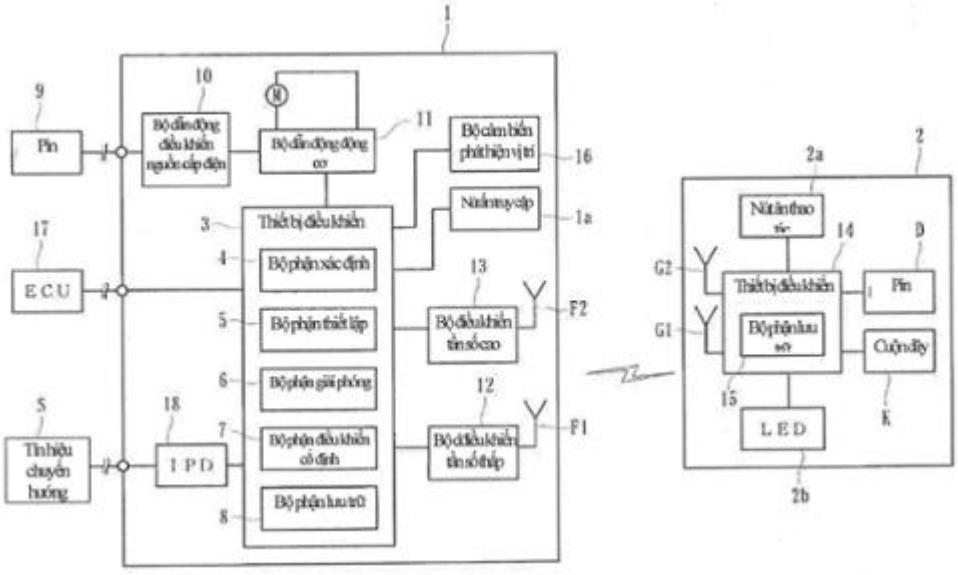
(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ
(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ
(11) **1-0036859**
(51)[8] **H04W 4/00** (13) **B**

(21) 1-2018-04454 (22) 09/10/2018
(30) 2017-197431 11/10/2017 JP; 2018-164396 03/09/2018 JP
(45) 25/09/2023 426 (43) 25/04/2019 373A
(73) ASAHI DENSO CO., LTD. (JP)
2-1, Somejidai 6-chome, Hamakita-ku, Hamamatsu-shi, Shizuoka 434-0046 Japan
(72) Shigeki HASHIMOTO (JP); Keita TAKEUCHI (JP).
(74) Công ty TNHH Trường Xuân (AGELESS CO.,LTD.)

(54) HỆ THỐNG TRUYỀN THÔNG KHÔNG DÂY

(57) Sáng chế đề xuất hệ thống truyền thông không dây bao gồm: thiết bị trên xe được gắn trên xe và có khả năng truyền không dây tín hiệu truy cập khi bộ phận vận hành được vận hành; thiết bị di động có khả năng truyền không dây mã xác thực xe cụ thể với điều kiện là tín hiệu truy cập được nhận; và bộ phận xác định có khả năng xác định mã xác thực có phải là mã xác thực thông thường hay không với điều kiện là mã nhận thực được nhận. Sự khởi động nguồn dẫn động của xe được phép hoặc được phép chạy xe khi bộ phận xác định xác định rằng mã xác thực là mã xác thực thông thường, và chế độ bảo mật trong đó chức năng truyền tín hiệu truy cập bằng thiết bị trên xe hoặc chức năng truyền mã xác thực bằng thiết bị di động được tắt có thể được thiết lập bằng hoạt động thiết lập định trước.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến hệ thống truyền thông không dây có khả năng cho phép khởi động nguồn dẫn động của xe cộ hoặc cho phép xe cộ chạy khi có được mã xác thực bởi thiết bị trên xe là mã xác thực thông thường.

Tình trạng kỹ thuật của sáng chế

Hệ thống truyền thông không dây (được gọi là thiết bị khóa điều khiển từ xa thụ động) bao gồm: thiết bị di động được thực hiện bởi người sở hữu và có khả năng truyền mã xác thực xe cụ thể bằng sóng vô tuyến; và thiết bị trên xe có khả năng nhận mã xác thực đã được truyền đã được phổ biến. Trong hệ thống truyền thông không dây này, chỉ khi mã xác thực được truyền không dây từ thiết bị di động là mã xác thực thông thường, việc cho phép mở nhiều ổ khóa khác nhau của xe cộ và khởi động nguồn dẫn động. Hệ thống truyền thông không dây như vậy có thể được cấu hình như sau. Khi nhấn nút ấn truy cập được bố trí trên thiết bị trên xe, tín hiệu truy cập được truyền không dây ở tần số thấp, và thiết bị di động mà đã nhận tín hiệu truy cập truyền không dây mã xác thực ở tần số cao. Hơn nữa, khi mã xác thực được nhận bởi thiết bị trên xe, có thể xác định mã xác thực có phải là mã xác thực thông thường hay không.

Bằng cách này, trong hệ thống truyền thông không dây như đã mô tả ở trên, có một vấn đề ở chỗ các biện pháp đối phó đạt hiệu quả không thể thực hiện được đối với các hành vi như là tấn công chuyển tiếp trong đó người thứ ba thực hiện bất hợp pháp sự truyền thông giữa thiết bị di động và thiết bị trên xe bằng sự chuyển tiếp. Tức là, vì người thứ ba có thể dễ dàng giải điều biến tín hiệu điều biến trong sự truyền thông giữa thiết bị di động và thiết bị trên xe, người thứ ba có thể truyền bất hợp pháp mã xác thực thông thường từ thiết bị di động đến thiết bị trên xe bằng cách sử dụng sự chuyển tiếp hoặc tương tự, do đó mở các ổ khóa khác nhau của xe cộ và khởi động nguồn dẫn động.

Các biện pháp đối phó khác nhau đã được đề xuất để ngăn chặn các hành vi bất hợp pháp như là tấn công chuyển tiếp như đã mô tả ở trên. Ví dụ, một biện pháp đối phó để đo thời gian cho đến khi nhận được tín hiệu tần số thấp bằng thiết bị di động, một biện pháp đối phó khác là thay đổi tần số của tín hiệu tần số cao, hoặc biện pháp đối phó khác là thay đổi cường độ sóng vô tuyến mà sẽ được truyền, hoặc tương tự có thể được thực hiện. Hơn nữa, như là một giải pháp kỹ thuật đã biết, ví dụ, như được bộc lộ trong JP-A-2016-220088, đã đề xuất giải pháp ngăn chặn các hành vi bất hợp pháp như là tấn công chuyển tiếp bằng cách sử dụng một thiết bị di động có khả năng điều chỉnh mã xác thực bằng nhiều sơ đồ điều biến.

Tuy nhiên, trong hệ thống truyền thông không dây đã biết, cấu hình xử lý tín hiệu được truyền thông giữa thiết bị trên xe và thiết bị di động là cực kỳ phức tạp, và do đó, có thể cần thời gian dài để xử lý xác thực người sở hữu có thiết bị di động hợp pháp hoặc độ chính xác của quá trình xác thực có thể bị hỏng. Vì vậy, có một vấn đề là hệ thống truyền thông không dây đã biết này không đủ để ngăn chặn một cách tin cậy các hành vi bất hợp pháp như là tấn công chuyển tiếp.

Sáng chế nhằm mục đích đề xuất hệ thống truyền thông không dây có khả năng cải thiện hiệu quả tính bảo mật trong khi tránh được sự phức tạp trong việc xử lý tín hiệu.

Bản chất kỹ thuật của sáng chế

Theo khía cạnh của sáng chế đã đề xuất hệ thống truyền thông không dây bao gồm: thiết bị trên xe được gắn trên xe và bao gồm bộ phận vận hành có thể được điều khiển tùy ý bởi người sở hữu, thiết bị trên xe có khả năng truyền không dây tín hiệu truy cập khi bộ phận vận hành được vận hành; thiết bị di động, mà có thể được mang bởi người sở hữu, có khả năng truyền không dây mã xác thực xe cụ thể với điều kiện là tín hiệu truy cập được nhận; và bộ phận xác định có khả năng xác định mã xác thực có phải là mã xác thực thông thường trên điều kiện mã xác thực được nhận hay không, trong đó sự khởi động nguồn dẫn

động của xe cộ được phép hoặc sự chạy xe là có thể khi bộ phận xác định xác định rằng mã xác thực là mã xác thực thông thường, và trong đó chế độ bảo mật trong đó chức năng truyền tín hiệu truy cập của thiết bị trên xe hoặc chức năng truyền mã xác thực bằng thiết bị di động được tắt có thể được thiết lập bởi hoạt động thiết lập định trước.

Mô tả vắn tắt các hình vẽ

FIG. 1 là hình phối cảnh thể hiện hệ thống truyền thông không dây theo phương án thứ nhất của sáng chế (chung cho phương án thứ hai);

FIG. 2 là sơ đồ khối thể hiện hệ thống truyền thông không dây;

FIG. 3 là lưu đồ thể hiện sự điều khiển tại thời điểm thiết lập chế độ bảo mật trong hệ thống truyền thông không dây;

FIG. 4 là lưu đồ thể hiện sự điều khiển tại thời điểm xác thực mã xác thực trong hệ thống truyền thông không dây (chung cho phương án thứ hai);

FIG. 5 là lưu đồ thể hiện sự điều khiển tại thời điểm giải phóng chế độ bảo mật trong hệ thống truyền thông không dây;

FIG. 6 là sơ đồ khối thể hiện hệ thống truyền thông không dây theo phương án thứ hai của sáng chế;

FIG. 7 là lưu đồ thể hiện sự điều khiển tại thời điểm thiết lập chế độ bảo mật trong hệ thống truyền thông không dây;

FIG. 8 là lưu đồ thể hiện sự điều khiển tại thời điểm giải phóng chế độ bảo mật trong hệ thống truyền thông không dây; và

FIG. 9 là hình chiếu thể hiện bộ phận vận hành trên xe trong hệ thống truyền thông không dây theo phương án khác của sáng chế.

Mô tả chi tiết sáng chế

Sau đây, các phương án của sáng chế sẽ được mô tả cụ thể cùng dựa vào các hình vẽ.

Như được thể hiện trên FIG. 1 và FIG. 2, hệ thống truyền thông không dây theo

phương án thứ nhất được cấu hình bằng thiết bị khóa điều khiển từ xa thụ động mà có thể thực hiện sự truyền thông không dây giữa thiết bị di động 2 (chìa khóa điện tử) được thực hiện bởi người sở hữu và thiết bị trên xe được gắn trên xe chẳng hạn xe mô tô và có thể cho phép khởi động động cơ là nguồn dẫn động hoặc cho phép chạy xe khi có được mã xác thực bởi thiết bị trên xe 1 là mã xác thực thông thường.

Thiết bị di động 2 có thể được mang bởi người sở hữu và có thể truyền không dây mã xác thực xe cụ thể với điều kiện nhận được tín hiệu truy cập từ thiết bị trên xe 1. Như được thể hiện trên FIG. 2, thiết bị di động 2 bao gồm nút ấn vận hành 2a (bộ phận vận hành), đèn LED 2b là thiết bị thông báo, ăngten tần số thấp G1 có khả năng nhận không dây tín hiệu truy cập (tín hiệu tần số thấp) từ thiết bị trên xe 1, ăngten tần số cao G2 có khả năng truyền không dây mã xác thực (tín hiệu tần số cao) đến thiết bị trên xe 1, thiết bị điều khiển 14 được kết nối điện với ăngten tần số thấp G1 và ăngten tần số cao G2, pin D, và cuộn dây K.

Bộ phận lưu trữ 15 có khả năng lưu trữ mã xác thực xe cụ thể được tạo ra trong thiết bị điều khiển 14. Thiết bị điều khiển 14 có thể được vận hành bằng cách nhận nguồn điện từ pin D hoặc cuộn dây K khi chức năng cố định được kích hoạt. Với điều kiện là tín hiệu truy cập từ thiết bị trên xe 1 được nhận bởi ăngten tần số thấp G1, thiết bị điều khiển 14 được điều chỉnh để truyền không dây mã xác thực xe cụ thể bằng ăngten tần số cao G2.

Thiết bị trên xe 1 được lắp trên xe (theo phương án này, trên thân xe của xe mô tô). Như được thể hiện trên FIG. 1, thiết bị trên xe 1 có nút ấn truy cập 1a (bộ phận vận hành) và thanh khóa L mà có thể được vận hành tùy ý bởi người sở hữu như là người lái xa. Thiết bị trên xe 1 có thể truyền không dây tín hiệu truy cập đến thiết bị di động 2 khi nút ấn truy cập 1a được vận hành. Như được thể hiện trên FIG. 2, ngoài nút ấn truy cập 1a và thanh khóa L, thiết bị trên xe 1 bao gồm thiết bị điều khiển 3, động cơ M có khả năng điều khiển thanh khóa L (xem FIG. 1), ăngten tần số thấp F1 và ăngten tần số cao F2.

Động cơ M được nối điện với pin 9 được gắn trên xe thông qua bộ dẫn động điều

khiển nguồn cấp điện 10. Động cơ M có thể được điều khiển bởi bộ dẫn động động cơ 11 và di chuyển thanh khóa L. Thanh khóa L có thể di chuyển được giữa vị trí khóa nơi nó được chèn vào lỗ khóa (không được thể hiện trên hình vẽ) được tạo ra trong tay lái của xe cộ để khóa tay lái và vị trí mở khóa nơi nó được rút lại từ lỗ khóa để giải phóng sự khóa tay lái.

Cụ thể, khi thanh khóa L ở vị trí khóa, tay lái bị khóa và không thể điều khiển xe. Khi thanh khóa L ở vị trí mở khóa, sự khóa của tay lái được nhả ra và xe có thể lái. Hơn nữa, vị trí của thanh khóa L có thể được phát hiện bởi bộ cảm biến phát hiện vị trí 16. Vị trí (vị trí khóa hoặc vị trí mở khóa) của thanh khóa L được phát hiện bởi bộ cảm biến phát hiện vị trí 16 có thể được truyền đến thiết bị điều khiển 3.

Thiết bị điều khiển 3 được nối điện với ăngten tần số thấp F1 thông qua bộ điều khiển tần số thấp 12 và được kết nối điện với ăngten tần số cao F2 thông qua bộ điều khiển tần số cao 13. Thiết bị điều khiển 3 có thể thực hiện việc điều khiển dựa trên sự truyền tín hiệu tần số thấp bằng ăngten tần số thấp F1 và sự nhận tín hiệu tần số cao bằng ăngten tần số cao F2. Hơn nữa, thiết bị điều khiển 3 được kết nối điện với nút ấn truy cập 1a (bộ phận vận hành) và được kết nối điện với ECU (Thiết bị điều khiển động cơ - Engine Control Unit) 17 được gắn trên xe và các tín hiệu chuyển hướng phải và trái S (các đèn chuyển hướng) thông qua IPD (Thiết bị nguồn thông minh - Intelligent Power Device) 18 hoặc tương tự.

Ngoài ra, với điều kiện là nút ấn truy cập 1a phải được ấn xuống, thiết bị điều khiển 3 theo phương án này có thể truyền không dây tín hiệu bao gồm tín hiệu tần số thấp từ ăngten tần số thấp F1 đến thiết bị di động 2. Với điều kiện là mã xác thực bao gồm tín hiệu tần số cao được truyền không dây từ thiết bị di động 2 được nhận bởi ăngten tần số cao F2, thiết bị điều khiển 3 có thể xác định mã xác thực đã nhận có phải là mã xác thực thông thường hay không. Thiết bị điều khiển 3 bao gồm bộ phận xác định 4 có khả năng xác định mã xác thực, bộ phận thiết lập 5 có khả năng thiết lập chế độ bảo mật, bộ phận giải phóng 6 có khả năng giải phóng chế độ bảo mật, bộ phận điều khiển cố định 7 có khả năng kích hoạt chức năng

cố định, và bộ phận lưu trữ 8 có khả năng lưu trữ mã số ngẫu nhiên hoặc tương tự.

Bộ phận xác định 4 được tạo ra trong thiết bị điều khiển 3 được bố trí trong thiết bị trên xe 1. Với điều kiện là mã xác thực được truyền từ thiết bị di động 2 được nhận bởi ăngten tần số cao F2, bộ phận xác định 4 có thể xác định mã xác thực có phải là mã xác thực thông thường hay không. Sau đó, khi được xác định rằng mã xác thực nhận được bởi bộ phận xác định 4 là mã xác thực thông thường, dưới sự điều khiểu của thiết bị điều khiển 3, động cơ M được điều khiển để di chuyển thanh khóa L đến vị trí mở khóa khi thanh khóa L ở vị trí khóa. Hơn nữa, dưới sự điều khiển của thiết bị điều khiển 3, tín hiệu cho phép được truyền đến ECU 17 và sự khởi động động cơ (nguồn dẫn động) được cho phép (ví dụ, hoạt động của bộ khởi động được cho phép). Mặt khác, khi được xác định rằng mã xác thực được nhận bởi bộ phận xác định 4 không phải là mã xác thực thông thường, động cơ M không được dẫn động và tín hiệu cho phép không được truyền đến ECU 17.

Ở đây, hệ thống truyền thông không dây theo phương án này có thể thiết lập chế độ bảo mật trong đó ít nhất chức năng truyền tín hiệu truy cập bằng thiết bị trên xe 1 bị tắt bởi hoạt động thiết lập định trước. Cụ thể, khi một hoạt động cụ thể (ví dụ, “thao tác ấn lâu" hoặc "thao tác ấn liên tục" hoặc tương tự khác với thao tác bình thường) được thực hiện trên nút ấn truy cập 1a (bộ phận vận hành) được bố trí trên thiết bị trên xe 1, chế độ bảo mật được thiết lập bởi bộ phận thiết lập 5, và ít nhất chức năng truyền tín hiệu truy cập bằng thiết bị trên xe 1 được tắt. Theo cách này, khi chế độ bảo mật được thiết lập, tín hiệu truy cập (tín hiệu tần số thấp) không được truyền từ ăngten tần số thấp F1 của thiết bị trên xe 1 ngay cả khi nút ấn truy cập 1a được ấn xuống. Do đó, tín hiệu truy cập không được nhận bởi ăngten tần số thấp G1 của thiết bị di động 2.

Ở chế độ bảo mật, ít nhất chức năng truyền tín hiệu truy cập bằng thiết bị trên xe 1 được tắt. Ở chế độ bảo mật, ngoài việc tắt chức năng truyền tín hiệu truy cập bằng thiết bị trên xe 1, chức năng truyền mã xác thực bằng thiết bị di động 2 có thể được tắt (tức là, cả

chức năng truyền tín hiệu truy cập bởi thiết bị trên xe và chức năng truyền mã xác thực bằng thiết bị di động có thể được tắt). Hơn nữa, hoạt động định trước để thiết lập chế độ bảo mật không bị giới hạn ở hoạt động cụ thể trên nút ấn truy cập (bộ phận vận hành) của thiết bị trên xe 1 như theo phương án này. Ví dụ, một hoạt động cụ thể (ví dụ, "thao tác ấn lâu" hoặc "thao tác ấn liên tục" hoặc tương tự khác với thao tác bình thường) trên nút thao tác 2a (bộ phận vận hành) được bố trí trong thiết bị di động 2 có thể được thực hiện.

Bộ phận giải phóng 6 có thể giải phóng chế độ bảo mật bằng cách thực hiện hoạt động giải phóng định trước trên nút thao tác 2a (bộ phận vận hành) được bố trí trong thiết bị di động. Hơn nữa, khi chế độ bảo mật được giải phóng, chức năng truyền tín hiệu truy cập bởi thiết bị trên xe 1 (theo phương án này, ngoài chức năng truyền tín hiệu truy cập, chức năng truyền mã xác thực bằng thiết bị di động 2) được khôi phục. Bằng cách này, thiết bị trên xe 1 có thể truyền tín hiệu truy cập và thiết bị di động 2 có thể truyền mã xác thực.

Hơn nữa, hoạt động định trước để giải phóng chế độ bảo mật không bị giới hạn ở thao tác cụ thể trên nút thao tác 2a (bộ phận vận hành) của thiết bị di động 2 như theo phương án này. Ví dụ, hoạt động cụ thể (ví dụ, "thao tác ấn lâu" hoặc "thao tác ấn liên tục" hoặc các thao tác khác với thao tác bình thường) có thể được thực hiện trên nút ấn truy cập 1a (bộ phận vận hành) của thiết bị trên xe 1 hoặc hoạt động có thể được thực hiện trên bộ phận vận hành (tốt nhất là bộ phận hoạt động được bố trí ở vị trí ẩn mà khó thấy bởi người thứ ba) được bố trí riêng trên thiết bị trên xe 1 hoặc xe cộ.

Hơn nữa, theo phương án này, khi chế độ bảo mật được thiết lập, các mã số ngẫu nhiên được tạo ra bởi thiết bị điều khiển 3 và được lưu trữ trong bộ phận lưu trữ 8 của thiết bị trên xe 1 và bộ phận lưu trữ 15 của thiết bị di động 2, tương ứng. Khi hoạt động giải phóng được thực hiện, mã số ngẫu nhiên được lưu trữ trong bộ phận lưu trữ 15 của thiết bị di động 2 được so sánh với mã số ngẫu nhiên được lưu trữ trong bộ phận lưu trữ 8 của thiết bị trên xe 1. Chỉ khi các mã số ngẫu nhiên này là khớp nhau, chế độ bảo mật được giải

phóng.

Bộ phận điều khiển cố định 7 được bố trí để bật chức năng cố định, ví dụ, với điều kiện là có hoạt động xác định trước (hoạt động cụ thể khác với hoạt động tại thời điểm truyền tín hiệu truy cập hoặc hoạt động tại thời điểm thiết lập chế độ bảo mật) được thực hiện trên nút ấn truy cập 1a của thiết bị trên xe 1. Ví dụ, khi pin D của thiết bị di động 2 cạn kiệt và việc cung cấp nguồn điện là không thể, hoạt động cụ thể sẽ được thực hiện trên nút ấn truy cập 1a ở trạng thái nơi thiết bị di động 2 được mang gần sát thiết bị trên xe 1. Sau đó, bộ phận điều khiển cố định 7 được vận hành và sóng tần số thấp được truyền đến thiết bị di động 2 để gây ra thiết bị di động 2 để tạo ra năng lượng điện trong cuộn dây K. Mã xác thực có thể được truyền không dây với nguồn điện đã được tạo ra.

Hơn nữa, trong thiết bị di động 2 theo phương án này, đèn LED 2b như là thiết bị thông báo được gắn vào. Đèn LED 2b có thể được bật hoặc nhấp nháy ở trạng thái mà chế độ bảo mật được thiết lập. Qua đó, có thể thông báo rằng chế độ bảo mật được đặt bằng cách bật hoặc nhấp nháy đèn LED 2b. Theo cách này, ngoài việc thông báo sự có hoặc không có của sự thiết lập chế độ bảo mật, đèn LED 2b (thiết bị thông báo) có thể được cấu hình để thông báo sự cố xảy ra lỗi (bao gồm lỗi tại thời điểm tạo số ngẫu nhiên hoặc tương tự, lỗi tại thời điểm sự truyền thông giữa thiết bị trên xe 1 và thiết bị di động 2, v.v.). Trong khi đó, thiết bị thông báo này không giới hạn ở đèn LED 2b được bố trí trong thiết bị di động 2. Ví dụ, thiết bị hiển thị khác được bố trí trong thiết bị di động 2, thiết bị hiển thị như là đèn LED được bố trí trong thiết bị trên xe 1, hoặc thiết bị hiển thị (ví dụ, bảng đồng hồ hoặc tấm hiển thị tinh thể lỏng riêng biệt, v.v..) được gắn vào xe có thể được sử dụng.

Sau đây, nội dung điều khiển tại thời điểm thiết lập chế độ bảo mật trong hệ thống truyền thông không dây theo phương án này sẽ được mô tả cùng dẫn chiếu đến lưu đồ của FIG. 3.

Đầu tiên, ở bước S1, được xác định có hay không hoạt động thiết lập định trước (theo

phương án này, hoạt động cụ thể trên nút ấn truy cập 1a) để thiết lập chế độ bảo mật được thực hiện. Khi được xác định rằng hoạt động thiết lập định trước được thực hiện, quá trình chuyển sang bước S2. Ở bước S2, mã số ngẫu nhiên được tạo ra bởi thiết bị điều khiển 3 và được truyền không dây đến thiết bị di động 2 bằng ăngten tần số thấp F1.

Sau đó, ở bước S3, mã số ngẫu nhiên được lưu trữ trong bộ phận lưu trữ 8 của thiết bị trên xe 1 và bộ phận lưu trữ 15 của thiết bị di động 2, tương ứng. Sau đó, ở bước S4, được xác định mã số ngẫu nhiên có thường được lưu trữ trong bộ phận lưu trữ 8 của thiết bị trên xe 1 hay không. Ở bước S5, được xác định có hay không mã số ngẫu nhiên thường được lưu trữ trong bộ phận lưu trữ 15 của thiết bị di động 2. Khi được xác định ở bước S4 hoặc S5 rằng mã số ngẫu nhiên không thường được lưu trữ, việc thiết lập chế độ bảo mật được tắt ở bước S7. Khi được xác định ở cả bước S4 và S5 rằng mã số ngẫu nhiên thường được lưu trữ, quá trình này sẽ được chuyển sang bước S6. Ở bước S6, chế độ bảo mật được thiết lập bởi bộ phận thiết lập 5.

Sau đây, nội dung điều khiển tại thời điểm xác thực mã xác thực trong hệ thống truyền thông không dây theo phương án này sẽ được mô tả cùng tham chiếu đến lưu đồ của FIG. 4.

Đầu tiên, ở bước S1, được xác định có hay không hoạt động (thao tác ấn xuống) được thực hiện trên nút ấn truy cập 1a. Khi được xác định rằng hoạt động được thực hiện, quá trình chuyển sang bước S2. Ở bước S2, được xác định có hay không chế độ bảo mật được thiết lập. Khi được xác định ở bước S2 rằng chế độ bảo mật không được thiết lập, quá trình chuyển sang bước S3. Ở bước S3, tín hiệu truy cập được truyền không dây bởi ăngten tần số thấp F1. Sau đó, ở bước S4, mã xác thực từ thiết bị di động 2 được nhận bởi ăngten tần số cao F2.

Sau đó, ở bước S5, bộ phận xác định 4 xác định có hay không mã xác thực từ thiết bị di động 2 là mã xác thực thông thường. Khi được xác định rằng mã xác thực là mã xác thực

thông thường, quá trình chuyển sang bước S6. Ở bước S6, tín hiệu cho phép được truyền đến ECU 17 và sự khởi động động cơ (nguồn dẫn động) được cho phép. Hơn nữa, theo phương án này, ở bước S6, ngoài việc truyền tín hiệu cho phép đến ECU 17, động cơ M được dẫn động để di chuyển thanh khóa L đến vị trí mở khóa khi thanh khóa L ở vị trí khóa. Theo cách này, xe được phép chạy.

Mặt khác, khi được xác định ở bước S2 rằng chế độ bảo mật được thiết lập, từ S3 đến S6 sau khi S2 được bỏ qua. Do đó, chức năng truyền tín hiệu truy cập từ thiết bị trên xe 1 được tắt. Hơn nữa, khi được xác định ở bước S5 rằng mã xác thực từ thiết bị di động 2 không phải là mã xác thực thông thường, S6 được bỏ qua. Do đó, động cơ (nguồn dẫn động) không thể khởi động và sự khóa bằng thanh khóa L không được giải phóng.

Tiếp theo, nội dung điều khiển tại thời điểm giải phóng giải phóng chế độ bảo mật trong hệ thống truyền thông không dây theo phương án này sẽ được mô tả cùng tham chiếu đến lưu đồ của FIG. 5.

Đầu tiên, ở bước S1, được xác định có hay không một hoạt động nhấn xuống (thao tác giải phóng định trước) trên nút ấn vận hành 2a được bố trí trong thiết bị di động 2 được thực hiện. Khi được xác định rằng hoạt động được thực hiện, quá trình chuyển sang bước S2. Ở bước S2, mã số ngẫu nhiên được lưu trữ trong thiết bị di động 2 được nhận. Tức là, khi nút ấn vận hành 2a của thiết bị di động 2 được vận hành, mã số ngẫu nhiên được lưu trữ trong bộ phận lưu trữ 15 của thiết bị cầm tay 2 có thể được truyền không dây bởi ăngten tần số cao G2 và có thể nhận được bởi ăngten tần số cáo F2 của thiết bị trên xe 1.

Sau đó, ở bước S3, thiết bị điều khiển 3 so sánh mã số ngẫu nhiên được lưu trữ trong bộ phận lưu trữ 8 của thiết bị trên xe 1 với mã số ngẫu nhiên được truyền từ thiết bị di động 2, và được xác định có hay không các mã số ngẫu nhiên này là khớp nhau. Sau đó, khi được xác định từ các kết quả so sánh của các mã số ngẫu nhiên mà các mã số ngẫu nhiên khớp nhau, quá trình chuyển sang bước bước S4. Ở bước S4, chế độ bảo mật được giải phóng bởi

bộ phận giải phóng 6. Khi được xác định rằng các mã số ngẫu nhiên không khớp nhau, quá trình sẽ chuyển sang S5. Ở bước S5, chế độ bảo mật không được giải phóng bởi bộ phận giải phóng 6 và việc thiết lập chế độ bảo mật được tiếp tục.

Tuy nhiên, khi hoạt động bình thường (thao tác nhấn xuống) được thực hiện trên nút ấn truy cập 1a của thiết bị trên xe 1 sau khi chế độ bảo mật được giải phóng, tín hiệu truy cập có thể được truyền từ ăngten tần số thấp F1 của thiết bị trên xe 1 và mã xác thực từ thiết bị di động 2 có thể được xác định bởi bộ phận xác định 4. Ngoài ra, khi chế độ bảo mật được giải phóng, tín hiệu truy cập có thể được truyền tự động từ ăngten tần số thấp F1 của thiết bị trên xe 1 và mã xác thực từ thiết bị di động 2 có thể được xác định bởi bộ phận xác định 4.

Theo cách này, khi thao tác trên nút ấn truy cập 1a được yêu cầu sau khi chế độ bảo mật được giải phóng, hiệu quả bảo mật có thể được tăng cường. Khi mã xác thực được xác định tự động, khả năng hoạt động có thể được cải thiện. Hơn nữa, tốt hơn chọn tùy ý sự điều khiển trong đó thao tác trên nút ấn truy cập 1a được yêu cầu sau khi chế độ bảo mật được giải phóng và sự điều khiển trong đó mã xác thực được xác định tự động.

Tiếp theo, hệ thống truyền thông tin không dây theo phương án thứ hai của sáng chế sẽ được mô tả.

Tương tự như phương án thứ nhất, như được thể hiện trên FIG. 1 và FIG. 6, hệ thống truyền thông không dây theo phương án thứ hai được cấu hình bằng thiết bị khóa điều khiển từ xa thụ động mà có thể thực hiện sự truyền thông không dây giữa thiết bị di động 2 (chìa khóa điện tử) do người sở hữu và thiết bị trên xe được lắp trên xe cộ như là xe mô tô và có thể cho phép khởi động động cơ là nguồn dẫn động hoặc cho phép chạy xe khi mã xác thực có được bởi thiết bị trên xe 1 là mã xác thực thông thường. Trong khi đó, các thành phần tương tự như là các thành phần của phương án thứ nhất được biểu thị bằng các số chỉ dẫn giống nhau và việc mô tả chi tiết chúng sẽ được bỏ qua.

Trong hệ thống truyền thông không dây theo phương án này, bộ phận thiết lập 5 và bộ phận giải phóng 6 theo phương án thứ nhất được bố trí trong thiết bị điều khiển 14 của thiết bị di động 2 (chìa khóa điện tử). Ở đây, hệ thống truyền thông không dây theo phương án này có thể thiết lập chế độ bảo mật trong đó ít nhất chức năng truyền mã xác thực bằng thiết bị di động 2 được tắt bởi hoạt động thiết lập định trước. Cụ thể, khi hoạt động cụ thể (ví dụ "thao tác ấn lâu" hoặc "thao tác ấn liên tục" hoặc tương tự khác với thao tác thông thường) được thực hiện trên nút thao tác 2a (bộ phận vận hành) được bố trí trong thiết bị di động 2, chế độ bảo mật được thiết lập bởi bộ phận thiết lập 5, và ít nhất là chức năng truyền mã xác thực bằng thiết bị di động 2 được tắt. Theo cách này, khi chế độ bảo mật được thiết lập, mã xác thực (tín hiệu tần số cao) không được truyền từ ăngten tần số cao G2 của thiết bị di động 2 ngay cả khi nút ấn truy cập 1a được nhấn xuống sao cho tín hiệu truy cập được truyền từ ăngten tần số thấp F1 của thiết bị trên xe 1 và được nhận bởi ăngten tần số thấp G1 của thiết bị di động 2.

Ở chế độ bảo mật, là đủ để tắt ít nhất chức năng truyền mã xác thực bằng thiết bị di động 2. Ở chế độ bảo mật, ngoài việc tắt chức năng truyền mã xác thực bằng thiết bị di động 2, chức năng truyền tín hiệu truy cập bằng thiết bị trên xe 1 có thể được tắt (tức là cả chức năng truyền tín hiệu truy cập của thiết bị trên xe và chức năng truyền mã xác thực bằng thiết bị di động có thể được tắt). Hơn nữa, hoạt động định trước để thiết lập chế độ bảo mật không bị giới hạn ở hoạt động cụ thể trên nút thao tác 2a (bộ phận vận hành) của thiết bị di động 2 như theo phương án này. Ví dụ, hoạt động cụ thể (ví dụ: "thao tác ấn lâu" hoặc "thao tác ấn liên tục" hoặc các hoạt động tương tự khác với thao tác thông thường) trên nút ấn truy cập (bộ phận vận hành) được bố trí trong thiết bị trên xe 1 có thể được thực hiện.

Bộ phận giải phóng 6 có thể giải phóng chế độ bảo mật bằng cách thực hiện thao tác giải phóng định trước trên nút thao tác 2a (bộ phận vận hành) được bố trí trong thiết bị di động. Hơn nữa, khi chế độ bảo mật được giải phóng, chức năng truyền mã xác thức bởi thiết

bị di động 2 (theo phương án này, ngoài chức năng truyền mã xác thực, chức năng truyền tín hiệu truy cập của thiết bị trên xe 1) được khôi phục. Theo cách này, thiết bị trên xe 1 có thể truyền tín hiệu truy cập và thiết bị di động 2 có thể truyền mã xác thực.

Hơn nữa, hoạt động định trước để giải phóng chế độ bảo mật không bị giới hạn ở hoạt động cụ thể trên nút thao tác 2a (bộ phận vận hành) của thiết bị di động 2 như theo phương án này. Ví dụ, hoạt động cụ thể (ví dụ, "thao tác ấn lâu" hoặc "thao tác ấn liên tục" hoặc các hoạt động khác với thao tác thông thường) có thể được thực hiện trên nút ấn truy cập 1a (bộ phận vận hành) của thiết bị trên xe 1 hoặc hoạt động có thể được thực hiện trên bộ phận vận hành (tốt nhất là thiết bị hoạt động được bố trí ở vị trí ẩn mà khó nhìn thấy bởi người thứ ba) được bố trí riêng trên thiết bị trên xe 1 hoặc xe cộ.

Hơn nữa, như theo phương án thứ nhất, khi chế độ bảo mật được thiết lập, mã số ngẫu nhiên có thể được tạo bởi thiết bị điều khiển 3 và được lưu trữ trong bộ phận lưu trữ 8 của thiết bị trên xe 1 và bộ phận lưu trữ 15 của thiết bị di động 2, tương ứng. Khi hoạt động giải phóng được thực hiện, mã số ngẫu nhiên được lưu trữ trong bộ phận lưu trữ 15 của thiết bị di động 2 có thể được so sánh với mã số ngẫu nhiên được lưu trữ trong bộ phận lưu trữ 8 của thiết bị trên xe 1. Chỉ khi các mã số ngẫu nhiên này khớp nhau, chế độ bảo mật có thể được giải phóng.

Hơn nữa, trong thiết bị di động 2 theo phương án này, đèn LED 2b như là thiết bị thông báo được gắn vào. Đèn LED 2b có thể được bật sáng hoặc nhấp nháy ở trạng thái mà chế độ bảo mật được thiết lập. Qua đó, có thể thông báo rằng chế độ bảo mật được thiết lập bằng sự bật sáng hoặc nhấp nháy của đèn LED 2b. Theo cách này, ngoài việc thông báo sự có hoặc không có sự thiết lập chế độ bảo mật, đèn LED 2b (thiết bị thông báo) có thể được cấu hình để thông báo sự cố xảy ra lỗi. Trong khi đó, thiết bị thông báo này không giới hạn ở đèn LED 2b được bố trí trong thiết bị di động 2. Ví dụ, thiết bị hiển thị khác được bố trí trong thiết bị di động 2, thiết bị hiển thị như là đèn LED được bố trí trong thiết bị trên xe 1

hoặc thiết bị hiển thị (ví dụ, bảng đồng hồ hoặc tấm hiển thị tinh thể lỏng riêng biệt, v.v..) được gắn vào xe có thể được sử dụng.

Ở đây, theo phương án này, bố trí bộ phận lựa chọn 19 có khả năng kích hoạt hoặc vô hiệu hóa hoạt động thiết lập định trước để thiết lập chế độ bảo mật sẵn trước. Bộ phận lựa chọn 19 như vậy được cấu hình bằng công tắc vận hành hoặc các thiết bị tương tự được bố trí trong thiết bị trên xe 1, thiết bị di động 2 hoặc xe cộ, là một ví dụ. Bằng cách vận hành công tắc vận hành hoặc tương tự trước bởi người dùng, việc bật hoặc tắt hoạt động thiết lập định trước để thiết lập chế độ bảo mật có thể được đặt trước.

Tiếp theo, nội dung điều khiển tại thời điểm thiết lập chế độ bảo mật trong hệ thống truyền thông không dây theo phương án này sẽ được mô tả cùng dẫn chiếu đến lưu đồ của FIG. 7.

Khi hoạt động thiết lập định trước (theo phương án này, một thao tác cụ thể trên nút vận hành 2a (bộ phận vận hành) của thiết bị di động 2) để thiết lập chế độ bảo mật được thực hiện, được xác định, ở mặt bên của thiết bị trên xe 1, hoạt động thiết lập có được kích hoạt bởi bộ phận lựa chọn 19 (S1) hay không. Khi được xác định rằng hoạt động thiết lập được kích hoạt, quá trình chuyển sang bước S2. Ở bước S2, tín hiệu mã bảo mật được truyền không dây đến thiết bị di động 2 bằng ăngten tần số thấp F1.

Sau đó, ở mặt bên của thiết bị di động 2, khi tín hiệu mã bảo mật được nhận bởi ăngten tần số thấp G1 của thiết bị di động 2 (S3), được xác định có hay không tín hiệu mã bảo mật nhận được là chính xác (S4). Khi được xác định rằng tín hiệu mã bảo mật nhận được là chính xác, quá trình chuyển sang bước S5. Ở bước S5, tín hiệu thiết lập chế độ bảo mật được truyền bởi ăngten tần số cao G2 của thiết bị di động 2. Sau đó, quá trình này sẽ chuyển sang bước S6. Ở bước S6, chế độ bảo mật được thiết lập bởi bộ phận thiết lập 5. Quá trình này chuyển sang bước S7. Ở bước S7, thông báo rằng chế độ bảo mật được thiết lập được thực hiện bởi đèn LED 2b được bố trí trong thiết bị di động 2 hoặc một thiết bị

hiển thị riêng biệt hoặc tương tự. Trong khi đó, khi được xác định ở bước S4 rằng tín hiệu mã bảo mật là không chính xác, quá trình chuyển sang bước S8. Ở bước S8, việc thiết lập chế độ bảo mật được tắt.

Mặt khác, khi tín hiệu thiết lập chế độ bảo mật được truyền ở bước S5, điều này được xác định, ở mặt bên của thiết bị trên xe 1, tín hiệu thiết lập chế độ bảo mật (S9) đã được nhận hay không. Khi tín hiệu thiết lập chế độ bảo mật được nhận chính xác, quá trình sẽ chuyển sang bước S10. Ở bước S10, thông báo rằng chế độ bảo mật được thiết lập được thực hiện bởi đèn LED được bố trí trong thiết bị trên xe 1 hoặc một thiết bị hiển thị riêng biệt hoặc tương tự. Trong khi đó, khi được xác định ở bước S1 rằng hoạt động thiết lập được tắt bởi bộ phận lựa chọn 19, các bước S2, S9 và S10 được bỏ qua. Ngoài ra, khi được xác định ở bước S9 rằng tín hiệu thiết lập chế độ bảo mật không được nhận đúng, bước S10 được bỏ qua.

Tiếp theo, nội dung điều khiển tại thời điểm giải phóng chế độ bảo mật trong hệ thống truyền thông không dây theo phương án này sẽ được mô tả cùng tham chiếu đến lưu đồ của FIG. 8 và FIG. 4.

Khi thao tác nhấn xuống (thao tác giải phóng định trước) được thực hiện trên nút thao tác 2a được bố trí trong thiết bị di động 2, được xác định ở bước Sa xem hoạt động giải phóng có được thực hiện hay không. Khi được xác định rằng các hoạt động giải phóng được thực hiện, quá trình chuyển sang bước Sb. Ở bước Sb, chế độ bảo mật được giải phóng bởi bộ phận giải phóng 6. Khi được xác định rằng hoạt động giải phóng không được thực hiện, quá trình chuyển sang bước Sc. Ở bước Sc, chế độ bảo mật vẫn tiếp tục. Sau đó, khi một thao tác được thực hiện trên nút ấn truy cập 1a sau khi chế độ bảo mật được giải phóng ở bước Sb, sự điều khiển A tương tự như theo phương án thứ nhất được thực hiện.

Cụ thể, như được thể hiện trong lưu đồ của FIG. 4, trong sự điều khiển A, mà được xác định ở bước S1 xem hoạt động (một thao tác nhấn xuống) có được thực hiện trên nút ấn

truy cập 1a hay không. Khi được xác định rằng hoạt động được thực hiện, quá trình chuyển sang bước S2. Ở bước S2, được xác định chế độ bảo mật có được thiết lập hay không. Khi được xác định ở bước S2 rằng chế độ bảo mật không được thiết lập, quá trình chuyển sang bước S3. Ở bước S3, tín hiệu truy cập được truyền không dây bởi ăngten tần số thấp F1. Sau đó, ở bước S4, mã xác thực từ thiết bị di động 2 được nhận bởi ăngten tần số cao F2.

Sau đó, ở bước S5, bộ phận xác định 4 xác định có hay không mã xác thực từ thiết bị di động 2 là mã xác thực thông thường. Khi được xác định rằng mã xác thực là mã xác thực thông thường, quá trình chuyển sang bước S6. Ở bước S6, tín hiệu cho phép được truyền đến ECU 17 và khởi động động cơ (nguồn dẫn động) được cho phép. Hơn nữa, theo phương án này, ở bước S6, ngoài việc truyền tín hiệu cho phép đến ECU 17, động cơ M được dẫn động để di chuyển thanh khóa L đến vị trí mở khóa khi thanh khóa L ở vị trí khóa. Theo cách này, xe được phép chạy.

Mặt khác, khi được xác định ở bước S2 rằng chế độ bảo mật được thiết lập, các bước S3 đến S6 sau bước S2 được bỏ qua. Do đó, chức năng truyền tín hiệu truy cập từ thiết bị trên xe 1 được tắt. Hơn nữa, khi được xác định ở bước S5 rằng mã xác thực từ thiết bị di động 2 không phải là mã xác thực thông thường, bước S6 được bỏ qua. Do đó, không thể khởi động động cơ (nguồn dẫn động) và sự khóa bằng thanh khóa L không được giải phóng.

Theo các phương án thứ nhất và thứ hai, chế độ bảo mật trong đó chức năng truyền tín hiệu truy cập (phương án thứ nhất) bằng thiết bị trên xe 1 hoặc chức năng truyền mã xác thực (phương án thứ hai) bằng thiết bị di động 2 được tắt có thể được thiết lập bởi hoạt động thiết lập định trước. Bằng cách này, các hành vi bất hợp pháp như là tấn công chuyển tiếp có thể được ngăn chặn một cách tin cậy chỉ bằng cách tắt chức năng truyền. Hơn nữa, có thể nâng cao hiệu quả bảo mật trong khi tránh được sự phức tạp trong việc xử lý tín hiệu. Hơn nữa, khi cả hai chức năng truyền tín hiệu truy cập bằng thiết bị trên xe 1 và chức năng truyền mã xác thực bằng thiết bị di động 2 được tắt ở chế độ bảo mật, cả chức năng truyền

tín hiệu truy cập và chức năng của việc truyền mã xác thực được tắt và hiệu quả bảo mật có thể được nâng cao thêm nữa.

Hơn nữa, vì hoạt động thiết lập định trước cho thiết lập chế độ bảo mật được cấu hình bởi một hoạt động cụ thể trên nút ấn truy cập 1a (bộ phận vận hành) được bố trí trong thiết bị trên xe 1, không cần thiết phải bố trí bộ phận vận hành mới riêng biệt để thiết lập chế độ bảo mật và có thể ngăn chặn sự gia tăng chi phí sản xuất. Hơn nữa, vì chế độ bảo mật có thể được thiết lập mà không cần đến thiết bị di động 2, khả năng hoạt động có thể được cải thiện. Hơn nữa, khi hoạt động thiết lập định trước để thiết lập chế độ bảo mật được cấu hình bởi một hoạt động cụ thể trên nút thao tác 2a (bộ phận vận hành) được bố trí trong thiết bị di động 2, hoạt động thiết lập có thể được thực hiện từ vị trí từ xa và khả năng hoạt động có thể được cải thiện hơn nữa.

Hơn nữa, chế độ bảo mật có thể được giải phóng khi thao tác giải phóng định trước được thực hiện trên nút thao tác 2a (bộ phận vận hành) được bố trí trong thiết bị di động 2. Do đó, so với trường hợp mà thao tác giải phóng được thực hiện trên nút ấn truy cập 1a của thiết bị trên xe 1, mà có thể ngăn chặn một cách tin cậy người thứ ba không thể thực hiện thao tác giải phóng, và do đó, hiệu quả bảo mật có thể được nâng cao hơn nữa. Hơn nữa, khi chế độ bảo mật có thể được giải phóng bằng cách thực hiện thao tác giải phóng định trước trên nút ấn truy cập 1a (bộ phận vận hành) được bố trí trong thiết bị trên xe 1, không cần thiết phải bố trí bộ phận vận hành mới riêng biệt để giải phóng chế độ bảo mật, và có thể ngăn chặn sự gia tăng chi phí sản xuất. Hơn nữa, vì chế độ bảo mật có thể được giải phóng mà không cần đến thiết bị di động 2, khả năng hoạt động có thể được cải thiện.

Ngoài ra, theo phương án này, khi hoạt động giải phóng được thực hiện trên nút thao tác 2a (bộ phận vận hành) của thiết bị di động 2, chế độ bảo mật có thể được giải phóng và tín hiệu chuyển hướng S của xe có thể bị nhấp nháy. Do đó, hoạt động giải phóng có thể đóng vai trò như hoạt động giải phóng chế độ bảo mật và hoạt động nhấp nháy của tín hiệu

chuyển hướng S của xe để kích hoạt cuộc gọi ngược trả lời.

Hơn nữa, khi chế độ bảo mật được thiết lập, các mã số ngẫu nhiên được tạo ra và được lưu trữ trong bộ phận lưu trữ (8, 15) của thiết bị trên xe 1 và thiết bị di động 2, tương ứng. Khi hoạt động giải phóng được thực hiện, mã số ngẫu nhiên được lưu trữ trong bộ phận lưu trữ 15 của thiết bị di động 2 được so sánh với mã số ngẫu nhiên được lưu trữ trong bộ phận lưu trữ 8 của thiết bị trên xe 1. Chỉ khi các mã số ngẫu nhiên này khớp nhau, chế độ bảo mật được giải phóng. Do đó, hiệu quả bảo mật có thể được duy trì bằng cách so sánh các mã số ngẫu nhiên.

Hơn nữa, vì thiết bị trên xe 1 theo phương án này có chức năng cố định truyền sóng tần số thấp đến thiết bị di động 2 để làm cho thiết bị di động 2 tạo ra nguồn điện và truyền không dây mã xác thực bằng nguồn điện đã được tạo ra, nên có thể xử lý thuận lợi đối với trường hợp khẩn cấp như là cạn kiệt nguồn pin của thiết bị di động 2. Hơn nữa, thiết bị di động 2 (có thể là thiết bị trên xe 1) bao gồm đèn LED 2b (thiết bị thông báo) có khả năng thông báo rằng chế độ bảo mật được thiết lập. Do đó, khi hành khách rời khỏi xe, hành khách có thể nhận ra và nắm bắt trạng thái thiết lập của chế độ bảo mật. Trong khi đó, thiết bị thông báo có thể là thiết bị hiển thị khác được bố trí trên xe.

Mặc dù phương án này đã được mô tả ở trên, sáng chế không bị hạn chế ở phương án này. Ví dụ, hoạt động thiết lập định trước để thiết lập chế độ bảo mật hoặc một hoạt động giải phóng định trước để giải phóng chế độ bảo mật có thể được thực hiện trên bộ phận vận hành ở bên của xe được gắn trên xe. Trong trường hợp này, như được thể hiện trên FIG. 9, công tắc M1 hoặc công tắc M2 được bố trí trong hộp công tắc điều khiển bằng tay C được gắn vào tay lái H của xe có thể được sử dụng làm bộ phận vận hành ở bên của xe. Trong khi đó, số chỉ dẫn G trên FIG. 9 biểu thị tay nắm mà có thể được nắm bởi người lái xe.

Công tắc M1 được cấu hình bằng phím chéo có thể được nhấn ở bên trái, bên phải, phía lên và phía dưới. Ví dụ, chế độ bảo mật có thể được thiết lập hoặc giải phóng bằng

cách hiển thị bảng chọn trên thiết bị hiển thị (bảng đồng hồ hoặc thiết bị hiển thị tinh thể lỏng riêng biệt, v.v.) được bố trí trên xe và lựa chọn và xác định các mục liên quan đến chế độ bảo mật từ bảng chọn bằng công tắc M1. Hơn nữa, công tắc M2 được cấu hình bằng nút thao tác có thể được nhấn xuống. Chế độ bảo mật có thể được thiết lập hoặc giải phóng bằng cách nhấn nút thao tác này.

Theo cách này, khi hoạt động thiết lập định trước để thiết lập chế độ bảo mật hoặc hoạt động giải phóng định trước có thể được thực hiện trên bộ phận vận hành ở bên của xe được gắn trên xe, hoạt động thiết lập định trước để thiết lập chế độ bảo mật hoặc hoạt động giải phóng định trước để giải phóng chế độ bảo mật có thể được thực hiện ở vị trí tùy ý của xe, và do đó, khả năng hoạt động có thể được cải thiện. Đặc biệt, vì bộ phận vận hành ở bên của xe được bố trí trong hộp công tắc điều khiển bằng tay C được gắn vào tay lái H của xe, nên có thể cải thiện khả năng hoạt động của hoạt động thiết lập định trước để thiết lập chế độ bảo mật hoặc hoạt động giải phóng định trước để giải phóng chế độ bảo mật.

Ngoài ra, ví dụ, khi bộ phận xác định 4 xác định rằng mã xác thực là mã xác thực thông thường, chỉ một trong số các hoạt động truyền tín hiệu cho phép đến ECU 17 để cho phép khởi động động cơ (nguồn dẫn động) của xe và hoạt động di chuyển thanh khóa L đến vị trí mở khóa để cho phép chạy xe có thể được thực hiện, thay cho hoạt động truyền tín hiệu cho phép đến ECU 17 để cho phép khởi động động cơ (nguồn dẫn động) của xe và di chuyển thanh khóa L đến vị trí mở khóa để cho phép chạy xe như theo phương án này.

Hơn nữa, khi thao tác giải phóng được thực hiện trên nút thao tác 2a của thiết bị di động 2, cuộc gọi ngược trả lời có thể không được kích hoạt hoặc chức năng khác có thể được kích hoạt cùng với việc giải phóng chế độ bảo mật, thay cho việc giải phóng chế độ bảo mật, nhấp nháy tín hiệu chuyển hướng của xe và kích hoạt cuộc gọi ngược trả lời. Hơn nữa, chức năng cố định có thể không được cung cấp hoặc thiết bị thông báo như là đèn LED 2b có thể không được bố trí. Trong khi đó, theo phương án này, sáng chế được áp dụng cho

xe mô tô. Tuy nhiên, sáng chế có thể được áp dụng cho các phương tiện khác như là ATV (tàu tự hành – Automated transfer Vehicle), xe trượt tuyết, máy xây dựng, máy móc nông nghiệp và ô tô.

Hệ thống truyền thông không dây có thể có hình thức bên ngoài khác hoặc có thể có thêm chức năng khác, miễn là có thể thiết lập, bằng hoạt động thiết lập định sẵn, chế độ bảo mật trong đó chức năng truyền tín hiệu truy nhập bằng thiết bị trên xe hoặc chức năng truyền mã xác thực bằng thiết bị di động được tắt.

Theo một khía cạnh của sáng chế, đã đề xuất hệ thống truyền thông không dây bao gồm: thiết bị trên xe được gắn trên xe và bao gồm bộ phận vận hành có thể được điều khiển bởi người sở hữu, thiết bị trên xe có khả năng truyền không dây tín hiệu truy cập khi bộ phận bộ phận vận hành được vận hành; thiết bị di động, có thể được mang bởi người sở hữu, có khả năng truyền không dây mã xác thực xe cụ thể với điều kiện là tín hiệu truy cập được nhận; và bộ phận xác định có khả năng xác định mã xác thực có phải là mã xác thực thông thường hay không với điều kiện là mã nhận thực được nhận, trong đó sự khởi động nguồn dẫn động của xe được phép hoặc được phép chạy xe khi bộ phận xác định xác định rằng mã xác thực là mã xác thực thông thường, và trong đó chế độ bảo mật trong đó chức năng truyền tín hiệu truy cập bằng thiết bị trên xe hoặc chức năng truyền mã xác thực bằng thiết bị di động được tắt có thể được thiết lập bằng hoạt động thiết lập định trước.

Theo khía cạnh của sáng chế, chế độ bảo mật trong đó chức năng truyền tín hiệu truy cập bằng thiết bị trên xe hoặc chức năng truyền mã xác thực bằng thiết bị di động được tắt có thể được thiết lập bằng hoạt động thiết lập định trước. Bằng cách này, các hành vi bất hợp pháp như là tấn công chuyển tiếp có thể được ngăn chặn một cách tin cậy chỉ bằng cách tắt chức năng truyền. Hơn nữa, có thể cải thiện hiệu quả bảo mật trong khi tránh được sự phức tạp của việc xử lý tín hiệu.

Ở chế độ bảo mật, cả chức năng truyền tín hiệu truy cập bằng thiết bị trên xe và chức

năng truyền mã xác thực bằng thiết bị di động có thể được tắt.

Trong trường hợp này, ở chế độ bảo mật, cả chức năng truyền tín hiệu truy cập bằng thiết bị trên xe và chức năng truyền mã xác thực bằng thiết bị di động sẽ được tắt. Do đó, cả chức năng truyền tín hiệu truy cập và chức năng truyền mã xác thực đều được tắt, và hiệu quả bảo mật có thể được nâng cao hơn nữa.

Hoạt động thiết lập định trước có thể bao gồm một hoạt động cụ thể trên bộ phận vận hành được bố trí trong thiết bị trên xe.

Trong trường hợp này, vì hoạt động thiết lập định trước được cấu hình bởi hoạt động cụ thể trên bộ phận vận hành được bố trí trong thiết bị trên xe, nên không cần thiết phải bố trí bộ phận vận hành mới riêng biệt để thiết lập chế độ bảo mật, và có thể ngăn chặn sự gia tăng chi phí sản xuất. Hơn nữa, vì chế độ bảo mật có thể được thiết lập mà không cần đến thiết bị di động, khả năng hoạt động có thể được cải thiện.

Hoạt động thiết lập định trước có thể bao gồm hoạt động cụ thể trên bộ phận vận hành được bố trí trong thiết bị di động.

Trong trường hợp này, vì hoạt động thiết lập định trước được cấu hình bởi hoạt động cụ thể trên bộ phận vận hành được bố trí trên thiết bị di động, hoạt động thiết lập có thể được thực hiện từ vị trí từ xa và khả năng hoạt động có thể được cải thiện hơn nữa.

Chế độ bảo mật có thể được giải phóng khi hoạt động giải phóng cụ thể được thực hiện tại bộ phận vận hành được bố trí trên thiết bị trên xe.

Trong trường hợp này, vì chế độ bảo mật có thể được giải phóng khi hoạt động giải phóng định trước được thực hiện trên bộ phận vận hành được bố trí trên thiết bị trên xe, nên không cần bố trí bộ phận vận hành mới riêng biệt để giải phóng chế độ bảo mật. Do đó, có thể ngăn chặn sự gia tăng chi phí sản xuất và khả năng hoạt động có thể được cải thiện.

Chế độ bảo mật có thể được giải phóng khi hoạt động giải phóng cụ thể được thực hiện trên bộ phận vận hành được bố trí trên thiết bị di động.

Trong trường hợp này, vì chế độ bảo mật có thể được giải phóng khi hoạt động giải phóng định trước được thực hiện trên thiết bị di động, nên có thể ngăn chặn một cách tin cậy người thứ ba không thực hiện được hoạt động giải phóng, và do đó, hiệu quả bảo mật có thể được cải thiện hơn nữa.

Khi hoạt động giải phóng được thực hiện trên bộ phận vận hành, chế độ bảo mật có thể được giải phóng và tín hiệu chuyển hướng của xe có thể được nhấp nháy.

Trong trường hợp này, khi hoạt động giải phóng được thực hiện trên bộ phận vận hành, chế độ bảo mật có thể được giải phóng và tín hiệu chuyển hướng của xe có thể được nhấp nháy. Do đó, hoạt động giải phóng có thể đóng vai trò như hoạt động giải phóng chế độ bảo mật và như hoạt động nhấp nháy tín hiệu chuyển hướng của xe để kích hoạt cuộc gọi ngược trả lời.

Hoạt động thiết lập định trước để thiết lập chế độ bảo mật hoặc hoạt động giải phóng định trước để giải phóng chế độ bảo mật có thể được thực hiện trên bộ phận vận hành ở bên của xe được gắn trên xe.

Trong trường hợp này, vì hoạt động thiết lập định trước để thiết lập chế độ bảo mật hoặc hoạt động giải phóng định trước có thể được thực hiện trên bộ phận vận hành ở bên của xe mà được gắn trên xe, hoạt động thiết lập định trước để thiết lập chế độ bảo mật hoặc hoạt động giải phóng định trước để giải phóng chế độ bảo mật có thể được thực hiện ở vị trí tùy ý của xe, và do đó, khả năng hoạt động có thể được cải thiện.

Bộ phận vận hành ở bên của xe có thể được bố trí trong hộp công tắc điều khiển bằng tay được gắn vào tay lái của xe.

Trong trường hợp này, vì bộ phận vận hành ở bên của xe được bố trí trong hộp công tắc điều khiển bằng tay được gắn vào tay lái của xe, nên có thể nâng cao thêm nữa khả năng hoạt động của hoạt động thiết lập định trước để thiết lập chế độ bảo mật hoặc hoạt động giải phóng định trước để giải phóng chế độ bảo mật.

Khi chế độ bảo mật được thiết lập, các mã số ngẫu nhiên có thể được tạo ra và được lưu trữ trong bộ phận lưu trữ của thiết bị trên xe và bộ phận lưu trữ của thiết bị di động tương ứng, và khi hoạt động giải phóng được thực hiện, mã số ngẫu nhiên được lưu trữ trong bộ phận lưu trữ của thiết bị di động có thể được so sánh với mã số ngẫu nhiên được lưu trữ trong bộ phận lưu trữ của thiết bị trên xe, và chế độ bảo mật có thể được giải phóng chỉ khi khớp mã số ngẫu nhiên.

Trong trường hợp này, khi chế độ bảo mật được thiết lập, các mã số ngẫu nhiên được tạo ra và được lưu trữ trong bộ phận lưu trữ của thiết bị trên xe và bộ phận lưu trữ của thiết bị di động, tương ứng. Hơn nữa, khi hoạt động giải phóng được thực hiện, mã số ngẫu nhiên được lưu trữ trong bộ phận lưu trữ của thiết bị di động được so sánh với mã số ngẫu nhiên được lưu trữ trong bộ phận lưu trữ của thiết bị trên xe. Chỉ khi các mã số ngẫu nhiên này khớp nhau, chế độ bảo mật được giải phóng. Do đó, hiệu quả bảo mật có thể được duy trì bằng cách so sánh các mã số ngẫu nhiên.

Thiết bị trên xe có thể có chức năng cố định mà có khả năng truyền sóng tần số thấp đến thiết bị di động để làm cho thiết bị di động tạo ra nguồn điện và truyền không dây mã xác thực bằng nguồn điện đã được tạo ra.

Trong trường hợp này, thiết bị trên xe có chức năng cố định mà có khả năng truyền tần số thấp đến thiết bị di động để làm cho thiết bị di động tạo ra nguồn điện và truyền không dây mã xác thực bằng nguồn điện đã được tạo ra. Vì vậy, có thể thuận lợi đối phó với trường hợp khẩn cấp như là cạn kiệt pin của thiết bị di động.

Hệ thống truyền thông không dây có thể còn bao gồm thiết bị thông báo có khả năng thông báo sự có hoặc không có của việc thiết lập chế độ bảo mật hoặc xảy ra lỗi.

Trong trường hợp này, sự truyền thông không dây bao gồm thiết bị thông báo có khả năng thông báo sự có hoặc không có của việc thiết lập chế độ bảo mật hoặc khi xảy ra lỗi. Do đó, có thể nhận biết và nắm bắt được trạng thái thiết lập của chế độ bảo mật hoặc sự có

hoặc không có lỗi.

Hoạt động thiết lập định trước để thiết lập chế độ bảo mật có thể được bật hoặc tắt trước.

Trong trường hợp này, việc thiết lập định trước để thiết lập chế độ bảo mật có thể được bật hoặc tắt trước. Vì vậy, có thể ngăn chặn sự thiết lập chế độ bảo mật do hoạt động lỗi bằng cách làm cho hoạt động thiết lập định trước bị vô hiệu hóa trước.

Yêu cầu bảo hộ

1. Hệ thống truyền thông không dây bao gồm:

thiết bị trên xe được gắn trên xe, thiết bị trên xe có khả năng truyền không dây tín hiệu truy cập;

thiết bị chìa khóa từ xa di động, mà có thể được mang bởi người sở hữu, có khả năng truyền không dây mã xác thực xe cụ thể với điều kiện là tín hiệu truy cập được nhận từ thiết bị trên xe;

thiết bị đầu vào vật lý được tạo cấu hình để thiết lập hoặc giải phóng chế độ bảo mật, trong đó thông báo được gửi đến cả thiết bị trên xe và thiết bị đầu vào vật lý và thiết bị chìa khóa từ xa di động khi chế độ bảo mật được thiết lập; và

bộ điều khiển có khả năng:

xác định liệu chế độ an toàn có được thiết lập hay không bởi thiết bị đầu vào vật lý được vận hành bởi người sở hữu;

khi chế độ an toàn được thiết lập trong thiết bị trên xe, làm vô hiệu hóa thiết bị chìa khóa từ xa di động để truy cập thiết bị trên xe thông qua mạng không dây, hoặc làm vô hiệu hóa thiết bị trên xe để truy cập thiết bị chìa khóa từ xa di động thông qua mạng không dây; và

khi chế độ an toàn không được thiết lập trong thiết bị trên xe, cho phép thiết bị chìa khóa từ xa di động truy cập thiết bị trên xe thông qua mạng không dây,

trong đó chế độ an toàn được thiết lập bởi hoạt động thiết lập định trước.

2. Hệ thống truyền thông không dây theo điểm 1, trong đó:

ở chế độ bảo mật, cả chức năng truyền tín hiệu truy cập bằng thiết bị trên xe và chức năng truyền mã xác thực xe cụ thể bằng thiết bị chìa khóa từ xa di động được dừng.

3. Hệ thống truyền thông không dây theo điểm 1, trong đó:

chế độ bảo mật có thể được thiết lập từ thiết bị trên xe.

4. Hệ thống truyền thông không dây theo điểm 1, trong đó:

chế độ bảo mật có thể được thiết lập từ thiết bị chìa khóa từ xa di động.

5. Hệ thống truyền thông không dây theo điểm 1, trong đó:

chế độ bảo mật có thể từ thiết bị trên xe.

6. Hệ thống truyền thông không dây theo điểm 5, trong đó:

khi chế độ bảo mật được thiết lập, các mã số ngẫu nhiên được tạo ra và được lưu trữ trong bộ phận lưu trữ của thiết bị trên xe và bộ phận lưu trữ của thiết bị chìa khóa từ xa di động tương ứng, và

khi hoạt động giải phóng được thực hiện, mã số ngẫu nhiên được lưu trữ trong bộ phận lưu trữ của thiết bị chìa khóa từ xa di động có thể được so sánh với mã số ngẫu nhiên được lưu trữ trong bộ phận lưu trữ của thiết bị trên xe, và chế độ bảo mật được giải phóng chỉ khi các mã số ngẫu nhiên khớp nhau.

7. Hệ thống truyền thông không dây theo điểm 1, trong đó:

chế độ bảo mật có thể được giải phóng từ thiết bị chìa khóa từ xa di động.

8. Hệ thống truyền thông không dây theo điểm 7, trong đó,

khi chế độ bảo mật được giải phóng, tín hiệu chuyển hướng phương tiện được nhấp nháy.

9. Hệ thống truyền thông không dây theo điểm 1, trong đó:

thiết lập chế độ bảo mật hoặc giải phóng chế độ an toàn có thể được thực hiện trong bộ phận vận hành ở bên của xe được gắn với xe.

10. Hệ thống truyền thông không dây theo điểm 9, trong đó:

bộ phận vận hành ở bên của xe được bố trí ở trong hộp công tắc điều khiển bằng tay được gắn vào tay lái của xe.

11. Hệ thống truyền thông không dây theo điểm 1, trong đó thiết bị trên xe có chức năng cố định mà có khả năng truyền sóng tần số thấp đến thiết bị chìa khóa từ xa di động để làm cho

thiết bị chìa khóa từ xa di động để tạo ra nguồn điện và truyền không dây mã xác thực xe cụ thể bằng nguồn điện đã được tạo ra.

12. Hệ thống truyền thông không dây theo điểm 1, trong đó hệ thống còn bao gồm bộ chỉ báo có khả năng thông báo việc có hoặc không có sự thiết lập chế độ bảo mật hoặc sự xuất hiện lỗi.

13. Hệ thống truyền thông không dây theo điểm 1, trong đó:

hoạt động thiết lập định trước để thiết lập chế độ bảo mật có thể được phép hoặc vô hiệu hóa trước.

14. Hệ thống truyền thông không dây theo điểm 1, trong đó:

khi mã xác thực xe cụ thể nhận được bởi thiết bị trên xe được xác minh, thiết bị chìa khóa từ xa di động được phép khởi động động cơ của xe.

15. Hệ thống truyền thông không dây theo điểm 1, trong đó:

khi chế độ bảo mật được thiết lập, thiết bị trên xe không được truyền tín hiệu truy cập, hoặc thiết bị chìa khóa từ xa di động không được truyền mã xác thực xe cụ thể đến thiết bị trên xe.

16. Hệ thống truyền thông không dây theo điểm 1, trong đó thiết bị đầu vào vật lý là nút ấn hoặc công tác.

17. Hệ thống truyền thông không dây theo điểm 1, trong đó thiết bị đầu vào vật lý được tạo cấu hình để thiết lập chế độ bảo mật mà vô hiệu hóa thiết bị chìa khóa từ xa di động để truyền thông với thiết bị trên xe thông qua mạng không dây, hoặc vô hiệu hóa thiết bị trên xe để truyền thông với thiết bị chìa khóa từ xa di động thông qua mạng không dây.

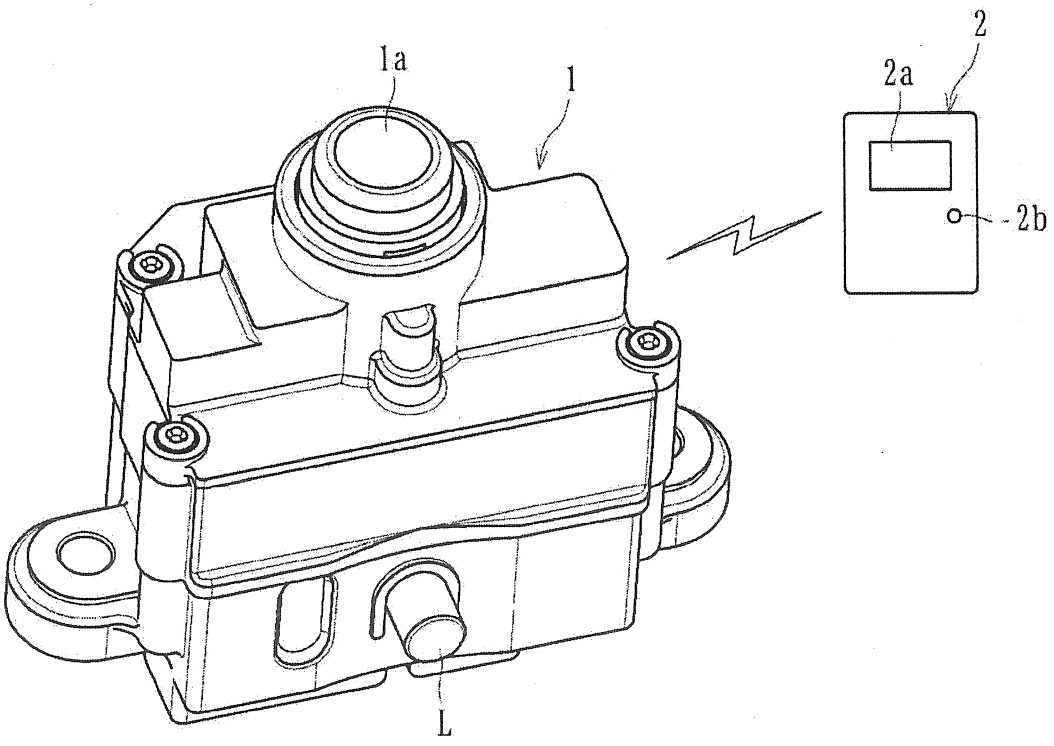


FIG. 1

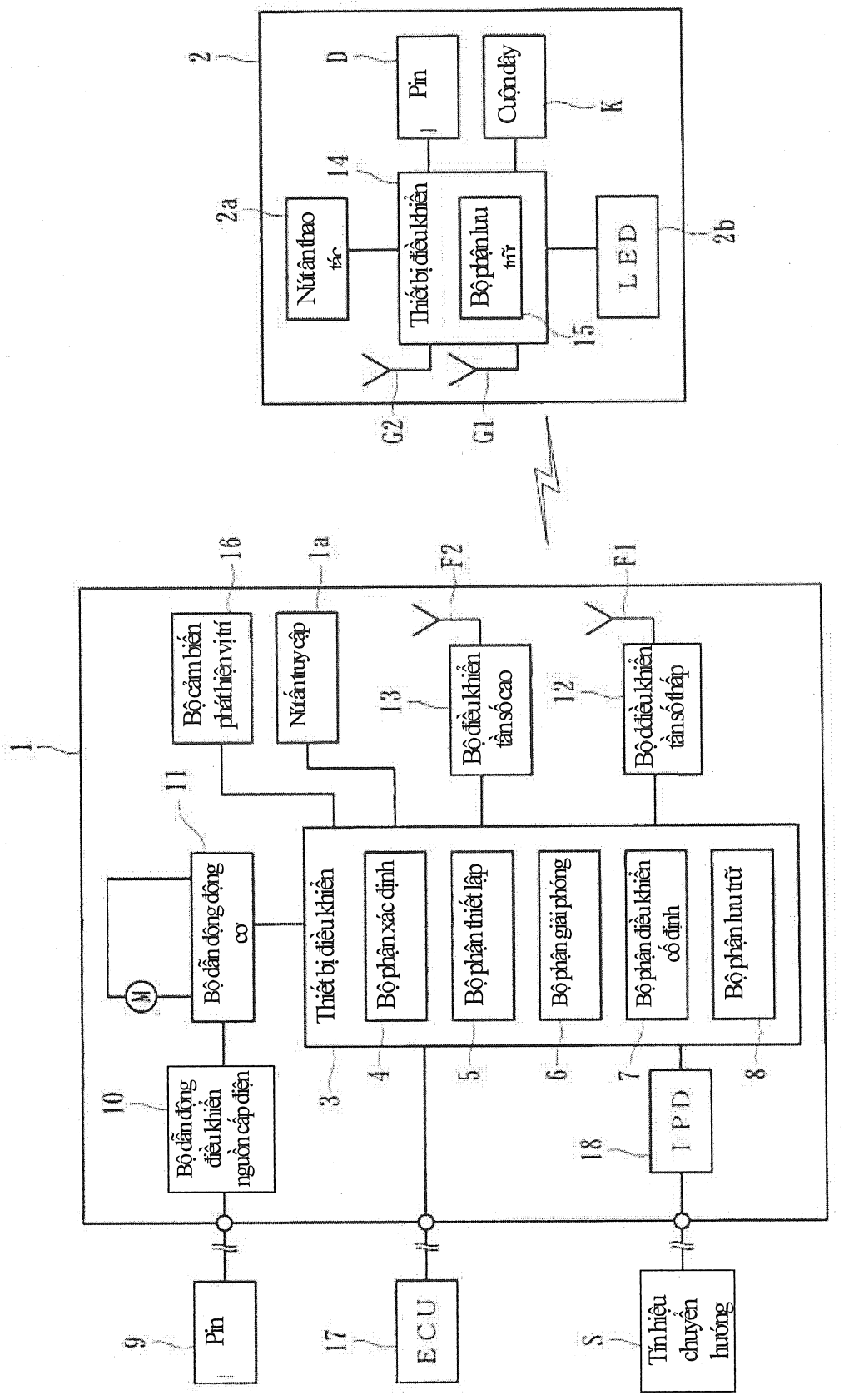

2
D
Pin
Cuộn dây
K
14
2a
Nút ấn thao tác
Thiết bị điều khiển
Bộ phận lưu trữ
15
L E D
2b
G2
G1
1
16
Bộ cảm biến phát hiện vị trí
1a
Nút ấn truy cập
F2
F1
13
Bộ điều khiển tần số cao
12
Bộ điều khiển tần số thấp
11
Bộ dẫn động động cơ
M
Thiết bị điều khiển
Bộ phận xác định
Bộ phận thiết lập
Bộ phận giải phóng
Bộ phận điều khiển cố định
Bộ phận lưu trữ
10
Bộ dẫn động điều khiển nguồn cấp điện
3
4
5
6
7
8
18
I P D
9
Pin
17
E C U
S
Tín hiệu chuyển hướng

FIG. 2

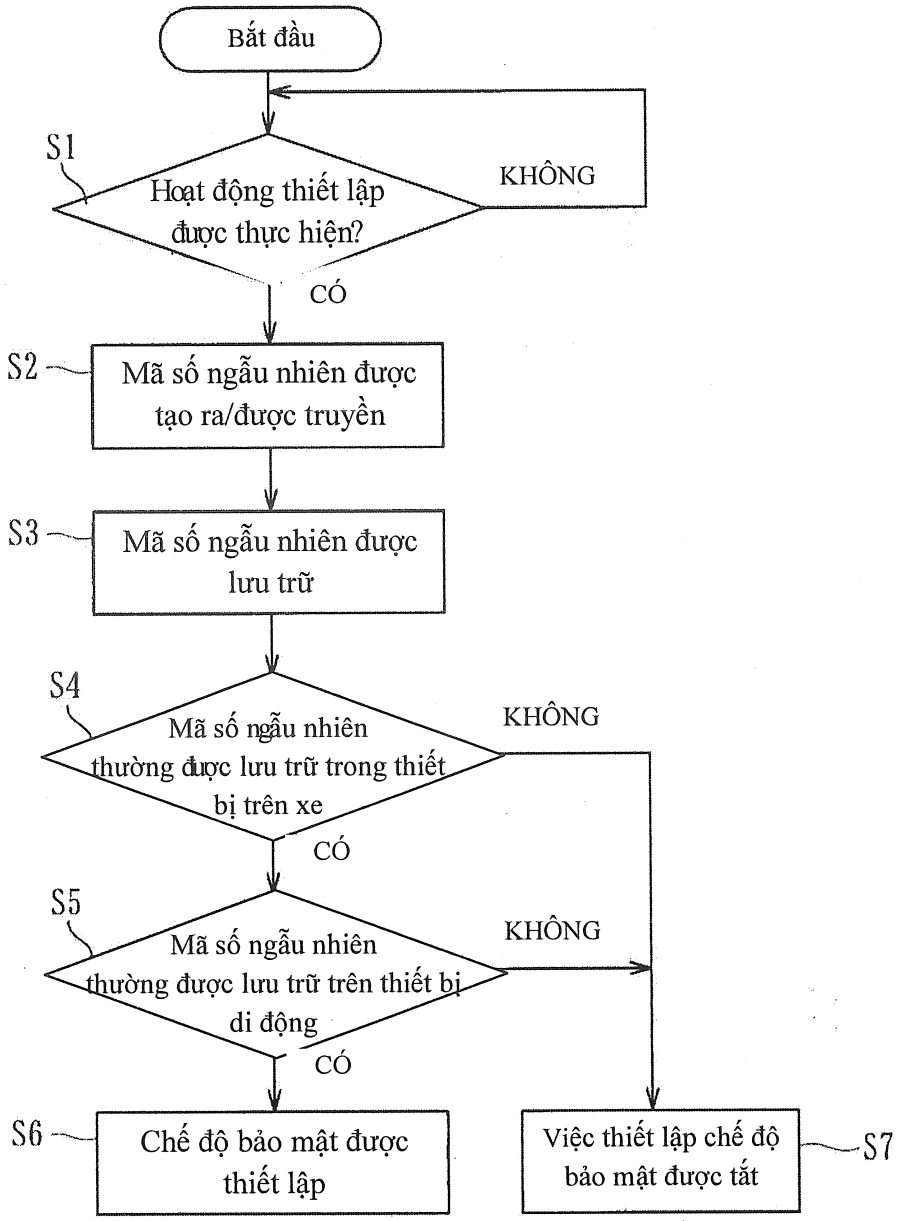

Bắt đầu
S1
Hoạt động thiết lập được thực hiện?
KHÔNG
CÓ
S2
Mã số ngẫu nhiên được tạo ra/được truyền
S3
Mã số ngẫu nhiên được lưu trữ
S4
Mã số ngẫu nhiên thường được lưu trữ trong thiết bị trên xe
KHÔNG
CÓ
S5
Mã số ngẫu nhiên thường được lưu trữ trên thiết bị di động
KHÔNG
CÓ
S6
Chế độ bảo mật được thiết lập
Việc thiết lập chế độ bảo mật được tắt
S7

FIG. 3

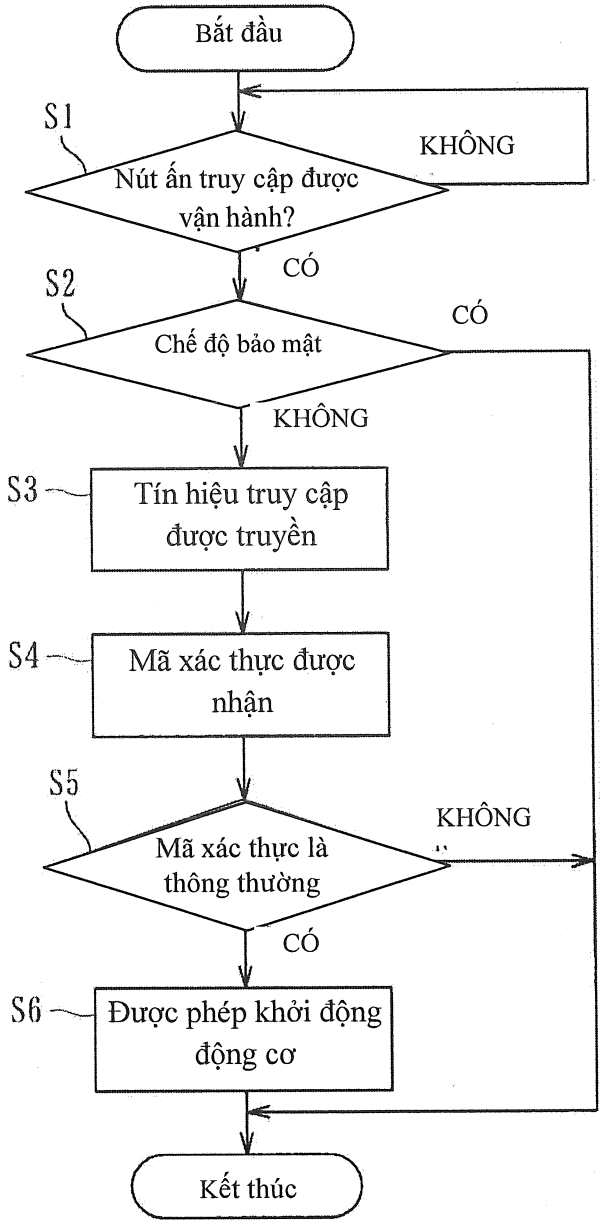

Bắt đầu
S1
Nút ấn truy cập được vận hành?
KHÔNG
CÓ
S2
Chế độ bảo mật
CÓ
KHÔNG
S3
Tín hiệu truy cập được truyền
S4
Mã xác thực được nhận
S5
Mã xác thực là thông thường
KHÔNG
CÓ
S6
Được phép khởi động động cơ
Kết thúc

FIG. 4

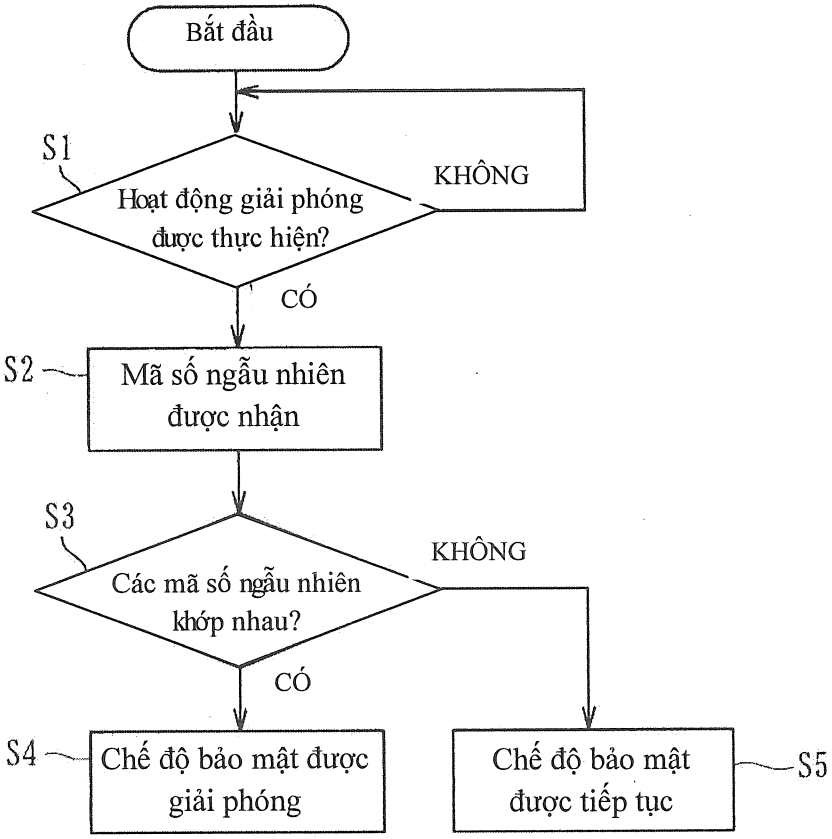

Bắt đầu
S1
Hoạt động giải phóng được thực hiện?
KHÔNG
CÓ
S2
Mã số ngẫu nhiên được nhận
S3
Các mã số ngẫu nhiên khớp nhau?
KHÔNG
CÓ
S4
Chế độ bảo mật được giải phóng
Chế độ bảo mật được tiếp tục
S5

FIG. 5

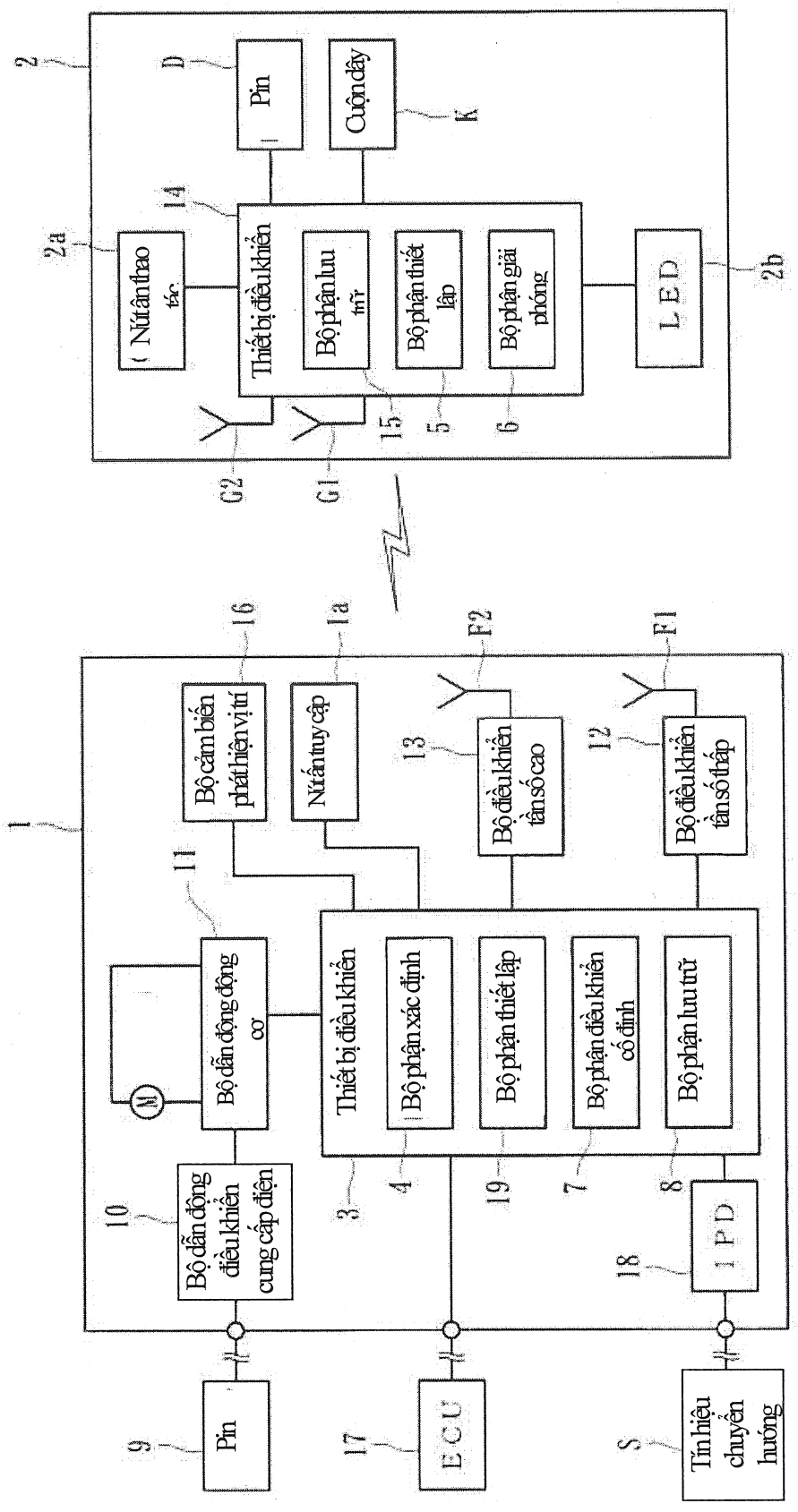

2
D
Pin
Cuộn dây
K
14
2a
Nút thao tác
Thiết bị điều khiển
Bộ phận lưu trữ
Bộ phận thiết lập
Bộ phận giải phóng
LED
2b
G2
G1
15
5
6
1
16
1a
F2
F1
Bộ cảm biến phát hiện vị trí
Nút ấn tuy cập
13
12
Bộ điều khiển tần số cao
Bộ điều khiển tần số thấp
11
M
Bộ dẫn động động cơ
Thiết bị điều khiển
Bộ phận xác định
Bộ phận thiết lập
Bộ phận điều khiển cố định
Bộ phận lưu trữ
10
Bộ dẫn động điều khiển cung cấp điện
3
4
19
7
8
18
IPD
9
Pin
17
ECU
S
Tín hiệu chuyển hướng

FIG. 6

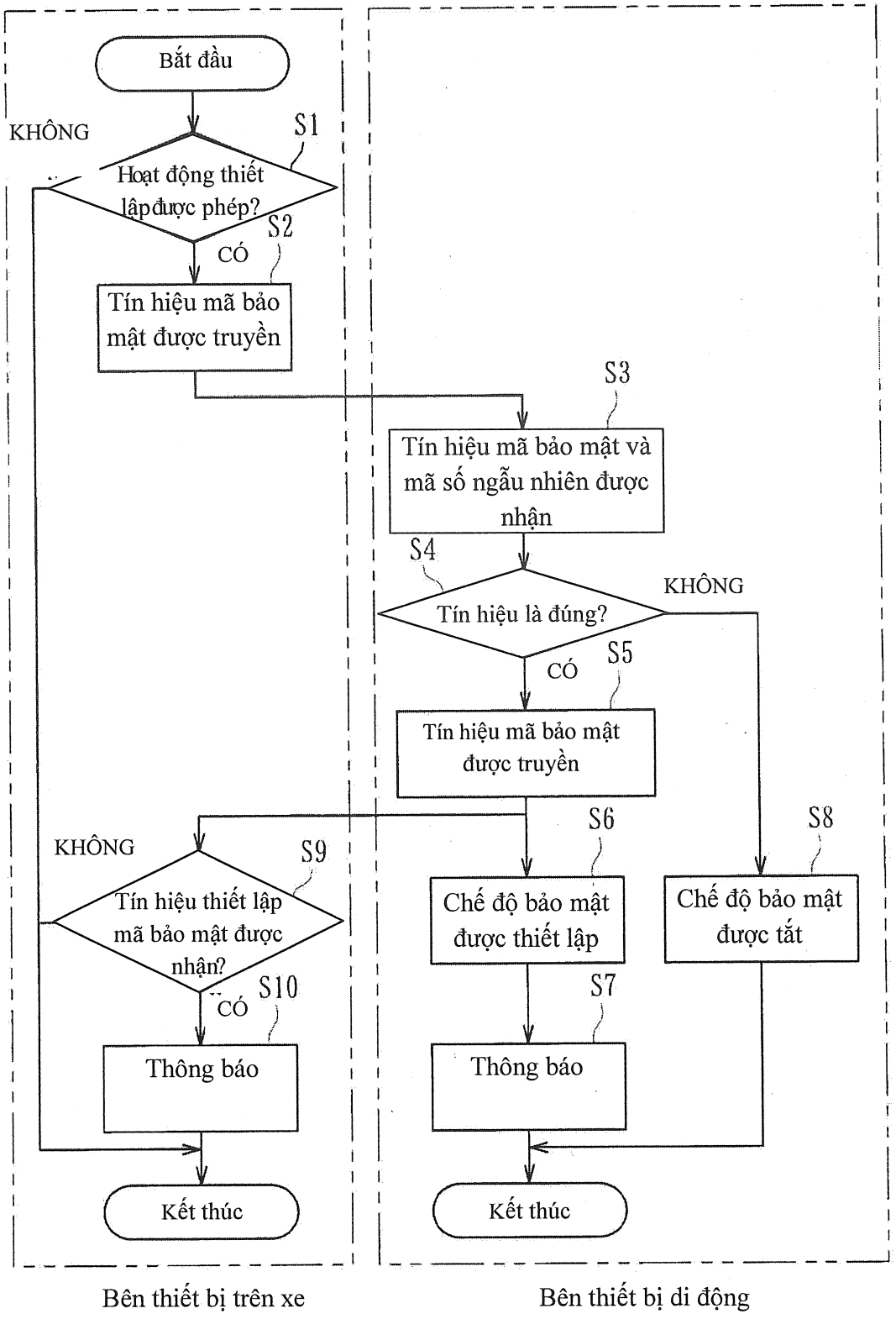

Bắt đầu
KHÔNG
S1
Hoạt động thiết lập được phép?
CÓ
S2
Tín hiệu mã bảo mật được truyền
S3
Tín hiệu mã bảo mật và mã số ngẫu nhiên được nhận
S4
Tín hiệu là đúng?
KHÔNG
CÓ
S5
Tín hiệu mã bảo mật được truyền
S6
Chế độ bảo mật được thiết lập
S8
Chế độ bảo mật được tắt
S7
Thông báo
KHÔNG
S9
Tín hiệu thiết lập mã bảo mật được nhận?
CÓ
S10
Thông báo
Kết thúc
Kết thúc
Bên thiết bị trên xe
Bên thiết bị di động

FIG. 7

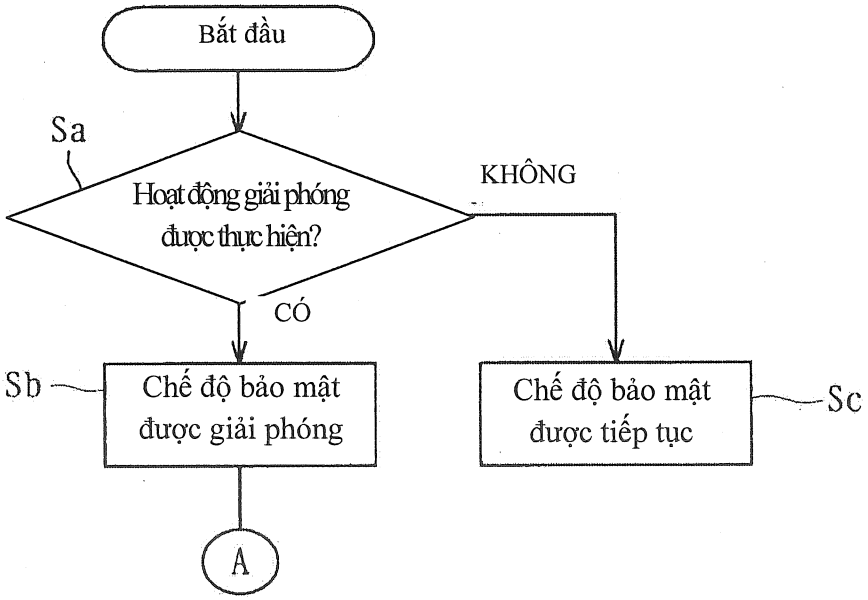

Bắt đầu
Sa
Hoạt động giải phóng được thực hiện?
KHÔNG
CÓ
Sb
Chế độ bảo mật được giải phóng
Chế độ bảo mật được tiếp tục
Sc
A

FIG. 8

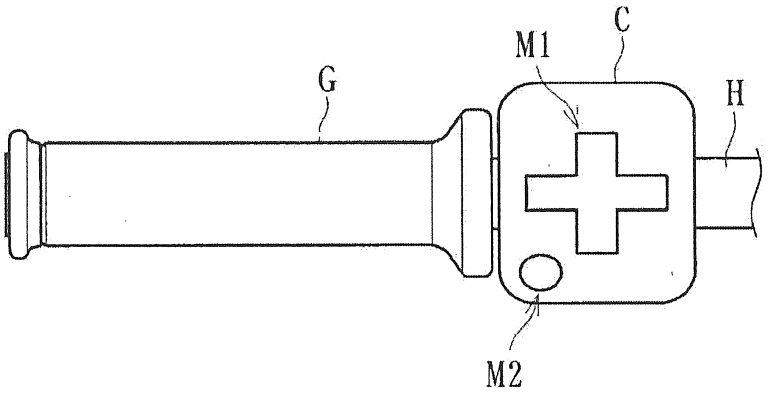

C
M1
G
H
M2

FIG. 9