计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2018,27(11):247−251 [doi: 10.15888/j.cnki.csa.006638]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于 UDS 协议的 PEPS 系统安全认证方法①

詹克旭

(博世华域转向系统有限公司, 上海 201821)
通讯作者: 詹克旭, E-mail: zhankexu@163.com

摘　要: 无钥匙进入启动系统 (PEPS) 相对于传统的钥匙开启车门和启动汽车, 其通过低频和射频的通信, 实现汽车与钥匙之间复杂的双向身份认证. 为了保障双向身份认证, 本文详细介绍了基于 UDS 协议的 PEPS 系统安全认证方法. 通过 UDS 协议的诊断学习功能, 实现了遥控钥匙与 BCM、EMS 以及 ESCL 的认证保护机制, 以此保证了无钥匙进入启动系统 (PEPS) 工作的安全性, 为其迅速发展提供了有力的技术支撑.

关键词: UDS 协议; PEPS; 诊断服务; ESCL; LIN

引用格式: 詹克旭.基于 UDS 协议的 PEPS 系统安全认证方法.计算机系统应用,2018,27(11):247–251. http://www.c-s-a.org.cn/1003-3254/6638.html

Security Authentication Method of PEPS System Based on UDS Protocol

ZHAN Ke-Xu

(BOSCH HUAYU Steering System Co. Ltd., Shanghai 201821, China)

Abstract: Compared with the traditional key to open the door and start the car, the keyless Passive Entry and Passive Start (PEPS) system realizes the complex bi-directional identity authentication between the car and the key through the communication between low frequency and radio frequency. In order to guarantee two-way identity authentication, this paper introduces the security authentication method of PEPS system based on UDS protocol in detail. Through the diagnostic learning function of UDS protocol, the authentication protection mechanism of remote keys and BCM, EMS, and ESCL is realized, which ensures the safety of the keyless PEPS system and provides strong technical support for its rapid development.

Key words: UDS protocol; Passive Entry and Passive Start (PEPS); diagnostic service; ESCL; LIN

无钥匙进入及启动系统, 简称 PEPS (Passive Entry Passive Start) 系统, 它采用先进的 RFID 无线射频技术和车辆身份编码识别系统, 实现无需按动遥控器即可进入车内以及一键启动发动机等功能[1]. 当驾驶员携带智能钥匙进入车辆附近的有效范围内, 车辆会自动检测钥匙并进行身份识别. 如果身份识别成功, 相应门锁会解除防盗并自动打开. 当驾驶员进入车内时, 车辆会自动检测钥匙是否位于主驾位置. 如果检测成功, 驾驶员想要启动车辆, 只需通过按下启动按钮即可. 在整个开门上车到启动车辆过程, 驾驶员都无需拿出车钥匙. PEPS 系统的应用, 给用户带来更加舒适的体验以及更为安全的保障. 与传统的钥匙相比, 具有更高的防盗性能, 并给驾驶员带来了舒适、便利的全新驾车体验.

1　PEPS 系统构成

无钥匙进入及启动系统由智能钥匙、主控制器、一键启动、车门把手、电子转向锁 (ESCL) 等组成, 主控制器采用 LIN 总线与其他模块通讯[2, 3].

① 收稿时间: 2018-04-09; 修改时间: 2018-05-08; 采用时间: 2018-05-14; csa 在线出版时间: 2018-10-24

1.1 LIN 总线

LIN (Local Interconnect Network) 是一种低成本的串行通讯网络, 用于实现汽车中的分布式电子系统控制. LIN 的目标是为现有汽车网络 (例如 CAN 总线) 提供辅助功能, 因此 LIN 总线是一种辅助的总线网络. 在不需要 CAN 总线的带宽和多功能的场合, 使用 LIN 总线可大大节省成本[4–6].

在 PEPS 系统中, 主控制器有三路 LIN, 通过三路 LIN 实现相应的控制功能. 其系统构成如图 1 所示.

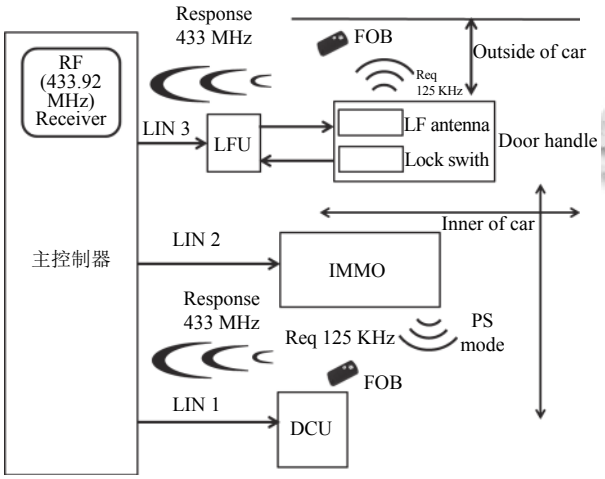

图 1 LIN 网络的构成

LIN1: 实现主控制器与门锁控制模块 (DCU) 的通讯;

LIN2: 实现主控制器与电源管理单元 (EBS) 和发动机防盗单元 (IMMO) 的通讯;

LIN3: 实现主控制器与低频控制单元 (LFU) 和电子转向锁 (ESCL) 的通讯.

1.2 主控制器

当拉动车门把手时, 主控制器产生 125 KHz 低频信号, 并通过射频接收器接收智能钥匙发送 433 MHz 的高频认证信号对智能钥匙进行身份识别. 主控制器主要实现了对射频响应信号的接受及低频询问信号的产生和发送、CAN 总线通信、发动机防盗认证、电源模块和 ESCL 认证等功能.

1.3 智能钥匙

为了保证在任意角度智能钥匙均能接收到的低频信号, 智能钥匙内安装三维全向 125 KHz 的低频接收天线. 智能钥匙验证低频信号合法后, 为了完成身份识别, 将产生 433.92 MHz 的高频认证信号向外发送.

1.4 一键启动

遥控钥匙认证后, 通过按下启停按钮启动车辆.

1.5 门把手

门把手由一个低频天线和微动开关组成, 当驾驶员拉动汽车门把时, 低频天线产生低频磁场在门把手周围特定区域内发射低频信号.

1.6 电子转向锁 (ESCL)

电子转向锁通过 LIN 总线进行学习和通讯, 转向锁的解锁和闭锁通过内置的小型电机通过驱动锁舌的伸缩动作来实现.

2 PEPS 工作原理

2.1 无钥匙进入

当驾驶员按下门把手上的按键后, 会触发主控制器驱动门把手上的低频天线发送 125 KHz 低频认证信号, 具有身份识别的智能钥匙接收到低频信号后, 与智能钥匙中保存的身份识别信息进行比较, 如果一致, 智能钥匙将被唤醒. 为了保证车辆发出的唤醒信号在有效范围内的任何方位都能检测到, 智能钥匙上采用三维全向天线能. 为了提高安全性, 智能钥匙被唤醒后发送 433 MHz 高频信号, 这些信号都经过加密处理. 车辆会将内部保存的信息同接收到的信号相比较, 若相同, 则表明验证通过, 进行解锁[7]. 驾驶员在无需掏出钥匙的情况下, 通过拉门把手上车. 无钥匙进入工作原理见图 2 所示.

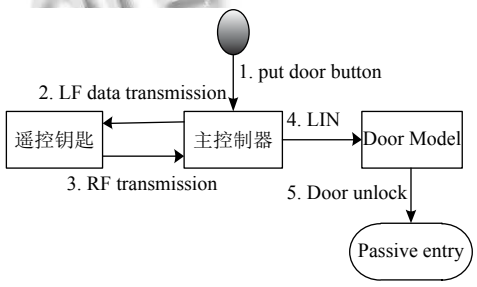

图 2 无钥匙进入工作原理

2.2 无钥匙启动

驾驶员进入车内后, 按下启停按钮, 主控制器驱动低频天线向外发送 125 kHz 低频信号. 智能钥匙将接收到的低频信号与智能钥匙保存的信息对比, 识别通过后智能钥匙发射 433.92 MHz 高频加密信号. 主控制器将接收到的高频加密信号进行解密、认证. 如果与系统内部的存储信息相吻合, 则表示钥匙辨识成功. 为

了确保非法用户无法使用车辆, 只有当识别成功后才能启动发动机, 否则如果钥匙识别错误或使用了非法钥匙, 则发动机将不能起动. 再启动发动机之前, 还要进行 ESCL 的加密通信来驱动锁舌至解锁位置、EMS 加密防盗通信, 最后才能启动车辆. 无钥匙启动工作原理见图 3 所示.

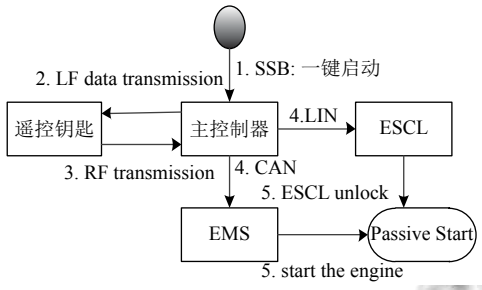

图 3 无钥匙启动工作原理

3 PEPS 学习匹配

由于 PEPS 系统通过低频和射频的双向通信, 汽车与智能钥匙之间需要完成复杂的双向身份认证. 为了保障系统的安全性, 实现系统的双向身份认证, 需要在车辆和遥控钥匙交付之前进行学习匹配工作. 本系统采用基于 UDS 协议的诊断服务进行学习匹配, 通过一定的诊断流程, 将主控制器与 EMS(发动机 ECU)、智能钥匙、ESCL 进行学习匹配.

3.1 UDS 协议

UDS 协议即 ISO14229 统一诊断服务 (Unified Diagnostic Services), 是诊断服务的规范化标准, 比如读取故障码应该向汽车 ECU 发什么指令, 读数据流又是发什么指令. 作为诊断仪与汽车 ECU 之间进行诊断通信必不可少的一部分, 一系列的诊断服务在诊断规范中被描述. 诊断规范定义了诊断仪和汽车 ECU 之间的请求响应规则、以及对于请求报文汽车 ECU 的处理行为. 汽车 CAN 诊断遵循 ISO15765 标准, 其中应用层遵循 ISO15765-3 标准, 作为 CAN 通讯软件设计的一个重要部分, 汽车 ECU 需要解析这些收到的报文, 从而得出完整的诊断服务[8,9].

本系统诊断服务参考 ISO 14229 标准[10]. 为了让汽车 ECU 能够执行相应的操作, 通过诊断仪 (Tester) 将诊断服务发送给汽车 ECU. 主控制器与遥控钥匙匹配学习必须至少支持如表 1 所示的诊断服务.

3.1.1 诊断会话控制 (10)

诊断会话控制服务由 Tester 发起请求, ECU 响应请求, 请求第一个字节为服务 0x10, 第二个字节为模式定义, 表示 ECU 处于不同的诊断会话模式, 在 Tester 请求不同模中, 其中 1 代表默认会话模式, 2 代表编程模式, 3 代表扩展会话模式. 对于本方案学习过程中使用到的安全访问 (27) 和例程控制 (31) 必须在扩展会话模式下才能进行.

表 1 诊断服务表

SID	诊断服务
0x10	诊断会话控制 DiagnosticSessionControl
0x27	安全访问 SecurityAccess
0x31	例程控制 RoutineControl

3.1.2 安全访问 (27)

安全访问的引入, 是为了对受限于访问安全的一些功能进行保护, 如例程控制、学习匹配等, 避免对汽车的安全性造成风险. 安全访问的概念使用“种子”和“密钥”来实现.

Tester 请求 ECU 解锁首先发送“RequestSeed”服务报文. ECU 发送一个种子进行响应, 此种子是密钥计算算法的输入参数. Tester 使用该种子计算出相应的密钥.

第二步, Tester 通过发送包含密钥的“SendKey”服务报文给 ECU 来请求比较密钥. ECU 须将此密钥与内部存储或计算的密钥进行比较, 如果两数相符, ECU 启动 (解锁)Tester 对特定服务和资料的访问权限. 如果两数不相符, 此访问被认为是一次错误的访问尝试. 安全访问流程如图 4 所示.

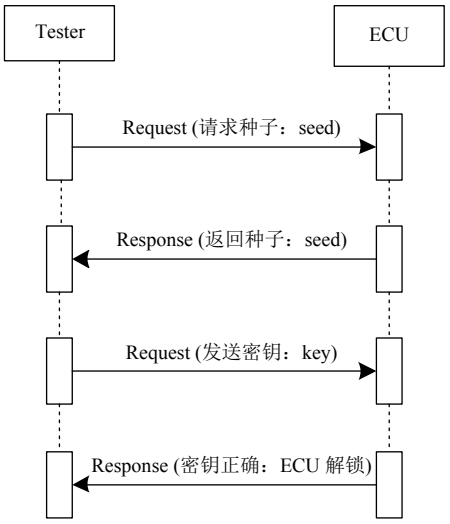

图 4 安全访问流程

为了系统的安全性, 一般采用两级安全访问策略, 本系统匹配学习需要两级安全进入才可以实现.

3.1.3 例程控制 (31)

Tester 使用本服务启动或停止 ECU 内存中的例程和请求例程结果. 例程由两字节的例程标识来确定, 为启动例程, 必须使用例程控制服务——启动例程 (31 01). 如果 ECU 支持停止例程的操作, 则必须使用例程控制服务——停止例程 (31 02), 本方案中无需停止例程操作.

根据例程标识的不同, 对 PEPS 系统进行不同的操作, 以达到学习匹配的目的. 本方案将会使用到发送 VIN&SC、匹配 EMS、学习遥控钥匙、复位 ESCL、学习 ESCL 等, 为了方便理解, 假定以上功能对应的例程标识分别为 0x0001、0x0002、0x0003、0x0004、0x0005, 具体设置根据 OEM 来设定.

3.2 匹配 EMS

在匹配主控制器和 EMS 时, 需要学习以下数据:

1) VIN: 汽车身份识别码, OEM 定义. 主控制器将 VIN 存在 EEPROM 中, 通过诊断服务 ($22/$2E) 读取或修改

2) SC: 由 VIN 码产生, 用于安全进入使用. 算法 SC=f(VIN) 由 OEM 控制.

3) SK: 主控制器与 EMS 认证的密钥, EMS 学习过程中由 Tester 设备随机产生, 并学习给主控制器与 EMS.

4) OUTCODE 为主控制器产生的随机数, INCODE=f2(SC, OUTCODE), 函数 f1() 和 f2() 由 OEM 控制.

为了保证 PEPS 系统的安全性, 本方案采用两级安全进入的工作方式, 具体匹配 EMS 流程如图 5 所示, 具体步骤如下:

1) Tester 设备一级解锁;

2) Tester 设备发送 VIN 码和 SC 给主控制器;

3) Tester 设备二级解锁, 主控制器随机产生 outcode 并返回给 Tester 设备;

4) Tester 设备根据接收到的 outcode 和 SC 计算 incode, 并将 incode 返回给主控制器;

5) 主控制器检查 incode 是否合法, 若不合法则此次安全进入不成功, 主控制器回复负响应, 等待下次学习指令, Tester 设备提示“安全进入失败”;

6) 主控制器检查 incode 是否合法, 若合法则此次安全进入成功, 主控制器回复负响应, Tester 设备提示“主控制器安全解除状态”;

7) Tester 设备接收到“主控制器安全解除状态”信息以后, 随机产生 SK, 进行匹配 EMS;

8) Tester 设备向主控制器发匹配 EMS 指令, 将 SK 信息写入主控制器;

9) Tester 设备向 EMS 发匹配 EMS 指令, 将 SC 和 SK 信息写入 EMS;

10) EMS 判断 SC 和 SK 的合法性 (非全 0 和全 F), 若合法则保存, 并向 Tester 设备回复正响应.

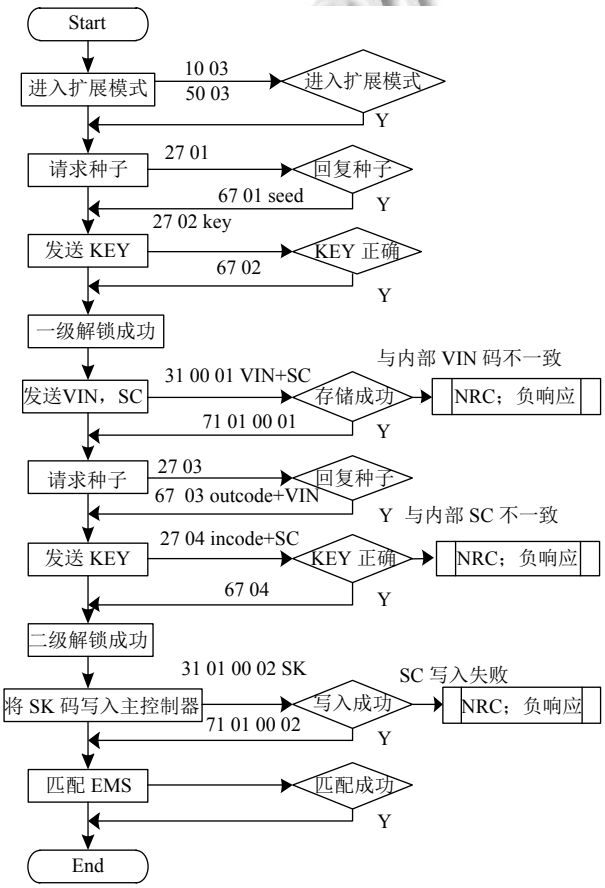

图 5 匹配 EMS

3.3 匹配钥匙和 ESCL

与匹配 EMS 方法相同, 为了保证系统的安全性, 匹配钥匙和匹配 ESCL 同样采用两级安全进入的工作方式, 具体流程如图 6 所示:

1) 二级解锁成功后进行钥匙学习;

2) 钥匙学习成功后进行 ESCL 复位命令, 主控制器通过 LIN 总线进行 LIN 诊断操作来复位 ESCL.

3) 复位成功后, 发送 ESCL 学习命令, ESCL 的学习通过 LIN 诊断实现.

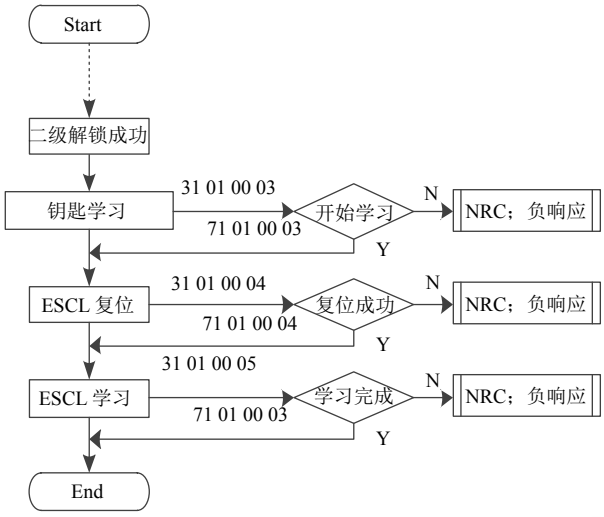

图 6 匹配钥匙和 ESCL

4 实验分析

经过 UDS 服务的诊断学习后, 智能钥匙已经与 PEPS 系统匹配成功. 为了验证经过学习匹配的智能钥匙的功能, 测试人员对无钥匙进入和启动功能进行了大量测试, 以验证系统的稳定性.

1) 无钥匙进入功能: 测试人员在车门锁好的情况下, 携带智能钥匙到车门前并拨动门把手, 此时车门被打开. 经过数次测试均能正常开启车门, 没有出现无法开启车门的情况, 符合无钥匙进入功能的要求;

2) 无钥匙启动功能: 携带智能钥匙的测试人员进入车门后, 按下一键启动按钮, 车辆可以正常启动. 经反复多次启动测试, 车辆均能正常启动, 没有出现无法启动的情况, 符合无钥匙启动功能的要求.

由于具备 PEPS 功能的汽车只能识别与其配对成功的智能钥匙, 本系统设计的学习匹配有一套完善的安全机制, 因此其他未学习匹配的职能钥匙并不能开启车辆, 对整车的安全性提供了保障.

经过验证, 系统运行稳定、有效性好, 正确率达到了百分之百. 同时, 系统的安全性高, 未经过学习匹配的智能钥匙无法开启车门, 进入车辆后也无法启动车辆. 此外, 该系统可以根据需要增加智能钥匙数量, 最大匹配钥匙数量为 3, 系统具有良好的易用性和可扩展性等优点.

5 结论和展望

本文详细介绍 PEPS 的工作原理和安全认证方法. 作为实现汽车与智能钥匙之间可以完成复杂的双向身份认证的有效的前提, 通过对 UDS 协议的诊断服务的详细介绍, 提供了一种有效的学习匹配方法.

UDS 协议作为汽车 ECU 开发中必不可缺的组成部分, 无论在汽车诊断、系统升级还是在学习匹配过程中, 都发挥着重要的作用. 一个完善的 UDS 协议学习匹配方法, 提高了系统的易用性和安全性, 对整个 PEPS 系统的开发有着重要的意义. 基于 UDS 协议的 PEPS 系统安全认证方法在国内某平台车型上已经得到了较好的应用, 并具有高度可扩展性和可维护性. 相信随着汽车产业的不断发展, PEPS 系统会进一步的普及, 本文介绍的安全性方案将会在越来越多的车型上应用.

参考文献

1 於仕达, 冯金芝, 郑松林, 等. 无钥匙进入起动系统的起动机控制功能模型研究. 控制工程, 2012, 19(S1): 207–210.
2 王成辉, 许勇. 基于 Turbo 码模型的汽车 PEPS 系统加密算法. 桂林电子科技大学学报, 2017, 37(1): 49–53. [doi: 10.3969/j.issn.1673-808X.2017.01.010]
3 路平, 孙灿, 张进明. PEPS 系统集成 TPMS 的方案设计研究. 汽车电器, 2016, (5): 47–50. [doi: 10.3969/j.issn.1003-8639.2016.05.013]
4 江学焕, 张金亮, 樊红莉, 等. 基于 CAN/LIN 双总线电动汽车数字仪表系统的设计. 计算机工程与科学, 2015, 37(11): 2182–2187. [doi: 10.3969/j.issn.1007-130X.2015.11.028]
5 张昱, 鲁睿婷, 唐厚君, 等. 基于 CAN/LIN 混合网络的车门控制系统. 电气自动化, 2013, 35(3): 36–38. [doi: 10.3969/j.issn.1000-3886.2013.03.013]
6 凌滨, 索健文, 许景涛. 基于指纹识别与 LIN 总线的汽车车门系统设计. 计算机测量与控制, 2016, 24(3): 193–195.
7 李滨, 秦贵和, 赵睿, 等. 基于 CAN 总线和互联网的被动无钥匙进入系统. 计算机工程与设计, 2016, 37(4): 897–901.
8 陈姿霖, 宋磊锋, 张龙岗, 等. 基于 UDS 的整车诊断系统设计方法. 汽车电器, 2017, (4): 14–17.
9 游长能. 基于 LabVIEW 的 CAN 总线 UDS 诊断工具开发. 电子测试, 2016, (19): 59–60. [doi: 10.3969/j.issn.1000-8519.2016.19.024]
10 ISO. ISO 14229-1: 2013 Road vehicles—Unified diagnostic services (UDS) —Part 1: Specification and requirements. 2013.