論文の内容の要旨

論文題目

HIGH-SPEED STRING MATCHING METHOD FOR MULTI-STREAM PACKET SCANNING SYSTEMS

(マルチストリームパケット検査機構向け高速文字列照合手法)

氏名　菅原　豊

近年、インターネットは急速に普及し、生活にとって不可欠なインフラストラクチャの一つとなりつつある。それに伴い、ネットワーク経由の攻撃や情報漏洩等の被害が与える影響は増大しており、これらのセキュリティ脅威を阻止する事の重要性が増している。NIDS はネットワークを流れるデータを検査し、これらのセキュリティ脅威を検知するシステムであり、ネットワークの安全性を守る有効な方法の一つである。実際、攻撃者は対象サイトに NIDS が存在するか否かを調べ、存在する場合は攻撃の対象から外す傾向があるというデータが公開されている。

NIDS では、攻撃を確実に発見できる事が重要である。なぜなら、一部の条件下で攻撃が発見できない場合、攻撃者は意図的にその条件を作り出し、NIDS をすり抜けるからである。最低でも、攻撃を発見できない条件を攻撃者が意図的に成立させる事が可能であってはならない。

収集したネットワークデータの検査方法は、シグネチャ方式とアノーマリ方式に大きく分けられる。シグネチャ方式では、セキュリティ脅威に関わるパケットを、その中に含まれる特定のオクテットパターンを探索する事により発見する。一方、アノーマリ方式では、ネットワークの異常な振る舞いから間接的にセキュリティ脅威を検出する。シグネチャ方式は登録外の攻撃は発見できないが、登録された攻撃は確実に発見可能である。一方、アノーマリ方式は未知の攻撃を発見可能であるが、現状では一部の攻撃は見逃される。前述のように NIDS では攻撃を確実に発見できる事が重要である。そのため、snort 等の多くの実用 NIDS は、シグネチャ方式を単体もしくは他方式との組み合わせで使用している。そのような背景から、本論文ではシグネチャ方式について議論を行う。

シグネチャ方式では、攻撃を確実に発見するために各パケットではなく TCP ストリームのレベルでパターン探索を行う事が重要である。なぜなら、パケット毎に検査を行う場合、パケット分割の手法により NIDS をすり抜けることが可能になるからである。同時に、NIDS を各ホストではなく、バックボーンネットワークに配置して検査を行う事が求められる。なぜなら、特に大学や大企業等の大規模ネットワークにおいては全てのホストに NIDS を導入・管理する事は実用上困難であるが、バックボーンでの一括管理方式であれば導入・管理を行う事が容易なためである。そのため、パターン探索機構には近年の 10Gbps に達するバックボーンネットワークに対応するスループットが必要である。

10Gbps で TCP レベルのパターン検査を行う場合、速度の点からソフトウェアではなくハードウェア方式が必要である。しかし、TCP レベルでの検査を行うには(1)TCP 毎の照合状態を切り替えるオーバーヘッドを抑え、かつ(2)大部分のパケットはバッファリング無しでパケット落ちと順序交換に対応できる事、が求められる。(2)は、バックボーンネットワークでは多数の TCP ストリームを対象に検査を行う必要があり、全てのパケットをバッファリングする事は性能上困難なためである。また、パケットをバッファリングしないため、パケットを到着順に処理する必要があり、ストリーム間の状態切り替えを高速で行う必要があり(1)必要となる。

本研究では、(1)と(2)の両方を達成可能な FPGA ベースのパターン照合方式を提案する。FPGA を用いる理由は、再構成によりルールを変更可能にしつつソフトウェアよりも高いスループットを実現するためである。(1)を満たす照合方式として Suffix Based Traversing (SBT)法を、(2)に対応する方式としてパケットシグネチャ付き双方向検査方式を提案する。

SBT 法は Aho-Corasick アルゴリズム法の拡張である。状態ビット数が従来方式と比較して少なく、結果として軽量のストリーム切り替えが可能である。また、SBT 法では複数文字を並列に処理できるため、高いスループットを達成可能である。我々は、与えられたルールから SBT 文字列照合機構の VHDL 記述を自動的に生成する変換器を実装した。また、出力された SBT 照合機構の評価を行った。Xilinx XC2V6000-6 FPGA を用いた場合、1000 文字のルールに対して 32Gbps、2000 文字のルールに対して 14Gbps を達成した。ステートのビット数は典型的な場合 20 ビット、最大 24 ビットであった。その結果、オーバーヘッドクロック無しでのストリーム切り替えを実現した。

双方向検査方式は、正順 SBT 機構と逆順 SBT 機構という 2 つの SBT 機構をパケット検査に用いる。正順 SBT 機構は元のルール文字列を検出し、逆順 SBT 機構はルール文字列を反転させたものを検出する。この 2 つを組み合わせる事により、高々パケットにまたがるパターンはバッファリング無しで発見可能である。そのため、パケットが最長のルール文字列よりも長い限場合はバッファリング不要であり、結果としてバッファリング量を削減できる。また、一回目の送信と異なる内容のパケットを再送して正常な検査を妨げるという攻撃を防ぐためにパケットシグネチャというハッシュを用いる。

SBT 法と双方向検査、パケットシグネチャを組み合わせた方式で TCP ストリームレベルでのパターンマッチ機構を Xilinx XC2VP70-5 FPGA を用いた NIC 向けに製作した。1000 文字のルールを使用し、バッファリングが行われない場合について評価を行った。動作クロック速度から計算した結果、順序交換が無い場合で 13.1Gbps、パケット落ち、順序交換がある場合で 11.2Gbps を実現できる事が分かった。