大域ディペンダブル情報基盤プロジェクト
～ディペンダブルアーキテクチャグループ　平木研究室～

平木　敬

情報理工学系研究科コンピュータ科学専攻

あらまし　平成１６年度における平木研究室では、アーキテクチャ的アプローチによるディペンダビリティの実現、超高速 IDS の実現によるディペンダビリティの確保を目指し（1）CPU そのものを超ディペンダブルとすることを目的とした、FPGA を用いた代用と再構成プロセッサアーキテクチャの研究と、（2）超高速ネットワークを対象とした IDS をアーキテクチャを用いて実現する方式の研究を実施した。FPGA を用いた代用と再構成プロセッサアーキテクチャの研究では、超高信頼性を実現する部分を、演算器からプロセッサ全体に拡大し、System　C 言語を用いてプロセッサのシミュレーションを実施した。超高速ネットワークを対象とした IDS アーキテクチャでは、マルチストリームの TCP を対象に 10Gbps 以上の速度でストリングマッチングが可能な SBT アルゴリズムを開発し、FPGA を用いて実現した。

１．はじめに

情報システムのディペンダビリティを向上させるアーキテクチャ的アプローチとしては、情報システムの中枢である CPU に超ディペンダビリティを実現することと並び、情報システム全体のディペンダビリティをアーキテクチャ技術を用いて向上させることが求められる。平木研究室では、前者の問題を解決することを目的として、平成１５年度に引き続き代用と再構成を用いた FPGA による超高信頼 CPU の研究を実施した。このテーマにおける目標は、100 万から 200 万ゲート規模の FPGA を用いることにより、構成要素の９０％の論理セルに故障が発生した場合でも、数倍の性能低下に影響をとどめ、動作を実現する CPU を実現することである。平成１６年度はその第三年度として、CPU 全体を高信頼とするための基本方式を策定した。

また、平成１５年度から開始した FPGA ベースネットワークインタフェースカードを用いた、超高速 IDS の実現方式の研究を更に発展させ、マルチストリーム TCP 用ストリングマッチングアルゴリズムを提案し、FPGA に実装した。本稿では、後者、すなわちマルチストリーム向けストリングマッチングの研究開発について述べる。

２．超高速 IDS アーキテクチャ

IDS に必要な技術のうち、主に以下の 2 点が高速化研究の対象になっている。

(1) 高速な文字列マッチ(exact match もしくは正規表現)
(2) TCP ストリームの認識

(1)は、IDS でパケットのペイロードに特定のパターンが含まれているかどうかをチェックする処理に使う。この部分は IDS の中でも特に処理が重い部分で、高速化の必要性が高い。有名なフリーの IDS ツールである Snort[2]を用いた研究が多い。

(2)は、安全性を高めたい場合は TCP パケットのストリームを組み立て直し、これに対してパターンマッチを適用する必要があるためである。さもないと、パケットを分割する等の手法により検査をすり抜けられてしまう。あまり網羅していないが、パケット順序交換等が無い場合について HW でサポートを行う方式として[3]や[4]がある。

他に、分割された IP パケットのデータ範囲が重なった場合のホストの振る舞いの曖昧性を利用して IDS をくぐり抜ける手法等がある。そこで、トラフィック・ノーマライザ[5]を使えば、セマンティックスに影響が無い範囲でパケットを作り直し、曖昧性を取り除く事ができる。曖昧性を取り除いた後の TCP ストリームに対して IDS を適用すればより高い安全性を確保できる。

しかし、このような処理を高帯域で行うためには、ハードウェアによる有効な方式を見つける必要がある。現在の所、実用に堪える方式はまだ無い。

IDS で用いるストリームマッチングのアルゴリズムを、平成１５年度の成果から拡張し、様々なパターンの攻撃にたいして有効にストリングマッチングによる攻撃検出か可能な方式を平成１６年度に開発し、評価を行った。

ハードウェア構成

IDS は、図１に示す 10Gbps イーサネットアダプタを２個、カード間高速リンクで結合したもので実現する。実装されている Xilinx の FPGA には、10GBASE のイーサーネットの MAC,PCI-X インタフェースおよび IDS のためのストリングマッチング回路が実装される。

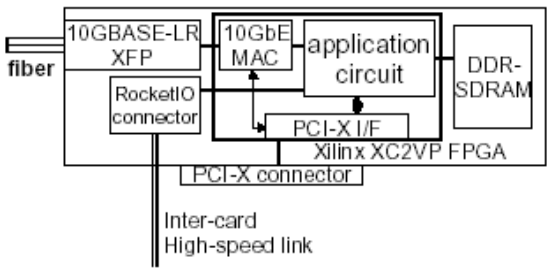

図１．FPGA を用いた 10Gbps イーサネット NIC

IDS などを目的とし、ストリングマッチングを FPGA を用いて実現する方法は、すでに多数提案されているが、実際に基幹ネットワークなどに挿入して使うためには、既存方式では多くの問題点を持つ。

（1）マッチングするストリングは、TCP ストリーム上に存在するため、多数のストリームが同時並行的に通信する場合には、全 TCP ストリームに関してマッチングを並行して取る必要があること。（図２）

（2）複数パケットにまたがる TCP ストリームにおいて、構成パケットの長さを極小にして IDS へ高負荷をかける場合があること。

（3）TCP はパケットの順序変更、パケットの欠落を許すプロトコルであるため、順序を変更したり、再送に異なるコンテンツを載せることでマッチングを妨害可能なこと。（図３）

これら、複数 TCP ストリームを正しくマッチングすることは、エンドノードでない位置でパケットのマッチングを取る場合、例えば基幹ネットワークにおける IDS にとり多くの困難点を生じさせる。

（2）に示す、極小パケットによる負荷の上昇は、ソフトウェアによる IDS の限界を超えさせることにより、事実上システムを停止させる攻撃を可能とする。今回、FPGA を用い、10Gbps ネットワークのワイヤレートにおいて動作可能なストリングマッチングを提案する背景である。

（3）は、特に基幹ネットワークにおける IDS にとり大きな問題である。複数のストリームにおいて、パケット順序の変更やパケットの再送を含む入力に対するマッチングは、コンジェスチョン・ウィンドウサイズが非常に大きくなる可能性のある 10Gbps レベルのネットワークにおいては、メモリ容量、処理速度などの点から困難な課題となる。

私たちが平成１５年度に提案した、FPGA を用いたストリングマッチング方式は、（1）に示した複数 TCP ストリーム環境での超高速マッチングを、退避・復旧するステートを極小化する Trie ベースアルゴリズムを用いることにより初めて解決した。

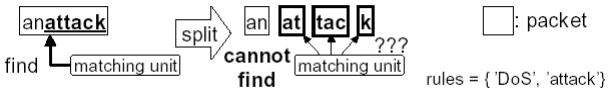

図２．複数パケットへ分割されたストリング

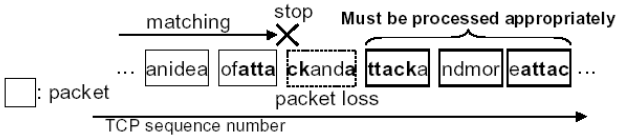

図３．パケット再送によるマッチング動作の変化

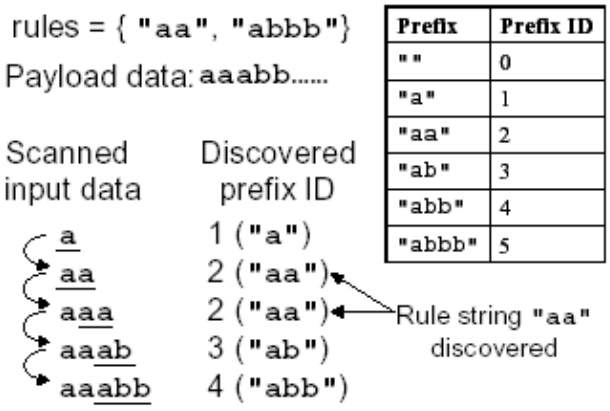

図４．Prefix 表を用いたマッチング

マッチング方式

上記問題点を解決することを目的として、平成１７年度には、ストリングマッチングアルゴリズムの拡張を行った。図４は、マッチング方式の概要を示すものである。

性能評価

今回開発したストリングマッチングアルゴリズムを、FPGA 上に実装し、シミュレーションにより性能評価を行った。

評価は Snort に含まれるストリングを用いた。図５は、

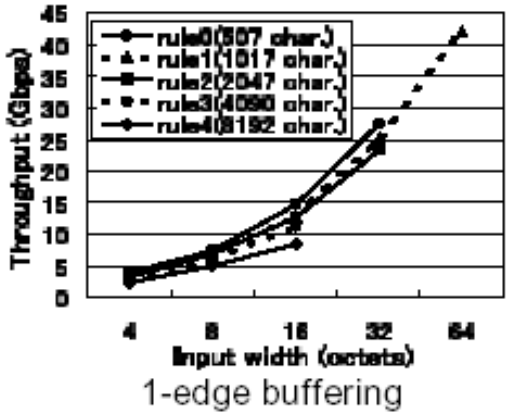

図５．単方向ストリングマッチングの性能

提案アルゴリズムによる１方向ストリングマッチングの処理性能である。同時処理幅が 16 バイト以上で、10Gbps 以上の処理能力が得られることが示されている。一方、図６は双方向ストリングマッチングの処理性能を示している。前記のパケット順序の変更、パケットの再送に対処するためには双方向ストリングマッチングが必要である。

図６においても、１６バイト以上の並列マッチングにより、10Gbps 以上の性能が得られることが示されている。

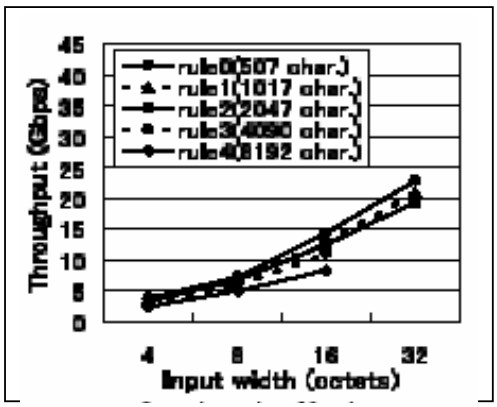

図７．双方向ストリングマッチングの処理性能

４．おわりに

平木研究室で行った２個の研究テーマは、異なるアプローチで情報システムの超高信頼性を実現することを目的としたものである。代用と再構成を用いる超高信頼 CPU アーキテクチャの研究では、今後詳細なシミュレーションを実施するとともに、実際の FPGA 上に提案アーキテクチャを実装し、評価する予定である。

平成１６年度には、平木研究室では IDS 用ストリングマッチング方式の研究のほか、（1）FPGA を用い、代用と

再構成による超高信頼 CPU アーキテクチャの研究開発、（２）動的コンパイラを用いた、エラー処理を含むプログラムの冗長性除去手法、（３）値の局所性を利用する投機的並列化方式、（４）ニューラルネットワークを用いる高精度分岐予測方式、（５）キャッシュからのハードウェア情報を利用したプロセススケジューリング方式と、（６）TCP 高速化方式の研究を実施した。詳細は発表文献を参照のこと。

発表文献

[1] Kei Hiraki, Makoto Nakamura, Junsuke Senbon, Yutaka Sugawara, Tsuyoshi Itoh, Mary Inaba,"End-node transmission rate control kind to intermediate routers - towards 10Gbps era",Second International Workshop on Protocols for Fast Long-Distance Networks(PFLDnet 2004), Web,2004

[2] Hiroyuki Kamezawa, Makoto Nakamura, Mary Inaba, Kei Hiraki,"Coordination between parallel TCP streams on Long Fat Pipe Network",1st International Workshop on Data Processing and Storage Networking: towards Grid Computing" (DPSN04), 2004

[3] Makoto Nakamura, Hiroyuki Kamezawa, Junji Tamatsukuri, Mary Inaba, Kei Hiraki, Kenji Mizuguchi, Kenichi Torii, Satoru Nakano, Shoichi Yoshita, Ryutaro Kurusu, Masakazu Sakamoto, Yuki Furukawa,"Long Fat Pipe Congestion Control for Multi-Stream Data Transfer#, Proceedings of the International Symposium on Parallel Architectures, Algorithms and Networks (ISPAN2004), PP. 294-299, 2004

[4] Yutaka Sugawara, Kei Hiraki,"A computer architecture education curriculum through the design and implementation of original processors using FPGAs", Proc. of Workshop on Computer Architecture Education (WCAE 2004), PP.3-7,2004

[5] Yutaka Sugawara, Mary Inaba, Kei Hiraki,,"Over 10Gbps String Matching Mechanism for Multi-Stream Packet Scanning Systems",Field-Programmable Logic and Applications, 14th International Conference (FPL 2004), LNCS 3203,PP.484-493,2004

[6] Rei Odaira, Kei Hiraki,"Partial Value Number Redundancy Elimination", Proceedings of the International Workshop on Languages and Compilers for Parallel Computing (LCPC 2004), Lecture Notes in Computer Science, 2004

[7] Hiroyuki Kamezawa, Makoto Nakamura, Junji Tamatsukuri, Nao Aoshima, Mary Inaba, Kei Hiraki, Junichiro Shitami, Akira Jinzaki, Ryutaro Kurusu, Masakazu Sakamoto, and Yukichi Ikuta,"Inter-layer coordination for parallel TCP streams on Long Fat pipe Networks", Super Computing 2004, High Performance Networking and Computing (SC2004),CD-ROM 2004

[8] Shoichi Hirasawa, Kei Hiraki, Utilizing Dynamic Data Value Localities in Internal Variables",5th International Conference, Parallel and Distributed Computing: Applications and Technologies(PDCAT) LNCS3320 ,pp. 305-309, 2004

[9] Rei Odaira, Kei Hiraki,"Sentinel {PRE}: Hoisting beyond Exception Dependency with Dynamic Deoptimization", Proceedings of the 2005 International Symposium on Code Generation and Optimization (CGO), pp. 328-338, 2005

[10]大平玲、平木敬,"値番号に基づく部分冗長性除去",情報処理学会論文誌：プログラミング SIG 9-45,pp.59-79, 2004

[11]亀沢寛之,中村誠,稲葉真理,平木敬,陣崎明,下見淳一郎,来栖竜太郎,中野理,鳥居健一,柳沢敏孝,生田祐吉,"長距離・高バンド幅通信における並列 TCP ストリーム間の調停の実現",先進的計算基盤システムシンポジウム Symposium on Advanced Computing Systems and Infrastructures(SACSIS). 2004

[12]菅原豊、稲葉真理、平木敬,"インテリジェント NIC を用いた高帯域ネットワーク向け TCP 通信方式",情報処理学会研究報告、2005 年並列／分散／協調処理に関する『青森』サマー・ワークショップ (SWoPP2004), OS-97-82, pp. 57-64, 2004

[13]中村誠, 亀沢寛之, 稲葉真理, 平木敬,"協調動作する並列 TCP ストリームへの Packet Spacing の適用とその評価", 情報処理学会研究報告、2005 年並列／分散／協調処理に関する『青森』サマー・ワークショップ (SWoPP2004), pp. 199-204, 2004

[14]平澤将一、平木敬, "プロファイルを利用した値の局所性による高速化手法", 情報処理学会研究報告、2005 年並列／分散／協調処理に関する『青森』サマー・ワークショップ (SWoPP2004)ARC-159, pp. 1-6, 2004

[15]大平玲、平木敬,"例外依存関係を越える部分冗長性除去", 情報処理学会論文誌：プログラミング、2005 年並列／分散／協調処理に関する『青森』サマー・ワークショップ (SWoPP2004)SIG 1-46,pp. 134-148 2004

[15]小川周吾、平木敬,"ハードウェア統計情報を用いたプロセスの動的な最適スケジューリング手法",情報処理学会研究報告、2005 年並列／分散／協調処理に関する『青森』サマー・ワークショップ (SWoPP2004)ARC-159,pp.55-60 2004

[16]下見淳一郎, 河合純, 下國治, 陣崎明, 中村誠, 稲葉真理, 平木敬, "長距離 TCP 高速化機構の開発", インターネットコンファレンス 2004", pp.83-91 2004