

要 旨

データ駆動型ファイアウォールにおける TCP パケット処理の 並列実現法

嶋田 栄悟

インターネットが普及したことにより、不正アクセスや悪意のある侵入、ネットワークウィルスなどの検出方法として、ネットワークセキュリティが非常に重要視されている。様々なネットワークセキュリティの中で、ファイアウォールが一般的に利用されている。

誰にでも知られているように、ネットワークでは最大転送単位 (MTU) が設定されており、そのサイズを超えるパケットは複数パケットに分割されてネットワーク上に送信される。

そのためファイアウォールなどのネットワークセキュリティでは、分割されたことによって、シグナチャマッチングなどの機能で、不正パケットが検出できないというミスをなくすために、分割されたパケットを再構築する必要がある。

本稿では、TCP リアセンブル処理への応用実装を視野に入れて、データ駆動処理方式を用いて IP パケットの再構成処理である IP デフラグメント処理の並列実現法の検討と実装ならびに性能評価を行った。

性能評価の結果、259 IPPacket/sec の性能が確認できた。また再構築時のデータ格納処理の処理速度のボトルネックが課題であるということを確認した。

キーワード データ駆動型プロセッサ、データ駆動型ファイアウォール、パターンマッチング、IP デフラグメント、TCP リアセンブル、MTU

Abstract

Parallel Implementation of TCP Processing on Data-Driven Firewall Processor

Eigo Shimada

With the prevalence of Internet, the network security is becoming an important aspect which should be considered in order to keep the network off numerous unauthorized access, malicious intrusion, network virus and so on. Among the exiting security products, firewall system is popular. My work is based on the TCP processing module of an embedded data-driven firewall processor. As we all know, because of the length limitation of IP packet and the maximum transition unit (MTU) of link layer, longer TCP/IP packets will be fragmented when they pass through the network. As far as the TCP processing module of a firewall system is concerned, a IP defragment and TCP reassemble processing of the fragmented packets is required before they pass through other packet content analysis modules such as signature matching so that no malicious signature which spans two fragments would be ignored. As for the increasing bandwidth of network, a high processing speed is also important. In my previous work, a parallel implementation of IP defragment module and its evaluation on the data-driven network processor (DDNP) board are accomplished. The evaluation result shows that the performance gets to 259 IPPacket/sec.

key words Date Driven Processor, Date Driven Firewall Processor, Pattern Matching, IPdefragment, TCPreassemble, MTU