doi:10.3772/j.issn.1002-0470.2021.03.004

虚假数据注入攻击下网联车辆自适应巡航状态安全估计①

宋秀兰② 漏小鑫 孟利民 何德峰

(浙江工业大学信息工程学院 杭州 310023)

摘 要 考虑网联车辆自适应巡航控制系统中的无线监控网络受到虚假数据注入攻击下的车辆状态估计问题,提出了一种状态估计方法重构网联车辆系统中的车辆状态。首先建立自适应巡航控制系统模型和无线监控网络中的虚假数据注入攻击模型;再根据车辆巡航状态被损坏的数据,利用压缩感知原理,将网联车辆巡航状态安全估计问题描述为 L_1 范数优化问题;进而根据 S 稀疏性重构网联车辆自适应巡航状态;最后,通过典型车辆自适应巡航场景仿真验证该方法的有效性。

关键词 网联车辆;自适应巡航控制;网络攻击;状态估计

0 引 言

随着城市车辆保有量的急剧增加,安全、拥堵和尾气排放等交通问题日益严峻[1-2]。由于智能交通系统能有效提高道路吞吐量,减少环境污染和提高交通安全,近年来备受关注。作为智能交通系统重要组成部分的智能网联车辆,可以有效地降低交通事故并提高道路通行率[3]。但由于网联车辆中车与车、车与人、车与路所处的开放移动无线网络容易受到恶意的网络攻击[4],如虚假数据注入网络攻击等,可能造成严重的安全事故。因此,有必要在智能网联车辆的监控平台实现车辆巡航状态的安全估计。

智能网联车辆内部包含了车载传感器、控制器、执行器等装置,融合了现代通信与网络技术,能够实现车与 X(车、路、人、云等)的智能信息交换,能够感知周边复杂环境即时做出智能决策,帮助驾驶人员达成对智能网联汽车自身的协同控制,并最终可替代人实现“安全、高效、舒适、节能”的自动化智能驾驶[4]。然而无线网络通信也存在一些固有的缺点,如网络时延、通信丢包等问题,甚至由于无线网络的开放性,存在被人为攻击的可能[5-9]。在过去十年里,研究人员对无线网络控制相关课题进行了深入研究,从而设计出了可以容忍网络缺陷(如丢包、时延等)的控制方法[10-12]。例如文献[13]考虑了通信时延,在此基础上分析了智能网联车辆系统的稳定性。

近年来,智能网联车辆信息安全问题日益凸显,如在2015年7月,“白帽黑客”查理米勒和克里斯瓦拉塞克演示了如何通过入侵克莱斯勒公司 Uconnect 车载系统,以远程指令方式“劫持”正在行驶中的 Jeep 自由光,并最终导致其“翻车”[4]。这使得国内外学者开始关注网联车辆系统中的网络攻击检测问题。文献[14]提出一种用于检测智能网联车辆遭受拒绝服务攻击(denial of service, DoS)的方法,并能较准确估计 DoS 攻击产生的延时。文献[15]研究了传感器被篡改的影响,这会严重影响车辆系统的弦稳定性。此外,文献[16]研究了攻击者入侵车辆的能力,证明了攻击者能够控制车辆的个体位置和速度。

近年来,由于网络攻击对人身财产安全的重大

① 国家自然科学基金(61803336)资助项目。

② 女,1982年生,博士,讲师;研究方向:车联网系统安全与控制;联系人,E-mail: songxl2008@zjut.edu.cn

(收稿日期:2020-03-19)

威胁，越来越多的学者研究网络攻击下车辆的安全问题。例如，文献[17,18]分析虚假数据注入攻击检测方法，即残差检验，对于每一个测量值均存在一个残差信号，当残差值大于给定阈值时，则认为该测量值被攻击。但当攻击者通过设置一些特殊数据使残差仍小于阈值时，该方法则无法很好地应用于智能网联车辆的攻击检测。文献[19]考虑了无线信道受到干扰时，将扰动视作一定的随机过程，并分析网络系统的控制和估计问题。文献[20]设计了一个类龙伯格观测器，并使用一种新的投影算子方法从一系列连续测量值中重构状态。文献[21]提出了滑模观测器方法用于从被污染的传感器测量数据中估计系统状态。文献[22,23]假定状态攻击在满足稀疏性的前提下，提出了利用 L_1 范数优化问题对状态进行重构。

本文针对无线监控网络受到虚假数据注入攻击下的网联车辆系统状态估计问题，提出一种状态估计方法重构车辆状态。该方法利用压缩感知中的稀疏性，当被攻击传感器少于传感器数量一半时，可将攻击向量视作稀疏向量并转化为 L_1 范数优化问题进行状态重构。最后通过仿真实验验证该方法可以有效地重构车辆系统状态，以及存在噪声情况下仍能保证算法的有效性。

1　问题描述

对于智能网联车辆系统来说，底层车辆自适应巡航控制系统需要无线监控网络来实时监控，同时根据监控结果会有路径规划器来规划车辆路线。但由于无线网络的开放性，实时运行中的车辆在传输数据到监控端时可能会存在数据攻击的情况。针对该问题，本节分析并给出网联车辆自适应巡航控制系统模型和网络攻击模型。

1.1　网联车辆自适应巡航控制系统模型

考虑网联车辆自适应巡航系统使用前继跟随(predecessor-following, PF)通信拓扑，将两车相连组成两车模型，如图 1 所示。其中每辆车都装备车载雷达用于检测前后车的相对距离与相对速度，并且每辆车还通过专用短程通信技术(dedicated short range communications, DSRC)获取前车加速度信息，利用这些信息来实施控制。

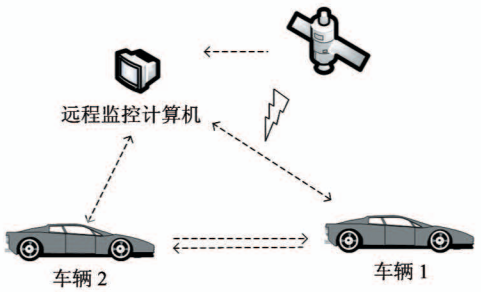

图 1　监控层攻击模型

考虑网联车辆自适应巡航系统，采用固定间距安全策略，即两车安全间距为 $\delta_d>0$。两车间的绝对位置、速度以及加速度由 z_i、v_i 和 a_i 表示，其中 $i=0,1$，$i=0$ 表示领导车，$i=1$ 表示本车。在该车辆队列中，后车通过 DSRC 获取前车加速度信息对本车进行控制。根据牛顿第二定律，考虑相邻两车的速度差与加速度差：

$$\begin{aligned}\dot{\delta}(t) &= v_0(t)-v_1(t)\\ \ddot{\delta}(t) &= a_0(t)-a_1(t)\end{aligned} \tag{1}$$

其中，时间 $t>0$，$\delta=z_0-z_1-L-\delta_d$ 表示两车间距与设定的安全跟车距离的误差，其中 z_0-z_1-L 表示由雷达测得的两车间距，δ_d 为设定的安全跟车距离，L 为后车车身长度。

假定车辆节气门与制动踏板具有理想的性能，自车的纵向加速度可表示为

$$a_1(t)=-\dot{a}_1(t)/\zeta_1+u_1(t)/\zeta_1 \tag{2}$$

其中，ζ_1 表示车辆内部执行器动力学参数，$u_1(t)$ 表示后车的理想加速度。

本文选取 $\boldsymbol{x}=[\delta\ \ \dot{\delta}\ \ \ddot{\delta}]^{\mathrm{T}}$ 作为状态变量，再结合式(1)和式(2)，可得三阶状态空间模型：

$$\dot{\boldsymbol{x}}(t)=\bar{\boldsymbol{A}}\boldsymbol{x}(t)+\bar{\boldsymbol{B}}u_1(t) \tag{3}$$

其中相应矩阵为

$$\bar{\boldsymbol{A}}=\begin{bmatrix}0 & 1 & 0\\ 0 & 0 & 1\\ 0 & 0 & -1/\zeta_1\end{bmatrix},\ \bar{\boldsymbol{B}}=\begin{bmatrix}0\\ 0\\ 1/\zeta_1\end{bmatrix}$$

同时，本车通过雷达获取两车间距和两车速度差以及通过 DSRC 来获取前车加速度信息，自身的

加速度传感器可以得到本车的加速度信息,并利用上述相关状态变量来实现车辆的控制。状态变量输出如下:

$$\boldsymbol{y}(t) = \boldsymbol{C}\boldsymbol{x}(t) \tag{4}$$

其中,矩阵 $\boldsymbol{C}$ 为三阶单位阵,本文不考虑信道衰减和数据包丢失情况。

将该网联车辆自适应巡航控制系统模型以采样间隔 T_s 离散化后得到的三阶离散状态空间模型表示如下:

$$\boldsymbol{x}(k+1) = \hat{\boldsymbol{A}}\boldsymbol{x}(k) + \boldsymbol{B}u_1(k) \tag{5}$$

其中 k 表示采样时刻,相关矩阵形式如下:

$$\hat{\boldsymbol{A}} = \begin{bmatrix} 1 & T_s & 0 \\ 0 & 1 & T_s \\ 0 & 0 & 1 - T_s/\zeta_1 \end{bmatrix}, \boldsymbol{B} = \begin{bmatrix} 0 \\ 0 \\ T_s/\zeta_1 \end{bmatrix}$$

对于上述模型,本文采用状态反馈控制器 $\boldsymbol{u}_1(k) = -\boldsymbol{K}\boldsymbol{x}(k)$,使该网联车辆系统形成闭环系统:

$$\boldsymbol{x}(k+1) = \boldsymbol{A}\boldsymbol{x}(k) \tag{6}$$

其中,闭环系统矩阵 $\boldsymbol{A} = \hat{\boldsymbol{A}} - \boldsymbol{B}\boldsymbol{K}$。

1.2 虚假数据注入攻击模型

本文考虑在网联车辆与监控层之间的相关网络受到攻击,如图 1 所示。在数据传输过程中,监控层所需的网联车辆系统相关运行数据可能会被非法分子恶意篡改,影响监控层的正常工作。常见的网络攻击有多种,如拒绝服务攻击、干扰攻击、虚假数据注入攻击等[14-16]。

本文主要考虑虚假数据注入攻击,即攻击者通过截取传输的数据包并修改其中的有效负载,并将修改后的数据包发送给监控层,就会导致监控层对车辆实时运行情况做出错误判断,从而影响监控层的正常运行。

现有研究表明[22-23],只有当传感器被攻击数量小于一半时才可以利用相邻观测值的相关性实现状态安全估计,反之则无法重构状态。因此本文假设每个时刻发送的车辆三个巡航状态信息中只有一个可能被虚假数据注入攻击。由于攻击者受到自身经济实力的限制,并不可能截取到网络中负载相关数据的所有数据包,即如果攻击者有能力获取所有数据包并任意篡改,其可以向监控端模拟任意车辆行驶场景而不被监控端发现。进一步,在任意时刻只改变其中部分数据,使得网络攻击更具隐蔽性,从而导致监控端难以觉察到网络攻击的发生。

考虑网联车辆系统发送两车间距、两车速度差和加速度差等信息到无线监控网络。显然当无线网络中不存在虚假数据注入攻击时,监控层接收到的实际车辆运行数据如式(4)所示。因此对于监控层来说观测矩阵仍是三阶单位阵。但当无线网络中发生虚假数据注入攻击时,监控层接收到的数据 $\boldsymbol{y}(k)$ 中会有部分状态量被攻击。

考虑对于发往无线监控网络的数据,向其中某个数据加入一个未知值表示该数据受到攻击,其攻击模型描述如下:

$$\boldsymbol{y}(k) = \boldsymbol{C}\boldsymbol{x}(k) + \boldsymbol{\Gamma}\boldsymbol{e}(k) \tag{7}$$

式中,$\boldsymbol{\Gamma} = \mathrm{diag}(\lambda_1, \cdots, \lambda_3)$ 代表相应的攻击选择矩阵,当 $\lambda_i = 1$ 时代表第 i 个车辆信息遭受虚假数据注入攻击;否则 $\lambda_i = 0$。每一时刻 i 的数值未知,即并不知道某一时刻哪个系统状态量被攻击,$\boldsymbol{e}(k)$ 表示的是由攻击者向车辆状态信息中加入的变量,代表攻击强度。

2 车辆巡航状态重构

考虑上文描述的网联车辆虚假数据注入攻击状态重构问题,首先利用连续 M 个时刻监控层接收到的被攻击的状态观测值 $\boldsymbol{y}(k)$,其中 $k = 0, \cdots, M-1$,将其纵向排列为

$$\bar{\boldsymbol{Y}} = \begin{bmatrix} \boldsymbol{y}(0) \\ \boldsymbol{y}(1) \\ \vdots \\ \boldsymbol{y}(M-1) \end{bmatrix} = \begin{bmatrix} \boldsymbol{C}\boldsymbol{x}(0) + \boldsymbol{\Gamma}_1\boldsymbol{e}(0) \\ \boldsymbol{C}\boldsymbol{A}\boldsymbol{x}(0) + \boldsymbol{\Gamma}_2\boldsymbol{e}(1) \\ \vdots \\ \boldsymbol{C}\boldsymbol{A}^{M-1}\boldsymbol{x}(0) + \boldsymbol{\Gamma}_{M-1}\boldsymbol{e}(M-1) \end{bmatrix}$$

$$= \boldsymbol{\Phi}_1\boldsymbol{x}(0) + \boldsymbol{E}_1 \tag{8}$$

其中,

$$\boldsymbol{\Phi}_1 = [\boldsymbol{C} \quad \boldsymbol{C}\boldsymbol{A} \quad \cdots \quad \boldsymbol{C}\boldsymbol{A}^{M-1}]^{\mathrm{T}}$$

$$\boldsymbol{E}_1 = \begin{bmatrix} \boldsymbol{\Gamma}_0 & & & \\ & \boldsymbol{\Gamma}_1 & & \\ & & \ddots & \\ & & & \boldsymbol{\Gamma}_{M-1} \end{bmatrix} \begin{bmatrix} \boldsymbol{e}(0) \\ \boldsymbol{e}(1) \\ \vdots \\ \boldsymbol{e}(M-1) \end{bmatrix}$$

$\boldsymbol{\Gamma}_i$ 为式(7)描述的攻击选择矩阵($i = 0, \cdots, M-1$),$\boldsymbol{\Phi}_1$ 和 $\boldsymbol{E}_1 \in R^{3M\times 3}$,$M$ 表示观测值的数量。

本文需要根据式(8)估计出车辆状态的初始值 $\boldsymbol{x}(0)$。为了求解该问题,引入如下压缩感知定理[24]:

$$\min_{\boldsymbol{x}} \| \boldsymbol{x} \|_0 \quad \text{subject to } \boldsymbol{b} = \boldsymbol{P}\boldsymbol{x} \tag{9}$$

其中,$\boldsymbol{b} \in R^m$ 是观测向量,$\boldsymbol{P} \in R^{m \times n}$ 为传感矩阵,$\boldsymbol{x} \in R^n$ 为状态向量,同时向量 $\boldsymbol{x}$ 是稀疏向量。根据文献[24],如果式(9)的稀疏解 $\boldsymbol{x}$ 满足 $\| \boldsymbol{x} \|_0 = q$, $m \geqslant 2q$,且 $\boldsymbol{P}$ 的任意 $2q$ 行满秩,则式(9)的解唯一。

证明　利用反证法证明,如果存在两个不同解 $\boldsymbol{x}_1, \boldsymbol{x}_2$ 满足条件,则 $\boldsymbol{b} = \boldsymbol{P}\boldsymbol{x}_1, \boldsymbol{b} = \boldsymbol{P}\boldsymbol{x}_2$。相减可得 $\boldsymbol{P}(\boldsymbol{x}_1 - \boldsymbol{x}_2) = 0$。由于 $\boldsymbol{x}_1, \boldsymbol{x}_2$ 不同,因此 $\| \boldsymbol{x}_1 - \boldsymbol{x}_2 \|_0$ 最大为 $2q$,由于 $\boldsymbol{P}$ 的任意 $2q$ 行满秩,因此 $\boldsymbol{P}(\boldsymbol{x}_1 - \boldsymbol{x}_2) \neq 0$,与 $\boldsymbol{P}(\boldsymbol{x}_1 - \boldsymbol{x}_2) = 0$ 矛盾。因此,式(9)成立。

要利用压缩感知问题求解式(8)的状态估计问题,首先需要确定合适的 M。根据文献[23]结论,当系统被攻击的传感器固定时,M 的取值为系统状态变量个数;而当被攻击传感器可变时,M 的取值在部分情况下会大于系统状态变量个数,经仿真验证,在该车辆系统中 M 取 3 即可满足状态重构。因此将 $M = 3$ 代入式(8),即将 3 个时刻的车辆状态量数据竖直排列,可得如下等式:

$$\begin{aligned} \boldsymbol{Y} &= \begin{bmatrix} \boldsymbol{y}(0) \\ \boldsymbol{y}(1) \\ \boldsymbol{y}(2) \end{bmatrix} = \begin{bmatrix} \boldsymbol{C}\boldsymbol{x}(0) + \boldsymbol{\Gamma}\boldsymbol{e}(0) \\ \boldsymbol{C}\boldsymbol{A}\boldsymbol{x}(0) + \boldsymbol{\Gamma}\boldsymbol{e}(1) \\ \boldsymbol{C}\boldsymbol{A}^2\boldsymbol{x}(0) + \boldsymbol{\Gamma}\boldsymbol{e}(2) \end{bmatrix} \\ &= \boldsymbol{\Phi}\boldsymbol{x}(0) + \boldsymbol{E} \end{aligned} \tag{10}$$

其中,矩阵 $\boldsymbol{E}$ 表示 3 个时刻对车辆状态的攻击值,同时如果车辆的大部分状态量都可以被攻击,则显然无法重构车辆状态,因为这时候攻击者可以模拟任意攻击场景来欺骗无线监控网络。因此本文假设每个时刻车辆被攻击状态量不超过车辆总状态量的一半,即符合攻击矩阵 $\boldsymbol{E}$ 为稀疏向量。且相应矩阵如下

$$\boldsymbol{\Phi} = \begin{bmatrix} \boldsymbol{C} \\ \boldsymbol{C}\boldsymbol{A} \\ \boldsymbol{C}\boldsymbol{A}^2 \end{bmatrix} \quad \boldsymbol{E} = \begin{bmatrix} \boldsymbol{\Gamma}_0 & & \\ & \boldsymbol{\Gamma}_1 & \\ & & \boldsymbol{\Gamma}_2 \end{bmatrix} \begin{bmatrix} \boldsymbol{e}(0) \\ \boldsymbol{e}(1) \\ \boldsymbol{e}(2) \end{bmatrix}$$

采取先估计攻击向量 $\boldsymbol{E}$,然后再根据估计的攻击向量 $\hat{\boldsymbol{E}}$ 估计 $\boldsymbol{x}(0)$ 的方法,先对矩阵 $\boldsymbol{\Phi}$ 进行正交三角(QR)分解,可得:

$$\boldsymbol{\Phi} = [\boldsymbol{Q}_1 \quad \boldsymbol{Q}_2][\boldsymbol{R}_1 \quad 0]^{\mathrm{T}} \tag{11}$$

其中,$[\boldsymbol{Q}_1 \quad \boldsymbol{Q}_2]$ 为正交矩阵,且 $\boldsymbol{Q}_1 \in R^{9 \times 3}, \boldsymbol{Q}_2 \in R^{9 \times 6}$,并且 $\boldsymbol{R}_1 \in R^{3 \times 3}$ 为满秩的上三角矩阵。将式(11)代入式(10),整理后可得:

$$\boldsymbol{Y} = [\boldsymbol{Q}_1 \quad \boldsymbol{Q}_2][\boldsymbol{R}_1 \quad 0]^{\mathrm{T}} \boldsymbol{x}(0) + \boldsymbol{E} \tag{12}$$

式(12)左右同乘 $[\boldsymbol{Q}_1 \quad \boldsymbol{Q}_2]^{\mathrm{T}}$,由于 $[\boldsymbol{Q}_1 \quad \boldsymbol{Q}_2]$ 是正交矩阵,通过化简可得

$$\begin{bmatrix} \boldsymbol{Q}_1^{\mathrm{T}} \\ \boldsymbol{Q}_2^{\mathrm{T}} \end{bmatrix} \boldsymbol{Y} = \begin{bmatrix} \boldsymbol{R}_1 \\ 0 \end{bmatrix} \boldsymbol{x}(0) + \begin{bmatrix} \boldsymbol{Q}_1^{\mathrm{T}} \\ \boldsymbol{Q}_2^{\mathrm{T}} \end{bmatrix} \boldsymbol{E} \tag{13}$$

将式(13)上下分离以达到先估计攻击向量再估计初始状态量的目的,即

$$\boldsymbol{Q}_1^{\mathrm{T}} \boldsymbol{Y} = \boldsymbol{R}_1 \boldsymbol{x}(0) + \boldsymbol{Q}_1^{\mathrm{T}} \boldsymbol{E} \tag{14}$$

$$\boldsymbol{Q}_2^{\mathrm{T}} \boldsymbol{Y} = \boldsymbol{Q}_2^{\mathrm{T}} \boldsymbol{E} \tag{15}$$

对于式(15),可以采取式(9)描述的压缩感知方法重构攻击向量 $\boldsymbol{E}$。如上文所述,本文假设每个时刻被攻击的状态量个数为 1,以满足式(9)中保证解唯一的条件。因为如果车辆状态被攻击状态量大于 1,则式(9)中 $q > 1$,同时由于本文讨论的网联车辆系统中观测值个数为 3,所以 $m = 3$,因此 $m < 2q$,与式(9)所需解唯一的条件矛盾。因此如果被攻击状态量为 1 则满足该条件,借助压缩感知原理,便可以求出式(15)的唯一解,即车辆攻击向量 $\boldsymbol{E}$。

接下来采用式(9)描述的压缩感知原理先估计攻击向量 $\boldsymbol{E}$,如下:

$$\hat{\boldsymbol{E}} = \min_{\boldsymbol{E}} \| \hat{\boldsymbol{E}} \|_{L_0} \quad \text{s.t. } \boldsymbol{Q}_2^{\mathrm{T}} \boldsymbol{Y} = \boldsymbol{Q}_2^{\mathrm{T}} \hat{\boldsymbol{E}} \tag{16}$$

在式(16)中,由于在求解攻击向量 $\boldsymbol{E}$ 的过程中,采用了 L_0 范数,而众所周知,由于 NP 难问题的存在,L_0 范数问题很难优化求解,对于计算压力负担很大。考虑到 L_1 范数是 L_0 范数的最优凸近似,因此将 L_0 范数转化成 L_1 范数求解,可减轻计算负担。L_1 优化问题定义如下:

$$\hat{\boldsymbol{E}} = \min_{\boldsymbol{E}} \| \hat{\boldsymbol{E}} \|_{L_0} \quad \text{s.t. } \boldsymbol{Q}_2^{\mathrm{T}} \boldsymbol{Y} = \boldsymbol{Q}_2^{\mathrm{T}} \hat{\boldsymbol{E}} \tag{17}$$

计算式(17)后可以获得攻击向量的估计值 $\hat{\boldsymbol{E}}$,同时由于压缩感知理论的证明,可以知道该估计值趋近于真实的攻击向量 $\boldsymbol{E}$。因此将攻击向量估计值代入式(14),化简可得初始状态向量的估计值

$$\boldsymbol{x}(0) = \boldsymbol{R}_1^{-1} \boldsymbol{Q}_1^{\mathrm{T}} (\boldsymbol{Y} - \hat{\boldsymbol{E}}) \tag{18}$$

由于矩阵 $\boldsymbol{R}_1$ 是上三角矩阵,且满秩,因此可以直接求逆运算。同时由于攻击向量的估计值 $\hat{\boldsymbol{E}}$ 唯

一,所以估计的初始状态 $\boldsymbol{x}(0)$ 也是唯一的,即趋近于真实的网联车辆自适应巡航状态。

3 仿真与分析

考虑两车在直道上纵向行驶,每辆车上都装有巡航控制器,并且远程监控层通过无线网络获得实际运行过程中车辆的相关状态信息(如图 1 所示)。在信号传输过程中存在虚假数据注入攻击,车辆状态信息可能会被篡改。仿真中,车辆参数设置如下:车身长 $L=4$ m, 后车车辆执行器参数 $\zeta=0.25$ s,由于本车只需要前车加速度信息,因此不需要前车执行器参数,车辆安全间距 $\delta_d=2$ m,且本文采用文献[9]设计网联车辆自适应巡航控制器增益 $\boldsymbol{K}=-[0.2293, 0.8056, 0.2825]$。对于无线网络,信道增益矩阵为三阶单位阵。后车通过传感器和无线网络获得前车相关信息对本车进行控制,同时利用无线通信将对应车辆状态信息传送给网络监控层,并且在通信过程中遭受虚假数据注入攻击。

假设攻击者为了扰乱无线监控网络的正常监控,随机在每一时刻捕捉到的数据包中修改其中的有效负载。因此仿真场景设置如下,每一时刻随机攻击速度或加速度,攻击幅值如图 2 所示。

图 2 和图 3 中的实线表示车辆间的实际相对速度与相对加速度,虚线则表示受到随机假数据注入攻击后的相对速度与相对加速度,这些数据都是无线监控网络对实际车辆运动的还原。若是无线网络中不存在人为攻击,则实线代表无线监控网络还原的实际交通场景。而受到攻击后,虚线则代表无线监控网络接收到的车辆间被攻击的相对速度。与黑色实线代表的真实值存在一定的偏差。如果无线监控网络接收到的为被攻击的值,即虚线所示状态,则会影响其正常工作。

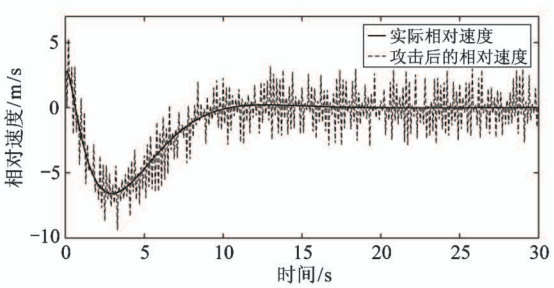

图 2 攻击后与实际的相对速度对比

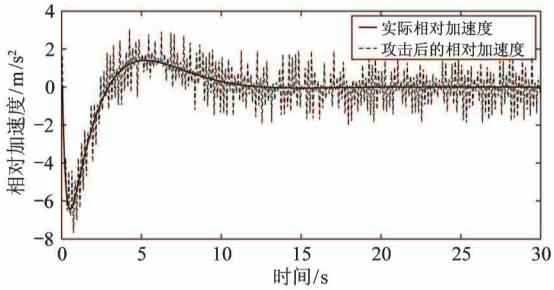

图 3 攻击后与实际的相对加速度对比

由图 2 和图 3 可知,对相对速度与相对加速度均注入随机型虚假数据攻击(攻击幅值均值不为 0),其中,虚线表示被攻击后的值,实线表示正常值,同时每一时刻只攻击一个观测值。设置前后两车初始间距为 30 m,前车以 50 km/h 的速度匀速运行,后车初始速度为 40 km/h。状态重构后的车辆状态值如图 4 ~ 图 6 所示。

由图 5 可见,在 0 ~ 10 s 时由于后车速度小于前车同时两车间距大于安全跟车距离,所以后车需要加速追赶前车。而在 10 ~ 20 s 左右由于跟车距离小于安全跟车距离,所以后车减速,20 s 后两车达到稳定跟车。

利用状态重构算法重构初始状态,实验使用的观测值数量为3,重构后的车辆系统状态值与实际

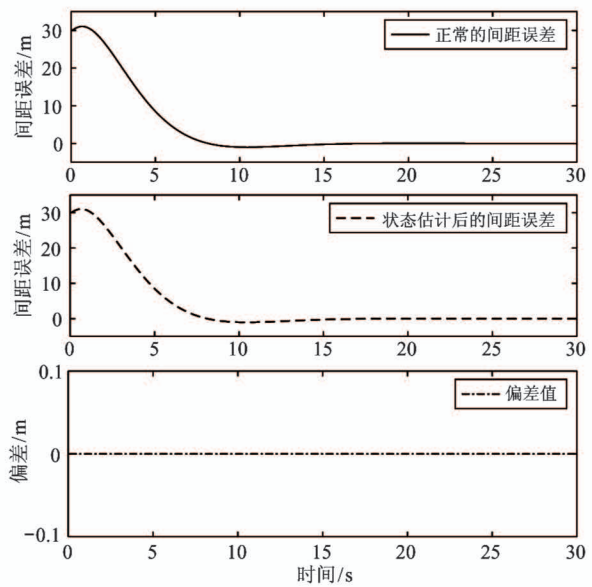

图 4 间距误差

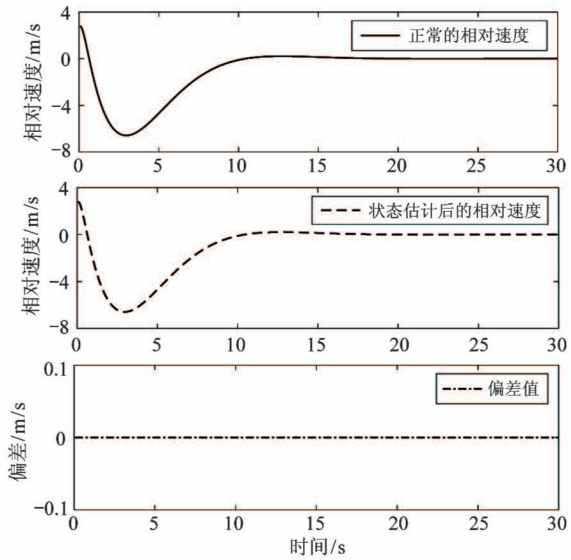

图 5　相对速度

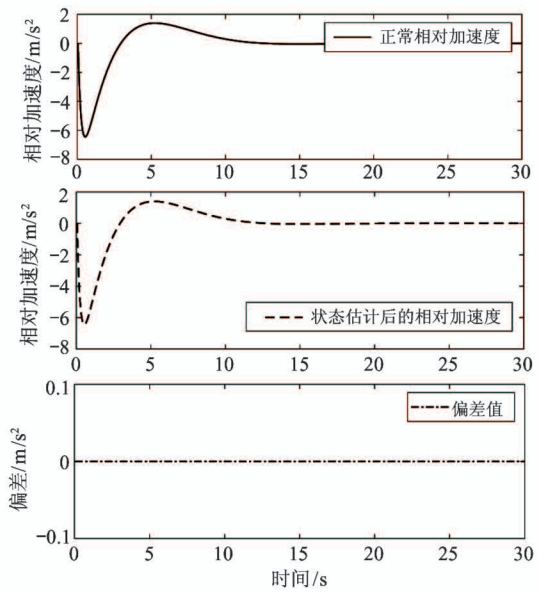

图 6　相对加速度

值对比如图 4 ~ 图 6 所示，其中，图中的第 1 子图表示正常状态，第 2 子图为状态估计后的状态。可以从图中的第 3 子图看出，状态重构后的值与实际值基本重合（偏差值均为 0）。由此可知该状态重构方法可以精确重构车辆状态信息。

上述仿真实验在无噪声环境下运行，这与实际场景不符，为了确保该算法对于噪声有一定的鲁棒性，接下来在车辆巡航控制系统中加入噪声验证算法的适用性。

本次实验仿真参数设置与上次仿真相同，同时在自适应巡航系统中加入了过程噪声以及测量噪声，两者均为高斯白噪声，且协方差矩阵分别为 $\mathrm{diag}\{0.01,0.01,0.01\}$，$\mathrm{diag}\{0.16,0.16,0.16\}$，而数据发往监控端受到的攻击如图 2 和图 3 所示。为此，先用卡尔曼滤波方法逼近车辆的实际状态量。由于观测值受到了人为攻击，将攻击视作一部分噪声后，实际噪声 $\tilde{v}=v+e$，其中 v 为测量噪声，e 为攻击值。而显然人为攻击很难建模为高斯白噪声。因此利用式(17)计算出的攻击值 $\hat{E}$，令 $\tilde{e}=\hat{E}(6:9)$，$\tilde{v}-\tilde{e}$ 可近似看作 0 均值高斯白噪声，从而利用卡尔曼滤波，可利用观测值逼近系统实际值，结果如图 7 ~ 图 9 所示。

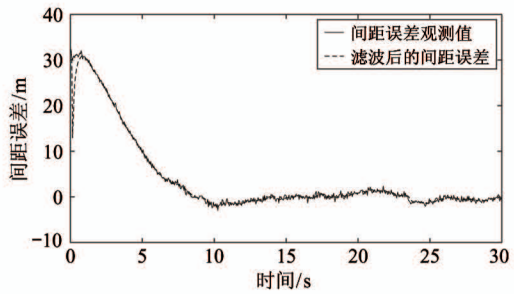

图 7　间距误差

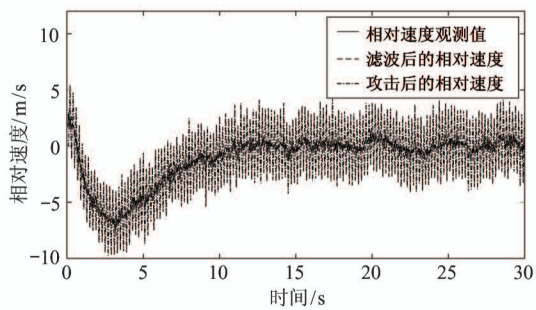

图 8　相对速度

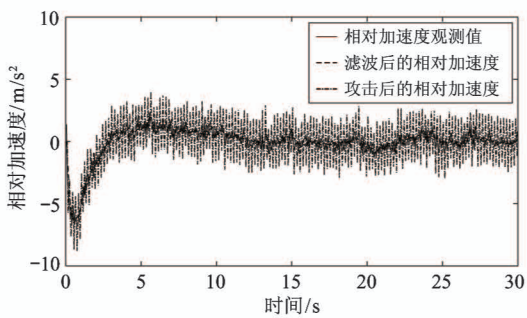

图 9　相对加速度

图 7 ~ 图 9 中，实线代表了车辆的实际状态观

测值,而点划线则表示被攻击者攻击后的车辆状态,虚线则表示结合卡尔曼滤波和本文算法重构后的车辆状态。图中车辆状态观测值与滤波后的车辆状态值更接近,即在网络攻击存在的情况下,利用被攻击的车辆状态值,结合卡尔曼滤波和本文算法,可以使得重构后的状态接近车辆状态的观测值。由此可知结合卡尔曼滤波和本文算法后可以更精确地重构车辆真实状态。

仿真结果表明,联合本文算法和卡尔曼滤波可以令监控端获取相对准确的网联车辆自适应巡航系统的状态,同时验证了本文算法对过程噪声和观测噪声具有一定的鲁棒性。

4 结 论

本文考虑了连接自适应巡航系统和无线监控网络的无线信道受到虚假数据注入攻击的情况,并提出了状态重构方法重构车辆初始状态。仿真结果验证了该算法的有效性。在后续研究中,将进一步考虑在车辆系统中存在较大噪声的情况下如何继续保证算法的有效性,并且在执行器受到攻击的情况下如何对受污染的数据进行重构。

参考文献

[1] Milanés V, Shladover S E. Modeling cooperative and autonomous adaptive cruise control dynamic responses using experimental data[J]. *Transportation Research Part C*, 2014, 48: 285-300

[2] Jia D, Lu K, Wang J, et al. A survey on platoon-based vehicular cyber-physical systems[J]. *IEEE Communications Surveys and Tutorials*, 2016, 18(1): 263-284

[3] Willke T L, Tientrakool P, Maxemchuk N F, et al. A survey of inter-vehicle communication protocols and their applications[J]. *IEEE Communications Surveys and Tutorials*, 2009, 11(2): 3-20

[4] 李骏. 智能网联汽车信息安全白皮书[S]. 北京:中国汽车工程学会北京航空航天大学梆梆安全研究院, 2016

[5] Yang X, Liu L, Vaidya N H, et al. A vehicle-to-vehicle communication protocol for cooperative collision warning [C]//International Conference on Mobile and Ubiquitous Systems, Boston, USA, 2004: 22-25

[6] Larson U E, Nilsson D K. A roadmap for securing vehicles against cyber attacks[C]//NITRD National Workshop on High-confidence Automotive Cyber-physical Systems, Synopsys, Japan, 2008: 1

[7] Yin X, Ma X, Trivedi K S, et al. Performance and reliability evaluation of BSM broadcasting in DSRC with multi-channel schemes[J]. *IEEE Transactions on Computers*, 2014, 63(12): 3101-3113

[8] Qin W B, Gomez M M, Orosz G. Stability analysis of connected cruise control with stochastic delays[C]//2014 American Control Conference, Portland, USA, 2014: 4624-4629

[9] Song X L, Lou X X, Meng L M. Time-delay feedback cooperative adaptive cruise control of connected vehicles by heterogeneous channel transmission [J]. *Measurement and Control*, 2019(52): 369-378

[10] Ploeg J, Shukla D P, Nathan V D W, et. al. Controller synthesis for string stability of vehicle platoons[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2014, 15(2): 854-865

[11] Ploeg J, Nathan V D W, Nijmeijer H. L_p string stability of cascaded systems: application to vehicle platooning [J]. *IEEE Transactions on Control Systems Technology*, 2014, 22(2): 786-793

[12] Ploeg J, Elham S K, Guido L, et al. Graceful degradation of cooperative adaptive cruise control [J]. *IEEE Transactions on Intelligent Transportation Systems*, 2015, 16(1): 488-497

[13] Vugts R P A. String-Stable CACC Design and Experimental Validation[D]. Department Mechanical Engineering Control Systems Technology Group, Technische Universiteit Eindhoven, 2010

[14] Biron Z A, Dey S, Pisu P. Real-time detection and estimation of denial of service attack in connected vehicle systems[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2018, 19(12): 3893-3902

[15] 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

[16] Dadras S, Gerdes R M, Sharma R. Vehicular platooning in an adversarial environment[C]//ACM Symposium on

Information, Singapore, 2018: 167-178

[17] Massoumnia M A, Verghese G C, Willsky A S. Failure detection and identification[J]. *IEEE Transactions on Automatic Control*, 1989, 34(3): 316-321

[18] Blanke M, Kinnaert M, Lunze J. Fault diagnosis and fault-tolerant control[M]. New York: Springer, 2006

[19] Schenato L, Sinopoli B, Franceschetti M, et al. Foundations of control and estimation over lossy networks[J]. *Proceedings of the IEEE*, 2007, 95(1): 163-187

[20] Lu A Y, Yang G H. Secure luenberger-like observers for cyber-physical systems under sparse actuator and sensor attacks[J]. *Automatica*, 2018, 98: 124-129

[21] Wu C, Hu Z, Liu J, et al. Secure estimation for cyber-physical systems via sliding mode[J]. *IEEE Transactions on Cybernetics*, 2018, 48(12): 3420-3431

[22] Fawzi H, Tabuada P, Diggavi S. Secure estimation and control for cyber-physical systems under adversarial attacks[J]. *IEEE Transactions on Automatic Control*, 2014, 59(6): 1454-1467

[23] Hwan C Y, Qie H, Tomlin C J. Secure estimation based Kalman filter for cyber-physical systems against sensor attacks[J]. *Automatica*, 2018, 95: 399-412

[24] Candes E J, Tao T. Decoding by linear programming[J]. *IEEE Transactions on Information Theory*, 2005, 51(12): 4203-4215

Adaptive cruising state secure estimation of connected vehicles under false data injection attack

Song Xiulan, Lou Xiaoxin, Meng Limin, He Defeng

(College of Information Engineering, Zhejiang University of Technology, Hangzhou 310023)

Abstract

This paper considers the state estimation problem of the connected vehicles when the wireless monitoring network in the adaptive cruise control system of the connected vehicle is under the false data injection attack. A state secure estimation method is proposed to reconstruct the vehicle state in the connected vehicle system. First, the adaptive cruise control system model and the false injection attack model in the wireless monitoring network are established. Then, based on the corrupted data, the compressed sensing principle is used and the secure estimation problem of the connected vehicle cruise state is described as the L_1 norm optimization problem. Furthermore, the initial state of the connected vehicle's cruise state is reconstructed based on S-sparsity. Finally, the effectiveness of the algorithm is verified by simulation of typical vehicle cruise scenarios.

Key words: connected vehicle, adaptive cruise control, cyber attack, state estimation