキテクチャ

ここでは、本アーキテクチャの基本事項を述べる[2]。

2.1. 構成要素

表 1に本アーキテクチャの構成要素を挙げる。

表 1 構成機器一覧

名称	説明
不正アクセスセンサ	・不正アクセスを検知し、追跡マネージャに追跡を依頼する。
トレーサ	・搭載メモリの一部(以下、パケットバッファ)にパケットフィーチャを蓄積する。 ・パケットバッファを検索し、転送元を特定する。
追跡マネージャ	・発信源が特定されるまで、次々とトレーサにパケット転送元を問合せる。 ・管理範囲(AMN)を超えた場合、他AMNのマネージャに追跡継続を依頼する。

2.2. 処理手順

図 1に、本アーキテクチャにおける追跡動作の処理手順を示す。

追跡依頼を受けた追跡マネージャは、トレーサに追跡指示を出す。トレーサでは、蓄積したパケットバッファから追跡対象のパケットフィーチャを検索し、一つ前の転送元であるトレーサを特定する。この動作を発信源を特定するまで繰返すことにより発信源追跡を実現する。

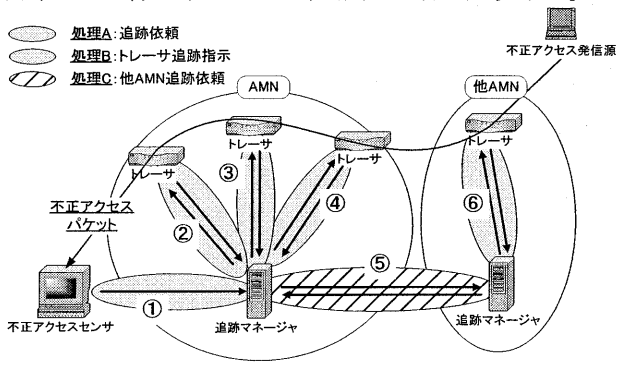

図 1 追跡システム処理手順

2.3. 追跡成功の条件

トレーサでは、搭載しているメモリが有限であることから、継続してパケットフィーチャを記録するために、古いパケットフィーチャに新しいパケットフィーチャを上書きする必要がある。従って、追跡に時間がかかると、経路途中のトレーサにおいて追跡対象のパケットフィーチャの記録が失われ、発信源を特定できなくなる。つまり、記録が失われるまでの時間内に追跡が完了することが追跡可能な条件である。

不正アクセスセンサで検知した時刻を起点として、発信源を特定するまでの時間を追跡時間(以下、T)、経路途中のトレーサから追跡対象のパケットフィーチャの記録が失われるまでの時間を追跡可能時間(以下、t)としたとき、T< tが成り立つ場合に追跡が成功するといえる。

3. 追跡時間の計算式

ここでは、Tを求める計算式を導出する。

図 1から、処理A,B,Cにかかる時間をそれぞれT_A、T_B、T_C、ホップ数をN_H、他AMNの数をN_Aとすると、Tは式(1)で求められる。

$$T = T_A + T_B \times N_H + T_C \times N_A \quad (1)$$

AMN内のメッセージ伝送時間をT_{IN}、他AMNのマネージャとのメッセージ伝送時間をT_{OUT}、追跡マネージャ内の処理時間をT_M、トレーサ内処理時間をT_Tとし、

A study of architecture for unauthorized access tracing system
Motoki IKEDA†, Shunsuke TANAKA‡,
Akihiro HAYAKAWA‡, Shigeyuki MATSUDA‡,
†Public Administration Community Business Sector,
‡Department of Information Technology,
NTT DATA CORPORATION

T_A、T_B、T_C を展開すると、式(2)となる。

$$T_A=T_{IN}+T_M,\ T_B=(2T_{IN}+T_M+T_T),\ T_C=2(T_{OUT}+T_M) \quad (2)$$

処理 B に含まれるトレーサ内の処理の大部分は、パケットフィーチャの検索時間である。検索時間の最大値は、比較件数の最大値と比較処理時間の積である。

比較件数の最大値は、パケットバッファのサイズと記録するパケットフィーチャのサイズによって求めることができる。従って、パケットバッファのサイズを M、記録するパケットフィーチャのサイズを S_F、1 件あたりの比較処理時間を T_Sとすると、T_Tは、式(3)によって求められる。

$$T_T=\frac{M}{S_F}\times T_S \quad (3)$$

式(1)、(2)、(3)により、T は、式(4)により求められる。

$$T=(T_{IN}+T_M)+(2T_{IN}+T_M+\frac{M}{S_F}T_S)N_H+2(T_{OUT}+T_M)N_A \quad (4)$$

4. 追跡可能時間の計算式

次に、t を求める計算式を導出する。

トレーサ上で記録されたパケットフィーチャが上書きされるまでの時間(T_L) は、パケットバッファのサイズと記録速度によって求められる。従って、トレーサを通過するトラフィック流量を W、ネットワーク上の平均パケットサイズを S_Pとすると、T_Lは、式(4)によって求められる。

$$T_L=\frac{M}{\frac{W}{S_P}\times S_F} \quad (5)$$

不正アクセスパケットがトレーサを通過してから、不正アクセスセンサへ到達するまでの時間遅延を考慮すると、1 ホップあたりのパケット転送時間を δ とするとき、t は、式(6)によって求められる。

$$t=T_L-\delta\times N_H \quad (6)$$

5. アーキテクチャの有効性検証

5.1. 検証のための条件設定

各処理の時間を、インターネットを想定し、表 2の値に定めた。

表 2 計算に用いる定数および変数の値

要素名	説明	定数	値
N_H	発信源までのホップ数	—	1→100 ホップ
N_A	発信源まで経由している他 AMN 数	—	10 ホップあたり 1AMN
T_{IN}	AMN 内メッセージ伝送遅延時間	定数	10msec
T_{OUT}	他 AMN との伝送遅延時間	定数	100msec
T_M	追跡マネージャ内処理時間	定数	1msec
M	パケットバッファのサイズ	—	8、16、32MBytes
S_F	パケットフィーチャのサイズ	定数	100bytes
T_S	1 件あたりの比較処理時間	定数	1 μ sec
W	トレーサにおけるトラフィック流量	定数	100Mbps
S_P	平均パケットサイズ	定数	1000bytes
δ	1 ホップあたりの伝送遅延	定数	1msec

5.2. 検証結果

5.1で定めた値と、式(4)、(6)を用いて T と t を算出した結果をグラフ化し図 2に示す。

図 2から、パケットバッファのサイズが 8Mbytes の場合、52ホップ、32Mbytes に拡張すると、70ホップの追跡が可能であることがわかる。筆者らの独自の調査によると、実際のインターネットにおけるホップ数は、平均 20 ホップ程度であり、最大でも 40 ホップ程度であった。以上の考察から、本アーキテクチャは、インターネットにおいても十分追跡可能であるといえる。

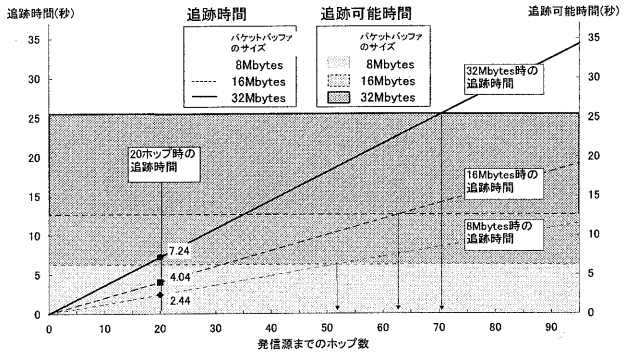

図 2 追跡時間と追跡可能時間との関係

また、発信源までのホップ数が 20 ホップだった場合の追跡時間は 2.5 秒以内(パケットバッファのサイズが 8Mbytes の場合)であり、リアルタイムな追跡が十分可能であるといえる。

6. まとめ

本アーキテクチャは、ホップ数に比例して追跡時間が増加するが、追跡時間がかかり過ぎた場合に発信源を特定できない。そこで、本アーキテクチャにおける追跡時間、追跡可能時間を算出する式、追跡の成否の判定式を導出し、筆者らが想定するインターネットにおいて追跡可能なホップ数を求めた。その結果、インターネットにおいても十分に追跡が可能であることが判明した。

今後は、プロトタイプを用いて実際の追跡時間を測定し、本アーキテクチャの評価を行う予定である。

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] 太田他:インターネットにおける不正アクセス検出技術, 信学論(B), vol.J83-B, No.9, pp.1209-1216, Sep.2000

[2] 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,6Q-6,Mar.2000.

[3] 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, 6Q-7, Mar.2000