高速 IDP を実現するコンテンツベース検索エンジンの実装

鈴木 清彦* 竹内 清史* 稲田 徹* 小貫 淳史* 後沢 忍*

三菱電機株式会社 情報技術総合研究所

1. はじめに

近年、ネットワークは、社会インフラとして機能し始め、それに伴い、ネットワークを舞台としたテロや犯罪行為が急増している。これらの行為の対策として、不正侵入の検知と同時に不正侵入パケットそのものを遮断する IDP(侵入検知/遮断装置)を導入するケースが増えている。IDP は、その特性上、ネットワークの中間に位置するため、通常のネットワークトラフィックに影響を与えない、非常に高速な検知が必要とされる。我々は Gigabit Ethernet 上で動作する高速な IDP を実現するために、必要な機能の全てを H/W により実現した。他方、IDP ではコンテンツへの柔軟な処理が要求される。

本稿では、H/W の高速さを生かしながら、柔軟なコンテンツ処理を実現する手法について提案する。

2. コンテンツ検索高速化の課題

複数の IP パケットとしてネットワークを流れているデータが不正なものであるか判断するためには、それら IP パケットを、到達点において特定の意味をなす情報 (コンテンツ)に直し、その後に解析を行い判断する必要がある。

一般的なその手順は以下のようになる。

０)パケットデータのリアセンブル
１) コンテンツへの整形
２) データ検索
３) アラートの処理

本項では上記１)～３)について述べる。

２．１ コンテンツへの整形

複数のパケットにより構成されたあるデータは、整形処理されて始めてコンテンツとなる。

例えば、組みあがった文字列データがバックスペース（以下[BS]）を含む場合、S/W による処理では一度メモリに全て保存した後、バイト単位で[BS]による文字消去処理を実行しなければならない。今回の高速 IDP では 1Gbps を目標とする。動作周波数を 100MHz と設定しても、バイト単位の処理ではスループットは 800Mbps となり、S/W の処理をそのまま用いることは性能上採用できない。

```
a  b  c  d  e  f  g  h                    a b c d e f g h
i  j  (k) (l) (m) (n) (o) (p)              i j w x z A B C
(q) [BS][BS] (r) (s) [BS][BS] (t)     →    D E F G H I [CR][LF]
(u) (v) [BS][BS][BS][BS][BS][BS]
[BS][BS] w  x  (y) [BS] z  A
B  C  D  E  F  G [CR][LF]
```

図１：バックスペースを含むデータの整形処理
（(X)は[BS]によって消去される文字 X を表す）

２．２ データ検索

コンテンツからの不正データ検知を H/W により行ういくつかの従来法が存在する。しかしながら、いずれの場合においても、今回要求される性能を満たしてはいない。

フリーソフトウェアである Snort[1]と同様の検索方式[2]を FPGA に実装した方法[3]では、有限状態機械を用いて検索を行う。ルール毎に有限状態機械を構成するため、現実的な論理量で実用レベルのルール数を登録するのは不可能である。またスループットはルール数の増加とともに減少し、試験的なルール数においてもスループットは 568Mbps であったことが報告されている。また CAM を並列に用いる方法[4]では、検知可能な最長パターンが 16byte に制限されている。実利用を考慮した設定において、こちらも 568Mbps と報告されている。

２．３ アラートの処理

コンテンツ内に不正なパターンを検知した場合、検索エンジンはアラートを作成する必要がある。これは上位処理部が統計的性質などの、より詳細な解析を行うためである。アラートは複数のパケットがリアセンブルされ整形されたコンテンツと検索結果から成る。そのデータ量は TCP のフレームサイズに依存するため一般に膨大となる。他方、IDP はパケットを遮断するためにも、このアラートが必要となる。

性能に対する要求を満足するためには、高速遮断を妨げることなく、これら大量のアラートを適切に処理できなければならない。

3. 提案するコンテンツ検索実装方式

H/W により構成されたコンテンツベース検索エン

“Implementation of contents-base search engine in the Gigabit IDP system”

*Kiyohiko SUZUKI, Kiyohumi TAKEUCHI, Toru INADA, Atsushi ONUKI and Shinobu USHIROZAWA
Information Technology R&D Center, Mitsubishi Electric Corporation

ジンを提案する。その機能は以下の 3 点である。

1) 高速な整形処理の実装
2) 検索専用 LSI の並列実行
3) 遮断用コマンドの作成

３．１ 高速な整形処理の実装

本エンジンは１ワード＝32bit で設計し、50MHz の周波数で動作する。

本 IDP の整形処理部では、[BS]による文字消去処理のみならず、重複スペースの単一化処理、エスケープ文字のデコードが行われる。本来バイト処理が要求されるこれらデータ整形処理は、本 IDP において全て単一のアーキテクチャに基づいて設計された。

考案したアーキテクチャは、与えられたデータの整形処理をワード単位のストリームで処理することを可能とした。1 サイクル毎に 32bit を処理することが可能となり、整形処理において 1.6Gbps を達成した。

３．２ 検索専用 LSI の並列実行

要求される性能を満足するため、本検索エンジンではコンテンツの検索に、最大スループットが 1.6Gbps の専用 LSI を用いた。

検索エンジンが不正データを検出する時、検索対象はヘッダ情報とコンテンツに大別される。コンテンツが小さい場合はヘッダ情報の検索が、コンテンツが大きい場合はその検索が、それぞれ性能を左右する要因となる。そこで本方式では、ヘッダ情報とコンテンツをそれぞれ検索する 2 石の LSI を用い、これらを並列に動作させ、得られた結果の突合せから不正な内容であったかを判断している。

３．３ 遮断用コマンドの作成

不正を検知した際、上位処理部へ通知するアラートは各レイヤにおけるヘッダ情報やコンテンツを含むが、IDP が高速遮断を実現するための情報はごく限られた内容で十分である。そこで、同一のリアセンブル単位となる IP パケットについて、装置内では同一のデータ ID を付加する。一方検索エンジンは、アラート作成時に上位処理部へ通知するアラートとは別に、{データ ID,遮断/透過}の情報のみを持つ遮断用コマンドをアラート情報から作成する。このコマンドをアラートとは別のパスを通すことで、上位処理部へ通知するアラートに妨げられることなく、高速な通信の遮断を実現した。

4. シミュレーションによる評価

設計されたコンテンツベース検索エンジンは FPGA(Field Programmable Gate Array)により実装した。その論理の動作検証には論理シミュレータを用いた。

シミュレーション結果から、提案する本検索エンジンが検索対象コンテンツの整形処理を１ワード１サイクルで実現できることを確認した。また、アラートとは別に遮断用コマンドを作成し別パスを通すことで、遮断に特化した情報が上位処理部へのアラート送信に妨げられることなく処理され、要求される性能を満足して遮断が行われることを確認した。

5. おわりに

我々は 1Gbps の通信路において不正パケットを検知、遮断する高速 IDP を開発した。本 IDP は性能についての要求を満足するため、必要な機能の全てを H/W により実現した。本稿では、高速なコンテンツベース検索エンジンを H/W により実現する方式を確立し、これを実装した。

提案する検索エンジンの実装方式では、本来バイト単位の処理が求められるデータの整形処理をワード単位で実現でき、データの整形処理において 1.6Gbps を達成した。またアラートとは別に、遮断用コマンドを作成することで、上位処理部への膨大なアラートの送信に妨げられることなく高速な遮断を実現した。

今回は、要求される性能を満足するために、IDP に必要な機能の全てを H/W により実現した。しかし、H/W による設計は、一度設計した後に変更することが困難であるという問題を含んでいる。他方、近年では CPU を内部に含む FPGA が登場した。IDP に要求される機能を見直し、H/W と S/W の有効な協調処理方式を検討することが今後の課題である。

参考文献

[1] Snort: The Open Source Network Intrusion Detection System, http://www.snort.org .

[2] A.V.Aho and M.J.Corasick, “Efficient string an aid to bibliographic search,” Communications of the ACM, Vol.18, No.6, pp.333-340, 1975.

[3] 栗原純・丹羽雄平　他, “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,”信学技報, CPSY2002-42, pp.11-16, Aug.2002.

[4] 鈴木　論司・西山怜　他, “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,”情報処理学会第 65 回全国大会, Vol.3, pp.555-556, Mar.2003.