不正アクセス発信源追跡システムにおける追跡時間の評価

3H－06

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、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基本アーキテクチャを提案し、プロトタイプシステムを開発した。また、基本機能を検証し結果を示した[1][2]。

本稿では、開発したプロトタイプを用いて測定した各処理時間をもとに、発信源特定までの時間を算出する。さらに追跡成功の条件から推察される制限事項を考察し対策を提案する。

2. 追跡時間の算出式と追跡成功条件

2.1. 追跡時間

提案方式では、不正アクセスを検知した不正アクセスセンサが、追跡マネージャに追跡を依頼し、依頼を受けた追跡マネージャは、不正アクセスパケットの通過した経路上のトレーサを逆順にたどり、発信源を特定する。

不正アクセスセンサで検知した時刻を起点とし、発信源を特定するまでにかかる時間を追跡時間とする。追跡時間は、トレーサへの問い合わせ回数、すなわち不正アクセスが通過したトレーサの数(ホップ数)に比例し増加する。

2.2. 追跡時間の算出式

筆者らは、同一機器間のメッセージ遅延時間や同一機器の処理時間は一定であるという条件の下で追跡時間を求める計算式を示した[3]。より精度の高い追跡時間の計算を行うため、プロトタイプ開発の設計を踏まえ、図 1のように処理をより細分化し、算出式の見直しを行った。各式の n はホップ数、m は経由した AMN の数である。

(a) AMN 内の場合

$$T(n) = T_1 + T_2 + \sum_{i=1}^{n-1}(T_3 + T_4 + T_5 + T_6) + T_3 + T_4 \qquad \text{(式 1)}$$

(b) 二つ以上の AMN を通過した場合

$$T(n,m) = T_1 + T_2 + \sum_{i=1}^{n-1}(T_3 + T_4 + T_5 + T_6) + \sum_{j=1}^{m-2}\{T_7 + T_8 + T_9 + T_{10}\} + T_7 + T_8 + T_3 + T_4 \qquad \text{(式 2)}$$

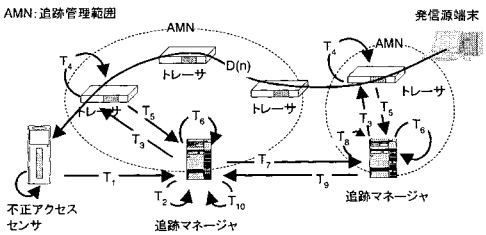

図1 追跡の基本動作

2.3. 追跡成功条件

プロトタイプでは、通過するパケットに必要なパケットフィーチャを時系列順にリングバッファに蓄積する[2]。そのため、追跡に時間がかかると記録が失われ、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成功の条件である。

単位時間あたりの通過パケット数(トラフィック量)を P(パケット/秒)、リングバッファに記録可能なレコード数を R とした場合、記録が失われるまでの時間は、R/P 秒となる。あるネットワークの最大ホップ数が n である場合、パケットが到着するまでの遅延時間を D(n)、不正アクセスセンサにて検知する時間を C とするとき、以下の不等式が成立することが必要である。

$$\frac{R}{P} > T(n) + D(n) + C \qquad \text{(式 3)}$$

3. プロトタイプによる測定

3.1. 各処理時間の測定

式 1 から式 3 の計算に必要な T_1 から T_{10} および D(n)と C について、プロトタイプを用いて測定した。表 1に測定した時間の一覧を示す。

トレーサ内処理(T_4)は、パケットバッファ内の全レコードと照合処理をするため、T_4 はレコード数 R に比例して増加する[2][3]。そこで、記録可能なレコード数を変化させて T_4 を測定し、1 レコードあたりの処理時間を係数とした計算式を求めた。

追跡指示送信処理(T_3)は、実装ルータにおけるタスクスイッチのタイミングがランダムであるため、処理の度に±0.1 秒の差が生じる。このことを踏まえ、表 1の値を式 1 および式 2 に代入すると、以下のような式が求まる。

(a) AMN 内の場合

$$T(n) = (13.32\times10^{-6}R + 0.13824 \pm 0.1)n + 0.02002 \qquad \text{(式 4)}$$

(b) 二つ以上の AMN を通過した場合

$$T(n,m) = (13.32\times10^{-6}R + 0.13824 \pm 0.1)n + 0.06272m - 0.05282 \quad \text{ただし}(n \geq m \geq 2) \qquad \text{(式 5)}$$

表1 各処理の処理時間

時間	時間(秒)	時間	時間(秒)
T_1	0.01555	T_7	0.04226
T_2	0.01034	T_8	0.01034
T_3	0.12376±0.1	T_9	0.00851
T_4	(13.32×10^{-6})R+0.00861	T_{10}	0.00161
T_5	0.00426	C	0.02995
T_6	0.00161	D(n)	0.00087n

3.2. 追跡時間のシミュレーションによる予測値と測定値

式 4 および式 5 を用いて、各レコード数およびホップ数において予測される追跡時間と実際に測定した追跡時間を表 2に示す。プロトタイプでは、1 レコードのサイズを 100 バイトとしたため、トレーサに搭載するメモリ量は、レコード数×100 バイトで計算される。結果から、式 4 および式 5 を利用して追跡時間を予測できることが判明した。

表2 追跡時間の予測値と測定値

n	m	レコード数	必要メモリ	予測値(秒)	測定値(秒)
5	1	10000	1Mbytes	1.37722 ±0.5	1.16406
		80000	8Mbytes	6.03922 ±0.5	5.98925
9	1	10000	1Mbytes	2.46298 ±0.9	2.22123
		80000	8Mbytes	10.85458 ±0.9	10.72546
9	2	10000	1Mbytes	2.51558 ±0.9	2.49442
		80000	8Mbytes	10.90718 ±0.9	11.08235

Evaluation of tracing time on unauthorized access tracing system
Akihiro HAYAKAWA,Tatsuya BABA,
Katsutoshi KOKUBO, Shigeyuki MATSUDA,
Research and Development Headquarters,
NTT DATA CORPORATION

3.3. 追跡成功の条件式

式 3 に表 1 の結果を代入すると、式 6 と式 7 の不等式が求まる。式 6 は、パケット数とホップ数の関係式であり、追跡が成功するためのネットワークの条件を定める。式 7 は、適用したネットワークに必要な最小限のレコード数を定める。

$$1-13.32\times10^{-6}Pn>0 \qquad (式6)$$

$$R>\frac{P}{(1-13.32\times10^{-6}Pn)}\{(0.13911\pm0.1)n+0.04997\} \quad (式7)$$

3.4. 想定ネットワークにおける追跡時間のシミュレーション

プロトタイプのインタフェースは、10Mbps の Ethernet である。そこで、最大 20 ホップの Ethernet で構成されたネットワークを考え、必要なメモリ量と追跡時間についてシミュレーションした。Ethernet 上のパケットサイズは可変長であるため、想定ネットワークにおけるトラフィック量を 2500pps と設定し計算した。

想定した条件は、式 6 の不等式を満たすことから、プロトタイプの適用が可能である。式 7 の最悪ケースを計算すると、20 ホップの追跡に必要なレコード数は、36,1697 レコード以上であると求まり、トレーサに必要なメモリ量は約 3.7M バイトとなる。この条件下では、20 ホップ先まで追跡する追跡時間は、約 14.4 秒となる。ホップ数による追跡時間の変化を図 2に示す。

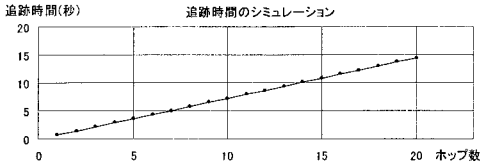

図2 プロトタイプを用いた場合の追跡時間

4. 考察

4.1. プロトタイプにおける制限事項

式 6 の条件は、トレーサに搭載するメモリを増やしてレコード数を非常に多く搭載しても、追跡可能なネットワーク条件が制限されることを示している。式 6 が成立する P と n の組合せ範囲を図 3に示す。図 3 から、トラフィック量が 7500pps の回線で構成されるネットワークの場合は、10 ホップまでしか追跡できない。この要因の一つとして、プロトタイプとして実装した装置の処理性能の低さがあげられる。装置の 1 レコードの検索に要する処理性能を α (秒/レコード)とした場合、式 6 が以下のように変更される。

$$1-\alpha Pn>0 \qquad (式8)$$

式 8 は、α がより小さくなることで、P および n の条件が緩和されることを示している。

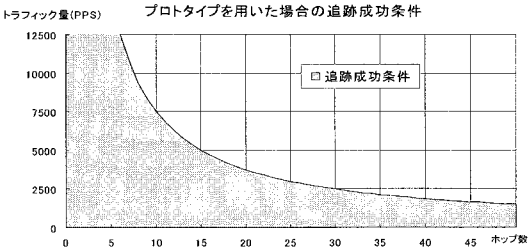

図3 プロトタイプを用いた場合の適用範囲

4.2. CPU の高速化による成功条件の緩和

プロトタイプシステムのトレーサに搭載されている CPU(MC68360 25MHz)よりも処理性能の高いマシンを用いてトレーサと同様の検索処理のシミュレーションを行い、処理性能の向上によって適用可能なネットワーク条件がどのように緩和されるか検討した。

Pentium4(2GHz)を CPU に持つマシンでシミュレーションしてみた結果、$T_4=(0.07\times10^{-6})R+0.00053$ となった。この値を利用すると、追跡成功の条件式は、式 9 と式 10 の不等式となる。式 9 が成立する P と n の組合せ範囲を図 5 に示す。

$$1-0.07\times10^{-6}Pn>0 \qquad (式9)$$

$$R>\frac{P}{(1-0.07\times10^{-6}Pn)}\{(0.13103\pm0.1)n+0.04997\} \quad (式10)$$

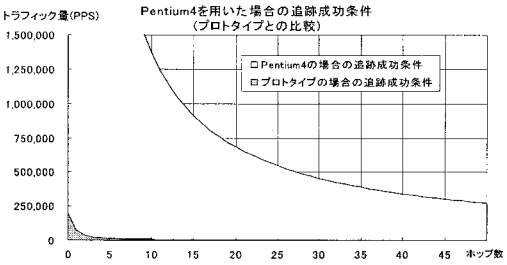

図 4 処理性能を向上させた場合の適用範囲

結果から、CPU の性能を向上させることにより、トラフィック量 250,000pps である回線で構成されたネットワークであっても、40 ホップ以上の追跡が可能であることがわかる。

式 10 から 40 ホップの追跡に必要なレコード数は 7,742,642 レコード以上であると求まり、トレーサに必要なメモリ量は約 775M バイトとなる。この条件下では、40 ホップ先まで追跡する追跡時間は、約 32.9 秒となる。

5. まとめ

プロトタイプを用いて、9 ホップ先の発信源を特定するまで、レコード数を 80,000 レコードとした場合、約 11 秒で完了した。また、トラフィック量が 2500pps であるネットワークに対して、3.7M バイトのメモリを搭載したプロトタイプを用いて、20 ホップ先の発信源を特定するまで、約 14.4 秒で追跡が完了することが予想されることを示した。

一方、プロトタイプの処理性能では、トラフィック量の多いネットワークへの対応には限界があることが判明した。そこで、処理性能の高いプロセッサを用いた場合の処理時間をシミュレーションし、トラフィック量がプロトタイプで想定した 100 倍の 250,000pps であるネットワークに対しても 40 ホップ以上の追跡が可能であることを示し、適用可能なネットワーク条件を大幅に緩和できる結果を示した。

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,松田,渡辺,栁田,小久保: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,pp287-289, Mar.2000

[2] 早川,馬場,小久保,松田: 不正アクセス発信源追跡システムの実装と検証,情処 63 全大,pp491-492,Sep.2001

[3] 池田,田中,早川,松田: 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