平成26年度 情報工学コース卒業研究報告要旨

高倉 研究室	氏　　名	淵 上　智 史
卒業研究題目	オンボードメモリを活用するFPGAを用いたTCPセッション特徴量抽出手法	

ゼロデイ攻撃を始めとする巧妙な攻撃の増加が問題となっている。特に、TCPプロトコルは様々なサイバー攻撃に利用されることが多い。TCPでの通信は複数パケットで成立するため、TCPの通常通信にまぎれる未知攻撃検知を目的とするアノマリ型IDSにおいては、パケット単位ではなくセッション単位の特徴量に着目したトラフィックの監視と分析が期待されている。そのうえ、インターネットトラフィック量は今後も継続的に増加していくと予測されており、アノマリ型IDSにはより高いスループットでの処理能力が求められる。

そこで本研究では、アノマリ型IDSのスループット向上を目的として、FPGAを用いてTCPセッション単位の特徴量抽出手法の提案と開発を行った（図1）。抽出する特徴量はIPアドレス、ポート番号、パケット数、ペイロードサイズ、ペイロード特徴量などである。提案構成では、FPGAボードに備えられているイーサネットポートからパケットを受信して特徴量を抽出する（図1(a)）。セッション単位の特徴量抽出処理の実現において、セッション継続中に特徴量を一時的に記憶しておく必要がある。高スループットを実現できるバッファとして、FPGA内のブロックRAMの利用が考えられる。しかし、ブロックRAMの容量は目標とするスループットを実現するためには大幅に不足するため、本手法ではFPGAに接続されたTCAMとDRAMを活用する。提案手法の実装では、TCPセッション開始時にTCAMとDRAM上にセッション特徴量を記憶するためのエントリを作成し（図1(b)）、セッションが持続している間は一連の受信パケットから逐次的に特徴量を抽出して積算する（図1(c)）。TCAM/DRAMエントリのアクセス方法については、TCPヘッダの情報から生成する検索キーを用いてTCAMのエントリを検索し（図1(d)）、それに記載されているDRAMアドレスをもとに計算途中の特徴量にアクセスする（図1(e)）。セッション終了時には抽出した特徴量をアノマリ検知処理が実行される汎用サーバに出力し、エントリを削除する（図1(f)）。

本研究では図1に示すシステムの特徴量抽出回路部の実装と論理合成を行い、抽出処理が可能なスループットの見積もりを行った。今後の課題として、実トラフィックにおけるシステムの性能評価を行う必要が挙げられる。更に、より高いスループットのネットワーク環境に対応させるために、抽出処理のボトルネックとなっているFPGA/DRAMのデータ通信量を抑える改良を行う予定である。

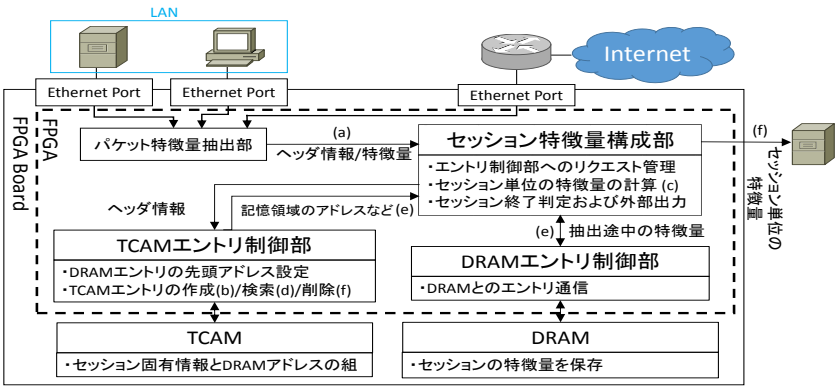

図1：TCPセッション特徴量抽出システム