基于 CPK 的车内高速总线动态密钥管理方案

薛梦阳[1]，　陈　铎[1]，　巢时刚[2]，　李益发[1]

(1. 郑州大学 网络空间安全学院　河南 郑州 450001；2. 宜春学院 数学与计算机科学学院　江西 宜春 336000)

摘要：随着车联网的高速发展,车内安全问题越来越突出。使用密码算法实现认证和保密是解决车内安全问题的必然选择,其关键是密钥管理。常用的公钥证书方案消耗较多的计算资源,时延较大,缺乏安全防护。提出了一种基于组合公钥(CPK)的无证书新型动态密钥管理方案,在汽车启动瞬间,由车载网关动态生成 CPK 矩阵并更新私钥,既可实现强认证和保密,同时能防止 OBD 静态攻击。

关键词：车载网络；密钥管理；组合公钥(CPK)；安全通信

中图分类号：TN918　　**文献标志码**：A　　**文章编号**：1671-6841(2023)02-0018-07

DOI：10.13705/j.issn.1671-6841.2022100

Dynamic Key Management Scheme In-vehicle High-speed Bus Based on CPK

XUE Mengyang[1], CHEN Duo[1], CHAO Shigang[2], LI Yifa[1]

(1. *School of Cyber Science and Engineering, Zhengzhou University, Zhengzhou* 450001, *China*; 2. *Mathematics and Computer Science, Yichun University, Yichun* 336000, *China*)

Abstract: With the rapid development of the internet of vehicles, the issue of in-vehicle security was becoming prominent. Using cryptographic algorithms to achieve authentication and confidentiality was an inevitable choice to solve the problem of vehicle interior security, and the most important was the key management. The common public key certificate schemes consumed more computing resources, with longer delay and lower security protection. A new certificateless dynamic key management scheme based on combined public key (CPK) was proposed. At the moment of vehicle startup, the CPK matrix was dynamically generated by the vehicle gateway and the private key was updated. The strong authentication and confidentiality were realized, and the OBD static attacks was prevented.

Key words: vehicle network; key management; combination public key(CPK); secure communication

0　引言

随着智能网联汽车日渐成为全球汽车领域的研究热点和产业增长的新动力,我国也把研究发展智能网联汽车作为中国汽车产业发展的国家战略,智能网联是抢占未来汽车工程领域的关键核心技术。

相应地,汽车安全问题也日益受到重视。网联使得汽车在不断智能化的同时,由独立封闭走向互联开放,从而使网络攻击可远程实施于车身。车内的电子控制单元(electronic control unit,ECU)节点使用以太网、CAN[1]、FlexRAY[2]、LIN[3]等多种网络通信协议,其中,使用较多的是以太网和 CAN,但其协议中或缺乏必要的安全机制,仅有简单的完整性校验,或使用对称密码算法和固定密钥,极易被攻击。为方便诊断维护,汽车都存在 OBD 接口,使得

收稿日期:2022-04-15
基金项目:2020 年工业互联网创新发展工程项目-智能网联汽车车载安全网关项目(TC200H033)。
第一作者:薛梦阳(1996—),男,硕士研究生,主要从事密码学、车联网安全通信研究,E-mail:zzu2249846678@163.com。
通信作者:李益发(1964—),男,教授,主要从事物联网安全研究,E-mail:alphalyf@163.com。

从该接口可获得车内各 ECU 的信息。在停车状态下,通过该接口可轻易窃取固定密钥。而密钥被窃取后,汽车安全机制形同虚设。

通过对车载 ECU 的分析和攻击实验[4],可实现远程操控汽车方向盘、窃取车内数据,暴露出汽车在智能化、网联化过程中所存在的隐私数据泄露、人身安全威胁等诸多安全问题。因此,有必要在智能网联汽车中采用更强的安全机制。

国际上已有很多相关研究和探讨,形成了诸多安全方案,涉及标识认证机制、保密通信机制、安全存储机制、车载密钥管理等方面,其中密钥管理是研究的核心所在[5]。

早期的车内通信都是基于低速高可靠 CAN 总线结构,这种结构限制了很多密码技术的应用,因此加密和认证功能较弱。随着智能网联汽车的发展,混合型结构成为主流技术,如高速 CAN 总线和低速 CAN 总线混合[6]、以太网与 CAN 总线混合[7]、其他新型总线与传统低速高可靠 CAN 总线混合[8]等。

为解决当前车内总线网络被恶意攻击的安全问题,文献[9]提出基于加密方法的安全机制,为现有车内网安全通信奠定了基础。文献[10]提出了一个采用代理重加密(PRE)方案的车载网络模型,所有数据都使用一个主密钥进行加密。该主密钥由 VCU 单独保存,而且针对一组特殊节点同时多次请求数据的情况提出了一种组密钥管理方案。针对车内的密钥分发问题,文献[11]提出了基于集中式网关的方案,它使用证书验证每个 ECU,然后根据不同类型的总线分发组密钥。文献[12]提出了基于对称密钥的集中式密钥管理方案,解决了相互认证问题。但此方案的安全性完全依赖于集中式密钥生成器,这可能导致单点故障从而影响全车安全。因此文献[13]提出了一个半集中式的动态密钥管理框架,该框架在车辆运行过程中提供分散和动态的密钥生成。

使用非对称算法必须对公钥进行管理,国际上通常使用 RSA 和 ECC 算法,国内则使用 SM2 算法,确保公钥的真实性。国际通用的公钥管理模式是 PKI/CA 模式[14],即由证书机构为每个公钥签发证书。但证书验证会增加时延,难以满足网联汽车对低时延的需求。

基于标识的组合公钥(combined public key,CPK)是一种新型集中式无证书公钥管理模式[15-17],在公钥管理方面具有诸多优势,且在无线传感器密钥管理方案[18]和远程身份认证方案[19]等多种安全方案中得到了应用。因此,本文提出了一种基于 CPK 的动态密钥管理方案。该方案使用 SM2/3/4 国标算法[20],在汽车启动瞬间(3 s 内),由网关作为车内的密钥管理中心(key management center,KMC),动态生成公、私钥矩阵,先广播公钥矩阵(私钥矩阵由网关安全保存),然后采用专门的密钥分发协议安全分发各节点的私钥。每个节点只需要存储一个通过广播接收的公钥矩阵、广播密钥、会话密钥及自己的私钥,不需要公钥证书和其他额外存储空间。

由于 CPK 具有无证书、本地化的特点,所有节点的公钥可根据标识在本地查找,因此一个节点可以即时发起与另一节点的保密通信或密钥协商,且只需要一次签名验证即可实现标识鉴别,完成节点间的身份认证。

此外,由于本方案在每次汽车启动的瞬间更新车内所有域控和 ECU 终端的密钥,因此停车状态下即使密钥被窃取,也不影响汽车启动后的安全,所以本方案可有效防止 OBD 静态攻击。

1　车内高速总线动态密钥管理方案

汽车网关是汽车的中心设备。在智能网联汽车中,车载网关既是汽车的内部管理中心,也是与外部连接的关口。由于静态环境下(停车状态),OBD 接口容易获取 ECU 和网关内的数据,因此私钥在静态环境下是不安全的。所以本文采用动态更新方案,即在每次汽车启动时更新矩阵及私钥。

汽车熄火后,网关处于待机状态,一些功能已经关闭,但并没有完全关机,还可以接受网络指令。此时网关功耗很低,由蓄电池供电。网关对汽车的熄火有明确的自动感知功能。当汽车再次点火时,网关重新生成 CPK 矩阵,并分发到车载以太网直联的域控和 ECU 中。

1.1　CPK 动态公、私钥矩阵生成

CPK 基于 ECC 或国标 SM2 算法,文献[21-23]对其安全性有详细分析。尽管存在共谋攻击,但在动态更新公、私钥矩阵的车内环境下,其安全性不受影响。

动态 CPK 矩阵生成方法如下。网关先切断与外界的通信,结束一切不必要的进程,确保生成公、私钥矩阵及分发公钥矩阵的过程不受网络入侵和木马攻击。

首先生成私钥因子,若网关内有真随机数发生器,则用该生成器生成需要的私钥因子即可。

否则,取北斗授时(如果没有的话取网关本地时钟的时间)信息,读取车内的温度、油量、里程数

等数据,加上网关内安全保存的根密钥,用 SM3 计算其哈希值,记为 IV,

$$IV = h_{SM3}(k_0 \| T \| t \| s \| o \| kiv), \quad (1)$$

其中:k_0 为网关内安全保存的根密钥;T 为北斗授时或本地网关时钟的时间;t 为车内温度;s 为车辆目前的里程数;o 是车内当前油量;kiv 是一个指定的键值,用于生成特定的初始向量。然后网关计算 $a_i = h_{SM3}(IV, c_i)$,h_{SM3} 为一个哈希函数;c_i 为计数器的值,$i = 1,2,\cdots,32$;a_i 作为私钥因子,按列填充为 4×8 的矩阵,即 $r_{11} = a_1, r_{21} = a_2, \cdots, r_{48} = a_{32}$。

私钥因子所对应的公钥因子为 $R = rP$。其中 P 为所选择的 ECC 椭圆曲线群 G 上的 n 阶生成元。

于是,生成公、私钥矩阵分别为

$$\boldsymbol{SKM} = \begin{pmatrix} r_{11} & r_{12} & \cdots & r_{18} \\ r_{21} & r_{22} & \cdots & r_{28} \\ r_{31} & r_{32} & \cdots & r_{38} \\ r_{41} & r_{42} & \cdots & r_{48} \end{pmatrix} = \begin{pmatrix} a_1 & a_5 & \cdots & a_{29} \\ a_2 & a_6 & \cdots & a_{30} \\ a_3 & a_7 & \cdots & a_{31} \\ a_4 & a_8 & \cdots & a_{32} \end{pmatrix},$$

$$\boldsymbol{PKM} = \begin{Bmatrix} R_{11} & R_{12} & \cdots & R_{18} \\ R_{21} & R_{22} & \cdots & R_{28} \\ R_{31} & R_{32} & \cdots & R_{38} \\ R_{41} & R_{42} & \cdots & R_{48} \end{Bmatrix}。$$

然后,网关将公钥矩阵 $\boldsymbol{PKM}$ 广播给所有域控和 ECU 等终端,终端收到公钥矩阵后,开始申请私钥。

1.2 动态 CPK 设备私钥分发协议

车辆出厂前,需要在每个 ECU 节点中预先安全存放一个用于与网关来进行传递私钥的共享秘密 x_i, x_i 写入 ECU 的芯片内,OBD 接口不可读取。网关通过使用 x_i 并结合一些参数来生成相应的会话密钥,用来加密私钥,完成私钥的传递,避免私钥被恶意 ECU 节点冒领。

动态 CPK 的设备私钥分发协议如图 1。

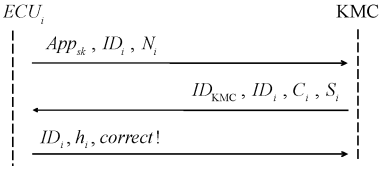

图 1 私钥分发协议

Figure 1 Private key distribution protocol

其中 KMC 的功能由车载网关完成。具体分发步骤如下。

1)节点 ECU_i 发起私钥申请,App_{sk} 为申请私钥标识符。申请时,要先生成一次性随机数 N_i,然后将 ECU_i 节点的标识 ID_i 和 N_i 一起发送给网关。

2)网关使用共享秘密 x_i、N_i 和 ID_i 生成会话密钥 k_i。根据 ECU_i 的标识查询私钥矩阵 $\boldsymbol{SKM}$,计算出 ECU_i 的私钥 sk_i。接着,网关生成一个广播密钥 k^*,将广播密钥 k^* 和 ECU_i 的私钥 sk_i 用会话密钥 k_i 加密,发送给 ECU_i。同时,网关保存该会话密钥 k_i 和广播密钥 k^*,k_i 为此后与 ECU_i 通信时密钥,k^* 为广播信息的加密、解密密钥。同时,网关对密文进行签名。

$$k_i = h_{SM3}(ID_i \| N_i \| x_i),$$

$$C_i = E_{SM4}(k_i, sk_i \| ID_{KMC} \| ID_i \| k^*),$$

$$S_i = Sig_{SM2}(sk_{KMC}, ID_i \| C_i),$$

其中:ID_{KMC} 为 KMC 的标识;E_{SM4} 为加密函数;C_i 为加密的密文;Sig_{SM2} 为签名函数;S_i 为签名值。KMC 计算节点 ECU_i 的私钥过程为

$$sk_i = \varphi_{SKM}(h_{SM3}(ID_i)) = \sum_{k=1}^{8} r_{i_k,k} \bmod n,$$

$$k^* = E_{SM4}(k_0, T \| t \| s \| o),$$

其中:φ_{SKM} 为私钥查询函数;$r_{i_k,k}$ 为私钥矩阵 $\boldsymbol{SKM}$ 中第 i_k 行、第 k 列的私钥因子。

3)ECU_i 收到信息后,先验证网关的签名。验证签名时,KMC 的公钥可直接通过本地公钥矩阵 $\boldsymbol{PKM}$ 查询。然后解密密文,获得签名私钥和广播密钥。获得私钥后,立即验证自己的私钥是否正确。验证私钥时,先用公钥矩阵查询 ECU_i 的公钥 pk_i,然后对 N_i 进行一次加密、解密运算,

$$pk_i = \varphi_{PKM}(h_{SM3}(ID_i)) = \sum_{k=1}^{8} R_{i_k,k},$$

$$VC_i = E_{SM2}(pk_i, N_i),$$

$$N_i =? = D_{SM2}(sk_i, VC_i),$$

其中:φ_{PKM} 为公钥查询函数;$R_{i_k,k}$ 为公钥矩阵 $\boldsymbol{PKM}$ 中第 i_k 行、第 k 列的公钥因子;VC_i 为使用 pk_i 对 N_i 加密后的密文;D_{SM2} 为解密函数。若解密结果与 N_i 不等,则向网关发送出错信息,要求重新分发私钥。若相等,则安全保存私钥 sk_i 和广播密钥 k^*,并计算

$$h_i = h_{SM3}(k_i, ID_i \| sk_i),$$

发送 ID_i 和 h_i 通知网关已成功接收私钥。

网关收到消息后,校验哈希值 h_i,确认 ECU_i 已成功接收私钥。在分发 ECU 私钥的过程中,网关保存广播密钥和各 ECU 的会话密钥,形成会话密钥

表,同时删除私钥矩阵 ***SKM***, 以免受到在线攻击。

2　性能分析

2.1　安全性分析

首先,对私钥分发协议的安全性进行分析,它是保证私钥在分发过程不被窃取的基础。

私钥分发协议的前提是,网关作为 KMC 已生成公、私钥矩阵,并广播公钥矩阵,使得所有 ECU 节点都获得了公钥矩阵,且每个 ECU 都有一个与网关共享的秘密值 x_i。

在申请私钥的过程中,ECU 节点将自己的标识(ID_i)、一次性随机数(N_i)等信息发送给网关。

在此过程,如果车内有 ECU 节点被植入了攻击性软件,该 ECU 能够获取普通 ECU 所发送的 ID_i、N_i 等消息,但是并没有该 ECU 和网关之间的共享秘密 x_i, 无法生成会话密钥 k_i, 不能解密使用 k_i 加密过的密文。网关还可利用 N_i 判别该会话密钥的新鲜性,确保该消息不是重放的。

网关通过 ID_i 在私钥矩阵中查找并计算该 ECU 节点对应的私钥 sk_i, 并生成一个广播密钥 k^*, 将 k^* 和 sk_i 等用会话密钥 k_i 加密后发送给 ECU。同时还用自己的私钥对该密文进行签名,证明 sk_i 是由网关发送给该 ECU 节点的私钥。由于 k_i 是 x_i 结合其他参数生成的,使用该密钥加密的密文即使被敌手获取,也无法获取 sk_i, 因为这相当于攻破了加密算法。私钥分发协议可以有效保证 sk_i 和 k^* 的机密性。而网关的签名也保证了该私钥一定是网关生成的。同时, N_i 和 k_i 的使用,保证了 k^* 和 sk_i 的新鲜性。

其次,分析 CPK 的安全性。CPK 基于 SM2 算法,其理论基础是椭圆曲线上离散对数难题。密码算法是安全的。但 CPK 的确存在共谋攻击[21-23]。共谋的前提是知道一定数量的私钥,因此保护私钥是抵抗共谋攻击的关键。

在本方案中,我们所采取的措施是动态分配私钥。车内节点所使用的公、私钥矩阵在生成前,网关会先切断与外界的通信,结束一切不必要的进程,确保生成公、私钥矩阵及分发公钥矩阵的过程不受网络入侵和木马攻击。网关将公钥矩阵广播给所有域控和 ECU。ECU 收到公钥矩阵后,执行私钥分发协议申请私钥。当所有 ECU 节点收到私钥后,网关保存自己的私钥、广播密钥及各 ECU 的会话密钥,之后会删除私钥矩阵,避免私钥矩阵的泄露。

外部设备可以通过对外接口在车停下来的静态情况下获得网关及车内节点的各种信息。但是一旦车辆启动,网关会重新生成新的公、私钥矩阵,完成私钥的分配。因此敌手无法通过静态攻击获取有用的私钥。即便敌手能控制个别 ECU,但也只能获得其他 ECU 在密钥分发协议中的加密信息,仍无法获得新的密钥。

另外,车内通常采用 4×8 的小型公钥矩阵,而文献[21-23]的研究表明,至少需要获得 $4\times8-8+1=25$ 个线性无关的密钥才能进行共谋攻击。事实上,连接在高速总线上的节点也只有几十个,其他节点连接在低速总线上。考虑部分密钥是线性相关的,这意味着攻击者要获得大部分节点的私钥才能实施有效攻击。在汽车运动状态下,想要通过远程攻击获取 ECU 的密钥,必须要先攻破车载网关的安全防护。在车载网关实施安全认证的前提下,这几乎是不可能的。而获取多个 ECU 私钥实施共谋攻击,更是难以实现的。因此在汽车运动过程中无论是获取节点私钥还是进行共谋攻击都是难以实现的。

下面在 CPK 共谋攻击不成立的前提下,采用安全协议分析本征逻辑方法(SPALL[24]),对本方案中密钥分发协议的安全性进行分析。

根据协议过程,以 ID_i 代替 ECU_i, 以 ID_{KMC} 代替 KMC,即以标识代替实体,则有 $\Sigma=\{ID_i,ID_{KMC},N_i,C_i,S_i,h_i\}$, 且有

$$ID_i \ni N_i \in N,$$

$$ID_i \ni k_i = h_{SM3}(ID_i \| N_i \| x_i) \in R,$$

$$ID_{KMC} \ni k_i = h_{SM3}(ID_i \| N_i \| x_i) \in R,$$

$$ID_{KMC} \ni k^* \in R,$$

$$ID_{KMC} \ni C_i = E_{SM4}(k_i, sk_i \| ID_{KMC} \| ID_i \| k^*),$$

$$ID_{KMC} \ni S_i = Sig_{SM2}(sk_{KMC}, ID_i \| C_i),$$

$$ID_i \ni h_i = h_{SM3}(k_i, ID_i \| sk_i),$$

$$ID_{KMC} \ni h_i = h_{SM3}(k_i, ID_i \| sk_i),$$

$$ID_i \lhd \{C_i, S_i\}, ID_i \in \Omega, ID_{KMC} \in \Omega, x_i \in \Pi, N_i \in N,$$

其中:Σ 为基本消息集合;N 为随机数集合;Π 为共享秘密集合;Ω 为主机集合;R 为对称密钥集合;$\in$ 表示属于;$\ni$ 表示生成;$\lhd$ 表示看到。

由于 CPK 的特性决定了每个公钥都是由标识唯一确定的,因此有以下结论:

1) ID_i 相信 pk_{KMC} 是 ID_{KMC} 的公钥, ID_{KMC} 相信 pk_i 是 ID_i 的公钥。

2) x_i 是双方共享的秘密,因此有 ID_i 相信 ID_i 和 ID_{KMC} 共享 x_i, ID_{KMC} 相信 ID_i 与 ID_{KMC} 共享 x_i。

协议目标为 ID_i 获得私钥 sk_i, ID_i 相信私钥 sk_i

是新鲜的,保证最终只有 ID_i 和 ID_{KMC} 能够获得该私钥 sk_i,其他人无法获得,ID_i 要相信 sk_i 是双向可认证的。将目标公式中的 sk_i 换成 k^*,则 k^* 具有可获得性、新鲜性和双向可认证性。以下对 sk_i 进行分析,k^* 的相关性可同样能证明。

证明 由 $ID_i \lhd \{C_i, S_i\}$ 和 $ID_i \ni k_i$ 得

$$ID_i \lhd (sk_i, ID_{KMC}, ID_i, k^*),$$

从而有 $ID_i \lhd sk_i$,$ID_i \lhd k^*$。

由 $ID_i \ni N_i \in N$ 可得,ID_i 相信 N_i 是新鲜的,再由 $ID_i \ni k_i = h_{SM3}(ID_i \| N_i \| x_i)$ 可得,ID_i 相信 k_i 是新鲜的,进而有 ID_i 相信 C_i 是新鲜的,从而有 ID_i 相信 sk_i 是新鲜的。

由 $ID_i \lhd S_i$ 可推导出,ID_i 相信 ID_{KMC} 生成了私钥 sk_i,以及 ID_i 相信 sk_i 是发送给自己的,于是有 ID_i 相信 sk_i 是双向可认证的。

对于机密性,假设 $U \lhd sk_i$,则或者 $U \ni sk_i$,由此可得 $U = ID_{KMC}$;或者 $U \lhd C_i$,且 U 相信 sk_i 可以从密文 C_i 中恢复出来,于是有 $U \lhd k_i$。但 $k_i = h_{SM3}(ID_i \| N_i \| x_i)$,从而必有 $U \lhd x_i$。

由于 ID_i 相信 ID_i 和 ID_{KMC} 共享 x_i,以及 ID_{KMC} 也相信 ID_i 与 ID_{KMC} 共享 x_i,可推出 U 为 ID_i 或是 ID_{KMC}。

综合以上情况可得:如果 $U \lhd sk_i$,那么 U 一定是 ID_i 和 ID_{KMC} 其中之一。这表明,得到私钥 sk_i 的只有 ID_i 和 ID_{KMC},机密性得证。

密钥管理方案具有机密性、认证性和新鲜性。

机密性:由上述证明可知,只有网关与申请该私钥的 ECU 节点能够得到 k^* 和 sk_i,其他节点无法获得 k^* 和 sk_i,因此机密性得证。

认证性:当 ECU 节点从网关处获得私钥时,可对网关的签名进行验证,从而认证 sk_i 必源自网关,不存在仿冒。

新鲜性:在 ECU 和网关的交互过程中,N_i 是 ECU 临时生成的,而 k_i 生成依赖于 N_i,从而保证了 k^* 和 sk_i 的新鲜性。

2.2 其他性能分析

1) 密钥存储空间分析。每个公钥因子为 512 bit,因此公钥矩阵仅需要 2 kB,与一个完整数字证书的大小几乎一样。

2) 私钥生成与分发效率分析。由于网关承担 KMC 的任务,而网关通常有比较高的计算性能,选择龙芯 2K1000 芯片为网关芯片。ECU 的芯片通常算力较低,实验时采用龙芯 1D-300 芯片,已符合大多数 ECU 的性能需求。对这两款芯片进行 100 轮测试,结果如表 1。

表 1 两种方案中各阶段时延

Table 1 The necessary time of different part in two schemes

单位:ms

方案	密钥生成	密钥分发	ECDH协商	通信认证	
				以太网	CAN
基于 CPK 方案	14.694	589.5	4.692	3.8	6.8
基于证书方案	127.132	821.3	6.855	8.8	73.8

以上测试中,密钥生成在本方案(基于 CPK 方案)中指公、私钥矩阵生成时间,共生成 64 个公、私钥因子,在证书方案中指生成 100 张证书的时间;密钥分发在本方案中指由私钥矩阵生成私钥,并分发私钥及公钥矩阵给 100 个 ECU 节点的时间,在证书方案中指分发私钥及证书给 100 个 ECU 节点的时间;ECDH 协商指的是两个 ECU 节点分别在两种方案下进行密钥协商的时间;通信认证指的是两个 ECU 节点分别在两种方案下进行保密通信及标识认证所需要的时间。

由表 1 可知,在密钥生成中,本方案所用时间是证书方案的 1/9;在密钥分发和 ECDH 协商中,本方案时间均少于证书方案;通信认证时,以太网环境下,本方案用时不到证书方案的 50%;CAN 环境下,本方案所需要时间不足证书方案通信认证的 10%,极大缩短了认证时间。本方案的密钥生成时延小于 20 ms,密钥分发时延小于 600 ms,考虑各 ECU 之间产生的时延,因此总的密钥分发时间在 3 s 内即可以完成。

使用密钥进行认证和保密通信的效率分析。

① 保密通信。基于数字证书,每次通信时需要先传递数字证书,不仅会增加通信内容,也增加了保密通信协议的步数,而且使用证书前还要对证书进行验证。而基于 CPK 的保密通信,可在公钥矩阵中直接查找对方的公钥,即刻发起保密通信。效率明显高于数字证书模式。

② 标识认证。基于证书的认证,必然要验证证书,需要 2 个单位的标量乘法时间[25],再对签名进行验证,又需要 2 个单位时间,共需要 4 个单位时间。而基于 CPK 的认证,查找公钥的运算时间可以忽略不计,然后签名验证需要 2 个单位时间,共只需要 2 个单位时间即可。综上,本方案 2 个单位时间即可完成验证,而证书模式需要 4 个单位时间,效率比证书模式高一倍,从而认证时延也较短。

3　结语

本文在车载 ECU 设备存储和计算资源受限、车载网络异构的条件下,针对要求时延极短,同时需要强认证和保密通信等安全需求,提出了一种基于 CPK 的车载网关动态密钥管理方案。该方案不需要公钥证书,即可安全分发节点私钥,并在私钥分发完成后,高效实现 ECU 节点的身份认证,且存储开销也较小。由于节点私钥在每次汽车点火时都会动态更新,有效防止了利用 OBD 接口的静态攻击。

参考文献:

[1] LING C L, FENG D Q. An algorithm for detection of malicious messages on CAN buses[C]//Proceedings of National Conference on Information Technology and Computer Science. Paris: Atlantis Press, 2012: 630-647.

[2] 韩正士, 秦贵和, 赵睿, 等. 车载 FlexRay 总线安全协议的设计与实现[J]. 西安交通大学学报, 2018, 52(12): 63-69.
HAN Z S, QIN G H, ZHAO R, et al. Design and implementation of security protocol for in-vehicle FlexRay buses [J]. Journal of Xi′an jiaotong university, 2018, 52(12): 63-69.

[3] 史宏宇. 基于 LIN 总线的标定系统的研究与设计[D]. 重庆: 重庆邮电大学, 2020.
SHI H Y. Research and design of calibration system based on LIN bus[D]. Chongqing: Chongqing University of Posts and Telecommunications, 2020.

[4] 王喜文.汽车信息安全问题不容忽视[J].汽车工业研究,2013(11):34-39.
WANG X W. The problem of automobile information security cannot be ignored[J]. Auto industry research, 2013(11):34-39.

[5] 闫鸿滨. 密钥管理关键技术研究[J]. 南通纺织职业技术学院学报, 2010, 10(4): 5-7.
YAN H B. Research on critical technology of key management[J]. Journal of Nantong textile vocational technology college, 2010, 10(4): 5-7.

[6] 舒浩敏. 基于 CAN 总线的车身控制系统设计[D]. 长沙: 湖南大学, 2012.
SHU H M. Car body control module design based on CAN bus[D]. Changsha: Hunan University, 2012.

[7] 刘旭. 基于车载以太网与 CAN 总线互联技术研究[D]. 天津: 河北工业大学, 2018.
LIU X. Research on the interconnection technology based on vehicle ethnernet and CAN bus[D]. Tianjin: Hebei University of Technology,2018.

[8] 吕孟恩, 韩晓明, 张鹏军. FlexRay-CAN 网关在火控系统中的应用[J]. 自动化与仪表, 2021, 36(3): 81-85, 94.
LV M E, HAN X M, ZHANG P J. Application of FlexRay-can bus in artillery system[J]. Automation & instrumentation, 2021, 36(3): 81-85, 94.

[9] WOLF M, WEIMERSKIRCH A, PAAR C. Secure in-vehicle communication[M]//LEMKE K, PAAR C, WOLF M. Embedded security in cars. Berlin: Springer Press, 2006: 95-109.

[10] PARK Y H. Key management and data re-encryption schemes for secure in-vehicle network[J]. Journal of intelligent & fuzzy systems, 2018, 35(6): 6079-6087.

[11] WOLF M, WEIMERSKIRCH A, PAAR C. Security in automotive bus systems[C]//Proceedings of the Workshop on Embedded Security in Cars. Berlin: Springer Press, 2004: 1-13.

[12] KURACHI R, MATSUBARA Y, TAKADA H, et al. CaCAN-centralized authentication system in CAN[C]// International Conference on Embedded Security in Cars. Berlin: Springer Press, 2014:1-10.

[13] CARVAJAL-ROCA I E, WANG J, DU J, et al. A semi-centralized dynamic key management framework for in-vehicle networks[J]. IEEE transactions on vehicular technology, 2021, 70(10): 10864-10879.

[14] 朱泉. PKI CA 身份认证技术研究[J]. 网络空间安全, 2016, 7(S1): 37-39.
ZHU Q. Researchof the PKI CA authentication technology [J]. Cyberspace security, 2016, 7(S1): 37-39.

[15] 南湘浩,陈化平,陈钟,等.组合公钥(CPK)体制标准(v3.0)[J].计算机安全,2009(11):1-2.
NAN X H, CHEN H P, CHEN Z, et al. Combined public key (CPK) system standard (v3.0) [J] Computer security,2009(11):1-2.

[16] 南湘浩. CPK 组合公钥体制(v7.0)[J]. 计算机安全, 2012(5): 2-4, 7.
NAN X H. CPK Combined public key system (v7.0) [J]. Computer security, 2012(5):2-4,7.

[17] 南湘浩. CPK 组合公钥体制(v8.0)[J]. 信息安全与通信保密, 2013, 11(3): 39-41, 44.
NAN X H. NAN X H. CPK Combined public key system (v8.0) [J]. Information security and communications privacy, 2013, 11(3): 39-41, 44.

[18] 张爱丽, 吴传伟. 一种基于 CPK 的无线传感器网络密钥管理方法[J]. 通信技术, 2019, 52(2): 439-443.
ZHANG A L, WU C W. Key management method for wireless sensor network based on CPK[J]. Communications technology, 2019, 52(2): 439-443.

[19] 陈亚茹, 陈庄, 齐锋. 一种基于 CPK 的远程认证方案

[J]. 信息安全研究, 2018, 4(11): 1034-1039.
CHEN Y R, CHEN Z, QI F. A remote authentication scheme based on CPK[J]. Journal of information security research, 2018, 4(11): 1034-1039.

[20] 胡景秀, 杨阳, 熊璐, 等. 国密算法分析与软件性能研究[J]. 信息网络安全, 2021, 21(10): 8-16.
HU J X, YANG Y, XIONG L, et al. SM algorithm analysis and software performance research[J]. Netinfo security, 2021, 21(10): 8-16.

[21] 廖国鸿, 袁宇恒, 黎伟杰, 等. 组合公钥体制的线性共谋攻击[J]. 计算机应用与软件, 2016, 33(12): 291-294.
LIAO G H, YUAN Y H, LI W J, et al. Linear collusion attack in combined public key cryptosystem[J]. Computer applications and software, 2016, 33(12): 291-294.

[22] 熊荣华, 李增欣, 杨恒亮, 等. 组合公钥(CPK)体制密钥间的线性关系[J]. 计算机安全, 2012(1): 30-33.
XIONG R H, LI Z X, YANG H L, et al. On the linear relations between the keys of combined public key cryptosystem(CPK)[J]. Computer security, 2012(1): 30-33.

[23] 马安君, 李方伟, 朱江. 组合公钥体制的线性共谋攻击分析[J]. 计算机应用, 2013, 33(8): 2225-2227.
MA A J, LI F W, ZHU J. Linear collusion attack analysis of combined public key cryptosystem[J]. Journal of computer applications, 2013, 33(8): 2225-2227.

[24] 张文政, 王立斌, 李益发. 安全协议设计与分析[M]. 北京: 国防工业出版社, 2015: 33-60.
ZHANG W Z, WANG L B, LI Y F. Design and analysis of security protocols[M]. Beijing: National Defense Industry Press, 2015: 33-60.

[25] 韩笑,施荣华. 一种高效的椭圆曲线数字签名方案[J]. 微计算机信息,2012,28(9):395-396.
HAN X,SHI R H. An efficient elliptic curve digital signature scheme [J]. Microcomputer information,2012,28(9):395-396.

(上接第17页)

[12] NAIK N, JENKINS P, SAVAGE N, et al. Fuzzy-import hashing: a malware analysis approach[C]//IEEE International Conference on Fuzzy Systems. Piscataway: IEEE Press, 2020: 1-8.

[13] SHIEL I, O'SHAUGHNESSY S. Improving file-level fuzzy hashes for malware variant classification[J]. Digital investigation, 2019, 28: S88-S94.

[14] DAMIANI E, DI VIMERCATI S D C, PARABOSCHI S, et al. An open digest-based technique for spam detection [C]//Proceedings of the ISCA 17th International Conference on Parallel and Distributed Computing Systems. New York: ACM Press, 2004, 559-564.