審 査 の 結 果 の 要 旨

氏　　名　　菅原　豊

インターネットにおける侵入検知システム(Intrusion Detection System, IDS)ではパケットのペイロード解析を必要とする。ペイロード解析法の一つである厳密文字列照合をTCPストリームに対して行う場合、パケット毎の照合と異なり (1)ストリーム毎の照合途中経過の保存、(2)パケット落ちへの対応、(3)一貫性の無い再送への対応、の3つの処理が必要である。本論文ではこれらの処理をFPGAハードウェアで実現するための新しい手法を提案し評価した。

限られたハードウェア資源下では、ストリーム毎の照合途中経過の保存状態数を少なくする必要がある。このために照合ステートビット数を減らすための文字列照合法として、本論文では、Suffix Based Traversing(SBT)法を提案した。本方式は複数文字並列処理による高速化が可能で、なおかつステートビット数がO(log ルール文字列合計長)で抑えられる初めての方式である。合計文字数1000のルールに対してステートビット数が既存方式であるDFA(Deterministic Finite Automaton)法の1/15に抑えられることを示した。ユーザが定義するルール文字列から自動生成器により回路が自動生成される。ユーザは、ルール文字列を記述するだけで本システムを利用することが可能となる。このように単なる手法の提案にとどまらず実用的なシステムを実現した。

本論文では、さらに、パケット落ちに対応する方式として双方向検査法を提案した。本検査法の特徴は、パケット間にまたがるパターンをパケット到着順に依らず文字列照合を可能としていることである。このために、本手法では、文字列照合のためのオクテット列走査をシーケンス番号の昇順に対し順方向だけではなく逆方向にも行う。

一貫性の無い再送パケットへの対応方式としてパケットフィンガープリントを提案した。再送パケットに一貫性があるかを厳密にチェックのためには、最初に送信されたパケットデータを全て保存しておく必要があるためメモリ使用量が増大する。パケットフィンガープリント方式では情報理論的に最も精度が高い方式であるハッシュ値を用いた近似検査を行う。

SBT法の実装では、Xilinx社のXC2V6000FPGA(6Mゲート、RAM324KB)において32オクテットの並列処理を実現し、32Gbpsの照合スループットを達成した。また、本論文で提案している３つの方式をXilinx社のXC2VP50(5Mゲート、RAM 522KB) FPGAを用いて評価した。ルールの合計サイズは約1000、パケットフィンガープリントのハッシュ値を64ビットとし、最大13.1Gbps、最小11.2Gbpsのパケット処理速度を達成できることを実証した。

本研究では、現在および将来の高速ネットワークに対するTCPレベル文字列照合器を実用的なメモリ量で実装可能にし、かつ、再送一貫性の検査を可能にした。SBT法は既存方式では不可能だった複数文字の並列処理とステートビット数抑制を両立した。双方向検査法はパケット落ちに対処する際に必要なパケットバッファリング量を抑制した。パケットフィンガープリントはハードウェア方式で初めて一貫性の無い再送へ対処し、同時に使用メモリ量を抑えた。このようにインターネットワークにおいて重要性が高まっている侵入検知システムにおいて、その実現における最も重要な要素技術である文字列照合器のハードウェア化に対して、実現課題を体系的にまとめ、かつ、新しい実現手法を提案し評価しており、当該分野に顕著なる貢献を行った。よって本論文は博士（情報理工学）の学位請求論文として合格と認められる。