(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) **1-0035944**

(51)[2020.01] **H04L 9/08**

(13) **B**

(21) 1-2020-04979
(22) 15/08/2018
(86) PCT/CN2018/100618 15/08/2018
(87) WO2019/153701 15/08/2019
(30) 201810147255.9 12/02/2018 CN
(45) 26/06/2023 423
(43) 25/12/2020 393
(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)
Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129, P. R. China
(72) ZHOU, Chong (CN); FU, Tianfu (CN); ZHANG, Dacheng (CN); WEI, Jianxiong (CN).
(74) Công ty Luật TNHH T&G (TGVN)

(54) PHƯƠNG PHÁP THU KÝ HIỆU NHẬN DẠNG THIẾT BỊ, ĐẦU CUỐI VÀ THIẾT BỊ MẠNG

(57) Sáng chế đề xuất phương tháp thu ký hiệu nhận dạng (identifier, ID) thiết bị, đầu cuối, thiết bị mạng, và phương tiện lưu trữ đọc được bằng máy tính. Phương pháp này gồm có các bước: gửi, bởi đầu cuối đến thiết bị mạng, thông báo thứ nhất được sử dụng để thu ID thiết bị, trong đó ID thiết bị được sử dụng để nhận dạng toàn cầu đầu cuối theo cách duy nhất; nhận, bởi đầu cuối, cặp khóa được mã hóa được gửi bởi thiết bị mạng, trong đó cặp khóa này gồm có khóa công cộng thứ nhất và khóa riêng thứ nhất; nhận, bởi đầu cuối, thông tin được gửi bởi thiết bị mạng, trong đó thông tin này được sử dụng để nhận dạng rằng khóa công cộng thứ nhất là ID thiết bị của đầu cuối; và xác định, bởi đầu cuối, rằng khóa công cộng thứ nhất là ID thiết bị. Phương pháp này có thể tránh một cách hiệu quả sự lặp lại ID thiết bị, đơn giản hóa quá trình tạo cấu hình, giảm các mức bổ sung hệ thống, và cải thiện tính bảo mật và tính khả dụng của sơ đồ thu ID thiết bị tổng thể.


Đầu cuối
Thiết bị mạng 1
Thiết bị mạng 2
S201. Gửi thông báo 1 và yêu cầu đăng ký
S202. Gửi thông báo 2 để yêu cầu ID thiết bị
S203. Thực hiện việc xác minh mã nhận dạng trên đầu cuối
S204. Tạo ra cặp khóa 2, trong đó cặp khóa 1 bao gồm khóa công cộng 2 và khóa riêng 2
S205. Gửi cặp khóa 2 và thông tin 1
S206. Gửi thông báo 2 và cặp khóa được mã hóa 2
S207. Nhận và lưu trữ cặp khóa 2
S208. Xác định rằng khóa công cộng 2 là ID thiết bị
S209. Gửi thông báo 2 được ký bằng cách sử dụng khóa riêng 2

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực công nghệ truyền thông, và đề cập đến phương pháp thu ký hiệu nhận dạng thiết bị và máy, và cụ thể là, đến phương pháp thu ký hiệu nhận dạng thiết bị của đầu cuối trong mạng lưới vạn vật kết nối Internet và máy.

Tình trạng kỹ thuật của sáng chế

Mạng lưới vạn vật kết nối Internet (Internet of things, IoT) là mạng kết nối đối tượng bất kỳ với internet theo giao thức thỏa thuận bằng cách sử dụng thiết bị thu thập thông tin như sự nhận dạng tần số vô tuyến (Radio Frequency Identification, RFID), bộ cảm biến, bộ cảm biến hồng ngoại, hệ thống định vị toàn cầu, hoặc máy quét laze, để trao đổi thông tin và thực hiện truyền thông, để thực thi việc nhận dạng thông minh, định vị, theo dõi, giám sát, và quản lý. Mạng lưới vạn vật kết nối Internet kết nối các đầu cuối khác nhau với chức năng gửi thông tin đến nền tảng mạng lưới vạn vật kết nối Internet bằng cách sử dụng mạng truyền thông di động.

Đầu cuối với chức năng gửi thông tin có thể còn được gọi là thiết bị đầu cuối, đầu cuối mạng lưới vạn vật kết nối Internet, hoặc thiết bị mạng lưới vạn vật kết nối Internet. Với sự phát triển mạnh mẽ của ngành công nghiệp mạng lưới vạn vật kết nối Internet, nhiều loại đầu cuối khác nhau trao đổi thông tin với mạng và ứng dụng bằng cách sử dụng kênh dữ liệu giao thức internet (Internet Protocol, IP) cố định hoặc di động. Vì vậy, các ký hiệu nhận dạng thiết bị cần được gán cho các đầu cuối, để giúp quản lý các đầu cuối.

Trong mạng thông thường, ký hiệu nhận dạng thiết bị của đầu cuối thường được tạo cấu hình trước. Chẳng hạn, đối với đầu cuối di động, thông tin nhận dạng người dùng được cung cấp bởi nhà điều hành cho đầu cuối và thông tin nhận dạng được ghi vào đầu cuối khi giao hàng được sử dụng để tính để tạo ra mã nhận dạng của đầu cuối để xác thực đầu cuối di động. Đối với đầu cuối nối dây, khóa truy nhập mạng được cung cấp bởi nhà điều hành và thông tin nhận dạng được ghi vào đầu cuối khi giao hàng được sử dụng để tạo ra mã nhận dạng. Các nhà cung cấp khác

nhau sử dụng các cách tạo cấu hình khác nhau, và các loại và đặc điểm của các ký hiệu nhận dạng được tạo cấu hình bởi các nhà cung cấp khác nhau cho đầu cuối có thể là khác nhau. Ngoài ra, các nhà cung cấp khác nhau có thể tạo cấu hình ký hiệu nhận dạng giống nhau cho các đầu cuối khác nhau. Vì vậy, việc quản lý thiết bị trong mạng lưới vạn vật kết nối Internet phức tạp ở một mức độ nào đó.

Để tạo cấu hình ký hiệu nhận dạng thiết bị duy nhất toàn cầu, theo giải pháp kỹ thuật đã biết, đầu cuối di động thường được nhận dạng duy nhất bằng cách sử dụng mã nhận dạng trang thiết bị di động quốc tế (international mobile equipment identify, IMEI) hoặc tương tự, nhưng cần phải đăng ký trước với cơ quan đăng ký. Do đó, quá trình tạo cấu hình tương đối phức tạp, các chi phí đăng ký cao, và hiệu quả quay vòng ký hiệu nhận dạng thấp.

Hơn nữa, do ký hiệu nhận dạng thiết bị được tạo ra theo cách đã nêu ở trên quá đơn giản, ký hiệu nhận dạng thiết bị này có thể bị đánh cắp, và dễ dàng giả mạo khi ký hiệu nhận dạng thiết bị bị đánh cắp hoặc xâm nhập bất hợp pháp.

Là bước quan trọng trong quản lý bảo mật, việc làm thế nào để thực hiện việc xác thực đáng tin cậy trên thiết bị và cách làm thế nào để tạo ra ký hiệu nhận dạng thiết bị duy nhất để tạo điều kiện quản lý, đơn giản hóa quá trình tạo cấu hình, và cải thiện tính bảo mật và tính khả dụng của sơ đồ thu ký hiệu nhận dạng thiết bị tổng thể trở thành các vấn đề cấp bách cần được giải quyết hiện tại.

Bản chất kỹ thuật của sáng chế

Theo quan điểm này, các phương án của sáng chế đề xuất phương tháp thu ID thiết bị, để tạo ra sơ đồ thu ID thiết bị tổng thể với tính bảo mật và tính khả dụng cao hơn.

Theo khía cạnh thứ nhất, phương án của sáng chế đề xuất phương tháp thu ID thiết bị. Phương pháp này gồm có các bước: đầu cuối gửi, đến thiết bị mạng, thông báo thứ nhất được sử dụng để yêu cầu ID thiết bị cho đầu cuối, trong đó ID thiết bị được sử dụng để nhận dạng toàn cầu đầu cuối theo cách duy nhất. Đầu cuối nhận cặp khóa được mã hóa được gửi bởi thiết bị mạng, trong đó cặp khóa này gồm có khóa công cộng thứ nhất và khóa riêng thứ nhất. Đầu cuối nhận thông tin được gửi bởi thiết bị mạng, trong đó thông tin này được sử dụng để nhận dạng rằng khóa công

cộng thứ nhất là ID thiết bị của đầu cuối. Đầu cuối xác định, dựa trên cặp khóa nhận được và thông tin nhận được, rằng khóa công cộng thứ nhất là ID thiết bị.

Cặp khóa được gửi bởi thiết bị mạng và được nhận bởi đầu cuối và thông tin được gửi bởi thiết bị mạng và được nhận bởi đầu cuối có thể được mang trong thông báo giống nhau, hoặc có thể được mang trong các thông báo khác nhau. Khi cặp khóa và thông tin được mang trong thông báo giống nhau, hoạt động (để dễ mô tả, được gọi tắt là hoạt động 1) mà đầu cuối nhận cặp khóa được mã hóa được gửi bởi thiết bị mạng và hoạt động (hoạt động 2) mà đầu cuối nhận thông tin được gửi bởi thiết bị mạng có thể được hiểu là được hoàn thành bởi hoạt động giống nhau. Khi cặp khóa và thông tin được mang trong các thông báo khác nhau, hoạt động 1 có thể được thực hiện trước, sau, hoặc đồng thời với hoạt động 2.

Theo giải pháp đã nêu ở trên, đầu cuối tạo ra yêu cầu thu ID thiết bị, và thiết bị mạng gửi cặp khóa đến đầu cuối dựa trên yêu cầu nhận được, và gửi thông tin đến đầu cuối để chỉ báo rằng khóa công cộng được chứa trong cặp khóa là ID thiết bị. Vì vậy, thiết bị mạng gán động ID thiết bị cho đầu cuối dựa trên yêu cầu của đầu cuối và không cần tạo cấu hình trước ID cho đầu cuối, và đầu cuối không cần đăng ký trước với cơ quan đăng ký. Điều này đơn giản hóa quá trình tạo cấu hình, giảm các chi phí đăng ký, và cải thiện hiệu quả quay vòng ID thiết bị do không cần tạo cấu hình trước ID thiết bị. Ngoài ra, khóa công cộng trong cặp khóa được sử dụng làm ID thiết bị, nên tính duy nhất của ID thiết bị được bảo đảm, và tránh được sự lặp lại ID thiết bị. Hơn nữa, ID thiết bị dựa trên khóa công cộng phức tạp hơn ID thiết bị hiện hành, nên giảm được khả năng ký hiệu nhận dạng thiết bị bị giả mạo do ký hiệu nhận dạng thiết bị quá đơn giản.

Trong thiết kế có thể, phương pháp này còn gồm có bước: Đầu cuối gửi, đến thiết bị mạng, thông báo thứ hai được ký bằng cách sử dụng khóa riêng thứ nhất, trong đó thông báo thứ hai này mang khóa công cộng thứ nhất được sử dụng làm ID thiết bị của đầu cuối.

Trong thiết kế có thể, thông báo thứ nhất mang khóa công cộng thứ hai, và khóa công cộng thứ hai là khóa công cộng được tạo ra bởi đầu cuối dựa trên chức năng không thể có bản sao vật lý.

Trong thiết kế có thể, bước đầu cuối nhận cặp khóa được mã hóa được gửi bởi

thiết bị mạng gồm có bước: Đầu cuối nhận cặp khóa được gửi bởi thiết bị mạng và được mã hóa bằng cách sử dụng khóa công cộng thứ hai. Sau khi nhận cặp khóa được gửi bởi thiết bị mạng và được mã hóa bằng cách sử dụng khóa công cộng thứ hai, đầu cuối có thể thực hiện giải mã chỉ bằng cách sử dụng khóa riêng thứ hai tương ứng với khóa công cộng thứ hai. Do khóa công cộng thứ hai và khóa riêng thứ hai là các khóa được tạo ra bởi đầu cuối dựa trên PUF, và chỉ đầu cuối lưu trữ khóa riêng thứ hai, nên khó giả mạo khóa riêng thứ hai, và tính bảo mật truyền của cặp khóa có thể được cải thiện một cách hiệu quả.

Trong thiết kế có thể, sau khi đầu cuối nhận cặp khóa được mã hóa được gửi bởi thiết bị mạng, phương pháp này còn gồm có bước: Đầu cuối lưu trữ khóa riêng thứ nhất, và mã hóa khóa riêng thứ nhất đã lưu trữ bằng cách sử dụng khóa công cộng thứ hai. Khóa riêng thứ nhất đã lưu trữ được mã hóa bằng cách sử dụng khóa công cộng thứ hai, và có thể được giải mã chỉ bằng cách sử dụng khóa riêng thứ hai tương ứng với khóa công cộng thứ hai. Do khóa công cộng thứ hai và khóa riêng thứ hai được tạo ra dựa trên PUF, và chỉ đầu cuối có khóa riêng thứ hai, nên khó giả mạo khóa riêng thứ hai, và tính bảo mật lưu trữ của khóa riêng thứ nhất có thể được bảo đảm một cách hiệu quả.

Trong thiết kế có thể, thông báo thứ nhất mang chứng nhận khóa công cộng được phát hành bởi cơ sở chứng nhận (certificate authority, CA), và chứng nhận khóa công cộng này mang khóa công cộng thứ hai. CA phát hành chứng nhận, nên khóa công cộng thứ hai không cần được triển khai trước trong thiết bị mạng. Điều này đơn giản hóa quá trình tạo cấu hình.

Theo khía cạnh thứ hai, sáng chế đề xuất phương tháp thu ID thiết bị. Phương pháp này gồm có các bước: thiết bị mạng thứ nhất nhận thông báo thứ nhất được gửi bởi đầu cuối và được sử dụng để yêu cầu ID thiết bị cho đầu cuối, trong đó ID thiết bị được sử dụng để nhận dạng toàn cầu đầu cuối theo cách duy nhất. Thiết bị mạng thứ nhất gửi cặp khóa được mã hóa đến đầu cuối, trong đó cặp khóa này gồm có khóa công cộng thứ nhất và khóa riêng thứ nhất. Thiết bị mạng thứ nhất gửi thông tin thứ nhất đến đầu cuối, trong đó thông tin thứ nhất được sử dụng để nhận dạng rằng khóa công cộng thứ nhất là ID thiết bị của đầu cuối. Đối với các hiệu quả kỹ thuật của phương pháp được đề xuất theo khía cạnh thứ hai, tham khảo các phần mô tả theo

khía cạnh thứ nhất. Các chi tiết không được mô tả lại ở đây.

Cặp khóa được gửi bởi thiết bị mạng đến đầu cuối và thông tin được gửi bởi thiết bị mạng đến đầu cuối có thể được mang trong thông báo giống nhau, hoặc có thể được mang trong các thông báo khác nhau. Khi cặp khóa và thông tin được mang trong thông báo giống nhau, hoạt động (để dễ mô tả, được gọi tắt là hoạt động 1) mà thiết bị mạng thứ nhất gửi cặp khóa được mã hóa đến đầu cuối và hoạt động (hoạt động 2) mà thiết bị mạng thứ nhất gửi thông tin thứ nhất đến đầu cuối có thể được hiểu là được hoàn thành bởi hoạt động giống nhau. Khi cặp khóa và thông tin được mang trong các thông báo khác nhau, hoạt động 1 có thể được thực hiện trước, sau, hoặc đồng thời với hoạt động 2.

Trong thiết kế có thể, hệ thống quản lý thiết bị được triển khai trong thiết bị mạng thứ nhất, và thiết bị mạng thứ nhất nhận thông báo thứ hai được gửi bởi đầu cuối và được ký bằng cách sử dụng khóa riêng thứ nhất, trong đó thông báo thứ hai mang khóa công cộng thứ nhất được sử dụng làm ID thiết bị của đầu cuối. Thông báo thứ hai có thể được sử dụng để báo cáo ID thiết bị, nghĩa là, thông tin như khóa công cộng thứ nhất, thông tin trạng thái thiết bị, thông tin vị trí thiết bị, và/hoặc loại thiết bị, cho hệ thống quản lý thiết bị được triển khai trong thiết bị mạng thứ nhất. Cụ thể là, hoạt động cần được thực hiện bằng cách sử dụng thông báo thứ hai có thể được nhận dạng bằng cách sử dụng loại thông báo trong thông báo thứ hai hoặc bit tương ứng trong thông báo thứ hai. Thông báo thứ hai có thể mang khóa công cộng thứ nhất được sử dụng làm ID thiết bị. Sau khi nhận thông báo thứ hai, thiết bị mạng thứ nhất có thể xác minh chữ ký bằng cách sử dụng khóa công cộng thứ nhất, để thực hiện tiếp việc xác minh mã nhận dạng trên đầu cuối. Vì vậy, theo giải pháp đã nêu ở trên, thiết bị mạng trả lại cặp khóa đến đầu cuối dựa trên yêu cầu dùng để thu ID thiết bị và được gửi bởi đầu cuối. Đầu cuối sử dụng khóa công cộng trong cặp khóa làm ID thiết bị, và ký gói cần được gửi bằng cách sử dụng khóa riêng trong cặp khóa, để thực hiện việc xác minh mã nhận dạng trên đầu cuối. Vì vậy, không cần tạo cấu hình lại ủy nhiệm xác thực mới, và trong kịch bản với nhiều đầu cuối trong mạng lưới vạn vật kết nối Internet, quá trình tạo cấu hình được đơn giản hóa một cách hiệu quả, và các mức bổ sung hệ thống được giảm xuống.

Trong thiết kế có thể, hệ thống quản lý thiết bị được triển khai trong thiết bị

mạng thứ nhất, và hệ thống quản lý ID được triển khai trong thiết bị mạng thứ hai. Sau khi thiết bị mạng thứ nhất nhận thông báo thứ nhất, và trước khi thiết bị mạng thứ nhất gửi cặp khóa được mã hóa đến đầu cuối, phương pháp này còn gồm có các bước: Thiết bị mạng thứ nhất gửi thông báo thứ ba đến thiết bị mạng thứ hai, trong đó thông báo thứ ba được sử dụng để yêu cầu ID thiết bị cho đầu cuối. Thiết bị mạng thứ nhất nhận cặp khóa và thông tin thứ hai được trả lại bởi thiết bị mạng thứ hai, trong đó thông tin thứ hai được sử dụng để chỉ báo rằng khóa công cộng thứ nhất được chứa trong cặp khóa là ID thiết bị.

Trong thiết kế có thể, hệ thống quản lý ID được triển khai trong thiết bị mạng thứ nhất. Sau khi nhận thông báo thứ nhất mang khóa công cộng thứ hai, thiết bị mạng thứ nhất thực hiện việc xác minh mã nhận dạng trên đầu cuối dựa trên khóa công cộng thứ hai và khóa công cộng thứ hai được lưu trữ trong thiết bị mạng thứ nhất.

Trong thiết kế có thể, thông báo thứ nhất mang khóa công cộng thứ hai, và khóa công cộng thứ hai là khóa công cộng được tạo ra bởi đầu cuối dựa trên chức năng không thể có bản sao vật lý (physical unclonable function, PUF).

Trong thiết kế tùy chọn, thông báo thứ ba mang khóa công cộng thứ hai, và thiết bị mạng thứ hai thực hiện việc xác minh mã nhận dạng trên đầu cuối dựa trên khóa công cộng thứ hai được mang trong thông báo thứ ba. Cụ thể là, sau khi nhận thông báo thứ nhất mang khóa công cộng thứ hai, thiết bị mạng thứ nhất thu khóa công cộng thứ hai dựa trên thông báo thứ nhất, tạo ra thông báo thứ ba mang khóa công cộng thứ hai, và gửi thông báo thứ ba đến thiết bị mạng thứ hai. Thiết bị mạng thứ hai thực hiện việc xác minh mã nhận dạng trên đầu cuối dựa trên khóa công cộng thứ hai được mang trong thông báo thứ ba và khóa công cộng thứ hai được lưu trữ trong thiết bị mạng thứ hai. Nếu xác định rằng đầu cuối thành công trong việc xác minh mã nhận dạng, thiết bị mạng thứ hai tạo ra cặp khóa và thông tin thứ hai, và gửi cặp khóa và thông tin thứ hai đến thiết bị mạng thứ nhất. Nếu xác định rằng khóa công cộng thứ hai được mang trong thông báo thứ ba giống như khóa công cộng thứ hai được lưu trữ trong thiết bị mạng thứ hai, thiết bị mạng thứ hai xác định rằng đầu cuối thành công trong việc xác minh mã nhận dạng.

Việc xác minh mã nhận dạng được thực hiện trên các đầu cuối, nên hệ thống

quản lý ID chỉ gán ID thiết bị cho đầu cuối mà thành công trong việc xác minh mã nhận dạng. Điều này giúp tránh một cách hiệu quả việc tiêu thụ tài nguyên gây ra khi đầu cuối không đáng tin cậy áp dụng vào hệ thống quản lý ID đối với ID thiết bị.

Trong thiết kế có thể, bước thiết bị mạng thứ nhất gửi cặp khóa được mã hóa đến đầu cuối gồm có: Thiết bị mạng thứ nhất gửi, đến đầu cuối, cặp khóa được mã hóa bằng cách sử dụng khóa công cộng thứ hai. Sau khi nhận cặp khóa được gửi bởi thiết bị mạng và được mã hóa bằng cách sử dụng khóa công cộng thứ hai, đầu cuối có thể thực hiện giải mã chỉ bằng cách sử dụng khóa riêng thứ hai tương ứng với khóa công cộng thứ hai. Do khóa công cộng thứ hai và khóa riêng thứ hai là các khóa được tạo ra bởi đầu cuối dựa trên PUF, và chỉ đầu cuối lưu trữ khóa riêng thứ hai, nên khó giả mạo khóa riêng thứ hai, và tính bảo mật truyền của cặp khóa có thể được cải thiện một cách hiệu quả.

Trong thiết kế có thể, thông báo thứ nhất mang chứng nhận khóa công cộng được phát hành bởi cơ sở chứng nhận CA, và chứng nhận khóa công cộng này mang khóa công cộng thứ hai. CA phát hành chứng nhận, nên khóa công cộng thứ hai không cần được triển khai trong thiết bị mạng trước. Điều này đơn giản hóa quá trình tạo cấu hình.

Theo khía cạnh thứ ba, phương án của sáng chế đề xuất đầu cuối, được tạo cấu hình để thực hiện phương pháp theo khía cạnh thứ nhất hoặc thiết kế có thể bất kỳ của khía cạnh thứ nhất. Cụ thể là, đầu cuối gồm có các môđun được tạo cấu hình để thực hiện phương pháp theo khía cạnh thứ nhất hoặc biện pháp thực thi có thể bất kỳ của khía cạnh thứ nhất.

Theo khía cạnh thứ tư, phương án của sáng chế đề xuất thiết bị mạng, được tạo cấu hình để thực hiện phương pháp theo khía cạnh thứ hai hoặc thiết kế có thể bất kỳ của khía cạnh thứ hai. Cụ thể là, thiết bị mạng gồm có các môđun được tạo cấu hình để thực hiện phương pháp theo khía cạnh thứ hai hoặc biện pháp thực thi có thể bất kỳ của khía cạnh thứ hai.

Theo khía cạnh thứ năm, phương án của sáng chế đề xuất đầu cuối, gồm có bộ thu phát, bộ xử lý, và bộ nhớ. Bộ thu phát, bộ xử lý, và bộ nhớ có thể được kết nối bằng cách sử dụng hệ thống bus. Bộ nhớ được tạo cấu hình để lưu trữ chương trình, lệnh, hoặc mã. Bộ xử lý được tạo cấu hình để thi hành chương trình, lệnh, hoặc

mã trong bộ nhớ, để hoàn thành hoạt động ngoài nhận và gửi thông tin được thực hiện bởi đầu cuối trong phương pháp theo khía cạnh thứ nhất hoặc thiết kế có thể bất kỳ của khía cạnh thứ nhất.

Theo khía cạnh thứ sáu, phương án của sáng chế đề xuất thiết bị mạng, gồm có bộ thu phát, bộ xử lý, và bộ nhớ. Bộ thu phát, bộ xử lý, và bộ nhớ có thể được kết nối bằng cách sử dụng hệ thống bus. Bộ nhớ được tạo cấu hình để lưu trữ chương trình, lệnh, hoặc mã. Bộ xử lý được tạo cấu hình để thi hành chương trình, lệnh, hoặc mã trong bộ nhớ, để hoàn thành hoạt động ngoài nhận và gửi thông tin được thực hiện bởi thiết bị mạng trong phương pháp theo khía cạnh thứ hai hoặc thiết kế có thể bất kỳ của khía cạnh thứ hai.

Theo khía cạnh thứ bay, phương án của sáng chế đề xuất hệ thống truyền thông, gồm có đầu cuối được đề xuất theo khía cạnh thứ ba hoặc khía cạnh thứ năm và thiết bị mạng được đề xuất theo khía cạnh thứ tư hoặc khía cạnh thứ sáu.

Theo khía cạnh thứ tám, 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 lệnh, và khi lệnh được chạy trên máy tính, máy tính được kích hoạt để thực hiện phương pháp theo khía cạnh thứ nhất hoặc biện pháp thực thi có thể bất kỳ của khía cạnh thứ nhất hoặc phương pháp theo khía cạnh thứ hai hoặc biện pháp thực thi có thể bất kỳ của khía cạnh thứ hai.

Theo phương pháp, đầu cuối, thiết bị mạng, và hệ thống được đề xuất theo các phương án của sáng chế, cặp khóa được tạo ra, và khóa công cộng trong cặp khóa được sử dụng làm ID thiết bị, nên tính duy nhất của ID thiết bị có thể được bảo đảm một cách hiệu quả, và đặc biệt là trong kịch bản với nhiều thiết bị mạng lưới vạn vật kết nối Internet, có thể tránh được một cách hiệu quả vấn đề khó quản lý do sự lặp lại ID thiết bị. Hơn nữa, thông tin được gửi bởi đầu cuối được ký bằng cách sử dụng khóa riêng trong cặp khóa, nên không cần tạo cấu hình trước ủy nhiệm xác thực hoặc dàn xếp khóa bổ sung trong khi truyền thông. Vì vậy, trong kịch bản với nhiều đầu cuối, các mức bổ sung cần phải có để tạo cấu hình ủy nhiệm xác thực và dàn xếp khóa được giảm đáng kể, quá trình tạo cấu hình được đơn giản hóa đáng kể, và hiệu quả xử lý được cải thiện.

Mô tả vắn tắt các hình vẽ

Fig.1 là sơ đồ kiến trúc giản lược của hệ thống mạng lưới vạn vật kết nối Internet theo phương án của sáng chế;

Fig.2 là lưu đồ giản lược của phương tháp thu ID thiết bị theo phương án của sáng chế;

Fig.3 là lưu đồ giản lược của phương tháp thu ID thiết bị theo phương án của sáng chế;

Fig.4 là lưu đồ giản lược của phương pháp đăng ký đầu cuối theo phương án của sáng chế;

Fig.5 là lưu đồ giản lược của phương pháp đăng ký đầu cuối theo phương án của sáng chế;

Fig.6 là lưu đồ giản lược của phương tháp thu ID thiết bị theo phương án của sáng chế;

Fig.7 là lưu đồ giản lược của phương tháp thu ID thiết bị theo phương án của sáng chế;

Fig.8 là lưu đồ giản lược của phương tháp thu ID thiết bị theo phương án của sáng chế;

Fig.9 là sơ đồ cấu trúc giản lược của đầu cuối theo phương án của sáng chế; và

Fig.10 là sơ đồ cấu trúc giản lược của thiết bị mạng theo phương án của sáng chế.

Mô tả chi tiết sáng chế

Kịch bản ứng dụng được mô tả theo các phương án của sáng chế nhằm mục đích mô tả rõ ràng hơn các giải pháp kỹ thuật theo các phương án của sáng chế, nhưng không được dự định để chỉ báo rằng các giải pháp kỹ thuật được đề xuất theo các phương án của sáng chế có thể bị giới hạn chỉ ở tình uống ứng dụng này. Người có kỹ năng trong lĩnh vực này có thể hiểu rằng với sự phát triển của các kiến trúc mạng và sự xuất hiện của các kịch bản dịch vụ mới, các giải pháp kỹ thuật được đề xuất theo các phương án của sáng chế cũng có thể áp dụng cho vấn đề kỹ thuật tương tự.

Trừ khi có quy định khác, các số thứ tự như "1", "2", "3", "thứ nhất", "thứ hai", và "thứ ba" được đề cập trong sáng chế được sử dụng để phân biệt giữa nhiều đối tượng, nhưng không được sử dụng để giới hạn trình tự của nhiều đối tượng.

"A và/hoặc B" được đề cập trong sáng chế nên được hiểu là trường hợp sau đây: chỉ gồm có A, chỉ gồm có B, hoặc gồm có cả A và B.

Phần sau đây mô tả ngắn gọn một số thuật ngữ trong sáng chế, để tạo điều kiện cho sự hiểu biết của người có kỹ năng trong lĩnh vực này.

"PUF" được mô tả trong sáng chế là chức năng không thể có bản sao vật lý (physical unclonable function, PUF), và là công nghệ nhận dạng "dấu hiệu sinh học" trong lĩnh vực chip. Trong quá trình sản xuất chip, ngay cả nếu hai chip có thiết kế giống nhau hoặc ngay cả quá trình sản xuất giống nhau, các thuộc tính vật lý của hai chip vẫn khác nhau. Trên quy mô phân tử, luôn luôn có các biến không thể tránh khỏi và không thể kiểm soát được khiến mỗi chíp trở nên duy nhất. Các biến này hoàn toàn ngẫu nhiên và không thể loại bỏ được. Ngay cả trên dây chuyền sản xuất tiên tiến nhất, vẫn có sự khác biệt về cấu trúc bên trong giữa các chip trên lát giống nhau. Các khóa hoàn toàn ngẫu nhiên được tạo ra bằng cách tách ra các biến trong quá trình sản xuất chip dựa trên PUF. Các khóa này không thể được phỏng đoán hoặc lập lịch biểu, tồn tại vĩnh viễn, và không thể bị bắt chước ngay cả bởi các nhà sản xuất chip. Thuật toán tạo khóa dựa trên PUF có thể là thuật toán hiện hành như thuật toán Rivest-Shamir-Adelman (Rivest-Shamir-Adelman, RSA) hoặc thuật toán chữ ký số (digital signature algorithm, DSA). Các chi tiết không được mô tả trong sáng chế.

"Đầu cuối" trong sáng chế có thể là thiết bị được giữ, được quản lý, hoặc được sử dụng bởi nhà điều hành hoặc nhà cung cấp dịch vụ nội dung, hoặc có thể là đầu cuối người dùng thông thường. "Đầu cuối" có thể còn được gọi là thiết bị đầu cuối, thiết bị mạng, nút, hoặc thiết bị nút. Khi được áp dụng cho mạng lưới vạn vật kết nối Internet, đầu cuối có thể còn được gọi là nút mạng mạng lưới vạn vật kết nối Internet, đầu cuối mạng lưới vạn vật kết nối Internet, thiết bị đầu cuối, thiết bị mạng lưới vạn vật kết nối Internet, thiết bị nút mạng lưới vạn vật kết nối Internet, hoặc thiết bị đầu cuối mạng lưới vạn vật kết nối Internet. Tóm lại là, thiết bị bất kỳ với chức năng gửi thông tin có thể được gọi là đầu cuối. Đầu cuối có thể là thiết bị như máy điện thoại di động (hoặc được gọi là máy điện thoại "chia ô"), máy điện thoại dịch vụ truyền

thông cá nhân (Personal Communication Service, PCS), máy điện thoại không dây, bộ máy điện thoại giao thức khởi tạo phiên (Session Initiation Protocol, SIP), trạm vòng cục bộ không dây (Wireless Local Loop, a WLL), hoặc thiết bị trợ giúp số cá nhân (Personal Digital Assistant, PDA). Theo cách khác, đầu cuối có thể là, chẳng hạn, các thiết bị mạng khác, mà có thể còn được gọi là các thiết bị mạng truy nhập, chẳng hạn, gNB (gNodeB), trạm cơ sở thông thường (chẳng hạn, nút B (NodeB, NB) trong hệ thống WCDMA, nút B cải tiến (Evolved NodeB, eNB hoặc eNodeB) trong hệ thống LTE, hoặc trạm thu phát cơ sở (Base Transceiver Station, BTS) trong GSM hoặc CDMA), bộ điều khiển vô tuyến mới (New Radio controller, NR controller), phần tử mạng tập trung, trạm cơ sở vô tuyến mới, bộ phận vô tuyến từ xa, thực thể quản lý tính di động (mobile management entity, MME), trạm cơ sở cỡ nhỏ, phần tử mạng phân tán (Distributed Unit), điểm thu phát (Transmission Reception Point, TRP) hoặc điểm phát (Transmission Point, TP), và bộ điều khiển vô tuyến trong kịch bản mạng truy nhập vô tuyến đám mây (Cloud Radio Access Network, CRAN). Theo cách khác, thiết bị mạng có thể là trạm chuyển tiếp, điểm truy nhập, thiết bị lắp đặt trên phương tiện giao thông, hoặc thiết bị mạng hoặc thiết bị truy nhập khác bất kỳ trong mạng tương lai. Tuy nhiên, các phương án của sáng chế không bị giới hạn ở đó. Theo cách khác, đầu cuối có thể là cổng nối dùng trong gia đình, thiết bị đeo được thông minh (chẳng hạn, đồng hồ thông minh, băng thông minh, kính thông minh, ống choàng đầu thông minh, mũ bảo hiểm thông minh, vòng thông minh, giày thông minh, hoặc vòng cổ thông minh), các thiết bị điện gia dụng khác (chẳng hạn, tủ lạnh, máy giặt, vô tuyến, thiết bị đun nước, nồi cơm điện, lò vi sóng, lò nướng, máy nướng bánh mì, khoang tắm đứng, máy lọc không khí, máy hút ẩm, và loa), các phương tiện vận tải khác (chẳng hạn, xe ôtô, máy bay, tàu điện, thuyền, xe đạp, và xe gắn máy), các khí cụ và máy đo khác, các thiết bị mạng khác (chẳng hạn, bộ định tuyến, bộ chuyển mạch, máy chủ, bức tường lửa, và bộ điều khiển), hoặc tương tự. Sáng chế không bị giới hạn ở đó, và không thể cung cấp sự liệt kê thấu đáo. Vì vậy, các chi tiết không được mô tả.

"Nền tảng mạng lưới vạn vật kết nối Internet" được mô tả trong sáng chế là khái niệm tương đối rộng, có thể thực hiện các hoạt động như tích hợp, phân loại, phân tích, và phản hồi trên thông tin dữ liệu được thu thập bởi đầu cuối mạng lưới

vạn vật kết nối Internet, và chủ yếu thực hiện quản lý trên nhiều đầu cuối, quản lý dữ liệu, quản lý hoạt động, và quản lý bảo mật. Nền tảng mạng lưới vạn vật kết nối Internet tích hợp nhiều công nghệ tiên tiến, gồm có điện toán đám mây, dữ liệu lớn, trí thông minh nhân tạo, và tương tự, để đáp ứng các nhu cầu để thực hiện truyền thông tin và trao đổi trên mạng lưới vạn vật kết nối Internet. Nền tảng mạng lưới vạn vật kết nối Internet có thể gồm có nhiều nền tảng xử lý với các chức năng khác nhau, và chịu trách nhiệm tách ra dữ liệu được sử dụng để điều khiển và ra quyết định từ dữ liệu nhận thức dựa trên yêu cầu ứng dụng, và chuyển đổi dữ liệu thành các định dạng khác để dùng chung trong nhiều hệ thống ứng dụng. Trong ứng dụng thực tế, nền tảng mạng lưới vạn vật kết nối Internet có thể gồm có một hoặc nhiều thiết bị. Theo loại, nền tảng mạng lưới vạn vật kết nối Internet có thể được phân chia thành bốn loại nền tảng từ dưới lên trên: nền tảng quản lý đầu cuối, nền tảng quản lý kết nối, nền tảng phát triển ứng dụng, và nền tảng phân tích dịch vụ. Nền tảng quản lý đầu cuối chủ yếu chịu trách nhiệm thực hiện quản lý đăng ký, nhận dạng mã nhận dạng, điều khiển truy nhập, tạo cấu hình, giám sát, hỏi, nâng cấp hệ thống, xử lý sự cố, quản lý chu kỳ đời sống, và tương tự trên đầu cuối mạng lưới vạn vật kết nối Internet. Nền tảng quản lý kết nối chủ yếu chịu trách nhiệm thực hiện tạo cấu hình và quản lý sai hỏng, quản lý sử dụng tài nguyên mạng, quản lý tài nguyên kết nối, thay đổi gói, quản lý tài nguyên số/địa chỉ IP/MAC, và tương tự trên kết nối mạng lưới vạn vật kết nối Internet. Nền tảng phát triển ứng dụng có thể cung cấp nền tảng làm dịch vụ (platform as a service, Paas) là nền tảng được sử dụng để phát triển ứng dụng và lưu trữ dữ liệu hợp nhất, và cung cấp công cụ phát triển ứng dụng, phần sụn, lưu trữ dữ liệu, máy logic dịch vụ, giao diện nền tảng ứng dụng (application platform interface, API) để kết nối với bên thứ ba, và tương tự. Nền tảng phân tích dịch vụ chủ yếu được tạo cấu hình để xếp loại và phân tích dữ liệu dịch vụ, và cung cấp kết quả phân tích dữ liệu trực quan. Nền tảng phân tích dịch vụ giám sát trạng thái thiết bị và đưa ra cảnh báo nhờ phép phân tích động học thời gian thực, hoặc phân tích và dự đoán dịch vụ nhờ việc học của máy.

"Thiết bị mạng" được mô tả trong sáng chế được sử dụng để chỉ báo phần cứng bất kỳ có thể nhận và gửi thông tin và có thể xử lý thông tin trong quá trình trao đổi thông tin. Chẳng hạn, thiết bị mạng có thể là máy tính cá nhân, máy chủ, bộ định

tuyến, hoặc bộ chuyển mạch. Khi được áp dụng cho nền tảng mạng lưới vạn vật kết nối Internet, thiết bị mạng có thể được tạo cấu hình để thực hiện một số hoặc tất cả các chức năng của nền tảng quản lý đầu cuối, nền tảng quản lý kết nối, nền tảng phát triển ứng dụng, và/hoặc nền tảng phân tích dịch vụ. Hệ thống quản lý thiết bị và/hoặc hệ thống quản lý ký hiệu nhận dạng (identifier, ID) có thể được triển khai trong thiết bị mạng.

"Hệ thống quản lý thiết bị" được mô tả trong sáng chế được triển khai trong nền tảng mạng lưới vạn vật kết nối Internet, chẳng hạn, có thể được triển khai trong nền tảng quản lý đầu cuối đã nêu ở trên. "Hệ thống quản lý thiết bị" là hệ thống quản lý thiết bị tập trung, và chủ yếu được tạo cấu hình để quản lý (chẳng hạn, tạo cấu hình, hỏi, và giám sát) tất cả các thiết bị (chẳng hạn, các đầu cuối) và thông tin dịch vụ liên quan của các thiết bị. Hệ thống quản lý thiết bị có thể được triển khai trong một hoặc nhiều thiết bị mạng.

"Hệ thống quản lý ID" được mô tả trong sáng chế được triển khai trong nền tảng mạng lưới vạn vật kết nối Internet, chẳng hạn, có thể được triển khai trong nền tảng quản lý đầu cuối đã nêu ở trên. "Hệ thống quản lý ID" có thể là, chẳng hạn, hệ thống mã nhận dạng làm dịch vụ (Identity as a service, IDaas), và được tạo cấu hình để quản lý thông tin ID thiết bị của thiết bị (chẳng hạn, đầu cuối), chẳng hạn, tạo lập, tạo cấu hình, xác minh, khởi động, và hỏi ID thiết bị. Hệ thống quản lý ID có thể được triển khai trong một hoặc nhiều thiết bị mạng.

Cả hệ thống quản lý ID và hệ thống quản lý thiết bị có thể được triển khai trong thiết bị mạng giống nhau, hoặc có thể được triển khai riêng rẽ trong các thiết bị mạng khác nhau. Điều này không bị giới hạn cụ thể theo các phương án của sáng chế.

"IDaas" được mô tả trong sáng chế có thể được gọi là mã nhận dạng làm dịch vụ, hoặc có thể được gọi là quản lý mã nhận dạng và truy nhập làm dịch vụ, và sử dụng cơ sở hạ tầng điện toán đám mây để quản lý mã nhận dạng và truy nhập của người dùng một cách an toàn.

"Khóa công cộng duy nhất toàn cầu" được mô tả trong sáng chế có nghĩa là khóa công cộng được tạo ra bởi đầu cuối bất kỳ khác biệt với khóa công cộng được tạo ra bởi đầu cuối khác trong mạng hoặc hệ thống gồm có nhiều đầu cuối. Nói cách

khác, không xảy ra sự lặp lại. Chẳng hạn, đầu cuối 1 tạo ra khóa công cộng 1, và đầu cuối khác như đầu cuối 2 không thể tạo ra, dựa trên thuật toán giống nhau hoặc các thuật toán khác nhau, khóa công cộng giống như khóa công cộng 1.

"Ký hiệu nhận dạng duy nhất toàn cầu" được mô tả trong sáng chế có nghĩa là ID thiết bị của đầu cuối bất kỳ khác biệt với ID thiết bị của đầu cuối khác trong mạng hoặc hệ thống gồm có nhiều đầu cuối. Nói cách khác, không xảy ra sự lặp lại.

Trong sáng chế, "khóa công cộng" có thể còn được gọi là "public key", và "khóa riêng" có thể còn được gọi là "private key". Khóa công cộng và khóa riêng là cặp khóa thu được bằng cách sử dụng thuật toán cụ thể. Nói cách khác, cặp khóa gồm có khóa công cộng và khóa riêng. Khóa công cộng là phần công cộng trong cặp khóa, và khóa riêng là phần riêng trong cặp khóa. Trong sáng chế, "khóa công cộng và khóa riêng tương ứng với khóa công cộng" (hoặc sự mô tả tương tự) chỉ báo rằng khóa riêng và khóa công cộng này tạo thành cặp khóa. Tương tự, "khóa riêng và khóa công cộng tương ứng với khóa riêng" (hoặc sự mô tả tương tự) cũng chỉ báo rằng khóa riêng và khóa công cộng này tạo thành cặp khóa.

Fig.1 là sơ đồ giản lược của kiến trúc hệ thống của hệ thống mạng lưới vạn vật kết nối Internet theo phương án của sáng chế. Hệ thống mạng lưới vạn vật kết nối Internet gồm có nhiều đầu cuối 101 và nền tảng mạng lưới vạn vật kết nối Internet 102 được kết nối truyền thông với nhiều đầu cuối 101. Nền tảng mạng lưới vạn vật kết nối Internet 102 gồm có nền tảng quản lý đầu cuối 103, nền tảng quản lý kết nối 104, nền tảng phát triển ứng dụng 105, và nền tảng phân tích dịch vụ 106. Ít nhất một thiết bị mạng được triển khai trong nền tảng quản lý đầu cuối 103. Chỉ hai thiết bị mạng (thiết bị mạng 107 và thiết bị mạng 108) được sử dụng làm ví dụ để mô tả trên Fig.1. Điều này không tạo ra giới hạn lên sáng chế. Hệ thống quản lý thiết bị và hệ thống quản lý ID có thể được triển khai trong thiết bị mạng được triển khai trong nền tảng quản lý đầu cuối 103. Hệ thống quản lý thiết bị được tạo cấu hình để: quản lý các đầu cuối với nhau, tạo cấu hình các đầu cuối, và kiểm tra và giám sát trạng thái đầu cuối và trạng thái dịch vụ. Hệ thống quản lý ID được tạo cấu hình để tạo ra, cập nhật, xóa, và/hoặc xác minh ID thiết bị của đầu cuối. Hệ thống quản lý thiết bị và hệ thống quản lý ID có thể được triển khai trong thiết bị mạng giống nhau như thiết bị mạng 107. Các chức năng tương ứng của hệ thống quản lý thiết bị và hệ thống quản

lý ID có thể được hoàn thành bởi các chip khác nhau, hoặc hệ thống quản lý thiết bị và hệ thống quản lý ID có thể là hai quá trình trên chip giống nhau. Hệ thống quản lý thiết bị và hệ thống quản lý ID có thể được triển khai theo cách khác trong các thiết bị mạng khác nhau. Chẳng hạn, hệ thống quản lý thiết bị được triển khai trong thiết bị mạng 107, và hệ thống quản lý ID được triển khai trong thiết bị mạng 108. Điều này không bị giới hạn cụ thể trong sáng chế. Hệ thống mạng lưới vạn vật kết nối Internet có thể còn gồm có cơ sở chứng nhận (certification authority, CA) 109. CA là cơ sở chịu trách nhiệm phát hành chứng nhận, xác thực chứng nhận, và quản lý chứng nhận đã phát hành. Chẳng hạn, CA phát hành chứng nhận số cho mỗi đầu cuối sử dụng khóa công cộng. Chứng nhận số được sử dụng để chứng minh rằng người dùng được liệt kê trong chứng nhận sở hữu hợp pháp khóa công cộng được liệt kê trong chứng nhận. Cần lưu ý rằng Fig.1 đơn thuần là sơ đồ giản lược, và sự tương tác giữa nền tảng mạng lưới vạn vật kết nối Internet và mỗi trong số nhiều đầu cuối đơn thuần được sử dụng làm ví dụ để mô tả, và không tạo thành giới hạn lên kịch bản ứng dụng của sáng chế. Hệ thống mạng lưới vạn vật kết nối Internet có thể gồm có đầu cuối khác. Các chức năng của nền tảng quản lý đầu cuối 103, nền tảng quản lý kết nối 104, nền tảng phát triển ứng dụng 105, và nền tảng phân tích dịch vụ 106 có thể được thực hiện một cách riêng rẽ bởi các thiết bị mạng khác nhau. Theo cách khác, tất cả các chức năng của bốn nền tảng này có thể được thực hiện bởi một thiết bị mạng. Theo cách khác, một số chức năng của bốn nền tảng này có thể được thực hiện bởi một thiết bị mạng, và các chức năng khác được thực hiện bởi một hoặc nhiều thiết bị mạng khác. Điều này không bị giới hạn cụ thể trong sáng chế. Số lượng của các đầu cuối và số lượng của các thiết bị mạng không bị giới hạn trong phương án này của sáng chế. Chẳng hạn, khi có nhiều thiết bị mạng, mỗi thiết bị mạng có thể quản lý một hoặc nhiều đầu cuối, hoặc nhiều thiết bị mạng có thể quản lý chung một hoặc nhiều đầu cuối.

Mặc dù mạng lưới vạn vật kết nối Internet được sử dụng làm ví dụ trong sáng chế để mô tả kịch bản ứng dụng của sáng chế, người có kỹ năng trong lĩnh vực này có thể hiểu được rằng các giải pháp kỹ thuật của sáng chế có thể áp dụng được cho nhiều kịch bản mạng khác. Điều này không bị giới hạn cụ thể trong sáng chế.

Fig.2 là lưu đồ giản lược của phương tháp thu ID thiết bị 200 theo phương án

của sáng chế. Kiến trúc mạng mà phương pháp 200 được áp dụng gồm có ít nhất đầu cuối, thiết bị mạng 1, và thiết bị mạng 2. Chẳng hạn, đầu cuối có thể là đầu cuối 101 trong kiến trúc mạng được thể hiện trên Fig.1, thiết bị mạng 1 có thể là thiết bị mạng 108 ở trong kiến trúc mạng được thể hiện trên Fig.1 và trong đó hệ thống quản lý thiết bị được triển khai, và thiết bị mạng 2 có thể là thiết bị mạng 107 ở trong kiến trúc mạng được thể hiện trên Fig.1 và trong đó hệ thống quản lý ID được triển khai. Hệ thống quản lý ID có thể là, chẳng hạn, hệ thống IDaas. Kiến trúc mạng có thể là kiến trúc mạng được thể hiện trên Fig.1. Phương pháp 200 gồm có các hoạt động sau đây.

S201. Đầu cuối gửi thông báo 1 đến thiết bị mạng 1.

Thông báo 1 được sử dụng để gửi yêu cầu đăng ký đến thiết bị mạng 1, và còn được sử dụng để ra lệnh thiết bị mạng 1 yêu cầu ID thiết bị cho đầu cuối. Cụ thể là, khi đầu cuối cần truy nhập mạng lưới vạn vật kết nối Internet, đầu cuối này cần đăng ký với hệ thống quản lý thiết bị. Đầu cuối đăng ký thành công với hệ thống quản lý thiết bị có thể truy nhập mạng lưới vạn vật kết nối Internet để thực hiện hoạt động liên quan.

S202. Thiết bị mạng 1 gửi thông báo 2 đến thiết bị mạng 2.

Thông báo 2 được sử dụng để yêu cầu ID thiết bị cho đầu cuối. Sau khi nhận thông báo 1, thiết bị mạng 1 tạo ra thông báo 2 và gửi thông báo 2 đến thiết bị mạng 2 theo lệnh của thông báo 1, để yêu cầu ID thiết bị cho đầu cuối.

Thông báo 1 và thông báo 2 có thể là các thông báo giao thức điều khiển truyền (Transmission Control Protocol, TCP), hoặc có thể là các thông báo giao thức gói dữ liệu người dùng (User datagram protocol, UDP). Đối với thông báo 1 và thông báo 2, có thể nhận dạng được, bằng cách sử dụng loại thông báo hoặc bit tương ứng, rằng thông báo 2 được sử dụng để yêu cầu ID thiết bị.

Theo biện pháp thực thi cụ thể, sau S202, phương pháp 200 có thể còn gồm có bước sau đây: S203. Thiết bị mạng 2 thực hiện việc xác minh mã nhận dạng trên đầu cuối.

Thiết bị mạng 2 có thể thực hiện việc xác minh mã nhận dạng trên đầu cuối theo các cách mà gồm có nhưng không bị giới hạn ở một vài cách sau đây.

Cách 1:

Thiết bị mạng 2 thực hiện việc xác minh mã nhận dạng trên đầu cuối dựa trên ủy nhiệm xác thực được dàn xếp với đầu cuối. Cụ thể là, thiết bị mạng 2 dàn xếp ủy nhiệm xác thực với đầu cuối trước, và lưu trữ cục bộ ủy nhiệm xác thực đã được dàn xếp. Khi yêu cầu thu ID thiết bị, đầu cuối bổ sung ủy nhiệm xác thực vào thông báo 1. Thông báo 2 được gửi bởi thiết bị mạng 1 đến thiết bị mạng 2 còn mang ủy nhiệm xác thực. Sau khi nhận thông báo 2, thiết bị mạng 2 thực hiện việc xác minh mã nhận dạng trên đầu cuối dựa trên ủy nhiệm xác thực được mang trong thông báo 2 và ủy nhiệm xác thực đã lưu trữ cục bộ. Nếu ủy nhiệm xác thực được mang trong thông báo 2 so khớp ủy nhiệm xác thực đã lưu trữ cục bộ, cho rằng đầu cuối thành công trong việc xác minh mã nhận dạng.

Cách 2:

Thiết bị mạng 2 thực hiện việc xác minh mã nhận dạng trên đầu cuối dựa trên cặp khóa duy nhất toàn cầu. Cụ thể là, đầu cuối tạo ra cặp khóa duy nhất toàn cầu trước. Chẳng hạn, trong pha phân phối của đầu cuối, đầu cuối tạo ra, dựa trên PUF, cặp khóa 1 gồm có khóa công cộng 1 và khóa riêng 1, và nhà quản trị mạng hoặc hệ thống quản lý mạng tạo cấu hình trước khóa công cộng 1 trong thiết bị mạng 2. Khi yêu cầu thu ID thiết bị, đầu cuối bổ sung khóa công cộng 1 vào thông báo 1. Thông báo 2 được gửi bởi thiết bị mạng 1 đến thiết bị mạng 2 còn mang khóa công cộng 1. Sau khi nhận thông báo 2, thiết bị mạng 2 thực hiện việc xác minh mã nhận dạng trên đầu cuối dựa trên khóa công cộng 1 được mang trong thông báo 2 và khóa công cộng 1 đã lưu trữ cục bộ. Nếu khóa công cộng 1 được mang trong thông báo 2 giống như khóa công cộng 1 đã lưu trữ trong thiết bị mạng 2, cho rằng đầu cuối thành công trong việc xác minh mã nhận dạng.

Cách 3:

Thiết bị mạng 2 thực hiện việc xác minh mã nhận dạng trên đầu cuối dựa trên chứng nhận khóa. Cụ thể là, đầu cuối tạo ra cặp khóa duy nhất toàn cầu trước. Chẳng hạn, trong pha phân phối của đầu cuối, đầu cuối tạo ra, dựa trên PUF, cặp khóa 1 gồm có khóa công cộng 1 và khóa riêng 1. Đầu cuối gửi khóa công cộng 1 đến CA, và CA phát hành chứng nhận khóa công cộng, và trả lại chứng nhận khóa công cộng đến đầu cuối. Chứng nhận khóa công cộng mang khóa công cộng 1. CA phát hành chứng nhận khóa công cộng, nên khóa công cộng 1 không cần được tạo cấu hình

trước trong thiết bị mạng 2. Điều này đơn giản hóa quá trình tạo cấu hình. Khi yêu cầu thu ID thiết bị, đầu cuối bổ sung chứng nhận khóa công cộng vào thông báo 1. Thông báo 2 được gửi bởi thiết bị mạng 1 đến thiết bị mạng 2 còn mang chứng nhận khóa công cộng. Sau khi nhận thông báo 2, thiết bị mạng 1 xác minh chứng nhận khóa công cộng. Nếu việc xác minh thành công, xác nhận rằng đầu cuối thành công trong việc xác minh mã nhận dạng.

Việc xác minh mã nhận dạng được thực hiện trên các đầu cuối, và đặc biệt là bằng cách sử dụng phương pháp theo cách 2 hoặc cách 3, nên hệ thống quản lý ID trong thiết bị mạng 2 chỉ gán ID thiết bị cho đầu cuối thành công trong việc xác minh mã nhận dạng. Điều này giúp tránh một cách hiệu quả việc tiêu thụ tài nguyên gây ra khi đầu cuối không đáng tin cậy áp dụng vào hệ thống quản lý ID đối với ID thiết bị. S203 không phải là hoạt động cần thiết. Khi S203 không được thực hiện, S204 có thể được thực hiện sau S202.

S204. Thiết bị mạng 2 tạo ra cặp khóa 2 dựa trên thông báo 2, trong đó cặp khóa gồm có khóa công cộng 2 và khóa riêng 2.

S205. Thiết bị mạng 2 gửi cặp khóa 2 và thông tin 1 đến thiết bị mạng 1.

Sau khi nhận thông báo 2, thiết bị mạng 2 tạo ra cặp khóa 2 đáp lại yêu cầu của thông báo 2. Cặp khóa 2 có thể được tạo ra bởi hệ thống quản lý ID trong thiết bị mạng 2, và thông tin 1 được sử dụng để nhận dạng rằng khóa công cộng 2 là ID thiết bị. Thông tin 1 có thể là loại thông báo, hoặc có thể là bit tương ứng trong thông báo. Cặp khóa 2 và thông tin 1 có thể được mang trong thông báo giống nhau, hoặc có thể được mang trong các thông báo khác nhau.

S206. Thiết bị mạng 1 gửi thông tin 2 và cặp khóa được mã hóa 2 đến đầu cuối.

Thông tin 2 được sử dụng để nhận dạng rằng khóa công cộng 2 là ID thiết bị. Thông tin 2 có thể là loại thông báo, hoặc có thể là bit tương ứng trong thông báo. Cặp khóa 2 và thông tin 2 có thể được mang trong thông báo giống nhau, hoặc có thể được mang trong các thông báo khác nhau.

Thiết bị mạng 1 có thể mã hóa cặp khóa 2 theo các cách mà gồm có nhưng không bị giới hạn ở các cách sau đây.

Cách 1:

Trước S201, chẳng hạn, trong pha phân phối của đầu cuối, đầu cuối tạo ra cặp khóa 1 dựa trên PUF. Cặp khóa 1 gồm có khóa công cộng 1 và khóa riêng 1. Sau khi đầu cuối tạo ra cặp khóa 2, thiết bị mạng 1 có thể thu khóa công cộng 1 theo các cách sau đây: Cách a: Thông báo 1 mang khóa công cộng 1, và thiết bị mạng 1 tách ra khóa công cộng 1 từ thông báo 1 và lưu trữ khóa công cộng 1. Cách 2: Nhà quản trị mạng hoặc hệ thống quản lý mạng tạo cấu hình khóa công cộng 1 trong thiết bị mạng 1. Khi gửi cặp khóa 2 đến đầu cuối, thiết bị mạng 1 thực hiện bảo vệ mã hóa trên cặp khóa 2 bằng cách sử dụng khóa công cộng 1. Sau khi nhận cặp khóa 2 được mã hóa bằng cách sử dụng khóa công cộng 1, đầu cuối thực hiện giải mã bằng cách sử dụng khóa riêng 1.

Theo cách 1, thiết bị mạng 1 mã hóa cặp khóa 1 bằng cách sử dụng khóa công cộng 2, và đầu cuối thực hiện giải mã bằng cách sử dụng khóa riêng 2 được lưu trữ trong đầu cuối. Do khóa công cộng 2 và khóa riêng 2 được tạo ra dựa trên PUF, và chỉ đầu cuối lưu trữ khóa riêng 2, nên khó giả mạo khóa riêng 2, và tính bảo mật truyền của cặp khóa 1 có thể được cải thiện một cách hiệu quả.

Cách 2: Thiết bị mạng 1 dàn xếp khóa với đầu cuối trước, và mã hóa cặp khóa 2 bằng cách sử dụng khóa đã được dàn xếp.

S207. Đầu cuối nhận và lưu trữ cặp khóa 2.

Sau khi nhận cặp khóa 2, đầu cuối lưu trữ cặp khóa 2. Theo biện pháp thực thi cụ thể, đầu cuối mã hóa cặp khóa đã lưu trữ 2 bằng cách sử dụng khóa công cộng 1 được tạo ra dựa trên PUF, hoặc chỉ mã hóa khóa riêng đã lưu trữ 2 bằng cách sử dụng khóa công cộng 1. Khóa riêng 1 tương ứng với khóa công cộng 1 được sử dụng để giải mã. Do khóa công cộng 1 và khóa riêng 1 được tạo ra dựa trên PUF và khó giả mạo, tính bảo mật lưu trữ của khóa riêng 2 có thể được cải thiện. Chắc chắn là, đầu cuối có thể theo cách khác thực hiện bảo vệ mã hóa trên cặp khóa 2 hoặc ít nhất khóa riêng 2 bằng cách sử dụng khóa khác hoặc theo cách khác, để cải thiện tính bảo mật lưu trữ của khóa riêng 2.

S208. Đầu cuối xác định rằng khóa công cộng 1 là ID thiết bị.

Đầu cuối thu được cặp khóa 1, và xác định, theo lệnh của thông tin 2, rằng khóa công cộng 1 là ID thiết bị. Theo cách này, đầu cuối xác định rằng đầu cuối thu ID thiết bị của đầu cuối.

Cần lưu ý rằng hoạt động lưu trữ cặp khóa 2 bởi đầu cuối trong S207 và hoạt động trong S208 không được thực hiện theo trình tự. Cụ thể là, đầu cuối có thể lưu trữ cặp khóa 2 trước S208, hoặc có thể lưu trữ cặp khóa 2 sau S208, hoặc có thể lưu trữ cặp khóa 2 đồng thời khi hoàn thành hoạt động trong S208.

Theo cách thực thi cụ thể, sau S207, phương pháp 200 có thể còn gồm có bước sau đây:

S209. Đầu cuối gửi, đến thiết bị mạng 1, thông báo 2 được ký bằng cách sử dụng khóa riêng 1.

Cụ thể là, thông báo 2 có thể được sử dụng để xác nhận, từ hệ thống quản lý thiết bị được triển khai trong thiết bị mạng 1, rằng đầu cuối được đăng ký thành công. Thông báo 2 có thể còn được sử dụng để báo cáo ID thiết bị, nghĩa là, thông tin như khóa công cộng 1, thông tin trạng thái thiết bị, thông tin vị trí thiết bị, và/hoặc loại thiết bị, đến thiết bị mạng 1. Cụ thể là, hoạt động cần được thực hiện bằng cách sử dụng thông báo 2 có thể được nhận dạng bằng cách sử dụng loại thông báo trong thông báo 2 hoặc bit tương ứng trong thông báo 2. Thông báo 2 có thể mang khóa công cộng 1 được sử dụng làm ID thiết bị. Sau khi nhận thông báo 2, thiết bị mạng 1 có thể xác minh chữ ký của thông báo 2 bằng cách sử dụng khóa công cộng 1, để thực hiện tiếp việc xác minh mã nhận dạng trên đầu cuối.

S209 và S208 không được thực hiện theo trình tự. Cụ thể là, S209 có thể được thực hiện trước S208, hoặc S209 có thể được thực hiện sau S208, hoặc S209 và S208 có thể được thực hiện đồng thời.

Theo biện pháp thực thi cụ thể, sau S208, phương pháp 200 có thể còn gồm có bước sau đây: Đầu cuối gửi, đến thiết bị mạng 3, thông báo 3 được ký bằng cách sử dụng khóa riêng 1.

Thiết bị mạng 3 là đầu cuối ngoài đầu cuối đã nêu ở trên. Đầu cuối và thiết bị mạng 3 trao đổi thông tin với nhau. Đầu cuối ký, bằng cách sử dụng khóa riêng 1, thông tin được mang trong thông báo 3, và thông báo 3 mang khóa công cộng 1 được sử dụng làm ID thiết bị. Sau khi nhận thông báo 3, thiết bị mạng 3 có thể trực tiếp tách ra khóa công cộng 1 từ thông báo 3, nên thiết bị mạng 3 có thể xác minh chữ ký của thông báo 3 mà không thu khóa công cộng 1 trước, để thực hiện tiếp việc xác minh mã nhận dạng trên đầu cuối.

Fig.3 là lưu đồ giản lược của phương tháp thu ID thiết bị 300 theo phương án của sáng chế. Kiến trúc mạng mà phương pháp 300 được áp dụng gồm có ít nhất đầu cuối và thiết bị mạng 1. Chẳng hạn, đầu cuối có thể là, chẳng hạn, đầu cuối 101 trong kiến trúc mạng được thể hiện trên Fig.1, và thiết bị mạng 1 có thể là, chẳng hạn, thiết bị mạng 107 được thể hiện trên Fig.1 và trong đó hệ thống quản lý ID được triển khai, hoặc thiết bị mạng 108 được thể hiện trên Fig.1 và trong đó hệ thống quản lý ID được triển khai. Hệ thống quản lý ID có thể là, chẳng hạn, hệ thống IDaas. Kiến trúc mạng có thể là kiến trúc mạng được thể hiện trên Fig.1. Phương pháp 300 gồm có các hoạt động sau đây.

S301. Đầu cuối gửi thông báo 1 đến thiết bị mạng 1.

Thông báo 1 được sử dụng để yêu cầu ID thiết bị cho đầu cuối. Đối với thông báo 1, có thể nhận dạng được, bằng cách sử dụng loại thông báo hoặc bit tương ứng, mà thông báo được sử dụng để yêu cầu ID thiết bị.

Theo biện pháp thực thi cụ thể, sau S301, phương pháp 300 có thể còn gồm có bước sau đây: S302. Thiết bị mạng 1 thực hiện việc xác minh mã nhận dạng trên đầu cuối.

Thiết bị mạng 1 có thể thực hiện việc xác minh mã nhận dạng trên đầu cuối theo các cách mà gồm có nhưng không bị giới hạn ở một vài cách sau đây.

Cách 1: Thiết bị mạng 1 thực hiện việc xác minh mã nhận dạng trên đầu cuối dựa trên ủy nhiệm xác thực được dàn xếp với đầu cuối. Cụ thể là, thiết bị mạng 1 dàn xếp ủy nhiệm xác thực với đầu cuối, và lưu trữ ủy nhiệm xác thực. Khi yêu cầu thu ID thiết bị, đầu cuối bổ sung ủy nhiệm xác thực đã được dàn xếp vào thông báo 1. Sau khi nhận thông báo 1, thiết bị mạng 1 thực hiện việc xác minh mã nhận dạng trên đầu cuối dựa trên ủy nhiệm xác thực được mang trong thông báo 1 và ủy nhiệm xác thực được lưu trữ trong thiết bị mạng 1. Nếu thiết bị mạng 1 xác định rằng ủy nhiệm xác thực được mang trong thông báo 1 so khớp ủy nhiệm xác thực đã lưu trữ cục bộ, cho rằng đầu cuối thành công trong việc xác minh mã nhận dạng.

Cách 2: Thiết bị mạng 1 thực hiện việc xác minh mã nhận dạng trên đầu cuối dựa trên cặp khóa duy nhất toàn cầu. Cụ thể là, đầu cuối tạo ra cặp khóa duy nhất toàn cầu trước. Chẳng hạn, trong pha phân phối của đầu cuối, đầu cuối tạo ra, dựa trên PUF, cặp khóa 1 gồm có khóa công cộng 1 và khóa riêng 1, và nhà quản trị mạng

hoặc hệ thống quản lý mạng tạo cấu hình trước khóa công cộng 1 trong thiết bị mạng 1. Khi yêu cầu thu ID thiết bị, đầu cuối bổ sung khóa công cộng 1 vào thông báo 1. Sau khi nhận thông báo 1, thiết bị mạng 1 thực hiện việc xác minh mã nhận dạng trên đầu cuối dựa trên khóa công cộng 1 được mang trong thông báo 1 và khóa công cộng 1 được lưu trữ. Nếu khóa công cộng 2 được mang trong thông báo 1 giống như khóa công cộng 1 được lưu trữ trong thiết bị mạng 1, cho rằng đầu cuối thành công trong việc xác minh mã nhận dạng.

Cách 3: Thiết bị mạng 1 thực hiện việc xác minh mã nhận dạng trên đầu cuối dựa trên chứng nhận khóa. Cụ thể là, đầu cuối tạo ra cặp khóa duy nhất toàn cầu trước. Chẳng hạn, trong pha phân phối của đầu cuối, đầu cuối tạo ra, dựa trên PUF, cặp khóa 1 gồm có khóa công cộng 1 và khóa riêng 1. Đầu cuối gửi khóa công cộng 1 đến CA để phát hành chứng nhận, và CA phát hành chứng nhận khóa công cộng, và trả lại chứng nhận khóa công cộng đến đầu cuối. Chứng nhận khóa công cộng mang khóa công cộng 1. CA phát hành chứng nhận khóa công cộng, nên khóa công cộng 1 không cần được tạo cấu hình trước trong thiết bị mạng 1. Điều này đơn giản hóa quá trình tạo cấu hình. Khi yêu cầu thu ID thiết bị, đầu cuối bổ sung chứng nhận khóa công cộng vào thông báo 1. Sau khi nhận thông báo 1, thiết bị mạng 1 xác minh chứng nhận khóa công cộng được mang trong thông báo 1. Nếu việc xác minh thành công, xác nhận rằng đầu cuối thành công trong việc xác minh mã nhận dạng.

Việc xác minh mã nhận dạng được thực hiện trên các đầu cuối, nên hệ thống quản lý ID trong thiết bị mạng 2 chỉ gán ID thiết bị cho đầu cuối thành công trong việc xác minh mã nhận dạng. Điều này giúp tránh một cách hiệu quả việc tiêu thụ tài nguyên gây ra khi đầu cuối không đáng tin cậy áp dụng vào hệ thống quản lý ID đối với ID thiết bị. S302 không phải là hoạt động cần thiết. Khi S302 không được thực hiện, S303 được thực hiện sau S301.

S303. Thiết bị mạng 1 tạo ra cặp khóa 2, trong đó cặp khóa 2 gồm có khóa công cộng 2 và khóa riêng 2.

S304. Thiết bị mạng 1 gửi cặp khóa được mã hóa 2 và thông tin 1 đến đầu cuối.

Sau khi nhận thông báo 1, thiết bị mạng 1 tạo ra cặp khóa 2 đáp lại yêu cầu của đầu cuối. Cặp khóa 2 có thể được tạo ra bởi hệ thống quản lý ID trong thiết bị

mạng 2, và thông tin 1 được sử dụng để nhận dạng rằng khóa công cộng 2 là ID thiết bị. Thông tin 1 có thể là loại thông báo, hoặc có thể là bit tương ứng trong thông báo. Cặp khóa 2 và thông tin 1 có thể được mang trong thông báo giống nhau, hoặc có thể được mang trong các thông báo khác nhau.

Phương pháp mã hóa cặp khóa 2 bởi thiết bị mạng 1 tương tự với phương pháp mã hóa cặp khóa 2 bởi thiết bị mạng 1 trong phương pháp 200. Để biết chi tiết, tham khảo các phần mô tả liên quan của S206 trong phương pháp 200. Các chi tiết không được mô tả lại ở đây.

S305. Đầu cuối nhận và lưu trữ cặp khóa 2.

Sau khi nhận cặp khóa 2, đầu cuối lưu trữ cặp khóa 2. Theo biện pháp thực thi cụ thể, đầu cuối mã hóa cặp khóa đã lưu trữ 2 bằng cách sử dụng khóa công cộng 1 được tạo ra dựa trên PUF, hoặc chỉ mã hóa khóa riêng đã lưu trữ 2 bằng cách sử dụng khóa công cộng 1. Khóa riêng 1 tương ứng với khóa công cộng 1 được sử dụng để giải mã. Do khóa công cộng 1 và khóa riêng 1 được tạo ra dựa trên PUF và khó giả mạo, tính bảo mật lưu trữ của khóa riêng 2 có thể được cải thiện. Chắc chắn là, đầu cuối có thể theo cách khác thực hiện bảo vệ mã hóa trên cặp khóa 2 hoặc ít nhất khóa riêng 2 bằng cách sử dụng khóa khác hoặc theo cách khác, để cải thiện tính bảo mật lưu trữ của khóa riêng 2.

S306. Đầu cuối xác định rằng khóa công cộng 2 là ID thiết bị.

Đầu cuối thu được cặp khóa 1, và xác định, theo lệnh của thông tin 1, rằng khóa công cộng 2 là ID thiết bị. Theo cách này, đầu cuối thu được ID thiết bị của đầu cuối.

Cần lưu ý rằng hoạt động lưu trữ cặp khóa 2 bởi đầu cuối trong S305 và hoạt động trong S306 không được thực hiện theo trình tự. Cụ thể là, đầu cuối có thể lưu trữ cặp khóa 2 trước S306, hoặc có thể lưu trữ cặp khóa 2 sau S306, hoặc có thể lưu trữ cặp khóa 2 đồng thời khi hoàn thành hoạt động trong S306.

Fig.4 là lưu đồ giản lược của phương pháp đăng ký đầu cuối 400 theo phương án của sáng chế.

Theo biện pháp thực thi cụ thể, phương pháp 400 có thể được thực hiện sau S305 trong phương pháp 300. Phần sau đây mô tả phương pháp 400 dựa vào Fig.4. Phương pháp 400 gồm có các hoạt động sau đây.

S401. Đầu cuối gửi yêu cầu đăng ký đến thiết bị mạng 2, trong đó yêu cầu đăng ký mang khóa công cộng 2 được sử dụng làm ID thiết bị. Thiết bị mạng 2 và thiết bị mạng 1 được triển khai trong kiến trúc mạng giống nhau, và hệ thống quản lý thiết bị được triển khai trong thiết bị mạng 2. Chẳng hạn, thiết bị mạng 1 có thể là thiết bị mạng 108 trong kiến trúc mạng được thể hiện trên Fig.1, và thiết bị mạng 2 có thể là thiết bị mạng 107 trong kiến trúc mạng được thể hiện trên Fig.1.

S402. Sau khi nhận yêu cầu đăng ký, thiết bị mạng 2 gửi yêu cầu xác nhận đến thiết bị mạng 1, trong đó yêu cầu xác nhận mang khóa công cộng 2, và yêu cầu xác nhận được sử dụng để xác nhận việc đầu cuối đã đăng ký với thiết bị mạng 1 hay chưa.

S403. Thiết bị mạng 1 nhận yêu cầu xác nhận, và xác minh, dựa trên khóa công cộng 2 đã lưu trữ cục bộ và khóa công cộng 2 được mang trong yêu cầu xác nhận, việc đầu cuối có được đăng ký hay không. Cụ thể là, thiết bị mạng 1 có thể hỏi liệu khóa công cộng 1 của đầu cuối có được lưu trữ trong hệ thống quản lý ID hay không. Nếu khóa công cộng 2 được lưu trữ trong hệ thống quản lý ID, điều này chỉ báo rằng thiết bị mạng 1 đã được tạo cấu hình ID thiết bị cho đầu cuối. Nói cách khác, điều này chỉ báo rằng đầu cuối đã đăng ký với hệ thống quản lý ID.

S404. Thiết bị mạng 1 xác nhận rằng đầu cuối được đăng ký thành công, và gửi trả lời xác nhận đến thiết bị mạng 2 để chỉ báo, đến thiết bị mạng 2, rằng đầu cuối được đăng ký thành công.

S405. Sau khi nhận trả lời xác nhận, thiết bị mạng 2 có thể gửi trả lời đăng ký đến đầu cuối để khai báo rằng đầu cuối đăng ký thành công với thiết bị mạng 2.

Fig.5 là lưu đồ giản lược của phương pháp đăng ký đầu cuối 500 khác theo phương án của sáng chế.

Theo biện pháp thực thi cụ thể, phương pháp 500 có thể được thực hiện sau S303 trong phương pháp 300. Phần sau đây mô tả phương pháp 500 dựa vào Fig.5. Phương pháp 500 gồm có các hoạt động sau đây.

S501. Thiết bị mạng 1 gửi khóa công cộng 2 và thông tin 2 đến thiết bị mạng 2.

Thông tin 2 được sử dụng để chỉ báo rằng khóa công cộng 2 là ID thiết bị. Chẳng hạn, thông tin 2 có thể là loại thông báo, hoặc có thể là bit tương ứng trong

thông báo. Khóa công cộng 2 và thông tin 2 có thể được mang trong thông báo giống nhau, hoặc có thể được mang trong các thông báo khác nhau. Thiết bị mạng 2 và thiết bị mạng 1 được triển khai trong kiến trúc mạng giống nhau, và hệ thống quản lý thiết bị được triển khai trong thiết bị mạng 2. Chẳng hạn, thiết bị mạng 1 có thể là thiết bị mạng 108 trong kiến trúc mạng được thể hiện trên Fig.1, và thiết bị mạng 2 có thể là thiết bị mạng 107 trong kiến trúc mạng được thể hiện trên Fig.1. Sau khi nhận khóa công cộng 2, thiết bị mạng 2 xác nhận, theo lệnh của thông tin 2, rằng khóa công cộng 2 là ID thiết bị. Thiết bị mạng 2 lưu trữ khóa công cộng 2, chẳng hạn, lưu trữ khóa công cộng 2 trong cơ sở dữ liệu của hệ thống quản lý thiết bị.

S502. Thiết bị mạng 2 nhận yêu cầu đăng ký được gửi bởi đầu cuối, trong đó yêu cầu đăng ký mang khóa công cộng 2 được sử dụng làm ID thiết bị.

S503. Thiết bị mạng 2 xác minh đầu cuối dựa trên khóa công cộng 2 đã lưu trữ và khóa công cộng 2 trong yêu cầu đăng ký.

Nếu thiết bị mạng xác nhận rằng khóa công cộng 2 đã lưu trữ giống như khóa công cộng 2 trong yêu cầu đăng ký, cho rằng đầu cuối thành công trong việc xác minh.

S504. Thiết bị mạng gửi trả lời đăng ký đến đầu cuối để chỉ báo rằng đầu cuối được đăng ký thành công.

Sau S504, phương pháp 500 có thể còn gồm có bước sau đây: S505. Đầu cuối gửi, đến thiết bị mạng 2, thông báo 2 được ký bằng cách sử dụng khóa riêng 2.

Thông báo 2 có thể được sử dụng để xác nhận, từ thiết bị mạng 2, rằng đầu cuối được đăng ký thành công. Thông báo 2 có thể còn được sử dụng để báo cáo ID thiết bị, nghĩa là, thông tin như khóa công cộng 2, thông tin trạng thái thiết bị, thông tin vị trí thiết bị, và/hoặc loại thiết bị, đến hệ thống quản lý thiết bị được triển khai trong thiết bị mạng 2. Cụ thể là, hoạt động cần được thực hiện bằng cách sử dụng thông báo 2 có thể được nhận dạng bằng cách sử dụng loại thông báo trong thông báo 2 hoặc bit tương ứng trong thông báo 2. Thông báo 2 có thể mang khóa công cộng 2 được sử dụng làm ID thiết bị. Sau khi nhận thông báo 2, thiết bị mạng 2 có thể xác minh chữ ký của thông báo 2 bằng cách sử dụng khóa công cộng 2, để thực hiện tiếp việc xác minh mã nhận dạng trên đầu cuối.

Cần lưu ý rằng trình tự hoạt động của S501 và S304 đến S306 không bị giới

hạn cụ thể trong phương án này của sáng chế. Chẳng hạn, S501 có thể được hoàn thành trước S304, hoặc có thể được hoàn thành sau S304, hoặc có thể được hoàn thành đồng thời với S304; S501 có thể được hoàn thành trước S305, hoặc có thể được hoàn thành sau S305, hoặc có thể được hoàn thành đồng thời với S305; hoặc S501 có thể được hoàn thành trước S306, hoặc có thể được hoàn thành sau S306, hoặc có thể được hoàn thành đồng thời với S306. S502 được thực hiện sau S306.

Theo biện pháp thực thi cụ thể, sau S504, phương pháp 500 có thể còn gồm có bước sau đây: S505. Đầu cuối gửi, đến thiết bị mạng 3, thông báo 3 được ký bằng cách sử dụng khóa riêng 2.

Thiết bị mạng 3 có thể là đầu cuối ngoài đầu cuối đã nêu ở trên. Đầu cuối và thiết bị mạng 3 trao đổi thông tin với nhau. Đầu cuối ký, bằng cách sử dụng khóa riêng 2, thông tin được mang trong thông báo 3, và thông báo 3 mang khóa công cộng 2 được sử dụng làm ID thiết bị. Sau khi nhận thông báo 3, thiết bị mạng 3 có thể trực tiếp tách ra khóa công cộng 2 từ thông báo 3, nên thiết bị mạng 3 có thể xác minh chữ ký của thông báo 3 mà không thu khóa công cộng 2 trước, để thực hiện tiếp việc xác minh mã nhận dạng trên đầu cuối.

Fig.6 là lưu đồ giản lược của phương tháp thu ID thiết bị 600 theo phương án của sáng chế. Kiến trúc mạng mà phương pháp 600 được áp dụng gồm có ít nhất đầu cuối và thiết bị mạng 1. Chẳng hạn, đầu cuối có thể là đầu cuối 101 được thể hiện trên Fig.1, và thiết bị mạng 1 có thể là thiết bị mạng 107 hoặc thiết bị mạng 108 trong kiến trúc mạng được thể hiện trên Fig.1. Hệ thống quản lý thiết bị và hệ thống quản lý ID được triển khai trong thiết bị mạng 1, và hệ thống quản lý ID có thể là, chẳng hạn, hệ thống IDaas. Kiến trúc mạng có thể là kiến trúc mạng được thể hiện trên Fig.1. Phương pháp 600 gồm có các hoạt động sau đây.

S601. Đầu cuối gửi thông báo 1 đến thiết bị mạng 1.

Thông báo 1 được sử dụng để yêu cầu ID thiết bị cho đầu cuối từ hệ thống quản lý ID và gửi yêu cầu đăng ký đến hệ thống quản lý thiết bị. Đối với thông báo 1, có thể nhận dạng được, bằng cách sử dụng loại thông báo hoặc bit tương ứng, rằng thông báo 1 được sử dụng để yêu cầu ID thiết bị cho đầu cuối và đăng ký với hệ thống quản lý thiết bị.

Theo biện pháp thực thi cụ thể, sau S601, phương pháp 600 có thể còn gồm

có bước sau đây: S602. Thiết bị mạng 1 thực hiện việc xác minh mã nhận dạng trên đầu cuối.

Cách trong đó thiết bị mạng 1 thực hiện việc xác minh mã nhận dạng trên đầu cuối giống như cách trong đó thiết bị mạng 1 thực hiện việc xác minh mã nhận dạng trên đầu cuối trong phương pháp 300. Để biết chi tiết, tham khảo các phần mô tả liên quan của S302 trong phương pháp 300. Các chi tiết không được mô tả lại ở đây.

Việc xác minh mã nhận dạng được thực hiện trên các đầu cuối, nên hệ thống quản lý ID trong thiết bị mạng 2 chỉ gán ID thiết bị cho đầu cuối thành công trong việc xác minh mã nhận dạng. Điều này giúp tránh một cách hiệu quả việc tiêu thụ tài nguyên gây ra khi đầu cuối không đáng tin cậy áp dụng vào hệ thống quản lý ID đối với ID thiết bị. S602 không phải là hoạt động cần thiết. Khi S602 không được thực hiện, S603 được thực hiện sau S601.

S603. Thiết bị mạng 1 tạo ra cặp khóa 2, trong đó cặp khóa 2 gồm có khóa công cộng 2 và khóa riêng 2.

S604. Thiết bị mạng 1 gửi cặp khóa được mã hóa 2 và thông tin 1 đến đầu cuối.

Sau khi nhận thông tin 1, thiết bị mạng 1 tạo ra cặp khóa 2 đáp lại yêu cầu của đầu cuối. Cặp khóa 2 có thể được tạo ra bởi hệ thống quản lý ID trong thiết bị mạng 1. Thông tin 1 được sử dụng để nhận dạng rằng khóa công cộng 2 là ID thiết bị. Thông tin 1 có thể là loại thông báo, hoặc có thể là bit tương ứng trong thông báo. Cặp khóa 2 và thông tin 1 có thể được mang trong thông báo giống nhau, hoặc có thể được mang trong các thông báo khác nhau.

Phương pháp mã hóa cặp khóa 2 bởi thiết bị mạng 1 tương tự với phương pháp mã hóa cặp khóa 2 bởi thiết bị mạng 1 trong phương pháp 200. Để biết chi tiết, tham khảo các phần mô tả liên quan của S206 trong phương pháp 200. Các chi tiết không được mô tả lại ở đây.

S605. Đầu cuối nhận và lưu trữ cặp khóa 2.

Sau khi nhận cặp khóa 2, đầu cuối lưu trữ cặp khóa 2. Theo biện pháp thực thi cụ thể, đầu cuối mã hóa cặp khóa đã lưu trữ 2 bằng cách sử dụng khóa công cộng 1 được tạo ra dựa trên PUF, hoặc chỉ mã hóa khóa riêng đã lưu trữ 2 bằng cách sử dụng khóa công cộng 1. Khóa riêng 1 tương ứng với khóa công cộng 1 được sử dụng để

giải mã. Do khóa công cộng 1 và khóa riêng 1 được tạo ra dựa trên PUF và khó giả mạo, tính bảo mật lưu trữ của khóa riêng 2 có thể được cải thiện. Chắc chắn là, đầu cuối có thể theo cách khác thực hiện bảo vệ mã hóa trên cặp khóa 2 hoặc ít nhất khóa riêng 2 bằng cách sử dụng khóa khác hoặc theo cách khác, để cải thiện tính bảo mật lưu trữ của khóa riêng 2.

S606. Đầu cuối xác định rằng khóa công cộng 2 là ID thiết bị.

Đầu cuối thu cặp khóa 1, và xác định, theo lệnh của thông tin 1, rằng khóa công cộng 2 là ID thiết bị.

Cần lưu ý rằng hoạt động lưu trữ cặp khóa 2 bởi đầu cuối trong S605 và hoạt động trong S606 không được thực hiện theo trình tự. Cụ thể là, đầu cuối có thể lưu trữ cặp khóa 2 trước S606, hoặc có thể lưu trữ cặp khóa 2 sau S606, hoặc có thể lưu trữ cặp khóa 2 đồng thời khi hoàn thành hoạt động trong S606.

Theo biện pháp thực thi cụ thể, sau S606, phương pháp 600 có thể còn gồm có bước sau đây: S607. Đầu cuối gửi, đến thiết bị mạng 1, thông báo 2 được ký bằng cách sử dụng khóa riêng 2.

Cụ thể là, thông báo 2 có thể được sử dụng để xác nhận, từ hệ thống quản lý thiết bị được triển khai trong thiết bị mạng 1, rằng đầu cuối được đăng ký thành công. Thông báo 2 có thể còn được sử dụng để báo cáo ID thiết bị, nghĩa là, thông tin như khóa công cộng 2, thông tin trạng thái thiết bị, thông tin vị trí thiết bị, và/hoặc loại thiết bị, đến thiết bị mạng 1. Cụ thể là, hoạt động cần được thực hiện bằng cách sử dụng thông báo 2 có thể được nhận dạng bằng cách sử dụng loại thông báo trong thông báo 2 hoặc bit tương ứng trong thông báo 2. Thông báo 2 có thể mang khóa công cộng 2 được sử dụng làm ID thiết bị. Sau khi nhận thông báo 2, thiết bị mạng 1 có thể xác minh chữ ký của thông báo 2 bằng cách sử dụng khóa công cộng 2, để thực hiện tiếp việc xác minh mã nhận dạng trên đầu cuối.

Theo biện pháp thực thi cụ thể, sau S606, phương pháp 600 có thể còn gồm có bước sau đây: Đầu cuối gửi, đến thiết bị mạng 3, thông báo 3 được ký bằng cách sử dụng khóa riêng 2.

Thiết bị mạng 3 có thể là đầu cuối ngoài đầu cuối đã nêu ở trên. Đầu cuối và thiết bị mạng 3 trao đổi thông tin với nhau. Đầu cuối ký, bằng cách sử dụng khóa riêng 2, thông tin được mang trong thông báo 3, và thông báo 3 mang khóa công

cộng 2 được sử dụng làm ID thiết bị. Sau khi nhận thông báo 3, thiết bị mạng 3 có thể trực tiếp tách ra khóa công cộng 2 từ thông báo 3, nên thiết bị mạng 3 có thể xác minh chữ ký của thông báo 3 mà không thu khóa công cộng 2 trước, để thực hiện tiếp việc xác minh mã nhận dạng trên đầu cuối.

Fig.7 là lưu đồ giản lược của phương tháp thu ID thiết bị 700 khác theo phương án của sáng chế. Kiến trúc mạng mà phương pháp 700 được áp dụng gồm có ít nhất đầu cuối và thiết bị mạng thứ nhất. Chẳng hạn, đầu cuối có thể là đầu cuối 101 trong kiến trúc mạng được thể hiện trên Fig.1, và thiết bị mạng thứ nhất có thể là thiết bị mạng 108 trong kiến trúc mạng được thể hiện trên Fig.1. Hệ thống quản lý thiết bị và/hoặc hệ thống quản lý ID được triển khai trong thiết bị mạng thứ nhất. Kiến trúc mạng có thể là kiến trúc mạng được thể hiện trên Fig.1. Phương pháp 700 gồm có các hoạt động sau đây.

S701. Đầu cuối gửi, đến thiết bị mạng thứ nhất, thông báo thứ nhất được sử dụng để yêu cầu ID thiết bị cho đầu cuối, trong đó ID thiết bị được sử dụng để nhận dạng toàn cầu đầu cuối theo cách duy nhất.

Thông báo thứ nhất có thể là thông báo TCP, hoặc có thể là thông báo UDP. Đối với thông báo thứ nhất, có thể nhận dạng được, bằng cách sử dụng loại thông báo hoặc bit tương ứng, rằng thông báo thứ nhất được sử dụng để yêu cầu ID thiết bị.

S702. Đầu cuối nhận cặp khóa được mã hóa được gửi bởi thiết bị mạng thứ nhất, trong đó cặp khóa này gồm có khóa công cộng thứ nhất và khóa riêng thứ nhất.

Đối với phương pháp mã hóa cặp khóa bởi thiết bị mạng thứ nhất, tham khảo các phần mô tả liên quan của bước mã hóa cặp khóa 2 bởi thiết bị mạng 1 trong S206 trong phương pháp 200. Các chi tiết không được mô tả lại ở đây.

S703. Đầu cuối nhận thông tin được gửi bởi thiết bị mạng thứ nhất, trong đó thông tin này được sử dụng để nhận dạng rằng khóa công cộng thứ nhất là ID thiết bị của đầu cuối.

Thông tin có thể là loại thông báo, hoặc có thể là bit tương ứng trong thông báo. Thông tin được gửi trong S703 và cặp khóa được gửi trong S702 có thể được mang trong một thông báo, hoặc có thể được mang trong các thông báo khác nhau.

Cặp khóa được nhận bởi đầu cuối trong S702 và thông tin được nhận bởi đầu

cuối trong S703 có thể được mang trong thông báo giống nhau, hoặc có thể được mang trong các thông báo khác nhau. Khi cặp khóa và thông tin được mang trong thông báo giống nhau, S702 và S703 có thể được hiểu là được hoàn thành bởi hoạt động giống nhau, hoặc có thể được hiểu là được hoàn thành bởi hai hoạt động. Khi cặp khóa và thông tin được mang trong các thông báo khác nhau, S703 có thể được thực hiện trước, sau, hoặc đồng thời với S702.

S704. Đầu cuối xác định rằng khóa công cộng thứ nhất là ID thiết bị.

Đầu cuối thu được cặp khóa và thông tin, và xác định, theo lệnh của thông tin, rằng khóa công cộng thứ nhất là ID thiết bị. Theo cách này, đầu cuối xác định rằng đầu cuối thu được ID thiết bị của đầu cuối.

Theo biện pháp thực thi cụ thể, hệ thống quản lý thiết bị được triển khai trong thiết bị mạng thứ nhất, và phương pháp 700 có thể còn gồm có bước sau đây: S705. Đầu cuối gửi, đến thiết bị mạng thứ nhất, thông báo thứ hai được ký bằng cách sử dụng khóa riêng thứ nhất, trong đó thông báo thứ hai này mang khóa công cộng thứ nhất được sử dụng làm ID thiết bị của đầu cuối.

Thông báo thứ hai có thể được sử dụng để xác nhận, từ hệ thống quản lý thiết bị được triển khai trong thiết bị mạng thứ nhất, rằng đầu cuối được đăng ký thành công. Thông báo thứ hai có thể còn được sử dụng để báo cáo ID thiết bị, nghĩa là, thông tin như khóa công cộng thứ nhất, thông tin trạng thái thiết bị, thông tin vị trí thiết bị, và/hoặc loại thiết bị, đến thiết bị mạng thứ nhất. Cụ thể là, hoạt động cần được thực hiện bằng cách sử dụng thông báo thứ hai có thể được nhận dạng bằng cách sử dụng loại thông báo trong thông báo thứ hai hoặc bit tương ứng trong thông báo thứ hai. Thông báo thứ hai có thể mang khóa công cộng thứ nhất được sử dụng làm ID thiết bị. Sau khi nhận thông báo thứ hai, thiết bị mạng thứ nhất có thể xác minh chữ ký của thông báo thứ hai bằng cách sử dụng khóa công cộng thứ nhất, để thực hiện tiếp việc xác minh mã nhận dạng trên đầu cuối.

Theo biện pháp thực thi, thông báo thứ nhất mang khóa công cộng thứ hai, và khóa công cộng thứ hai là khóa công cộng được tạo ra bởi đầu cuối dựa trên PUF.

Đầu cuối có thể tạo ra, dựa trên PUF, khóa công cộng thứ hai và khóa riêng thứ hai trước S701, chẳng hạn, trong pha phân phối của đầu cuối. Nhà quản trị mạng hoặc hệ thống quản lý mạng có thể tạo cấu hình trước khóa công cộng thứ hai trong

thiết bị mạng trong đó hệ thống quản lý ID được triển khai. Theo cách khác, đầu cuối gửi khóa công cộng thứ hai đến CA, và CA phát hành chứng nhận, và trả lại chứng nhận khóa công cộng đã được phát hành đến đầu cuối. CA phát hành chứng nhận, nên khóa công cộng thứ hai không cần được triển khai trong thiết bị mạng trước. Điều này đơn giản hóa quá trình tạo cấu hình. Việc thông báo thứ nhất mang khóa công cộng thứ hai gồm có: Thông báo thứ nhất trực tiếp mang khóa công cộng thứ hai; hoặc thông báo thứ nhất mang chứng nhận khóa công cộng được phát hành bởi CA, trong đó chứng nhận khóa công cộng mang khóa công cộng thứ hai. Khi yêu cầu thu ID thiết bị, đầu cuối bổ sung khóa công cộng thứ hai vào thông báo thứ nhất. Nếu hệ thống quản lý ID được triển khai trong thiết bị mạng thứ nhất, thiết bị mạng thứ nhất thực hiện việc xác minh mã nhận dạng trên đầu cuối dựa trên khóa công cộng thứ hai được mang trong thông báo thứ nhất và khóa công cộng thứ hai được lưu trữ trong thiết bị mạng thứ nhất. Nếu không có hệ thống quản lý ID được triển khai trong thiết bị mạng thứ nhất, nhưng chỉ hệ thống quản lý thiết bị được triển khai trong thiết bị mạng thứ nhất, sau khi thiết bị mạng thứ nhất nhận thông báo thứ nhất được gửi bởi đầu cuối, thiết bị mạng thứ nhất tạo ra thông báo thứ hai mang khóa công cộng thứ hai, và gửi thông báo thứ hai đến thiết bị mạng thứ hai. Hệ thống quản lý ID được triển khai trong thiết bị mạng thứ hai, và thiết bị mạng thứ hai lưu trữ khóa công cộng thứ hai. Sau khi nhận thông báo thứ hai, thiết bị mạng thứ hai thực hiện việc xác minh mã nhận dạng trên đầu cuối dựa trên khóa công cộng thứ hai được mang trong thông báo thứ hai và khóa công cộng thứ hai được lưu trữ trong thiết bị mạng thứ hai.

Theo biện pháp thực thi, bước đầu cuối nhận cặp khóa được mã hóa được gửi bởi thiết bị mạng thứ nhất gồm có:

Đầu cuối nhận cặp khóa được gửi bởi thiết bị mạng thứ nhất và được mã hóa bằng cách sử dụng khóa công cộng thứ hai.

Sau khi nhận cặp khóa được gửi bởi thiết bị mạng thứ nhất và được mã hóa bằng cách sử dụng khóa công cộng thứ hai, đầu cuối có thể thực hiện giải mã chỉ bằng cách sử dụng khóa riêng thứ hai tương ứng với khóa công cộng thứ hai. Do khóa công cộng thứ hai và khóa riêng thứ hai là các khóa được tạo ra bởi đầu cuối dựa trên PUF, và chỉ đầu cuối lưu trữ khóa riêng thứ hai, nên khó giả mạo khóa riêng

thứ hai, và tính bảo mật truyền của cặp khóa có thể được cải thiện một cách hiệu quả.

Theo biện pháp thực thi, sau khi đầu cuối nhận cặp khóa được mã hóa được gửi bởi thiết bị mạng thứ nhất, phương pháp này còn gồm có:

Đầu cuối lưu trữ khóa riêng thứ nhất, và mã hóa khóa riêng thứ nhất đã lưu trữ bằng cách sử dụng khóa công cộng thứ hai.

Khóa riêng thứ nhất được sử dụng để ký gói tiếp theo cần được gửi bởi đầu cuối, và khóa riêng thứ nhất đã lưu trữ được mã hóa bằng cách sử dụng khóa công cộng thứ hai, nên tính bảo mật lưu trữ của khóa riêng thứ nhất có thể được bảo đảm một cách hiệu quả.

Fig.8 là lưu đồ giản lược của phương tháp thu ID thiết bị 800 khác nữa theo phương án của sáng chế. Kiến trúc mạng mà phương pháp 800 được áp dụng gồm có ít nhất đầu cuối và thiết bị mạng thứ nhất. Chẳng hạn, đầu cuối có thể là đầu cuối 101 trong kiến trúc mạng được thể hiện trên Fig.1, và thiết bị mạng thứ nhất có thể là thiết bị mạng 108 trong kiến trúc mạng được thể hiện trên Fig.1. Hệ thống quản lý thiết bị và/hoặc hệ thống quản lý ID được triển khai trong thiết bị mạng thứ nhất. Kiến trúc mạng có thể là kiến trúc mạng được thể hiện trên Fig.1. Phương pháp 800 gồm có các hoạt động sau đây.

S801. Thiết bị mạng thứ nhất nhận thông báo thứ nhất được gửi bởi đầu cuối và được sử dụng để yêu cầu ID thiết bị cho đầu cuối, trong đó ID thiết bị được sử dụng để nhận dạng toàn cầu đầu cuối theo cách duy nhất.

Thông báo thứ nhất có thể là thông báo TCP, hoặc có thể là thông báo UDP. Đối với thông báo thứ nhất, có thể nhận dạng được, bằng cách sử dụng loại thông báo hoặc bit tương ứng, rằng thông báo thứ nhất được sử dụng để yêu cầu ID thiết bị.

S802. Thiết bị mạng thứ nhất gửi cặp khóa được mã hóa đến đầu cuối, trong đó cặp khóa này gồm có khóa công cộng thứ nhất và khóa riêng thứ nhất.

Đối với phương pháp mã hóa cặp khóa bởi thiết bị mạng thứ nhất, tham khảo các phần mô tả liên quan của bước mã hóa cặp khóa 2 bởi thiết bị mạng 1 trong S206 trong phương pháp 200. Các chi tiết không được mô tả lại ở đây.

S803. Thiết bị mạng thứ nhất gửi thông tin thứ nhất đến đầu cuối, trong đó thông tin thứ nhất được sử dụng để nhận dạng rằng khóa công cộng thứ nhất là ID thiết bị của đầu cuối.

Thông tin thứ nhất có thể là loại thông báo, hoặc có thể là bit tương ứng trong thông báo.

Cặp khóa được gửi trong S802 và thông tin thứ nhất được gửi trong S803 có thể được mang trong thông báo giống nhau, hoặc có thể được mang trong các thông báo khác nhau. Khi cặp khóa và thông tin được mang trong thông báo giống nhau, S802 và S803 có thể được hiểu là được hoàn thành bởi hoạt động giống nhau. Khi cặp khóa và thông tin được mang trong các thông báo khác nhau, S803 có thể được thực hiện trước, sau, hoặc đồng thời với S802.

Khóa riêng thứ nhất được sử dụng bởi đầu cuối để ký thông báo thứ hai được gửi bởi thiết bị mạng thứ nhất, và thông báo thứ hai mang khóa công cộng thứ nhất được sử dụng làm ID thiết bị của đầu cuối.

Theo biện pháp thực thi cụ thể, hệ thống quản lý thiết bị được triển khai trong thiết bị mạng thứ nhất. Thông báo thứ hai có thể được sử dụng để xác nhận, từ hệ thống quản lý thiết bị được triển khai trong thiết bị mạng thứ nhất, rằng đầu cuối được đăng ký thành công. Thông báo thứ hai có thể còn được sử dụng để báo cáo ID thiết bị, nghĩa là, thông tin như khóa công cộng thứ nhất, thông tin trạng thái thiết bị, thông tin vị trí thiết bị, và/hoặc loại thiết bị, đến thiết bị mạng thứ nhất. Cụ thể là, hoạt động cần được thực hiện bằng cách sử dụng thông báo thứ hai có thể được nhận dạng bằng cách sử dụng loại thông báo trong thông báo thứ hai hoặc bit tương ứng trong thông báo thứ hai. Thông báo thứ hai có thể mang khóa công cộng thứ nhất được sử dụng làm ID thiết bị. Sau khi nhận thông báo thứ hai, thiết bị mạng thứ nhất có thể xác minh chữ ký của thông báo thứ hai bằng cách sử dụng khóa công cộng thứ nhất, để thực hiện tiếp việc xác minh mã nhận dạng trên đầu cuối.

Theo biện pháp thực thi, thông báo thứ nhất mang khóa công cộng thứ hai, và khóa công cộng thứ hai là khóa công cộng được tạo ra bởi đầu cuối dựa trên chức năng không thể có bản sao vật lý PUF.

Trước khi gửi thông tin thứ nhất đến thiết bị mạng thứ nhất, chẳng hạn, trong pha phân phối của đầu cuối, đầu cuối tạo ra khóa công cộng thứ hai và khóa riêng thứ hai dựa trên PUF. Nhà quản trị mạng hoặc hệ thống quản lý mạng có thể tạo cấu hình trước khóa công cộng thứ hai trong thiết bị mạng trong đó hệ thống quản lý ID được triển khai. Theo cách khác, đầu cuối gửi khóa công cộng thứ hai đến CA, và

CA phát hành chứng nhận, và trả lại chứng nhận khóa công cộng đã được phát hành đến đầu cuối. CA phát hành chứng nhận, nên khóa công cộng thứ hai không cần được triển khai trong thiết bị mạng trước. Điều này đơn giản hóa quá trình tạo cấu hình. Việc thông báo thứ nhất mang khóa công cộng thứ hai gồm có: Thông báo thứ nhất trực tiếp mang khóa công cộng thứ hai; hoặc thông báo thứ nhất mang chứng nhận khóa công cộng được phát hành bởi CA, trong đó chứng nhận khóa công cộng mang khóa công cộng thứ hai. Khi yêu cầu thu ID thiết bị, đầu cuối bổ sung khóa công cộng thứ hai vào thông báo thứ nhất.

Theo biện pháp thực thi cụ thể, hệ thống quản lý ID được triển khai trong thiết bị mạng thứ nhất. Sau khi tạo ra khóa công cộng thứ hai, đầu cuối có thể tạo cấu hình khóa công cộng thứ hai cho thiết bị mạng thứ nhất bằng cách sử dụng nhà quản trị mạng hoặc hệ thống quản lý mạng. Khi yêu cầu thu ID thiết bị, đầu cuối bổ sung khóa công cộng thứ hai vào thông báo thứ nhất. Sau khi nhận thông báo thứ nhất, thiết bị mạng thứ nhất thực hiện việc xác minh mã nhận dạng trên đầu cuối dựa trên khóa công cộng thứ hai được mang trong thông báo thứ hai và khóa công cộng thứ hai được lưu trữ trong thiết bị mạng thứ nhất. Nếu xác định rằng khóa công cộng thứ hai được mang trong thông báo thứ ba giống như khóa công cộng thứ hai được lưu trữ trong thiết bị mạng thứ nhất, thiết bị mạng thứ nhất xác định rằng đầu cuối thành công trong việc xác minh mã nhận dạng.

Theo biện pháp thực thi cụ thể khác, hệ thống quản lý thiết bị được triển khai trong thiết bị mạng thứ nhất, và không có hệ thống quản lý ID được triển khai trong thiết bị mạng thứ nhất. Sau khi thiết bị mạng thứ nhất nhận thông báo thứ nhất, và trước khi thiết bị mạng thứ nhất gửi cặp khóa được mã hóa đến đầu cuối, phương pháp này còn gồm có các bước:

Thiết bị mạng thứ nhất tạo ra thông báo thứ ba, trong đó thông báo thứ ba mang khóa công cộng thứ hai, và khóa công cộng thứ hai được sử dụng bởi thiết bị mạng thứ hai để thực hiện việc xác minh mã nhận dạng trên đầu cuối.

Thiết bị mạng thứ nhất gửi thông báo thứ ba đến thiết bị mạng thứ hai, trong đó thông báo thứ ba mang khóa công cộng thứ hai, và khóa công cộng thứ hai được sử dụng bởi thiết bị mạng thứ hai để thực hiện việc xác minh mã nhận dạng trên đầu cuối.

Thiết bị mạng thứ nhất nhận cặp khóa và thông tin thứ hai được gửi bởi thiết bị mạng thứ hai, trong đó thông tin thứ hai được sử dụng để chỉ báo rằng khóa công cộng thứ nhất được chứa trong cặp khóa là ID thiết bị.

Hệ thống quản lý ID được triển khai trong thiết bị mạng thứ hai. Sau khi tạo ra khóa công cộng thứ hai, đầu cuối có thể tạo cấu hình khóa công cộng thứ hai cho thiết bị mạng thứ hai bằng cách sử dụng nhà quản trị mạng hoặc hệ thống quản lý mạng. Khi yêu cầu thu ID thiết bị, đầu cuối bổ sung khóa công cộng thứ hai vào thông báo thứ nhất. Sau khi nhận thông báo thứ nhất, thiết bị mạng thứ nhất tạo ra thông báo thứ ba, và gửi thông báo thứ ba đến thiết bị mạng thứ hai. Thiết bị mạng thứ hai nhận thông báo thứ ba, và thực hiện việc xác minh mã nhận dạng trên đầu cuối dựa trên khóa công cộng thứ hai được mang trong thông báo thứ ba và khóa công cộng thứ hai được lưu trữ trong thiết bị mạng thứ hai. Nếu xác định rằng khóa công cộng thứ hai được mang trong thông báo thứ ba giống như khóa công cộng thứ hai được lưu trữ trong thiết bị mạng thứ hai, thiết bị mạng thứ hai xác định rằng đầu cuối thành công trong việc xác minh mã nhận dạng.

Theo biện pháp thực thi, bước thiết bị mạng thứ nhất gửi cặp khóa được mã hóa đến đầu cuối gồm có bước: Thiết bị mạng thứ nhất gửi, đến đầu cuối, cặp khóa được mã hóa bằng cách sử dụng khóa công cộng thứ hai.

Theo phương pháp được đề xuất theo các phương án của sáng chế, cặp khóa được tạo ra, và khóa công cộng trong cặp khóa được sử dụng làm ID thiết bị, nên tính duy nhất của ID thiết bị có thể được bảo đảm một cách hiệu quả, và đặc biệt là trong kịch bản với nhiều thiết bị mạng lưới vạn vật kết nối Internet, có thể tránh được một cách hiệu quả vấn đề khó quản lý do sự lặp lại ID thiết bị. Hơn nữa, thông tin được gửi bởi đầu cuối được ký bằng cách sử dụng khóa riêng trong cặp khóa công cộng, nên không cần tạo cấu hình trước ủy nhiệm xác thực hoặc dàn xếp khóa bổ sung trong khi truyền thông. Vì vậy, trong kịch bản với nhiều đầu cuối, các mức bổ sung cần phải có để tạo cấu hình ủy nhiệm xác thực và dàn xếp khóa được giảm đáng kể, quá trình tạo cấu hình được đơn giản hóa đáng kể, và hiệu quả xử lý được cải thiện.

Phương tháp thu ID thiết bị được đề xuất theo các phương án của sáng chế trong bản mô tả này được mô tả ở trên dựa vào Fig.2 đến Fig.8. Đầu cuối và thiết bị

mạng tương ứng với các phương án phương pháp đã nêu ở trên được mô tả dưới đây dựa vào Fig.9 và Fig.10.

Fig.9 là sơ đồ giản lược của đầu cuối 900 theo phương án của sáng chế. Đầu cuối 900 có thể được áp dụng cho kiến trúc mạng được thể hiện trên Fig.1, chẳng hạn, có thể là đầu cuối 101 trong kiến trúc mạng được thể hiện trên Fig.1. Như được thể hiện trên Fig.9, đầu cuối 900 có thể gồm có bộ xử lý 910, bộ nhớ 920 được ghép cặp với bộ xử lý 910, và bộ thu phát 930. Bộ xử lý 910 có thể là bộ xử lý trung tâm (central processing unit, gọi tắt là CPU), bộ xử lý mạng (network processor, gọi tắt là NP), hoặc phối hợp của CPU và NP. Bộ xử lý có thể còn gồm có chip phần cứng. Chip phần cứng có thể là mạch tích hợp chuyên dụng (application-specific integrated circuit, gọi tắt là ASIC), thiết bị logic khả lập trình (programmable logic device, gọi tắt là PLD), hoặc phối hợp của chúng. PLD có thể là thiết bị logic khả lập trình phức hợp (complex programmable logic device, gọi tắt là CPLD), mảng cổng khả lập trình bằng trường (field-programmable gate array, gọi tắt là FPGA), logic mảng chung (generic array logic, gọi tắt là GAL), hoặc phối hợp bất kỳ của chúng. Bộ xử lý 910 có thể là một hoặc nhiều bộ xử lý. Bộ nhớ 920 có thể là bộ nhớ khả biến (volatile memory) như bộ nhớ truy nhập ngẫu nhiên (random-access memory, gọi tắt là RAM), hoặc có thể là bộ nhớ bất khả biến (non-volatile memory) như bộ nhớ chỉ đọc (read-only memory, gọi tắt là ROM), bộ nhớ tác động nhanh (flash memory), ổ đĩa cứng (hard disk drive, gọi tắt là HDD), hoặc ổ đĩa trạng thái rắn (solid-state drive, gọi tắt là SSD), hoặc có thể là phối hợp của các loại bộ nhớ đã nêu ở trên. Theo biện pháp thực thi, bộ nhớ 920 có thể gồm có nhiều môđun phần mềm, chẳng hạn, môđun gửi 921, môđun xử lý 922, và môđun nhận 923. Bằng cách thi hành lệnh trong môđun phần mềm đã nêu ở trên, bộ xử lý 910 có thể được tạo cấu hình để thực hiện nhiều hoạt động. Bộ nhớ 920 có thể là một hoặc nhiều bộ nhớ. Theo một số biện pháp thực thi, khi một môđun được tạo cấu hình để thực hiện một hoạt động, trên thực tế có thể chỉ báo rằng bộ xử lý 910 được tạo cấu hình để thi hành lệnh trong môđun để hoàn thành hoạt động đã nêu ở trên. Bằng cách thi hành lệnh trong bộ nhớ 920, bộ xử lý 910 có thể thực hiện một số hoặc tất cả các hoạt động được thực hiện bởi đầu cuối trong phương pháp 200, 300, 400, 500, 600, 700, hoặc 800. Chẳng hạn, bộ xử lý 910 có thể gửi, đến thiết bị mạng 1 bằng cách sử dụng bộ thu phát 930, thông báo 1 để

yêu cầu ID thiết bị, nhận, bằng cách sử dụng bộ thu phát 930, cặp khóa gồm có khóa công cộng 1 và khóa riêng 1 và thông tin mã nhận dạng mà khóa công cộng 1 là ID thiết bị, trong đó cặp khóa và thông tin được gửi bởi thiết bị mạng 1, và xác định, dựa trên cặp khóa nhận được và thông tin nhận được, rằng khóa công cộng 1 là ID thiết bị của đầu cuối.

Môđun gửi 921 được tạo cấu hình để gửi, đến thiết bị mạng, thông báo thứ nhất được sử dụng để yêu cầu ID thiết bị cho đầu cuối, trong đó ID thiết bị được sử dụng để nhận dạng toàn cầu đầu cuối theo cách duy nhất. Môđun nhận 923 được tạo cấu hình để: nhận cặp khóa được mã hóa được gửi bởi thiết bị mạng, trong đó cặp khóa này gồm có khóa công cộng thứ nhất và khóa riêng thứ nhất; và nhận thông tin được gửi bởi thiết bị mạng, trong đó thông tin này được sử dụng để nhận dạng rằng khóa công cộng thứ nhất là ID thiết bị của đầu cuối. Môđun xử lý 922 được tạo cấu hình để xác định rằng khóa công cộng thứ nhất là ID thiết bị.

Môđun gửi 921 còn được tạo cấu hình để gửi, đến thiết bị mạng, thông báo thứ hai được ký bằng cách sử dụng khóa riêng thứ nhất, trong đó thông báo thứ hai này mang khóa công cộng thứ nhất được sử dụng làm ID thiết bị của đầu cuối.

Theo biện pháp thực thi cụ thể, thông báo thứ nhất mang khóa công cộng thứ hai, và khóa công cộng thứ hai là khóa công cộng được tạo ra bởi đầu cuối dựa trên chức năng không thể có bản sao vật lý. Môđun nhận 923 còn được tạo cấu hình để nhận cặp khóa được gửi bởi thiết bị mạng và được mã hóa bằng cách sử dụng khóa công cộng thứ hai.

Fig.10 là sơ đồ giản lược của thiết bị mạng 1000 theo phương án của sáng chế. Thiết bị mạng 1000 có thể được áp dụng cho kiến trúc mạng được thể hiện trên Fig.1, chẳng hạn, có thể là thiết bị mạng 107 hoặc thiết bị mạng 108 trong kiến trúc mạng được thể hiện trên Fig.1. Như được thể hiện trên Fig.10, thiết bị mạng 1000 có thể gồm có bộ xử lý 1010, bộ nhớ 1020 được ghép cặp với bộ xử lý 1001, và bộ thu phát 1030. Bộ xử lý 1010 có thể là CPU, NP, hoặc phối hợp của CPU và NP. Bộ xử lý có thể còn gồm có chip phần cứng. Chip phần cứng có thể là ASIC, PLD, hoặc phối hợp của chúng. PLD có thể là CPLD, FPGA, GAL, hoặc phối hợp bất kỳ của chúng. Bộ xử lý 1010 có thể là một hoặc nhiều bộ xử lý. Bộ nhớ 1020 có thể là bộ nhớ khả biến (volatile memory) như RAM, hoặc có thể là bộ nhớ bất khả biến (non-volatile

memory) như ROM, bộ nhớ tác động nhanh (flash memory), HDD, hoặc SSD, hoặc có thể là phối hợp của các loại bộ nhớ đã nêu ở trên. Theo biện pháp thực thi, bộ nhớ 1020 có thể gồm có nhiều môđun phần mềm, chẳng hạn, môđun gửi 1021, môđun xử lý 1022, và môđun nhận 1023. Bằng cách thi hành lệnh trong môđun phần mềm đã nêu ở trên, bộ xử lý 1010 có thể được tạo cấu hình để thực hiện nhiều hoạt động. Bộ nhớ 1020 có thể là một hoặc nhiều bộ nhớ. Theo một số biện pháp thực thi, khi một môđun được tạo cấu hình để thực hiện một hoạt động, nó có thể chỉ báo rằng bộ xử lý 1010 được tạo cấu hình để thi hành lệnh trong môđun để hoàn thành hoạt động đã nêu ở trên. Theo biện pháp thực thi, bằng cách thi hành lệnh trong bộ nhớ 1020, bộ xử lý 1010 có thể thực hiện một số hoặc tất cả các hoạt động được thực hiện bởi thiết bị mạng 1 trong phương pháp 200, 300, 400, 500, hoặc 600 và một số hoặc tất cả các hoạt động được thực hiện bởi thiết bị mạng thứ nhất trong phương pháp 700 hoặc phương pháp 800. Chẳng hạn, bộ xử lý 1010 có thể nhận, bằng cách sử dụng bộ thu phát 1030, thông báo 1 mà dùng để yêu cầu ID thiết bị và được gửi bởi đầu cuối, và gửi, đến đầu cuối bằng cách sử dụng bộ thu phát 1030, cặp khóa gồm có khóa công cộng 1 và khóa riêng 1 và thông tin mã nhận dạng rằng khóa công cộng 1 là ID thiết bị.

Môđun nhận 1023 được tạo cấu hình để nhận thông báo thứ nhất được gửi bởi đầu cuối và được sử dụng để yêu cầu ID thiết bị cho đầu cuối, trong đó ID thiết bị được sử dụng để nhận dạng toàn cầu đầu cuối theo cách duy nhất. Môđun gửi 1021 được tạo cấu hình để gửi cặp khóa được mã hóa đến đầu cuối, trong đó cặp khóa này gồm có khóa công cộng thứ nhất và khóa riêng thứ nhất. Môđun gửi 1021 còn được tạo cấu hình để gửi thông tin thứ nhất đến đầu cuối, trong đó thông tin thứ nhất được sử dụng để nhận dạng rằng khóa công cộng thứ nhất là ID thiết bị của đầu cuối.

Theo biện pháp thực thi, môđun nhận 1023 còn được tạo cấu hình để nhận thông báo thứ hai được gửi bởi đầu cuối và được ký bằng cách sử dụng khóa riêng thứ nhất, trong đó thông báo thứ hai mang khóa công cộng thứ nhất được sử dụng làm ID thiết bị của đầu cuối.

Theo biện pháp thực thi, thông báo thứ nhất mang khóa công cộng thứ hai, và khóa công cộng thứ hai là khóa công cộng được tạo ra bởi đầu cuối dựa trên chức năng không thể có bản sao vật lý PUF.

Theo biện pháp thực thi, sau khi môđun nhận 1023 nhận thông báo thứ nhất, và trước khi môđun gửi 1021 gửi cặp khóa được mã hóa đến đầu cuối, môđun xử lý 1022 còn được tạo cấu hình để: tạo ra thông báo thứ ba, trong đó thông báo thứ ba mang khóa công cộng thứ hai, và khóa công cộng thứ hai được sử dụng bởi thiết bị mạng thứ hai để thực hiện việc xác minh mã nhận dạng trên đầu cuối; gửi thông báo thứ ba đến thiết bị mạng thứ hai; và nhận cặp khóa và thông tin thứ hai được gửi bởi thiết bị mạng thứ hai, trong đó thông tin thứ hai được sử dụng để chỉ báo rằng khóa công cộng thứ nhất được chứa trong cặp khóa là ID thiết bị.

Theo biện pháp thực thi, môđun xử lý 1022 còn được tạo cấu hình để gửi, đến đầu cuối, cặp khóa được mã hóa bằng cách sử dụng khóa công cộng thứ hai.

Theo biện pháp thực thi, thông báo thứ nhất mang chứng nhận khóa công cộng được phát hành bởi cơ sở chứng nhận CA, và chứng nhận khóa công cộng này mang khóa công cộng thứ hai.

Theo biện pháp thực thi, bằng cách thi hành lệnh trong bộ nhớ 1020, bộ xử lý 1010 có thể còn thực hiện tất cả hoặc một số hoạt động được thực hiện bởi thiết bị mạng 2 trong phương pháp 200, thiết bị mạng 2 trong phương pháp 400 hoặc phương pháp 500, và thiết bị mạng 1 trong phương pháp 600, hoặc tất cả các hoạt động được thực hiện bởi thiết bị mạng thứ hai trong phương pháp 800.

Theo các phương án của sáng chế, bộ thu phát có thể là bộ thu phát nối dây, bộ thu phát không dây, hoặc phối hợp của chúng. Bộ thu phát nối dây có thể là, chẳng hạn, giao diện Ethernet. Giao diện Ethernet có thể là giao diện quang, giao diện điện, hoặc phối hợp của chúng. Bộ thu phát không dây có thể là, chẳng hạn, bộ thu phát mạng vùng cục bộ không dây, bộ thu phát mạng chia ô, hoặc phối hợp của chúng. Giao diện bus có thể còn được chứa trong Fig.9 đến Fig.10, và giao diện bus có thể gồm có số lượng bất kỳ của các bus và các cầu nối được liên kết mạng. Cụ thể là, nhiều mạch khác nhau của một hoặc nhiều bộ xử lý được đại diện bởi bộ xử lý và các bộ nhớ được đại diện bởi bộ nhớ được liên kết với nhau. Giao diện bus có thể còn liên kết với các mạch khác nhau với nhau, chẳng hạn, thiết bị ngoại vi, bộ điều chỉnh điện thế, và mạch quản lý nguồn. Điều này đã được biết rõ trong lĩnh vực này, và vì vậy không được mô tả thêm nữa trong bản mô tả. Giao diện bus cung cấp giao diện. Bộ thu phát cung cấp bộ phận để truyền thông với nhiều thiết bị khác trên

phương tiện truyền. Bộ xử lý chịu trách nhiệm quản lý kiến trúc bus và xử lý thông thường. Bộ nhớ có thể lưu trữ dữ liệu được sử dụng khi bộ xử lý thực hiện hoạt động.

Sáng chế còn đề xuất hệ thống truyền thông, gồm có đầu cuối và thiết bị mạng. Đầu cuối có thể là đầu cuối được đề xuất trong phương án tương ứng với Fig.9. Thiết bị mạng có thể là thiết bị mạng được đề xuất trong phương án tương ứng với Fig.10. Hệ thống truyền thông được tạo cấu hình để thực hiện phương pháp theo bất kỳ một trong số các phương án trên Fig.2 đến Fig.8.

Người có kỹ năng trong lĩnh vực này có thể nhận thức được rằng, các bước (bước) khác nhau được liệt kê theo các phương án của sáng chế có thể được thực thi bằng cách sử dụng phần cứng điện tử, phần mềm máy tính, hoặc phối hợp của chúng. Việc các chức năng có được thực thi bằng cách sử dụng phần cứng hoặc phần mềm hay không phụ thuộc vào các ứng dụng cụ thể và yêu cầu thiết kế của toàn bộ hệ thống. Người có kỹ năng trong lĩnh vực này có thể sử dụng các phương pháp khác nhau để thực thi các chức năng đã được mô tả đối với mỗi ứng dụng cụ thể, nhưng không nên coi rằng biện pháp thực thi này vượt quá phạm vi của các phương án của sáng chế.

Các bước của các phương pháp hoặc các thuật toán được mô tả theo các phương án của sáng chế có thể được nhúng trực tiếp vào trong phần cứng, bộ phận phần mềm được thi hành bởi bộ xử lý, hoặc phối hợp của chúng. Bộ phận phần mềm có thể được lưu trữ trong bộ nhớ RAM, bộ nhớ tác động nhanh, bộ nhớ ROM, bộ nhớ EPROM, bộ nhớ EEPROM, bộ ghi, ổ đĩa cứng, ổ đĩa từ tháo lắp được, CD-ROM, hoặc phương tiện lưu trữ có dạng khác bất kỳ trong lĩnh vực kỹ thuật này. Chẳng hạn, phương tiện lưu trữ có thể được kết nối với bộ xử lý, nên bộ xử lý có thể đọc thông tin từ phương tiện lưu trữ và viết thông tin vào phương tiện lưu trữ. Phương tiện lưu trữ có thể còn được tích hợp vào trong bộ xử lý.

Cần phải hiểu rằng các số thứ tự của các quá trình đã nêu ở trên không có nghĩa là các trình tự thi hành theo các phương án khác nhau của sáng chế. Các trình tự thi hành của các quá trình nên được xác định theo các chức năng và logic bên trong của các quá trình này, và không nên tạo ra giới hạn bất kỳ lên các quy trình thực thi của các phương án của sáng chế.

Người có kỹ năng trung bình trong lĩnh vực này có thể nhận thức được rằng,

việc phối hợp với các ví dụ được mô tả theo các phương án được bộc lộ trong bản mô tả, các môđun và các hoạt động của phương pháp có thể được thực thi bằng phần cứng điện tử hoặc phối hợp của phần mềm máy tính và phần cứng điện tử. Việc các chức năng có được thực hiện bằng phần cứng hoặc phần mềm hay không phụ thuộc vào các ứng dụng cụ thể và các điều kiện ràng buộc về thiết kế của các giải pháp kỹ thuật. Người có kỹ năng trong lĩnh vực này có thể sử dụng các phương pháp khác để thực thi các chức năng đã được mô tả đối với các ứng dụng cụ thể.

Người có kỹ năng trong lĩnh vực này có thể hiểu rõ rằng, đối với mục đích mô tả thuận tiện và ngắn gọn, cho một quy trình làm việc chi tiết của hệ thống, thiết bị và môđun đã nêu ở trên, tham khảo quy trình tương ứng theo các phương án phương pháp đã nêu ở trên. Các chi tiết không được mô tả lại ở đây.

Tất cả hoặc một số phương án đã nêu ở trên có thể được thực thi bằng cách sử dụng phầm mềm, phần cứng, phần sụn, hoặc phối hợp bất kỳ của chúng. Khi phần mềm được sử dụng để thực thi các phương án, tất cả hoặc một số phương án có thể được thực thi ở dạng sản phẩm chương trình máy tính. Sản phẩm chương trình máy tính gồm có một hoặc nhiều lệnh máy tính. Khi các lệnh chương trình máy tính được nạp và thi hành trên máy tính, tất cả hoặc một số thủ tục hoặc chức năng theo các phương án của sáng chế được tạo ra. Máy tính có thể là máy tính đa năng, máy tính chuyên dụng, mạng máy tính, hoặc các máy khả lập trình khác. Các lệnh máy tính có thể được lưu trữ trong phương tiện lưu trữ đọc được bằng máy tính hoặc có thể được truyền từ một phương tiện lưu trữ đọc được bằng máy tính đến phương tiện lưu trữ đọc được bằng máy tính khác. Chẳng hạn, các lệnh máy tính có thể được truyền từ một trang mạng, máy tính, máy chủ, hoặc trung tâm dữ liệu đến trang mạng, máy tính, máy chủ, hoặc trung tâm dữ liệu khác theo cách được nối dây (chẳng hạn, cáp đồng trục, sợi quang, hoặc đường dây thuê bao dạng số (digital subscriber line, DSL)) hoặc không dây (chẳng hạn, hồng ngoại, vô tuyến, hoặc vi ba). Phương tiện lưu trữ đọc được bằng máy tính có thể là phương tiện khả dụng bất kỳ có thể truy nhập bởi máy tính, hoặc thiết bị lưu trữ dữ liệu, như máy chủ hoặc trung tâm dữ liệu, tích hợp một hoặc nhiều phương tiện khả dụng. Phương tiện khả dụng có thể là phương tiện có từ tính (chẳng hạn, đĩa mềm, đĩa cứng, hoặc băng từ), phương tiện quang (chẳng hạn, DVD), hoặc phương tiện bán dẫn (chẳng hạn, đĩa trạng thái rắn (Solid State

Disk, SSD)), hoặc tương tự.

Tất cả các phần trong bản mô tả này được mô tả theo cách tăng dần lên. Các phần giống nhau hoặc tương tự theo các biện pháp thực thi có thể được tham chiếu lẫn nhau. Mỗi biện pháp thực thi tập trung vào sự phác biệt với biện pháp thực thi khác. Đặc biệt là, các phương án về máy và hệ thống về cơ bản là tương tự như phương án về phương pháp, và vì vậy được mô tả ngắn gọn. Đối với các phần liên quan, tham khảo các phần mô tả tương ứng trong phương án về phương pháp.

Theo phần mô tả đã nêu ở trên của bản mô tả trong sáng chế, các công nghệ trong lĩnh vực kỹ thuật này có thể sử dụng hoặc thực thi nội dung của sáng chế. Biến thể bất kỳ dựa trên nội dung đã được bộc lộ sẽ được coi là hiển nhiên trong lĩnh vực kỹ thuật này. Các nguyên lý cơ bản được mô tả trong sáng chế có thể được áp dụng cho các biến thể khác mà không đi trệch khỏi bản chất và phạm vi của sáng chế. Vì vậy, nội dung được bộc lộ trong sáng chế không bị giới hạn ở các phương án và các thiết kế đã được mô tả nhưng có thể còn được mở rộng đến phạm vi tối đa phù hợp với các nguyên lý và các dấu hiệu mới đã được bộc lộ của sáng chế. Các phần mô tả đã nêu ở trên đơn thuần là các biện pháp thực thi cụ thể của sáng chế, nhưng không được dự định để giới hạn phạm vi bảo hộ của sáng chế. Dạng biến thể hoặc thay thế bất kỳ dễ dàng được luận ra bởi người có kỹ năng trong lĩnh vực này trong phạm vi kỹ thuật được bộc lộ trong sáng chế sẽ nằm trong phạm vi bảo hộ của sáng chế. Do đó, phạm vi bảo hộ của sáng chế sẽ tuân theo phạm vi bảo hộ của các điểm yêu cầu bảo hộ.

YÊU CẦU BẢO HỘ

1. Phương tháp thu ký hiệu nhận dạng (identifier, ID) thiết bị, phương pháp này bao gồm các bước:

gửi, bởi đầu cuối đến thiết bị mạng, thông báo thứ nhất được sử dụng để yêu cầu ID thiết bị cho đầu cuối, trong đó ID thiết bị được sử dụng để nhận dạng toàn cầu đầu cuối theo cách duy nhất;

nhận, bởi đầu cuối, cặp khóa được mã hóa được gửi bởi thiết bị mạng, trong đó cặp khóa này bao gồm khóa công cộng thứ nhất và khóa riêng thứ nhất;

nhận, bởi đầu cuối, thông tin được gửi bởi thiết bị mạng, trong đó thông tin này được sử dụng để nhận dạng rằng khóa công cộng thứ nhất là ID thiết bị của đầu cuối; và

xác định, bởi đầu cuối, rằng khóa công cộng thứ nhất là ID thiết bị.

2. Phương pháp theo điểm 1, trong đó phương pháp này còn bao gồm bước:

gửi, bởi đầu cuối đến thiết bị mạng, thông báo thứ hai được ký bằng cách sử dụng khóa riêng thứ nhất, trong đó thông báo thứ hai này mang khóa công cộng thứ nhất được sử dụng làm ID thiết bị của đầu cuối.

3. Phương pháp theo điểm 1 hoặc 2, trong đó thông báo thứ nhất mang khóa công cộng thứ hai, và khóa công cộng thứ hai này là khóa công cộng được tạo ra bởi đầu cuối dựa trên chức năng không thể có bản sao vật lý.

4. Phương pháp theo điểm 3, trong đó:

bước nhận, bởi đầu cuối, cặp khóa được mã hóa được gửi bởi thiết bị mạng bao gồm bước:

nhận, bởi đầu cuối, cặp khóa được gửi bởi thiết bị mạng và được mã hóa bằng cách sử dụng khóa công cộng thứ hai.

5. Phương pháp theo điểm 3, trong đó sau bước nhận, bởi đầu cuối, cặp khóa được mã hóa được gửi bởi thiết bị mạng, phương pháp này còn bao gồm bước:

lưu trữ, bởi đầu cuối, khóa riêng thứ nhất, và mã hóa khóa riêng thứ nhất đã lưu trữ bằng cách sử dụng khóa công cộng thứ hai.

6. Phương pháp theo điểm 3, trong đó:

thông báo thứ nhất mang chứng nhận khóa công cộng được phát hành bởi cơ sở chứng nhận (certificate authority, CA), và chứng nhận khóa công cộng này mang khóa công cộng thứ hai.

7. Phương tháp thu ký hiệu nhận dạng (ID) thiết bị, phương pháp này bao gồm các bước:

nhận, bởi thiết bị mạng thứ nhất, thông báo thứ nhất được gửi bởi đầu cuối và được sử dụng để yêu cầu ID thiết bị cho đầu cuối, trong đó ID thiết bị được sử dụng để nhận dạng toàn cầu đầu cuối theo cách duy nhất;

gửi, bởi thiết bị mạng thứ nhất, cặp khóa được mã hóa đến đầu cuối, trong đó cặp khóa này bao gồm khóa công cộng thứ nhất và khóa riêng thứ nhất; và

gửi, bởi thiết bị mạng thứ nhất, thông tin thứ nhất đến đầu cuối, trong đó thông tin thứ nhất này được sử dụng để nhận dạng rằng khóa công cộng thứ nhất là ID thiết bị của đầu cuối.

8. Phương pháp theo điểm 7, trong đó phương pháp này còn bao gồm bước:

nhận, bởi thiết bị mạng thứ nhất, thông báo thứ hai được gửi bởi đầu cuối và được ký bằng cách sử dụng khóa riêng thứ nhất, trong đó thông báo thứ hai mang khóa công cộng thứ nhất được sử dụng làm ID thiết bị của đầu cuối.

9. Phương pháp theo điểm 7 hoặc 8, trong đó thông báo thứ nhất mang khóa công cộng thứ hai, và khóa công cộng thứ hai này là khóa công cộng được tạo ra bởi đầu cuối dựa trên chức năng không thể có bản sao vật lý (physical unclonable function, PUF).

10. Phương pháp theo điểm 9, trong đó sau bước nhận, bởi thiết bị mạng thứ nhất, thông báo thứ nhất, và trước bước gửi, bởi thiết bị mạng thứ nhất, cặp khóa được mã

hóa đến đầu cuối, phương pháp này còn bao gồm các bước:

tạo ra, bởi thiết bị mạng thứ nhất, thông báo thứ ba, trong đó thông báo thứ ba mang khóa công cộng thứ hai, và khóa công cộng thứ hai này được sử dụng bởi thiết bị mạng thứ hai để thực hiện việc xác minh mã nhận dạng trên đầu cuối;

gửi, bởi thiết bị mạng thứ nhất, thông báo thứ ba đến thiết bị mạng thứ hai; và

nhận, bởi thiết bị mạng thứ nhất, cặp khóa và thông tin thứ hai được gửi bởi thiết bị mạng thứ hai, trong đó thông tin thứ hai này được sử dụng để chỉ báo rằng khóa công cộng thứ nhất được bao gồm trong cặp khóa là ID thiết bị.

11. Phương pháp theo điểm 9, trong đó bước gửi, bởi thiết bị mạng thứ nhất, cặp khóa được mã hóa đến đầu cuối bao gồm bước:

gửi, bởi thiết bị mạng thứ nhất đến đầu cuối, cặp khóa được mã hóa bằng cách sử dụng khóa công cộng thứ hai.

12. Phương pháp theo điểm 9, trong đó:

thông báo thứ nhất mang chứng nhận khóa công cộng được phát hành bởi cơ sở chứng nhận CA, và chứng nhận khóa công cộng này mang khóa công cộng thứ hai.

13. Đầu cuối, đầu cuối này bao gồm:

bộ nhớ, trong đó bộ nhớ này bao gồm các lệnh; và

bộ xử lý truyền thông với bộ nhớ, trong đó bộ xử lý này được tạo cấu hình để thi hành các lệnh để thực hiện các hoạt động sau đây:

gửi, đến thiết bị mạng, thông báo thứ nhất được sử dụng để yêu cầu ID thiết bị cho đầu cuối, trong đó ID thiết bị được sử dụng để nhận dạng toàn cầu đầu cuối theo cách duy nhất;

nhận cặp khóa được mã hóa được gửi bởi thiết bị mạng, trong đó cặp khóa này bao gồm khóa công cộng thứ nhất và khóa riêng thứ nhất;

nhận thông tin được gửi bởi thiết bị mạng, trong đó thông tin này được sử dụng để nhận dạng rằng khóa công cộng thứ nhất là ID thiết bị của đầu cuối; và

xác định rằng khóa công cộng thứ nhất là ID thiết bị.

14. Đầu cuối theo điểm 13, trong đó bộ xử lý còn được tạo cấu hình để thi hành các lệnh để thực hiện hoạt động sau đây:

gửi, đến thiết bị mạng, thông báo thứ hai được ký bằng cách sử dụng khóa riêng thứ nhất, trong đó thông báo thứ hai này mang khóa công cộng thứ nhất được sử dụng làm ID thiết bị của đầu cuối.

15. Đầu cuối theo điểm 13 hoặc 14, trong đó thông báo thứ nhất mang khóa công cộng thứ hai, và khóa công cộng thứ hai này là khóa công cộng được tạo ra bởi đầu cuối dựa trên chức năng không thể có bản sao vật lý.

16. Đầu cuối theo điểm 15, trong đó bộ xử lý còn được tạo cấu hình để thi hành các lệnh để thực hiện hoạt động sau đây:

nhận cặp khóa được gửi bởi thiết bị mạng và được mã hóa bằng cách sử dụng khóa công cộng thứ hai.

17. Đầu cuối theo điểm 15, trong đó bộ xử lý còn được tạo cấu hình để thi hành các lệnh để thực hiện các hoạt động sau đây:

lưu trữ khóa riêng thứ nhất, và mã hóa khóa riêng thứ nhất đã lưu trữ bằng cách sử dụng khóa công cộng thứ hai.

18. Đầu cuối theo điểm 15, trong đó thông báo thứ nhất mang chứng nhận khóa công cộng được phát hành bởi cơ sở chứng nhận (CA), và chứng nhận khóa công cộng mang khóa công cộng thứ hai.

19. Thiết bị mạng được sử dụng làm thiết bị mạng thứ nhất, thiết bị này bao gồm:

bộ nhớ, trong đó bộ nhớ này bao gồm các lệnh; và

bộ xử lý truyền thông với bộ nhớ, trong đó bộ xử lý này được tạo cấu hình để thi hành các lệnh để thực hiện các hoạt động sau đây:

nhận thông báo thứ nhất được gửi bởi đầu cuối và được sử dụng để yêu cầu ID thiết bị cho đầu cuối, trong đó ID thiết bị được sử dụng để nhận dạng toàn cầu

đầu cuối theo cách duy nhất;

gửi cặp khóa được mã hóa đến đầu cuối, trong đó cặp khóa này bao gồm khóa công cộng thứ nhất và khóa riêng thứ nhất; và

gửi thông tin thứ nhất đến đầu cuối, trong đó thông tin thứ nhất này được sử dụng để nhận dạng rằng khóa công cộng thứ nhất là ID thiết bị của đầu cuối.

20. Thiết bị mạng theo điểm 19, trong đó bộ xử lý còn được tạo cấu hình để thi hành các lệnh để thực hiện hoạt động sau đây:

nhận thông báo thứ hai được gửi bởi đầu cuối và được ký bằng cách sử dụng khóa riêng thứ nhất, trong đó thông báo thứ hai này mang khóa công cộng thứ nhất được sử dụng làm ID thiết bị của đầu cuối.

21. Thiết bị mạng theo điểm 19 hoặc 20, trong đó thông báo thứ nhất mang khóa công cộng thứ hai, và khóa công cộng thứ hai này là khóa công cộng được tạo ra bởi đầu cuối dựa trên chức năng không thể có bản sao vật lý (PUF).

22. Thiết bị mạng theo điểm 21, trong đó sau khi bộ xử lý nhận thông báo thứ nhất, và trước khi bộ xử lý gửi cặp khóa được mã hóa đến đầu cuối, bộ xử lý còn được tạo cấu hình để thi hành các lệnh để thực hiện các hoạt động sau đây:

tạo ra thông báo thứ ba, trong đó thông báo thứ ba mang khóa công cộng thứ hai, và khóa công cộng thứ hai này được sử dụng bởi thiết bị mạng thứ hai để thực hiện việc xác minh mã nhận dạng trên đầu cuối;

gửi thông báo thứ ba đến thiết bị mạng thứ hai; và

nhận cặp khóa và thông tin thứ hai được gửi bởi thiết bị mạng thứ hai, trong đó thông tin thứ hai này được sử dụng để chỉ báo rằng khóa công cộng thứ nhất được bao gồm trong cặp khóa là ID thiết bị.

23. Thiết bị mạng theo điểm 21, trong đó bộ xử lý còn được tạo cấu hình để thi hành các lệnh để thực hiện hoạt động sau đây:

gửi, đến đầu cuối, cặp khóa được mã hóa bằng cách sử dụng khóa công cộng thứ hai.

24. Thiết bị mạng theo điểm 21, trong đó:

thông báo thứ nhất mang chứng nhận khóa công cộng được phát hành bởi cơ sở chứng nhận CA, và chứng nhận khóa công cộng này mang khóa công cộng thứ hai.

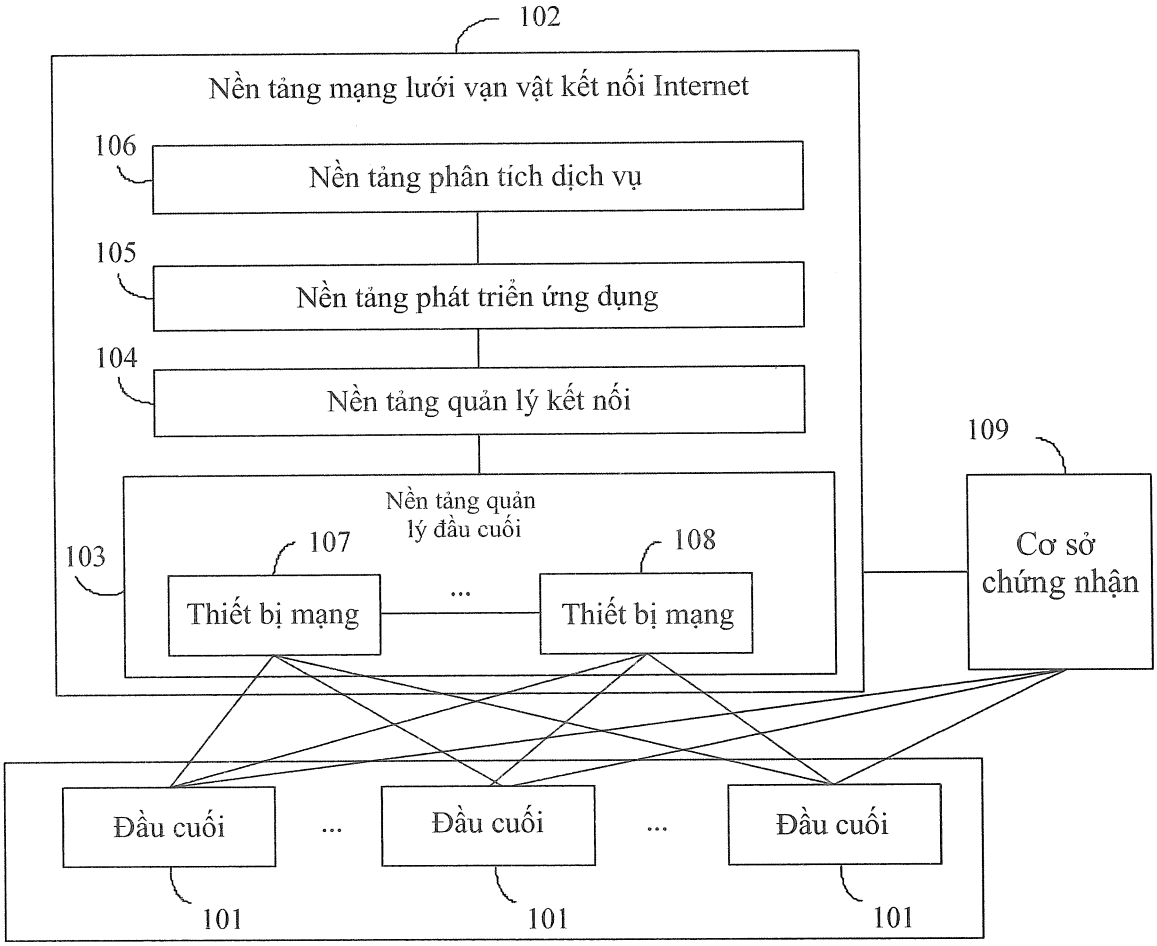
102
Nền tảng mạng lưới vạn vật kết nối Internet
106
Nền tảng phân tích dịch vụ
105
Nền tảng phát triển ứng dụng
104
Nền tảng quản lý kết nối
Nền tảng quản lý đầu cuối
103
107
108
Thiết bị mạng
...
Thiết bị mạng
109
Cơ sở chứng nhận
Đầu cuối
...
Đầu cuối
...
Đầu cuối
101
101
101

Fig.1

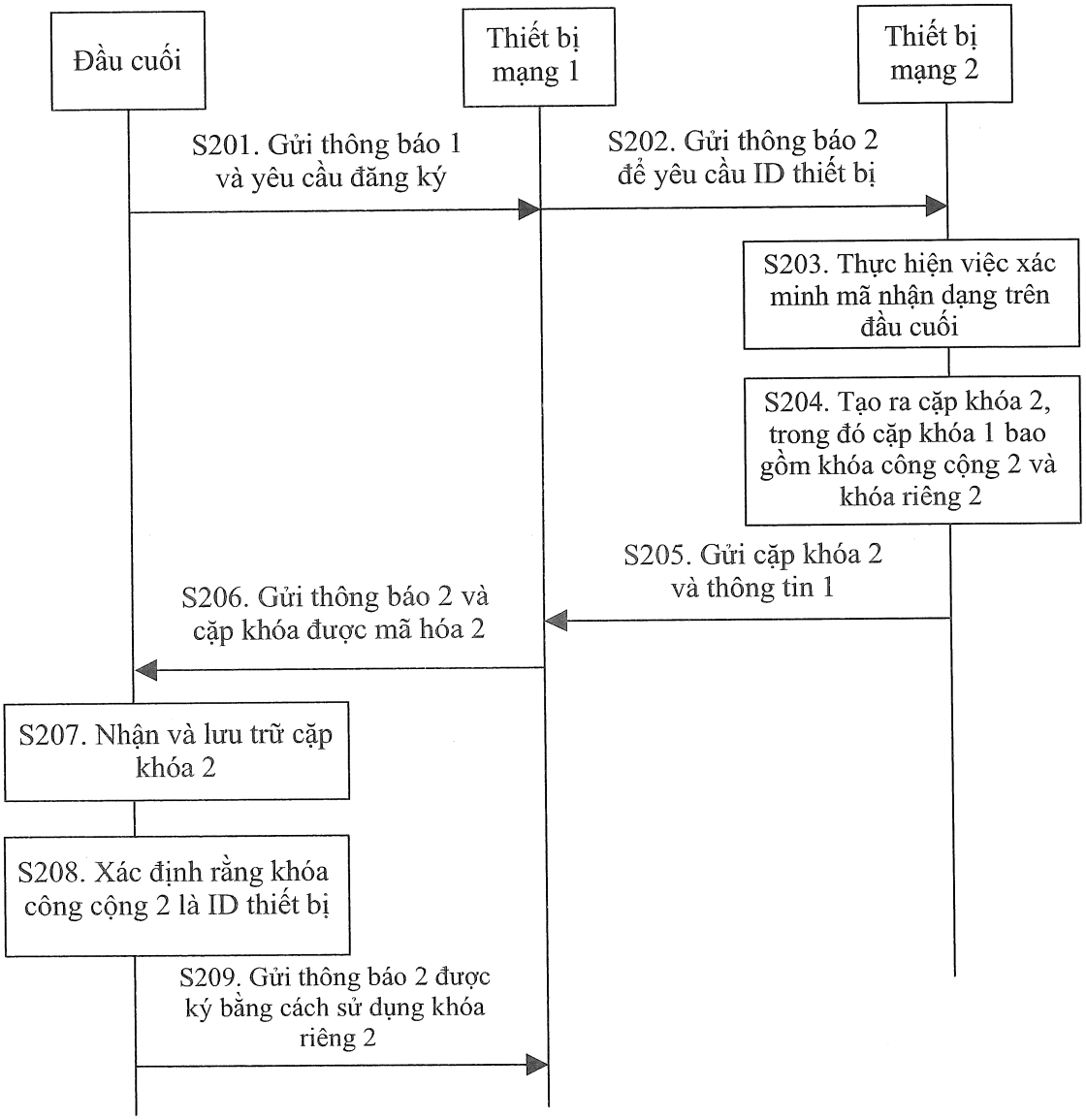
Đầu cuối
Thiết bị mạng 1
Thiết bị mạng 2
S201. Gửi thông báo 1 và yêu cầu đăng ký
S202. Gửi thông báo 2 để yêu cầu ID thiết bị
S203. Thực hiện việc xác minh mã nhận dạng trên đầu cuối
S204. Tạo ra cặp khóa 2, trong đó cặp khóa 1 bao gồm khóa công cộng 2 và khóa riêng 2
S205. Gửi cặp khóa 2 và thông tin 1
S206. Gửi thông báo 2 và cặp khóa được mã hóa 2
S207. Nhận và lưu trữ cặp khóa 2
S208. Xác định rằng khóa công cộng 2 là ID thiết bị
S209. Gửi thông báo 2 được ký bằng cách sử dụng khóa riêng 2

Fig.2

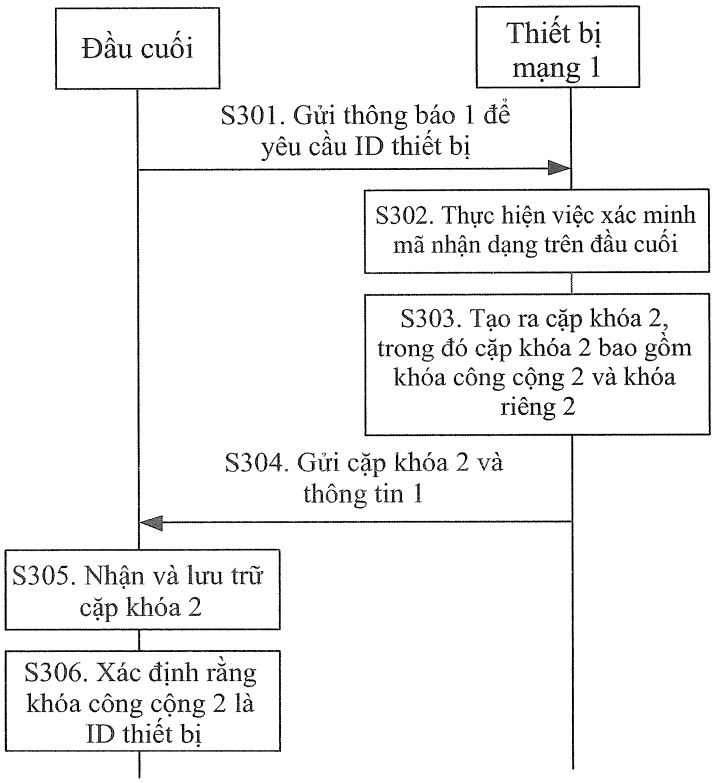
Đầu cuối
Thiết bị mạng 1
S301. Gửi thông báo 1 để yêu cầu ID thiết bị
S302. Thực hiện việc xác minh mã nhận dạng trên đầu cuối
S303. Tạo ra cặp khóa 2, trong đó cặp khóa 2 bao gồm khóa công cộng 2 và khóa riêng 2
S304. Gửi cặp khóa 2 và thông tin 1
S305. Nhận và lưu trữ cặp khóa 2
S306. Xác định rằng khóa công cộng 2 là ID thiết bị

Fig.3

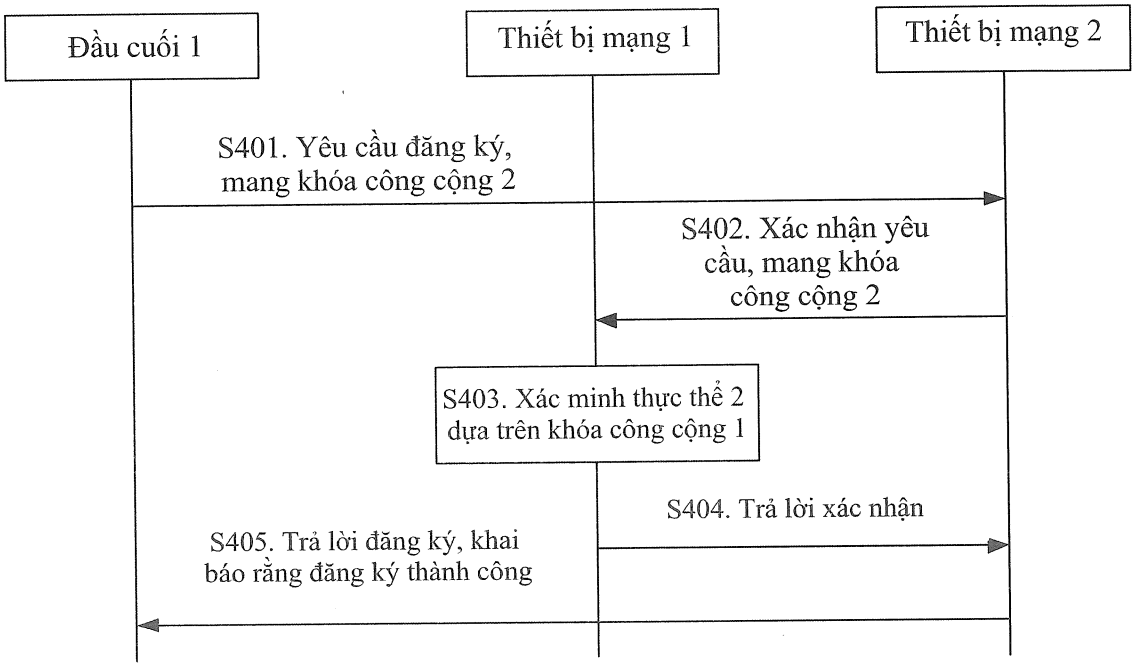
Đầu cuối 1
Thiết bị mạng 1
Thiết bị mạng 2
S401. Yêu cầu đăng ký, mang khóa công cộng 2
S402. Xác nhận yêu cầu, mang khóa công cộng 2
S403. Xác minh thực thể 2 dựa trên khóa công cộng 1
S404. Trả lời xác nhận
S405. Trả lời đăng ký, khai báo rằng đăng ký thành công

Fig.4

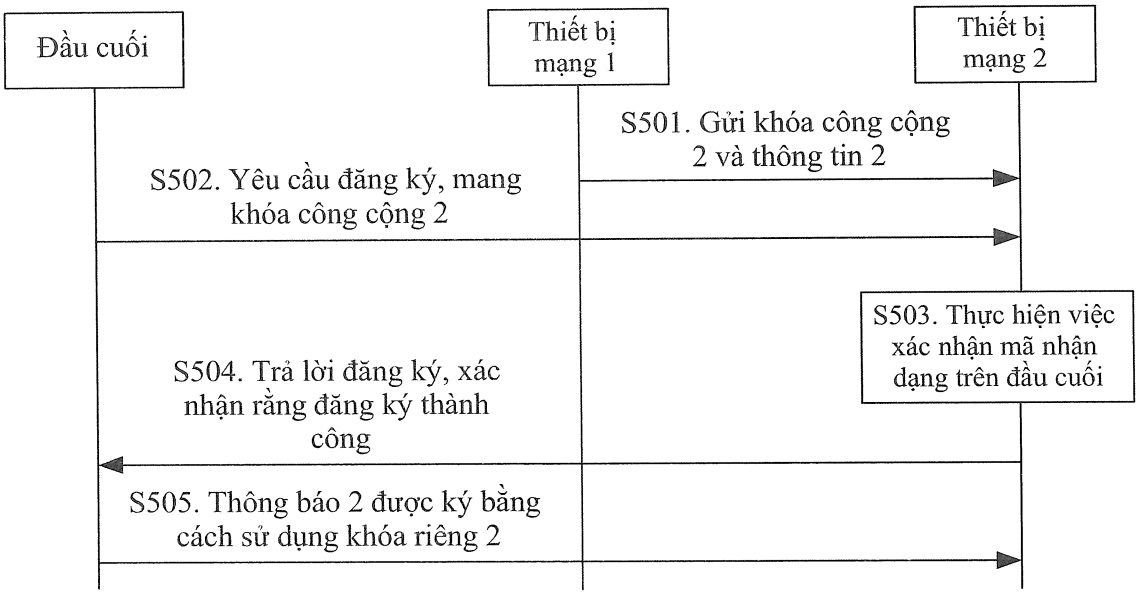
Đầu cuối
Thiết bị mạng 1
Thiết bị mạng 2
S501. Gửi khóa công cộng 2 và thông tin 2
S502. Yêu cầu đăng ký, mang khóa công cộng 2
S503. Thực hiện việc xác nhận mã nhận dạng trên đầu cuối
S504. Trả lời đăng ký, xác nhận rằng đăng ký thành công
S505. Thông báo 2 được ký bằng cách sử dụng khóa riêng 2

Fig.5

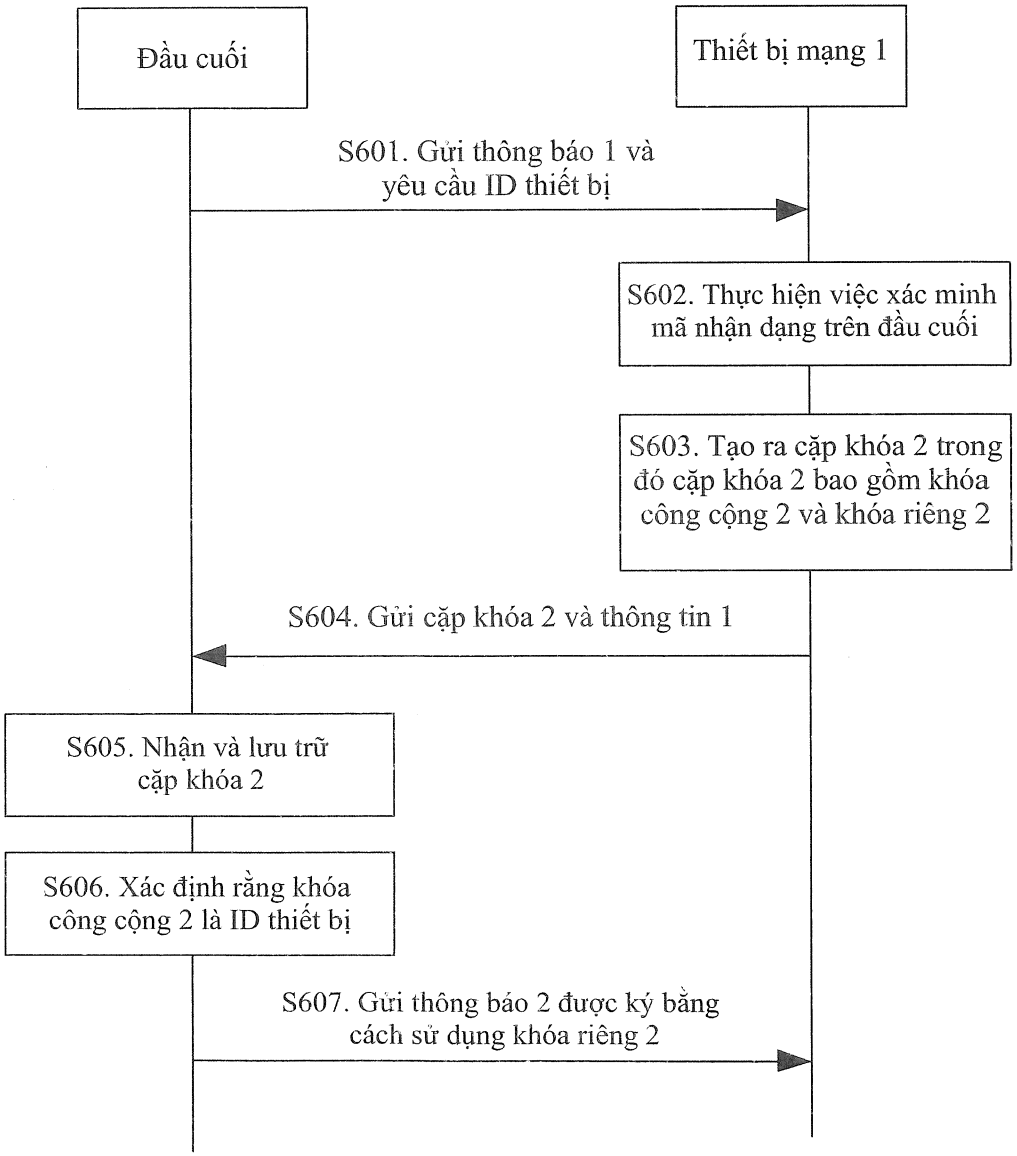
Đầu cuối
Thiết bị mạng 1
S601. Gửi thông báo 1 và yêu cầu ID thiết bị
S602. Thực hiện việc xác minh mã nhận dạng trên đầu cuối
S603. Tạo ra cặp khóa 2 trong đó cặp khóa 2 bao gồm khóa công cộng 2 và khóa riêng 2
S604. Gửi cặp khóa 2 và thông tin 1
S605. Nhận và lưu trữ cặp khóa 2
S606. Xác định rằng khóa công cộng 2 là ID thiết bị
S607. Gửi thông báo 2 được ký bằng cách sử dụng khóa riêng 2

Fig.6

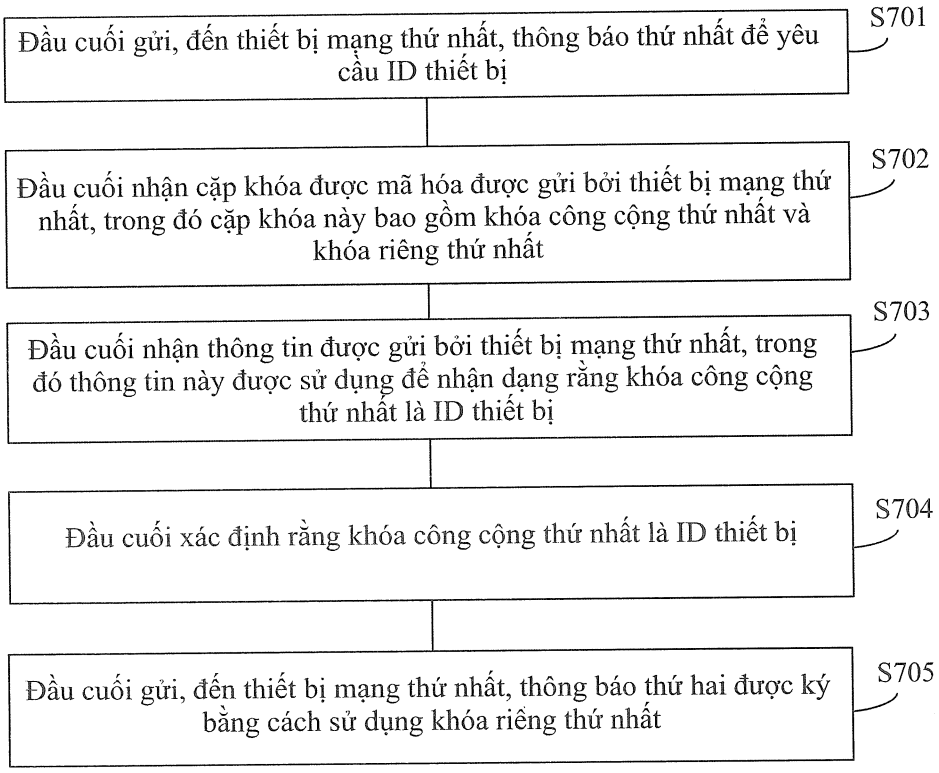
Đầu cuối gửi, đến thiết bị mạng thứ nhất, thông báo thứ nhất để yêu cầu ID thiết bị
S701
Đầu cuối nhận cặp khóa được mã hóa được gửi bởi thiết bị mạng thứ nhất, trong đó cặp khóa này bao gồm khóa công cộng thứ nhất và khóa riêng thứ nhất
S702
Đầu cuối nhận thông tin được gửi bởi thiết bị mạng thứ nhất, trong đó thông tin này được sử dụng để nhận dạng rằng khóa công cộng thứ nhất là ID thiết bị
S703
Đầu cuối xác định rằng khóa công cộng thứ nhất là ID thiết bị
S704
Đầu cuối gửi, đến thiết bị mạng thứ nhất, thông báo thứ hai được ký bằng cách sử dụng khóa riêng thứ nhất
S705

Fig.7

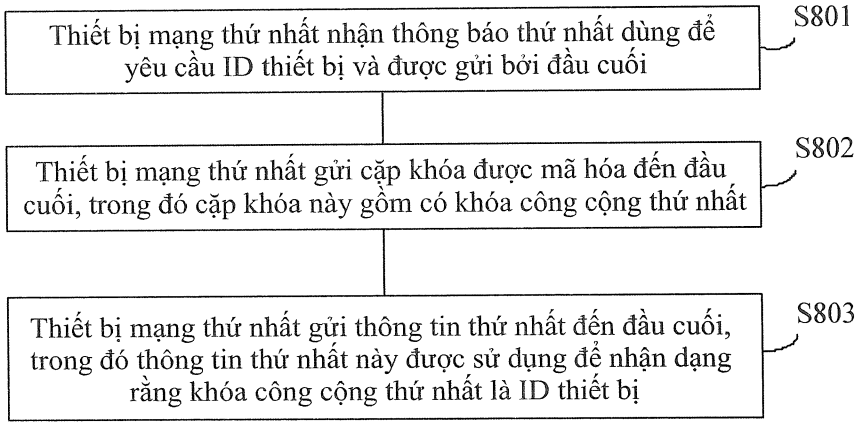
Thiết bị mạng thứ nhất nhận thông báo thứ nhất dùng để yêu cầu ID thiết bị và được gửi bởi đầu cuối
S801
Thiết bị mạng thứ nhất gửi cặp khóa được mã hóa đến đầu cuối, trong đó cặp khóa này gồm có khóa công cộng thứ nhất
S802
Thiết bị mạng thứ nhất gửi thông tin thứ nhất đến đầu cuối, trong đó thông tin thứ nhất này được sử dụng để nhận dạng rằng khóa công cộng thứ nhất là ID thiết bị
S803

Fig.8

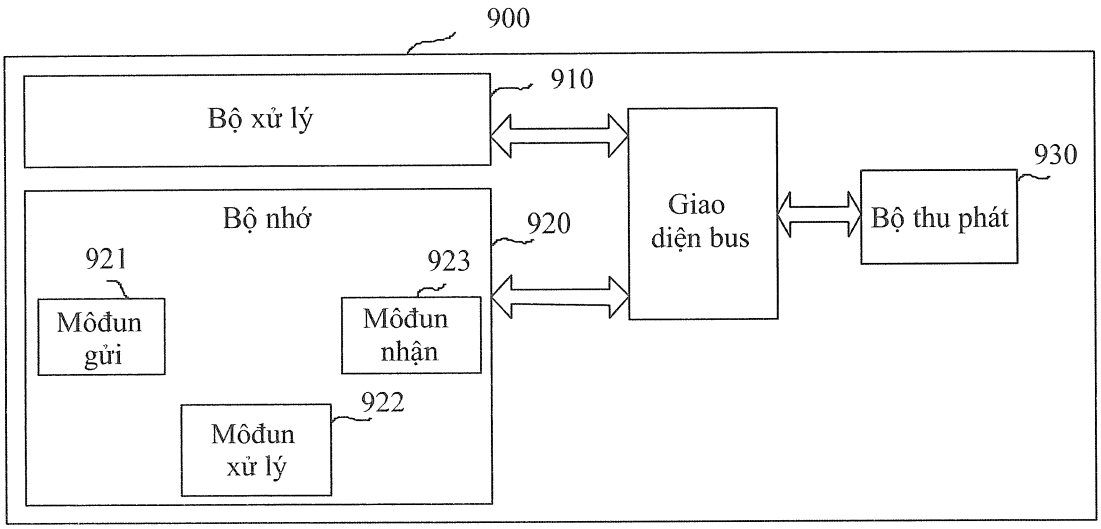
900
910
Bộ xử lý
930
Bộ nhớ
920
Giao diện bus
Bộ thu phát
921
923
Môđun gửi
Môđun nhận
922
Môđun xử lý

Fig.9

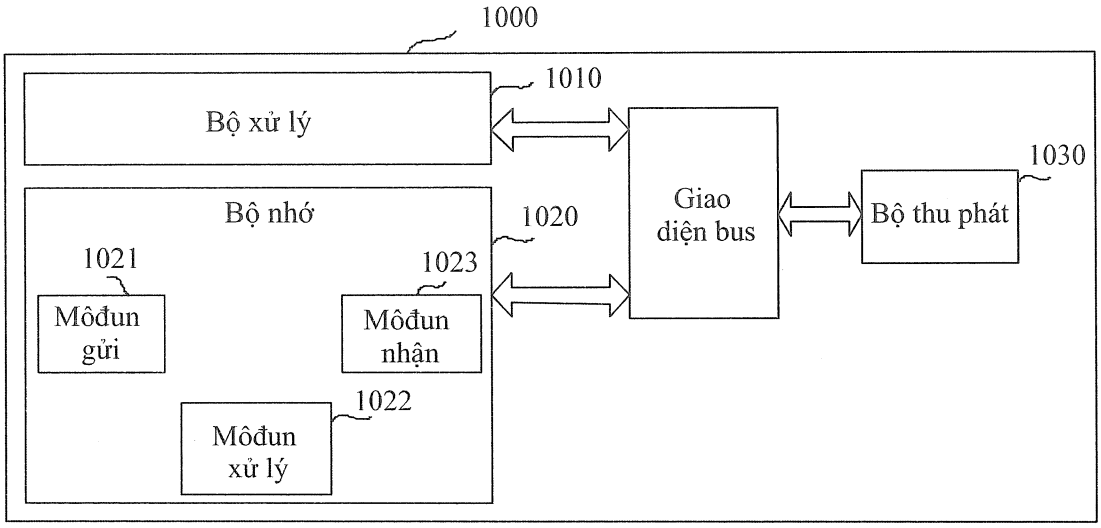
1000
1010
Bộ xử lý
1030
Bộ nhớ
1020
Giao diện bus
Bộ thu phát
1021
1023
Môđun gửi
Môđun nhận
1022
Môđun xử lý

Fig.10