(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) **1-0041990**

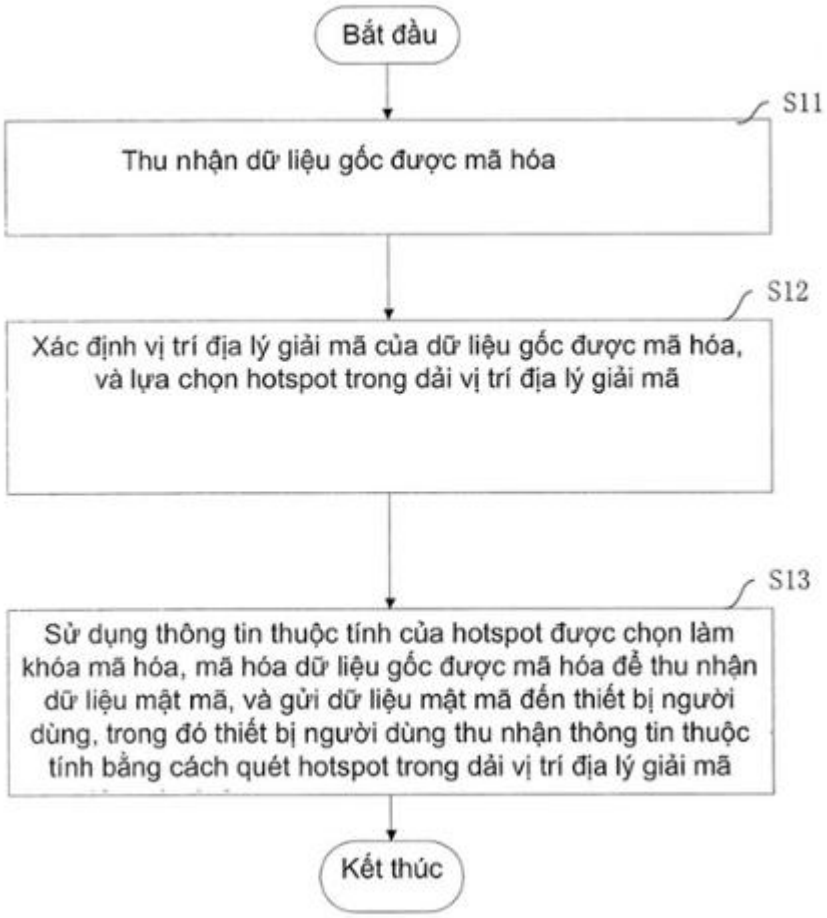
(51)[7] **H04L 12/28**

(13) **B**

(21) 1-2019-07121
(22) 17/05/2018
(86) PCT/CN2018/087230 17/05/2018
(87) WO/2018/210288 22/11/2018
(30) 201710350737.X 18/05/2017 CN
(45) 25/12/2024 441
(43) 25/05/2020 386
(73) Shanghai lianshang Network Technology Co., Ltd. (CN)
2F, No. 979 Yunhan Road, Nicheng Town, Pudong Shanghai 201306, China
(72) ZHENG, Xiaoping (CN).
(74) Công ty TNHH Sở hữu trí tuệ Thảo Thọ Quyến (INVENCO.,LTD)

(54) PHƯƠNG PHÁP TRUYỀN DỮ LIỆU TRÊN THIẾT BỊ MẠNG

(57) Sáng chế đề cập đến phương pháp và thiết bị để truyền dữ liệu, bao gồm: thu nhận dữ liệu gốc được mã hóa trên thiết bị mạng; xác định vị trí địa lý giải mã của dữ liệu gốc được mã hóa, và chọn hotspot trong dải vị trí địa lý giải mã; sau đó, sử dụng thông tin thuộc tính của hotspot được chọn như khóa mã hóa để mã hóa dữ liệu gốc được mã hóa, và thu nhận dữ liệu mật mã và gửi dữ liệu mật mã đến thiết bị người dùng. Thiết bị người dùng thu nhận thông tin thuộc tính bằng cách quét hotspot trong dải vị trí địa lý giải mã. Sáng chế thực hiện mã hóa dữ liệu gốc dựa trên vị trí địa lý giải mã thực tế được sử dụng như khóa mã hóa dữ liệu gốc được mã hóa. Do đó, dữ liệu gốc được gửi an toàn đến thiết bị người dùng, ngăn ngừa người sử dụng bất hợp pháp bẻ khóa mã hóa và thu nhận dữ liệu gốc tại các vị trí khác.


Bắt đầu
S11
Thu nhận dữ liệu gốc được mã hóa
S12
Xác định vị trí địa lý giải mã của dữ liệu gốc được mã hóa, và lựa chọn hotspot trong dải vị trí địa lý giải mã
S13
Sử dụng thông tin thuộc tính của hotspot được chọn làm khóa mã hóa, mã hóa dữ liệu gốc được mã hóa để thu nhận dữ liệu mật mã, và gửi dữ liệu mật mã đến thiết bị người dùng, trong đó thiết bị người dùng thu nhận thông tin thuộc tính bằng cách quét hotspot trong dải vị trí địa lý giải mã
Kết thúc

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực máy tính. Cụ thể hơn, sáng chế đề cập đến phương pháp và thiết bị để truyền dữ liệu.

Tình trạng kỹ thuật của sáng chế

Trong kỹ thuật đã biết, quá trình truyền dữ liệu dựa trên quy trình định trước, và thông tin dữ liệu được gửi đến thiết bị đầu cuối của người dùng thông qua liên kết đơn hoặc nhiều liên kết. Nhằm đảm bảo sự an toàn của dữ liệu trong quá trình truyền dữ liệu, kỹ thuật đã biết thực hiện mã hóa trên dữ liệu được truyền đi để thu nhận gói dữ liệu được mã hóa gói và sau đó gói dữ liệu được mã hóa được gửi đến thiết bị đầu cuối của người dùng. Sau đó, thiết bị đầu cuối của người dùng giải mã gõi dữ liệu được mã hóa dựa trên thuật toán giải mã cài đặt sẵn, do đó thu nhận dữ liệu gốc được truyền, và đảm bảo sự an toàn của dữ liệu trong quá trình truyền. Tuy nhiên, trong các kỹ thuật trước đây, có nhiều người sử dụng bất hợp pháp đã thâm nhập vào kênh truyền dữ liệu và chặn các gói dữ liệu được mã hóa và thuật toán giải mã, để thu nhận dữ liệu gốc trong quá trình truyền với sự trợ giúp của dữ liệu mã hóa thu được bất hợp pháp và thuật toán giải mã, từ đó đặt ra vấn đề về bảo mật tiềm tàng và nguy cơ vi phạm dữ liệu trong quá trình truyền.

Bản chất kỹ thuật của sáng chế

Đối tượng của sáng chế là cung cấp phương pháp và thiết bị để truyền dữ liệu để giải quyết vấn đề về bảo mật tiềm tàng và nguy cơ rò rỉ dữ liệu trong quá trình truyền dữ liệu trong kỹ thuật trước đây.

Theo khía cạnh đầu tiên, sáng chế cung cấp phương pháp truyền dữ liệu trên thiết bị mạng, phương pháp này bao gồm:

thu nhận dữ liệu gốc được mã hóa;

xác định vị trí địa lý giải mã của dữ liệu gốc được mã hóa, và chọn hotspot trong dải vị trí địa lý giải mã; và

sử dụng thông tin thuộc tính của hotspot được chọn là khóa mã hóa, mã hóa dữ liệu gốc được mã hóa để thu nhận dữ liệu mật mã, và gửi dữ liệu mật mã đến thiết bị người dùng, trong đó thiết bị người dùng thu nhận thông tin thuộc tính bằng cách quét hotspot trong dải vị trí địa lý giải mã.

Hơn nữa, theo phương pháp này, thông tin thuộc tính bao gồm địa chỉ vật lý của hotspot được chọn.

Hơn nữa, theo phương pháp này, thông tin thuộc tính bao gồm địa chỉ vật lý của hotspot được lựa chọn và thông tin nhận dạng người sử dụng của thiết bị người dùng thuộc hotspot được chọn.

Hơn nữa, theo phương pháp này, bước xác định vị trí địa lý giải mã của dữ liệu gốc được mã hóa bao gồm:

xác định vị trí địa lý trong khoảng cách định trước từ vị trí địa lý hiện tại của thiết bị người dùng như là vị trí địa lý giải mã của dữ liệu gốc được mã hóa; hoặc

xác định vị trí địa lý giải mã của dữ liệu gốc được mã hóa theo lịch sử di chuyển địa lý của thiết bị người dùng.

Hơn nữa, theo phương pháp này, khi dữ liệu gốc được mã hóa được mã hóa tiếp để thu nhận dữ liệu mật mã và dữ liệu mật mã được gửi đến thiết bị người dùng, phương pháp còn bao gồm:

gửi tên hotspot tương ứng với hotspot được chọn cho thiết bị người dùng.

Hơn nữa, theo phương pháp này, bước sử dụng thông tin thuộc tính của hotspot được chọn là khóa mã hóa, mã hóa dữ liệu gốc được mã hóa để thu nhận dữ liệu mật mã, và gửi dữ liệu mật mã đến thiết bị người dùng bao gồm:

sử dụng thông tin thuộc tính tương ứng với hotspot được chọn như khóa mã hóa, mã hóa dữ liệu gốc được mã hóa dựa trên thuật toán mã hóa cài sẵn và khóa mã hóa để thu nhận dữ liệu mật mã, và gửi dữ liệu mật mã đến thiết bị người dùng.

Hơn nữa, theo phương pháp này, dữ liệu gốc bao gồm ít nhất một trong số sau:

thông tin dữ liệu thích hợp của hotspot;

thông tin thuộc tính người dùng của thiết bị người dùng; và

thông tin dữ liệu kinh doanh được lưu trữ trong thiết bị mạng.

Hơn nữa, theo phương pháp này, khi dữ liệu gốc được mã hóa được mã hóa nữa để thu nhận dữ liệu mật mã và dữ liệu mật mã được gửi đến thiết bị người dùng, phương pháp còn bao gồm:

gửi thuật toán giải mã hóa cài sẵn đến thiết bị người dùng.

Theo khía cạnh thứ hai, sáng chế cung cấp phương pháp truyền dữ liệu trên thiết bị mạng, phương pháp này bao gồm:

thu nhận yêu cầu truy vấn dữ liệu được gửi bởi thiết bị người dùng, trong đó yêu cầu truy vấn dữ liệu bao gồm thông tin thuộc tính hotspot được chọn quét và thu nhận bằng thiết bị người dùng trong dải vị trí địa lý giải mã hiện tại; và

thu nhận dữ liệu gốc được mã hóa dựa trên yêu cầu truy vấn dữ liệu, sử dụng thông tin thuộc tính của hotspot được chọn như khóa mã hóa để mã hóa dữ liệu gốc, thu nhận dữ liệu mật mã, và gửi dữ liệu mật mã này đến thiết bị người dùng.

Theo khía cạnh thứ ba, sáng chế cung cấp phương pháp thu nhận dữ liệu trên thiết bị người dùng, phương pháp này bao gồm:

nhận dữ liệu mật mã được gửi bởi thiết bị mạng;

thu nhận thông tin thuộc tính của hotspot được quét trong dải vị trí địa lý giải mã; và

sử dụng thông tin thuộc tính của hotspot được quét như khóa mã hóa, và giải mã dữ liệu mật mã để thu nhận dữ liệu gốc.

Hơn nữa, theo phương pháp này, thông tin thuộc tính bao gồm địa chỉ vật lý của hotspot được chọn.

Hơn nữa, theo phương pháp này, thông tin thuộc tính bao gồm địa chỉ vật lý của hotspot được chọn và thông tin nhận dạng người dùng của thiết bị người dùng thuộc hotspot được chọn.

Hơn nữa, theo phương pháp này, vị trí địa lý giải mã bao gồm:

vị trí địa lý của thiết bị người dùng sau khi thiết bị người dùng di chuyển khoảng cách định sẵn; và

vị trí địa lý trong lịch sử di chuyển địa lý của thiết bị người dùng.

Hơn nữa, theo phương pháp này, khi dữ liệu mật mã được gửi bởi thiết bị mạng được nhận, phương pháp còn bao gồm:

nhận tên hotspot gửi bởi thiết bị mạng; và

bước sử dụng thông tin thuộc tính của hotspot được quét như khóa mã hóa và giải mã dữ liệu mật mã để thu nhận dữ liệu gốc bao gồm:

sử dụng thông tin thuộc tính tương ứng với tên hotspot trong thông tin thuộc tính của hotspot được quét như khóa mã hóa, và giải mã dữ liệu mật mã để thu nhận dữ liệu gốc.

Hơn nữa, trong phương pháp này, trước khi thông tin thuộc tính của hotspot được quét được sử dụng như khóa mã hóa, và dữ liệu mật mã được giải mã để thu nhận dữ liệu gốc, phương pháp còn bao gồm:

nhận thuật toán giải mã được gửi bởi thiết bị mạng; và

bước sử dụng thông tin thuộc tính của hotspot được quét như khóa mã hóa và giải mã dữ liệu mật mã để thu nhận dữ liệu gốc bao gồm:

sử dụng thông tin thuộc tính của hotspot được quét như khóa mã hóa, và giải mã dữ liệu mật mã dựa trên thuật toán giải mã nhận được và khóa mã hóa để thu nhận dữ liệu gốc.

Hơn nữa, theo phương pháp này, dữ liệu gốc bao gồm ít nhất một trong số:

thông tin dữ liệu thích hợp của hotspot;

thông tin thuộc tính người dùng của thiết bị người dùng; và

thông tin dữ liệu kinh doanh được lưu trữ trong thiết bị mạng.

Theo khía cạnh thứ tư, sáng chế cung cấp phương pháp thu nhận dữ liệu trên thiết bị của người dùng, trong đó phương pháp bao gồm:

xác định vị trí địa lý thực tế hiện tại là vị trí địa lý giải mã hiện tại, và quét và chọn hotspot trong dải vị trí địa lý giải mã hiện tại và thu nhận thông tin thuộc tính của hotspot được lựa chọn;

gửi yêu cầu truy vấn dữ liệu đến thiết bị mạng dựa trên thông tin thuộc tính của hotspot được chọn;

nhận dữ liệu mật mã được thiết bị mạng trả về dựa trên yêu cầu truy vấn dữ liệu; và

sử dụng thông tin thuộc tính của hotspot được quét được chọn là khóa mã hóa để giải mã dữ liệu mật mã, thu nhận dữ liệu gốc.

Theo khía cạnh thứ năm, sáng chế cung cấp thiết bị mạng để truyền dữ liệu, trong đó trong thiết bị mạng bao gồm:

thiết bị nhận dữ liệu, được cấu hình để thu nhận dữ liệu gốc được mã hóa;

thiết bị xác định, được cấu hình để xác định vị trí địa lý giải mã của dữ liệu gốc được mã hóa, và chọn hotspot trong dải vị trí địa lý giải mã;

thiết bị mã hóa, được cấu hình để sử dụng thông tin thuộc tính của hotspot được chọn như khóa mã hóa, mã hóa dữ liệu gốc được mã hóa để thu nhận dữ liệu mật mã, và gửi dữ liệu mật mã đến thiết bị người dùng, trong đó thiết bị người dùng thu nhận thông tin thuộc tính bằng cách quét hotspot trong dải vị trí địa lý giải mã.

Hơn nữa, trong thiết bị mạng nêu trên, thông tin thuộc tính bao gồm địa chỉ vật lý của hotspot được chọn.

Hơn nữa, trong thiết bị mạng nêu trên, thông tin thuộc tính bao gồm địa chỉ vật lý của hotspot được lựa chọn và thông tin nhận dạng người sử dụng của thiết bị người dùng thuộc hotspot được chọn.

Hơn nữa, trong thiết bị mạng nêu trên, thiết bị xác định được định cấu hình để:

xác định vị trí địa lý trong các khoảng cách định sẵn từ vị trí địa lý hiện tại của thiết bị người dùng như vị trí địa lý giải mã của dữ liệu gốc được mã hóa; hoặc

xác định vị trí địa lý giải mã của dữ liệu gốc được mã hóa theo lịch sử di chuyển địa lý của thiết bị người dùng.

Hơn nữa, trong thiết bị mạng nêu trên, thiết bị mã hóa được cấu hình để:

gửi tên hotspot tương ứng với hotspot được chọn đến thiết bị người dùng.

Hơn nữa, trong thiết bị mạng nêu trên, thiết bị mã hóa được cấu hình để:

sử dụng thông tin thuộc tính tương ứng với hotspot được chọn như khóa mã hóa; mã hóa dữ liệu gốc được mã hóa dựa trên thuật toán mã hóa cài đặt trước và khóa mã hóa để thu nhận dữ liệu mật mã; và gửi dữ liệu mật mã đến thiết bị người dùng.

Hơn nữa, trong thiết bị mạng được đề cập ở trên, dữ liệu gốc bao gồm ít nhất một trong số:

thông tin dữ liệu thích hợp của hotspot;

thông tin thuộc tính người dùng của thiết bị người dùng; và

thông tin dữ liệu kinh doanh được lưu trữ trong thiết bị mạng.

Hơn nữa, trong thiết bị mạng được đề cập ở trên, thiết bị mã hóa được cấu hình để:

gửi thuật toán giải mã cài đặt sẵn đến thiết bị người dùng.

Theo khía cạnh thứ sáu, sáng chế cung cấp thiết bị mạng để truyền dữ liệu, trong đó thiết bị mạng này bao gồm:

thiết bị thu nhận yêu cầu, được cấu hình để thu nhận yêu cầu truy vấn dữ liệu được gửi bởi thiết bị người dùng, trong đó yêu cầu truy vấn dữ liệu bao gồm thông tin thuộc tính của hotspot được chọn được quét và thu nhận bằng thiết bị người dùng trong dải vị trí địa lý giải mã hiện tại; và

thiết bị truyền dữ liệu mật mã, được cấu hình để thu nhận dữ liệu gốc được mã hóa dựa trên yêu cầu truy vấn dữ liệu; sử dụng thông tin thuộc tính của hotspot được chọn làm khóa mã hóa để mã hóa dữ liệu gốc được mã hóa; và thu nhận dữ liệu mật mã và gửi dữ liệu mật mã đến thiết bị người dùng.

Theo khía cạnh thứ bảy, sáng chế cung cấp thiết bị người dùng để thu nhận dữ liệu, trong đó thiết bị người dùng này bao gồm:

thiết bị nhận, được cấu hình để nhận dữ liệu mật mã được gửi bởi thiết bị mạng;

thiết bị thu nhận thông tin, được cấu hình để thu nhận thông tin thuộc tính của hotspot được quét trong dải vị trí địa lý giải mã; và

thiết bị giải mã, được cấu hình để sử dụng thông tin thuộc tính của hotspot được quét như khóa mã hóa để giải mã dữ liệu mật mã, và thu nhận dữ liệu gốc.

Hơn nữa, trong thiết bị người dùng nêu trên, thông tin thuộc tính bao gồm địa chỉ vật lý của hotspot được chọn.

Hơn nữa, trong thiết bị người dùng nêu trên, thông tin thuộc tính bao gồm địa chỉ vật lý của hotspot được lựa chọn và thông tin nhận dạng người sử dụng của thiết bị người dùng thuộc hotspot được chọn.

Hơn nữa, trong thiết bị người dùng được đề cập ở trên, vị trí địa lý giải mã bao gồm:

vị trí địa lý của thiết bị người dùng sau khi thiết bị người dùng di chuyển các khoảng cách định sẵn; và

vị trí địa lý trong lịch sử di chuyển địa lý của thiết bị người dùng.

Hơn nữa, trong thiết bị người dùng được đề cập ở trên, thiết bị nhận được cấu hình để:

nhận tên hotspot được gửi bởi thiết bị mạng; và

sử dụng thông tin thuộc tính của hotspot được quét như khóa mã hóa, và giải mã dữ liệu mật mã để thu nhận dữ liệu gốc, bao gồm:

sử dụng thông tin thuộc tính tương ứng với tên hotspot trong thông tin thuộc tính của hotspot được quét như khóa mã hóa, và giải mã dữ liệu mật mã để thu nhận dữ liệu gốc.

Hơn nữa, trong thiết bị người dùng được đề cập ở trên, thiết bị nhận được cấu hình để:

nhận thuật toán giải mã được gửi bởi thiết bị mạng; và

sử dụng thông tin thuộc tính của hotspot được quét như khóa mã hóa, và giải mã dữ liệu mật mã để thu nhận dữ liệu gốc, bao gồm:

sử dụng thông tin thuộc tính của hotspot được quét như khóa mã hóa, và giải mã dữ liệu mật mã dựa trên thuật toán giải mã nhận được và khóa mã hóa, và thu nhận dữ liệu gốc.

Hơn nữa, trong thiết bị người dùng được đề cập ở trên, dữ liệu gốc bao gồm ít nhất một trong số:

thông tin dữ liệu thích hợp của hotspot;

thông tin thuộc tính người dùng của thiết bị người dùng; và

thông tin dữ liệu kinh doanh được lưu trữ trong thiết bị mạng.

Theo khía cạnh thứ tám, sáng chế cung cấp thiết bị người dùng để thu nhận dữ liệu, trong đó thiết bị người dùng này bao gồm:

thiết bị thu xác định, được cấu hình để xác định vị trí địa lý thực tế hiện tại là vị trí địa lý giải mã hiện tại; quét và chọn hotspot trong dải vị trí địa lý giải mã hiện tại; và thu nhận thông tin thuộc tính của hotspot được lựa chọn;

thiết bị truyền yêu cầu, được cấu hình để gửi yêu cầu truy vấn dữ liệu đến thiết bị mạng dựa trên thông tin thuộc tính của hotspot được chọn;

thiết bị nhận dữ liệu mật mã, được cấu hình để nhận dữ liệu mật mã được thiết bị mạng trả về dựa trên yêu cầu truy vấn dữ liệu;

thiết bị thu giải mã, được cấu hình để sử dụng thông tin thuộc tính của hotspot được quét được chọn là khóa mã hóa để giải mã dữ liệu mật mã, và thu nhận dữ liệu gốc.

Theo khía cạnh thứ chín, sáng chế cung cấp thiết bị dựa trên máy tính, trong đó thiết bị dựa trên máy tính này bao gồm:

bộ xử lý; và

bộ nhớ được cấu hình để lưu trữ lệnh thực thi của máy tính, và trong đó các lệnh thực thi khi được thực hiện cho phép bộ xử lý:

thu nhận dữ liệu gốc được mã hóa;

xác định vị trí địa lý giải mã của dữ liệu gốc được mã hóa, và chọn hotspot trong dải vị trí địa lý giải mã; và

sử dụng thông tin thuộc tính của hotspot được chọn như khóa mã hóa, và mã hóa dữ liệu gốc được mã hóa để thu nhận dữ liệu mật mã và gửi dữ liệu mật

mã đến thiết bị người dùng, trong đó thiết bị người dùng thu nhận thông tin thuộc tính bằng cách quét hotspot trong dải vị trí địa lý giải mã.

Theo khía cạnh thứ mười, sáng chế cung cấp thiết bị dựa trên máy tính, trong đó thiết bị dựa trên máy tính này bao gồm:

bộ xử lý; và

bộ nhớ được cấu hình để lưu trữ lệnh thực thi của máy tính, và các lệnh thực thi này khi được thực hiện cho phép bộ xử lý:

thu nhận yêu cầu truy vấn dữ liệu được gửi bởi thiết bị người dùng, trong đó yêu cầu truy vấn dữ liệu bao gồm thông tin thuộc tính của hotspot được chọn được quét và thu nhận bởi thiết bị người dùng trong dải vị trí địa lý giải mã hiện tại; và

thu nhận dữ liệu gốc được mã hóa dựa trên yêu cầu truy vấn dữ liệu; sử dụng thông tin thuộc tính của hotspot được chọn làm khóa mã hóa; mã hóa dữ liệu gốc được mã hóa để thu nhận dữ liệu mật mã và gửi dữ liệu mật mã đến thiết bị người dùng.

Theo khía cạnh thứ mười một, sáng chế cung cấp thiết bị dựa trên máy tính, trong đó thiết bị dựa trên máy tính này bao gồm:

bộ xử lý; và

bộ nhớ được cấu hình để lưu trữ lệnh thực thi bởi máy tính, và các lệnh thực thi này được thực hiện cho phép bộ xử lý:

nhận dữ liệu mật mã được gửi bởi thiết bị mạng;

thu nhận thông tin thuộc tính của hotspot được quét trong dải vị trí địa lý giải mã; và

sử dụng thông tin thuộc tính của hotspot được quét như khóa mã hóa, và giải mã dữ liệu mật mã để thu nhận dữ liệu gốc.

Theo khía cạnh thứ mười hai, sáng chế cung cấp thiết bị dựa trên máy tính, trong đó thiết bị dựa trên máy tính này bao gồm:

bộ xử lý; và

bộ nhớ được cấu hình để lưu trữ lệnh thực thi bởi máy tính, và các lệnh thực thi này khi được thực hiện cho phép bộ xử lý:

xác định vị trí địa lý thực tế hiện tại là vị trí địa lý giải mã hiện tại; quét và chọn hotspot trong dải vị trí địa lý giải mã hiện tại; và thu nhận thông tin thuộc tính của hotspot được lựa chọn;

gửi yêu cầu truy vấn dữ liệu đến thiết bị mạng dựa trên thông tin thuộc tính của hotspot được lựa chọn;

nhận dữ liệu mật mã được thiết bị mạng trả về dựa trên yêu cầu truy vấn dữ liệu; và

sử dụng thông tin thuộc tính của hotspot được quét được chọn là khóa mã hóa để giải mã dữ liệu mật mã, và thu nhận dữ liệu gốc.

So với kỹ thuật đã biết, sáng chế bao gồm các bước: thu nhận dữ liệu gốc được mã hóa trên thiết bị mạng; xác định vị trí địa lý giải mã của dữ liệu gốc được mã hóa, và chọn hotspot trong dải vị trí địa lý giải mã; sau đó, sử dụng thông tin thuộc tính của hotspot được chọn như khóa mã hóa, mã hóa dữ liệu gốc được mã hóa để thu nhận dữ liệu mật mã, và gửi dữ liệu mật mã đến thiết bị người dùng, trong đó thiết bị người dùng thu nhận thông tin thuộc tính bằng cách quét hotspot trong dải vị trí địa lý giải mã. Trong sáng chế, vị trí địa lý giải mã thực tế được sử dụng như khóa mã hóa của dữ liệu gốc được mã hóa, để mã hóa dữ liệu gốc. Bằng cách này, dữ liệu gốc được gửi an toàn đến thiết bị người dùng, ngăn ngừa người sử dụng bất hợp pháp bẻ khóa mã hóa và thu nhận dữ liệu gốc tại các vị trí khác nhau.

Hơn nữa, sau khi dữ liệu mật mã được gửi bởi thiết bị mạng được nhận bởi thiết bị người dùng, sáng chế bao gồm các bước: thu nhận thông tin thuộc tính của hotspot được quét trong dải vị trí địa lý giải mã; sử dụng thông tin thuộc tính của hotspot được quét như khoá mật mã để giải mã dữ liệu mật mã, và thu nhận dữ liệu gốc. Thông tin thuộc tính của hotspot thu nhận dựa trên vị trí địa lý giải mã thực tế được sử dụng như khóa mã hóa để giải mã dữ liệu mật mã nhận được, để thu nhận dữ liệu gốc tương ứng. Do đó, bảo mật dữ liệu gốc thu nhận bằng thiết bị người dùng được đảm bảo để ngăn người sử dụng bất hợp pháp bẻ khóa khóa mã hóa và thu nhận dữ liệu gốc tại các các vị trí khác nhau.

Mô tả vắn tắt các hình vẽ

Fig.1 là lưu đồ của phương pháp truyền dữ liệu trên thiết bị mạng theo sáng chế;

Fig.2 là lưu đồ thể hiện kịch bản ứng dụng thực tế để truyền dữ liệu trên thiết bị mạng theo sáng chế;

Fig.3 là lưu đồ của phương pháp để thu nhận dữ liệu trên thiết bị người dùng theo sáng chế;

Fig.4 là lưu đồ thể hiện kịch bản ứng dụng thực tế để thu nhận dữ liệu trên thiết bị người dùng theo sáng chế;

Fig.5 là sơ đồ của thiết bị mạng để truyền dữ liệu theo sáng chế; và

Fig.6 là sơ đồ của thiết bị người dùng để thu nhận dữ liệu theo sáng chế.

Các số tham chiếu giống nhau hoặc tương tự nhau trên các hình vẽ đại diện cho cùng đơn vị hoặc các đơn vị tương tự nhau.

Mô tả chi tiết sáng chế

Sáng chế sẽ được mô tả chi tiết sau đây có dựa trên các hình vẽ kèm theo.

Trong cấu hình điển hình của sáng chế, thiết bị đầu cuối, thiết bị của mạng dịch vụ, và thiết bị được tin cậy bao gồm một hoặc nhiều bộ xử lý/đơn vị xử lý trung tâm (CPU), giao diện đầu vào/đầu ra, giao diện mạng, và bộ nhớ.

Bộ nhớ bao gồm bộ nhớ bay hơi, bộ nhớ truy cập ngẫu nhiên (RAM) và/hoặc bộ nhớ không bay hơi trong phương tiện có thể đọc được bởi máy tính, ví dụ bộ nhớ chỉ đọc (ROM) hoặc bộ nhớ flash (RAM flash). Bộ nhớ là ví dụ về phương tiện có thể đọc được bởi máy tính.

Phương tiện có thể đọc được bởi máy tính bao gồm cả hai phương tiện bay hơi và không bay hơi, phương tiện có thể di chuyển và không di chuyển có thể lưu trữ thông tin bằng phương pháp hoặc công nghệ bất kỳ. Thông tin có thể là lệnh đọc được bởi máy tính, cấu trúc dữ liệu, mô đun chương trình hoặc dữ liệu khác. Phương tiện lưu trữ máy tính bao gồm, nhưng không giới hạn đến, bộ nhớ truy cập ngẫu nhiên thay đổi pha (PCRAM), bộ nhớ truy cập ngẫu nhiên tĩnh (SRAM), bộ nhớ truy cập ngẫu nhiên động (DRAM), các loại bộ nhớ truy

cập ngẫu nhiên (RAM), bộ nhớ chỉ đọc (ROM) khác, bộ nhớ chỉ đọc có thể lập trình có thể xóa bằng điện (EEPROM), bộ nhớ flash hoặc công nghệ bộ nhớ khác, bộ nhớ chỉ đọc trên đĩa compact (CD-ROM), đĩa đa năng kỹ thuật số (DVD) hoặc bộ nhớ quang khác, băng từ catxet, bộ nhớ băng từ hoặc thiết bị lưu trữ từ khác hoặc phương tiện không truyền khác bất kỳ.

Fig.1 là lưu đồ của phương pháp truyền dữ liệu theo khía cạnh của sáng chế. Phương pháp được áp dụng cho thiết bị mạng trong quá trình truyền dữ liệu, bao gồm bước S11, S12, và bước S13. Trong bước S11, dữ liệu gốc được mã hóa được thu nhận. Trong bước S12, vị trí địa lý giải mã của dữ liệu gốc được mã hóa được xác định, và hotspot trong dải vị trí địa lý giải mã được chọn. Trong bước S13, thông tin thuộc tính của hotspot được chọn được sử dụng như khóa mã hóa để mã hóa dữ liệu gốc được mã hóa, và dữ liệu mật mã được thu nhận và gửi đến thiết bị người dùng. Cụ thể, thiết bị người dùng thu nhận thông tin thuộc tính bằng cách quét hotspot trong dải vị trí địa lý giải mã. Trong sáng chế, vị trí địa lý giải mã thực tế được sử dụng như khóa mã hóa dữ liệu gốc được mã hóa, để mã hóa dữ liệu gốc. Do đó, dữ liệu gốc được gửi an toàn đến thiết bị người dùng, ngăn ngừa người sử dụng bất hợp pháp bẻ khóa mã hóa và thu nhận dữ liệu gốc tại các vị trí khác nhau. Theo phương án khác của sáng chế, dữ liệu gốc có thể bao gồm ít nhất một trong số thông tin dữ liệu thích hợp của hotspot; thông tin thuộc tính người dùng của thiết bị người dùng và thông tin dữ liệu kinh doanh được lưu trữ trong thiết bị mạng. Cụ thể, thông tin dữ liệu thích hợp của hotspot có thể bao gồm tên hotspot của hotspot, thông tin vị trí địa lý của điểm truy cập, và các nhà cung cấp của hotspot. Thông tin thuộc tính người sử dụng của thiết bị người dùng có thể bao gồm thông tin nhận dạng người dùng (như định danh người dùng (ID)), tài khoản người dùng, và mật khẩu của tài khoản người dùng. Thông tin dữ liệu kinh doanh lưu trữ trong thiết bị mạng có thể bao gồm tài khoản thẻ ngân hàng và mật khẩu trong dịch vụ ngân hàng liên quan đến người sử dụng, hoặc bao gồm tài khoản thành viên và thông tin thành viên trong dịch vụ thành viên liên quan đến người sử dụng. Chắc chắn rằng dữ liệu gốc khác hiện có hoặc được phát triển trong thời gian tới để truyền dữ liệu có thể

được áp dụng cho sáng chế và sẽ nằm trong phạm vi của sáng chế và được kết hợp để tham chiếu.

Theo phương án khác của sáng chế, vị trí địa lý giải mã là vị trí địa lý thực tế với kinh độ và vĩ độ giữa thiết bị mạng và thiết bị người dùng trong quy trình truyền dữ liệu thực tế. Do có ít nhất một hotspot được bao phủ tại vị trí địa lý thực tế, và để đảm bảo sự độc đáo của khóa mã hóa được sử dụng để mã hóa và giải mã, hotspot hoặc các hotspot có thể được lựa chọn trong số tất cả các hotspot trong dải vị trí địa lý giải mã thực tế. Khi chọn các hotspot, thông tin thuộc tính của các hotspot phải được sử dụng như khóa mã hóa cùng lúc. Ví dụ, có 10 hotspot trong dải vị trí địa lý giải mã, được đại diện bởi hotspot 1 tới hotspot 10, tương ứng. Nếu hotspot 5 được lựa chọn từ 10 hotspot trong dải vị trí địa lý giải mã trong bước S12, thông tin thuộc tính của hotspot 5 được chọn được sử dụng như khóa mã hóa trong bước S13 để mã hóa dữ liệu gốc được mã hóa thu nhận ở bước S11. Nếu hotspot 2, 4 và 8 được lựa chọn từ 10 hotspot trong dải vị trí địa lý giải mã trong bước S12, thông tin thuộc tính (bộ định danh bộ dịch vụ cơ sở (BSSID2) của hotspot 2, thông tin thuộc tính của hotspot 4 (BSSID 4), và thông tin thuộc tính của hotspot 8 (BSSID8) được sử dụng như khóa mã hóa (nghĩa là khóa mã hóa là: BSSID 2 và BSSID 4 và BSSID 8) bởi quan hệ logic "VÀ", để mã hóa dữ liệu gốc được truyền và để giải mã dữ liệu mật mã được mã hóa. Do đó, quá trình mã hóa dữ liệu gốc và quá trình giải mã dữ liệu mật mã được mã hóa phải đạt được tại vị trí địa lý giải mã cụ thể, do đó đảm bảo an toàn của dữ liệu gốc trong quá trình truyền dữ liệu. Cụ thể, thông tin thuộc tính của hotspot được chọn có thể thu nhận khi thiết bị người dùng quét hotspot trong thời gian thực, hoặc được lưu trữ trước trên thiết bị mạng. Tốt hơn là, thông tin thuộc tính có thể bao gồm địa chỉ vật lý của hotspot được chọn, trong đó địa chỉ vật lý (nghĩa là địa chỉ điều khiển truy cập phương tiện truyền thông (Media Access Control-MAC)) của hotspot được chọn trong phương án của sáng chế được thể hiện ở dạng BSSID (nghĩa là địa chỉ MAC của hotspot) thu nhận được bằng hotspot tại địa chỉ vật lý thực tế. Tốt hơn là, thông tin thuộc tính bao gồm địa chỉ vật lý của hotspot được chọn (tức là địa chỉ MAC) và thông

tin nhận dạng người dùng (ID người dùng) của thiết bị người dùng thuộc hotspot được chọn. Bằng cách này, thiết bị người dùng và hotspot được chọn được quét bởi thiết bị người dùng có thể được xác định, do đó đảm bảo độ an toàn và độ chính xác của việc truyền dữ liệu gốc.

Theo phương án của sáng chế, khóa mã hóa trong bước S13 được biểu thị bằng chuỗi ký tự. Khoá mã hóa có thể là địa chỉ vật lý của hotspot được chọn, hoặc thông tin thuộc tính của hotspot được chọn, trong đó thông tin thuộc tính phải bao gồm địa chỉ vật lý của hotspot với mục đích đảm bảo sự an toàn của dữ liệu gốc trong quá trình truyền dữ liệu. Do địa chỉ vật lý thực tế được sử dụng như khóa mã hóa, người sử dụng bất hợp pháp tại các vị trí khác nhau được ngăn chặn khỏi việc giải mã dữ liệu mật mã được mã hóa dựa trên khóa mã hóa. Ví dụ, khóa mã hóa được dùng để mã hóa dữ liệu gốc được mã hóa có thể là địa chỉ vật lý (BSSID) của hotspot được chọn, hoặc thông tin thuộc tính (BSSID và ID người dùng) của hotspot được chọn. Thông tin thuộc tính bao gồm địa chỉ vật lý của hotspot được chọn trong dải vị trí địa lý giải mã thực tế được sử dụng như khóa mã hóa, do đó đảm bảo độ an toàn của truyền dữ liệu.

Hơn nữa, vị trí địa lý giải mã của dữ liệu gốc được mã hóa được xác định trong bước S12, cụ thể bao gồm:

vị trí địa lý trong các khoảng cách định sẵn từ vị trí địa lý hiện tại của thiết bị người dùng được xác định là vị trí địa lý giải mã của dữ liệu gốc được mã hóa; hoặc

vị trí địa lý giải mã của dữ liệu gốc được mã hóa được xác định theo lịch sử di chuyển địa lý của thiết bị người dùng.

Theo phương án khác của sáng chế, do hotspot có vị trí địa lý thực tế, khi vị trí địa lý giải mã của dữ liệu gốc được mã hóa được xác định trong bước S12, vị trí địa lý thực tế trong dải khoảng cách định sẵn từ vị trí địa lý hiện tại của thiết bị người dùng được xác định là vị trí địa lý giải mã. Thông tin thuộc tính của hotspot được chọn trong dải được thu nhận dựa trên vị trí địa lý giải mã. Do đó, sau khi dữ liệu mật mã được mã hóa được ngăn chặn khỏi người sử dụng bất hợp pháp, những người sử dụng bất hợp pháp là không biết gì về khóa mã hóa

(thông tin thuộc tính của hotspot) xác định dựa trên vị trí địa lý giải mã thực tế để mã hóa và giải mã, do đó không thu nhận được dữ liệu gốc. Ngoài ra, vị trí địa lý thực tế trong đó thiết bị người dùng có thể đi trong lịch sử di chuyển địa lý có thể được dự đoán theo lịch sử di chuyển địa lý của thiết bị người dùng. Thiết bị người dùng chọn thông tin thuộc tính của hotspot từ tất cả các hotspot được sử dụng như khóa mã hóa dựa trên dải vị trí địa lý thực tế trong lịch sử di chuyển địa lý. Tính độc đáo và tính xác thực của khóa mã hóa được sử dụng để mã hóa được đảm bảo, do đó đảm bảo sự an toàn của việc truyền dữ liệu gốc được mã hóa, và ngăn chặn người dùng bất hợp pháp khỏi việc ăn cắp khóa mã hóa tại vị trí khác và dẫn đến sự rò rỉ dữ liệu gốc.

Hơn nữa, trong bước S13, dữ liệu gốc được mã hóa được mã hóa để thu nhận dữ liệu mật mã và dữ liệu mật mã được gửi đến thiết bị người dùng, và trong khi đó, tên hotspot tương ứng với hotspot được chọn được gửi đến thiết bị người dùng.

Theo phương án khác của sáng chế, để tạo điều kiện thuận lợi cho thiết bị người dùng để nhanh chóng chọn hotspot bao gồm địa chỉ vật lý từ các hotspot được quét trong dải vị trí địa lý giải mã, dữ liệu mật mã được mã hóa được thu nhận được gửi cho thiết bị người sử dụng trong bước S13, và trong khi đó tên hotspot (bộ định danh bộ dịch vụ (SSID)) tương ứng với hotspot được chọn mà bao gồm địa chỉ vật lý, được gửi đến thiết bị người dùng, để thiết bị người dùng có thể nhanh chóng xác định BSSID tương ứng với tên hotspot (SSID) từ tất cả các hotspot được quét trong dải vị trí địa lý giải mã dựa trên tên hotspot nhận được (SSID). Sau đó, dữ liệu mật mã nhanh chóng được giải mã dựa trên địa chỉ vật lý (BSSID) mà tương ứng với tên hotspot (SSID) và được sử dụng như khóa mã hóa, để thu nhận được dữ liệu gốc.

Hơn nữa, trong bước S13, thông tin thuộc tính tương ứng với hotspot được chọn được sử dụng như khóa mã hóa, và dữ liệu gốc được mã hóa được mã hóa để thu nhận dữ liệu mật mã và dữ liệu mật mã được gửi đến thiết bị người dung, cụ thể bao gồm:

Thông tin thuộc tính tương ứng với hotspot được chọn được sử dụng như khóa mã hóa. Dữ liệu gốc được mã hóa được mã hóa dựa trên thuật toán mã hóa cài sẵn và khóa mã hóa để thu nhận dữ liệu mật mã, và dữ liệu mật mã được gửi đến thiết bị người dùng.

Theo phương án khác của sáng chế, thuật toán mã hóa có thể là chuẩn mã hóa tiên tiến (AES), hoặc chuẩn mã hóa dữ liệu (DES) hoặc sự mã hóa tương đương khác. Chắc chắn rằng các thuật toán mã hóa hiện có hoặc được phát triển trong tương lai để mã hóa dữ liệu gốc được mã hóa có thể được áp dụng cho sáng chế và thuộc phạm vi của sáng chế và được bao gồm ở đây.

Theo phương án khác của sáng chế, nếu thông tin thuộc tính (ví dụ như địa chỉ vật lý BSSID và ID người dùng) tương ứng với hotspot được chọn được sử dụng làm khóa mã hóa, dữ liệu gốc được mã hóa (ví dụ như mật khẩu của hotspot mà người sử dụng cần để đăng nhập) được mã hóa dựa trên khóa mã hóa (các BSSID và ID người dùng) và thuật toán mã hóa (ví dụ như AES) cài sẵn trong quá trình truyền dữ liệu, thì dữ liệu mật mã tương ứng được thu nhận và được gửi đến thiết bị người dùng. Do đó quá trình mã hóa gửi dữ liệu gốc được mã hóa (ví dụ như mật khẩu của hotspot mà người sử dụng cần để đăng nhập) đến thiết bị người dùng được thu nhận. Trong khi đó, sự an toàn của việc truyền dữ liệu gốc được mã hóa đến thiết bị người dùng (ví dụ như mật khẩu của hotspot mà người dùng cần phải sử dụng để đăng nhập) được đảm bảo. Hơn nữa, chỉ có thiết bị người dùng tương ứng với ID người dùng là có thể giải mã dữ liệu mật mã, do đó dữ liệu gốc (ví dụ như mật khẩu của hotspot mà người sử dụng cần để đăng nhập) được truyền an toàn và trực tiếp.

Hơn nữa, trong bước S13, dữ liệu gốc được mã hóa được mã hóa để thu nhận dữ liệu mật mã và dữ liệu mật mã được gửi đến thiết bị người dùng, và trong khi đó, thuật toán giải mã cài sẵn sẽ được gửi đến thiết bị người dùng.

Theo phương án khác của sáng chế, để đảm bảo rằng dữ liệu mật mã nhận được được giải mã nhanh chóng và chính xác bởi thiết bị người dùng, trong bước S13, dữ liệu mật mã được mã hóa được gửi đến thiết bị người dùng, và thuật toán giải mã cài sẵn được gửi đến thiết bị người dùng trong khi đó. Theo

cách này, thiết bị người dùng có thể giải mã chính xác và nhanh chóng dữ liệu mật mã dựa trên khóa mã hóa thu nhận tại vị trí địa lý thực tế và thuật toán giải mã, trong đó thuật toán giải mã có thể là thuật toán giải mã đối xứng với thuật toán mã hóa, hoặc thuật toán giải mã không đối xứng với thuật toán mã hóa.

Fig.2 thể hiện kịch bản ứng dụng thực tế của thiết bị mạng trong quá trình truyền dữ liệu. Dữ liệu gốc được mã hóa là mật khẩu hotspot, và khóa mã hóa là địa chỉ vật lý BSSID của hotspot SSID được chọn. Thứ nhất, hotspot và thông tin thuộc tính tương ứng của nó được thu nhận bằng thiết bị mạng dựa trên vị trí địa lý giải mã (ví dụ vĩ độ và kinh độ) của dữ liệu gốc được mã hóa, do đó việc thu nhận tên hotspot SSID, mật khẩu hotspot (tức là dữ liệu gốc được mã hóa), và khóa mã hóa BSSID. Sau đó, dữ liệu gốc được mã hóa (mật khẩu hotspot) được mã hóa bởi thiết bị mạng dựa trên thông tin thuộc tính BSSID, được sử dụng là khóa mã hóa BSSID, của hotspot được chọn trong dải vị trí địa lý giải mã, do đó, thu dữ liệu mật mã được mã hóa và tên hotspot SSID tương ứng. Dữ liệu mật mã được mã hóa thu nhận được được gửi cho thiết bị người dùng. Do đó, dữ liệu gốc (mật khẩu hotspot) được mã hóa được mã hóa và được truyền an toàn. Để đảm bảo rằng thiết bị người dùng có thể nhanh chóng và chính xác chọn địa chỉ vật lý BSSID tương ứng với hotspot từ tất cả các hotspot được quét trong dải vị trí địa lý giải mã, thiết bị mạng gửi tên hotspot SSID tương ứng với hotspot đến thiết bị người dùng, để thiết bị người dùng có thể nhanh chóng thu nhận BSSID tương ứng với SSID, và do đó thu nhận khóa mã hóa (SSID) để giải mã.

Khi thiết bị người dùng cần thu nhận dữ liệu gốc của thiết bị mạng theo thời gian thực, thiết bị người dùng gửi yêu cầu truy vấn dữ liệu đến thiết bị mạng. Do đó, phương pháp thu nhận dữ liệu trên thiết bị mạng theo các khía cạnh khác của sáng chế là như sau.

Đầu tiên, thiết bị mạng thu nhận yêu cầu truy vấn dữ liệu được gửi bởi thiết bị người dùng, trong đó yêu cầu truy vấn dữ liệu bao gồm thông tin thuộc tính (ví dụ như địa chỉ vật lý SSID của hotspot, theo cách khác, địa chỉ vật lý SSID của hotspot và thông tin nhận dạng người dùng của thiết bị người dùng

thuộc hotspot, tức là ID người dùng, v.v.) của hotspot được chọn được quét và thu nhận bằng thiết bị người dùng trong dải vị trí địa lý giải mã hiện tại.

Sau đó, thiết bị mạng thu nhận dữ liệu gốc được mã hóa mà thiết bị người dùng cần thu nhận trong thời gian thực dựa trên yêu cầu truy vấn dữ liệu. Bên cạnh đó, thông tin thuộc tính của hotspot được chọn được sử dụng như khóa mã hóa để mã hóa dữ liệu gốc được mã hóa, để thu nhận dữ liệu mật mã.

Cuối cùng, dữ liệu mật mã được gửi đến thiết bị người dùng tương ứng với yêu cầu truy vấn dữ liệu, và dữ liệu mật mã được giải mã dựa trên khóa mã hóa, tức là thông tin thuộc tính của hotspot được chọn, để thu nhận dữ liệu gốc. Do đó, thiết bị người dùng có thể thu nhận dữ liệu gốc an toàn mà cần được truy vấn trên thiết bị mạng trong thời gian thực, đảm bảo sự an toàn và kịp thời của dữ liệu gốc thu nhận được.

Fig.3 thể hiện lưu đồ của phương pháp thu nhận dữ liệu trên thiết bị người dùng theo một khía cạnh khác của sáng chế. Phương pháp này được áp dụng cho thiết bị người dùng trong quy trình truyền dữ liệu và bao gồm bước S21, bước S22 và bước S23. Trong bước S21, dữ liệu mật mã được gửi bởi thiết bị mạng được nhận. Sau đó, trong bước S22, thông tin thuộc tính của hotspot được quét trong dải vị trí địa lý giải mã được thu nhận. Sau đó, trong bước S23, thông tin thuộc tính của hotspot được quét được sử dụng là khóa mã hóa để giải mã dữ liệu mật mã, để thu nhận dữ liệu gốc. Thông tin thuộc tính của hotspot thu nhận dựa trên vị trí địa lý giải mã thực tế được sử dụng như khoá mã hóa để giải mã dữ liệu mật mã nhận được, để thu nhận dữ liệu gốc tương ứng. Do đó, sự an toàn của dữ liệu gốc được mã hóa được thu nhận bằng thiết bị người dùng được đảm bảo, ngăn chặn người dùng bất hợp pháp khỏi việc ăn cắp dữ liệu gốc tại vị trí khác.

Theo phương án khác của sáng chế, dữ liệu gốc có thể bao gồm ít nhất một trong số sau: thông tin dữ liệu thích hợp của hotspot; thông tin thuộc tính người dùng của thiết bị người dùng; thông tin dữ liệu kinh doanh được lưu trữ trong thiết bị mạng. Cụ thể là, thông tin dữ liệu thích hợp của hotspot có thể bao gồm tên hotspot của hotspot, thông tin vị trí địa lý của hotspot, và nhà cung cấp

của hotspot. Thông tin thuộc tính người sử dụng của thiết bị người dùng có thể bao gồm thông tin nhận dạng người dùng (nghĩa là ID người dùng), tài khoản người dùng, và mật khẩu của tài khoản người dùng, v.v.; và thông tin dữ liệu kinh doanh được lưu trữ trong thiết bị mạng có thể bao gồm tài khoản thẻ ngân hàng và mật khẩu của nó trong dịch vụ ngân hàng liên quan đến người sử dụng, hoặc tài khoản thành viên và thông tin thành viên trong dịch vụ thành viên liên quan đến người sử dụng. Chắc chắn là, dữ liệu gốc hiện có hoặc được phát triển trong tương lai khác để truyền dữ liệu có thể được áp dụng cho sáng chế, đều thuộc phạm vi của sáng chế và được kết hợp ở đây để tham khảo.

Tốt hơn là, thông tin thuộc tính bao gồm địa chỉ vật lý của hotspot được chọn, trong đó địa chỉ vật lý (nghĩa là địa chỉ MAC của hotspot) được chọn trong sáng chế được thể hiện bằng BSSID (địa chỉ MAC của hotspot) được thu nhận bởi hotspot trong địa chỉ vật lý thực tế.

Hơn nữa, vị trí địa lý giải mã bao gồm:

vị trí địa lý của thiết bị người dùng sau khi thiết bị người dùng di chuyển khoảng cách định sẵn; và

vị trí địa lý trong lịch sử di chuyển địa lý của thiết bị người dùng.

Theo phương án khác của sáng chế, vị trí địa lý giải mã được sử dụng để thu nhận thông tin thuộc tính của hotspot có thể là vị trí địa lý thực tế của thiết bị người dùng sau khi thiết bị người dùng di chuyển trong khoảng cách định sẵn, hoặc vị trí địa lý thực tế trong lịch sử di chuyển địa lý của thiết bị người dùng. Bằng cách này, thông tin thuộc tính của hotspot có thể được thu nhận với điều kiện là thiết bị người dùng thực tế nằm ở vị trí địa lý giải mã thực tế, và sau đó dữ liệu mật mã nhận được được giải mã, đảm bảo an toàn của quá trình giải mã dữ liệu mật mã và dữ liệu gốc tương ứng với dữ liệu mật mã được giải mã và thu nhận bởi thiết bị người dùng. Do người sử dụng bất hợp pháp không thể thu nhận được vị trí địa lý giải mã thực tế, được sử dụng cho việc giải mã, thông tin thuộc tính của hotspot, người sử dụng bất hợp pháp không thể đạt được vị trí địa lý giải mã thực tế để thu nhận khóa mã hóa (thông tin thuộc tính của hotspot),

ngăn ngừa người dùng bất hợp pháp tại vị trí khác ăn cắp dữ liệu mật mã và giải mã dữ liệu mật mã.

Hơn nữa, trong bước S21, dữ liệu mật mã được gửi bởi thiết bị mạng được nhận, trong khi đó, và khi đó:

tên hotspot được gửi bởi thiết bị mạng được nhận.

Trong bước S23, thông tin thuộc tính của hotspot được quét được sử dụng như khóa mã hóa, và dữ liệu mật mã được giải mã để thu nhận dữ liệu gốc, cụ thể bao gồm:

thông tin thuộc tính tương ứng với tên hotspot trong thông tin thuộc tính của hotspot được quét được sử dụng như khóa mã hóa, và dữ liệu mật mã được giải mã để thu nhận dữ liệu gốc.

Theo phương án khác của sáng chế, để tạo thuận lợi cho thiết bị người dùng nhanh chóng quét hotspot bao gồm thông tin thuộc tính của hotspot từ các hotspot được quét trong dải vị trí địa lý giải mã, tên hotspot nhận được (SSID) được so sánh với thông tin thuộc tính của mỗi hotspot được quét sau khi tên hotspot (SSID) được gửi bằng thiết bị mạng được nhận. Sau đó, thông tin thuộc tính tương ứng với tên hotspot (SSID) được thu nhận, và được sử dụng như khóa mã hóa để giải mã dữ liệu mật mã nhận được, để thu nhận dữ liệu gốc. Khoá mã hóa để giải mã được thu nhận nhanh chóng dựa trên tên hotspot (SSID) và thông tin thuộc tính (ví dụ BSSID, hoặc BSSID và ID người dùng, v.v.) của hotspot, do đó nhận biết giải mã nhanh chóng dữ liệu mật mã.

Hơn nữa, trong bước S23, trước khi thông tin thuộc tính của hotspot được quét được sử dụng làm khóa mã hóa để giải mã dữ liệu mật mã để thu nhận dữ liệu gốc, thuật toán giải mã được gửi bởi thiết bị mạng được nhận.

Trong bước S23, thông tin thuộc tính của hotspot được quét được sử dụng như chìa khóa mã hóa, và dữ liệu mật mã được giải mã để thu nhận dữ liệu gốc, cụ thể bao gồm:

thông tin thuộc tính của hotspot được quét được sử dụng làm khóa mã hóa, và dữ liệu mật mã được giải mã dựa trên thuật toán giải mã nhận được và khóa mã hóa, để thu nhận dữ liệu gốc. Theo phương án của sáng chế, thuật toán

mã hóa có thể là thuật toán đảo ngược của thuật toán mã hóa tiên tiến (AES), hoặc thuật toán đảo ngược của thuật toán mã hóa chuẩn (DES), hoặc thuật toán mã hóa tương đương. Chắc chắn rằng, thuật toán giải mã khác hiện có hoặc được phát triển trong tương lai cho việc mã hóa dữ liệu gốc có thể được áp dụng cho sáng chế, và đều thuộc phạm vi của sáng chế.

Theo phương án của sáng chế, nếu thông tin thuộc tính (ví dụ như địa chỉ vật lý BSSID và ID người dùng) của hotspot được quét được sử dụng là khóa mã hóa, dữ liệu mật mã nhận được (ví dụ như dữ liệu mật mã bao gồm mật khẩu của hotspot mà người sử dụng cần để đăng nhập) được giải mã dựa trên khóa mã hóa (BSSID và ID người dùng) và thuật toán giải mã (ví dụ như thuật toán ngược của thuật toán mã hóa AES) nhận được bởi thiết bị người dùng trong quá trình truyền dữ liệu. Theo đó, dữ liệu gốc tương ứng (mật khẩu của hotspot mà người dùng sử dụng để đăng nhập) được thu nhận, do đó thiết bị người dùng thực hiện quá trình kinh doanh tương ứng và phản ứng trên thiết bị người dùng dựa trên dữ liệu gốc (mật khẩu của hotspot mà người dùng cần để đăng nhập) được thu nhận bằng cách giải mã. Do đó, dữ liệu mật mã được gửi bởi thiết bị mạng được giải mã bởi thiết bị người dùng dựa trên thông tin thuộc tính của hotspot được quét trong dải vị trí địa lý giải mã, để thu nhận được dữ liệu gốc mà thiết bị mạng cần truyền. Ngoài ra, với điều kiện thiết bị người dùng thực tế đạt đến vị trí địa lý giải mã, thông tin thuộc tính (khóa mã hóa) của hotspot để giải mã có thể được thu nhận, và sau đó dữ liệu mật mã được giải mã dựa trên khóa mã hóa. Do đó, sự an toàn của dữ liệu gốc (ví dụ như mật khẩu của hotspot mà người dùng sử dụng để đăng nhập) trong quá trình truyền dữ liệu được đảm bảo.

Fig.4 thể hiện kịch bản thực tế áp dụng cho thiết bị người dùng trong quá trình truyền dữ liệu theo sáng chế, trong đó dữ liệu mật mã bao gồm mật khẩu hotspot, và khóa mã hóa là địa chỉ vật lý BSSID của hotspot. Đầu tiên, dữ liệu mật mã được tạo thành bằng cách mã hóa mật khẩu hotspot và tên hotspot SSID của hotspot được gửi bởi thiết bị mạng và được nhận bởi thiết bị người dùng. Sau đó, hotspot trong dải vị trí địa lý giải mã được quét dựa trên tên hotspot

SSID nhận được để thu nhận địa chỉ vật lý (BSSID) của hotspot tương ứng với tên hotspot SSID, và địa chỉ vật lý (BSSID) của hotspot tương ứng được sử dụng làm khóa mã hóa. Sau đó, dữ liệu mật mã được giải mã dựa trên khóa mã hóa (BSSID) và thuật toán giải mã để thu nhận dữ liệu gốc tương ứng (mật khẩu hotspot). Thông tin thuộc tính của hotspot được thu nhận dựa trên vị trí địa lý giải mã thực tế được sử dụng như khóa mã hóa để giải mã dữ liệu mật mã nhận được, để thu nhận dữ liệu gốc tương ứng. Do đó, sự an toàn của dữ liệu gốc được thu nhận bởi thiết bị người dùng được đảm bảo, ngăn ngừa người dùng bất hợp pháp ăn cắp dữ liệu gốc tại vị trí khác.

Khi thiết bị người dùng cần thu nhận dữ liệu gốc trên thiết bị mạng trong thời gian thực, phương pháp thu nhận dữ liệu trên thiết bị người dùng theo khía cạnh khác của sáng chế như sau.

Đầu tiên, thiết bị người dùng xác định vị trí địa lý thực tế hiện tại là vị trí địa lý giải mã và quét và chọn hotspot trong dải vị trí địa lý giải mã hiện tại, và thu nhận thông tin thuộc tính (ví dụ như địa chỉ vật lý SSID của hotspot, theo cách khác, địa chỉ vật lý SSID của hotspot và thông tin nhận dạng người sử dụng của thiết bị người dùng thuộc hotspot, tức là ID người dùng, v.v.) của hotspot được chọn.

Sau đó, thiết bị người dùng gửi yêu cầu truy vấn dữ liệu đến thiết bị mạng dựa trên thông tin thuộc tính của hotspot được chọn.

Sau khi nhận được yêu cầu truy vấn dữ liệu, thiết bị mạng thu nhận dữ liệu gốc được mã hóa mà thiết bị người dùng cần phải thu nhận theo thời gian thực. Để đảm bảo an toàn của truyền dữ liệu gốc, thiết bị mạng sử dụng thông tin thuộc tính của hotspot được chọn như khóa mã hóa để mã hóa dữ liệu gốc được mã hóa, và dữ liệu mật mã được thu nhận và gửi đến thiết bị người dùng.

Sau đó, thiết bị người dùng nhận dữ liệu mật mã mà được trả về bởi thiết bị mạng dựa trên yêu cầu truy vấn dữ liệu.

Cuối cùng, thiết bị người dùng sử dụng thông tin thuộc tính của hotspot được quét được chọn là khoá mật mã để giải mã dữ liệu mật mã, và sau đó thu

nhận dữ liệu gốc, do đó đảm bảo an toàn dữ liệu gốc thu nhận được và tính kịp thời của dữ liệu gốc thu nhận được từ thiết bị mạng.

Fig.5 thể hiện sơ đồ của thiết bị mạng để truyền dữ liệu theo một khía cạnh của sáng chế. Thiết bị mạng được áp dụng cho các quá trình truyền dữ liệu, và bao gồm thiết bị thu nhận dữ liệu 11, thiết bị xác định 12, và thiết bị mã hóa 13. Cụ thể, thiết bị thu nhận dữ liệu 11 được cấu hình để thu nhận dữ liệu gốc được mã hóa. Thiết bị xác định 12 được cấu hình để xác định vị trí địa lý giải mã của dữ liệu gốc được mã hóa, và chọn hotspot trong dải vị trí địa lý giải mã. Thiết bị mã hóa 13 được cấu hình để sử dụng thông tin thuộc tính của hotspot được chọn như khóa mã hóa để mã hóa dữ liệu gốc được mã hóa, và thu nhận dữ liệu mật mã và gửi dữ liệu mật mã đến thiết bị người dùng. Cụ thể, thiết bị người dùng thu nhận thông tin thuộc tính bằng cách quét hotspot trong dải vị trí địa lý giải mã. Trong sáng chế, vị trí địa lý giải mã thực tế được sử dụng như khóa mã hóa dữ liệu gốc được mã hóa, để mã hóa dữ liệu gốc. Do đó, dữ liệu gốc được gửi an toàn đến thiết bị người dùng, ngăn ngừa người dùng bất hợp pháp bẻ khóa mã hóa và thu nhận dữ liệu gốc tại vị trí khác.

Theo phương án khác của sáng chế, dữ liệu gốc có thể bao gồm ít nhất một trong số sau: thông tin dữ liệu thích hợp của hotspot; thông tin thuộc tính người dùng của thiết bị người dùng; và thông tin dữ liệu kinh doanh lưu trữ trong thiết bị mạng. Cụ thể, thông tin dữ liệu thích hợp của hotspot có thể bao gồm tên hotspot của hotspot, thông tin vị trí địa lý của hotspot, và nhà cung cấp của hotspot. Thông tin thuộc tính người dùng của thiết bị người dùng có thể bao gồm thông tin nhận dạng người dùng (nghĩa là ID người dùng), tài khoản người dùng, và mật khẩu của tài khoản người dùng. Thông tin dữ liệu kinh doanh lưu trữ trong thiết bị mạng có thể bao gồm tài khoản thẻ ngân hàng và mật khẩu của nó trong dịch vụ ngân hàng liên quan đến người sử dụng, hoặc tài khoản thành viên và thông tin thành viên trong dịch vụ thành viên liên quan đến người sử dụng. Chắc chắn là, dữ liệu gốc hiện có hoặc được phát triển trong thời gian tới để truyền dữ liệu có thể được áp dụng cho sáng chế, và đều thuộc phạm vi của sáng chế và được đưa vào trong sáng chế.

Theo một phương án của sáng chế, vị trí địa lý giải mã là vị trí địa lý thực tế có kinh độ và vĩ độ giữa thiết bị mạng và thiết bị người dùng trong trình truyền truyền dữ liệu thực tế. Do có ít nhất một hotspot được bao phủ tại vị trí địa lý thực tế, và để đảm bảo sự độc đáo của khóa mã hóa được sử dụng để mã hóa và giải mã, hotspot hoặc các hotspot có thể được lựa chọn trong số tất cả các hotspot trong dải vị trí địa lý giải mã thực tế. Khi chọn các hotspot, thông tin thuộc tính của các hotspot phải được sử dụng như khóa mã hóa cùng lúc. Ví dụ, có 10 hotspot trong dải vị trí địa lý giải mã, được đại diện bởi hotspot 1 tới hotspot 10, tương ứng. Nếu một hotspot 5 được lựa chọn từ 10 hotspot này trong dải vị trí địa lý giải mã trong bước S12, thông tin thuộc tính của hotspot 5 được chọn được sử dụng như khóa mã hóa trong bước S13 để mã hóa dữ liệu gốc được mã hóa được thu nhận ở bước S11. Nếu hotspot 2, 4 và 8 được lựa chọn từ 10 hotspot trong dải vị trí địa lý giải mã ở bước S12, thông tin thuộc tính (BSSID 2) của hotspot 2, thông tin thuộc tính (BSSID 4) của hotspot 4, và thông tin thuộc tính (BSSID 8) của hotspot 8 được sử dụng như khóa mã hóa (khóa mã hóa là: BSSID 2 and BSSID 4 and BSSID 8) sử dụng phép logic "AND", để mã hóa dữ liệu gốc được truyền và giải mã dữ liệu mật mã được mã hóa. Do đó, quá trình mã hóa dữ liệu gốc và quá trình giải mã dữ liệu mật mã được mã hóa chỉ đạt được tại vị trí địa lý giải mã cụ thể, do đó đảm bảo an toàn của dữ liệu gốc trong quá trình truyền dữ liệu. Cụ thể, thông tin thuộc tính của hotspot được chọn có thể được thu nhận khi thiết bị người dùng quét hotspot trong thời gian thực, hoặc lưu trữ trước trong thiết bị mạng.

Tốt hơn là, thông tin thuộc tính bao gồm địa chỉ vật lý của hotspot được chọn, trong đó địa chỉ vật lý (nghĩa là địa chỉ MAC) của hotspot được chọn trong phương án của sáng chế được thể hiện ở dạng BSSID (nghĩa là địa chỉ MAC của hotspot) được thu nhận bởi hotspot tại địa chỉ vật lý thực tế. Tốt hơn là, thông tin thuộc tính bao gồm địa chỉ vật lý của hotspot được chọn (nghĩa là địa chỉ MAC) và thông tin nhận dạng người dùng (ID người dùng) của thiết bị người dùng thuộc hotspot được chọn. Bằng cách này, thiết bị người dùng và

hotspot được chọn được quét bởi thiết bị người dùng có thể được xác định, do đó đảm bảo độ an toàn và độ chính xác của việc truyền dữ liệu gốc.

Theo một phương án của sáng chế, khóa mã hóa trong bước S13 được biểu thị bằng chuỗi ký tự. Khoá mã hóa có thể là địa chỉ vật lý của hotspot được chọn, hoặc thông tin thuộc tính của hotspot được chọn, trong đó thông tin thuộc tính phải bao gồm địa chỉ vật lý của hotspot với mục đích đảm bảo sự an toàn của dữ liệu gốc trong quá trình truyền dữ liệu. Địa chỉ vật lý thực tế được sử dụng như khóa mã hóa, như vậy để ngăn chặn người sử dụng bất hợp pháp tại vị trí khác giải mã dữ liệu mật mã được mã hóa dựa trên khóa mã hóa. Ví dụ, khóa mã hóa dùng để mã hóa dữ liệu gốc được mã hóa có thể là địa chỉ vật lý (BSSID) của hotspot được chọn, hoặc thông tin thuộc tính (BSSID và ID người dùng) của hotspot được chọn. Địa chỉ vật lý bao gồm điểm truy cập được chọn trong dải vị trí địa lý giải mã thực tế được sử dụng xác thực như khóa mã hóa, do đó đảm bảo độ an toàn của việc truyền dữ liệu.

Hơn nữa, thiết bị xác định 12 được cấu hình để:

xác định địa lý vị trí trong các khoảng cách định sẵn từ vị trí địa lý hiện tại của thiết bị người dùng như là vị trí địa lý giải mã của dữ liệu gốc được mã hóa; hoặc

xác định vị trí địa lý giải mã của dữ liệu gốc được mã hóa theo lịch sử di chuyển địa lý của thiết bị người dùng.

Theo phương án khác của sáng chế, do hotspot có vị trí địa lý thực tế, khi vị trí địa lý giải mã của dữ liệu gốc được mã hóa được xác định trong bước S12, vị trí địa lý thực tế trong khoảng cách định sẵn của vị trí địa lý hiện tại của thiết bị người dùng được xác định là vị trí địa lý giải mã. Thông tin thuộc tính của hotspot được chọn trong dải này được thu nhận dựa trên vị trí địa lý giải mã. Theo cách này, dữ liệu mật mã được mã hóa được ngăn chặn khỏi người sử dụng bất hợp pháp, do người sử dụng bất hợp pháp không thể thu nhận khóa mã hóa (nghĩa là thông tin thuộc tính của hotspot) được xác định dựa trên vị trí địa lý giải mã thực tế để mã hóa và giải mã, và do đó không thể thu nhận dữ liệu gốc. Ngoài ra, vị trí địa lý thực tế trong đó thiết bị người dùng có thể di chuyển

trong lịch sử di chuyển địa lý có thể được dự đoán theo lịch sử di chuyển địa lý của thiết bị người dùng. Thiết bị người dùng chọn thông tin thuộc tính của hotspot từ tất cả các hotspot được sử dụng như khóa mã hóa dựa trên dải vị trí địa lý thực tế trong lịch sử di chuyển địa lý. Tính độc đáo và tính xác thực của khóa mã hóa được sử dụng để mã hóa và sự an toàn của dữ liệu gốc được mã hóa được đảm bảo, ngăn chặn người dùng bất hợp pháp ăn cắp khóa mã hóa tại vị trí khác và dẫn đến sự rò rỉ dữ liệu gốc.

Hơn nữa, thiết bị mã hóa 13 được cấu hình để:

gửi tên hotspot tương ứng với hotspot được chọn đến thiết bị người dùng.

Theo phương án khác của sáng chế, để tạo thuận lợi cho thiết bị người dùng nhanh chóng chọn hotspot bao gồm địa chỉ vật lý từ các hotspot trong dải vị trí địa lý giải mã, dữ liệu mật mã mã hóa được truyền đến thiết bị người dùng bởi thiết bị mã hóa 13, và trong khi đó, tên hotspot (SSID) tương ứng với hotspot được chọn bao gồm địa chỉ vật lý được gửi đến thiết bị người dùng, để thiết bị người dùng có thể nhanh chóng xác định BSSID tương ứng với tên hotspot (SSID) từ tất cả các hotspot được quét trong dải vị trí địa lý giải mã dựa trên tên hotspot đã nhận (SSID). Sau đó, dữ liệu mật mã sẽ nhanh chóng được giải mã dựa trên khóa mã hóa, tức là địa chỉ vật lý (BSSID) tương ứng với tên hotspot (SSID), để thu nhận dữ liệu gốc.

Hơn nữa, thiết bị mã hóa 13 được cấu hình để:

sử dụng thông tin thuộc tính tương ứng với hotspot được chọn như khóa mã hóa, mã hóa dữ liệu gốc được mã hóa dựa trên thuật toán mã hóa cài sẵn và khóa mã hóa để thu nhận dữ liệu mật mã, và gửi dữ liệu mật mã đến thiết bị người dùng.

Theo một phương án của sáng chế, thuật toán mã hóa bao gồm AES và DES. Chắc chắn rằng các thuật toán mã hóa hiện có hoặc được phát triển trong tương lai cho việc mã hóa dữ liệu gốc có thể được áp dụng cho sáng chế, và đều thuộc phạm vi của sáng chế.

Theo phương án khác sáng chế, thông tin thuộc tính (ví dụ như địa chỉ vật lý BSSID và ID người dùng) tương ứng với hotspot được chọn được sử dụng

như khóa mã hóa, dữ liệu gốc được mã hóa (ví dụ mật khẩu của hospot mà người sử dụng cần để đăng nhập) được mã hóa dựa trên khóa mã hóa (BSSID và ID người dùng) và thuật toán mã hóa (ví dụ như AES) được cài sẵn trong quá trình truyền dữ liệu. Sau đó, dữ liệu mật mã tương ứng được thu nhận và được gửi đến thiết bị người dùng. Do đó, dữ liệu gốc được mã hóa (ví dụ như mật khẩu của hotspot mà người dùng sử dụng cần để đăng nhập) mà cần phải được gửi đến thiết bị người dùng được mã hóa, do đó đảm bảo sự an toàn của việc truyền dữ liệu gốc được mã hóa (ví dụ như mật khẩu của hotspot mà người dùng cần để đăng nhập) vào thiết bị người dùng. Hơn nữa, chỉ có thiết bị người dùng tương ứng với ID người dùng là có thể giải mã dữ liệu mật mã, do đó dữ liệu gốc (ví dụ như mật khẩu của hotspot mà người dùng cần để đăng nhập) được truyền trực tiếp và an toàn.

Hơn nữa, thiết bị mã hóa 13 được cấu hình để:

gửi thuật toán giải mã cài sẵn đến thiết bị người dùng.

Theo phương án khác của sáng chế, để đảm bảo rằng dữ liệu mật mã nhận được được giải mã nhanh chóng và chính xác bởi thiết bị người dùng, thiết bị mã hóa 13 gửi dữ liệu mật mã thu nhận được bởi sự mã hóa đến thiết bị người dùng, và gửi thuật toán giải mã cài đặt sẵn để thiết bị người dùng cùng lúc. Theo cách này, thiết bị người dùng có thể giải mã chính xác và nhanh chóng dữ liệu mật mã dựa trên khóa mã hóa thu nhận được tại vị trí địa lý thực tế và thuật toán giải mã, trong đó thuật toán giải mã có thể là thuật toán giải mã đối xứng với thuật toán mã hóa, hoặc thuật toán giải mã không đối xứng với thuật toán mã hóa.

Fig.2 thể hiện kịch bản ứng dụng thực tế của thiết bị mạng trong quá trình truyền dữ liệu theo sáng chế. Dữ liệu gốc được mã hóa là mật khẩu hotspot, và khóa mã hóa là địa chỉ vật lý BSSID của hotspot được chọn SSID. Đầu tiên, hotspot và thông tin thuộc tính tương ứng thu nhận được bởi thiết bị mạng dựa trên vị trí địa lý giải mã (ví dụ kinh độ và vĩ độ) của dữ liệu gốc được mã hóa. Tên hotspot SSID, mật khẩu hotspot, tức là dữ liệu gốc được mã hóa, và khóa mã hóa BSSID được thu nhận. Sau đó, dữ liệu gốc được mã hóa (mật khẩu

hotspot) được mã hóa bởi thiết bị mạng dựa trên thông tin thuộc tính BSSID, mà được sử dụng như khóa mã hóa BSSID, hotspot được chọn với dải vị trí địa lý giải mã. Dữ liệu mật mã được mã hóa và tên hotspot tương ứng SSID được thu nhận, và dữ liệu mật mã được mã hóa thu nhận được gửi cho thiết bị người dùng. Do đó, dữ liệu gốc được mã hóa (mật khẩu hotspot) được mã hóa và được truyền an toàn. Để đảm bảo thiết bị người dùng có thể chọn nhanh chóng và chính xác địa chỉ vật lý BSSID tương ứng với hotspot từ tất cả các hotspot được quét trong dải vị trí địa lý giải mã, thiết bị mạng gửi tên hotspot SSID tương ứng với hotspot đến thiết bị người dùng, để thiết bị người dùng có thể nhanh chóng thu nhận BSSID tương ứng với SSID, và thu nhận khóa mã hóa (SSID) để giải mã.

Khi thiết bị người dùng cần thu nhận dữ liệu gốc của thiết bị mạng theo thời gian thực, thiết bị người dùng gửi yêu cầu truy vấn dữ liệu đến thiết bị mạng. Thiết bị mạng để truyền dữ liệu theo khía cạnh khác của sáng chế cụ thể bao gồm:

thiết bị thu nhận yêu cầu, được cấu hình để thu nhận yêu cầu truy vấn dữ liệu được gửi bởi thiết bị người dùng, trong đó yêu cầu truy vấn dữ liệu bao gồm (ví dụ như địa chỉ vật lý SSID của hotspot, cách khác, địa chỉ vật lý SSID của hotspot và thông tin nhận dạng người dùng của thiết bị người dùng thuộc hotspot, tức là ID người dùng, v.v.) của hotspot được chọn được quét và thu nhận bằng thiết bị người dùng trong dải vị trí địa lý giải mã hiện tại; và

thiết bị truyền dữ liệu mật mã, được cấu hình để thu nhận dữ liệu gốc được mã hóa mà thiết bị người dùng cần thu nhận trong thời gian thực dựa trên yêu cầu truy vấn dữ liệu; sử dụng thông tin thuộc tính của hotspot được chọn làm khóa mã hóa để mã hóa dữ liệu gốc được mã hóa và thu nhận dữ liệu mật mã; và gửi dữ liệu mật mã đến thiết bị người dùng tương ứng với yêu cầu truy vấn dữ liệu. Do đó, dữ liệu mật mã được giải mã bởi thiết bị người dùng dựa trên thông tin thuộc tính, mà được sử dụng là khóa mã hóa của hotspot được chọn để thu nhận dữ liệu gốc, để thiết bị người dùng có thể thu nhận an toàn dữ

liệu gốc mà cần được truy vấn trên thiết bị mạng trong thời gian thực, và đảm bảo sự an toàn và kịp thời của dữ liệu gốc thu nhận được.

Fig.6 là sơ đồ của thiết bị người dùng để thu nhận dữ liệu theo khía cạnh khác của sáng chế. Thiết bị người dùng được sử dụng cho quá trình truyền dữ liệu, và bao gồm thiết bị nhận 21, thiết bị thu nhận thông tin 22, và thiết bị giải mã 23. Thiết bị nhận 21 được cấu hình để nhận dữ liệu mật mã được gửi bởi thiết bị mạng. Thiết bị thu nhận thông tin 22 được cấu hình để thu nhận thông tin thuộc tính của hotspot được quét trong dải vị trí địa lý giải mã. Thiết bị giải mã 23 được cấu hình để sử dụng thông tin thuộc tính của hotspot được quét như khoá mật mã để giải mã dữ liệu mật mã, để thu nhận dữ liệu gốc. Thông tin thuộc tính của hotspot thu nhận được dựa trên vị trí địa lý giải mã thực tế được sử dụng như khóa mã hóa để giải mã dữ liệu mật mã nhận được, để thu nhận dữ liệu gốc tương ứng. Do đó, sự an toàn của dữ liệu gốc được thu nhận bởi thiết bị người dùng được đảm bảo, để ngăn ngừa người sử dụng bất hợp pháp ăn cắp dữ liệu gốc tại các vị trí khác.

Theo phương án khác của sáng chế, dữ liệu gốc có thể bao gồm ít nhất một trong số sau: thông tin dữ liệu thích hợp của hotspot; thông tin thuộc tính người dùng của thiết bị người dùng; và thông tin dữ liệu kinh doanh được lưu trữ trong thiết bị mạng. Cụ thể, thông tin dữ liệu thích hợp của hotspot có thể bao gồm tên hotspot của hotspot, thông tin vị trí địa lý của điểm truy cập, và nhà cung cấp của hotspot. Thông tin thuộc tính người dùng của thiết bị người dùng có thể bao gồm thông tin nhận dạng người dùng (nghĩa là ID người dùng), tài khoản người dùng, và mật khẩu của tài khoản người dùng, v,v.. Thông tin dữ liệu kinh doanh lưu trữ trong thiết bị mạng có thể bao gồm tài khoản thẻ ngân hàng và mật khẩu của nó trong dịch vụ ngân hàng liên quan đến người sử dụng, hoặc tài khoản thành viên và thông tin thành viên trong dịch vụ thành viên liên quan đến người sử dụng. Chắc chắn là dữ liệu gốc hiện có hoặc được phát triển trong thời gian tới để truyền dữ liệu có thể được áp dụng cho sáng chế, và đều thuộc phạm vi của sáng chế.

Tốt hơn là, thông tin thuộc tính bao gồm địa chỉ vật lý của hotspot được chọn, trong đó địa chỉ vật lý (nghĩa là địa chỉ MAC) của hotspot được chọn trong phương án của sáng chế được thể hiện ở dạng là BSSID (nghĩa là địa chỉ MAC của hotspot) được thu nhận bởi hotspot trong địa chỉ vật lý thực tế. Tốt hơn là, thông tin thuộc tính cũng có thể bao gồm địa chỉ vật lý của hotspot được chọn (nghĩa là địa chỉ MAC) và thông tin nhận dạng người dùng (ID người dùng) của thiết bị người dùng thuộc hotspot được chọn. Do đó, thiết bị người dùng và hotspot được chọn được quét bởi thiết bị người dùng được xác định, để đảm bảo rằng dữ liệu gốc, cần được thu nhận sau khi dữ liệu mật mã được truyền được giải mã, được thu nhận chính xác và an toàn bởi thiết bị người dùng.

Hơn nữa, vị trí địa lý giải mã bao gồm:

vị trí địa lý của thiết bị người dùng sau khi thiết bị người dùng di chuyển khoảng cách định sẵn; và

vị trí địa lý trong lịch sử di chuyển địa lý của thiết bị người dùng.

Theo phương án khác của sáng chế, vị trí địa lý giải mã được sử dụng để thu nhận thông tin thuộc tính của hotspot có thể là vị trí địa lý thực tế của thiết bị người dùng sau khi thiết bị người dùng di chuyển trong khoảng cách định sẵn, hoặc vị trí địa lý thực tế trong lịch sử di chuyển địa lý của thiết bị người dùng. Bằng cách này, thông tin thuộc tính của hotspot có thể được thu nhận với điều kiện là thiết bị người dùng thực tế nằm ở vị trí địa lý giải mã thực tế, và sau đó dữ liệu mật mã nhận được được giải mã, do đó đảm bảo an toàn cho quá trình giải mã dữ liệu mật mã và dữ liệu gốc tương ứng sau khi dữ liệu mật mã được giải mã và thu nhận bởi thiết bị người dùng. Do người sử dụng bất hợp pháp không thể thu nhận vị trí địa lý giải mã thực tế của thông tin thuộc tính của hotspot để giải mã, người sử dụng bất hợp pháp không thể đạt được vị trí địa lý giải mã thực tế để thu nhận khóa mã hóa (thông tin thuộc tính của hotspot), điều này ngăn chặn người dùng bất hợp pháp khỏi việc thu nhận dữ liệu mật mã tại vị trí khác và giải mã dữ liệu mật mã.

Hơn nữa, thiết bị nhận 21 được cấu hình để:

nhận tên hotspot được gửi bởi thiết bị mạng.

Thiết bị giải mã 23 được cấu hình để:

sử dụng thông tin thuộc tính tương ứng với tên hotspot trong thông tin thuộc tính của hotspot được quét như khóa mã hóa, và giải mã dữ liệu mật mã để thu nhận dữ liệu gốc.

Theo phương án khác của sáng chế, để tạo thuận lợi cho thiết bị người dùng nhanh chóng quét hotspot bao gồm thông tin thuộc tính của hotspot này từ các hotspot được quét trong dải vị trí địa lý giải mã, sau khi tên hotspot (SSID) được gửi bằng thiết bị mạng được nhận, tên hotspot (SSID) nhận được được so sánh với thông tin thuộc tính của mỗi hotspot được quét. Sau đó, thông tin thuộc tính tương ứng với tên hotspot (SSID) thu nhận được và được sử dụng như khóa mã hóa để giải mã dữ liệu mật mã nhận được, để thu nhận được dữ liệu gốc. Khoá mã hóa để giải mã được nhanh chóng thu nhận dựa trên tên hotspot (SSID) và thông tin thuộc tính (BSSID, hoặc BSSID và ID người dùng, v.v.) của hotspot, qua đó thực hiện giải mã nhanh dữ liệu mật mã.

Hơn nữa, thiết bị giải mã 23 được cấu hình để:

nhận thuật toán giải mã được gửi bởi thiết bị mạng.

Thiết bị giải mã 23 được cấu hình để sử dụng thông tin thuộc tính của hotspot được quét như khóa mã hóa, và giải mã dữ liệu mật mã để thu nhận dữ liệu gốc, cụ thể được cấu hình để:

sử dụng thông tin thuộc tính của hotspot được quét như khóa mã hóa, và giải mã dữ liệu mật mã dựa trên thuật toán giải mã nhận và khóa mã hóa để thu nhận dữ liệu gốc. Theo phương án của sáng chế, thuật toán mã hóa có thể là thuật toán đảo ngược của AES, hoặc thuật toán đảo ngược của DES. Chắc chắn là thuật toán mã hóa hiện có khác hoặc được phát triển trong tương lai cho việc mã hóa dữ liệu gốc có thể được áp dụng cho sáng chế, và đều thuộc phạm vi của sáng chế.

Theo phương án khác, thông tin thuộc tính (ví dụ như địa chỉ vật lý BSSID và ID người dùng) của hotspot được quét được sử dụng như khóa mã hóa, và dữ liệu mật mã nhận được (ví dụ như dữ liệu mật mã bao gồm mật khẩu

của hotspot mà người dùng sử dụng cần để đăng nhập) được giải mã dựa trên khóa mã hóa (BSSID và ID người dùng) và thuật toán giải mã (ví dụ như thuật toán ngược của thuật toán mã hóa AES) nhận được bởi thiết bị người dùng trong quá trình truyền dữ liệu. Sau đó, dữ liệu gốc tương ứng (mật khẩu của hotspot mà người dùng sử dụng cần để đăng nhập) được thu nhận, để cho thiết bị người dùng thực hiện quá trình kinh doanh tương ứng và phản ứng trên thiết bị người dùng dựa trên dữ liệu gốc (mật khẩu của hotspot mà người dùng cần để đăng nhập) được thu nhận bằng cách giải mã. Do đó, thiết bị người dùng giải mã dữ liệu mật mã được gửi bởi thiết bị mạng dựa trên thông tin thuộc tính của hotspot được quét trong dải vị trí địa lý giải mã, để thu nhận được dữ liệu gốc mà thiết bị mạng cần truyền. Ngoài ra, do thông tin thuộc tính (khóa mã hóa) của hotspot để giải mã có thể thu được với điều kiện thiết bị người dùng thực tế đến vị trí địa lý giải mã, và sau đó dữ liệu mật mã được giải mã dựa trên khóa mã hóa này, nhờ đó đảm bảo an toàn cho dữ liệu gốc (ví dụ như mật khẩu của hotspot mà người dùng cần để đăng nhập) trong quá trình truyền dữ liệu.

Fig.4 thể hiện kịch bản ứng dụng thực tế của thiết bị người dùng trong quá trình truyền dữ liệu theo sáng chế. Dữ liệu mật mã bao gồm mật khẩu hotspot, và khóa mã hóa là địa chỉ vật lý BSSID của hotspot được quét. Đầu tiên, dữ liệu mật mã có mật khẩu hotspot mã hóa và tên hotspot SSID của hotspot được gửi bởi thiết bị mạng được nhận bởi thiết bị người dùng. Sau đó, thiết bị người dùng quét hotspot trong dải vị trí địa lý giải mã dựa trên tên hotspot SSID nhận được để thu nhận địa chỉ vật lý (BSSID) của hotspot tương ứng với tên hotspot SSID, địa chỉ vật lý (BSSID) của hotspot tương ứng được sử dụng làm khóa mã hóa. Sau đó, dữ liệu mật mã được giải mã dựa trên khóa mã hóa (BSSID) và thuật toán giải mã để thu nhận dữ liệu gốc tương ứng (mật khẩu hotspot). Thông tin thuộc tính của hotspot thu nhận được dựa trên vị trí địa lý giải mã thực tế được sử dụng như khóa mã hóa để giải mã dữ liệu mật mã nhận được, để thu nhận dữ liệu gốc tương ứng. Do đó, sự an toàn của dữ liệu gốc thu nhận bằng thiết bị người dùng được đảm bảo, ngăn ngừa việc người sử dụng bất hợp pháp ăn cắp dữ liệu gốc tại các vị trí khác.

Khi thiết bị người dùng cần thu nhận dữ liệu gốc của thiết bị mạng theo thời gian thực, thiết bị người dùng thu nhận dữ liệu theo khía cạnh khác của sáng chế cụ thể bao gồm:

xác định thiết bị thu nhận, được cấu hình để xác định vị trí địa lý thực tế hiện tại là vị trí địa lý giải mã hiện có; quét và chọn hotspot trong dải vị trí địa lý giải mã thực tế; và thu nhận thông tin thuộc tính (ví dụ như địa chỉ vật lý SSID của hotspot, cách khác, địa chỉ vật lý SSID của hotspot, và thông tin nhận dạng người sử dụng của thiết bị người dùng thuộc hotspot, tức là ID người dùng, v.v.) của hotspot được chọn;

thiết bị truyền yêu cầu, được cấu hình để gửi yêu cầu truy vấn dữ liệu đến thiết bị mạng dựa trên thông tin thuộc tính của hotspot được chọn; trong đó

sau khi yêu cầu truy vấn dữ liệu nhận được bởi thiết bị mạng, dữ liệu gốc được mã hóa mà thiết bị người dùng cần phải thu nhận trong thời gian thực được thu nhận; để đảm bảo an toàn của dữ liệu gốc được truyền, thiết bị mạng sử dụng thông tin thuộc tính của hotspot được chọn làm khóa mã hóa để mã hóa dữ liệu gốc được mã hóa và dữ liệu mật mã được thu nhận và gửi đến thiết bị người dùng;

thiết bị nhận dữ liệu mật mã, được cấu hình để nhận dữ liệu mật mã được trả về bởi thiết bị mạng dựa trên yêu cầu truy vấn dữ liệu; và

thiết bị giải mã, được cấu hình để sử dụng thông tin thuộc tính của hotspot được quét được chọn là khoá mã hóa để giải mã dữ liệu mật mã, để thu nhận dữ liệu gốc. Do đó, sự an toàn của dữ liệu gốc nhận được và tính kịp thời thu nhận dữ liệu gốc từ thiết bị mạng được đảm bảo.

Tóm lại, sáng chế sử dụng các bước sau. Đầu tiên, dữ liệu gốc được mã hóa được thu nhận bởi thiết bị mạng. Sau đó, vị trí địa lý giải mã của dữ liệu gốc được mã hóa được xác định, và hotspot trong dải vị trí địa lý giải mã được chọn. Sau đó, thông tin thuộc tính của hotspot được chọn được sử dụng như khóa mã hóa để mã hóa dữ liệu gốc được mã hóa, và dữ liệu mật mã được thu nhận và gửi đến thiết bị người dùng, trong đó thiết bị người dùng thu nhận thông tin thuộc tính bằng cách quét hotspot trong dải vị trí địa lý giải mã. Giải pháp theo

sáng chế thực hiện giải mã dữ liệu gốc dựa trên vị trí địa lý giải mã thực tế được sử dụng như khóa mã hóa của dữ liệu gốc được mã hóa. Do đó, dữ liệu gốc được gửi an toàn đến thiết bị người dùng, ngăn ngừa người sử dụng bất hợp pháp bẻ khóa mã hóa và thu nhận dữ liệu gốc tại các vị trí khác.

Hơn nữa, sau khi thiết bị người dùng nhận được dữ liệu mật mã được gửi bởi thiết bị mạng, thông tin thuộc tính của hotspot đã quét được thu nhận trong dải vị trí địa lý giải mã. Sau đó, thông tin thuộc tính của hotspot được quét được sử dụng như khóa mã hóa để giải mã dữ liệu mật mã, để thu nhận được dữ liệu gốc. Thông tin thuộc tính của hotspot được thu nhận dựa trên vị trí địa lý giải mã thực tế được sử dụng như khóa mã hóa để mã hóa dữ liệu mật mã nhận được, để thu nhận dữ liệu gốc tương ứng. Do đó, sự an toàn của dữ liệu gốc thu nhận bởi thiết bị người dùng được đảm bảo, ngăn ngừa người sử dụng bất hợp pháp ăn cắp dữ liệu gốc tại các vị trí khác.

Cần lưu ý rằng sáng chế có thể được triển khai trong phần mềm và/hoặc kết hợp phần mềm và phần cứng. Ví dụ, sáng chế có thể đạt được bằng cách sử dụng mạch tích hợp chuyên dụng ứng dụng (ASIC), máy tính đa năng hoặc thiết bị phần cứng tương tự khác. Trong một phương án, chương trình phần mềm trong sáng chế có thể được thực hiện bởi bộ xử lý để thực hiện các bước hoặc chức năng được mô tả ở trên. Tương tự, chương trình phần mềm (bao gồm các cấu trúc dữ liệu liên quan) trong sáng chế có thể được lưu trữ trong phương tiện ghi có thể đọc được bởi máy tính như bộ nhớ RAM, ổ đĩa từ hoặc ổ quang hoặc đĩa mềm và những thứ tương tự. Ngoài ra, một số bước hoặc chức năng của ứng dụng có thể được triển khai trong phần cứng, ví dụ: mạch hợp tác với bộ xử lý để thực hiện các bước hoặc chức năng.

Ngoài ra, một phần của sáng chế có thể được áp dụng cho sản phẩm chương trình máy tính, chẳng hạn như lệnh chương trình máy tính. Lệnh chương trình máy tính, khi được thực hiện bởi máy tính, có thể gọi hoặc cung cấp phương pháp và/hoặc giải pháp kỹ thuật theo sáng chế bằng các hoạt động của máy tính. Cần phải hiểu rằng dạng của lệnh chương trình máy tính trong phương tiện có thể đọc được bởi tính bao gồm, nhưng không giới hạn ở, tệp nguồn, tệp

thực thi, tệp gói cài đặt và tương tự. Theo cách khác, cách thức mà lệnh máy tính được thực thi bởi máy tính bao gồm, nhưng không giới hạn ở: máy tính trực tiếp thực hiện lệnh hoặc máy tính biên dịch lệnh và sau đó thực hiện chương trình được biên dịch tương ứng, hoặc máy tính đọc và thực hiện lệnh, hoặc máy tính đọc và cài đặt lệnh và sau đó thực hiện chương trình đã cài đặt tương ứng. Trong trường hợp này, phương tiện có thể đọc được bởi tính có thể là phương tiện lưu trữ bất kỳ có thể đọc được bởi tính hoặc phương tiện truyền thông bất kỳ mà máy tính có thể truy cập được.

Rõ ràng là sáng chế không giới hạn ở các chi tiết của các phương án minh họa ở trên, và sáng chế có thể được thực hiện trong các triển khai khác mà vẫn thuộc phạm vi của sáng chế. Do đó, các phương án nên được coi là có tính minh họa không giới hạn từ bất kỳ quan điểm nào. Phạm vi của sáng chế được xác định bởi các điểm yêu cầu bảo hộ thay vì phần mô tả ở trên. Do đó, tất cả các thay đổi nằm trong ý nghĩa và phạm vi tương đương của các yêu cầu bảo hộ đều được bao gồm trong sáng chế. Bất kỳ dấu hiệu tham chiếu nào trong các điểm yêu cầu bảo hộ không nên được hiểu là giới hạn các điểm yêu cầu bảo hộ này. Ngoài ra, rõ ràng là cụm từ "bao gồm" không loại trừ các yếu tố hoặc các bước khác và số ít không loại trừ số nhiều. Một số đơn vị hoặc thiết bị được mô tả trong phần yêu cầu bảo hộ cho thiết bị cũng có thể được thực hiện bởi một đơn vị hoặc thiết bị bằng phần mềm hoặc phần cứng. Các từ như thứ nhất, thứ hai và tương tự được sử dụng để biểu thị tên và không biểu thị bất kỳ trật tự cụ thể nào.

YÊU CẦU BẢO HỘ

1. Phương pháp truyền dữ liệu trên thiết bị mạng, phương pháp này bao gồm các bước:

- thu nhận dữ liệu gốc được mã hóa;

- bước xác định vị trí địa lý giải mã của dữ liệu gốc được mã hóa, và chọn hotspot trong dải vị trí địa lý giải mã; trong đó bước xác định vị trí địa lý giải mã của dữ liệu gốc được mã hóa bao gồm:

xác định vị trí địa lý trong khoảng cách định sẵn từ vị trí địa lý hiện tại của thiết bị người dùng như vị trí địa lý giải mã của dữ liệu gốc được mã hóa và xác định vị trí địa lý giải mã của dữ liệu gốc được mã hóa theo lịch sử di chuyển địa lý của thiết bị người dùng; và

bước sử dụng thông tin thuộc tính của hotspot là khóa mã hóa, mã hóa dữ liệu gốc được mã hóa để thu nhận dữ liệu mật mã, và gửi dữ liệu mật mã đến thiết bị người dùng, trong đó thông tin thuộc tính là có sẵn cho thiết bị người dùng bởi thiết bị người dùng quét hotspot trong dải vị trí địa lý giải mã,

trong đó dữ liệu gốc có thể bao gồm ít nhất một trong số thông tin dữ liệu thích hợp của hotspot, thông tin thuộc tính người dùng của thiết bị người dùng, hoặc thông tin dữ liệu kinh doanh được lưu trữ trong thiết bị mạng và trong đó dữ liệu kinh doanh được lưu trữ trong thiết bị mạng có thể bao gồm ít nhất một trong số tài khoản thẻ ngân hàng liên quan đến người sử dụng, mật khẩu trong dịch vụ ngân hàng liên quan đến người sử dụng, tài khoản thành viên trong dịch vụ thành viên liên quan đến người sử dụng, hoặc thông tin thành viên trong dịch vụ thành viên liên quan đến người sử dụng.

2. Phương pháp theo điểm 1, trong đó thông tin thuộc tính bao gồm địa chỉ vật lý của hotspot.

3. Phương pháp theo điểm 1, trong đó thông tin thuộc tính bao gồm địa chỉ vật lý của hotspot và thông tin nhận dạng người dùng của thiết bị người dùng, trong đó hotspot thuộc về thiết bị người dùng.

4. Phương pháp theo điểm 1, trong đó khi dữ liệu gốc được mã hóa được mã hóa để thu được dữ liệu mật mã và dữ liệu mật mã được gửi đến thiết bị người dùng, phương pháp này còn bao gồm:

gửi tên hotspot tương ứng với hotspot đến thiết bị người dùng.

5. Phương pháp theo điểm 1, trong đó bước sử dụng thông tin thuộc tính của hotspot là khóa mã hóa, mã hóa dữ liệu gốc được mã hóa để thu nhận dữ liệu mật mã, và gửi dữ liệu mật mã đến thiết bị người dùng, bao gồm:

sử dụng thông tin thuộc tính tương ứng với hotspot như khóa mã hóa, mã hóa dữ liệu gốc được mã hóa dựa trên thuật toán mã hóa cài sẵn và khóa mã hóa để thu nhận dữ liệu mật mã, và gửi dữ liệu mật mã đến thiết bị người dùng.

6. Phương pháp theo điểm 1, trong đó trong dữ liệu gốc bao gồm ít nhất một trong số sau:

thông tin dữ liệu thích hợp của hotspot;

thông tin thuộc tính người dùng của thiết bị người dùng; và

thông tin dữ liệu kinh doanh được lưu trữ trong thiết bị mạng.

7. Phương pháp theo điểm 1, trong đó khi dữ liệu gốc được mã hóa được mã hóa để thu nhận dữ liệu mật mã và dữ liệu mật mã được gửi đến thiết bị người dùng, phương pháp này còn bao gồm:

gửi thuật toán giải mã cài sẵn đến thiết bị người dùng.

8. Phương pháp nhận dữ liệu trên thiết bị người dùng, phương pháp này bao gồm:

bước xác định vị trí địa lý thực tế hiện tại là vị trí địa lý giải mã hiện tại, quét và chọn hotspot trong dải vị trí địa lý giải mã hiện tại và thu nhận thông tin thuộc tính của hotspot;

gửi yêu cầu truy vấn dữ liệu đến thiết bị mạng dựa trên thông tin thuộc tính của hotspot;

nhận dữ liệu mật mã được thiết bị mạng trả về dựa trên yêu cầu truy vấn dữ liệu; và

bước sử dụng thông tin thuộc tính của hotspot là khóa mã hóa, và giải mã dữ liệu mật mã để thu nhận dữ liệu gốc

trong đó thông tin thuộc tính bao gồm địa chỉ vật lý của hotspot và dữ liệu gốc có thể bao gồm ít nhất một trong số thông tin dữ liệu thích hợp của hotspot, thông tin thuộc tính người dùng của thiết bị người dùng, hoặc thông tin dữ liệu kinh doanh được lưu trữ trong thiết bị mạng và trong đó dữ liệu kinh doanh được lưu trữ trong thiết bị mạng có thể bao gồm ít nhất một trong số tài khoản thẻ ngân hàng liên quan đến người sử dụng, mật khẩu trong dịch vụ ngân hàng liên quan đến người sử dụng, tài khoản thành viên trong dịch vụ thành viên liên quan đến người sử dụng, hoặc thông tin thành viên trong dịch vụ thành viên liên quan đến người sử dụng.

9. Phương pháp theo điểm 1, trong đó thông tin dữ liệu thích hợp của hotspot có thể bao gồm ít nhất một trong số tên hotspot của hotspot, thông tin vị trí địa lý của hotspot, hoặc nhà cung cấp hotspot.

10. Phương pháp theo điểm 1, trong đó thông tin thuộc tính người dùng của thiết bị người dùng có thể bao gồm thông tin nhận dạng người dùng của tài khoản người dùng.

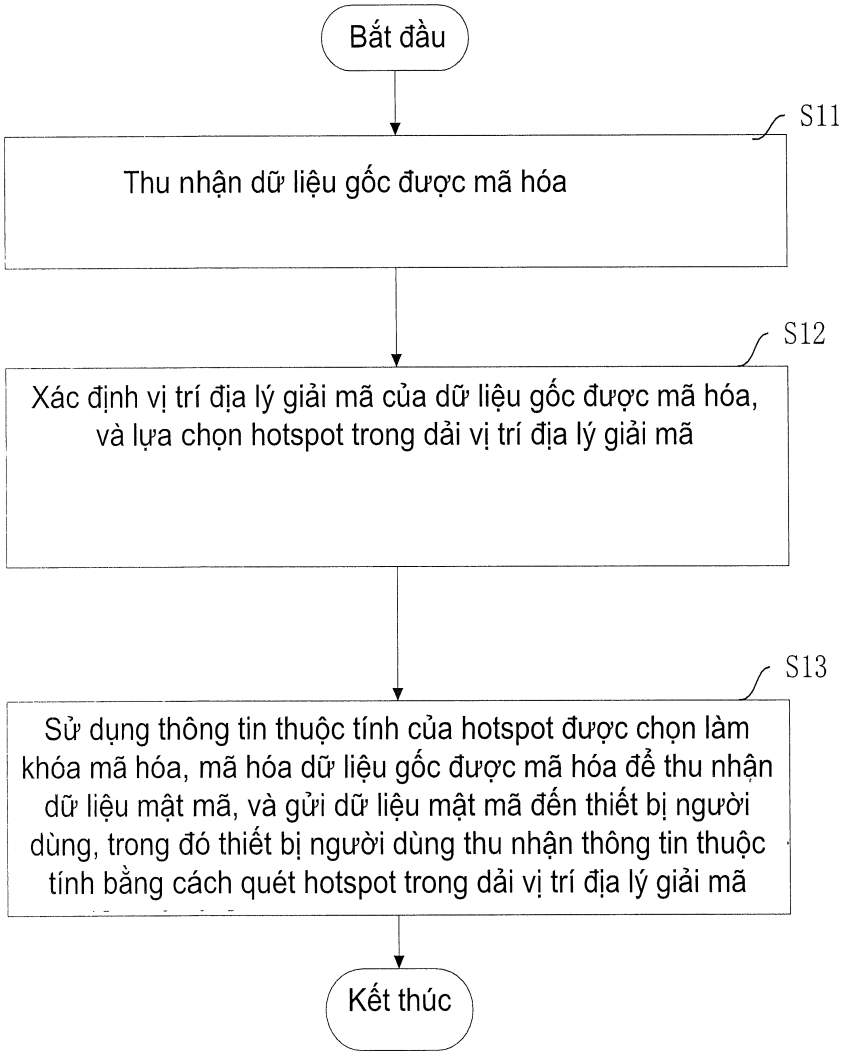

Bắt đầu
S11
Thu nhận dữ liệu gốc được mã hóa
S12
Xác định vị trí địa lý giải mã của dữ liệu gốc được mã hóa, và lựa chọn hotspot trong dải vị trí địa lý giải mã
S13
Sử dụng thông tin thuộc tính của hotspot được chọn làm khóa mã hóa, mã hóa dữ liệu gốc được mã hóa để thu nhận dữ liệu mật mã, và gửi dữ liệu mật mã đến thiết bị người dùng, trong đó thiết bị người dùng thu nhận thông tin thuộc tính bằng cách quét hotspot trong dải vị trí địa lý giải mã
Kết thúc

FIG. 1

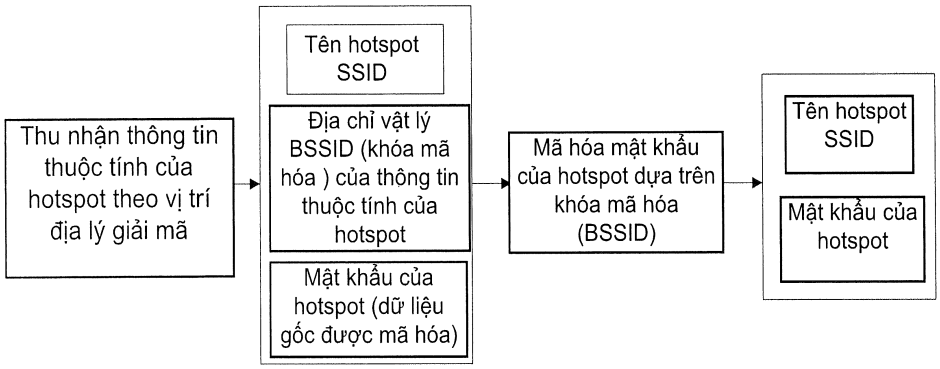

Thu nhận thông tin thuộc tính của hotspot theo vị trí địa lý giải mã
Tên hotspot SSID
Địa chỉ vật lý BSSID (khóa mã hóa) của thông tin thuộc tính của hotspot
Mật khẩu của hotspot (dữ liệu gốc được mã hóa)
Mã hóa mật khẩu của hotspot dựa trên khóa mã hóa (BSSID)
Tên hotspot SSID
Mật khẩu của hotspot

FIG. 2

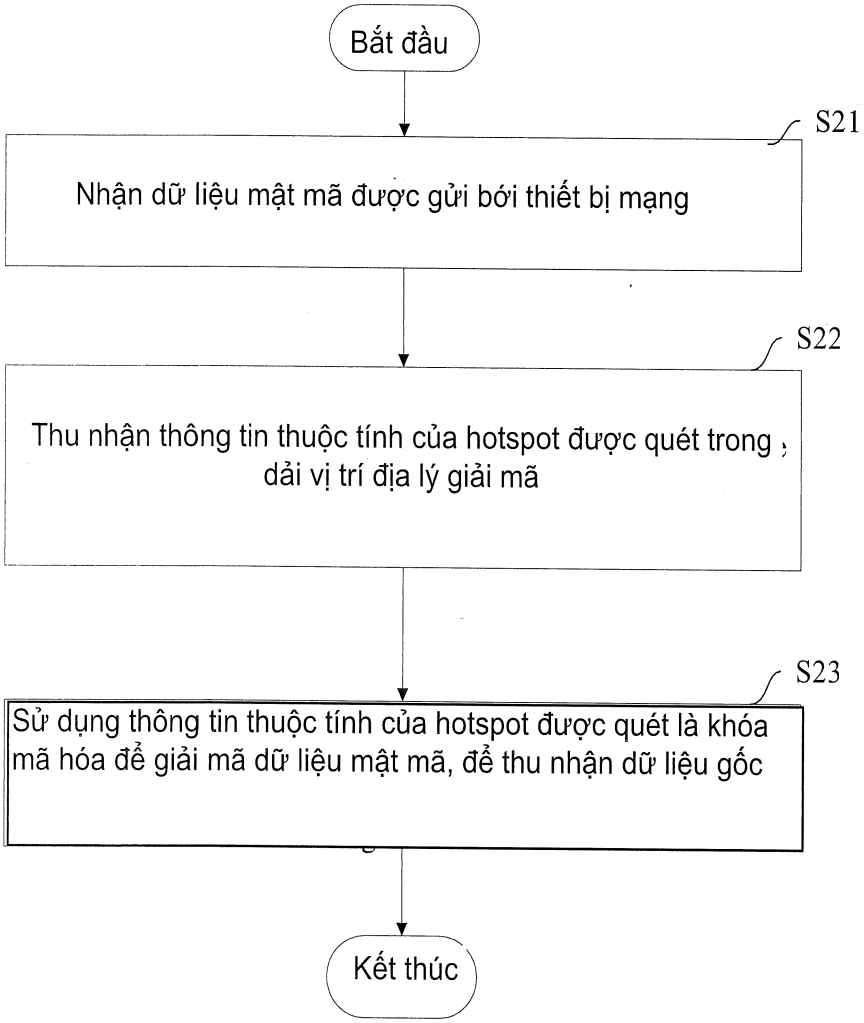

Bắt đầu
S21
Nhận dữ liệu mật mã được gửi bởi thiết bị mạng
S22
Thu nhận thông tin thuộc tính của hotspot được quét trong dải vị trí địa lý giải mã
S23
Sử dụng thông tin thuộc tính của hotspot được quét là khóa mã hóa để giải mã dữ liệu mật mã, để thu nhận dữ liệu gốc
Kết thúc

FIG. 3


Quét và thu nhận SSID tên hotspot và thông tin thuộc tính của hotspot trong dải vị trí địa lý giải mã
Tên hotspot SSID
Địa chỉ vật lý BSSID (khóa mã hóa) của thông tin thuộc tính của hotspot
Dữ liệu mật mã mã hóa (bao gồm mật khẩu hotspot)
Giải mã dữ liệu mật mã dựa trên khóa mã hóa (BSSID)
Tên hotspot SSID
Mật khẩu hotspot

FIG. 4

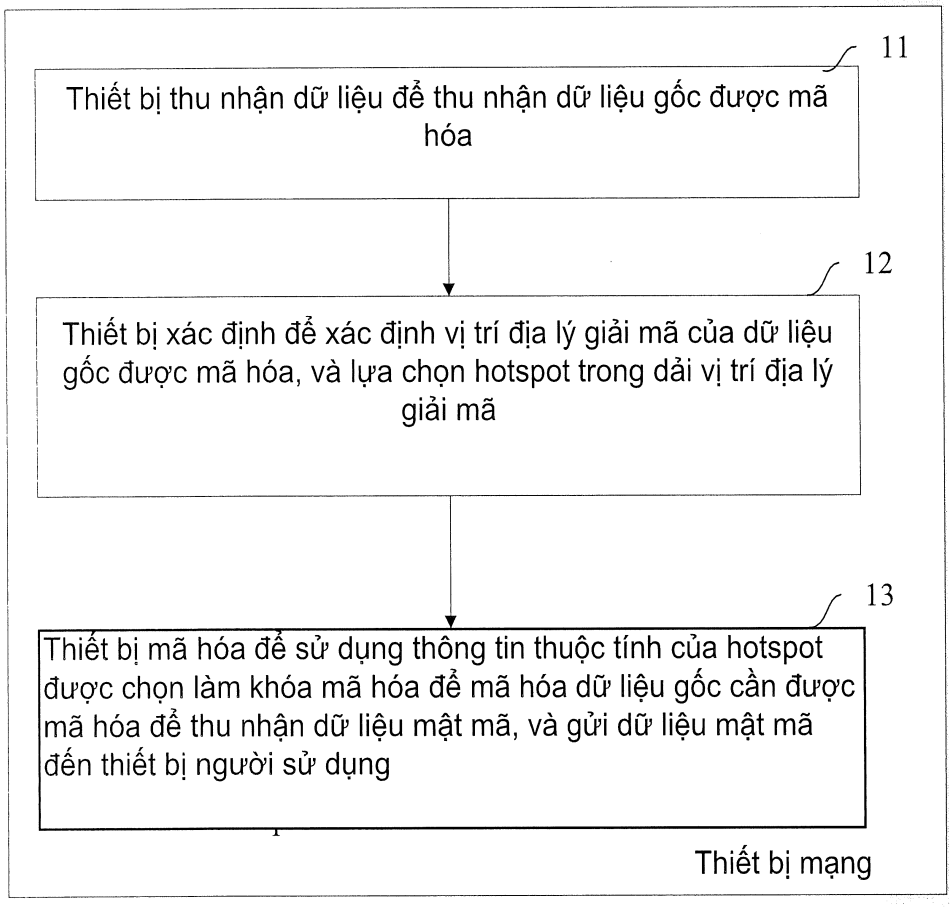

11
Thiết bị thu nhận dữ liệu để thu nhận dữ liệu gốc được mã hóa
12
Thiết bị xác định để xác định vị trí địa lý giải mã của dữ liệu gốc được mã hóa, và lựa chọn hotspot trong dải vị trí địa lý giải mã
13
Thiết bị mã hóa để sử dụng thông tin thuộc tính của hotspot được chọn làm khóa mã hóa để mã hóa dữ liệu gốc cần được mã hóa để thu nhận dữ liệu mật mã, và gửi dữ liệu mật mã đến thiết bị người sử dụng
Thiết bị mạng

FIG. 5

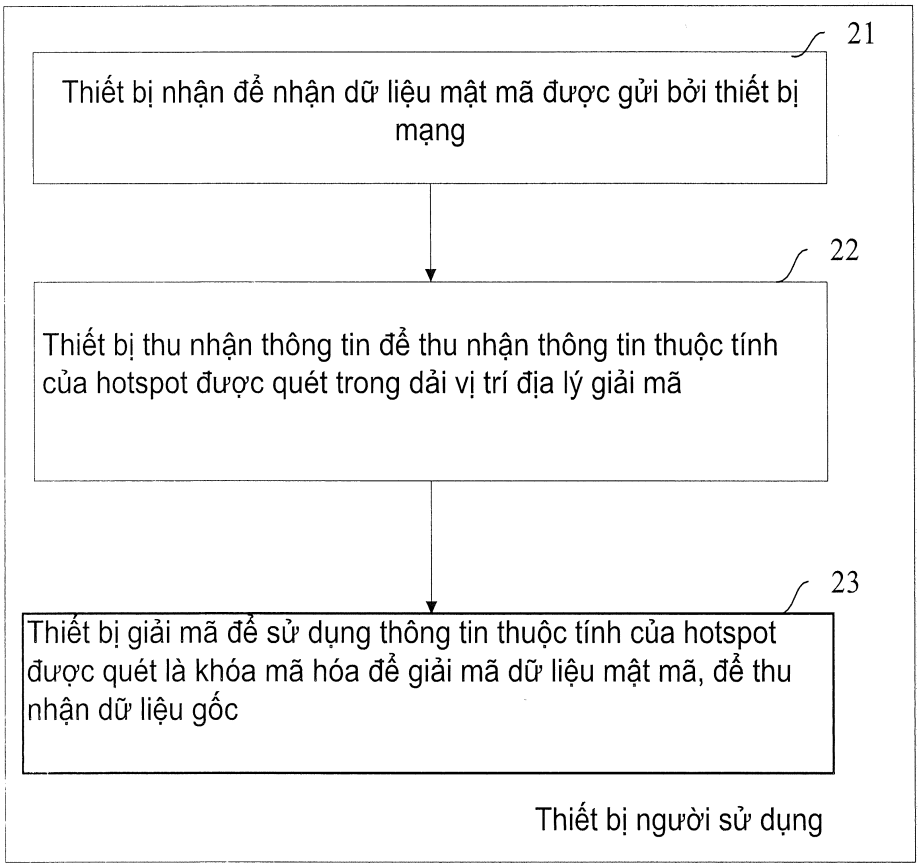

21
Thiết bị nhận để nhận dữ liệu mật mã được gửi bởi thiết bị mạng
22
Thiết bị thu nhận thông tin để thu nhận thông tin thuộc tính của hotspot được quét trong dải vị trí địa lý giải mã
23
Thiết bị giải mã để sử dụng thông tin thuộc tính của hotspot được quét là khóa mã hóa để giải mã dữ liệu mật mã, để thu nhận dữ liệu gốc
Thiết bị người sử dụng

FIG. 6