超高速ネットワークに対応した悪意のある通信の遮断技術の研究開発（072003008）

Research Development on Blocking Technology of Malicious Communication over Ultrahigh-speed Networks

研究代表者

戸田賢二　（独）産業技術総合研究所

Kenji TODA　National Institute of Advanced Industrial Science and Technology (AIST)

研究分担者

戸田賢二[†]　関山守[†]　片下敏宏[†]　坂根広史[†]　堀洋平[†]　高橋栄一[†]　岩田昌也[†]　村川正宏[†]　樋口哲也[†]
三宅優[††]　竹森敬祐[††]　山田明[††]　原正憲[††]　澤谷雪子[††]

Kenji TODA[†]　Mamoru SEKIYAMA[†]　Toshihiro KATASHITA[†]　Hirofumi SAKANE[†]　Yohei HORI[†]
Eiichi TAKAHASHI[†]　Masaya IWATA[†]　Masahiro MURAKAWA[†]　Tetsuya HIGUCHI[†]
Yutaka MIYAKE[††]　Keisuke TAKEMORI[††]　Akira YAMADA[††]　Masanori HARA[††]　Yukiko SAWAYA[††]

[†]（独）産業技術総合研究所　[††]（株）KDDI 研究所

[†]National Institute of Advanced Industrial Science and Technology (AIST)

[††]KDDI R&D Laboratories

研究期間　平成 19 年度～平成 21 年度

概要

インターネットを安心・安全に利用できるようにするために、なりすましによって口座情報などを詐取するフィッシング、DoS 攻撃などによるサービスの停止、不正侵入による情報漏洩・Web サイトの改ざん・システムの乗っ取り、コンピュータウイルスなどの悪意ある通信の遮断技術の研究開発を行った。特に、近年の情報量の増大とネットワークの高速化に対応するため、悪意のある通信の分析・検出を自動で効果的に行う方法の開発と共に、論理プログラマブルデバイス(FPGA)などのハードウェア技術を応用することにより、漏れのない検知・遮断を数十 Gbps～数 Tbps の超高速ネットワークで行うことのできる小型かつ省電力なシステムの開発を行った。

Abstract

For the sake of using internet safely and securely, the blocking technology of malicious communications such as phishing (by web spoofing) , shutting down services, information leak, defacing of web sites, hijack of systems (by DoS attack, computer viruses and hacking of company networks) is the target of this research. In particular, along with the automatic and effective analysis and detection method of malicious communication, the high performance, compact and energy efficient hardware system utilizing logic programming device (FPGA) was developed to deal with enormous increase of communication over ultrahigh-speed networks. It can perform detection and/or filtering without omission at speed from tens of Gbps – to multiple Tbps.

１．まえがき

情報通信インフラは、現代社会の主要な柱となっているが、同時にそれを悪用しようとする「悪意のある通信」によってもたらされる被害も甚大で大きな社会問題となってきている。今後、高精細画像・映像の配信やクラウドサービスなどますます通信が高速広帯域化する状況にあり、スマートグリッドなどエネルギーの制御に情報通信技術を用いる応用も期待されているが、通信速度と共に安全性の確保が不可欠である。この様な状況に対処するため本研究課題は、情報通信サービスのバックボーンなどの超高速ネットワークにおいて、フィシング、サイバー攻撃、コンピュータウイルスなど悪意のある通信を除去する技術を開発しようとするものであり、有害情報を遮断するハードウェア技術と有害情報の収集識別技術の研究開発を行った。

２．研究内容及び成果

本課題での研究開発の概要を図１に示し、以下各項目の内容を紹介する。

◆ハードウェア開発

セキュリティ装置のハードウェアは、本研究課題で開発を行った FPGA ボード REX3（図２）及び PC で構成される。REX3 は，本研究で必要とされる侵入防御、有害情報フィルタリング、ウイルス防御などの高速ネットワーク応用を行うことを主眼としたもので、大容量 FPGA（Xilinx Virtex5）を搭載し、10GbE を 6 ポート、ブラックリストなど処理データの格納のためメモリは DRAM 用ソケットを 2 個装備している。PC との連携のため

<table>
<tr><td colspan="3"></td><td>自動フィルタによる URL 生成（ソフトウェア）</td></tr>
<tr><td>侵入遮断（回路）</td><td>ウイルス遮断（回路）</td><td>URL フィルタリング（回路）</td><td>キャプチャ（回路）</td></tr>
<tr><td colspan="4">拡張可能 60Gbps 光ポート搭載 FPGA ボード (REX3)</td></tr>
</table>

図１．研究開発の概要

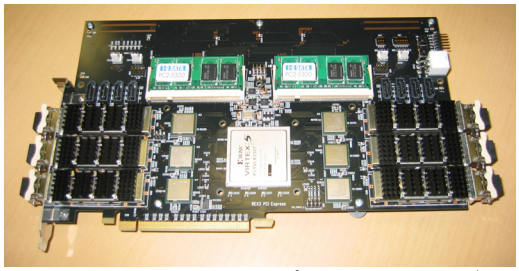

図２．拡張可能 60Gbps 光ポート搭載 FPGA ボード（REX3）

PCI-Express で高いバンド幅の確保し、ハードディスクなどへのデータ蓄積を高帯域で行うための SATA を８ポート有している。図３は、 PC の PCI-Express ソケットに REX3 を装着したネットワークセキュリティ装置の試験風景である。必要に応じて複数枚装着することができる。

◆応用：URL フィルタリング（フィシングサイトなどの遮断）

高速マッチングを実現するため必要なメモリ帯域を押さえることの出来るハッシュ＋バイナリサーチ方式を考案し、60Gbps を超える性能を達成した。ブラックリストは、本課題で開発した以下の URL フィルタ自動生成方式によって得られた 34,000 エントリを用いたが、ブラックリストを格納しているメモリは 4GB であり、マルチエントリの解決にはバイナリサーチを用いるため大規模データにも十分対応可能である（誌上発表リスト[2]）。

◆ソフト：URL フィルタ自動生成方式

マルウェア配布、フィッシング、有害情報など Web サイトが問題となっており、組織内のネットワークにおけるフィルタリングが必須なっている。しかし、サイトが短期間で発生と消滅を繰り返すため、フィルタリングリストの収集更新が課題であった。そこで、キャプチャしたトラヒックと外部の信頼情報を組み合わせて、候補となる URL を自動的に生成・配信する方式を開発した。特に、個人情報を詐取するフィッシングサイトとプライバシ情報を漏洩させる Web バグサイトを対象として、80～90%の精度のリスト生成を実現した（誌上発表リスト[3]）。

◆応用：侵入遮断（サイバー攻撃などの遮断）

公開されている侵入検知ソフトである SNORT ルールのサブセット 1200 ルールを非決定性オートマトン化し、並列処理方式を工夫することで、侵入の防御を 30Gbps で行えることを示した。

◆応用：ウイルス遮断

公開されているシグニチャ方式のアンチウイルスソフトである ClamAV のルールのサブセットをマッチング回路を並列化することにより 6.4Gbps でウイルスの除去を実現した。これは、１世代前の FPGA ボードを用いたデータであり、REX3 では、30Gbps で処理できる見通しである。

◆応用：通信レコーダ（トラフィックキャプチャ）

ボード当たり SATA でハードディスク（RAID や SSD も接続可）８台に同時にアクセスできるため、遮断の記録の他、様々な用途に用いることが可能であり、必要な回路量が少ないため同一ボードで他の応用と併用できる。

◆高通信帯域ボードが実現する強力な拡張性

上記応用における性能は、REX3 FPGA ボード１枚でのものであり、必要な機能と性能に応じてスケーラブルにボードを組み合わせることができる。すなわち、これら３種類の機能が全て必要であれば、３枚のボードを 10GbE ポートで直列接続し、１台の PC の PCI-Express ポートに挿し内蔵させることで実現できる。また、URL フィルタリング専用であれば、ボード 1 枚の処理速度は 60Gbps であるため、17 枚で、1Tbps の性能が得られる。PCI-Express が６枚装着可能なマザーボードを用いれば３台のデスクトップ PC で 1Tbps が処理可能となる。また、10GbE で PC クラスタを構成することもできるため、高速データサーバなどクラウド応用も期待できる。

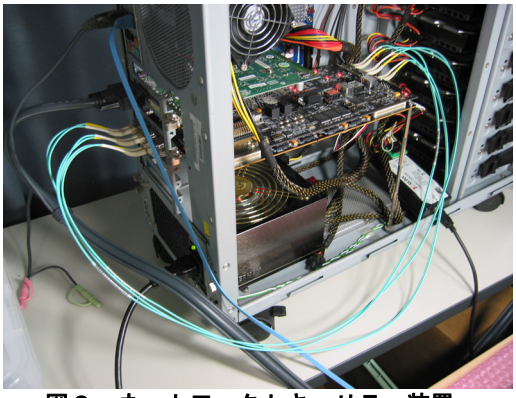

図３．ネットワークセキュリティ装置（試験風景）

３．むすび

数十 Gbps～数 Tbps の超高速ネットワークに対応しリアルタイムに悪意のある通信を遮断するネットワーク接続型セキュリティ装置の開発に成功した。本装置は、専用に開発した高通信帯域の FPGA ボードをベースとしており、フィシングサイトや有害情報サイトなどの URL フィルタリング、サイバー攻撃、ウイルスなどの遮断機能に加えて通信レコーダ機能を搭載可能であり、ボードを複数枚組み合わせて用いることで、必要な機能及び性能を得ることが出来る。フィシングなど有害 Web サイトのリスト構築については、キャプチャしたトラヒックと外部の信頼情報を組み合わせて、候補となる URL を自動的に生成・配信する方式を開発し高い精度と即時性を実現した。本装置は、FPGA の書き換えにより、様々な情報収集やフィルタリングにも用いることができるため、今後の幅広い活用が期待される。

【誌上発表リスト】

[1] 片下敏宏, 坂根広史, 堀洋平, 戸田賢二, “10 Gigabit Ethernet に対応したネットワークフィルタリング試験装置,” 情報処理学会論文誌, Vol.49, No.6, 2008, pp.2118-2128 (2008 年6月15日)

[2]戸田賢二、関山 守 、久保田 貴也、"超高速ネットワーク対応 URLフィルタリング装置の開発"、信学技報, Vol.109, No.474, CPSY2009-92, pp.483-488, 2009 (2010年3月28日)

[3] Akira Yamada, Hara Masanori and Yutaka Miyake、"Web Tracking Site Detection Based on Temporal Link Analysis", The 2010 IEEE International Symposium on Mining and Web (2010 年 4 月 20 日)

【申請特許リスト】

[1] 山田明、原正憲、三宅優、ウェブアクセス制御装置、ウェブアクセス制御システム及びコンピュータプログラム、日本、2008 年 9 月 11 日

[2] 堀洋平、佐藤証、坂根広史、戸田賢二、再構成可能論理デバイスの論理プログラムデータ保護システム及び保護方法、日本、特願 2008-291864、2008 年 11 月 14 日

【受賞リスト】

[1] 堀 洋平、デザインガイア ポスタ賞、“サイドチャネル攻撃に対する標準評価ボード SASEBO とツールの開発”、電子情報通信学会 VLD、DC、CPSY、RECONF、ICD、CPM 研究会、情報処理学会 SLDM 研究会、2008 年 11 月 19 日