5X-03

オンボードメモリを活用するFPGAを用いたTCPセッション再構成手法

淵上 智史† 嶋田 創†† 山口由紀子†† 高倉 弘喜††
†名古屋大学工学部電気電子情報工学科 ††名古屋大学情報基盤センター

1 はじめに

サイバー攻撃が巧妙化する現代において、ネットワークトラフィック監視による侵入の早期検知が重要である。しかしながら、増加するトラフィックにより IDS（侵入検知装置）の負荷は増える傾向にある。そこで、IDS に再構成可能ハードウェアである FPGA を用いる研究が行われている。シグネチャ型 IDS の研究では、FPGA 上でパケットのパターンマッチングを行い、検出した不正通信をブロックする手法が提案されている [1]。

一方、我々は、未知攻撃の早期検知を目的とするアノマリ型 IDS の性能向上のため、FPGA に TCP セッション単位の特徴量を抽出させ、外部の汎用サーバでアノマリ検知処理を行う IDS の研究を行っている [2]。しかしながら、セッション特徴量の保存に容量が少ない FPGA 内のブロック RAM を用いており、長時間にわたるセッションや、同時に存在する多数のセッションの特徴量抽出には適さないという問題点があった。

そこで、本研究では FPGA に接続されたオンボード DRAM/TCAM に抽出途中のセッション特徴量を保存することで、長時間かつ、より多数のセッションに対応可能とする手法を提案する。

2 提案システム

2.1 システム構成と機能

提案システムの実装には Altera 社の FPGA Stratix V GX を搭載した FPGA ボードを用いる。このボードに存在している SFP+スロットのうち、L2 スイッチの機能が実装されている 8 ポートを 1000BASE モードで用いてパケットを受信する。ボードには 18byte × 128K のエントリ数に設定された TCAM 8 個（総容量 18MB）と DDR3-1600 SDRAM（総容量 16GB）がそれぞれデュアルチャネルで接続されている。

提案手法では、TCP パケットのみを対象とし、受信したパケットごとにヘッダ情報とペイロード特徴量を抽出する。ヘッダ情報は、ペイロードサイズとセッションを特定するための宛先/送信元 IP アドレスおよびポート番号である。ペイロード特徴量については、byte 単位での 1-gram 特徴量であり、ペイロードの各バイトの値（0-255）のヒストグラムである。検出処理を行う汎用サーバに渡すセッション特徴量を構成するため、セッション開始から終了までのパケットから以下のデータを生成する。

- IP アドレス : C(クライアント) / S(サーバ)
- ポート番号 : C / S
- パケット数 : 通信方向別の総数
- ペイロード量 : 通信方向別の総量
- 1-gram 特徴量 : 通信方向別の総和
- 終了状態情報 : 出力時のセッションの状態

セッションが終了した場合、またはバッファ容量不足により積算を中断する場合これらのセッション特徴量を出力する。終了状態情報は、正常終了（FIN）、強制切断（RST）、積算中断という 3 状態を表す。

2.2 データ構造

1 セッションに対して、TCAM と DRAM にそれぞれ 1 エントリ分の固定長領域を割り当てる。新規セッションが開始されるとエントリを作成し、セッションが終了するとエントリを削除する。各エントリの内容は次の通りである。

TCAM エントリ

IPaddr_Low(4byte) , IPaddr_Low-port(2byte) ,
IPaddr_High(4byte) ,IPaddr_High-port(2byte),
IsIPaddr_High_Server(1byte), DRAMaddr(4byte)

DRAM エントリ

1-gram 特徴量 (1024byte × 2), パケット数 (4byte × 2) , ペイロード量 (4byte × 2), 接続状態情報 (1byte)

双方向の通信に対して TCAM のエントリを 1 エントリにまとめて検索回数を 1 回に抑えるために、各フィールドを IP アドレスの大小の順に記憶する。IP アドレスを 32bit 符号なし整数とみなして比較し、小さい方を IPaddr_Low とし、そのホストのポート番号を IPaddr_Low-port とする。他方の IP アドレスとポート番号については、IPaddr_High、IPaddr_High-port となる。

TCP Session Reconstruction by FPGA utilizing Onboard Memory
Satoshi FUCHIGAMI† Hajime SHIMADA†† Yukiko YAMAGUCHI†† Hiroki TAKAKURA††
†Department of Information Engineering,School of Engineering, Nagoya University
††Information Technology Center, Nagoya University

IPaddr_Low、IPaddr_Low-port、IPaddr_High、IPaddr_High-port を合わせて TCAM エントリの検索キーとする。IPaddr_Low、IPaddr_High のうちどちらがサーバ側か示すため、IsIPaddr_High_Server フィールドを用意する。DRAMaddr 項目は、当該セッションの DRAM 上のエントリの先頭 DRAM アドレスである。

DRAM には積算中の特徴量を通信方向別に保存しておく。また、TCP セッションの状態遷移を把握するために、接続状態情報フィールドに記録しておく。

2.3 動作

パケット入力時のシステム全体の動作を図 1 に示す。図の点線内のブロックは FPGA に実装する回路モジュールであり、破線矢印は制御の流れ、実線矢印はデータの流れを示す。受信したパケットからヘッダ情報、TCP フラグ、ヘッダ特徴量、ペイロードを抽出する（図 1(1)）。ペイロードは 1-gram 特徴量計算部に送られ、1-gram 特徴量を計算する。これらの情報を用いて TCAM/DRAM アクセスを行うが、複数サイクルかかる TCAM/DRAM アクセスを待つために、ヘッダ情報、TCP フラグ、ヘッダ特徴量、1-gram 特徴量の組を一旦バッファ制御部で保存する（図 1(2)）。TCAM 制御部ではヘッダ情報をキーとして TCAM の検索を行う（図 1(3)）。エントリが存在せず、かつ、SYN フラグのみが有効なパケットであれば新規セッションとみなして TCAM/DRAM に新規エントリを作成する（図 1(4a),(5a)）。マッチするエントリが存在する場合は同一セッションで積算中のセッション特徴量が存在するため、マッチしたエントリの DRAMaddr を読み出すとともに、IsIPaddr_High_Server フィールドをもとにサーバの IP アドレスを求めて宛先 IP アドレスと比較して通信方向を判定し、バッファ制御部の通信方向、DRAM アドレスフィールドに書き込む（図 1(4b)）。その後、バッファ制御部にある DRAM アドレスを DRAM 制御部に送信して、DRAM から積算中のセッション特徴量を読み出す（図 1(5b)）。読み出された積算中のセッション特徴量に対して受信パケットの 1-gram 特徴量、パケット数、ペイロードサイズを加算し、TCP セッションの状態情報を更新する（図 1(6)）。この時、接続状態をもとにセッションの終了を判断する（図 1(7)）。セッションが終了していなければ、DRAM に更新された特徴量と状態を書き込む（図 1(8a)）。セッションが終了した場合、2.1 節に示した項目を出力してそのセッションに対応する TCAM エントリを削除する（図 1(8b)）。

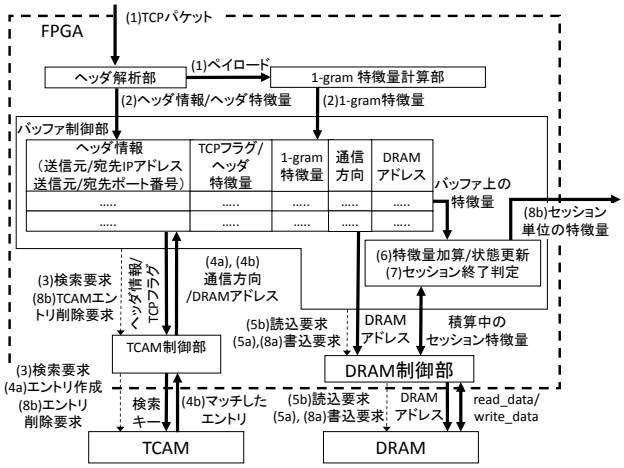

図 1: パケット入力時の動作

3 従来手法との比較

FPGA 内のブロック RAM で特徴量を保存する場合、1 TCP セッションあたりのエントリサイズは 2,082 byte が必要となる。従来では FPGA 内のメモリブロックがおよそ 5.675Mbyte 余っているため、最大 2,725 個のエントリを保持できるという計算になる。

提案手法では保持できるエントリ数は TCAM に保持できるエントリ数に等しい。各 TCAM を 1 エントリあたり 18byte であるので、TCAM1 個が 128K エントリ、8 個で 1,024K エントリとなる。よって、保持可能なセッション数はおよそ 102 万セッションとなり、従来手法に比べて同時に 375 倍以上の数の TCP セッションが扱える。

4 おわりに

FPGA 上のオンボードメモリを利用した、アノマリ検知のための TCP セッションの特徴量を抽出する手法について提案した。今後は、実装と性能評価を行う。さらに、複数の TCP セッションにまたがる特徴量を抽出できるようにシステムの改良を行う予定である。

参考文献

[1] T. KATASHITA, Y. YAMAGUCHI, A. MAEDA, and K. TODA. FPGA-based intrusion detection system for 10 gigabit ethernet. *IEICE transactions on information and systems*, 90(12):1923–1931, 2007.

[2] S. YANASE, H. SHIMADA, Y. YAMAGUCHI, and H. TAKAKURA. Network access control by FPGA-based network switch using HW/SW cooperated IDS. 信学技報, 114(286):91–96, 2014.