基于周期耦合处理的 CAN 总线数据组合加密方法

秦武韬[1]，王鹏[1]，李玉峰[1,2]
（1. 网络通信与安全紫金山实验室, 江苏 南京 211111；
2. 上海大学计算机工程与科学学院, 上海 200444）

摘 要：针对智能网联时代控制器局域网络（CAN）总线传输轻量化安全加密的需求，提出了一种响应快、安全性高的 CAN 总线数据加密方法，针对 64 位 CAN 报文周期性发送特点，设计与报文传输周期耦合的在线离线分组加密方案，离线段利用高级加密标准生成动态会话密钥，在线段则利用动态会话密钥快速响应报文的分组加解密请求。通过离线段的预加密计算大幅降低在线计算时延，实现低时延、轻量化；同时，基于 CAN 各车载单元属性，利用基于密文策略的属性加密方法对 CAN 报文的分组密码进行加密、分发，通过数据发送单元制定的访问控制策略确保仅目标单元可解密分组密码，实现针对性加密。

关键词：CAN 总线；在线离线；分组加密；低时延加密；网联汽车
中图分类号：TN918.8
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2023017

Combined encryption method for CAN bus data based on periodic coupled processing

QIN Wutao[1], WANG Peng[1], LI Yufeng[1,2]
1. Purple Mountain Laboratories, Nanjing 211111, China
2. School of Computer Engineering and Science, Shanghai University, Shanghai 200444, China

Abstract: In the intelligent connected age, CAN bus transmission faces the urgent demand of light weighted security encryption. Based on this, a fast response and high security CAN bus data encryption method was proposed. Since the 64 bit CAN packets were sent periodically, an online-offline block encryption algorithm coupled with message transmission cycle was proposed. In offline phase, the dynamic session key was generated by using advanced encryption standard. In online phase, the dynamic session key was used to quickly respond to encryption and decryption requests. The online computation delay was greatly reduced by the pre-encryption computation in offline phase, which helped achieving low latency and lightweight computation. At the same time, the ciphertext policy attribute based encryption was used to encrypt the block cipher. The access control policy made by the data sending OBU ensures that only the target OBU can decrypt the block cipher, so as to achieve targeted encryption.

Keywords: CAN bus, online-offline, block encryption, low latency encryption, connected vehicle

0 引言

随着新一轮科技革命的蓬勃发展，网络通信技术、深度学习技术、计算机技术等不断进步，并与传统汽车技术相结合，使智能网联汽车快速发展，大量网联汽车逐渐步入人们的日常生活中[1-2]。智能

收稿日期：2022−09−30；**修回日期：**2022−12−01
通信作者：王鹏，15803846349@163.com
基金项目：国家自然科学基金资助项目（No.61702547）；河南省重大科技专项资金资助项目（No.221100240100）
Foundation Items: The National Natural Science Foundation of China (No.61702547), Henan Science and Technology Major Project (No.221100240100)

网联汽车在带来巨大便利的同时，导致针对汽车的各种攻击入口被打开，用户、车辆、环境等海量隐私或敏感信息存在被非法窃取的巨大风险，不仅带来了巨大的网络安全问题，也使传统的功能安全问题与网络安全问题相互交织，引发复杂的广义功能安全问题[3-5]。

车内通信安全是汽车广义安全的重要组成部分，一旦通信安全受到威胁，轻则导致隐私泄露、财产损失，重则导致汽车故障、车辆恶意被控，引发行车安全及其他恶性事件[6]。在车内通信网络中，控制器局域网络（CAN）总线凭借简单、轻量化、可靠性好、布线灵活、成本低等优势，一直是车内通信网络的主力军，连接着动力域、车身域等车内各个域（如图 1 所示），承担着绝大多数的通信任务，特别是包含位置、速度、转向、发动机转速等有关行车安全的信息[7]。

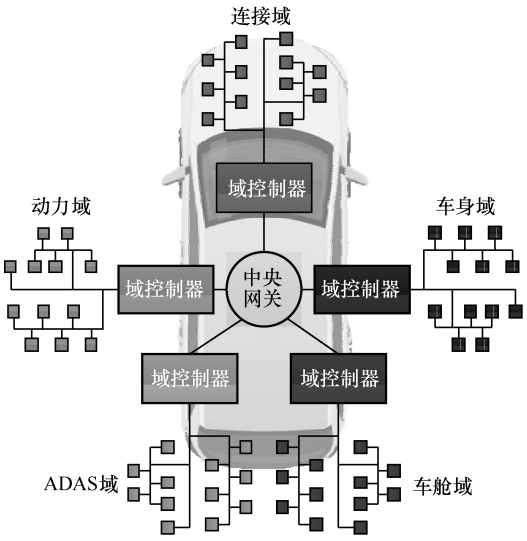

图 1 车内 CAN 架构

然而，基于 CAN 总线的通信是一种广播形式的网络通信，出于轻量化和快速响应的考虑，CAN 总线在设计阶段没有应用加密技术，因此通过一些手段可以轻易地获取总线上传输的真实信息，不仅导致车内各类数据极易泄露，而且攻击者可以利用这些信息对网络上的其他单元进行攻击，严重危害车辆安全[8]。因此，在智能网联化的今天，必须对 CAN 传输的数据进行加密处理。

智能网联汽车的信息传输和车辆的安全控制要求车内数据传输必须具有低时延的特点，而 CAN 总线本身的数据传输能力相对较弱，且具有固定的数据格式，每个标准帧所能传输的数据固定为 8 字节（64 位），这就要求在对 CAN 数据进行加密时需采用快速、轻量化的分组加密方法，加密前后数据长度不变，不增加 CAN 总线的传输负担，不改变原有数据的传输节奏和格式。

此外，CAN 总线的广播形式使一个车载单元（OBU, on board unit）被攻破俘获，则所有经 CAN 总线传输的数据均会泄露。如果简单采用同样的分组对称密码进行加密，将使所有经 CAN 总线传输的数据面临“全军覆没”的巨大风险。如果各 OBU 两两之间分配密钥，尽管可以确保数据传输的保密性，但会带来大量的密钥，如果同一数据需要发送至 n 个 OBU，则需要重复加密、传输 n 次，带来了极大的计算量和沉重的总线传输负担，这在当前 CAN 总线传输负载率已经较高的情况下并不现实，将显著增加传输时延，危害行车安全。

因此，需要设计一种轻量化、低时延的加密策略，在不显著增加计算量、数据传输量的情况下确保 CAN 总线传输的密文仅能被数据发送的目标单元解密，即同时满足以下 3 个特点。1) 轻量化、低时延，确保高效加解密；2) 报文数据 64 bit 分组加密，不改变原有传输节奏和格式；3) 针对性地加解密，非目标数据用户无法得到明文信息。

在现有的 CAN 数据加密方法中，1977 年由美国政府颁布的数据加密标准（DES, data encryption standard）具有典型代表性[9]，DES 为 64 bit 分组对称加密，分组位数与 CAN 标准帧中的数据长度（如图 2 所示）一致，应用简单方便、适用性强，但随着现代计算能力的提升存在着暴力破解的风险；而基于 DES 的改进算法 3DES 通过多次加解密运算提升了安全性[10]，但加密的计算量大幅增加，加密时间是 DES 算法的 3 倍多。因此，美国政府颁布了高级加密标准（AES, advanced encryption standard）用于取代 DES[11-12]，AES 算法由于其出色的安全性和较小的计算量，已经成为主流的对称加密算法，但其要求明文长度至少达到 128 bit，超过了 CAN 数据帧的 64 bit，无法直接应用。一种典型解决方法是利用 64 bit 空白报文补位至 128 bit，再利用 AES 进行加密处理，生成 128 bit 的密文后连续发送两帧，接收方则连续接收两帧后再进行解密，但该方法明显存在着加解密计算量和总线数据传输量翻倍的问题[13]；另一种方法则是通过累积两帧数据帧

补位至 128 bit，再利用 AES 进行加解密，但该方法的奇数拍报文必须等待偶数拍报文配对后才能发送，增加了奇数拍报文的等待时间，带来了时延的不确定性。

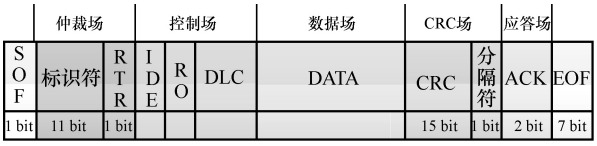

图 2　标准帧数据格式

此外，现有的 CAN 数据加密算法直接对明文数据进行处理，在明文出现之前不进行预加解密计算，所有计算累积到加密或解密请求出现后，未能充分利用离线段的计算能力，增大了在线段的运算负担和加解密时延。同时，现有的 CAN 总线数据加密方法仍采用简单的对称密码设计思路，各 OBU 通过预设相同的密码来实现数据的加解密，增加了数据泄露的风险，无法满足 CAN 总线传输中针对性加解密的需求。

因此，本文面向 CAN 报文加解密快速响应需求，利用 CAN 总线周期性传输特点，提出一种基于在线–离线处理的组合加密方法，如图 3 所示。首先，利用 OBU 的身份属性制定访问策略对分组密码进行加密、分发，确保仅有目标 OBU 可以完成密码解密，获取分组密码。然后，对 CAN 报文加解密方法进行在线离线处理改造，其中，在离线阶段利用 AES 算法动态生成 8 字节会话密钥，在线段则利用会话密钥通过异或运算迅速响应数据的加解密需求，实现高速、轻量化、64 位分组和针对性加解密，同时满足智能网联汽车 CAN 报文加解密的 3 个需求。

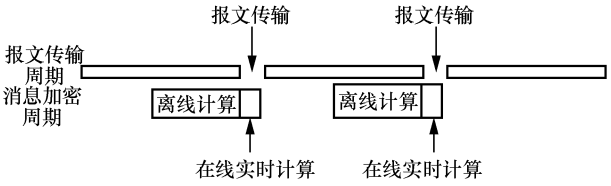

图 3　与周期耦合的在线离线加解密模式

1　AES 算法

AES 加解密流程如图 4 所示。从图 4 中可以看出，其核心运算主要包括轮密钥加、字节代换（逆字节代换）、密钥扩展、行移位（逆行移位）、列混合（逆列混合）5 种，具体方法介绍如下。

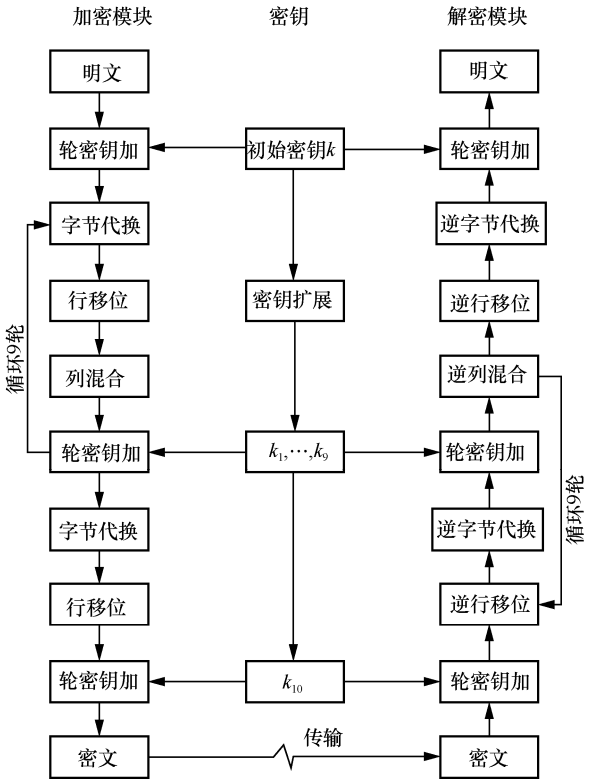

图 4　AES 加解密流程

1) 轮密钥加。如图 5 所示，将数据逐个与本轮相应密钥进行异或运算。其中，m 为待运算数据，k 为本轮密钥，c 为异或运算结果。

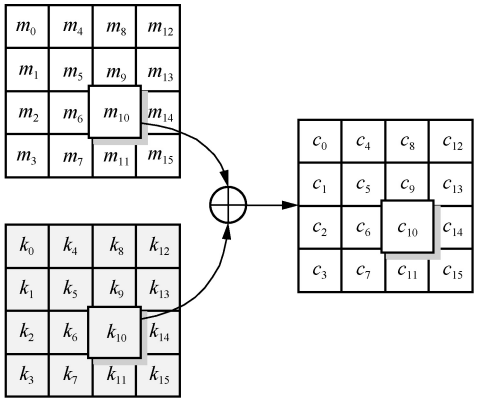

图 5　轮密钥加

2) 字节代换（逆字节代换）。把轮密钥加后产生的每一个字节用十六进制表示，然后以十六进制的第一个数字为行，第二个数字为列，在 S 盒[14]表中查找对应的数字代替原先的数字，完成字节代换。逆字节代换则从逆 S 盒中查找元素替代。

3) 密钥扩展。基于 16 字节原始密钥，按顺序以每 4 字节为一组，按位进行依次连接，获得第一轮密钥 $W[0]$、$W[1]$、$W[2]$、$W[3]$。对于后续轮密钥，

采用如图 6 所示的方法进行计算，即

$$\begin{cases} W[i]=W[i-4]\oplus W[i-1], \mathrm{mod}(i,4)\neq 0 \\ W[i]=W[i-4]\oplus \mathcal{T}\left(W[i-1]\right), \mathrm{mod}(i,4)=0 \end{cases} \tag{1}$$

其中，$\mathcal{T}(\cdot)$ 为包括字循环移位、字节替换和轮常量异或运算的非线性函数[11]。

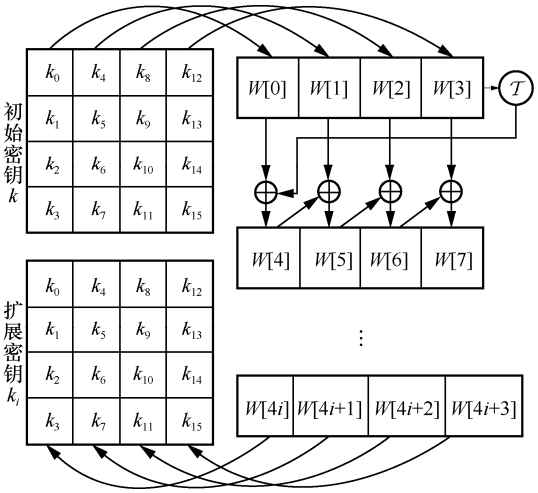

图 6　密钥扩展

4) 行移位（逆行移位）。把字节代换得到的矩阵逐行进行左环移，逆行移位则与行移位相反。

5) 列混合（逆列混合）。利用给定矩阵对上一步获得的矩阵进行变换，其中，列混合为

$$\begin{bmatrix} b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 02 & 01 & 01 \end{bmatrix} \begin{bmatrix} a_0 & a_4 & a_8 & a_{12} \\ a_1 & a_5 & a_9 & a_{13} \\ a_2 & a_6 & a_{10} & a_{14} \\ a_3 & a_7 & a_{11} & a_{15} \end{bmatrix}$$

逆列混合为

$$\begin{bmatrix} b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \end{bmatrix} = \begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix} \begin{bmatrix} a_0 & a_4 & a_8 & a_{12} \\ a_1 & a_5 & a_9 & a_{13} \\ a_2 & a_6 & a_{10} & a_{14} \\ a_3 & a_7 & a_{11} & a_{15} \end{bmatrix}$$

2　在线离线处理的组合加密方案

针对车内 CAN 网络数据加密 64 位分组、轻量化、低时延、针对性解密的需求，本文提出一种与 CAN 总线通信周期耦合的组合加密方案，具体流程如图 7 所示。

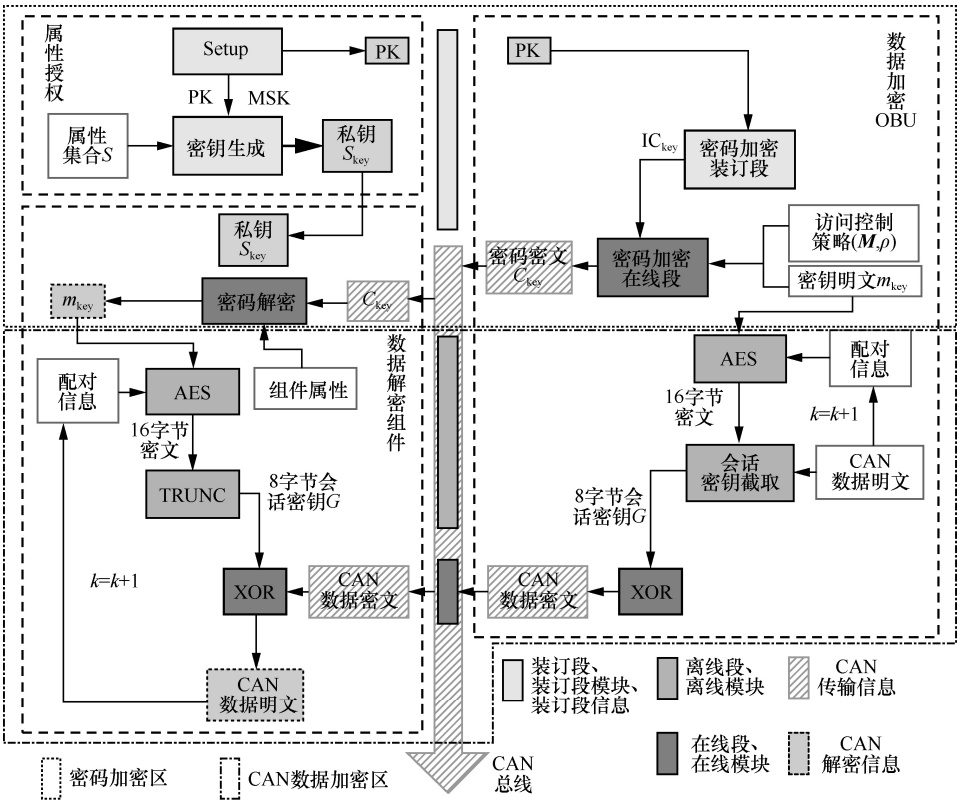

图 7　在线离线处理的组合加密流程

组合加密方案由两部分组成，一部分为基于属性的分组密码加密方法，确保用于 CAN 报文加密的分组密码仅由目标数据用户获得，防止加密信息扩散，避免某一单元被攻破后全车信息泄露。

另一部分为基于分组加密方法的 CAN 报文数据加密，该方法利用 AES 算法动态生成 8 字节会话密钥，实现分组对称加密，密文与明文长度不变，实现了数据传输节奏和格式的稳定。

此外，在加解密过程中，使用了在线离线处理技术，将计算量大、不依赖实时报文信息的计算放入通信间歇的离线段进行，可大幅度降低计算时延。本文方案具体内容介绍如下。

2.1　基于身份属性的分组密码加密

该方法首先根据确定的报文收发 OBU 确定收发组，在本收发组第一帧 CAN 报文发送前，利用基于身份属性加密方案对分组密码 m_{key} 进行加密，确保仅有目标数据用户可完成解密获得分组密码 m_{key}，确保后续报文的安全。具体步骤介绍如下。

1) Ex.SysAtt()：收集汽车各 OBU 的属性，包括所属域、单元类型、种类、编号等，如自动驾驶域、传感器、相机、1，确定系统属性集 $U=\{u_1,u_2,\cdots,u_u\}$。

2) Ex.Setup(τ, U)：进行设置，输入安全选取的隐含安全参数 τ 与各 OBU 单元属性集合 U，计算公钥 PK 和主私钥 MSK

$$\text{PK}=\left\langle \begin{matrix} p_1=g,\ p_2=e(g,g)^a, \\ p_3=g^b,\ p_4=\{\gamma_1,\gamma_2,\cdots,\gamma_u\} \end{matrix} \right\rangle$$

$$\text{MSK}=g^a$$

其中，g 为 G_1 的生成元，G_1 为双线性映射概念下的循环群，其元素包括 $\gamma_1,\gamma_2,\cdots,\gamma_u$，相关概念可参考文献[15]，随机参数 $a,b\in Z_p$。

3) Ex.KeyGen(MSK, PK, S)：根据各 OBU 属性，利用主私钥 MSK 和公钥 PK 生成相应私钥，预设至各组件中，对于第 k 个组件，其私钥为

$$S_{\text{key}}=\left\langle K=g^a g^{bt},\ L=g^t,\ K_i=\gamma_{\varsigma(i)}^t,\ i=1,2,\cdots,s \right\rangle$$

其中，$1,2,\cdots,s$ 表示 OBU 属性集 S 中的属性标号，L 表示私钥的组成参数，用于后续解密，$\varsigma(i)$ 表示第 k 个 OBU 的属性到系统属性集 U 中元素的映射，随机参数 $t\in Z_p$。

以上三步均在系统联网实验前完成，确保各私钥安全装订。

4) Offline.EncryptKey(PK)：在离线段，数据发送 OBU 选择随机数 $r\in Z_p$，利用公钥 PK 计算中间密文 IC_{key}。

$$\text{IC}_{\text{key}}=\left\langle \tilde{C}=g^r \right\rangle \tag{2}$$

5) Online.EncryptKey(PK, IC_{key}, m_{key}, $(\boldsymbol{M},\rho)$, v)：此时已经确定密钥明文 m_{key} 和访问控制策略 $(\boldsymbol{M},\rho)$，利用中间结果完成加密，输出密文 C_{key}。

$$C_{\text{key}}=\left\langle C=m_{\text{key}}p_2^r,\tilde{C}=g^r,\left\{C_i=p_3^{\lambda_i}\gamma_{\rho(i)}^{-r_i},D_i=g^{r_i}\right\}_{i\in[1,l]} \right\rangle \tag{3}$$

其中，$\boldsymbol{M}$ 为根据访问结构生成的访问矩阵[16]，$\{r_1,r_2,\cdots,r_l\}\in Z_p$ 为随机数，l 为 $\boldsymbol{M}$ 的行数；函数 $\rho(\cdot)$ 表示访问矩阵行序列到属性集属性标号的映射，即 $\{1,2,\cdots,l\}\to\{1,2,\cdots,u\}$；$\lambda_i=\boldsymbol{v}\boldsymbol{M}_i^{\mathrm{T}}$，$\boldsymbol{M}_i^{\mathrm{T}}$ 表示 $\boldsymbol{M}$ 第 i 行的转置，随机向量 $\boldsymbol{v}=(r,k_2,k_3,\cdots,k_q)\in Z_p^q$，$q$ 表示 $\boldsymbol{M}$ 的列数。

6) DecryptKey(S_{key}, C_{key})：数据用户运行该算法，利用密文 C_{key} 和私钥 S_{key}，输出密钥明文 m_{key}。

由式(3)，有 $m_{\text{key}}=\dfrac{C}{p_2^r}$。在解密时，$p_2^r$ 的计算方法为

$$p_2^r=\frac{e(g,g)^{ar}e(g,g)^{rbt}}{\prod_{i\in I}e(g,g)^{bt\lambda_i w_i}}=\frac{e(\tilde{C},K)}{\prod_{i\in I}\left(e(C_i,L)e\left(D_i,K_{\rho(i)}\right)\right)^{w_i}}$$

因此，密钥明文 m_{key} 为

$$m_{\text{key}}=\frac{C\prod_{i\in \text{I}}\left(e(C_i,L)e\left(D_i,K_{\rho(i)}\right)\right)^{w_i}}{e(\tilde{C},K)} \tag{4}$$

其中，$I=\{i:\rho(i)\in\boldsymbol{S}\}$ 为索引集，w_i 为向量 $\boldsymbol{W}$ 的第 i 个元素 $(i\in I)$，满足 $\sum_{i\in I}w_i\boldsymbol{M}_i=(1,0,0,\cdots,0)$。

2.2　基于在线离线 AES 的 CAN 报文分组加密

针对传统分组对称加密方法加密安全性不足、最小加密长度与 CAN 数据长度不匹配、缺乏在线离线处理导致在线段计算负担过重等问题，本节给出一种基于在线离线 AES（OOAES, online-offline AES）的 CAN 报文分组加密方法，具体流程如图 8 所示。该方法在离线阶段利用 128 位 AES 分组密码对由计数器和上一帧明文信息构成的配对信息进行预加密，通过截取 8 字节密文生成动态会话密钥，等待加密请求；在线段则利用动态会话密钥通过异或运算对 8 字节的 CAN 数据进行加密，生成 8 字节密文通过 CAN 网络进行传输。

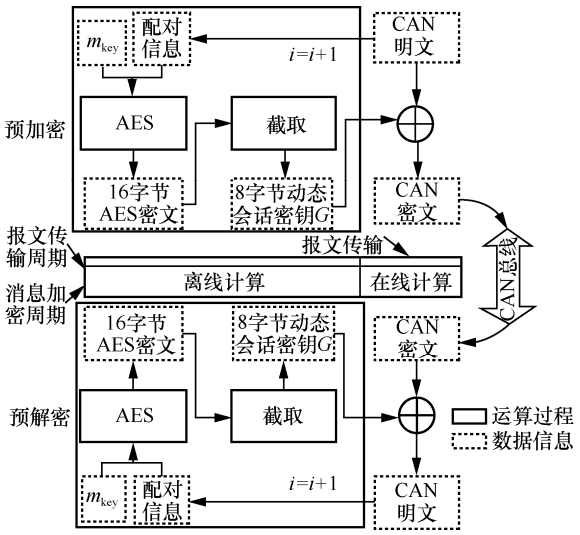

图 8　加解密处理流程

图 8 中，m_{key} 是长度为 16 字节的 AES 分组密码，由数据加密方自定义；配对信息是长度为 16 字节的明文信息，由 8 字节的循环计数器和上一数据帧 CAN 数据的明文消息构成，对于初始帧则采用事先约定的消息，如{00 00 00 00 00 00 00 00}。

利用 AES 对 16 字节配对信息进行加密处理后，获得 16 字节长度的 AES 密文。在 CAN 标准数据帧中，数据长度为 8 字节，因此可从 16 字节的密文中截取 8 字节构成动态会话密钥 G，利用 8 字节的会话密钥 G 与 CAN 明文进行异或加密运算获得 8 字节的 CAN 密文进行传输。解密流程与加密流程相似，区别在于解密流程利用动态会话密钥与经 CAN 总线传输的密文进行异或解密运算，获得明文完成解密。

在 CAN 报文的加解密过程中，充分设计了在线离线的处理方法。对于加密过程，系统启动后，首先在离线阶段完成预加密计算，获得加密会话密钥 G；当 CAN 明文生成并触发加密请求时，进入在线段，此时利用 G 对明文进行快速加密，生成密文数据并发送；加密过程随后进入离线阶段，更新配对信息并进行预加密，生成新的会话密钥等待 CAN 报文数据。解密过程与加密过程类似，系统启动后，首先在离线阶段完成预解密计算，获得解密会话密钥 G；当接收到 CAN 密文数据时，进入在线段，运行异或运算恢复明文数据；完成解密后进入离线阶段，更新配对信息进行预解密，生成新的解密会话密钥等待 CAN 密文数据。

通过在线–离线加解密处理方法的运用，显著减少了在线段的运算量，节约了运算时间，将巨大的预加密计算工作前置到了计算资源相对空闲的离线阶段，确保了在线段能快速响应加密和解密请求，大幅降低了加解密带来的时延。

3　实验仿真分析

3.1　安全通信验证

为了验证加解密的正确性，生成 1 000 帧描述汽车速度变化的 CAN 报文，对比数据非加密传输和使用本文提出的 CAN 报文加密方法进行加密传输的结果，分别如图 9 和图 10 所示。

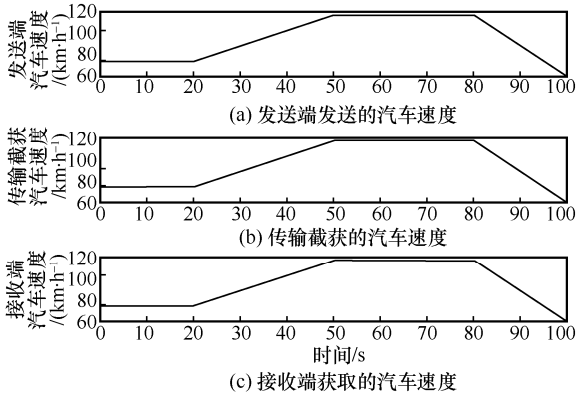

图 9　非加密网络数据

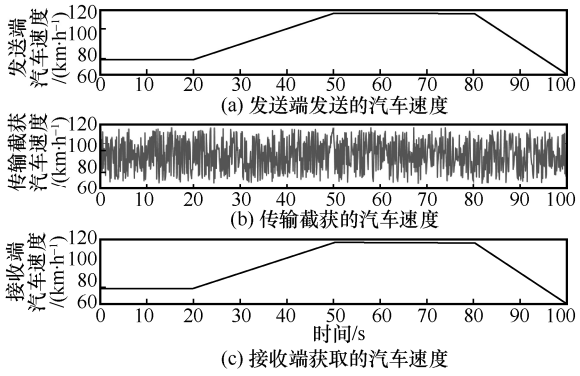

图 10　加密网络数据

从图 9 和图 10 中可以看出，对于未采用加密处理的 CAN 报文传输方法，可以轻易从网络端窃取汽车真实的速度数据，不具备传输的安全性；而采用加密处理后的数据呈现出类似于高斯噪声的不规则变化，趋势、结果与真实数据明显不同。接收端获取的结果与发送端一致，证明本文所提加密方法可以有效准确地对 CAN 数据进行加解密，确保了 CAN 网络传输数据的安全性。

3.2　雪崩测试

雪崩效应是指明文或密钥发生微小变化时，密

文会出现不可区分的改变，理想情况是每个二进制位有 50%的概率发生翻转。本节将分别进行密钥雪崩效应测试和密文雪崩效应测试，其中，密钥雪崩效应测试中将 128 位密钥的最后一位翻转，观测密钥翻转前后 1 000 帧 CAN 密文二进制位的翻转概率；密文雪崩效应测试中将 CAN 报文中速度数据的最后一位翻转，观测翻转前后 1 000 帧密文的翻转概率。图 11 给出了 1 000 帧报文的雪崩率曲线，图 12 给出了密钥雪崩率和密文雪崩率统计，表 1 给出了雪崩效应特性的测试统计结果。图 12 中，横坐标表示组别，组 1 为密钥调整带来的雪崩率，称为“密钥–雪崩率”，组 2 为明文调整带来的雪崩率，称为“明文–雪崩率”。从图 12 中可以看出，本文方法具有优异的雪崩特性效应，密文二进制翻转概率约为 50%，达到了某一位微小的输入变化使输出发生不可区分改变的效果。

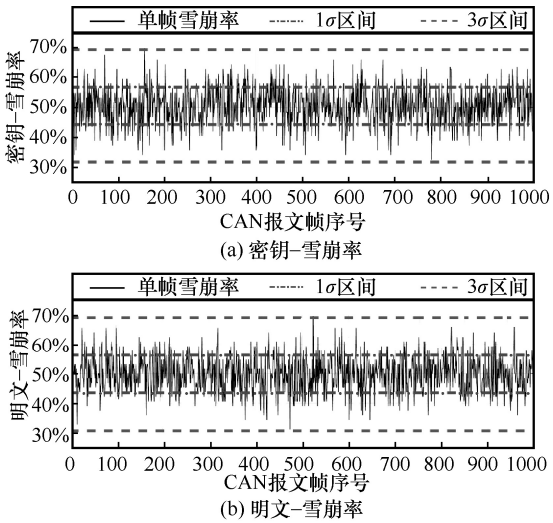

图 11　1 000 帧报文雪崩率

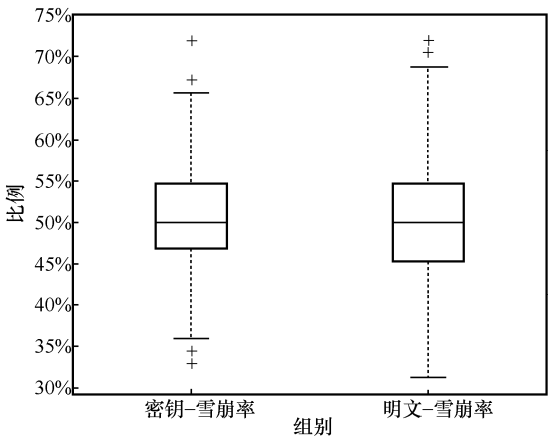

图 12　密钥雪崩率和密文雪崩率统计

表 1　　**雪崩效应特性测试结果**

统计项		密钥调整一位	明文调整一位
平均雪崩率		50.48%	49.88%
雪崩率 1σ 值		6.14%	6.40%
雪崩率 3σ 上下限		[32.06%, 68.90%]	[30.67%, 69.09%]
某帧密文	调整前	F1 5F EC A9 E8 D1 06 1F	F1 5F EC A9 E8 D1 06 1F
	调整后	CF 98 A7 1E B0 93 EF 52	FD 43 83 AF CF F2 F3 D5

3.3　加解密耗时分析

基于 3.1 节生成的 1 000 帧 CAN 报文数据，分别利用 DES、3DES、AES 和 OOAES 在一台搭载 i5-9400 @2.9 GHz 处理器的 windows 10 机器上进行 500 次蒙特卡罗仿真实验，编程语言为 C++11，统计加解密总耗时和明文出现后的在线段耗时。其中，加密时长定义为加密运算阶段耗时，即各个加密运算步骤耗时之和；解密时长定义为解密运算阶段耗时，即各个解密运算步骤耗时之和；在线运行时长等于加密在线运行时长和解密在线运行时长之和，表示明文出现后转换为密文的时间和密文出现后转换为明文的时间。在实验中，利用 C++ chrono 库中的 steady_clock 函数统计 1 000 次加解密的耗时之和，以减少单次统计的不必要误差。

在仿真结果中，图 13 和图 14 分别给出了总耗时和在线段耗时对比，表 2 给出了各阶段耗时的平均统计结果。从图 13、图 14 和表 2 可以看出，本文提出的 OOAES 具有良好的全程计算效率和极其优异的在线段计算效率，主要体现在以下两点。

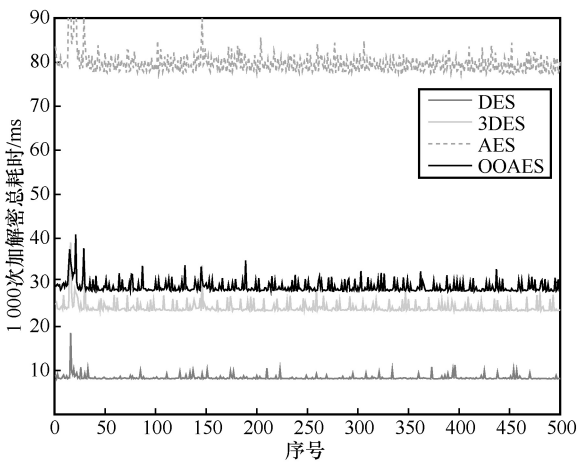

图 13　1 000 帧报文加解密总耗时对比

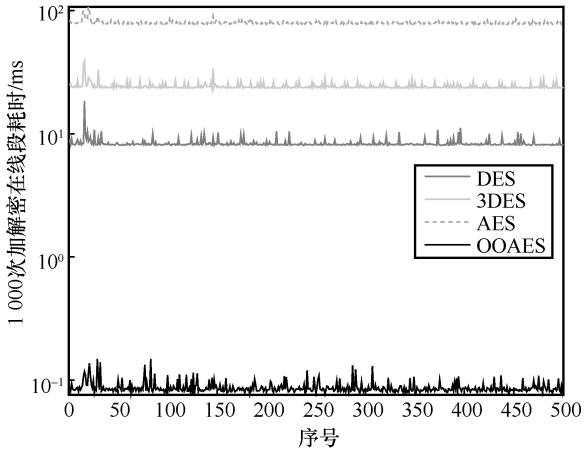

图 14　1 000 帧报文加解密在线段耗时对比

表 2　1 000 帧 CAN 报文加解密各阶段耗时的平均统计结果

统计项	DES	3DES	AES	OOAES
总耗时/ms	8.329	24.306	79.416	28.730
加密耗时/ms	4.002	11.982	14.009	14.334
解密耗时/ms	4.008	11.969	65.067	14.085
在线段运行耗时/ms	8.329	24.306	79.416	0.0853

1) OOAES 的加解密总耗时远小于常规 AES 算法。OOAES 的加密部分与常规 AES 基本一致，该部分单帧耗时大致相同，约为 14 μs，但 AES 的解密部分运算量很大，单帧耗时达到 65 μs。OOAES 绕过 AES 的解密模块，仍然利用加密方法生成解密所采用的动态会话密钥，大大降低了解密计算量，单帧解密耗时仅 14 μs，获得了更优异的加解密总耗时成绩。

2) OOAES 的在线段耗时呈指数级降低。常规的 DES、3DES、AES 等方法直接对明文（密文）进行加密（解密）处理，在未获取明文（密文）前的离线段缺乏预加密工作，导致所有加解密计算累积到加解密需求出现后，使在线段的计算负担巨大，增加了 CAN 报文数据产生到解密段的时延。从测试结果看，DES、3DES 和 AES 的在线段单帧计算耗时分别达到了 8.3 μs、24.3 μs 和 79.4 μs，而采用了在线–离线处理技术的 OOAES 方法将大量计算前移至离线段，在线段仅利用动态会话密钥进行异或加解密运算，计算量指数级减小，每千帧在线段耗时仅为 85 μs，单帧耗时为 0.085 μs，领先 DES 和 AES 2~3 个数量级，单帧 CAN 报文加密接近零时延，可以做到“即请求，即加（解）密”。

3.4　不同消息周期下车载芯片资源占用分析

为了进一步验证本文提出的方法在车载系统的可行性和有效性，利用一款搭载 Arm Cortex-A53 max @1.2 GHz 的车载旭日 X3 芯片进行不同消息周期 CAN 报文的加解密分析。

基于上述软硬件条件，进行 1 000 组不同 CAN 消息周期的仿真实验，每组仿真所采用的数据均为 1 000 帧 8 字节 CAN 报文信息，消息周期根据文献[17]给出的统计规律随机采样，确保小于 10 ms 周期的实验组数占比约为 41%，10~20 ms 周期的实验组数占比约为 31%。单帧 CAN 报文加解密平均计算耗时分布如表 3 所示。

表 3　单帧 CAN 报文加解密平均计算耗时分布

统计项	数量/组
<0.5 ms	60
0.55~0.65 ms	240
0.65~0.7 ms	117
0.7~0.75 ms	583
>0.75 ms	0

图 15 给出了单帧加解密平均耗时分布。从图 15 可以看出，相较于运算能力更强的 Intel i5 芯片，基于车载旭日 X3 芯片的加解密计算耗时有所增加，但单帧数据的加解密平均耗时仍然不超过 0.75 ms（图 15 中超过 0.75 ms 的平均耗时占比为 0），显著小于 CAN 消息周期，具有良好的可行性。为了进一步分析 CPU 计算资源占用情况，实验中同步统计了加解密过程中的 CPU 占用率。

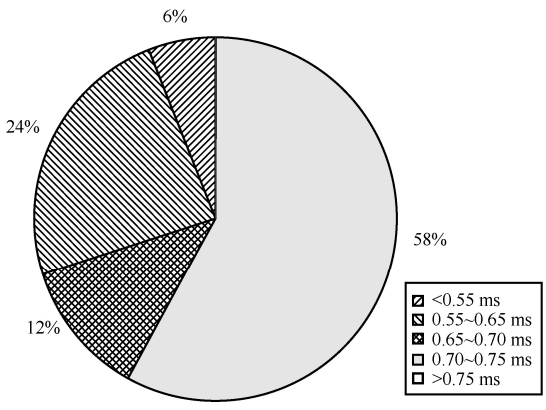

图 15　单帧加解密平均耗时分布

图 16 给出了不同消息周期下 CPU 利用率的情况。从图 16 可以看出，消息周期越长，CPU 利用率

越低；消息周期越短，CPU 利用率越高。这是因为一定时间内，加解密的计算负担随着消息收发频率的增加而增加。尽管如此，从图 17 可以看出，CPU 利用率超过 4%的情况很少，占比不超过 1%，事实上，在本次仿真中也仅出现一次，利用率为 4.027 5%，这说明本文提出的 OOAES 计算资源占用有限，对其他应用的影响不大。

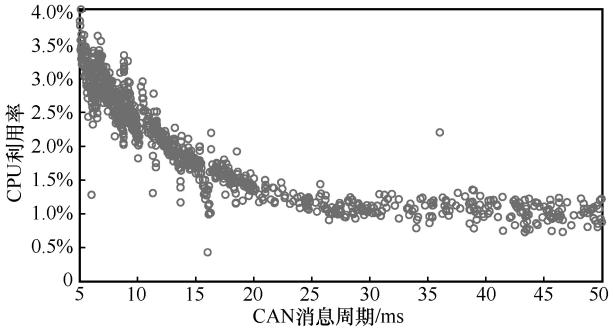

图 16　不同消息周期下 CPU 利用率的情况

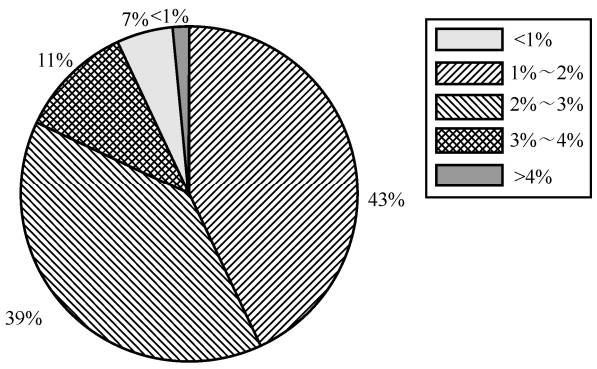

图 17　CPU 利用率分布

4　结束语

根据车内 CAN 总线对数据加密低时延、轻量化、分组、针对性保密的需求，设计了基于在线离线处理的组合加密方法。该方法首先利用身份属性对分组密码进行加密分发，确保仅数据目标 OBU 可以完成密码解密，避免单一 OBU 攻破后全车信息泄露的风险。基于在线离线处理框架设计基于 AES 的 CAN 报文分组加密方法，巧妙地利用离线段进行预加密计算，生成 8 字节动态会话密钥，不仅解决 AES 最小加密长度与 CAN 报文长度不匹配的问题，更实现量级地降低在线段加（解）密时长，具备报文数据“即请求、即加（解）密”的能力。

参考文献：

[1] YANG D G, JIANG K, ZHAO D, et al. Intelligent and connected vehicles: current status and future perspectives[J]. Science China Technological Sciences, 2018, 61(10): 1446-1471.

[2] 邬贺铨. 5G 赋能智能网联汽车[J]. 智能网联汽车, 2019(1): 75-76.
WU H Q. 5G enables intelligent connected vehicle[J]. Intelligent Connected Vehicles, 2019(1): 75-76.

[3] 吴武飞, 李仁发, 曾刚, 等. 智能网联车网络安全研究综述[J]. 通信学报, 2020, 41(6): 161-174.
WU W F, LI R F, ZENG G, et al. Survey of the intelligent and connected vehicle cybersecurity[J]. Journal on Communications, 2020, 41(6): 161-174.

[4] WANG H R, WANG Q D, CHEN W W, et al. A novel path tracking approach considering safety of the intended functionality for autonomous vehicles[J]. Journal of Automobile Engineering, 2022, 236(4): 738-752.

[5] 邬江兴. 工业控制网络广义功能安全问题与解决之道[J]. 信息安全研究, 2022, 8(6): 524-527.
WU J X. Generalized functional safety problems and solutions in industry control network[J]. Journal of Information Security Research, 2022, 8(6): 524-527.

[6] CHEN W, CAI S W. Ad hoc peer-to-peer network architecture for vehicle safety communications[J]. IEEE Communications Magazine, 2005, 43(4): 100-107.

[7] LIMBASIYA T, DAS D. VCom: secure and efficient vehicle-to-vehicle message communication protocol[J]. IEEE Transactions on Network and Service Management, 2021, 18(2): 2365-2376.

[8] ZHANG Y N, LIU T Y, ZHAO H, et al. Risk analysis of CAN bus and Ethernet communication security for intelligent connected vehicles[C]//Proceedings of 2021 IEEE International Conference on Artificial Intelligence and Industrial Design. Piscataway: IEEE Press, 2021: 291-295.

[9] DIFFIA W, HELLAMN, MARTIN, E. Exhaustive cryptanalysis of the NBS data encryption standard[J]. Computer, 1977, 10(6): 74-84.

[10] COPPERSMITH D, JOHNSON D B, MATYAS S M. A proposed mode for triple-DES encryption[J]. IBM Journal of Research and Development, 1996, 40(2): 253-262.

[11] BERTONI G, BREVEGLIERI L, KOREN I, et al. Error analysis and detection procedures for a hardware implementation of the advanced encryption standard[J]. IEEE Transactions on Computers, 2003, 52(4): 492-505.

[12] 曹春杰, 程大果, 王隆娟, 等. 基于 AES 加密算法和轻量级 ROV 的水质监测系统[J]. 通信学报, 2018, 39(S2): 204-212.
CAO C J, CHENG D G, WANG L J, et al. Water quality monitoring

system based on AES encryption algorithm and lightweight ROV[J]. Journal on Communications, 2018, 39(S2): 204-212.

[13] 朱嘉桦. 基于 AES 算法的 CAN 总线加密认证通信 IP 核设计与实现[D]. 西安: 西安电子科技大学, 2021.
ZHU J H. Design and implementation of CAN bus encrypted authentication communication IP based on AES algorithm[D]. Xi'an: Xidian University, 2021.

[14] MOZAFFARI-KERMANI M, REYHANI-MASOLEH A. A low-cost S-box for the advanced encryption standard using normal basis[C]//Proceedings of 2009 IEEE International Conference on Electro/Information Technology. Piscataway: IEEE Press, 2009: 52-55.

[15] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//Proceedings of 2007 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2007: 321-334.

[16] LIU Z, CAO Z. On efficiently transferring the linear secret-sharing scheme matrix in ciphertext-policy attribute-based encryption[J]. The International Association for Cryptologic Research Cryptology ePrint Archive, 2010, 2010: 374-401.

[17] XIE Y, ZENG G, KURACHI R, et al. Balancing bandwidth utilization and interrupts: two heuristic algorithms for the optimized design of automotive CPS[J]. IEEE Transactions on Industrial Informatics, 2020, 16(4): 2382-2392.

[作者简介]

秦武韬（1993– ），男，安徽淮北人，博士，网络通信与安全紫金山实验室助理研究员，主要研究方向为多源信息融合、智能网联汽车纵深安全防护等。

王鹏（1985– ），男，河南周口人，博士，网络通信与安全紫金山实验室副教授，主要研究方向为智能网联系统安全、网络空间安全等。

李玉峰（1975– ），男，山东烟台人，博士，上海大学教授、博士生导师，主要研究方向为通信与信息系统、网络安全、物理信息系统广义功能安全等。