NP のトレースバックシステムへの応用

田中貴志　星野浩志　新美誠　清水孝祥　山下邦夫†

†横河電機株式会社
〒180-8750 東京都武蔵野市中町 2-9-32

E-mail: †{Takashi.Tanaka,Hiroshi.Hoshino,Makoto.Niimi}@jp.yokogawa.com
{Takayoshi.Shimizu,Kunio.Yamashita}@jp.yokogawa.com

あらまし トレースバック手法の一つであるハッシュベースのトレースバックでは、経路中でパケット毎にハッシュ値を演算・記録し、問合せパケットに対応したハッシュ値が記録されているかどうかを検索することによりトレースを行う。本稿では、Intel のネットワークプロセッサ (NP) IXP1200 シリーズを利用することにより GbE クラスのネットワークへの対応を可能にした、ハッシュベーストレースバックシステムの実装について述べるとともに、その評価結果と課題をまとめる。

キーワード Network Processor, IP traceback, Hash, IXP1200

A Network Processor Application for Traceback Systems

Takashi TANAKA,　Hiroshi HOSHINO,　Makoto NIIMI
Takayoshi SHIMIZU, Kunio YAMASHITA†

†Yokogawa Electric Corporation
2-9-32 Nakacho, Musashino-shi, Tokyo, 180-8750 Japan

E-mail: †{Takashi.Tanaka,Hiroshi.Hoshino,Makoto.Niimi}@jp.yokogawa.com
{Takayoshi.Shimizu,Kunio.Yamashita}@jp.yokogawa.com

Abstract Hash-based traceback, one of packet traceback methods, traces IP packets by calculating the hash for each traversing packet, recording the hash in its database and searching the database for the queried packet's hash. Network processor is a good choice to realize these functions in high traffic networks. We implemented a hash-based traceback system on Intel's network processor IXP1240. This paper describes the implementation of the system which can be applied to GbE class networks, its evaluation results and its problems.

Keywords Network Processor, IP traceback, Hash, IXP1200

1. はじめに

不正なパケットを大量に送りつけてサービスを妨害する DoS (Denial of Service) 攻撃や、複数地点から DoS 攻撃を行う DDoS (Distributed DoS) 攻撃が、社会的な問題となっている。DoS 攻撃への対処の方法として、DoS 攻撃パケットの送信元になるべく近いところで、フィルタなどの手段により DoS 攻撃パケットを制限することがあげられる。しかし、攻撃パケットの送信元 IP address が偽装されている場合もあり、真の送信元の調査は手間のかかる作業である。この問題を解決するための手法は、総称して「IP Traceback」手法と呼ばれており、ダイジェスト方式やマーキング方式など様々な方式が提案されている。

一方、対象となるネットワークは高速化が進んでおり、流れるパケット全てをソフトウェアのみで処理することが難しくなっている。しかし高速化のために ASIC などを用いたハードウェア主体の実装は、その開発費用・期間・人材面で制約が大きく、まだ仕様が確立されていないトレースバックのようなアプリケーションに適用することは難しい。そのような状況の中、ハードウェア実装に近い高速性と、ソフトウェア処理による柔軟性を併せ持ったネットワークプロセッサ(NP) が注目されている。

我々は、高速ネットワークに対応可能なダイジェスト方式のトレースバックシステムを、NP を用いて実装した。本稿では、そのトレースバックシステムの実装および評価結果と課題について報告する。

2. Traceback System

2.1 システムの構成

我々が作成したトレースバックシステムは、図 1 に示すように Footmarker、Manager、Gate の 3 つの構成要素からなる。

Footmarker は各観測点に設置され、そこを通過するパケットのダイジェスト（ハッシュ）を計算し記録する。

Manager は Footmarker の管理を行うと共に、Gate からの検索要求を受け付けて、Footmarker に問合せを行い回答する。

Gate は本システムと他システムとのゲートウェイの役割を担う。Intrusion Detection System (IDS) やパケットダンプツールなどから得た攻撃パケットを入力とし、Manager に問合せを行う。

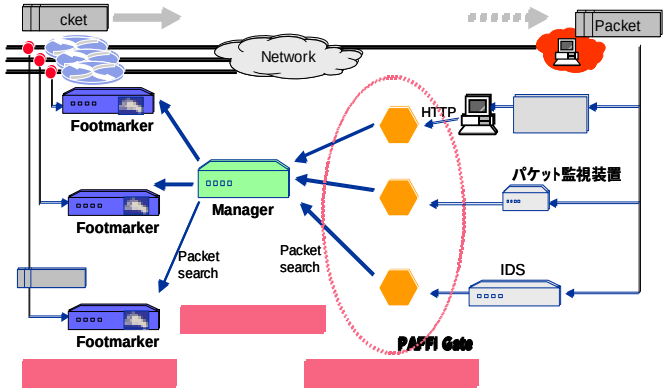

図 1: Traceback System の構成

3. Footmarker の設計

3.1 Footmarker の概要

Footmarker では、接続するネットワークに流れる全てのパケットのハッシュ値を算出するため、その流量に対応した高速なパケット処理が必要とされる。我々は、この処理のため、ネットワークプロセッサを利用したネットワークボードを作成した。本研究で採用したネットワークプロセッサは、Intel 社の IXP1240 であり、その内部はパケット処理用 RISC プロセッサである 6 つのマイクロエンジンと、これらを管理制御するプロセッサである StrongARM コアから構成されている。

Footmarker のブロック図（ハードウェア）を図 2 に示す。Gigabit Ethernet (GbE)のネットワークに対応するため 1000Base-SX の観測用インタフェースを 2 ポート実装した。パケットの処理は IXP1240（マイクロエンジン、StrongARM コア）上のソフトウェア（ファームウェア）で実現している。

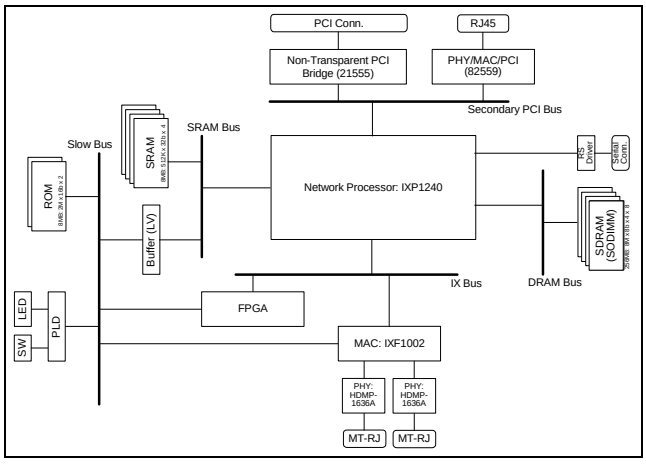

図 2: Footmarker のハードウェアブロック図

表 1 : GbE 対応 Footmarker のハードウェア仕様

Network Processor	Intel IXP1240 (232MHz)
Onboard Memory	* SDRAM: 256Mbytes * SRAM: 8Mbytes * Flash ROM: 8Mbytes
Network I/F	1000Base-SX x 2, 10/100Base-TX x 1
Console	Serial I/F
Card Form	Full-size PCI
Power Dissipation	20W (estimated)
Optional Feature	200,000 gate FPGA on I/O bus

3.2 Footmarker の構成

Footmarker のソフトウェアは、以下の 3 つのモジュールから構成される（図 3 参照)。

(1) Packet Search Engine

PAFFI Manager からのパケット検索問合わせを受け付け、それに返答する。検索パケットのハッシュ値を算出し、パケット通過記録への問合わせを行う。

(2) Footmark Table Handler

パケット通過記録 (Footmark) とそのアクセス手段を提供する。通過記録は複数の Digest table により構成される。

(3) Footmark Engine

ネットワーク上を流れるパケットのハッシュ値を順次算出し、パケット通過記録として保存する。

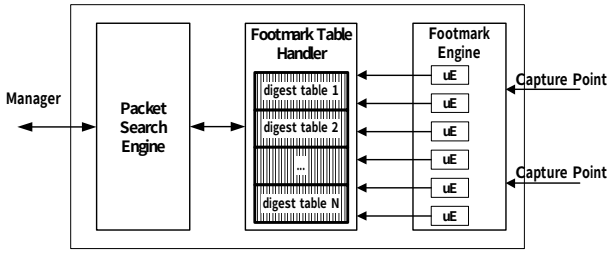

図 3: Footmarker のモジュール構成

3.3 Footmark Engine とネットワークプロセッサ

Footmarker の構成の中で、処理速度が要求されるのは、Footmark Engine の部分である。この処理を IXP1240 上のマイクロエンジン部で行っている。具体的な内容は、パケットの受信、ハッシュ値の算出、テーブルへの記録である。

ハッシュ値の算出には、IXP に内蔵されている 64bit ハッシュ演算ユニットを利用し、テーブルへのマークは、SRAM 制御ユニット中のビットマーク機能を利用することで、ネットワークプロセッサの持つハードウェアアシストを活用している。

4. 評価

4.1 キャプチャ性能の測定条件と方法

測定対象と負荷発生装置を図 4 のように接続する。負荷発生装置（Flame Thrower）で特定の長さ (順次変更) のパケットを繰り返し生成し、測定対象に送信してその処理能力を測定する。

比較対照として GbE の NIC を取り付けた汎用 PC を用意し、併せて測定を行った。

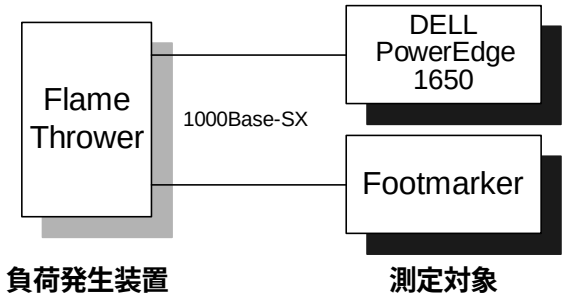

図 4: 測定環境

表 2: 比較対照 PC の仕様概略

Model	DELL Power Edge 1650
Processor	Intel Pentium III (1.13Hz)
Memory	SDRAM: 1.0Gbytes Primary Cache : 512Kbytes
Network I/F	Intel Pro-1000F
OS	FreeBSD 4.7

4.2 GbE 対応 Footmarker のキャプチャ性能測定結果

Footmarker に通常の動作を行わせ、3 種類のパケットを流して測定した結果を図 5 に示す。

最小パケット (64bytes) から最大パケット (1518bytes) まで全域に渡り理論値に近い性能を出していることが分る。

4.3 PC＋汎用 OS のキャプチャ性能測定結果

汎用 PC 上で動く Footmarker プログラムは現時点では存在しないので、PC での測定に当っては一般的に用いられているパケットキャプチャソフトウェア”tcpdump”を使用した。

Footmarker の動作に近づけるため、TCP だけを選択するフィルタオプションを指定して測定を行った。結果を図 5 に重ねて示す。

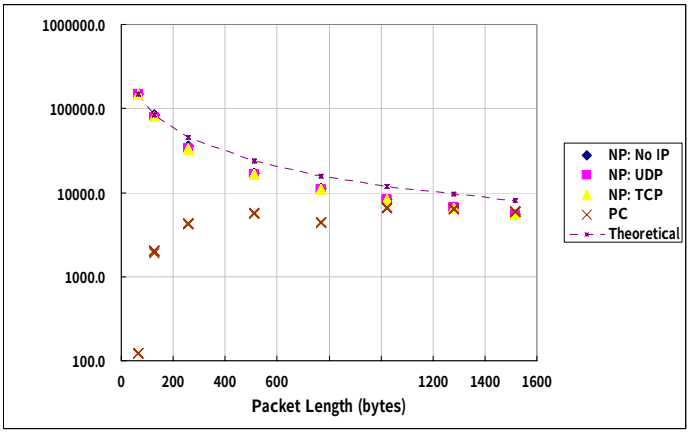

図 5: 測定結果

5. 考察

ネットワーク機器の性能を考える上では、単純な流量 (bps, bits per second) ではなく、毎秒の処理パケット数 (pps, packets per second) が重要な指標となる。パケット単位で特徴情報を記録する Footmarker においてもそれは同様である。

測定結果のグラフ（図 5）からは、以下のようなことが分る。

- パケット長が大きい場合には、NP ベースの実装も汎用 PC も理論限界値に近いパケット処理能力を持っている。
- しかし、パケット長が小さい場合には、汎用 PC の処理能力は急激に悪化する。パケット毎に上がる割込みの負荷が重いためと考えられる。
- それに対して、NP ベースの実装ではパケット長が小さい場合にも理論限界値に近い処理能力を発揮している。

なお、Footmarker ではキャプチャだけではなくパケットの特徴情報を得るためにハッシュ値の生成などの処理まで行っているのに対し、今回測定した PC では tcpdump のフィルタリングまでしか行っていない。同じ処理を行わせた場合には、処理性能差は今回の結果よりもさらに開くことが予想される。

また、現時点での Footmarker のプログラムは改善の余地を多く残している。NP のマイクロエンジン部はその並列性を活かすプログラムの最適化によって性能が大きく向上するので、今後のチューニングによってさらに高い性能を示すことも期待できる。

実ネットワークでは、100%のビットレートのトラフィックが流れ続けることはまずないので、今回の NP ベース Footmarker 程度の処理性能があれば GbE ネットワーク環境においても実用上問題のない IP Traceback システムが構築できる見込みが得られた。

6. まとめ

ハッシュベースのトレースバックシステムをネットワークプロセッサ上で実装し、評価を行った結果、PC に比べよいパフォーマンスを得られた。

今後、プログラムの最適化をさらに進め、このようなアプリケーションへのネットワークプロセッサの適用についてより詳細な評価を行う予定である。

文　献

[1] Alex C. Snoeren, Craig Partridge, Luis A. Sanchez, Christine E. Jones, Fabrice Tchakountio, Stephen T. Kent, and W. Timothy Strayer, “Hash-Based IP Traceback”, Proc. SIGCOMM 2001.

[2] Intel Corporation. IXP1200 Software Development Kit, v2.01, http://developer.intel.com/design/network/products/npfamily.

[3] Intel Corporation, “Intel IXP1200 Network Processor”, Product Datasheet, Dec 2001

[4] Erik J. Johnson, Aaron R. Kunze, “IXP1200 Programming”, Intel Press

[5] A. Sanchez, Walter C. Milliken, Alex C. Snoeren, Fabrice Tchakountio,Christine E. Jones, Stephen T. Kent, Craig Partrige, and W. Timothy Strayer.” Hardware Support for a Hash-Based IP Traceback”, Proc. of the 2nd DARPA Information Survivability Conference and Exposition, June 2001.

[6] 門林雄基、大江将史, “IP トレースバック技術”,情報処理 ,pp 1175-1180,Vol.42 No.12

[7] Stefan Savage, David Wetherall, Anna Karlin and Tom Anderson, “Practical Network Support for IP Traceback”, Proc. of the 2000 ACM SIGCOMM Conference, pp. 295-306, August 2000.