



(12) 发明专利

(10) 授权公告号 CN 101599193 B

(45) 授权公告日 2011. 02. 09

(21) 申请号 200910304337. 0

CN 1322326 A, 2001. 11. 14, 全文.

(22) 申请日 2009. 07. 14

US 5146067 A, 1992. 09. 08, 全文.

(73) 专利权人 深圳市科陆电子科技股份有限公司

CN 2519246 Y, 2002. 10. 30, 全文.

地址 518057 广东省深圳市南山区科技园南区 T2 栋五楼

审查员 李宁馨

(72) 发明人 崔丰曦

(74) 专利代理机构 深圳市科吉华烽知识产权事务所 44248

代理人 胡吉科

(51) Int. Cl.

G07F 7/08 (2006. 01)

G07F 7/10 (2006. 01)

G07F 7/12 (2006. 01)

(56) 对比文件

US 4731575, 1988. 03. 15, 全文.

CN 101447107 A, 2009. 06. 03, 全文.

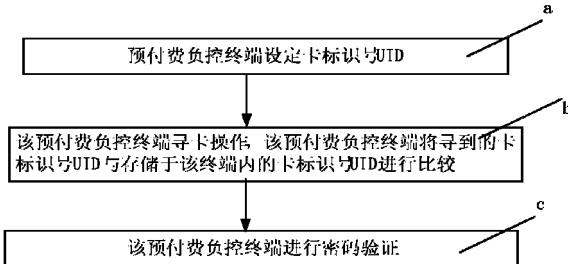
权利要求书 1 页 说明书 5 页 附图 2 页

(54) 发明名称

在预付费终端中防 M1 卡破解的方法

(57) 摘要

本发明涉及电力供配电技术领域，其公开了在预付费终端中防 M1 卡破解的方法，本发明是通过以下技术方案实现的：设计一种在预付费终端中防 M1 卡破解的方法，包括如下步骤，a 预付费负控终端设定卡标识号 UID；b 预付费负控终端寻卡操作，该预付费负控终端将寻到的卡标识号 UID 与存储于该终端内的卡标识号 UID 进行比较；c 该预付费负控终端进行密码验证。本发明的有益效果是：本发明将终端与卡配对，可以解决 M1 卡被破解带来的安全性问题，同时可解决现有系统要求终端实时在线才能防范破解的问题，并且提高了刷卡操作时间，减少了用户持卡等待的时间。



1. 一种在预付费终端中防 M1 卡破解的方法，其特征在于，包括如下步骤：

(a) 预付费负控终端设定卡标识号 UID；

(b) 该预付费负控终端寻卡操作，该预付费负控终端将寻到的卡标识号 UID 与存储于该终端内的卡标识号 UID 进行比较；

(c) 该预付费负控终端进行密码验证；

(d) 该预付费负控终端在线状态检查，若其处于在线状态，则该负控终端完成刷卡操作并将信息上报给主站；否则则跳转到步骤 (e)；

(e) 该预付费负控终端处于离线状态，检查终端的操作次数是否超过设定值；

所述步骤(a)具体包括：

(a1) 用户交费购电时，营业人员为用户办理 IC 卡，根据用户所购电量对 IC 卡进行充值；每个所述用户使用固定的 IC 卡；该 IC 卡设定有卡标识号 UID；

(a2) 主站将该 IC 卡的卡标识号 UID 下载到用户所使用的对应的预付费负控终端或者手工录入 UID 号到用户所使用的对应的预付费负控终端；

所述步骤(c)中，所述负控终端中存储的卡标识号 UID 对应的密码由主站生成下发或者所述负控终端中存储的卡标识号 UID 对应的密码由该负控终端获得卡标识号 UID 时生成；所述在预付费终端中防 M1 卡破解的方法还包括以下步骤：所述步骤(c)具体包括：  
(c1) 该负控终端验证卡密码时，使用该负控终端中存储的对应卡标识号 UID 的密码进行比较；  
(c2) 该负控终端验证卡密码时，当该卡密码和存储在该负控终端中对应的卡标识号 UID 的密码一致时，跳转到步骤(d)；否则不进行刷卡消费操作，并告警；

所述步骤(d)具体包括：该负控终端每隔一段时间会与主站通信，上报信息，并接收主站信息，如果已有一段时间未收到该主站信息，则视为不在线；当该负控终端不在线时跳转到步骤(e)；

所述步骤(e)进一步包括：

(e1) 该负控终端检测存储在其中的操作卡次数；

(e2) 该负控终端将已操作卡次数跟设定的可操作卡次数作比较，看是否超出；

(e3) 该负控终端发现操作卡次数未超过设定值，则完成刷卡消费操作，并将此次刷卡信息保存，等待能连上主站时将信息上报；

(e4) 该负控终端发现操作卡次数已超过设定值，则不进行刷卡消费操作，并告警。

## 在预付费终端中防 M1 卡破解的方法

### 【技术领域】

[0001] 本发明涉及电力供配电技术领域，尤其是涉及一种预付费负控终端和 IC 卡校验技术。

### 【背景技术】

[0002] 电力负荷管理终端是广大电力用户用于用电管理、现场监测和远程抄表的设备，不仅能实现负荷预测、负荷控制和错峰避峰的功能，而且可以实现用户负荷现场监测、提高用电效率、发布供电信息等。为解决电力用户抄表收费难的问题，预付费技术已得到广泛应用，其中 IC 卡预收费已得到广大用户认可。IC 卡预购电系统即在营业窗口建立 IC 卡发放、充值管理软件，在客户侧安装 IC 卡售电装置，客户通过到银行预存电费，凭交费单到营业窗口计算预购电量并充值到 IC 卡，客户再将所购电量刷卡到 IC 卡售电装置进行用电。预付费负控终端是将自助式 IC 卡售电功能结合到负控终端中，既克服了 IC 卡售电装置远程通讯和监控问题，又克服了现有的负控终端由控制中心发送信息进行电量定值来实现预付费控制，用户不易接受，当通讯网络遇到故障时将面临用户交费后不能正常用电的问题。而现有的 IC 卡预购电系统使用的非接触式 IC 卡基本都是使用 M1 卡。M1 卡是 PhilipsMifare 1 卡的简称，是一种非接触式逻辑加密卡。截至 2008 年 11 月，我国已有 170 余个城市应用了不同规模的公用事业 IC 卡系统，发卡量已超过 1.5 亿张，约有 95% 的城市在应用 IC 卡系统时选择使用 M1 卡。2008 年，德国研究员亨里克·普洛茨和美国弗吉尼亚大学计算机科学在读博士卡尔斯滕·诺尔最先利用电脑成功破解了恩智浦半导体 M1 芯片的安全算法。工业和信息部也发布了《关于做好应对部分 IC 卡出现严重安全漏洞工作的通知》，M1 芯片安全算法的破解，导致应用 M1 卡的系统出现了应对安全性的冲击。针对 M1 卡的加密算法被破解导致的安全性问题，业界也提出了几种应对方式。一种方式是将卡上的重要数据不使用明文存储，而是用加密后的数据。这样即使卡的密码被破解，也无法随意对卡充值。但这种方式无法防止复制卡，即无法阻止复制与破解卡同样数值的卡进行消费；另一种方式是在发卡时用 UID 号来生成卡的密码，做到一卡一密，但目前也出现了用 FPGA 模拟出任意卡号的技术，这种方式也无法阻止复制出大量同样 UID 号，同样数值的卡来进行消费。

### 【发明内容】

[0003] 为了解决上述现有技术中的不足，本发明提供一种在预付费终端中防 M1 卡破解的方法，解决了 M1 卡被破解对预付费负控终端带来的预付费安全性问题，尤其是通讯故障时离线安全刷卡的问题。

[0004] 本发明是通过以下技术方案实现的：设计一种在预付费终端中防 M1 卡破解的方法，包括如下步骤，

[0005] a 预付费负控终端设定卡标识号 UID；

[0006] b 预付费负控终端寻卡操作，该预付费负控终端将寻到的卡标识号 UID 与存储于该终端内的卡标识号 UID 进行比较；

- [0007] c 该预付费负控终端进行密码验证。
- [0008] 本发明进一步改进的是：所述步骤 a 具体包括：
- [0009] a1 用户开户交费购电或交费购电时，营业人员为用户办理 IC 卡，根据用户所购电量对 IC 卡进行充值；所述每个用户使用固定的 IC 卡；该 IC 卡设定有卡标识号 UID；
- [0010] a2 主站将该 IC 卡的卡标识号 UID 下载到用户所使用的对应的预付费负控终端或者手工录入 UID 号到用户所使用的对应的预付费负控终端。
- [0011] 本发明进一步改进的是：所述步骤 c 中，所述负控终端中存储的卡标识号 UID 对应的密码由主站生成下发或者所述负控终端中存储的卡标识号 UID 对应的密码由该负控终端获得卡标识号 UID 时生成。
- [0012] 本发明进一步改进的是：所述在预付费终端中防 M1 卡破解的方法还包括以下步骤：
- [0013] d 该预付费负控终端在线状态检查，若其处于在线状态，则该负控终端完成刷卡操作并将信息上报给该主机；否则则跳转到步骤 e；
- [0014] e 该预付费负控终端处于离线状态，检查终端的操作次数是否操作设定值。
- [0015] 本发明进一步改进的是：所述步骤 d 具体包括：该负控终端每隔一段时间会与主站通信，上报信息，并接收主站信息，如果已有一段时间未收到该主站信息，则可视为不在线；当该负控终端不在线时跳转到步骤 e。
- [0016] 本发明进一步改进的是：所述步骤 e 进一步包括：
- [0017] e1 该负控终端检测存储在其中的操作卡次数；
- [0018] e2 该负控终端将已操作卡次数跟设定的可操作卡次数作比较，看是否超出；
- [0019] e3 该负控终端发现操作卡次数未超过设定值，则完成刷卡消费操作，并将此次刷卡信息保存，等待能连上主站时将信息上报；
- [0020] e4 该负控终端发现操作卡次数已超过设定值，则不进行刷卡消费操作，并告警。
- [0021] 本发明进一步改进的是：所述步骤 c 具体包括：
- [0022] c1 该负控终端验证卡密码时，使用该负控终端中存储的对应卡标识号 UID 的密码进行比较；
- [0023] c2 该负控终端验证卡密码时，当该卡密码和存储在该负控终端中对应的卡标识号 UID 的密码一致时，跳转到步骤 d；否则不进行刷卡消费操作，并告警。
- [0024] 本发明的有益效果是：本发明将终端与卡配对，可以解决 M1 卡被破解带来的安全性问题，同时可解决现有系统要求终端实时在线才能防范破解的问题，并且提高了刷卡操作时间，减少了用户持卡等待的时间。

### 【附图说明】

- [0025] 图 1 是本发明在预付费终端中防 M1 卡破解的方法的步骤流程图。
- [0026] 图 2 是本发明的预付费负控终端操作卡流程图。
- [0027] 图 3 是本发明的主站与预付费负控终端的信息交互图。
- [0028] 图 4 是本发明的预付费负控终端的可用 UID 号更改方式图。

**【具体实施方式】**

- [0029] 下面结合附图和具体实施例,对发明作进一步的描述。
- [0030] 如图 1,一种在预付费终端中防 M1 卡破解的方法,包括如下步骤,
- [0031] a 预付费负控终端设定卡标识号 UID ;
- [0032] b 预付费负控终端寻卡操作,该预付费负控终端将寻到的卡标识号 UID 与存储于该终端内的卡标识号 UID 进行比较;
- [0033] c 该预付费负控终端进行密码验证。
- [0034] 所述步骤 a 具体包括 :a1 用户开户交费购电或交费购电时,营业人员为用户办理 IC 卡,根据用户所购电量对 IC 卡进行充值;所述每个用户使用固定的 IC 卡;该 IC 卡设定有卡标识号 UID ;a2 主站将该 IC 卡的卡标识号 UID 下载到用户所使用的对应的预付费负控终端或者手工录入 UID 号到用户所使用的对应的预付费负控终端。
- [0035] 所述步骤 c 中,所述负控终端中存储的卡标识号 UID 对应的密码由主站生成下发或者所述负控终端中存储的卡标识号 UID 对应的密码由该负控终端获得卡标识号 UID 时生成。
- [0036] 所述在预付费终端中防 M1 卡破解的方法还包括以下步骤 :
- [0037] d 该预付费负控终端在线状态检查,若其处于在线状态,则该负控终端完成刷卡操作并将信息上报给该主机;否则则跳转到步骤 e;
- [0038] e 该预付费负控终端处于离线状态,检查终端的操作次数是否操作设定值。
- [0039] 所述步骤 d 具体包括 :该负控终端每隔一段时间会与主站通信,上报信息,并接收主站信息,如果已有一段时间未收到该主站信息,则可视为不在线;当该负控终端不在线时跳转到步骤 e。
- [0040] 所述步骤 e 进一步包括 :
- [0041] e1 该负控终端检测存储在其中的操作卡次数;
- [0042] e2 该负控终端将已操作卡次数跟设定的可操作卡次数作比较,看是否超出;
- [0043] e3 该负控终端发现操作卡次数未超过设定值,则完成刷卡消费操作,并将此次刷卡信息保存,等待能连上主站时将信息上报;
- [0044] e4 该负控终端发现操作卡次数已超过设定值,则不进行刷卡消费操作,并告警。
- [0045] 所述步骤 c 具体包括 :
- [0046] c1 该负控终端验证卡密码时,使用该负控终端中存储的对应卡标识号 UID 的密码进行比较;
- [0047] c2 该负控终端验证卡密码时,当该卡密码和存储在该负控终端中对应的卡标识号 UID 的密码一致时,跳转到步骤 d;否则不进行刷卡消费操作,并告警。
- [0048] 如图 2,为本发明的预付费负控终端操作卡流程,在本发明的一个实施例中 IC 卡采用目前国际流行的 M1 卡,用户交费购电,营业人员通过 IC 卡售电管理软件为用户办理新卡或充值旧卡,根据所交电费所购电量对 IC 卡进行充值。每个用户使用固定的 IC 卡。首先是终端的寻卡操作,当终端寻到卡时,先读取卡的 UID 号,并将读到的 UID 号与终端中存储的可用 UID 号作比较。图 4 示出了预付费负控终端的可用 UID 号更改方式。终端中存储的 UID 号可由主站在线下发,也可由工作人员在终端上自行手动输入。如果读到的卡的 UID 号与终端上存储的 UID 号不符合,则终端发出告警信息并在显示屏上显示错误信息,这样系统中其它被破解的卡不会对终端造成任何影响。

[0049] 如果读到的卡的 UID 号与终端上存储的 UID 号相符合, 终端对卡进行密码校验。发卡时用卡的 UID 号来生成卡的密码, 做到一卡一密。在终端校验卡时, 可以直接读取存储在终端上的对应 UID 号密码来校验卡。如果不采用终端与卡配对的方式, 终端需要满足对所有 UID 号作校验, 同时是一卡一密, 信息量太过庞大, 终端不可能事先将所有 UID 号对应密码存储在终端中。每次校验卡时都必须利用读到的 UID 号实时生成密码, 增加了刷卡操作时间, 因为刷卡操作时必须使卡片始终保持在终端有效读写距离内, 增加刷卡操作时间增加了出错可能。同时密码需要在终端实时生成, 影响了可采用的加密算法的复杂程度。而采用终端与卡的 UID 号配对的方式, 终端只需要操作固定的 UID 号, 可以将对应的密码预先存储在终端中, 校验时可以直接读取。同时密码不需要实时生成, 就可以采用较复杂的算法, 增加可靠性。如果密码校验不通过, 则终端发出告警信息并在显示屏上显示错误信息。

[0050] 如果终端对卡的密码校验通过, 终端查询自身是否在线。终端每隔一段时间会与主站通信, 上报信息, 如果已有一段时间未收到主站信息, 则可视为不在线。如果终端在线, 则终端将卡里的电费信息与终端中存储的对应 UID 号的电费值作比较, 如果符合, 则完成刷卡消费, 并将刷卡信息上报主站, 主站再将终端中记录的操作卡次数清零。如果不符, 则终端发出告警信息并在显示屏上显示错误信息。如图 3 所示, 主站在用户交费并将卡充值后, 将充值信息下发给对应卡的 UID 号的终端。这样终端在用户刷卡时, 如果判断自己在线, 则可先用自己存储的电费信息来验证卡的电费信息, 完成刷卡后, 再将信息上报。这样可以在用户刷卡时省掉用户等待终端与系统来回通信的时间, 因为刷卡操作时必须使卡片始终保持在终端有效读写距离内, 省掉操作时间可以减少操作未完成而卡已经脱离终端有效读写距离的问题。在用户交费并将卡充值后, 如果没采用终端与卡配对的方式, 主站需要将充值信息发送给所有终端, 而采用终端与卡配对的方式主站只需要将充值信息传送给对应卡的 UID 号的终端, 这样可以极大减少主站与终端的通信信息量, 也减少了出错可能。这样完美复制的卡也只能使用一次, 使用过后终端会将数据上报, 系统中对应卡片 UID 号的电费值会清零。这样再次使用其他的复制卡时, 系统中对应 UID 号的卡电费值已清零, 复制卡无法再使用。这样即使能完美破解卡, 只要不能攻破系统, 就不能更改系统中的充值信息, 不会造成电费损失。

[0051] 如果终端对卡的密码校验通过, 并且终端发现自身处于离线状态。终端查询自身的操作卡次数, 如果大于设定的值, 则终端发出告警信息并在显示屏上显示错误信息。如果操作卡次数小于设定的值, 则终端完成刷卡操作, 并将操作卡次数加 1, 然后将此次刷卡的信息储存在终端中。在终端再次连接到主站时, 将此次刷卡信息上报。终端离线时可能发生用户已交费冲值, 而主站无法通知终端。所以终端在离线用户刷卡时, 不能再验证自己存储的电费信息, 而必须完成一次刷卡操作。如果没有采用终端与卡的 UID 号配对的方式, 即使限制了每个 UID 号的刷卡次数, 仍可能出现大量不同 UID 号的复制卡刷卡可能, 造成电费损失。采用终端与卡配对的方式, 只有对应 UID 号的卡能在终端上完成刷卡操作, 如果将设定的离线允许刷卡次数设为 1, 这样同样 UID 号的复制卡只能使用一次, 并且因为 UID 号与其它终端不配对, 不能在其它可能离线的终端上使用, 这样离线状态下也不会造成电费损失。而且终端与卡配对的方式也可防止用户的卡被不小心盗用复制, 这样即使卡被盗用复制, 也不能在其它终端上使用, 不会对用户造成损失。

[0052] 图 3 示出了主站与预付费负控终端的信息交互。主站将将终端可操作的 UID 号下

发到终端，并且在用户交费充值后，将交费冲值信息下发到可操作此 UID 号的卡的终端。用户完成正常的刷卡消费后，将此次刷卡信息上报给主站，主站收到刷卡信息后通知终端将保存在终端中的操作卡次数清零。终端在刷卡出现异常状态时，将异常状态上报给主站。

[0053] 通过本发明，能够解决 M1 卡被破解带来的安全性问题，同时减少了用户持卡等待时间。

[0054] 以上内容是结合具体的优选实施方式对本发明所作的进一步详细说明，不能认定本发明的具体实施只局限于这些说明。对于本发明所属技术领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干简单推演或替换，都应当视为属于本发明的保护范围。

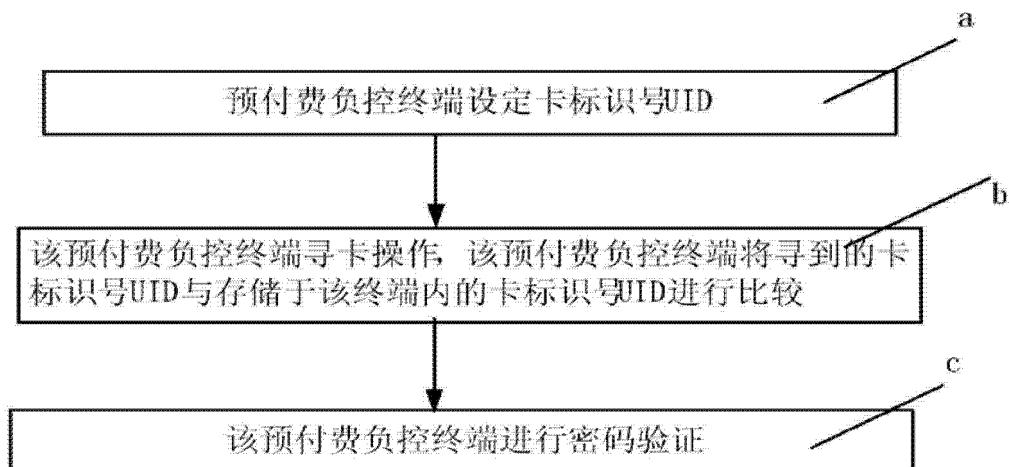


图 1

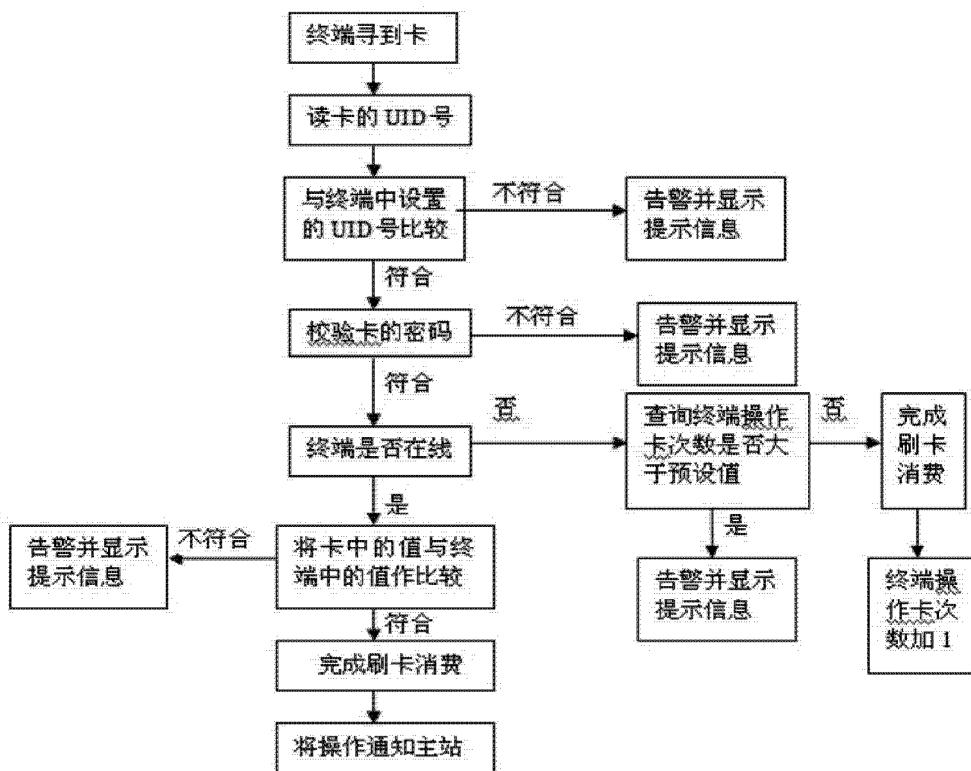


图 2

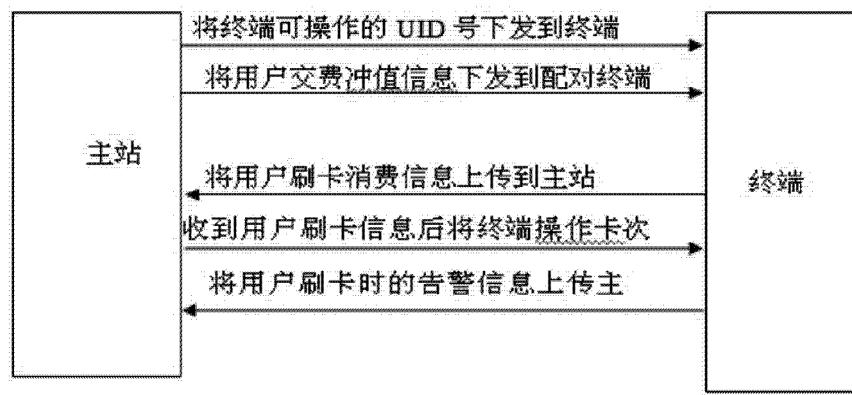


图 3

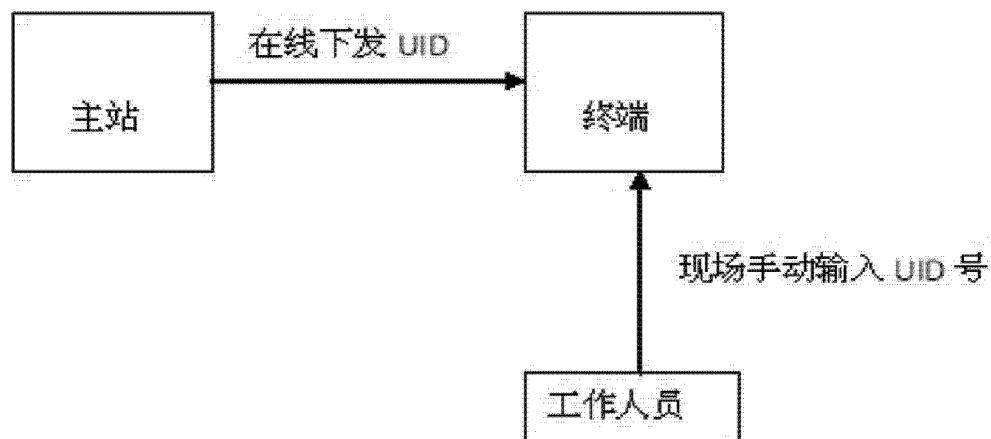


图 4