(12) **BẢN MÔ TẢ GIẢI PHÁP HỮU ÍCH THUỘC BẰNG ĐỘC QUYỀN**
GIẢI PHÁP HỮU ÍCH

(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ

(11) **2-0003177**

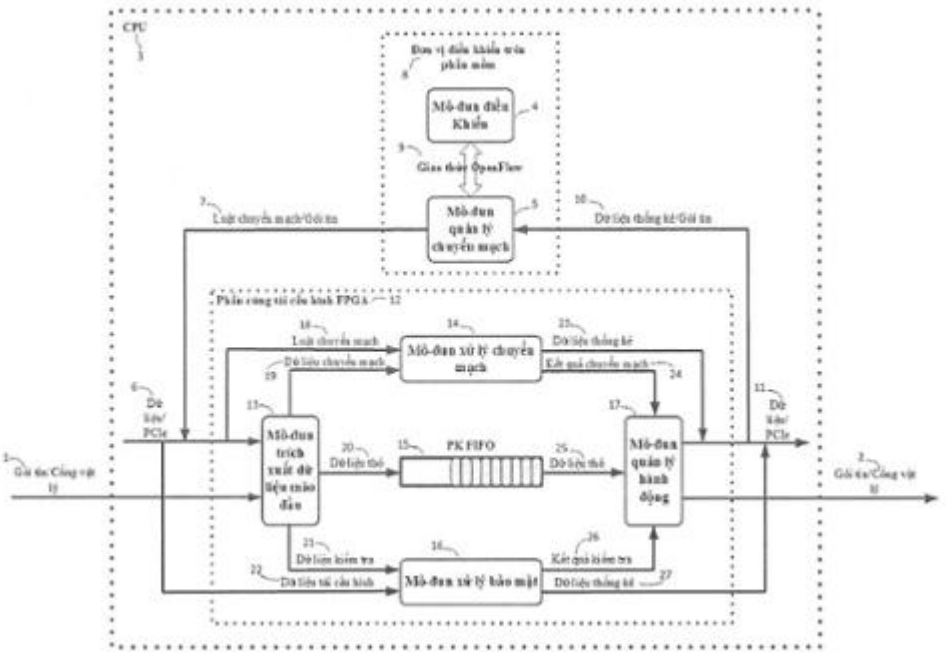
(51)[7] **G06F 21/00**

(13) **Y**

(21) 2-2017-00146
(22) 02/06/2017
(45) 26/06/2023 423
(43) 25/12/2018 369A
(73) Trường Đại học Bách Khoa - Đại Học Quốc Gia thành phố Hồ Chí Minh (VN)
268 Lý Thường Kiệt, phường 14, quận 10, thành phố Hồ Chí Minh
(72) Trần Ngọc Thịnh (VN); Ngô Đức Minh (VN).

(54) HỆ THỐNG CHUYỂN MẠCH DỰA TRÊN OPENFLOW SỬ DỤNG PHẦN CỨNG TÁI CẤU HÌNH

(57) Giải pháp hữu ích đề cập đến hệ thống chuyển mạch dựa trên OpenFlow có khả năng ngăn chặn tấn công từ chối dịch vụ phân tán trong môi trường mạng tốc độ cao được thiết kế dựa trên phần cứng tái cấu hình. Hệ thống cho phép quản lý các phiên kết nối TGP dựa trên giao thức luồng mở (OpenFlow protocol) và có khả năng phát hiện, phát sinh cảnh báo tấn công mạng. Thêm vào đó, hệ thống hoạt động tách bạch giữa đường dữ liệu với đường điều khiển, giữa đường chuyển mạch và đường bảo mật, có áp dụng linh hoạt các phương pháp khác nhau để đưa ra phương pháp tối ưu và hoạt động linh hoạt ở tốc độ cao.



Lĩnh vực kỹ thuật được đề cập

Giải pháp hữu ích đề cập đến hệ thống chuyển mạch dựa trên giao thức OpenFlow, tích hợp một số khả năng phát hiện và ngăn chặn tấn công từ chối dịch vụ phân tán (DDoS – Distributed Denial of Service) hiện thực trên phần cứng tái cấu hình cho tốc độ xử lý và độ linh hoạt cao.

Tình trạng kỹ thuật của giải pháp hữu ích

Đã biết thông tin về sáng chế "Active security defense for software defined network" được cấp Bằng sáng chế Mỹ số US 0359697 A1.

Sáng chế này đề cập đến phương pháp bảo mật cho mạng định nghĩa bằng phần mềm (SDN – Software Defined Networking) sử dụng giao thức OpenFlow trên các thiết bị chuyển mạch. Đầu tiên, đơn vị điều khiển ghi một luật chuyển mạch xuống bộ chuyển mạch, mọi kết nối mạng đi qua bộ chuyển mạch được so trùng với luật chuyển mạch lưu trữ trong bộ chuyển mạch. Nếu kết quả kiểm tra trả về thành công, bộ chuyển mạch vừa gửi cảnh báo cho bộ điều khiển, vừa tiếp tục xử lý dữ liệu mạng theo luật chuyển mạch. Bộ điều khiển tiến hành kiểm tra lỗ hổng bảo mật trên máy chủ đích khi nhận được cảnh báo, nếu kết quả trả về thành công đồng nghĩa với máy chủ có lỗ hổng bảo mật, kết nối mạng tới máy chủ đích sẽ bị ngăn chặn tại bộ chuyển mạch, ngược lại máy chủ đích sẽ được thêm vào danh sách an toàn trong một khoảng thời gian nhất định.

Sáng chế sử dụng bộ điều khiển để tiến hành kiểm tra bảo mật và quản lý các luồng kết nối dẫn đến hạn chế về hiệu suất điều khiển, kiểm tra bảo mật của bộ điều khiển và khả năng ngăn chặn tấn công một cách nhanh chóng và kịp thời.

Đã biết thông tin về sáng chế "DDoS attack processing apparatus and method in Openflow switch" được cấp Bằng sáng chế Mỹ số US 0189867 A1.

Sáng chế này đề cập đến phương pháp bảo mật chống tấn công từ chối dịch vụ phân

tán cho mạng định nghĩa bằng phần mềm sử dụng giao thức OpenFlow trên các thiết bị chuyển mạch, trong đó khối bảo mật được tích hợp trên phần cứng của bộ chuyển mạch OpenFlow. Đầu tiên, mọi dữ liệu về số lượng gói tin và băng thông được tổng hợp và phân tích, nếu kết quả trả về là thành công, khối bảo mật trên phần cứng tiến hành kích hoạt khối đáp ứng tấn công từ chối dịch vụ phân tán bằng cách loại bỏ gói tin. Dữ liệu chuyển mạch và tấn công đi qua hệ thống được thu thập và lưu trữ hoặc gửi cho bộ điều khiển sau một khoảng thời gian định trước. Phương pháp được đề cập thực hiện loại bỏ những dữ liệu được xem là tấn công dựa trên kết quả tổng hợp và phân tích số lượng gói tin trong một khoảng thời gian nhất định, những dữ liệu này đều bị loại bỏ khi đi qua hệ thống dẫn đến hạn chế đó là giảm tính đáp ứng khi hệ thống phát hiện sai người dùng hợp lệ là tấn công. Thêm nữa, việc hiện thực cố định khối bảo mật trên phần cứng sẽ gây khó khăn và ảnh hưởng tới hoạt động mạng khi muốn thay đổi chức năng bảo mật.

Bản chất kỹ thuật của giải pháp hữu ích

Giải pháp hữu ích được thực hiện nhằm giải quyết vấn đề kỹ thuật nêu trên. Mục đích chính của giải pháp hữu ích là đề xuất một hệ thống chuyển mạch dựa trên OpenFlow có khả năng giám sát và ngăn chặn tấn công từ chối dịch vụ phân tán qua mạng. Hệ thống có khả năng quản lý các luồng dữ liệu và được hiện thực trên phần cứng tái cấu hình với khả năng linh hoạt và tốc độ cao.

Để thực hiện mục đích này, giải pháp hữu ích đề xuất hệ thống chuyển mạch hoạt động dựa vào sự kết hợp giữa đơn vị điều khiển trên phần mềm và bộ chuyển mạch trên phần cứng tái cấu hình. Đơn vị điều khiển trên phần mềm cung cấp khả năng tương tác với dữ liệu chuyển mạch trên phần cứng và quản lý các luồng chuyển mạch trong khi bộ chuyển mạch trên phần cứng tái cấu hình làm nhiệm vụ chuyển mạch dữ liệu và có khả năng tương tác với đơn vị điều khiển trên phần mềm thông qua giao tiếp thiết bị ngoại vi tốc độ cao (bus PCIe).

Theo một khía cạnh của giải pháp hữu ích, các gói tin đi qua hệ thống sẽ được đệm lại trong bộ nhớ hệ thống. Các gói tin này được phân tách thành ba luồng dữ liệu độc lập: phần mào đầu dùng cho quá trình xử lý chuyển mạch, phần mào đầu dùng

cho quá trình xử lý bảo mật và phần dữ liệu thô của gói tin được chuyển mạch dựa trên kết quả của quá trình xử lý chuyển mạch và quá trình xử lý bảo mật.

Theo một khía cạnh khác của giải pháp hữu ích, hệ thống tích hợp một số khối bảo mật có khả năng xử lý bảo mật chống tấn công từ chối dịch vụ phân tán được thực hiện dựa trên thông tin dữ liệu mào đầu trích xuất từ gói tin đến hệ thống. Cũng theo khía cạnh này, khả năng tái cấu hình được sử dụng cho những khối xử lý bảo mật để đáp ứng kịp thời những thay đổi, cập nhật mới trong quá trình xử lý bảo mật. Thêm nữa, khối xử lý bảo mật có khả năng quản lý quá trình tái cấu hình từng phần trên phần cứng mà không làm ảnh hưởng đến hoạt động chuyển mạch của hệ thống.

Theo một khía cạnh của giải pháp hữu ích, hệ thống có khả năng phát hiện và phòng chống tấn công làm ngập lụt SYN – một dạng tấn công từ chối dịch vụ phân tán, việc phát hiện tấn công dựa trên sự kết hợp hai thông số dữ liệu trong mạng bao gồm: số lượng gói tin xin thiết lập kết nối SYN trên một đơn vị thời gian và độ chênh lệch giữa số lượng gói tin SYN và số lượng gói tin ACK đi qua hệ thống trên một đơn vị thời gian. Trong quá trình phòng chống tấn công làm ngập lụt SYN, hệ thống chuyển mạch trên phần cứng xác thực người dùng thông qua giải thuật SYN Cookies kết hợp hàm băm Shift-Add-Xor đảm bảo phòng chống tấn công làm ngập lụt SYN và giảm thiểu đụng độ cũng như khả năng phát hiện sai trong quá trình chuyển mạch.

Theo một khía cạnh của giải pháp hữu ích, hệ thống có khả năng gửi báo cáo về đơn vị điều khiển thông qua giao thức UDP. Nội dung gói tin báo cáo bao gồm nhưng không giới hạn cho mã mô tả hành vi độc hại phát hiện được, nội dung thông tin dữ liệu chứa hành vi độc hại.

Những khía cạnh được trình bày và các chức năng khác của giải pháp hữu ích sẽ được hiểu rõ hơn thông qua việc xem xét mô tả chi tiết giải pháp hữu ích, các hình vẽ và yêu cầu bảo hộ của giải pháp hữu ích.

Mô tả vắn tắt các hình vẽ

Hình 1 mô tả sơ đồ khối tổng quát của hệ thống.

Hình 2 mô tả sơ đồ khối tổng quát của mô-đun trích xuất dữ liệu mào đầu.

Hình 3 mô tả sơ đồ khối tổng quát của mô-đun quản lý chuyển mạch.

Hình 4 mô tả sơ đồ khối tổng quát của mô-đun quản lý bảo mật.

Hình 5 mô tả sơ đồ khối tổng quát của mô-đun quản lý hành động.

Hình 6 mô tả sơ đồ nguyên lý hoạt động của mô-đun bảo mật SYN-defender.

Hình 7 mô tả cấu trúc gói tin báo cáo.

Mô tả chi tiết giải pháp hữu ích

Hình 1 mô tả kiến trúc của hệ thống chuyển mạch có tính năng bảo mật dựa trên OpenFlow triển khai trên phần cứng tái cấu hình FPGA (Field-programmable Gate Array) 12 có khả năng giao tiếp với đơn vị điều khiển trên phần mềm 8 và cùng được tích hợp trên đơn vị xử lý trung tâm CPU (Central Processing Unit) 3. Đơn vị điều khiển trên phần mềm 8 gồm các khối chính sau:

- Mô-đun điều khiển 4: thực hiện việc nhận thông tin từ Mô-đun quản lý chuyển mạch 5 thông qua giao thức OpenFlow (giao thức luồng mở rộng) 9, quản lý các phiên làm việc UDP/TCP và là mô-đun điều khiển hoạt động của hệ thống chuyển mạch dựa trên OpenFlow.
- Mô-đun quản lý chuyển mạch 5: thực hiện việc quản lý bảng chuyển mạch của hệ thống trên phần mềm, đồng bộ dữ liệu với bảng chuyển mạch trên phần cứng. Từ mô-đun này, luật chuyển mạch/gói tin 7 sau khi đã xử lý được trả về cho hệ thống chuyển mạch trên phần cứng tái cấu hình FPGA 12.

Hệ thống chuyển mạch trên phần cứng tái cấu hình FPGA 12 gồm các mô-đun chính sau:

- Mô-đun trích xuất dữ liệu mào đầu 13: thực hiện việc nhận gói tin từ gói tin/cổng vật lý 1 và dữ liệu/PCIe 6 (bao gồm gói tin, luật chuyển mạch và dữ liệu tái cấu hình), trích xuất dữ liệu mào đầu từ nội dung gói tin và chuyển dữ liệu thô 20 cho mô-đun lưu trữ PK FIFO 15. Từ mô-đun này hai phần quan trọng trong quá trình xử lý là phần dữ liệu chuyển mạch 19 và dữ liệu kiểm tra 21 được gửi cho các mô-đun phía sau xử lý.
- Mô-đun xử lý chuyển mạch 14: thực hiện quản lý bảng chuyển mạch, luật chuyển mạch trên phần cứng. Mô-đun này trả về kết quả chuyển mạch 24 và dữ liệu thống kê 23 cho các mô-đun phía sau xử lý.
- Mô-đun xử lý bảo mật 16: thực hiện kiểm tra, phát hiện nội dung dữ liệu chứa hành vi độc hại và quản lý việc tái cấu hình các bộ quét bảo mật. Mô-đun này trả về kết quả kiểm tra 26 cho mô-đun phía sau xử lý và dữ liệu thống kê 27 cho phần mềm.
- Mô-đun quản lý hành động 17: tổng hợp các kết quả chuyển mạch 24 và kết quả kiểm tra 26, đưa ra kết quả cuối cùng đối với dữ liệu thô 25. Từ kết quả cuối cùng, mô-đun này gửi dữ liệu/PCIe 11 (bao gồm các dữ liệu thống kê và gói tin) cho đơn vị điều khiển trên phần mềm 8 hoặc gửi dữ liệu gói tin/cổng vật lý 2 ra mạng bên ngoài.

Theo một khía cạnh của giải pháp hữu ích, hệ thống chia môi trường mạng thành hai phần cụ thể là gói tin từ giao tiếp mạng vật lý hai chiều (đầu vào và đầu ra) và từ cổng giao tiếp thiết bị ngoại vi tốc độ cao (bus PCIe) thông qua giao thức truy xuất bộ nhớ trực tiếp (DMA – Direct Memory Access). Dữ liệu từ cổng giao tiếp thiết bị ngoại vi tốc độ cao (bus PCIe) là các dữ liệu từ phần mềm (các luật chuyển mạch, gói tin, dữ liệu tái cấu hình và dữ liệu thống kê). Toàn bộ dữ liệu mạng đến đi vào hệ thống từ cổng vật lý và gói tin đi vào hệ thống từ cổng giao tiếp thiết bị ngoại vi tốc độ cao (bus PCIe) nói chung, được nhận và trích xuất bởi mô-đun trích xuất dữ liệu mào đầu 13. Tại đây, các trường thuộc tầng hai (lớp mạng) và tầng ba (lớp vận chuyển) được trích xuất. Dữ liệu chuyển mạch 19 được trích xuất và gửi cho mô-đun xử lý chuyển mạch 14, dữ liệu kiểm tra 21 được trích xuất và gửi cho

mô-đun xử lý bảo mật 16 và dữ liệu thô 20 gửi cho khối lưu trữ dữ liệu thô PK FIFO 15. Chỉ những dữ liệu mạng an toàn mới được phép gửi đến đơn vị điều khiển trên phần mềm 8 hoặc gửi ra gói tin/cổng vật lý 2. Mô-đun xử lý chuyển mạch 14 cập nhật bảng chuyển mạch bởi những luật chuyển mạch 18 gửi từ phần mềm, đưa ra dữ liệu thống kê 23 và thực hiện tìm kiếm luật chuyển mạch trong bảng chuyển mạch, đưa ra kết quả chuyển mạch 24. Mô-đun xử lý bảo mật 16 nhận dữ liệu tái cấu hình 22 gửi từ phần mềm, thực hiện tái cấu hình phần cứng, đưa ra dữ liệu thống kê 27 và tìm kiếm hành vi độc hại trong phần mào đầu gói tin, đưa ra kết quả kiểm tra 26. Kết quả tổng hợp gửi đến mô-đun quản lý hành động 17 và đưa ra quyết định xử lý dữ liệu thô 25 từ khối lưu trữ dữ liệu thô PK FIFO 15, mô-đun quản lý hành động 17 dựa trên kết quả việc tìm kiếm hành vi độc hại xuất hiện trong phần mào đầu của gói tin để ra quyết định chuyển mạch đối với gói tin. Nếu có xuất hiện hành vi độc hại, gói tin bị ngăn chặn và phát sinh cảnh báo cho đơn vị điều khiển trên phần mềm 8.

Theo một khía cạnh khác của giải pháp hữu ích, hệ thống yêu cầu tối thiểu (nhưng không giới hạn cho) một giao tiếp mạng vật lý hai chiều (đầu vào và đầu ra) và một giao tiếp cho dữ liệu từ cổng giao tiếp thiết bị ngoại vi tốc độ cao (bus PCIe).

Mô-đun trích xuất dữ liệu mào đầu

Theo một khía cạnh của giải pháp hữu ích, mô-đun trích xuất dữ liệu mào đầu 13 nhận dữ liệu, trích xuất dữ liệu đến hệ thống; liên kết với (nhưng không giới hạn cho) một giao tiếp mạng vật lý hai chiều và một giao tiếp cho dữ liệu từ cổng giao tiếp thiết bị ngoại vi tốc độ cao (bus PCIe).

Hình 2 mô tả kiến trúc của mô-đun trích xuất dữ liệu mào đầu 13 bao gồm: bộ trích xuất mào đầu 28, bộ phân tách dữ liệu 29, khối lưu trữ dữ liệu chuyển mạch OF FIFO 30, khối lưu trữ dữ liệu kiểm tra SC FIFO 31.

Bộ trích xuất mào đầu 28 thực hiện trích xuất dữ liệu mào đầu từ gói tin, tại đây gói tin đến hệ thống được phân tích và tách ra các trường: giao thức mạng, chiều dài mào đầu (Internet header length), thời gian sống (Time to live), địa chỉ IP nguồn, địa chỉ IP đích, địa chỉ MAC nguồn, địa chỉ MAC đích, loại dịch vụ (Type

of service), cổng nguồn gửi, cổng đích đến, cờ đánh dấu (Flags), cổng nguồn FPGA, số xác thực (ACK number), kích thước mảnh dữ liệu lớn nhất (Maximum segment size) và giá trị kiểm tra TCP (TCP checksum).

Theo một khía cạnh của giải pháp hữu ích, bộ trích xuất dữ liệu mào đầu 28 thực hiện chuyển dữ liệu đã trích xuất 32 cho bộ phân tách dữ liệu 29 và chuyển dữ liệu thô 20 vào khối lưu trữ dữ liệu thô PK FIFO 15.

Bộ phân tách dữ liệu 29 dựa trên dữ liệu đã trích xuất 32 từ mô-đun trích xuất mào đầu 28, lựa chọn và sắp xếp những trường dữ liệu đặc trưng cần thiết một cách đồng thời cho các bộ nhớ đệm riêng biệt; dữ liệu chuyển mạch 33 được lưu vào bộ nhớ OF FIFO 30, dữ liệu kiểm tra bảo mật 34 được lưu vào bộ nhớ SC FIFO 31.

OF FIFO 30 đóng vai trò là bộ nhớ vào trước ra trước chứa những khối dữ liệu đệm cho mô-đun xử lý chuyển mạch 14 sử dụng. Một khối dữ liệu chứa dữ liệu chuyển mạch 19 cần cho mô-đun xử lý chuyển mạch 14 bao gồm các trường: loại dịch vụ (Type of service), cổng nguồn FPGA, địa chỉ MAC nguồn, địa chỉ MAC đích, địa chỉ IP nguồn, địa chỉ IP đích, cổng nguồn gửi, cổng đích đến và giao thức mạng.

SC FIFO 31 đóng vai trò là bộ nhớ vào trước ra trước chứa những khối dữ liệu đệm cho mô-đun xử lý bảo mật 16 sử dụng. Một khối dữ liệu chứa dữ liệu kiểm tra 21 cần cho mô-đun xử lý bảo mật 16 bao gồm các trường: giao thức mạng, chiều dài mào đầu (Internet header length), thời gian sống (Time to live), địa chỉ IP nguồn, địa chỉ IP đích, cổng nguồn gửi, cổng đích đến, cờ đánh dấu (Flags), số xác thực (ACK number), kích thước mảnh dữ liệu lớn nhất (Maximum segment size) và giá trị kiểm tra TCP (TCP checksum).

Mô-đun xử lý chuyển mạch

Theo một khía cạnh của giải pháp hữu ích mô-đun xử lý chuyển mạch 14 liên kết với Mô-đun quản lý chuyển mạch 5 trên phần mềm, gửi dữ liệu thống kê 23 cho bộ quản lý chuyển mạch và quản lý luật chuyển mạch cho gói tin đi qua phần cứng.

Hình 3 mô tả kiến trúc của mô-đun xử lý chuyển mạch 14 bao gồm: bộ giao tiếp chuyển mạch 35 và bộ quản lý bảng chuyển mạch 36.

Bộ giao tiếp chuyển mạch 35 sử dụng chuẩn giao tiếp AXI-lite liên kết trực tiếp với Mô-đun quản lý chuyển mạch 5 trên phần mềm thông qua giao thức đọc/ghi AXI. Luật chuyển mạch 18 sử dụng để chuyển mạch gói tin được ghi vào bảng chuyển mạch bởi Mô-đun quản lý chuyển mạch 5 thông qua bộ giao tiếp chuyển mạch 35.

Bộ quản lý bảng chuyển mạch 36 chứa hai bảng chuyển mạch, bảng so trùng chính xác (exact match) và bảng so trùng đại diện (wildcard match), dữ liệu chuyển mạch 19 từ mô-đun trích xuất dữ liệu mào đầu 13 được sử dụng để so trùng trong hai bảng chuyển mạch với các luật chuyển mạch 37 đã được ghi vào bảng chuyển mạch bởi bộ giao tiếp chuyển mạch 35. Dữ liệu thống kê 38 được tính toán và gửi cho bộ giao tiếp chuyển mạch 35.

PK FIFO

Theo một khía cạnh của giải pháp hữu ích, dữ liệu thô 20 trong thời gian chờ kết quả phân tích từ mô-đun xử lý chuyển mạch 14 và mô-đun xử lý bảo mật 16 được lưu trữ tại khối lưu trữ dữ liệu thô PK FIFO 15, việc sử dụng khối lưu trữ dữ liệu thô PK FIFO nhằm tăng hiệu suất hệ thống và loại bỏ thời gian chờ cho mô-đun trích xuất dữ liệu mào đầu 13 trong khi hai mô-đun xử lý chuyển mạch 14 và mô-đun xử lý bảo mật 16 thực hiện phân tích dữ liệu mào đầu để đưa ra kết quả xử lý. Khối lưu trữ dữ liệu thô PK FIFO 15 đóng vai trò là bộ nhớ vào trước ra trước có khả năng lưu trữ cố định một lượng gói tin và gửi dữ liệu thô 25 ra ngoài khi có yêu cầu từ mô-đun quản lý hành động 17.

Mô-đun xử lý bảo mật

Theo một khía cạnh của giải pháp hữu ích, mô-đun xử lý bảo mật 16 kiểm tra bảo mật từ dữ liệu kiểm tra 21 đã trích xuất từ gói tin và thực hiện tái cấu hình, quản lý quá trình tái cấu hình phần cứng với dữ liệu tái cấu hình 22 gửi từ phần mềm thông qua cổng giao tiếp thiết bị ngoại vi tốc độ cao (bus PCIe).

Hình 4 mô tả kiến trúc mô-đun xử lý bảo mật 16 bao gồm: bộ phân chia dữ liệu 38, bộ kết nối AXI-lite 39, bộ điều khiển ICAP (Internal Configuration Access

Port) 40, bộ điều khiển tái cấu hình động 41, các bộ quét bảo mật 42, bộ điều khiển SDRAM 43 và bộ tổng hợp kết quả 44.

Bộ phân chia dữ liệu 38 nhận và phân chia dữ liệu đến thành hai luồng riêng biệt, dữ liệu kiểm tra 21 được xử lý thành dữ liệu quét bảo mật 46 và gửi cho bộ điều khiển tái cấu hình động 41, dữ liệu tái cấu hình 45 được đệm từ dữ liệu tái cấu hình 22 và gửi cho bộ điều khiển ICAP 40.

Bộ kết nối AXI-lite 39 thực hiện kết nối và giao tiếp dữ liệu cho mô-đun xử lý bảo mật 16 và đơn vị điều khiển trên phần mềm 8 thông qua chuẩn giao tiếp AXI-lite.

Theo một khía cạnh của giải pháp hữu ích, bộ điều khiển ICAP 40 nhận dữ liệu tái cấu hình và ghi dữ liệu tái cấu hình vào phần cứng. Bộ điều khiển ICAP 40 và bộ điều khiển tái cấu hình động 41 trao đổi thông tin dữ liệu thông qua đồng bộ giao tiếp 48, quá trình tái cấu hình được thực hiện khi có tín hiệu cho phép từ bộ điều khiển tái cấu hình động 41, bộ điều khiển ICAP 40 bắt đầu ghi dữ liệu tái cấu hình xuống phần cứng, giao thức đồng bộ giao tiếp này giúp hệ thống có thể tiếp tục hoạt động trong thời gian tái cấu hình phần cứng.

Bộ điều khiển tái cấu hình động 41 thực hiện ba chức năng bao gồm: gửi/nhận dữ liệu quét bảo mật 49 (dữ liệu quét hoặc kết quả quét) từ các bộ quét bảo mật 42, điều khiển việc tái cấu hình thông qua đồng bộ giao tiếp 48 và trả kết quả quét bảo mật 52 cho mô-đun phía sau xử lý.

Theo một khía cạnh của giải pháp hữu ích, bộ quét bảo mật 42 bao gồm các bộ quét bảo mật có khả năng tái cấu hình. Bộ quét bảo mật 42 thực hiện kiểm tra bảo mật gói tin dựa trên dữ liệu quét bảo mật 49 có khả năng truy xuất bộ nhớ 50 thông qua bộ điều khiển SDRAM 43.

Bộ điều khiển SDRAM 43 đảm bảo việc truy xuất bộ nhớ cho các bộ quét bảo mật, cung cấp khả năng truy xuất thanh ghi 47 đến bộ điều khiển ICAP thông qua bộ kết nối AXI-lite 39.

Bộ tổng hợp kết quả 44 tổng hợp kết quả tái cấu hình 51 gửi cho phần mềm thông qua dữ liệu thống kê/PCIe 27, kết quả quét bảo mật 52 được đóng gói thành kết quả kiểm tra 26 và gửi cho mô-đun phía sau xử lý.

Bộ quét bảo mật

Theo một khía cạnh của giải pháp hữu ích, bộ quét bảo mật 42 bao gồm các bộ quét bảo mật có khả năng tái cấu hình: I/E Filtering (bộ lọc Ingress/Engress) 401, Hop-Count Filtering (bộ lọc Hop-Count) 402, SYN-Defender (bộ chống tấn công làm ngập lụt SYN) 403 và có thể tích hợp thêm các bộ quét bảo mật khác 404.

I/E Filtering 401 là bộ quét bảo mật hoạt động dựa trên cơ chế so trùng địa chỉ IP nguồn của gói tin với những địa chỉ IP được lưu trong bộ nhớ trên chip (BlockRAM). Nếu kết quả so trùng trả về thành công, gói tin với địa chỉ IP nguồn bị so trùng sẽ được đánh dấu và không được đi qua hệ thống.

Hop-Count Filtering 402 là bộ quét bảo mật chống tấn công từ chối dịch vụ phân tán dựa trên cơ chế tính toán, thu thập dữ liệu từ dữ liệu đầu vào là địa chỉ IP và chỉ số thời gian sống của gói tin (time to live) sau đó so trùng với dữ liệu IP, chỉ số thời gian sống của gói tin đến hệ thống. Nếu kết quả trả về là thành công, gói tin sẽ được đánh dấu và không được đi qua hệ thống.

Hình 5 mô tả hoạt động của khối bảo mật SYN-Defender 403 phát hiện và chống tấn công làm ngập lụt SYN xử lý theo bốn bước đường ống (pipelining).

Một kết nối mạng TCP được hình thành khi người dùng gửi gói tin xin thiết lập kết nối với duy nhất cờ SYN trong phần mào đầu TCP được thiết lập, sau khi nhận được gói xác nhận kết nối từ máy chủ với cờ SYN-ACK được thiết lập, người dùng lúc này gửi gói ACK xác thực và kết nối hợp lệ được thiết lập. Một kết nối mạng TCP khi người dùng chỉ gửi gói SYN, sau khi nhận được gói xác nhận kết nối từ máy chủ SYN-ACK nhưng người dùng không gửi lại gói xác thực ACK, người dùng và gói tin này được cho là có khả năng tấn công làm ngập lụt SYN đến máy chủ đích.

Bước đầu tiên 53, mô-đun bảo mật SYN-Defender tiến hành nhận dữ liệu quét bảo mật 49 từ bộ điều khiển tái cấu hình động 41, các dữ liệu này là một chuỗi bit giá trị các trường dữ liệu mào đầu trong một gói tin được trích xuất và lưu trữ bởi mô-đun trích xuất dữ liệu mào đầu 13.

Bước thứ hai 54, tiến hành sử dụng những thông tin đã đệm từ bước đầu để thực hiện ba công việc: nhận dạng gói tin, sinh giá trị xác thực và xác thực người dùng qua hàm băm.

Bộ phân chia loại gói tin 58 dựa trên dữ liệu đã xử lý 64 để nhận dạng gói tin bằng phương pháp so trùng thông tin giao thức và loại gói tin với giá trị xác định, đối với những gói tin thiết lập kết nối, gói tin xác thực kết nối sẽ được đánh dấu riêng để xử lý.

Bộ sinh giá trị xác thực 59 nhận dữ liệu sinh Cookies 65 và tiến hành sinh 32 bit dữ liệu dựa trên địa chỉ IP nguồn, địa chỉ IP đích, cổng nguồn gửi, cổng đích đến, kích thước mảnh dữ liệu lớn nhất và biến đếm thời gian cục bộ của hệ thống dựa trên hàm băm CRC. Giá trị 32 bit dữ liệu (Cookies 71) này dùng để làm chỉ số tuần tự cho gói tin xác thực kết nối SYN-ACK mà hệ thống gửi đến người dùng.

Bộ băm xác thực người dùng 60 tiến hành sinh 10 bit địa chỉ dựa trên dữ liệu xác thực 66 bao gồm: địa chỉ IP nguồn và địa chỉ IP đích. Bộ băm xác thực sử dụng hàm băm Shift-Add-Xor làm nhiệm vụ sinh ra 10 bit địa chỉ xác thực 72 cho việc tìm kiếm địa chỉ IP được lưu trong bộ nhớ trên chip, xử lý đụng độ do hàm băm gây ra bằng phương pháp so trùng địa chỉ IP với giá trị đã lưu trong bộ nhớ trên chip.

Theo một khía cạnh của giải pháp hữu ích, khối bảo mật SYN-Defender sử dụng hai loại hàm băm CRC và Shift-Add-Xor. Hàm băm CRC được sử dụng để sinh dữ liệu xác thực cho gói tin xác thực kết nối SYN-ACK trong khi hàm băm Shift-Add-Xor được sử dụng để sinh địa chỉ phục vụ việc tìm kiếm địa chỉ IP nguồn/đích được lưu trong bộ nhớ trên chip với tốc độ nhanh và giảm thiểu đụng độ.

Bước thứ ba 55, tiến hành thống kê và phát hiện tấn công làm ngập lụt SYN bằng bộ phát hiện tấn công SYN 61. Bộ phát hiện tấn công SYN 61 dựa trên thông tin loại gói tin 67 đã phân tích từ bước thứ hai để thống kê và đưa ra kết quả phân tích 69. Chi tiết hơn, bộ phát hiện tấn công SYN 61 sử dụng kết hợp hai thông số: số lượng gói tin xin thiết lập kết nối SYN trên một đơn vị thời gian và độ chênh lệch giữa số lượng gói SYN trên số lượng gói ACK mà hệ thống nhận được. Một hệ thống bị tấn công làm ngập lụt SYN thông thường sẽ có số lượng gói tin xin thiết lập kết nối SYN nhiều bất thường trên một đơn vị thời gian, theo một khía cạnh khác, đối với một hệ thống phục vụ với tốc độ Gigabit thì lượng gói xin thiết lập kết nối SYN trên một đơn vị thời gian là rất lớn, lúc này cần thêm một thông số bất thường khác để xác định được tấn công SYN, thông số này có thể là số lượng chênh

lệch giữa gói tin xin thiết lập kết nối SYN và gói xác thực kết nối ACK. Ví dụ cụ thể: hệ thống sẽ đưa ra kết luận bị tấn công khi số lượng gói SYN trên một giây vượt mức 100 gói hoặc số lượng gói SYN phát hiện nhiều hơn 10 gói so với số lượng gói ACK trên một giây.

Theo một khía cạnh của giải pháp hữu ích, bộ đệm dữ liệu 62 nhận dữ liệu đệm 68 và ra quyết định kích hoạt chế độ phòng chống tấn công làm ngập lụt SYN. Thông thường khi sử dụng những hàm băm để sinh giá trị xác thực Cookies 71 hay sinh địa chỉ xác thực ở bước thứ hai sẽ cần thêm xung nhịp xử lý để cho ra kết quả, bước thứ ba sẽ đệm lại gói tin từ bước thứ hai để đồng bộ với kết quả hàm băm được sử dụng để xử lý ở bước thứ tư.

Bước thứ tư 56, tiến hành xử lý thông tin từ bước thứ ba, khi dữ liệu đệm 70 ở bước thứ ba cho kết quả là hệ thống đang bị tấn công, bộ xử lý trung tâm 63 ở bước thứ tư chặn tất cả những gói tin xin thiết lập kết nối SYN và hệ thống lúc này trở thành máy chủ xác thực kết nối trung gian với máy chủ đích, bộ xử lý sử dụng kết quả 32 bit dữ liệu Cookies 71 và một tín hiệu điều khiển có độ dài 3 bit được gói trong kết qủa dữ liệu quét bảo mật 49 và trả về cho bộ điều khiển tái cấu hình động 41. Đối với những gói xác thực ACK sẽ được so trùng hai giá trị xác thực: giá trị thứ nhất là 32 bit dữ liệu Cookies 71 sinh ra với 32 bit chỉ số xác thực (ACK number) của gói tin mới nhận được, giá trị thứ hai đó là địa chỉ IP nguồn, địa chỉ IP đích của gói tin với giá trị địa chỉ IP nguồn, địa chỉ IP đích tìm được trong bộ nhớ trên chip ở địa chỉ xác thực 72. Khi hai giá trị so trùng đều trả về kết quả thành công, đồng nghĩa với người dùng là hợp lệ, bộ xử lý trung tâm sẽ gửi 3 bit tín hiệu điều khiển được gói trong kết quả dữ liệu quét bảo mật 49 yêu cầu gửi gói tin tái thiết lập kết nối (Reset) trả về cho bộ điều khiển tái cấu hình động 41, đồng thời ghi giá trị 1 vào thanh ghi xác thực ở 10 bit địa chỉ đã sinh ra để gói tin xin thiết lập kết nối tiếp theo của địa chỉ IP nguồn, địa chỉ IP đích này sẽ được cho qua hệ thống. Các trường hợp khác gói tin nằm ngoài phạm vi của bộ quét bảo mật sẽ được đi qua hệ thống.

Mô-đun quản lý hành động

Theo một khía cạnh của giải pháp hữu ích, mô-đun quản lý hành động 17 dựa trên kết quả chuyển mạch 24 và kết quả kiểm tra 26 đưa ra quyết định chuyển mạch hoặc thay đổi dữ liệu đối với dữ liệu thô lưu trữ tại khối lưu trữ dữ liệu thô PK FIFO 15.

Hình 6 mô tả kiến trúc mô-đun quản lý hành động 17 bao gồm: bộ đồng bộ dữ liệu nhận 73, bộ ra quyết định chuyển mạch 75, bộ phát sinh cảnh báo 74, bộ tính toán checksum 76 và bộ đồng bộ dữ liệu xuất 77.

Theo một khía cạnh của giải pháp hữu ích, kết quả chuyển mạch 24, kết quả kiểm tra 26, dữ liệu thô 25 được xử lý và hoàn thành độc lập với nhau. Bộ đồng bộ dữ liệu nhận 73 làm nhiệm vụ đồng bộ các dữ liệu này và gửi cho mô-đun phía sau xử lý. Bộ đồng bộ dữ liệu nhận 73 thực hiện tổng hợp kết quả chuyển mạch 24 và kết quả kiểm tra 26 sau đó sinh dữ liệu đầu ra là kết quả tổng hợp 78 bao gồm kết quả chuyển mạch 24, kết quả kiểm tra 26 và dữ liệu thô 25.

Bộ ra quyết định chuyển mạch 75 dựa trên kết quả tổng hợp 78 để ra quyết định chuyển mạch đối với gói tin. Những quyết định chuyển mạch của hệ thống chuyển mạch có tính năng bảo mật phòng chống kiểu tấn công làm ngập lụt SYN bao gồm: loại bỏ gói tin, phát tán gói tin, gửi gói tin SYN-ACK, gửi gói tin tái thiết lập kết nối (gói tin reset) và chuyển mạch theo kết quả chuyển mạch. Theo một khía cạnh của giải pháp hữu ích, hệ thống ra quyết định gửi gói tin SYN-ACK và gửi gói tin tái thiết lập kết nối dựa trên dữ liệu gói tin ban đầu, hệ thống phải thay đổi thông tin gói tin và tính toán lại các giá trị kiểm tra IP checksum và TCP checksum. Bộ ra quyết định chuyển mạch 75 gửi dữ liệu cảnh báo 79 đến bộ phát sinh cảnh báo 74, dữ liệu tính toán 80 đến bộ tính toán checksum 76 và gửi kết quả chuyển mạch đến bộ đồng bộ dữ liệu xuất 77.

Theo một khía cạnh của giải pháp hữu ích, bộ phát sinh cảnh báo 74 dựa trên dữ liệu cảnh báo 79 để sinh dữ liệu cho gói tin cảnh báo theo cấu trúc xác định và gửi cho bộ đồng bộ dữ liệu xuất 77.

Theo một khía cạnh khác của giải pháp hữu ích, bộ tính toán checksum 76 dựa trên dữ liệu tính toán 80 bao gồm dữ liệu checksum ban đầu và dữ liệu thay đổi để tính toán giá trị checksum mới mà không cần phải tính toán lại checksum một cách

toàn bộ, điều này giúp việc tính toán checksum mới được hoàn thành một cách nhanh chóng và ít hao tốn tài nguyên phần cứng.

Kết quả chuyển mạch 82 bao gồm quyết định chuyển mạch và gói tin tương ứng. Bộ đồng bộ dữ liệu xuất 77 tổng hợp kết quả và thay đổi gói tin tương ứng với kết quả chuyển mạch 82 sử dụng dữ liệu sau xử lý 83. Kết quả xử lý của bộ đồng bộ dữ liệu xuất 77 là gói tin/PCIe 11 được gửi đến phần mềm thông qua cổng giao tiếp thiết bị ngoại vi (PCIe) hoặc gói tin/cổng vật lý 2 được gửi ra cổng vật lý.

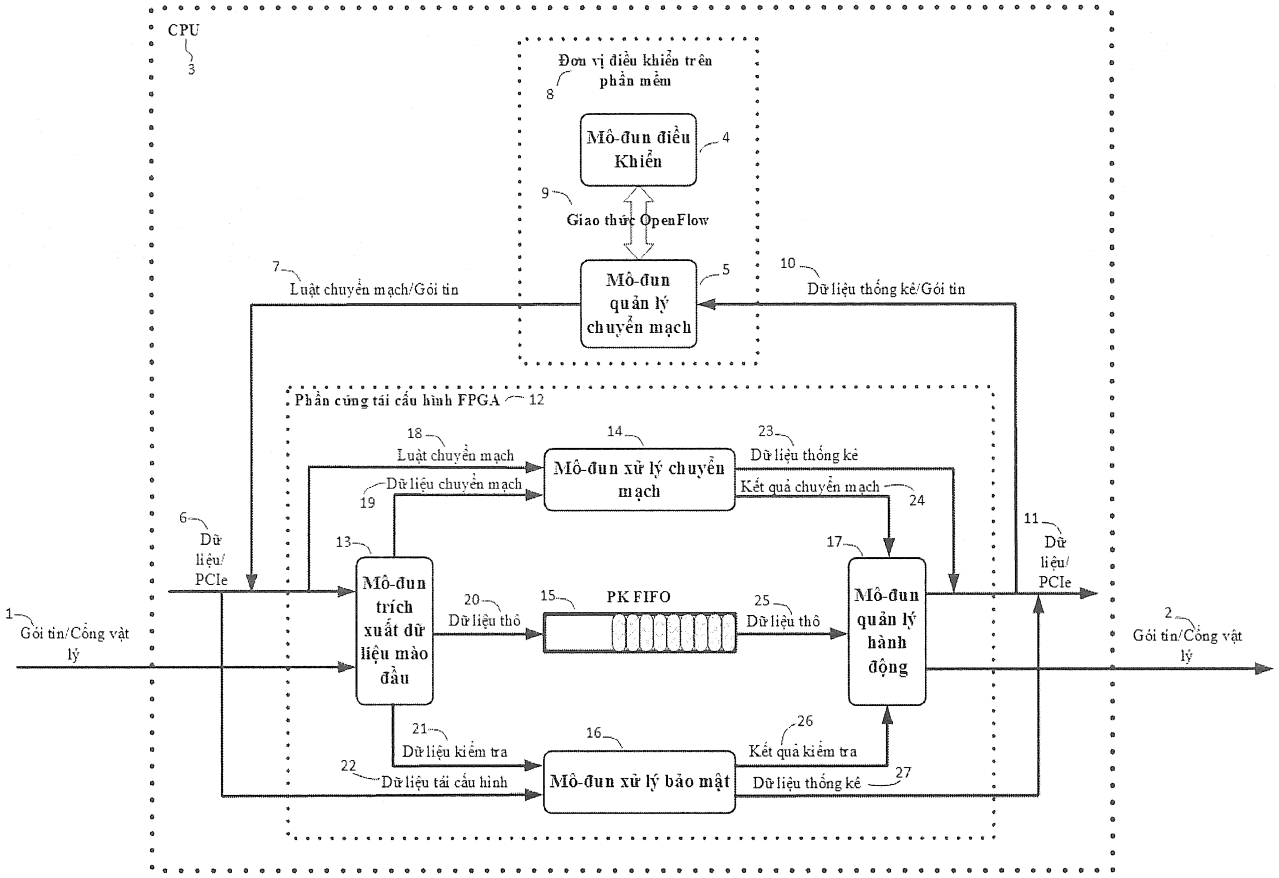
Đóng gói báo cáo

Theo một khía cạnh của giải pháp hữu ích, hệ thống cho phép gửi các gói tin UDP chứa nội dung cảnh báo về hành vi độc hại xuất hiện. Cấu trúc của một gói tin UDP báo cáo được mô tả trong Hình 7. Hệ thống có thể mở rộng cho phép phát hiện nhiều hành vi độc hại xuất hiện trong hệ thống và gửi thông báo cho đơn vị điều khiển trên phần mềm 8.

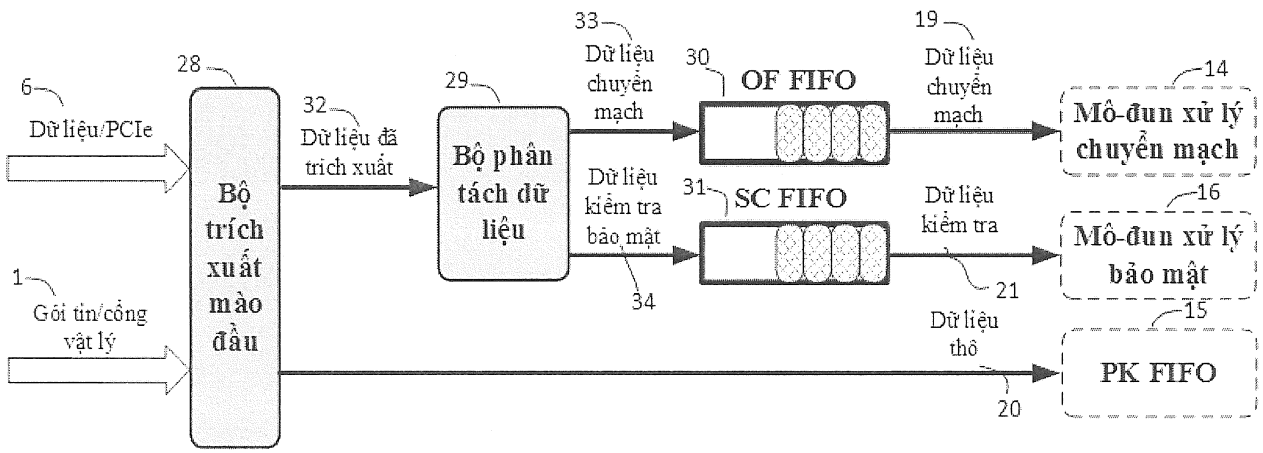
- Phần đầu Ethernet/IP/UDP 84 chứa 42 byte thông tin mào đầu của các lớp mạng: 14 byte Ethernet, 20 byte IP và 8 byte UDP. Các thông tin này được cấu hình cố định từ nguồn là hệ thống trên phần cứng tái cấu hình FPGA 12 đến đích là đơn vị điều khiển trên phần mềm 8.
- Byte nhận dạng 85: là byte dữ liệu chứa mã nhận dạng hành vi độc hại thống nhất giữa phần cứng 12 và đơn vị điều khiển trên phần mềm 8.
- Byte phân cách 86: do số lượng hành vi độc hại phát hiện được có thể mở rộng thêm, gói tin cảnh báo được dành thêm 2 byte đặc biệt (0x0000) để phân cách giữa vùng chứa mã hành vi độc hại và vùng chứa thông tin dữ liệu. Vùng byte phân cách 86 kết hợp với byte nhận dạng 85 còn có chức năng giúp cho đơn vị điều khiển có thể phân biệt giữa gói tin UDP trong mạng và gói tin UDP phát sinh cảnh báo.
- Phần thông tin trích xuất 87: chứa 17 byte các thông tin về gói tin độc hại bao gồm địa chỉ IP nguồn tấn công, địa chỉ IP đích bị tấn công, cổng nguồn gửi, cổng đích đến và cổng mạng vật lý gói tin đến trên phần cứng.

YÊU CẦU BẢO HỘ

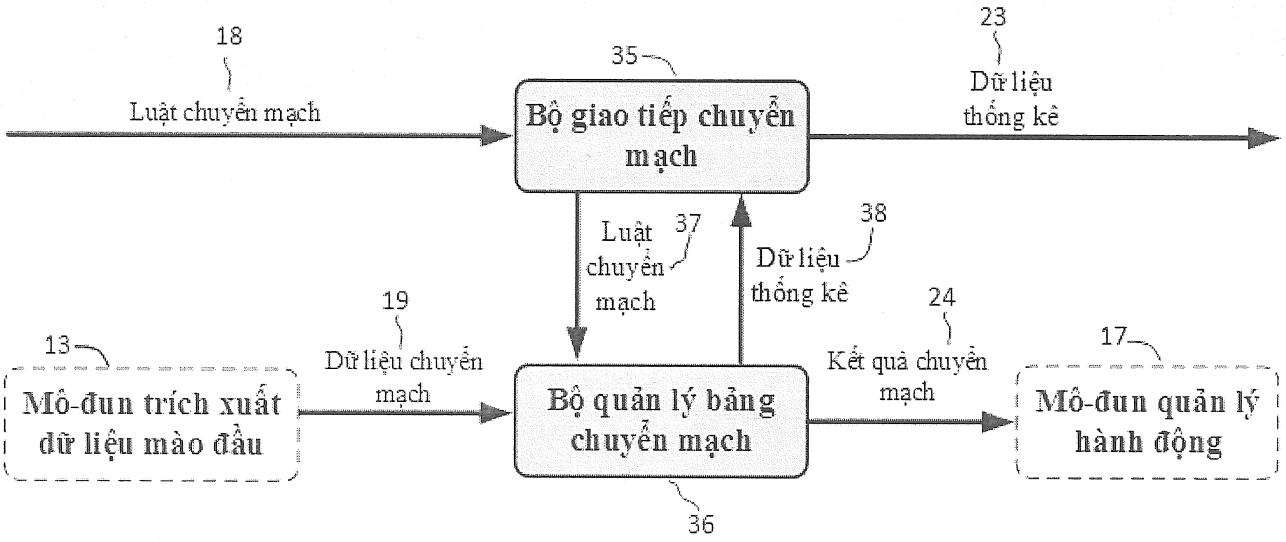
1. Hệ thống chuyển mạch dựa trên OpenFlow có tính năng bảo mật được hiện thực trên phần cứng tái cấu hình bao gồm tối thiểu nhưng không giới hạn cho một giao tiếp mạng hai chiều (đầu vào và đầu ra) cho gói tin từ cổng vật lý và một giao tiếp dữ liệu dành riêng cho việc giao tiếp giữa phần cứng mà phần mềm trong điều khiển; hệ thống được hiện thực tách bạch giữa đường chuyển mạch và đường điều khiển, giữa việc xử lý chuyển mạch và xử lý bảo mật; hệ thống có khả năng phòng chống tấn công từ chối dịch vụ phân tán và quản lý tái cấu hình từng phần trong thời gian thực cho các bộ quét bảo mật; đặc trưng ở chỗ hệ thống chuyển mạch dựa trên OpenFlow có tính năng bảo mật được hiện thực trên phần cứng tái cấu hình, có khả năng phát hiện và ngăn chặn tấn công từ chối dịch vụ phân tán xử lý bằng cơ chế đường ống, hệ thống có tính năng phát sinh cảnh báo cho bộ điều khiển trên phần mềm thông qua giao thức UDP. Hệ thống chuyển mạch dựa trên OpenFlow có tích hợp bộ quét bảo mật SYN-Defender; có khả năng phát hiện và phòng chống tấn công từ chối dịch vụ phân tán xử lý theo cơ chế đường ống vào hệ thống trên phần cứng tái cấu hình; khối SYN-Defender có thể tái cấu hình linh hoạt trong thời gian thực và khả năng phát hiện tấn công từ chối dịch vụ phân tán dựa trên hai thông số: số lượng gói xin thiết lập kết nối SYN trên một đơn vị thời gian và số lượng gói tin chênh lệch giữa gói xin thiết lập kết nối và gói xác thực ACK; đặc trưng ở chỗ bộ quét bảo mật Syn-Defender có cơ chế xác thực sử dụng kết hợp hai hàm băm CRC và Shift-Add-Xor xử lý theo cơ chế đường ống vào hệ thống trên phần cứng tái cấu hình; trong đó phương pháp xác thực người dùng tấn công làm ngập lụt SYN mà chỉ duy nhất một gói tin xác thực SYN được đi qua hệ thống sau khi gói tin trước đó đã xác thực thành công, gói xác thực SYN sau đó được hệ thống tái xác thực.


CPU
3
Đơn vị điều khiển trên phần mềm
8
Mô-đun điều Khiển
4
9
Giao thức OpenFlow
Mô-đun quản lý chuyển mạch
5
7
Luật chuyển mạch/Gói tin
10
Dữ liệu thống kê/Gói tin
Phần cứng tái cấu hình FPGA
12
18
Luật chuyển mạch
14
Mô-đun xử lý chuyển mạch
23
Dữ liệu thống kê
19
Dữ liệu chuyển mạch
Kết quả chuyển mạch
24
6
Dữ liệu/ PCIe
13
Mô-đun trích xuất dữ liệu mào đầu
20
Dữ liệu thô
15
PK FIFO
25
Dữ liệu thô
17
Mô-đun quản lý hành động
11
Dữ liệu/ PCIe
1
Gói tin/Cổng vật lý
2
Gói tin/Cổng vật lý
21
Dữ liệu kiểm tra
16
Mô-đun xử lý bảo mật
26
Kết quả kiểm tra
22
Dữ liệu tái cấu hình
Dữ liệu thống kê
27

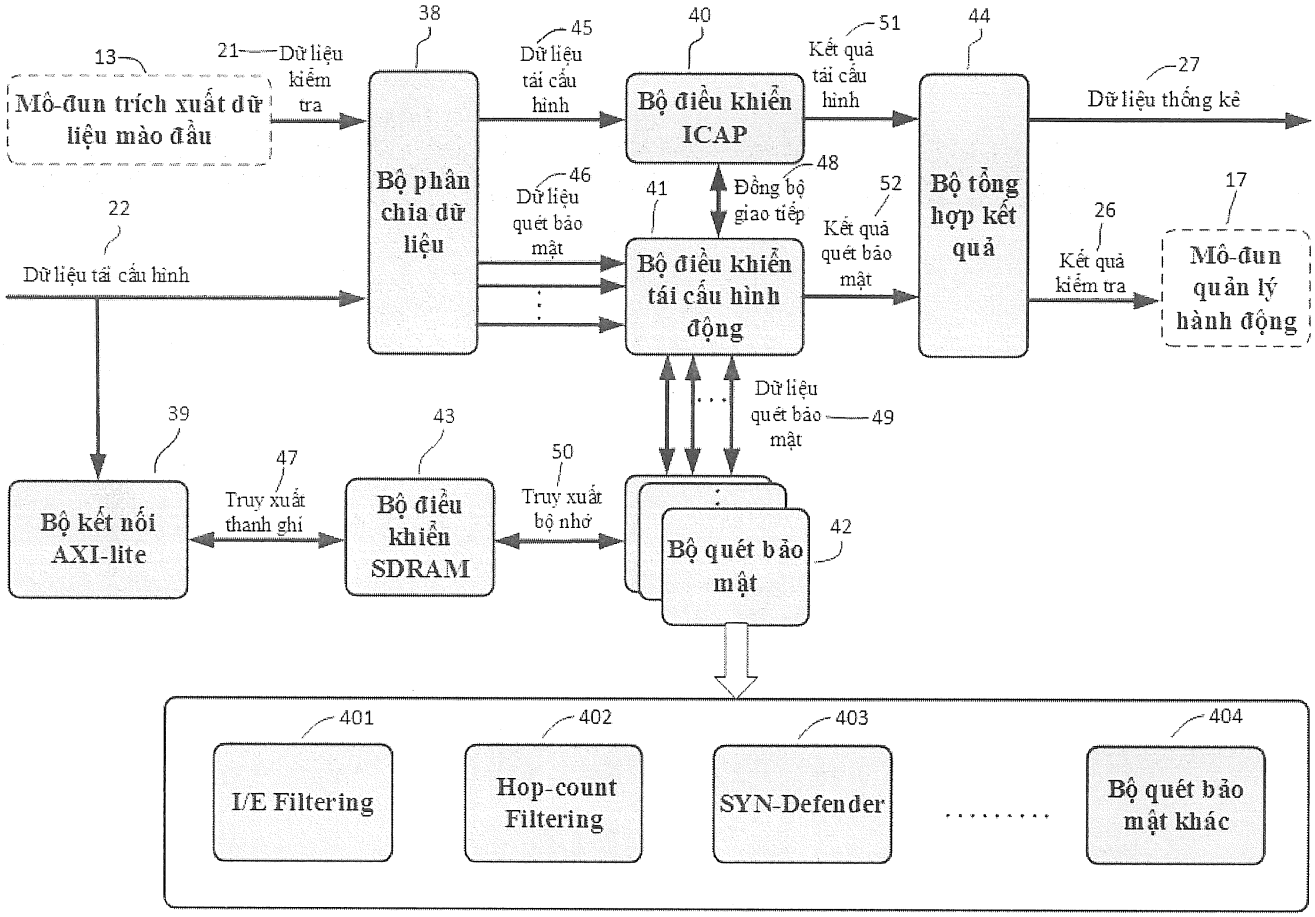
Hình 1


6
Dữ liệu/PCIe
28
Bộ trích xuất mào đầu
1
Gói tin/cổng vật lý
32
Dữ liệu đã trích xuất
29
Bộ phân tách dữ liệu
33
Dữ liệu chuyển mạch
30
OF FIFO
Dữ liệu kiểm tra bảo mật
31
SC FIFO
34
19
Dữ liệu chuyển mạch
14
Mô-đun xử lý chuyển mạch
Dữ liệu kiểm tra
16
Mô-đun xử lý bảo mật
21
Dữ liệu thô
15
PK FIFO
20

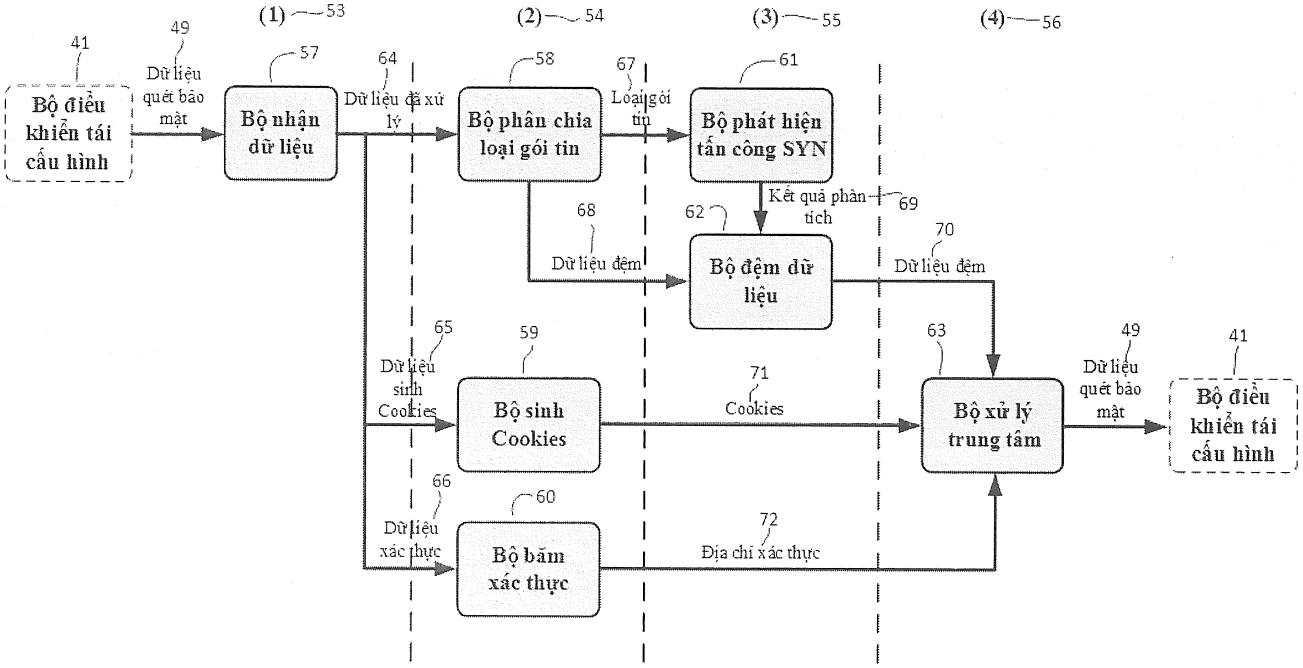
Hình 2


18
Luật chuyển mạch
35
Bộ giao tiếp chuyển mạch
23
Dữ liệu thống kê
Luật chuyển mạch
37
Dữ liệu thống kê
38
19
Dữ liệu chuyển mạch
24
Kết quả chuyển mạch
13
Mô-đun trích xuất dữ liệu mào đầu
Bộ quản lý bảng chuyển mạch
17
Mô-đun quản lý hành động
36

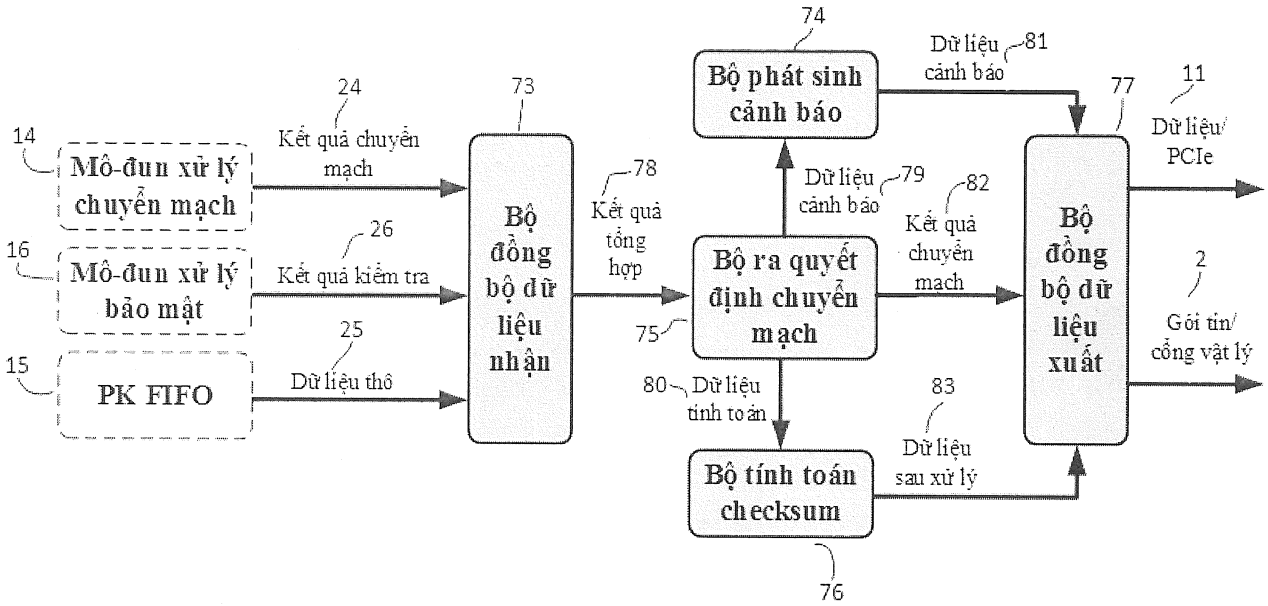
Hình 3


13
Mô-đun trích xuất dữ liệu mào đầu
21
Dữ liệu kiểm tra
38
Bộ phân chia dữ liệu
45
Dữ liệu tái cấu hình
40
Bộ điều khiển ICAP
51
Kết quả tái cấu hình
44
Bộ tổng hợp kết quả
27
Dữ liệu thống kê
22
Dữ liệu tái cấu hình
46
Dữ liệu quét bảo mật
41
Bộ điều khiển tái cấu hình động
48
Đồng bộ giao tiếp
52
Kết quả quét bảo mật
26
Kết quả kiểm tra
17
Mô-đun quản lý hành động
Dữ liệu quét bảo mật
49
39
Bộ kết nối AXI-lite
47
Truy xuất thanh ghi
43
Bộ điều khiển SDRAM
50
Truy xuất bộ nhớ
42
Bộ quét bảo mật
401
I/E Filtering
402
Hop-count Filtering
403
SYN-Defender
404
Bộ quét bảo mật khác

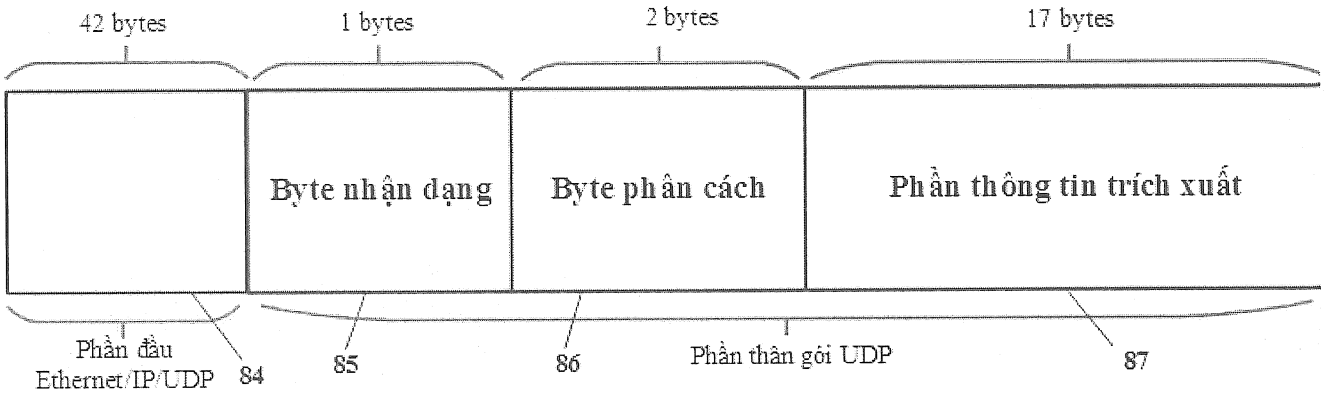
Hình 4


(1)
(2)
(3)
(4)
53
54
55
56
41
Bộ điều khiển tái cấu hình
49
Dữ liệu quét bảo mật
57
Bộ nhận dữ liệu
64
Dữ liệu đã xử lý
58
Bộ phân chia loại gói tin
67
Loại gói tin
61
Bộ phát hiện tấn công SYN
Kết quả phân tích
69
62
68
Dữ liệu đệm
Bộ đệm dữ liệu
70
Dữ liệu đệm
65
Dữ liệu sinh Cookies
59
Bộ sinh Cookies
71
Cookies
63
Bộ xử lý trung tâm
49
Dữ liệu quét bảo mật
41
Bộ điều khiển tái cấu hình
66
Dữ liệu xác thực
60
Bộ băm xác thực
72
Địa chỉ xác thực

Hình 5


14
Mô-đun xử lý chuyển mạch
16
Mô-đun xử lý bảo mật
15
PK FIFO
24
Kết quả chuyển mạch
26
Kết quả kiểm tra
25
Dữ liệu thô
73
Bộ đồng bộ dữ liệu nhận
78
Kết quả tổng hợp
74
Bộ phát sinh cảnh báo
Dữ liệu cảnh báo
81
77
11
Dữ liệu/ PCIe
Dữ liệu cảnh báo
79
82
Kết quả chuyển mạch
Bộ ra quyết định chuyển mạch
75
Bộ đồng bộ dữ liệu xuất
2
Gói tin/ cổng vật lý
80
Dữ liệu tính toán
83
Dữ liệu sau xử lý
Bộ tính toán checksum
76

Hình 6


42 bytes
1 bytes
2 bytes
17 bytes
Byte nhận dạng
Byte phân cách
Phần thông tin trích xuất
Phần đầu
Ethernet/IP/UDP
84
85
86
Phần thân gói UDP
87

Hình 7