文章编号:1671-4598(2024)08-0153-08 DOI:10.16526/j.cnki.11-4762/tp.2024.08.022 中图分类号:TP13 文献标识码:A

Paillier 同态加密下车辆协同自适应预测巡航控制

杨敏艺，宋秀兰，杨燕玲，柴伟豪
（浙江工业大学 信息工程学院，杭州 310014）

摘要：车辆协同式自适应巡航控制（CACC）以其高效便捷的特点成为智能交通系统的研究热点，但随着车辆接入网络，网络攻击对车联网系统的安全性造成了很大威胁；针对传统方案较繁琐、密文密钥同时传输数据仍可能被篡改的问题，采用 Paillier 同态加密算法对加速度进行加密，仅传输密文；针对控制目标设计一综合跟踪信号，并基于 Paillier 算法的同态性设计密文数乘运算，使加速度密文无须解密而直接用于自车构建跟踪信号；将跟踪信号与分布式模型预测控制（MPC）结合，采用线性矩阵不等式对控制策略的优化问题进行转化，求解最优控制输入，保证车辆队列的安全协同行驶；经 Matlab 仿真验证了控制系统的性能指标以及 Paillier 同态加密的有效性。

关键词：Paillier 同态加密；网络安全；协同自适应巡航控制；线性矩阵不等式；模型预测控制

Cooperative Adaptive Predictive Cruise Control for Vehicles with Paillier Homomorphic Encryption

YANG Minyi, SONG Xiulan, YANG Yanling, CHAI Weihao
(College of Information Engineering, Zhejiang University of Technology, Hangzhou 310014, China)

Abstract: Vehicle cooperative adaptive cruise control (CACC) has become a research hotspot for intelligent transportation systems with its efficient and convenient features, but with the access of vehicles to networks, cyber attacks cause a significant threat to the security of connected vehicle systems. To address the problems of complex traditional scheme ciphertext key to be simultaneously changed during transmitting data, the Paillier homomorphic encryption algorithm is used to encrypt the acceleration, only transmitting the ciphertext. To achieve the control object, this paper designs an integrated tracking signal and ciphertext multiplication operation based on the homomorphism of the Paillier algorithm, so that the acceleration ciphertext directly constructs the tracking signal from the vehicle without decryption. The tracking signal is combined with the distributed model predictive control (MPC), the linear matrix inequalities are used to transform the optimization problem of the control strategy, solve the optimal control inputs, and ensure the safety cooperative movement of the vehicle queue. The performance of the control system and effectiveness of the Paillier homomorphic encryption are verified by MATLAB simulation.

Keywords: Paillier homomorphic encryption; cybersecurity; cooperative adaptive cruise control; linear matrix inequality; model predictive control

0 引言

近年来，不断增长的交通需求导致道路愈发拥堵。车辆协同式自适应巡航控制（CACC）使车辆队列中的所有车辆保持理想的车间距，以协调的速度安全地在道路上行驶，被认为是目前缓解交通压力最有价值和应用前景的技术之一[1-3]。CACC 车辆间通过无线通信进行数据传输，而车辆间的车间距、相对速度以及加速度等重要数据的透明传输使得整个 CACC 系统在数据传输时尤为脆弱，潜在的网络攻击严重影响了 CACC 队列的稳定性[4-9]，文献［10］通过数值模拟，表明随着车辆队列中遭受网络攻击的车辆数量增加以及网络攻击严重程度的提高，交通容量会降低，且 CACC 车辆间追尾碰撞风险增加，空气污染物的排放以及燃料消耗量显著增加。因此，CACC 车辆队列的数据安全传输成为亟待解决的问题。

许多研究致力于维护车联网系统的数据安全。传统的方案大致分为两类，第一类是设计网络攻击检测机制[11-15]，然后采取一定的防御措施[16-17]。文献［11］将统计广义极端学生偏差（GESD, generalized extreme studentized deviate）方法与运动学的物理定律相结合，应用于车辆队列中的每辆车，根据车辆自身的超速决策实时检测异常，实验结果表明所提出的检测机制可以检测出 92% 以上的异常，具有较高的检测精度。文献［12］提出了一种基于长短期记忆的恶意信息检测机制（LMID, long short-term memory (LSTM) based malicious information detection），在车辆队

收稿日期:2023-07-12； **修回日期**:2023-08-20。
基金项目:国家自然科学基金(62273307);浙江省公益性技术应用研究项目(LGF22F030013)。
作者简介:杨敏艺(2001-),女,大学本科生。
通讯作者:宋秀兰 (1982-),女,博士,副教授。
引用格式:杨敏艺,宋秀兰,杨燕玲,等. Paillier 同态加密下车辆协同自适应预测巡航控制[J]. 计算机测量与控制,2024,32(8):153-160.

列中每辆车对数据延时以及前车的发动机驱动滞后等影响因素反应不同的复杂情况下，利用深度学习技术建立攻击检测模型，使每个车辆使用经过训练的网络对接收到的数据进行分类，从而进行有效的攻击检测。在多种车辆轨迹的仿真模型下，LMID 攻击检测机制的准确率都超过了 96%。使用两种攻击模型（即相关和非相关攻击）评估 LMID 攻击检测机制，性能评估结果表明 LMID 都可以快速地检测到相关的攻击。文献［13］基于可量化攻击、隐形攻击以及非隐形攻击 3 种网络攻击情境下，提出了一种基于滑模观察器（SMO，sliding mode observer）的 CACC 车辆队列网络攻击检测方案，经实验模拟 3 种攻击场景，发现这种检测方案可以实现对这 3 类攻击的有效检测和估计。文献［14］提出了一种新的分布式网络异常攻击检测方式，通过对数据进行迭代聚类，将正常和异常数据进行分类，建立矩阵映射模型并进行数据矩阵对比，初步对异常攻击数据进行判断。在矩阵中建立粒子密度函数，通过粒子密度变化计算其异常攻击概率，最后对其数据进行加权和滤波确定数据异常攻击特征，建立攻击检测模型。文献［15］针对 CACC 车辆队列通信过程中的网络攻击提出了一种使用未知输入观察器（UIO，unknown input observer）的攻击检测和防御机制，在每辆车上装备未知输入观察器，将 V2V 通信中获得的不可靠数据视为未知输入用来估计前车的状态，根据估计的结果来检测系统是否受到网络攻击。当检测到攻击时，自车系统的控制器输入切换到基于状态估计的安全输入，以此来保障车队的稳定行驶。文献［16］针对车辆队列遭受网络攻击的背景，提出了波束成形防御技术、双重锚定技术以及全球定位系统验证技术。经过仿真评估，这些防御技术对于减少外部干扰、提高车队中车辆在遭遇网络攻击时的稳定性具有很好的效益。文献［17］针对网联车辆在通信中的身份认证过程，提出一种基于移动目标防御的匿名身份认证方案来保证车辆的身份信息安全。第一类传统方案通常至少需要两个控制器，一个用于控制车辆正常行驶，另一个则用于攻击防御[18]。第二类传统方案是使用一种加密算法将数据在前车上加密后再进行传输，后车接收到密文后进行解密，得到原始数据后用于自车的控制系统。根据加密算法密钥类型的不同可以将加密的技术分为对称加密算法（私钥密码体系）和非对称加密算法（公钥密码体系）。在对称加密算法中，数据加密和解密采用的都是同一个密钥。数据发送方将明文（原始数据）与加密所用的密钥一起经过特殊加密算法处理后，使其变成复杂的加密密文发送出去。接收方收到密文后，若想得到原始数据，则需要使用加密时用的密钥及相同加密算法的逆算法对密文进行解密，才能从复杂密文中恢复出所需要的原始数据。文献［19］针对车辆网系统遭受黑客攻击、安全漏洞、隐私泄露等安全问题，采用全面改进的高级加密标准（AES，advanced encryption *stan*dard）对称加密算法来提高车载 FlexRay 总线数据传输的安全性。与传统的 AES 对称加密算法相比，其改进后的加密算法在加密速度和解密速度上分别提高了 26% 和 30%。文献［20］将车辆队列间通信的数据碎片化，拆分为多个小块后分别用 AES 对称算法加密，再发送到云，攻击者难以解密且重建数据，使得数据更加安全。但碎片化的加密使得整个数据块占用存储空间与未加密时相比大大增加。非对称加密算法中，密钥被分解为一对公开密钥和私有密钥。这对密钥中任何一把都可以作为公钥用于数据加密，通过非保密方式向他人公开，而另一把作为私有密钥，用于解密密文，恢复数据，由接收方加以保存。非对称加密的算法，其安全性能在广义上优于对称加密算法。文献［21］采用基于非对称椭圆曲线加密算法（ECC，elliptic curve cryptography）对车联网系统的重要数据进行加密，并使用批量处理的加密方式来提高方案的计算效率，在一定程度上节省了计算成本以及通信开销。进行了严格的安全分析，评估结果表明这种方案可以有效抵御多种网络攻击。文献［22］采用非对称 RSA 加密算法在路侧单元（RSU，road side unit）中使用公钥将数据进行加密，计算出的对应密文传输给车辆，车辆通过私钥解密恢复出原始数据。并在 Matlab 环境下对基于路侧单元 RSU 和加密安全系统的车辆进行了仿真，建立交通场景模型，加入恶意的网络攻击，仿真结果表明基于 RSA 的高级加密和解密域方案能够有效提高车联网系统的安全性能，缺少加密处理时，数据有效交付率降低，甚至不能进行有意义的数据通信。

对于上述两类传统方案：第一类对网络攻击的处理方案是检测到攻击再启动防御机制，在不同控制器间切换，使得车辆整体的控制系统较为复杂；第二类方案使用传统的数据加密，密文与密钥同时传输，车辆的控制动作只有将密文解密后才能进行，且用于数据解密的密钥在传输过程中存在被盗风险，数据在很大概率上仍可能泄露并遭到网络攻击。基于这些问题，本文提出一种使用 Paillier 同态加密的方案来传输 CACC 车辆队列间的重要数据。首先，基于复合剩余类的 Paillier 算法[23]具有优越的性能，研究表明其在解密方面比 RSA 更快[24]，与未填充的 RSA 相比，Paillier 算法具有语义安全性[25]，其加性同态特性已广泛应用于隐私保护安全计算、加密数据库、加密数据机器学习等应用[26]。其次，本文所设计的系统只使用 MPC 控制器对车辆进行控制，不用在正常行驶的控制系统和攻击防御时的控制系统之间切换，降低了系统的复杂性。最后，Paillier 加密算法作为一种同态密码系统，其最大特点是：原始数据经同态加密后，对所得密文进行指定的运算，其运算结果等价于原始数据直接进行相同运算所得结果。因此不需要在接收端对密文解密后再使用，与传统的加密方案相比，节省了解密运算的时间和使用的存储空间。传输过程仅需传输密文，不需要传输密钥，安全性大幅提升。

本文考虑在公路上行驶的异构车辆组成的 CACC 队列，对其纵向队列进行建模。设计一个综合跟踪信号，对跟踪信号中自车接收到的来自前车的理想加速度使用 Paillier 同态加密算法在前车上进行加密，基于 Paillier 加密算法的同

态性，设计密文与常量间的数乘运算，使自车接收到的加速度密文直接与其权重系数相乘用于跟踪信号的建立，与传统方案相比，节省了自车对密文解密所需的时空资源。将构建好的综合跟踪信号用于 MPC 控制器，控制器的控制目标是使车辆的输出状态与综合跟踪信号的误差最小。为实现控制目标，定义一个代价函数，将控制最优的问题转换为代价函数最小问题，并采用线性矩阵不等式对控制策略的优化问题转化，求解最优控制输入。最后，通过 MATLAB 对车辆队列进行建模仿真，证明方案的有效性。

1　系统建模及问题描述

由于在 CACC 车辆队列中，车辆之间通过无线通信网络传输状态信息，若不对前车发送的数据进行一些处理，而直接将重要的数据透明传输，很可能遭受恶意的网络攻击，如拒绝服务（DoS，denial-of-service）攻击和欺骗攻击。攻击者一般通过干扰无线通信信道上的无线电频率来实施 DoS 攻击。欺骗攻击会破坏车载传感器，篡改信道中传输的数据。例如，GPS 欺骗可以伪造 GPS 读数，激光雷达欺骗攻击可以通过消除真实的障碍物或在车辆前添加假的障碍物。这些网络攻击会导致自车接收到错误的信息，破坏车辆队列的稳定性，严重时甚至会造成安全事故。本文采用一种满足加法同态和数乘同态，且具有高效运行性能的 Paillier 同态加密算法。CACC 车辆队列中的每辆车均装备有 Paillier 加密器以及 MPC 控制器。首先，前车欲发送给后车的理想加速度在前车的 Paillier 加密器中进行加密，将相关密文传输到云端服务器，自车接收器接收从云端服务器下传的密文，由于此加密算法具有同态性，故不需要解密，可以直接将接收到的密文送入 MPC 控制器中进行线性运算以构建综合跟踪信号，控制器解出最优的控制输入后将其发送到自车执行器，控制自车的运动状态。此过程同时应用于车队中的每辆车，系统整体模型如图 1 所示。

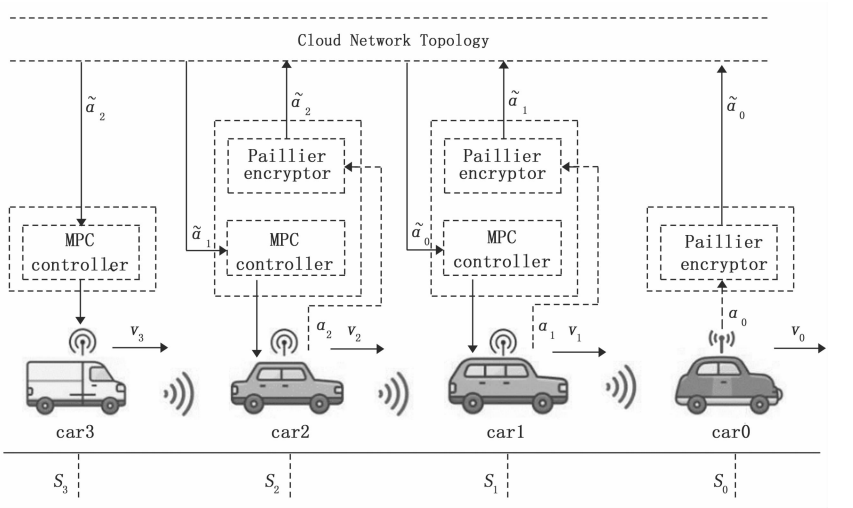

图 1　车辆 CACC 队列示意图

1.1　车辆队列纵向模型

单向前车跟随式（PF，predecessor following）的通信拓扑模型具有通信距离短、通信时延低、可靠性较高的优点，而且由于较少的车间通信，这种车队拓扑模型的频带资源占用少。另一方面，车辆队列中除领导车辆外的其余车辆只接收其前车发送出的信息，在一定程度上可以防止攻击者攻击某辆车而致使整个车队均受冲击的情形发生。因此本文选取 PF 通信拓扑结构对车队进行建模。

设车辆队列中的第 i 辆车的绝对位置、速度、加速度分别表示为 $s_i(t)$、$v_i(t)$、$a_i(t)$。第 i 辆车的车辆长度表示为 l_i。

则车辆的车间距 $d_i(t)$ 以及相对速度 $\Delta v_i(t)$ 可以表示为：

$$\begin{cases} d_i(t) = s_i(t) - s_{i-1}(t) - l_{i-1} \\ \Delta v_i(t) = v_i(t) - v_{i-1}(t) \end{cases} \tag{1}$$

车辆的加速度与控制输入的关系可由误差动力学的公式推导出来[27]，形式如下：

$$\dot{a}_i(t) = -\frac{1}{\tau_i}a_i(t) + \frac{1}{\tau_i}u_i(t) \tag{2}$$

其中：τ_i 是车辆系统动力学的时间常数，$u_i(t)$ 是车辆的控制输入。

选择车辆的车间距 $d_i(t)$、相对速度 $\Delta v_i(t)$ 以及由车辆加速度和控制输入得到的加速度 $\dot{a}_i(t)$ 作为状态向量 $\boldsymbol{x}_i(t) = [d_i(t), \Delta v_i(t), \dot{a}_i(t)]^T$，建立如下车辆状态空间模型：

$$\dot{x}_i(t) = \boldsymbol{A}x_i(t) + \boldsymbol{B}u_i(t) + \boldsymbol{C}x_{i-1}(t) \tag{3}$$

其中：$\boldsymbol{A}$、$\boldsymbol{B}$、$\boldsymbol{C}$ 参数矩阵表达式如下：

$$\boldsymbol{A} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -1/\tau_i \end{bmatrix}, \boldsymbol{B} = \begin{bmatrix} 0 \\ 0 \\ 1/\tau_i \end{bmatrix}, \boldsymbol{C} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 0 & 0 \end{bmatrix}$$

为了方便对车辆的实时控制，将车辆纵向跟随模型离散化，因此，以 T_s 为周期对式（3）采样。离散化后的状态空间模型形式如下式：

$$\dot{x}_i(k+1) = \boldsymbol{A}x_i(k) + \boldsymbol{B}u_i(k) + \boldsymbol{C}x_{i-1}(k) \tag{4}$$

其中，离散化后的参数矩阵如下：

$$\boldsymbol{A} = \begin{bmatrix} 1 & T_s & 0 \\ 0 & 1 & T_s \\ 0 & 0 & 1 - T_s/\tau_i \end{bmatrix}, \boldsymbol{B} = \begin{bmatrix} 0 \\ 0 \\ T_s/\tau_i \end{bmatrix}, \boldsymbol{C} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & -T_s \\ 0 & 0 & 0 \end{bmatrix}$$

2　基于 Paillier 加密算法的 MPC 控制器设计

2.1　综合跟踪信号设计

CACC 车辆队列在行驶过程中会出现不同的情形。比如当自车与前车的车间距大于理想的车间距，速度和加速度也都大于前车时，这种情况下自车的状态是一个比较正常的驾驶行为，此时由于车间距误差是负数，速度和加速度误差是正数，综合后可以得到一个较小的跟踪误差，控制器只会进行较小的调整；而当自车与前车的车间距小于理想的车间距，速度和加速度均大于前车时，自车处于一个比较危险的驾驶状态，此时由于车间距误差是正数，速

度和加速度误差也是正数，综合后会得到一个较大的跟踪误差，控制器将会进行较大的调整，其他的驾驶情形也会有类似的结果。因此，本文采用综合的跟踪信号，因为它可以更灵活地表现车辆队列行驶过程中的不同情形。

选取理想车间距 $d_{i,des}(k)$、理想相对速度 $\Delta v_{i,des}(k)$ 以及理想加速度 $a_{i-1}(k)$，将三者进行权重分配，权重系数分别为 w_1、w_2、w_3，设计一个综合跟踪信号 $\dot{r}_i(k)$，使自车行驶过程中的状态信息不断逼近综合跟踪信号 $\dot{r}_i(k)$，实现 CACC 车辆队列的控制目标。综合跟踪信号 $\dot{r}_i(k)$ 设计如下：

$$\dot{r}_i(k) = w_1 d_{i,des}(k) + w_2 \Delta v_{i,des}(k) + w_3 a_{i-1}(k)$$

CACC 车辆队列在行驶过程中，跟随车辆除了可以通过无线通信网络获取前车的位置和速度信息，还可以通过一些车载传感器来获取，甚至可以接收一些路边基础设施关于前车的位置和速度信息，通过数据融合来融合这些信息，可以获得相当可靠的前车位置和速度的近似值[28]。但是理想加速度往往需要由前车通过无线通信网络传递给跟随车辆。理想加速度 $a_{i-1}(k)$ 由前车通过无线通信网络传向后车，由于通信网络具有一定的开放性，$a_{i-1}(k)$ 透明传输易遭受网络攻击，在受到攻击的情况下会向跟随车辆发送虚假信息，影响 CACC 队列的稳定性。所以我们需要对前车传递的加速度 $a_{i-1}(k)$ 先进行加密处理，处理之后再代入所设计的综合跟踪信号。

2.2 加密算法设计

2.2.1 Paillier 加密算法

本节对前车传向后车的理想加速度 $a_{i-1}(k)$ 进行加密处理，方法如下：

1）生成密钥：

（1）生成两个长度相同的大素数 p、q，且 $p \neq q$，满足 $\gcd[pq,(p-1)(q-1)]=1$。该性质确保这两个素数 p、q 长度相同。

（2）计算 $n = pq$。生成随机数 r，满足 $(0 \leqslant r \leqslant n, r \in Z_n^*)$。

（3）公钥 $PK = (n,g)$。

2）数据加密：

选择随机数 $r \in Z_n^*$，加密后的理想加速度密文 $\tilde{a}_{i-1}(k) = g^{a_{i-1}(k)} \cdot r^n \bmod n^2$。

3）数据解密：

本文直接利用 Paillier 加密算法的同态性，无须对理想加速度密文进行解密。所谓同态性，是指原始数据经同态加密处理后，对所得密文进行指定的运算，其运算结果等价于原始数据直接进行相同运算所得结果。

理想加速度 $a_{i-1}(k)$ 的加密过程如图 2 所示。

2.2.2 Paillier 加密算法数乘同态运算设计

本节设计 Paillier 加密算法的数乘同态运算⊗。设 $\tilde{a}_{i-1}(k) = g^{a_{i-1}(k)} \cdot r^n \bmod n^2 = Enc_{PK}[a_{i-1}(k)]$，$Enc_{PK}()$ 表示以 PK 为公钥对明文进行 Paillier 加密。

$$w_3 \otimes \tilde{a}_{i-1}(k) = \tilde{a}_{i-1}(k)^{w_3} \bmod n^2 = g^{w_3 a_{i-1}(k)} \cdot (r^{w_3})^n \bmod n^2 = Enc_{PK}(w_3 \cdot a_{i-1}(k) \bmod n) \quad (5)$$

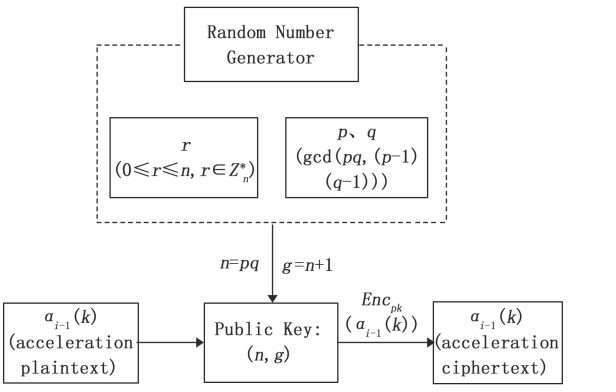

图 2 理想加速度加密过程

式（5）为加速度密文 $\tilde{a}_{i-1}(k)$ 与其权重系数 w_3 的数乘同态运算⊗。运算结果表示密文 $\tilde{a}_{i-1}(k)$ 与常量 w_3 的数乘运算⊗结果与明文 $a_{i-1}(k)$ 与常量 w_3 相乘后再加密的结果相同，即：

$$w_3 \otimes \tilde{a}_{i-1}(k) = Enc_{PK}(w_3 \cdot a_{i-1}(k) \bmod n) \quad (6)$$

研究车辆中装有接收器，接收器接收从云端服务器下传得到的理想加速度密文 $\tilde{a}_{i-1}(k)$，由前述所设计的数乘同态运算可知，我们无须解密恢复出 $a_{i-1}(k)$，直接将密文 $\tilde{a}_{i-1}(k)$ 用于跟踪信号的建立，控制自车行驶。由加密后的理想加速度 $\tilde{a}_{i-1}(k)$ 构建的综合跟踪信号 $r_i(k)$ 如下：

$$r_i(k) = w_1 d_{i,des}(k) + w_2 \Delta v_{i,des}(k) + w_3 \otimes \tilde{a}_{i-1}(k) \quad (7)$$

2.3 MPC 控制器设计

车辆的实时输出状态 $y_i(k)$ 可由如下状态输出方程获得：

$$y_i(k) = \boldsymbol{D} x_i(k) \quad (8)$$

其中：参数矩阵 $\boldsymbol{D} = [w_1, w_2, w_3]$。在车辆输出状态逼近综合跟踪信号的过程中，定义 $e_i(k)$ 表示综合跟踪信号与实时输出状态间的误差，误差变量 $e_i(k)$ 的形式如下：

$$e_i(k) = r_i(k) - y_i(k) \quad (9)$$

为了消除自车跟随前车行驶的过程中，车辆的实时状态与理想状态之间的稳态误差，对状态空间模型（4）进行修改。

用状态误差以及车辆的状态增量，定义增广状态向量 $\tilde{\boldsymbol{x}}_i(k) = [e_i(k+1), x_i(k+1)^T - x_i(k)^T]^T$，经修改后，车辆的状态空间模型（4）改为如下形式：

$$\tilde{\boldsymbol{x}}_i(k+1) = \overline{\boldsymbol{A}} \tilde{x}_i(k) + \boldsymbol{B}_u \tilde{u}_i(k) + \boldsymbol{B}_p \tilde{x}_{i-1}(k) + \boldsymbol{B}_r \tilde{r}_i(k) \quad (10)$$

上式中的各个参数矩阵形式如下：

$$\overline{\boldsymbol{A}} = \begin{bmatrix} I & -\boldsymbol{D} \\ 0 & A \end{bmatrix}, \boldsymbol{B}_u = \begin{bmatrix} 0 \\ B \end{bmatrix}, \boldsymbol{B}_r = \begin{bmatrix} I \\ 0 \end{bmatrix}, \boldsymbol{B}_p = \begin{bmatrix} 0 & 0 \\ 0 & C \end{bmatrix}$$

且有：

$$\tilde{\boldsymbol{u}}_i(k) = \boldsymbol{u}_i(k+1) - \boldsymbol{u}_i(k)$$

$$\tilde{\boldsymbol{r}}_i(k) = \boldsymbol{r}_i(k+1) - \boldsymbol{r}_i(k)$$

为了实现控制目标，定义一个代价函数 $J(x)$，其形式如下：

$$J(x) = \sum_{j=0}^{\infty} \boldsymbol{z}_i(k+j \mid k)^T \boldsymbol{z}_i(k+j \mid k) \quad (11)$$

其中：

$$\boldsymbol{z}_i(k)=\boldsymbol{E}\tilde{\boldsymbol{x}}_i(k)+\boldsymbol{F}\tilde{u}_i(k)$$

$$\boldsymbol{E}=\begin{bmatrix}w_4&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{bmatrix}\quad\boldsymbol{F}=\begin{bmatrix}0&0&0&w_5\end{bmatrix}^{\mathrm{T}}$$

$\boldsymbol{E}$，$\boldsymbol{F}$ 是权重矩阵。矩阵 $\boldsymbol{E}$，$\boldsymbol{F}$ 定义了性能变量 $z_i(k)$，且满足 $\boldsymbol{EF}=0$。由此可以得到网联车辆协同自适应预测巡航控制的优化问题，即使代价函数 $J(x)$ 最小：

$$\min_{\tilde{u}_i(k+j|k),j=0,1,\cdots,\infty}J(x)\tag{12}$$

s. t.

$$\left\|T_{\tilde{x}}\right\|_\infty^2<\delta\tag{13}$$

$$\left\|\tilde{\boldsymbol{u}}(k\mid k)+\bar{\boldsymbol{u}}\right\|^2\leqslant\hat{\boldsymbol{u}},\bar{\boldsymbol{u}}=\sum_{i=0}^{k-1}\tilde{\boldsymbol{u}}(i)\tag{14}$$

其中：$\delta>0$ 是给定的 H_∞ 性能界限，$\hat{u}$ 是加速度约束量。在设计 CACC 车辆队列控制器时，由于存在外界干扰、通信延时以及网络攻击等因素，我们所建立的车辆状态空间模型并不能总是精确预测下一时刻的状态，为了得到较为理想的控制输入，设计如下形式的状态反馈控制律：

$$\tilde{\boldsymbol{u}}_i(k)=\boldsymbol{F}(k)\tilde{\boldsymbol{x}}_i(k)\tag{15}$$

其中：$\boldsymbol{F}(k)$ 是状态反馈控制矩阵，用其控制增广状态向量 $\tilde{\boldsymbol{x}}_i(k)$，从而得到控制输入变化量 $\tilde{\boldsymbol{u}}_i(k)$。

在上述网联车辆协同自适应预测巡航控制优化问题中，由于反馈控制矩阵 $\boldsymbol{F}(k)$ 的求解较为困难，因此将求解代价函数最小的优化问题（12）转变为线性矩阵不等式进行求解。定义函数 $\boldsymbol{V}(\tilde{\boldsymbol{x}}_i(k))=\tilde{\boldsymbol{x}}_i^T(k)\boldsymbol{P}\tilde{\boldsymbol{x}}_i(k)$，$\boldsymbol{P}>0$。对优化问题（12）进行转化，基于定义的二次函数，有：

$$\boldsymbol{V}(\tilde{\boldsymbol{x}}_i(k+j+1\mid k))-\boldsymbol{V}(\tilde{\boldsymbol{x}}_i(k+j\mid k))=\tilde{\boldsymbol{X}}^T\tilde{\boldsymbol{A}}\tilde{\boldsymbol{X}}\tag{16}$$

其中：

$$\tilde{\boldsymbol{X}}=\begin{bmatrix}\tilde{\boldsymbol{x}}_i(k+j\mid k)\\\tilde{\boldsymbol{r}}_i(k+j\mid k)\\\tilde{\boldsymbol{x}}_{i-1}(k+j\mid k)\end{bmatrix}$$

$$\tilde{\boldsymbol{A}}=\begin{bmatrix}\boldsymbol{A}_d^T\boldsymbol{P}\boldsymbol{A}_d-\boldsymbol{P}&*&*\\\boldsymbol{B}_r^T\boldsymbol{P}\boldsymbol{A}_d&\boldsymbol{B}_r^T\boldsymbol{P}\boldsymbol{B}_r&*\\\boldsymbol{B}_p^T\boldsymbol{P}\boldsymbol{A}_d&\boldsymbol{B}_p^T\boldsymbol{P}\boldsymbol{B}_r&\boldsymbol{B}_p^T\boldsymbol{P}\boldsymbol{B}_p\end{bmatrix}$$

$$\boldsymbol{A}_d=\bar{\boldsymbol{A}}+\boldsymbol{B}_u\boldsymbol{F}(k)$$

在协同自适应巡航控制车辆队列的行驶过程中，车辆的最终状态将趋于稳定，因此可以得到 $\tilde{x}(\infty\mid k)=0$。将等式（16）从 $i=0$ 到 $i=\infty$ 累加可以得到：

$$-\boldsymbol{V}(\tilde{\boldsymbol{x}}_i(k\mid k))=\sum_{j=0}^{\infty}\tilde{\boldsymbol{X}}^T\tilde{\boldsymbol{A}}\tilde{\boldsymbol{X}}\tag{17}$$

由于在代价函数的定义中 $\boldsymbol{EF}=0$，于是等式（11）可以等价为如下形式：

$$J(k)=\sum_{j=0}^{\infty}\boldsymbol{z}_i(k+j\mid k)^T\boldsymbol{z}_i=\delta\sum_{j=0}^{\infty}\tilde{\boldsymbol{r}}_i(k+j\mid k)^T\tilde{\boldsymbol{r}}_i(k+j\mid k)+\delta\sum_{j=0}^{\infty}\tilde{\boldsymbol{x}}_{i-1}(k+j\mid k)^T\tilde{\boldsymbol{x}}_{i-1}(k+j\mid k)+\sum_{j=0}^{\infty}\tilde{\boldsymbol{X}}^T\tilde{\boldsymbol{B}}\tilde{\boldsymbol{X}}\tag{18}$$

其中：

$$\tilde{\boldsymbol{B}}=\begin{bmatrix}\boldsymbol{E}^T\boldsymbol{E}+\boldsymbol{F}(k)^T\boldsymbol{F}^T\boldsymbol{F}\boldsymbol{F}(k)&*&*\\0&-\delta&*\\0&0&-\delta\end{bmatrix}$$

将（17）式和（18）式相加后，移项可得到：

$$J(k)=\boldsymbol{V}(\tilde{\boldsymbol{x}}_i(k\mid k))+\delta\sum_{j=0}^{\infty}\tilde{\boldsymbol{r}}_i(k+j\mid k)^T\tilde{\boldsymbol{r}}_i(k+j\mid k)+\delta\sum_{j=0}^{\infty}\tilde{\boldsymbol{x}}_{i-1}(k+j\mid k)^T\tilde{\boldsymbol{x}}_{i-1}(k+j\mid k)+\sum_{j=0}^{\infty}\tilde{\boldsymbol{X}}^T\Lambda\tilde{\boldsymbol{X}}\tag{19}$$

其中：$\Lambda=\tilde{\boldsymbol{A}}+\tilde{\boldsymbol{B}}$。根据有界实引理[29]，约束（13）成立当且仅当 $\Lambda\leqslant0$，因此式（19）可以转化为

$$J(k)\leqslant V(\tilde{\boldsymbol{x}}_i(k\mid k))+\delta\sum_{j=0}^{\infty}\tilde{\boldsymbol{r}}_i(k+j\mid k)^T\tilde{\boldsymbol{r}}_i(k+j\mid k)+\delta\sum_{j=0}^{\infty}\tilde{\boldsymbol{x}}_{i-1}(k+j\mid k)^T\tilde{\boldsymbol{x}}_{i-1}(k+j\mid k)\tag{20}$$

因为

$$\sum\nolimits_{j=0}^{\infty}\tilde{\boldsymbol{x}}_{i-1}(k+j\mid k)^T\tilde{\boldsymbol{x}}_{i-1}(k+j\mid k)\leqslant\hat{\boldsymbol{r}}_i^2<\infty$$

$$\sum_{j=0}^{\infty}\tilde{\boldsymbol{x}}_{i-1}(k+j\mid k)^T\tilde{\boldsymbol{x}}_{i-1}(k+j\mid k)\leqslant\hat{\boldsymbol{x}}_{i-1}^2<\infty\tag{21}$$

令 $\boldsymbol{V}(\tilde{\boldsymbol{x}}_i(k\mid k))\leqslant\gamma$，则可以得到：

$$J(x)\leqslant\gamma+\delta\tilde{\boldsymbol{r}}_i^2(k)+\delta\hat{\boldsymbol{x}}_{i-1}^2(k)\tag{22}$$

因此，网联车辆协同自适应 MPC 控制优化问题（12）转化为如下形式的优化问题：

$$\min_{F(k),P}\gamma\tag{23}$$

s. t.

$$\Lambda\leqslant0$$

$$\tilde{\boldsymbol{x}}_i^T(k\mid k)\boldsymbol{P}\tilde{\boldsymbol{x}}(k\mid k)\leqslant\gamma$$

$$\left\|\tilde{\boldsymbol{u}}(k\mid k)+\bar{\boldsymbol{u}}\right\|^2\leqslant\hat{\boldsymbol{u}},\bar{\boldsymbol{u}}=\sum_{i=0}^{k-1}\tilde{\boldsymbol{u}}(i)$$

由于 $\Lambda\leqslant0$ 不等式在求解控制器的反馈控制矩阵 $\boldsymbol{F}(k)$ 时较为困难，故进一步利用 Schur 补引理对其进行转化，得到如下形式的线性矩阵不等式：

$$\begin{bmatrix}-\boldsymbol{P}&*&*&*&*&*\\0&-\delta\boldsymbol{I}&*&*&*&*\\0&0&-\delta\boldsymbol{I}&*&*&*\\\bar{\boldsymbol{A}}+\boldsymbol{B}_u\boldsymbol{F}(k)&\boldsymbol{B}_r&\boldsymbol{B}_p&-\boldsymbol{P}^{-1}&*&*\\\boldsymbol{E}&0&0&0&-\boldsymbol{I}&*\\\boldsymbol{F}\boldsymbol{F}(k)&0&0&0&0&-\boldsymbol{I}\end{bmatrix}\tag{24}$$

利用 Schur 补引理，$\tilde{\boldsymbol{x}}_i\mid\tilde{\boldsymbol{x}}_i^T(k\mid k)\boldsymbol{P}\tilde{\boldsymbol{x}}_i(k\mid k)\leqslant\gamma$ 不等式可以转化为如下形式的线性矩阵不等式：

$$\begin{bmatrix}1&*\\\tilde{\boldsymbol{x}}(\boldsymbol{k}\mid\boldsymbol{k})&\boldsymbol{\gamma P}^{-1}\end{bmatrix}\geqslant0\tag{25}$$

令矩阵 $\boldsymbol{Q}=\gamma\boldsymbol{P}^{-1}$（$\boldsymbol{Q}>0$ 且 $\boldsymbol{Q}=\boldsymbol{Q}^T$），$\boldsymbol{Y}=\boldsymbol{F}(k)\boldsymbol{Q}$，则式（24）（25）转化为：

$$\begin{bmatrix}-\boldsymbol{Q}&*&*&*&*&*\\0&-\gamma\delta\boldsymbol{I}&*&*&*&*\\0&0&-\gamma\delta\boldsymbol{I}&*&*&*\\\bar{\boldsymbol{A}}\boldsymbol{Q}+\boldsymbol{B}_u\boldsymbol{Y}&\gamma\boldsymbol{B}_r&\gamma\boldsymbol{B}_p&-\boldsymbol{Q}&*&*\\\boldsymbol{E}\boldsymbol{Q}&0&0&0&-\gamma\boldsymbol{I}&*\\\boldsymbol{F}\boldsymbol{Y}&0&0&0&0&-\gamma\boldsymbol{I}\end{bmatrix}\leqslant0\tag{26}$$

$$\begin{bmatrix} 1 & * \\ \tilde{\boldsymbol{x}}(k\mid k) & \boldsymbol{Q} \end{bmatrix} \geqslant 0 \tag{27}$$

输入约束条件（14）也可以通过如下变换转化为线性矩阵不等式：

$$\begin{aligned} &\|\tilde{\boldsymbol{u}}(k\mid k)+\bar{\boldsymbol{u}}\|^2 = \|\tilde{\boldsymbol{u}}(k\mid k)\|^2+2\tilde{\boldsymbol{u}}\bar{\boldsymbol{u}}(k\mid k)+\bar{\boldsymbol{u}}^2 = \\ &\|\boldsymbol{Y}\boldsymbol{Q}^{-1/2}\boldsymbol{Q}^{-1/2}\tilde{\boldsymbol{x}}(k\mid k)\|^2+\bar{\boldsymbol{u}}^2+2\bar{\boldsymbol{u}}\boldsymbol{Y}\boldsymbol{Q}^{-1}\tilde{\boldsymbol{x}}(k\mid k) \leqslant \\ &\|\boldsymbol{Y}\boldsymbol{Q}^{-1/2}\|^2\|\boldsymbol{Q}^{-1/2}\tilde{\boldsymbol{x}}(k\mid k)\|^2+\bar{\boldsymbol{u}}^2+2\bar{\boldsymbol{u}}\boldsymbol{Y}\boldsymbol{Q}^{-1}\tilde{\boldsymbol{x}}(k\mid k) \leqslant \\ &\|\boldsymbol{Y}\boldsymbol{Q}^{-1/2}\|^2+\bar{\boldsymbol{u}}^2+2\bar{\boldsymbol{u}}\boldsymbol{Y}\boldsymbol{Q}^{-1}\tilde{\boldsymbol{x}}(k\mid k) = \\ &\|\boldsymbol{Y}\boldsymbol{Q}^{-1/2}+\bar{\boldsymbol{u}}\tilde{\boldsymbol{x}}(k\mid k)^T\boldsymbol{Q}^{-1/2}\|^2+\bar{\boldsymbol{u}}^2-\|\bar{\boldsymbol{u}}\boldsymbol{Q}^{-1/2}\tilde{\boldsymbol{x}}(k\mid k)\|^2 = \\ &\|\boldsymbol{Y}\boldsymbol{Q}^{-1/2}+\bar{\boldsymbol{u}}\tilde{\boldsymbol{x}}(k\mid k)^T\boldsymbol{Q}^{-1/22}+\bar{\boldsymbol{u}}_m^2(1-\beta) \end{aligned}$$

其中：$0\leqslant\beta=\tilde{\boldsymbol{x}}(k\mid k)^T\boldsymbol{Q}^{-1}\tilde{\boldsymbol{x}}(k\mid k)\leqslant 1$。$\beta$为松弛变量，$\beta$越趋近于 0 则输入约束越保守[30]。因此，若不等式 $\|\boldsymbol{Y}\boldsymbol{Q}^{-1/2}+\bar{\boldsymbol{u}}\tilde{\boldsymbol{x}}(k\mid k)\boldsymbol{Q}^{-1/2}\|^2+\bar{\boldsymbol{u}}_m^2(1-\beta)\leqslant\hat{\boldsymbol{u}}^2$ 成立，则输入约束满足。进一步由 Schur 补引理可得

$$\begin{bmatrix} \hat{\boldsymbol{u}}^2-\bar{\boldsymbol{u}}^2(1-\beta) & * \\ \boldsymbol{Y}^T\bar{\boldsymbol{u}}\tilde{\boldsymbol{x}}(k\mid k) & \boldsymbol{Q} \end{bmatrix} \geqslant 0 \tag{28}$$

最终，使用 Paillier 同态加密算法设计的 MPC 控制器设计成如下形式，通过该控制器可以使 CACC 车辆队列安全协同行驶。

$$\begin{aligned} &\min_{F(k),P}\gamma \\ &\text{s.t.}\,(26),(27),(28) \end{aligned} \tag{29}$$

综上所述，Paillier 同态加密下 CACC 车辆队列的协同自适应巡航控制器的总体实现步骤如下：

1）初始化车辆的状态信息和控制输入，初始化参数矩阵 $\bar{\boldsymbol{A}}$，$\boldsymbol{B}_u$，$\boldsymbol{C}$，$\boldsymbol{D}$，$\boldsymbol{B}_p$。

2）车辆队列中的车辆 i 根据 k 时刻自车和前车的状态信息，控制输入 $\boldsymbol{u}_i(k)$ 计算出 $\boldsymbol{x}_i(k)$，$\boldsymbol{x}_i(k+1)$。

3）前车 k 时刻欲传给后车的加速度用 Paillier 加密算法进行加密，将密文上传到云端服务器，后车接收器从云端下载加密后的加速度 $\tilde{\boldsymbol{a}}_{i-1}(k)$，由式（7）建立跟踪信号，再根据式（11）（13）（14）得出误差函数 $e_i(k+1)$。

4）由 2）所得的 $\boldsymbol{x}_i(k)$，$x_i(k+1)$ 以及 3）所得的误差 $e_i(k+1)$ 计算得到状态变量 $\tilde{\boldsymbol{x}}_i(k)$。

5）通过式（29）解出矩阵 $\boldsymbol{Y}$、$\boldsymbol{Q}$，计算反馈控制矩阵 $\boldsymbol{F}(k)$。

6）由 4）、5）得出的 $\tilde{\boldsymbol{x}}_i(k)$、$\boldsymbol{F}(k)$ 通过式（14）得出加速度变化量 $\tilde{\boldsymbol{u}}_i(k)$，由加速度变化量可得 $k+1$ 时刻的控制输入 $\boldsymbol{u}_i(k+1)$，返回 2），如此往复。

3 仿真验证与分析

本文的仿真场景为一组由四辆异质车辆组成的 CACC 车辆队列，仿真时间为 100 s。式（7）中理想车间距 $d_{i,des}(k)$、理想相对速度 $\Delta v_{i,des}(k)$ 以及理想加速度 $a_{i-1}(k)$ 的权重系数 w_1、w_2、w_3 分别取 0.4、0.1、0.02。四辆车的初始速度均设为 15 m/s，4 辆车的初始位置分别是 $s_0=0$ m，$s_1=20$ m，$s_2=40$ m，$s_3=60$ m。设定恒定车头时距 $h=1.0$ s，最小安全车间距为 $d_0=5$ m，H_∞ 约束条件 δ 取值为 2，松弛变量 β 取 0.05。前车传递给后车的加速度 $a_i(k)$ 在前车上经 Paillier 加密算法处理后，将得到的加密后的加速度 $\tilde{a}_i(k)$ 上传到云端服务器，再下传给后车，由于 Paillier 加密算法具有同态性，故无需对接收到的密文解密，可直接将理想加速度密文 $\tilde{a}_i(k)$ 应用于构建自车的综合跟踪信号 $r_i(k)$，进而得到误差状态量、控制输入量，控制自车稳定跟随前车行驶。行驶过程中，四辆车的速度、加速度，两两之间的车间距以及车间距与理想车间距的误差等参数的仿真结果如图 3 和图 4 所示。

表 1 仿真参数设置

参数	值
初始速度 $v_i(0)$ /(m/s)(i=0,1,2,3)	15
初始加速度 $a_i(0)$ /(m/s^2)(i=0,1,2,3)	0
车头时距 h_i/s(i=0,1,2,3)	1.0
采样间隔 T_s/s	0.1
仿真持续时间 T/s	100
最小安全距离 d_0/m	5
性能约束 δ/m	2
松弛变量 β	0.05

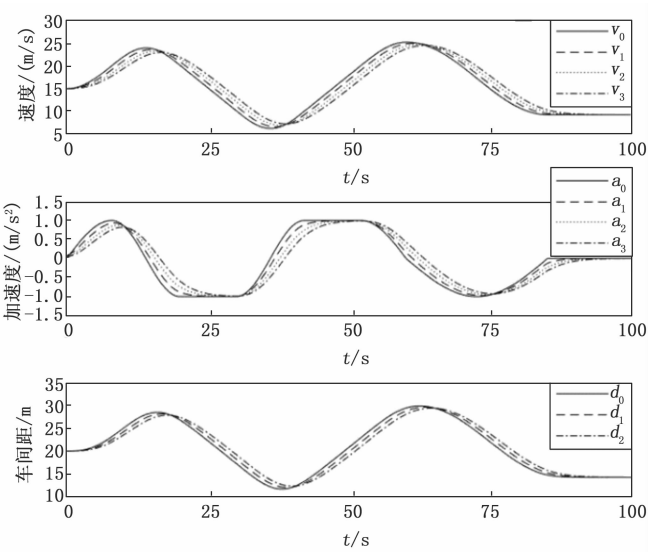

图 3 加密传输条件下各指标的情况

图 3 表示仿真时间段内四辆车速度、加速度以及 4 辆车两两之间的车间距变化曲线。领导车辆初始速度为 0，从 0 时刻开始到 14.2 s 期间先进行加速度逐渐增大的加速运动，再做加速度逐渐减小的加速运动。在 14.2～36.2 s 内先做加速度增大的减速运动，再做匀减速运动，最后做加速度减小的减速运动。在 36.2～60 s 内做加速度逐渐增大的加速运动，再做匀加速运动，最后做加速度减小的加速运动。在 60～85 s 先做加速度逐渐增大的减速运动，再做加速度逐渐减小的减速运动。第 85～100 s，保持 9.27 m/s 的速度匀速行驶。跟随车辆的整体运动趋势与领导车辆一致，车队稳定跟随行驶。由图 3 可以看出，四辆车的车间距最大为 20.89 m，最小为 11.69 m，始终大于所设置的最小安全

车间距 $d_0=5$ m。

在前车传向后车的加速度均经过 Paillier 加密后再传输的条件下，车间距与理想车间距的误差曲线如图 4（a）所示。现模拟前车向后车传输的加速度没有经过 Paillier 加密过程，而是直接以明文形式传输，并在 0～100 s 的仿真时间内持续加入网络攻击，跟随车辆的加速度以及此时车间距与理想车间距的误差曲线仿真结果如图 4（b）所示。

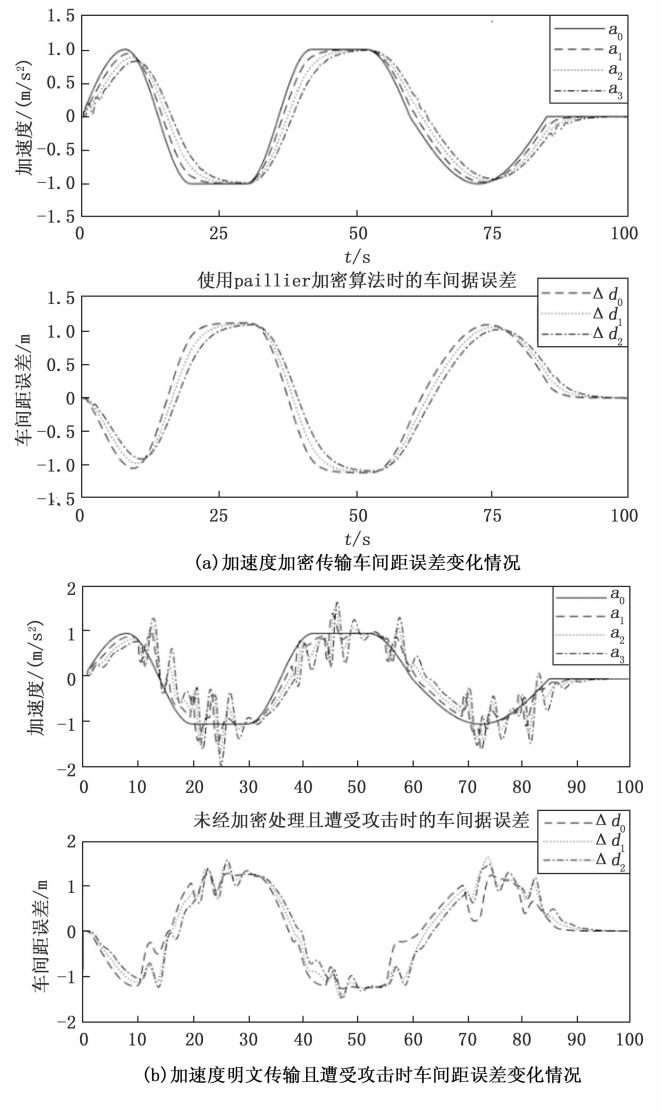

图 4　加密传输和未经加密处理对比图

由图 4（a）可以看出，当加速度在前车上加密，后车接收后用加速度密文建立综合跟踪信号，控制自车行驶时，车辆间的车间距与理想车间距的误差 Δd_i 较小，且异构车辆间的车间距误差也较为一致，车间距误差曲线平坦且稳定。与图 3 的各个参数对应，在加速度增大或减小变化时，车队中前车与后车间的车间距与理想车间距的误差在 -1.092～1.116 m 之间变化，保持同态加密下 CACC 车辆队列的稳定行驶。由图 4（b）可看出，当 car1 接收到的 car0 传递的加速度 a_1，car2 接收到的 car1 传递的加速度 a_2 以及 car3 接收到的 car2 传递的加速度 a_3 未在前车上加密，而是以明文形式直接传输，在遭受到持续的网络攻击后，后车接收到的加速度经恶意篡改，产生的综合跟踪信号存在一定的不合理性，致使车队中两两之间的车间距误差 Δd 存在较大的波动，车与车间的距离非常不稳定，跟随车辆的车间距误差曲线也不同步且误差比加密条件下的车间距误差增大，严重影响到网联车辆队列的安全性。

4　结束语

本文简要介绍了当前对车联网系统遭受网络攻击的两种处理方案，针对第一种传统方案需要先检测攻击再采取防御措施的繁琐性，第二种传统方案需要先加密传输，接收后再进行解密，对时间空间消耗较大且密钥仍然可能泄露等问题，本文基于 Paillier 加密算法的同态性，提出用 Paillier 同态加密算法对 CACC 车辆队列中前车传向后车的加速度进行加密后再传输的策略，以对抗潜在的网络攻击。将加密后的加速度密文直接应用到所设计的综合跟踪信号中，再将此综合跟踪信号应用到 MPC 控制器中。最后，通过 Matlab 仿真，对 Paillier 加密条件下的各项指标进行分析，并设计未使用加密算法的情况进行对比，验证所设计的方案可以使车辆队列稳定安全协同行驶。在本文的方法中，主要考虑在无线通信过程中传输的数据遭受网络攻击的情况，在以后的研究中，将进一步考虑前车的加密系统也受到攻击的情形。

参考文献：

[1] DEYK，YAN L，WANG X J，et al. A review of communication，driver characteristics，and controls aspects of cooperative adaptive cruise control（CACC）[J]. IEEE Transactions on Intelligent Transportation Systems，2016，17（2）：491－509.

[2] QIN Y Y，LI S Q. String stability analysis of mixed CACC vehicular flow with vehicle-to-vehicle communication [J]. IEEE Access，2020，8：174132－174141.

[3] WANG Z R，WU G Y，BARTH M J. A review on cooperative adaptive cruise control（CACC）systems：architectures，controls，and applications [C] //2018 21st International Conference on Intelligent Transportation Systems（ITSC）. Maui，HI，USA：IEEE，2018：2884－2891.

[4] AMOOZADEH M，RAGHURAMU A，CHUAH C N，et al. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving [J]. IEEE Communications Magazine，2015，53（6）：126－132.

[5] SINGH P K，TABJUL G S，IMRAN M，et al. Impact of security attacks on cooperative driving use case：CACC platooning [C] //2018 IEEE Region 10 Conference. Jeju，Korea（South）：IEEE，2018：138－143.

[6] HEIJDEN R W D，LUKASEDER T，KARGL F. Analyzing attacks on cooperative adaptive cruise control（CACC）[C] //2017 IEEE Vehicular Networking Conference（VNC）. Turin，Italy：IEEE，2017：45－52.

[7] ALIPOUR-FANID A, DABAGHCHIAN M, ZENG K. Impact of jamming attacks on vehicular cooperative adaptive cruise control systems [J]. IEEE Transactions on Vehicular Technology, 2020, 69 (11): 12679 - 12693.

[8] SARDESAI S, ULYBYSHEV D, OTHMANE L B, et al. Impacts of security attacks on the effectiveness of collaborative adaptive cruise control mechanism [C] //2018 IEEE International Smart Cities Conference (IS-C2). Kansas City, MO, USA: IEEE, 2018: 1 - 5.

[9] HASHEM EIZA M, NI Q. Driving with sharks: rethinking connected vehicles with vehicle cybersecurity [J]. IEEE Vehicular Technology Magazine, 2017, 12 (2): 45 - 51.

[10] DONG C Y, WANG H, NI D H, et al. Impact evaluation of cyber-attacks on traffic flow of connected and automated vehicles [J]. IEEE Access, 2020, 8: 86824 - 86835.

[11] ALOTIBI F, ABDELHAKIM M. Anomaly detection for cooperative adaptive cruise control in autonomous vehicles using statistical learning and Kinematic model [J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22 (6): 3468 - 3478.

[12] KO B, SON S H. An approach to detecting malicious information attacks for platoon safety [J]. IEEE Access, 2021, 9: 101289 - 101299.

[13] KEIJZER T, FERRARI R M G. Detection of network and sensor cyber-attacks in platoons of cooperative autonomous vehicles: a sliding-mode observer approach [C] //2021 European Control Conference (ECC), Delft, Netherlands: IEEE, 2021: 515 - 520.

[14] 王芳芳. 分布式网络异常攻击检测模型仿真分析 [J]. 计算机测量与控制, 2016, 24 (10): 61 - 63.

[15] YAMAMOTO Y, KUZE N, USHIO T. Attack detection and defense system using an unknown input observer for cooperative adaptive cruise control systems [J]. IEEE Access, 2021, 9: 148810 - 148820.

[16] PATOUNAS G, ZHANG Y, GJESSING S. Evaluating defence schemes against jamming in vehicle platoon networks [C] //2015 IEEE 18th International Conference on Intelligent Transportation Systems, Gran Canaria, Spain: IEEE, 2015: 2153 - 2158.

[17] BAI S H, ZHANG Z. Anonymous identity authentication scheme for internet of vehicles based on moving target defense [C] //2021 International Conference on Advanced Computing and Endogenous Security, Nanjing, IEEE, 2022: 1 - 4.

[18] YAMAMOTO Y, KUZE N, USHIO T. Attack detection and defense system using an unknown input observer for cooperative adaptive cruise control systems [J]. IEEE Access, 2021, 9: 148810 - 148820.

[19] PIAO J H, WANG Z L, WU Y J, et al. In-vehicle flexray network security based on modified AES encryption algorithm [C] //The 2nd International Conference on Distributed Sensing and Intelligent Systems (ICDSIS 2021), OnlineConference: IEEE, 2021: 17 - 27.

[20] MURAD S, KHAN A, SHIAELES S, et al. Data encryption and fragmentation in autonomous vehicles using raspberry Pi 3 [C] //2019 IEEE World Congress on Services (SER-VICES), Milan, Italy: IEEE, 2019: 212 - 216.

[21] HONG Z, WEN J Y, CUI J, et al. Efficient conditional privacy-preserving and authentication scheme for secure service provision in VANET [J]. Tsinghua Science and Technology, 2016, 21: 620 - 629.

[22] NEMA M, STALIN S, TIWARI R. RSA algorithm based encryption on secure intelligent traffic system for VANET using Wi-Fi IEEE 802.11p [C] //2015 International Conference on Computer, Communication and Control (I-C4), Indore, India, 2015: 1 - 5.

[23] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes [C] //International Conference on the Theory and Applications of Cryptographic Techniques. Berlin Heidelberg: Springer-Verlag, 1999: 223 - 238.

[24] SRIDOKMAI T, PRAKANCHAROEN S. The homomorphic other property of Paillier cryptosystem [C] //2015 International Conference on Science and Technology (TICST), Pathum Thani, Thailand, 2015: 356 - 359.

[25] MOHAMMED S J, TAHA D B. Performance evaluation of RSA, ElGamal, and Paillier partial homomorphic encryption algorithms [C] //2022 International Conference on Computer Science and Software Engineering (CSASE), Duhok, Iraq, 2022: 89 - 94.

[26] TAO Y T, KONG F Y, YU J, et al. Modification and performance improvement of Paillier homomorphic cryptosystem [C] //2021 IEEE 19th International Conference on Embedded and Ubiquitous Computing (EUC), Shenyang, China, 2021: 131 - 136.

[27] VAN NUNEN E, VERHAEGH J, SILVAS E, et al. Robust model predictive cooperative adaptive cruise control subject to V2V impairments [C] //2017 IEEE 20th International Conference on Intelligent Transportation Systems (ITSC), Yokohama, Japan, 2017: 1 - 8.

[28] ALOTIBI F, ABDELHAKIM M. Anomaly detection in cooperativeadaptive cruise control using physics laws and data fusion [C] //2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), Honolulu, HI, USA, 2019: 1 - 7.

[29] HE Y, WU M AND SHE J H. Improved bounded-real-lemma representation and H/sub/spl infin. control of systems with polytopic uncertainties [J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2005, 52 (7): 380 - 383.

[30] LE F, WANG J L, POH E, et al. Multiobjective robust model predictive control: trajectory tracking problem through LMI formulation [C] //2007American Control Conference, New York, 2007: 5589 - 5594.