2005－ＳＬＤＭ－119（９）
2005／3／17

ネットワークフィルタリング試験装置の試作

片下 敏宏† 坂巻 佳壽美‡ 乾 剛‡ 名古屋 貢§ 戸田 賢二†

† 産業技術総合研究所 〒305-8568 茨城県つくば市梅園 1-1-1 中央第２
‡ 東京都立産業技術研究所 〒115-8586 東京都北区西が丘 3-13-10
§ デュアキシズ株式会社 〒100-6014 東京都千代田区霞ヶ浦 3-2-5 霞ヶ浦ビルディング 14F

E-mail: † {t-katashita, k-toda}@aist.go.jp, ‡ {sakamaki.kazumi, inui.takeshi}@iri.metro.tokyo.jp, § mnago@duaxes.co.jp

あらまし 近年、ネットワークにおけるセキュリティ強化の必要性がますます高まっており、ファイアウォールや迷惑メールフィルタ、WEB コンテンツフィルタ等のネットワークフィルタリング装置が研究開発されている。本論文では、ネットワークフィルタリング装置の研究開発で必要となる、評価試験を行うための試験装置の回路構成を提案する。本回路構成はハッシュテーブルを用いて送受信フレームデータを検査することにより、試験装置の実装を軽量にする特長を持つ。本稿では提案する回路構成について述べ、さらに Gigabit Ethernet 向けの試験装置の試作について述べる。

キーワード パケットフィルタリング、ネットワークセキュリティ、FPGA

An Experimental Circuit for the Evaluation of Network Filtering Systems

Toshihiro Katahishita† Kazumi Sakamaki‡ Takeshi Inui‡ Mitsugu Nagoya§ and Kenji Toda†

† National Institute of Advanced Industrial Science and Technology
Tsukuba Central 2, 1-1-1 Umezono, Tsukuba-shi, Ibaraki, 305-8568 Janan
‡ Tokyo Metropolitan Industrial Technology Research Institute 3-13-10 Nishigaoka, Kita-ku, Tokyo, 115-8586 Japan
§ DUAXES Corporation. 3-2-5 Kasumigaura, Chiyoda-ku, Tokyo, 100-6014 Japan

E-mail: † {t-katashita, k-toda}@aist.go.jp, ‡ {sakamaki.kazumi, inui.takeshi}@iri.metro.tokyo.jp, § mnago@duaxes.co.jp

Abstract Recently importance of the network security has increased. And various filtering devices – such as firewalls, SPAM filtering, and contents filtering - are developed. In this paper, we propose a circuit composition for the evaluation of the network filtering system. Evaluating network systems with the hash table, our circuit composition does not need huge memory resources. And we made an experimental evaluation system for the gigabit ethernet with our circuit composition.

Keyword packet filtering, network security, FPGA

1. はじめに

近年、社会がコンピュータネットワークによるサービスに依存する傾向にあり、ネットワークサービスに対する攻撃や侵入、不正な情報の流出などに対するネットワークセキュリティが重要となっている。このネットワークセキュリティの方策として、ネットワークのパケットをある条件に従って遮断し、不正な情報の伝達を防ぐパケットフィルタリングがあり、[1][2]のような様々な研究・開発が行われている。

本研究では、このネットワークフィルタリングの評価を行うフィルタリング試験装置の回路構成を提案する。

本回路構成では、ハッシュテーブルを用いた送受信パケットの比較によりフィルタリング機能の評価を行う。これにより、試験時に送受信パケットを記録するための巨大な記憶領域を必要としない。また、全ての送受信パケットを比較することが無く、高速な評価を可能とする。さらに、ネットワークの物理層インタフェース(以後、PHY と呼ぶ)を直接制御することで、ソフトウェアによる試験では困難であった Gigabit Ethernet、10 Gigabit Ethernet(以後、それぞれ 1gE、10gE と呼ぶ)におけるワイヤスピードの試験や、任意の長さの IFG (Inter Frame Gap、フレーム間ギャップ)や不正フレームを用いた試験を可能としている。そして提案する回路構成により 1gE 用の試験装置を試作した。

本論文では、まずネットワークフィルタリング装置とその試験装置について述べる。次に提案する試験装置の構成方法について述べ、最後に試験装置の試作について述べる。

2. フィルタリング装置と試験装置

特定の条件にしたがってネットワークを通過する

パケットを破棄し安全を確保するセキュリティ技術がフィルタリングであり、用途に応じて様々なフィルタリング装置が研究開発されている。パケットのアドレス・ポート情報を元に不正なアクセスを遮断するファイアウォールのパケットフィルタリング、特定のキーワードや送信元アドレスを元に迷惑メールや情報漏洩メールを削除するメールフィルタリング、特定のURLへのWEBアクセスを防止し有害なコンテンツや業務と関連のないコンテンツにアクセスさせないWEBコンテンツフィルタリング等が挙げられる[3]。

このようなフィルタリング装置を評価する項目として次のようなものが考えられる。

1) フィルタリング機能の評価

フィルタリングが正しく機能するか評価を行う。削除すべきパケットがフィルタリングされ、その他のパケットは通過することを確認する。

実際には、削除対象パケット／対象でないパケットが混在したトラフィックを試験対象装置に入力し、装置からの出力を入力したトラフィックと比較して評価する。

2) ネットワーク装置としての機能評価

フィルタリング装置がネットワーク装置として正しく動作するか評価を行う。規定されていない異常なフレームが入力された場合でも装置が停止せずフレームを破棄できるか等を確認する。

実際には、様々な種類のフレームが混在したトラフィックを試験対象装置へ入力し、装置からの出力の検証や装置の状態を評価する。

3) スループット計測

フィルタリング装置のスループットの評価を行う。フィルタリングを行わない状態のネットワーク装置としてのスループットと、フィルタリングを行った場合のスループット等を測定する。

実際には、試験対象装置へ入力するトラフィックのスループット、フィルタリングされるフレームを除いた場合のスループット、装置から出力されたトラフィックのスループットを測定する。

このような試験を実施する環境として、実際の運用環境に似たネットワークを構築する方法[4]や、ソフトウェアで擬似的にトラフィックを生成する方法(図１)、またはソフトウェアの代わりに専用ハードウェアによりトラフィックの生成を行う方法などが挙げられる。

実際の運用環境に似たネットワークを構築する方法では試験に多くの装置が必要であり、また、試験において同じトラフィックを再現することが難しい。ソフトウェアで擬似的なトラフィックを生成する方法は安価に試験環境が構築でき、トラフィックを再現することもできるが、コンピュータ上のNIC(Network Interface Card)を用いるため、IFGを調整してトラフィックの密度を変化させるなど、トラフィックの詳細な操作を行うことが困難である。また、1gEや10gEの環境ではショートパケットを理想的なスループットで送出することが難しく、詳細なスループットの測定を行うことが困難である。また、誤ったFCS(Frame Check Sequence)やプリアンブルなどの異常な状態を持ったフレームを生成できないため、異常な状態における装置の挙動を評価することができない。

一方ハードウェア試験装置は、PHYを直接操作することにより、詳細なトラフィック状態の操作を行うことが可能であるため、様々な条件の下で試験を行うことができる。このような理由から、フィルタリングの試験環境はハードウェアによるものが最も適していると考えられる。

本研究では、このハードウェア試験装置の回路構成を考案した。

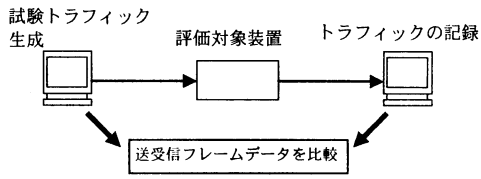

図 1：擬似トラフィックによる試験環境

3. フィルタリング装置の試験装置

フィルタリング機能やネットワーク装置としての機能は、試験対象装置に対して送信するフレームと試験対象装置から出力されたフレームを比較することにより評価する。しかし、単純に送受信されたフレームデータを記録して比較を行う場合、巨大な記憶領域が必要となる。また、フレームが試験対象装置を通過する際にフレームの順番が入れ替わる場合があるため、送受信フレームデータの比較に時間を要する。

本研究ではハッシュテーブルを用いて送受信フレームデータの比較を容易にすることで、巨大な記憶領域を必要とせず高速な比較が行える回路構成を提案する。

3.1. 提案する試験装置の回路構成

提案する試験装置の回路構成を図２に示す。試験装置は送信器と受信器の組から構成され、以下に示す手順で送受信フレームデータを比較することによりフィルタリング機能の評価を行う。

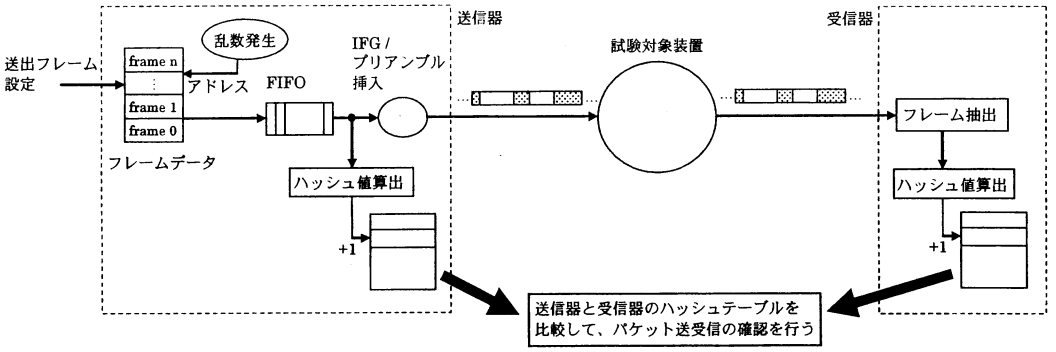

図 2： 提案する試験装置の回路構成

まず、ソフトウェアであらかじめ送信すべきフレームデータを生成する。このフレームデータを試験装置の送信器へ設定し、このフレームデータをランダムに選択して FIFO へ入力する。そして FIFO からフレームデータを順次取り出し、指定された間隔の IFG とプリアンブルを追加して試験対象装置へ送出する。このとき、FIFO から取り出したフレームデータからハッシュ値を計算し、ハッシュテーブルの値を 1 加算する。

次に、試験対象装置を通過したフレームデータを受信器で入力し、送信器と同様にハッシュ値の計算とテーブルの変更を行う。最後に送信器・受信器のハッシュテーブルを比較することで、送受信が正常に行われたかどうかを評価する。ハッシュテーブルの値が異なる場合、異なっているテーブルのハッシュ値より異常が発生したフレームを特定することができる。

フレームデータ間のハッシュ値の重なりは、フレームデータ生成時にハッシュ値を計算することであらかじめ想定できる。

送信器に設定するフレームデータには、フレームデータ長やフィルタリング装置で削除されるかどうかを示すフラグを記録したヘッダを付加する。送信器でハッシュ値を計算する際、このヘッダ情報からフレームがフィルタリング装置で削除されるかを判断し、削除されるべきフレームデータからはハッシュ値を算出しない。このようにしてフィルタリング機能により正常にフレームデータが削除されるかどうかを検証することができる。なお、フレームデータのヘッダは、送信時に削除し試験対象装置には送出送信しない。

図 2 では、スループットを計測する部分は省略している。

3.2. 試験装置の実装

提案する回路構成で、1gE 用のフィルタリング試験装置を試作した。実装は FPGA ボード REX[5]に 1gE の PHY チップを接続した環境へ行った。FPGA は Xilinx xcv2000e-6 [6]である。

実装した送信器の構成を図 4 に、受信器の構成を図 5 に示す。また、図 6 、 7 に試作機の写真を示す。

試作した試験装置は、送信フレームを SDRAM に格納し、最大 32768 個のフレームデータをシーケンシャルに送信する。フレームデータ間の IFG はホスト PC から設定した固定値とした。ハッシュ値はフレームデータを 16bit 毎に区切り、そのビット毎の論理和の 16bit とした。ハッシュテーブルは送信器・受信器ともに SRAM に格納し、試験終了時にホスト PC へ収集されホスト PC 上で検査される（図 3）。試験はホスト PC から送信器へトリガをかけて開始し、あらかじめ設定した数のフレームを 1 度送出して終了する。試験の開始・終了は特定の ARP フレームを用いて送信器から受信器へ通知される。

今回の試作ではスループット計測機構は付加していないが、送信器のフレーム生成部、受信器のフレーム抽出部に回路を付加することで計測可能な回路構成となっている。

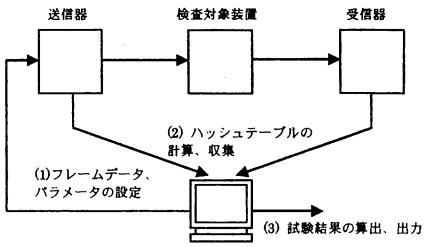

図 3：試作した試験装置の概念図

回路規模は、送信器で 1238 Slice、受信器で 442 Slice であった。最大動作周波数は送信器で 60MHz、受信器で 74MHz であるが、回路中でフレームデータを 32bit 毎に扱っているため、動作周波数は 31.25MHz 固定としている。(32bit × 31.25MHz = 1Gbps)

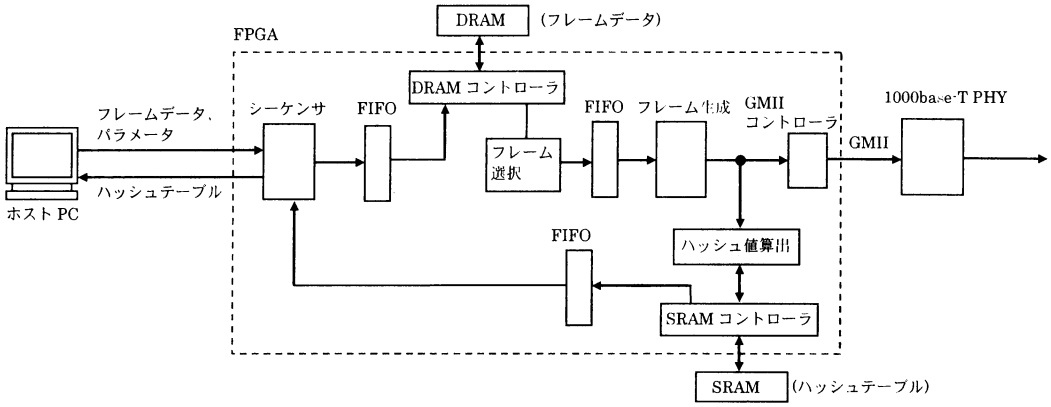

図 4：送信器のブロック図

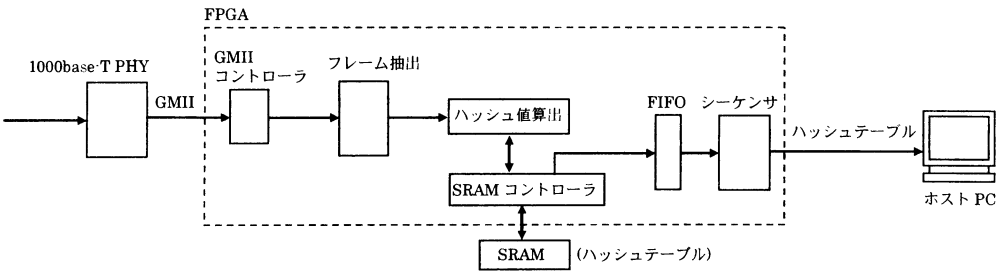

図 5：受信器のブロック図

試作した試験装置に 1gE のスイッチングハブを試験対象装置として接続し動作確認を行った。1500 個の URL アドレスをランダムに選択して生成した 8192 個の HTTP GET フレームデータと、IFG が約 131us(16384 クロックサイクル)の設定で試験を行い、収集したハッシュテーブルが一致することを確認した。なお、試験装置は MAC アドレスを持たないため、試験フレームデータの宛先 MAC アドレスはブロードキャストアドレスとした。試験において、IFG を 0.5us 程度(64 クロックサイクル)に短くするとスイッチングハブでいくつかのフレームが欠落しまうことも分かった。

しかしこのとき、テスト終了を通知するフレームも欠落してしまう場合があり、受信器からハッシュテーブルが出力されない問題があった。この問題は送信器と受信器を直接接続する信号を用いてテストの開始・終了を通知することにより改善する予定である。

今回の試験では、試験対象装置にフィルタリング機能が搭載されていないためネットワーク装置としての評価のみ行った。今後はフィルタリング装置を用いて検証機能の動作確認を行う予定である。

この試作により、本回路構成による試験装置は回路規模が小さく、また、ハッシュテーブルによる送受信フレームデータの比較が可能であることが分かった。

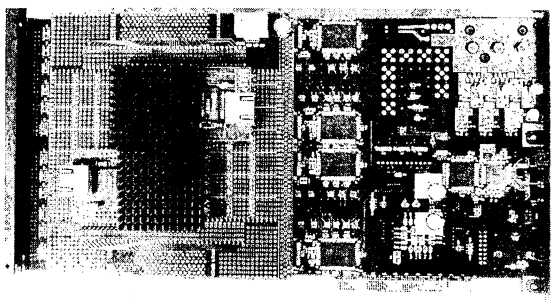

図 6：試作した試験装置(ネットワーク PHY)

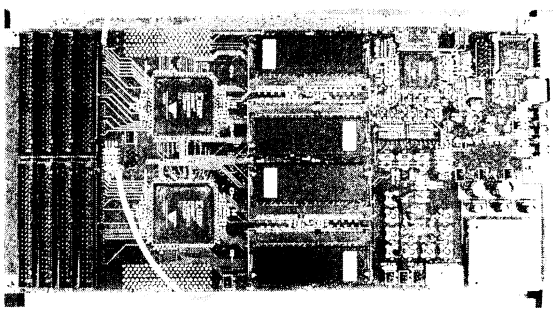

図 7：試作した試験装置(FPGA)

4. まとめ

フィルタリング装置の試験装置をハッシュテーブルにより軽量に実装する回路構成を提案した。本回路構成は送受信フレームデータを直接比較することなく試験を行うためフレームデータを保存する記憶領域を必要とせず、かつ、高速な検証を行うことができる特長を持ち、フィルタリング装置の連続試験を可能とする。また、ネットワークPHYを直接操作することで、様々な条件の下でワイヤスピードのフィルタリング性能試験を可能とする。

本論文では、提案する回路構成による1gE用の試験装置の試作を行い、ハッシュテーブルによる送受信フレームデータの比較動作を確認した。

今後は、フィルタリング装置を試験対象装置として接続し、フィルタリング機能試験の動作確認を行う予定である。また、試作した試験装置に以下の改善を行う予定である。

・ テスト開始・終了通知の改善

送信器と受信器を直接接続する信号を設けることにより、試作で発生したテスト開始・終了通知が欠落する問題を改善する。

・ ハッシュテーブル収集・検査の自動化

FPGA上でハッシュテーブルの収集・検査を自動的に行い、結果のみをホストPCに通知する。

・ ハッシュテーブルの多重化

ハッシュテーブルの読み書きを同時に行える様に多重化し、前項のハッシュテーブル収集・検査の自動化と組み合わせることにより、長時間の試験を連続的に行う。

・ スループット測定回路の付加

送信器・受信器に測定回路を付加し、スループットの測定や、フレームが欠落するスループットの境界の自動検出を行う。

・ ハッシュ値算出の改善

試作におけるビット毎の論理和によるハッシュ値の生成ではハッシュ値の衝突が起こり易いため、ハッシュ値算出アルゴリズムを改善する。

・ フレームデータのランダム選択の実装

試作ではシーケンシャルにフレームデータを選択しているが、これをランダムに選択できる様改善する。

これらの試験装置の改善のほか、10gE用試験装置の試作を行う予定である。

追記：

本研究は、平成１６年度 地域新生コンソーシアム研究「パターンマッチング回路の超高速化とフィルタリング装置への応用」の一環として実施されたものである。

文　献

[1] Kartik Gopalan, Tzi-cker Chiueh, "SBFilter: A Fast URL Filter Engine for Internet Access Management", ESCL Technical Report TR-57, Computer Science Dept, Stony Brook University, Stony Brook, 1999.

[2] John W. Lockwood, Christopher Neely, Christopher Zuver, James Moscola, Sarang Dharmapurikar, David Lim, "An Extensible, System-On-Programmable-Chip, Content-Aware Internet Firewall", FPL 2003, Lisbon, Portugal, Paper 14B, Sep 1-3, 2003.

[3] 片山 善治 監修, "IT セキュリティソリューション大全 下巻 IT セキュリティエンジニアリング", フジ・テクノシステム, 2004.

[4] Richard P. Lippmann, David J. Fried, Isaac Graf, Joshua W. Haines,Kristopher R. Kendall, David McClung, Dan Weber, Seth E. Webster, Dan Wyschogrod, Robert K. Cunningham, and Marc A. Zissman, "Evaluating Intrusion Detection Systems: the 1998 DARPA Off-Line Intrusion Detection Evaluation", Proceedings of the 2000 DARPA Information Survivability Conference and Exposition, 2000, Vol. 2.

[5] Yuetsu Kodama, Toshihiro Katashita, Kenji Sayano, "REX: A Reconfigurable Experimental System for Evaluating Parallel Computer Systems", IEICE Transaction Information & Systems, Vol. E86-D, No.10, Oct. 2003.

[6] Xilinx, "Virtex-E 1.8V Field Programmable Gate Arrays"