(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) **1-0048204**

(51)[2021.01] **H04W 12/00**; H04W 12/04; H04L 9/32 (13) **B**

(21) 1-2022-03720 (22) 26/11/2020
(86) PCT/CN2020/131968 26/11/2020 (87) WO 2021/104408 03/06/2021
(30) 201911207543.X 29/11/2019 CN
(45) 25/07/2025 448 (43) 25/08/2022 413A
(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)
Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129, P. R. China
(72) GAN, Lu (CN); HUANG, Jianhao (CN); MA, Xiaoshuang (CN); ZHOU, Chong (CN).
(74) Công ty Cổ phần Sở hữu công nghiệp INVESTIP (INVESTIP)

(54) PHƯƠNG PHÁP ĐÀM PHÁN KHÓA, THIẾT BỊ ĐIỆN TỬ, CHIP, PHƯƠNG TIỆN LƯU TRỮ MÁY TÍNH, VÀ HỆ THỐNG TRUYỀN THÔNG

(21) 1-2022-03720

(57) Sáng chế đề cập đến phương pháp đàm phán khóa, thiết bị điện tử, chip, phương tiện lưu trữ máy tính, và hệ thống truyền thông, và đề cập đến lĩnh vực công nghệ truyền thông. Cụ thể, phương pháp bao gồm: Thiết bị điều khiển mạng lưới thiết bị kết nối Internet (Internet of Things, IoT) truyền đa hướng, trong mạng cục bộ thứ nhất, thông điệp khám phá mà mang khóa công khai thứ nhất, và gửi văn bản mật mã thứ hai đến thiết bị IoT thứ nhất sau khi nhận văn bản mật mã thứ nhất và khóa công khai thứ hai. Sau khi nhận văn bản mật mã thứ ba từ thiết bị IoT thứ nhất, thiết bị điều khiển IoT giải mã văn bản mật mã thứ ba dựa trên khóa phiên thứ nhất, để thu được chữ ký thứ hai và thông tin phiên thứ hai; xác minh chữ ký thứ hai dựa trên khóa công khai dài hạn của thiết bị IoT thứ nhất; và thực hiện truyền thông được mã hóa với thiết bị IoT thứ nhất dựa trên khóa phiên thứ nhất sau khi chữ ký thứ hai được xác minh thành công. Trong giải pháp kỹ thuật như vậy, vì thiết bị điều khiển IoT thêm khóa công khai thứ nhất vào thông điệp khám phá, quá trình đàm phán trạm đến trạm được tích hợp vào trong quá trình khám phá, do đó giúp giảm số lượng thông điệp trao đổi giữa thiết bị IoT và thiết bị điều khiển IoT, và cải thiện hiệu quả của việc thu được khóa phiên.

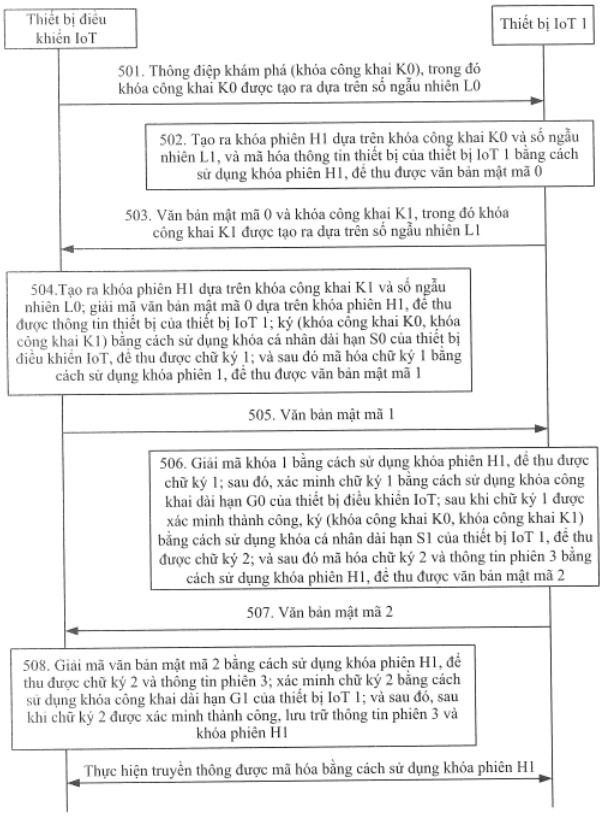


FIG. 5

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực công nghệ truyền thông, và cụ thể, là đến phương pháp đàm phán khóa và thiết bị điện tử.

Tình trạng kỹ thuật của sáng chế

Sau khi thiết bị mạng lưới thiết bị kết nối Internet (internet of things, IoT) truy nhập mạng, người dùng có thể điều khiển thiết bị IoT bằng cách sử dụng chương trình ứng dụng IoT (ứng dụng IoT viết tắt dưới đây) được lắp đặt trên điện thoại di động. Trong ví dụ, thiết bị IoT là đèn bàn thông minh. Người dùng thực hiện thao tác tương ứng trên ứng dụng IoT được lắp đặt trên điện thoại di động, sao cho điện thoại di động có thể gửi chỉ thị điều khiển đến đèn bàn thông minh để phản hồi lại thao tác của người dùng, để điều khiển đèn bàn thông minh, ví dụ, điều khiển đèn bàn thông minh để được bật hoặc tắt.

Để đảm bảo bảo mật của truyền thông giữa điện thoại di động và thiết bị IoT, khóa phiên thường được sử dụng để thực hiện truyền thông được mã hóa giữa điện thoại di động và thiết bị IoT. Tuy nhiên, trong mô tả trước, khóa phiên thu được bởi điện thoại di động thông qua đàm phán đầu cuối (trạm đến trạm, station to station, STS) với thiết bị IoT sau khi tìm ra thiết bị IoT. Cách thu được khóa phiên này có hiệu quả tương đối thấp.

Bản chất kỹ thuật của sáng chế

Sáng chế đề xuất phương pháp đàm phán khóa và thiết bị điện tử, để giảm số lượng thông điệp trao đổi giữa thiết bị IoT và thiết bị điều khiển IoT, để cải thiện hiệu quả của việc thu được khóa phiên.

Theo khía cạnh thứ nhất, phương án của sáng chế đề xuất phương pháp đàm phán khóa, cụ thể bao gồm:

Thiết bị điều khiển IoT truyền đa hướng thông điệp khám phá trong mạng cục bộ thứ nhất. Thông điệp khám phá bao gồm khóa công khai thứ nhất. Mạng cục bộ thứ nhất là mạng mà đã được truy nhập bởi thiết bị điều khiển IoT. Khóa công khai thứ nhất thu được dựa trên số ngẫu nhiên thứ nhất.

Thiết bị IoT thứ nhất nhận thông điệp khám phá từ thiết bị điều khiển IoT, và gửi phản hồi khám phá đến thiết bị điều khiển IoT. Phản hồi khám phá bao gồm văn bản mật mã thứ nhất và khóa công khai thứ hai. Văn bản mật mã thứ nhất thu được bằng cách mã

hóa thông tin thiết bị của thiết bị IoT thứ nhất dựa trên khóa phiên thứ nhất. Khóa công khai thứ hai thu được dựa trên số ngẫu nhiên thứ hai. Khóa phiên thứ nhất thu được bởi thiết bị IoT thứ nhất dựa trên số ngẫu nhiên thứ hai và khóa công khai thứ nhất.

Sau khi nhận phản hồi khám phá từ thiết bị IoT thứ nhất, thiết bị điều khiển IoT gửi văn bản mật mã thứ hai đến thiết bị IoT thứ nhất. Văn bản mật mã thứ hai thu được bằng cách mã hóa chữ ký thứ nhất dựa trên khóa phiên thứ nhất. Chữ ký thứ nhất là chữ ký trên thông tin phiên thứ nhất dựa trên khóa cá nhân dài hạn của thiết bị điều khiển IoT. Thông tin phiên thứ nhất bao gồm khóa công khai thứ nhất và khóa công khai thứ hai. Khóa phiên thứ nhất thu được bởi thiết bị điều khiển IoT dựa trên số ngẫu nhiên thứ nhất và khóa công khai thứ hai.

Sau khi nhận văn bản mật mã thứ hai được gửi bởi thiết bị điều khiển IoT, thiết bị IoT thứ nhất giải mã văn bản mật mã thứ hai dựa trên khóa phiên thứ nhất, để thu được chữ ký thứ nhất. Ngoài ra, thiết bị IoT thứ nhất gửi văn bản mật mã thứ ba đến thiết bị điều khiển IoT sau khi xác minh thành công chữ ký thứ nhất dựa trên khóa công khai dài hạn của thiết bị điều khiển IoT. Văn bản mật mã thứ ba thu được bằng cách mã hóa chữ ký thứ hai và thông tin phiên thứ hai dựa trên khóa phiên thứ nhất. Chữ ký thứ hai là chữ ký trên thông tin phiên thứ ba dựa trên khóa cá nhân dài hạn của thiết bị IoT. Thông tin phiên thứ ba bao gồm khóa công khai thứ hai và khóa công khai thứ nhất. Thông tin phiên thứ hai bao gồm mã định danh (identifier, ID) phiên.

Sau khi nhận văn bản mật mã thứ ba từ thiết bị IoT thứ nhất, thiết bị điều khiển IoT giải mã văn bản mật mã thứ ba dựa trên khóa phiên thứ nhất, để thu được chữ ký thứ hai và thông tin phiên thứ hai; và xác minh chữ ký thứ hai dựa trên khóa công khai dài hạn của thiết bị IoT thứ nhất. Sau khi chữ ký thứ hai được xác minh thành công, thiết bị điều khiển IoT lưu trữ khóa phiên thứ nhất và thông tin phiên thứ hai.

Cuối cùng, thiết bị điều khiển IoT thực hiện truyền thông được mã hóa với thiết bị IoT thứ nhất dựa trên khóa phiên thứ nhất.

Theo phương án này của sáng chế, vì thiết bị điều khiển IoT thêm khóa công khai thứ nhất vào thông điệp khám phá và truyền đa hướng thông điệp khám phá đến thiết bị IoT, quá trình đàm phán STS được tích hợp vào trong quá trình khám phá. Điều này giúp giảm số lượng thông điệp trao đổi giữa thiết bị IoT và thiết bị điều khiển IoT, và cải thiện hiệu quả của việc thu được khóa phiên. Ngoài ra, trong quá trình khám phá, thiết bị IoT có thể còn mã hóa thông tin thiết bị bằng cách sử dụng khóa phiên, và sau đó gửi thông

tin thiết bị được mã hóa đến thiết bị điều khiển IoT, do đó giảm nguy cơ tấn công gây ra bởi việc bộc lộ thông tin thiết bị của thiết bị IoT trong mạng.

Trong thiết kế khả thi, thông tin phiên thứ hai còn bao gồm khoảng thời gian hiệu lực của khóa phiên thứ nhất. Giải pháp kỹ thuật trên giúp giảm nguy cơ rò rỉ khóa phiên thứ nhất, và cải thiện bảo mật của truyền thông giữa thiết bị điều khiển IoT và thiết bị IoT.

Trong thiết kế khả thi, sau khi nhận thông điệp khám phá từ thiết bị điều khiển IoT, thiết bị IoT thứ nhất gửi phản hồi khám phá đến thiết bị điều khiển IoT nếu thiết bị IoT thứ nhất xác định rằng khóa phiên thứ hai được lưu trữ giữa thiết bị IoT thứ nhất và thiết bị điều khiển IoT không ở trong khoảng thời gian hiệu lực hoặc không có thông tin phiên giữa thiết bị IoT thứ nhất và thiết bị IoT được lưu trữ.

Trong thiết kế khả thi, sau khi nhận thông điệp khám phá, thiết bị IoT thứ nhất gửi văn bản mật mã thứ tư đến thiết bị điều khiển IoT nếu thiết bị IoT thứ nhất xác định rằng khóa phiên thứ hai được lưu trữ giữa thiết bị IoT thứ nhất và thiết bị điều khiển IoT ở trong khoảng thời gian hiệu lực hoặc thông tin phiên được lưu trữ giữa thiết bị IoT thứ nhất và thiết bị IoT không bị mất. Văn bản mật mã thứ tư thu được bằng cách mã hóa thông tin thứ nhất dựa trên khóa phiên thứ nhất. Thông tin thứ nhất bao gồm thông tin thiết bị của thiết bị IoT. Sau khi nhận văn bản mật mã thứ tư được gửi bởi thiết bị IoT thứ nhất, thiết bị điều khiển IoT thực hiện truyền thông được mã hóa với thiết bị IoT thứ nhất dựa trên khóa phiên thứ hai nếu thiết bị điều khiển IoT xác định rằng khóa phiên thứ hai được lưu trữ giữa thiết bị điều khiển IoT và thiết bị IoT thứ nhất ở trong khoảng thời gian hiệu lực hoặc thông tin phiên được lưu trữ giữa thiết bị điều khiển IoT và thiết bị IoT thứ nhất không bị mất. Khi khóa phiên thứ hai được lưu trữ trong thiết bị IoT thứ nhất và thiết bị điều khiển IoT ở trong khoảng thời gian hiệu lực, hoặc thông tin phiên được lưu trữ giữa thiết bị IoT thứ nhất và thiết bị điều khiển IoT không bị mất, thiết bị điều khiển IoT và thiết bị IoT thứ nhất thực hiện truyền thông được mã hóa dựa trên khóa phiên thứ hai, do đó còn giúp giảm số lượng thông điệp trao đổi, và cải thiện hiệu quả của đàm phán khóa phiên.

Trong thiết kế khả thi, thông tin thứ nhất còn bao gồm thông tin phiên thứ tư, và thông tin phiên thứ tư bao gồm ID được lưu trữ của phiên với thiết bị IoT thứ nhất, sao cho thiết bị điều khiển IoT tìm kiếm thông tin phiên giữa thiết bị điều khiển IoT và thiết bị IoT thứ nhất.

Trong thiết kế khả thi, thiết bị điều khiển IoT có thể truyền đa hướng thông điệp khám phá theo cách sau:

truyền đa hướng định kỳ thông điệp khám phá trong mạng cục bộ thứ nhất; và/hoặc

truyền đa hướng thông điệp khám phá trong mạng cục bộ thứ nhất khi chuyển mạch từ mạng cục bộ thứ hai sang mạng cục bộ thứ nhất; và/hoặc

truyền đa hướng thông điệp khám phá trong mạng cục bộ thứ nhất khi được liên kết với thiết bị IoT mới; và/hoặc

truyền đa hướng thông điệp khám phá trong mạng cục bộ thứ nhất khi khóa phiên của thiết bị IoT thứ hai đạt đến thời điểm hết hạn của khoảng thời gian hiệu lực.

Trong thiết kế khả thi, thiết bị IoT thứ nhất có thể nhận, theo cách sau, sự truyền đa hướng thông điệp khám phá bởi thiết bị điều khiển IoT trong mạng cục bộ thứ nhất:

nhận định kỳ sự truyền đa hướng thông điệp khám phá bởi thiết bị điều khiển IoT trong mạng cục bộ thứ nhất; và/hoặc

nhận, trong lúc chuyển mạch mạng, sự truyền đa hướng thông điệp khám phá bởi thiết bị điều khiển IoT trong mạng cục bộ thứ nhất; và/hoặc

nhận, sau khi được liên kết với thiết bị điều khiển IoT, sự truyền đa hướng thông điệp khám phá bởi thiết bị điều khiển IoT trong mạng cục bộ thứ nhất; và/hoặc

nhận, khi khóa phiên thứ hai được lưu trữ giữa thiết bị IoT thứ nhất và thiết bị điều khiển IoT đạt đến thời điểm hết hạn của khoảng thời gian hiệu lực, sự truyền đa hướng thông điệp khám phá bởi thiết bị điều khiển IoT trong mạng cục bộ thứ nhất.

Trong thiết kế khả thi, thiết bị IoT thứ nhất ở trong mạng cục bộ thứ hai.

Theo khía cạnh thứ hai, phương án của sáng chế đề xuất hệ thống truyền thông, bao gồm thiết bị điều khiển IoT và thiết bị IoT thứ nhất.

Thiết bị điều khiển IoT được tạo cấu hình để truyền đa hướng thông điệp khám phá trong mạng cục bộ thứ nhất. Thông điệp khám phá bao gồm khóa công khai thứ nhất. Mạng cục bộ thứ nhất là mạng mà đã được truy nhập bởi thiết bị điều khiển IoT. Khóa công khai thứ nhất thu được dựa trên số ngẫu nhiên thứ nhất.

Thiết bị điều khiển IoT thứ nhất còn được tạo cấu hình để: nhận phản hồi khám phá từ thiết bị IoT thứ nhất, và gửi văn bản mật mã thứ hai đến thiết bị IoT thứ nhất. Phản hồi khám phá bao gồm văn bản mật mã thứ nhất và khóa công khai thứ hai. Văn bản mật mã thứ nhất thu được bằng cách mã hóa thông tin thiết bị của thiết bị IoT thứ nhất dựa trên khóa phiên thứ nhất. Khóa công khai thứ hai thu được dựa trên số ngẫu nhiên thứ

hai. Văn bản mật mã thứ hai thu được bằng cách mã hóa chữ ký thứ nhất dựa trên khóa phiên thứ nhất. Chữ ký thứ nhất là chữ ký trên thông tin phiên thứ nhất dựa trên khóa cá nhân dài hạn của thiết bị điều khiển IoT. Thông tin phiên thứ nhất bao gồm khóa công khai thứ nhất và khóa công khai thứ hai. Khóa phiên thứ nhất thu được bởi thiết bị điều khiển IoT dựa trên số ngẫu nhiên thứ nhất và khóa công khai thứ hai.

Thiết bị điều khiển IoT còn được tạo cấu hình để: nhận văn bản mật mã thứ ba từ thiết bị IoT thứ nhất, và giải mã văn bản mật mã thứ ba dựa trên khóa phiên thứ nhất, để thu được chữ ký thứ hai và thông tin phiên thứ hai, sau đó, xác minh chữ ký thứ hai dựa trên khóa công khai dài hạn của thiết bị IoT thứ nhất; lưu trữ khóa phiên thứ nhất và thông tin phiên thứ hai sau khi chữ ký thứ hai được xác minh thành công; và cuối cùng, thực hiện truyền thông được mã hóa với thiết bị IoT thứ nhất dựa trên khóa phiên thứ nhất.

Thiết bị IoT thứ nhất được tạo cấu hình để: nhận thông điệp khám phá từ thiết bị điều khiển IoT, và gửi phản hồi khám phá đến thiết bị điều khiển; nhận văn bản mật mã thứ hai được gửi bởi thiết bị điều khiển IoT, và sau đó giải mã văn bản mật mã thứ hai dựa trên khóa phiên thứ nhất để thu được chữ ký thứ nhất; và gửi văn bản mật mã thứ ba đến thiết bị điều khiển IoT sau khi thiết bị IoT thứ nhất xác minh thành công chữ ký thứ nhất dựa trên khóa công khai dài hạn của thiết bị điều khiển IoT. Văn bản mật mã thứ ba thu được bằng cách mã hóa chữ ký thứ hai và thông tin phiên thứ hai dựa trên khóa phiên thứ nhất. Chữ ký thứ hai là chữ ký trên thông tin phiên thứ ba dựa trên khóa cá nhân dài hạn của thiết bị IoT. Thông tin phiên thứ ba bao gồm khóa công khai thứ hai và khóa công khai thứ nhất. Thông tin phiên thứ hai bao gồm mã định danh (identifier, ID) phiên.

Theo khía cạnh thứ ba, phương án của sáng chế đề xuất thiết bị điện tử, bao gồm bộ xử lý, bộ nhớ, và bộ truyền nhận. Bộ xử lý được ghép nối với bộ nhớ và bộ truyền nhận. Bộ nhớ lưu trữ các chỉ thị chương trình. Bộ xử lý được tạo cấu hình để đọc và thực thi các chỉ thị chương trình được lưu trữ trong bộ nhớ. Khi các chỉ thị chương trình được thực thi bởi bộ xử lý, thiết bị điện tử được cho phép để triển khai các bước được thực hiện bởi thiết bị điều khiển IoT hoặc thiết bị IoT trong phương pháp theo bất kỳ một trong số khía cạnh thứ nhất và các thiết kế khả thi của khía cạnh thứ nhất theo các phương án của sáng chế.

Theo khía cạnh thứ tư, phương án của ứng dụng đề xuất thiết bị điện tử, bao gồm bộ máy cho việc thực hiện các bước được thực hiện bởi thiết bị điều khiển IoT hoặc thiết

bị IoT trong phương pháp theo bất kỳ một trong số khía cạnh thứ nhất và các thiết kế khả thi của khía cạnh thứ nhất.

Theo khía cạnh thứ năm, phương án của sáng chế đề xuất phương tiện lưu trữ đọc được bằng máy tính. Phương tiện lưu trữ đọc được bằng máy tính lưu trữ các chỉ thị chương trình. Khi các chỉ thị chương trình chạy trên thiết bị điện tử, thiết bị điện tử được cho phép để thực hiện các bước được thực hiện bởi thiết bị điều khiển IoT hoặc thiết bị IoT trong phương pháp theo bất kỳ một trong số khía cạnh thứ nhất và các thiết kế khả thi của khía cạnh thứ nhất theo các phương án của sáng chế.

Theo khía cạnh thứ sáu, phương án của sáng chế đề xuất sản phẩm chương trình máy tính. Khi sản phẩm chương trình máy tính chạy trên thiết bị điện tử, thiết bị điện tử được cho phép để thực hiện các bước được thực hiện bởi thiết bị điều khiển IoT hoặc thiết bị IoT trong phương pháp theo bất kỳ một trong số khía cạnh thứ nhất và các thiết kế khả thi của khía cạnh thứ nhất theo các phương án của sáng chế.

Theo khía cạnh thứ bảy, phương án của sáng chế đề xuất chip. Chip được ghép nối với bộ nhớ trong thiết bị điện tử, và điều khiển thiết bị điện tử để thực hiện các bước được thực hiện bởi thiết bị điều khiển IoT hoặc thiết bị IoT trong phương pháp theo bất kỳ một trong số khía cạnh thứ nhất và các thiết kế khả thi của khía cạnh thứ nhất theo các phương án của sáng chế.

Ngoài ra, đối với các hiệu quả kĩ thuật được đem lại bởi khía cạnh thứ hai đến khía cạnh thứ bảy, tham chiếu đến các mô tả liên quan của các phương pháp thiết kế trong phần phương pháp trên. Các chi tiết không được mô tả ở đây lần nữa.

Cần lưu ý rằng "việc ghép nối" theo các phương án của sáng chế có nghĩa rằng hai thành phần được kết nối trực tiếp hoặc gián tiếp với nhau.

Mô tả vắn tắt các hình vẽ

Fig.1 là kịch bản mà trong đó thiết bị điều khiển IoT điều khiển thiết bị IoT theo phương án của sáng chế;

Fig.2 là kịch bản khác mà trong đó thiết bị điều khiển IoT điều khiển thiết bị IoT theo phương án của sáng chế;

Fig.3 là lưu đồ dạng giản đồ của phương pháp đàm phán khóa theo phương án của sáng chế;

Fig.4 là sơ đồ dạng giản đồ của kiến trúc mạng theo phương án của sáng chế;

Fig.5 là lưu đồ dạng giản đồ của phương pháp đàm phán khóa khác theo phương

án của sáng chế;

Fig.6 là sơ đồ dạng giản đồ của quy trình liên kết thiết bị IoT theo phương án của sáng chế;

Fig.7A đến Fig.7E là sơ đồ dạng giản đồ của giao diện người dùng theo phương án của sáng chế;

Fig.8 là sơ đồ dạng giản đồ của giao diện người dùng khác theo phương án của sáng chế;

Fig.9 là sơ đồ dạng giản đồ của giao diện người dùng khác theo phương án của sáng chế;

Fig.10 là lưu đồ dạng giản đồ của phương pháp đàm phán khóa khác theo phương án của sáng chế;

Fig.11 là sơ đồ cấu trúc dạng giản đồ của thiết bị điện tử theo phương án của sáng chế; và

Fig.12 là sơ đồ dạng giản đồ của hệ thống truyền thông theo phương án của sáng chế.

Mô tả chi tiết bản sáng chế

Nên được hiểu rằng, trừ khi được chỉ định theo cách khác trong sáng chế, "/" có nghĩa là hoặc. Ví dụ như, A/B có thể biểu diễn A hoặc B. Thuật ngữ "và/hoặc" trong sáng chế chỉ mô tả mối quan hệ kết hợp cho việc mô tả các đối tượng được kết hợp và biểu diễn rằng ba mối quan hệ có thể tồn tại. Ví dụ, A và/hoặc B có thể biểu diễn các trường hợp sau: Chỉ có A tồn tại, cả hai A và B tồn tại, và chỉ có B tồn tại. "Ít nhất một" có nghĩa là một hoặc nhiều. "Nhiều" có nghĩa là hai hoặc nhiều hơn hai. Ví dụ, ít nhất một trong số a, b, hoặc c có thể biểu diễn bảy trường hợp: a, b, c, a và b, a và c, b và c, và a, b và c.

Trong sáng chế, "ví dụ", "theo một số phương án", "theo một số phương án khác", và tương tự được sử dụng để biểu diễn các ví dụ, các minh họa, hoặc các mô tả. Bất kỳ phương án hoặc sơ đồ thiết kế được mô tả như "ví dụ" trong sáng chế không nên được giải thích là được ưu tiên hơn hoặc có nhiều ưu điểm hơn so với phương án hoặc sơ đồ thiết kế khác. Chính xác, "ví dụ" được sử dụng để trình bày khái niệm theo cách cụ thể.

Ngoài ra, các thuật ngữ "thứ nhất" và "thứ hai" trong sáng chế chỉ đơn thuần nhằm mục đích mô tả, và sẽ không được hiểu là chỉ báo hoặc ngụ ý về tầm quan trọng tương đối hoặc chỉ báo ngầm định về số lượng của các đặc điểm kỹ thuật được chỉ báo.

Người dùng có thể điều khiển thiết bị IoT bằng cách sử dụng thiết bị điện tử mà

trên đó ứng dụng IoT được lắp đặt. Thiết bị điện tử mà trên đó ứng dụng IoT được lắp đặt được gọi là thiết bị điều khiển IoT dưới đây. Ví dụ, thiết bị điều khiển IoT có thể là thiết bị điện tử cầm tay như là điện thoại di động, máy tính bảng, máy tính xách tay, máy tính cá nhân siêu di động (ultra-mobile personal computer, UMPC), máy tính siêu di động thu nhỏ, thiết bị kỹ thuật số hỗ trợ cá nhân (personal digital assistant, PDA). Ví dụ khác, thiết bị điều khiển IoT có thể còn là máy tính bàn, màn hình thông minh, hoặc tương tự. Kiểu cụ thể của thiết bị điều khiển IoT không bị giới hạn theo các phương án của sáng chế. Cần lưu ý rằng, không như tivi truyền thống, màn hình thông minh là sản phẩm màn hình lớn mới. Ngoài việc triển khai âm thanh và phát video, màn hình thông minh đóng nhiều vai trò trong nhà. Ví dụ, màn hình thông minh có thể là trung tâm tương tác, trung tâm chia sẻ thông tin, và trung tâm quản lý điều khiển của thiết bị trí thông minh như là thiết bị nhà thông minh hoặc điện thoại di động.

Trong sáng chế, thiết bị IoT có thể là thiết bị nhà thông minh, ví dụ, loa thông minh, đèn bàn thông minh, điều hoàn không khí thông minh, tủ lạnh thông minh, rèm thông minh. Ngoài ra, thiết bị IoT có thể còn là thiết bị thông minh như là thiết bị trong phương tiện giao thông, thiết bị đeo được, hoặc thiết bị thực tế tăng cường (augmented reality, AR)/ thực tế ảo (virtual reality, VR). Kiểu cụ thể của thiết bị IoT không bị giới hạn theo các phương án của sáng chế.

Cụ thể, thiết bị điều khiển điều khiển thiết bị IoT bằng cách gửi chỉ thị điều khiển đến thiết bị IoT. Thông thường, thiết bị IoT gửi chỉ thị điều khiển đến thiết bị IoT để phản hồi lại thao tác được thực hiện bởi người dùng trên ứng dụng IoT. Cần lưu ý rằng các chỉ thị điều khiển đối với các loại thiết bị IoT khác nhau có thể là giống nhau hoặc có thể là khác nhau. Ví dụ, đối với loa thông minh, chỉ thị điều khiển có thể bao gồm chỉ thị phát, chỉ thị tạm dừng phát, chỉ thị điều chỉnh âm lượng, lệnh điều chỉnh tiến độ phát, chỉ thị chuyển nội dung phát, hoặc tương tự. Ví dụ khác, đối với đèn bàn thông minh, chỉ thị điều khiển có thể bao gồm chỉ thị bật đèn, chỉ thị tắt đèn, chỉ thị điều chỉnh độ sáng, hoặc tương tự.

Ngoài ra, thiết bị IoT có thể còn báo cáo thông tin tình trạng thiết bị cho thiết bị điều khiển IoT, sao cho thiết bị điều khiển IoT có thể trình bày tình trạng hiện tại của thiết bị IoT cho người dùng. Thông tin tình trạng thiết bị được sử dụng để chỉ báo tình trạng hiện tại của thiết bị IoT. Ví dụ, tình trạng hiện tại của thiết bị IoT có thể bao gồm tình trạng chạy hiện tại của thiết bị IoT, tình trạng sử dụng hiện tại của thiết bị IoT, và

tương tự.

Loa thông minh được sử dụng như ví dụ. Thiết bị điều khiển IoT gửi chỉ thị phát đến loa thông minh. Sau khi nhận chỉ thị phát được gửi bởi thiết bị điều khiển IoT trong trạng thái tạm dừng phát, loa thông minh phát nội dung tương ứng để phản hồi lại chỉ thị phát, sao cho tình trạng hiện tại của loa thông minh thay đổi sang trạng thái phát. Khi tình trạng hiện tại của loa thông minh thay đổi từ trạng thái tạm dừng phát sang trạng thái phát, loa thông minh có thể báo cáo thông tin tình trạng thiết bị cho thiết bị điều khiển IoT. Thông tin tình trạng thiết bị được sử dụng để chỉ báo rằng tình trạng hiện tại của hộp âm thanh thông minh là trạng thái phát. Sau khi nhận thông tin tình trạng thiết bị được báo cáo bởi loa thông minh, thiết bị điều khiển IoT có thể cập nhật, dựa trên thông tin tình trạng thiết bị, tình trạng hiện tại của loa thông minh được trình bày cho người dùng.

Trong kịch bản mà trong đó thiết bị điều khiển IoT và thiết bị IoT được kết nối riêng biệt với máy chủ đám mây, như được thể hiện trên Fig.1, thiết bị điều khiển IoT gửi chỉ thị điều khiển đến thiết bị IoT bằng cách sử dụng máy chủ đám mây, và thiết bị IoT gửi thông tin tình trạng thiết bị đến thiết bị đám mây IoT bằng cách sử dụng máy chủ đám mây. Trong kịch bản này, bất kể thiết bị IoT và thiết bị điều khiển IoT có ở trong cùng mạng cục bộ hay không, người dùng có thể điều khiển thiết bị IoT bằng cách sử dụng thiết bị điều khiển IoT. Tuy nhiên, vì cả hai báo hiệu điều khiển và thông tin tình trạng thiết bị cần được chuyển tiếp bằng cách sử dụng máy chủ đám mây, sự thực thi của lệnh điều khiển và sự tiếp nhận của thông tin tình trạng thiết bị dễ gây ra độ trễ tương đối cao và tỷ lệ thành công tương đối thấp.

Để đạt được mục đích này, giải pháp IoT điều khiển cục bộ được đề xuất. Trong giải pháp IoT điều khiển cục bộ, thiết bị điều khiển IoT và thiết bị IoT thường ở trong cùng mạng cục bộ. Như được thể hiện trên Fig.2, báo hiệu điều khiển và thông tin tình trạng thiết bị trao đổi giữa thiết bị điều khiển IoT và thiết bị IoT có thể không cần được chuyển tiếp bởi máy chủ đám mây, do đó giúp giảm độ trễ trong việc thực thi lệnh điều khiển và nhận thông tin tình trạng thiết bị. Ví dụ, mạng cục bộ trong sáng chế có thể là mạng Wi-Fi hoặc mạng có dây.

Cụ thể, việc thiết bị điều khiển IoT và thiết bị IoT ở trong cùng mạng cục bộ có thể được hiểu là: Thiết bị điều khiển IoT và thiết bị IoT được kết nối với cùng một bộ định tuyến. Ngoài ra, cần lưu ý rằng, trong giải pháp IoT điều khiển cục bộ, thiết bị điều khiển IoT và thiết bị IoT có thể còn ở trong các mạng cục bộ khác. Ví dụ, thiết bị điều

khiển IoT ở trong mạng cục bộ thứ nhất và được kết nối với bộ định tuyến thứ nhất, và thiết bị IoT ở trong mạng cục bộ thứ hai và được kết nối với bộ định tuyến thứ hai. Bộ định tuyến thứ nhất và bộ định tuyến thứ hai được kết nối với nhau. Nên được hiểu rằng, việc bộ định tuyến thứ nhất và bộ định tuyến thứ hai được kết nối với nhau có thể được hiểu như sau: Bộ định tuyến thứ nhất và bộ định tuyến thứ hai có thể trao đổi các thông điệp với nhau, và sự trao đổi thông tin giữa bộ định tuyến thứ nhất và bộ định tuyến thứ hai bao gồm sự trao đổi thông điệp truyền đa hướng.

Trong ví dụ, thiết bị điều khiển IoT ở trong mạng cục bộ thứ nhất. Trong giải pháp IoT điều khiển cục bộ, thiết bị điều khiển IoT khởi tạo quy trình khám phá thiết bị IoT để khám phá thiết bị IoT, do đó triển khai truyền thông với thiết bị IoT. Ngoài ra, để đảm bảo bảo mật của truyền thông giữa thiết bị điều khiển IoT và thiết bị IoT, khóa phiên thường được sử dụng để thực hiện truyền thông được mã hóa giữa thiết bị điều khiển IoT và thiết bị IoT. Ví dụ, khóa phiên có thể thu được bởi thiết bị điều khiển IoT thông qua sự đàm phán dựa trên giao thức đầu cuối (trạm đến trạm, Station to Station, STS) sau khi khám phá thiết bị IoT. Quy trình cụ thể được thể hiện trên Fig.3, bao gồm các bước sau.

Bước 301: Thiết bị điều khiển IoT truyền đa hướng thông điệp khám phá trong mạng cục bộ thứ nhất. Mạng cục bộ thứ nhất là mạng mà đã được truy nhập hiện tại bởi thiết bị điều khiển IoT. Ví dụ, thiết bị điều khiển IoT có thể truyền đa hướng thông điệp khám phá trong mạng cục bộ thứ nhất dựa trên giao thức dữ liệu người dùng (user datagram protocol, UDP) hoặc giao thức hệ thống tên miền truyền đa hướng (multicast domain name system, mDNS).

Có thể được hiểu rằng thông điệp khám phá có thể cũng được gọi là thông điệp phát hiện, thông điệp khám phá thiết bị, thông điệp phát hiện thiết bị, hoặc tương tự. Ví dụ, thông điệp khám phá có thể bao gồm thông tin liên quan của thiết bị điều khiển IoT, ví dụ, mã định danh (nhận dạng, identity, ID) thiết bị, địa chỉ IP, và ID người dùng của thiết bị điều khiển IoT.

Bước 302: Thiết bị IoT 1 trả lại thông tin thiết bị của thiết bị IoT 1 cho thiết bị điều khiển IoT sau khi nhận thông điệp khám phá.

Ví dụ, thiết bị IoT 1 có thể thêm thông tin thiết bị của thiết bị 1 vào phản hồi khám phá và trả lại phản hồi khám phá cho thiết bị điều khiển. Phản hồi khám phá có thể cũng được gọi là phản hồi phát hiện, phản hồi khám phá thiết bị, phản hồi phát hiện thiết bị, hoặc tương tự.

Cụ thể, thông tin thiết bị của thiết bị IoT 1 theo phương án này của sáng chế có thể bao gồm một hoặc nhiều ID thiết bị, loại thiết bị, địa chỉ giao thức mạng (internet protocol, IP), số hiệu cổng, và tương tự. Ví dụ, thông tin thiết bị của thiết bị IoT 1 bao gồm ID thiết bị. Ví dụ khác, thông tin thiết bị của thiết bị IoT 1 bao gồm địa chỉ IP. Ví dụ khác, thông tin thiết bị của thiết bị IoT 1 bao gồm ID thiết bị, loại thiết bị, và địa chỉ IP. Vẫn ví dụ khác, thông tin thiết bị của thiết bị IoT 1 bao gồm ID thiết bị, loại thiết bị, và địa chỉ IP, và số hiệu cổng.

Cần lưu ý rằng loại thiết bị có thể bao gồm tivi, loa, điều hòa không khí, đèn điện, tủ lạnh, hoặc tương tự. Ví dụ, thiết bị IoT 1 là đèn bàn thông minh, và loại thiết bị IoT 1 là đèn điện. Ví dụ khác, thiết bị IoT 1 là tủ lạnh thông minh, và loại thiết bị IoT 1 là tủ lạnh.

Bước 303: Thiết bị điều khiển IoT gửi khóa công khai K0 đến thiết bị IoT 1 sau khi nhận thông tin thiết bị của thiết bị IoT 1. Khóa công khai K0 được tạo ra dựa trên số ngẫu nhiên L0.

Cần lưu ý rằng theo phương án này của sáng chế, số ngẫu nhiên L0 có thể cũng được gọi là khóa cá nhân, và tạo thành cặp khóa cùng với khóa công khai K0. Ví dụ, theo phương án này của sáng chế, thiết bị điều khiển IoT có thể sử dụng số ngẫu nhiên L0 như đầu vào của hàm f(), và sử dụng đầu ra của hàm f() như khóa công khai K0. Hàm f() có thể là hàm mũ, hàm lũy thừa, hàm bậc hai, hàm bậc ba, hoặc tương tự. Điều này không bị giới hạn. Ví dụ, hàm f() is $y=g^x$, và khi số ngẫu nhiên L0 là x0, khóa công khai K0 là y0, trong đó $y0=g^{x0}$. Hàm f() có thể được định nghĩa bằng cách sử dụng giao thức, hoặc có thể được xác định bởi thiết bị điều khiển IoT dựa trên chính sách hoặc thuật toán. Điều này không bị giới hạn.

Bước 304: Thiết bị IoT 1 tạo ra khóa phiên H1 dựa trên khóa công khai K0 và số ngẫu nhiên L1 sau khi nhận khóa công khai K0. Ngoài ra, thiết bị IoT 1 ký thông tin phiên 1 bằng cách sử dụng khóa cá nhân dài hạn S1 của thiết bị IoT 1, để thu được chữ ký 1. Thông tin phiên 1 bao gồm khóa công khai K1 và khóa công khai K0, và khóa công khai K1 được tạo ra dựa trên số ngẫu nhiên L1. Sau đó, thiết bị IoT 1 mã hóa chữ ký 1 bằng cách sử dụng khóa phiên H1 để thu được văn bản mật mã (ciphertext) 1.

Ví dụ, thông tin phiên 1 bao gồm (khóa công khai K1, khóa công khai K0).

Cần lưu ý rằng số ngẫu nhiên L1 và khóa công khai K1 tạo thành cặp khóa. Đối với cách mà trong đó thiết bị IoT 1 tạo ra khóa công khai K1 dựa trên số ngẫu nhiên L1,

tham chiếu đến cách mà trong đó khóa công khai K0 được tạo ra dựa trên số ngẫu nhiên L0. Các chi tiết không được mô tả ở đây lần nữa.

Khoảng thời gian hiệu lực của khóa cá nhân dài hạn S1 của thiết bị IoT 1 lớn hơn hoặc bằng ngưỡng. Ví dụ, khóa cá nhân dài hạn S1 với thiết bị IoT 1 có thể hợp lệ trong thời gian dài, và có thể được tạo cấu hình trước khi thiết bị được vận chuyển. Cần lưu ý rằng, khoảng thời gian hiệu lực của khóa công khai dài hạn G1 tương ứng với khóa cá nhân dài hạn S1 trong thiết bị IoT 1 giống như khoảng thời gian hiệu lực của khóa cá nhân dài hạn S1, và có thể cũng được tạo cấu hình trước khi thiết bị được vận chuyển.

Bước 305: Thiết bị IoT 1 gửi khóa công khai K1 và văn bản mật mã 1 đến thiết bị điều khiển IoT.

Bước 306: Thiết bị điều khiển IoT tạo ra khóa phiên H1 dựa trên khóa công khai K1 và số ngẫu nhiên L0 sau khi nhận khóa công khai K1 và văn bản mật mã 1. Sau đó, thiết bị điều khiển IoT giải mã văn bản mật mã 1 bằng cách sử dụng khóa phiên H1, để thu được chữ ký 1. Thiết bị điều khiển IoT xác minh chữ ký 1 bằng cách sử dụng khóa công khai dài hạn G1 của thiết bị IoT 1. Ngoài ra, sau khi chữ ký 1 được xác minh thành công, thiết bị điều khiển IoT ký thông tin phiên 2 bằng cách sử dụng khóa cá nhân dài hạn S0 của thiết bị điều khiển IoT, để thu được chữ ký 2, và mã hóa chữ ký 2 bằng cách sử dụng khóa phiên H1, để thu được văn bản mật mã 2. Thông tin phiên 2 bao gồm khóa công khai K0 và khóa công khai K1. Ví dụ, thông tin phiên 2 bao gồm (khóa công khai K0, khóa công khai K1).

Cụ thể, khoảng thời gian hiệu lực của khóa cá nhân dài hạn S0 của thiết bị điều khiển IoT lớn hơn hoặc bằng ngưỡng. Ví dụ, khóa cá nhân dài hạn S0 với thiết bị điều khiển IoT 1 có thể hợp lệ trong thời gian dài, và có thể được tạo cấu hình trước khi thiết bị được vận chuyển. Cần lưu ý rằng, khoảng thời gian hiệu lực của khóa công khai dài hạn G0 tương ứng với khóa cá nhân dài hạn S0 trong thiết bị điều khiển IoT giống như khoảng thời gian hiệu lực của khóa cá nhân dài hạn S0, và có thể cũng được tạo cấu hình trước khi thiết bị được vận chuyển.

Bước 307: Thiết bị điều khiển IoT gửi văn bản mật mã 2 đến thiết bị IoT 1.

Bước 308: Sau khi nhận văn bản mật mã 2, thiết bị IoT 1 giải mã văn bản mật mã 2 bằng cách sử dụng khóa phiên H1, để thu được chữ ký 2. Thiết bị IoT xác minh chữ ký 2 bằng cách sử dụng khóa công khai dài hạn G0 của thiết bị điều khiển IoT.

Bước 309: Thiết bị IoT 1 gửi thông tin phiên 3 đến thiết bị điều khiển IoT sau khi

chữ ký 2 được xác minh thành công. Ví dụ, thiết bị IoT 1 có thể giải mã trước tiên thông tin phiên 3 bằng cách sử dụng khóa phiên H1, và sau đó gửi thông tin phiên được mã hóa 3 đến thiết bị điều khiển IoT, do đó cải thiện bảo mật của việc gửi thông tin phiên 3.

Ví dụ, thông tin phiên 3 có thể bao gồm ID phiên và tương tự. Sau khi thiết bị điều khiển IoT nhận thông tin phiên 3 được gửi bởi thiết bị IoT 1, thiết bị điều khiển IoT và thiết bị IoT 1 có thể thực hiện truyền thông được mã hóa bằng cách sử dụng khóa phiên H1.

Ví dụ, thiết bị điều khiển IoT mã hóa chỉ thị điều khiển bằng cách sử dụng khóa phiên H1, và gửi chỉ thị điều khiển được mã hóa đến thiết bị IoT 1.

Cần lưu ý rằng, đối với thiết bị IoT 1, bước 301 và bước 302 là quá trình khám phá thiết bị IoT. Bước 303 đến bước 309 là quá trình đàm phán STS. Thiết bị IoT khác (ví dụ, thiết bị IoT 2 hoặc thiết bị IoT n) cũng trả lại thông tin thiết bị của thiết bị IoT khác cho thiết bị điều khiển IoT nếu nhận sự truyền đa hướng thông điệp khám phá bởi thiết bị điều khiển trong mạng cục bộ thứ nhất. Trong trường hợp này, quá trình đàm phán STS có thể cũng được thực hiện giữa thiết bị điều khiển IoT và thiết bị IoT khác, để thu được khóa phiên được sử dụng cho truyền thông giữa thiết bị điều khiển IoT và thiết bị IoT khác. Đối với quá trình đàm phán STS giữa thiết bị điều khiển IoT và thiết bị IoT khác, tham chiếu đến quá trình đàm phán STS giữa thiết bị điều khiển IoT và thiết bị IoT 1. Các chi tiết không được mô tả ở đây lần nữa.

Trong phương pháp được thể hiện trên Fig.3, sau khi khám phá thiết bị IoT, thiết bị điều khiển IoT thực hiện quá trình đàm phán STS để thu được khóa phiên, để triển khai truyền thông được mã hóa giữa thiết bị điều khiển IoT và thiết bị IoT. Vì thế, theo cách thu được khóa phiên này, hiệu quả là tương đối thấp. Ngoài ra, trong quá trình khám phá thiết bị IoT, sau khi nhận thông điệp khám phá được gửi bởi thiết bị điều khiển IoT, thiết bị IoT trả lại thông tin thiết bị cho thiết bị điều khiển IoT dưới dạng văn bản thuần túy. Nhờ đó, thông tin thiết bị của thiết bị IoT bị bộc lộ dễ dàng trong mạng, và kẻ tấn công có thể tấn công thiết bị IoT.

Theo quan điểm của điều này, phương án của sáng chế đề xuất phương pháp đàm phán khóa. Quá trình đàm phán STS được tích hợp vào trong quá trình khám phá, do đó giúp giảm số lượng thông điệp trao đổi giữa thiết bị IoT và thiết bị điều khiển IoT, và cải thiện hiệu quả của việc thu được khóa phiên. Ngoài ra, trong quá trình khám phá, thiết bị IoT có thể còn mã hóa thông tin thiết bị bằng cách sử dụng khóa phiên, và sau đó gửi

thông tin thiết bị được mã hóa đến thiết bị điều khiển IoT, do đó giảm nguy cơ tấn công gây ra bởi việc bộc lộ thông tin thiết bị của thiết bị IoT trong mạng.

Ví dụ, Fig.4 là sơ đồ dạng giản đồ của kiến trúc mạng mà theo phương án của sáng chế là áp dụng được. Kiến trúc mạng bao gồm thiết bị điều khiển IoT, bộ định tuyến, và thiết bị IoT. Cần lưu ý rằng, theo phương án này của sáng chế, cách kết nối giữa thiết bị IoT và bộ định tuyến có thể là kết nối không dây, hoặc có thể là kết nối có dây. Cách kết nối giữa thiết bị điều khiển IoT và bộ định tuyến có thể là kết nối không dây hoặc kết nối có dây.

Nên được hiểu rằng Fig.4 chỉ đơn thuần là ví dụ của kiến trúc mạng mà phương án này của sáng chế là áp dụng được, và không cấu thành sự giới hạn trên kiến trúc mạng mà phương án này của sáng chế là áp dụng được.

Cụ thể, Fig.5 là lưu đồ dạng giản đồ của phương pháp đàm phán khóa theo phương án của sáng chế. Phương pháp cụ thể bao gồm các bước sau.

Bước 501: Thiết bị điều khiển IoT truyền đa hướng thông điệp khám phá trong mạng cục bộ thứ nhất. Mạng cục bộ thứ nhất là mạng mà đã được truy nhập bởi thiết bị điều khiển IoT. Thông điệp khám phá bao gồm khóa công khai K0. Khóa công khai K0 được tạo ra dựa trên số ngẫu nhiên L0.

Đối với triển khai cụ thể mà trong đó thiết bị điều khiển IoT tạo ra khóa công khai K0 dựa trên số ngẫu nhiên L0, tham chiếu đến các mô tả liên quan của triển khai mà trong đó khóa công khai K0 được tạo ra dựa trên số ngẫu nhiên L0 theo bước 303. Các chi tiết không được mô tả ở đây lần nữa. Ngoài ra, thông điệp khám phá có thể còn bao gồm thông tin liên quan của thiết bị điều khiển IoT, ví dụ, ID thiết bị, địa chỉ IP, và ID người dùng của thiết bị điều khiển IoT.

Cần lưu ý rằng, đối với triển khai cụ thể mà trong đó thiết bị điều khiển IoT truyền đa hướng thông điệp khám phá trong mạng cục bộ thứ nhất, tham chiếu có thể được thực hiện cho triển khai liên quan theo bước 301. Các chi tiết không được mô tả ở đây lần nữa.

Cụ thể, thiết bị điều khiển IoT có thể truyền đa hướng thông điệp khám phá trong mạng cục bộ thứ nhất định kỳ và/hoặc thông qua việc kích hoạt bởi sự kiện. Ví dụ, sau khi được cấp nguồn, thiết bị điều khiển IoT có thể phát hiện truy nhập vào mạng cục bộ (ví dụ, mạng cục bộ thứ nhất), và kích hoạt việc truyền đa hướng định kỳ của thông điệp khám phá trong mạng cục bộ thứ nhất. Ngoài ra, ví dụ khác, sự kiện mà kích hoạt việc truyền đa hướng của thông điệp khám phá trong mạng cục bộ thứ nhất hoặc kích hoạt

việc truyền đa hướng định kỳ của thông điệp khám phá trong mạng cục bộ thứ nhất có thể bao gồm: mạng được truy nhập bởi thiết bị điều khiển IoT được chuyển mạch từ mạng cục bộ thứ hai sang mạng cục bộ thứ nhất, thiết bị điều khiển IoT được liên kết với thiết bị IoT mới; chỉ báo đàm phán khóa phiên (ví dụ, chỉ báo đàm phán khóa phiên được gửi đến thiết bị điều khiển IoT bởi thiết bị IoT sau khi bị tắt nguồn và khởi động lại, trong đó ví dụ, chỉ báo có thể là ký hiệu hoặc trình tự cụ thể) được gửi bởi thiết bị IoT trong mạng cục bộ thứ nhất được nhận; số lượng phiên của thiết bị IoT được liên kết với thiết bị điều khiển IoT lớn hơn hoặc bằng giá trị tối đa bị giới hạn bởi hệ thống, hoặc khóa phiên của thiết bị IoT được liên kết với thiết bị điều khiển IoT đã đạt đến hoặc sắp đạt đến thời điểm hết hạn của khoảng thời gian hiệu lực. Ví dụ, nếu khoảng thời gian hiệu lực của khóa phiên là 30 phút, và thiết bị điều khiển IoT lưu trữ khóa phiên ở lúc 5:00, thời điểm hết hạn của khoảng thời gian hiệu lực của khóa phiên là 5:30. Cần lưu ý rằng, việc khóa phiên của thiết bị IoT được liên kết với thiết bị điều khiển IoT sắp đạt đến thời điểm hết hạn của khoảng thời gian hiệu lực có thể được hiểu như sau: Khóa phiên của thiết bị IoT được liên kết với thiết bị điều khiển IoT đạt đến thời điểm hết hạn của khoảng thời gian hiệu lực sau thời hạn thứ nhất. Thời hạn thứ nhất có thể được định nghĩa trước, hoặc có thể được xác định bởi thiết bị IoT dựa trên thuật toán hoặc chính sách. Ví dụ, thời hạn thứ nhất có thể là hai phút, 15 giây, hoặc tương tự. Điều này không bị giới hạn. Ví dụ, nếu khoảng thời gian hiệu lực của khóa phiên là 10 phút, và thiết bị điều khiển IoT lưu trữ khóa phiên ở lúc 4:00, thời điểm hết hạn của khoảng thời gian hiệu lực của khóa phiên là 4:10. Ví dụ, thời hạn thứ nhất là một phút. Khi đạt đến 4:09, thiết bị điều khiển IoT kích hoạt việc truyền đa hướng của thông điệp khám phá trong mạng cục bộ thứ nhất.

Cần lưu ý rằng phần trên chỉ đơn thuần là ví dụ để mô tả sự kiện mà kích hoạt thiết bị điều khiển IoT để truyền đa hướng thông điệp khám phá trong mạng cục bộ thứ nhất. Điều này không bị giới hạn theo phương án này của sáng chế.

Ngoài ra, khi thiết bị IoT truyền đa hướng định kỳ thông điệp khám phá, các khóa công khai K0 được mang trong các thông điệp khám phá truyền đa hướng trong các khoảng thời gian liền kề có thể là khác nhau, hoặc các khóa công khai K0 được mang trong các thông điệp khám phá truyền đa hướng trong các khoảng thời gian khác nhau có thể là khác nhau, do đó giúp cải thiện bảo mật của đàm phán khóa. Để các thông điệp khám phá trong các khoảng thời gian liền kề hoặc khác nhau mang các khóa công khai K0 khác nhau, thiết bị điều khiển IoT có thể tạo ra khóa công khai K0 bằng cách sử dụng

các số ngẫu nhiên L0 khác nhau và/hoặc các thuật toán khác nhau trong các khoảng thời gian liền kề hoặc khác nhau.

Theo một số phương án, thiết bị điều khiển IoT gửi thông điệp khám phá đến bộ định tuyến thứ nhất, và bộ định tuyến thứ nhất truyền đa hướng thông điệp khám phá đến một hoặc nhiều thiết bị IoT trong mạng cục bộ thứ nhất. Bộ định tuyến thứ nhất là bộ định tuyến được sử dụng bởi thiết bị điều khiển IoT để truy nhập mạng cục bộ thứ nhất.

Bước 502: Thiết bị IoT 1 tạo ra khóa phiên H1 dựa trên khóa công khai K0 và số ngẫu nhiên L1 sau khi nhận thông điệp khám phá. Sau đó, thiết bị IoT 1 mã hóa thông tin thiết bị của thiết bị IoT 1 bằng cách sử dụng khóa phiên H1, để thu được văn bản mật mã 0. Đối với thông tin thiết bị của thiết bị IoT 1, tham chiếu đến các mô tả liên quan của thông tin thiết bị của thiết bị IoT 1 trên Fig.3. Các chi tiết không được mô tả ở đây lần nữa.

Cần lưu ý rằng thiết bị IoT 1 có thể ở trong mạng cục bộ thứ nhất, hoặc có thể không ở trong mạng cục bộ thứ nhất. Nghĩa là, mạng được truy nhập bởi thiết bị IoT 1 có thể ở trong mạng cục bộ thứ nhất, hoặc có thể không ở trong mạng cục bộ thứ nhất. Điều này không bị giới hạn.

Hơn nữa, sau khi nhận thông điệp khám phá, thiết bị IoT 1 xác định xem thiết bị IoT 1 đã được liên kết với thiết bị điều khiển IoT. Nếu thiết bị IoT 1 đã được liên kết với thiết bị điều khiển IoT, thiết bị IoT 1 tạo ra khóa phiên H1 dựa trên khóa công khai K0 và số ngẫu nhiên L1, và sau đó thực hiện bước tiếp theo. Ví dụ, thiết bị IoT 1 có thể xác định xem ID người dùng được lưu trữ trong thiết bị IoT 1 là giống như hay được kết hợp với ID người dùng được mang trong thông điệp khám phá, để xác định xem thiết bị IoT 1 đã được liên kết với thiết bị điều khiển IoT hay chưa. Ví dụ, nếu ID người dùng được lưu trữ trong thiết bị IoT 1 là giống như hoặc được kết hợp với ID người dùng được mang trong thông điệp khám phá, thiết bị IoT 1 xác định rằng thiết bị IoT 1 đã được liên kết với thiết bị điều khiển IoT. Ví dụ khác, thiết bị IoT 1 có thể còn xác định xem thiết bị IoT 1 lưu trữ khóa công khai dài hạn tương ứng với ID thiết bị được mang trong thông điệp khám phá, để xác định xem thiết bị IoT 1 đã được liên kết với thiết bị điều khiển IoT hay chưa.

Ví dụ, nếu thiết bị IoT mà không được liên kết với thiết bị điều khiển nhận thông điệp khám phá từ thiết bị điều khiển IoT, sau khi thiết bị IoT xác định rằng thiết bị IoT không được liên kết với thiết bị điều khiển IoT, thiết bị điều khiển IoT xem xét thông

điệp khám phá như thông điệp không hợp lệ và loại bỏ hoặc bỏ qua thông điệp khám phá. Có thể được hiểu rằng, sau khi mua thiết bị IoT, người dùng thường khởi tạo quy trình liên kết thiết bị IoT bằng cách thực hiện thao tác trên thiết bị điều khiển IoT, để liên kết thiết bị IoT với thiết bị điều khiển IoT, để tạo điều kiện điều khiển thiết bị IoT bởi người dùng. Cụ thể, đối với quy trình liên kết thiết bị IoT 1 và thiết bị điều khiển IoT, tham chiếu đến các mô tả liên quan trên Fig.6. Các chi tiết không được mô tả ở đây lần nữa.

Thuật toán được sử dụng bởi thiết bị IoT 1 để tạo ra khóa phiên H1 dựa trên khóa công khai K0 và số ngẫu nhiên L1 có thể là thuật toán Diffie-Hellman hoặc thuật toán khác được sử dụng để tạo ra khóa đối xứng. Điều này không bị giới hạn. Cụ thể, thuật toán được sử dụng bởi thiết bị IoT 1 để tạo ra khóa phiên H1 có thể được định nghĩa bằng cách sử dụng giao thức, hoặc có thể được xác định bởi thiết bị điều khiển IoT và thiết bị IoT 1 thông qua đàm phán. Điều này không bị giới hạn.

Theo một số phương án, thiết bị IoT 1 có thể nhận thông điệp khám phá định kỳ và/hoặc thông qua việc kích hoạt bởi sự kiện. Ví dụ, sự kiện mà kích hoạt thiết bị IoT 1 để nhận thông điệp khám phá có thể là: thiết bị IoT 1 được cấp nguồn; thiết bị IoT 1 chuyển mạch mạng mà được truy nhập bởi thiết bị IoT 1; thiết bị IoT 1 hoàn tất liên kết với thiết bị điều khiển IoT; khóa phiên giữa thiết bị IoT 1 và thiết bị điều khiển IoT đạt đến hoặc sắp đạt đến thời điểm hết hạn của khoảng thời gian hiệu lực; hoặc số lượng phiên giữa thiết bị IoT 1 và thiết bị điều khiển IoT vượt quá giá trị tối đa bị giới hạn bởi hệ thống.

Bước 503: Thiết bị IoT 1 gửi văn bản mật mã 0 và khóa công khai K1 đến thiết bị điều khiển IoT. Khóa công khai K1 được tạo ra bởi thiết bị IoT 1 dựa trên số ngẫu nhiên L1. Ví dụ, thiết bị IoT có thể thêm văn bản mật mã 0 và khóa công khai K1 vào phản hồi khám phá và trả lại phản hồi khám phá cho thiết bị điều khiển IoT.

Ví dụ, đối với chức năng được sử dụng bởi thiết bị IoT 1 để tạo ra khóa công khai K1 dựa trên số ngẫu nhiên L1, tham chiếu đến mô tả liên quan của hàm f() theo bước 303. Các chi tiết không được mô tả ở đây lần nữa.

Theo một số phương án, thiết bị IoT 1 gửi văn bản mật mã 0 và khóa công khai K1 đến bộ định tuyến thứ hai, và bộ định tuyến thứ hai gửi khóa 0 và khóa công khai K1 đến thiết bị điều khiển IoT. Bộ định tuyến thứ hai là bộ định tuyến được sử dụng bởi thiết bị IoT 1 để truy nhập mạng cục bộ. Cần lưu ý rằng khi bộ định tuyến thứ hai và bộ định tuyến thứ nhất là cùng một bộ định tuyến, thiết bị IoT 1 ở trong mạng cục bộ thứ nhất.

Khi bộ định tuyến thứ hai và bộ định tuyến thứ nhất là hai bộ định tuyến mà được kết nối với nhau, thiết bị IoT 1 không ở trong mạng cục bộ thứ nhất. Trong trường hợp này, bộ định tuyến thứ hai có thể gửi trước tiên khóa 0 và khóa công khai K1 đến bộ định tuyến thứ nhất, và sau đó bộ định tuyến thứ nhất gửi khóa 0 và khóa công khai K1 đến thiết bị điều khiển IoT.

Bước 504: Thiết bị điều khiển IoT tạo ra khóa phiên H1 dựa trên khóa công khai K1 và số ngẫu nhiên L0 sau khi nhận văn bản mật mã 0 và khóa công khai K1. Sau đó, thiết bị điều khiển IoT giải mã văn bản mật mã 0 bằng cách sử dụng khóa phiên H1, để thu được thông tin thiết bị của thiết bị IoT 1. Thiết bị điều khiển IoT ký thông tin phiên 1 bằng cách sử dụng khóa cá nhân dài hạn S0 của thiết bị điều khiển IoT, để thu được chữ ký 1. Thiết bị điều khiển IoT mã hóa chữ ký 1 bằng cách sử dụng khóa phiên 1, để thu được văn bản mật mã 1. Thông tin phiên 1 bao gồm khóa công khai K0 và khóa công khai K1. Ví dụ, thông tin phiên 1 bao gồm (khóa công khai K0, khóa công khai K1).

Thuật toán được sử dụng bởi thiết bị điều khiển IoT để tạo ra khóa phiên H1 dựa trên khóa công khai K1 và số ngẫu nhiên L0 thường là giống như thuật toán được sử dụng bởi thiết bị IoT 1 để tạo ra khóa phiên H1, sao cho khóa phiên H1 được tạo ra bởi thiết bị điều khiển IoT dựa trên khóa công khai K1 và số ngẫu nhiên L0 là giống như khóa phiên H1 được tạo ra bởi thiết bị IoT 1 dựa trên khóa công khai K0 và số ngẫu nhiên L1. Ví dụ, thuật toán được sử dụng bởi thiết bị điều khiển IoT để tạo ra khóa phiên H1 dựa trên khóa công khai K1 và số ngẫu nhiên L0 có thể là thuật toán Diffie-Hellman hoặc thuật toán khác được sử dụng để tạo ra khóa đối xứng. Điều này không bị giới hạn.

Bước 505: Thiết bị điều khiển IoT gửi văn bản mật mã 1 đến thiết bị IoT 1.

Ví dụ, thiết bị điều khiển IoT gửi văn bản mật mã 1 đến bộ định tuyến thứ nhất, và bộ định tuyến thứ nhất gửi văn bản mật mã 1 đến thiết bị IoT 1.

Bước 506: Sau khi nhận văn bản mật mã 1, thiết bị IoT 1 giải mã văn bản mật mã 1 bằng cách sử dụng khóa phiên H1, để thu được chữ ký 1. Sau đó, thiết bị IoT 1 xác minh chữ ký 1 bằng cách sử dụng khóa công khai dài hạn G0 của thiết bị điều khiển IoT, và sau khi chữ ký 1 được xác minh thành công, ký thông tin phiên 2 bằng cách sử dụng khóa cá nhân dài hạn S1 của thiết bị điều khiển IoT, để thu được chữ ký 2. Thiết bị IoT 1 mã hóa chữ ký 2 và thông tin phiên 3 bằng cách sử dụng khóa phiên, để thu được văn bản mật mã 2. Thông tin phiên 2 bao gồm khóa công khai K1 và khóa công khai K0. Ví dụ, thông tin phiên 2 bao gồm (khóa công khai K1, khóa công khai K0). Thông tin phiên

3 bao gồm ID phiên. Ví dụ, thông tin phiên 3 có thể còn bao gồm khoảng thời gian hiệu lực của khóa phiên 1. Ví dụ, khoảng thời gian hiệu lực của khóa phiên 1 có thể là 12 tiếng, một ngày, bảy ngày, hoặc tương tự, và có thể được định nghĩa trước, hoặc có thể được xác định bởi thiết bị IoT 1 dựa trên thuật toán hoặc chính sách. Điều này không bị giới hạn. Hơn nữa, theo một số phương án khác, thông tin phiên 3 có thể còn bao gồm một hoặc nhiều cách kết nối phiên, giao thức truyền, cách xác thực, và tương tự. Điều này không bị giới hạn.

Bước 507: Thiết bị IoT 1 gửi văn bản mật mã 2 đến thiết bị điều khiển IoT.

Ví dụ, thiết bị IoT 1 gửi văn bản mật mã 2 đến bộ định tuyến thứ hai, và bộ định tuyến thứ hai gửi văn bản mật mã 2 đến thiết bị điều khiển IoT.

Bước 508: Sau khi nhận văn bản mật mã 2, thiết bị điều khiển IoT giải mã văn bản mật mã 2 bằng cách sử dụng khóa phiên H1, để thu được chữ ký 2 và thông tin phiên 3. Sau đó, thiết bị điều khiển IoT xác minh chữ ký 2 bằng cách sử dụng khóa công khai dài hạn G1 của thiết bị IoT 1. Sau khi chữ ký 2 được xác minh thành công, thiết bị điều khiển IoT lưu trữ thông tin phiên 3 và khóa phiên H1. Vì thế, truyền thông được mã hóa giữa thiết bị điều khiển IoT và thiết bị IoT 1 có thể được triển khai tiếp theo dựa trên khóa phiên H1. Khóa công khai dài hạn G1 của thiết bị IoT được tìm thấy bởi thiết bị điều khiển dựa trên thông tin thiết bị (ví dụ, ID thiết bị của thiết bị IoT 1) của thiết bị IoT 1.

Theo phương án này của sáng chế, các thiết bị IoT trong mạng cục bộ thứ nhất thu được cùng một khóa công khai từ thông điệp khám phá, nhưng có xác suất tương đối thấp rằng các thiết bị IoT khác nhau sử dụng cùng một số ngẫu nhiên khi tạo ra các khóa phiên. Vì thế, các khóa phiên của các thiết bị IoT khác nhau cũng khác nhau. Vì thế, bảo mật truyền thông không bị giảm khi các khóa phiên thu được bằng cách sử dụng phương pháp đàm phán khóa theo phương án này của sáng chế được sử dụng cho truyền thông được mã hóa.

Thiết bị IoT 1 được sử dụng như ví dụ để mô tả quy trình liên kết thiết bị IoT và thiết bị điều khiển IoT. Ví dụ, như được thể hiện trên Fig.6, các bước sau được bao gồm cụ thể.

Bước 601: Thiết bị điều khiển IoT nhận thao tác thứ nhất. Thao tác thứ nhất được sử dụng để nhập vào số định danh cá nhân (personal identification number, PIN) của thiết bị IoT 1.

Bước 602: Để phản hồi lại kết thúc của thao tác thứ nhất, thiết bị điều khiển IoT

thu được PIN của thiết bị IoT 1, và gửi yêu cầu liên kết thiết bị đến thiết bị IoT 1.

Ví dụ, thao tác thứ nhất có thể là thao tác nhập vào PIN của thiết bị IoT 1 bởi người dùng, thao tác quét mã hai chiều của thiết bị IoT 1 bởi người dùng, hoặc tương tự. Ví dụ, thiết bị điều khiển IoT hiển thị màn hình chính trên màn hình hiển thị, và màn hình chính bao gồm biểu tượng của ứng dụng IoT. Ví dụ, màn hình chính là màn hình 700 được thể hiện trên Fig.7A đến Fig.7E. Thiết bị điều khiển IoT có thể hiển thị màn hình của ứng dụng IoT trên màn hình hiển thị để phản hồi lại thao tác chạm vào biểu tượng 701 của ứng dụng IoT bởi người dùng. Ví dụ, màn hình của ứng dụng IoT là màn hình 710 được thể hiện trên Fig.7A đến Fig.7E. Màn hình 710 bao gồm điều khiển 711 cho việc thêm thiết bị IoT. Thiết bị điều khiển IoT có thể hiển thị màn hình 720 để phản hồi lại việc chạm vào điều khiển 711 của thiết bị IoT bởi người dùng. Màn hình 720 bao gồm điều khiển 721 và điều khiển 722. Hơn nữa, khi tài khoản người dùng của ứng dụng IoT ở trong trạng thái đã đăng nhập, thiết bị điều khiển IoT hiển thị màn hình 720 để phản hồi lại việc chạm vào điều khiển 711 của thiết bị IoT người dùng. Ví dụ, khi tài khoản người dùng của ứng dụng IoT ở trong trạng thái không đăng nhập, thiết bị điều khiển IoT nhắc người dùng đăng ký hoặc đăng nhập vào tài khoản người dùng. Ví dụ, thiết bị điều khiển IoT hiển thị màn hình đăng nhập để phản hồi lại việc chạm vào điều khiển 711 của thiết bị IoT bởi người dùng. Ví dụ, màn hình đăng nhập được thể hiện trên Fig.8, và bao gồm ô nhập tài khoản người dùng 801, ô nhập mật khẩu đăng nhập 802, điều khiển 803 cho chế độ đăng nhập khác, điều khiển đăng ký 804, và tương tự. Người dùng có thể nhập vào tài khoản người dùng trong ô nhập tài khoản người dùng 801, và nhập vào mật khẩu đăng nhập trong ô nhập mật khẩu đăng nhập, sao cho tài khoản người dùng của ứng dụng IoT ở trong trạng thái đăng nhập. Tài khoản người dùng có thể là số di động, địa chỉ thư điện tử, biệt danh, hoặc tương tự, và là ID người dùng.

Thiết bị IoT hiển thị màn hình 730 trên màn hình hiển thị để phản hồi lại việc chạm vào điều khiển 721 bởi người dùng. Màn hình 730 bao gồm ô nhập PIN. Người dùng có thể nhập vào PIN của thiết bị IoT trong ô nhập PIN. Thiết bị điều khiển IoT có thể thu được PIN của thiết bị IOT 1 từ ô nhập PIN. Ngoài ra, thiết bị IoT hiển thị màn hình 740 trên màn hình hiển thị để phản hồi lại việc chạm vào điều khiển 722 bởi người dùng. Màn hình 740 bao gồm ô quét. Người dùng có thể quét mã hai chiều của thiết bị IoT 1 trong ô quét, để thu được PIN của thiết bị IoT 1.

Theo một số phương án khác, thiết bị điều khiển IoT có thể còn hiển thị màn hình

730 hoặc màn hình 740 để phản hồi lại việc chạm vào điều khiển 711 của thiết bị IoT bởi người dùng.

Cần lưu ý rằng theo phương án này của sáng chế, màn hình nhập PIN hoặc màn hình quét mã hai chiều của thiết bị IoT 1 có thể được hiện thị bằng cách sử dụng thao tác khác, ví dụ, chỉ thị bằng giọng nói hoặc thao tác cử chỉ tắt.

Bước 603: Sau khi nhận yêu cầu liên kết thiết bị, thiết bị IoT 1 gửi số ngẫu nhiên (muối, mà có thể cũng được gọi là giá trị muối) đến thiết bị điều khiển IoT.

Bước 604: Thiết bị điều khiển IoT nhận số ngẫu nhiên (muối), và gửi khóa công khai A đến thiết bị IoT 1, trong đó khóa công khai A và khóa cá nhân A là cặp khóa, và được tạo ra bởi thiết bị điều khiển IoT dựa trên số ngẫu nhiên (muối) và PIN của thiết bị IoT 1.

Ví dụ, thiết bị điều khiển IoT tạo ra khóa công khai A và khóa cá nhân A dựa trên số ngẫu nhiên (muối), PIN của thiết bị IoT 1, và giao thức đàm phán khóa xác thực mật khẩu (PAKE).

Bước 605: Thiết bị IoT 1 gửi khóa công khai B đến thiết bị điều khiển IoT. Khóa công khai B và khóa cá nhân B là cặp khóa khác, và được tạo ra bởi thiết bị IoT 1 dựa trên số ngẫu nhiên (muối) và PIN của thiết bị IoT 1.

Bước 606: Sau khi nhận khóa công khai B, thiết bị điều khiển IoT tạo ra khóa được chia sẻ dựa trên khóa công khai B và khóa cá nhân A. Sau đó, thiết bị điều khiển IoT mã hóa khóa công khai dài hạn G0 của thiết bị điều khiển IoT bằng cách sử dụng khóa được chia sẻ, để thu được văn bản mật mã của khóa công khai dài hạn G0 của thiết bị điều khiển IoT.

Bước 607: Thiết bị điều khiển IoT gửi văn bản mật mã của khóa công khai dài hạn G0 của thiết bị điều khiển IoT đến thiết bị IoT 1.

Bước 608: Sau khi nhận khóa công khai A, thiết bị IoT 1 tạo ra khóa được chia sẻ dựa trên khóa công khai A và khóa cá nhân B. Sau đó, thiết bị IoT 1 mã hóa khóa công khai dài hạn G1 của thiết bị IoT 1 bằng cách sử dụng khóa được chia sẻ, để thu được văn bản mật mã của khóa công khai dài hạn G1 của thiết bị IoT 1.

Bước 609: Thiết bị IoT 1 gửi văn bản mật mã của khóa công khai dài hạn G1 của thiết bị IoT 1 đến thiết bị điều khiển IoT.

Bước 610: Sau khi nhận văn bản mật mã của khóa công khai dài hạn G0 của thiết bị điều khiển IoT, thiết bị IoT 1 giải mã văn bản mật mã của khóa công khai dài hạn G0

của thiết bị điều khiển IoT dựa trên khóa được chia sẻ, để thu được khóa công khai dài hạn G0 của thiết bị điều khiển IoT, và lưu trữ cục bộ khóa công khai dài hạn G0 của thiết bị điều khiển IoT.

Bước 611: Sau khi nhận văn bản mật mã của khóa công khai dài hạn G1 của thiết bị IoT 1, thiết bị điều khiển IoT giải mã văn bản mật mã của khóa công khai dài hạn G1 của thiết bị IoT 1 dựa trên khóa được chia sẻ, để thu được khóa công khai dài hạn G1 của thiết bị IoT 1, và lưu trữ cục bộ khóa công khai dài hạn G1 của thiết bị IoT 1. Theo cách này, thiết bị điều khiển IoT được liên kết với thiết bị IoT 1.

Cần lưu ý rằng không có trình tự cần thiết giữa bước 603 và bước 605, và giữa bước 604 và bước 605, nhưng bước 603 là trước bước 604.

Theo một số phương án, sau thiết bị điều khiển IoT được liên kết với thiết bị IoT 1, tiện ích của thiết bị IoT 1 có thể được thêm vào màn hình của ứng dụng IoT. Ví dụ, màn hình của ứng dụng IoT là màn hình 900 được thể hiện trên Fig.9, và bao gồm tiện ích 901 của thiết bị IoT 1. Người dùng có thể cho phép hoặc vô hiệu hóa thiết bị bằng cách thực hiện thao tác trên điều khiển trên tiện ích 900 của thiết bị IoT 1. Hơn nữa, người dùng có thể còn hiển thị, trên màn hình hiển thị bằng cách thao tác tiện ích 901 của thiết bị IoT, màn hình chi tiết bao gồm điều khiển của thiết bị IoT 1. Người dùng có thể thực hiện thao tác trên điều khiển liên quan trên màn hình, sao cho thiết bị điều khiển IoT gửi chỉ thị bằng giọng nói điều khiển đến thiết bị IoT 1, để điều khiển thiết bị IoT.

Ngoài ra, Cần lưu ý rằng, đối với mỗi thiết bị điều khiển IoT và thiết bị IoT 1, khóa công khai dài hạn và khóa cá nhân dài hạn có thể được tạo cấu hình trước trong thiết bị trước khi thiết bị được vận chuyển.

Ngoài ra, trong kịch bản mà trong đó thông tin phiên (ví dụ, ID phiên) trong thiết bị IoT không bị mất và khóa phiên vẫn ở trong khoảng thời gian hiệu lực, phương án của sáng chế còn đề xuất phương pháp đàm phán khóa, để giúp giảm các bước đàm phán khóa giữa thiết bị IoT và thiết bị điều khiển IoT, và cải thiện hiệu quả đàm phán khóa.

Ví dụ, Fig.10 thể hiện phương pháp đàm phán khóa khác theo phương án của sáng chế. Phương pháp cụ thể bao gồm các bước sau.

Bước 1001: Thiết bị điều khiển IoT truyền đa hướng thông điệp khám phá trong mạng cục bộ thứ nhất. Thông điệp khám phá bao gồm khóa công khai K2. Khóa công khai K2 được tạo ra dựa trên số ngẫu nhiên L2. Mạng cục bộ thứ nhất là mạng mà đã được truy nhập bởi thiết bị điều khiển IoT.

Đối với bước 1001, tham chiếu đến các mô tả liên quan của bước 501. Các chi tiết không được mô tả ở đây lần nữa.

Bước 1002: Thiết bị IoT 1 tạo ra khóa phiên H2 dựa trên khóa công khai K2 và số ngẫu nhiên L3 sau khi nhận thông điệp khám phá; và nếu khóa phiên H0 giữa thiết bị IoT 1 và thiết bị điều khiển IoT mà được lưu trữ trong thiết bị IoT vẫn ở trong khoảng thời gian hiệu lực, và thông tin phiên giữa thiết bị IoT 1 và thiết bị điều khiển IoT không bị mất, mã hóa thông tin thứ nhất của thiết bị IoT 1 bằng cách sử dụng khóa phiên H2, để thu được văn bản mật mã 3.

Thông tin thứ nhất bao gồm thông tin thiết bị của thiết bị IoT 1. Ngoài ra, thông tin thứ nhất có thể còn bao gồm thông tin phiên giữa thiết bị IoT 1 và thiết bị điều khiển IoT hoặc thông tin liên quan khác mà được lưu trữ trong thiết bị IoT 1. Ví dụ, thông tin phiên được bao gồm trong thông tin thứ nhất có thể là thông tin như là ID phiên.

Cụ thể, đối với các mô tả liên quan của thông tin thiết bị của thiết bị IoT 1, sự tạo ra khóa phiên H2, và tương tự, tham chiếu đến các mô tả liên quan theo các phương án trên. Các chi tiết không được mô tả ở đây lần nữa.

Theo một số phương án, nếu khóa phiên H1 giữa thiết bị IoT 1 và thiết bị IoT mà được lưu trữ trong thiết bị IoT 1 không ở trong khoảng thời gian hiệu lực hoặc thông tin phiên bị mất, thiết bị IoT 1 mã hóa thông tin thiết bị của thiết bị IoT 1 bằng cách sử dụng khóa phiên H2, để thu được văn bản mật mã 0, và sau đó thực hiện bước 503 và các bước tiếp theo.

Ví dụ, thiết bị IoT 1 có thể xác định xem thông tin phiên giữa thiết bị IoT 1 và thiết bị điều khiển IoT có bị mất hay không bằng cách xác định xem số lượng phiên giữa thiết bị IoT 1 và thiết bị điều khiển IoT có lớn hơn hoặc bằng giá trị tối đa bị giới hạn bởi hệ thống hay không. Ví dụ, nếu số lượng phiên giữa thiết bị IoT 1 và thiết bị điều khiển IoT lớn hơn hoặc bằng giá trị tối đa bị giới hạn bởi hệ thống, thiết bị IoT 1 xác định rằng thông tin phiên giữa thiết bị IoT 1 và thiết bị điều khiển IoT bị mất. Ví dụ khác, nếu số lượng phiên giữa thiết bị IoT 1 và thiết bị điều khiển IoT nhỏ hơn giá trị tối đa bị giới hạn bởi hệ thống, thiết bị IoT 1 xác định rằng thông tin phiên giữa thiết bị IoT 1 và thiết bị điều khiển IoT không bị mất.

Bước 1003: Thiết bị IoT 1 gửi văn bản mật mã 3 và khóa công khai K3 đến thiết bị điều khiển IoT. Khóa công khai K3 được tạo ra dựa trên số ngẫu nhiên L3.

Bước 1004: Thiết bị điều khiển IoT tạo ra khóa phiên H2 dựa trên khóa công khai

K3 và số ngẫu nhiên L2 sau khi nhận văn bản mật mã 3 và khóa công khai K3. Sau đó, thiết bị điều khiển IoT giải mã văn bản mật mã 3 bằng cách sử dụng khóa phiên H2, để thu được thông tin thứ nhất. Nếu khóa phiên H0 giữa thiết bị điều khiển IoT và thiết bị IoT 1 mà được lưu trữ trong thiết bị điều khiển IoT vẫn ở trong khoảng thời gian hiệu lực, và thông tin phiên giữa thiết bị điều khiển IoT và thiết bị IoT 1 không bị mất, được xác định rằng đàm phán khóa được hoàn tất.

Tiếp theo, truyền thông được mã hóa giữa thiết bị điều khiển IoT và thiết bị IoT 1 được triển khai dựa trên khóa phiên H0.

Theo một số phương án, nếu thông tin phiên giữa thiết bị điều khiển IoT và thiết bị IoT 1 bị mất, thiết bị điều khiển IoT ký thông tin phiên A bằng cách sử dụng khóa cá nhân dài hạn S0 của thiết bị điều khiển IoT, để thu được chữ ký A. Thông tin phiên A bao gồm khóa công khai K2 và khóa công khai K3. Ví dụ, thông tin phiên A bao gồm (khóa công khai K2, khóa công khai K3). Sau đó, thiết bị điều khiển IoT mã hóa chữ ký A bằng cách sử dụng khóa phiên H2, để thu được văn bản mật mã A, và gửi văn bản mật mã A đến thiết bị IoT 1. Sau khi nhận văn bản mật mã A, thiết bị IoT 1 giải mã văn bản mật mã A bằng cách sử dụng khóa phiên H2, để thu được chữ ký A, và sau đó, xác minh chữ ký A bằng cách sử dụng khóa công khai dài hạn G0 của thiết bị điều khiển IoT. Sau khi xác minh thành công chữ ký A, thiết bị IoT 1 ký thông tin phiên B bằng cách sử dụng khóa cá nhân dài hạn S1 của thiết bị IoT, để thu được chữ ký B. Thông tin phiên B bao gồm khóa công khai K3 và khóa công khai K2. Ví dụ, thông tin phiên B bao gồm (khóa công khai K3, khóa công khai K2). Thiết bị IoT 1 mã hóa chữ ký B2 và thông tin phiên C bằng cách sử dụng khóa phiên H2, để thu được văn bản mật mã B. Đối với thông tin phiên C, tham chiếu đến các mô tả liên quan của thông tin phiên 3. Thiết bị IoT 1 gửi văn bản mật mã B đến thiết bị điều khiển IoT. Sau khi nhận văn bản mật mã B, thiết bị điều khiển IoT giải mã văn bản mật mã B bằng cách sử dụng khóa phiên H2, để thu được chữ ký B và thông tin phiên C. Thiết bị điều khiển IoT xác minh chữ ký B bằng cách sử dụng khóa công khai dài hạn G1 của thiết bị IoT 1, và lưu trữ khóa phiên H2 và thông tin phiên C sau khi xác minh thành công chữ ký B. Vì thế, truyền thông được mã hóa giữa thiết bị điều khiển IoT và thiết bị IoT 1 có thể được triển khai tiếp theo dựa trên khóa phiên H2.

Các phương án trên có thể được sử dụng riêng biệt, hoặc có thể được sử dụng kết hợp với nhau. Điều này không bị giới hạn.

Theo các phương án được đề xuất trên trong sáng chế, các phương pháp được đề

xuất theo các phương án của sáng chế được mô tả từ góc độ mà thiết bị điện tử được sử dụng như thân thực thi. Để triển khai các chức năng trong phương pháp được đề xuất theo các phương án trên của sáng chế, thiết bị điện tử có thể bao gồm cấu trúc phần cứng và/hoặc mô-đun phần mềm, và triển khai các chức năng trên dưới dạng của cấu trúc phần cứng, mô-đun phần mềm, hoặc cấu trúc phần cứng cộng mô-đun phần mềm. Chức năng trong số các chức năng trên có được thực hiện dưới dạng cấu trúc phần cứng, mô-đun phần mềm, hoặc cấu trúc phần cứng cộng mô-đun phần mềm hay không phụ thuộc vào ứng dụng cụ thể và điều kiện ràng buộc thiết kế của giải pháp kỹ thuật.

Dựa trên cùng một khái niệm, Fig.11 thể hiện thiết bị điện tử 1100 theo sáng chế. Ví dụ, thiết bị điện tử 1100 bao gồm ít nhất một bộ xử lý 1110 và bộ nhớ 1120. Bộ xử lý 1110 được ghép nối với bộ nhớ 1120. Việc ghép nối theo phương án này của sáng chế là ghép nối gián tiếp hoặc kết nối truyền thông giữa các bộ máy, các đơn vị, hoặc các mô-đun, có thể dưới dạng điện, dạng cơ khí, hoặc dạng khác, và được sử dụng thông tin trao đổi giữa các bộ máy, các đơn vị, hoặc các mô-đun.

Cụ thể, bộ nhớ 1120 được tạo cấu hình để lưu trữ các chỉ thị chương trình. Khi bộ xử lý 1110 được tạo cấu hình để đọc các chỉ thị chương trình được lưu trữ trong bộ nhớ 1120, thiết bị điện tử 1100 được cho phép để thực hiện phương pháp đàm phán khóa theo các phương án của sáng chế. Ví dụ, khi bộ xử lý 1110 gọi các chỉ thị chương trình được lưu trữ trong bộ nhớ 1120, thiết bị điện tử 1100 được cho phép để thực hiện các bước được thực hiện bởi thiết bị điều khiển IoT hoặc thiết bị IoT 1 trong phương pháp đàm phán khóa được thể hiện trên Fig.5 hoặc Fig.10.

Theo một số phương án, thiết bị điện tử 1100 còn bao gồm bộ truyền nhận 1130. Ví dụ, khi thiết bị điện tử 1100 thực hiện các bước được thực hiện bởi thiết bị điều khiển IoT trong phương pháp được thể hiện trên Fig.5 hoặc Fig.10, bộ truyền nhận 1130 có thể được tạo cấu hình để truyền đa hướng thông điệp khám phá, nhận phản hồi khám phá từ thiết bị IoT, và tương tự. Ví dụ khác, khi thiết bị điện tử 1100 thực hiện các bước được thực hiện bởi thiết bị IoT 1 trong phương pháp được thể hiện trên Fig.5 hoặc Fig.10, bộ truyền nhận 1130 có thể được tạo cấu hình để nhận thông điệp khám phá, gửi phản hồi khám phá đến thiết bị điều khiển IoT, và tương tự.

Nên được hiểu rằng thiết bị điện tử 1100 có thể được tạo cấu hình để triển khai phương pháp đàm phán khóa theo các phương án của sáng chế. Đối với đặc điểm liên quan, tham chiếu đến mô tả trên. Các chi tiết không được mô tả ở đây lần nữa.

Ngoài ra, phương án của sáng chế còn đề xuất hệ thống truyền thông. Như được thể hiện trên Fig.12, hệ thống truyền thông bao gồm thiết bị điều khiển IoT 1201 và một hoặc nhiều thiết bị IoT 1202. Thiết bị điều khiển IoT 1201 được tạo cấu hình để thực hiện các bước được thực hiện bởi thiết bị điều khiển IoT trong phương pháp đàm phán khóa theo các phương án của sáng chế. Ví dụ, thiết bị điều khiển IoT 1201 thực hiện các bước được thực hiện bởi thiết bị điều khiển IoT trong phương pháp đàm phán khóa được thể hiện trên Fig.5 hoặc Fig.10. Thiết bị IoT 1202 được tạo cấu hình để chỉ báo các bước được thực hiện bởi thiết bị IoT 1 trong phương pháp đàm phán khóa theo các phương án của sáng chế. Ví dụ, thiết bị IoT 1202 thực hiện các bước được thực hiện bởi thiết bị IoT 1 trong phương pháp đàm phán khóa được thể hiện trên Fig.5 hoặc Fig.10. Đối với triển khai cụ thể, tham chiếu đến các mô tả liên quan trong phần phương pháp. Các chi tiết không được mô tả ở đây lần nữa.

Người có hiểu biết trung bình trong lĩnh vực có thể hiểu rõ ràng rằng các phương án của sáng chế có thể được triển khai bởi phần cứng, chương trình cơ sở hoặc kết hợp của chúng. Khi các phương án của sáng chế được triển khai bởi phần mềm, các chức năng trên có thể được lưu trữ trong phương tiện đọc được bằng máy tính hoặc được truyền như một hoặc nhiều chỉ thị hoặc mã trong phương tiện đọc được bằng máy tính. Phương tiện đọc được bằng máy tính có thể bao gồm phương tiện lưu trữ máy tính và phương tiện truyền thông, trong đó phương tiện truyền thông bao gồm bất kỳ phương tiện mà cho phép chương trình máy tính được truyền từ một địa điểm đến địa điểm khác. Phương tiện lưu trữ có thể là bất kỳ phương tiện khả dụng truy nhập được vào máy tính. Các ví dụ của phương tiện đọc được bằng máy tính bao gồm nhưng không bị giới hạn ở: RAM, ROM, bộ nhớ chỉ đọc lập trình và xóa được bằng điện (electrically erasable programmable read-only memory, EEPROM), đĩa compắc chứa dữ liệu chỉ đọc (compact disc read-only memory, CD-ROM) hoặc bộ lưu trữ đĩa quang khác, bộ lưu trữ đĩa quang, phương tiện lưu trữ đĩa máy tính, hoặc bộ lưu trữ đĩa máy tính khác, hoặc bất kỳ phương tiện khác mà có thể được sử dụng để mang hoặc lưu trữ mã chương trình được dự kiến dưới dạng cấu trúc lệnh hoặc dữ liệu và có thể được truy nhập bởi máy tính. Ngoài ra, bất kỳ kết nối được định nghĩa thích hợp là phương tiện đọc được bằng máy tính. Ví dụ, nếu phần mềm được truyền từ trang mạng, máy chủ hoặc nguồn từ xa khác bằng cách sử dụng cáp đồng trục, cáp sợi/dây cáp quang, cặp vặn xoắn, đường dây thuê bao kỹ thuật số (digital subscriber line, DSL) hoặc các công nghệ không dây như là tia hồng ngoại, vô

tuyến, và vi ba, cáp đồng trục, cáp sợi/dây cáp quang, cặp vặn xoắn, DSL hoặc các công nghệ không dây như là tia hồng ngoại, vô tuyến, và vi ba được bao gồm trong sự cố định của phương tiện mà chúng thuộc về. Đĩa máy tính (disk) và đĩa (disc) được sử dụng theo các phương án của sáng chế bao gồm đĩa compắc (compact disc, CD), đĩa la-de, đĩa quang, đĩa phim kỹ thuật số (digital video disc, DVD), đĩa mềm, và đĩa Blu-ray, trong đó đĩa máy tính nói chung sao chép dữ liệu bằng các phương thức từ tính, và đĩa sao chép dữ liệu quang bằng phương thức la-de. Sự kết hợp trên cũng nên được bao gồm trong phạm vi bảo hộ của phương tiện đọc được bằng máy tính.

Tóm lại, những gì được mô tả trên chỉ đơn thuần là các phương án của sáng chế, nhưng không nhằm để giới hạn phạm vi bảo hộ của sáng chế. Bất kỳ sửa đổi, thay thế tương đương, hoặc cải thiện được thực hiện mà không rời xa phạm vi và nguyên lý của sáng chế sẽ nằm trong phạm vi bảo hộ của sáng chế.

YÊU CẦU BẢO HỘ

1. Phương pháp đàm phán khóa, trong đó phương pháp bao gồm các bước:

truyền đa hướng, bởi thiết bị điều khiển mạng lưới thiết bị kết nối Internet (Internet of Things, IoT), thông điệp khám phá trong mạng cục bộ thứ nhất, trong đó thông điệp khám phá bao gồm khóa công khai thứ nhất, mạng cục bộ thứ nhất là mạng mà đã được truy nhập bởi thiết bị điều khiển IoT, và khóa công khai thứ nhất thu được dựa trên số ngẫu nhiên thứ nhất;

nhận, bởi thiết bị điều khiển IoT, phản hồi khám phá từ thiết bị IoT thứ nhất, trong đó phản hồi khám phá bao gồm văn bản mật mã thứ nhất và khóa công khai thứ hai, văn bản mật mã thứ nhất thu được bằng cách mã hóa thông tin thiết bị của thiết bị IoT thứ nhất dựa trên khóa phiên thứ nhất, và khóa công khai thứ hai thu được dựa trên số ngẫu nhiên thứ hai.

gửi, bởi thiết bị điều khiển IoT, văn bản mật mã thứ hai đến thiết bị IoT thứ nhất, trong đó văn bản mật mã thứ hai thu được bằng cách mã hóa chữ ký thứ nhất dựa trên khóa phiên thứ nhất, chữ ký thứ nhất là chữ ký trên thông tin phiên thứ nhất dựa trên khóa cá nhân dài hạn của thiết bị điều khiển IoT, thông tin phiên thứ nhất bao gồm khóa công khai thứ nhất và khóa công khai thứ hai, và khóa phiên thứ nhất thu được dựa trên số ngẫu nhiên thứ nhất và khóa công khai thứ hai;

nhận, bởi thiết bị điều khiển IoT, văn bản mật mã thứ ba đến thiết bị IoT thứ nhất, trong đó văn bản mật mã thứ ba thu được bằng cách mã hóa chữ ký thứ hai và thông tin phiên thứ hai dựa trên khóa phiên thứ nhất, chữ ký thứ hai là chữ ký trên thông tin phiên thứ ba dựa trên khóa cá nhân dài hạn của thiết bị IoT thứ nhất, thông tin phiên thứ ba bao gồm khóa công khai thứ hai và khóa công khai thứ nhất, và thông tin phiên thứ hai bao gồm mã định danh (identifier, ID) phiên;

giải mã, bởi thiết bị điều khiển IoT, văn bản mật mã thứ ba dựa trên khóa phiên thứ nhất, để thu được chữ ký thứ hai và thông tin phiên thứ hai; và xác minh chữ ký thứ hai dựa trên khóa công khai dài hạn của thiết bị IoT thứ nhất;

lưu, bởi thiết bị điều khiển IoT, khóa phiên thứ nhất và thông tin phiên thứ hai sau khi chữ ký thứ hai được xác minh thành công; và

thực hiện, bởi thiết bị điều khiển IoT, truyền thông được mã hóa với thiết bị IoT thứ nhất dựa trên khóa phiên thứ nhất.

2. Phương pháp theo điểm 1, trong đó thông tin phiên thứ hai còn bao gồm khoảng

thời gian hiệu lực của khóa phiên thứ nhất.

3. Phương pháp theo điểm 1 hoặc 2, trong đó sau khi truyền đa hướng, bởi thiết bị điều khiển IoT, thông điệp khám phá trong mạng cục bộ thứ nhất, phương pháp còn bao gồm các bước:

nhận, bởi thiết bị điều khiển IoT, văn bản mật mã thứ tư được gửi bởi thiết bị IoT thứ nhất, trong đó văn bản mật mã thứ tư thu được bằng cách mã hóa thông tin thứ nhất dựa trên khóa phiên thứ nhất, và thông tin thứ nhất bao gồm thông tin thiết bị của thiết bị IoT thứ nhất; và

thực hiện, bởi thiết bị IoT thứ nhất, truyền thông được mã hóa với thiết bị IoT thứ nhất dựa trên khóa phiên thứ hai nếu thiết bị điều khiển IoT xác định rằng khóa phiên thứ hai được lưu trữ giữa thiết bị điều khiển IoT và thiết bị IoT thứ nhất ở trong khoảng thời gian hiệu lực hoặc thông tin phiên được lưu trữ giữa thiết bị điều khiển IoT và thiết bị IoT thứ nhất không bị mất.

4. Phương pháp theo điểm 3, trong đó thông tin thứ nhất còn bao gồm thông tin phiên thứ tư, và thông tin phiên thứ tư bao gồm ID được lưu trữ của phiên giữa thiết bị IoT thứ nhất và thiết bị IoT thứ nhất.

5. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 4, trong đó việc truyền đa hướng, bởi thiết bị điều khiển IoT, thông điệp khám phá trong mạng cục bộ thứ nhất bao gồm các bước:

truyền đa hướng định kỳ, bởi thiết bị điều khiển IoT, thông điệp khám phá trong mạng cục bộ thứ nhất; và/hoặc

truyền đa hướng, bởi thiết bị điều khiển IoT, thông điệp khám phá trong mạng cục bộ thứ nhất khi thiết bị điều khiển IoT chuyển mạch từ mạng cục bộ thứ hai sang mạng cục bộ thứ nhất; và/hoặc

truyền đa hướng, bởi thiết bị điều khiển IoT, thông điệp khám phá trong mạng cục bộ thứ nhất khi thiết bị điều khiển IoT được liên kết với thiết bị IoT mới; và/hoặc

truyền đa hướng, bởi thiết bị điều khiển IoT, thông điệp khám phá trong mạng cục bộ thứ nhất khi khóa phiên của thiết bị IoT thứ hai đạt đến thời điểm hết hạn của khoảng thời gian hiệu lực.

6. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 5, trong đó thiết bị IoT thứ nhất ở trong mạng cục bộ thứ hai.

7. Phương pháp đàm phán khóa, trong đó phương pháp bao gồm các bước:

nhận, bởi thiết bị mạng lưới thiết bị kết nối Internet (Internet of Things, IoT), sự truyền đa hướng thông điệp khám phá bởi thiết bị điều khiển IoT trong mạng cục bộ thứ nhất, trong đó thông điệp khám phá bao gồm khóa công khai thứ nhất, mạng cục bộ thứ nhất là mạng mà đã được truy nhập bởi thiết bị điều khiển IoT, và khóa công khai thứ nhất thu được dựa trên số ngẫu nhiên thứ nhất;

gửi, bởi thiết bị IoT, phản hồi khám phá đến thiết bị điều khiển IoT, trong đó phản hồi khám phá bao gồm văn bản mật mã thứ nhất và khóa công khai thứ hai, văn bản mật mã thứ nhất thu được bằng cách mã hóa thông tin thiết bị của thiết bị IoT thứ nhất dựa trên khóa phiên thứ nhất, khóa phiên thứ nhất thu được dựa trên khóa công khai thứ nhất và số ngẫu nhiên thứ hai, và khóa công khai thứ hai thu được dựa trên số ngẫu nhiên thứ hai;

nhận, bởi thiết bị IoT, văn bản mật mã thứ hai được gửi bởi thiết bị điều khiển IoT, trong đó văn bản mật mã thứ hai thu được bằng cách mã hóa chữ ký thứ nhất dựa trên khóa phiên thứ nhất, chữ ký thứ nhất là chữ ký trên thông tin phiên thứ nhất dựa trên khóa cá nhân dài hạn của thiết bị điều khiển IoT, và thông tin phiên thứ nhất bao gồm khóa công khai thứ nhất và khóa công khai thứ hai; và

giải mã, bởi thiết bị IoT, văn bản mật mã thứ hai dựa trên khóa phiên thứ nhất để thu được chữ ký thứ nhất, và gửi văn bản mật mã thứ ba đến thiết bị điều khiển IoT sau khi xác minh chữ ký thứ nhất dựa trên khóa công khai hợp lệ lâu dài của thiết bị điều khiển IoT, trong đó

văn bản mật mã thứ ba thu được bằng cách mã hóa chữ ký thứ hai và thông tin phiên thứ hai dựa trên khóa phiên thứ nhất, chữ ký thứ hai là chữ ký trên thông tin phiên thứ ba dựa trên khóa cá nhân dài hạn của thiết bị IoT, thông tin phiên thứ ba bao gồm khóa công khai thứ hai và khóa công khai thứ nhất, và thông tin phiên thứ hai bao gồm mã định danh (identifier, ID) phiên.

8. Phương pháp theo điểm 7, trong đó thông tin phiên thứ hai còn bao gồm khoảng thời gian hiệu lực của khóa phiên thứ nhất.

9. Phương pháp theo điểm 7 hoặc 8, trong đó sau khi nhận, bởi thiết bị IoT, thông điệp khám phá và trước khi gửi, bởi thiết bị IoT, phản hồi khám phá đến thiết bị điều khiển IoT, phương pháp còn bao gồm các bước:

xác định, bởi thiết bị IoT, rằng khóa phiên thứ hai được lưu trữ giữa thiết bị IoT và thiết bị điều khiển IoT không ở trong khoảng thời gian hiệu lực, hoặc không có thông

tin phiên giữa thiết bị IoT và thiết bị IoT được lưu trữ.

10. Phương pháp theo điểm 9, trong đó sau khi nhận, bởi thiết bị IoT, thông điệp khám phá, phương pháp còn bao gồm các bước:

gửi, bởi thiết bị IoT, văn bản mật mã thứ tư đến thiết bị điều khiển IoT nếu thiết bị IoT xác định rằng khóa phiên thứ hai được lưu trữ giữa thiết bị IoT và thiết bị điều khiển IoT ở trong khoảng thời gian hiệu lực hoặc thông tin phiên được lưu trữ giữa thiết bị IoT và thiết bị IoT không bị mất, trong đó

văn bản mật mã thứ tư thu được bằng cách mã hóa thông tin thứ nhất dựa trên khóa phiên thứ nhất, và thông tin thứ nhất bao gồm thông tin thiết bị của thiết bị IoT.

11. Phương pháp theo điểm 10, trong đó thông tin thứ nhất còn bao gồm thông tin phiên.

12. Phương pháp theo điểm bất kỳ trong số các điểm từ 7 đến 11, trong đó việc nhận, bởi thiết bị IoT, sự truyền đa hướng thông điệp khám phá bởi thiết bị điều khiển IoT trong mạng cục bộ thứ nhất bao gồm:

nhận định kỳ, bởi thiết bị IoT, sự truyền đa hướng thông điệp khám phá bởi thiết bị điều khiển IoT trong mạng cục bộ thứ nhất; và/hoặc

nhận, bởi thiết bị IoT trong lúc chuyển mạch mạng, sự truyền đa hướng thông điệp khám phá bởi thiết bị điều khiển IoT trong mạng cục bộ thứ nhất; và/hoặc

nhận, bởi thiết bị IoT sau khi được liên kết với thiết bị điều khiển IoT, sự truyền đa hướng thông điệp khám phá bởi thiết bị điều khiển IoT trong mạng cục bộ thứ nhất; và/hoặc

nhận, bởi thiết bị IoT khi khóa phiên thứ hai được lưu trữ giữa thiết bị IoT và thiết bị điều khiển IoT đạt đến thời điểm hết hạn của khoảng thời gian hiệu lực, thông điệp khám phá truyền đa hướng bởi thiết bị điều khiển IoT trong mạng cục bộ thứ nhất.

13. Phương pháp theo điểm bất kỳ trong số các điểm từ 7 đến 12, trong đó thiết bị IoT ở trong mạng cục bộ thứ hai.

14. Thiết bị điện tử, trong đó thiết bị điện tử bao gồm bộ truyền nhận, bộ nhớ, và bộ xử lý, trong đó

bộ truyền nhận được tạo cấu hình để gửi hoặc nhận thông tin;

bộ nhớ được tạo cấu hình để lưu trữ các chỉ thị chương trình; và

bộ xử lý được tạo cấu hình để đọc và thực thi các chỉ thị chương trình được lưu trữ trong bộ nhớ, trong đó khi các chỉ thị chương trình được thực thi bởi bộ xử lý, thiết

bị điện tử được cho phép để thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 13.

15. Chip, trong đó chip được ghép nối với bộ nhớ trong thiết bị điện tử, và điều khiển thiết bị điện tử để thực hiện phương pháp đàm phán khóa theo điểm bất kỳ trong số các điểm từ 1 đến 6, hoặc điều khiển thiết bị điện tử để thực hiện phương pháp đàm phán khóa theo điểm bất kỳ trong số các điểm từ 7 đến 13.

16. Phương tiện lưu trữ máy tính, trong đó phương tiện lưu trữ máy tính lưu trữ các chỉ thị chương trình, và khi các chỉ thị chương trình chạy trên thiết bị điện tử, thiết bị điện tử được cho phép để thực hiện phương pháp đàm phán khóa theo điểm bất kỳ trong số các điểm từ 1 đến 6 hoặc phương pháp đàm phán khóa theo điểm bất kỳ trong số các điểm từ 7 đến 13.

17. Hệ thống truyền thông, bao gồm thiết bị điều khiển IoT và ít nhất một thiết bị IoT, trong đó thiết bị điều khiển IoT được tạo cấu hình để thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 6, và thiết bị IoT được tạo cấu hình để thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 7 đến 13.

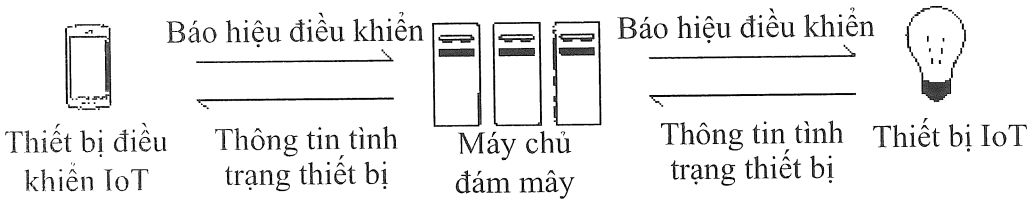

Báo hiệu điều khiển
Báo hiệu điều khiển
Thiết bị điều khiển IoT
Thông tin tình trạng thiết bị
Máy chủ đám mây
Thông tin tình trạng thiết bị
Thiết bị IoT

FIG. 1

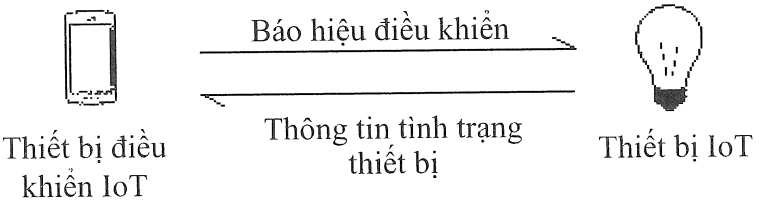

Báo hiệu điều khiển
Thiết bị điều khiển IoT
Thông tin tình trạng thiết bị
Thiết bị IoT

FIG. 2

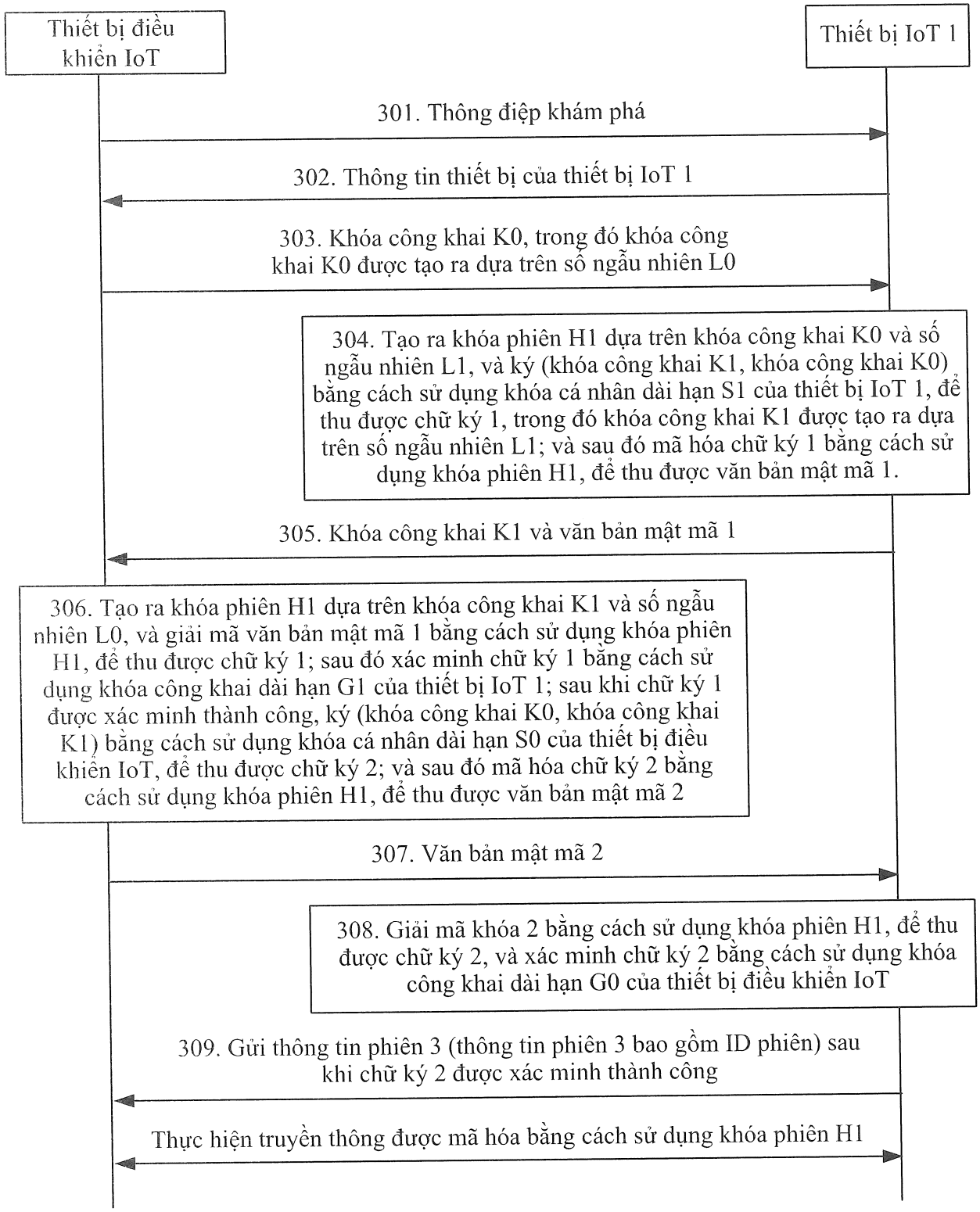

Thiết bị điều khiển IoT
Thiết bị IoT 1
301. Thông điệp khám phá
302. Thông tin thiết bị của thiết bị IoT 1
303. Khóa công khai K0, trong đó khóa công khai K0 được tạo ra dựa trên số ngẫu nhiên L0
304. Tạo ra khóa phiên H1 dựa trên khóa công khai K0 và số ngẫu nhiên L1, và ký (khóa công khai K1, khóa công khai K0) bằng cách sử dụng khóa cá nhân dài hạn S1 của thiết bị IoT 1, để thu được chữ ký 1, trong đó khóa công khai K1 được tạo ra dựa trên số ngẫu nhiên L1; và sau đó mã hóa chữ ký 1 bằng cách sử dụng khóa phiên H1, để thu được văn bản mật mã 1.
305. Khóa công khai K1 và văn bản mật mã 1
306. Tạo ra khóa phiên H1 dựa trên khóa công khai K1 và số ngẫu nhiên L0, và giải mã văn bản mật mã 1 bằng cách sử dụng khóa phiên H1, để thu được chữ ký 1; sau đó xác minh chữ ký 1 bằng cách sử dụng khóa công khai dài hạn G1 của thiết bị IoT 1; sau khi chữ ký 1 được xác minh thành công, ký (khóa công khai K0, khóa công khai K1) bằng cách sử dụng khóa cá nhân dài hạn S0 của thiết bị điều khiển IoT, để thu được chữ ký 2; và sau đó mã hóa chữ ký 2 bằng cách sử dụng khóa phiên H1, để thu được văn bản mật mã 2
307. Văn bản mật mã 2
308. Giải mã khóa 2 bằng cách sử dụng khóa phiên H1, để thu được chữ ký 2, và xác minh chữ ký 2 bằng cách sử dụng khóa công khai dài hạn G0 của thiết bị điều khiển IoT
309. Gửi thông tin phiên 3 (thông tin phiên 3 bao gồm ID phiên) sau khi chữ ký 2 được xác minh thành công
Thực hiện truyền thông được mã hóa bằng cách sử dụng khóa phiên H1

FIG. 3

3/14

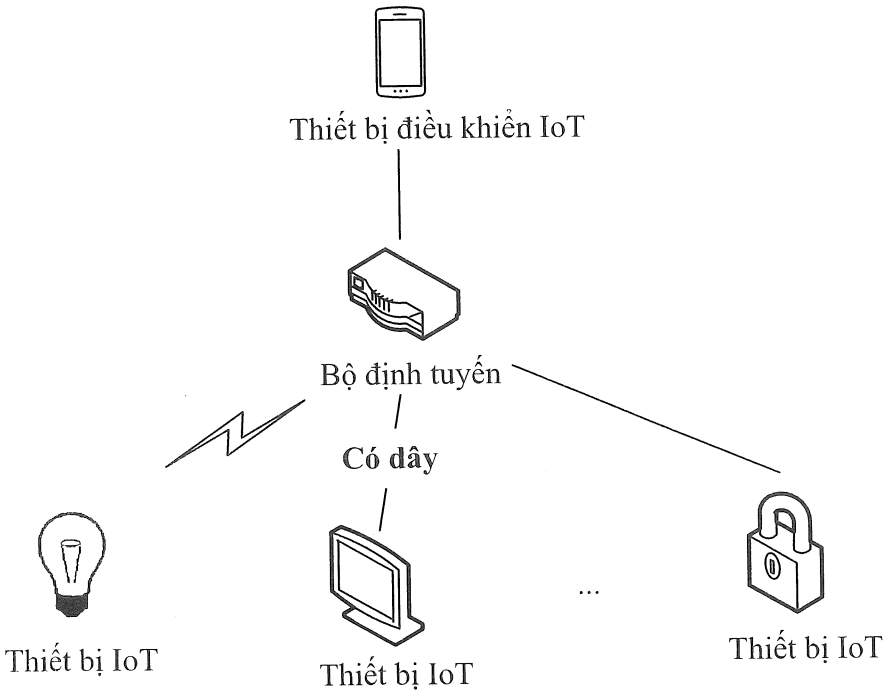

Thiết bị điều khiển IoT
Bộ định tuyến
Có dây
Thiết bị IoT
Thiết bị IoT
...
Thiết bị IoT

FIG. 4

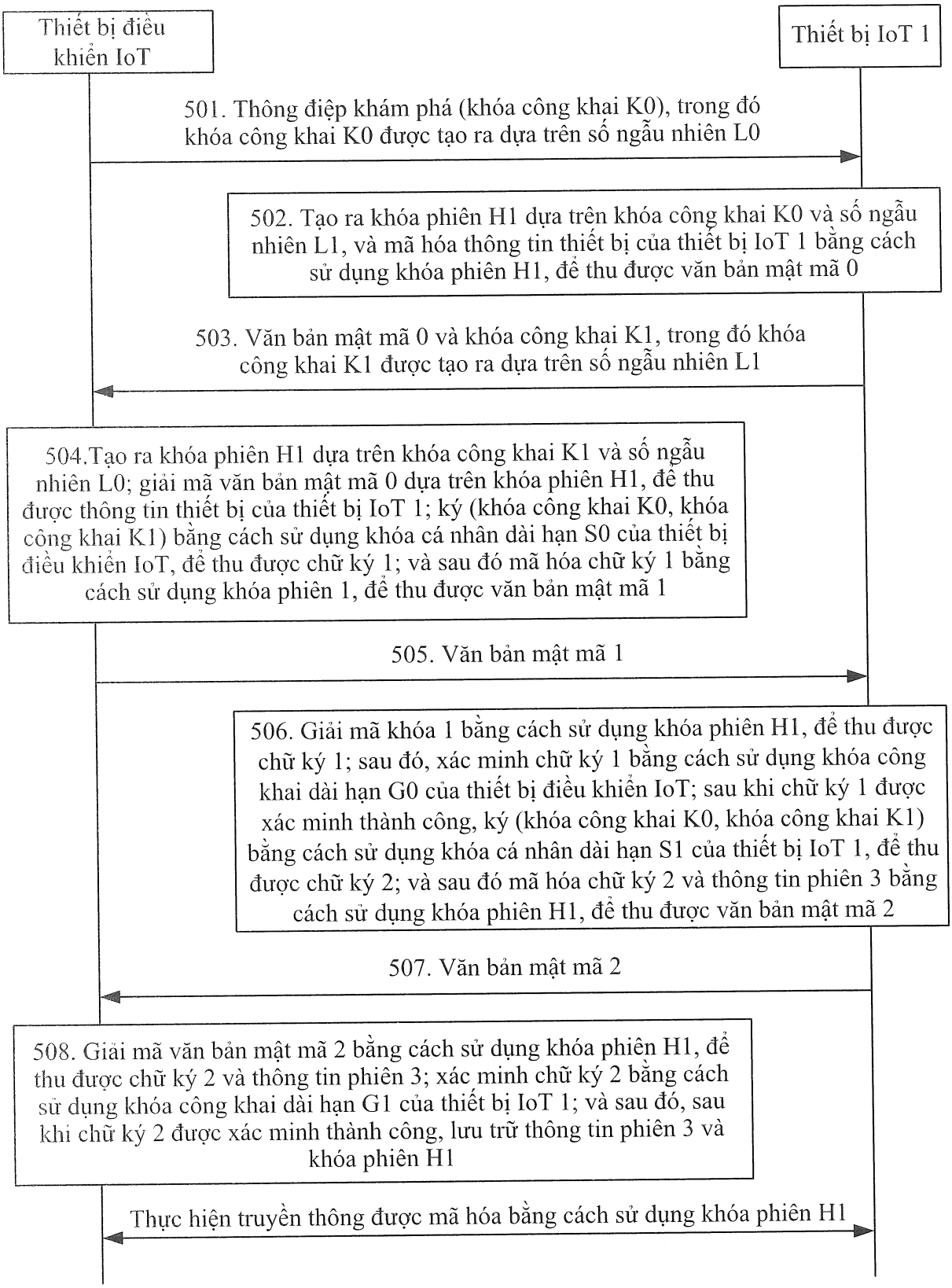

Thiết bị điều khiển IoT
Thiết bị IoT 1
501. Thông điệp khám phá (khóa công khai K0), trong đó khóa công khai K0 được tạo ra dựa trên số ngẫu nhiên L0
502. Tạo ra khóa phiên H1 dựa trên khóa công khai K0 và số ngẫu nhiên L1, và mã hóa thông tin thiết bị của thiết bị IoT 1 bằng cách sử dụng khóa phiên H1, để thu được văn bản mật mã 0
503. Văn bản mật mã 0 và khóa công khai K1, trong đó khóa công khai K1 được tạo ra dựa trên số ngẫu nhiên L1
504.Tạo ra khóa phiên H1 dựa trên khóa công khai K1 và số ngẫu nhiên L0; giải mã văn bản mật mã 0 dựa trên khóa phiên H1, để thu được thông tin thiết bị của thiết bị IoT 1; ký (khóa công khai K0, khóa công khai K1) bằng cách sử dụng khóa cá nhân dài hạn S0 của thiết bị điều khiển IoT, để thu được chữ ký 1; và sau đó mã hóa chữ ký 1 bằng cách sử dụng khóa phiên 1, để thu được văn bản mật mã 1
505. Văn bản mật mã 1
506. Giải mã khóa 1 bằng cách sử dụng khóa phiên H1, để thu được chữ ký 1; sau đó, xác minh chữ ký 1 bằng cách sử dụng khóa công khai dài hạn G0 của thiết bị điều khiển IoT; sau khi chữ ký 1 được xác minh thành công, ký (khóa công khai K0, khóa công khai K1) bằng cách sử dụng khóa cá nhân dài hạn S1 của thiết bị IoT 1, để thu được chữ ký 2; và sau đó mã hóa chữ ký 2 và thông tin phiên 3 bằng cách sử dụng khóa phiên H1, để thu được văn bản mật mã 2
507. Văn bản mật mã 2
508. Giải mã văn bản mật mã 2 bằng cách sử dụng khóa phiên H1, để thu được chữ ký 2 và thông tin phiên 3; xác minh chữ ký 2 bằng cách sử dụng khóa công khai dài hạn G1 của thiết bị IoT 1; và sau đó, sau khi chữ ký 2 được xác minh thành công, lưu trữ thông tin phiên 3 và khóa phiên H1
Thực hiện truyền thông được mã hóa bằng cách sử dụng khóa phiên H1

FIG. 5

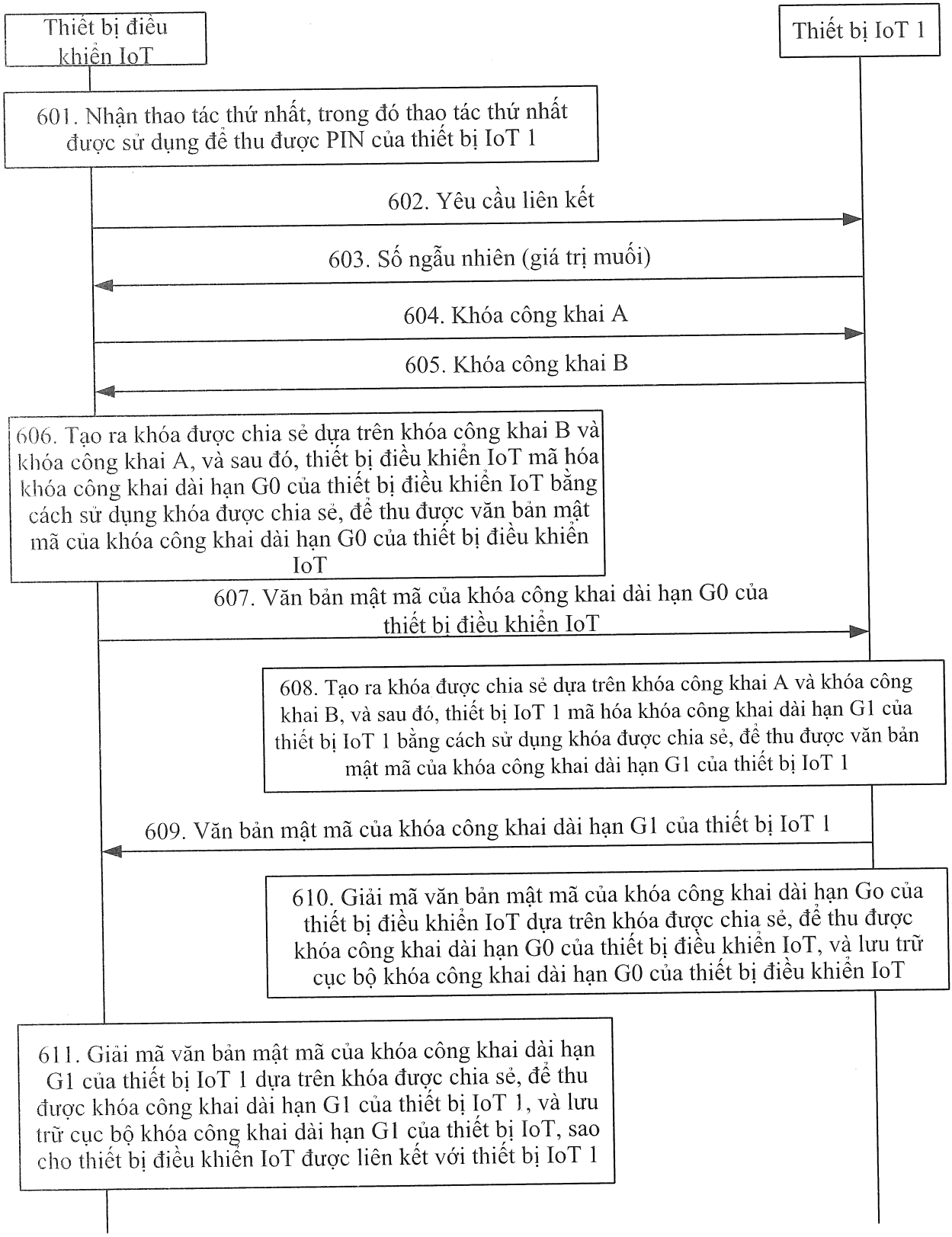
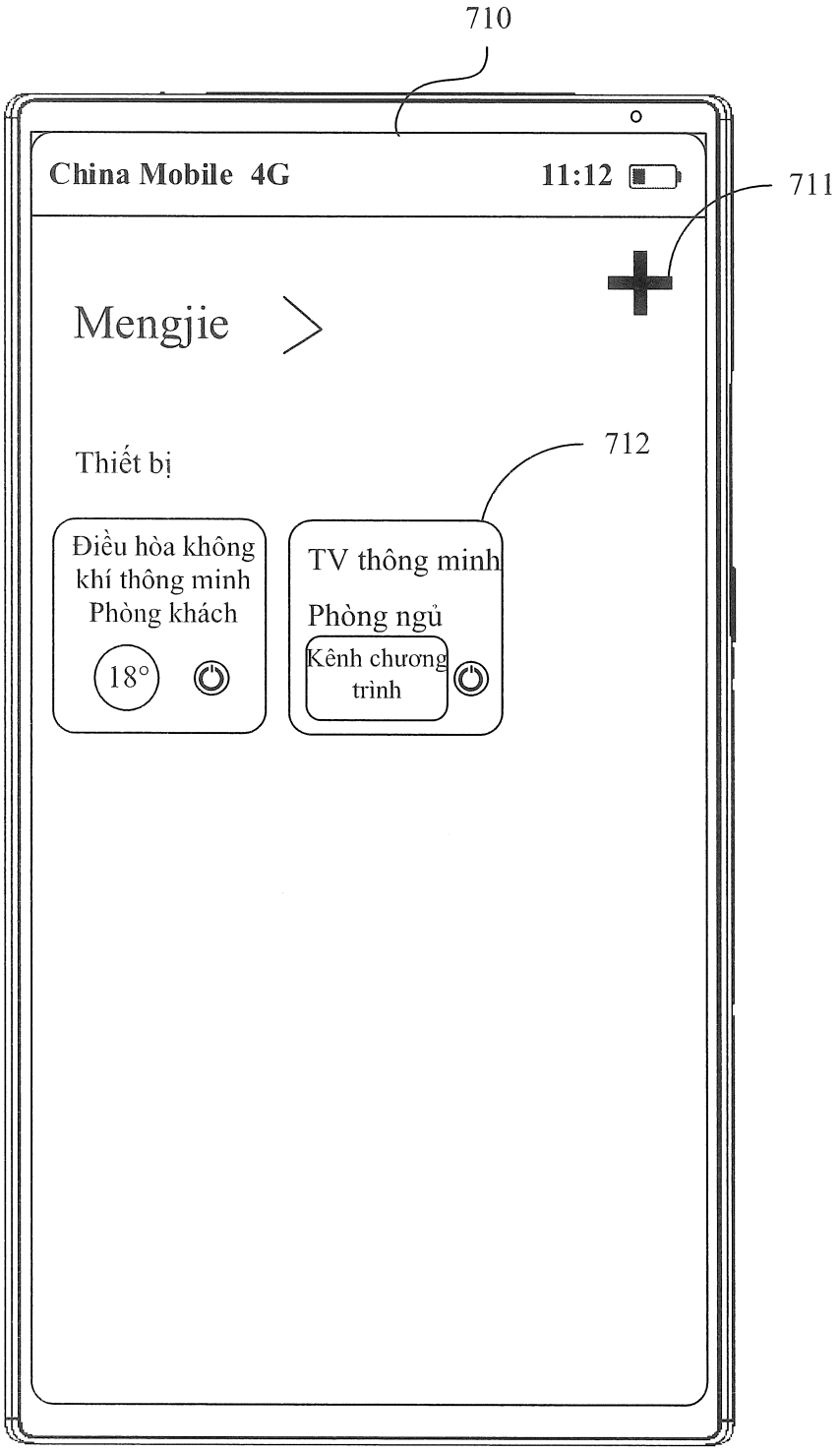

Thiết bị điều khiển IoT
Thiết bị IoT 1
601. Nhận thao tác thứ nhất, trong đó thao tác thứ nhất được sử dụng để thu được PIN của thiết bị IoT 1
602. Yêu cầu liên kết
603. Số ngẫu nhiên (giá trị muối)
604. Khóa công khai A
605. Khóa công khai B
606. Tạo ra khóa được chia sẻ dựa trên khóa công khai B và khóa công khai A, và sau đó, thiết bị điều khiển IoT mã hóa khóa công khai dài hạn G0 của thiết bị điều khiển IoT bằng cách sử dụng khóa được chia sẻ, để thu được văn bản mật mã của khóa công khai dài hạn G0 của thiết bị điều khiển IoT
607. Văn bản mật mã của khóa công khai dài hạn G0 của thiết bị điều khiển IoT
608. Tạo ra khóa được chia sẻ dựa trên khóa công khai A và khóa công khai B, và sau đó, thiết bị IoT 1 mã hóa khóa công khai dài hạn G1 của thiết bị IoT 1 bằng cách sử dụng khóa được chia sẻ, để thu được văn bản mật mã của khóa công khai dài hạn G1 của thiết bị IoT 1
609. Văn bản mật mã của khóa công khai dài hạn G1 của thiết bị IoT 1
610. Giải mã văn bản mật mã của khóa công khai dài hạn Go của thiết bị điều khiển IoT dựa trên khóa được chia sẻ, để thu được khóa công khai dài hạn G0 của thiết bị điều khiển IoT, và lưu trữ cục bộ khóa công khai dài hạn G0 của thiết bị điều khiển IoT
611. Giải mã văn bản mật mã của khóa công khai dài hạn G1 của thiết bị IoT 1 dựa trên khóa được chia sẻ, để thu được khóa công khai dài hạn G1 của thiết bị IoT 1, và lưu trữ cục bộ khóa công khai dài hạn G1 của thiết bị IoT, sao cho thiết bị điều khiển IoT được liên kết với thiết bị IoT 1

FIG. 6

ĐẾN FIG. 7B

FIG. 7A



TIẾP TỪ FIG. 7A

ĐẾN FIG. 7C

FIG. 7B

TIẾP
TỪ
FIG. 7B

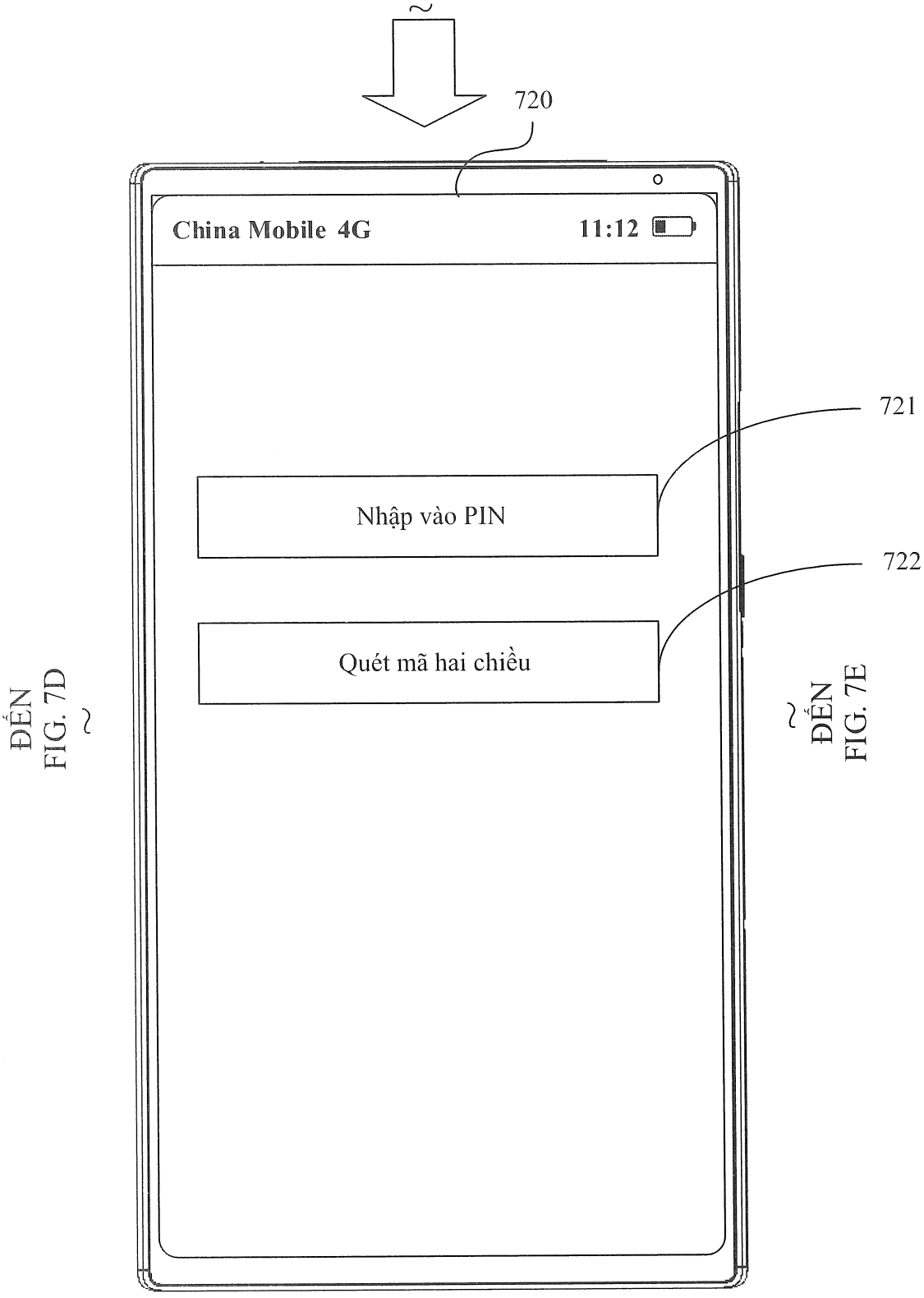
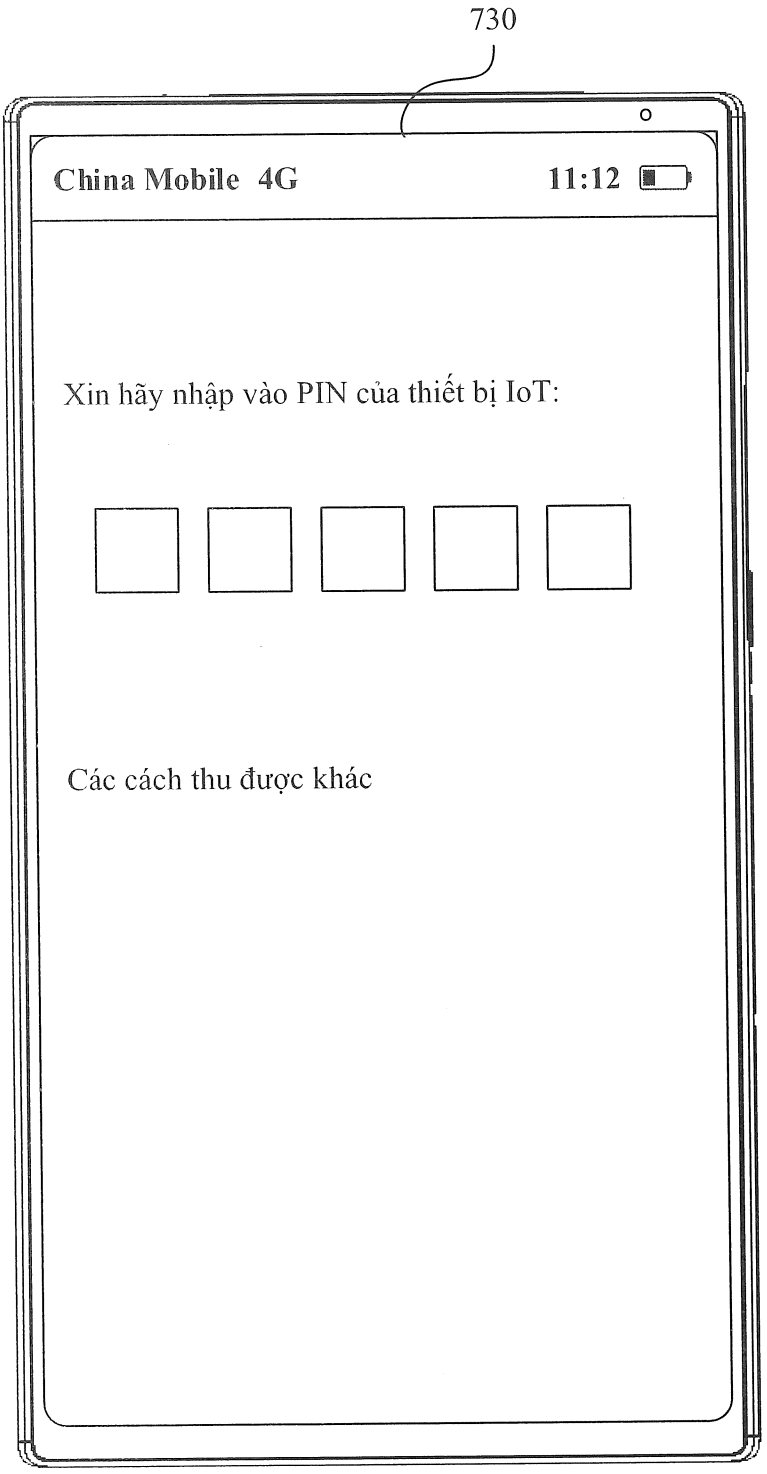


FIG. 7C



TIẾP TỪ FIG. 7C

FIG. 7D

10/14

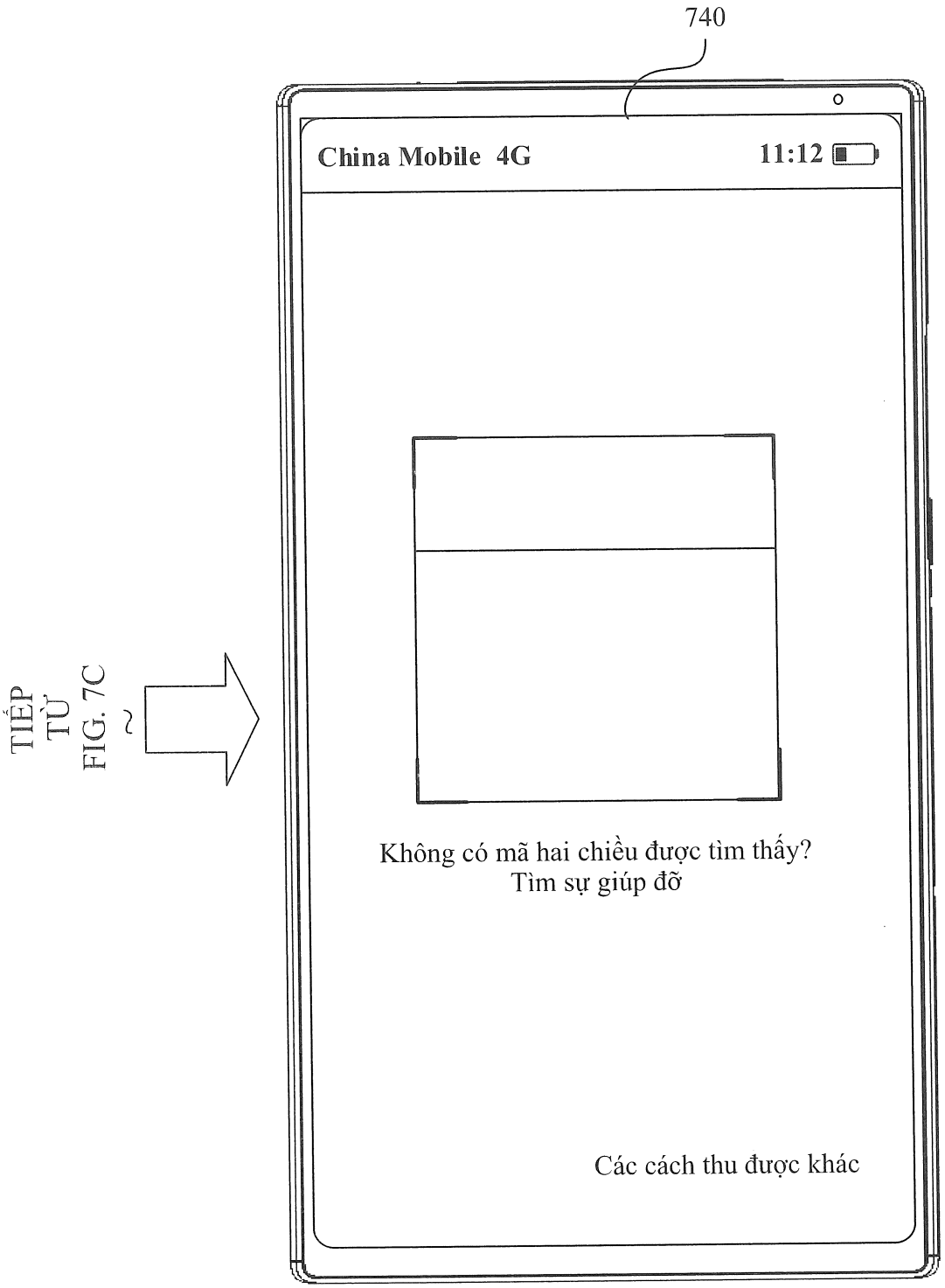

740
China Mobile 4G
11:12
Không có mã hai chiều được tìm thấy?
Tìm sự giúp đỡ
Các cách thu được khác
TIẾP TỪ FIG. 7C

FIG. 7E

11/14

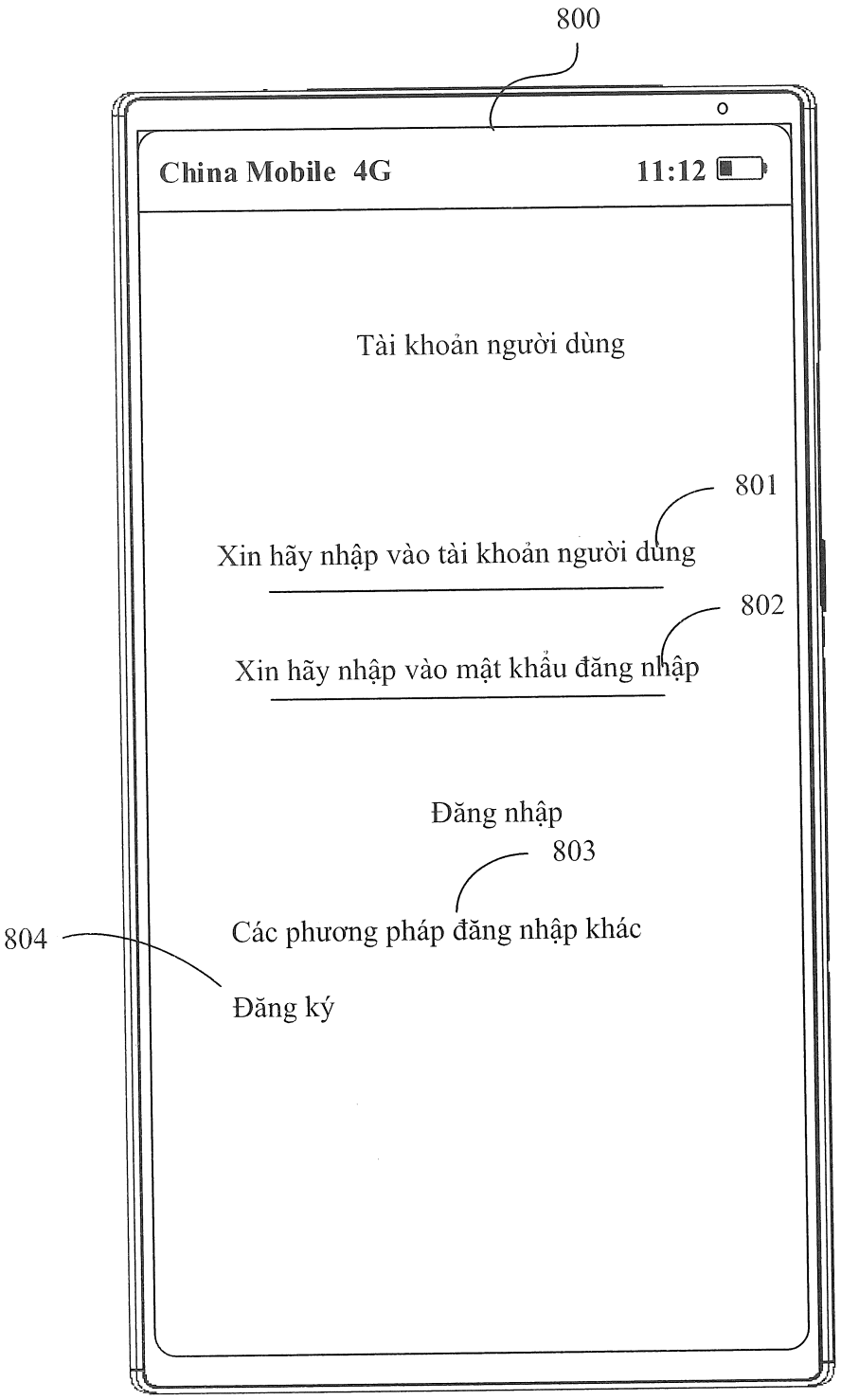

800
China Mobile 4G
11:12
Tài khoản người dùng
801
Xin hãy nhập vào tài khoản người dùng
802
Xin hãy nhập vào mật khẩu đăng nhập
Đăng nhập
803
Các phương pháp đăng nhập khác
804
Đăng ký

FIG. 8

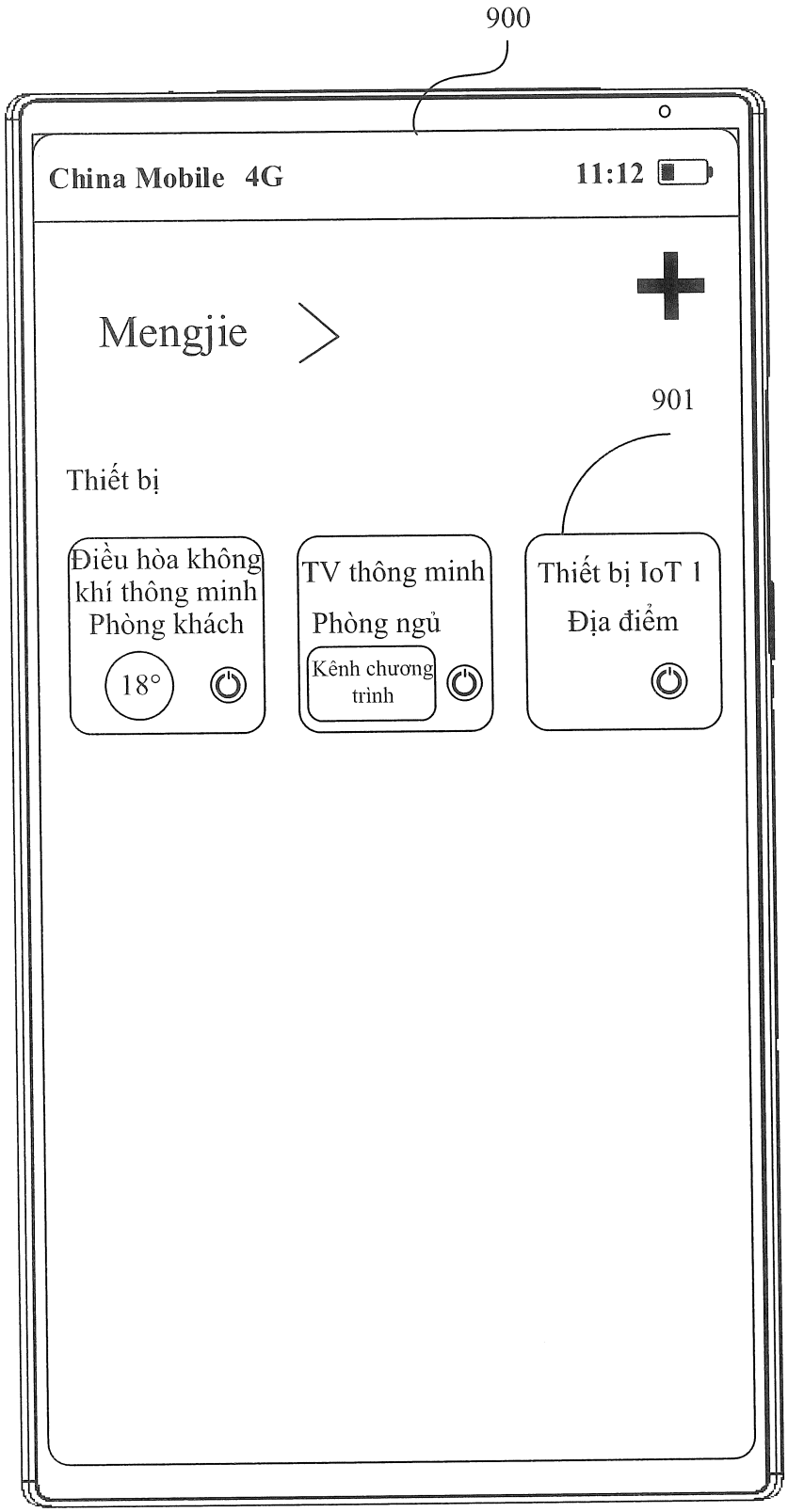

900
China Mobile 4G
11:12
Mengjie
901
Thiết bị
Điều hòa không khí thông minh
Phòng khách
18°
TV thông minh
Phòng ngủ
Kênh chương trình
Thiết bị IoT 1
Địa điểm

FIG. 9

13/14

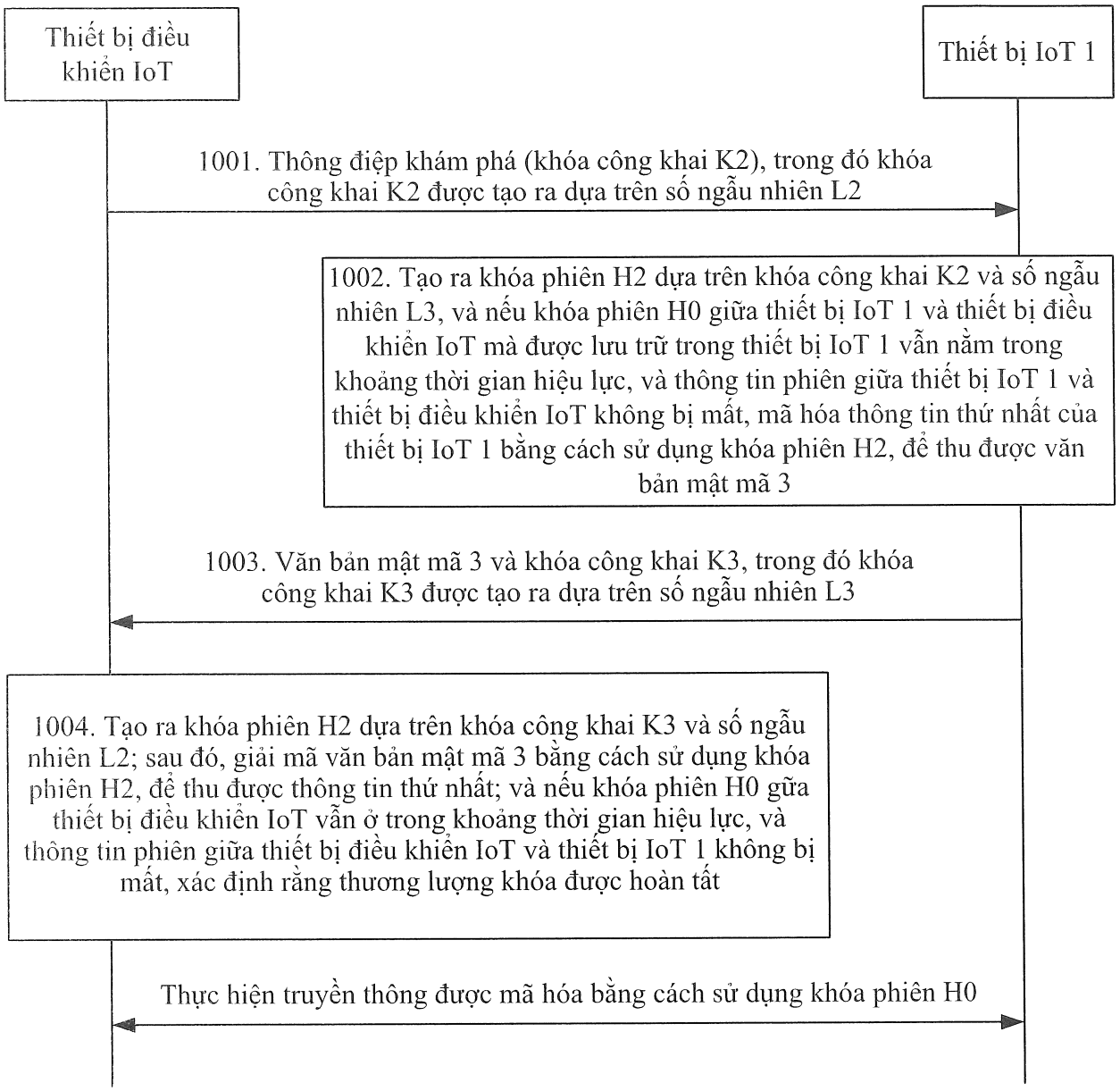

Thiết bị điều khiển IoT
Thiết bị IoT 1
1001. Thông điệp khám phá (khóa công khai K2), trong đó khóa công khai K2 được tạo ra dựa trên số ngẫu nhiên L2
1002. Tạo ra khóa phiên H2 dựa trên khóa công khai K2 và số ngẫu nhiên L3, và nếu khóa phiên H0 giữa thiết bị IoT 1 và thiết bị điều khiển IoT mà được lưu trữ trong thiết bị IoT 1 vẫn nằm trong khoảng thời gian hiệu lực, và thông tin phiên giữa thiết bị IoT 1 và thiết bị điều khiển IoT không bị mất, mã hóa thông tin thứ nhất của thiết bị IoT 1 bằng cách sử dụng khóa phiên H2, để thu được văn bản mật mã 3
1003. Văn bản mật mã 3 và khóa công khai K3, trong đó khóa công khai K3 được tạo ra dựa trên số ngẫu nhiên L3
1004. Tạo ra khóa phiên H2 dựa trên khóa công khai K3 và số ngẫu nhiên L2; sau đó, giải mã văn bản mật mã 3 bằng cách sử dụng khóa phiên H2, để thu được thông tin thứ nhất; và nếu khóa phiên H0 giữa thiết bị điều khiển IoT vẫn ở trong khoảng thời gian hiệu lực, và thông tin phiên giữa thiết bị điều khiển IoT và thiết bị IoT 1 không bị mất, xác định rằng thương lượng khóa được hoàn tất
Thực hiện truyền thông được mã hóa bằng cách sử dụng khóa phiên H0

FIG. 10

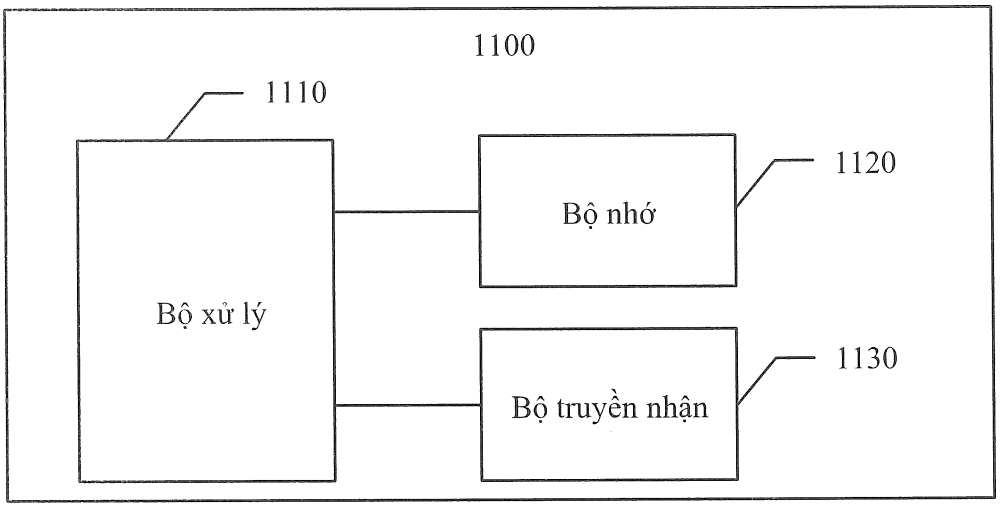

1100
1110
Bộ xử lý
1120
Bộ nhớ
1130
Bộ truyền nhận

FIG. 11

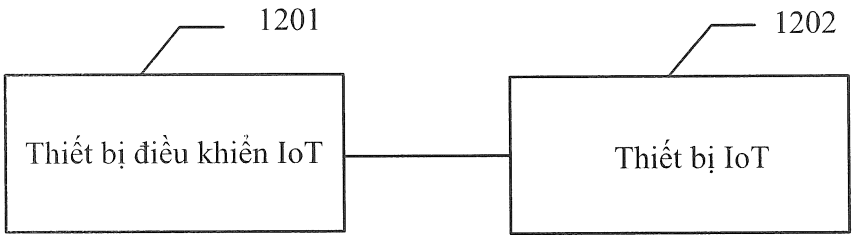

1201
Thiết bị điều khiển IoT
1202
Thiết bị IoT

FIG. 12