(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104821031 A
(43)申请公布日 2015.08.05

(21)申请号 201510277471.1

(22)申请日 2015.05.27

(71)申请人 重庆大学
地址 400044 重庆市沙坪坝区沙坪坝正街174号

(72)发明人 陈建军

(74)专利代理机构 重庆为信知识产权代理事务所(普通合伙) 50216
代理人 陈千

(51)Int.Cl.
G07C 9/00(2006.01)

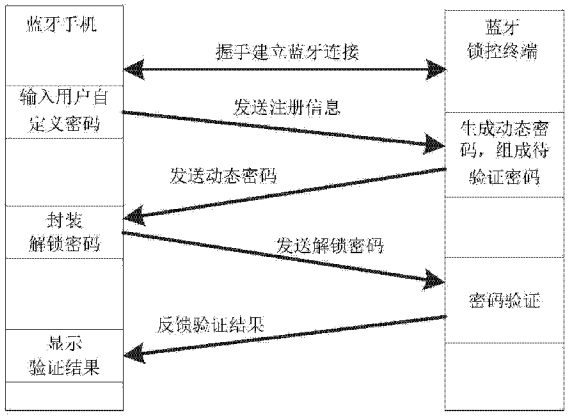
权利要求书1页 说明书3页 附图1页

(54)发明名称

蓝牙手机智能锁控系统动态认证方法

(57)摘要

本发明公开蓝牙手机智能锁控系统动态认证方法,包括以下步骤:S1:建立连接;S2:发送注册信息,包括用户自定义密码和蓝牙手机标识码;S3:蓝牙锁控终端生成动态密码,并将动态密码、用户自定义密码和蓝牙手机标识码共同组成待验证密码;S4:向蓝牙手机发送动态密码;S5:蓝牙手机将接收的动态密码与步骤S2中发送的用户自定义密码和蓝牙手机标识码封装成解锁密码;S6:向蓝牙锁控终端发送解锁密码;S7:蓝牙锁控终端接收解锁密码并与待验证密码进行验证;S8:反馈验证结果,验证成功,执行解锁操作,生成新的动态密码;验证失败,输出提示信息或报警信息。其效果是:密码的复杂度高,动态性强,能有效防止利用电磁波复制进行技术性开锁。



CN 104821031 A

1. 一种蓝牙手机智能锁控系统动态认证方法，其特征在于包括以下步骤：

S1：蓝牙手机与蓝牙锁控终端建立连接的步骤；

S2：蓝牙手机向蓝牙锁控终端发送注册信息的步骤，所述注册信息包括用户自定义密码和蓝牙手机标识码；

S3：蓝牙锁控终端生成动态密码，并将所述动态密码、用户自定义密码和蓝牙手机标识码共同组成待验证密码的步骤；

S4：蓝牙锁控终端向蓝牙手机发送动态密码的步骤；

S5：蓝牙手机将接收的动态密码与步骤 S2 中发送的用户自定义密码和蓝牙手机标识码封装成解锁密码的步骤；

S6：蓝牙手机向所述蓝牙锁控终端发送解锁密码的步骤；

S7：蓝牙锁控终端接收解锁密码并与所述待验证密码进行验证的步骤；

S8：反馈验证结果，验证成功，蓝牙锁控终端执行解锁操作，并返回步骤 S3 生成新的动态密码；验证失败，蓝牙锁控终端输出提示信息或报警信息。

2. 根据权利要求 1 所述的蓝牙手机智能锁控系统动态认证方法，其特征在于：步骤 S2 中的蓝牙手机标识码为手机蓝牙模块的 MAC 地址。

3. 根据权利要求 1 所述的蓝牙手机智能锁控系统动态认证方法，其特征在于：步骤 S2 中的蓝牙手机标识码为蓝牙手机的 IMEI 码。

4. 根据权利要求 1 所述的蓝牙手机智能锁控系统动态认证方法，其特征在于：蓝牙手机与蓝牙锁控终端之间传输的信息采用 64 位或 128 位的 AES 加密算法进行数据加密。

5. 根据权利要求 1 所述的蓝牙手机智能锁控系统动态认证方法，其特征在于：步骤 S5 中，当蓝牙手机将接收的动态密码与步骤 S2 中发送的用户自定义密码和蓝牙手机标识码封装成解锁密码后，所述蓝牙手机的应用界面上生成该蓝牙锁控终端对应的开锁控件。

6. 根据权利要求 5 所述的蓝牙手机智能锁控系统动态认证方法，其特征在于：用户触发应用界面上的开锁控件时，蓝牙手机自动向所述蓝牙锁控终端发送解锁密码。

7. 根据权利要求 5 所述的蓝牙手机智能锁控系统动态认证方法，其特征在于：当用户触发蓝牙手机应用界面上的开锁控件时，蓝牙手机提示输入密码，当用户输入的密码与步骤 S2 中用户自定义密码相匹配时，蓝牙手机向所述蓝牙锁控终端发送解锁密码。

8. 根据权利要求 1 所述的蓝牙手机智能锁控系统动态认证方法，其特征在于：步骤 S7 中，蓝牙锁控终端先将解锁密码中的动态密码与待验证密码中的动态密码进行验证，再将解锁密码中的蓝牙手机标识码与待验证密码中的蓝牙手机标识码进行验证；最后再将解锁密码中的用户自定义密码与待验证密码中的用户自定义密码进行验证，一旦有误即认定为验证失败，只有三次验证全部通过，才认定为验证成功。

9. 根据权利要 1 至 8 任意一项所述的蓝牙手机智能锁控系统动态认证方法，其特征在于：所述蓝牙锁控终端安装在房门、车门或电动摩托车上。

蓝牙手机智能锁控系统动态认证方法

技术领域

[0001] 本发明涉及电子控制技术，具体地讲，是一种蓝牙手机智能锁控系统动态认证方法。

背景技术

[0002] 随着智能手机的普及，利用手机蓝牙通信实现智能开锁或者智能启动的应用也越来越多，如中国专利 201310246771.4 公开了一种基于蓝牙模块的门禁系统及门禁控制方法，中国专利 200510011185.7 公开了一种手机汽车电子钥匙及开锁方法及汽车电子锁等等。

[0003] 但现有的应用中，智能手机与蓝牙锁控终端之间所设定的密码过于单一，大多的技术方案都是简单的以手机蓝牙唯一性的物理地址作为密码载体，或者是以人为设定的一段密码段作为密码载体，当需要解锁时，只要通过手机应用软件发送代表手机唯一性的物理地址或者预设的几位密码，蓝牙锁控终端即可实现解锁操作。

[0004] 这种传统的加密方式很容易通过无线信号进行复制，一旦被破解，很容易造成重大财产损失。

发明内容

[0005] 为了克服上述缺陷，本发明提出一种蓝牙手机智能锁控系统动态认证方法，解决现有系统采用单一的且固定的加密方式所带来的安全隐患。

[0006] 为了实现上述目的，本发明的具体的技术方案如下：

[0007] 一种蓝牙手机智能锁控系统动态认证方法，其关键在于包括以下步骤：

[0008] S1：蓝牙手机与蓝牙锁控终端建立连接的步骤；

[0009] S2：蓝牙手机向蓝牙锁控终端发送注册信息的步骤，所述注册信息包括用户自定义密码和蓝牙手机标识码；

[0010] S3：蓝牙锁控终端生成动态密码，并将所述动态密码、用户自定义密码和蓝牙手机标识码共同组成待验证密码的步骤；

[0011] S4：蓝牙锁控终端向蓝牙手机发送动态密码的步骤；

[0012] S5：蓝牙手机将接收的动态密码与步骤 S2 中发送的用户自定义密码和蓝牙手机标识码封装成解锁密码的步骤；

[0013] S6：蓝牙手机向所述蓝牙锁控终端发送解锁密码的步骤；

[0014] S7：蓝牙锁控终端接收解锁密码并与所述待验证密码进行验证的步骤；

[0015] S8：反馈验证结果，验证成功，蓝牙锁控终端执行解锁操作，并返回步骤 S3 生成新的动态密码；验证失败，蓝牙锁控终端输出提示信息或报警信息。

[0016] 作为进一步描述，步骤 S2 中的蓝牙手机标识码为手机蓝牙模块的 MAC 地址。

[0017] 当然，步骤 S2 中的蓝牙手机标识码也可以为蓝牙手机的 IMEI 码。

[0018] 为了提高数据传输的安全性，蓝牙手机与蓝牙锁控终端之间传输的信息采用 64

位或 128 位的 AES 加密算法进行数据加密。

[0019] 结合智能手机操作系统的发展，步骤 S5 中，当蓝牙手机将接收的动态密码与步骤 S2 中发送的用户自定义密码和蓝牙手机标识码封装成解锁密码后，所述蓝牙手机的应用界面上生成该蓝牙锁控终端对应的开锁控件。

[0020] 为了便于实现智能控制，用户触发应用界面上的开锁控件时，蓝牙手机自动向所述蓝牙锁控终端发送解锁密码。

[0021] 为了进一步提高安全性能，当用户触发蓝牙手机应用界面上的开锁控件时，蓝牙手机提示输入密码，当用户输入的密码与步骤 S2 中用户自定义密码相匹配时，蓝牙手机向所述蓝牙锁控终端发送解锁密码。

[0022] 为了提高认证速度，步骤 S7 中，蓝牙锁控终端先将解锁密码中的动态密码与待验证密码中的动态密码进行验证，再将解锁密码中的蓝牙手机标识码与待验证密码中的蓝牙手机标识码进行验证；最后再将解锁密码中的用户自定义密码与待验证密码中的用户自定义密码进行验证，一旦有误即认定为验证失败，只有三次验证全部通过，才认定为验证成功。

[0023] 结合不同的应用场景，所述蓝牙锁控终端安装在房门、车门或电动摩托车上。

[0024] 本发明的显著效果是：

[0025] 在现有蓝牙手机智能锁控系统的基础上，通过软件升级即可实现本发明的内容，实施方便，通过改变蓝牙手机与蓝牙锁控终端之间的密码构建方式，提升了现有系统的安全性能，能有效防止利用电磁波复制进行技术性开锁。

附图说明

[0026] 图 1 是本发明的方法步骤图；

[0027] 图 2 是本发明的所采用的密码格式。

具体实施方式

[0028] 下面结合附图对本发明的具体实施方式以及工作原理作进一步详细说明。

[0029] 如图 1- 图 2 所示，本实施例以智能蓝牙门禁系统为例进一步解释本发明所提出的一种蓝牙手机智能锁控系统动态认证方法，具体包括以下步骤：

[0030] S1：蓝牙手机与蓝牙锁控终端建立连接的步骤，该步骤主要通过开启终端的蓝牙功能，通过手动选择或自动搜索等方式，握手建立蓝牙连接；

[0031] S2：蓝牙手机向蓝牙锁控终端发送注册信息的步骤，所述注册信息包括用户自定义密码和蓝牙手机标识码；这里的蓝牙手机标识码为手机蓝牙模块的 MAC 地址或者是蓝牙手机的 IMEI 码，均能唯一性的代表每一台蓝牙手机设备，具备钥匙功能；

[0032] 在进行用户注册时，蓝牙手机需要预先下载和安装专用的 APP 应用程序，打开 APP 应用软件后，系统会自动开启手机蓝牙功能模块，在蓝牙锁控终端上设置有匹配按钮，只有在按下匹配按钮后，非注册用户的蓝牙手机才能进行用户注册，每一个用户注册成功后，蓝牙锁控终端即执行步骤 S3。

[0033] S3：蓝牙锁控终端生成动态密码，并将所述动态密码、用户自定义密码和蓝牙手机标识码共同组成待验证密码的步骤；

[0034] 该步骤中的动态密码是通过蓝牙锁控终端内部固化的一个随机函数产生的一段随机序列，序列的长度可以根据密码级别设定，每一次成功开锁后都产生一个新的动态密码供下次使用，从而克服密码的可复制性。

[0035] S4：蓝牙锁控终端向蓝牙手机发送动态密码的步骤；

[0036] S5：蓝牙手机将接收的动态密码与步骤 S2 中发送的用户自定义密码和蓝牙手机标识码封装成解锁密码的步骤；

[0037] 在该步骤中，当蓝牙手机将接收的动态密码与步骤 S2 中发送的用户自定义密码和蓝牙手机标识码封装成解锁密码后，所述蓝牙手机的应用界面上生成该蓝牙锁控终端对应的开锁控件。

[0038] S6：蓝牙手机向所述蓝牙锁控终端发送解锁密码的步骤；

[0039] 根据不同用户的需求，在具体实施过程中，用户可以通过触发应用界面上的开锁控件直接发送解锁密码，实现一键开锁；也可以配置更高的安全级别，用户触发蓝牙手机应用界面上的开锁控件时，蓝牙手机提示输入密码，当用户输入的密码与步骤 S2 中用户自定义密码相匹配时，蓝牙手机才向所述蓝牙锁控终端发送解锁密码。

[0040] S7：蓝牙锁控终端接收解锁密码并与所述待验证密码进行验证的步骤；

[0041] 蓝牙锁控终端先将解锁密码中的动态密码与待验证密码中的动态密码进行验证，再将解锁密码中的蓝牙手机标识码与待验证密码中的蓝牙手机标识码进行验证；最后再将解锁密码中的用户自定义密码与待验证密码中的用户自定义密码进行验证，一旦有误即认定为验证失败，只有三次验证全部通过，才认定为验证成功。

[0042] 当然也可以直接将三段密码组装一起一次性验证，但是由于密码位数较长，算法计算量大，对硬件设备的运算速度要求较高。

[0043] S8：反馈验证结果，验证成功，蓝牙锁控终端执行解锁操作，并返回步骤 S3 生成新的动态密码；验证失败，蓝牙锁控终端输出提示信息或报警信息。

[0044] 在上述过程中，蓝牙手机与蓝牙锁控终端之间传输的信息采用 64 位或 128 位的 AES 加密算法进行数据加密，提高信息传输的安全性。

[0045] 通过上述方法实现蓝牙手机智能锁控系统的动态认证，密码的复杂度高，动态性强，能有效防止利用电磁波复制进行技术性开锁，根据不同的用户需求可以配置不同的安全级别，当选择需要输入用户自定义密码进行开锁时，及时手机被盗，依然无法直接开锁，安全性高，系统的应用更加灵活。

[0046] 最后需要说明的是，以上实施例仅用以说明本发明最佳技术方案而非限制技术方案，上述文字参照较佳实施例对本发明作了详细说明，而且本领域技术人员也可以对本发明技术方案进行的修改或者等同替换，不能脱离本技术方案的宗旨和范围的，均应涵盖在本发明权利要求范围当中。

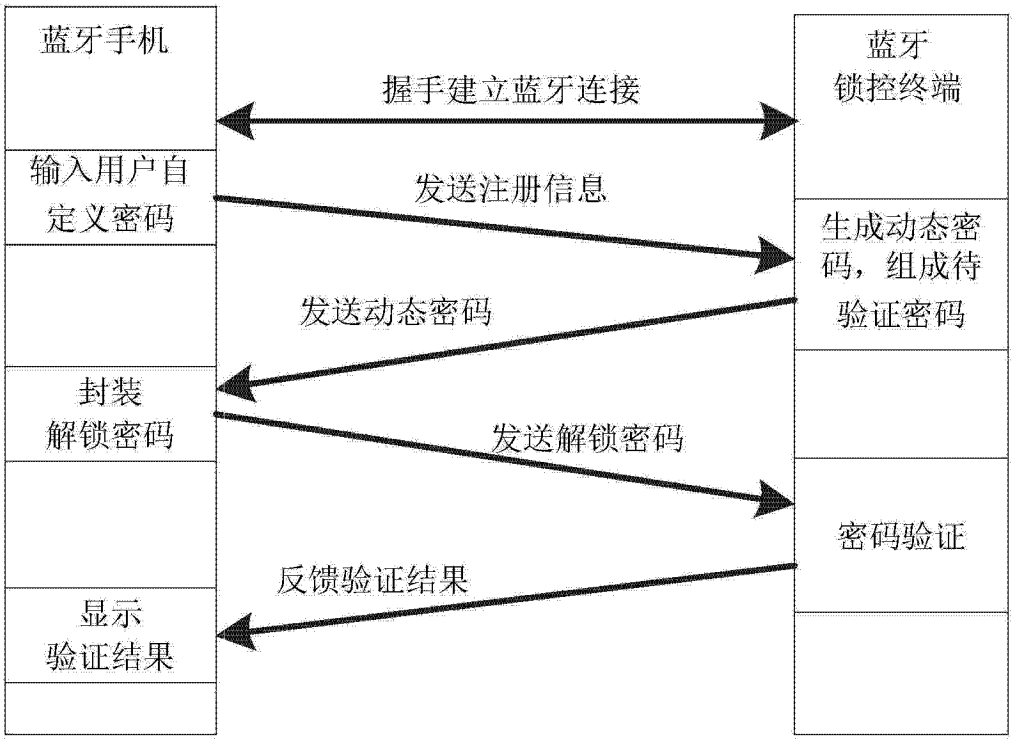


图 1

动态密码	蓝牙手机标识码	用户自定义密码

图 2