(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ

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

(11) **1-0023978**

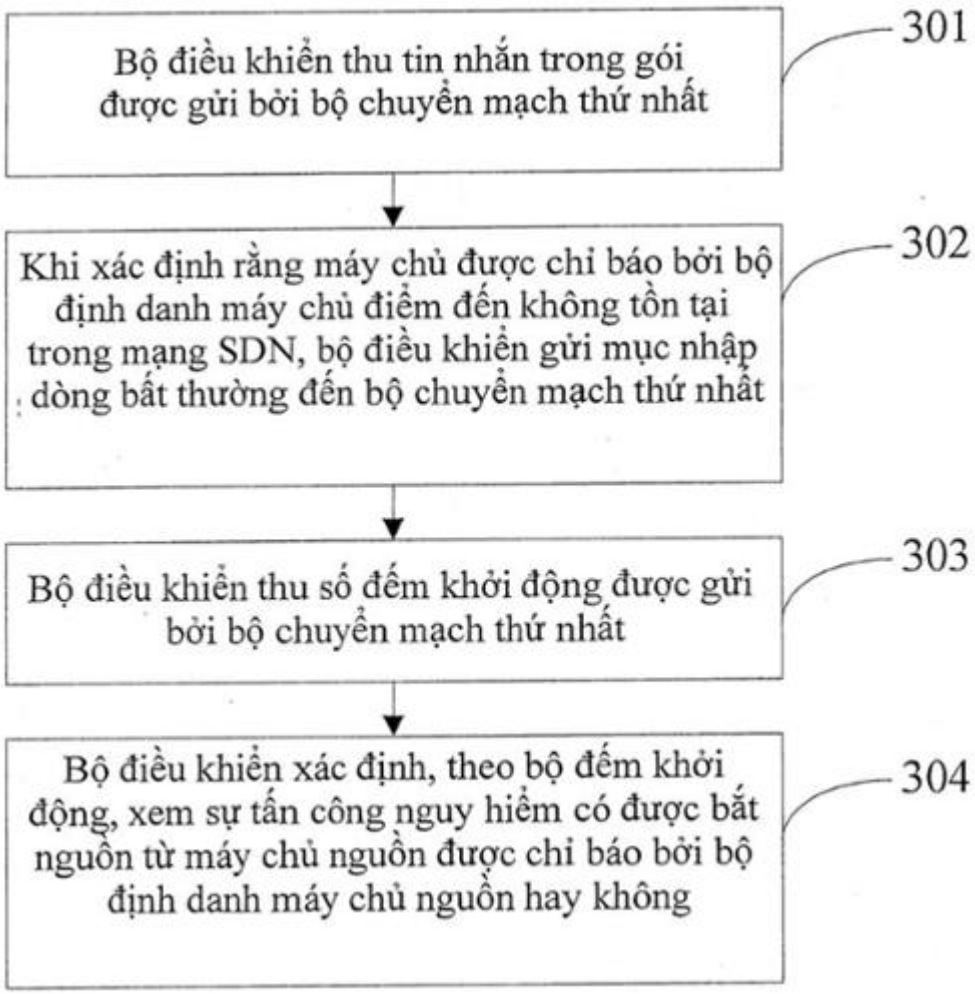
(51)[7] **H04L 29/06**

(13) **B**

(21) 1-2016-02265
(22) 05/09/2014
(86) PCT/CN2014/085989 05/09/2014
(87) WO2015/074451A1 28/05/2015
(30) 201310596661.0 22/11/2013 CN
(45) 25/06/2020 387
(43) 26/09/2016 342A
(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)
Huawei Administration Building, Bantian, Longgang, Shenzhen, Guangdong 518129, China
(72) LIN, Ke (CN); WANG, Yongcan (CN); TIAN, Yingjun (CN)
(74) Công ty TNHH một thành viên Sở hữu trí tuệ VCCI (VCCI-IP CO.,LTD)

(54) PHƯƠNG PHÁP VÀ THIẾT BỊ PHÁT HIỆN SỰ TẤN CÔNG NGUY HIỂM

(57) Sáng chế đề cập đến phương pháp và thiết bị phát hiện sự tấn công nguy hiểm, phương pháp bao gồm các bước: thu, bởi bộ điều khiển, tin nhắn trong gói được gửi bởi bộ chuyển mạch thứ nhất, trong đó tin nhắn trong gói bao gồm bộ định danh máy chủ nguồn và bộ định danh máy chủ điểm đến của gói dữ liệu mà bộ chuyển mạch thứ nhất không tìm thấy mục nhập dòng; khi xác định được rằng máy chủ được chỉ báo bởi bộ định danh máy chủ điểm đến không tồn tại trong mạng do phần mềm quyết định (SDN), gửi, bởi bộ điều khiển, mục nhập dòng bất thường tới bộ chuyển mạch thứ nhất, trong đó mục nhập dòng bất thường bao gồm bộ định danh máy chủ nguồn; thu, bởi bộ điều khiển, số đếm khởi động được gửi bởi bộ chuyển mạch thứ nhất, trong đó số đếm khởi động được gửi bởi bộ chuyển mạch thứ nhất sau khi mục nhập dòng bất thường hết thời gian chờ, và số đếm khởi động là số lượng các lần mà mục nhập dòng bất thường được khởi động; và xác định, bởi bộ điều khiển theo số đếm khởi động, xem sự tấn công nguy hiểm có được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn hay không. Trong các phương án của sáng chế, sự tấn công nguy hiểm từ máy chủ có thể được phát hiện, lượng xử lý dữ liệu của bộ điều khiển có thể được giảm bớt, và hiệu suất của bộ điều khiển có thể được cải thiện.


Bộ điều khiển thu tin nhắn trong gói được gửi bởi bộ chuyển mạch thứ nhất
301
Khi xác định rằng máy chủ được chỉ báo bởi bộ định danh máy chủ điểm đến không tồn tại trong mạng SDN, bộ điều khiển gửi mục nhập dòng bất thường đến bộ chuyển mạch thứ nhất
302
Bộ điều khiển thu số đếm khởi động được gửi bởi bộ chuyển mạch thứ nhất
303
Bộ điều khiển xác định, theo bộ đếm khởi động, xem sự tấn công nguy hiểm có được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn hay không
304

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến các lĩnh vực truyền thông, và cụ thể là, đến phương pháp và thiết bị phát hiện sự tấn công nguy hiểm.

Tình trạng kỹ thuật của sáng chế

Ý tưởng cơ bản của mạng do phần mềm quyết định (SDN, Software Defined Networking) là để thực hiện việc phân tách giữa mặt phẳng điều khiển và mặt phẳng chuyển tiếp. Mạng SDN thông thường bao gồm bộ điều khiển (Controller), bộ chuyển mạch (Switch), và máy chủ (Host). Bộ điều khiển được tạo cấu hình để đề ra, dựa vào hình thức của toàn bộ mạng, chính sách chuyển mạch, và phân phối chính sách chuyển mạch tới bộ chuyển mạch dưới hình thức mục nhập dòng, để bộ chuyển mạch lưu mục nhập dòng vào bảng dòng, và do đó bộ điều khiển thực hiện điều khiển tập trung trên toàn bộ mạng bằng cách điều khiển bảng dòng trên bộ chuyển mạch; bộ chuyển mạch được tạo cấu hình để chuyển tiếp gói dữ liệu của máy chủ theo mục nhập dòng địa phương của bộ chuyển mạch.

Trong mạng SDN, bối cảnh truyền thông thông thường của máy chủ được thể hiện trên Fig.1, trong đó máy chủ A gửi gói dữ liệu tới bộ chuyển mạch 1 được kết nối với máy chủ A, và coi rằng máy chủ điểm đến của gói dữ liệu là máy chủ B trong mạng SDN; bộ chuyển mạch 1 tìm kiếm bảng dòng địa phương cho mục nhập dòng của gói dữ liệu, và nếu bộ chuyển mạch 1 tìm thấy mục nhập dòng của gói dữ liệu, bộ chuyển mạch 1 chuyển tiếp gói dữ liệu theo mục nhập dòng, hoặc nếu bộ chuyển mạch 1 không tìm thấy mục nhập dòng của gói dữ liệu, bộ chuyển mạch 1 gửi tin nhắn trong gói tới bộ điều khiển; bộ điều khiển lựa chọn đường chuyển tiếp cho gói dữ liệu, và phân phối đường chuyển tiếp tới tất cả các bộ chuyển mạch trên đường chuyển tiếp dưới dạng mục nhập dòng; và bộ chuyển mạch 1 và các bộ chuyển mạch trên đường chuyển tiếp chuyển tiếp gói dữ liệu theo mục nhập dòng phân phối.

Do bộ điều khiển đã phân phối mục nhập dòng để truyền thông giữa máy chủ A và máy chủ B tới tất cả các bộ chuyển mạch trên đường chuyển tiếp, khi máy chủ A sau đó gửi gói dữ liệu mà máy chủ điểm đến của nó là máy chủ B, bộ chuyển mạch 1 có thể chuyển tiếp trực tiếp gói dữ liệu theo mục nhập dòng, và bộ chuyển mạch 1 không tạo ra tin nhắn trong gói một lần nữa.

Nếu máy chủ điểm đến của gói dữ liệu được gửi bởi máy chủ là máy chủ C ở ngoài mạng SDN, bối cảnh truyền thông được thể hiện trên Fig.2, trong đó

máy chủ A gửi gói dữ liệu tới bộ chuyển mạch 1 được kết nối với máy chủ A, và được coi rằng máy chủ điểm đến của gói dữ liệu là máy chủ C, và mạng SDN không bao gồm máy chủ C;

bộ chuyển mạch 1 tìm kiếm bảng dòng địa phương của bộ chuyển mạch cho mục nhập dòng của gói dữ liệu, và do máy chủ C không phải trong mạng SDN, bộ chuyển mạch 1 không thể tìm thấy mục nhập dòng của gói dữ liệu, và gửi tin nhắn trong gói tới bộ điều khiển; và

bộ điều khiển thu tin nhắn trong gói, và tìm kiếm mạng SDN cho máy chủ C; do máy chủ C không phải trong mạng SDN, bộ điều khiển không thể tìm thấy máy chủ C, và sau đó bộ điều khiển loại bỏ tin nhắn trong gói, và không phân phối mục nhập dòng cho gói dữ liệu tới bộ chuyển mạch 1.

Nếu máy chủ A sau đó gửi lại gói dữ liệu mà máy chủ điểm đến của nó là máy chủ C, cả bộ chuyển mạch 1 lẫn bộ điều khiển đều lặp lại các bước nêu trên, và cuối cùng bộ điều khiển loại bỏ tin nhắn trong gói.

Dựa vào phương pháp truyền thông nêu trên của máy chủ trong mạng SDN, có thể coi rằng tin nhắn trong gói trong bối cảnh được thể hiện trên Fig.1 là tin nhắn trong gói bình thường, trong khi tin nhắn trong gói trong bối cảnh được thể hiện trên Fig.2 là tin nhắn trong gói không hợp lệ. Nếu máy chủ trong mạng SDN thực hiện sự tấn công nguy hiểm trên bộ điều khiển, và gửi số lượng lớn các gói dữ liệu mà máy chủ điểm đến của chúng không phải là trong mạng SDN hoặc máy chủ điểm đến của chúng thậm chí không tồn tại, bộ chuyển mạch được kết nối với máy chủ tạo ra lượng lớn các tin nhắn trong gói không hợp lệ và gửi các

tin nhắn trong gói không hợp lệ tới bộ điều khiển, và bộ điều khiển cần phải tiêu thụ một lượng lớn các tài nguyên xử lý để xử lý các tin nhắn trong gói không hợp lệ này, để tìm máy chủ điểm đến mà không phải trong mạng SDN hoặc thậm chí không tồn tại, do đó ảnh hưởng đến quy trình xử lý của tin nhắn trong gói bình thường bởi bộ điều khiển.

Do đó, việc phát hiện sự tấn công nguy hiểm trên bộ điều khiển từ máy chủ cần phải được thực hiện trong mạng SDN. Hiện nay, phương pháp phát hiện sự tấn công nguy hiểm từ máy chủ là như sau: bộ điều khiển thu thập các thống kê về số lượng các tin nhắn trong gói, được tạo ra tương ứng bởi mỗi máy chủ là máy chủ nguồn, được thu trong một thời gian đơn vị; tính toán, bằng cách sử dụng số lượng, hệ số ở đó mỗi máy chủ tạo ra các tin nhắn trong gói là máy chủ nguồn; và xác định, theo hệ số, xem mỗi máy chủ có thực hiện sự tấn công nguy hiểm trên bộ điều khiển hay không.

Trong phương pháp phát hiện sự tấn công nguy hiểm từ máy chủ như vậy, bộ điều khiển cần phải thu tin nhắn trong gói được thông báo bởi mỗi bộ chuyển mạch và xử lý tin nhắn trong gói; ngoài ra, bộ điều khiển còn cần thu thập một cách độc lập các thống kê về số lượng các tin nhắn trong gói, được tạo ra tương ứng bởi mỗi máy chủ là máy chủ nguồn, được thu trong thời gian đơn vị, và sau đó xác định xem mỗi máy chủ có thực hiện sự tấn công nguy hiểm trên bộ điều khiển hay không. Lượng dữ liệu được xử lý bởi bộ điều khiển là lớn, và hiệu suất của bộ điều khiển là thấp.

Bản chất kỹ thuật của sáng chế

Các phương án của sáng chế đề xuất phương pháp và thiết bị phát hiện sự tấn công nguy hiểm, sao cho sự tấn công nguy hiểm từ máy chủ có thể được phát hiện, lượng xử lý dữ liệu của bộ điều khiển có thể được giảm bớt, và hiệu suất của bộ điều khiển có thể được cải thiện.

Theo khía cạnh thứ nhất, phương pháp phát hiện sự tấn công nguy hiểm được đề xuất, bao gồm:

thu, bởi bộ điều khiển, tin nhắn trong gói được gửi bởi bộ chuyển

mạch thứ nhất, trong đó tin nhắn trong gói bao gồm bộ định danh máy chủ nguồn và bộ định danh máy chủ điểm đến của gói dữ liệu mà bộ chuyển mạch thứ nhất không tìm thấy mục nhập dòng;

khi xác định được rằng máy chủ được chỉ báo bởi bộ định danh máy chủ điểm đến không tồn tại trong mạng SDN, gửi, bởi bộ điều khiển, mục nhập dòng bất thường tới bộ chuyển mạch thứ nhất, trong đó mục nhập dòng bất thường bao gồm bộ định danh máy chủ nguồn;

thu, bởi bộ điều khiển, số đếm khởi động được gửi bởi bộ chuyển mạch thứ nhất, trong đó số đếm khởi động được gửi bởi bộ chuyển mạch thứ nhất sau khi mục nhập dòng bất thường hết thời gian chờ, và số đếm khởi động là số lượng các lần mà mục nhập dòng bất thường được khởi động; và

xác định, bởi bộ điều khiển theo số đếm khởi động, xem sự tấn công nguy hiểm có được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn hay không.

Theo khía cạnh thứ nhất, trong cách có thể thực hiện thứ nhất của khía cạnh thứ nhất, việc xác định, bởi bộ điều khiển theo số đếm khởi động, xem sự tấn công nguy hiểm được bắt nguồn từ máy chủ nguồn có được chỉ báo bởi bộ định danh máy chủ nguồn hay không bao gồm các bước:

tính toán, bởi bộ điều khiển, hệ số khởi động của mục nhập dòng bất thường theo số đếm khởi động và thời gian trôi qua của mục nhập dòng bất thường; và

xác định, bởi bộ điều khiển, xem hệ số khởi động có lớn hơn ngưỡng hệ số hay không; và nếu hệ số khởi động lớn hơn ngưỡng hệ số, xác định, bởi bộ điều khiển, rằng sự tấn công nguy hiểm được bắt nguồn từ máy chủ nguồn; hoặc, nếu hệ số khởi động không lớn hơn ngưỡng hệ số, xác định, bởi bộ điều khiển, rằng không có sự tấn công nguy hiểm nào bắt nguồn từ máy chủ nguồn.

Theo khía cạnh thứ nhất, trong cách có thể thực hiện thứ hai của khía cạnh thứ nhất, việc xác định, bởi bộ điều khiển theo số đếm khởi động, xem sự tấn công nguy hiểm được bắt nguồn từ máy chủ nguồn có được chỉ báo bởi bộ định

danh máy chủ nguồn hay không bao gồm các bước:

xác định, bởi bộ điều khiển, xem số đếm khởi động có lớn hơn ngưỡng số đếm hay không; và nếu số đếm khởi động lớn hơn ngưỡng số đếm, xác định, bởi bộ điều khiển, rằng sự tấn công nguy hiểm được bắt nguồn từ máy chủ nguồn; hoặc hoặc, nếu số đếm khởi động không lớn hơn ngưỡng số đếm, xác định, bởi bộ điều khiển, rằng không có sự tấn công nguy hiểm nào bắt nguồn từ máy chủ nguồn.

Theo khía cạnh thứ nhất, và/hoặc cách có thể thực hiện thứ nhất của khía cạnh thứ nhất, và/hoặc cách có thể thực hiện thứ hai của khía cạnh thứ nhất, trong cách có thể thực hiện thứ ba của khía cạnh thứ nhất, trước khi gửi, bởi bộ điều khiển, mục nhập dòng bất thường tới bộ chuyển mạch thứ nhất, phương pháp ngoài ra còn bao gồm các bước:

xác định, bởi bộ điều khiển, xem mục nhập dòng bất thường của máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn đã được phân phối tới bộ chuyển mạch thứ nhất hay chưa; và nếu mục nhập dòng bất thường của máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn chưa được phân phối tới bộ chuyển mạch thứ nhất, thực hiện, bởi bộ điều khiển, bước gửi mục nhập dòng bất thường tới bộ chuyển mạch thứ nhất.

Theo khía cạnh thứ nhất, và/hoặc cách có thể thực hiện thứ nhất của khía cạnh thứ nhất, và/hoặc cách có thể thực hiện thứ hai của khía cạnh thứ nhất, và/hoặc cách có thể thực hiện thứ ba của khía cạnh thứ nhất, trong cách có thể thực hiện thứ tư của khía cạnh thứ nhất, phương pháp ngoài ra còn bao gồm các bước:

khi xác định được rằng bảng dòng cuối cùng trong bộ chuyển mạch thứ nhất là bảng dung hợp chính xác bao gồm miền dung hợp bộ định danh máy chủ nguồn, gửi, bởi bộ điều khiển, chỉ dẫn thứ nhất tới bộ chuyển mạch thứ nhất, trong đó chỉ dẫn thứ nhất được sử dụng để chỉ dẫn cho bộ chuyển mạch thứ nhất tạo cấu hình bảng dung hợp chính xác như bảng dung hợp chính xác chỉ khớp với miền dung hợp bộ định danh máy chủ nguồn, để bộ chuyển mạch thứ nhất lưu trữ

mục nhập dòng bất thường trong bảng dòng cuối cùng.

Theo khía cạnh thứ nhất, và/hoặc cách có thể thực hiện thứ nhất của khía cạnh thứ nhất, và/hoặc cách có thể thực hiện thứ hai của khía cạnh thứ nhất, và/hoặc cách có thể thực hiện thứ ba của khía cạnh thứ nhất, trong cách có thể thực hiện thứ năm của khía cạnh thứ nhất, phương pháp ngoài ra còn bao gồm các bước:

khi xác định được rằng bảng dòng cuối cùng trong bộ chuyển mạch thứ nhất là bảng dung hợp chính xác, và bảng ký tự đại diện bao gồm miền dung hợp bộ định danh máy chủ nguồn tồn tại trong bộ chuyển mạch thứ nhất, gửi, bởi bộ điều khiển, chỉ dẫn thứ hai tới bộ chuyển mạch thứ nhất, trong đó chỉ dẫn thứ hai được sử dụng để chỉ dẫn cho bộ chuyển mạch thứ nhất điều chỉnh bảng ký tự đại diện bao gồm miền dung hợp bộ định danh máy chủ nguồn thành bảng dòng cuối cùng, để bộ chuyển mạch thứ nhất lưu trữ mục nhập dòng bất thường trong bảng dòng cuối cùng.

Theo khía cạnh thứ nhất, và/hoặc cách có thể thực hiện thứ nhất của khía cạnh thứ nhất, và/hoặc cách có thể thực hiện thứ hai của khía cạnh thứ nhất, và/hoặc cách có thể thực hiện thứ ba của khía cạnh thứ nhất, và/hoặc cách có thể thực hiện thứ tư của khía cạnh thứ nhất, và/hoặc cách có thể thực hiện thứ năm của khía cạnh thứ nhất, trong cách có thể thực hiện thứ sáu của khía cạnh thứ nhất, quyền ưu tiên của mục nhập dòng bất thường là quyền ưu tiên thấp nhất của mục nhập dòng trong bộ chuyển mạch thứ nhất.

Theo khía cạnh thứ nhất, và/hoặc cách có thể thực hiện thứ nhất của khía cạnh thứ nhất, và/hoặc cách có thể thực hiện thứ hai của khía cạnh thứ nhất, và/hoặc cách có thể thực hiện thứ ba của khía cạnh thứ nhất, và/hoặc cách có thể thực hiện thứ tư của khía cạnh thứ nhất, và/hoặc cách có thể thực hiện thứ năm của khía cạnh thứ nhất, và/hoặc cách có thể thực hiện thứ sáu của khía cạnh thứ nhất, trong cách có thể thực hiện thứ bảy của khía cạnh thứ nhất, phương pháp ngoài ra còn bao gồm các bước:

khi xác định, theo số đếm khởi động, rằng sự tấn công nguy hiểm

được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn, gửi, bởi bộ điều khiển, chỉ dẫn thứ ba tới bộ chuyển mạch thứ nhất, trong đó chỉ dẫn thứ ba được sử dụng để chỉ dẫn cho bộ chuyển mạch thứ nhất xóa gói dữ liệu từ máy chủ nguồn.

Theo khía cạnh thứ hai, phương pháp phát hiện sự tấn công nguy hiểm được đề xuất, bao gồm các bước:

khi xác định được rằng mục nhập dòng tương ứng với gói dữ liệu không được tìm thấy, gửi, bởi bộ chuyển mạch thứ nhất, tin nhắn trong gói tới bộ điều khiển, trong đó tin nhắn trong gói bao gồm bộ định danh máy chủ nguồn và bộ định danh máy chủ điểm đến của gói dữ liệu;

thu và lưu, bởi bộ chuyển mạch thứ nhất, mục nhập dòng bất thường, trong đó mục nhập dòng bất thường được gửi bởi bộ điều khiển khi xác định được rằng máy chủ được chỉ báo bởi bộ định danh máy chủ điểm đến không tồn tại trong mạng SDN; và

ghi, bởi bộ chuyển mạch thứ nhất trong khoảng thời gian trôi qua của mục nhập dòng bất thường, số đếm khởi động của mục nhập dòng bất thường, và gửi số đếm khởi động tới bộ điều khiển sau khi mục nhập dòng bất thường hết thời gian chờ, khiến cho bộ điều khiển xác định, theo số đếm khởi động, xem sự tấn công nguy hiểm có được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn hay không.

Theo khía cạnh thứ hai, trong cách có thể thực hiện thứ nhất của khía cạnh thứ hai, phương pháp ngoài ra còn bao gồm các bước:

thu, bởi bộ chuyển mạch thứ nhất, chỉ dẫn thứ nhất được gửi bởi bộ điều khiển, và tạo cấu hình, theo chỉ dẫn thứ nhất, bảng dung hợp chính xác địa phương mà là bảng dòng cuối cùng như bảng dung hợp chính xác chỉ khớp với miền dung hợp bộ định danh máy chủ nguồn; hoặc,

thu, bởi bộ chuyển mạch thứ nhất, chỉ dẫn thứ hai được gửi bởi bộ điều khiển, và điều chỉnh bảng ký tự đại diện bao gồm miền dung hợp bộ định danh máy chủ nguồn thành bảng dòng cuối cùng theo chỉ dẫn thứ hai.

Theo cách có thể thực hiện thứ nhất của khía cạnh thứ hai, trong cách có thể thực hiện thứ hai của khía cạnh thứ hai, việc lưu, bởi bộ chuyển mạch thứ nhất, mục nhập dòng bất thường bao gồm các bước:

lưu, bởi bộ chuyển mạch thứ nhất, mục nhập dòng bất thường vào bảng dòng cuối cùng.

Theo khía cạnh thứ hai, và/hoặc cách có thể thực hiện thứ nhất của khía cạnh thứ hai, và/hoặc cách có thể thực hiện thứ hai của khía cạnh thứ hai, trong cách có thể thực hiện thứ ba của khía cạnh thứ hai, phương pháp ngoài ra còn bao gồm các bước:

thu, bởi bộ chuyển mạch thứ nhất, chỉ dẫn thứ ba được gửi bởi bộ điều khiển, trong đó chỉ dẫn thứ ba được gửi bởi bộ điều khiển khi xác định, theo số đếm khởi động, rằng sự tấn công nguy hiểm được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn; và

xóa, bởi bộ chuyển mạch thứ nhất theo chỉ dẫn thứ ba, gói dữ liệu từ máy chủ nguồn.

Theo khía cạnh thứ ba, thiết bị phát hiện sự tấn công nguy hiểm được đề xuất, bao gồm:

bộ thu thứ nhất, được tạo cấu hình để thu tin nhắn trong gói được gửi bởi bộ chuyển mạch thứ nhất, trong đó tin nhắn trong gói bao gồm bộ định danh máy chủ nguồn và bộ định danh máy chủ điểm đến của gói dữ liệu mà bộ chuyển mạch thứ nhất không tìm thấy mục nhập dòng;

bộ gửi thứ nhất, được tạo cấu hình để: khi xác định được rằng máy chủ được chỉ báo bởi bộ định danh máy chủ điểm đến được thu bởi bộ thu thứ nhất không tồn tại trong mạng SDN, gửi mục nhập dòng bất thường tới bộ chuyển mạch thứ nhất, trong đó mục nhập dòng bất thường bao gồm bộ định danh máy chủ nguồn, trong đó

bộ thu thứ nhất ngoài ra còn được tạo cấu hình để thu số đếm khởi động được gửi bởi bộ chuyển mạch thứ nhất, trong đó số đếm khởi động được gửi bởi bộ chuyển mạch thứ nhất sau khi mục nhập dòng bất thường hết thời gian

chờ, và số đếm khởi động là số lượng các lần mà mục nhập dòng bất thường được khởi động; và

bộ phát hiện, được tạo cấu hình để xác định, theo số đếm khởi động được thu bởi bộ thu thứ nhất, xem sự tấn công nguy hiểm có được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn hay không.

Theo khía cạnh thứ ba, trong cách có thể thực hiện thứ nhất của khía cạnh thứ ba, bộ phát hiện được tạo cấu hình riêng để:

tính toán hệ số khởi động của mục nhập dòng bất thường theo số đếm khởi động được thu bởi bộ thu thứ nhất và thời gian trôi qua của mục nhập dòng bất thường; và

xác định xem hệ số khởi động có lớn hơn ngưỡng hệ số hay không; và nếu hệ số khởi động lớn hơn ngưỡng hệ số, xác định rằng sự tấn công nguy hiểm được bắt nguồn từ máy chủ nguồn; hoặc, nếu hệ số khởi động không lớn hơn ngưỡng hệ số, xác định rằng không có sự tấn công nguy hiểm nào bắt nguồn từ máy chủ nguồn.

Theo khía cạnh thứ ba, trong cách có thể thực hiện thứ hai của khía cạnh thứ ba, bộ phát hiện được tạo cấu hình riêng để:

xác định xem số đếm khởi động có lớn hơn ngưỡng số đếm hay không; và nếu số đếm khởi động lớn hơn ngưỡng số đếm, xác định rằng sự tấn công nguy hiểm được bắt nguồn từ máy chủ nguồn; hoặc nếu, hệ số khởi động không lớn hơn ngưỡng hệ số, xác định rằng không có sự tấn công nguy hiểm nào bắt nguồn từ máy chủ nguồn.

Theo khía cạnh thứ ba, và/hoặc cách có thể thực hiện thứ nhất của khía cạnh thứ ba, và/hoặc cách có thể thực hiện thứ hai của khía cạnh thứ ba, trong cách có thể thực hiện thứ ba của khía cạnh thứ ba, phương pháp ngoài ra còn bao gồm các bước:

bộ xác định, được tạo cấu hình để xác định xem mục nhập dòng bất thường của máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn đã được phân phối tới bộ chuyển mạch thứ nhất hay chưa; và nếu mục nhập dòng

bất thường của máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn chưa được phân phối tới bộ chuyển mạch thứ nhất, khởi động bộ gửi thứ nhất để gửi mục nhập dòng bất thường tới bộ chuyển mạch thứ nhất.

Theo khía cạnh thứ ba, và/hoặc cách có thể thực hiện thứ nhất của khía cạnh thứ ba, và/hoặc cách có thể thực hiện thứ hai của khía cạnh thứ ba, và/hoặc cách có thể thực hiện thứ ba của khía cạnh thứ ba, trong cách có thể thực hiện thứ tư của khía cạnh thứ ba, bộ gửi thứ nhất ngoài ra còn được tạo cấu hình để: khi xác định được rằng bảng dòng cuối cùng trong bộ chuyển mạch thứ nhất là bảng dung hợp chính xác bao gồm miền dung hợp bộ định danh máy chủ nguồn, chỉ dẫn bộ chuyển mạch thứ nhất tạo cấu hình bảng dung hợp chính xác như bảng dung hợp chính xác chỉ khớp với miền dung hợp bộ định danh máy chủ nguồn, để bộ chuyển mạch thứ nhất lưu trữ mục nhập dòng bất thường trong bảng dòng cuối cùng.

Theo khía cạnh thứ ba, và/hoặc cách có thể thực hiện thứ nhất của khía cạnh thứ ba, và/hoặc cách có thể thực hiện thứ hai của khía cạnh thứ ba, và/hoặc cách có thể thực hiện thứ ba của khía cạnh thứ ba, trong cách có thể thực hiện thứ năm của khía cạnh thứ ba, bộ gửi thứ nhất ngoài ra còn được tạo cấu hình để:

khi xác định được rằng bảng dòng cuối cùng trong bộ chuyển mạch thứ nhất là bảng dung hợp chính xác, và bảng ký tự đại diện bao gồm miền dung hợp bộ định danh máy chủ nguồn tồn tại trong bộ chuyển mạch thứ nhất, gửi chỉ dẫn thứ hai tới bộ chuyển mạch thứ nhất, trong đó chỉ dẫn thứ hai được sử dụng để chỉ dẫn cho bộ chuyển mạch thứ nhất điều chỉnh bảng ký tự đại diện bao gồm miền dung hợp bộ định danh máy chủ nguồn thành bảng dòng cuối cùng, để bộ chuyển mạch thứ nhất lưu trữ mục nhập dòng bất thường trong bảng dòng cuối cùng.

Theo khía cạnh thứ ba, và/hoặc cách có thể thực hiện thứ nhất của khía cạnh thứ ba, và/hoặc cách có thể thực hiện thứ hai của khía cạnh thứ ba, và/hoặc cách có thể thực hiện thứ ba của khía cạnh thứ ba, và/hoặc cách có thể thực hiện thứ tư của khía cạnh thứ ba, và/hoặc cách có thể thực hiện thứ năm của khía cạnh thứ ba, trong cách có thể thực hiện thứ sáu của khía cạnh thứ ba, bộ gửi thứ nhất ngoài ra

còn được tạo cấu hình để:

khi xác định được, theo số đếm khởi động, rằng sự tấn công nguy hiểm được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn, gửi chỉ dẫn thứ ba tới bộ chuyển mạch thứ nhất, trong đó chỉ dẫn thứ ba được sử dụng để chỉ dẫn cho bộ chuyển mạch thứ nhất xóa gói dữ liệu từ máy chủ nguồn.

Theo khía cạnh thứ tư, thiết bị phát hiện sự tấn công nguy hiểm được đề xuất, bao gồm:

bộ gửi thứ hai, được tạo cấu hình để: khi xác định được rằng mục nhập dòng tương ứng với gói dữ liệu không được tìm thấy, gửi tin nhắn trong gói tới bộ điều khiển, trong đó tin nhắn trong gói bao gồm bộ định danh máy chủ nguồn và bộ định danh máy chủ điểm đến của gói dữ liệu;

bộ thu thứ hai, được tạo cấu hình để thu mục nhập dòng bất thường, trong đó mục nhập dòng bất thường được gửi bởi bộ điều khiển khi xác định được rằng máy chủ được chỉ báo bởi bộ định danh máy chủ điểm đến không tồn tại trong mạng SDN;

bộ lưu trữ, được tạo cấu hình để lưu mục nhập dòng bất thường được thu bởi bộ thu thứ hai; và

bộ ghi số đếm, được tạo cấu hình để ghi, trong khoảng thời gian trôi qua của mục nhập dòng bất thường được lưu bởi bộ lưu trữ, số đếm khởi động của mục nhập dòng bất thường, trong đó

bộ gửi thứ hai ngoài ra còn được tạo cấu hình để: sau khi mục nhập dòng bất thường được lưu bởi bộ lưu trữ hết hạn, gửi số đếm khởi động được ghi bởi bộ ghi số đếm tới bộ điều khiển, khiến cho bộ điều khiển xác định, theo số đếm khởi động, xem sự tấn công nguy hiểm có được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn hay không.

Theo khía cạnh thứ tư, trong cách có thể thực hiện thứ nhất của khía cạnh thứ hai, bộ thu thứ hai ngoài ra còn được tạo cấu hình để thu chỉ dẫn thứ nhất được gửi bởi bộ điều khiển; và

thiết bị ngoài ra còn bao gồm: bộ cấu hình, được tạo cấu hình để tạo cấu hình, theo chỉ dẫn thứ nhất, bảng dung hợp chính xác địa phương mà là bảng dòng cuối cùng như bảng dung hợp chính xác chỉ khớp với miền dung hợp bộ định danh máy chủ nguồn; hoặc

bộ thu thứ hai ngoài ra còn được tạo cấu hình để thu chỉ dẫn thứ hai được gửi bởi bộ điều khiển; và

thiết bị ngoài ra còn bao gồm: bộ cấu hình, được tạo cấu hình để điều chỉnh bảng ký tự đại diện bao gồm miền dung hợp bộ định danh máy chủ nguồn thành bảng dòng cuối cùng theo chỉ dẫn thứ hai.

Theo cách có thể thực hiện thứ nhất của khía cạnh thứ hai, trong cách có thể thực hiện thứ hai của khía cạnh thứ hai, bộ lưu trữ được tạo cấu hình riêng để lưu mục nhập dòng bất thường vào bảng dòng cuối cùng.

Theo khía cạnh thứ hai, và/hoặc cách có thể thực hiện thứ nhất của khía cạnh thứ hai, và/hoặc cách có thể thực hiện thứ hai của khía cạnh thứ hai, trong cách có thể thực hiện thứ ba của khía cạnh thứ hai, bộ thu thứ hai ngoài ra còn được tạo cấu hình để thu chỉ dẫn thứ ba được gửi bởi bộ chuyển mạch thứ nhất; và

thiết bị ngoài ra còn bao gồm: bộ điều khiển, được tạo cấu hình để xóa gói dữ liệu từ máy chủ nguồn.

Trong các phương án này, bộ điều khiển thu tin nhắn trong gói được gửi bởi bộ chuyển mạch thứ nhất, trong đó tin nhắn trong gói bao gồm bộ định danh máy chủ nguồn và bộ định danh máy chủ điểm đến của gói dữ liệu mà bộ chuyển mạch thứ nhất không tìm thấy mục nhập dòng; khi xác định được rằng máy chủ được chỉ báo bởi bộ định danh máy chủ điểm đến không tồn tại trong mạng SDN, bộ điều khiển gửi mục nhập dòng bất thường tới bộ chuyển mạch thứ nhất, trong đó mục nhập dòng bất thường bao gồm bộ định danh máy chủ nguồn; bộ điều khiển thu số đếm khởi động, của mục nhập dòng bất thường, được gửi bởi bộ chuyển mạch thứ nhất sau khi mục nhập dòng bất thường hết thời gian chờ; và bộ điều khiển xác định, theo số đếm khởi động, xem sự tấn công nguy hiểm có được

bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn hay không. Trong các phương án, bộ điều khiển không cần thiết phải thu thập các thống kê về các tin nhắn trong gói tương ứng với mỗi máy chủ, thay vào đó, bộ chuyển mạch thứ nhất thu thập thống kê bằng cách sử dụng số đếm khởi động của mục nhập dòng bất thường. Theo cách này, việc thu thập các thống kê tin nhắn được thực hiện đầu tiên bởi bộ điều khiển được phân phối tới mỗi bộ chuyển mạch để thực hiện, do đó giảm bớt lượng xử lý dữ liệu của bộ điều khiển, và cải thiện hiệu suất của bộ điều khiển.

Mô tả vắn tắt các hình vẽ

Nhằm mô tả các giải pháp kỹ thuật trong các phương án của sáng chế hoặc trong kỹ thuật đã biết một cách rõ ràng hơn, dưới đây giới thiệu sơ lược các hình vẽ kèm theo cần thiết để mô tả các phương án. Rõ ràng rằng, các hình vẽ kèm theo trong phần mô tả dưới đây đơn thuần chỉ thể hiện một số phương án của sáng chế, và người có trình độ trung bình trong lĩnh vực vẫn có thể tạo ra các hình vẽ khác từ các hình vẽ kèm theo này mà không cần các nỗ lực mang tính sáng tạo.

Fig.1 là hình vẽ bối cảnh truyền thông máy chủ 1 trong mạng SDN trong kỹ thuật đã biết;

Fig.2 là hình vẽ bối cảnh truyền thông máy chủ 2 trong mạng SDN trong kỹ thuật đã biết;

Fig.2A là sơ đồ cấu trúc bảng dòng trong bộ chuyển mạch trong kỹ thuật đã biết;

Fig.3 là lưu đồ của phương pháp phát hiện sự tấn công nguy hiểm theo phương án thứ nhất của sáng chế;

Fig.4 là lưu đồ của phương pháp phát hiện sự tấn công nguy hiểm theo phương án thứ hai của sáng chế;

Fig.5 là lưu đồ của phương pháp phát hiện sự tấn công nguy hiểm theo phương án thứ ba của sáng chế;

Fig.5A là sơ đồ so sánh trước và sau bảng dung hợp chính xác mà là bảng

dòng cuối cùng được tạo cấu hình theo sáng chế;

Fig.5B là sơ đồ cấu trúc các vị trí lúc trước của bảng dung hợp chính xác và bảng ký tự đại diện được hoán đổi theo sáng chế;

Fig.5C là sơ đồ cấu trúc các vị trí lúc sau của bảng dung hợp chính xác và bảng ký tự đại diện được hoán đổi theo sáng chế;

Fig.5D là sơ đồ cấu trúc cách thực hiện của mục nhập dòng bất thường theo sáng chế;

Fig.6 là lược đồ cấu trúc của thiết bị phát hiện sự tấn công nguy hiểm theo phương án thứ nhất của sáng chế;

Fig.7 là lược đồ cấu trúc của thiết bị phát hiện sự tấn công nguy hiểm theo phương án thứ hai của sáng chế;

Fig.8 là lược đồ cấu trúc của bộ điều khiển theo sáng chế; và

Fig.9 là lược đồ cấu trúc của bộ chuyển mạch theo sáng chế.

Mô tả chi tiết sáng chế

Đầu tiên, bảng dòng trong bộ chuyển mạch và cấu trúc bảng dòng được mô tả.

Thông thường, bộ chuyển mạch bao gồm ít nhất một bảng dòng và tối đa 255 bảng dòng. Bộ chuyển mạch bao gồm đường liên hợp, các bảng dòng của bộ chuyển mạch được bố trí trong đường liên hợp theo thứ tự. Bộ chuyển mạch không cần thiết phải sử dụng tất cả các bảng dòng trong bộ chuyển mạch, mà có thể chỉ một số bảng dòng. Ví dụ như, bộ chuyển mạch trên Fig.2A có thể bao gồm mười bảng dòng, nhưng bộ chuyển mạch thực chất sử dụng chỉ bảy bảng dòng đầu tiên bảng 0 đến bảng 6 trong đường liên hợp, ba bảng dòng cuối bảng 7 đến bảng 9 không được thể hiện trên các Fig. và không được sử dụng bởi bộ chuyển mạch. Mục nhập dòng được lưu trữ trong bảng dòng và được sử dụng để ghi đường chuyển tiếp giữa hai máy chủ.

Như được thể hiện trên Fig.2A, khi thu gói dữ liệu, bộ chuyển mạch tìm kiếm, theo gói dữ liệu, các bảng dòng của đường liên hợp theo thứ tự cho mục nhập dòng mà có thể khớp với gói dữ liệu, cho đến khi mục nhập dòng mà có thể

khớp với gói dữ liệu được tìm thấy, hoặc cho đến khi bảng dòng cuối cùng được tìm kiếm trong khi không có mục nhập dòng nào mà có thể khớp với gói dữ liệu được tìm thấy.

Bảng dòng là cốt lõi của chính sách chuyển tiếp của bộ chuyển mạch, và tương tự với bảng định tuyến của bộ định tuyến hội tụ, và chiếm giữ hầu hết các phần của các tài nguyên lưu trữ của bộ chuyển mạch. Các bảng dòng có thể được phân chia thành hai loại: bảng ký tự đại diện và bảng dung hợp chính xác:

Trong bảng dung hợp chính xác, các chỉ số cụ thể phải được cung cấp cho tất cả các miền dung hợp của mục nhập dòng. Khi gói dữ liệu được khớp với mục nhập dòng trong bảng dung hợp chính xác, coi rằng gói dữ liệu và mục nhập dòng chỉ khớp khi các giá trị của tất cả các miền dung hợp của gói dữ liệu và các giá trị của mục nhập dòng là tương ứng bằng nhau. Ví dụ như, như được thể hiện trên bảng 1, bảng dung hợp chính xác bao gồm năm miền dung hợp: giao thức Internet nguồn (Src IP), giao thức Internet điểm đến (Dst IP), cổng nguồn (SrcPort), cổng điểm đến (DstPort), và giao thức IP (IP Protocol), và ba chỉ dẫn (Instructions): viết các hành động (Write Actions), viết siêu dữ liệu (Write Metadata), và đi tới bảng (GoToTable). Mỗi miền dung hợp trong mục nhập dòng được thể hiện trên bảng 1 có giá trị cụ thể. Khi gói dữ liệu được khớp với mục nhập dòng, có thể coi rằng gói dữ liệu khớp với mục nhập dòng chỉ khi các giá trị của năm miền dung hợp: Src IP, Dst IP, SrcPort, DstPort, và giao thức IP của gói dữ liệu và các giá trị của mục nhập dòng là tương ứng bằng nhau.

Bảng 1

Các miền dung hợp					Các chỉ dẫn		
Src IP	Dst IP	SrcPort	DstPort	Giao thức IP	Viết các hành động	Viết siêu dữ liệu	Đi tới bảng
192.168.1.1	192.168.20.1	1000	3000	TCP			Bảng 5

Trong bảng ký tự đại diện, các giá trị có thể được cung cấp chỉ một phần các

miền dung hợp của mục nhập dòng. Khi gói dữ liệu được khớp với mục nhập dòng trong bảng ký tự đại diện, được coi rằng gói dữ liệu và mục nhập dòng khớp được cung cấp các giá trị của một phần của các miền dung hợp của gói dữ liệu và các giá trị của mục nhập dòng là tương ứng bằng nhau. Ví dụ như, như được thể hiện trên bảng 2, bảng ký tự đại diện bao gồm năm miền dung hợp: Src IP, Dst IP, SrcPort, DstPort, và giao thức IP, và ba chỉ dẫn: Các hành động, Viết siêu dữ liệu, và Đi tới bảng; chỉ miền dung hợp Dst IP trong mục nhập dòng được thể hiện trên bảng 2 có giá trị cụ thể 192.168.20.1. Khi gói dữ liệu được khớp với mục nhập dòng trong bảng dung hợp, coi rằng gói dữ liệu và mục nhập dòng được thể hiện trên bảng 2 khớp được cung cấp giá trị của miền dung hợp Dst IP trong gói dữ liệu cũng là 192.168.20.1.

Bảng 2

Các miền dung hợp					Các chỉ dẫn		
Src IP	Dst IP	SrcPort	DstPort	Giao thức IP	Viết các hành động	Viết siêu dữ liệu	Đi tới bảng
Bất kỳ (Any)	192.168.20.1	Bất kỳ	Bất kỳ	Bất kỳ			Bảng 5

Sau đây mô tả một cách rõ ràng và đầy đủ các giải pháp kỹ thuật trong các phương án của sáng chế dựa vào các hình vẽ kèm theo trong các phương án của sáng chế. Rõ ràng rằng, các phương án được mô tả chỉ đơn thuần là một số chứ không phải là tất cả các phương án của sáng chế. Tất cả các phương án khác thu được bởi người có trình độ trung bình trong lĩnh vực dựa vào các phương án của sáng chế mà không cần các nỗ lực mang tính sáng tạo thì cũng nằm trong phạm vi bảo hộ của sáng chế.

Theo Fig.3, Fig.3 là lưu đồ phương pháp phát hiện sự tấn công nguy hiểm theo phương án thứ nhất của sáng chế, trong đó phương pháp bao gồm các bước:

Bước 301: Bộ điều khiển thu tin nhắn trong gói được gửi bởi bộ chuyển mạch thứ nhất, trong đó tin nhắn trong gói bao gồm bộ định danh máy chủ nguồn

và bộ định danh máy chủ điểm đến của gói dữ liệu mà bộ chuyển mạch thứ nhất không tìm thấy mục nhập dòng.

Bước 302: Khi xác định được rằng máy chủ được chỉ báo bởi bộ định danh máy chủ điểm đến không tồn tại trong mạng SDN, bộ điều khiển gửi mục nhập dòng bất thường tới bộ chuyển mạch thứ nhất, trong đó mục nhập dòng bất thường bao gồm bộ định danh máy chủ nguồn.

Bước 303: Bộ điều khiển thu số đếm khởi động được gửi bởi bộ chuyển mạch thứ nhất, trong đó số đếm khởi động được gửi bởi bộ chuyển mạch thứ nhất sau khi mục nhập dòng bất thường hết thời gian chờ, và số đếm khởi động là số lượng các lần mà mục nhập dòng bất thường được khởi động.

Bước 304: Bộ điều khiển xác định, theo số đếm khởi động, xem sự tấn công nguy hiểm có được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn hay không.

Trong phương án này, bộ điều khiển không cần thiết phải thu thập các thống kê về các tin nhắn trong gói tương ứng với mỗi máy chủ, và thay vào đó gửi mục nhập dòng bất thường tới bộ chuyển mạch thứ nhất; bộ chuyển mạch thứ nhất thu thập các thống kê về số đếm khởi động của mục nhập dòng bất thường và thông báo số đếm khởi động tới bộ điều khiển; bộ điều khiển xác định trực tiếp, theo số đếm khởi động, xem sự tấn công nguy hiểm có được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn hay không. Theo cách này, việc thu thập các thống kê tin nhắn được thực hiện đầu tiên bởi bộ điều khiển được phân phối tới mỗi bộ chuyển mạch để thực hiện, do đó giảm bớt lượng xử lý dữ liệu của bộ điều khiển, và cải thiện hiệu suất của bộ điều khiển.

Theo Fig.4, Fig.4 là lưu đồ phương pháp phát hiện sự tấn công nguy hiểm theo phương án thứ hai của sáng chế, trong đó phương pháp bao gồm các bước:

Bước 401: Khi xác định được rằng mục nhập dòng tương ứng với gói dữ liệu không được tìm thấy, bộ chuyển mạch thứ nhất gửi tin nhắn trong gói tới bộ điều khiển, trong đó tin nhắn trong gói bao gồm bộ định danh máy chủ nguồn và bộ định danh máy chủ điểm đến của gói dữ liệu.

Bước 402: Bộ chuyển mạch thứ nhất thu và lưu mục nhập dòng bất thường được gửi bởi bộ điều khiển, trong đó mục nhập dòng bất thường được gửi bởi bộ điều khiển khi xác định được rằng máy chủ được chỉ báo bởi bộ định danh máy chủ điểm đến không tồn tại trong mạng SDN.

Bước 403: Bộ chuyển mạch thứ nhất ghi, trong khoảng thời gian trôi qua của mục nhập dòng bất thường, số đếm khởi động của mục nhập dòng bất thường, và gửi số đếm khởi động tới bộ điều khiển sau khi mục nhập dòng bất thường hết thời gian chờ, khiến cho bộ điều khiển xác định, theo số đếm khởi động, xem sự tấn công nguy hiểm có được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn hay không.

Trong phương án này, bộ điều khiển không cần thiết phải thu thập các thống kê về các tin nhắn trong gói tương ứng với mỗi máy chủ, và thay vào đó, bộ chuyển mạch thứ nhất thu thập các thống kê về số đếm khởi động của mục nhập dòng bất thường và thông báo số đếm khởi động tới bộ điều khiển; bộ điều khiển xác định trực tiếp, theo số đếm khởi động, xem sự tấn công nguy hiểm có được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn hay không. Theo cách này, việc thu thập các thống kê tin nhắn được thực hiện đầu tiên bởi bộ điều khiển được phân phối tới mỗi bộ chuyển mạch để thực hiện, do đó giảm bớt lượng xử lý dữ liệu của bộ điều khiển, và cải thiện hiệu suất của bộ điều khiển.

Theo Fig.5, Fig.5 là lưu đồ phương pháp phát hiện sự tấn công nguy hiểm theo phương án thứ ba của sáng chế, trong đó phương pháp bao gồm các bước:

Bước 501: Bộ điều khiển thu thập cấu trúc bảng dòng trong bộ chuyển mạch thứ nhất, và khi xác định được rằng bảng dòng cuối cùng trong bộ chuyển mạch thứ nhất là bảng dung hợp chính xác bao gồm miền dung hợp bộ định danh máy chủ nguồn, gửi chỉ dẫn thứ nhất tới bộ chuyển mạch thứ nhất, trong đó chỉ dẫn thứ nhất được sử dụng để chỉ dẫn cho bộ chuyển mạch thứ nhất tạo cấu hình bảng dung hợp chính xác như bảng dung hợp chính xác chỉ khớp với miền dung hợp bộ định danh máy chủ nguồn.

Được quy định trong giao thức OpenFlow1.3 rằng bộ điều khiển có thể tạo cấu hình loại miền dung hợp của mỗi bảng dòng trong bộ chuyển mạch bằng cách sử dụng tin nhắn nhiều phần loại TABLE_FEATURES. Do đó, trong bước này, bộ điều khiển cũng có thể tạo cấu hình, bằng cách sử dụng cách này, bảng dung hợp chính xác bao gồm miền dung hợp bộ định danh máy chủ nguồn như bảng dung hợp chính xác chỉ khớp với miền dung hợp bộ định danh máy chủ nguồn.

Ví dụ như, theo Fig.5A, coi rằng bộ định danh máy chủ nguồn là địa chỉ MAC máy chủ nguồn, rằng miền dung hợp bộ định danh máy chủ nguồn được thực hiện bằng cách sử dụng miền dung hợp ETH_SRC, và rằng bảng dòng cuối cùng của bộ chuyển mạch thứ nhất là bảng dung hợp chính xác có bốn miền dung hợp: Eth_type, Eth_src, Eth_dst và In_port, bộ điều khiển có thể chỉ dẫn, bằng cách phân phối tin nhắn nhiều phần của loại đặc điểm bảng (TABLE_FEATURES), bộ chuyển mạch thứ nhất tạo cấu hình bảng dung hợp chính xác như bảng dung hợp chính xác chỉ khớp với miền dung hợp Eth_src.

Mục đích của bước này là nhằm đảm bảo rằng bảng dòng cuối cùng trong bộ chuyển mạch thứ nhất là bảng ký tự đại diện bao gồm miền dung hợp bộ định danh máy chủ nguồn, hoặc, bảng dung hợp chính xác chỉ khớp với miền dung hợp bộ định danh máy chủ nguồn. Do đó, bước 501 còn có thể được thay thế bằng bước sau:

Bộ điều khiển thu thập cấu trúc bảng dòng trong bộ chuyển mạch thứ nhất; và khi xác định được rằng bảng dòng cuối cùng trong bộ chuyển mạch thứ nhất là bảng dung hợp chính xác hoặc bảng ký tự đại diện không bao gồm miền dung hợp bộ định danh máy chủ nguồn và rằng bảng ký tự đại diện bao gồm miền dung hợp bộ định danh máy chủ nguồn tồn tại trong bộ chuyển mạch thứ nhất, gửi chỉ dẫn thứ hai tới bộ chuyển mạch thứ nhất, trong đó chỉ dẫn thứ hai được sử dụng để chỉ dẫn cho bộ chuyển mạch thứ nhất điều chỉnh bảng ký tự đại diện bao gồm miền dung hợp bộ định danh máy chủ nguồn thành bảng dòng cuối cùng.

Sau giao thức OpenFlow1.2, bộ điều khiển có thể chỉ dẫn, bằng cách sử dụng tin nhắn tùy thích, bộ chuyển mạch bố trí lại các bảng dòng trong bộ chuyển mạch; do đó, bộ điều khiển có thể chỉ dẫn, bằng cách sử dụng tin nhắn tùy thích,

bộ chuyển mạch điều chỉnh bảng ký tự đại diện bao gồm miền dung hợp bộ định danh máy chủ nguồn thành bảng dòng cuối cùng. Bộ chuyển mạch thứ nhất có thể hoán đổi trực tiếp các vị trí của bảng dung hợp chính xác cuối cùng và bảng ký tự đại diện, do đó điều chỉnh bảng ký tự đại diện bao gồm miền dung hợp bộ định danh máy chủ nguồn thành bảng dòng cuối cùng; hoặc, bộ chuyển mạch thứ nhất có thể bố trí lại các bảng dòng trong bộ chuyển mạch thứ nhất, do đó điều chỉnh bảng ký tự đại diện bao gồm miền dung hợp bộ định danh máy chủ nguồn thành bảng dòng cuối cùng. Ví dụ như, được coi rằng bộ định danh máy chủ nguồn là địa chỉ máy chủ nguồn MAC, và miền dung hợp bộ định danh máy chủ nguồn được thực hiện bằng cách sử dụng miền dung hợp ETH_SRC. Theo Fig.5B, coi rằng bộ chuyển mạch thứ nhất bao gồm năm bảng dòng, và trước khi điều chỉnh bảng dòng, bảng 2 của đường liên hợp là bảng ký tự đại diện bao gồm miền dung hợp ETH_SRC và bảng 4 là bảng dung hợp chính xác không bao gồm miền dung hợp Eth_src, bộ điều khiển có thể chỉ dẫn bộ chuyển mạch thứ nhất để hoán đổi các bảng dòng bảng 2 và bảng 4. Đối với cấu trúc sau khi điều chỉnh bảng dòng, theo Fig.5C. Bảng 2 thực chất là bảng dung hợp chính xác của bảng 4 lúc ban đầu, và bảng 4 là bảng ký tự đại diện của bảng 2 lúc ban đầu.

Bước 501 và bước thay thế của bước 501 nêu trên có thể được thực hiện khi bộ chuyển mạch thứ nhất truy cập bộ điều khiển.

Bước 502: Bộ chuyển mạch thứ nhất thu gói dữ liệu được gửi bởi máy chủ nguồn, và khi mục nhập dòng của gói dữ liệu không được tìm thấy trong bảng dòng địa phương, tạo ra tin nhắn trong gói, trong đó tin nhắn trong gói bao gồm bộ định danh máy chủ nguồn và bộ định danh máy chủ điểm đến của gói dữ liệu.

Bộ định danh máy chủ nguồn có thể là địa chỉ MAC, địa chỉ IP, giao diện đầu vào, hoặc tương tự của máy chủ nguồn, mà không bị giới hạn ở đây.

Khi bộ chuyển mạch thứ nhất tìm thấy mục nhập dòng của gói dữ liệu trong bảng dòng địa phương, như được thể hiện trên Fig.1, bộ chuyển mạch thứ nhất chuyển tiếp gói dữ liệu theo mục nhập dòng. Các chi tiết sẽ không được mô tả ở đây.

Bước 503: Bộ điều khiển thu tin nhắn trong gói được gửi bởi bộ chuyển mạch thứ nhất; và khi xác định được rằng máy chủ được chỉ báo bởi bộ định danh máy chủ điểm đến không tồn tại trong mạng SDN, bộ điều khiển xác định xem mục nhập dòng bất thường của máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn có được phân phối tới bộ chuyển mạch thứ nhất hay không, và nếu mục nhập dòng bất thường của máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn không được phân phối tới bộ chuyển mạch thứ nhất, gửi mục nhập dòng bất thường tới bộ chuyển mạch thứ nhất, trong đó mục nhập dòng bất thường bao gồm bộ định danh máy chủ nguồn, và bước 504 được thực hiện; nếu mục nhập dòng bất thường của máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn đã được phân phối tới bộ chuyển mạch thứ nhất, quy trình xử lý của nhánh này kết thúc.

Đối với phương pháp xử lý của bộ điều khiển khi bộ điều khiển xác định rằng máy chủ được chỉ báo bởi bộ định danh máy chủ điểm đến tồn tại trong mạng SDN, theo Fig.2 và phần mô tả tương ứng của nó. Các chi tiết sẽ không được mô tả ở đây.

Cách thực hiện của mục nhập dòng bất thường có thể là giống như mục nhập dòng bình thường, và mục nhập dòng được gọi là bất thường được sử dụng chỉ đơn thuần để phân biệt với mục nhập dòng bình thường được gửi bởi bộ điều khiển, và được sử dụng để thể hiện rằng mục nhập dòng được gửi khi bộ điều khiển không thể tìm thấy máy chủ điểm đến.

Trong bộ điều khiển, cờ phân phối mục nhập dòng bất thường có thể được thiết đặt cho mỗi máy chủ, và xem bộ điều khiển phân phối mục nhập dòng bất thường của máy chủ tương ứng có đồng nhất hay không bằng cách sử dụng các giá trị cờ khác nhau ví dụ như có và không. Trong bước này, bộ điều khiển có thể xác định, bằng cách sử dụng cờ phân phối mục nhập dòng bất thường tương ứng với máy chủ nguồn, xem mục nhập dòng bất thường của máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn đã được phân phối tới bộ chuyển mạch thứ nhất hay chưa. Hơn nữa, trong bước này, sau khi gửi mục nhập dòng bất thường tới bộ chuyển mạch thứ nhất, bộ điều khiển cần phải thiết lập lại giá trị cờ của cờ

phân phối mục nhập dòng bất thường tương ứng với máy chủ nguồn, ví dụ như, thiết lập lại giá trị cờ từ không thành có. Trong bước 507, sau khi thu số đếm khởi động, bộ điều khiển cần phải thiết đặt lại giá trị cờ của cờ phân phối mục nhập dòng bất thường tương ứng với máy chủ nguồn, ví dụ như, thiết lập lại giá trị cờ từ có thành không.

Bước 504: Bộ chuyển mạch thứ nhất thu mục nhập dòng bất thường, và lưu trữ mục nhập dòng bất thường trong bảng dòng cuối cùng.

Trong cách có thể thực hiện, mục nhập dòng bất thường có thể bao gồm: miền dung hợp ETH_SRC, được sử dụng để ghi địa chỉ MAC của máy chủ cần được phát hiện, nghĩa là, địa chỉ MAC của máy chủ nguồn; hành động, được sử dụng để ghi thao tác được thực hiện bởi bộ chuyển mạch; idle_timeout, được sử dụng để ghi thời gian trôi qua chạy không của mục nhập dòng bất thường; hard_timeout, được sử dụng để ghi thời gian trôi qua của mục nhập dòng bất thường; cờ, được sử dụng để ghi thuộc tính của mục nhập dòng bất thường; và quyền ưu tiên, được sử dụng để ghi quyền ưu tiên của mục nhập dòng bất thường. Ví dụ như, cách thực hiện của mục nhập dòng bất thường được thể hiện trên Fig.5D, giá trị của miền dung hợp ETH_SRC là 11:22:33:44:55:66, giá trị của hành động là đầu ra của bộ điều khiển, giá trị của idle_timeout bằng 0, giá trị của hard_timeout bằng 1, giá trị của cờ là SEND_FLOW_REM + CHECK_OVERLAP, và giá trị của quyền ưu tiên là quyền ưu tiên thấp nhất 0.

Một cách tùy chọn, quyền ưu tiên của mục nhập dòng bất thường được phân phối bởi bộ điều khiển tốt hơn là quyền ưu tiên thấp nhất của mục nhập dòng trong bộ chuyển mạch thứ nhất.

Bước 505: Bộ chuyển mạch thứ nhất ghi, trong khoảng thời gian trôi qua của mục nhập dòng bất thường, số đếm khởi động của mục nhập dòng bất thường.

Trong ứng dụng thực tế, khi mục nhập dòng bất thường được khởi động, tốt hơn là, bộ chuyển mạch thứ nhất tiếp tục thông báo tin nhắn trong gói tương ứng tới bộ điều khiển như trong kỹ thuật đã biết. Kết hợp với quyền ưu tiên thấp nhất

của mục nhập dòng bất thường và quy trình xử lý để lưu trữ mục nhập dòng bất thường vào bảng dòng cuối cùng, phương án này của sáng chế ngoài ra còn có các ưu điểm sau đây:

Coi rằng lý do ban đầu khiến máy chủ điểm đến B của gói dữ liệu được gửi bởi máy chủ nguồn A tới bộ chuyển mạch thứ nhất không thể được tìm thấy là bởi máy chủ điểm đến B không nối với nguồn điện, hoặc tương tự, bộ điều khiển phân phối mục nhập dòng bất thường.

Nếu bộ chuyển mạch thứ nhất thông báo tin nhắn trong gói tương ứng tới bộ điều khiển khi mục nhập dòng bất thường được khởi động, nếu máy chủ điểm đến B được nối với nguồn điện trong khoảng thời gian trôi qua của mục nhập dòng bất thường, sau khi máy chủ điểm đến B được nối với nguồn điện, khi thu tin nhắn trong gói mà mang bộ định danh máy chủ nguồn A và bộ định danh máy chủ điểm đến B và được gửi bởi bộ chuyển mạch thứ nhất, bộ điều khiển có thể tìm thấy máy chủ điểm đến B, và phân phối mục nhập dòng bình thường về máy chủ nguồn A và máy chủ điểm đến B tới bộ chuyển mạch thứ nhất.

Trong trường hợp này, do mục nhập dòng bất thường có quyền ưu tiên thấp nhất và được lưu trữ trong bảng dòng cuối cùng, khi thu gói dữ liệu từ máy chủ nguồn A tới máy chủ điểm đến B một lần nữa, bộ chuyển mạch thứ nhất đầu tiên khớp gói dữ liệu với mục nhập dòng bình thường, và chuyển tiếp gói dữ liệu bằng cách sử dụng mục nhập dòng bình thường, mà không khởi động mục nhập dòng bất thường.

Do đó, quy trình xử lý nêu trên của phương án của sáng chế có thể ngăn ngừa bộ chuyển mạch thứ nhất không tiếp tục khởi động mục nhập dòng bất thường và thu thập các thống kê về số đếm khởi động trong trường hợp này, ngoài ra còn ngăn ngừa bộ chuyển mạch thứ nhất khỏi việc không có khả năng chuyển tiếp bình thường gói dữ liệu từ máy chủ nguồn A đến máy chủ điểm đến B trong trường hợp này, và ngăn ngừa bộ điều khiển khỏi việc xác định một cách nhầm lẫn, theo số đếm khởi động được thông báo bởi bộ chuyển mạch thứ nhất, rằng máy chủ nguồn A thực hiện sự tấn công nguy hiểm, do đó cải thiện tính chính xác của kết quả phát hiện sự tấn công nguy hiểm của sáng chế.

Bước 506: Bộ chuyển mạch thứ nhất gửi số đếm khởi động tới bộ điều khiển sau khi mục nhập dòng bất thường hết thời gian chờ.

Trong kỹ thuật đã biết, sau khi mục nhập dòng hết hạn, bộ chuyển mạch có thể gửi tin nhắn đã được loại bỏ khỏi dòng tới bộ điều khiển để thông báo bộ điều khiển rằng mục nhập dòng hết hạn. Trong bước này, bộ chuyển mạch thứ nhất cũng có thể gửi số đếm khởi động bằng cách sử dụng tin nhắn đã được loại bỏ khỏi dòng, và cụ thể là, số đếm khởi động có thể được mang trong trường đếm gói trong tin nhắn đã được loại bỏ khỏi dòng.

Bước 507: Bộ điều khiển thu số đếm khởi động, và xác định, theo số đếm khởi động, xem sự tấn công nguy hiểm có được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn hay không.

Trong cách có thể thực hiện, bộ điều khiển xác định, theo số đếm khởi động, xem sự tấn công nguy hiểm có được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn hay không có thể bao gồm các bước:

tính toán, bởi bộ điều khiển, hệ số khởi động của mục nhập dòng bất thường theo số đếm khởi động và thời gian trôi qua của mục nhập dòng bất thường; và

xác định, bởi bộ điều khiển, xem hệ số khởi động có lớn hơn ngưỡng hệ số hay không; và nếu hệ số khởi động lớn hơn ngưỡng hệ số, xác định, bởi bộ điều khiển, rằng sự tấn công nguy hiểm được bắt nguồn từ máy chủ nguồn; hoặc, nếu hệ số khởi động không lớn hơn ngưỡng hệ số, xác định, bởi bộ điều khiển, rằng không có sự tấn công nguy hiểm nào bắt nguồn từ máy chủ nguồn.

Trong cách có thể thực hiện thứ hai, bộ điều khiển xác định, theo số đếm khởi động, xem sự tấn công nguy hiểm có được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn hay không có thể bao gồm các bước:

xác định, bởi bộ điều khiển, xem số đếm khởi động có lớn hơn ngưỡng số đếm hay không; và nếu số đếm khởi động lớn hơn ngưỡng số đếm, xác định, bởi bộ điều khiển, rằng sự tấn công nguy hiểm được bắt nguồn từ máy chủ nguồn; hoặc, nếu số đếm khởi động không lớn hơn ngưỡng số đếm, xác định,

bởi bộ điều khiển, rằng không có sự tấn công nguy hiểm nào bắt nguồn từ máy chủ nguồn.

Cách có thể thực hiện thứ hai thông thường được sử dụng trong bối cảnh trong đó các thời gian trôi qua của các mục nhập dòng bất thường được phân phối bởi bộ điều khiển tới các bộ chuyển mạch khác nhau được cố định.

Các chỉ số cụ thể của giá trị ngưỡng hệ số và giá trị ngưỡng số đếm có thể được thiết đặt theo môi trường ứng dụng cụ thể, mà không bị giới hạn bởi sáng chế.

Bước 508: Khi xác định được rằng sự tấn công nguy hiểm được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn, bộ điều khiển gửi chỉ dẫn thứ ba tới bộ chuyển mạch thứ nhất, trong đó chỉ dẫn thứ ba được sử dụng để chỉ dẫn cho bộ chuyển mạch thứ nhất xóa gói dữ liệu từ máy chủ nguồn.

Bộ điều khiển có thể xóa gói dữ liệu từ máy chủ nguồn bằng cách phân phối mục nhập dòng đặc biệt hoặc danh sách điều khiển truy cập (ACL, Access Control List) tới bộ chuyển mạch thứ nhất.

Trong phương án này, bộ điều khiển không cần thiết phải thu thập các thống kê về các tin nhắn trong gói tương ứng với mỗi máy chủ, và thay vào đó, bộ chuyển mạch thứ nhất thu thập các thống kê về số đếm khởi động của mục nhập dòng bất thường và thông báo số đếm khởi động tới bộ điều khiển; bộ điều khiển xác định trực tiếp, theo số đếm khởi động, xem sự tấn công nguy hiểm có được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn hay không. Theo cách này, việc thu thập các thống kê tin nhắn được thực hiện đầu tiên bởi bộ điều khiển được phân phối tới mỗi bộ chuyển mạch để thực hiện, do đó giảm bớt lượng xử lý dữ liệu của bộ điều khiển, và cải thiện hiệu suất của bộ điều khiển.

Ngoài ra, mục nhập dòng bất thường có quyền ưu tiên thấp nhất, và bộ chuyển mạch thứ nhất lưu trữ mục nhập dòng bất thường trong bảng dòng cuối cùng, khiến kết quả phát hiện sự tấn công nguy hiểm trong phương án này của sáng chế chính xác hơn.

Các phương pháp phát hiện sự tấn công nguy hiểm được thể hiện trên Fig.3 đến Fig.5 có thể được sử dụng như một chức năng tùy chọn của bộ chuyển mạch và bộ điều khiển, để thực hiện việc phát hiện sự tấn công nguy hiểm trên máy chủ cụ thể ở thời điểm cụ thể. Thời điểm phát hiện cụ thể có thể bao gồm nhưng không bị giới hạn ở các trường hợp sau đây:

1. Việc phát hiện liên tục được thực hiện trên máy chủ được kết nối tới bộ chuyển mạch, hoặc, người dùng có thể thiết đặt lúc nào để thực hiện việc phát hiện trên máy chủ nào.

2. Không có phát hiện nào được thực hiện trên máy chủ bởi mặc định, và hệ số mà ở đó bộ chuyển mạch tạo ra các tin nhắn trong gói được gây ra bởi mỗi cổng có thể được giám sát. Nếu hệ số lớn hơn so với giá trị ngưỡng giới hạn trên được thiết đặt trước, việc phát hiện sự tấn công nguy hiểm trên tất cả các máy chủ được kết nối với cổng là có thể.

3. Không có phát hiện nào được thực hiện trên máy chủ bằng mặc định. Giao thức OpenFlow1.3 xác định bộ đếm để giám sát hệ số chảy và ngoài ra còn xác định bộ đếm loại OFPM_CONTROLLER để giám sát hệ số mà tại đó bộ chuyển mạch gửi tin nhắn trong gói. Nếu hệ số trong gói lớn hơn hệ số giới hạn trên của bộ đếm, sự phát hiện tấn công nguy hiểm trên máy chủ được kết nối tới bộ chuyển mạch được khởi động.

Tương ứng với các phương pháp nên trên, các phương án của sáng chế ngoài ra còn đề xuất thiết bị phát hiện sự tấn công nguy hiểm, bộ điều khiển, và bộ chuyển mạch.

Theo Fig.6, Fig.6 là lược đồ thiết bị phát hiện sự tấn công nguy hiểm 600 theo phương án thứ nhất của sáng chế. Thiết bị 600 có thể được bố trí trong bộ điều khiển, và thiết bị 600 bao gồm:

bộ thu thứ nhất 610, được tạo cấu hình để thu tin nhắn trong gói được gửi bởi bộ chuyển mạch thứ nhất, trong đó tin nhắn trong gói bao gồm bộ định danh máy chủ nguồn và bộ định danh máy chủ điểm đến của gói dữ liệu mà bộ chuyển mạch thứ nhất không tìm thấy mục nhập dòng;

bộ gửi thứ nhất 620, được tạo cấu hình để: khi xác định được rằng máy chủ được chỉ báo bởi bộ định danh máy chủ điểm đến được thu bởi bộ thu thứ nhất 610 không tồn tại trong mạng SDN, gửi mục nhập dòng bất thường tới bộ chuyển mạch thứ nhất, trong đó mục nhập dòng bất thường bao gồm bộ định danh máy chủ nguồn, trong đó

bộ thu thứ nhất 610 ngoài ra còn được tạo cấu hình để thu số đếm khởi động được gửi bởi bộ chuyển mạch thứ nhất, trong đó số đếm khởi động được gửi bởi bộ chuyển mạch thứ nhất sau khi mục nhập dòng bất thường hết thời gian chờ, và số đếm khởi động là số lượng các lần mà mục nhập dòng bất thường được khởi động; và

bộ phát hiện 630, được tạo cấu hình để xác định, theo số đếm khởi động được thu bởi bộ thu thứ nhất 610, xem sự tấn công nguy hiểm có được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn hay không.

Trong cách có thể thực hiện thứ nhất, bộ phát hiện 630 có thể được tạo cấu hình riêng để:

tính toán hệ số khởi động của mục nhập dòng bất thường theo số đếm khởi động được thu bởi bộ thu thứ nhất 610 và thời gian trôi qua của mục nhập dòng bất thường; và

xác định xem hệ số khởi động có lớn hơn ngưỡng hệ số hay không; hoặc, nếu hệ số khởi động không lớn hơn ngưỡng hệ số, xác định rằng sự tấn công nguy hiểm được bắt nguồn từ máy chủ nguồn; hoặc nếu hệ số khởi động không lớn hơn ngưỡng hệ số, xác định rằng không có sự tấn công nguy hiểm nào bắt nguồn từ máy chủ nguồn.

Trong cách có thể thực hiện thứ hai, bộ phát hiện 630 có thể được tạo cấu hình riêng để:

xác định xem số đếm khởi động có lớn hơn ngưỡng số đếm hay không; và nếu số đếm khởi động lớn hơn ngưỡng số đếm, xác định rằng sự tấn công nguy hiểm được bắt nguồn từ máy chủ nguồn; hoặc nếu, số đếm khởi động không

lớn hơn ngưỡng số đếm, xác định rằng không có sự tấn công nguy hiểm nào bắt nguồn từ máy chủ nguồn.

Một cách tùy chọn, thiết bị có thể ngoài ra còn bao gồm:

bộ xác định, được tạo cấu hình để xác định xem mục nhập dòng bất thường của máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn đã được phân phối tới bộ chuyển mạch thứ nhất hay chưa; và nếu mục nhập dòng bất thường của máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn chưa được phân phối tới bộ chuyển mạch thứ nhất, khởi động bộ gửi thứ nhất 620 để gửi mục nhập dòng bất thường tới bộ chuyển mạch thứ nhất.

Trong cách có thể thực hiện thứ nhất, bộ gửi thứ nhất 620 có thể ngoài ra còn được tạo cấu hình để: khi xác định được rằng bảng dòng cuối cùng trong bộ chuyển mạch thứ nhất là bảng dung hợp chính xác bao gồm miền dung hợp bộ định danh máy chủ nguồn, chỉ dẫn bộ chuyển mạch thứ nhất tạo cấu hình bảng dung hợp chính xác như bảng dung hợp chính xác chỉ khớp với miền dung hợp bộ định danh máy chủ nguồn, để bộ chuyển mạch thứ nhất lưu trữ mục nhập dòng bất thường trong bảng dòng cuối cùng.

Trong cách có thể thực hiện thứ hai, bộ gửi thứ nhất 620 có thể ngoài ra còn được tạo cấu hình để: khi xác định được rằng bảng dòng cuối cùng trong bộ chuyển mạch thứ nhất là bảng dung hợp chính xác, và bảng ký tự đại diện bao gồm miền dung hợp bộ định danh máy chủ nguồn tồn tại trong bộ chuyển mạch thứ nhất, gửi chỉ dẫn thứ hai tới bộ chuyển mạch thứ nhất, trong đó chỉ dẫn thứ hai được sử dụng để chỉ dẫn cho bộ chuyển mạch thứ nhất điều chỉnh bảng ký tự đại diện bao gồm miền dung hợp bộ định danh máy chủ nguồn thành bảng dòng cuối cùng, để bộ chuyển mạch thứ nhất lưu trữ mục nhập dòng bất thường trong bảng dòng cuối cùng.

Một cách tùy chọn, bộ gửi thứ nhất 620 có thể ngoài ra còn được tạo cấu hình để:

khi xác định được, theo số đếm khởi động, rằng sự tấn công nguy hiểm được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ

nguồn, gửi chỉ dẫn thứ ba tới bộ chuyển mạch thứ nhất, trong đó chỉ dẫn thứ ba được sử dụng để chỉ dẫn cho bộ chuyển mạch thứ nhất xóa gói dữ liệu từ máy chủ nguồn.

Trong phương án này, bộ điều khiển không cần thiết phải thu thập các thống kê về các tin nhắn trong gói tương ứng với mỗi máy chủ, và thay vào đó gửi mục nhập dòng bất thường tới bộ chuyển mạch thứ nhất; bộ chuyển mạch thứ nhất thu thập các thống kê về số đếm khởi động của mục nhập dòng bất thường và thông báo số đếm khởi động tới bộ điều khiển; bộ điều khiển xác định trực tiếp, theo số đếm khởi động, xem sự tấn công nguy hiểm có được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn hay không. Theo cách này, việc thu thập các thống kê tin nhắn được thực hiện đầu tiên bởi bộ điều khiển được phân phối tới mỗi bộ chuyển mạch để thực hiện, do đó giảm bớt lượng xử lý dữ liệu của bộ điều khiển, và cải thiện hiệu suất của bộ điều khiển.

Theo Fig.7, Fig.7 là lược đồ thiết bị phát hiện sự tấn công nguy hiểm 700 theo phương án thứ hai của sáng chế. Thiết bị 700 có thể được bố trí trong bộ chuyển mạch thứ nhất, và thiết bị 700 bao gồm:

bộ gửi thứ hai 710, được tạo cấu hình để: khi xác định được rằng mục nhập dòng tương ứng với gói dữ liệu không được tìm thấy, gửi tin nhắn trong gói tới bộ điều khiển, trong đó tin nhắn trong gói bao gồm bộ định danh máy chủ nguồn và bộ định danh máy chủ điểm đến của gói dữ liệu;

bộ thu thứ hai 720, được tạo cấu hình để thu mục nhập dòng bất thường được gửi bởi bộ điều khiển, trong đó mục nhập dòng bất thường được gửi bởi bộ điều khiển khi xác định được rằng máy chủ được chỉ báo bởi bộ định danh máy chủ điểm đến không tồn tại trong mạng SDN;

bộ lưu trữ 730, được tạo cấu hình để lưu mục nhập dòng bất thường được thu bởi bộ thu thứ hai 720; và

bộ ghi số đếm 740, được tạo cấu hình để ghi, trong khoảng thời gian trôi qua của mục nhập dòng bất thường được lưu bởi bộ lưu trữ 730, số đếm khởi động của mục nhập dòng bất thường, trong đó

bộ gửi thứ hai 710 ngoài ra còn được tạo cấu hình để: sau khi mục nhập dòng bất thường được lưu bởi bộ lưu trữ hết hạn, gửi số đếm khởi động tới bộ điều khiển, khiến cho bộ điều khiển xác định, theo số đếm khởi động, xem sự tấn công nguy hiểm có được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn hay không.

Một cách tùy chọn, bộ thu thứ hai 720 có thể ngoài ra còn được tạo cấu hình để thu chỉ dẫn thứ nhất được gửi bởi bộ điều khiển; và

thiết bị ngoài ra còn bao gồm: bộ cấu hình, được tạo cấu hình để tạo cấu hình, theo chỉ dẫn thứ nhất, bảng dung hợp chính xác địa phương mà là bảng dòng cuối cùng như bảng dung hợp chính xác chỉ khớp với miền dung hợp bộ định danh máy chủ nguồn; hoặc

bộ thu thứ hai 720 có thể ngoài ra còn được tạo cấu hình để thu chỉ dẫn thứ hai được gửi bởi bộ điều khiển; và

thiết bị ngoài ra còn bao gồm: bộ cấu hình, được tạo cấu hình để điều chỉnh bảng ký tự đại diện bao gồm miền dung hợp bộ định danh máy chủ nguồn thành bảng dòng cuối cùng theo chỉ dẫn thứ hai.

Một cách tùy chọn, bộ lưu trữ 730 có thể được tạo cấu hình riêng để lưu mục nhập dòng bất thường vào bảng dòng cuối cùng.

Một cách tùy chọn, bộ thu thứ hai 720 có thể ngoài ra còn được tạo cấu hình để thu chỉ dẫn thứ ba được gửi bởi bộ chuyển mạch thứ nhất; và

có thể ngoài ra còn bao gồm: bộ điều khiển, được tạo cấu hình để xóa gói dữ liệu từ máy chủ nguồn.

Trong phương án này, bộ điều khiển không cần thiết phải thu thập các thống kê về các tin nhắn trong gói tương ứng với mỗi máy chủ, và thay vào đó, bộ chuyển mạch thứ nhất thu thập các thống kê về số đếm khởi động của mục nhập dòng bất thường và thông báo số đếm khởi động tới bộ điều khiển; bộ điều khiển xác định trực tiếp, theo số đếm khởi động, xem sự tấn công nguy hiểm có được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn hay không. Theo cách này, việc thu thập các thống kê tin nhắn được thực hiện

đầu tiên bởi bộ điều khiển được phân phối tới mỗi bộ chuyển mạch để thực hiện, do đó giảm bớt lượng xử lý dữ liệu của bộ điều khiển, và cải thiện hiệu suất của bộ điều khiển.

Theo Fig.8, Fig.8 là lược đồ cấu trúc của bộ điều khiển 800 theo một phương án của sáng chế sáng chế. Bộ điều khiển 800 bao gồm: bộ xử lý 810, bộ nhớ 820, bộ thu phát 830, và bus 840.

Bộ xử lý 810, bộ nhớ 820, và bộ thu phát 830 được kết nối với nhau bằng cách sử dụng bus 840. Bus 840 có thể là bus ISA, bus PCI, hoặc bus EISA. Bus có thể là bus địa chỉ, bus dữ liệu, hoặc bus điều khiển. Để dễ dàng minh họa, bus được thể hiện bằng cách sử dụng đường kẻ đậm trên Fig.8, nhưng không có nghĩa là chỉ có một bus hoặc một loại bus.

Bộ nhớ 820 được tạo cấu hình để lưu trữ chương trình. Cụ thể là, chương trình có thể bao gồm mã chương trình, và mã chương trình bao gồm chỉ dẫn thao tác máy tính. Bộ nhớ 820 có thể bao gồm bộ nhớ RAM tốc độ cao, và có thể ngoài ra còn bao gồm bộ nhớ bất biến (non-volatile memory), ví dụ như, ít nhất một bộ nhớ đĩa từ.

Bộ thu phát 830 được tạo cấu hình để kết nối với một thiết bị khác, và truyền thông với một thiết bị khác. Cụ thể là, bộ thu phát 830 được tạo cấu hình để thu tin nhắn trong gói được gửi bởi bộ chuyển mạch thứ nhất, trong đó tin nhắn trong gói bao gồm bộ định danh máy chủ nguồn và bộ định danh máy chủ điểm đến của gói dữ liệu mà bộ chuyển mạch thứ nhất không tìm thấy mục nhập dòng; gửi mục nhập dòng bất thường tới bộ chuyển mạch thứ nhất, trong đó mục nhập dòng bất thường bao gồm bộ định danh máy chủ nguồn; và thu số đếm khởi động được gửi bởi bộ chuyển mạch thứ nhất, trong đó số đếm khởi động được gửi bởi bộ chuyển mạch thứ nhất sau khi mục nhập dòng bất thường hết thời gian chờ, và số đếm khởi động là số lượng các lần mà mục nhập dòng bất thường được khởi động.

Bộ xử lý 810 thực hiện mã chương trình, và được tạo cấu hình để xác định xem máy chủ được chỉ báo bởi bộ định danh máy chủ điểm đến có tồn tại trong

mạng SDN hay không, và khi xác định được rằng máy chủ được chỉ báo bởi bộ định danh máy chủ điểm đến không tồn tại trong mạng SDN, điều khiển bộ thu phát 830 để gửi mục nhập dòng bất thường tới bộ chuyển mạch thứ nhất; và ngoài ra còn được tạo cấu hình để xác định, theo số đếm khởi động được thu bởi bộ thu phát 830, xem sự tấn công nguy hiểm có được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn hay không.

Một cách tùy chọn, bộ xử lý 810 có thể được tạo cấu hình riêng để tính toán hệ số khởi động của mục nhập dòng bất thường theo số đếm khởi động và thời gian trôi qua của mục nhập dòng bất thường; và xác định xem hệ số khởi động có lớn hơn ngưỡng hệ số hay không; và nếu hệ số khởi động lớn hơn ngưỡng hệ số, xác định rằng sự tấn công nguy hiểm được bắt nguồn từ máy chủ nguồn; hoặc, nếu hệ số khởi động không lớn hơn ngưỡng hệ số, xác định rằng không có sự tấn công nguy hiểm nào bắt nguồn từ máy chủ nguồn.

Một cách tùy chọn, bộ xử lý 810 có thể được tạo cấu hình riêng để xác định xem số đếm khởi động có lớn hơn ngưỡng số đếm hay không; và nếu số đếm khởi động lớn hơn ngưỡng số đếm, xác định rằng sự tấn công nguy hiểm được bắt nguồn từ máy chủ nguồn; hoặc, nếu số đếm khởi động không lớn hơn ngưỡng số đếm, xác định rằng không có sự tấn công nguy hiểm nào bắt nguồn từ máy chủ nguồn.

Một cách tùy chọn, bộ xử lý 810 có thể ngoài ra còn được tạo cấu hình để: trước khi bộ thu phát 830 gửi mục nhập dòng bất thường tới bộ chuyển mạch thứ nhất, xác định xem mục nhập dòng bất thường của máy chủ nguồn được chỉ báo bộ định danh máy chủ nguồn đã được phân phối tới bộ chuyển mạch thứ nhất hay chưa; nếu mục nhập dòng bất thường của máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn chưa được phân phối tới bộ chuyển mạch thứ nhất, thực hiện bước điều khiển bộ thu phát 830 để gửi mục nhập dòng bất thường tới bộ chuyển mạch thứ nhất.

Một cách tùy chọn, bộ xử lý 810 có thể ngoài ra còn được tạo cấu hình để: khi xác định được rằng bảng dòng cuối cùng trong bộ chuyển mạch thứ nhất là bảng dung hợp chính xác bao gồm miền dung hợp bộ định danh máy chủ nguồn,

điều khiển bộ thu phát 830 để gửi chỉ dẫn thứ nhất tới bộ chuyển mạch thứ nhất, trong đó chỉ dẫn thứ nhất được sử dụng để chỉ dẫn cho bộ chuyển mạch thứ nhất tạo cấu hình bảng dung hợp chính xác như bảng dung hợp chính xác chỉ khớp với miền dung hợp bộ định danh máy chủ nguồn, để bộ chuyển mạch thứ nhất lưu trữ mục nhập dòng bất thường trong bảng dòng cuối cùng.

Bộ thu phát 830 có thể ngoài ra còn được tạo cấu hình để gửi chỉ dẫn thứ nhất tới bộ chuyển mạch thứ nhất.

Một cách tùy chọn, bộ xử lý 810 có thể ngoài ra còn được tạo cấu hình để: khi xác định được rằng bảng dòng cuối cùng trong bộ chuyển mạch thứ nhất là bảng dung hợp chính xác, và bảng ký tự đại diện bao gồm miền dung hợp bộ định danh máy chủ nguồn tồn tại trong bộ chuyển mạch thứ nhất, điều khiển bộ thu phát 830 để gửi chỉ dẫn thứ hai tới bộ chuyển mạch thứ nhất, trong đó chỉ dẫn thứ hai được sử dụng để chỉ dẫn cho bộ chuyển mạch thứ nhất điều chỉnh bảng ký tự đại diện bao gồm miền dung hợp bộ định danh máy chủ nguồn thành bảng dòng cuối cùng, để bộ chuyển mạch thứ nhất lưu trữ mục nhập dòng bất thường trong bảng dòng cuối cùng.

Bộ thu phát 830 có thể ngoài ra còn được tạo cấu hình để gửi chỉ dẫn thứ hai tới bộ chuyển mạch thứ nhất.

Một cách tùy chọn, bộ xử lý 810 có thể ngoài ra còn được tạo cấu hình để: khi xác định được, theo số đếm khởi động, rằng sự tấn công nguy hiểm được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn, điều khiển bộ thu phát 830 để gửi chỉ dẫn thứ ba tới bộ chuyển mạch thứ nhất, trong đó chỉ dẫn thứ ba được sử dụng để chỉ dẫn cho bộ chuyển mạch thứ nhất xóa gói dữ liệu từ máy chủ nguồn.

Bộ thu phát 830 có thể ngoài ra còn được tạo cấu hình để gửi chỉ dẫn thứ ba tới bộ chuyển mạch thứ nhất.

Trong phương án này, bộ điều khiển không cần phải thu thập các thống kê về các tin nhắn trong gói tương ứng với mỗi máy chủ, và thay vào đó gửi mục nhập dòng bất thường tới bộ chuyển mạch thứ nhất; bộ chuyển mạch thứ nhất thu

thập các thống kê về số đếm khởi động của mục nhập dòng bất thường và thông báo số đếm khởi động tới bộ điều khiển; bộ điều khiển xác định trực tiếp, theo số đếm khởi động, xem sự tấn công nguy hiểm có được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn hay không. Theo cách này, việc thu thập các thống kê tin nhắn được thực hiện đầu tiên bởi bộ điều khiển được phân phối tới mỗi bộ chuyển mạch để thực hiện, do đó giảm bớt lượng xử lý dữ liệu của bộ điều khiển, và cải thiện hiệu suất của bộ điều khiển.

Theo Fig.9, Fig.9 là lược đồ cấu trúc của bộ chuyển mạch thứ nhất 900 theo một phương án của sáng chế sáng chế. Bộ chuyển mạch thứ nhất 900 bao gồm: bộ xử lý 910, bộ nhớ 920, bộ thu phát 930, và bus 940.

Bộ xử lý 910, bộ nhớ 920, và bộ thu phát 930 được liên kết nối bằng cách sử dụng bus 940. Bus 940 có thể là bus ISA, bus PCI, hoặc bus EISA. Bus có thể là bus địa chỉ, bus dữ liệu, hoặc bus điều khiển. Để dễ minh họa, bus được thể hiện bằng dòng kẻ đậm trên Fig.9, nhưng không có nghĩa rằng chỉ có một bus hoặc một loại bus.

Bộ nhớ 920 được tạo cấu hình để lưu trữ chương trình. Cụ thể là, chương trình có thể bao gồm mã chương trình, và mã chương trình bao gồm chỉ dẫn thao tác máy tính. Bộ nhớ 920 có thể bao gồm bộ nhớ RAM tốc độ cao, và có thể ngoài ra còn bao gồm bộ nhớ bất biến (non-volatile memory), ví dụ như, ít nhất một bộ nhớ đĩa từ. Hơn nữa, bộ nhớ 920 ngoài ra còn được tạo cấu hình để lưu trữ bảng dòng.

Bộ thu phát 930 được tạo cấu hình để kết nối với một thiết bị khác, và truyền thông với một thiết bị khác. Cụ thể là, bộ thu phát 930 được tạo cấu hình để gửi tin nhắn trong gói tới bộ điều khiển, trong đó tin nhắn trong gói bao gồm bộ định danh máy chủ nguồn và bộ định danh máy chủ điểm đến của gói dữ liệu; thu mục nhập dòng bất thường được gửi bởi bộ điều khiển khi xác định được rằng máy chủ được chỉ báo bởi bộ định danh máy chủ điểm đến không tồn tại trong mạng SDN; và gửi số đếm khởi động của mục nhập dòng bất thường tới bộ điều khiển, khiến cho bộ điều khiển xác định, theo số đếm khởi động, xem sự tấn công nguy hiểm có được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định

danh máy chủ nguồn hay không.

Bộ xử lý 910 thực hiện mã chương trình, và được tạo cấu hình để: khi xác định được rằng mục nhập dòng tương ứng với gói dữ liệu không được tìm thấy, điều khiển bộ thu phát 930 để gửi tin nhắn trong gói tới bộ điều khiển; lưu mục nhập dòng bất thường được thu bởi bộ thu phát 930 tới bộ nhớ 920, trong đó mục nhập dòng bất thường được gửi bởi bộ điều khiển khi xác định được rằng máy chủ được chỉ báo bởi bộ định danh máy chủ điểm đến không tồn tại trong mạng SDN; và ghi, trong thời gian trôi qua của mục nhập dòng bất thường, số đếm khởi động của mục nhập dòng bất thường, và điều khiển bộ thu phát 930 để gửi số đếm khởi động tới bộ điều khiển sau khi mục nhập dòng bất thường hết thời gian chờ.

Một cách tùy chọn, bộ thu phát 930 có thể ngoài ra còn được tạo cấu hình để thu chỉ dẫn thứ nhất được gửi bởi bộ điều khiển; và

bộ xử lý 910 có thể ngoài ra còn được tạo cấu hình để tạo cấu hình bảng dung hợp chính xác địa phương mà là bảng dòng cuối cùng như bảng dung hợp chính xác chỉ khớp với miền dung hợp bộ định danh máy chủ nguồn theo chỉ dẫn thứ nhất được thu bởi bộ thu phát 930; hoặc

bộ thu phát 930 có thể ngoài ra còn được tạo cấu hình để thu chỉ dẫn thứ hai được gửi bởi bộ điều khiển; và

bộ xử lý 910 có thể ngoài ra còn được tạo cấu hình để điều chỉnh bảng ký tự đại diện bao gồm miền dung hợp bộ định danh máy chủ nguồn thành bảng dòng cuối cùng theo chỉ dẫn thứ hai được thu bởi bộ thu phát 930.

Một cách tùy chọn, bộ xử lý 910 có thể được tạo cấu hình riêng để lưu mục nhập dòng bất thường vào bảng dòng cuối cùng trong bộ nhớ 920.

Một cách tùy chọn, bộ thu phát 930 có thể ngoài ra còn được tạo cấu hình để thu chỉ dẫn thứ ba được gửi bởi bộ điều khiển, trong đó chỉ dẫn thứ ba được gửi bởi bộ điều khiển khi xác định, theo số đếm khởi động, sự tấn công nguy hiểm được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn.

Bộ xử lý 910 có thể ngoài ra còn được tạo cấu hình để xóa, theo chỉ dẫn thứ ba được thu bởi bộ thu phát 930, gói dữ liệu từ máy chủ nguồn.

Trong phương án này, bộ điều khiển không cần thiết phải thu thập các thống kê về các tin nhắn trong gói tương ứng với mỗi máy chủ, và thay vào đó, bộ chuyển mạch thứ nhất thu thập các thống kê về số đếm khởi động của mục nhập dòng bất thường và thông báo số đếm khởi động tới bộ điều khiển; bộ điều khiển xác định trực tiếp, theo số đếm khởi động, xem sự tấn công nguy hiểm có được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn hay không. Theo cách này, việc thu thập các thống kê tin nhắn được thực hiện đầu tiên bởi bộ điều khiển được phân phối tới mỗi bộ chuyển mạch để thực hiện, do đó giảm bớt lượng xử lý dữ liệu của bộ điều khiển, và cải thiện hiệu suất của bộ điều khiển.

Người có trình độ trung bình trong lĩnh vực có thể hiểu một cách rõ ràng rằng, các kỹ thuật trong các phương án của sáng chế có thể được thực hiện bởi phần mềm bên cạnh nền phần cứng cần thiết thông thường. Dựa vào hiểu biết như vậy, các giải pháp kỹ thuật của sáng chế về cơ bản hoặc một phần góp phần vào kỹ thuật trước đây có thể được thực hiện dưới dạng sản phẩm phần mềm. Sản phẩm phần mềm được lưu trữ trong phương tiện lưu trữ, ví dụ như ROM/RAM, đĩa cứng, hoặc đĩa quang, và bao gồm một số chỉ dẫn để chỉ dẫn thiết bị máy tính (mà có thể là máy tính cá nhân, máy chủ, hoặc thiết bị mạng) thực hiện các phương pháp được mô tả trong các phương án hoặc một số phần của các phương án của sáng chế.

Các phương án trong phần mô tả này đều được mô tả theo cách cấp tiến, đối với các phần giống nhau hoặc tương tự trong các cách thực hiện, theo các phương án này, và mỗi phương án tập trung vào một phần khác với phần của các phương án khác. Cụ thể là, phương án hệ thống về cơ bản là tương tự như phương án phương pháp, và do đó được mô tả sơ lược; đối với các phần có liên quan, tương ứng với các phần mô tả trong phương án phương pháp.

Các phần mô tả nêu trên là các cách thực hiện của sáng chế, nhưng không nhằm mục đích giới hạn phạm vi bảo hộ của sáng chế. Bất cứ cải biến, thay thế

tương đương, và cải tiến nào được thực hiện mà không trệch khỏi nguyên lý của sáng chế thì đều nằm trong phạm vi bảo hộ của sáng chế.

YÊU CẦU BẢO HỘ

1. Phương pháp phát hiện sự tấn công nguy hiểm bao gồm các bước:

thu, bởi bộ điều khiển, tin nhắn trong gói được gửi bởi bộ chuyển mạch thứ nhất, trong đó tin nhắn trong gói bao gồm bộ định danh máy chủ nguồn và bộ định danh máy chủ điểm đến của gói dữ liệu mà bộ chuyển mạch thứ nhất không tìm thấy mục nhập dòng;

khi xác định được rằng máy chủ được chỉ báo bởi bộ định danh máy chủ điểm đến không tồn tại trong mạng do phần mềm quyết định (SDN), gửi, bởi bộ điều khiển, mục nhập dòng bất thường tới bộ chuyển mạch thứ nhất, trong đó mục nhập dòng bất thường bao gồm bộ định danh máy chủ nguồn;

thu, bởi bộ điều khiển, số đếm khởi động được gửi bởi bộ chuyển mạch thứ nhất, trong đó số đếm khởi động được gửi bởi bộ chuyển mạch thứ nhất sau khi mục nhập dòng bất thường hết thời gian chờ, và số đếm khởi động là số lượng các lần mà mục nhập dòng bất thường được khởi động; và

xác định, bởi bộ điều khiển theo số đếm khởi động, xem sự tấn công nguy hiểm có được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn hay không.

2. Phương pháp theo điểm 1, trong đó việc xác định, bởi bộ điều khiển theo số đếm khởi động, xem sự tấn công nguy hiểm có được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn hay không bao gồm các bước:

tính toán, bởi bộ điều khiển, hệ số khởi động của mục nhập dòng bất thường theo số đếm khởi động và thời gian trôi qua của mục nhập dòng bất thường; và

xác định, bởi bộ điều khiển, xem hệ số khởi động có hơn hơn ngưỡng hệ số hay không; và nếu hệ số khởi động lớn hơn ngưỡng hệ số, xác định, bởi bộ điều khiển, rằng sự tấn công nguy hiểm được bắt nguồn từ máy chủ nguồn; hoặc, nếu hệ số khởi động không lớn hơn ngưỡng hệ số, xác định, bởi bộ điều khiển, rằng không có sự tấn công nguy hiểm nào bắt nguồn từ máy chủ nguồn.

3. Phương pháp theo điểm 1, trong đó việc xác định, bởi bộ điều khiển theo số đếm khởi động, xem sự tấn công nguy hiểm có được bắt nguồn từ máy chủ nguồn

được chỉ báo bởi bộ định danh máy chủ nguồn hay không bao gồm các bước:

xác định, bởi bộ điều khiển, xem số đếm khởi động có lớn hơn ngưỡng số đếm hay không; và nếu số đếm khởi động lớn hơn ngưỡng số đếm, xác định, bởi bộ điều khiển, rằng sự tấn công nguy hiểm được bắt nguồn từ máy chủ nguồn; hoặc, nếu số đếm khởi động không lớn hơn ngưỡng số đếm, xác định, bởi bộ điều khiển, rằng không có sự tấn công nguy hiểm nào bắt nguồn từ máy chủ nguồn.

4. Phương pháp theo điểm bất kì trong số các điểm từ 1 đến 3, trước khi gửi, bởi bộ điều khiển, mục nhập dòng bất thường tới bộ chuyển mạch thứ nhất, ngoài ra còn bao gồm các bước:

xác định, bởi bộ điều khiển, xem mục nhập dòng bất thường của máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn đã được phân phối tới bộ chuyển mạch thứ nhất hay chưa; và nếu mục nhập dòng bất thường của máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn chưa được phân phối tới bộ chuyển mạch thứ nhất, thực hiện, bởi bộ điều khiển, bước gửi mục nhập dòng bất thường tới bộ chuyển mạch thứ nhất.

5. Phương pháp theo điểm bất kì trong số các điểm từ 1 đến 4, ngoài ra còn bao gồm các bước:

khi xác định được rằng bảng dòng cuối cùng trong bộ chuyển mạch thứ nhất là bảng dung hợp chính xác có chứa miền dung hợp bộ định danh máy chủ nguồn, gửi, bởi bộ điều khiển, chỉ dẫn thứ nhất tới bộ chuyển mạch thứ nhất, trong đó chỉ dẫn thứ nhất được sử dụng để chỉ dẫn cho bộ chuyển mạch thứ nhất tạo cấu hình bảng dung hợp chính xác như bảng dung hợp chính xác chỉ khớp với miền dung hợp bộ định danh máy chủ nguồn, để bộ chuyển mạch thứ nhất lưu trữ mục nhập dòng bất thường trong bảng dòng cuối cùng.

6. Phương pháp theo điểm bất kì trong số các điểm từ 1 đến 4, ngoài ra còn bao gồm các bước:

khi xác định được rằng bảng dòng cuối cùng trong bộ chuyển mạch thứ nhất là bảng dung hợp chính xác, và bảng ký tự đại diện có chứa miền dung hợp bộ định danh máy chủ nguồn tồn tại trong bộ chuyển mạch thứ nhất, gửi, bởi bộ điều

khiển, chỉ dẫn thứ hai tới bộ chuyển mạch thứ nhất, trong đó chỉ dẫn thứ hai được sử dụng để chỉ dẫn cho bộ chuyển mạch thứ nhất điều chỉnh bảng ký tự đại diện có chứa miền dung hợp bộ định danh máy chủ nguồn thành bảng dòng cuối cùng, để bộ chuyển mạch thứ nhất lưu trữ mục nhập dòng bất thường trong bảng dòng cuối cùng.

7. Phương pháp theo điểm bất kì trong số các điểm từ 1 đến 6, trong đó quyền ưu tiên của mục nhập dòng bất thường là quyền ưu tiên thấp nhất của mục nhập dòng trong bộ chuyển mạch thứ nhất.

8. Phương pháp theo điểm bất kì trong số các điểm từ 1 đến 7, ngoài ra còn bao gồm các bước:

khi xác định, theo số đếm khởi động, rằng sự tấn công nguy hiểm được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn, gửi, bởi bộ điều khiển, chỉ dẫn thứ ba tới bộ chuyển mạch thứ nhất, trong đó chỉ dẫn thứ ba được sử dụng để chỉ dẫn cho bộ chuyển mạch thứ nhất xóa gói dữ liệu từ máy chủ nguồn.

9. Phương pháp phát hiện sự tấn công nguy hiểm, bao gồm các bước:

khi xác định được rằng mục nhập dòng tương ứng với gói dữ liệu không được tìm thấy, gửi, bởi bộ chuyển mạch thứ nhất, tin nhắn trong gói tới bộ điều khiển, trong đó tin nhắn trong gói bao gồm bộ định danh máy chủ nguồn và bộ định danh máy chủ điểm đến của gói dữ liệu;

thu và lưu, bởi bộ chuyển mạch thứ nhất, mục nhập dòng bất thường, trong đó mục nhập dòng bất thường được gửi bởi bộ điều khiển khi xác định được rằng máy chủ được chỉ báo bởi bộ định danh máy chủ điểm đến không tồn tại trong mạng SDN; và

ghi, bởi bộ chuyển mạch thứ nhất trong khoảng thời gian trôi qua của mục nhập dòng bất thường, số đếm khởi động của mục nhập dòng bất thường, và gửi số đếm khởi động tới bộ điều khiển sau khi mục nhập dòng bất thường hết thời gian chờ, khiến cho bộ điều khiển xác định, theo số đếm khởi động, xem sự tấn công nguy hiểm có được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định

danh máy chủ nguồn hay không.

10. Phương pháp theo điểm 9, ngoài ra còn bao gồm các bước:

thu, bởi bộ chuyển mạch thứ nhất, chỉ dẫn thứ nhất được gửi bởi bộ điều khiển, và tạo cấu hình, theo chỉ dẫn thứ nhất, bảng dung hợp chính xác địa phương mà là bảng dòng cuối cùng như bảng dung hợp chính xác chỉ khớp với miền dung hợp bộ định danh máy chủ nguồn; hoặc,

thu, bởi bộ chuyển mạch thứ nhất, chỉ dẫn thứ hai được gửi bởi bộ điều khiển, và điều chỉnh bảng ký tự đại diện có chứa miền dung hợp bộ định danh máy chủ nguồn thành bảng dòng cuối cùng theo chỉ dẫn thứ hai.

11. Phương pháp theo điểm 10, trong đó việc lưu, bởi bộ chuyển mạch thứ nhất, mục nhập dòng bất thường bao gồm bước:

lưu, bởi bộ chuyển mạch thứ nhất, mục nhập dòng bất thường vào bảng dòng cuối cùng.

12. Phương pháp theo điểm bất kì trong số các điểm từ 9 đến 11, ngoài ra còn bao gồm các bước:

thu, bởi bộ chuyển mạch thứ nhất, chỉ dẫn thứ ba được gửi bởi bộ điều khiển, trong đó chỉ dẫn thứ ba được gửi bởi bộ điều khiển khi xác định, theo số đếm khởi động, rằng sự tấn công nguy hiểm được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn; và

xóa, bởi bộ chuyển mạch thứ nhất theo chỉ dẫn thứ ba, gói dữ liệu từ máy chủ nguồn.

13. Thiết bị phát hiện sự tấn công nguy hiểm bao gồm:

bộ thu thứ nhất, được tạo cấu hình để thu tin nhắn trong gói được gửi bởi bộ chuyển mạch thứ nhất, trong đó tin nhắn trong gói bao gồm bộ định danh máy chủ nguồn và bộ định danh máy chủ điểm đến của gói dữ liệu mà bộ chuyển mạch thứ nhất không tìm thấy mục nhập dòng;

bộ gửi thứ nhất, được tạo cấu hình để: khi xác định được rằng máy chủ được chỉ báo bởi bộ định danh máy chủ điểm đến được thu bởi bộ thu thứ nhất không tồn tại trong mạng do phần mềm quyết định (SDN), gửi mục nhập dòng bất

thường tới bộ chuyển mạch thứ nhất, trong đó mục nhập dòng bất thường bao gồm bộ định danh máy chủ nguồn, trong đó:

bộ thu thứ nhất ngoài ra còn được tạo cấu hình để thu số đếm khởi động được gửi bởi bộ chuyển mạch thứ nhất, trong đó số đếm khởi động được gửi bởi bộ chuyển mạch thứ nhất sau khi mục nhập dòng bất thường hết thời gian chờ, và số đếm khởi động là số lượng các lần mà mục nhập dòng bất thường được khởi động; và

bộ phát hiện, được tạo cấu hình để xác định, theo số đếm khởi động được thu bởi bộ thu thứ nhất, xem sự tấn công nguy hiểm có được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn hay không.

14. Thiết bị theo điểm 13, trong đó bộ phát hiện được tạo cấu hình riêng để:

tính toán hệ số khởi động của mục nhập dòng bất thường theo số đếm khởi động được thu bởi bộ thu thứ nhất và thời gian trôi qua của mục nhập dòng bất thường; và

xác định xem hệ số khởi động có lớn hơn ngưỡng hệ số hay không; và nếu hệ số khởi động lớn hơn ngưỡng hệ số, xác định rằng sự tấn công nguy hiểm được bắt nguồn từ máy chủ nguồn; hoặc, nếu hệ số khởi động không lớn hơn ngưỡng hệ số, xác định rằng không có sự tấn công nguy hiểm nào bắt nguồn từ máy chủ nguồn.

15. Thiết bị theo điểm 13, trong đó bộ phát hiện được tạo cấu hình riêng để:

xác định xem số đếm khởi động có lớn hơn ngưỡng số đếm hay không; và nếu số đếm khởi động lớn hơn ngưỡng số đếm, xác định rằng sự tấn công nguy hiểm được bắt nguồn từ máy chủ nguồn; hoặc, nếu số đếm khởi động không lớn hơn ngưỡng số đếm, xác định rằng không có sự tấn công nguy hiểm nào bắt nguồn từ máy chủ nguồn.

16. Thiết bị theo điểm bất kì trong số các điểm từ 13 đến 15, ngoài ra còn bao gồm:

bộ xác định, được tạo cấu hình để xác định xem mục nhập dòng bất thường của máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn đã được phân

phối tới bộ chuyển mạch thứ nhất hay chưa; và nếu mục nhập dòng bất thường của máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn chưa được phân phối tới bộ chuyển mạch thứ nhất, khởi động bộ gửi thứ nhất để gửi mục nhập dòng bất thường tới bộ chuyển mạch thứ nhất.

17. Thiết bị theo điểm bất kì trong số các điểm từ 13 đến 16, trong đó bộ gửi thứ nhất ngoài ra còn được tạo cấu hình để: khi xác định được rằng bảng dòng cuối cùng trong bộ chuyển mạch thứ nhất là bảng dung hợp chính xác có chứa miền dung hợp bộ định danh máy chủ nguồn, chỉ dẫn bộ chuyển mạch thứ nhất tạo cấu hình bảng dung hợp chính xác như bảng dung hợp chính xác chỉ khớp với miền dung hợp bộ định danh máy chủ nguồn, để bộ chuyển mạch thứ nhất lưu trữ mục nhập dòng bất thường trong bảng dòng cuối cùng.

18. Thiết bị theo điểm bất kì trong số các điểm từ 13 đến 16, trong đó bộ gửi thứ nhất ngoài ra còn được tạo cấu hình để:

khi xác định được rằng bảng dòng cuối cùng trong bộ chuyển mạch thứ nhất là bảng dung hợp chính xác, và bảng ký tự đại diện có chứa miền dung hợp bộ định danh máy chủ nguồn tồn tại trong bộ chuyển mạch thứ nhất, gửi chỉ dẫn thứ hai tới bộ chuyển mạch thứ nhất, trong đó chỉ dẫn thứ hai được sử dụng để chỉ dẫn cho bộ chuyển mạch thứ nhất điều chỉnh bảng ký tự đại diện có chứa miền dung hợp bộ định danh máy chủ nguồn thành bảng dòng cuối cùng, để bộ chuyển mạch thứ nhất lưu trữ mục nhập dòng bất thường trong bảng dòng cuối cùng.

19. Thiết bị theo điểm bất kì trong số các điểm từ 13 đến 18, trong đó bộ gửi thứ nhất ngoài ra còn được tạo cấu hình để:

khi xác định được, theo số đếm khởi động, rằng sự tấn công nguy hiểm được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn, gửi chỉ dẫn thứ ba tới bộ chuyển mạch thứ nhất, trong đó chỉ dẫn thứ ba được sử dụng để chỉ dẫn cho bộ chuyển mạch thứ nhất xóa gói dữ liệu từ máy chủ nguồn.

20. Thiết bị phát hiện sự tấn công nguy hiểm bao gồm:

bộ gửi thứ hai, được tạo cấu hình để: khi xác định được rằng mục nhập dòng tương ứng với gói dữ liệu không được tìm thấy, gửi tin nhắn trong gói tới bộ điều

khiển, trong đó tin nhắn trong gói bao gồm bộ định danh máy chủ nguồn và bộ định danh máy chủ điểm đến của gói dữ liệu;

bộ thu thứ hai, được tạo cấu hình để thu mục nhập dòng bất thường, trong đó mục nhập dòng bất thường được gửi bởi bộ điều khiển khi xác định được rằng máy chủ được chỉ báo bởi bộ định danh máy chủ điểm đến không tồn tại trong mạng do phần mềm quyết định (SDN);

bộ lưu trữ, được tạo cấu hình để lưu mục nhập dòng bất thường được thu bởi bộ thu thứ hai; và

bộ ghi số đếm, được tạo cấu hình để ghi, trong khoảng thời gian trôi qua của mục nhập dòng bất thường được lưu bởi bộ lưu trữ, số đếm khởi động của mục nhập dòng bất thường, trong đó:

bộ gửi thứ hai ngoài ra còn được tạo cấu hình để: sau khi mục nhập dòng bất thường được lưu bởi bộ lưu trữ hết hạn, gửi số đếm khởi động được ghi bởi bộ ghi số đếm tới bộ điều khiển, khiến cho bộ điều khiển xác định, theo số đếm khởi động, xem sự tấn công nguy hiểm có được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn hay không.

21. Thiết bị theo điểm 20, trong đó bộ thu thứ hai ngoài ra còn được tạo cấu hình để thu chỉ dẫn thứ nhất được gửi bởi bộ điều khiển; và

thiết bị ngoài ra còn bao gồm: bộ cấu hình, được tạo cấu hình để tạo cấu hình, theo chỉ dẫn thứ nhất, bảng dung hợp chính xác địa phương mà là bảng dòng cuối cùng như bảng dung hợp chính xác chỉ khớp với miền dung hợp bộ định danh máy chủ nguồn; hoặc

bộ thu thứ hai ngoài ra còn được tạo cấu hình để thu chỉ dẫn thứ hai được gửi bởi bộ điều khiển; và

thiết bị ngoài ra còn bao gồm: bộ cấu hình, được tạo cấu hình để điều chỉnh bảng ký tự đại diện có chứa miền dung hợp bộ định danh máy chủ nguồn thành bảng dòng cuối cùng theo chỉ dẫn thứ hai.

22. Thiết bị theo điểm 21, trong đó bộ lưu trữ được tạo cấu hình riêng để lưu mục nhập dòng bất thường vào bảng dòng cuối cùng.

23. Thiết bị theo điểm bất kì trong số các điểm từ 20 đến 22, trong đó bộ thu thứ hai ngoài ra còn được tạo cấu hình để thu chỉ dẫn thứ ba được gửi bởi bộ chuyển mạch thứ nhất; và

thiết bị ngoài ra còn bao gồm: bộ điều khiển, được tạo cấu hình để xóa gói dữ liệu từ máy chủ nguồn.

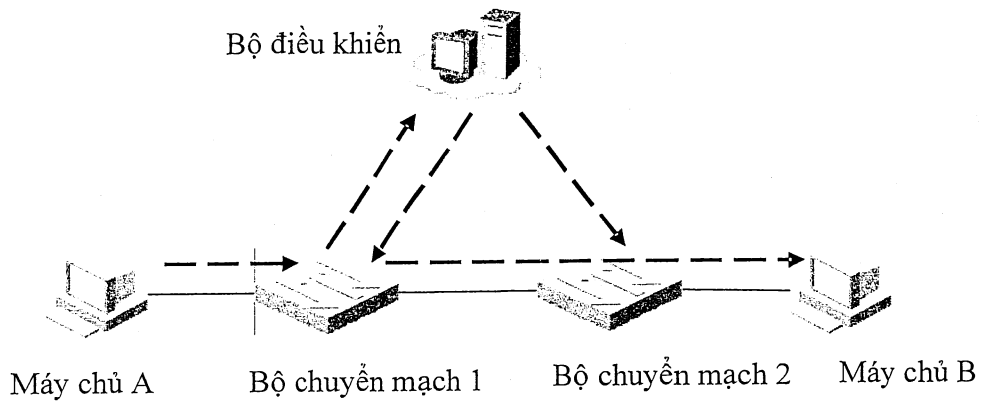


FIG. 1

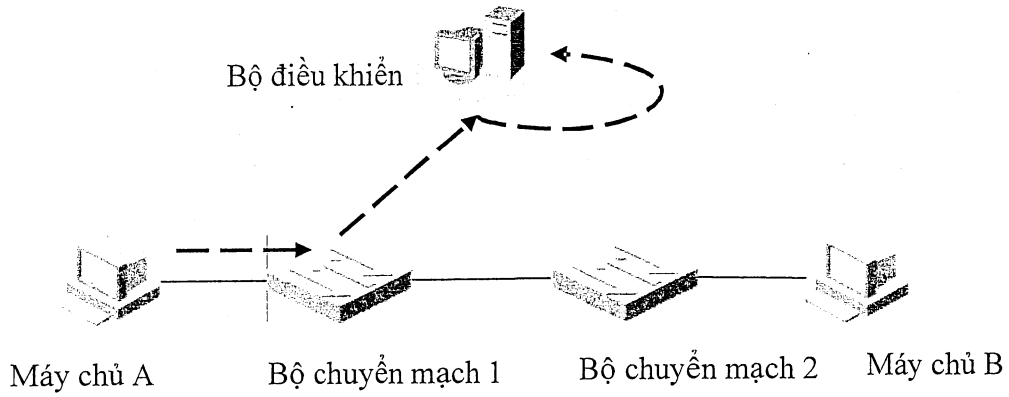


FIG. 2

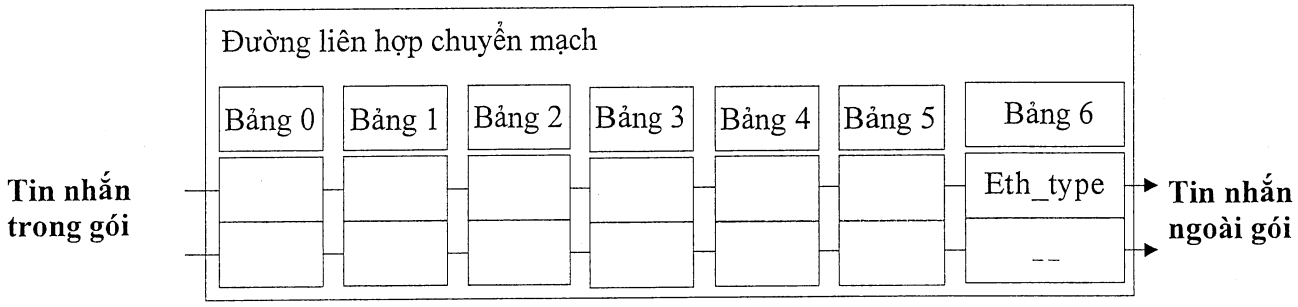


FIG. 2A

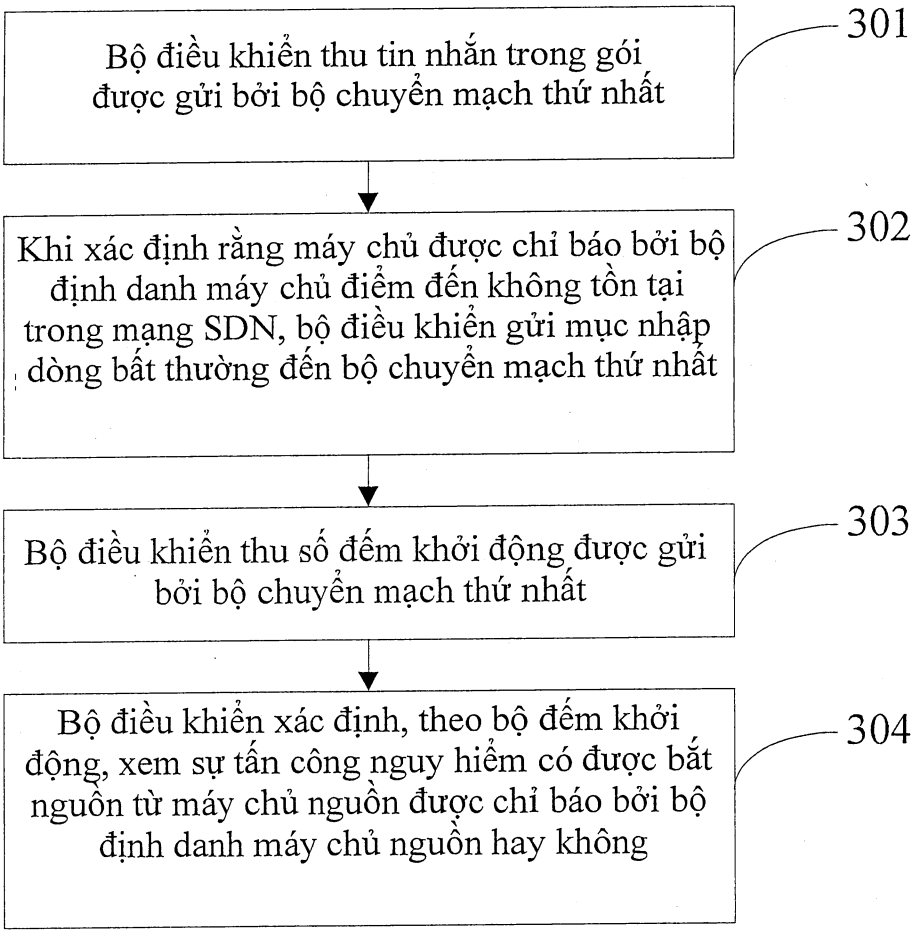

Bộ điều khiển thu tin nhắn trong gói được gửi bởi bộ chuyển mạch thứ nhất
301
Khi xác định rằng máy chủ được chỉ báo bởi bộ định danh máy chủ điểm đến không tồn tại trong mạng SDN, bộ điều khiển gửi mục nhập dòng bất thường đến bộ chuyển mạch thứ nhất
302
Bộ điều khiển thu số đếm khởi động được gửi bởi bộ chuyển mạch thứ nhất
303
Bộ điều khiển xác định, theo bộ đếm khởi động, xem sự tấn công nguy hiểm có được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn hay không
304

FIG. 3

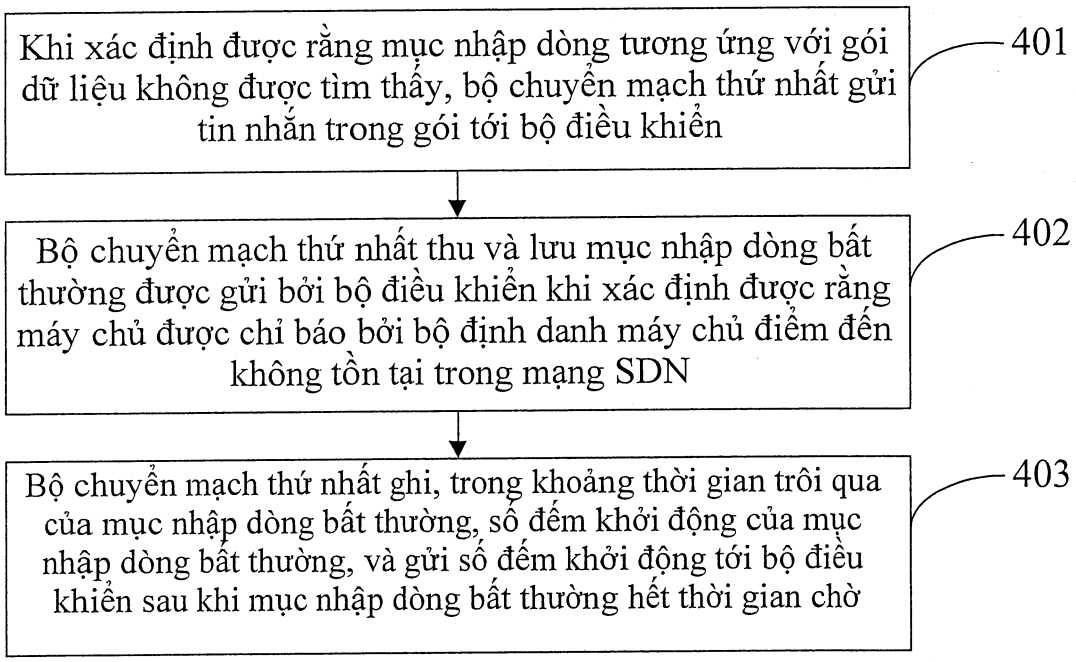

Khi xác định được rằng mục nhập dòng tương ứng với gói dữ liệu không được tìm thấy, bộ chuyển mạch thứ nhất gửi tin nhắn trong gói tới bộ điều khiển
401
Bộ chuyển mạch thứ nhất thu và lưu mục nhập dòng bất thường được gửi bởi bộ điều khiển khi xác định được rằng máy chủ được chỉ báo bởi bộ định danh máy chủ điểm đến không tồn tại trong mạng SDN
402
Bộ chuyển mạch thứ nhất ghi, trong khoảng thời gian trôi qua của mục nhập dòng bất thường, số đếm khởi động của mục nhập dòng bất thường, và gửi số đếm khởi động tới bộ điều khiển sau khi mục nhập dòng bất thường hết thời gian chờ
403

FIG. 4

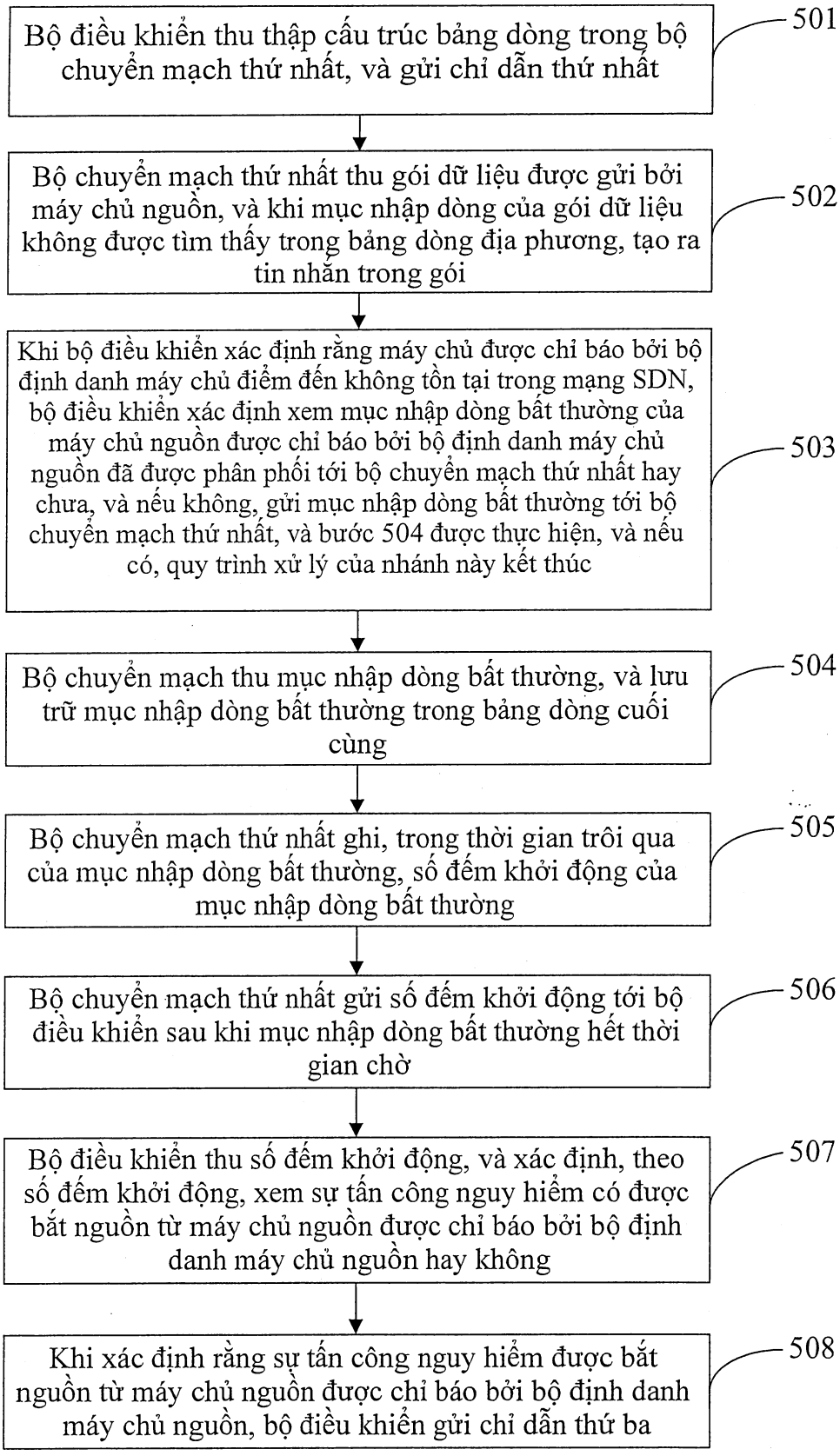

Bộ điều khiển thu thập cấu trúc bảng dòng trong bộ chuyển mạch thứ nhất, và gửi chỉ dẫn thứ nhất
501
Bộ chuyển mạch thứ nhất thu gói dữ liệu được gửi bởi máy chủ nguồn, và khi mục nhập dòng của gói dữ liệu không được tìm thấy trong bảng dòng địa phương, tạo ra tin nhắn trong gói
502
Khi bộ điều khiển xác định rằng máy chủ được chỉ báo bởi bộ định danh máy chủ điểm đến không tồn tại trong mạng SDN, bộ điều khiển xác định xem mục nhập dòng bất thường của máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn đã được phân phối tới bộ chuyển mạch thứ nhất hay chưa, và nếu không, gửi mục nhập dòng bất thường tới bộ chuyển mạch thứ nhất, và bước 504 được thực hiện, và nếu có, quy trình xử lý của nhánh này kết thúc
503
Bộ chuyển mạch thu mục nhập dòng bất thường, và lưu trữ mục nhập dòng bất thường trong bảng dòng cuối cùng
504
Bộ chuyển mạch thứ nhất ghi, trong thời gian trôi qua của mục nhập dòng bất thường, số đếm khởi động của mục nhập dòng bất thường
505
Bộ chuyển mạch thứ nhất gửi số đếm khởi động tới bộ điều khiển sau khi mục nhập dòng bất thường hết thời gian chờ
506
Bộ điều khiển thu số đếm khởi động, và xác định, theo số đếm khởi động, xem sự tấn công nguy hiểm có được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn hay không
507
Khi xác định rằng sự tấn công nguy hiểm được bắt nguồn từ máy chủ nguồn được chỉ báo bởi bộ định danh máy chủ nguồn, bộ điều khiển gửi chỉ dẫn thứ ba
508

FIG. 5

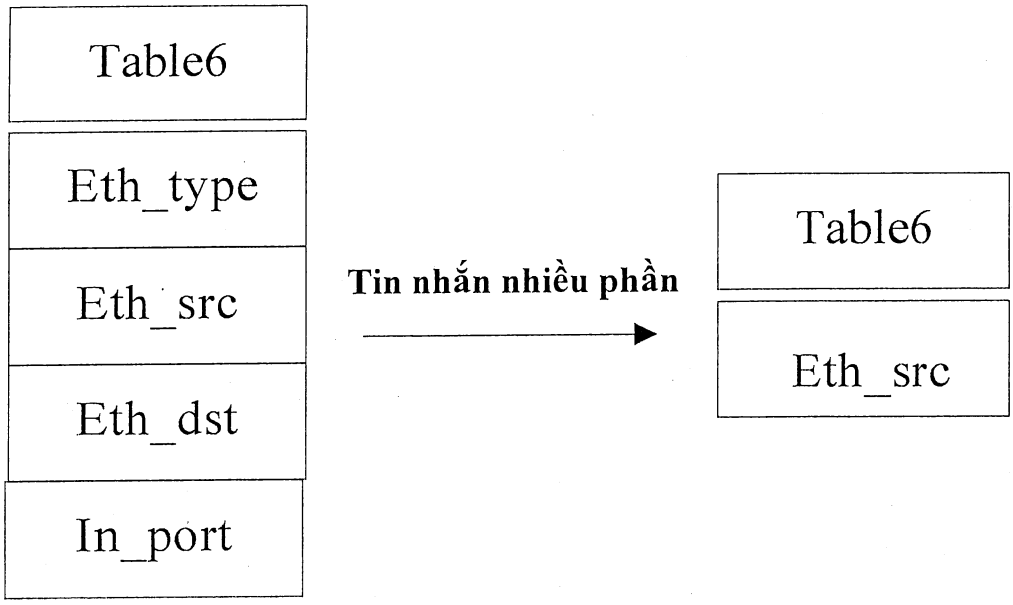


Table6
Eth_type
Eth_src
Eth_dst
In_port
Tin nhắn nhiều phần
Table6
Eth_src

FIG. 5A

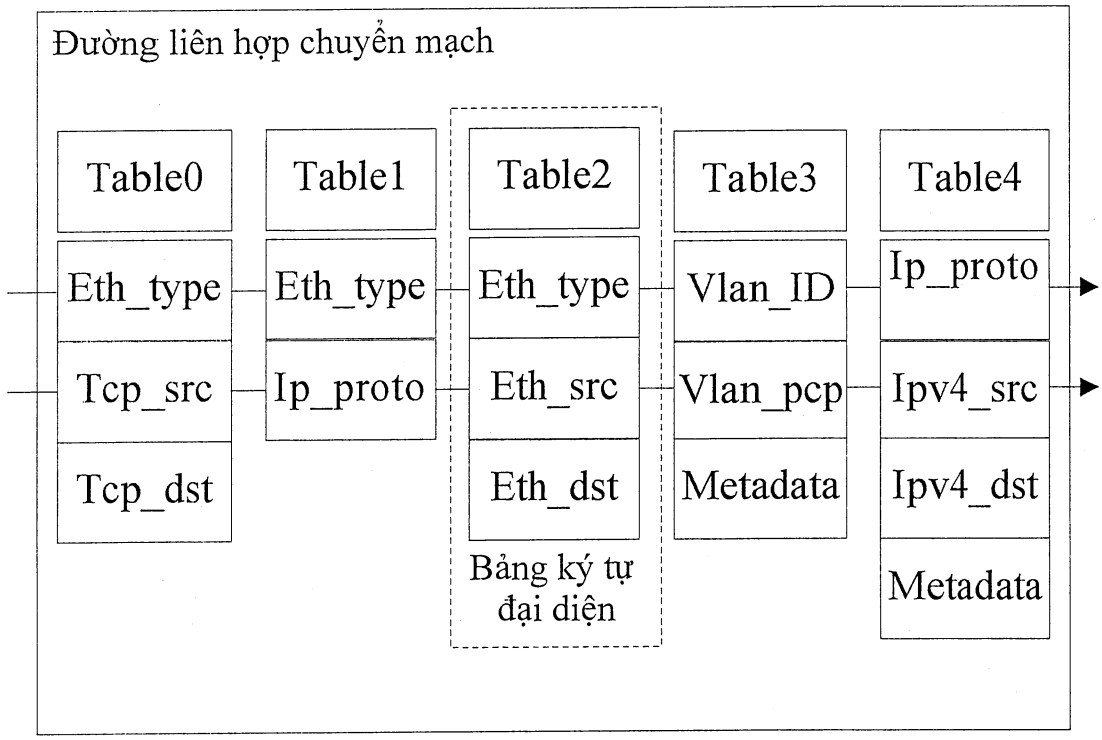

Đường liên hợp chuyển mạch
Table0
Eth_type
Tcp_src
Tcp_dst
Table1
Eth_type
Ip_proto
Table2
Eth_type
Eth_src
Eth_dst
Bảng ký tự đại diện
Table3
Vlan_ID
Vlan_pcp
Metadata
Table4
Ip_proto
Ipv4_src
Ipv4_dst
Metadata

FIG. 5B

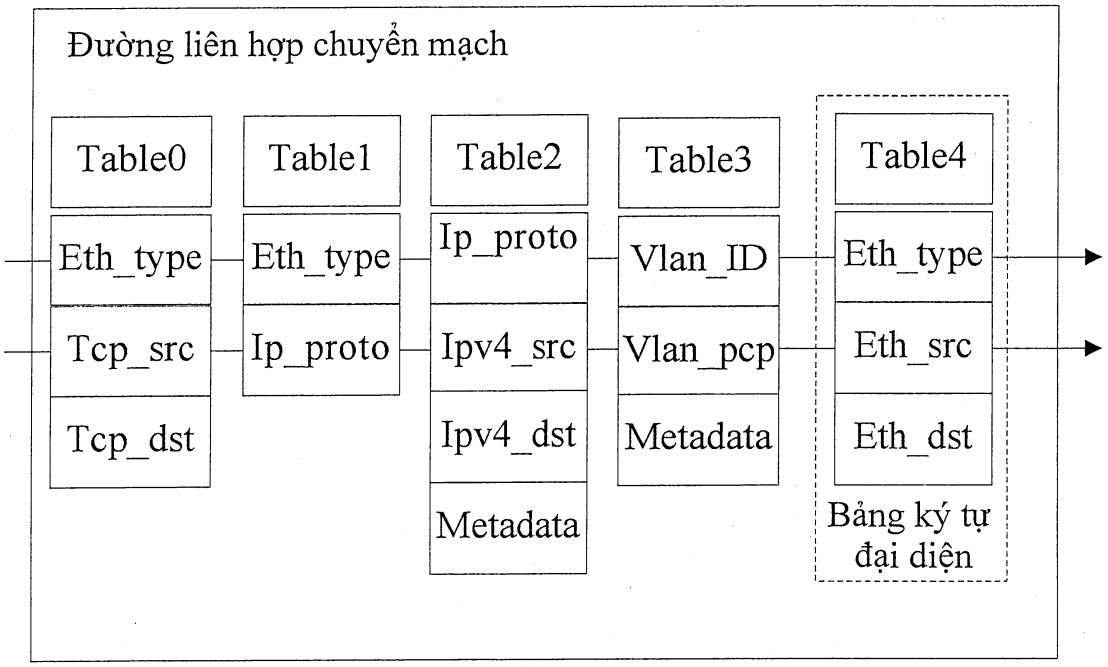


FIG. 5C

Flow-mod

command = ADD
table_id = 6
idle_timeout = 0
hard_timeout = 1
priority = 0
flag = SEND_FLOW_REM ||
CHECK_OVERLAP
match:
src_mac = 11:22:33:44:55:66
action:
outpurt, port = CONTROLLER

FIG. 5D

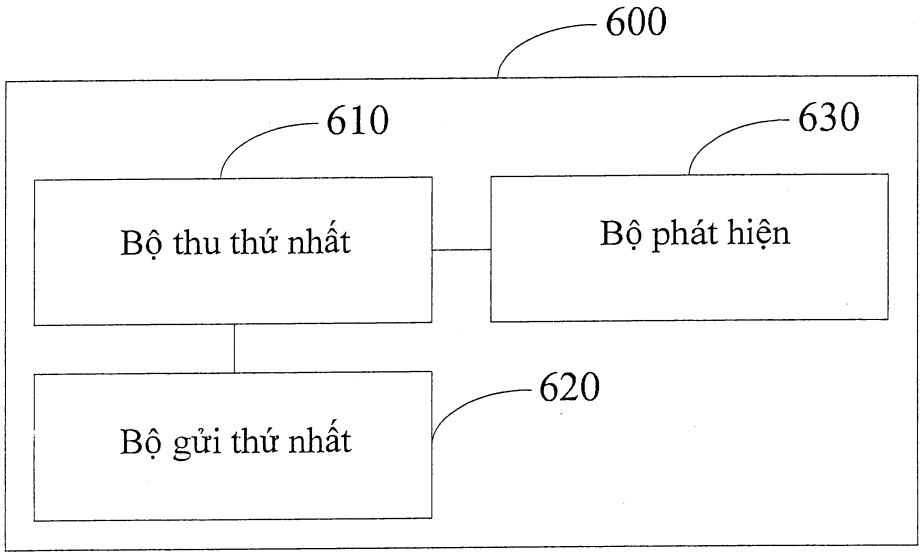

600
610
630
Bộ thu thứ nhất
Bộ phát hiện
Bộ gửi thứ nhất
620

FIG. 6

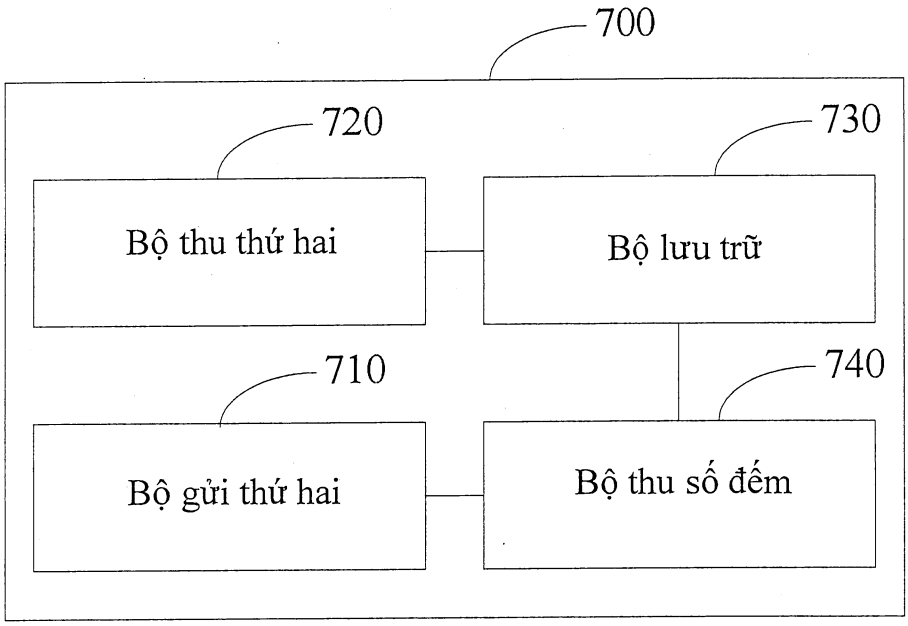

700
720
730
Bộ thu thứ hai
Bộ lưu trữ
710
740
Bộ gửi thứ hai
Bộ thu số đếm

FIG. 7

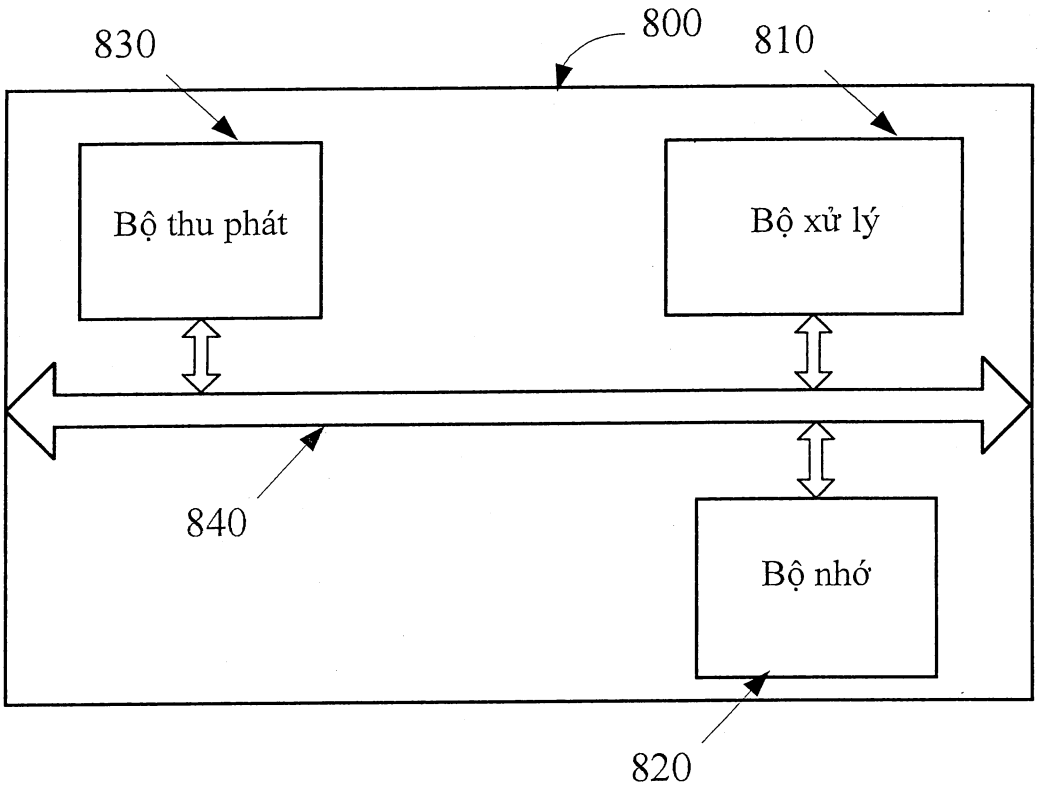

800
830
810
Bộ thu phát
Bộ xử lý
840
Bộ nhớ
820

FIG. 8

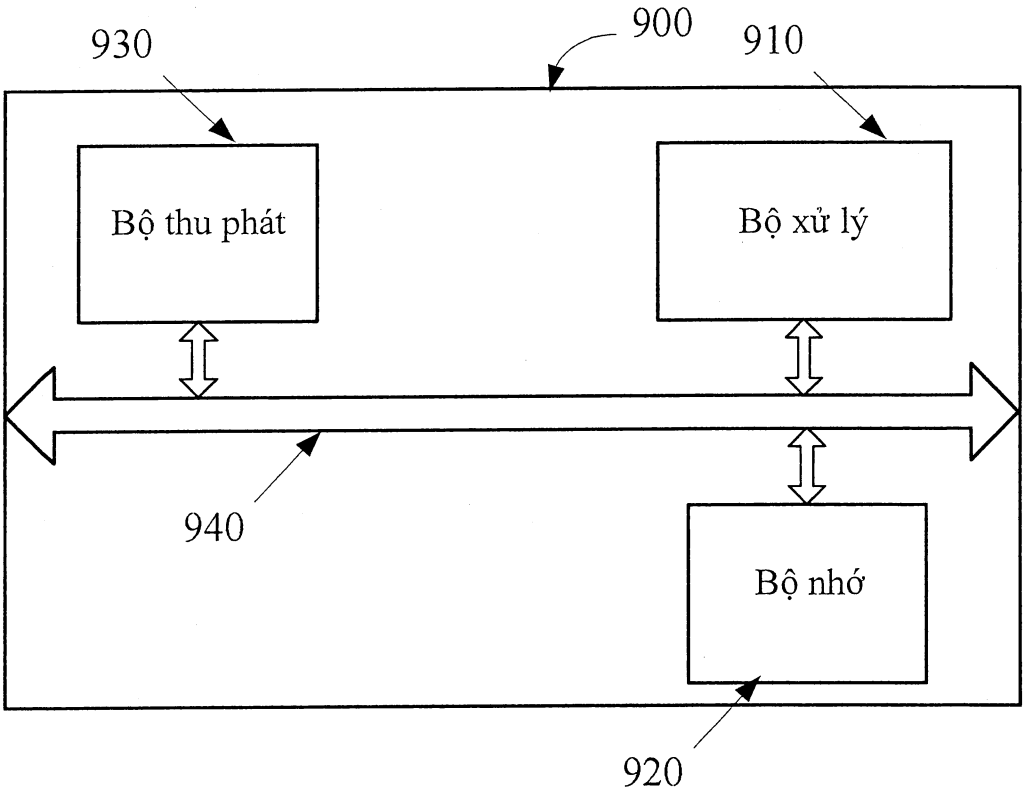

900
930
910
Bộ thu phát
Bộ xử lý
940
Bộ nhớ
920

FIG. 9