



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

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

(11)



2-0003912

(51) **H04L 12/00**
2022.01

(13) **Y**

(21) 2-2023-00415

(22) 28/10/2021

(67) 1-2021-06856

(45) 27/01/2025 442

(43) 27/12/2021 405

(73) Tập đoàn Công nghiệp - Viễn thông Quân Đội (VN)

Lô D26 khu đô thị mới Cầu Giấy, phường Yên Hòa, quận Cầu Giấy, thành phố Hà Nội

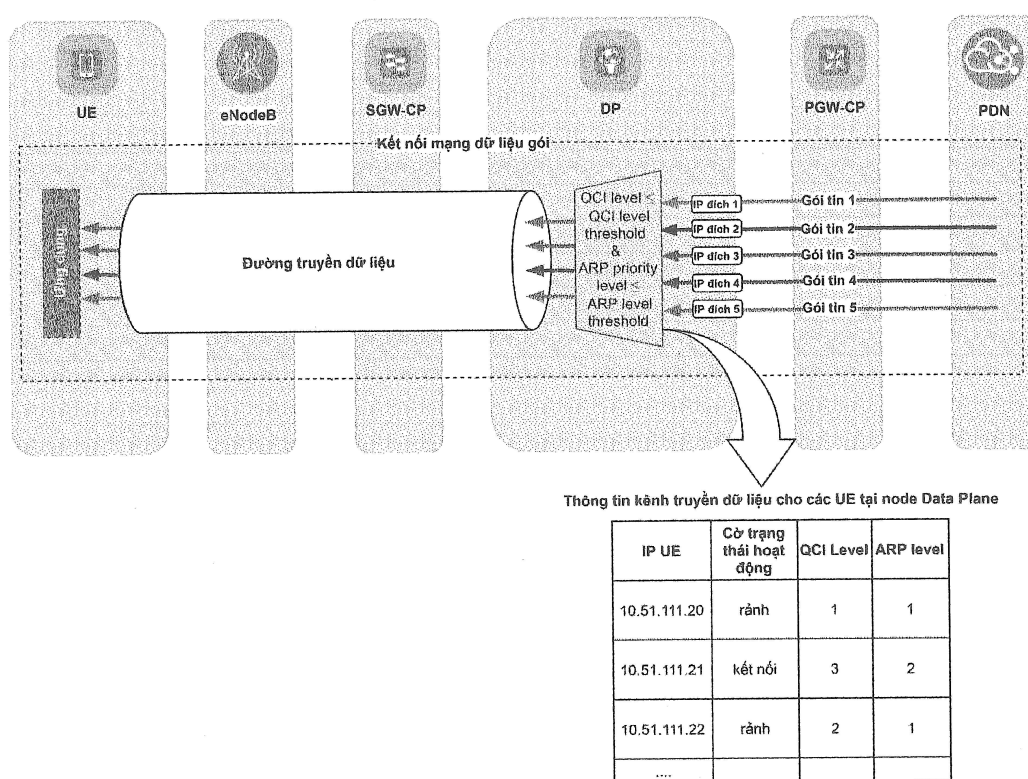
(72) Lê Ngọc Toàn (VN); Triệu Tuấn Anh (VN); Lê Ngọc Lâm (VN).

(74) Công ty TNHH NACILAW (NACILAW)

(54) **PHƯƠNG PHÁP BẢO VỆ TÂN CÔNG TỪ CHỐI DỊCH VỤ PHÂN TÁN ĐẾN HỆ
THỐNG MẠNG 4G LTE DỰA VÀO CƠ CHẾ PHÂN LOẠI CHẤT LƯỢNG
ĐƯỜNG TRUYỀN**

(21) 2-2023-00415

(57) Giải pháp hữu ích đề xuất phương pháp bảo vệ tấn công từ chối dịch vụ phân tán đến hệ thống mạng 4G LTE dựa vào cơ chế phân loại chất lượng đường truyền. Bằng việc phân tích thông tin đường truyền và loại bỏ các bản tin không thuộc dịch vụ ưu tiên khi hệ thống cao tải, phương pháp này bảo vệ các node trong hệ thống LTE khỏi tình trạng quá tải và ngăn chặn sự cố tê liệt hệ thống mạng LTE. Đây là phương pháp ưu việt vì tính dễ dàng cài đặt, đơn giản trong việc triển khai, vận hành mà không phát sinh phí đầu tư, tiết kiệm được rất nhiều chi phí cho nhà mạng khai thác viễn thông.



Hình 4

Lĩnh vực kỹ thuật được đề cập

Giải pháp hữu ích đề cập đến phương pháp bảo vệ tấn công từ chối dịch vụ phân tán đến hệ thống mạng 4G LTE dựa vào cơ chế phân loại chất lượng đường truyền. Cụ thể, phương pháp này bảo vệ các máy chủ trong hệ thống LTE khỏi tình trạng quá tải và ngăn chặn sự cố tê liệt hệ thống mạng LTE.

Tình trạng kỹ thuật của giải pháp hữu ích

Trong mạng di động 4G LTE (Long Term Evolution – 4G LTE), khi thiết bị người dùng (User Equipment - UE) vẫn duy trì đăng ký với mạng, nhưng trong trạng thái rảnh (*Idle*): không thực hiện cuộc gọi, gửi-nhận tin nhắn hoặc kết nối Internet, nếu thời gian đó có lưu lượng từ Internet, hoặc hệ thống mạng viễn thông khác gửi đến cho thuê bao, thực thể quản lý di động (Mobility Management Entity - MME) sẽ thực hiện thủ tục tìm gọi (Paging) – tìm kiếm UE đang trong vùng quản lý của trạm gốc eNodeB nào và yêu cầu UE thiết lập lại phiên kết nối với mạng lõi (Evolved Packet Core - EPC). Đáng chú ý, thủ tục thiết lập lại kết nối gồm thiết lập kênh vô tuyến, xác thực với mạng lõi, thiết lập các kênh truyền vô tuyến cho dữ liệu đường xuống, đường truyền dữ liệu trên giao diện S1-U, S5/S8. Khi đối tượng tấn công gửi hàng loạt gói dữ liệu tới các thuê bao đang ở trạng thái đó và thuộc quản lý của hệ thống mạng LTE, việc số lượng lớn các UE thực thi đồng thời các thủ tục sẽ chiếm dụng nhiều tài nguyên vô tuyến, tài nguyên mạng và làm quá tải CPU ở các máy chủ mạng dẫn tới tê liệt hệ thống.

Để hạn chế nguồn lưu lượng này, ta có thể thiết lập lọc gói dữ liệu và tiến hành loại bỏ chúng.

Bản chất kỹ thuật của giải pháp hữu ích

Mục đích của giải pháp hữu ích nhằm đưa ra phương pháp kiểm soát lưu lượng gói dữ liệu từ mạng ngoài để ngăn chặn cuộc tấn công từ chối dịch vụ phân tán (Distributed Denial of Service - DDoS) nhằm vào hệ thống mạng LTE. Theo thiết kế của LTE, máy chủ quản lý gói dữ liệu người dùng (Data Plane - DP) là máy chủ cuối cùng để gửi dữ liệu của UE tới hệ thống mạng ngoài. Ở chiều ngược lại, đây là máy chủ trực tiếp nhận dữ liệu từ hệ thống mạng bên ngoài, gửi qua các máy chủ (server) khác để phân phối dữ

liệu tới các UE trong hệ thống mạng của mình. Bởi vậy, việc tiến hành lọc gói dữ liệu sẽ đặt tại máy chủ này, nhằm đảm bảo an toàn cho các node khác trong hệ thống khi có nguồn lưu lượng đột biến đến từ mạng ngoài.

Khi UE vẫn giữ đăng ký với mạng LTE, nhưng không được cấp phát tài nguyên vô tuyến, kết nối với mạng lõi EPC đã bị hủy, lúc đó UE trong trạng thái rảnh. Nếu tại thời điểm đó, phát sinh luồng lưu lượng mới từ mạng ngoài tới UE, trong mạng lõi, máy chủ DP dựa vào IP đích của bản tin (IP của UE) để lấy thông tin chất lượng đường truyền (Bearer QoS) giành cho UE. Thông tin này được lưu trữ sau phiên làm việc trước của UE (yêu cầu vào mạng - attach, yêu cầu dịch vụ - service request, ...). Nếu đường truyền đó đang ở trạng thái rảnh (*idle*), thông thường DP sẽ tiến hành:

- Gửi bản tin thông báo dữ liệu đường xuống (Downlink Data Notification) kèm thông tin định danh đường truyền (Bearer Id), chất lượng đường truyền (Bearer QoS) tới cổng dịch vụ (Serving Gateway - SGW), thông báo có dữ liệu đường xuống giành cho UE, SGW gửi sang MME để khởi tạo thủ tục tìm gọi Paging tới các eNodeB thuộc vùng đeo bám (Tracking Area - TA) mà UE đã đăng ký. Sau khi nhận được bản tin Paging từ mạng truy nhập vô tuyến, UE khởi tạo thủ tục yêu cầu dịch vụ (Service Request), chuyển sang trạng thái kết nối (*connected*) và nhận gói tin từ mạng ngoài.

Tuy nhiên, trong giải pháp hữu ích này, DP thực thi:

- Khởi tạo ngưỡng cho phép số lượng bản tin thông báo dữ liệu đường xuống (Downlink Data Notification) cần tạo trong khoảng thời gian cho phép, khoảng thời gian này là cố định và đảm bảo chính xác cho việc theo dõi lưu lượng dữ liệu tới.
- Phát hiện ngưỡng và xử lý dữ liệu: nếu số lượng bản tin cần tạo chưa vượt ngưỡng, DP gửi bản tin thông báo dữ liệu đường xuống (Downlink Data Notification) tới SGW, ngược lại, thực thi chính sách lọc dữ liệu.
- Thực thi chính sách lọc dữ liệu: nếu chất lượng đường truyền có mức định danh loại chất lượng dịch vụ (QCI level) và mức ưu tiên cung cấp và duy trì dịch vụ (ARP priority level) không đạt ngưỡng cho trước, DP sẽ loại bỏ các gói dữ liệu nhận được, đồng thời không thực hiện gửi bản tin thông báo dữ liệu đường xuống (Downlink Data Notification) đến SGW. Ngược lại, DP gửi bản tin đó kèm với các thông tin định danh đường truyền (Bearer Id), chất lượng đường truyền tới SGW, SGW gửi tới MME để kích hoạt tìm kiếm UE.

- Tăng giá trị đếm và kết thúc chu kỳ giám sát: với mỗi bản tin thông báo dữ liệu đường xuống (Downlink Data Notification) được gửi, giá trị đếm được tăng thêm 1. Giá trị này được đặt lại bằng 0 mỗi khi kết thúc một chu kỳ giám sát.

Bằng việc phân tích thông tin bearer và loại bỏ các bản tin thông báo dữ liệu khi số lượng của chúng vượt ngưỡng an toàn trong thời gian cho phép, DP đã hạn chế việc MME kích hoạt thủ tục tìm gọi UE cũng như UE yêu cầu thiết lập kết nối dịch vụ với mạng LTE.

Mô tả vắn tắt các hình vẽ

Hình 1 mô tả cách truyền tải dữ liệu giữa UE với mạng dữ liệu ngoài thông qua đường truyền hệ thống gói dữ liệu phát triển.

Hình 2 mô tả chu trình giám sát thực thi chính sách.

Hình 3 biểu diễn trình tự các bước thực thi lọc gói lưu lượng trong một chu kỳ giám sát.

Hình 4 minh họa phương pháp thực hiện giải pháp hữu ích.

Mô tả chi tiết giải pháp hữu ích

Trong mạng di động LTE, EPC cung cấp dịch vụ kết nối giữa một UE và mạng dữ liệu gói bên ngoài, gọi là dịch vụ kết nối mạng dữ liệu gói (Packet Data Network Connectivity Service) (Hình 1). Dịch vụ kết nối này được cung cấp bởi đường truyền hệ thống gói dữ liệu phát triển (Evolved Packet System - EPS bearer). Một đường truyền thiết lập khi UE khởi tạo kết nối tới một mạng dữ liệu gói (Packet Data Network - PDN) và nó duy trì thiết lập trong suốt thời gian PDN cung cấp kết nối giữa UE và Internet gọi là đường truyền mặc định (*default bearer*). Những đường truyền bổ sung khác được thiết lập cho cùng dịch vụ PDN là đường truyền chuyên dụng (*dedicated bearer*). Mỗi đường truyền xác định các luồng dữ liệu mà nó đảm nhận để truyền tải gói dữ liệu giữa UE và mạng lõi với một QoS (*Quality of Service*) xác định. QoS bao gồm:

- Định danh loại chất lượng dịch vụ (QoS Class Identifier - QCI);
- Ưu tiên cung cấp và duy trì dịch vụ (Allocation and Retention Priority - ARP);
- Tốc độ bit tối đa (Maximum Bit Rate - MBR), trong đó: tốc độ bit này được cam kết;
- Tốc độ bit cam kết (Guaranteed Bit Rate - GBR), trong đó: tốc độ bit này được cam kết;
- Tốc độ bit tổng hợp tối đa của mạng truy cập (Access Point Name-Aggregated Maximum Bit Rate - AMBR), trong đó: tốc độ bit này không được cam kết;

- Tốc độ bit tổng hợp tối đa của người dùng (User Equipment-Aggregated Maximum Bit Rate), trong đó: tốc độ bit này không được cam kết.

Trong đó:

QCI là tham chiếu điều khiển chuyển tiếp gói (lập lịch tải trọng, quản lý ngưỡng hàng đợi, cấu hình giao thức lớp liên kết, ...) tại các node eNodeB, SGW, PGW. Các giá trị QCI được quy chuẩn hóa với từng loại dịch vụ khác nhau.

ARP quyết định khi nào một yêu cầu thiết lập kênh mang có thể được chấp nhận hoặc cần thiết để từ chối bởi vì giới hạn nguồn tài nguyên.

MBR chỉ ra băng thông tối đa được cho phép trên kênh mang.

GBR chỉ ra băng thông tối thiểu trên kênh mang.

APN-AMBR quy định trên PDN, xác định băng thông tối đa cho phép cho tất cả các kênh mang không cam kết băng thông tối thiểu được gán cho một PDN kết nối với UE.

UE-AMBR quy định trên UE, xác định băng thông tối đa được cho phép cho tất cả các kênh mang không cam kết băng thông tối thiểu được gán với một UE.

Việc giảm tải lưu lượng được thực hiện trong chu trình giám sát gồm ba bước (Hình 2): khởi tạo chu kỳ giám sát mới, giám sát và thực thi chính sách, kết thúc chu kỳ và chuyển sang chu kỳ mới. Các bước cụ thể như sau:

Bước 1: khởi tạo chu kỳ giám sát mới. Tại bước này tiến hành khởi tạo giá trị ngưỡng, khởi tạo biến đếm bản tin thông báo dữ liệu đường xuống và khởi tạo bộ đếm thời gian giám sát lưu lượng, cụ thể hơn:

Khởi tạo giá trị ngưỡng, bao gồm:

- Số yêu cầu được thực thi trên một đơn vị thời gian (DdnTpsThreshold): đây là số lượng bản tin thông báo dữ liệu đường xuống (Downlink Data Notification) được SGW gửi sang MME để thực hiện thủ tục tìm gọi UE. Các bản tin này được đếm trong đơn vị thời gian định kỳ DdnObserveInterval - mức thời gian này phải đủ lớn để giám sát được chính xác. Ví dụ: giá trị thời gian = 1000 ms. Khởi tạo giá trị này tùy thuộc vào khả năng đáp ứng của hệ thống EPC.

- Ngưỡng thực thi chính sách:

Giá trị định danh loại chất lượng dịch vụ (QciValueThreshold): chỉ cho phép gửi các gói dữ liệu với loại dịch vụ tương ứng tới UE. Thông thường chỉ cho phép

dịch vụ cơ bản như thoại đa phương tiện qua Internet (QCI = 1), gọi thoại (QCI = 2), loại bỏ các gói dữ liệu với QCI khác.

Mức ưu tiên cung cấp và duy trì dịch vụ (ARP Priority Level) (ArpLevelThreshold): SGW thực thi với những gói dữ liệu thuộc kênh mang có mức ưu tiên và cung cấp duy trì dịch vụ $\leq$ giá trị này, các gói dữ liệu khác bị loại bỏ. Ví dụ: ARP Priority Level = 1.

Thông thường, các giá trị ngưỡng này được khởi tạo một lần trong chu kỳ đầu tiên và cố định trong suốt thời gian hoạt động của hệ thống. Tuy nhiên, nó có thể được thay đổi để phù hợp với chính sách thực thi mà không cần dừng hệ thống.

- Khởi tạo biến đếm bản tin thông báo dữ liệu đường xuống (Downlink Data Notification) (DdnCounter): gán giá trị 0 cho biến đếm DdnCounter.
- Khởi tạo bộ đếm thời gian giám sát lưu lượng:

Một chu kỳ giám sát có thời gian DdnObserveInterval ms. Giá trị biến đếm DdnCounter tồn tại trong một chu kỳ. Hết thời gian này, chuyển sang chu kỳ giám sát tiếp theo. Bộ đếm thời gian là một tiến trình độc lập, việc khởi tạo bao gồm các tham số sau:

+ Thời gian bắt đầu giám sát lưu lượng (TimeStartObserve): gán giá trị thời gian hiện tại của hệ thống cho biến TimeStartObserved.

+ Thời gian hiện tại đang giám sát (TimeCurrentObserve): biến TimeCurrentObserve cho biết thời gian hiện tại của hệ thống. Cách lấy giá trị TimeStartObserve và TimeCurrentObserve được hỗ trợ bằng thư viện dựa vào nền tảng phần mềm sử dụng. Vòng lặp kiểm tra điều kiện $\text{TimeStartObserved} + \text{DdnObserveInterval} < \text{TimeCurrentObserve}$ được sử dụng, nếu điều kiện đúng, thoát vòng lặp và chuyển sang chu kỳ giám sát mới. Ngược lại, tiếp tục vòng lặp kiểm tra điều kiện.

Bước 2: giám sát và thực thi chính sách; đầu vào bước này là các ngưỡng và biến đếm bản tin được khởi tạo có ở đầu ra bước 1, bước này được thực hiện qua các bước nhỏ như sau:

B2.1 (bước 1 - Hình 3): trên máy chủ DP, khi nhận được gói dữ liệu từ mạng ngoài, DP kiểm tra địa chỉ IP đích của gói tin, nếu đây là địa chỉ của một UE đang thuộc quản lý của mạng LTE, chuyển xuống bước b2.2. Ngược lại chuyển tới bước b2.6.

B2.2 (bước 2 - Hình 3): dựa vào địa chỉ IP của UE, DP kiểm tra thông tin chất lượng đường truyền, cờ trạng thái hoạt động (Active Flag) của đường truyền sẽ vận chuyển các gói tin này cho UE. Các thông tin này được lưu trữ sau phiên làm việc trước

của UE. Nếu cờ trạng thái hoạt động (Active Flag) = rảnh (Idle), DP xác định UE đang trong trạng thái rảnh (Idle), chuyển xuống bước b2.3, ngược lại chuyển tới bước b2.5.

B2.3 (bước 3 - Hình 3): tăng biến đếm DdnCounter lên một đơn vị, kiểm tra giá trị DdnTpsThreshold. Nếu $DdnCounter \leq DdnTpsThreshold$, DP gửi bản tin thông báo dữ liệu đường xuống (Downlink Data Notification) đến SGW, ngược lại chuyển tới bước b2.4.

B2.4 (bước 4 - Hình 3): kiểm tra điều kiện QoS, nếu cả hai điều kiện QCI của đường truyền $\leq QciValueThreshold$ và mức ưu tiên cung cấp và duy trì dịch vụ $\leq ArpLevelThreshold$ được thỏa mãn, DP gửi bản tin thông báo dữ liệu đường xuống (Downlink Data Notification) đến SGW, SGW gửi đến MME, tiến hành thủ tục tìm gọi UE. Ngược lại, chuyển tới bước b2.6.

B2.5 (bước 5 - Hình 3): DP chuyển tiếp gói tin đến eNodeB, quay lại bước b2.1.

B2.6 (bước 6 - Hình 3): DP loại bỏ bản tin, quay lại bước b2.1.

Bước 3: kết thúc chu kỳ và chuyển sang chu kỳ tiếp theo.

Khi chuyển sang chu kỳ giám sát mới, biến đếm DdnCounter được đặt lại bằng 0, DP khởi tạo bộ đếm thời gian mới có thời gian DdnObserveInterval mili giây và tiếp tục thực thi chính sách lọc gói lưu lượng.

Ví dụ thực hiện giải pháp hữu ích

Phương pháp này được áp dụng trong thủ tục mạng Internet kích hoạt yêu cầu dịch vụ tới thuê bao người dùng - Network Trigger Service Request của phân hệ SGW trong hệ thống chuyển mạch gói 4G EPC do Tập đoàn Công nghiệp – Viễn thông Quân đội Viettel phát triển.

Hiệu quả đạt được của giải pháp hữu ích

Phương pháp đạt được những hiệu quả khi áp dụng trong thực tế:

- Đảm bảo khả năng xử lý cao tải, tính sẵn sàng của hệ thống khi bị tấn công dịch vụ.
- Đảm bảo độ mức độ ưu tiên dịch vụ của hệ thống, những dịch vụ có độ ưu tiên cao sẽ được ưu tiên xử lý trong trường hợp hệ thống bị tấn công.

Yêu cầu bảo hộ

1. Phương pháp bảo vệ tấn công DDoS đến hệ thống mạng 4G LTE dựa vào cơ chế phân loại chất lượng đường truyền bao gồm:

bước 1: khởi tạo chu kỳ giám sát mới; bước này có đầu vào là chương trình phần mềm được cài đặt để xử lý nghiệp vụ, nhiệm vụ của bước này là thiết lập các giá trị ngưỡng, biến đếm bản tin, bộ đếm thời gian cho việc giám sát lưu lượng; cụ thể, trong bước này cần khởi tạo các giá trị sau:

khởi tạo giá trị ngưỡng: khai báo và cấp phát ngưỡng dưới dạng hằng số với giá trị cố định, giá trị này phụ thuộc tùy vào yêu cầu của từng hệ thống, theo đánh giá thực tế khi áp dụng; giá trị ngưỡng là mức đánh giá trạng thái hoạt động của hệ thống là bình thường hay quá tải; ngưỡng bao gồm:

số bản tin thông báo dữ liệu đường xuống được thực thi trên một đơn vị thời gian $DdnTpsThreshold$; các bản tin đó được giám sát trong chu kỳ mili giây có thời gian $DdnObserveInterval$;

ngưỡng thực thi chính sách: cho phép các bản tin thuộc loại dịch vụ tối thiểu bằng $QciValueThreshold$ với kênh mang có mức ưu tiên và cung cấp dịch vụ $ArpPriority$ tối thiểu bằng $ArpLevelThreshold$ được đi qua DP;

khởi tạo biến đếm bản tin thông báo dữ liệu đường xuống: khai báo biến đếm $DdnCounter$, gán giá trị 0;

khởi tạo bộ đếm thời gian giám sát lưu lượng: một chu kỳ giám sát có thời gian $DdnObserveInterval$ ms; giá trị biến đếm $DdnCounter$ tồn tại trong một chu kỳ; hết thời gian này, chuyển sang chu kỳ giám sát tiếp theo; bộ đếm thời gian là một tiến trình độc lập, việc khởi tạo bao gồm:

thời gian bắt đầu giám sát lưu lượng $TimeStartObserve$: gán giá trị thời gian hiện tại của hệ thống cho biến $TimeStartObserved$;

thời gian hiện tại đang giám sát $TimeCurrentObserve$: biến $TimeCurrentObserve$ cho biết thời gian hiện tại của hệ thống; cách lấy giá trị $TimeStartObserve$ và $TimeCurrentObserve$ được hỗ trợ bằng thư viện dựa vào nền tảng phần mềm sử dụng; vòng lặp kiểm tra điều kiện $TimeStartObserved + DdnObserveInterval < TimeCurrentObserve$ được sử dụng, nếu điều kiện đúng, thoát vòng lặp và tiến trình chuyển sang chu kỳ giám sát mới; ngược lại, tiếp tục vòng lặp kiểm tra;

bước 2: giám sát và thực thi chính sách; đầu vào bước này là các ngưỡng và biến đếm bản tin được khởi tạo có ở đầu ra bước 1, bước này được thực hiện qua các bước nhỏ như sau:

b2.1: Trên node DP, khi nhận được gói dữ liệu từ mạng ngoài, DP kiểm tra địa chỉ IP đích của gói tin, nếu đây là địa chỉ của 1 UE đang thuộc quản lý của mạng LTE, chuyển xuống bước b2.2. Ngược lại chuyển tới bước b2.6;

b2.2: Dựa vào địa chỉ IP của UE, DP kiểm tra thông tin chất lượng đường truyền, cờ trạng thái hoạt động của đường truyền sẽ vận chuyển các gói tin này cho UE; các thông tin này được lưu trữ sau phiên làm việc trước của UE; nếu cờ trạng thái hoạt động = rảnh (idle), DP xác định UE đang trong trạng thái rảnh (idle), chuyển xuống bước b2.3, ngược lại chuyển tới bước b2.5;

b2.3: tăng biến đếm DdnCounter lên một đơn vị, kiểm tra giá trị DdnTpsThreshold; nếu $DdnCounter \leq DdnTpsThreshold$, DP gửi bản tin Downlink Data Notification đến SGW, ngược lại chuyển tới bước b2.4.

b2.4: kiểm tra điều kiện QoS, nếu cả hai điều kiện QCI của đường truyền $\leq QciValueThreshold$ và mức ưu tiên cung cấp và duy trì dịch vụ $\leq ArpLevelThreshold$ được thỏa mãn, DP gửi bản tin thông báo dữ liệu đường xuống đến SGW, SGW gửi đến MME, tiến hành thủ tục tìm gọi UE; ngược lại, chuyển tới bước b2.6;

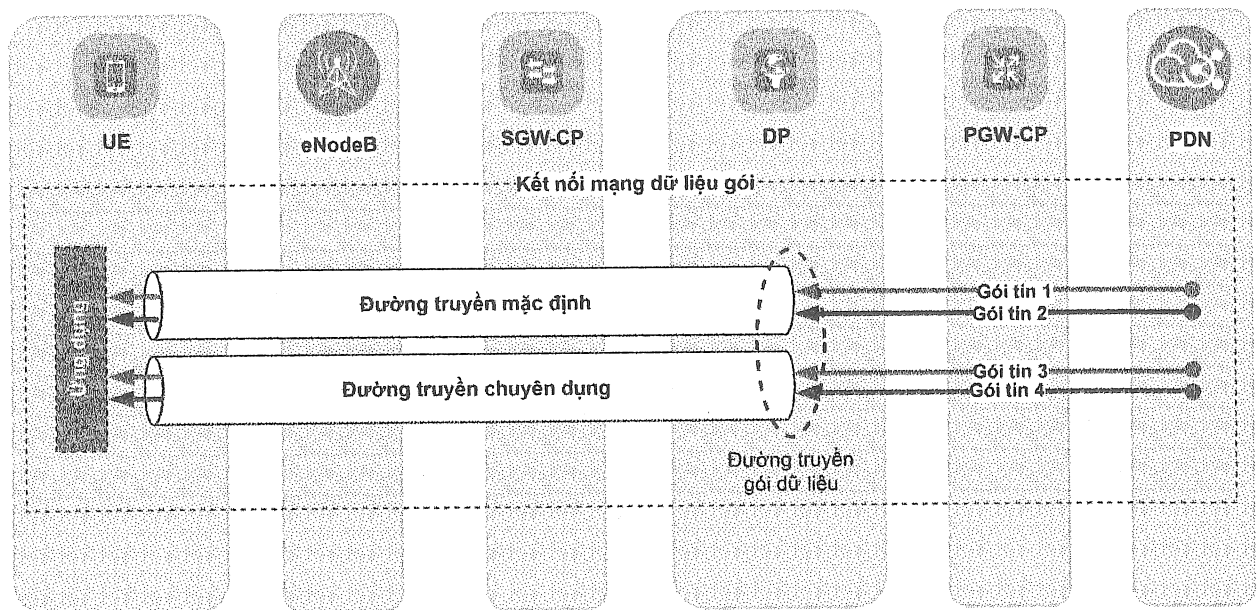
b2.5: DP chuyển tiếp gói tin đến eNodeB, quay lại bước b2.1.

b2.6: DP loại bỏ bản tin, quay lại bước b2.1.

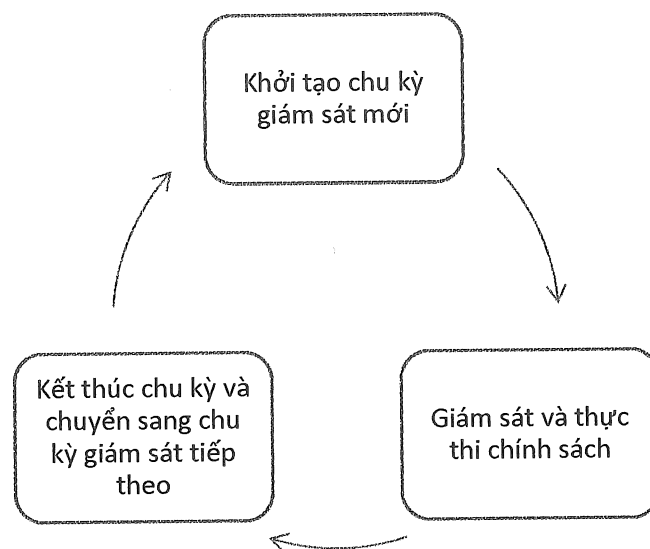
bước 3: kết thúc chu kỳ và chuyển sang chu kỳ tiếp theo; đầu vào là các ngưỡng, biến đếm bản tin, bộ đếm thời gian, thực hiện:

biến đếm DdnCounter được đặt lại bằng 0, DP khởi tạo bộ đếm thời gian mới có thời gian DdnObserveInterval ms và tiếp tục thực thi chính sách lọc gói lưu lượng;

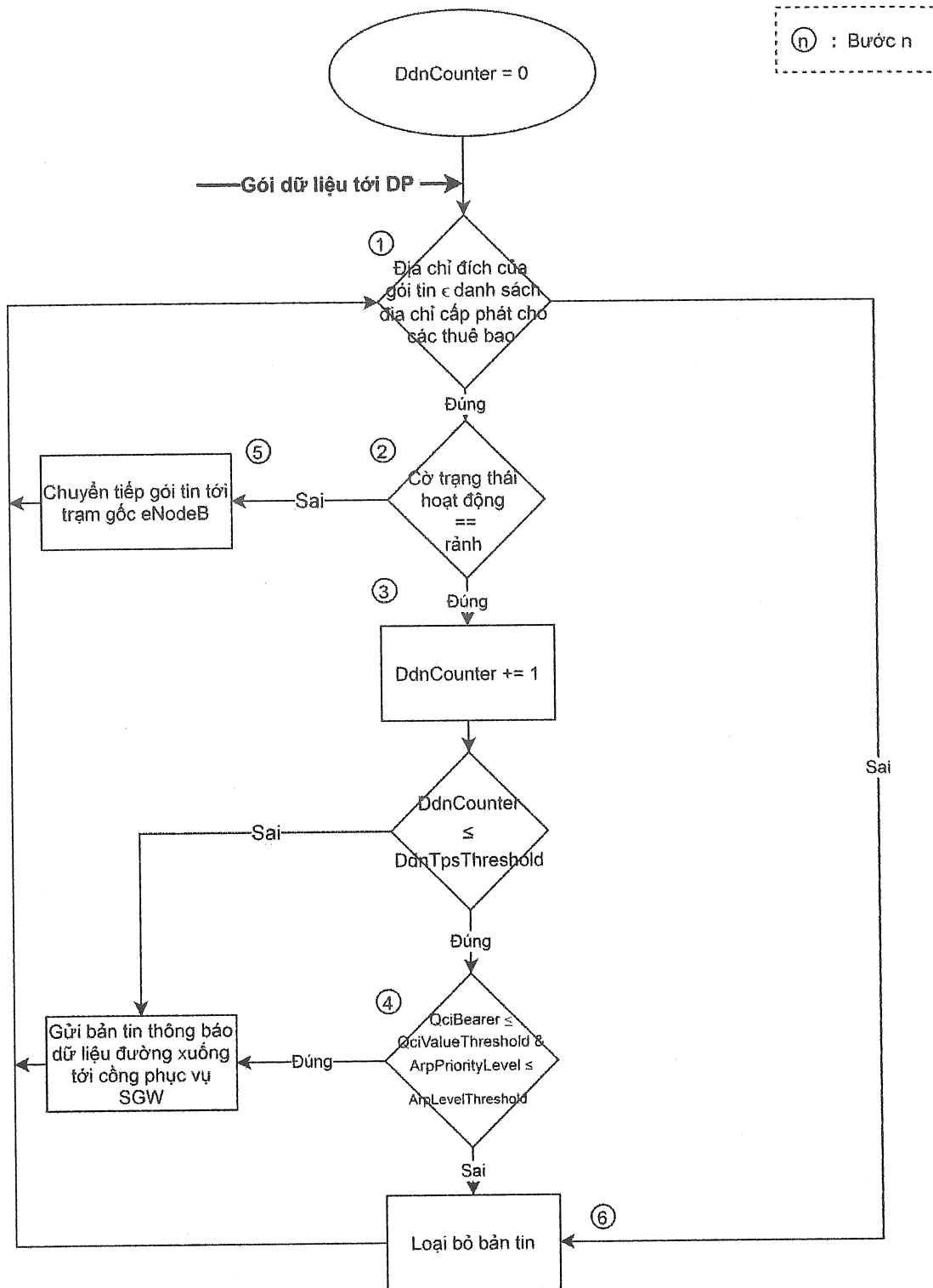
kết quả cuối cùng: DP kiểm soát được lưu lượng từ mạng internet bên ngoài và quyết định cho phép loại gói dịch vụ dữ liệu được đi tiếp vào hệ thống mạng của mình để bảo vệ các máy chủ trong hệ thống khỏi tình trạng quá tải.



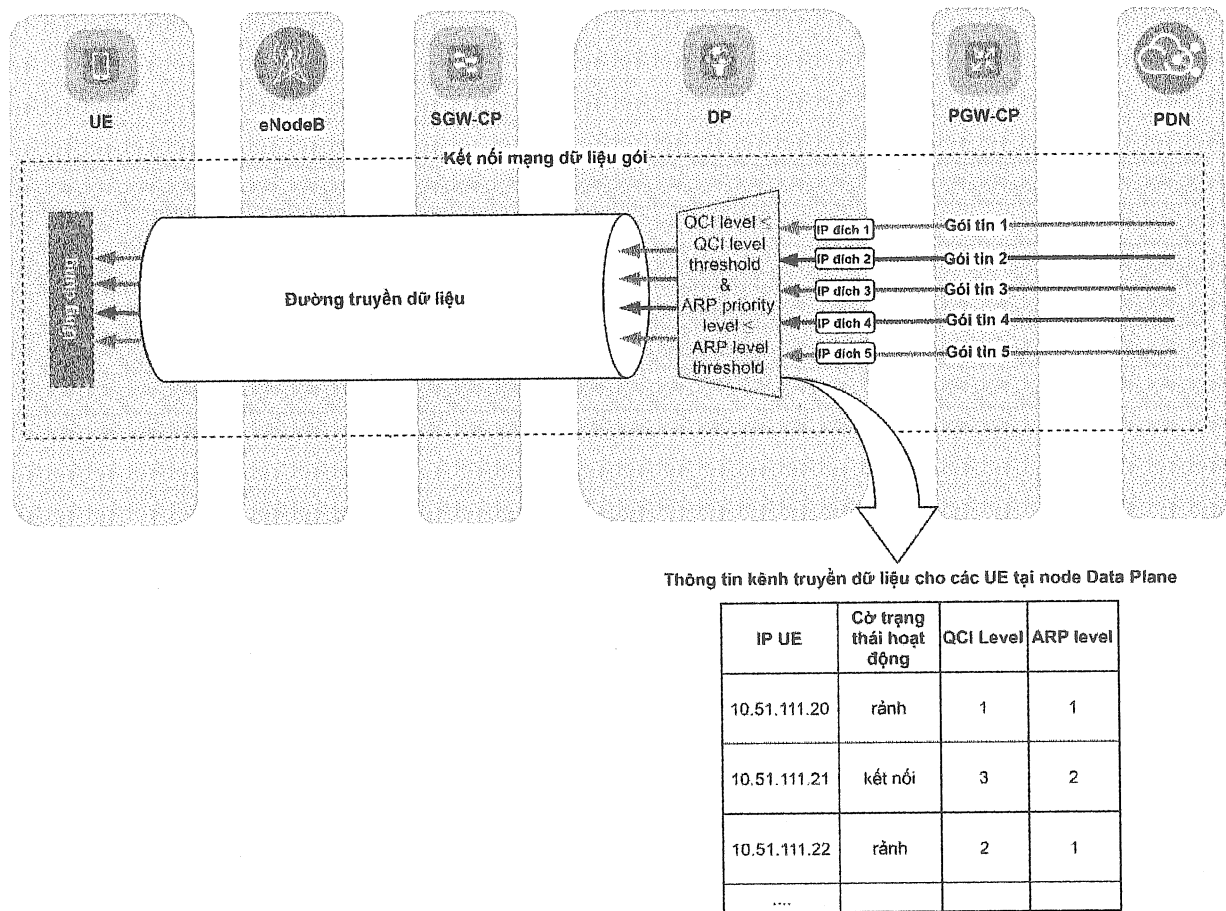
Hình 1



Hình 2



Hình 3



Hình 4