

CAMを用いた不正検知型侵入検知システム実装手法の提案

鈴木 諭司 西山 怜 熊木 武志 梶崎 浩嗣 岩井 啓輔 黒川 恭一

防衛大学校情報工学科

1 はじめに

近年，組織内部のネットワークへの不正侵入を防止するセキュリティ技術が重要になってきており，それに伴い，侵入検知システム (Intrusion Detection System :IDS) が普及し始めている．これまで IDS は，シグネチャの更新を容易にするため，ソフトウェアによる実装が行われてきたが，これらの性能は近年のネットワークの急速な進歩に遅れをとっている．高速なネットワークにおいて，リアルタイムに侵入検知処理を行うことが不可能になってきているため，従来の IDS は現状に十分対応しきれていない．そこで本稿では，CAM を用いた新たな IDS を提案する．本稿では FPGA を用いて実装し，そのことにより高いスループットが得られ，また容易にシグネチャを更新することができることを示す．

2 IDS の概要と問題点

IDS は，セキュリティ侵害を発見するために，コンピュータ・ユーザ・ネットワークの状態を監視しつつ，もしセキュリティ侵害を発見した場合には，発見した内容を管理者へ通報するものである．

現在の侵入検知システムのタイプを入力データによって分類すると，ホスト上のログファイルやその他のファイルからデータを取得して侵入を発見する Host based IDS と，ネットワークを流れるパケットからデータを取得する Network based IDS に分類される[1]．前者については長い歴史があるが，ネットワークの利用が著しく急増した近年，後者の NIDS が脚光を浴びている．NIDS はポートスキャンの有無や，様々なアタック手法の特徴を総合し，一つの検知システムとしたものであり，Host based IDS では防ぎ事のできない攻撃に対しても有効なシステムである．

一方，検出アルゴリズムの観点から IDS を分類すると，不正検知と異常検知の2つに大きく分けられる．前者は，不正な操作や不正な接続に際して発生する特徴情報 (シグネチャ) をあらかじめ登録しておき，このシグネチャと同じものを入力イベント中から検出し，侵入を発見する手法である．後者はシステムやユーザの正常時における振る舞いの傾向をプロファイルデータとしてコンピュータに記憶させ，ユーザの実際の振る舞いがこれと大きく異なる状態を検出することによって侵入を発見する手法である[1]．本稿では，前者の不正検知型の NIDS をとりあげる．ネットワークの能力は年々向上しており，その速度は数十 Gbps が当然となってきている．これにより，従来のソフトウェア実装された NIDS では，ネットワークのすべてのト

ラヒックを監視することがほとんど不可能になりつつある．そのボトルネックとなるのは，ネットワークを流れるすべてのパケットに対して，シグネチャと一致するかを調べるパターンマッチングの部分 (センサー部) である．

文献[2]では，現在の IDS はソフトウェアによる実装のため，最新のプロセッサを用いてもリアルタイム処理できるスループットは 300Mbps であり，現在の 10Gbps のネットワーク速度に対応できないことが示されている．さらにこの文献では，FPGA を用いてセンサー部を実装し，568Mbps のスループットを得ているが，未だ実用段階には達していない．また，パターンマッチングに有限状態機械を用いるため，シグネチャの更新時に FPGA の回路自体から変更しなければならず，専門的な知識を必要とし，回路変更回数に数時間程度必要とする[2]．

3 提案システムの概要

3.1 NIDS の概要

一般的な NIDS はセンサー部，アナライザ部，マネージャー部及び記録からなり，センサー部分において入力されたパケットがシグネチャと一致するかパターンマッチングを行い，マッチングしたならアナライザ部において，それまでの履歴をもちいて分析を行いそれが検知すべき事象かを解析する．マネージャー部において解析の結果をログにして記録に残したり，アナライザ部への警告を行う．図1に一般的な NIDS の構成を示す．

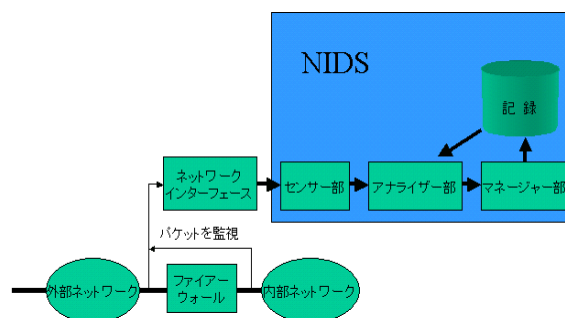


図1 一般的な NIDS の構成

本稿では，NIDS スループットのボトルネックとなるセンサー部に CAM を用いる新たな IDS を提案し，センサー部のスループットの向上を図るとともにシグネチャの更新が容易になることを示す．

3.2 CAM の概要

CAM (Content Addressable Memory) は連想メモリとも呼ばれるデバイスであり，コンテンツテーブルに格納された比較対照データに対し，入力された任意のデータと一致検索を行う．

A proposal of Implementation method for NIDS with CAM
Satoshi Suzuki, Satoshi Nishiyama, Kumaki Takeshi,
Hiroto Kujisaki, Keisuke Iwai, and Takakazu Kurokawa
Department of Computer Science, National Defense Academy

また、これまでの CAM は、入力の一つのものが主であったが、我々はその入力を複数にし、入力のそれぞれに対応する出力を設けるとともに、データマスクもかけられるマルチポート連想メモリ (FMCAM[3], [4]) を開発した。

FMCAM は、コンテンツテーブルを複数の入力で共用し、コンテンツをカテゴリに分類することによって、入力ポート数の増加に対して最大動作周波数が安定する上、ハードウェア資源の使用率が入力ポート数に正比例して大きくならないという特徴を有している。

これらの特徴を活かすことにより、FMCAM を用いてシグネチャのパターンマッチングを行うと、複数の入力を同時に並列処理できるためスループットを向上させられる上、ハードウェア資源も、複数の CAM を同時並行に用いるものと比べて極めて少量で実現できることから IDS のハードウェア実装に適切な利点を有しているといえる。また、データマスクを利用して可変長のシグネチャも検索可能となる。

3.3 CAM の容量の検討

CAM の容量を決定するため、IDS のフリーウェアである Snort[5]を用いてシグネチャについて事前の検討を行った。現在のシグネチャ総数は約 1,800 程度であり、その文字列の長さの平均は 11 程度であった。シグネチャの文字列の長さを調べた結果を図2に示す。

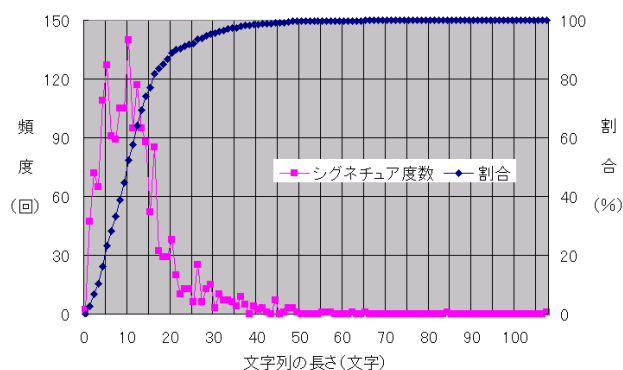
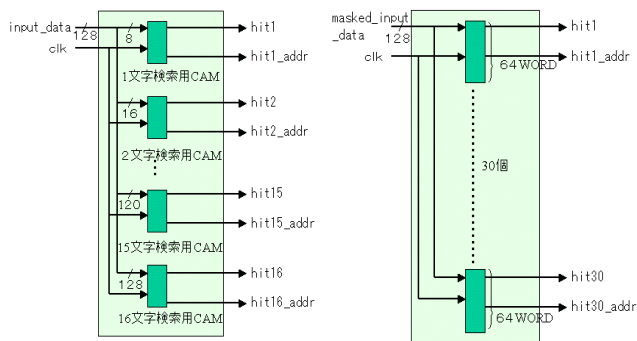


図2 シグネチャの文字列の長さ

図2より、16文字位までのシグネチャに全体の約80%が収まり、また16文字位までは線形にシグネチャ数が増加していくことが分かった。この結果から、CAMのコンテンツテーブル幅を最大16文字(128bit)とした。そのため文字列長が16文字を超えるシグネチャについては、16文字目以降の文字列に対してソフトウェアによるパターンマッチングを行うこととした。

3.4 CAM を用いた IDS センサー部の実装

本稿では、シングルポート入力の CAM を用いた IDS のスループットを検証し、今後 FMCAM を用いたマルチポート化の足掛かりとする。シングルポート入力の IDS のスループットがどの程度になるかを実際に FPGA に実装して調べた。図3に実装した IDS のブロック図を示す。(a)ではシグネチャの文字数ごとの CAM を用意し、並列にパターンマッチングを行う。(b)ではターナリ CAM を使い、入力をマスク化することで可変長のシグネチャについても並列にパターンマッチングを行う。



(a) マスクを用いない場合 (b) マスクを用いた場合

図3 センサー部のブロック図

4 実装結果

今回の実装では、開発ツールとして Xilinx 社の ISE5.0 を利用し、デバイスとして Xilinx 社の Virtex-II xc2v6000 を使用した。回路設計は verilog HDL にて行った。実装した結果を表1に示す。今回の実装結果から、CAM を利用したセンサー部はマスク無しで最大動作周波数 157MHz、マスク有りで 71MHz で動作することが分かった。従ってこのセンサー部のスループットは、1クロックにつき入力を1文字(8ビット)ずつシフトさせつつ処理するため、

マスク無センサー部：157(MHz)×8(bit)=1,256(Mbps)

マスク有センサー部：71(MHz)×8(bit)= 568(Mbps)

となる。従来のソフトウェア及びハードウェア実装によるセンサー部と比べると、スループットが同等若しくは倍程度まで向上している。また、シグネチャを追加更新する際、CAM のコンテンツテーブルを変更するだけでよいので、数十秒程度でシグネチャを容易に更新できる。

表1 実装結果

	マスク無し IDS	マスク有り IDS
最大動作周波数	157MHz	71MHz
スライス数	35,570	146,160

5 おわりに

今回の FPGA を用いた実装結果より、CAM を用いた不正検出型 IDS の高速性とシグネチャを容易に更新することができることを明らかにすることができた。今後、IDS のセンサー部を FMCAM を用いてマルチポート化し、更なる速度向上を目指すとともに、ハードウェア資源の少量化を図る。また、ネットワークインターフェース等を完成させ、実用化を図っていく。

参考文献

- [1] 武田圭史, 磯崎宏, “ネットワーク侵入検知,” SOFT BANK 社, 2000.
- [2] 栗原純, 丹羽雄平, 前田敦司, 山口喜教, “FPGA/ソフトウェア協調処理による侵入検知システムの提案,” 信学技法, CPSY2002-42, pp. 11-16, Aug. 2002.
- [3] 熊木武志, 岩井啓輔, 黒川恭一, “改良型多機能マルチポート CAM の提案,” Forum on Information Technology2002 (FIT2002), 1. 10, pp. 205-206, Sept. 2002.
- [4] T. Kumaki, K. Iwai, T. Kurokawa, “A Proposal of MFMCAM and Its Applications,” Proc. ITC CSCC2002, 1, pp. 224-227, July. 2002.
- [5] M. Roesch. Snort Users Manual. <http://www.snort.org>, 2002.