电子不停车收费系统（ETC）安全模型设计*

全晓琪 陈积常 黄赢** 李建

南宁学院信息工程学院，南宁 530200

摘 要 随着移动通信网络技术的不断发展，电子不停车收费（ETC）系统已然成为一种便捷经济的通行方式。但伴随而来的ETC网络安全威胁不容忽视。因此，如何应用国密技术保护ETC系统的安全是一个亟待解决的重要课题。论文首先分析了当前电子不停车收费（ETC）系统面临的网络安全风险并进行了风险评估，提出了ETC安全通信需求，构建了ETC安全通信模型，设计了ETC安全通信协议，对通信协议进行了安全性分析。分析结果表明：ETC通信协议能够抵御网络黑客发动的身份假冒、信息篡改、信息重放、敏感信息窃取以及通信业务否认等主动和被动攻击，能够有效保护用户信息的安全和支付交易的正常进行。

关键字 电子不停车收费系统,CA, SM3国密算法, PKI技术, Xshell软件

Electronic Free-Flow Toll Collection System (ETC) Security Model Design

Quan Xiaoqi Cheng Jichang Huang ying Li Jian

School of Information Engineering Nanning University
Nanning 530200, China;
2425463574@qq.com

Abstract—With the continuous development of mobile communication network technology, Electronic Toll Collection (ETC) system has become a convenient and economical way. However, the security threat of ETC network can not be ignored. Therefore, how to protect the security of ETC system by using state secret technology is an important issue to be solved urgently.Firstly, the paper analyzes the network security risks faced by the current electronic toll collection (ETC) system, evaluates the risks, puts forward the security communication requirements of ETC, and constructs the ETC security communication model. The ETC secure communication protocol is designed and the security of the communication protocol is analyzed. The analysis results show that ETC communication protocol can resist the active and passive attacks such as identity impersonation, information tampering, information replay, sensitive information theft and communication service denial launched by network hackers, and can effectively protect the security of user information and the normal payment transaction.

Keywords—Electronic Free-Stop Charging (ETC) System, CA, SM3 National Cryptography Algorithm, PKI Technology, Xshell Sof

1 引 言

随着 ETC 系统的普及，网络安全威胁如影随行，为应对日益严峻的网络安全形势，国内外学者进行了大量的研究工作[1]。文献[2]从互联网可见资产排查、网络安全管理自查、系统安全管理自查、系统漏洞检查和加固、入侵痕迹排查和修复的角度检查了 ETC 系统面临的网络安全风险。文献[3]针对高速公路用户的办公网络需要更加开放，网络系统不可避免地会遭受外界环境的恶意攻击，提出了专用网络通信加密、入侵检测系统和三级安全管理等建议，但是没有具体的解决方案。文献[4]就长三角 ETC 的应用中存在的网络安全问题进行了研究，提出了基于 RSA、DES 的密码解决方案，但这些算法已被证明存在安全漏洞，可能为黑客攻击打开方便之门。文献[5]在介绍现有的电子不停车收费系统的基础上，提出了基于 DES 和 RSA 密码技术的安全方案，由于这两种都是国外存在安全漏洞的技术，不符合国家信息系统密码应用基本要求。

国外 ETC 系统的发展从萌芽阶段一直到 80 年代，其研究人员对 ETC 系统进行了深入研究。例如基于 RFID、DSRC、GPS / GNSS 和基于视频分析的电子收费系统[6]。他们关注 ETC 系统在通信和数据传输过程中的安全问题，提出了一系列的安全措施和加密算法，保护用户隐私和防止数据泄露。研究人员通过对 ETC 系统数据的分析，可以实现实时交通监测和路况预测解决交通拥堵和安全隐患问题[7]。

综上所述，ETC 信息系统是整个网络空间的重要一环，如何应用《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》[8]等标准，使用国家商用密码技术提供解决方案是一个亟待研究的重要课题。

*基金资助：本文得到南宁学院教学质量与教学改革工程项目《网络安全》核心课程（2022BKHXK09）和南宁学院一流专业培育项目（2020YLZYPY01）资助。

**通讯作者：黄赢 293453561@qq.com

2 ETC 安全通信系统模型需求分析

2．1 系统安全风险与评估

ETC 系统的安全风险大致有以下几种:

（1）重放攻击。攻击者通过窃取合法节点或车辆身份 ID 的认证信息，并将信息再重新发送到认证节点或车辆，以通过认证，从而达到欺骗的目的[9]。

（2）篡改攻击。通过攻击节点截获信道中的传输信息，然后对信息进行删除、篡改或替换再重新发送给其他节点，从而达到非法目的[10]。例如，不法分子企图篡改用户信息，从而获取不当利益。

（3）假冒攻击是指两个方面，一方面是黑客盗取 OBU 设备中的信息，篡改帐号和密码、冒用用户信息，导致给用户带来损失，进而破坏整个 ETC 系统通信甚至导致瘫痪。另一方面是黑客利用虚拟的网络假冒实体，进而给系统间的相互认证造成安全威胁。

2．2 模型功能需求分析

（1）身份鉴别的可靠性。当OBU、ETC和银行三方进行相互认证、信息传输时，会先进行双方身份鉴别，保证双方通信身份真实有效，防止黑客入侵ETC，进而进行篡改、伪造或传播虚假信息。

（2）传输信息的完整性和机密性。在安全通信系统中，确定信息传输的保密性和数据完整性的最基本要求是使用加密算法对信息进行加密，以便在交换信息时保护双方之间的通信信息。

（3）不可否认性。为了防止接收方或发送方否认接收过某条信息或否认发送过某条信息，双方都需采用数字签名[11]技术对数据进行处理，保证双方通信的不可否认。

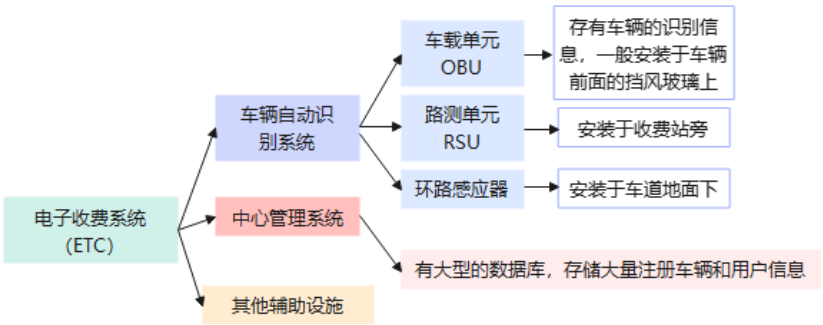

图 1 电子收费系统 ETC 组成图

ETC 是一种利用微波通信、自动控制和移动通信技术的先进收费方式。相比于半自动收费 MTC，ETC 完全采用电子联网收费方式[14]，收费站的收费方式如图 2 所示。

图 2 ETC 安全通信收费方式图

3 基于国密技术的 ETC 安全模型研究

3．1 安全通信系统架构

电子收费系统，主要由车辆自动识别系统、中心管理系统和辅助设施三部分组成，其中车辆自动识别系统，主要由安装于车辆挡风玻璃上的车载单元（OBU）、安装于收费站旁边的路边单元（RSU）和安装于车道下面的环路感应器构成。而中心管理系统作为 ETC 的大脑，内部存储大量注册车辆的基本信息[12]。

ETC 不停车收费系统的工作原理是通过安装在车辆挡风玻璃上的车载电子标签（OBU 设备），与在收费站 ETC 车道上路测单元（RSU）的微波天线之间进行短程通信，并利用计算机联网技术与银行系统进行后台实时结算处理，从而达到车辆通过路桥收费站时，不需要停车而能缴纳路桥费的目的[13]，ETC 电子收费系统组成如图 1 所示。

通信流程：车辆进入通讯范围时 ETC 系统与 OBU 设备（电子标签和 CPU 卡）进行通讯，判别车辆是否有效，如有效则进行交易；无效则报警并封闭车道，直到车辆离开检测线圈。安全通信架构如图 3 所示。

3．2 密码保障方案

（1）证书机构CA。CA(Certificate Authority，证书授权)是由认证机构服务者签发，是数字签名的技术基础保障，也是网上实体身份的证明，能够证明某一实体的身份及其公钥的合法性，证明该实体与公钥二

者之间的匹配关系。CA认证系统[15]组成如图4所示。

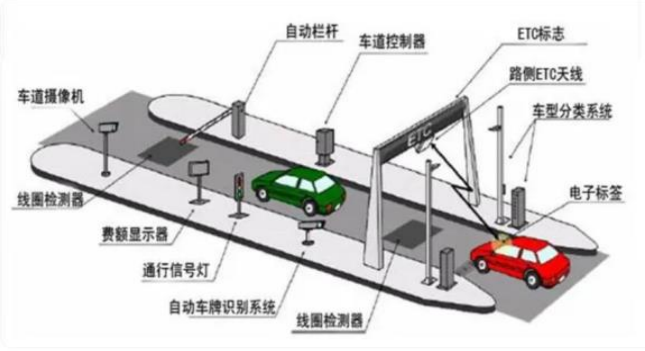

图 3 ETC 安全通信系统架构图

（2）数字证书。数字证书是一种数字文档，证明用于加密在线资产（即电子邮件通信、文档、网站或软件应用程序）的公钥的真实性。数字证书使用密码学和公钥验证站点、计算机或个人的身份，保证只有授权的设备才能连接到组织的网络。

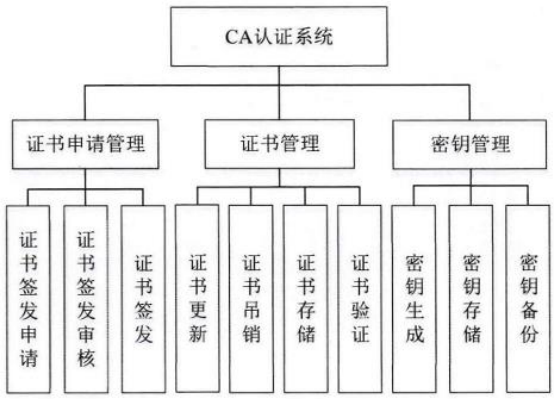

图 4 CA 认证系统组成

（3）数字证书签名。数字签名仅是消息发送者创建的数字字符串，其他人无法伪造此数字字符串，这证明发送者的消息是真实的，用于标识数字信息的公钥密码字段。ETC 系统使用数字签名是确保网络信息安全的重要手段,通过数字签名机制有效避免伪造、抵赖、篡改、假冒[16]。

（4）哈希运算。哈希算法是一种将任意长度的输入数据输出为固定长度值的算法，输入数据一般被称为消息，其长度一般为一个有限的值以内的任意值，输出值称为摘要或散列值[17]。ETC 系统使用哈希算法的目的就是为了验证原始数据是否被篡改。

4 ETC 系统的安全通信协议

4．1 ETC 系统安全通信协议设计

本协议先利用 CA 对三方颁发证书，再使用 SM2、SM3、数字签名技术以及数字证书实现 OBU 设备、ETC 系统和银行系统之间的双向身份鉴别，如果鉴别通过，就可以使用加密算法实现 OBU 设备、ETC 系统和银行系统之间的数据传输。协议中所使用的符号如表 1 所示，ETC 安全通信协议流程如图 5 所示。

ETC 安全通信协议流程如图 5 所示。

表 1 协议通信符号说明

符 号	说 明
ID_E	ETC系统身份
ID_O	OBU设备身份
ID_B	银行系统身份
T_X	时间戳
H	杂凑运算值
||	拼接操作
Ex[Y]	用x对Y进行加密
Dx[Y]	用x对Y进行解密
SK_E	ETC系统用SM2算法的私钥
PK_E	ETC系统用SM2算法的公钥
SK_O	OBU设备用SM2算法的私钥
PK_O	OBU设备用SM2算法的公钥
SK_B	银行系统用SM2算法的私钥
PK_B	银行系统用SM2算法的公钥
SK_{CA}	CA用SM2算法的私钥
PK_{CA}	CA用SM2算法的公钥
Verified OK	验证成功
Read IC	读身份卡命令
Information	车主身份卡中余额
Balance	银行扣费中的余额
OK	身份认证和扣费成功

4．2 ETC 系统安全通信协议流程说明

① $E_{SKCA}(ID_E||PK_E||T_2)||ID_E||ID_B||T_1||E_{SKE}[H(ID_E||ID_B||T_1)]$

ETC系统将CA颁发的ETC系统的证书、身份信息、时间戳和数字签发送给银行系统。

② 银行系统对ETC系统进行如下身份鉴别：

（1）在银行系统中，首先从CA发行证书中提取CA公钥值，然后从ETC系统的证书中提取CA签名值，最后，用ETC系统证书的CA签名值验证CA的公钥。

$H_1=D_{PKCA}[E_{SKCA}H(PK_E||ID_E||T_2)]=H(PK_E||ID_E||T_2)$

银行系统计算哈希值H_2 $H_2=H(PK_E||ID_E||T_2)$

判断H_1、H_2是否相等，如果$H_1=H_2$则可确认此证书是由CA签发的证书且证书没有被篡改。

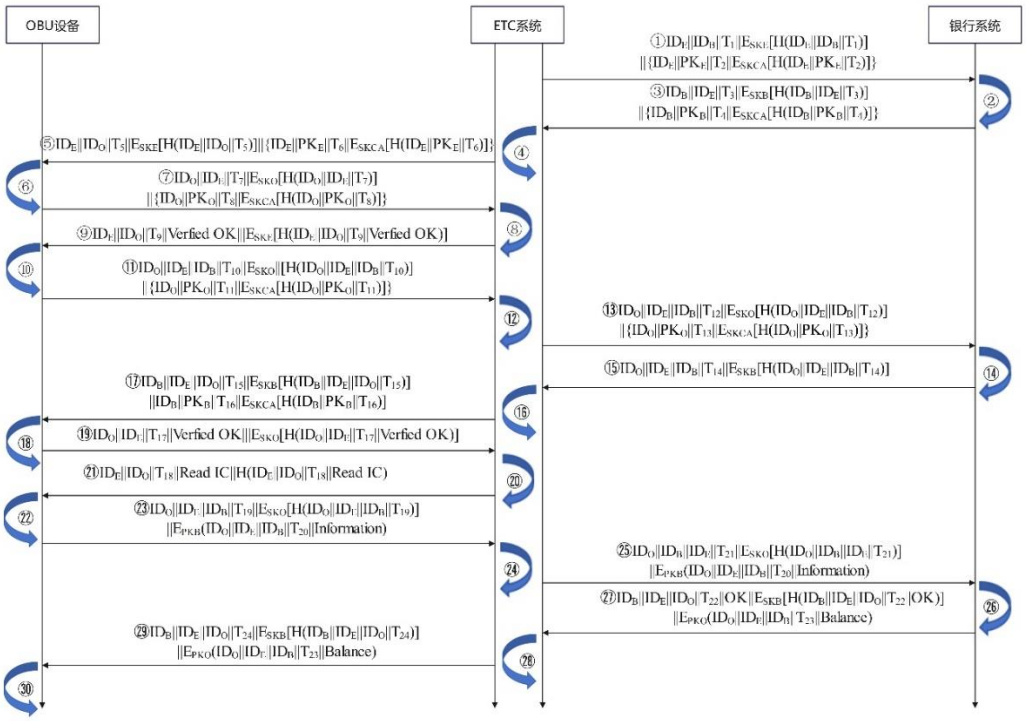

图 5 ETC 安全通信协议流程图

（2）用ETC系统的公钥验证ETC系统的签名

$H_3=D_{PKE}[E_{SKE}(H(ID_E||ID_B||T_1))]=H(ID_E||ID_B||T_1)$

（3）银行系统计算哈希值H_4 $H_4=H(ID_E||ID_B||T_1)$

（4）判断H_3是否等于H_4，如果$H_3=H_4$则银行系统则可以确认发送者是真正的ETC系统，并且确认数据在传输过程中没有被改变。

③ $E_{SKCA}(PK_B||ID_B||T_4)||ID_B||ID_E||T_3||E_{SKB}[H(ID_B||ID_E||T_3)]$

银行系统将CA颁发的证书连同身份信息、数字签名和时间戳一发送给ETC系统。

④ ETC系统对银行系统进行了如下身份鉴别：

（1）ETC系统使用CA的公钥来验证银行系统证书的是否为真。

$H_5=D_{PKCA}[E_{SKCA}(H(PK_B||ID_B||T_4))]=H(PK_B||IDB||T_4)$

ETC系统计算哈希值H_6 $H_6=(PK_B||ID_B||T_4)$

判断H_5、H_6是否相等，如果$H_5=H_6$则可以确认CA签发的证书是有效的并且证书没有被篡改。

（2）使用银行系统的公钥来验证银行系统的签名

$H_7=D_{PKB}[E_{SKB}(H(ID_B||ID_E||T_3))]=H(ID_B||ID_E||T_3)$

（3）ETC系统计算哈希值H_8 $H_8=H(ID_B||ID_E||T_3)$

判断H_7、H_8是否相等，如果$H_7=H_8$则ETC系统则可以确认发送者是真正的银行系统，且数据未被改变。

⑤ $E_{SKCA}(ID_E||PK_E||T_6)||ID_E||ID_O||T_5||E_{SKE}[H(ID_E||ID_O||T_5)]$

ETC系统将CA颁发的证书连同身份信息、数字签名和时间戳一发送给OBU设备。

⑥ OBU设备对ETC系统进行身份鉴别如下：

（1）OBU先从CA颁发的证书中提取CA公钥值，再从ETC系统证书中提取CA签名值，最后使用CA公钥值验证ETC系统证书中的CA签名值。

$H_9=D_{PKCA}[E_{SKCA}(H(ID_E||PK_E||T_6))]=H(ID_E||PK_E||T_6)$

OBU设备计算哈希值H_{10} $H_{10}=H(ID_E||PK_E||T_6)$

判断H_9、H_{10}是否相等，如果$H_9=H_{10}$则可确认此证书是有效的并且证书在传输过程中没有被篡改。

（2）用ETC系统的公钥来验证ETC系统的签名

$H_{11}=D_{PKE}[E_{SKE}(H(ID_E||ID_O||T_5))]=H(ID_E||ID_O||T_5)$

（3）OBU设备计算哈希值H_{12} $H_{12}=H(ID_E||ID_O||T_5)$

判断H_{11}、H_{12}是否相等，如果$H_{11}=H_{12}$则OBU设备则发送者就是真正的ETC系统，且数据没有被改变，

⑦ $E_{SKCA}(PK_O||ID_O||T_8)||ID_O||ID_E||T_7||E_{SKO}[H(ID_O||ID_E||T_7)]$

OBU设备将CA签发的OBU设备证书、身份信息、数字签名以及时间戳一同发给ETC系统。

⑧ 同②④⑥采用的技术一样：ETC系统对OBU设备进行了身份鉴别；若是鉴别通过，则确认OBU。

⑨ $ID_E||ID_O||T_9||Verified\ OK||E_{SKE}[H(ID_E||ID_O||T_9||Verified\ OK)]$

ETC系统将发送身份、时间戳、数字签名以及确认信息一同发给OBU设备。

⑩ 用ETC系统的公钥来验证ETC系统的签名

$H_{15}=D_{PKE}[E_{SKE}(H(ID_E||ID_O||T_9||Verified\ OK))]=H(ID_E||ID_O||T_9||Verified\ OK)$

OBU设备计算哈希值H_{16}

$H_{16}=H(ID_E||ID_O||T_9||Verified\ OK)$

判断H_{15}、H_{16}是否等于，如果$H_{15}=H_{16}$则OBU设备可确认发送者是真正的ETC系统。

⑪ $ID_O||ID_E||ID_B||T_{10}||H(ID_O||ID_E||ID_B||T_{10})$

OBU设备将设备证书、身份信息、时间戳、数字签名的指示，通过ETC系统转发给银行系统。

⑫ 同上步骤：ETC系统对OBU设备进行身份鉴别；若是鉴别通过，则可确认通信的是OBU设备。

⑬$E_{SKCA}(PK_O||ID_O||T_8)||ID_O||ID_E||ID_B||T_{11}||E_{SKE}[H(ID_O||ID_E||ID_B||T_{11})]$

ETC系统将由CA签发的OBU设备的证书、身份信息、时间戳以及数字签名一同发给银行系统。

⑭ 同上步骤：银行系统对OBU设备进行身份鉴别；若是鉴别通过，则可确认通信的是OBU设备。

⑮ $ID_O||ID_E||ID_B||T_{12}||E_{SKB}[H(ID_O||ID_E||ID_B||T_{12})]$

银行系统确认了OBU身份并向ETC系统发出指示让ETC系统帮忙发送身份、时间戳、数字签名给OBU。

⑯ 同上步骤：ETC系统对银行系统进行身份鉴别；若是鉴别通过，则可确认通信的是银行系统。

⑰ $E_{SKCA}(PK_B||ID_B||T_4)||ID_B||ID_E||\ ID_O||T_{13}||H(ID_B||ID_E||ID_O||T_{13})$

ETC系统将银行系统的身份信息、用户名、时间戳以及数字签名一同发给OBU设备。

⑱同上步骤：OBU设备对银行系统进行身份鉴别；若是鉴别通过，则可确认通信的是银行系统。

⑲ $E_{SKO}[H(ID_O||ID_E||T_{14}||Verified\ OK)||ID_O||ID_E||T_{14}||Verified\ OK$

OBU设备将身份、时间戳、确认信息以及数字签名发给ETC系统。

⑳ 用OBU设备的公钥验证OBU设备的签名

$H_{25}=D_{PKE}[E_{SKE}(H(ID_E||ID_O||T_{14}||Verified\ OK))]=H(ID_E||ID_O||T_{14}||Verified\ OK)$

OBU设备计算哈希值H_{26}

$H_{26}=H(ID_E||ID_O||T_{14}||Verified\ OK)$

判断H_{25}是否等于H_{25}，如果$H_{25}=H_{26}$则OBU确认发送者就是ETC系统。

㉑ $ID_E||ID_O||T_{15}||Read\ IC||H(ID_E||ID_O||\ T_{15}||Read\ IC)$

ETC系统想要读取OBU设备的卡里的信息。

㉒ OBU用ETC的公钥验证ETC系统的数字签名

$H_{27}=H(ID_E||ID_O||\ T_{15}||Read\ IC)$

OBU设备计算哈希值H_{28}

$H_{28}=H(ID_E||ID_O||T_{15}||Read\ IC)$

判断H_{27}是否等于H_{28}，如果相等则OBU设备确认发送者就是ETC系统，否则将不与其进行通信。

㉓ $ID_O||ID_E||ID_B||T_{16}||E_{SKO}[H(ID_O||ID_E||ID_B||T_{16})]||E_{PKB}[H(ID_O||ID_E||ID_B||T_{17}||Information)]$

OBU向ETC发送身份、时间戳并向ETC系统发指示让ETC转发加密$ID_O||ID_E||ID_B||T_{17}||Information$的值

㉔ 用OBU设备的公钥验证OBU设备的签名

$H_{29}=D_{PKO}[E_{SKO}(H(ID_O||ID_E||ID_B||T_{16}))]=H(ID_O||ID_E||ID_B||T_{16})$

ETC系统计算哈希值H_{30}，$H_{30}=H(ID_O||ID_E||ID_B||T_{16})$

判断H_{29}是否等于H_{30}，如果$H_{29}=H_{30}$则ETC系统确认发送者就是OBU设备，否则将不与其进行通信。

㉕ $ID_O||ID_E||ID_B||T_{18}||E_{SKO}[H(ID_O||ID_E||ID_B||T_{18})]||E_{PKB}[H(ID_O||ID_E||ID_B||T_{17}||Information)]$

ETC系统向银行系统转发OBU设备需要发送给银行系统的信息

㉖ 银行系统对OBU设备进行身份鉴别如下：

（1）用ETC系统的公钥验证ETC系统的签名

$H_{31}=D_{PKE}[E_{SKE}(H(ID_O||ID_E||ID_B||T_{18}))]=H(ID_O||ID_E||ID_B||T_{18})$

银行计算哈希值H_{32}，$H_{32}=H(ID_O||ID_E||ID_B||T_{18})$，判断$H_{31}$是否等于$H_{32}$，若$H_{31}=H_{32}$则信息没有被篡改。

（2）用自己的公钥进行解密

$H_{33}=D_{SKB}[E_{PKB}[H(ID_O||ID_E||ID_B||T_{17}||Information)]=H(ID_O||ID_E||ID_B||T_{17}||Information)$

银行系统计算哈希值H_{34}

$H_{34}=H(ID_O||ID_E||ID_B||T_{17}||Information)$

判断H_{34}是否等于H_{35}，如果$H_{34}=H_{35}$则确认信息在传输过程中没有被篡改，验证成功后进行下一步。

㉗ $ID_B||ID_E||ID_O||T_{19}||OK||E_{SKE}[H(ID_B||ID_E||ID_O||T_{19}||OK)]||E_{PKO}[H(ID_B||ID_E||ID_O||T_{20}||Balance)$

银行向ETC发送身份、时间戳、向ETC系统发出OK指示并让ETC加密$ID_O||ID_E||ID_B||T_{20}||$ Balance。

㉘ ETC系统对银行系统进行身份鉴别如下：

（1）用银行系统的公钥验证银行系统的签名

$H_{33}=D_{PKE}[E_{SKE}(H(ID_B||ID_E||ID_O||T_{19}||OK))]=H(ID_B||ID_E||ID_O||T_{19}||OK)$

银行系统计算哈希值H_{34}

$H_{34}=H(ID_B||ID_E||ID_O||T_{19}||OK)$

判断H_{33}是否等于H_{34}，如果$H_{33}=H_{34}$则ETC系统确认发送者就是银行系统且信息在传输中没有被篡改。

（2）ETC系统确认得到OK的指令，打开闸门。

㉙ $ID_E||ID_O||T_{24}||E_{SKB}[H(ID_B||ID_E||ID_O||T_{21})]||E_{PKO}[H\ (ID_B||ID_E||ID_O||T_{20}||Balance)$

ETC向OBU转发银行系统发送给OBU的信息

㉚ OBU设备对ETC系统进行身份鉴别如下：

（1）用银行系统的公钥验证银行系统的签名

$H_{35}=D_{PKB}[E_{SKB}(H(ID_B||ID_E||ID_O||T_{21}))]=H(ID_B||ID_E||ID_O||T_{21}$

OBU计算哈希值H_{36}，$H_{36}=H(ID_B||ID_E||ID_O||T_{21})$

判断H_{35}是否等于H_{36}，如果$H_{35}=H_{36}$则OBU确认发送者就是ETC系统且信息在传输过程中没有被篡改。

（2）用自己的公钥进行解密

$H_{37}=D_{SKO}[E_{PKO}[H(ID_B||ID_E||ID_O||T_{20}||Balance)]=ID_B||ID_E||ID_O||T_{20}||Balanc$

OBU计算哈希值H_{38}

$H_{38}=H(ID_B||ID_E||ID_O||T_{20}||Balance)$

判断H_{37}是否等于H_{38}，如果相等则信息没有被篡改，OBU接收到来自银行系统发送余额并进行存储。

4．3　安全性分析

（1）抗身份假冒攻击。该协议利用 OBU、ETC 和银行间的双向身份认证来抵抗身份假冒攻击。在认证过程中，ETC 向银行发送 $E_{SKCA}(ID_E||PK_E||T_2)||ID_E||ID_B||T_1||E_{SKE}[H(ID_E||ID_B||T_1)]$。银行通过验证 $D_{PKCA}[E_{SKCA}H(PK_E||ID_E||T_2)]=H(PK_E||ID_E||T_2)$ 和 $H(PK_E||ID_E||T_2)$ 通信两方是否相等验证 ETC 身份，银行系统运用 ETC 系统的公钥来进行运算。ETC 系统也能通过运算哈希值 $D_{PKCA}[E_{SKCA}(H(PK_B||ID_B||T_4))]=H(PK_B||ID_B||T_4)$是否等于 $H(PK_B||ID_B||T_4)$验证银行系统的身份。OBU 和 ETC 之间也是相同原理进行相互验证。黑客要想伪造通信双方的签名，需要从对方的公钥提取相应的私钥，黑客要求椭圆曲线上的离散对数是不可能的。

（2）抗重放攻击。为了防止重放攻击，ETC 系统给银行系统发送验证请求时会含有一个时间戳。这个时间戳是由数字签名技术生成，用于验证消息是否是即时消息。当 ETC 系统发出 $ID_E||ID_B||T_1||E_{SKE}[H(ID_E||ID_B||T_1)]||\{ID_E||PK_E||T_2||E_{SKCA}[H(ID_E||PK_E||T_2)]\}$的消息，该消息以密文传输。所以，当黑客想将以前的 ETC 的消息重放发给银行系统时，银行系统计算 $D_{PKE}[E_{SKE}(H(ID_E||ID_B||T_1))]=H(ID_E||ID_B||T_1)$与 $H(ID_E||ID_B||T_1)$来验证时间戳的时效性。所以，就算攻击者向银行系统发送相同的信息，银行系统也会检查时间更新，以确定它是否非法。

（3）抗篡改攻击。当通信方两两完成身份验证时，协议会对通信双方进行数字签名运算，如在 ETC 系统和银行系统之间进行相互验证，传输的消息为 $ID_E||ID_B||T_1||E_{SKE}[H(ID_E||ID_B||T_1)]||\{ID_E||PK_E||T_2||E_{SKCA}[H(ID_E||PK_E||T_2)]\}$，倘若黑客想要改变身份 ID_E，$H_1=H(ID_E||ID_B||T_1)$就会发生改变，通信双方的身份验证就会不成功。在这种情况下，银行系统将确定对方不是合法的 ETC 系统，或者 ETC 系统的身份信息可能被黑客入侵。如果黑客试图操纵 ETC 系统的身份和签名信息，他们需要从客户端的公钥中获取私钥。但这是一个离散对数的问题,这是非常困难的，使用数字签名技术可以有效抵御黑客的操纵攻击，保护信息完整。

（4）防非法窃听。当数据通过通信传输时，SM2 算法会加密重要数据，例如在数据传输期间，如果黑客试图非法窃取数据，则需要使用同一密钥进行解密。否则将收到无法读取的加密文本字符串。因此，黑客是不能窃取到正在进行信息传输的数据。

4．4　代码运行测试

为了验证本文设计的的可行性，我们基于 Linux 操作系统，使用 Xshell 终端模拟软件和 GmSSL 密码 工具箱，编码实现了 ETC 功能模块和安全通信协议。三方双向身份鉴别和数据传输实现的代码运行的部分结果如图 6 所示。从代码运行结果来看，本文设计的 ETC 安全通信模型是可行并有效的。

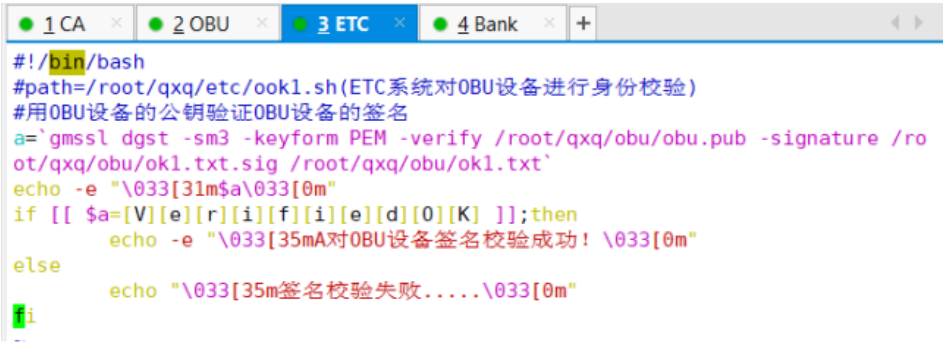

图 6　三方双向身份鉴别和数据传输图

5　结束语

论文首先分析了电子不停车收费（ETC）系统面临的网络安全风险并进行了风险评估，提出了 ETC 安全通信需求，构建了 ETC 安全通信模型。使用数字签名、数字签名验证、数字证书、加密与解密、密钥管理等密码技术，设计了 ETC 安全通信协议，对通信协议进行了安全性分析。

利用 PKI 技术、VMware 虚拟机、Xshell 软件、GmSSL 密码工具箱创建 CA，接着颁发数字证书给 OBU、ETC、银行，为建立网络信任打下了坚实基础。在三方双向认证和交易过程中，利用 SM2 算法对数据进行加解密和数字签名以及签名验证，利用 SM3 算法完成了对信息的哈希运算，保证了信息的完整性和交易顺利进行。

参 考 文 献

[1] 苏丽娅·艾尔肯.电子不停车收费系统(ETC)的设计及实际应用[J].机电信息,2019,(17):159+161.

[2] 王洪川.高速公路联网收费系统网络安全攻防演练综述[J].北方交通,2022(03):91-94

[3] 范平.高速公路联网收费系统网络安全浅析[J].城市建设理论研究(电子版),2023,(17):217-219.

[4] 杨祥妹,徐明,柯翔,等.长三角联网ETC在沪苏浙高速的应用[J].中国交通信息产业,2009(06):66-70.

[5] 范耀东. 陕西省高速公路ETC建设及运营体系研究[D].长安大学,2012.

[6] Electronic Toll Collection System Market by Type (ETC and AET), Product (AVI and AVC), Technology (RFID, DSRC, Video Analytics, and GNSS/GPS), Application (Highway and Urban) and Geography - Analysis Forecast (2014-2020)[J].M2 Presswire,2015,

[7] Design and Application of Electronic Toll Collection Special Situation Processing System[J].SAE International Journal of Connected and Automated Vehicles,2024,7(3):

[8] 中华人民共和国国家标准.GBT 39786-2021信息安全技术 信息系统密码应用基本要求[S].

[9] 郭焰辉,徐梓燕,杨知玲.车联网通信的安全性分析[J].中国新通信,2021,23(20):11-12.

[10] 密码行业标准化技术委员会.GM/T 0003.2-2012 SM2椭圆曲线公钥密码算法第2部分：数字签名算法[S].

[11] Digital Signatures[B]. Jonathan Katz. 2010

[12] 王主华.关于ETC车道经常出现邻道干扰现象的预防措施[A]. 《建筑科技与管理》组委会, 2020年5月建筑科技与管理学术交流会论文集[C]. 陕西汉唐计算机有限责任公司;: 2020: 81-82

[13] 雷菊华,赖波.停车场ETC收费系统进行车辆出入管理的应用探究[J].信息通信,2015,(03):274.

[14] 刘科文.高速公路ETC系统应用研究[J].企业科技与发展,2021,(07):52-54.

[15] 郭亚州.基于国密算法的CA认证应用研究[D].华北电力大学(北京),2023.DOI:10.27140/d.cnki.ghbbu.2023.001425.

[16] 田柳,林黄智.数字签名的车联网安全体系架构设计研究[J].太原学院学报(自然科学版),2024,42(01):47-53.DOI:10.14152/j.cnki.2096-191X.2024.01.008.

[17] 邱亚飞. 哈希算法的实现与验证[D].广东工业大学,2022.DOI:10.27029/d.cnki.ggdgu.2021.001943.