IDP における TCP 再構築処理の高速実装

竹内 清史† 稲田 徹† 鈴木 清彦† 小貫 淳史† 後沢 忍†

三菱電機(株)情報技術総合研究所†

1. はじめに

インターネットの普及につれ、様々なネットワーク犯罪が増加している現在、IDS（Intrusion Detection System), IDP（Intrusion Detection and Prevention System）が不正アクセスに対抗するネットワークセキュリティ装置として導入され始めている。IDP は不正アクセスの有無を検知すると同時にこれを遮断する機能を持つ。我々は、現在、普及し始めた 1G イーサネットに対応するため、パケットの受信から、コンテンツの検索までを全て H/W で行う IDP を開発した。本稿では IDP の TCP 再構築処理において、メモリの使用量を抑えて、高速に処理する H/W 実装方式を提案する。

2. 既存システムの概要と課題

一般にネットワークプロセッサも含めた CPU による S/W 実装で IP および TCP 再構築を実現した場合、ショートパケットも含め 1Gbps スループットで不正パケットの検知および遮断を実現するのは性能上困難である。この解決策として我々は H/W 実装を採用した。

一方で IDP は、全ての通過パケットに対してコンテンツ検索を行うため、潜在的に多くのメモリを必要とし、メモリ使用量の削減が課題として挙げられる。特に TCP 再構築処理では、セッションごとに Window Size 分の組立て用バッファを用意した場合には 64Mbyte といった大容量のメモリを必要とする（Window Size を 64Kbyte、組立て可能セッション数を 1024 個とした場合)。

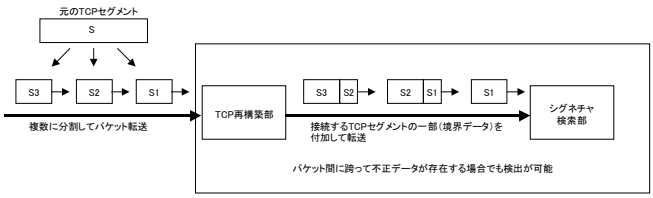
本稿で提案する TCP 再構築処理方式は、4 Mbyte のメモリ容量で実装可能な方式である。次項よりメモリの使用量を抑えて高速に実装する方式を述べる。

3. 提案システムの概要

IDP における TCP 再構築処理の目的は、パケットを跨る攻撃パターンを正確に検出することにある。提案方式では、パケット受信ごとに TCP セグメントに接続する他パケットのセグメントの境界にあたるデータ（以下、境界データと記述）を付加してシグネチャ検索に転送することでこれを実現する。図１に処理の例を示す。

図１. TCP 再構築処理例

この方式は CAM と SRAM を使用して、以下の方法



で実装する。

① 受信パケットのアドレスと TCP シーケンス番号から、これに接続する受信済みパケットを CAM で検索する。

② 接続パケットが無く、受信 TCP セグメントサイズが一定サイズ（今回の実装では 384 byte）未満の場合は SRAM に保持し、シグネチャ検索に転送しない。

③ 接続パケットが無く、受信 TCP セグメントサイズが一定サイズ以上の場合は受信 TCP セグメントの境界データ 192byte 分のみを SRAM にコピーし、受信 TCP セグメント全体をシグネチャ検索に転送する。

④ 接続パケットがあり、接続後の合計サイズが一定サイズ未満の場合は SRAM で組み立てて保持する。

⑤ 接続パケットがあり、接続後の合計サイズが一定サイズ以上となる場合は接続パケットを SRAM から読み出し、組立て後のセグメントをシグネチャ検索に転送する。このとき、組立て後セグメントの境界データを SRAM にコピーしておく（エントリは増やさず上書きする)。

図２に提案する TCP 再構築処理フローのブロック構成を示す。

Implementation of the TCP reassemble in IDP
Kiyofumi TAKEUCHI Toru INADA, Kiyohiko SUZUKI, Atsushi ONUKI, Shinobu USHIROZAWA,
Information Technoloty R & D Center, Mitsubishi Electric Corporation

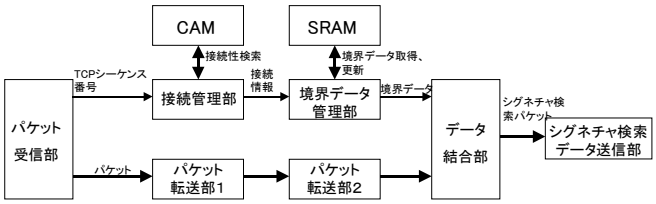


図 2 . TCP 再構築処理フロー

接続管理部では上記フロー①の処理を、境界データ管理部では上記フロー②, ③, ④, ⑤の処理を行う。

ここで、パケット受信ごとに付加する境界データについては、シグネチャ検索に 2 度転送するため、この部分はオーバーヘッドとなり、帯域の圧迫及び処理量の増加要因となる。しかし、一定サイズ以下のパケットを受信した場合は SRAM で組立てを行うため、転送時のオーバーヘッドとなるデータ量を少なくすることが可能となる。

提案方式では、境界データの管理と一定サイズまでの組立てのため 1 エントリあたり 1.1 Kbyte 必要とし、SRAM の容量 4 Mbyte では約 3600 エントリ分の連結データが受信可能である。また、セッションごとにバッファエリアを区切らないため、セッション数に依存せずメモリを有効に使用することが可能である。

4. 性能見積もり

我々は IDP における TCP 再構築処理とシグネチャ検索処理を FPGA で実装した。本稿で提案する TCP 再構築処理は Xilinx 社の XC2V6000 –5 で実装している。また、CAM は NETLOGIC 社の NSE3128-66 を、SRAM は IDT 社の IDT71V416S10PH を使用した。

提案方式の実装にあたり、性能を見積もり、シミュレーションにて実現性を確認した結果を以下に記述する。

4.1 接続管理部の性能

接続管理部による CAM アクセスは TCP セグメント長に依存しないため、ショートフレームのワイヤーレートから逆算した時間 672ns が処理許容時間であり、一番厳しいケースとなる。動作周波数 50MHz で CAM アクセスを行った場合、新規セグメント登録、接続検索及びエントリの更新処理が目標性能を満たすことをシミュレーションで確認した。

4.2 境界データ管理部の性能

境界データ管理部による SRAM アクセスは、ショートフレーム受信時に TCP 構築サイズが一定サイズを超えて SRAM からセグメントをリードする場合が、許容時間内の処理の達成が一番厳しい条件となる。設定する構築サイズは小さいほど SRAM アクセスとしては処理が軽くなるが、構築サイズ以上のパケットを受信したときは毎回シグネチャ検索に送信され、転送時にオーバーヘッドとなる境界データの割合が大きくなるため、構築サイズは大きいことが望ましい。

SRAM アクセスデータ幅 128bit, 動作周波数 50MHz においては、16 byte × 33 サイクル（660ns）が処理許容時間における限界転送サイズとなるが、その他の処理のオーバーヘッド時間を考慮し、実装では最大転送サイクル数を 24 サイクルとし、構築上限サイズは 384 byte にとして実装している。

4.3 帯域について

今回の実装においてデータ転送帯域は 1.6Gbps（32bit@50MHz）としている。提案方式ではパケットごとに付加される境界データがオーバーヘッドとなり帯域を圧迫するため、境界データのサイズと受信 TCP セグメントサイズの組み合わせ次第で帯域が足りなくなる場合がある。今回の実装では境界データサイズを現時点での文字列検索の最大サイズである 192 byte とした場合、受信 TCP セグメントサイズが 192～213 byte において 1Gbps での実装は不可能であることが判明した。今回の実装では境界データサイズを 161byte 以下とすれば 1Gbps を満たす計算であり、もしくは帯域を 2Gbps 程度に増加すれば境界データが 192byte の場合でも十分実装が可能である。

5.おわりに

IDP の H/W 実装において、提案した TCP 再構築処理が目標性能を満たすことが可能であることを示した。今後は実ネットの環境で 1Gbps の性能を確認する計画である。

6.参考文献

[1] Norimitsu NAGASHIMA : “A study of packet reassembly method in Intrusion Detection and Prevention System”,APSITT 2003, pp.133-138, Nor.2003.

[2] 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.

[3] **澤川 渡**, **網島 明浩** : “TCP/IP **解析とソケットプログラミング**”,**オーム社**,Feb.2000.