(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) **1-0051150**

(51)[2020.01] **H04W 24/00**

(13) **B**

(21) 1-2020-06177

(22) 08/04/2019

(86) PCT/CN2019/081696 08/04/2019

(87) WO2019/196773 17/10/2019

(30) 201810312936.6 09/04/2018 CN; 201810349848.3 18/04/2018 CN

(45) 25/09/2025 450

(43) 25/01/2021 394A

(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)
Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129, China

(72) ZHU, Fenqin (CN).

(74) Công ty Luật TNHH T&G (TGVN)

(54) HỆ THỐNG, THIẾT BỊ VÀ PHƯƠNG PHÁP GIÁM SÁT SỰ KIỆN, CHIP VÀ PHƯƠNG TIỆN LƯU TRỮ ĐỌC ĐƯỢC BẰNG MÁY TÍNH

(21) 1-2020-06177

(57) Sáng chế đề cập đến phương pháp và thiết bị giám sát sự kiện, và phương tiện lưu trữ đọc được bằng máy tính, sao cho chức năng lộ diện khả năng dịch vụ hoặc chức năng lộ diện mạng có thể xóa bỏ cấu hình sự kiện giám sát cho nhóm sau khi nhận các báo cáo sự kiện cho tất cả các thành viên trong nhóm, nhờ đó tránh được sự lãng phí tài nguyên và lỗi thực thi chính sách tiếp theo sau. Phương pháp bao gồm các bước: nhận, bởi thực thể chức năng lộ diện, thông điệp thứ nhất, trong đó thông điệp thứ nhất được sử dụng để tạo cấu hình sự kiện giám sát cho nhóm người dùng; thu được, bởi thực thể chức năng lộ diện, thông tin thành viên của nhóm người dùng; và xác định, bởi thực thể chức năng lộ diện dựa trên thông tin thành viên, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận, và xóa bỏ cấu hình sự kiện giám sát cho nhóm người dùng.

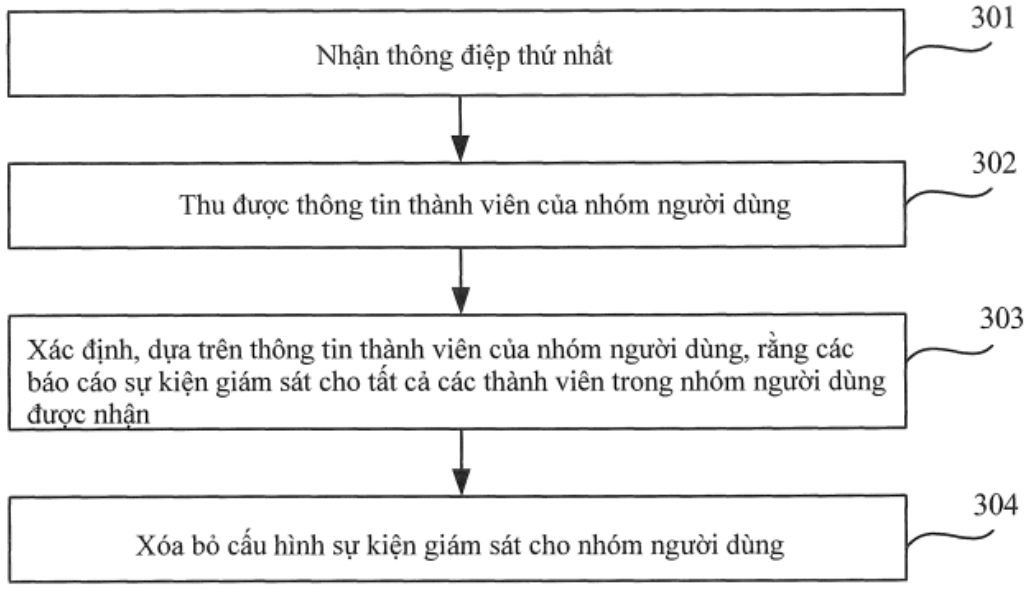

FIG. 3

Lĩnh vực kỹ thuật được đề cập

Các phương án thực hiện của sáng chế liên quan đến lĩnh vực công nghệ truyền thông, và cụ thể là, liên quan đến phương pháp và thiết bị giám sát sự kiện.

Tình trạng kỹ thuật của sáng chế

Cùng với sự phát triển của internet di động, người vận hành cần liên kết với nhà cung cấp ứng dụng bên thứ ba để đảm bảo dịch vụ được tạo ra bởi nhà cung cấp ứng dụng bên thứ ba. Trong hệ thống truyền thông phát triển dài hạn (Long Term Evolution, LTE), chức năng lộ diện khả năng dịch vụ (Service Capability Exposure Function, SCEF) có thể cho phép mạng dự án đối tác thế hệ thứ ba (3rd generation partnership project, 3GPP) cung cấp một cách an toàn khả năng dịch vụ cho nhà cung cấp dịch vụ bên thứ ba, sao cho các ứng dụng và các dịch vụ bên trong và bên ngoài có thể khả dụng và làm việc liên kết với nhau. Ứng dụng bên thứ ba thu được khả năng dịch vụ từ SCEF bằng cách sử dụng máy chủ khả năng dịch vụ (Services Capability Server, SCS)/máy chủ ứng dụng (Application Server - AS). Hệ thống truyền thông thế hệ thứ 5 (5th Generation, 5G) là kiến trúc dựa vào dịch vụ. Chức năng lộ diện mạng (Network Exposure Function - NEF) có chức năng tương tự với chức năng của SCEF, và NEF cung cấp, cho SCS/AS qua dịch vụ, dịch vụ và khả năng mà được hỗ trợ bởi mạng 3GPP. Trong kiến trúc lộ diện khả năng dịch vụ, cả hệ thống LTE và hệ thống 5G có thể hỗ trợ SCS/AS trong giám sát sự kiện cho người dùng, và có thể giám sát các sự kiện cho người dùng, như khả năng tiếp cận và ngắt kết nối thiết bị người dùng (User Equipment, UE).

Trong hệ thống LTE, qua cấu hình sự kiện giám sát, SCEF có thể nhận yêu cầu giám sát mà mang bộ nhận dạng nhóm bên ngoài, và bộ nhận dạng nhóm bên ngoài được sử dụng để xác định nhóm của các thành viên, và chỉ báo rằng sự kiện giám sát sẽ được thực hiện trên thành viên trong nhóm. Thực thể quản lý di động phần tử mạng mạng lõi (mobility management entity, MME)/nút hỗ trợ GPRS phục

vụ (serving GPRS support node, SGSN) gửi báo cáo sự kiện giám sát đến SCEF sau khi giám sát sự kiện cho mỗi thành viên trong nhóm. Trong hệ thống truyền thông 5G, NEF có thể nhận yêu cầu giám sát mà mang bộ nhận dạng nhóm bên ngoài, và chức năng quản lý truy cập và di động (Access and Mobility Management Function, AMF) gửi báo cáo sự kiện giám sát đến SCEF sau khi giám sát sự kiện cho mỗi thành viên trong nhóm.

Cả SCEF trong hệ thống LTE lẫn NEF trong hệ thống 5G đều không thể biết liệu các báo cáo sự kiện giám sát đã được yêu cầu có được hoàn thành cho tất cả các thành viên trong nhóm hay không. Nếu SCEF/NEF vẫn giữ cấu hình sự kiện giám sát cho nhóm sau khi các báo cáo sự kiện giám sát đã được yêu cầu được hoàn thành cho tất cả các thành viên trong nhóm, thì làm lãng phí các tài nguyên, và gây ra lỗi thực thi chính sách theo sau.

Bản chất kỹ thuật của sáng chế

Các phương án thực hiện của sáng chế đề xuất phương pháp và thiết bị giám sát sự kiện, sao cho chức năng lộ diện khả năng dịch vụ hoặc chức năng lộ diện mạng có thể xóa bỏ cấu hình sự kiện giám sát cho nhóm sau khi nhận các báo cáo sự kiện cho tất cả các thành viên trong nhóm, nhờ đó tránh được sự lãng phí tài nguyên và lỗi thực thi chính sách tiếp theo sau.

Các giải pháp kỹ thuật cụ thể được đề xuất ở các phương án thực hiện của sáng chế là như sau:

Theo khía cạnh thứ nhất, phương pháp giám sát sự kiện được đề xuất, trong đó phương pháp được thực hiện bởi thực thể chức năng lộ diện. Thủ tục cụ thể của phương pháp chủ yếu như sau: nhận thông điệp thứ nhất, trong đó thông điệp thứ nhất được sử dụng để tạo cấu hình sự kiện giám sát cho nhóm người dùng; thu được thông tin thành viên của nhóm người dùng; xác định, dựa trên thông tin thành viên, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận; và xóa bỏ cấu hình sự kiện giám sát cho nhóm người dùng. Theo cách này, thực thể chức năng lộ diện thu được thông tin thành viên của nhóm người dùng, sao cho khi nhận báo cáo sự kiện giám sát, thực thể chức năng lộ diện có thể xác

định, dựa trên thông tin thành viên của nhóm người dùng, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận, và có thể tiếp tục xóa bỏ cấu hình sự kiện giám sát cho nhóm người dùng, nhờ đó tránh được sự lãng phí tài nguyên và giúp đảm bảo sự thực thi đúng của chính sách tiếp theo sau.

Theo cách tùy chọn, thực thể chức năng lộ diện là thực thể chức năng lộ diện khả năng dịch vụ (Service Capability Exposure Function, SCEF), hoặc thực thể chức năng lộ diện là thực thể chức năng lộ diện mạng (Network Exposure Function - NEF). Theo cách này, phương pháp mà được đề xuất theo phương án thực hiện này của sáng chế có thể phù hợp với hệ thống LTE và hệ thống 5G.

Theo phương án có thể có, thông tin thành viên của nhóm người dùng có thể là số lượng của các thành viên có trong nhóm người dùng, và số lượng của các thành viên có thể được chỉ báo bởi N. Theo cách khác, thông tin thành viên của nhóm người dùng có thể là bộ nhận dạng của mỗi thành viên trong nhóm người dùng, nói cách khác, thông tin thành viên của nhóm người dùng là N bộ nhận dạng. Theo cách này, thực thể chức năng lộ diện có thể xác định, dựa trên số lượng của các thành viên có trong nhóm người dùng hoặc dựa trên bộ nhận dạng của thành viên, số lượng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng, để xác định liệu các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng có được nhận hay không.

Theo phương án có thể có, thông tin thành viên của nhóm người dùng có thể thu được theo hai cách dưới đây hoặc theo cách khác. Cách 1: Thông điệp thứ nhất mang thông tin thành viên của nhóm người dùng, và thông tin thành viên của nhóm người dùng được thu được từ thông điệp thứ nhất. Cách 2: Thông tin thành viên của nhóm người dùng mà được gửi bởi thực thể quản lý dữ liệu người dùng được nhận, nói cách khác, thông tin thành viên của nhóm người dùng được thu được từ thực thể quản lý dữ liệu người dùng. Theo cách này, thông tin thành viên của nhóm người dùng được mang trong báo hiệu đang tồn tại, nhờ đó làm giảm các phí tổn của việc bổ sung báo hiệu mới.

Theo phương án có thể có, thông điệp thứ nhất có thể còn mang số lượng tối đa của các báo cáo, và số lượng tối đa của các báo cáo được sử dụng để chỉ báo số lần báo cáo được phép tối đa của báo cáo sự kiện giám sát cho thành viên, hoặc số

lượng tối đa của các báo cáo được sử dụng để chỉ báo số lần báo cáo được phép tối đa của báo cáo sự kiện giám sát cho sự kiện giám sát của thành viên, hoặc số lượng tối đa của các báo cáo được sử dụng để chỉ báo tổng số lần báo cáo được phép tối đa của báo cáo sự kiện giám sát cho các sự kiện giám sát của thành viên. Số lượng tối đa của các báo cáo được thiết lập cho mỗi thành viên trong nhóm người dùng, và có thể áp dụng cho mỗi thành viên trong nhóm người dùng.

Theo cách tùy chọn, thông điệp thứ nhất có thể còn mang khoảng thời gian giám sát, và khoảng thời gian giám sát được sử dụng để chỉ báo thời gian tuyệt đối mà tại đó yêu cầu giám sát hết hạn. Khoảng thời gian giám sát được thiết lập cho mỗi thành viên trong nhóm người dùng, và có thể áp dụng cho mỗi thành viên trong nhóm người dùng.

Việc xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận có thể bao gồm các trường hợp sau đây:

Theo phương án có thể có, nếu thông điệp thứ nhất được sử dụng để tạo cấu hình yêu cầu giám sát một lần cho nhóm người dùng, thực thể chức năng lộ diện có thể xác định, khi nhận các báo cáo sự kiện giám sát cho N thành viên, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận.

Theo cách tùy chọn, nếu thông điệp thứ nhất không bao gồm cả số lượng tối đa của các báo cáo cũng như khoảng thời gian, thực thể chức năng lộ diện xác định rằng thông điệp thứ nhất được sử dụng để tạo cấu hình yêu cầu giám sát một lần cho nhóm người dùng; hoặc nếu thông điệp thứ nhất bao gồm số lượng tối đa thứ nhất của các báo cáo và số lượng tối đa thứ nhất của các báo cáo bằng 1, thì thực thể chức năng lộ diện xác định rằng thông điệp thứ nhất được sử dụng để tạo cấu hình yêu cầu giám sát một lần cho nhóm người dùng.

Theo phương án có thể có, nếu thông điệp thứ nhất được sử dụng để tạo cấu hình các sự kiện giám sát cho nhóm người dùng, thực thể chức năng lộ diện xác định, khi nhận báo cáo sự kiện giám sát của mỗi sự kiện trong số các sự kiện giám sát cho mỗi thành viên trong số N thành viên, rằng các báo cáo sự kiện giám sát cho tất cả các người dùng trong nhóm thành viên được nhận.

Theo phương án có thể có, nếu thông điệp thứ nhất bao gồm số lượng tối đa thứ hai của các báo cáo, thực thể chức năng lộ diện xác định, khi số lần nhận báo cáo

sự kiện giám sát cho mỗi thành viên trong số N thành viên đạt tới số lượng tối đa thứ hai của các báo cáo, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm thành viên được nhận.

Theo cách tùy chọn, nếu thông điệp thứ nhất được sử dụng để tạo cấu hình các sự kiện giám sát cho nhóm người dùng, thực thể chức năng lộ diện xác định, khi số lần nhận báo cáo sự kiện giám sát của mỗi sự kiện trong số các sự kiện giám sát cho mỗi thành viên trong số N thành viên đạt đến số lượng tối đa thứ hai của các báo cáo, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận.

Theo một số phương pháp nêu trên, có thể xác định được rằng các báo cáo sự kiện giám sát cho các thành viên trong nhóm người dùng được nhận, để tiếp tục khởi tạo việc xóa bỏ cấu hình sự kiện giám sát cho nhóm người dùng.

Theo phương án có thể có, nếu thông tin thành viên của nhóm người dùng bao gồm N bộ nhận dạng, thực thể chức năng lộ diện xác định, mỗi lần báo cáo sự kiện giám sát được nhận, cho dù báo cáo sự kiện giám sát là báo cáo sự kiện giám sát cho thành viên, để thu được kết quả xác định. Kết quả xác định được sử dụng để xác định liệu các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng có được nhận hay không. Theo cách này, hoạt động này có thể giúp đảm bảo độ chính xác của bước xác định liệu các báo cáo sự kiện giám sát của các thành viên trong nhóm người dùng có được nhận hay không.

Theo phương án có thể có, việc xóa bỏ, bởi thực thể chức năng lộ diện, cấu hình sự kiện giám sát cho nhóm người dùng bao gồm ít nhất một trong số các hoạt động sau đây: xóa bỏ, bởi thực thể chức năng lộ diện, cấu hình sự kiện giám sát được lưu trữ cục bộ cho nhóm người dùng; gửi, bởi thực thể chức năng lộ diện, thông điệp thứ hai đến thực thể quản lý dữ liệu người dùng, trong đó thông điệp thứ hai được sử dụng để ra lệnh cho thực thể quản lý dữ liệu người dùng xóa cấu hình sự kiện giám sát cho nhóm người dùng; và gửi, bởi thực thể chức năng lộ diện, thông điệp thứ ba đến thực thể ứng dụng bên thứ ba, trong đó thông điệp thứ ba được sử dụng để ra lệnh cho thực thể ứng dụng bên thứ ba xóa cấu hình sự kiện giám sát cho nhóm người dùng. Theo cách tùy chọn, thực thể quản lý dữ liệu người dùng là thực thể máy chủ thuê bao gia đình HSS hoặc thực thể quản lý dữ liệu thống nhất UDM.

Theo khía cạnh thứ hai, phương pháp giám sát sự kiện được đề xuất, trong đó phương pháp được thực hiện bởi thực thể chức năng lộ diện. Thủ tục cụ thể của phương pháp chủ yếu như sau: nhận thông điệp thứ nhất, trong đó thông điệp thứ nhất được sử dụng để tạo cấu hình sự kiện giám sát cho nhóm người dùng; thu được thông tin thành viên của nhóm người dùng; và xác định, dựa trên thông tin thành viên, liệu các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng có được hoàn thành hay không. Theo cách tùy chọn, khi các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được hoàn thành, cấu hình sự kiện giám sát cho nhóm người dùng được xóa bỏ, hoặc hoạt động gửi báo cáo sự kiện giám sát đến ứng dụng bên thứ ba được dừng lại. Theo cách này, thực thể chức năng lộ diện thu được thông tin thành viên của nhóm người dùng, sao cho khi nhận báo cáo sự kiện giám sát, thực thể chức năng lộ diện có thể xác định, dựa trên thông tin thành viên của nhóm người dùng, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận, và có thể tiếp tục xóa bỏ cấu hình sự kiện giám sát cho nhóm người dùng hoặc dừng hoạt động gửi báo cáo sự kiện giám sát đến ứng dụng bên thứ ba, nhờ đó tránh được sự lãng phí tài nguyên và giúp đảm bảo sự thực thi đúng của chính sách tiếp theo sau.

Theo cách tùy chọn, thực thể chức năng lộ diện là thực thể chức năng lộ diện khả năng dịch vụ (Service Capability Exposure Function, SCEF), hoặc thực thể chức năng lộ diện là thực thể chức năng lộ diện mạng (Network Exposure Function - NEF). Theo cách này, phương pháp mà được đề xuất theo phương án thực hiện này của sáng chế có thể phù hợp với hệ thống LTE và hệ thống 5G.

Theo phương án có thể có, thông tin thành viên của nhóm người dùng có thể là số lượng của các thành viên có trong nhóm người dùng, và số lượng của các thành viên có thể được chỉ báo bởi N. Theo cách khác, thông tin thành viên của nhóm người dùng có thể là bộ nhận dạng của mỗi thành viên trong nhóm người dùng, nói cách khác, thông tin thành viên của nhóm người dùng là N bộ nhận dạng. Theo cách này, thực thể chức năng lộ diện có thể xác định, dựa trên số lượng của các thành viên có trong nhóm người dùng hoặc dựa trên bộ nhận dạng của thành viên, số lượng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng, để xác định liệu các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng

có được nhận hay không.

Theo phương án có thể có, thông tin thành viên của nhóm người dùng có thể thu được theo hai cách dưới đây hoặc theo cách khác. Cách 1: Thông điệp thứ nhất mang thông tin thành viên của nhóm người dùng, và thông tin thành viên của nhóm người dùng được thu được từ thông điệp thứ nhất. Cách 2: Thông tin thành viên của nhóm người dùng mà được gửi bởi thực thể quản lý dữ liệu người dùng được nhận, nói cách khác, thông tin thành viên của nhóm người dùng được thu được từ thực thể quản lý dữ liệu người dùng. Theo cách này, thông tin thành viên của nhóm người dùng được mang trong báo hiệu đang tồn tại, nhờ đó làm giảm các phí tổn của việc bổ sung báo hiệu mới.

Theo phương án có thể có, thông điệp thứ nhất có thể còn mang số lượng tối đa của các báo cáo, và số lượng tối đa của các báo cáo được sử dụng để chỉ báo số lần báo cáo được phép tối đa của báo cáo sự kiện giám sát cho thành viên, hoặc số lượng tối đa của các báo cáo được sử dụng để chỉ báo số lần báo cáo được phép tối đa của báo cáo sự kiện giám sát cho sự kiện giám sát của thành viên, hoặc số lượng tối đa của các báo cáo được sử dụng để chỉ báo tổng số lần báo cáo được phép tối đa của báo cáo sự kiện giám sát cho các sự kiện giám sát của thành viên. Số lượng tối đa của các báo cáo được thiết lập cho mỗi thành viên trong nhóm người dùng, và có thể áp dụng cho mỗi thành viên trong nhóm người dùng.

Theo cách tùy chọn, thông điệp thứ nhất có thể còn mang khoảng thời gian giám sát, và khoảng thời gian giám sát được sử dụng để chỉ báo thời gian tuyệt đối mà tại đó yêu cầu giám sát hết hạn. Khoảng thời gian giám sát được thiết lập cho mỗi thành viên trong nhóm người dùng, và có thể áp dụng cho mỗi thành viên trong nhóm người dùng.

Việc xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được hoàn thành có thể bao gồm các trường hợp sau đây:

Theo phương án có thể có, nếu thông điệp thứ nhất được sử dụng để tạo cấu hình yêu cầu giám sát một lần cho nhóm người dùng, thực thể chức năng lộ diện có thể xác định, khi nhận các báo cáo sự kiện giám sát cho N thành viên, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được hoàn thành.

Theo cách tùy chọn, nếu thông điệp thứ nhất không bao gồm cả số lượng tối đa của các báo cáo cũng như khoảng thời gian, thực thể chức năng lộ diện xác định rằng thông điệp thứ nhất được sử dụng để tạo cấu hình yêu cầu giám sát một lần cho nhóm người dùng; hoặc nếu thông điệp thứ nhất bao gồm số lượng tối đa thứ nhất của các báo cáo và số lượng tối đa thứ nhất của các báo cáo bằng 1, thì thực thể chức năng lộ diện xác định rằng thông điệp thứ nhất được sử dụng để tạo cấu hình yêu cầu giám sát một lần cho nhóm người dùng.

Theo phương án có thể có, nếu nếu thông điệp thứ nhất được sử dụng để tạo cấu hình yêu cầu giám sát một lần cho nhóm người dùng, và thông điệp thứ nhất được sử dụng để tạo cấu hình các sự kiện giám sát cho nhóm người dùng, thực thể chức năng lộ diện xác định, khi nhận báo cáo sự kiện giám sát của mỗi sự kiện trong số các sự kiện giám sát cho mỗi thành viên trong số N thành viên, rằng các báo cáo sự kiện giám sát cho tất cả các người dùng trong nhóm thành viên được hoàn thành.

Theo phương án có thể có, nếu thông điệp thứ nhất bao gồm số lượng tối đa thứ hai của các báo cáo, thực thể chức năng lộ diện xác định, khi số lần nhận báo cáo sự kiện giám sát cho mỗi thành viên trong số N thành viên đạt tới số lượng tối đa thứ hai của các báo cáo, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm thành viên được nhận.

Theo phương án có thể có, nếu thông điệp thứ nhất bao gồm số lượng tối đa thứ hai của các báo cáo, và thông điệp thứ nhất được sử dụng để tạo cấu hình các sự kiện giám sát cho nhóm người dùng, thực thể chức năng lộ diện xác định, khi số lần nhận báo cáo sự kiện giám sát của mỗi sự kiện trong số các sự kiện giám sát cho mỗi thành viên trong số N thành viên đạt đến số lượng tối đa thứ hai của các báo cáo, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được hoàn thành.

Theo một số phương pháp nêu trên, có thể xác định được rằng các báo cáo sự kiện giám sát của các thành viên trong nhóm người dùng được hoàn thành, để tiếp tục khởi tạo việc xóa bỏ cấu hình sự kiện giám sát cho nhóm người dùng hoặc dừng hoạt động gửi báo cáo sự kiện giám sát đến ứng dụng bên thứ ba.

Theo phương án có thể có, nếu thông tin thành viên của nhóm người dùng bao gồm N bộ nhận dạng, thực thể chức năng lộ diện xác định, mỗi lần báo cáo sự kiện

giám sát được nhận, cho dù báo cáo sự kiện giám sát là báo cáo sự kiện giám sát cho thành viên, để thu được kết quả xác định. Kết quả xác định được sử dụng để xác định liệu các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng có được hoàn thành hay không. Theo cách này, hoạt động này có thể giúp đảm bảo độ chính xác của bước xác định liệu các báo cáo sự kiện giám sát của các thành viên trong nhóm người dùng có được hoàn thành hay không.

Theo phương án có thể có, việc xóa bỏ, bởi thực thể chức năng lộ diện, cấu hình sự kiện giám sát cho nhóm người dùng bao gồm ít nhất một trong số các hoạt động sau đây: xóa bỏ, bởi thực thể chức năng lộ diện, cấu hình sự kiện giám sát được lưu trữ cục bộ cho nhóm người dùng; và gửi, bởi thực thể chức năng lộ diện, thông điệp thứ hai đến thực thể ứng dụng bên thứ ba, trong đó thông điệp thứ hai được sử dụng để ra lệnh cho thực thể ứng dụng bên thứ ba xóa cấu hình sự kiện giám sát cho nhóm người dùng.

Theo phương án có thể có, việc xóa bỏ, bởi thực thể chức năng lộ diện, cấu hình sự kiện giám sát cho nhóm người dùng bao gồm: gửi, bởi thực thể chức năng lộ diện, thông điệp thứ ba đến thực thể quản lý dữ liệu người dùng, trong đó thông điệp thứ ba được sử dụng để ra lệnh cho thực thể quản lý dữ liệu người dùng xóa cấu hình sự kiện giám sát cho nhóm người dùng; hoặc gửi, bởi thực thể chức năng lộ diện, thông điệp thứ tư đến thực thể quản lý dữ liệu người dùng, trong đó thông điệp thứ tư được sử dụng để ra lệnh cho thực thể quản lý dữ liệu người dùng xóa cấu hình sự kiện giám sát cho một hoặc nhiều thành viên trong nhóm người dùng.

Theo phương án có thể có, nếu thực thể chức năng lộ diện xác định rằng các báo cáo sự kiện giám sát cho một hoặc nhiều bộ phận được hoàn thành, thực thể chức năng lộ diện gửi thông điệp thứ tư đến thực thể quản lý dữ liệu người dùng.

Theo cách tùy chọn, thực thể quản lý dữ liệu người dùng là thực thể máy chủ thuê bao gia đình HSS hoặc thực thể quản lý dữ liệu thống nhất UDM.

Ở các phần mô tả nêu trên, khi các báo cáo sự kiện giám sát của các thành viên trong nhóm người dùng được hoàn thành, báo cáo sự kiện giám sát cho nhóm người dùng được hoàn thành, và khi xác định được rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được hoàn thành, xác định được rằng báo cáo sự kiện giám sát cho nhóm người dùng được hoàn thành.

Theo khía cạnh thứ ba, thiết bị giám sát sự kiện được đề xuất, trong đó thiết bị có chức năng thực hiện khía cạnh bất kỳ trong số khía cạnh thứ nhất, khía cạnh thứ hai, các phương án có thể có của khía cạnh thứ nhất, hoặc các phương án có thể có của khía cạnh thứ hai. Chức năng này có thể được thực thi bởi phần cứng, hoặc có thể được thực thi bởi phần cứng bằng cách chạy phần mềm tương ứng. Phần cứng hoặc phần mềm này bao gồm một hoặc nhiều môđun tương ứng với chức năng này.

Theo phương án có thể có, thiết bị có thể là chip hoặc mạch tích hợp.

Theo phương án có thể có, thiết bị bao gồm bộ thu phát và bộ xử lý, bộ thu phát được sử dụng bởi thiết bị để truyền thông với thực thể chức năng khác hoặc phần tử mạng, và bộ xử lý được tạo cấu hình để thực hiện nhóm các chương trình. Khi các chương trình được thực thi, thiết bị có thể thực hiện phương pháp theo khía cạnh bất kỳ trong số khía cạnh thứ nhất hoặc các phương án có thể có của khía cạnh thứ nhất.

Theo phương án có thể có, thiết bị còn bao gồm bộ nhớ, và bộ nhớ lưu trữ các chương trình được thực hiện bởi bộ xử lý.

Theo phương án có thể có, thiết bị là thực thể chức năng lộ diện khả năng dịch vụ (Service Capability Exposure Function, SCEF) hoặc thực thể chức năng lộ diện mạng (Network Exposure Function - NEF).

Theo khía cạnh thứ tư, chip được đề xuất, trong đó chip được kết nối với bộ nhớ hoặc chip bao gồm bộ nhớ, và được tạo cấu hình để đọc và thực thi chương trình phần mềm được lưu trữ trong bộ nhớ, để thực hiện phương pháp theo khía cạnh bất kỳ trong số khía cạnh thứ nhất, khía cạnh thứ hai, các phương án có thể có của khía cạnh thứ nhất, hoặc các phương án có thể có của khía cạnh thứ hai.

Theo khía cạnh thứ năm, phương pháp giám sát sự kiện được đề xuất, trong đó phương pháp được thực hiện bởi thực thể quản lý dữ liệu người dùng. Phương pháp bao gồm các bước cụ thể như sau: nhận thông điệp yêu cầu thứ nhất, trong đó thông điệp yêu cầu thứ nhất được sử dụng để tạo cấu hình sự kiện giám sát cho nhóm người dùng; và gửi thông điệp hồi đáp thứ nhất đến thực thể chức năng lộ diện, trong đó thông điệp hồi đáp thứ nhất mang thông tin thành viên của nhóm người dùng. Theo cách này, thông tin thành viên của nhóm người dùng được gửi đến thực thể chức năng lộ diện, sao cho khi nhận báo cáo sự kiện giám sát, thực thể chức năng lộ

diện có thể xác định, dựa trên thông tin thành viên của nhóm người dùng, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận, và có thể tiếp tục xóa bỏ cấu hình sự kiện giám sát cho nhóm người dùng hoặc dừng hoạt động gửi báo cáo sự kiện giám sát đến ứng dụng bên thứ ba, nhờ đó tránh được sự lãng phí tài nguyên và giúp đảm bảo sự thực thi đúng của chính sách tiếp theo sau.

Theo phương án có thể có, thông tin thành viên của nhóm người dùng có thể là số lượng của các thành viên có trong nhóm người dùng, và số lượng của các thành viên có thể được chỉ báo bởi N. Theo cách khác, thông tin thành viên của nhóm người dùng có thể là bộ nhận dạng của mỗi thành viên trong nhóm người dùng, nói cách khác, thông tin thành viên của nhóm người dùng là N bộ nhận dạng. Theo cách này, thực thể chức năng lộ diện có thể xác định, dựa trên số lượng của các thành viên có trong nhóm người dùng hoặc dựa trên bộ nhận dạng của thành viên, số lượng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng, để xác định liệu các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng có được nhận hay không.

Theo phương án có thể có, thực thể quản lý dữ liệu người dùng nhận thông điệp yêu cầu thứ hai được gửi bởi thực thể chức năng lộ diện, trong đó thông điệp yêu cầu thứ hai mang thông tin dùng để ra lệnh xóa cấu hình sự kiện giám sát cho nhóm người dùng, và thực thể quản lý dữ liệu người dùng xóa cấu hình sự kiện giám sát cho nhóm người dùng dựa trên thông điệp yêu cầu thứ hai.

Theo phương án có thể có, thực thể quản lý dữ liệu người dùng nhận thông điệp yêu cầu thứ tư được gửi bởi thực thể chức năng lộ diện, trong đó thông điệp yêu cầu thứ tư mang thông tin dùng để ra lệnh cho thực thể quản lý dữ liệu người dùng xóa cấu hình sự kiện giám sát cho một hoặc nhiều thành viên trong nhóm người dùng, và thực thể quản lý dữ liệu người dùng xóa cấu hình sự kiện giám sát cho một hoặc nhiều thành viên trong nhóm người dùng dựa trên thông điệp yêu cầu thứ tư.

Theo cách tùy chọn, thực thể quản lý dữ liệu người dùng là thực thể máy chủ thuê bao gia đình HSS hoặc thực thể quản lý dữ liệu thống nhất UDM.

Theo khía cạnh thứ sáu, thiết bị giám sát sự kiện được đề xuất, trong đó thiết bị có chức năng thực hiện khía cạnh bất kỳ trong số khía cạnh thứ ba hoặc các

phương án có thể có của khía cạnh thứ ba. Chức năng này có thể được thực thi bởi phần cứng, hoặc có thể được thực thi bởi phần cứng bằng cách chạy phần mềm tương ứng. Phần cứng hoặc phần mềm này bao gồm một hoặc nhiều môđun tương ứng với chức năng này.

Theo phương án có thể có, thiết bị có thể là chip hoặc mạch tích hợp.

Theo phương án có thể có, thiết bị bao gồm bộ thu phát và bộ xử lý, bộ thu phát được sử dụng bởi thiết bị để truyền thông với thực thể chức năng khác hoặc phần tử mạng, và bộ xử lý được tạo cấu hình để thực hiện nhóm các chương trình. Khi các chương trình được thực thi, thiết bị có thể thực hiện phương pháp theo khía cạnh bất kỳ trong số khía cạnh thứ hai hoặc các phương án có thể có của khía cạnh thứ hai.

Theo phương án có thể có, thiết bị còn bao gồm bộ nhớ, và bộ nhớ lưu trữ các chương trình được thực hiện bởi bộ xử lý.

Theo phương án có thể có, thiết bị là thực thể HSS hoặc thực thể UDM.

Theo khía cạnh thứ bảy, chip được đề xuất, trong đó chip được kết nối với bộ nhớ hoặc chip bao gồm bộ nhớ, và được tạo cấu hình để đọc và thực thi chương trình phần mềm được lưu trữ trong bộ nhớ, để thực hiện phương pháp theo khía cạnh bất kỳ trong số khía cạnh thứ ba hoặc các phương án có thể có của khía cạnh thứ ba.

Theo khía cạnh thứ tám, phương pháp giám sát sự kiện được đề xuất, trong đó phương pháp được thực hiện bởi thực thể ứng dụng bên thứ ba. Phương pháp bao gồm các bước cụ thể như sau: gửi thông điệp thứ nhất đến thực thể chức năng lộ diện, trong đó thông điệp thứ nhất được sử dụng để tạo cấu hình sự kiện giám sát cho nhóm người dùng, và thông điệp thứ nhất mang thông tin thành viên của nhóm người dùng. Theo cách này, thông tin thành viên của nhóm người dùng được gửi đến thực thể chức năng lộ diện, sao cho khi nhận báo cáo sự kiện giám sát, thực thể chức năng lộ diện có thể xác định, dựa trên thông tin thành viên của nhóm người dùng, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận, và có thể tiếp tục xóa bỏ cấu hình sự kiện giám sát cho nhóm người dùng, nhờ đó tránh được sự lãng phí tài nguyên và giúp đảm bảo sự thực thi đúng của chính sách tiếp theo sau.

Theo phương án có thể có, thông tin thành viên của nhóm người dùng có thể

là số lượng của các thành viên có trong nhóm người dùng, và số lượng của các thành viên có thể được chỉ báo bởi N. Theo cách khác, thông tin thành viên của nhóm người dùng có thể là bộ nhận dạng của mỗi thành viên trong nhóm người dùng, nói cách khác, thông tin thành viên của nhóm người dùng là N bộ nhận dạng. Theo cách này, thực thể chức năng lộ diện có thể xác định, dựa trên số lượng của các thành viên có trong nhóm người dùng hoặc dựa trên bộ nhận dạng của thành viên, số lượng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng, để xác định liệu các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng có được nhận hay không.

Theo phương án có thể có, thông điệp thứ ba được gửi bởi thực thể chức năng lộ diện được nhận, trong đó thông điệp thứ ba mang thông tin dùng để ra lệnh xóa cấu hình sự kiện giám sát cho nhóm người dùng, và thực thể ứng dụng bên thứ ba xóa cấu hình sự kiện giám sát cho nhóm người dùng dựa trên thông điệp thứ ba.

Theo cách tùy chọn, thực thể ứng dụng bên thứ ba là thực thể SCS hoặc thực thể AS.

Theo khía cạnh thứ chín, thiết bị giám sát sự kiện được đề xuất, trong đó thiết bị có chức năng thực hiện khía cạnh bất kỳ trong số khía cạnh thứ tư hoặc các phương án có thể có của khía cạnh thứ tư. Chức năng này có thể được thực thi bởi phần cứng, hoặc có thể được thực thi bởi phần cứng bằng cách chạy phần mềm tương ứng. Phần cứng hoặc phần mềm này bao gồm một hoặc nhiều môđun tương ứng với chức năng này.

Theo phương án có thể có, thiết bị có thể là chip hoặc mạch tích hợp.

Theo phương án có thể có, thiết bị bao gồm bộ thu phát và bộ xử lý, bộ thu phát được sử dụng bởi thiết bị để truyền thông với thực thể chức năng khác hoặc phần tử mạng, và bộ xử lý được tạo cấu hình để thực hiện nhóm các chương trình. Khi các chương trình được thực thi, thiết bị có thể thực hiện phương pháp theo khía cạnh bất kỳ trong số khía cạnh thứ tư hoặc các phương án có thể có của khía cạnh thứ tư.

Theo phương án có thể có, thiết bị còn bao gồm bộ nhớ, và bộ nhớ lưu trữ các chương trình được thực hiện bởi bộ xử lý.

Theo phương án có thể có, thiết bị là thực thể SCS hoặc thực thể AS.

Theo khía cạnh thứ mười, chip được đề xuất, trong đó chip được kết nối với bộ nhớ hoặc chip bao gồm bộ nhớ, và được tạo cấu hình để đọc và thực thi chương trình phần mềm được lưu trữ trong bộ nhớ, để thực hiện phương pháp theo khía cạnh bất kỳ trong số khía cạnh thứ tư hoặc các phương án có thể có của khía cạnh thứ tư.

Theo khía cạnh thứ mười một, phương tiện lưu trữ máy tính được đề xuất, trong đó phương tiện lưu trữ máy tính lưu trữ chương trình máy tính, và chương trình máy tính chứa lệnh được sử dụng để thực hiện phương pháp theo khía cạnh bất kỳ trong số các khía cạnh nêu trên hoặc các phương án có thể có của các khía cạnh nêu trên.

Theo khía cạnh thứ mười hai, sản phẩm chương trình máy tính chứa lệnh được đề xuất, trong đó khi sản phẩm chương trình máy tính chạy trên máy tính, máy tính được phép thực hiện phương pháp theo khía cạnh bất kỳ trong số các khía cạnh nêu trên hoặc các phương án có thể có của các khía cạnh nêu trên.

Mô tả vắn tắt các hình vẽ

Fig.1 là hình vẽ thể hiện kiến trúc lộ diện khả năng dịch vụ trong hệ thống LTE theo một phương án thực hiện của sáng chế;

Fig.2 là hình vẽ thể hiện kiến trúc lộ diện khả năng dịch vụ trong hệ thống 5G theo một phương án thực hiện của sáng chế;

Fig.3 là lưu đồ dạng sơ lược của phương pháp giám sát sự kiện theo một phương án thực hiện của sáng chế;

Fig.4 là lưu đồ dạng sơ lược 1 thể hiện hoạt động giám sát sự kiện trong trường hợp ứng dụng 1 theo một phương án thực hiện của sáng chế;

Fig.5 là lưu đồ dạng sơ lược 2 thể hiện hoạt động giám sát sự kiện trong trường hợp ứng dụng 1 theo một phương án thực hiện của sáng chế;

Fig.6A và Fig.6B là lưu đồ dạng sơ lược 1 thể hiện hoạt động giám sát sự kiện trong trường hợp ứng dụng 2 theo một phương án thực hiện của sáng chế;

Fig.7 là lưu đồ dạng sơ lược 2 thể hiện hoạt động giám sát sự kiện trong trường hợp ứng dụng 2 theo một phương án thực hiện của sáng chế;

Fig.8 là hình vẽ kết cấu dạng sơ lược của thiết bị giám sát sự kiện theo một

phương án thực hiện của sáng chế;

Fig.9 là hình vẽ kết cấu dạng sơ lược 2 của thiết bị giám sát sự kiện theo một phương án thực hiện của sáng chế.

Mô tả chi tiết sáng chế

Các phương án thực hiện của sáng chế đề xuất phương pháp và thiết bị giám sát sự kiện, sao cho trong hoạt động giám sát sự kiện dựa trên nhóm, khi nhận các báo cáo sự kiện cho tất cả các thành viên trong nhóm, SCEF trong hệ thống LTE hoặc NEF trong hệ thống 5G có thể xóa bỏ cấu hình sự kiện giám sát cho nhóm theo cách kịp thời, nhờ đó tiết kiệm các tài nguyên và giúp đảm bảo sự thực thi đúng của chính sách tiếp theo sau.

Kiến trúc hệ thống truyền thông mà phương pháp được đề xuất theo các phương án thực hiện của sáng chế có thể được áp dụng vào đó được mô tả dưới đây.

Fig.1 là hình vẽ thể hiện kiến trúc lộ diện khả năng dịch vụ (service capability exposure, SCE) trong hệ thống LTE, bao gồm SCEF 101, SCS/AS 102, máy chủ thuê bao gia đình (home subscriber server, HSS) 103, MME 104, và SGSN 105. Trong hệ thống LTE, SCEF 101 là phần tử mạng lõi trong kiến trúc lộ diện khả năng dịch vụ, và SCEF 101 được tạo cấu hình để đảm bảo rằng mạng cung cấp một cách an toàn khả năng dịch vụ cho nhà cung cấp dịch vụ bên thứ ba, sao cho các ứng dụng và các dịch vụ bên trong và bên ngoài có thể có sẵn và liên kết với nhau. Ứng dụng bên thứ ba thu được khả năng dịch vụ từ SCEF 101 bằng cách sử dụng SCS/AS 102. HSS 103 là máy chủ thuê bao người dùng gia đình, và được tạo cấu hình để lưu trữ thông tin thuê bao của người dùng. Các phần tử mạng quản lý khả năng di động bao gồm MME 104 và SGSN 105, và được tạo cấu hình để thực hiện quản lý khả năng di động trên đầu cuối. SCS/AS 102 gọi, bằng cách sử dụng giao diện T8 API, khả năng dịch vụ được cung cấp bởi SCEF 101.

Fig.2 là hình vẽ thể hiện kiến trúc SCE trong hệ thống 5G, bao gồm NEF 201, SCS/AS 202, UDM 203, và AMF 204. Trong hệ thống 5G, chức năng của NEF 201 tương tự với chức năng của SCEF 101 trong hệ thống LTE. NEF 201 mở, đến SCS/AS 202 qua dịch vụ Nnef, dịch vụ và khả năng mà được hỗ trợ bởi mạng 3GPP.

Chức năng của UDM 203 tương tự với chức năng của HSS 103 trong hệ thống LTE. UDM 203 cung cấp khả năng dịch vụ được hỗ trợ cho NEF 201 qua dịch vụ Nudm. Phần tử mạng quản lý khả năng di động bao gồm AMF 204. Chức năng của AMF 204 tương tự với chức năng của MME 104 trong hệ thống LTE. AMF 204 cung cấp dịch vụ được hỗ trợ và khả năng được hỗ trợ cho NEF 201 qua dịch vụ Namf.

Cần lưu ý rằng các kiến trúc hệ thống truyền thông được đề xuất trên Fig.1 và Fig.2 là các ví dụ. Phương pháp được đề xuất theo các phương án thực hiện của sáng chế không bị giới hạn ở hai hệ thống truyền thông, và có thể còn được áp dụng cho nhiều hệ thống truyền thông.

Một số các thuật ngữ theo các phương án thực hiện của sáng chế được giải thích và được mô tả dưới đây, để tạo điều kiện thuận lợi cho người có hiểu biết trung bình trong lĩnh vực tương ứng hiểu được sáng chế.

(1) Sự kiện giám sát

Theo các phương án thực hiện của sáng chế, dựa trên kiến trúc lộ diện khả năng dịch vụ được thể hiện trên Fig.1 hoặc Fig.2, SCS/AS có thể giám sát một hoặc nhiều sự kiện cho người dùng. Sự kiện có thể là, ví dụ, khả năng tiếp cận UE, mất kết nối, hoặc định vị.

(2) Nhóm người dùng

Nhóm người dùng còn được gọi là nhóm. Một nhóm người dùng bao gồm một hoặc nhiều thành viên, và thành viên là người dùng. Nói theo cách khác, một nhóm người dùng bao gồm một hoặc nhiều người dùng. Theo các phương án thực hiện của sáng chế, cấu hình sự kiện giám sát có thể dựa trên nhóm, và tất cả các thành viên trong nhóm có bộ nhận dạng nhóm bên ngoài giống nhau.

(3) Thông tin thành viên của nhóm người dùng

Thông tin thành viên của nhóm người dùng là thông tin liên quan đến thành viên có trong nhóm người dùng. Ví dụ, thông tin thành viên có thể là số lượng của các thành viên có trong nhóm người dùng, và số lượng của các thành viên theo sáng chế được biểu thị bởi N, trong đó N là số nguyên dương. Theo cách khác, thông tin thành viên có thể là bộ nhận dạng của mỗi thành viên có trong nhóm người dùng, và các bộ nhận dạng được sử dụng để phân biệt giữa các thành viên khác nhau, và cũng có thể được gọi là các bộ nhận dạng thành viên hoặc các bộ nhận dạng người dùng.

Bộ nhận dạng nhóm bên ngoài của thành viên trong nhóm được sử dụng để phân biệt giữa các nhóm người dùng khác nhau, và các bộ nhận dạng thành viên hoặc các bộ nhận dạng người dùng được sử dụng để phân biệt giữa các người dùng (hoặc thành viên) khác nhau.

(4) Thực thể chức năng lộ diện

Thực thể chức năng lộ diện là thực thể mà có thể thực hiện chức năng lộ diện dịch vụ, và là thực thể mà chức năng của nó giống hoặc tương tự với chức năng của SCEF 101 hoặc NEF 201. Thực thể chức năng lộ diện có thể là SCEF 101, hoặc có thể là NEF 201.

(5) Thực thể ứng dụng bên thứ ba

Thực thể ứng dụng bên thứ ba là thực thể mà chức năng của nó giống hoặc tương tự với chức năng của SCS/AS 102 hoặc SCS/AS 202. Thực thể ứng dụng bên thứ ba có thể là SCS/AS 102, hoặc có thể là SCS/AS 202.

(6) Phần tử mạng quản lý khả năng di động

Phần tử mạng quản lý khả năng di động là thực thể mà chức năng của nó là giống với hoặc tương tự với chức năng của MME 104 và SGSN 105, hoặc của AMF 204. Phần tử mạng quản lý khả năng di động có thể là MME 104 và SGSN 105, hoặc có thể là AMF 204.

(7) Thực thể quản lý dữ liệu người dùng

Thực thể quản lý dữ liệu người dùng là thực thể mà chức năng của nó giống hoặc tương tự với chức năng của HSS 103 hoặc UDM 203. Thực thể quản lý dữ liệu người dùng có thể là HSS 103, hoặc có thể là UDM 203.

(8) Báo cáo sự kiện giám sát

Báo cáo sự kiện giám sát là nội dung mà có liên quan đến sự kiện giám sát của thành viên trong nhóm người dùng và được báo cáo bởi phần tử mạng quản lý khả năng di động. Báo cáo sự kiện giám sát có thể mang nội dung liên quan đến một hoặc nhiều sự kiện giám sát. Thực thể chức năng lộ diện phân biệt giữa các báo cáo sự kiện giám sát của các sự kiện giám sát khác nhau bằng cách sử dụng các bộ nhận dạng của các sự kiện giám sát, và phân biệt giữa các báo cáo sự kiện giám sát của các thành viên khác nhau bằng cách sử dụng các bộ nhận dạng của các thành viên.

(9) Thuật ngữ "và/hoặc" mô tả quan hệ kết hợp để mô tả các đối tượng kết hợp và thể hiện rằng ba quan hệ có thể tồn tại. Ví dụ, A và/hoặc B có thể thể hiện ba trường hợp sau đây: Chỉ có A tồn tại, cả A và B đều tồn tại, và chỉ có B tồn tại. "Các" được nói đến theo sáng chế có nghĩa là "hai hoặc nhiều hơn hai". Các thuật ngữ như "thứ nhất" và "thứ hai" chỉ dùng cho sự phân biệt và phần mô tả, và sẽ không được hiểu là chỉ định hoặc ngụ ý của tầm quan trọng tương đối hoặc chỉ định hoặc ngụ ý của thứ tự. Ký tự "/" nói chung là thể hiện mối quan hệ "hoặc" giữa các đối tượng liên quan.

Phương pháp giám sát sự kiện được đề xuất theo phương án thực hiện của sáng chế được mô tả chi tiết dưới đây tham chiếu đến các hình vẽ kèm theo.

Như được thể hiện trên Fig.3, thủ tục cụ thể của phương pháp giám sát sự kiện được đề xuất theo phương án thực hiện của sáng chế là như sau. Phương pháp được thực hiện bởi thực thể chức năng lộ diện.

S301. Nhận thông điệp thứ nhất.

Thông điệp thứ nhất có thể là yêu cầu giám sát. Thông điệp thứ nhất được sử dụng để tạo cấu hình sự kiện giám sát cho nhóm người dùng, nói cách khác, thông điệp thứ nhất được sử dụng để tạo cấu hình yêu cầu giám sát cho nhóm người dùng. Nhóm người dùng bao gồm một hoặc nhiều thành viên, và sự kiện giám sát hoặc yêu cầu giám sát cho nhóm người dùng là sự kiện giám sát hoặc yêu cầu giám sát cho mỗi thành viên trong nhóm người dùng. Thông điệp thứ nhất được sử dụng để tạo cấu hình một hoặc nhiều sự kiện giám sát cho nhóm người dùng. Một hoặc nhiều sự kiện giám sát là cho mỗi thành viên trong nhóm người dùng. Thông điệp thứ nhất có thể mang bộ nhận dạng nhóm bên ngoài (external group ID) của nhóm người dùng. Bộ nhận dạng nhóm bên ngoài cũng là cho mỗi thành viên trong nhóm người dùng, và được sử dụng để phân biệt giữa các nhóm người dùng khác nhau. Yêu cầu giám sát cũng có thể được gọi là đăng ký sự kiện, và thông điệp thứ nhất được sử dụng để đăng ký với sự kiện giám sát cho nhóm người dùng.

Thông điệp thứ nhất có thể còn mang số lượng tối đa của các báo cáo, và số lượng tối đa của các báo cáo được sử dụng để chỉ báo số lần báo cáo tối đa của việc báo cáo sự kiện giám sát cho thành viên, hoặc số lượng tối đa của các báo cáo được sử dụng để chỉ báo số lần báo cáo tối đa của việc báo cáo sự kiện giám sát cho sự

kiện giám sát của thành viên, hoặc số lượng tối đa của các báo cáo được sử dụng để chỉ báo tổng số lần báo cáo tối đa của các báo cáo sự kiện giám sát cho các sự kiện giám sát của thành viên. Số lượng tối đa của các báo cáo được thiết lập cho mỗi thành viên trong nhóm người dùng, và có thể áp dụng cho mỗi thành viên trong nhóm người dùng. Số lượng tối đa của các báo cáo là số nguyên dương.

Thông điệp thứ nhất có thể còn mang khoảng thời gian giám sát, và khoảng thời gian giám sát được sử dụng để chỉ báo thời gian tuyệt đối mà ở đó yêu cầu giám sát hết hạn. Khoảng thời gian giám sát được thiết lập cho mỗi thành viên trong nhóm người dùng, và có thể áp dụng cho mỗi thành viên trong nhóm người dùng.

Trong ứng dụng thực tế, thông điệp thứ nhất có thể được sử dụng để tạo cấu hình yêu cầu giám sát một lần cho nhóm người dùng. Yêu cầu giám sát một lần có nghĩa là báo cáo sự kiện giám sát cần được báo cáo cho mỗi thành viên trong nhóm người dùng chỉ một lần. Nếu có một sự kiện giám sát, báo cáo sự kiện giám sát được báo cáo cho sự kiện giám sát một lần. Nếu có nhiều sự kiện giám sát, báo cáo sự kiện giám sát được báo cáo một lần cho sự kiện bất kỳ trong số các sự kiện giám sát trong yêu cầu giám sát hoặc báo cáo sự kiện giám sát được báo cáo một lần cho mỗi sự kiện trong số các sự kiện giám sát trong yêu cầu giám sát.

Cụ thể là, thông điệp thứ nhất được sử dụng để tạo cấu hình yêu cầu giám sát một lần cho nhóm người dùng, và có một số trường hợp sau đây: (1) Thông điệp thứ nhất bao gồm số lượng tối đa của các báo cáo, và số lượng tối đa của các báo cáo bằng 1. (2) Thông điệp thứ nhất không bao gồm cả số lượng tối đa của các báo cáo và khoảng thời gian giám sát.

S302. Thu được thông tin thành viên của nhóm người dùng.

Thông tin thành viên của nhóm người dùng có thể thu được theo hai cách dưới đây hoặc theo cách khác. Cách 1: Thông điệp thứ nhất mang thông tin thành viên của nhóm người dùng, và thông tin thành viên của nhóm người dùng được thu được từ thông điệp thứ nhất. Cách 2: Thông tin thành viên của nhóm người dùng mà được gửi bởi thực thể quản lý dữ liệu người dùng được nhận, nói cách khác, thông tin thành viên của nhóm người dùng được thu được từ thực thể quản lý dữ liệu người dùng. Thực thể quản lý dữ liệu người dùng ở đây có thể là thực thể HSS hoặc thực thể UDM.

S303. Xác định, dựa trên thông tin thành viên của nhóm người dùng, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận.

Cụ thể là, thực thể chức năng lộ diện nhận báo cáo sự kiện giám sát một hoặc nhiều lần, và mỗi lần thực thể chức năng lộ diện nhận báo cáo sự kiện giám sát, thực thể chức năng lộ diện lưu trữ cục bộ báo cáo sự kiện giám sát đã nhận, và xác định, dựa trên báo cáo sự kiện đã nhận và thông tin thành viên của nhóm người dùng, liệu các báo cáo sự kiện giám sát cho tất cả các thành viên có được nhận không (nói cách khác, xác định liệu các báo cáo sự kiện giám sát cho tất cả các thành viên có được hoàn thành không). Mỗi lần phần tử mạng quản lý khả năng di động báo cáo về một báo cáo sự kiện giám sát, phần tử mạng quản lý khả năng di động còn báo cáo bộ nhận dạng yêu cầu giám sát (bộ nhận dạng tham chiếu SCEF hoặc bộ nhận dạng thông báo sự kiện NEF), bộ nhận dạng sự kiện giám sát, và bộ nhận dạng thành viên, và bộ nhận dạng yêu cầu giám sát, bộ nhận dạng sự kiện giám sát, và bộ nhận dạng thành viên được mang trong báo cáo sự kiện giám sát hoặc được mang trong loại thông điệp cụ thể cùng với báo cáo sự kiện giám sát, ví dụ, thông điệp hồi đáp giám sát. Thực thể chức năng lộ diện xác định nhóm người dùng mà báo cáo sự kiện giám sát thuộc về nó, sự kiện giám sát, và thành viên dựa trên bộ nhận dạng yêu cầu giám sát, bộ nhận dạng sự kiện giám sát, và bộ nhận dạng thành viên.

Thông tin thành viên của nhóm người dùng có thể là số lượng của các thành viên có trong nhóm người dùng, và số lượng của các thành viên có thể được chỉ báo bởi N. Theo cách khác, thông tin thành viên của nhóm người dùng có thể là bộ nhận dạng của mỗi thành viên trong nhóm người dùng, nói cách khác, thông tin thành viên của nhóm người dùng là N bộ nhận dạng. Mỗi lần báo cáo sự kiện giám sát được nhận, thực thể chức năng lộ diện có thể xác định nhóm người dùng mà báo cáo sự kiện giám sát thuộc về nó, sự kiện giám sát, và thành viên mà báo cáo sự kiện giám sát thuộc về nó. Dựa trên điều này, thực thể chức năng lộ diện xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận, và có thể có một số trường hợp sau đây.

Trường hợp 1

Thông điệp thứ nhất được sử dụng để tạo cấu hình yêu cầu giám sát một lần

cho nhóm người dùng. Trong trường hợp này, báo cáo sự kiện giám sát cần được nhận cho một sự kiện giám sát của thành viên chỉ một lần.

Nếu thông điệp thứ nhất bao gồm một sự kiện giám sát, nói cách khác, thông điệp thứ nhất được sử dụng để tạo cấu hình một sự kiện giám sát cho nhóm người dùng, có các tình huống sau đây:

Xét rằng thông tin thành viên của nhóm người dùng là số lượng N của các thành viên trong nhóm người dùng, thực thể chức năng lộ diện có thể xác định, khi nhận N báo cáo sự kiện giám sát, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận, trong đó N báo cáo sự kiện giám sát thuộc về các thành viên khác nhau, nói cách khác, N báo cáo sự kiện giám sát là các báo cáo sự kiện giám sát cho N thành viên khác nhau. Do thực thể chức năng lộ diện có thể xác định thành viên mà báo cáo sự kiện giám sát thuộc về nó, thực thể chức năng lộ diện có thể xác định số lượng của các thành viên khác nhau mà các báo cáo sự kiện giám sát được nhận cho chúng.

Xét rằng thông tin thành viên của nhóm người dùng là N bộ nhận dạng, thực thể chức năng lộ diện so sánh bộ nhận dạng của thành viên được liên kết với báo cáo sự kiện giám sát đã nhận với N bộ nhận dạng. Nếu các báo cáo sự kiện giám sát của các thành viên của N bộ nhận dạng được nhận, thực thể chức năng lộ diện có thể xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận (nói cách khác, xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được hoàn thành).

Nếu thông điệp thứ nhất bao gồm nhiều sự kiện giám sát, nói cách khác, thông điệp thứ nhất được sử dụng để tạo cấu hình nhiều sự kiện giám sát cho nhóm người dùng, ví dụ, M sự kiện giám sát, có các tình huống sau đây:

Xét rằng thông tin thành viên của nhóm người dùng là số lượng N của các thành viên trong nhóm người dùng, thực thể chức năng lộ diện cũng có thể xác định, khi nhận N báo cáo sự kiện giám sát, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận. Nếu thông điệp thứ nhất bao gồm nhiều sự kiện giám sát, nói cách khác, thông điệp thứ nhất được sử dụng để tạo cấu hình nhiều sự kiện giám sát cho nhóm người dùng, ví dụ, M sự kiện giám sát, khi nhận báo cáo sự kiện giám sát cho mỗi thành viên trong số N thành viên, hoặc nhận

báo cáo sự kiện giám sát cho mỗi một trong số M sự kiện giám sát của mỗi thành viên trong số N thành viên, thực thể chức năng lộ diện xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận (nói cách khác, xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được hoàn thành).

Xét rằng thông tin thành viên của nhóm người dùng là N bộ nhận dạng, thực thể chức năng lộ diện cũng có thể xác định, khi nhận các báo cáo sự kiện giám sát cho các thành viên của N bộ nhận dạng, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận. Theo cách thay thế, thực thể chức năng lộ diện so sánh bộ nhận dạng của thành viên được liên kết với báo cáo sự kiện giám sát đã nhận với N bộ nhận dạng, và so sánh bộ nhận dạng của sự kiện giám sát được liên kết với báo cáo sự kiện giám sát đã nhận với các bộ nhận dạng của M sự kiện giám sát, và nếu báo cáo sự kiện giám sát cho mỗi một trong số M sự kiện giám sát cho mỗi thành viên trong số các thành viên của N bộ nhận dạng được nhận, thực thể chức năng lộ diện xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận (nói cách khác, xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được hoàn thành).

Trường hợp 2

Thông điệp thứ nhất mang số lượng tối đa của các báo cáo, và số lượng tối đa của các báo cáo lớn hơn 1. Trong trường hợp này, chỉ khi các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng mỗi đạt tới số lượng tối đa của các báo cáo, có thể xác định được rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận (nói cách khác, xác định được rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được hoàn thành).

Thực thể chức năng lộ diện xác định, dựa trên số lượng N của các thành viên trong nhóm người dùng hoặc N bộ nhận dạng, số lượng của các thành viên khác nhau mà các báo cáo sự kiện giám sát được nhận cho chúng, và khi số lần nhận báo cáo sự kiện giám sát cho mỗi thành viên trong số N thành viên đạt tới số lượng tối đa của các báo cáo, xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm thành viên được nhận. Nếu thông điệp thứ nhất bao gồm nhiều sự kiện

giám sát, nói cách khác, thông điệp thứ nhất được sử dụng để tạo cấu hình nhiều sự kiện giám sát cho nhóm người dùng, ví dụ, M sự kiện giám sát, khi số lần nhận báo cáo sự kiện cho mỗi thành viên trong số N thành viên đạt tới số lượng tối đa của các báo cáo, hoặc số lần nhận báo cáo sự kiện giám sát cho mỗi một trong số M sự kiện giám sát cho mỗi thành viên trong số N thành viên đạt tới số lượng tối đa của các báo cáo, thực thể chức năng lộ diện xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận (nói cách khác, xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được hoàn thành).

S304. Xóa bỏ cấu hình sự kiện giám sát cho nhóm người dùng.

Cụ thể là, thực thể chức năng lộ diện xóa một cách cục bộ cấu hình sự kiện giám sát cho nhóm người dùng. Theo cách tùy chọn, thực thể chức năng lộ diện có thể còn gửi thông điệp đến thực thể ứng dụng bên thứ ba, để ra lệnh cho thực thể ứng dụng bên thứ ba xóa cấu hình sự kiện giám sát cho nhóm người dùng. Theo cách tùy chọn, thực thể chức năng lộ diện có thể còn gửi thông điệp đến thực thể quản lý dữ liệu người dùng, để ra lệnh cho thực thể quản lý dữ liệu người dùng xóa cấu hình sự kiện giám sát cho nhóm người dùng hoặc để ra lệnh cho thực thể quản lý dữ liệu người dùng xóa cấu hình sự kiện giám sát cho một hoặc nhiều thành viên trong nhóm người dùng.

Theo phương án thực hiện có thể, nếu thông tin thành viên của nhóm người dùng là N bộ nhận dạng, mỗi lần báo cáo sự kiện giám sát được nhận, thực thể chức năng lộ diện có thể còn xác định liệu báo cáo sự kiện giám sát đã nhận có là báo cáo sự kiện giám sát cho thành viên trong nhóm người dùng hay không. Cụ thể là, thực thể chức năng lộ diện xác định liệu bộ nhận dạng của thành viên được liên kết với báo cáo sự kiện giám sát đã nhận có nằm trong N bộ nhận dạng hay không. Nếu có, thực thể chức năng lộ diện xác định rằng báo cáo sự kiện giám sát đã nhận là báo cáo sự kiện giám sát cho thành viên trong nhóm người dùng; hoặc ngược lại, thực thể chức năng lộ diện xác định rằng báo cáo sự kiện giám sát đã nhận không là báo cáo sự kiện giám sát cho thành viên trong nhóm người dùng. Kết quả xác định được sử dụng để tiếp tục xác định liệu các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng có được nhận không (nói cách khác, xác định rằng các báo

cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng có được hoàn thành không).

Tóm lại, theo phương pháp giám sát sự kiện mà được đề xuất theo phương án thực hiện này của sáng chế, thực thể chức năng lộ diện thu được thông tin thành viên của nhóm người dùng, sao cho khi nhận báo cáo sự kiện giám sát, thực thể chức năng lộ diện có thể xác định, dựa trên thông tin thành viên của nhóm người dùng, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận, và có thể tiếp tục xóa bỏ cấu hình sự kiện giám sát cho nhóm người dùng hoặc dừng hoạt động gửi báo cáo sự kiện giám sát đến ứng dụng bên thứ ba, nhờ đó tránh được sự lãng phí tài nguyên và giúp đảm bảo sự thực thi đúng của chính sách tiếp theo sau.

Phương pháp giám sát sự kiện theo sáng chế còn được mô tả một cách chi tiết tham chiếu đến các trường hợp ứng dụng cụ thể dựa trên phương pháp được đề xuất theo phương án nêu trên.

Trường hợp ứng dụng 1: hệ thống LTE. Thực thể chức năng lộ diện là SCEF, thực thể ứng dụng bên thứ ba là SCS/AS, các phần tử mạng quản lý khả năng di động là MME và SGSN, và thực thể quản lý dữ liệu người dùng là HSS.

Như được thể hiện trên Fig.4, thủ tục của hoạt động giám sát sự kiện trong trường hợp ứng dụng 1 được mô tả cụ thể như sau:

S401. SCS/AS gửi, đến SCEF, thông điệp yêu cầu giám sát thứ nhất được cấu hình dựa trên nhóm người dùng, và SCEF nhận thông điệp yêu cầu giám sát thứ nhất được gửi bởi SCS/AS.

Thông điệp yêu cầu giám sát thứ nhất là thông điệp thứ nhất trong phương án nêu trên, và có thuộc tính và chức năng của thông điệp thứ nhất.

Thông điệp yêu cầu giám sát thứ nhất mang thông tin thành viên của nhóm người dùng, và có thể còn mang, nhưng không bị giới hạn ở, ít nhất một trong số các thông tin sau đây: bộ nhận dạng SCS/AS, địa chỉ đích T8, loại giám sát, bộ nhận dạng nhóm bên ngoài, bộ nhận dạng tham chiếu giao dịch dài hạn T8 (T8 Long Term Transaction Reference ID, TLTRI), số lượng tối đa của các báo cáo, và/hoặc khoảng thời gian giám sát. Số lượng tối đa của các báo cáo và/hoặc khoảng thời gian giám sát được áp dụng cho mỗi thành viên trong nhóm người dùng. Nếu thông điệp yêu

cầu giám sát thứ nhất không mang cả số lượng tối đa của các báo cáo và khoảng thời gian giám sát, hoặc thông điệp yêu cầu giám sát thứ nhất mang số lượng tối đa của các báo cáo và giá trị của số lượng tối đa của các báo cáo bằng 1, thì nó chỉ báo rằng thông điệp yêu cầu giám sát thứ nhất là yêu cầu giám sát một lần.

S402. SCEF lưu trữ thông tin khác nhau được mang trong thông điệp yêu cầu giám sát thứ nhất đã nhận, và SCEF cho phép yêu cầu giám sát đã được cấu hình dựa trên chính sách cục bộ. Sau khi việc ủy quyền thành công, SCEF cấp phát bộ nhận dạng tham chiếu SCEF (ID tham chiếu SCEF), và lưu trữ sự tương ứng giữa ID tham chiếu SCEF và TLTRI. ID tham chiếu SCEF được sử dụng để xác định yêu cầu giám sát trong mạng lõi, để tiếp tục xác định nhóm người dùng.

S403. SCEF gửi thông điệp yêu cầu giám sát thứ hai đến HSS, và HSS nhận thông điệp yêu cầu giám sát thứ hai được gửi bởi SCEF.

Thông điệp yêu cầu giám sát thứ hai mang một hoặc nhiều loại thông tin được mang trong thông điệp yêu cầu giám sát thứ nhất ở bước S401, và tất nhiên không cần mang thông tin thành viên của nhóm người dùng. Ví dụ, thông điệp yêu cầu giám sát thứ hai có thể mang bộ nhận dạng nhóm bên ngoài, bộ nhận dạng SCEF, bộ nhận dạng tham chiếu SCEF, và loại giám sát.

S404. HSS kiểm tra thông điệp yêu cầu giám sát thứ hai. Sau khi việc kiểm tra thành công, HSS lưu trữ thông tin được mang trong thông điệp yêu cầu giám sát thứ hai đã nhận. HSS xác định nhóm bộ phận tương ứng với bộ nhận dạng nhóm bên ngoài.

S405. HSS trả lại thông điệp hồi đáp giám sát thứ nhất cho SCEF, và SCEF nhận thông điệp hồi đáp giám sát thứ nhất được gửi bởi HSS.

Thông điệp hồi đáp giám sát thứ nhất được sử dụng để báo nhận thông điệp yêu cầu giám sát thứ hai, và thông điệp hồi đáp giám sát thứ nhất có thể mang thông tin thành viên của nhóm người dùng. Thông điệp hồi đáp giám sát thứ nhất có thể còn mang bộ nhận dạng tham chiếu SCEF và chỉ báo nhận.

S406. SCEF trả lại thông điệp hồi đáp giám sát thứ hai cho SCS/AS, và SCS/AS nhận thông điệp hồi đáp giám sát thứ hai được trả lại bởi SCEF.

Thông điệp hồi đáp giám sát thứ hai mang TLTRI và chỉ báo nhận.

S407 đến S409 được thực hiện cho mỗi thành viên trong nhóm người dùng.

S407. HSS gửi yêu cầu chèn dữ liệu thuê bao người dùng đến tất cả các MME/SGSN đang phục vụ nhóm người dùng.

Phần lắp yêu cầu dữ liệu thuê bao người dùng mang loại giám sát, bộ nhận dạng SCEF, bộ nhận dạng tham chiếu SCEF, số lượng tối đa của các báo cáo và/hoặc khoảng thời gian giám sát, và bộ nhận dạng bên ngoài hoặc đầu số mạng số phục vụ tích hợp quốc tế thuê bao di động/mạng điện thoại chuyển số công cộng (Mobile Subscriber International ISDN/PSTN number, MSISDN).

S408. MME/SGSN lưu trữ thông số được mang trong yêu cầu chèn dữ liệu thuê bao người dùng đã nhận, và thực hiện quá trình tương ứng.

Ví dụ, MME/SGSN thiết lập số lượng của các báo cáo còn lại dựa trên số lượng tối đa của các báo cáo. Theo cách khác, MME/SGSN có thể thiết lập số lượng của các báo cáo còn lại bằng 1 cho yêu cầu giám sát một lần.

S409. MME/SGSN gửi thông điệp hồi đáp chèn dữ liệu thuê bao người dùng đến HHS, và HHS nhận thông điệp hồi đáp chèn dữ liệu thuê bao người dùng được gửi bởi MME/SGSN.

Thông điệp hồi đáp chèn dữ liệu thuê bao người dùng mang chỉ báo nhận. Nếu MME/SGSN sẵn sàng có sự kiện giám sát của yêu cầu giám sát hiện tại, MME/SGSN bổ sung báo cáo sự kiện giám sát vào thông điệp hồi đáp chèn dữ liệu thuê bao người dùng. Ngoài ra, nếu cả số lượng tối đa của các báo cáo và khoảng thời gian giám sát không được mang ở bước S407, hoặc số lượng của các báo cáo còn lại bằng 1, thì MME/SGSN xóa một cách cục bộ cấu hình sự kiện giám sát cho nhóm người dùng. Nếu giá trị của số lượng tối đa của các báo cáo được mang ở bước S407 lớn hơn 1, MME/SGSN trừ đi 1 khỏi số lượng của các báo cáo còn lại.

S410. Nếu thông điệp hồi đáp chèn dữ liệu thuê bao người dùng mang báo cáo sự kiện giám sát ở bước S409, HSS gửi thông điệp chỉ báo giám sát thứ nhất đến SCEF, và SCEF nhận thông điệp chỉ báo giám sát thứ nhất được gửi bởi HSS.

Thông điệp chỉ báo giám sát thứ nhất mang ID tham chiếu SCEF, báo cáo sự kiện giám sát, và bộ nhận dạng bên ngoài hoặc MSISDN tương ứng với báo cáo sự kiện giám sát. Trong ứng dụng thực tế, HSS có thể tổng hợp các báo cáo sự kiện giám sát từ MME/SGSN, và gửi các báo cáo sự kiện giám sát đến SCEF bằng cách sử dụng thông điệp chỉ báo giám sát. Cụ thể là, thông điệp chỉ báo giám sát mang

danh sách các mối quan hệ giữa ID tham chiếu SCEF, các báo cáo sự kiện giám sát, và bộ nhận dạng bên ngoài hoặc MSISDN.

S411. SCEF gửi thông điệp chỉ báo giám sát thứ hai đến SCS/AS, và SCS/AS nhận thông điệp chỉ báo giám sát thứ hai được gửi bởi SCEF.

Thông điệp chỉ báo giám sát thứ hai mang TLTRI, báo cáo sự kiện giám sát, và bộ nhận dạng bên ngoài hoặc MSISDN. Nếu thông điệp chỉ báo giám sát thứ nhất ở bước S410 mang các báo cáo sự kiện giám sát, thì thông điệp chỉ báo giám sát thứ hai mang danh sách các mối quan hệ giữa TLTRI, các báo cáo sự kiện giám sát, và bộ nhận dạng bên ngoài hoặc MSISDN.

S412. SCS/AS trả lại giám sát chỉ báo thông điệp hồi đáp cho SCEF, và SCEF nhận thông điệp hồi đáp chỉ báo giám sát được trả lại bởi SCS/AS.

S413. Quy trình xử lý của SCEF bao gồm một số trường hợp sau đây.

Nếu thông điệp yêu cầu giám sát thứ nhất là yêu cầu giám sát một lần ở bước S401, và MME/SGSN sẵn sàng có sự kiện giám sát của yêu cầu giám sát hiện tại ở bước S409, MME/SGSN bổ sung báo cáo sự kiện giám sát vào thông điệp hồi đáp chèn dữ liệu thuê bao người dùng, và HSS gửi, đến SCEF, báo cáo sự kiện giám sát từ MME/SGSN ở bước S410. SCEF thứ nhất xác định, dựa trên ID tham chiếu SCEF, nhóm người dùng tương ứng với báo cáo sự kiện, và sau đó xác định, dựa trên thông tin thành viên (ví dụ, N bộ nhận dạng hoặc số lượng N thành viên) của nhóm người dùng được nhận ở bước S401 hoặc S405, liệu báo cáo sự kiện giám sát được nhận ở bước S410 bao gồm các báo cáo sự kiện giám sát cho tất cả các thành viên. Nếu báo cáo sự kiện giám sát bao gồm các báo cáo sự kiện giám sát cho tất cả các thành viên, thì SCEF xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận (nói cách khác, xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được hoàn thành), và khởi tạo việc xóa cấu hình sự kiện giám sát cho nhóm người dùng hoặc dừng hoạt động gửi báo cáo sự kiện giám sát đến SCS/AS. Nếu thông điệp yêu cầu giám sát thứ nhất bao gồm các sự kiện giám sát, nói cách khác, thông điệp yêu cầu giám sát thứ nhất được sử dụng để tạo cấu hình các sự kiện giám sát cho nhóm người dùng, ví dụ, M sự kiện giám sát, dựa trên báo cáo sự kiện giám sát được nhận ở bước S410, khi nhận báo cáo sự kiện giám sát cho mỗi thành viên trong số N thành viên, hoặc nhận

báo cáo sự kiện giám sát cho mỗi một trong số M sự kiện giám sát của mỗi thành viên trong số N thành viên, SCEF xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận (nói cách khác, xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được hoàn thành). Khi các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được hoàn thành, thì báo cáo sự kiện giám sát cho nhóm người dùng được hoàn thành.

Cụ thể là, quá trình xác định, dựa trên thông tin thành viên của nhóm người dùng, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận là như sau: Nếu thông tin thành viên là số lượng thành viên, thì SCEF xác định, dựa trên số lượng của các bộ nhận dạng (các MSISDN hoặc các bộ nhận dạng bên ngoài) của các thành viên khác nhau được liên kết với báo cáo sự kiện giám sát được nhận ở bước S410, số lượng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng, và khi số lượng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng đạt đến số lượng của các thành viên trong thông tin thành viên, xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận. Nếu thông tin thành viên là bộ nhận dạng của mỗi thành viên, thì SCEF so sánh các bộ nhận dạng của các thành viên khác nhau được liên kết với báo cáo sự kiện giám sát được nhận ở bước S410 với bộ nhận dạng thành viên trong thông tin thành viên, để xác định số lượng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng, và khi các bộ nhận dạng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng đạt tới tất cả các bộ nhận dạng thành viên trong thông tin thành viên, xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận. Theo cách tùy chọn, khi nhận bộ nhận dạng của thành viên được liên kết với báo cáo sự kiện giám sát, thì SCEF xác định, dựa trên việc liệu bộ nhận dạng của thành viên có tồn tại trong bộ nhận dạng thành viên trong thông tin thành viên hay không, việc liệu thành viên với bộ nhận dạng có là thành viên trong nhóm người dùng không, và khi xác định rằng thành viên với bộ nhận dạng là thành viên trong nhóm người dùng, thì tiếp tục xác định liệu các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng có được nhận không.

Cấu hình sự kiện giám sát cho nhóm người dùng được xóa bỏ bằng cách sử dụng các bước S414 đến bước S418.

S414. SCEF gửi thông điệp yêu cầu giám sát thứ ba đến HSS, và HSS nhận thông điệp yêu cầu giám sát thứ ba được gửi bởi SCEF.

Thông điệp yêu cầu giám sát thứ ba mang ID tham chiếu SCEF và lệnh xóa. Lệnh xóa được sử dụng để ra lệnh cho HSS xóa cấu hình sự kiện giám sát cho nhóm người dùng.

S415. HSS xóa cấu hình sự kiện giám sát cho nhóm người dùng dựa trên thông điệp yêu cầu giám sát thứ ba.

S416. HSS gửi thông điệp hồi đáp giám sát thứ ba đến SCEF, và SCEF nhận thông điệp hồi đáp giám sát thứ ba được gửi bởi HSS.

Thông điệp hồi đáp giám sát thứ ba được sử dụng để báo nhận thông điệp yêu cầu giám sát thứ ba.

S417. SCEF gửi thông điệp yêu cầu giám sát thứ tư đến SCS/AS, và SCS/AS nhận thông điệp yêu cầu giám sát thứ tư được gửi bởi SCEF.

Thông điệp yêu cầu giám sát thứ tư mang TLTRI và lệnh xóa, và lệnh xóa được sử dụng để ra lệnh cho SCS/AS xóa cấu hình sự kiện giám sát cho nhóm người dùng.

S418. SCS/AS trả lại thông điệp hồi đáp giám sát thứ tư cho SCEF, và SCEF nhận thông điệp hồi đáp giám sát thứ tư được trả lại bởi SCS/AS.

Thông điệp hồi đáp giám sát thứ tư được sử dụng để báo nhận thông điệp yêu cầu giám sát thứ tư.

Cần lưu ý rằng các bước S414 và S417 không được thực hiện theo tuần tự nghiêm ngặt, và có thể trao đổi thứ tự, hoặc có thể được thực hiện một cách đồng thời.

Nếu MME/SGSN sẵn sàng có sự kiện giám sát của yêu cầu giám sát hiện tại ở bước S409, MME/SGSN bổ sung báo cáo sự kiện giám sát vào thông điệp hồi đáp chèn dữ liệu thuê bao người dùng, nhưng trị số của số lượng tối đa của các báo cáo lớn hơn 1. Theo cách thay thế, báo cáo sự kiện giám sát không được báo cáo ở bước S409 và S410. Trong hai trường hợp này, các bước S410 đến S418 được bỏ qua. S401 đến S409 là thủ tục để tạo cấu hình sự kiện giám sát cho nhóm người dùng.

Sau bước S409, hoạt động giám sát sự kiện tiếp sau có thể được thực hiện dựa trên thủ tục giám sát được thể hiện trên Fig.5.

Ngoài ra, nếu SCEF tạm thời không thực hiện các bước từ S414 đến S418 vì một số lý do, và trong chu kỳ này, SCEF nhận báo cáo sự kiện đối với yêu cầu giám sát ở bước S401, SCEF dừng hoạt động gửi báo cáo sự kiện giám sát đến SCS/AS.

Như được thể hiện trên Fig.5, thủ tục giám sát cụ thể được mô tả dưới đây.

S501. Sau khi nhận thông điệp yêu cầu chèn dữ liệu người thuê bao ở bước S407 trên Fig.4, MME/SGSN thu được thông tin hoặc thông số được mang trong thông điệp yêu cầu chèn dữ liệu người thuê bao, và giám sát sự kiện cho thành viên trong nhóm người dùng dựa trên thông tin hoặc thông số.

Cần hiểu rằng các thành viên trong nhóm người dùng có thể thuộc về thực thể quản lý di động giống nhau, hoặc có thể thuộc về các thực thể quản lý khả năng di động khác nhau, và có thể có một hoặc nhiều thực thể quản lý khả năng di động đang phục vụ nhóm người dùng. Mỗi thực thể quản lý di động thực hiện quy trình giống nhau hoặc các thủ tục tương tự cho các thành viên trong nhóm người dùng được phục vụ bởi thực thể quản lý di động.

S502. Khi phát hiện sự kiện cho thành viên trong nhóm người dùng, MME/SGSN gửi thông điệp chỉ báo giám sát đến SCEF, và SCEF nhận thông điệp chỉ báo giám sát được gửi bởi MME/SGSN.

Thông điệp chỉ báo giám sát mang ID tham chiếu SCEF, báo cáo sự kiện giám sát, và bộ nhận dạng bên ngoài hoặc MSISDN. Nếu thông điệp yêu cầu giám sát thứ nhất ở bước S401 là yêu cầu giám sát một lần, MME/SGSN tiếp tục xóa một cách cục bộ cấu hình sự kiện giám sát cho nhóm người dùng. Nếu giá trị của số lượng tối đa của các báo cáo chứa trong thông điệp yêu cầu giám sát thứ nhất ở bước S401 lớn hơn 1, thì MME/SGSN trừ đi 1 khỏi số lượng đã ghi nhận của các báo cáo còn lại. Khi số lượng của các báo cáo còn lại bằng 0, MME/SGSN xóa một cách cục bộ cấu hình sự kiện giám sát cho nhóm người dùng.

S503. SCEF gửi thông điệp chỉ báo giám sát đến SCS/AS, và SCS/AS nhận thông điệp chỉ báo giám sát được gửi bởi SCEF.

Thông điệp chỉ báo giám sát mang TLTRI, báo cáo sự kiện giám sát, và bộ nhận dạng bên ngoài hoặc MSISDN.

Theo cách tùy chọn, SCEF có thể tổng hợp các báo cáo sự kiện giám sát từ MME/SGSN, bổ sung các báo cáo sự kiện giám sát vào thông điệp chỉ báo giám sát, và gửi thông điệp chỉ báo giám sát đến SCS/AS. Trong trường hợp này, thông điệp chỉ báo giám sát mang danh sách các mối quan hệ giữa TLTRI, các báo cáo sự kiện giám sát, và bộ nhận dạng bên ngoài hoặc MSISDN.

S504. SCS/AS trả lại giám sát chỉ báo thông điệp hồi đáp cho SCEF, và SCEF nhận thông điệp hồi đáp chỉ báo giám sát được trả lại bởi SCS/AS.

Thông điệp hồi đáp chỉ báo giám sát được sử dụng để báo nhận thông điệp chỉ báo giám sát được nhận ở bước S503.

S505. Hoạt động xử lý của SCEF có thể bao gồm hai loại xử lý.

Đối với loại xử lý thứ nhất, quy trình bao gồm một số trường hợp sau đây.

SCEF xác định, dựa trên ID tham chiếu SCEF được nhận ở bước S502, nhóm người dùng tương ứng với báo cáo sự kiện, và sau đó xác định, dựa trên thông tin thành viên của nhóm người dùng mà được nhận ở bước S401 hoặc S405, liệu các báo cáo sự kiện giám sát cho tất cả các thành viên có được nhận không. Nếu các báo cáo sự kiện giám sát cho tất cả các thành viên được nhận, thì SCEF xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận (nói cách khác, xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được hoàn thành), và khởi tạo việc xóa cấu hình sự kiện giám sát cho nhóm người dùng hoặc dừng hoạt động gửi báo cáo sự kiện giám sát đến SCS/AS. Khi các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được hoàn thành, thì báo cáo sự kiện giám sát cho nhóm người dùng được hoàn thành.

Cụ thể là, quy trình xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận là như sau:

Nếu thông điệp yêu cầu giám sát thứ nhất ở bước S401 là yêu cầu giám sát một lần, quá trình xác định, dựa trên thông tin thành viên (ví dụ, N bộ nhận dạng hoặc số lượng N thành viên) của nhóm người dùng, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận là như sau: Nếu thông tin thành viên là số lượng thành viên, thì SCEF xác định, dựa trên số lượng của các bộ nhận dạng (các MSISDN hoặc các bộ nhận dạng bên ngoài) của các thành

viên khác nhau được liên kết với báo cáo sự kiện giám sát được nhận ở bước S502, số lượng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng, và khi số lượng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng đạt đến số lượng của các thành viên trong thông tin thành viên, xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận. Nếu thông tin thành viên là bộ nhận dạng của mỗi thành viên, thì SCEF so sánh các bộ nhận dạng của các thành viên khác nhau được liên kết với báo cáo sự kiện giám sát được nhận ở bước S502 với bộ nhận dạng thành viên trong thông tin thành viên, để xác định số lượng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng, và khi các bộ nhận dạng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng đạt tới tất cả các bộ nhận dạng thành viên trong thông tin thành viên, xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận. Theo cách tùy chọn, khi nhận bộ nhận dạng của thành viên được liên kết với báo cáo sự kiện giám sát, thì SCEF xác định, dựa trên việc liệu bộ nhận dạng của thành viên có tồn tại trong bộ nhận dạng thành viên trong thông tin thành viên hay không, việc liệu thành viên với bộ nhận dạng có là thành viên trong nhóm người dùng không, và khi xác định rằng thành viên với bộ nhận dạng là thành viên trong nhóm người dùng, thì tiếp tục xác định liệu các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng có được nhận không. Nếu thông điệp yêu cầu giám sát thứ nhất bao gồm các sự kiện giám sát, nói cách khác, thông điệp yêu cầu giám sát thứ nhất được sử dụng để tạo cấu hình các sự kiện giám sát cho nhóm người dùng, ví dụ, M sự kiện giám sát, dựa trên báo cáo sự kiện giám sát được nhận ở bước S502, khi nhận báo cáo sự kiện giám sát cho mỗi thành viên trong số N thành viên, hoặc nhận báo cáo sự kiện giám sát cho mỗi một trong số M sự kiện giám sát của mỗi thành viên trong số N thành viên, SCEF xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận.

Nếu giá trị của số lượng tối đa của các báo cáo lớn hơn 1, quy trình trong đó SCEF xác định, dựa trên thông tin thành viên (ví dụ, N bộ nhận dạng hoặc số lượng N thành viên) của nhóm người dùng, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận là như sau: Nếu thông tin thành viên

là số lượng thành viên, thì SCEF xác định, dựa trên số lượng của các bộ nhận dạng (các MSISDN hoặc các bộ nhận dạng bên ngoài) của các thành viên khác nhau được liên kết với báo cáo sự kiện giám sát được nhận ở bước S502, số lượng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng, và xác định liệu số lượng tích lũy của các báo cáo cho mỗi thành viên có đạt đến số lượng tối đa của các báo cáo không. Khi số lượng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng đạt đến số lượng của các thành viên trong thông tin thành viên, và số lượng tích lũy của các báo cáo cho mỗi thành viên đạt đến số lượng tối đa của các báo cáo, SCEF xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận. Nếu thông tin thành viên là bộ nhận dạng của mỗi thành viên, thì SCEF so sánh các bộ nhận dạng của các thành viên khác nhau được liên kết với báo cáo sự kiện giám sát được nhận ở bước S502 với bộ nhận dạng thành viên trong thông tin thành viên, để xác định số lượng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng, và xác định liệu số lượng tích lũy của các báo cáo cho mỗi thành viên có đạt tới số lượng tối đa của các báo cáo không. Khi các bộ nhận dạng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng đạt tới tất cả các bộ nhận dạng thành viên trong thông tin thành viên, và số lượng tích lũy của các báo cáo cho mỗi thành viên đạt đến số lượng tối đa của các báo cáo, SCEF xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận. Theo cách tùy chọn, khi nhận bộ nhận dạng của thành viên được liên kết với báo cáo sự kiện giám sát, thì SCEF xác định, dựa trên việc liệu bộ nhận dạng của thành viên có tồn tại trong bộ nhận dạng thành viên trong thông tin thành viên hay không, việc liệu thành viên với bộ nhận dạng có là thành viên trong nhóm người dùng không, và khi xác định rằng thành viên với bộ nhận dạng là thành viên trong nhóm người dùng, thì tiếp tục xác định liệu các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng có được nhận không.

Nếu thông điệp thứ nhất bao gồm nhiều sự kiện giám sát, nói cách khác, thông điệp thứ nhất được sử dụng để tạo cấu hình nhiều sự kiện giám sát cho nhóm người dùng, ví dụ, M sự kiện giám sát, khi số lần nhận báo cáo sự kiện cho mỗi thành viên trong số N thành viên đạt đến số lượng tối đa của các báo cáo, hoặc số lần

nhận báo cáo sự kiện giám sát cho mỗi một trong số M sự kiện giám sát của mỗi một trong số N thành viên đạt tới số lượng tối đa của các báo cáo, SCEF xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận.

Cấu hình sự kiện giám sát cho nhóm người dùng được xóa bỏ bằng cách sử dụng các bước S506 đến bước S510. (Trong loại xử lý thứ nhất, S506 đến bước S510 chỉ cần được thực hiện một lần.)

S506. SCEF gửi thông điệp yêu cầu giám sát đến HSS, và HSS nhận thông điệp yêu cầu giám sát được gửi bởi SCEF.

Thông điệp yêu cầu giám sát mang ID tham chiếu SCEF và lệnh xóa. Lệnh xóa được sử dụng để ra lệnh cho HSS xóa cấu hình sự kiện giám sát cho nhóm người dùng.

S507. HSS xóa cấu hình sự kiện giám sát cho nhóm người dùng dựa trên thông điệp yêu cầu giám sát.

S508. HSS gửi thông điệp hồi đáp giám sát đến SCEF, và SCEF nhận thông điệp hồi đáp giám sát được gửi bởi HSS.

Thông điệp hồi đáp giám sát được sử dụng để báo nhận thông điệp yêu cầu giám sát được nhận ở bước S506.

S509. SCEF gửi thông điệp yêu cầu giám sát đến SCS/AS, và SCS/AS nhận thông điệp yêu cầu giám sát được gửi bởi SCEF.

Thông điệp yêu cầu giám sát mang TLTRI và lệnh xóa, và lệnh xóa được sử dụng để ra lệnh cho SCS/AS xóa cấu hình sự kiện giám sát cho nhóm người dùng.

S510: SCS/AS trả lại thông điệp hồi đáp giám sát cho SCEF, và SCEF nhận thông điệp hồi đáp giám sát được trả lại bởi SCS/AS.

Thông điệp hồi đáp giám sát được sử dụng để báo nhận thông điệp yêu cầu giám sát ở bước S509.

Cần lưu ý rằng các bước S506 và S509 không được thực hiện theo tuần tự nghiêm ngặt, và có thể trao đổi thứ tự, hoặc có thể được thực hiện một cách đồng thời. Các bước S503 và S505 không được thực hiện theo tuần tự nghiêm ngặt, và có thể trao đổi thứ tự, hoặc có thể được thực hiện một cách đồng thời.

Đối với loại xử lý thứ hai, quy trình bao gồm một số trường hợp sau đây.

SCEF xác định, dựa trên ID tham chiếu SCEF được nhận ở bước S502, nhóm người dùng tương ứng với báo cáo sự kiện, xác định liệu báo cáo sự kiện giám sát cho thành viên bất kỳ tương ứng với báo cáo sự kiện có được nhận không (nói cách khác, liệu báo cáo sự kiện giám sát có được hoàn thành không), và nếu báo cáo sự kiện giám sát cho thành viên bất kỳ tương ứng với báo cáo sự kiện được nhận, yêu cầu HSS xóa cấu hình sự kiện giám sát cho thành viên. SCEF tiếp tục xác định, dựa trên thông tin thành viên của nhóm người dùng mà được nhận ở bước S401 hoặc S405, liệu các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng có được nhận không (nói cách khác, liệu các báo cáo sự kiện giám sát có được hoàn thành không). Nếu các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận, các bước sau đây được thực hiện: xóa một cách cục bộ cấu hình sự kiện giám sát cho nhóm người dùng, và yêu cầu SCS/AS xóa cấu hình sự kiện giám sát cho nhóm người dùng hoặc dừng hoạt động gửi báo cáo sự kiện đến SCS/AS. Theo cách tùy chọn, thông điệp có thể còn được gửi đến HSS, và thông điệp được sử dụng để ra lệnh cho HSS xóa cấu hình sự kiện giám sát cho nhóm người dùng. Cần lưu ý rằng, mỗi lần xác định được rằng báo cáo sự kiện giám sát cho thành viên được nhận, thì SCEF yêu cầu HSS xóa cấu hình sự kiện giám sát cho thành viên. Do đó, trường hợp mà SCEF gửi, đến HSS, thông điệp dùng để ra lệnh xóa cấu hình sự kiện giám sát cho nhóm người dùng ở đây là bước tùy chọn. Theo cách thay thế, nếu SCEF tiếp tục xác định rằng thông điệp yêu cầu để xóa cấu hình sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng đã được gửi đến HSS, thì SCEF xóa một cách cục bộ cấu hình sự kiện giám sát cho nhóm người dùng, và yêu cầu SCS/AS xóa cấu hình sự kiện giám sát cho nhóm người dùng hoặc dừng hoạt động gửi báo cáo sự kiện đến SCS/AS. Khi các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được hoàn thành, thì báo cáo sự kiện giám sát cho nhóm người dùng được hoàn thành.

Cụ thể là, quy trình xác định rằng các báo cáo sự kiện giám sát cho các thành viên tương ứng với các báo cáo sự kiện được nhận là như sau:

Nếu thông điệp yêu cầu giám sát thứ nhất là yêu cầu giám sát một lần ở bước S401 và báo cáo sự kiện của thành viên được nhận ở bước S502, thì SCEF xác định rằng báo cáo sự kiện giám sát cho thành viên tương ứng với báo cáo sự kiện được

nhận. Nếu giá trị của số lượng tối đa của các báo cáo lớn hơn 1 và sau bước S502, số lần nhận báo cáo sự kiện cho thành viên đạt đến số lượng tối đa của các báo cáo, thì SCEF xác định rằng báo cáo sự kiện giám sát cho thành viên tương ứng với báo cáo sự kiện được nhận. Theo cách tùy chọn, khi nhận bộ nhận dạng của thành viên được liên kết với báo cáo sự kiện giám sát, SCEF xác định, dựa trên việc liệu bộ nhận dạng của thành viên có tồn tại trong bộ nhận dạng thành viên trong thông tin thành viên hay không, việc liệu thành viên với bộ nhận dạng có là thành viên trong nhóm người dùng không, và khi xác định rằng thành viên với bộ nhận dạng là thành viên trong nhóm người dùng, thì tiếp tục xác định rằng báo cáo sự kiện giám sát cho thành viên tương ứng được nhận. Nếu thông điệp thứ nhất bao gồm nhiều sự kiện giám sát, nói cách khác, thông điệp thứ nhất được sử dụng để tạo cấu hình nhiều sự kiện giám sát cho nhóm người dùng, ví dụ, M sự kiện giám sát, khi số lần nhận báo cáo sự kiện cho thành viên đạt đến số lượng tối đa của các báo cáo, hoặc số lần nhận báo cáo sự kiện giám sát cho mỗi một trong số M sự kiện giám sát cho thành viên đạt tới số lượng tối đa của các báo cáo, SCEF xác định rằng báo cáo sự kiện giám sát cho thành viên tương ứng với báo cáo sự kiện được nhận.

Tương tự, bước S506 đến bước S508 được sử dụng để yêu cầu HSS xóa cấu hình sự kiện giám sát cho thành viên. (Trong loại xử lý thứ hai, bước S506 đến bước S508 cần được thực hiện nhiều lần, hoặc thậm chí N lần.)

S506. SCEF gửi thông điệp yêu cầu giám sát đến HSS, và HSS nhận thông điệp yêu cầu giám sát được gửi bởi SCEF.

Thông điệp yêu cầu giám sát mang ID tham chiếu SCEF, bộ nhận dạng nhóm bên ngoài, bộ nhận dạng thành viên (nói cách khác, bộ nhận dạng bên ngoài và/hoặc MSISDN), và lệnh xóa. Lệnh xóa được sử dụng để ra lệnh cho HSS xóa cấu hình sự kiện giám sát cho thành viên tương ứng với bộ nhận dạng thành viên.

S507. HSS xóa cấu hình sự kiện giám sát cho thành viên dựa trên thông điệp yêu cầu giám sát.

S508. HSS gửi thông điệp hồi đáp giám sát đến SCEF, và SCEF nhận thông điệp hồi đáp giám sát được gửi bởi HSS.

Thông điệp hồi đáp giám sát được sử dụng để báo nhận thông điệp yêu cầu giám sát được nhận ở bước S506.

Theo cách tùy chọn, SCEF bổ sung các bộ nhận dạng thành viên vào thông điệp yêu cầu giám sát ở bước S506, và HSS xóa cấu hình sự kiện giám sát tương ứng với các bộ nhận dạng thành viên.

Quy trình xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận là như sau:

Nếu thông điệp yêu cầu giám sát thứ nhất ở bước S401 là yêu cầu giám sát một lần, quá trình xác định, dựa trên thông tin thành viên (ví dụ, N bộ nhận dạng hoặc số lượng N thành viên) của nhóm người dùng, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận là như sau: Nếu thông tin thành viên là số lượng thành viên, thì SCEF xác định, dựa trên số lượng của các bộ nhận dạng (các MSISDN hoặc các bộ nhận dạng bên ngoài) của các thành viên khác nhau được liên kết với báo cáo sự kiện giám sát được nhận ở bước S502, số lượng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng, và khi số lượng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng đạt đến số lượng của các thành viên trong thông tin thành viên, xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận. Nếu thông tin thành viên là bộ nhận dạng của mỗi thành viên, thì SCEF so sánh các bộ nhận dạng của các thành viên khác nhau được liên kết với báo cáo sự kiện giám sát được nhận ở bước S502 với bộ nhận dạng thành viên trong thông tin thành viên, để xác định số lượng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng, và khi các bộ nhận dạng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng đạt tới tất cả các bộ nhận dạng thành viên trong thông tin thành viên, xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận. Theo cách tùy chọn, khi nhận bộ nhận dạng của thành viên được liên kết với báo cáo sự kiện giám sát, thì SCEF xác định, dựa trên việc liệu bộ nhận dạng của thành viên có tồn tại trong bộ nhận dạng thành viên trong thông tin thành viên hay không, việc liệu thành viên với bộ nhận dạng có là thành viên trong nhóm người dùng không, và khi xác định rằng thành viên với bộ nhận dạng là thành viên trong nhóm người dùng, thì tiếp tục xác định liệu các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng có được nhận không. Nếu thông điệp yêu cầu giám sát thứ nhất bao gồm các sự kiện giám sát, nói

cách khác, thông điệp yêu cầu giám sát thứ nhất được sử dụng để tạo cấu hình các sự kiện giám sát cho nhóm người dùng, ví dụ, M sự kiện giám sát, dựa trên báo cáo sự kiện giám sát được nhận ở bước S502, khi nhận báo cáo sự kiện giám sát cho mỗi thành viên trong số N thành viên, hoặc nhận báo cáo sự kiện giám sát cho mỗi một trong số M sự kiện giám sát của mỗi thành viên trong số N thành viên, SCEF xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận.

Nếu giá trị của số lượng tối đa của các báo cáo lớn hơn 1, quy trình trong đó SCEF xác định, dựa trên thông tin thành viên (ví dụ, N bộ nhận dạng hoặc số lượng N thành viên) của nhóm người dùng, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận là như sau: Nếu thông tin thành viên là số lượng thành viên, thì SCEF xác định, dựa trên số lượng của các bộ nhận dạng (các MSISDN hoặc các bộ nhận dạng bên ngoài) của các thành viên khác nhau được liên kết với báo cáo sự kiện giám sát được nhận ở bước S502, số lượng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng, và xác định liệu số lượng tích lũy của các báo cáo cho mỗi thành viên có đạt đến số lượng tối đa của các báo cáo không. Khi số lượng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng đạt đến số lượng của các thành viên trong thông tin thành viên, và số lượng tích lũy của các báo cáo cho mỗi thành viên đạt đến số lượng tối đa của các báo cáo, SCEF xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận. Nếu thông tin thành viên là bộ nhận dạng của mỗi thành viên, thì SCEF so sánh các bộ nhận dạng của các thành viên khác nhau được liên kết với báo cáo sự kiện giám sát được nhận ở bước S502 với bộ nhận dạng thành viên trong thông tin thành viên, để xác định số lượng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng, và xác định liệu số lượng tích lũy của các báo cáo cho mỗi thành viên có đạt tới số lượng tối đa của các báo cáo không. Khi các bộ nhận dạng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng đạt tới tất cả các bộ nhận dạng thành viên trong thông tin thành viên, và số lượng tích lũy của các báo cáo cho mỗi thành viên đạt đến số lượng tối đa của các báo cáo, SCEF xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận. Theo cách tùy chọn, khi nhận bộ nhận

dạng của thành viên được liên kết với báo cáo sự kiện giám sát, thì SCEF xác định, dựa trên việc liệu bộ nhận dạng của thành viên có tồn tại trong bộ nhận dạng thành viên trong thông tin thành viên hay không, việc liệu thành viên với bộ nhận dạng có là thành viên trong nhóm người dùng không, và khi xác định rằng thành viên với bộ nhận dạng là thành viên trong nhóm người dùng, thì tiếp tục xác định liệu các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng có được nhận không.

Nếu thông điệp thứ nhất bao gồm nhiều sự kiện giám sát, nói cách khác, thông điệp thứ nhất được sử dụng để tạo cấu hình nhiều sự kiện giám sát cho nhóm người dùng, ví dụ, M sự kiện giám sát, khi số lần nhận báo cáo sự kiện cho mỗi thành viên trong số N thành viên đạt đến số lượng tối đa của các báo cáo, hoặc số lần nhận báo cáo sự kiện giám sát cho mỗi một trong số M sự kiện giám sát của mỗi một trong số N thành viên đạt tới số lượng tối đa của các báo cáo, SCEF xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận.

Cấu hình sự kiện giám sát cho nhóm người dùng được xóa bỏ bằng cách sử dụng các bước S509 và S510.

S509. SCEF gửi thông điệp yêu cầu giám sát đến SCS/AS, và SCS/AS nhận thông điệp yêu cầu giám sát được gửi bởi SCEF.

Thông điệp yêu cầu giám sát mang TLTRI và lệnh xóa, và lệnh xóa được sử dụng để ra lệnh cho SCS/AS xóa cấu hình sự kiện giám sát cho nhóm người dùng.

S510: SCS/AS trả lại thông điệp hồi đáp giám sát cho SCEF, và SCEF nhận thông điệp hồi đáp giám sát được trả lại bởi SCS/AS.

Thông điệp hồi đáp giám sát được sử dụng để báo nhận thông điệp yêu cầu giám sát ở bước S509.

Các thông điệp yêu cầu giám sát và các thông điệp hồi đáp giám sát mà được gửi ở các bước khác nhau trên Fig.5 là không khác biệt. Có thể hiểu rằng các thông điệp với tên gọi giống nhau có thể mang nội dung giống nhau hoặc có thể mang nội dung khác nhau. Các bước được thể hiện ở bước S505 đến bước S510 trên Fig.5 là giống nhau. Tuy nhiên, thực tế là, dựa trên các phần mô tả nêu trên, các bước có thể được giải thích theo cách khác nhau dựa trên hai loại xử lý khác nhau của SCEF ở

bước S505. Đối với các mô tả chi tiết của các bước, tham chiếu đến các phần mô tả nêu trên.

Ngoài ra, nếu SCEF tạm thời không thực hiện các bước từ S506 đến S510 vì một số lý do, và trong chu kỳ này, SCEF nhận báo cáo sự kiện đối với yêu cầu giám sát ở bước S401, SCEF dừng hoạt động gửi báo cáo sự kiện giám sát đến SCS/AS.

Tóm lại, theo các phương pháp được thể hiện trên Fig.4 và Fig.5, trong hệ thống LTE, SCEF thu được thông tin thành viên của nhóm người dùng, sao cho khi nhận báo cáo sự kiện giám sát, SCEF có thể xác định, dựa trên thông tin thành viên của nhóm người dùng, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận, và có thể tiếp tục xóa bỏ cấu hình sự kiện giám sát cho nhóm người dùng hoặc dừng báo cáo sự kiện, nhờ đó tránh được sự lãng phí tài nguyên và giúp đảm bảo sự thực thi đúng của chính sách tiếp theo sau.

Trường hợp ứng dụng 2: hệ thống 5G. Thực thể chức năng lộ diện là NEF, thực thể ứng dụng bên thứ ba là SCS/làm phần tử mạng quản lý khả năng di động là AMF, và thực thể quản lý dữ liệu người dùng là UDM 203.

Như được thể hiện trên Fig.6A và Fig.6B, thủ tục của hoạt động giám sát sự kiện trong trường hợp ứng dụng 2 được mô tả cụ thể như sau:

S601. SCS/AS gửi thông điệp yêu cầu đăng ký sự kiện giám sát dựa trên nhóm người dùng (Nnef_EventExposure_Subscribe request) đến NEF, và NEF nhận thông điệp yêu cầu Nnef_EventExposure_Subscribe được gửi bởi SCS/AS. Thông điệp yêu cầu Nnef_EventExposure_Subscribe là thông điệp thứ nhất trong phương án nêu trên, và có thuộc tính và chức năng của thông điệp thứ nhất.

Thông điệp yêu cầu Nnef_EventExposure_Subscribe mang thông tin thành viên của nhóm người dùng, và có thể còn mang, nhưng không bị giới hạn ở, ít nhất một trong số các thông tin sau đây: địa chỉ thông báo sự kiện SCS/AS, bộ nhận dạng thông báo sự kiện SCS/AS, sự kiện giám sát (Monitoring Event), bộ nhận dạng nhóm bên ngoài (External Group Id), và chế độ báo cáo sự kiện. Giá trị của chế độ báo cáo sự kiện có thể đang báo cáo về số lần tối đa đã đạt tới được, báo cáo định kỳ, hoặc báo cáo về khoảng thời gian tối đa đã đạt tới được. Nếu độ chi tiết báo cáo sự kiện đang báo cáo về số lần tối đa đã đạt tới được, thông điệp yêu cầu Nnef_EventExposure_Subscribe tiếp tục mang số lượng tối đa của các báo cáo.

Cấu hình thông số trong thông điệp yêu cầu đăng ký sự kiện giám sát có thể áp dụng cho mỗi thành viên trong nhóm người dùng. Nếu độ chi tiết báo cáo sự kiện đang báo cáo về số lần tối đa đã đạt tới được, và giá trị của số lượng tối đa của các báo cáo được mang trong thông điệp yêu cầu Nnef_EventExposure_Subscribe bằng 1, thì nó chỉ báo rằng thông điệp yêu cầu Nnef_EventExposure_Subscribe là yêu cầu giám sát một lần.

Trong hệ thống 5G, sự kiện giám sát thuê bao có thể là tương tự với cấu hình sự kiện giám sát trong hệ thống LTE.

S602. NEF lưu trữ thông tin khác nhau được mang trong thông điệp được nhận ở bước S601, và NEF cho phép yêu cầu giám sát đã được đăng ký dựa trên chính sách cục bộ.

S603. NEF gửi thông điệp yêu cầu đăng ký sự kiện giám sát, cụ thể là, thông điệp yêu cầu Nudm_EventExposure_Subscribe, đến UDM, và UDM nhận thông điệp yêu cầu Nudm_EventExposure_Subscribe được gửi bởi NEF.

Thông điệp mang ID nhóm bên ngoài, sự kiện giám sát, địa chỉ thông báo sự kiện NEF, và bộ nhận dạng thông báo sự kiện NEF, và có thể còn mang một số các thông số tùy chọn trong thông điệp yêu cầu Nnef_EventExposure_Subscribe ở bước S601. Địa chỉ thông báo sự kiện NEF và bộ nhận dạng thông báo sự kiện NEF được sử dụng để kết hợp thông báo sự kiện tương lai, để xác định nhóm người dùng.

S604. UDM kiểm tra thông điệp yêu cầu Nudm_EventExposure_Subscribe được nhận ở bước S603, và sau khi việc kiểm tra thành công, UDM lưu trữ các thông số được mang trong thông điệp. UDM xác định sự tương ứng giữa bộ nhận dạng nhóm bên ngoài và bộ nhận dạng của thành viên trong nhóm người dùng.

S605. UDM gửi thông điệp hồi đáp đăng ký sự kiện giám sát (hồi đáp Nudm_EventExposure_Subscribe) đến NEF, và NEF nhận thông điệp hồi đáp đăng ký sự kiện giám sát được gửi bởi UDM.

Theo cách tùy chọn, thông điệp hồi đáp đăng ký sự kiện giám sát mang thông tin thành viên của nhóm người dùng. Thông điệp hồi đáp đăng ký sự kiện giám sát còn mang bộ nhận dạng thuê bao UDM đã được nhận và chỉ báo nhận.

S606. NEF gửi thông điệp hồi đáp đăng ký sự kiện giám sát (hồi đáp Nnef_EventExposure_Subscribe) đến SCS/AS, và SCS/AS nhận thông điệp hồi đáp

đăng ký sự kiện giám sát được gửi bởi NEF.

Thông điệp mang bộ nhận dạng thuê bao NEF và chỉ báo nhận.

S607 đến S611 được thực hiện cho mỗi thành viên trong nhóm người dùng.

S607. UDM gửi, cho thành viên trong nhóm người dùng, thông điệp yêu cầu thông báo quản lý dữ liệu thuê bao (Subscriber Data Management, SDM) (Nudm_SDM_Notification Request) đến AMF mà có vai trò thành viên, và AMF nhận thông điệp yêu cầu thông báo SDM được gửi bởi UDM.

Thông điệp mang bộ nhận dạng bên ngoài hoặc MSISDN, và có thể còn mang số lượng tối đa của các báo cáo.

S608. UDM gửi thông điệp yêu cầu đăng ký sự kiện giám sát(Namf_EventExposure_Subscribe Request) đến AMF cho thành viên ở bước S607, và AMF nhận thông điệp yêu cầu Namf_EventExposure_Subscribe được gửi bởi UDM.

Thông điệp mang sự kiện giám sát, địa chỉ thông báo sự kiện NEF, và bộ nhận dạng thông báo sự kiện NEF.

S609. AMF lưu trữ các thông số trong thông điệp yêu cầu Namf_EventExposure_Subscribe đã được nhận, và thực hiện xử lý tương ứng.

Quy trình xử lý bao gồm: thiết lập số lượng của các báo cáo còn lại dựa trên số lượng tối đa của các báo cáo.

S610. AMF gửi thông điệp hồi đáp thông báo SDM (Nudm_SDM_Notification Response) đến UDM, và UDM nhận thông điệp hồi đáp Nudm_SDM_Notification được gửi bởi AMF.

Thông điệp mang chỉ báo nhận.

S611. AMF trả lại thông điệp hồi đáp đăng ký sự kiện giám sát (Namf_EventExposure_Subscribe Response) đến UDM, và UDM nhận thông điệp hồi đáp Namf_EventExposure_Subscribe được gửi bởi AMF.

Thông điệp mang bộ nhận dạng thuê bao AMF và chỉ báo nhận. Nếu AMF có báo cáo sự kiện giám sát về sự kiện giám sát đã được đăng ký hiện tại, AMF bổ sung báo cáo sự kiện giám sát, địa chỉ thông báo sự kiện NEF, và bộ nhận dạng thông báo sự kiện NEF vào thông điệp hồi đáp Namf_EventExposure_Subscribe. Ngoài ra, nếu sự kiện giám sát thuê bao ở bước S607 là yêu cầu giám sát lần đầu, thì AMF xóa một

cách cục bộ cấu hình sự kiện giám sát cho nhóm người dùng. Nếu giá trị của số lượng tối đa của các báo cáo được mang ở bước S607 lớn hơn 1, AMF trừ đi 1 khỏi số lượng của các báo cáo còn lại.

Nếu báo cáo sự kiện giám sát được mang ở bước S611, các bước tiếp theo được thực hiện. Theo cách khác, không có bước tiếp sau được thực hiện.

S612. UDM gửi thông điệp yêu cầu thông báo sự kiện giám sát (Ndum_EventExposure_Notify Request) đến NEF, và NEF nhận thông điệp yêu cầu Ndum_EventExposure_Notify được gửi bởi UDM. NEF trả lại thông điệp hồi đáp Ndum_EventExposure_Notify cho UDM.

Thông điệp yêu cầu Ndum_EventExposure_Notify mang bộ nhận dạng thông báo sự kiện NEF, báo cáo sự kiện giám sát, và bộ nhận dạng bên ngoài hoặc MSISDN tương ứng với báo cáo sự kiện giám sát. Trong ứng dụng thực tế, UDM có thể tổng hợp các báo cáo sự kiện giám sát từ AMF, và gửi các báo cáo sự kiện giám sát đến NEF bằng cách sử dụng thông điệp yêu cầu thông báo sự kiện giám sát. Cụ thể là, thông điệp yêu cầu thông báo sự kiện giám sát mang danh sách các mối quan hệ giữa bộ nhận dạng thông báo sự kiện NEF, các báo cáo sự kiện giám sát, và bộ nhận dạng bên ngoài hoặc MSISDN.

S613. NEF gửi thông điệp yêu cầu đăng ký sự kiện giám sát (Nnef_Event Exposure_Notify Request) đến SCS/AS, và SCS/AS nhận thông điệp yêu cầu Nnef_EventExposure_Notify được gửi bởi NEF. SCS/AS trả lại thông điệp hồi đáp đăng ký sự kiện giám sát (Nnef_EventExposure_Notify Response) cho NEF, và NEF nhận thông điệp hồi đáp Nnef_EventExposure_Notify được trả lại bởi SCS/AS.

Thông điệp yêu cầu Nnef_EventExposure_Notify mang bộ nhận dạng thông báo sự kiện SCS/AS, báo cáo sự kiện giám sát, và bộ nhận dạng bên ngoài hoặc MSISDN. Nếu các báo cáo sự kiện giám sát được mang ở bước S612, thông điệp yêu cầu Nnef_EventExposure_Notify mang danh sách các mối quan hệ giữa bộ nhận dạng thông báo sự kiện SCS/AS, các báo cáo sự kiện giám sát, và bộ nhận dạng bên ngoài hoặc MSISDN.

S614. Quy trình xử lý của NEF bao gồm một số trường hợp sau đây.

Nếu thông điệp yêu cầu đăng ký sự kiện giám sát ở bước S601 là yêu cầu giám sát một lần, AMF bổ sung báo cáo sự kiện giám sát vào thông điệp hồi đáp

Namf_EventExposure_Subscribe ở bước S611, và UDM gửi, đến NEF, báo cáo sự kiện giám sát từ AMF ở bước S612, NEF xác định, dựa trên bộ nhận dạng thông báo NEF đã được nhận, nhóm người dùng tương ứng với báo cáo sự kiện, và sau đó xác định, dựa trên thông tin thành viên của nhóm người dùng được nhận ở các bước S601 hoặc S605, liệu báo cáo sự kiện giám sát có được nhận ở bước S612 không bao gồm các báo cáo sự kiện giám sát cho tất cả các thành viên. Nếu báo cáo sự kiện giám sát bao gồm các báo cáo sự kiện giám sát cho tất cả các thành viên, thì NEF xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận (nói cách khác, xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được hoàn thành), và khởi tạo việc xóa cấu hình sự kiện giám sát cho nhóm người dùng hoặc dừng hoạt động gửi báo cáo sự kiện giám sát đến SCS/AS. Khi các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được hoàn thành, thì báo cáo sự kiện giám sát cho nhóm người dùng được hoàn thành.

Cụ thể là, quá trình xác định, dựa trên thông tin thành viên (ví dụ, N bộ nhận dạng hoặc số lượng N thành viên) của nhóm người dùng, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận là như sau: Nếu thông tin thành viên là số lượng thành viên, thì NEF xác định, dựa trên số lượng của các bộ nhận dạng (các MSISDN hoặc các bộ nhận dạng bên ngoài) của các thành viên khác nhau được liên kết với báo cáo sự kiện giám sát được nhận ở bước S612, số lượng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng, và khi số lượng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng đạt đến số lượng của các thành viên trong thông tin thành viên, xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận. Nếu thông tin thành viên là bộ nhận dạng của mỗi thành viên, thì NEF so sánh các bộ nhận dạng của các thành viên khác nhau được liên kết với báo cáo sự kiện giám sát được nhận ở bước S612 với bộ nhận dạng thành viên trong thông tin thành viên, để xác định số lượng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng, và khi các bộ nhận dạng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng đạt tới tất cả các bộ nhận dạng thành viên trong thông tin thành viên, xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên

trong nhóm người dùng được nhận. Theo cách tùy chọn, khi nhận bộ nhận dạng của thành viên được liên kết với báo cáo sự kiện giám sát, thì NEF xác định, dựa trên việc liệu bộ nhận dạng của thành viên có tồn tại trong bộ nhận dạng thành viên trong thông tin thành viên hay không, việc liệu thành viên với bộ nhận dạng có là thành viên trong nhóm người dùng không, và khi xác định rằng thành viên với bộ nhận dạng là thành viên trong nhóm người dùng, thì tiếp tục xác định liệu các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng có được nhận không. Nếu yêu cầu đăng ký sự kiện giám sát bao gồm các sự kiện giám sát, nói cách khác, yêu cầu đăng ký sự kiện giám sát được sử dụng để tạo cấu hình các sự kiện giám sát cho nhóm người dùng, ví dụ, M sự kiện giám sát, dựa trên báo cáo sự kiện giám sát được nhận ở bước S612, khi nhận báo cáo sự kiện giám sát cho mỗi thành viên trong số N thành viên, hoặc nhận báo cáo sự kiện giám sát cho mỗi một trong số M sự kiện giám sát của mỗi thành viên trong số N thành viên, NEF xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận.

Đăng ký sự kiện giám sát cho nhóm người dùng được xóa bỏ bằng cách sử dụng các bước từ S615 đến S622.

S615. NEF gửi yêu cầu không đăng ký sự kiện giám sát (Nudm_EventExposure_Unsubscribe Request) đến UDM, và thông điệp yêu cầu Nudm_EventExposure_Unsubscribe mang bộ nhận dạng thuê bao UDM. UDM nhận thông điệp yêu cầu Nudm_EventExposure_Unsubscribe được gửi bởi NEF.

S616. UDM gửi yêu cầu không đăng ký sự kiện giám sát (Namf_EventExposure_Unsubscribe Request) đến AMF, và AMF nhận yêu cầu Namf_EventExposure_Unsubscribe được gửi bởi UDM.

Thông điệp yêu cầu Namf_EventExposure_Unsubscribe mang bộ nhận dạng thuê bao AMF.

S617. AMF xóa thông tin thuê bao sự kiện giám sát tương ứng với bộ nhận dạng thuê bao AMF.

S618. AMF trả lại thông điệp hồi đáp cho UDM.

S619. UDM xóa thông tin thuê bao sự kiện giám sát tương ứng với bộ nhận dạng thuê bao UDM, và trả lại thông điệp xác nhận cho NEF.

S620. NEF gửi thông điệp yêu cầu thông báo sự kiện giám sát

(Nnef_EventExposure_Notify Request) đến SCS/AS, và thông điệp yêu cầu Nnef_EventExposure_Notify mang bộ nhận dạng thông báo sự kiện SCS và lệnh xóa. SCS/AS trả lại thông điệp hồi đáp.

S621. SCS/AS gửi thông điệp yêu cầu không đăng ký sự kiện giám sát (Nnef_EventExposure_Unsubscribe Request) đến NEF, và thông điệp yêu cầu không đăng ký sự kiện giám sát (Nnef_EventExposure_Unsubscribe request) mang bộ nhận dạng thuê bao NEF.

S622. NEF trả lại thông điệp xác nhận sau khi xóa sự kiện thông tin thuê bao tương ứng với bộ nhận dạng thuê bao NEF.

Cần lưu ý rằng các bước S615 và S620 không được thực hiện theo tuần tự nghiêm ngặt, và có thể trao đổi thứ tự, hoặc có thể được thực hiện một cách đồng thời.

Ngoài ra, nếu NEF tạm thời không thực hiện các bước từ S615 đến S622 vì một số lý do, và trong khoảng thời gian này, NEF nhận báo cáo sự kiện giám sát cho yêu cầu đăng ký sự kiện giám sát ở bước S601, và SCEF dừng hoạt động gửi báo cáo sự kiện giám sát đến SCS/AS.

Nếu AMF mang báo cáo sự kiện giám sát ở bước S611, nhưng trị số của số lượng tối đa của các báo cáo lớn hơn 1, hoặc AMF không báo cáo về báo cáo sự kiện giám sát ở bước S611, hoạt động giám sát sự kiện tiếp sau có thể được thực hiện dựa trên thủ tục giám sát được thể hiện trên Fig.7.

Như được thể hiện trên Fig.7, thủ tục giám sát cụ thể được mô tả dưới đây.

S701. Sau khi nhận thông điệp hồi đáp Nudm_SDM_Notification ở bước S610 trên Fig.6A, AMF giám sát sự kiện cho thành viên trong nhóm người dùng dựa trên thông số được mang trong thông điệp hồi đáp Nudm_SDM_Notification.

Cần hiểu rằng các thành viên trong nhóm người dùng có thể thuộc về AMF giống nhau, hoặc có thể thuộc về các AMF khác nhau, và có thể có một hoặc nhiều AMF đang phục vụ nhóm người dùng. Mỗi AMF thực hiện quy trình giống nhau hoặc các thủ tục tương tự cho các thành viên trong nhóm người dùng được phục vụ bởi AMF.

S702. AMF gửi thông điệp yêu cầu thông báo sự kiện giám sát, cụ thể là, yêu cầu Namf_EventExposure_Notify, đến NEF, trong đó thông điệp yêu cầu

Namf_EventExposure_Notify mang địa chỉ thông báo sự kiện NEF, bộ nhận dạng thông báo sự kiện NEF, báo cáo sự kiện giám sát, và bộ nhận dạng bên ngoài hoặc MSISDN tương ứng với báo cáo sự kiện giám sát. Nếu chế độ báo cáo sự kiện đang báo cáo về số lần tối đa đã đạt tới được và số lượng tối đa của các báo cáo bằng 1, thì AMF xóa một cách cục bộ sự kiện giám sát thuê bao cho nhóm người dùng. Nếu giá trị của số lượng tối đa của các báo cáo lớn hơn 1, AMF trừ đi 1 khỏi số lượng đã ghi nhận của các báo cáo còn lại. Khi số lượng của các báo cáo còn lại bằng 0, AMF xóa một cách cục bộ cấu hình sự kiện giám sát cho nhóm người dùng.

S703. NEF trả lại thông điệp xác nhận, cụ thể là, hồi đáp Namf_EventExposure_Notify, cho AMF, và AMF nhận hồi đáp Namf_EventExposure_Notify được trả lại bởi NEF.

S704. NEF gửi yêu cầu thông báo sự kiện giám sát, cụ thể là, yêu cầu Nnef_EventExposure_Notify, đến SCS/AS, trong đó thông điệp yêu cầu Nnef_EventExposure_Notify mang bộ nhận dạng thông báo sự kiện SCS/AS, báo cáo sự kiện giám sát, và bộ nhận dạng bên ngoài hoặc MSISDN.

Theo cách tùy chọn, NEF có thể tổng hợp các báo cáo sự kiện giám sát từ AMF, và gửi các báo cáo sự kiện giám sát đến SCS/AS bằng cách sử dụng thông điệp yêu cầu Nnef_EventExposure_Notify, trong đó thông điệp yêu cầu Nnef_EventExposure_Notify mang danh sách các mối quan hệ giữa bộ nhận dạng thông báo sự kiện SCS/AS, các báo cáo sự kiện giám sát, và bộ nhận dạng bên ngoài hoặc MSISDN.

S705. SCS/AS trả lại thông điệp xác nhận, cụ thể là, hồi đáp Nnef_EventExposure_Notify, cho NEF, và NEF nhận hồi đáp Nnef_EventExposure_Notify được trả lại bởi SCS/AS.

S706. Quy trình xử lý của NEF bao gồm một số trường hợp sau đây.

NEF xác định, dựa trên bộ nhận dạng thông báo sự kiện được nhận ở bước S602, nhóm người dùng tương ứng với báo cáo sự kiện, và sau đó xác định, dựa trên thông tin thành viên của nhóm người dùng mà được nhận ở bước S601 hoặc S605, liệu các báo cáo sự kiện giám sát cho tất cả các thành viên có được nhận không. Nếu xác định được rằng các báo cáo sự kiện giám sát cho tất cả các thành viên được nhận, NEF xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên

trong nhóm người dùng được nhận (xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được hoàn thành), và khởi tạo việc xóa cấu hình sự kiện giám sát cho nhóm người dùng hoặc dừng hoạt động gửi báo cáo sự kiện giám sát đến SCS/AS. Khi các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được hoàn thành, thì báo cáo sự kiện giám sát cho nhóm người dùng được hoàn thành.

Cụ thể là, quy trình xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận là như sau:

Nếu yêu cầu đăng ký sự kiện giám sát ở bước S601 là yêu cầu giám sát một lần, quá trình xác định, dựa trên thông tin thành viên (ví dụ, N bộ nhận dạng hoặc số lượng N thành viên) của nhóm người dùng, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận là như sau: Nếu thông tin thành viên là số lượng thành viên, thì NEF xác định, dựa trên số lượng của các bộ nhận dạng (các MSISDN hoặc các bộ nhận dạng bên ngoài) của các thành viên khác nhau được liên kết với báo cáo sự kiện giám sát được nhận ở bước S612, số lượng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng, và khi số lượng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng đạt đến số lượng của các thành viên trong thông tin thành viên, xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận. Nếu thông tin thành viên là bộ nhận dạng của mỗi thành viên, thì NEF so sánh các bộ nhận dạng của các thành viên khác nhau được liên kết với báo cáo sự kiện giám sát được nhận ở bước S612 với bộ nhận dạng thành viên trong thông tin thành viên, để xác định số lượng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng, và khi các bộ nhận dạng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng đạt tới tất cả các bộ nhận dạng thành viên trong thông tin thành viên, xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận. Theo cách tùy chọn, khi nhận bộ nhận dạng của thành viên được liên kết với báo cáo sự kiện giám sát, thì NEF xác định, dựa trên việc liệu bộ nhận dạng của thành viên có tồn tại trong bộ nhận dạng thành viên trong thông tin thành viên hay không, việc liệu thành viên với bộ nhận dạng có là thành viên trong nhóm người dùng không, và khi xác định rằng thành viên với bộ nhận dạng là thành

viên trong nhóm người dùng, thì tiếp tục xác định liệu các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng có được nhận không. Nếu thông điệp yêu cầu giám sát thứ nhất bao gồm các sự kiện giám sát, nói cách khác, thông điệp yêu cầu giám sát thứ nhất được sử dụng để tạo cấu hình các sự kiện giám sát cho nhóm người dùng, ví dụ, M sự kiện giám sát, dựa trên báo cáo sự kiện giám sát được nhận ở bước S612, khi nhận báo cáo sự kiện giám sát cho mỗi thành viên trong số N thành viên, hoặc nhận báo cáo sự kiện giám sát cho mỗi một trong số M sự kiện giám sát của mỗi thành viên trong số N thành viên, NEF xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận.

Nếu giá trị của số lượng tối đa của các báo cáo lớn hơn 1, quy trình trong đó NEF xác định, dựa trên thông tin thành viên (ví dụ, N bộ nhận dạng hoặc số lượng N thành viên) của nhóm người dùng, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận là như sau: Nếu thông tin thành viên là số lượng thành viên, thì NEF xác định, dựa trên số lượng của các bộ nhận dạng (các MSISDN hoặc các bộ nhận dạng bên ngoài) của các thành viên khác nhau được liên kết với báo cáo sự kiện giám sát được nhận ở bước S612, số lượng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng, và xác định liệu số lượng tích lũy của các báo cáo cho mỗi thành viên có đạt đến số lượng tối đa của các báo cáo không. Khi số lượng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng đạt đến số lượng của các thành viên trong thông tin thành viên, và số lượng tích lũy của các báo cáo cho mỗi thành viên đạt đến số lượng tối đa của các báo cáo, NEF xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận.

Nếu thông tin thành viên là bộ nhận dạng của mỗi thành viên, thì NEF so sánh các bộ nhận dạng của các thành viên khác nhau được liên kết với báo cáo sự kiện giám sát được nhận ở bước S612 với bộ nhận dạng thành viên trong thông tin thành viên, để xác định số lượng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng, và xác định liệu số lượng tích lũy của các báo cáo cho mỗi thành viên có đạt tới số lượng tối đa của các báo cáo không. Khi các bộ nhận dạng của các thành viên mà các báo cáo sự kiện giám sát được nhận cho chúng đạt tới tất cả các bộ nhận dạng thành viên trong thông tin thành viên, và số lượng tích lũy của các báo

cáo cho mỗi thành viên đạt đến số lượng tối đa của các báo cáo, NEF xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận. Theo cách tùy chọn, khi nhận bộ nhận dạng của thành viên được liên kết với báo cáo sự kiện giám sát, thì NEF xác định, dựa trên việc liệu bộ nhận dạng của thành viên có tồn tại trong bộ nhận dạng thành viên trong thông tin thành viên hay không, việc liệu thành viên với bộ nhận dạng có là thành viên trong nhóm người dùng không, và khi xác định rằng thành viên với bộ nhận dạng là thành viên trong nhóm người dùng, thì tiếp tục xác định liệu các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng có được nhận không.

Nếu thông điệp thứ nhất bao gồm nhiều sự kiện giám sát, nói cách khác, thông điệp thứ nhất được sử dụng để tạo cấu hình nhiều sự kiện giám sát cho nhóm người dùng, ví dụ, M sự kiện giám sát, khi số lần nhận báo cáo sự kiện cho mỗi thành viên trong số N thành viên đạt đến số lượng tối đa của các báo cáo, hoặc số lần nhận báo cáo sự kiện giám sát cho mỗi một trong số M sự kiện giám sát của mỗi một trong số N thành viên đạt tới số lượng tối đa của các báo cáo, NEF xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận.

Đăng ký sự kiện giám sát cho nhóm người dùng được xóa bỏ bằng cách sử dụng các bước từ S707 đến S714. Cụ thể là, các bước từ S707 đến S714 là giống với các bước từ S615 đến S622, và các phần lặp lại không được mô tả lại.

Ngoài ra, nếu NEF tạm thời không thực hiện các bước từ S707 đến S714 vì một số lý do, và trong khoảng thời gian này, NEF nhận báo cáo sự kiện giám sát cho yêu cầu đăng ký sự kiện giám sát ở bước S601, NEF dừng hoạt động gửi báo cáo sự kiện giám sát đến SCS/AS.

Tóm lại, theo các phương pháp được thể hiện trên Fig.6A và Fig.6B và Fig.7, trong hệ thống 5G, NEF thu được thông tin thành viên của nhóm người dùng, sao cho khi nhận báo cáo sự kiện giám sát, NEF có thể xác định, dựa trên thông tin thành viên của nhóm người dùng, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận, và có thể tiếp tục xóa bỏ cấu hình sự kiện giám sát cho nhóm người dùng hoặc dừng hoạt động gửi báo cáo sự kiện giám sát đến SCS/AS, nhờ đó tránh được sự lãng phí tài nguyên và giúp đảm bảo sự thực thi

đúng của chính sách tiếp theo sau.

Dựa trên phương pháp giám sát sự kiện được đề xuất theo các phương án nêu trên, như được thể hiện trên Fig.8, phương án thực hiện của sáng chế còn đề xuất thiết bị giám sát sự kiện 800. Thiết bị giám sát sự kiện 800 bao gồm bộ phận nhận 801 và bộ phận xử lý 802.

Thiết bị giám sát sự kiện 800 được tạo cấu hình để thực hiện các bước mà được thực hiện bởi thực thể chức năng lộ diện trong phương pháp giám sát sự kiện được đề xuất theo các phương án nêu trên. Các chi tiết là như sau:

Bộ phận nhận 801 được tạo cấu hình để nhận thông điệp thứ nhất, trong đó thông điệp thứ nhất được sử dụng để tạo cấu hình sự kiện giám sát cho nhóm người dùng.

Bộ phận xử lý 802 được cấu hình để thu được thông tin thành viên của nhóm người dùng, xác định, dựa trên thông tin thành viên, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận, và xóa bỏ cấu hình sự kiện giám sát cho nhóm người dùng; hoặc được cấu hình để thu được thông tin thành viên của nhóm người dùng, và xác định, dựa trên thông tin thành viên, liệu các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng có được hoàn thành không.

Bộ phận nhận 801 và bộ phận xử lý 802 trong thiết bị giám sát sự kiện 800 có thể còn được tạo cấu hình để thực hiện các bước khác tương ứng với thực thể chức năng lộ diện trong phương pháp giám sát sự kiện được đề xuất theo các phương án nêu trên. Các phần lặp lại không được mô tả lại ở đây.

Thiết bị giám sát sự kiện 800 còn được cấu hình để thực hiện các bước mà được thực hiện bởi thực thể quản lý dữ liệu người dùng trong phương pháp giám sát sự kiện được đề xuất theo các phương án nêu trên. Các chi tiết là như sau:

nhận thông điệp yêu cầu thứ nhất, trong đó thông điệp yêu cầu thứ nhất được sử dụng để tạo cấu hình sự kiện giám sát cho nhóm người dùng; và gửi thông điệp hồi đáp thứ nhất đến thực thể chức năng lộ diện, trong đó thông điệp hồi đáp thứ nhất mang thông tin thành viên của nhóm người dùng.

Bộ phận nhận 801 và bộ phận xử lý 802 trong thiết bị giám sát sự kiện 800 có thể còn được tạo cấu hình để thực hiện các bước khác tương ứng với thực thể quản lý

dữ liệu người dùng trong phương pháp giám sát sự kiện được đề xuất theo các phương án nêu trên. Các phần lặp lại không được mô tả lại ở đây.

Thiết bị giám sát sự kiện 800 còn được cấu hình để thực hiện các bước mà được thực hiện bởi thực thể ứng dụng bên thứ ba trong phương pháp giám sát sự kiện được đề xuất theo các phương án nêu trên. Các chi tiết là như sau:

gửi thông điệp thứ nhất đến thực thể chức năng lộ diện, trong đó thông điệp thứ nhất được sử dụng để tạo cấu hình sự kiện giám sát cho nhóm người dùng, và thông điệp thứ nhất mang thông tin thành viên của nhóm người dùng.

Bộ phận nhận 801 và bộ phận xử lý 802 trong thiết bị giám sát sự kiện 800 có thể còn được tạo cấu hình để thực hiện các bước khác tương ứng với thực thể ứng dụng bên thứ ba trong phương pháp giám sát sự kiện được đề xuất theo các phương án nêu trên. Các phần lặp lại không được mô tả lại ở đây.

Dựa trên phương pháp giám sát sự kiện được đề xuất theo các phương án nêu trên, như được thể hiện trên Fig.9, phương án thực hiện của sáng chế còn đề xuất thiết bị giám sát sự kiện 900. Thiết bị giám sát sự kiện 900 được tạo cấu hình để thực hiện các phương pháp giám sát sự kiện nêu trên. Thiết bị giám sát sự kiện 900 bao gồm bộ thu phát 901, bộ xử lý 902, và bộ nhớ 903. Bộ nhớ 903 là tùy chọn. Bộ xử lý 902 được tạo cấu hình để gọi nhóm các chương trình. Khi các chương trình được thực hiện, bộ xử lý 902 thực hiện các phương pháp giám sát sự kiện nêu trên. Bộ nhớ 903 được tạo cấu hình để lưu trữ các chương trình được thực hiện bởi bộ xử lý 902. Trong các môđun chức năng trên Fig.8, bộ phận nhận 801 có thể được thực hiện nhờ sử dụng bộ thu phát 901, và bộ phận xử lý 802 có thể được thực hiện nhờ sử dụng bộ xử lý 902.

Bộ xử lý 902 có thể là bộ xử lý trung tâm (central processing unit, CPU), bộ xử lý mạng (network processor, NP), hoặc sự kết hợp của CPU và NP.

Bộ xử lý 902 có thể còn bao gồm chip phần cứng. Chip phần cứng có thể là mạch tích hợp chuyên dụng (application-specific integrated circuit, ASIC), thiết bị lôgic lập trình được (programmable logic device, PLD), hoặc sự kết hợp của chúng. PLD có thể là thiết bị lôgic lập trình được phức tạp (complex programmable logic device, CPLD), mảng cổng lập trình được dạng trường (field-programmable gate array, FPGA), mảng logic chung (generic array logic, GAL), hoặc sự kết hợp bất kỳ

của chúng.

Bộ nhớ 903 có thể bao gồm bộ nhớ khả biến (volatile memory), như bộ nhớ truy nhập ngẫu nhiên (random-access memory, RAM); hoặc bộ nhớ 903 có thể bao gồm bộ nhớ bất khả biến (non-volatile memory), như bộ nhớ tác động nhanh (flash memory), ổ đĩa cứng (hard disk drive, HDD), hoặc ổ cứng thể rắn (solid-state drive, SSD); hoặc bộ nhớ 903 có thể bao gồm sự kết hợp của các loại bộ nhớ nêu trên.

Để thực hiện chức năng của thiết bị được mô tả trên Fig.8, hoặc Fig.9, phương án thực hiện của sáng chế còn đề xuất chip, bao gồm bộ xử lý, được tạo cấu hình để hỗ trợ thiết bị trong việc thực hiện chức năng liên quan đến thực thể chức năng lộ diện, thực thể quản lý dữ liệu người dùng, hoặc thực thể ứng dụng bên thứ ba trong các phương pháp giám sát sự kiện nêu trên. Theo phương án có thể có, chip được kết nối với bộ nhớ hoặc chip bao gồm bộ nhớ, và bộ nhớ được tạo cấu hình để lưu trữ lệnh chương trình và dữ liệu mà cần thiết cho thiết bị.

Phương án thực hiện của sáng chế đề xuất phương tiện lưu trữ máy tính để lưu trữ chương trình máy tính, và chương trình máy tính được sử dụng để thực hiện các phương pháp giám sát sự kiện nêu trên.

Phương án thực hiện của sáng chế đề xuất sản phẩm chương trình máy tính chứa lệnh. Khi sản phẩm chương trình máy tính chạy trên máy tính, máy tính được phép thực hiện các phương pháp giám sát sự kiện nêu trên.

Người có kiến thức trung bình trong lĩnh vực cần hiểu rằng các phương án của sáng chế là có thể được thực hiện dưới dạng phương pháp, hệ thống, hoặc sản phẩm chương trình máy tính. Do đó, sáng chế có thể được thực hiện chỉ bằng phần cứng, chỉ bằng phần mềm, hoặc kết hợp phần mềm và phần cứng. Ngoài ra, sáng chế có thể sử dụng dạng sản phẩm chương trình máy tính mà được thực hiện trên một hoặc nhiều phương tiện lưu trữ có thể sử dụng bằng máy tính (bao gồm nhưng không bị giới hạn ở bộ nhớ đĩa từ, CD-ROM, bộ nhớ quang, và tương tự) mà chứa mã chương trình sử dụng được bằng máy tính.

Sáng chế được mô tả tham chiếu đến các lưu đồ và/hoặc các sơ đồ khối của phương pháp, thiết bị (hệ thống), và sản phẩm chương trình máy tính theo các phương án thực hiện sáng chế. Cần hiểu rằng các chỉ dẫn chương trình máy tính có thể được dùng để thực hiện mỗi tiến trình và/hoặc mỗi khối của các lưu đồ và/hoặc

các sơ đồ khối và tổ hợp của tiến trình và/hoặc khối của các lưu đồ và/hoặc các sơ đồ khối này. Các chỉ dẫn chương trình máy tính này có thể được cung cấp cho máy tính thông dụng, máy tính chuyên dụng, bộ xử lý kiểu nhúng, hoặc bộ xử lý của thiết bị xử lý dữ liệu lập trình được khác để tạo ra một bộ máy, để các chỉ dẫn mà được thực thi bởi máy tính hoặc bộ xử lý của thiết bị xử lý dữ liệu lập trình được khác này tạo ra thiết bị để thực hiện chức năng cụ thể trong một hoặc nhiều tiến trình của các lưu đồ và/hoặc ở một hoặc nhiều khối của các sơ đồ khối này.

Các lệnh chương trình máy tính này có thể được chứa trong bộ nhớ có thể đọc bằng máy tính mà có thể ra lệnh cho máy tính hoặc thiết bị xử lý dữ liệu khác để làm việc theo cách cụ thể, sao cho các lệnh chứa trong bộ nhớ có thể đọc bằng máy tính tạo ra artifact mà chứa thiết bị ra lệnh. Thiết bị chỉ dẫn này thực hiện chức năng cụ thể trong một hoặc nhiều tiến trình trên các lưu đồ và/hoặc ở một hoặc nhiều khối trong các sơ đồ khối này.

Các lệnh chương trình máy tính này cũng có thể được nạp vào máy tính hoặc thiết bị xử lý dữ liệu lập trình được khác, sao cho chuỗi hoạt động và bước được thực hiện trên máy tính hoặc thiết bị lập trình được khác, nhờ đó tạo ra quá trình được thực hiện bởi máy tính. Do đó, các lệnh được thực hiện trên máy tính hoặc thiết bị lập trình được khác sẽ tạo ra các bước để thực hiện chức năng cụ thể trong một hoặc nhiều quy trình trên các lưu đồ và/hoặc trong một hoặc nhiều khối trong các sơ đồ khối.

Mặc dù một số phương án thực hiện của sáng chế đã được mô tả, người có hiểu biết trung bình trong lĩnh vực tương ứng có thể tạo ra các thay đổi và các biến thể cho các phương án thực hiện này khi họ nắm được ý tưởng sáng tạo cơ bản. Do đó, các điểm yêu cầu bảo hộ sau đây được dự tính là được hiểu bao trùm các phương án thực hiện ưu tiên và tất cả thay đổi và các biến thể nằm bên trong phạm vi của sáng chế.

Rõ ràng là, người có hiểu biết trung bình trong lĩnh vực có thể tạo ra các phương án cải biến và biến thể khác nhau cho các phương án thực hiện của sáng chế mà không nằm ngoài phạm vi của các phương án thực hiện của sáng chế. Sáng chế bao trùm các phương án cải biến và biến thể này, chừng nào mà chúng nằm trong phạm vi bảo hộ được xác định bởi các điểm yêu cầu bảo hộ sau đây và các công

nghệ tương đương của chúng.

YÊU CẦU BẢO HỘ

1. Phương pháp giám sát sự kiện, bao gồm các bước:

nhận (301), bởi thực thể chức năng lộ diện, thông điệp thứ nhất, trong đó thông điệp thứ nhất được sử dụng để yêu cầu việc cấu hình sự kiện giám sát cho nhóm người dùng;

thu được (302), bởi thực thể chức năng lộ diện, thông tin thành viên của nhóm người dùng, trong đó thông tin thành viên của nhóm người dùng bao gồm: số lượng N của các thành viên trong nhóm người dùng;

xác định (303), bởi thực thể chức năng lộ diện dựa trên thông tin thành viên, liệu các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng có được nhận không, và

khi thực thể chức năng lộ diện xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận, xóa bỏ (304), bởi thực thể chức năng lộ diện, cấu hình sự kiện giám sát cho nhóm người dùng.

2. Phương pháp theo điểm 1, trong đó bước thu được, bởi thực thể chức năng lộ diện, thông tin thành viên của nhóm người dùng bao gồm:

thu được, bởi thực thể chức năng lộ diện, thông tin thành viên từ thông điệp thứ nhất, trong đó thông điệp thứ nhất mang thông tin thành viên của nhóm người dùng; hoặc

thu được, bởi thực thể chức năng lộ diện, thông tin thành viên của nhóm người dùng từ thực thể quản lý dữ liệu người dùng.

3. Phương pháp theo điểm 1 hoặc 2, trong đó bước xác định, bởi thực thể chức năng lộ diện dựa trên thông tin thành viên, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận bao gồm:

nếu thông điệp thứ nhất được sử dụng để tạo cấu hình yêu cầu giám sát một lần cho nhóm người dùng, thì xác định, bởi thực thể chức năng lộ diện khi nhận các báo cáo sự kiện giám sát cho N thành viên, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận.

4. Phương pháp theo điểm 3, trong đó bước xác định, bởi thực thể chức năng lộ diện dựa trên thông tin thành viên, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận bao gồm:

nếu thông điệp thứ nhất được sử dụng để tạo cấu hình các sự kiện giám sát cho nhóm người dùng, xác định, bởi thực thể chức năng lộ diện khi nhận báo cáo sự kiện giám sát của mỗi sự kiện trong số các sự kiện giám sát cho mỗi thành viên trong số N thành viên, rằng các báo cáo sự kiện giám sát cho tất cả các người dùng trong nhóm người dùng được nhận.

5. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 4, trong đó bước xóa bỏ, bởi thực thể chức năng lộ diện, cấu hình sự kiện giám sát cho nhóm người dùng bao gồm ít nhất một trong số các hoạt động sau đây:

xóa bỏ, bởi thực thể chức năng lộ diện, cấu hình sự kiện giám sát được lưu trữ cục bộ cho nhóm người dùng; hoặc

gửi, bởi thực thể chức năng lộ diện, thông điệp thứ hai đến thực thể quản lý dữ liệu người dùng, trong đó thông điệp thứ hai được sử dụng để ra lệnh cho thực thể quản lý dữ liệu người dùng xóa cấu hình sự kiện giám sát cho nhóm người dùng; hoặc

gửi, bởi thực thể chức năng lộ diện, thông điệp thứ ba đến thực thể ứng dụng bên thứ ba, trong đó thông điệp thứ ba được sử dụng để ra lệnh cho thực thể ứng dụng bên thứ ba xóa cấu hình sự kiện giám sát cho nhóm người dùng.

6. Phương pháp theo điểm 1, 2, 3 hoặc 5, trong đó bước xác định, bởi thực thể chức năng lộ diện dựa trên thông tin thành viên, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận bao gồm:

nếu thông điệp thứ nhất bao gồm số lượng tối đa thứ hai của các báo cáo, xác định, bởi thực thể chức năng lộ diện khi số lần nhận báo cáo sự kiện giám sát cho mỗi thành viên trong số N thành viên đạt đến số lượng tối đa thứ hai của các báo cáo, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận.

7. Thiết bị giám sát sự kiện được tạo cấu hình trong thực thể chức năng lộ diện, bao gồm:

bộ phận nhận, được tạo cấu hình để nhận (301) thông điệp thứ nhất, trong đó thông điệp thứ nhất được sử dụng để yêu cầu việc cấu hình sự kiện giám sát cho nhóm người dùng; và

cụm xử lý, được tạo cấu hình để:

thu được (302) thông tin thành viên của nhóm người dùng, trong đó thông tin thành viên của nhóm người dùng bao gồm: số lượng N của các thành viên trong nhóm người dùng;

xác định (303), dựa trên thông tin thành viên, liệu các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng có được nhận không, và

khi xác định được rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận, xóa bỏ (304) cấu hình sự kiện giám sát cho nhóm người dùng.

8. Thiết bị theo điểm 7, trong đó bộ phận xử lý được tạo cấu hình cụ thể để:

thu được thông tin thành viên từ thông điệp thứ nhất, trong đó thông điệp thứ nhất mang thông tin thành viên của nhóm người dùng; hoặc

thu được thông tin thành viên của nhóm người dùng từ thực thể quản lý dữ liệu người dùng.

9. Thiết bị theo điểm 7 hoặc 8, trong đó cụm xử lý được tạo cấu hình cụ thể để:

nếu thông điệp thứ nhất được sử dụng để tạo cấu hình yêu cầu giám sát một lần cho nhóm người dùng, thì xác định, khi nhận các báo cáo sự kiện giám sát cho N thành viên, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận.

10. Thiết bị theo điểm 9, trong đó bộ phận xử lý được tạo cấu hình cụ thể để:

nếu thông điệp thứ nhất được sử dụng để tạo cấu hình các sự kiện giám sát cho nhóm người dùng, thì xác định, khi nhận báo cáo sự kiện giám sát của mỗi sự kiện

trong số các sự kiện giám sát cho mỗi thành viên trong số N thành viên, rằng các báo cáo sự kiện giám sát cho tất cả các người dùng trong nhóm người dùng được nhận.

11. Thiết bị theo điểm bất kỳ trong số các điểm từ 7 đến 10, trong đó khi xóa bỏ cấu hình sự kiện giám sát cho nhóm người dùng, bộ phận xử lý thực hiện cụ thể ít nhất một trong số các hoạt động sau đây:

xóa bỏ cấu hình sự kiện giám sát được lưu trữ cục bộ cho nhóm người dùng; hoặc

gửi thông điệp thứ hai đến thực thể quản lý dữ liệu người dùng, trong đó thông điệp thứ hai được sử dụng để ra lệnh cho thực thể quản lý dữ liệu người dùng xóa cấu hình sự kiện giám sát cho nhóm người dùng; hoặc

gửi thông điệp thứ ba đến thực thể ứng dụng bên thứ ba, trong đó thông điệp thứ ba được sử dụng để ra lệnh cho thực thể ứng dụng bên thứ ba xóa cấu hình sự kiện giám sát cho nhóm người dùng.

12. Thiết bị theo điểm bất kỳ trong số các điểm 7, 8 hoặc 11, trong đó cụm xử lý được tạo cấu hình cụ thể để:

nếu thông điệp thứ nhất bao gồm số lượng tối đa thứ hai của các báo cáo, xác định, khi số lần nhận báo cáo sự kiện giám sát cho mỗi thành viên trong số N thành viên đạt đến số lượng tối đa thứ hai của các báo cáo, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận.

13. Phương tiện lưu trữ đọc được bằng máy tính, để lưu trữ các lệnh mà, khi được thực thi bởi thực thể chức năng lộ diện, khiến cho thực thể chức năng lộ diện thực hiện các bước theo điểm bất kỳ trong số các điểm từ 1 đến 6.

14. Chip được tạo cấu hình trong thực thể chức năng lộ diện, trong đó chip được nối với bộ nhớ hoặc chip bao gồm bộ nhớ, và trong đó chip được tạo cấu hình để đọc và thực thi chương trình phần mềm được lưu trữ trong bộ nhớ, để thực hiện các phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 6.

15. Hệ thống giám sát sự kiện, bao gồm: thiết bị giám sát sự kiện theo điểm bất kỳ trong số các điểm từ 7 đến 12, và thực thể quản lý dữ liệu người dùng,
trong đó thực thể quản lý dữ liệu người dùng được tạo cấu hình để gửi thông tin thành viên của nhóm người dùng tới thiết bị giám sát sự kiện; và
trong đó cụm xử lý của thiết bị giám sát sự kiện được tạo cấu hình để thu được thông tin thành viên của nhóm người dùng từ thực thể quản lý dữ liệu người dùng.

16. Hệ thống theo điểm 15, trong đó hệ thống này còn bao gồm: máy chủ có khả năng phục vụ hoặc máy chủ ứng dụng, được tạo cấu hình để gửi thông điệp thứ nhất tới thiết bị giám sát sự kiện.

17. Phương pháp giám sát sự kiện, bao gồm các bước:
nhận (301), bởi thực thể chức năng lộ diện, thông điệp thứ nhất, trong đó thông điệp thứ nhất được sử dụng để yêu cầu việc cấu hình sự kiện giám sát cho nhóm người dùng;
gửi, bởi thực thể quản lý dữ liệu người dùng, thông tin thành viên của nhóm người dùng tới thực thể chức năng lộ diện;
thu được (302), bởi thực thể chức năng lộ diện, thông tin thành viên của nhóm người dùng từ thực thể quản lý dữ liệu người dùng, trong đó thông tin thành viên của nhóm người dùng bao gồm: số lượng N của các thành viên trong nhóm người dùng; xác định (303), bởi thực thể chức năng lộ diện dựa trên thông tin thành viên, liệu các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng có được nhận không, và
khi thực thể chức năng lộ diện xác định rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận, xóa bỏ (304), bởi thực thể chức năng lộ diện, cấu hình sự kiện giám sát cho nhóm người dùng.

18. Phương pháp theo điểm 17, trong đó phương pháp còn bao gồm bước:
gửi, bởi máy chủ có khả năng phục vụ hoặc máy chủ ứng dụng, thông điệp thứ nhất tới thực thể chức năng lộ diện.

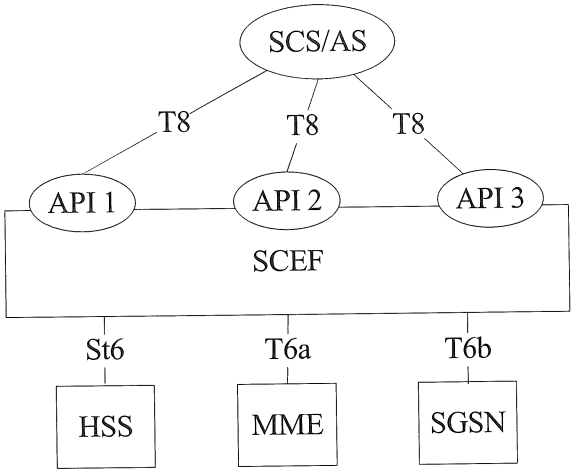
SCS/AS
T8
T8
T8
API 1
API 2
API 3
SCEF
St6
T6a
T6b
HSS
MME
SGSN

FIG. 1

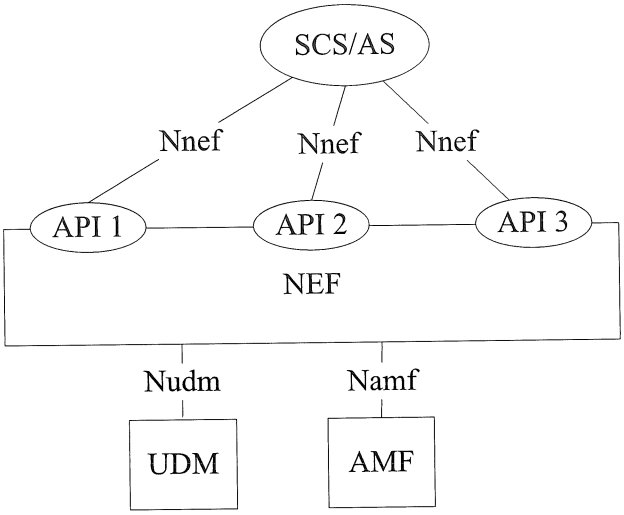
SCS/AS
Nnef
Nnef
Nnef
API 1
API 2
API 3
NEF
Nudm
Namf
UDM
AMF

FIG. 2

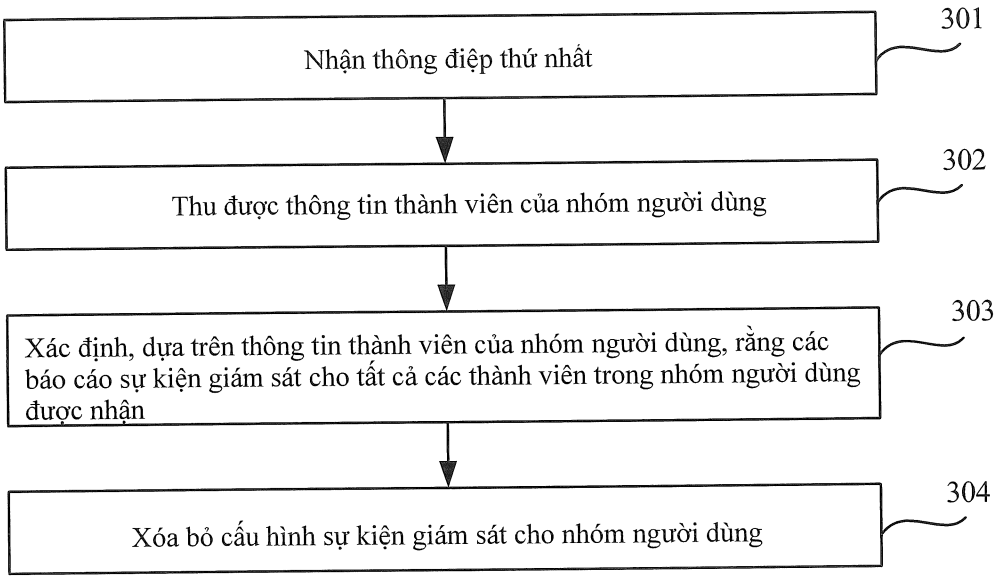
Nhận thông điệp thứ nhất
301
Thu được thông tin thành viên của nhóm người dùng
302
Xác định, dựa trên thông tin thành viên của nhóm người dùng, rằng các báo cáo sự kiện giám sát cho tất cả các thành viên trong nhóm người dùng được nhận
303
Xóa bỏ cấu hình sự kiện giám sát cho nhóm người dùng
304

FIG. 3

3/8

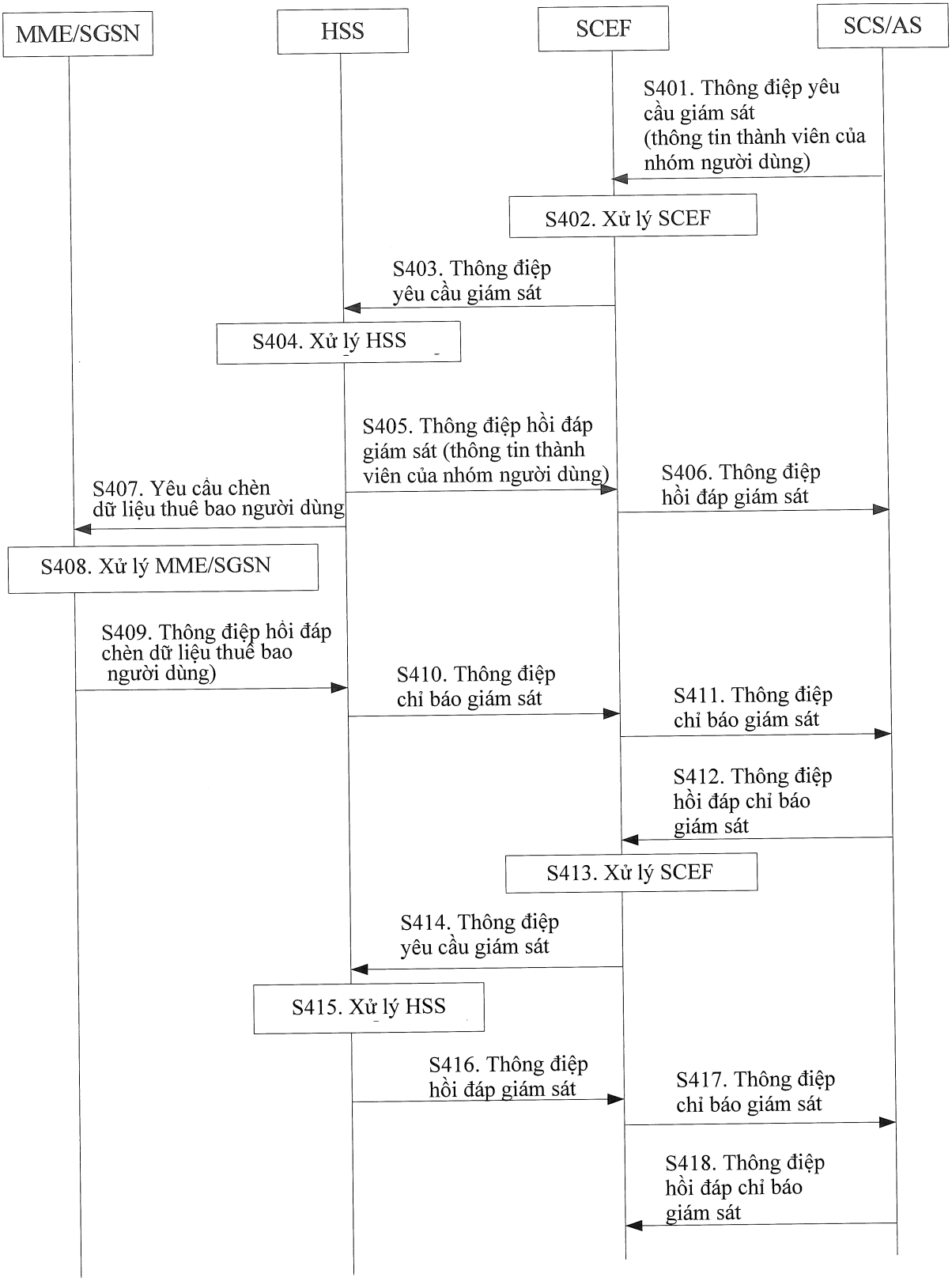
MME/SGSN
HSS
SCEF
SCS/AS
S401. Thông điệp yêu cầu giám sát (thông tin thành viên của nhóm người dùng)
S402. Xử lý SCEF
S403. Thông điệp yêu cầu giám sát
S404. Xử lý HSS
S405. Thông điệp hồi đáp giám sát (thông tin thành viên của nhóm người dùng)
S406. Thông điệp hồi đáp giám sát
S407. Yêu cầu chèn dữ liệu thuê bao người dùng
S408. Xử lý MME/SGSN
S409. Thông điệp hồi đáp chèn dữ liệu thuê bao người dùng)
S410. Thông điệp chỉ báo giám sát
S411. Thông điệp chỉ báo giám sát
S412. Thông điệp hồi đáp chỉ báo giám sát
S413. Xử lý SCEF
S414. Thông điệp yêu cầu giám sát
S415. Xử lý HSS
S416. Thông điệp hồi đáp giám sát
S417. Thông điệp chỉ báo giám sát
S418. Thông điệp hồi đáp chỉ báo giám sát

FIG. 4

4/8

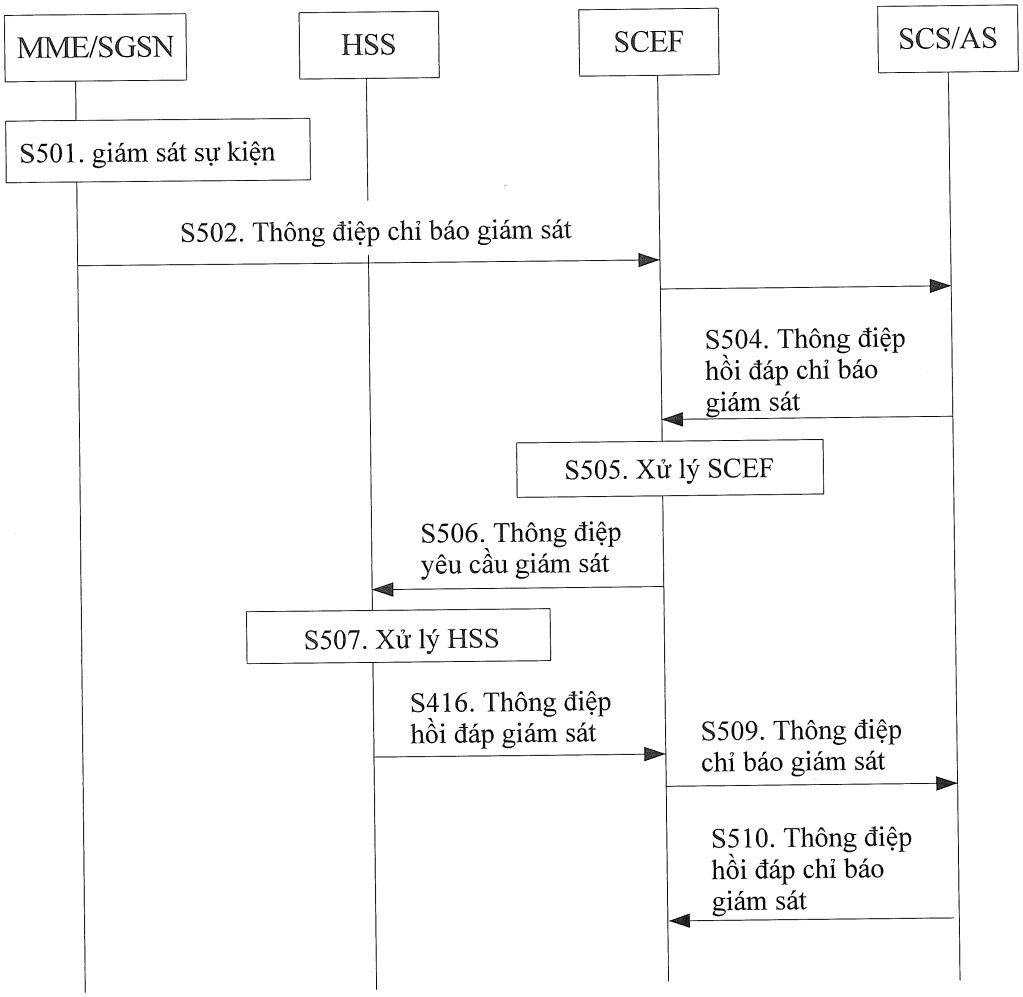
MME/SGSN
HSS
SCEF
SCS/AS
S501. giám sát sự kiện
S502. Thông điệp chỉ báo giám sát
S504. Thông điệp hồi đáp chỉ báo giám sát
S505. Xử lý SCEF
S506. Thông điệp yêu cầu giám sát
S507. Xử lý HSS
S416. Thông điệp hồi đáp giám sát
S509. Thông điệp chỉ báo giám sát
S510. Thông điệp hồi đáp chỉ báo giám sát

FIG. 5

5/8

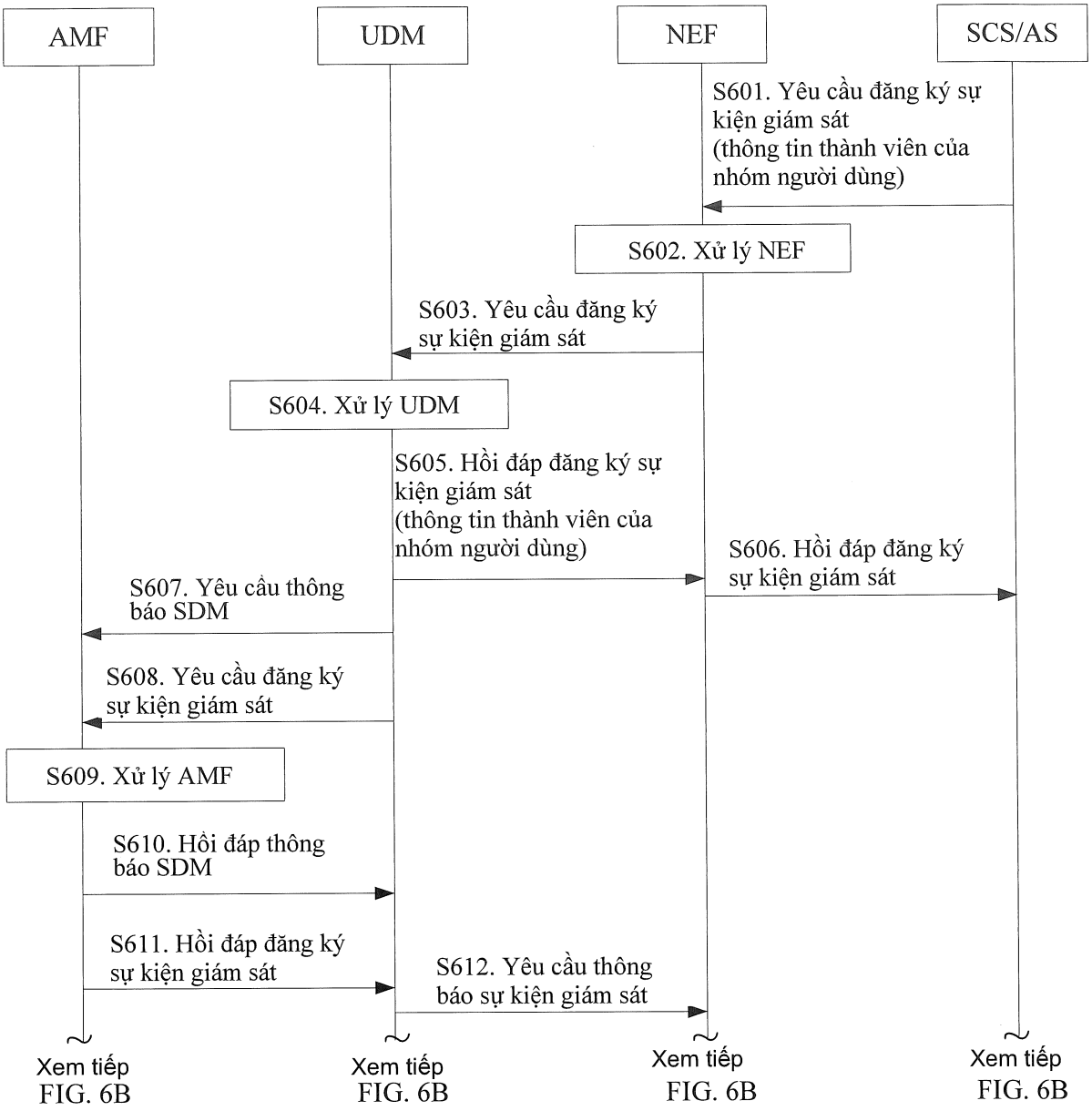
AMF
UDM
NEF
SCS/AS
S601. Yêu cầu đăng ký sự kiện giám sát (thông tin thành viên của nhóm người dùng)
S602. Xử lý NEF
S603. Yêu cầu đăng ký sự kiện giám sát
S604. Xử lý UDM
S605. Hồi đáp đăng ký sự kiện giám sát (thông tin thành viên của nhóm người dùng)
S606. Hồi đáp đăng ký sự kiện giám sát
S607. Yêu cầu thông báo SDM
S608. Yêu cầu đăng ký sự kiện giám sát
S609. Xử lý AMF
S610. Hồi đáp thông báo SDM
S611. Hồi đáp đăng ký sự kiện giám sát
S612. Yêu cầu thông báo sự kiện giám sát
Xem tiếp FIG. 6B
Xem tiếp FIG. 6B
Xem tiếp FIG. 6B
Xem tiếp FIG. 6B

FIG. 6A

6/8

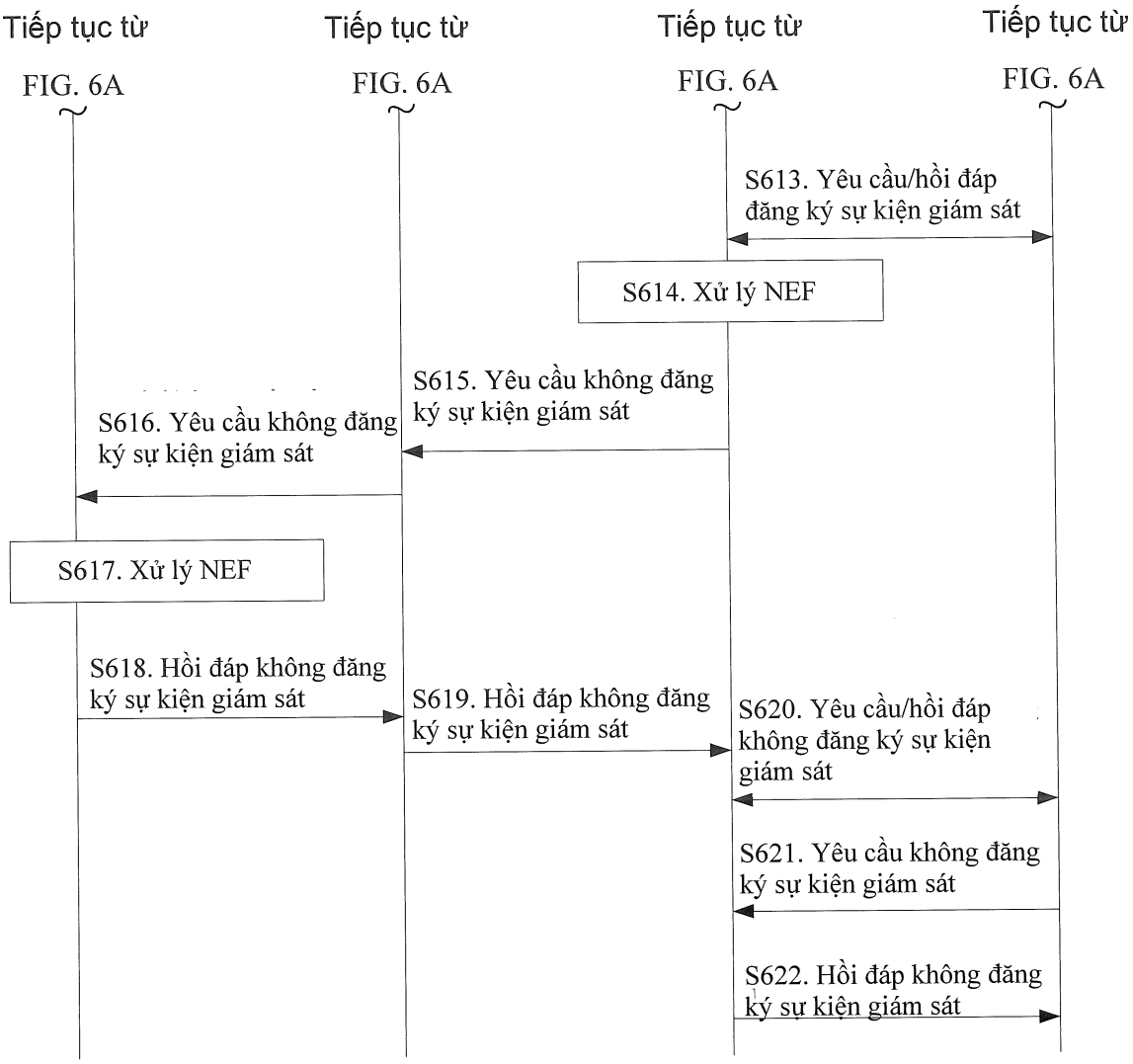
Tiếp tục từ FIG. 6A
Tiếp tục từ FIG. 6A
Tiếp tục từ FIG. 6A
Tiếp tục từ FIG. 6A
S613. Yêu cầu/hồi đáp đăng ký sự kiện giám sát
S614. Xử lý NEF
S615. Yêu cầu không đăng ký sự kiện giám sát
S616. Yêu cầu không đăng ký sự kiện giám sát
S617. Xử lý NEF
S618. Hồi đáp không đăng ký sự kiện giám sát
S619. Hồi đáp không đăng ký sự kiện giám sát
S620. Yêu cầu/hồi đáp không đăng ký sự kiện giám sát
S621. Yêu cầu không đăng ký sự kiện giám sát
S622. Hồi đáp không đăng ký sự kiện giám sát

FIG. 6B

7/8

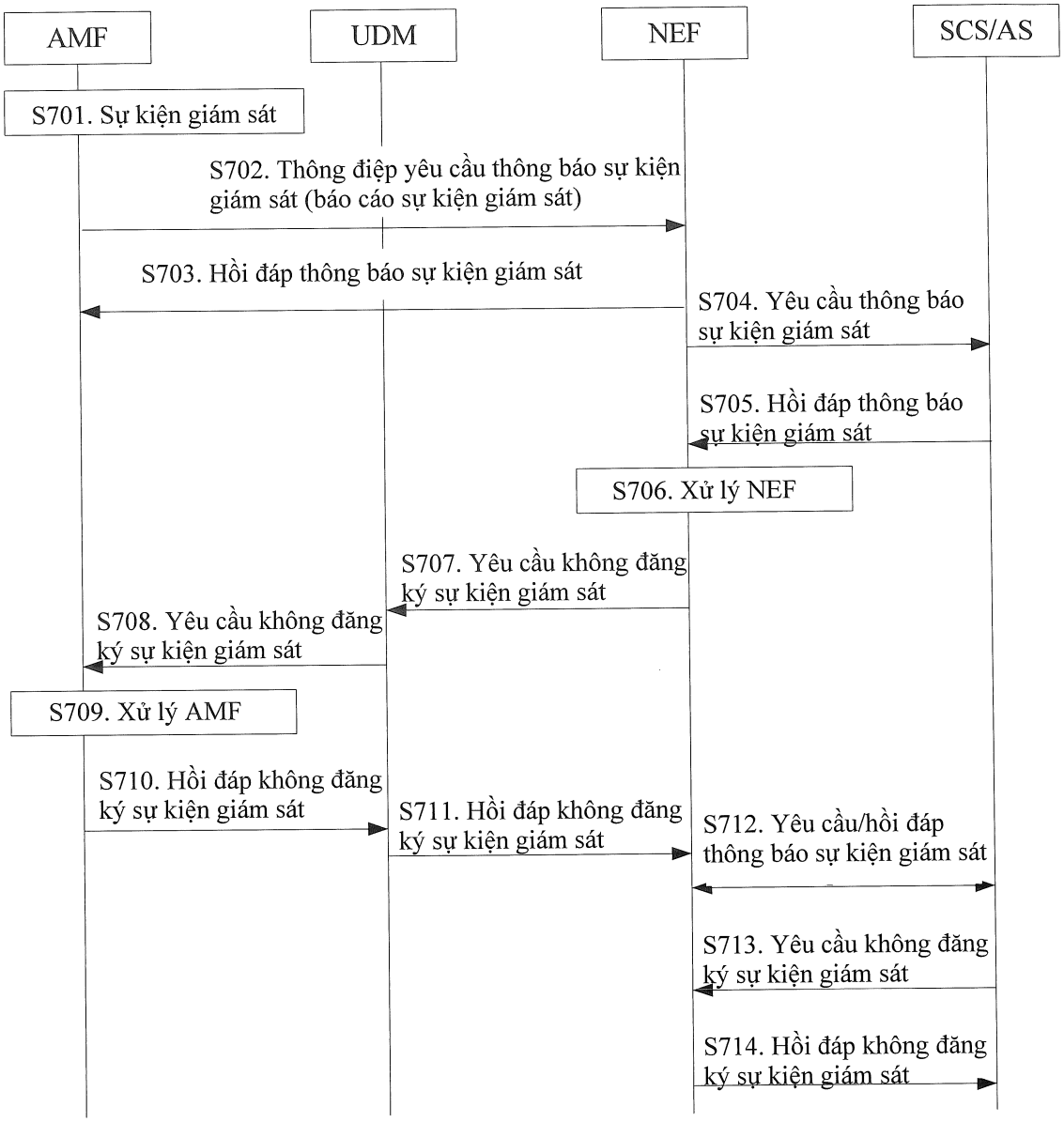
AMF
UDM
NEF
SCS/AS
S701. Sự kiện giám sát
S702. Thông điệp yêu cầu thông báo sự kiện giám sát (báo cáo sự kiện giám sát)
S703. Hồi đáp thông báo sự kiện giám sát
S704. Yêu cầu thông báo sự kiện giám sát
S705. Hồi đáp thông báo sự kiện giám sát
S706. Xử lý NEF
S707. Yêu cầu không đăng ký sự kiện giám sát
S708. Yêu cầu không đăng ký sự kiện giám sát
S709. Xử lý AMF
S710. Hồi đáp không đăng ký sự kiện giám sát
S711. Hồi đáp không đăng ký sự kiện giám sát
S712. Yêu cầu/hồi đáp thông báo sự kiện giám sát
S713. Yêu cầu không đăng ký sự kiện giám sát
S714. Hồi đáp không đăng ký sự kiện giám sát

FIG. 7

8/8

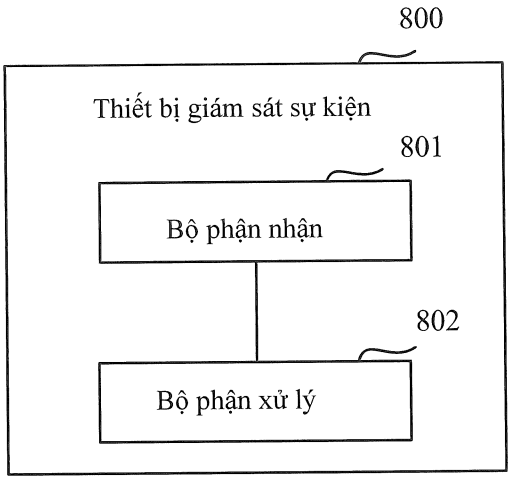
800
Thiết bị giám sát sự kiện
801
Bộ phận nhận
802
Bộ phận xử lý

FIG. 8

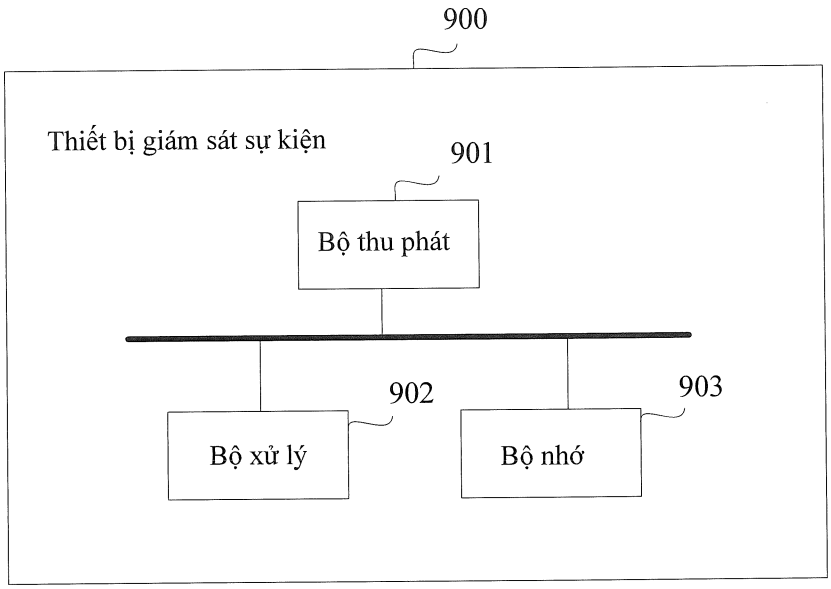
900
Thiết bị giám sát sự kiện
901
Bộ thu phát
902
Bộ xử lý
903
Bộ nhớ

FIG. 9