(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 104217230 B
(45)授权公告日 2017.03.15

(21)申请号 201410439094.2

(22)申请日 2014.08.29

(65)同一申请的已公布的文献号
申请公布号 CN 104217230 A

(43)申请公布日 2014.12.17

(73)专利权人 公安部交通管理科学研究所
地址 214151 江苏省无锡市滨湖区钱荣路88号

(72)发明人 孙正良 黄金 蔡岗 刘东波 胡家彬

(74)专利代理机构 无锡市大为专利商标事务所（普通合伙）32104
代理人 曹祖良 张涛

(51)Int.Cl.
G06K 17/00(2006.01)

(56)对比文件
US 2001041593 A1,2001.11.15,
CN 103413079 A,2013.11.27,
US 2002170960 A1,2002.11.21,
CN 101217362 A,2008.07.09,
肖娟凤.无源RFID标签防碰撞算法及安全认证协议研究.《中国优秀硕士学位论文全文数据库 信息科技辑》.2014,

审查员 李龙

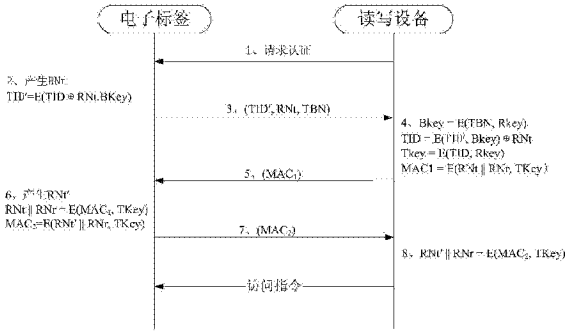
权利要求书2页 说明书5页 附图1页

(54)发明名称

隐藏超高频电子标签识别号的安全认证方法

(57)摘要

本发明公开了一种隐藏超高频电子标签识别号的安全认证方法，该安全认证方法通过对电子标签识别号TID进行随机数加密后，以密文方式返回，能有效防止非法读写设备获取TID信息实现对电子标签所标识的物品进行非法跟踪和身份识别。同时，该认证方法能有效抵御窃听、仿冒和重放等攻击，具有防止电子标签信息被窃取、防止伪造标签等优点。该安全认证方法使用国密对称加密算法，采用双密钥和二次认证机制，实现了批量卡同密钥的电子标签合法性验证和单标签单密钥的双向安全验证。



CN 104217230 B

1.一种隐藏超高频电子标签识别号的安全认证方法，其特征是，所述认证方法包括如下步骤：

(a)、读写设备向电子标签发送认证请求信息，电子标签在收到读写设备发送的认证请求信息后，从电子标签的安全信息区内读出批密钥BKey并从标识信息区内读出电子标签批号TBN；电子标签将批密钥BKey、电子标签批号TBN以及随机数RNt与电子标签识别号TID进行加密运算，得到标签加密识别号TID′，电子标签将标签加密识别号TID′、随机数RNt以及电子标签批号TBN作为应答返回至读写设备内；

(b)、读写设备接收标签加密识别号TID′、随机数RNt以及电子标签批号TBN，利用认证根密钥RKey对电子标签批号TBN进行加密分散，以得到读写批密钥BKey′，利用读写批密钥BKey′对标签加密识别号TID′以及随机数RNt进行解密运算，以得到读写标签解密识别号TID″；

(c)、读写设备利用认证根密钥RKey对读写标签解密识别号TID″加密分散，以获得读写单标签认证密钥TKey′，并将读写单标签认证密钥TKey′与随机数RNr进行加密运算，以得到读写访问控制码MAC_1，读写设备将读写访问控制码MAC_1发送至电子标签；

(d)、电子标签接收读写访问控制码MAC_1，利用安全信息区的单标签密钥TKey进行解密运算，以得到随机数RNt′；电子标签将随机数RNt′与随机数RNt进行比较，当随机数RNt′与随机数RNt不一致时，则终止与读写设备间的认证过程，否则，进入步骤(e)；

(e)、电子标签再次产生随机数RNt″，并将所述随机数RNt″与单标签认证密钥TKey进行加密运算，以得到标签访问控制码MAC_2，并将所述标签访问控制码MAC_2发送至读写设备；

(f)、读写设备接收标签访问控制码MAC_2，并利用读写单标签认证密钥TKey′对标签访问控制码MAC_2进行解密运算，以得到随机数RNr′；若随机数RNr′与随机数RNr一致时，则读写设备通过电子标签的认证，否则认证失败。

2.根据权利要求1所述的隐藏超高频电子标签识别号的安全认证方法，其特征是：所述步骤(b)中，认证根密钥RKey位于读写设备的安全控制模块SAM内，安全控制模块SAM利用认证根密钥RKey对电子标签批号TBN进行加密分散，以得到读写批密钥BKey′。

3.根据权利要求1所述的隐藏超高频电子标签识别号的安全认证方法，其特征是：所述步骤(a)中，电子标签对电子标签识别号TID、随机数RNt以及电子标签批密钥BKey进行加密运算，得到电子标签将标签加密识别号TID′为

$$TID' = E1(TID \oplus RNt, BKey)$$

其中，E1为对称加密运算函数，⊕为异或运算。

4.根据权利要求1所述的隐藏超高频电子标签识别号的安全认证方法，其特征是：所述步骤(b)中，读写设备得到读写标签解密识别号TID″为

$$TID'' = E2(TID', BKey) \oplus RNt$$

其中，E2为对称加密运算函数，⊕为异或运算。

5.根据权利要求1所述的隐藏超高频电子标签识别号的安全认证方法，其特征是：所述步骤(c)中，读写设备得到读写访问控制码MAC_1为

$MAC_1 = E2(RNt||RNr, TKey')$

其中，E2为对称加密运算函数，||表示信息级联运算。

6.根据权利要求1所述的隐藏超高频电子标签识别号的安全认证方法，其特征是：所述

步骤(d)中,电子标签得到随机数RNt′为

{RNt′||RNr}=E1(MAC_1,TKey)

其中,E1为对称加密运算函数,||表示信息级联运算。

7.根据权利要求1所述的隐藏超高频电子标签识别号的安全认证方法,其特征是:所述步骤(e)中,电子标签得到标签读写访问控制码MAC_2为

MAC_2=E1(RNt″||RNr,TKey)

其中,E1为对称加密运算函数,||表示信息级联运算。

8.根据权利要求1所述的隐藏超高频电子标签识别号的安全认证方法,其特征是:所述步骤(f)中,读写设备得到随机数RNr′为

{RNt″||RNr}=E2(MAC_2,TKey)

其中,E2为对称加密运算函数,||表示信息级联运算。

隐藏超高频电子标签识别号的安全认证方法

技术领域

[0001] 本发明涉及一种认证方法，尤其是一种隐藏超高频电子标签识别号的安全认证方法，属于超高频射频识别的技术领域。

背景技术

[0002] 射频识别(RFID)是一种基于无线通信的非接触式自动识别技术，是物联网领域的六大基础技术之一。射频识别技术无需通过物理接触，即可实现对物体信息的自动识别或读写，广泛应用于人员、动物、物品等身份自动识别和数字化管理。

[0003] 无源超高频射频识别(UHF RFID)是指工作频率为840～845MHz和920～925Mhz的射频识别系统。简单的电子标签识读系统由电子标签、读写设备、天线三部分组成，标签和读写设备采用电磁反向散射耦合方式进行通信，标签通过电磁感应获取工作所需能量，无需电池。

[0004] UHF RFID无线通信具有广播特性，特别是其识读距离远(5米至20米)，因此极容易遭受伪造、重放等攻击，因此，在射频识别系统应用中隐私保护和信息安全是需要重点考虑。目前，UHF RFID主要的空中接口协议标准有ISO18000-6C(简称6C标准)和我国2013年颁布的国家标准GB/T29768-2013。其中：6C标准只能通过访问密码保护电子标签用户区的数据，电子标签的访问密码和标识号(TID)在空中明文传输，因此，6C标准难于防止电子标签数据复制和盗用。而国家标准GB/T29768采用了基于对称密码算法的安全认证方法和通讯机制，因此，其安全性能与6C标准相比有了明显的提高。但是，由于国标GB/T 29768在安全认证过程中使用电子标签识别号(TID)作为密钥分散参数，需将TID明文返回，因此，国标GB/T29768仍然无法对TID信息进行读保护。而在涉车应用领域中，TID是电子标签所标识的车辆唯一标识信息，是涉车应用的核心信息，如果无法对TID进行保护，将存在非法读写设备通过识读TID，即可实现对车辆的轨迹跟踪，存在严重的安全隐患。

发明内容

[0005] 本发明的目的是克服现有技术中存在的不足，提供一种隐藏超高频电子标签识别号的安全认证方法，其能防止非法读写设备通过获取电子标签识别号实现车辆轨迹跟踪，确保电子标签与读写设备的身份互认和通讯。

[0006] 按照本发明提供的技术方案，一种隐藏超高频电子标签识别号的安全认证方法，所述认证方法包括如下步骤：

[0007] a、读写设备向电子标签发送认证请求信息，电子标签在收到读写设备发送的认证请求信息后，从电子标签的安全信息区内读出批密钥BKey并从标识信息区内读出电子标签批号TBN；电子标签将批密钥BKey、电子标签批号TBN以及随机数RNt与电子标签识别号TID进行加密运算，得到标签加密识别号TID′，电子标签将标签加密识别号TID′、随机数RNt以及电子标签批号TBN作为应答返回至读写设备内；

[0008] b、读写设备接收标签加密识别号TID′、随机数RNt以及电子标签批号TBN，利用认

证根密钥RKey对电子标签批号TBN进行加密分散，以得到读写批密钥BKey′，利用读写批密钥BKey′对标签加密识别号TID′以及随机数RNt进行解密运算，以得到读写标签解密识别号TID″；

[0009] c、读写设备利用认证根密钥RKey对读写标签解密识别号TID″加密分散，以获得读写单标签认证密钥TKey′，并将读写单标签认证密钥TKey′与随机数RNr进行加密运算，以得到读写访问控制码MAC_1，读写设备将读写访问控制码MAC_1发送至电子标签；

[0010] d、电子标签接收读写访问控制码MAC_1，利用安全信息区的单标签密钥TKey进行解密运算，以得到随机数RNt′；电子标签将随机数RNt′与随机数RNt进行比较，当随机数RNt′与随机数RNt不一致时，则终止与读写设备间的认证过程，否则，进入步骤e；

[0011] e、电子标签再次产生随机数RNt″，并将所述随机数RNt″与单标签认证密钥TKey进行加密运算，以得到标签访问控制码MAC_2，并将所述标签访问控制码MAC_2发送至读写设备；

[0012] f、读写设备接收标签访问控制码MAC_2，并利用读写单标签认证密钥TKey′对标签访问控制码MAC_2进行解密运算，以得到随机数RNr′；若随机数RNr′与随机数RNr一致时，则读写设备通过电子标签的认证，否则认证失败。

[0013] 所述步骤b中，认证根密钥RKey位于读写设备的安全控制模块SAM内，安全控制模块SAM利用认证根密钥RKey对电子标签批号TBN进行加密分散，以得到读写批密钥BKey′。

[0014] 所述步骤a中，电子标签对电子标签识别号TID、随机数RNt以及电子标签批密钥BKey进行加密运算，得到电子标签将标签加密识别号TID′为

[0015] $$TID' = E1(TID \oplus RNt, BKey)$$

[0016] 其中，E1为对称加密运算函数，⊕为异或运算。

[0017] 所述步骤b中，读写设备得到读写标签解密识别号TID″为

[0018] $$TID'' = E2(TID', BKey) \oplus RNt$$

[0019] 其中，E2为对称加密运算函数，⊕为异或运算。

[0020] 所述步骤c中，读写设备得到读写访问控制码MAC_1为

[0021] $MAC_1 = E2(RNt||RNr, TKey')$

[0022] 其中，E2为对称加密运算函数，||表示信息级联运算。

[0023] 所述步骤d中，电子标签得到随机数RNt′为

[0024] $\{RNt'||RNr\} = E1(MAC_1, TKey)$

[0025] 其中，E1为对称加密运算函数，||表示信息级联运算。

[0026] 所述步骤e中，电子标签得到标签读写访问控制码MAC_2为

[0027] $MAC_2 = E1(RNt''||RNr, TKey)$

[0028] 其中，E1为对称加密运算函数，||表示信息级联运算。

[0029] 所述步骤f中，读写设备得到随机数RNr′为

[0030] $\{RNt''||RNr\} = E2(MAC_2, TKey)$

[0031] 其中，E2为对称加密运算函数，||表示信息级联运算。

[0032] 本发明对射频识别系统存在的安全隐患和隐私问题都能较好的防护。特别针对涉车领域，这种安装认证方式优势更加明显。具体有如下优点：

[0033] 1、具有电子标签标识号TID信息保护功能。本发明的安全认证方法中，电子标签标识号TID信息与随机数异或并加密后返回。因此，同一个电子标签的每次返回值是不同的，

这样能有效防止非法读写设备通过记录标签响应信息，对标签进行跟踪。

[0034] 2、单标签单密钥的双向身份认证。所述安全认证方法中每张标签均有不同身份认证密钥，即使通过非法的方式获知了单标签密钥，也只能读取单张标签数据，无法读取其他电子标签存储的数据，从而有效的防止标签存储信息被窃取。

[0035] 3、所述安全认证方法适用于需要高速、远距离识读等涉车应用领域。在所述认证方法中，读写设备发出认证请求后，电子标签首先返回包含电子标签识别号TID的密文信息，因此，即使后续安全认证步骤失败，所述读写设备也能获得该电子标签的电子标签识别号TID。在涉车应用中，电子标签识别号TID可以唯一对应车辆，通过后台应用系统检索可获知车辆注册的身份信息。

附图说明

[0036] 图1为本发明无源超高频射频识别系统安全认证系统的结构示意图。

[0037] 图2为本发明隐藏超高频电子标签识别号的安全认证方法流程示意图。

具体实施方式

[0038] 下面结合具体附图和实施例对本发明作进一步说明。

[0039] 如图1所示：本发明的无源超高频射频识别系统认证系统的结构示意图，系统包括电子标签和读写设备组成。

[0040] 所述电子标签包含标识信息区、用户数据区、安全信息区三个存储分区。所述标识信息区存储电子标签识别号TID(唯一序列号)和电子标签批号TBN信息。所述电子标签识别号TID由标签芯片生产企业初始化写入，所述电子标签批号TBN由密钥管理中心完成电子标签的初始化写入，电子标签识别号TID、电子标签批号TBN写入后不可更改；所述用户数据区存储所标识物品的个性化信息，这些信息在电子标签实际使用时个性化写入；所述安全信息区存储批密钥BKey和单标签认证密钥TKey，所述批密钥BKey和单标签认证密钥TKey由认证根密钥RKey对电子标签批号TBN和电子标签识别号TID加密分散生成，与电子标签批号TBN信息同步写入。

[0041] 所述读写设备内置的安全控制模块SAM存储认证根密钥RKey信息，由授权的管理机关写入。

[0042] 为了能防止非法读写设备通过获取电子标签识别号实现车辆轨迹跟踪，确保电子标签与读写设备的身份互认和通讯，本发明的认证方法包括如下步骤：

[0043] a、读写设备向电子标签发送认证请求信息，电子标签在收到读写设备发送的认证请求信息后，从电子标签的安全信息区内读出批密钥BKey并从标识信息区内读出电子标签批号TBN；电子标签将批密钥BKey、电子标签批号TBN以及随机数RNt与电子标签识别号TID进行加密运算，得到标签加密识别号TID′，电子标签将标签加密识别号TID′、随机数RNt以及电子标签批号TBN作为应答返回至读写设备内；

[0044] 具体地，电子标签对电子标签识别号TID、随机数RNt以及电子标签批密钥BKey进行加密运算，得到电子标签将标签加密识别号TID′为

[0045] $TID' = E1(TID \oplus RNt, BKey)$

[0046] 其中，E1为对称加密运算函数，$\oplus$ 为异或运算。随机数RNt为在电子标签内随机产

生的数值。

[0047] b、读写设备接收标签加密识别号TID′、随机数RNt以及电子标签批号TBN，利用认证根密钥RKey对电子标签批号TBN进行加密分散，以得到读写批密钥BKey′，利用读写批密钥BKey′对标签加密识别号TID′以及随机数RNt进行解密运算，以得到读写标签解密识别号TID″；

[0048] 认证根密钥RKey位于读写设备的安全控制模块SAM内，安全控制模块SAM利用认证根密钥RKey对电子标签批号TBN进行加密分散，以得到读写批密钥BKey′。计算公式如下：

[0049] BKey′＝ED(TBN,RKey)

[0050] 其中，ED为加密分散运算函数。

[0051] 所述步骤b中，读写设备得到读写标签解密识别号TID″为

[0052] $TID'' = E2(TID', BKey) \oplus RNt$

[0053] 其中，E2为对称加密运算函数，⊕为异或运算。

[0054] 在具体实施时，对于经过授权合法的读写设备，所述电子标签内的加密函数E1与读写设备内的加密函数E2为预先设定的加密类型，经过电子标签加密得到的标签加密识别号TID′在读写设备内能够解密得到读写标签解密识别号TID″，具体实施过程为本技术领域人员所熟知。当读写设备为合法设备时，得到的读写批密钥BKey′会与电子标签内的批密钥BKey相一致。当为非法读写设备时，得到的读写批密钥BKey′与电子标签内的批密钥BKey不一致，因此，得到的读写标签解密识别号TID″不是预设得到的结果。

[0055] c、读写设备利用认证根密钥RKey对读写标签解密识别号TID″加密分散，以获得读写单标签认证密钥TKey′，并将读写单标签认证密钥TKey′与随机数RNr进行加密运算，以得到读写访问控制码MAC_1，读写设备将读写访问控制码MAC_1发送至电子标签；

[0056] 所述步骤c中，读写设备得到读写访问控制码MAC_1为

[0057] MAC_1＝E2(RNt||RNr,TKey′)

[0058] 其中，E2为对称加密运算函数，||表示信息级联运算。

[0059] d、电子标签接收读写访问控制码MAC_1，利用安全信息区的单标签密钥TKey进行解密运算，以得到随机数RNt′；电子标签将随机数RNt′与随机数RNt进行比较，当随机数RNt′与随机数RNt不一致时，则终止与读写设备间的认证过程，否则，进入步骤e；

[0060] 电子标签得到随机数RNt′为

[0061] {RNt′||RNr}＝E1(MAC_1,TKey)

[0062] 其中，E1为对称加密运算函数，||表示信息级联运算。

[0063] e、电子标签再次产生随机数RNt″，并将所述随机数RNt″与单标签认证密钥TKey进行加密运算，以得到标签访问控制码MAC_2，并将所述标签访问控制码MAC_2发送至读写设备；

[0064] 电子标签得到标签读写访问控制码MAC_2为

[0065] MAC_2＝E1(RNt″||RNr,TKey)

[0066] 其中，E1为对称加密运算函数，||表示信息级联运算。

[0067] f、读写设备接收标签访问控制码MAC_2，并利用读写单标签认证密钥TKey′对标签访问控制码MAC_2进行解密运算，以得到随机数RNr′；若随机数RNr′与随机数RNr一致时，则读写设备通过电子标签的认证，否则认证失败。

[0068] 读写设备得到随机数RNr′为

[0069] $\{RNt''||RNr\}=E2(MAC_2,TKey)$

[0070] 其中，E2为对称加密运算函数，||表示信息级联运算。

[0071] 本发明具体实施方式中，所述步骤中a-f的对称加密运算函数E1、E2的加密算法使用国密算法SM7，加密分散函数ED的加密算法使用SM1算法。但本发明具体实施方式所述对称加密算法不仅限于SM7算法，也可使用SM4、DES、3DES等对称加密算法。

[0072] 本发明通过对电子标签识别号TID进行随机数加密后，以密文方式返回，能有效防止非法读写设备获取电子标签识别号TID信息实现对电子标签所标识的物品进行非法跟踪和身份识别。同时，该认证方法能有效抵御窃听、仿冒和重放等攻击，具有防止电子标签信息被窃取、防止伪造标签等优点。该安全认证方法使用国密对称加密算法，采用双密钥和二次认证机制，实现了批量卡同密钥的电子标签合法性验证和单标签单密钥的双向安全验证。

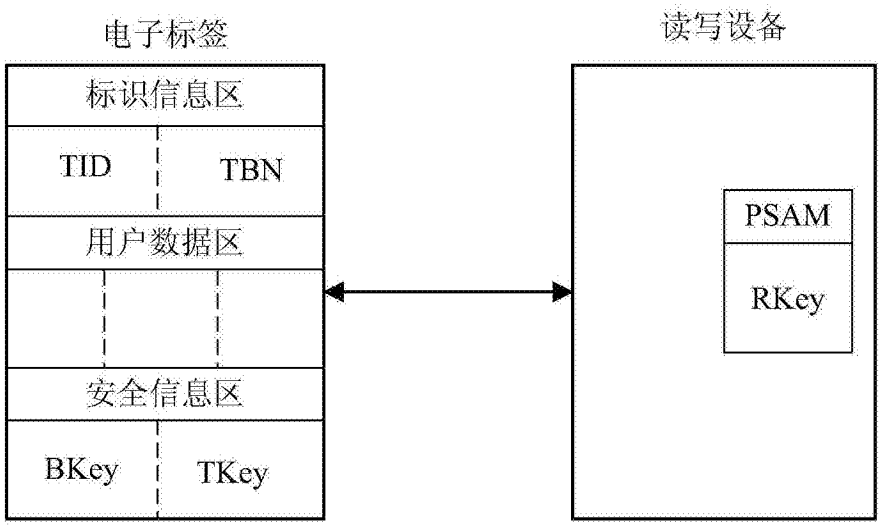

电子标签
读写设备
标识信息区
TID
TBN
用户数据区
安全信息区
BKey
TKey
PSAM
RKey

图1

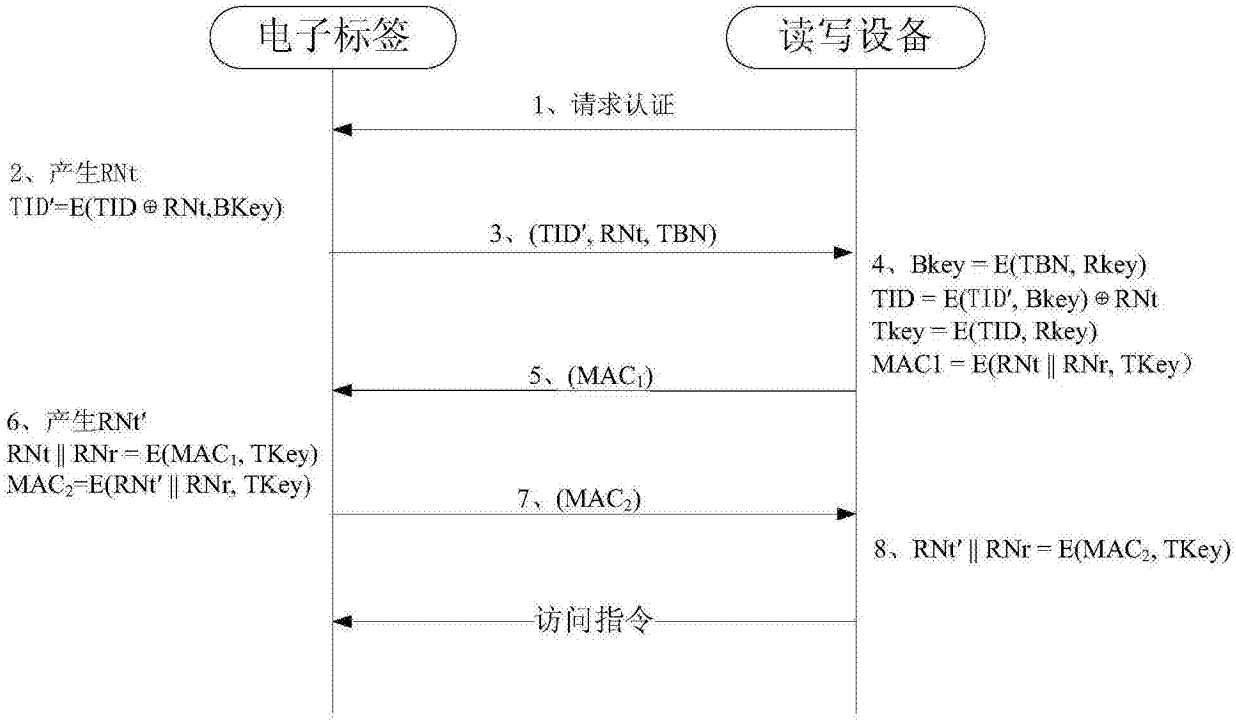

电子标签
读写设备
1、请求认证
2、产生RNt
TID'=E(TID ⊕ RNt,BKey)
3、(TID', RNt, TBN)
4、Bkey = E(TBN, Rkey)
TID = E(TID', Bkey) ⊕ RNt
Tkey = E(TID, Rkey)
MAC1 = E(RNt || RNr, TKey)
5、(MAC1)
6、产生RNt'
RNt || RNr = E(MAC1, TKey)
MAC2=E(RNt' || RNr, TKey)
7、(MAC2)
8、RNt' || RNr = E(MAC2, TKey)
访问指令

图2