(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104936129 B
(45)授权公告日 2018.11.16

(21)申请号 201510095533.7

(22)申请日 2015.03.03

(65)同一申请的已公布的文献号
申请公布号 CN 104936129 A

(43)申请公布日 2015.09.23

(30)优先权数据
1452225 2014.03.18 FR

(73)专利权人 质子世界国际公司
地址 比利时扎芬特姆
专利权人 意法半导体(鲁塞)公司

(72)发明人 O·范涅尤文胡伊泽
C·H·里卡尔

(74)专利代理机构 北京市金杜律师事务所 11256
代理人 王茂华 黄倩

(51)Int.Cl.
*H04W 4/80*(2018.01)
*H04W 40/24*(2009.01)

(56)对比文件
CN 102792724 A,2012.11.21,
CN 102792723 A,2012.11.21,
US 2010227553 A1,2010.09.09,

审查员 李宛璐

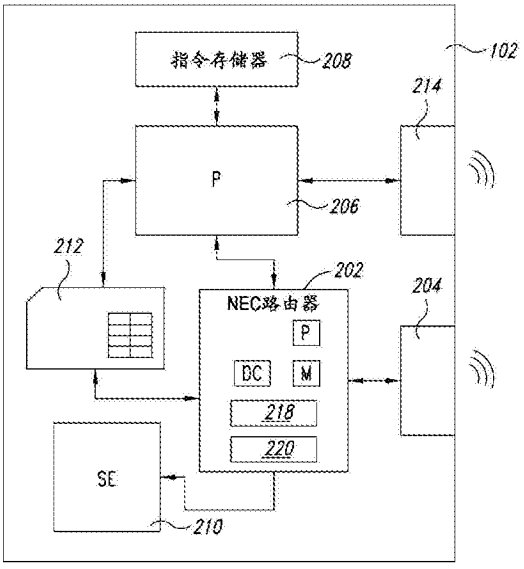
权利要求书3页 说明书9页 附图4页

(54)发明名称

安全NFC路由

(57)摘要

本发明的实施例涉及安全NFC路由。NFC设备的处理设备接收由被加载到NFC设备的存储器中的第一应用发起的请求，以修改NFC设备的NFC路由器的NFC路由表的一个或多个参数。NFC路由表具有指示NFC消息将被路由至何设备的参数。处理设备检索与应用相关联的第一标识符并向NFC路由器传输第一标识符。NFC路由器基于第一标识符验证应用是否被授权以修改路由表。




CN 104936129 B

1.一种用于修改路由参数的方法,包括:

由近场通信(NFC)设备的处理设备接收由加载到所述NFC设备的存储器中的第一应用发起的请求,以修改所述NFC设备的NFC路由器的NFC路由表的一个或多个参数,所述NFC路由表具有指示NFC消息将被路由至何设备的参数;

由所述处理设备检索与所述第一应用相关联的第一标识符;

由所述处理设备向所述NFC路由器传输所述第一标识符;以及

由所述NFC路由器基于所述第一标识符验证所述第一应用是否被授权以修改所述路由表。

2.根据权利要求1所述的方法,其中所述第一标识符是所述应用的数字签名。

3.根据权利要求1所述的方法,其中验证所述第一应用是否被授权以修改所述路由表包括:由所述NFC路由器访问被授权以修改所述路由表的应用的标识符的列表,以及验证所述第一标识符是否在所述列表上。

4.根据权利要求3所述的方法,包括在所述NFC设备的软件更新期间修改所述标识符的列表。

5.根据权利要求4所述的方法,包括通过所述NFC设备的安全元件执行在安全更新期间修改所述标识符的列表。

6.根据权利要求1所述的方法,包括使用第一消息格式在所述处理设备和所述NFC路由器之间传输与NFC通信相关的消息,并且使用与所述第一消息格式不同的第二消息格式从所述处理设备向所述NFC路由器传输所述第一标识符。

7.根据权利要求6所述的方法,其中所述第一消息格式使用第一头部,并且所述第二消息格式使用与所述第一头部不同的第二头部。

8.根据权利要求1所述的方法,其中所述处理设备包括适于与所述NFC路由器通信的通信驱动器,并且其中所述通信驱动器使用第一通信协议与所述NFC路由器通信以传输与NFC通信相关的消息,并使用与所述第一通信协议不同的第二通信协议向所述NFC路由器传输所述第一标识符。

9.根据权利要求8所述的方法,其中所述第二通信协议不同于所述第一通信协议之处在于所述第二通信协议包括不能被所述处理设备复制的传输规则。

10.根据权利要求8所述的方法,其中所述第一通信协议包括连续消息之间的停止条件,并且所述第二通信协议传输两个连续消息,而在所述两个连续消息之间没有停止条件。

11.一种近场通信(NFC)路由器,包括:

一个或多个存储器,其在操作时存储近场通信(NFC)路由表;以及

电路,其在操作时:

基于所述路由表确定接收的NFC消息的路由;以及

确定与修改所述路由表的请求相关联的接收的应用标识符是否与被授权以修改所述路由表的应用相关联。

12.根据权利要求11所述的NFC路由器,其中所述接收的应用标识符为数字应用签名。

13.根据权利要求11所述的NFC路由器,其中在操作时,所述电路访问存储在所述一个或多个存储器中的授权应用的标识符的列表,以确定所述接收的应用标识符是否与被授权以修改所述路由表的应用相关联。

14.根据权利要求11所述的NFC路由器，其中在操作时，所述电路使用第一消息格式路由接收的NFC消息，并使用与所述第一消息格式不同的第二消息格式来处理接收的应用标识符。

15.根据权利要求14所述的NFC路由器，其中所述第一消息格式使用第一头部，并且所述第二消息格式使用与所述第一头部不同的第二头部。

16.根据权利要求11所述的NFC路由器，其中在操作时，所述电路使用第一通信协议来处理NFC消息，并使用与所述第一通信协议不同的第二通信协议来接收应用标识符。

17.根据权利要求16所述的NFC路由器，其中所述第一通信协议包括连续消息之间的停止条件，并且所述第二通信协议使用两个连续消息来传输应用标识符，而在所述两个连续消息之间没有停止条件。

18.一种用于修改路由参数的系统，包括：

处理电路，被配置为执行一个或多个应用；以及

近场通信(NFC)路由器，包括一个或多个存储器，被配置为存储NFC路由表以及被授权以修改所述NFC路由表的一个或多个应用的标识符的列表，其中所述NFC路由器被配置为通过确定接收的应用标识符是否被列出在被授权以修改所述NFC路由表的应用的标识符的所述列表中，而响应与修改所述NFC路由表的请求相关联的接收的应用标识符。

19.根据权利要求18所述的系统，其中所述处理电路和所述NFC路由器被配置为使用第一消息格式来处理与接收的NFC通信相关的消息，并且所述处理电路被配置为使用与所述第一消息格式不同的第二消息格式，向所述NFC路由器传输与修改所述路由表的请求相关联的应用标识符。

20.根据权利要求19所述的系统，其中所述第一消息格式使用第一头部，并且所述第二消息格式使用与所述第一头部不同的第二头部。

21.根据权利要求18所述的系统，其中所述处理电路和所述NFC路由器被配置为使用第一通信协议传输与NFC通信相关的消息，并且所述处理电路被配置为使用与所述第一通信协议不同的第二通信协议，向所述NFC路由器传输与修改所述路由表的请求相关联的应用标识符。

22.根据权利要求21所述的系统，其中所述第一通信协议包括连续消息之间的停止条件，并且所述第二通信协议使用两个连续消息来传输应用标识符，而在所述两个连续消息之间没有停止条件。

23.一种非易失计算机可读介质，其内容使得近场通信(NFC)设备执行一种方法，所述方法包括：

通过以下步骤来响应应用的对于修改所述NFC设备的NFC路由器的NFC路由表的一个或多个参数的请求：

检索与所述应用相关联的应用标识符；

向所述NFC路由器传输所述标识符；以及

基于传输的所述标识符和存储在所述NFC路由器的存储器中的标识符的列表，来确定进行请求的所述应用是否被授权以修改所述路由表。

24.根据权利要求23所述的介质，其中所述方法包括使用第一消息格式处理与NFC通信相关的消息，以及使用与所述第一消息格式不同的第二消息格式向所述NFC路由器传输所

述标识符。

25.根据权利要求23所述的介质，其中所述方法包括使用第一通信协议处理与NFC通信相关的消息，并且使用与所述第一通信协议不同的第二通信协议向所述NFC路由器传输所述标识符。

26.根据权利要求25所述的介质，其中所述第一通信协议包括连续消息之间的停止条件，并且所述第二通信协议使用两个连续消息来传输应用标识符，而在所述两个连续消息之间没有停止条件。

# 安全NFC路由

## 技术领域

[0001] 本公开设计NFC通信领域，特别涉及一种修改NFC路由参数的方法和设备。

## 背景技术

[0002] 移动电话和其他类型移动设备越来越多地装备有NFC(近场通信)接口，其能够使它们执行除了其他功能外的电磁应答器功能。特别地，这些设备能够模仿电磁应答器的功能，其可为非接触卡类型，或者非接触读取器类型。此类功能例如增强移动设备，通过允许其被例如作为电子钱包用于各种应用，允许针对访问服务(例如传输网络)而进行支付。

[0003] 为了仿真非接触卡的操作，移动设备通常装备有非接触前端集成电路(CLF)，也称为NFC路由器。该路由器装备有射频(RF)收发器，其前端耦合至低程天线以匹配电磁应答器的通信能力。在一些应用中，集成在移动设备中或者包括在用户识别模块(SIM)、通用SIM(USIM)或μSD(微型安全数字)的微电路中的安全元件(SE)或嵌入式安全元件(eSE)可用来提供认证。

[0004] NFC路由器包括NFC路由表，其指示由NFC路由器接收的NFC消息应被路由至哪一硬件。例如，某些NFC消息(例如与电子支付的某些类型相关的NFC消息)被路由至移动设备的安全元件。举一个具体例子，VISA应用可运行以与USIM的安全元件通信。其他类型的NFC消息将被路由至移动设备的主处理器。作为一个例子，MasterCard应用可运行在HCE(Host Card Emulation，主卡仿真)，换言之运行在设备主机(Device Host)环境(名称“VISA”和“MasterCard”可对应于注册商标)。

[0005] 考虑到可能经NFC路由器传递的敏感信息，NFC路由表应被保护以避免未授权修改。但是，现有的方案在某些应用环境下不起作用。

## 发明内容

[0006] 在实施例中，一种方法包括：由NFC设备的处理设备接收由加载到NFC设备的存储器中的第一应用发起的请求，以修改NFC设备的NFC路由器的NFC路由表的一个或多个参数，NFC路由表具有指示NFC消息将被路由至何设备的参数；由处理设备检索与第一应用相关联的第一标识符；由处理设备向NFC路由器传输第一标识符；以及由NFC路由器基于第一标识符，验证第一应用是否被授权以修改路由表。

[0007] 根据一个实施例，第一标识符是第一应用的数字签名。

[0008] 根据一个实施例，验证第一应用是否被授权以修改路由表包括：由NFC路由器访问被授权以修改路由表的应用的标识符的列表，以及验证第一标识符是否在列表上。

[0009] 根据一个实施例，该方法包括在NFC设备的软件更新期间修改标识符的列表。

[0010] 根据一个实施例，该方法包括在NFC设备的安全元件执行在安全更新期间修改标识符的列表。

[0011] 根据一个实施例，处理设备使用第一消息格式与NFC路由器通信，并使用与第一消息格式不同的第二消息格式将第一标识符传输至NFC路由器。

[0012] 根据一个实施例，第一消息格式使用第一头部，并且第二消息格式使用与第一头部不同的第二头部。

[0013] 根据一个实施例，处理设备包括适于与NFC路由器通信的通信驱动器，通信驱动器使用第一传输协议与NFC路由器通信，并使用与第一传输协议不同的第二传输协议向NFC路由器传输第一标识符。

[0014] 根据一个实施例，第二传输协议不同于第一传输协议之处在于第二传输协议包括不能被处理设备复制的传输规则。

[0015] 根据一个实施例，第一传输协议提供连续消息之间的停止条件，而第二传输协议包括传输两个连续消息，而在它们之间没有停止条件。

[0016] 在一个实施例中，NFC设备包括：处理设备；以及NFC路由器，NFC路由器包括一个或多个存储器，其存储NFC路由表和被授权以修改NFC路由表的一个或多个应用的标识符的列表，NFC路由器适用于：接收加载到处理设备的存储器中的第一应用的第一标识符，以及期望修改NFC路由表的一个或多个参数；以及基于第一标识符验证第一应用是否被授权以修改路由表。

[0017] 根据一个实施例，第一标识符为应用的数字签名。

[0018] 在一个实施例中，一种方法包括：由近场通信(NFC)设备的处理设备接收由加载到NFC设备的存储器中的第一应用发起的请求，以修改NFC设备的NFC路由器的NFC路由表的一个或多个参数，NFC路由表具有指示NFC消息将被路由至何设备的参数；由处理设备检索与第一应用相关联的第一标识符；由处理设备将第一标识符传输至NFC路由器；以及由NFC路由器基于第一标识符验证第一应用是否被授权以修改路由表。在实施例中，第一标识符是应用的数字标签。在实施例中，验证第一应用是否被授权以修改路由表包括：由NFC路由器访问被授权以修改路由表的应用的标识符的列表，以及验证第一标识符是否在列表上。在实施例中，该方法包括在所述NFC设备的软件更新过程中修改所述标识符的列表。在实施例中，该方法包括在NFC设备的安全元件执行安全更新期间修改所述标识符的列表。在实施例中，该方法包括使用第一消息格式在处理设备和NFC路由器之间传输与NFC通信相关的消息，并且使用与第一消息格式不同的第二消息格式将第一标识符从处理设备传输至NFC路由器。在实施例中，第一消息格式使用第一头部，而第二消息格式使用与第一头部不同的第二头部。在实施例中，其中处理设备包括适于与NFC路由器通信的通信驱动器，并且其中通信驱动器使用第一通信协议与NFC路由器通信以传输与NFC通信相关的消息，并使用与第一通信协议不同的第二通信协议将第一标识符传输至NFC路由器。在实施例中，第二通信协议与第一通信协议的不同之处在于第二通信协议包括不能被处理设备复制的传输规则。在实施例中，第一通信协议包括连续消息之间的停止条件，而第二通信协议传输两个连续消息，而在所述两个连续消息之间没有停止条件。

[0019] 在实施例中，近场通信(NFC)路由器包括：一个或多个存储器，其操作时，存储近场通信(NFC)路由表；以及电路，其操作时：基于路由表确定接收的NFC消息的路由；以及确定与修改路由表的请求相关联的接收的应用标识符是否与被授权以修改路由表的应用相关联。在实施例中，接收的应用标识符为数字应用签名。在实施例中，在操作中，电路访问存储在一个或多个存储器中的授权应用的标识符的列表，以确定接收的应用标识符是否与被授权以修改路由表的应用相关联。在实施例中，在操作中，电路使用第一消息格式来路由接收

的NFC消息并使用与第一消息格式不同的第二消息格式来处理接收的应用标识符。在实施例中，第一消息格式使用第一头部，而第二消息格式使用与第一头部不同的第二头部。在实施例中，在操作中，电路使用第一通信协议来处理NFC消息并使用与第一通信协议不同的第二通信协议来接收应用标识符。在实施例中，第一通信协议包括连续消息之间的停止条件，并且第二通信协议使用两个连续消息传输应用标识符，而在该两个连续消息之间没有停止条件。

[0020] 在实施例中，一种系统包括：处理电路，被配置为执行一个或多个应用；以及近场通信(NFC)路由器，包括一个或多个存储器，被配置为存储NFC路由表以及被授权以修改NFC路由表的一个或多个应用的标识符的列表，其中NFC路由器被配置为通过确定接收的应用标识符是否被列出在被授权以修改NFC路由表的应用的标识符的列表中，而响应与修改NFC路由表的请求相关联的接收的应用标识符。在实施例中，处理电路和NFC路由器被配置为使用第一消息格式来处理与接收的NFC通信相关的消息，并且处理电路被配置为使用与第一消息格式不同的第二消息格式，将与修改路由表的请求相关联的应用标识符传输至NFC路由器。在实施例中，第一消息格式使用第一头部，而第二消息格式使用与第一头部不同的第二头部。在实施例中，处理电路和NFC路由器被配置为使用第一通信协议传输与NFC通信相关的消息，而处理电路被配置为使用与第一通信协议不同的第二通信协议，将与修改路由表的请求相关联的应用标识符传输至NFC路由器。在实施例中，第一通信协议包括连续消息之间的停止条件，并且第二通信协议使用两个连续消息传输应用标识符，而在该两个连续消息之间没有停止条件。

[0021] 在实施例中，非易失计算机可读介质的内容使得近场通信(NFC)设备执行一种方法，该方法包括：通过以下来响应应用对于修改NFC设备的NFC路由器的NFC路由表的一个或多个参数的请求：检索与应用相关联的应用标识符；向NFC路由器传输标识符；以及基于传输的标识符和存储在NFC路由器的存储器中的标识符的列表，来确定进行请求的应用是否被授权以修改路由表。在实施例中，该方法包括使用第一消息格式处理与NFC通信相关的消息，以及使用与第一消息格式不同的第二消息格式向NFC路由器传输标识符。在实施例中，该方法包括使用第一通信协议处理与NFC通信相关的消息，并且使用与第一通信协议不同的第二通信协议向NFC路由器传输标识符。在实施例中，第一通信协议包括连续消息之间的停止条件，而第二通信协议使用两个连续消息传输应用标识符，而在该两个连续消息之间没有停止条件。

## 附图说明

[0022] 前述和其他特征及优势将从以下实施例的详细描述中看出来，如附图所示但并不限于参考附图，其中：

[0023] 图1示意性地示出根据本公开的示例实施例的能够NFC通信的NFC设备；

[0024] 图2示意性地示出根据本公开的示例实施例的更详细的图1的NFC设备；

[0025] 图3示意性地表示根据本公开的示例实施例的NFC路由器的路由表；

[0026] 图4示意性地表示根据本公开的示例实施例的NFC设备的部件；

[0027] 图5为示出根据本公开的示例实施例的更新NFC路由表的参数的方法中的操作的流程图；

[0028] 图6示出根据示例实施例的更详细的图4的NFC接口。

[0029] 图7为根据本公开的示例实施例的表示NFC路由器和NFC设备的应用之间的交互的图表;以及

[0030] 图8为根据本公开的示例实施例的示出具有NFC路由器的通信协议的信号的时序图。

## 具体实施方式

[0031] 在以下描述中,给出许多具体细节以提供示例实施例的完全理解。这些实施例可实现为不具有一个或多个具体细节,或者具有其他方法、部件、材料等。在其他例子中,已知结构、材料或操作,例如集成电路、存储器、SIM卡、驱动器、总线系统等未具体示出或描述以避免使得实施例的各方面不清楚。

[0032] 说明书全文中引用的“一个实施例”或“实施例”意思是结合实施例描述的具体特性、结构或特征被包括在至少一个实施例中。因此,在说明书全文各处出现短语“在一个实施例中”、“根据实施例”或“在实施例中”以及类似短语并不必然都表示相同实施例。而且,具体特性、结构或特征可以适当方式结合在一个或多个实施例中。

[0033] 本文提供的标题仅仅是为方便起见,不能理解为实施例的范围或含义。

[0034] 图1示意性地示出NFC设备102,NFC设备102是能够进行NFC通信的设备。例如,设备102为移动设备,诸如装备有NFC电路(图1未示出)的移动电话、智能电话、平板电脑、数字媒体播放器等。

[0035] 在图1的左手侧,NFC设备102示出为与包含NFC应答器106的读取器104通信。例如,读取器104位于例如传输网络等的限制区域的入口障碍处。替换地,读取器104位于商店或餐馆的销售点处。当与这样的读取器一同使用时,NFC设备102的NFC电路例如操作在标签仿真模式下。

[0036] 在图1的右手侧,NFC设备102示出为经由NFC接口与另一NFC设备108通信。例如,类似于NFC设备102,NFC设备108为能够进行NFC通信的设备,NFC设备108可以为移动设备,例如装备有NFC电路的移动电话、智能电话、平板电脑、数字媒体播放器等。当与另一NFC设备通信时,NFC设备102的NFC电路例如操作在对等模式下,而且通信可由NFC设备中的任一个来发起。

[0037] 图2示意性地示出根据示例实施例的更详细的NFC设备102。

[0038] 如图所示,设备102例如包括NFC路由器(NFC ROUTER)202,本领域也称为非接触前端(contactless front-end,CLF)。NFC路由器202耦合至NFC天线204,而且路由器202和天线204共同提供NFC电路用于仿真NFC应答器的行为。

[0039] NFC路由器202也例如耦合至NFC设备102的主处理设备(P)206。设备206例如包括在存储于指令存储器(INSTR MEM)208的指令控制下的一个或多个处理器。指令存储器208例如为闪存,并且存储已经加载在设备上的一个或多个应用(图1未示出)。NFC路由器202也例如耦合至其他设备,其他设备的安全元件(SE)210和USIM(通用用户识别模块)电路212被示出。安全元件210例如为嵌入式SE(eSE),而USIM电路212例如经由SWP(单线协议)链路耦合至NFC路由器,并且还耦合至主处理设备206。

[0040] 主处理设备206也例如耦合至一个或多个天线214,天线214例如允许在蜂窝网络

和/或根据其他标准(例如Wi-Fi,蓝牙等)的无线通信中的通信。

[0041] NFC路由器202例如包括一个或多个存储器,存储NFC路由表218和被授权以修改NFC路由表的应用的标识符的列表220。NFC路由表218定义用于处理由NFC路由器202接收的NFC消息的规则。特别地,消息可被考虑以处理设备206或者安全元件210、212中的一个为目标。NFC路由器202可包括电路(例如一个或多个处理器P)、一个或多个处理器M、分立电路DC(例如一个或多个比较器、逻辑门等),其可被单独使用或以各种组合来实施NFC路由器202的各种功能。

[0042] 图3表示根据示例实施例的NFC路由器202的路由表218的示例。该表例如实施为查找表(look up table,LUT)。

[0043] 表218包括五列表示输入到表中的参数,包括:指示通信的NFC RF技术的RF技术列(RF);索引列(INDEX)、模式列(PATTERN)和指示与部分输入消息相关的条件的掩码列(MASK),其中索引指示将被考虑的消息的字节,模式定义有效负载的位的某种模式,而掩码指示将被考虑的那些位;以及功率区域(PWR),功率区域指示设备是被开启、关闭还是其电源关闭。图3的右手列包括针对表的每行的参数,其指示相应消息应被路由至哪一个目标设备。

[0044] 在图3的示例中,针对每行,索引为"1",例如指示消息的有效负载的第一字节将被考虑。在表的第一行302中,模式字段为十六进制模式"00FFFF",掩码等于"FFFFFF",意味着整个模式将被考虑,而且目标是设备主机(DH),换言之为处理设备206。在表的第二行304中,模式字段为十六进制模式"000001",掩码等于"0000FF",意味着仅最后两位十六进制值将被考虑,而且目标是安全元件210。在表的第三行306中,模式字段是十六进制模式"000002",掩码等于"0000FF",再次意味着仅最后两位十六进制值将被考虑,而且目标是USIM 212。

[0045] 图3仅提供基于模式识别的NFC路由表的一个示例。本文描述的实施例可被应用于大范围的不同路由表,其中路由由以下一个或多个来定义:

[0046] -用于NFC消息的RF技术;

[0047] -用于NFC消息的RF协议;

[0048] -NFC消息中的模式识别;

[0049] -选择命令,例如根据基于AID(应用ID)值的标准ISO7816。

[0050] 路由表218的未授权修改可例如使针对安全元件210或USIM212的敏感消息被路由至主处理设备,导致潜在安全漏洞或拒绝服务(denial of service,DoS),使终端用户通常感到非常不满意。

[0051] 图4示意性地表示用于执行NFC功能的NFC设备102的部件。NFC设备102例如在其指令存储器208中存储包含NFC功能的三个应用402A,402B和402C。这样的应用,例如运行在使用JVM(Java虚拟机)的Java环境中,并且可被用于如电子钱包这样的某些环境中。例如应用402A,402B和402C包含用于仿真支付卡或安全卡的NFC卡仿真功能,用于读取NFC标签的读卡器功能,和/或允许与另一NFC设备通信的对等功能。

[0052] 应用402A,402B和402C可由处理设备206来执行,处理设备206例如包括以下用于与NFC路由器202接合的功能元件:应用接口(APPLICATION INTERFACE)404,NFC接口(NFC INTERFACE)406,通信协议模块(COMMS PROTOCOL)408以及耦合至NFC路由器202的通信驱动

器(COMMS DRIVER)410。这些功能元件可实施在硬件、软件或固件等,以及其不同组合中。应用接口404例如与具有存储在设备上的各种应用的知识的软件框架相对应,而且允许这些应用被调用。通信协议模块408应用一协议来与NFC路由器202交互,通信驱动器410应用一传输协议来通过物理链路将NFC帧传输至NFC路由器202。在某些实施例中,驱动器410使用I2C接口。NFC接口406例如提供应用以及模块408和410之间的接口,模块408和410负责与NFC路由器202通信。

[0053] 某些防止非授权修改路由表218的保护可由NFC接口406来实施,其可防止某些应用执行这样的修改。但是,在某些情况下可能会绕过NFC接口406。例如,如图4中虚线箭头412所示,恶意软件可经由应用402A使得调试模式被进入,从而使得这种应用可绕过NFC接口406直接与通信协议模块408通信。因此,根据本文描述的实施例,由NFC路由器202存储的授权应用表220可提供替换的或附加的保护机制,现在将参考图5来更详细描述。

[0054] 图5为示出根据示例实施例防止非授权修改NFC路由表218的方法的操作的流程图。假设图4的应用402A已经发出修改路由表218的一个或多个参数的请求。

[0055] 在第一操作502中,修改NFC路由器的路由表的请求由处理设备206的通信协议模块408接收。该请求例如经由处理设备206的NFC接口406来接收。替换地,如上文所述,在设备上存在恶意软件的情况下,NFC接口406可以被绕过,由通信协议模块408直接从应用接收请求。

[0056] 在随后操作504中,应用的标识符由通信协议模块408来检索。例如,模块408从NFC接口406请求发起请求的应用的签名。这样的签名例如针对应用是唯一的,并且通过NFC设备102的操作系统提供商/手机制造商被归于该应用,以允许其被安装在设备上。

[0057] 在随后操作506中,标识符以验证请求的形式经由通信驱动器410传输至NFC路由器202。而且,如下文的更详细描述,在某些实施例中,这种请求可进一步通过调节消息传输协议被安全化,从而NFC路由器202可检查该验证请求来自通信协议模块408。

[0058] 在随后操作508中,NFC路由器202基于标识符来验证应用是否被授权以修改路由表218。

[0059] 如上文所述,NFC路由器202例如在存储器中存储所有授权应用的签名的列表220。该列表可例如仅在安全会话期间被修改,例如在由NFC设备的软件提供商提供的软件更新期间。特别地,如果应用开发者希望其应用被授权以修改路由表,其例如请求手机制造商/操作系统提供商将这些应用的签名加入授权应用表220中。这种修改继而可在(在例如使用MAC(消息验证码)来保护的安全会话期间执行的)后续软件更新期间进行。而且,在某些实施例中,该列表可附加地或替换地在由NFC设备的安全元件执行的安全更新期间(例如在安全管理会话期间)被修改。

[0060] 如果应用的签名在授权应用的标识符的列表上,则NFC路由器202例如允许路由表的修改,但是如果签名不在列表上,则NFC路由器202例如通知否定响应的通信协议408,并修改请求被拒绝。

[0061] 图6示出根据示例实施例的更详细NFC接口406的元件,其中NFC设备使用安卓操作系统,例如Android KitKat(“Android”和“Android KitKat”的名称可对应于注册商标)。

[0062] 接口406例如包括NFC服务模块(NFC SERVICE)602,该NFC服务模块602具有:公共子模块(PUBLIC)604,其支持可用于所有应用的NFC特性,包括路由机制;“NFC附加(NFC

EXTRAS)”子模块606，其支持与提供限制访问的安全元件相关的特性；以及专有子模块(PROPRIETARY)608。路由机制例如不被NFC EXTRAS子模块606相关联的安全性来保护，导致会允许路由表的非授权修改的潜在缺点。

[0063] NFC服务模块602与JNI(Java本地接口)通信，其提供应用接口404与本地(Native World)之间的接口，换言之，由处理设备206直接解译核心程序。JNI 610转而与NFC核心堆栈(NFC CORE STACK)612通信，该NFC核心堆栈提供NFC操作的操作管理。

[0064] 图7示出请求修改路由表的参数的应用(APP)402、经由NFC服务模块(NFC SERVICE)602、JNI 610和通信接口408(在通信接口408HAL(hardware abstraction layer，硬件抽象层)接口情况下)与NFC路由器(NFC R)202之间的通信示例。

[0065] 应用402A通过向NFC服务模块602提出请求(REQ)来发起进程以更新路由参数。该请求由模块602连同应用PID(进程标识符)一起转发至JNI 610。进程标识PID例如伴随来自应用402A的请求并指示哪个应用做出该请求。JNI随后发起将由HAL408来执行的名称检查(PID CHECK)。该名称检查经由NFC核心堆栈612(图7未示出)被传输至HAL 408。

[0066] 替换地，如图7中虚线箭头所示，在某些环境下，例如在NFC设备上存在恶意软件的情况下，用于名称检查的请求可被应用402A直接传输至HAL 408，绕过NFC服务模块602和JNI 610。

[0067] HAL 408接收请求，并从NFC服务模块602检索与应用相关联的应用标识符(APP ID)。例如，应用标识符是应用的数字签名。

[0068] HAL 408随后将应用标识符经由通信驱动器410(图7未示出)传输至NFC路由器202。NFC路由器202验证应用标识符是否对应于授权应用(CHECK APP ID)，并返回结果(RESULT)至HAL 408。该结果由HAL 408转发至JNI 610。

[0069] 在结果为肯定的情况下，例如应用标识符APP ID在授权应用表上，JNI 610继而将更新路由表(REQ UPDATE)的请求传输至HAL 408，HAL 408转而将该请求转发至NFC路由器202。NFC路由器202例如检查应用标识符已经关于该请求被验证，并继而处理该请求且更新由请求中指示的路由表的参数。确认信号(RESULT OK)例如被NFC路由器202传输至HAL408，其转而被HAL 408、JNI 610和NFC服务模块602转发至应用402A。

[0070] 替换地，在由NFC路由器提供以及由JNI 610接收的结果为否定的情况下(例如应用未被授权以修改路由表)，JNI 610例如发送失败消息(RESULT KO)至NFC服务模块602，其继而将该结果转发至应用402。

[0071] 如上文所述，用于验证应用标识符的请求，其在图7中由HAL 408例如使用独有协议传输至NFC路由器，该独有协议与用于通信协议模块408和NFC路由器202之间的消息的普通协议不同。这例如会提供模块408未被绕过的进一步验证。例如，标准消息的NFC帧具有以下元素：

[0072] -MT+GID/Conn ID，其表示消息类型、组标识符和/或消息针对的连接标识符；

[0073] -OID/RFU，(Object Identifier/Reserved for Future Use，对象标识符/预留用于将来使用)，其表示与消息类型和/或目标连接的补充信息；

[0074] -LEN，其表示消息的长度；以及

[0075] -有效负载，包括将由消息传送的数据。

[0076] 根据本文描述的实施例，这种标准NFC帧例如被更新以包括两个附加的头部之一，

一个附加的头部被用于标准消息，另一个不同的附加的头部被用于请求验证应用标识符。例如，用于普通帧的附加的头部为“0x01”，而用于标识符验证的附加的头部为“0x02”。

[0077] 附加地或替换地，在请求验证应用标识符的情况下，通信协议模块408使通信驱动器410修改其传输协议。在这种情况下，在HAL 408之外或者代替HAL 408，驱动器410例如检索来自NFC服务模块602的应用标识符。在实施例中，传输协议的修改例如包括应用不能被任何更高层应用复制的新传输规则。在实施例中，NFC路由器例如是能够解译和处理根据新传输规则所传输的消息的仅有设备。

[0078] 根据一个示例，通信驱动器410应用I2C传输协议，请求被在未由停止条件分离的两个连续帧上传输，现在将参考图8更详细描述。

[0079] 图8为示出根据在标准通信800以及请求验证应用标识符的通信801的情况下的I2C协议，驱动器410和NFC路由器202之间的时钟线SCL和数据线SDA上某些信号的示例。

[0080] 对于标准通信800，两连续帧802、804被停止条件806分离，其例如对应于当时钟线SCL为高时，数据线SDA上的上升沿。

[0081] 对于请求验证应用标识符的通信801，帧802和804之间的停止条件被去除。需要注意这种协议的修改不会影响线上存在的其他从属，因为其对它们来说是显然的，而且目标从属(例如NFC路由器)例如被适配为管理按这种方式修改的帧。

[0082] 本文描述的实施例的优势在于提供鲁棒保护机制来防止对NFC路由器的NFC路由表的未授权修改。

[0083] 因此已经描述至少一个图示的实施例，各种替换、修改和改进对本领域技术人员来说也将容易想到。

[0084] 例如，尽管已经描述与安卓操作系统相关的详细实施例，对本领域技术人员来说显见的是本文的教导可用于其他NFC设备操作系统，例如iOS(名称“iOS”可对应于注册商标)。

[0085] 某些实施例可使用计算机程序产品的形式或包括计算机程序产品。例如，根据一个实施例，提供计算机可读介质，包括适用于执行上文描述的一个或多个方法或功能的计算机程序。该介质可为物理存储介质，例如只读存储器(ROM)芯片，或者磁盘(例如数字通用光盘(DVD-ROM))、高密度磁盘(CD-ROM)、硬盘、存储器、网络或者将由适当驱动或通过适当连接读取的便携媒介物，包括被编码在一个或多个条形码中或者被存储在一个或多个此类算机可读介质上的其他相关代码中并且可被适当读取器设备读取。

[0086] 而且，在某些实施例中，某些系统和/或模块和/或电路和/或块可以其他方式实施或提供，例如至少部分地在固件和/或硬件中，包括但不限于一个或多个专用集成电路(ASICs)、数字信号处理器、分立电路、逻辑门、位移寄存器、标准集成电路、状态机、查找表、控制器(例如，通过执行合适指令，且包括微控制器和/或嵌入式控制器)、现场可编程门阵列(FPGAs)、复杂可编程逻辑控制器件(CPLDs)等，以及采用RFID技术的设备和上述的各种组合。

[0087] 上文描述的各实施例可组合来提供进一步的实施例。如果需要，可以修改实施例的方面以采用各种专利、应用和出版物的概念来提供进一步的实施例。

[0088] 根据上文的详细描述，实施例可进行这些或其他变化。通常地，在以下权利要求中，使用的术语不应解释为限制说明书和权利要求中公开的特定实施例，而应解释为包括

随同这些权利要求能够全部覆盖的等同实施例的各种可能的实施例。因此，权利要求并不被本公开所限制。

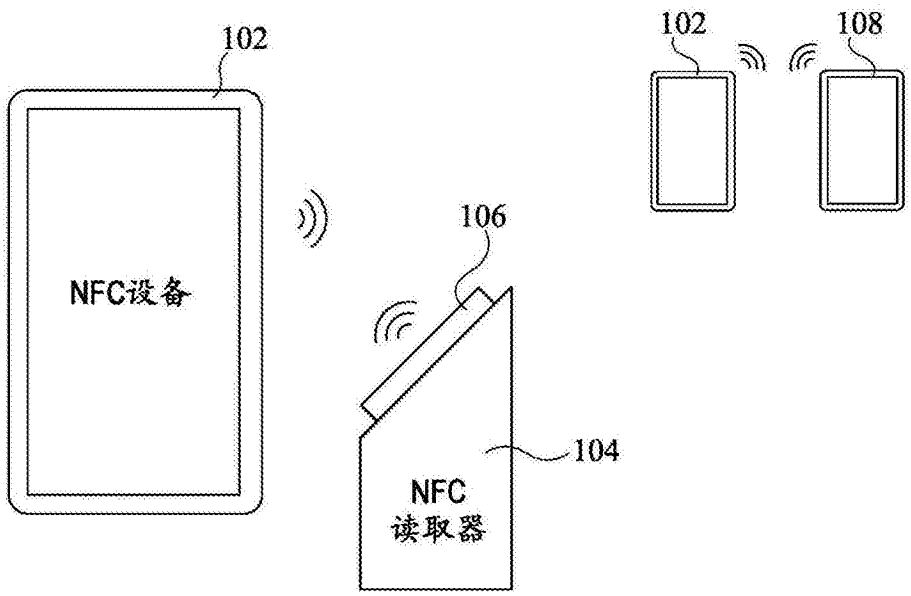

102
NFC设备
106
NFC
读取器
104
102
108

图1

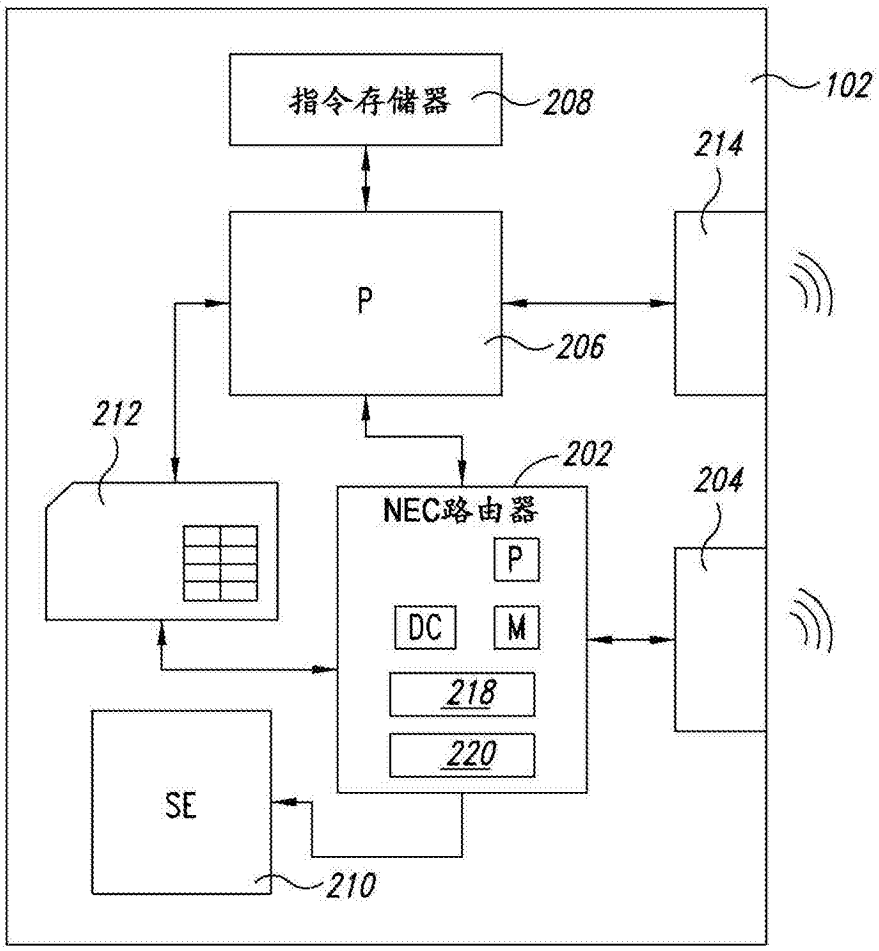

指令存储器
208
102
214
P
206
212
202
NEC路由器
204
P
DC
M
218
220
SE
210

图2

218

| RF | 索引 | 模式 | 掩码 | 功率 | 目标 | |
|---|---|---|---|---|---|---|
| F | 1 | 00FFFF | FFFFFF | 1 | DH | 302 |
| F | 1 | 000001 | 0000FF | 1 | SE | 304 |
| F | 1 | 000002 | 0000FF | 1 | USIM | 306 |

图3

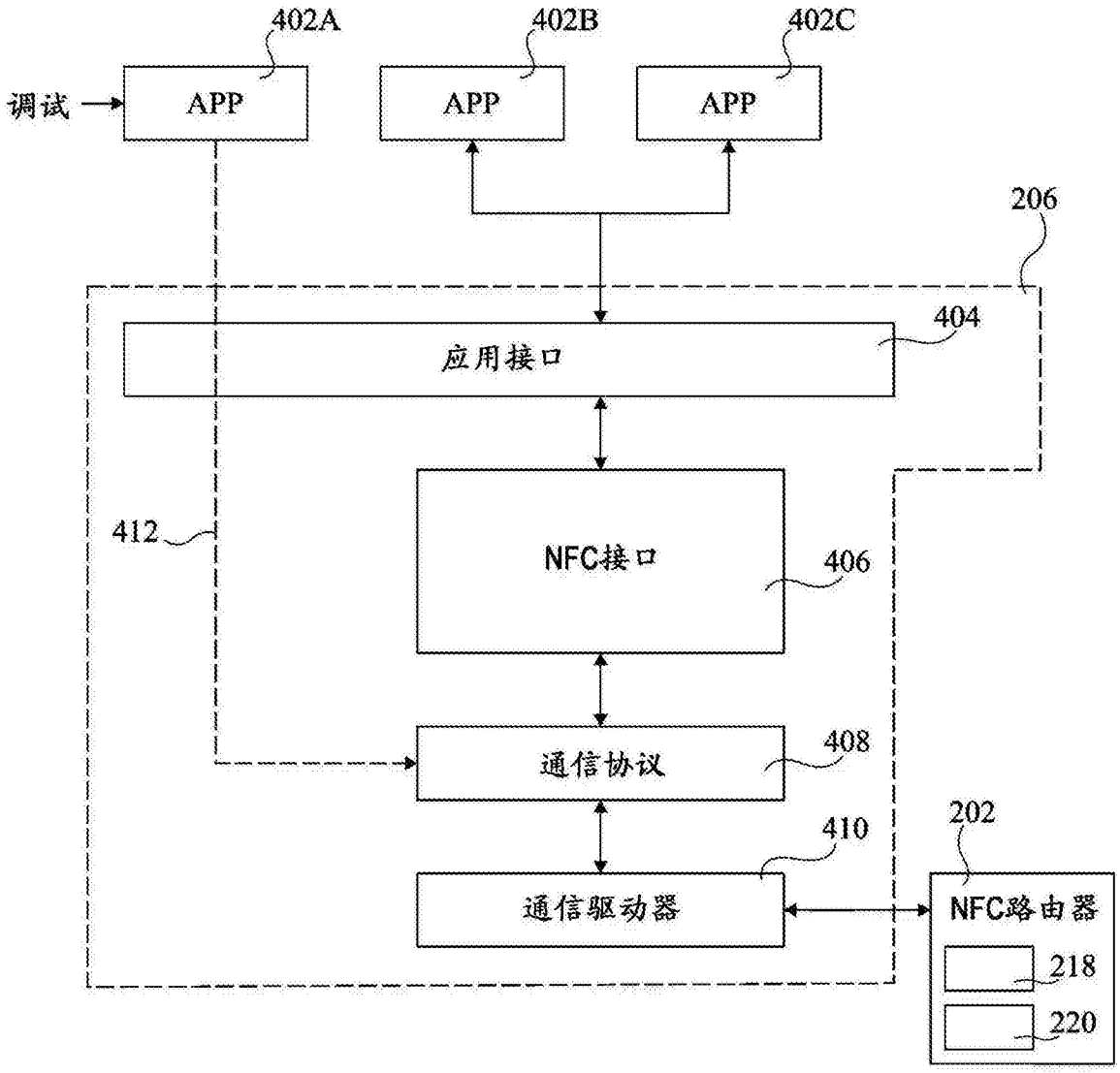



图4

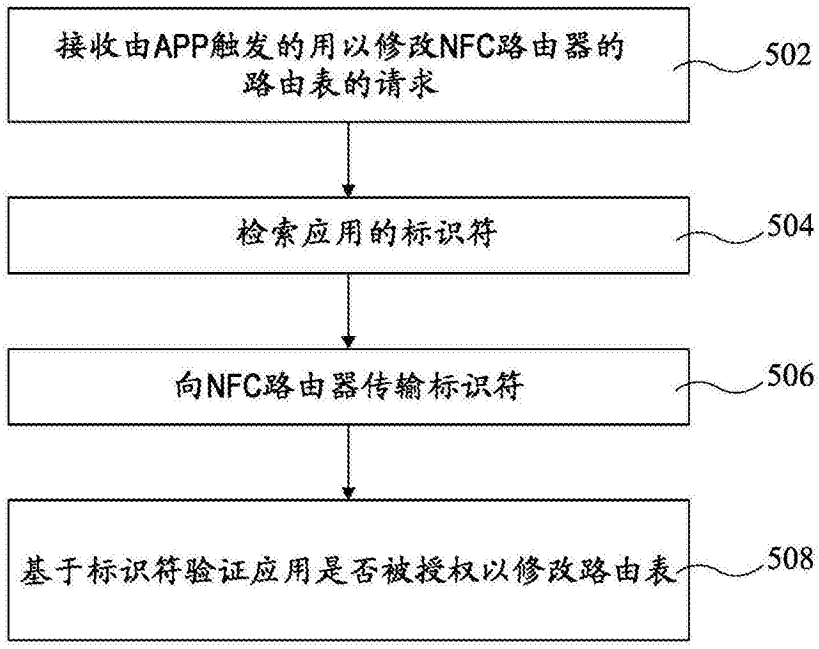

接收由APP触发的用以修改NFC路由器的路由表的请求
502
检索应用的标识符
504
向NFC路由器传输标识符
506
基于标识符验证应用是否被授权以修改路由表
508

图5

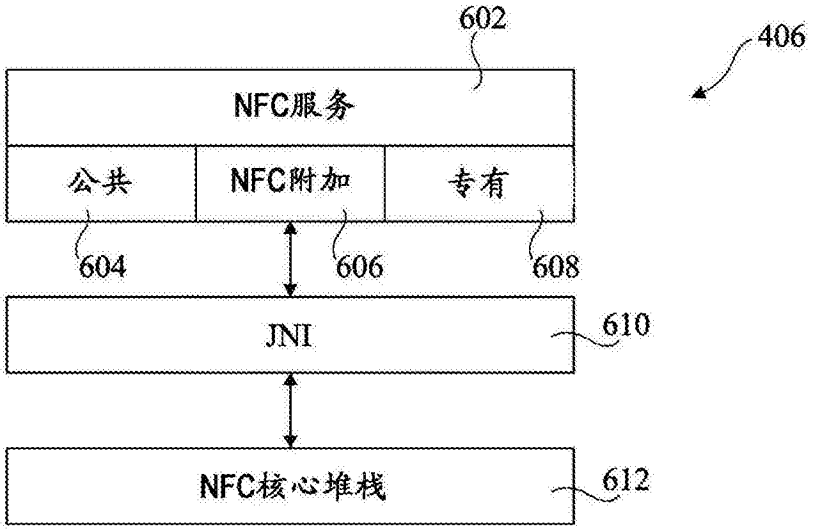

602
406
NFC服务
公共
NFC附加
专有
604
606
608
JNI
610
NFC核心堆栈
612

图6

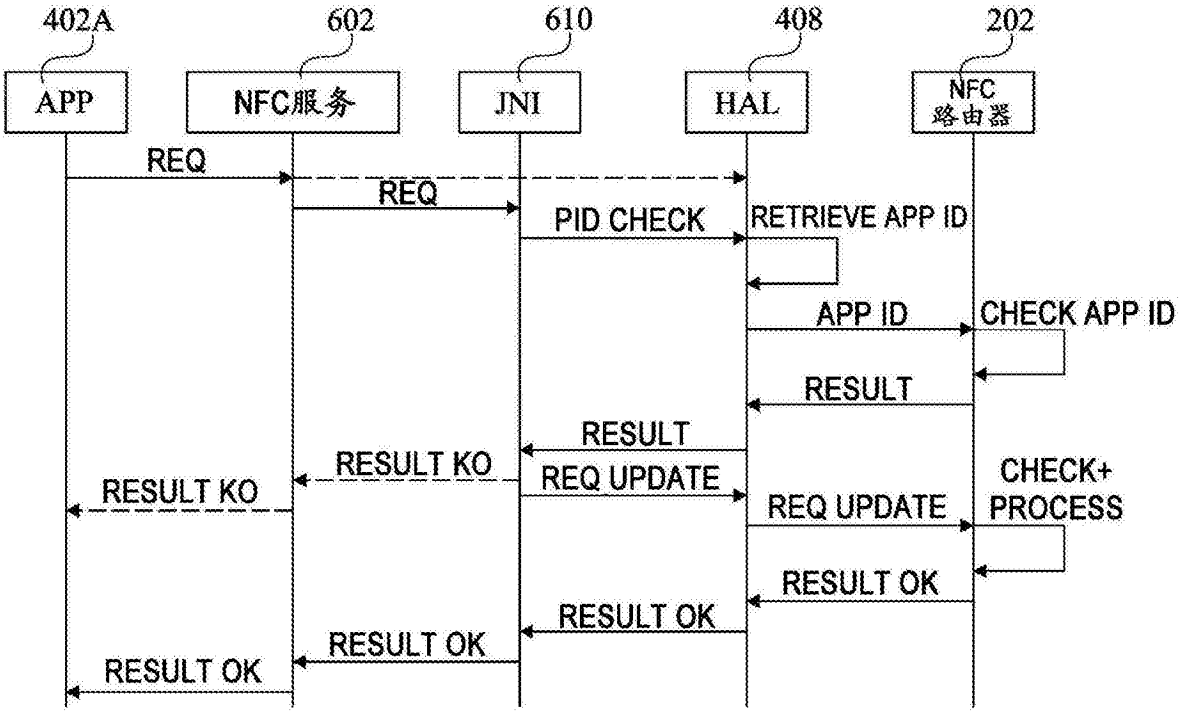

402A
602
610
408
202
APP
NFC服务
JNI
HAL
NFC
路由器
REQ
REQ
PID CHECK
RETRIEVE APP ID
APP ID
CHECK APP ID
RESULT
RESULT
RESULT KO
REQ UPDATE
CHECK+
PROCESS
RESULT KO
REQ UPDATE
RESULT OK
RESULT OK
RESULT OK
RESULT OK

图7

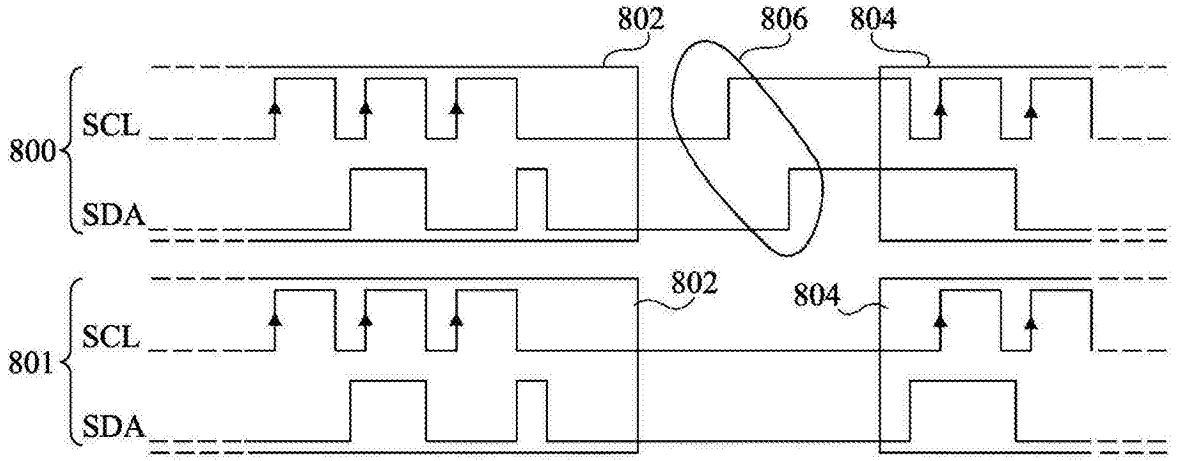

802
806
804
800
SCL
SDA
802
804
801
SCL
SDA

图8