基于博弈论的信息物理融合系统安全控制

庞 岩[1] 王 娜[2] 夏 浩[3]

摘 要 对于远程复杂的操控系统, 信息物理融合系统 (Cyber-physical system, CPS) 主要依靠无线网络实现从传感器到控制器, 从控制器到执行器间的信息传输, 由于其依靠网络传输数据的特性使其控制系统极易遭到安全威胁. 本文从物理系统入手, 意图保护 CPS 系统中物理实体的正常运行不受由于恶意攻击造成网络空间入侵带来的干扰. 以受到数据包时序攻击的信息物理融合系统为研究对象, 将其安全性研究抽象为一个博弈过程, 基于非合作博弈的两人零和博弈模型, 设计了可变延迟情况下鲁棒输出反馈的极大极小控制器. 并且采用参数化的软约束二次型目标函数, 在控制器设计时引入干扰衰减因子 γ, 通过对 γ 的取值使得二次型目标函数取极小值, 从而保证了最差情况下的稳定控制, 在满足 γ 的约束条件下, 本文通过粒子群搜索算法得出 γ 的值. 另外, 本文还对所设计的极大极小控制器, 与线性二次型高斯 (Linear quadratic Gaussian, LQG) 控制对比分析, 用双水箱系统进行了仿真验证, 发现在受攻击情况下本文所设计的控制器最终能够实现稳定控制, 而 LQG 却不能.

关键词 零和博弈, 极大极小控制, LQG 控制, 数据包时序攻击

引用格式 庞岩, 王娜, 夏浩. 基于博弈论的信息物理融合系统安全控制. 自动化学报, 2019, **45**(1): 185−195

DOI 10.16383/j.aas.2018.c180365

A Game Theory Approach for Secure Control of Cyber-physical Systems

PANG Yan[1] WANG Na[2] XIA Hao[3]

Abstract As a remote control system, the cyber-physical system (CPS) relies mainly on wireless networks to realize the transmission of information from sensors to controllers and from controllers to actuators. Because of this characteristic, the control system of CPS is vulnerable to security threats. Starting with physical devices, the aim of this paper is to protect normal operation of physical entities in CPS system from the interference of network intrusion caused by malicious attacks. Taking the cyber-physical systems suffered packets scheduling attacks into consideration, its secure control was abstracted as a process of two person zero sum game. Based on two person zero sum model of non-cooperative game, the paper designed a min-max controller with a robust output-feedback under time-varying delays. In this paper, a parameterized soft constraint quadratic objective function was adopted. Also, interference attenuation factor γ was introduced in the controller design and the minimum value of the quadratic objective function was determined by the value of γ which guaranteed the stability control under the worst case. Within the constraint of γ, we get the value of γ through particle swarm search algorithm. In addition, the min-max controller is analyzed and compared with the linear quadratic Gaussian (LQG) control, and the simulation was conducted on a two tanks system. The result showed that the min-max controller can stabilize the attacked system, but LQG cannot.

Key words Zero sum game, min-max control, linear quadratic Gaussian (LQG) control, packet scheduling attack

Citation Pang Yan, Wang Na, Xia Hao. A game theory approach for secure control of cyber-physical systems. *Acta Automatica Sinica*, 2019, **45**(1): 185−195

信息物理融合系统[1] (Cyber-physical system, CPS) 是在环境感知的基础上综合计算、网络和物理实体的高效能网络化智能信息系统, 通过 3C (Computation、communication、control) 技术的有机融合与深度协作, 实现大型工程系统的实时感知、动态控制和信息服务. 其本质是将计算过程和物理过程有效地融合在一起, 通过嵌入式计算机和网络对物理过程进行监控. 我国在 2009 年将 CPS 列入重点研究方向[2], 但对 CPS 的研究无论从软件还是硬件以及理论基础上都存在着诸多难点. 物联网、人工智能、云计算等技术的成熟和发展, 将会为 CPS 的研 究和应用带来巨大的转机.

收稿日期 2018-05-30 录用日期 2018-08-27
Manuscript received May 30, 2018; accepted August 27, 2018
国家自然科学基金 (61273098), 中央高校基本科研业务 (DUT16QY23), 辽宁省自然科学基金 (20180520023) 资助
Supported by National Natural Science Foundation of China (61273098), and Fundamental Research Funds for the Central Universities (DUT16QY23), and Natural Science Foundation of Liao Ning Province (20180520023)
本文责任编委 许斌
Recommended by Associate Editor XU Bin
1. 大连理工大学工业装备与结构分析国家重点实验室 航空航天学院 大连 116024 2. 上海飞机设计研究院 上海 201210 3. 大连理工大学控制科学与工程学院 大连 116024
1. State Key Laboratory of Structural Analysis for Industrial Equipment and School of Aeronautics and Astronautics, Dalian University of Technology, Dalian 116024 2. Shanghai Aircraft Design and Research Institute, Shanghai 201210 3. School of Control Science and Engineering, Dalian University of Technology, Dalian 116024

信息物理融合系统由深度集成、紧密耦合的计算和物理组件组成, 并具备通信能力. 然而依赖于通信网络和标准通信协议来传输测量和控制数据包增加了对物理系统的攻击的可能性. 因此, 对于可靠性差的通信网络下的网络控制系统研究也成为一个热门的研究领域[3]. 通信网络是 CPS 的核心, 系统的各部分元件在这里进行信息交换和传递, 而 CPS 中的信息系统结构复杂异构, 系统也随着发展变得更加复杂、开放, 因此极易受到外界干扰甚至恶意攻击. 在存在恶意攻击威胁情况下, 如何设计防御控制策略, 对故障进行控制和及时恢复, 使系统在短时间内更正错误, 防止错误扩散, 不影响系统正常的工作状态, 是 CPS 安全性研究[4−5] 的重点. CPS 的安全性也可分为故障安全和主动安全. 故障安全是对偶发故障的避免, 通过故障检测技术[6] 实现对故障的及时发现以及将故障对系统带来的危害降至最低. 而主动安全则侧重于对恶意攻击的主动防范. 对于 CPS 系统的安全设计来说, 主要关心怎么预防事故的发生, 因此故障安全和主动安全都需要保证. 而对于本文考虑的存在恶意攻击的情况下, 则主要研究主动安全, 从而对系统进行弹性与鲁棒控制.

目前国内相关的研究文献甚少, 国外的研究也处于起步阶段, 对于 CPS 的安全性研究大多集中于网络数据加密[7]、模型验证[8] 或借助网络安全[9] 的研究方法等, 而很少考虑物理系统的控制安全. 与上述研究方向不同, 本文将着重考虑通信对于控制的影响, 给予系统一定的容错能力, 从受控系统上保证物理设备的安全.

在现有文献研究中, 下列文献研究了控制系统中数据通信受到攻击时的影响及控制方法设计. 文献 [10−11] 致力于最小化控制目标函数的反馈控制器的设计, 在这两篇文献中, 仅考虑了数据包丢失, 未考虑延迟. 在文献 [12] 中提出了延迟和数据包丢失下的预测控制器设计, 但是没有明确考虑乱序. Sinopoli 等[13] 利用伯努利过程研究了测量损失下卡尔曼滤波的应用, 提出了数据包丢失概率对于最优估计的一个阈值条件, 并给出了阈值函数. 研究控制或者数据包丢包概率的条件是控制系统能够容忍并且仍然能够保持系统的可靠性. 控制系统中数据丢包模型常用伯努利模型, 伯努利模型由于其通用性强及易处理, 因此在最近几年被广泛地研究[14]. 然而伯努利过程仅给出了一个数据包丢失的离散概率分布模型, 对时延及观测噪声并没有考虑. 伊利诺伊大学的 Tamer Basar 教授对博弈论在控制中的应用做出了很多工作, 包括对采用博弈论的方法进行 H_∞ 控制器设计的专著, 并且在文献 [15] 中提出用动态博弈的方法对有损网络进行 H_∞ 优化控制. 文献 [16] 从数学范数概念出发, 提出把 H_2/H_∞ 混合控制问题抽象为两个对局者在信息不完全情况下的非零和博弈模型, 通过纳什均衡设计输出反馈控制器, 使系统在保持鲁棒稳定性的前提下最大程度地降低干扰对输出的影响, 使系统获得最优动态性能指标. 因此, 博弈论在针对冲突模式下的动态控制有良好的应用前景.

本文将研究信息物理融合系统受到攻击下的控制策略, 借助最优控制的理论和方法, 将其抽象为二人零和动态博弈问题, 设计了在网络控制系统中对数据包的时序攻击具有弹性的鲁棒输出反馈控制器. 对网络时间序列算法的攻击将导致产生时变延迟, 造成数据包接收顺序的改变. 对于无线传感器网络数据传输过程中由于对数据包时序攻击造成的可变延迟, 本文通过运用极大极小值原理并将其和黎卡提微分方程的解[17−18] 相结合给出了最优控制策略的控制律. 最后用双水箱模型进行仿真验证, 并与 LQG (Linear quadratic Gaussian) 控制进行了对比发现, 本文所用方法最终实现了系统的稳定控制, 而 LQG 控制在受到攻击后则出现剧烈震荡.

1 问题描述

1.1 数据包时序攻击

在典型的信息物理网络系统中, 通常有多传感器通过一个共享的通信频道发送信息给控制器, 控制器传输控制数据给连接在物理系统上的执行器. 数据包必须按照一定的顺序传输, 并在规定的时间内到达. 本文主要考虑攻击者在传感器和控制器之间的路径上进行干扰, 导致数据包丢失, 或者产生时变延迟和乱序等, 但不能改变数据包的内容[19].

我们称这种对网络数据传输的时间特性进行干预造成系统数据丢失或产生时变延迟, 从而导致数据包乱序的攻击行为称为数据包时序攻击 (Pactket scheduling attacks). 通过无线网络传输的数据包在进行加密前都是被做上时间标记的, 时间戳能够被用来检测已过时的信息.

数据包时序攻击是很容易做到的, 最直接的方式就是对手把恶意软件放在发送方和接收方之间数据传送的路由上, 或者在数据传输的路径上加入恶意节点 (Malicious node), 由于各节点间形成一个多跳的网络, 恶意节点的加入可造成数据延迟. 另一个不正当的攻击方式是拒绝服务攻击 (Denial of service, DoS), 在无线通信频道, 对手可以通过重复地发送数据包导致数据包冲突和自动重传, 使得数据包错过它的截止时限, 从而耗尽共享的通信频道或造成网络拥堵[19]. 因此数据包时序攻击可造成以下影响: 1) 产生时变延迟: 2) 改变控制器接收到的数据包顺序, 即乱序.

1.2 系统模型

由于网络和物理世界之间的紧密耦合和协调, CPS 是在多个空间和时间维度上动态地重组和重新配置具有高度自动化的控制系统. 为了使无缝集成, CPS 的实现依赖于整个系统的闭环设计的思考. 如图 1 所示, 在物理过程中感测到的事件需要反映在网络世界中, 而网络世界所采取的控制策略需要作用到物理受控系统上. 从这个过程中可以发现, 传感器和执行器充当物理和网络世界之间的接口, 并且通过网络通信基础设施闭合了物理世界和网络空间之间的间隙, 实现物理世界和计算进程的融合. 若在网络上有恶意节点的加入, 则可造成控制器接收数据时间及顺序的变化, 因此安全问题在整个系统中也就出现了.

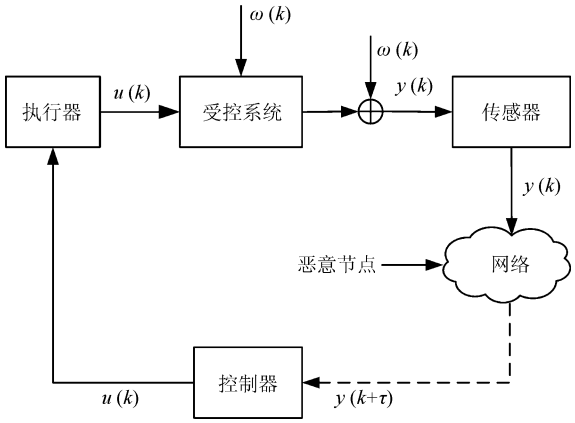


图 1　无线传感器网络控制系统模型 (虚线表示无线网络, 实线表示有线网络)

Fig. 1　Model of wireless sensor network control system (The dashed line shows the wireless network, and the solid line shows the wired network.)

本文采用离散时间的线性时不变系统进行极大极小控制器设计, 状态和输出都受到干扰影响, 离散的状态空间方程如下:

$$\begin{cases} \boldsymbol{x}(k+1) = A\boldsymbol{x}(k) + B\boldsymbol{u}(k) + D\boldsymbol{\omega}(k) \\ \boldsymbol{y}(k) = C\boldsymbol{x}(k) + E\boldsymbol{\omega}(k) \\ \boldsymbol{z}(k) = H\boldsymbol{x}(k) + G\boldsymbol{u}(k) + F\boldsymbol{\omega}(k) \end{cases} \tag{1}$$

$$J(\boldsymbol{\mu}, \boldsymbol{\upsilon}) = |\boldsymbol{x}(K)|^2_{Q_f} + \sum_{k=0}^{K-1} \left(|\boldsymbol{x}(k)|^2_{Q_K} + |\boldsymbol{u}(k)|^2 \right) \tag{2}$$

其中, $k = 1, 2, \cdots, K$, $\boldsymbol{x}(k) \in \mathbf{R}^n$, $\boldsymbol{y}(k) \in \mathbf{R}^p$, $\boldsymbol{u}(k) \in \mathbf{R}^m$, $\boldsymbol{\omega}(k) \in \mathbf{R}^l$ 分别是系统状态、输出、控制输入和干扰输入, Q_f、Q_K 是适当维度的正定权重矩阵. 让 U 和 W 分别表示控制策略的空间和干扰策略空间. 其控制策略和干扰策略分别表示为 $\boldsymbol{\mu} \in U$ 和 $\boldsymbol{\nu} \in W$. 定义 $\boldsymbol{\mu} = (\mu_0, \cdots, \mu_{K-1}), \boldsymbol{\nu} = (\nu_0, \cdots, \nu_{K-1})$, 有限域长度 K. $H^{\mathrm{T}}H = Q_K, H^{\mathrm{T}}G = 0, G^{\mathrm{T}}G = I, F = 0$. 另外, 假设 E 是满秩的, $N = EE^{\mathrm{T}} > 0$, $DE^{\mathrm{T}} = 0$, 即过程干扰和测量干扰是不耦合的.

1.3 控制算法研究

在过去几十年里, 控制理论主要发展了 "H_∞ 最优控制理论", 针对线性受控系统在受到未知的添加干扰和系统不确定性时最差情况的控制器设计问题, 包括干扰衰减、模型匹配、和跟踪问题等[20]. 常用的最优控制还有线性二次型最优控制, 即性能指标是状态变量和控制变量的二次函数积分. 其中线性二次型最优控制包括确定性系统的线性二次型最优控制问题 (Linear quadratic, LQ) 和随机系统的线性二次型高斯控制 (Linear quadratic Gaussian, LQG).

对于随机系统的最优控制, 常用的是 LQG 控制, 但是该控制算法的干扰模型是一个已知统计特性的随机模型, 即高斯分布. 由于本文采用的干扰为随机的且不知其统计特性的. 因此, 在研究 CPS 面临攻击行为情况下的安全性控制问题时, 采用了博弈论方法.

博弈论是近年来最优控制领域的研究重点之一, 随着最优控制研究方法的深入, 推动了博弈论研究的新高潮. 博弈论主要研究冲突模式, 寻求冲突局势下的最优策略, 通过对个体行为的预测并对实际行为进行分析把产生利益冲突现象的个体抽象为博弈模型, 利用博弈理论分析问题建立优化策略模型, 得到具有次优或最优效用值的博弈策略. 博弈的类型分为: 合作/非合作博弈、零和/非零和博弈、对称/非对称博弈、完全信息/不完全信息博弈[21] 等. 对于有利益冲突的双方, 一方试图对系统进行干扰, 另一方则尽力使干扰对系统的影响降到最小, 则博弈论无疑是对其进行优化控制中最合适的工具. 因此, 博弈论在网络安全控制方面将会有更加广泛的应用.

本文将攻击者和防御系统看成是一个博弈过程, 攻击者通过各种手段试图获取自己所需的信息资源或对系统造成直接的破坏, 而防御系统则采取相应的防御策略试图最大程度地减小攻击行为带来的损害. 在外部攻击者恶意干扰的情况中, 系统输入与外部干扰可看成是两人的零和动态博弈, 由于攻击者和防御系统的博弈是一个非合作博弈过程, 本文假设攻击者的行为是随机的, 且互相不知道对方的信息, 因此为了设计鲁棒性强的输出反馈控制器, 采用零和动态博弈的方法, 该控制器设计被视为两个玩家间的动态博弈过程. 控制器尽量使一个被给的

有限域二次型函数最小, 而干扰尽量使这个函数最大[22].

对于不完全信息状态, 干扰是不可预测的, 如何模型化误差信号将会是一个难点. 因此在这里我们需要假设干扰 $\boldsymbol{\omega}$ 是平方可积的, 即 $\boldsymbol{\omega}$ 是有限能量的[20]. 函数 J 是干扰的二次型函数, 如何阻止随着干扰的增加, 性能函数不断的增大, 一个可行的控制方法就是控制它的增长率. 给定一个正数 γ, 使得控制器满足下面不等式:

$$\frac{\|\boldsymbol{z}\|}{\|\boldsymbol{w}\|} \leq \gamma, \quad \|\boldsymbol{w}\|^2 = |\boldsymbol{x}_0|^2_{Q_0} + \|\boldsymbol{\omega}\|^2 \tag{3}$$

$\boldsymbol{z}$ 是控制输出, 将干扰和不确定的初始状态 $\boldsymbol{x}_0$ 共同作为未知的外界干扰因子 $\boldsymbol{w}$. 这个设计问题就转化为找到一个最小化下面性能函数的控制器.

用符号 $\|\cdot\|$ 表示欧几里得范数, 可将该问题的解决转化为零和博弈的软约束博弈方法, 则对于参数化有限域情况下性能函数如下:

$$\begin{aligned} J_\gamma^K(\boldsymbol{\mu},\boldsymbol{\upsilon}) = {} & |\boldsymbol{x}_K|^2_{Q_f} - \gamma^2 |\boldsymbol{x}_0|^2_{Q_0} + \\ & \sum_{k=0}^{K-1} \left(|\boldsymbol{x}_k|^2_{Q_k} + |\boldsymbol{u}_k|^2 - \gamma^2 |\boldsymbol{\omega}_k|^2\right) = \\ & |\boldsymbol{x}_K|^2_{Q_f} + \|\boldsymbol{x}_k\|^2_{Q_k} + \|\boldsymbol{u}_k\|^2 - \\ & \gamma^2 \|\boldsymbol{\omega}_k\|^2 - \gamma^2 |\boldsymbol{x}_0|^2_{Q_0} \end{aligned} \tag{4}$$

其中, $\gamma > 0$ 是干扰抑制水平, Q_0 是适当维度的正定权重矩阵, $\boldsymbol{x}_0$ 是未知的系统初始状态值. 需要找到一个 γ 值来满足零和博弈有解, 即使得:

$$\inf_{\boldsymbol{\mu}\in \mathrm{M}} \sup_{\boldsymbol{\omega}\in\Omega} J_\gamma^K(\boldsymbol{\mu},\boldsymbol{\nu}) = \sup_{\boldsymbol{\omega}\in\Omega} \inf_{\boldsymbol{\mu}\in \mathrm{M}} J_\gamma^K(\boldsymbol{\mu},\boldsymbol{\nu}) \tag{5}$$

有解. 该问题就变成相当于寻找 "$\gamma \geq 0$" 的最小值问题, 目标函数 $J_\gamma^K(\boldsymbol{\mu},\boldsymbol{\nu})$ 所定义的零和动态博弈有相等的上界值和下界值, 使得线性二次型动态博弈的鞍点解能直接应用于最差情况的设计问题上. 动态博弈的性能指标由 $J_\gamma^K(\boldsymbol{\mu},\boldsymbol{\nu})$ 给出, 也称为带干扰抑制的软约束博弈, "软约束" 常被用来获取在博弈中对于没有硬性边界的这一特征[20]. 动态优化类型的问题就类似一个两人零和动态博弈, 控制器 U 是最小化玩家 (可称为玩家 1) 使目标函数最小, 干扰 W 是最大化玩家 (称作玩家 2), 使目标函数最大.

用 M 表示玩家 1 的策略空间, N 表示玩家 2 的策略空间, 以规范形式给定一个零和动态博弈 $\{J : M, N\}$, 则策略对 $(\boldsymbol{\mu}^*, \boldsymbol{\nu}^*)$ 构成一个鞍点解, 对于所有的 $(\boldsymbol{\mu},\boldsymbol{\nu}) \in M \times N$,

$$J(\boldsymbol{\mu}^*,\boldsymbol{\nu}) \leq J^* = J(\boldsymbol{\mu}^*,\boldsymbol{\nu}^*) \leq J(\boldsymbol{\mu},\boldsymbol{\nu}^*) \tag{6}$$

J^* 的值就是动态博弈的值. J^* 的定义如下:

$$\bar{J} = \inf_{\boldsymbol{\mu}\in M} \sup_{\boldsymbol{\omega}\in N} J(\boldsymbol{\mu},\boldsymbol{\nu}) = J^* = \sup_{\boldsymbol{\omega}\in N} \inf_{\boldsymbol{\mu}\in M} J(\boldsymbol{\mu},\boldsymbol{\nu}) = \underline{J} \tag{7}$$

其中, $\bar{J}$ 和 $\underline{J}$ 分别是上界值和下界值, 满足不等式 $\bar{J} \geq \underline{J}$, 当它们相等时的值就是博弈值 J^*.

二次型目标函数要取得最小值, 需满足严格凸的. 因此, 对于 γ 的求解, 有如下定理:

定理 1. 由式 (4) 给出的二次型目标函数 $J_\gamma^K(\boldsymbol{\mu},\boldsymbol{\nu})$ 在状态方程 (1) 条件下, 对于玩家 1 的每一个开环策略 u 满足严格凸的, 当且仅当

$$\gamma^2 I - D^{\mathrm{T}} S_{k+1} D > 0, k \in [1, K]$$

其中, 序列 S_{K+1}, $k \in [1, K]$ 由下列黎卡提方程求解:

$$\begin{aligned} S_k = {} & A^{\mathrm{T}} S_{k+1} D [\gamma^2 I - D^{\mathrm{T}} S_{k+1} D]^{-1} D^{\mathrm{T}} S_{k+1} A + \\ & Q_k + A^{\mathrm{T}} S_{k+1} A \\ S_{K+1} = {} & Q_f \end{aligned}$$

因此, 在有干扰衰减情况下, 满足性能指标极值存在的所有 γ 值的下界表示为 γ^*, 此时相应的控制器为 H_∞ 控制器. 当没有干扰衰减情况时, 极小极大控制器相当于线性二次型高斯 (LQG) 控制器.

2 控制器设计

2.1 LQG 跟踪系统控制器设计

对于随机系统的 LQG 控制器的设计, 可以采用确定性系统 LQ 控制律的设计和 Kalman 状态最优估计的结合, 组成 LQG 控制器, 其控制模型[23] 为

$$\begin{cases} \bar{\boldsymbol{x}}(k) = F\hat{\boldsymbol{x}}(k-1) + G\boldsymbol{u}(k-1) \\ \hat{\boldsymbol{x}}(k) = \bar{\boldsymbol{x}}(k) + K[\boldsymbol{y}(k) - C\bar{\boldsymbol{x}}(k)] \\ \boldsymbol{u}(k) = -L\hat{\boldsymbol{x}}(k) \end{cases} \tag{8}$$

其中, $\bar{\boldsymbol{x}}(k)$ 为时间更新, $\hat{\boldsymbol{x}}(k)$ 为测量更新. 对于离散系统式 (1), 它使得如下的离散二次型性能指标函数极小

$$\begin{aligned} J = {} & \boldsymbol{x}^{\mathrm{T}}(N) Q_0 \boldsymbol{x}(N) + \\ & \sum_{k=0}^{N-1} [\boldsymbol{x}^{\mathrm{T}}(k) Q_1 \boldsymbol{x}(k) + \boldsymbol{u}^{\mathrm{T}}(k) Q_2 \boldsymbol{u}(k)] \end{aligned} \tag{9}$$

其中, Q_0 和 Q_1 是非负定矩阵, Q_2 是正定矩阵. 考虑控制器中加入积分作用, 引进积分后的跟踪系统的结构如图 2 所示, 其中

$$\boldsymbol{u}(k) = -L_i \boldsymbol{x}_c(k) - L_1 \hat{\boldsymbol{x}}(k) \tag{10}$$

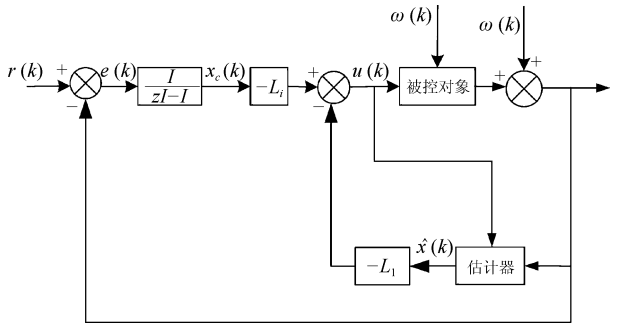


图 2　LQG 控制器结构图

Fig. 2　LQG controller structure diagram

最优反馈控制律 $L = [L_1 \quad L_i]$ 的求取方法与 LQ 跟踪系统相同:

$$\begin{cases} \boldsymbol{x}_c(k) = \dfrac{I}{zI - I}\boldsymbol{e}(k) \\ \boldsymbol{x}_c(k+1) = \boldsymbol{x}_c(k) + \boldsymbol{e}(k) = \boldsymbol{x}_c(k) + \boldsymbol{r}(k) - \boldsymbol{y}(k) \end{cases} \tag{11}$$

令系统增广状态为

$$\bar{\boldsymbol{x}}(k+1) = \begin{bmatrix} \boldsymbol{x}(k) \\ \boldsymbol{x}_c(k) \end{bmatrix}$$

则增广的系统状态方程为

$$\bar{\boldsymbol{x}}(k+1) = \bar{A}\bar{\boldsymbol{x}}(k) + \bar{B}\boldsymbol{u}(k) + Q\boldsymbol{r}(k) \tag{12}$$

可求得

$$\begin{cases} L = [Q_2 + \ B^{\mathrm{T}}S\bar{B}]^{-1}\bar{B}^{\mathrm{T}}S\bar{A} \\ S = Q_1 + \bar{A}^{\mathrm{T}}S\bar{A} - \\ \qquad \bar{A}^{\mathrm{T}}S\bar{B}[Q_2 + \bar{B}^{\mathrm{T}}S\bar{B}]^{-1}\bar{B}^{\mathrm{T}}S\bar{A} \end{cases} \tag{13}$$

估计器为 Kalman 滤波器. 滤波器的反馈增益 K 为

$$\begin{cases} K(k) = \ M(k)C^{\mathrm{T}}[CM(k)C^{\mathrm{T}} + W]^{-1} \\ M(k) = FP(k-1)F^{\mathrm{T}} + V \\ P(k) = \ [I - K(k)C]M(k)[I - K(k)C]^{\mathrm{T}} + \\ \qquad K(k)WK^{\mathrm{T}}(k) \end{cases} \tag{14}$$

2.2　有限域的极大极小控制器设计

对于有限域离散时间零和博弈, 需要引入一个鞍点解存在的有效条件, 考虑零和动态博弈有下列状态方程描述:

$$\begin{aligned} &\boldsymbol{x}_{k+1} = f_k(\boldsymbol{x}_k, \boldsymbol{u}_k, \boldsymbol{\omega}_k), \qquad k \in [1, K] \\ &\boldsymbol{y}_k = h_k(\boldsymbol{x}_k, \boldsymbol{\omega}_k), \qquad k \in [2, K] \end{aligned} \tag{15}$$

有限域的性能指标:

$$J(\boldsymbol{\mu}, \boldsymbol{\nu}) = \sum_{k=1}^{K} g_k(\boldsymbol{x}_{k+1}, \boldsymbol{u}_k, \boldsymbol{\omega}_k, \boldsymbol{x}_k) \tag{16}$$

引入信息结构模型, 将控制器收到的信息集合表示为:

$$\Pi_0^k = \{j \in \{0, \cdots, k\} | \text{数据包} j \text{在控制器里被收到}\} \tag{17}$$

在控制器中收到的测量值集合为

$$Y_0^k = \{\boldsymbol{y}(j) | j \in \Pi_0^k\} \tag{18}$$

在控制器中可利用的信息集合为

$$I_0^k = \{Y_0^k, \boldsymbol{u}_0^{k-1}, \Pi_0^k\} \tag{19}$$

其中, u_0^{k-1} 表示序列 $u(0), \cdots, u(k-1)$.

在单个玩家的优化问题中, 动态规划的方法提供了一个有效的方式来获取最优的鞍点解, 通过以倒推的方式来解一个静态优化问题. 对于动态博弈, 由鲁弗斯 · 艾萨克斯在 19 世纪 50 年代早期通过连续时间域推广获得的离散时间版的类似方程 — 艾萨克斯方程, 这样一个方程提供了鞍点解存在的有效条件.

$$\begin{aligned} V_k(\boldsymbol{x}) = &\min_{u\in U}\max_{w\in W}[g_k(f_k(\boldsymbol{x},\boldsymbol{u},\boldsymbol{w}),\boldsymbol{u},\boldsymbol{w},\boldsymbol{x}) + \\ &V_{k+1}(f_k(\boldsymbol{x},\boldsymbol{u},\boldsymbol{w}))] = \\ &\max_{w\in W}\min_{u\in U}[g_k(f_k(\boldsymbol{x},\boldsymbol{u},\boldsymbol{w}),\boldsymbol{u},\boldsymbol{w},\boldsymbol{x}) + \\ &V_{k+1}(f_k(\boldsymbol{x},\boldsymbol{u},\boldsymbol{w}))] = \\ &g_k(f_k(\boldsymbol{x},\mu_k^*(\boldsymbol{x}),v_k^*(\boldsymbol{x})),\mu_k^*(\boldsymbol{x}),v_k^*(\boldsymbol{x}),\boldsymbol{x}) + \\ &V_{k+1}(f_k(\boldsymbol{x},\mu_k^*(\boldsymbol{x}),v_k^*(\boldsymbol{x}))) \\ V_{K+1}(\boldsymbol{x}) \equiv &\ 0 \end{aligned} \tag{20}$$

控制器不能获取完全的状态信息, 因此, 采用最坏情况下的极大极小估计, 根据确定性等价原则, 将控制器设计分成两个部分: 1) 第一部分是设计一个观测器, 能够估计最坏的状态, 并与可利用的输入输出序列相匹配: 2) 第二部分是设计一个控制器, 利用估计的状态产生新的控制输入.

基于文献 [20] 中的一些结论, 来设计本文的极大极小控制器. 设置时间延迟为 τ, 因此在时间 $k \geq \tau$, 只有 $k-\tau$ 之前的信息是可用的, 也就是说测量信息集合 $Y_0^k = Y_0^{k-\tau}$. 极大极小控制器的设计按照从初始时间到时间 $k-\tau$ 是没有延迟的, 剩下的时间利用最差干扰状态下的估计, 因此这时候是没有观测值可利用的. 另外, 我们引入参数 α_k, 这里 $\alpha_k = 1$ 说明数据包在时间 k 被接收, $\alpha_k = 0$ 说明没有收到数据包. 用时刻 k 的值做时刻 $k+1$ 的状态估计, 表示为 $\hat{\boldsymbol{x}}(k+1)$, 为了描述更清晰, 用 $\hat{\boldsymbol{x}}(k+1) = \hat{\boldsymbol{x}}(k+1|k)$ 状态估计方程为:

$$\begin{aligned} \hat{\boldsymbol{x}}(k+1) = &A\hat{\boldsymbol{x}}(k) + B\boldsymbol{u}(k) + A\Lambda(k)[\gamma^{-2}Q\hat{\boldsymbol{x}}(k) + \\ &C^{\mathrm{T}}N^{-1}(\boldsymbol{y}(k) - C\hat{\boldsymbol{x}}(k))] \end{aligned} \tag{21}$$

对于以上的状态估计方程有以下控制律:

$$u(k) = -B^{\mathrm{T}}\Gamma(k)A(I-\gamma^{-2}\Sigma(k)M(k))^{-1}\hat{\boldsymbol{x}}(k) \tag{22}$$

其中

$$\Lambda(k) = [\Sigma(k)^{-1} + \alpha_k C^{\mathrm{T}}N^{-1}C - \gamma^{-2}Q]^{-1} \tag{23}$$

$$\Gamma(k) = [M(k+1)^{-1} + BB^{\mathrm{T}} - \gamma^{-2}DD^{\mathrm{T}}]^{-1} \tag{24}$$

$M(k)$ 和 $\Sigma(k)$ 是博弈代数黎卡提方程的解, $M(k) = Q_K$, $\Sigma(0) = Q_0^{-1}$.

$$M(k) = A^{\mathrm{T}}[M(k+1)^{-1} + BB^{\mathrm{T}} - \gamma^{-2}DD^{\mathrm{T}}]^{-1}A + Q \tag{25}$$

$$\Sigma(k+1) = A\Lambda(k)A^{\mathrm{T}} + DD^{\mathrm{T}} \tag{26}$$

另外, 当 $\alpha_k = 0$ 时,

$$\tilde{\Sigma}(k+1) = A(\Sigma(k)^{-1} - \gamma^{-2}Q)^{-1}A^{\mathrm{T}} + DD^{\mathrm{T}} \tag{27}$$

按照 Tamer Basar 在极大极小控制器设计的理论中, 极小极大控制器存在的条件[20] 为

1) 方程 (25) 在 $[0, K]$ 上有解;

2) 方程 (26) 有解;

3) 式 (25) 和 (26) 的解满足下列条件:

$$\rho(\Sigma(k)Q) < \gamma^2,\ k = 0, \cdots, K-1 \tag{28}$$

$$\rho(\tilde{\Sigma}(k+1)M(k+1)) < \gamma^2,\ k = 0, \cdots, K \tag{29}$$

对于上面的条件, 有任何一个不成立, 则不存在这样的控制器, 使得 $\gamma \geq \gamma^*$.

带积分状态控制的极大极小控制器结构如图 3 所示:

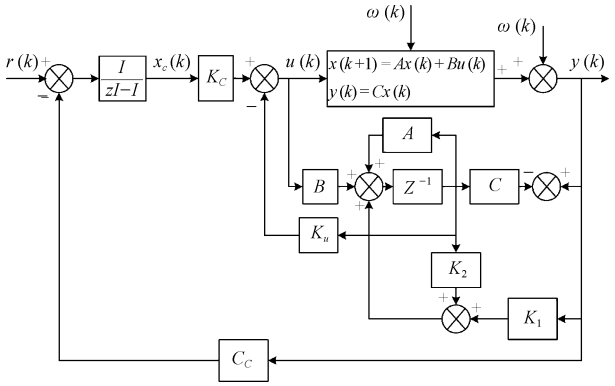


图 3 极大极小控制器结构图

Fig. 3 Minimax controller structure diagram

2.3 时序攻击下的极大极小控制器设计

图 4 为几种数据传输故障及解决方法, 取时间步为 $k = 6$, 图中三种分别为有固定延迟、测量损失、和可变延迟的情况[20]. 固定延迟的值取 $\tau = 4$, 对于固定延迟的情况, 只能收到前两步的数据, 因此利用第二步的数据值, 执行估计 $\hat{\boldsymbol{x}}(3|2)$. 在测量损失情况下, 损失的数据由已经收到的数据包进行估计. 在时变延迟下, 数据包传递出现乱序, 乱序出现在 $k = 5$ 时刻, 此时收到的数据包是 $k = 3$ 时刻的值. 对此需要设计一个补偿器来处理此类情况.

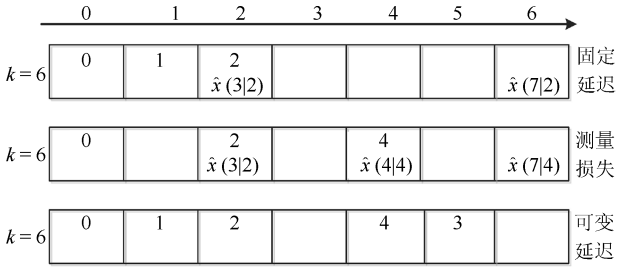


图 4 数据传输示意图

Fig. 4 Schematic diagram of data transmission

对于时变延迟和乱序情况下的信息结构既包括固定延迟下的信息结构又包含损失情况下的信息结构, 因此该类情况的控制策略如图 5 所示.

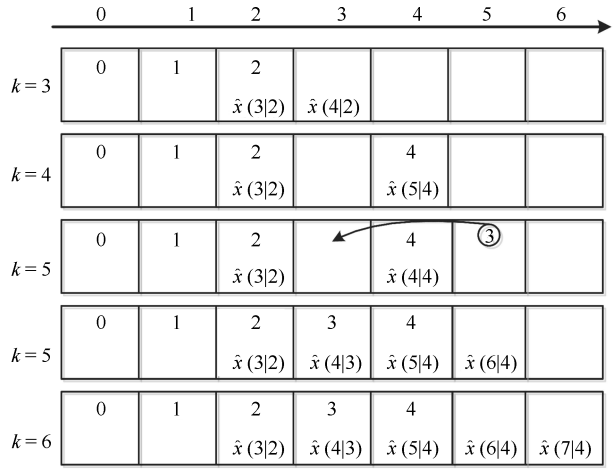


图 5 可变延迟下的数据传输示意图

Fig. 5 A schematic diagram of data transmission under variable delay

在时间步 $k = 3$ 时, 由于数据缺失 ($\alpha_3 = 0$), 估计器采用第二步的数据值进行估计 $\hat{\boldsymbol{x}}(4|2)$; 在 $k = 5$ 时, 时间步 $k = 3$ 的数据收到, 然后返回重新计算第三步的估计值. 因此对于时变引起的数据包乱序, 无论什么时候当延时数据包收到时, 估计器就返回重新计算, 直到所有的数据包都按照正确时序接收.

下面通过一个算法来描述极大极小控制器. 首先引入变量 κ_k, 该变量表示在时间 k 所获得的所有数据包按照正确时序被接收的时间值. 比如上述例子, 在 $k = \{3, 4\}$, $\kappa_k = 2$, 变为 $\kappa_k = 5$ 对于 $k \geq 5$. 在每个时间间隔内收到的数据包数目表示为 N_{pkts}. 设置缓冲区 Θ_y, Θ_u 和 Θ_{Π} 用来保存信息结构 $I_{k-\tau}^{k}$.

另外, 用缓冲区 Θ_x 和 Θ_Σ 来分别储存状态估计值 $\hat{\boldsymbol{x}}(k)$ 和 $\Sigma(k)$. 如果测量值在特定时间 k 没有被控制器收到, 它就不会被包含在信息结构中, 它的缓冲区的值就是空的. 此外, 我们用临时变量 $\bar{\boldsymbol{x}}(k)$ 和 $\bar{\Sigma}(k)$ 作为在线值. 该控制器的算法如下:

算法 1. 乱序数据包和时变延迟下的极大极小控制器

定义 N_{pkts}, Θ_y 是基于区间 $[k-1,k]$ 收到的数据包, 初始 $\kappa=0$.

if $N_{pkts}=0$ **then**　　//没有数据包收到
$\alpha_k \leftarrow 0$
$\bar{k}(k+1) \leftarrow (21)$
$\bar{\Sigma}(k+1) \leftarrow (26)$
else　　//收到数据包
Updata Θ_y
Updata Θ_Π
$\bar{x}(k+1) \leftarrow \Theta_k(\kappa)$　　//初始化
$\bar{\Sigma}(k+1) \leftarrow \Theta_\Sigma(\kappa)$
$u(t) \leftarrow \Theta_u(\kappa)$
$y(t) \leftarrow \Theta_y(\kappa)$
for $t=\kappa:k$ **do**　　//再次计算 $\bar{x}$ 和 $\bar{\Sigma}$
if $\Theta_\Pi(t) \in 0$ **then**　　//没有数据包到达
$\alpha_t \leftarrow 0$
else　　//如果有数据包到达
$\alpha_t \leftarrow 1$
end if
$\bar{x}(k+1) \leftarrow (21)$
$\bar{\Sigma}(k+1) \leftarrow (26)$
Updata Θ_x
Updata Θ_Σ
end for
end if
$M(k) \leftarrow (25)$
$u(k) \leftarrow (22)$　　//计算新的输入
Updata Θ_u
Updata κ

3　基于双水箱模型的系统仿真

3.1　双水箱模型

基于无线网络传输的双水箱系统, 包括水箱本体、供电设备, 还有三个无线传感器节点, 这三个传感器节点通过无线通信通道分别负责系统的传感, 控制和执行. 对于双水箱 CPS 的安全目标是保护物理实体的正常操作不受由于恶意攻击网络基础设施造成网络空间入侵带来的干扰. 对于如图 6 所示的双水箱物理模型, 双水箱液位的动力学方程[24] 如下:

$$\begin{cases} \dot{L}_1(t) = -\dfrac{a_1}{A_1}\sqrt{2gL_1(t)} + \dfrac{K_P}{A_1}V_P(t) \\ \dot{L}_2(t) = \dfrac{a_1}{A_2}\sqrt{2gL_1(t)} - \dfrac{a_2}{A_2}\sqrt{2gL_2(t)} \end{cases} \tag{30}$$

其中, g 是重力加速度, L_1、L_2 分别为水箱 1、2 的液位, A_1、A_2 分别为水箱 1、水箱 2 的横截面积. a_1、a_2 分别为出水孔 1、2 的横截面面积. K_P 为泵的流量常数, V_P 为作用在泵上的电压.

接下来, 定义一组变量集合:

$$\begin{aligned} \Delta L_1(t) &:= L_1(t) - L_{10} \\ \Delta L_2(t) &:= L_2(t) - L_{20} \\ u(t) &= V_P(t) - L_{P0} \end{aligned}$$

可将动力学方程 (30) 重新写为:

$$\begin{cases} \Delta\dot{L}_1(t) = & -\dfrac{a_1}{A_1}\sqrt{2g(\Delta L_1(t)+L_{10})}+ \\ & \dfrac{K_P}{A_1}(\boldsymbol{u}(t)+V_{P0}) \\ \Delta\dot{L}_2(t) = & \dfrac{a_1}{A_2}\sqrt{2g(\Delta L_1(t)+L_{10})}- \\ & \dfrac{a_2}{A_2}\sqrt{2g(\Delta L_2(t)+L_{20})} \end{cases} \tag{31}$$

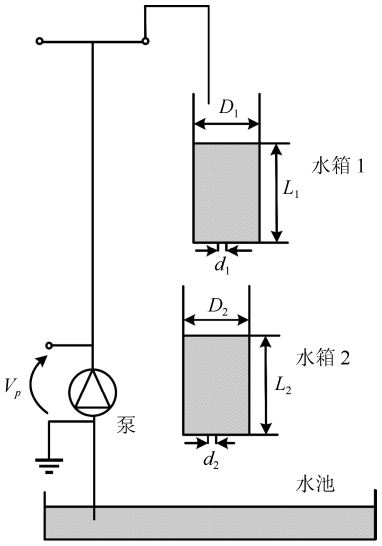


图 6　双水箱物理模型

Fig. 6　Physical model of double water tanks

最后, 在 $\triangle L_1=0$, $\triangle L_2=0$, $u=0$ 处, 对式 (31) 进行线性化, 可以得到双水箱系统的状态空间的形式, 如下:

$$\dot{\boldsymbol{x}}(t) = A\boldsymbol{x}(t) + B\boldsymbol{u}(t) \tag{32}$$

其中, $A = \begin{bmatrix} -\frac{a_1}{A_1}\sqrt{\frac{g}{2L_{10}}} & 0 \\ \frac{a_1}{A_1}\sqrt{\frac{g}{2L_{10}}} & -\frac{a_2}{A_2}\sqrt{\frac{g}{2L_{20}}} \end{bmatrix}$

$$B=\begin{bmatrix}\frac{K_P}{A_1}\\0\end{bmatrix}$$

水箱设备参数如表 1 所示:

表 1 水箱参数

Table 1 Water tank equipment parameters

名称	参数大小
设备质量	6.6 kg
模型尺寸 ($H\times W\times L$)	30.5 cm× 30.5 cm× 91.5 cm
泵流量常数	3.3 cm^3/(V·s)
压力传感器灵敏度	6.1 cm/V
水箱高度	30 cm
水箱内部直径	4.45 cm
流出孔直径	0.48 cm

取 $L_{10}=10\,\mathrm{cm}$, $L_{20}=10\,\mathrm{cm}$, $d_1=d_2=0.48\,\mathrm{cm}$, $D_1=D_2=4.45\,\mathrm{cm}$, $g=980\,\mathrm{cm/s^2}$, $K_P=3.3\,\mathrm{cm}^3/(\mathrm{V\cdot s})$, 则系统的状态空间方程为

$$\dot{\boldsymbol{x}}(t)=\begin{bmatrix}-0.08 & 0\\0.08 & -0.08\end{bmatrix}\boldsymbol{x}(t)+\begin{bmatrix}0.212\\0\end{bmatrix}\boldsymbol{u}(t) \tag{33}$$

采样时间 $T=2\,\mathrm{s}$, 将系统离散化得:

$$\boldsymbol{x}(k+1)=\begin{bmatrix}0.8521 & 0\\0.1363 & 0.8521\end{bmatrix}\boldsymbol{x}(k)+\begin{bmatrix}0.3918\\0.0305\end{bmatrix}\boldsymbol{u}(k) \tag{34}$$

对线性模型和非线性模型对比如图 7 所示.

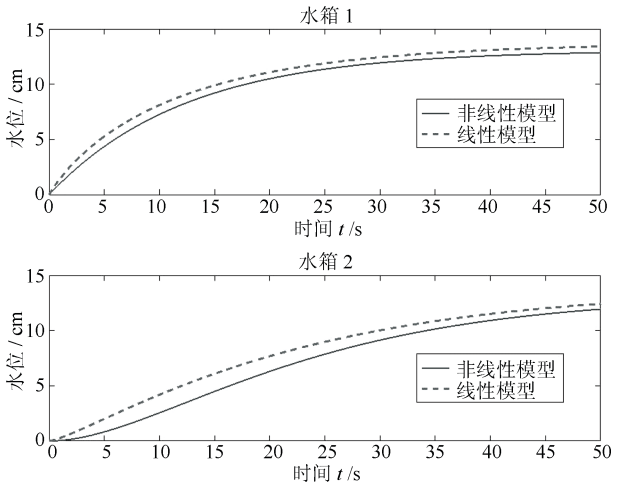


图 7 线性模型和非线性模型仿真对比图

Fig. 7 Comparison of linear and nonlinear models

由图 7 可看出非线性模型和线性模型的响应速度几乎一致, 而线性模型响应相对较平缓. 线性化后的模型在设定的平衡水位附近达到稳定, 其他与非线性模型差别不大. 因此线性化对系统的影响不大, 可忽略不计, 另线性化后模型可便于控制器设计.

考虑到外部干扰因素, 比如对水箱数据传输网络的干扰, 或由于外部震动原因导致压力传感器的数值失真等因素, 在这里我们采用如式 (1) 所示的干扰模型. 对于双水箱系统, 主要设计目标是跟踪低位水箱的一个分段的常数参考输入值, 系统模型由上文所述的双水箱连续系统模型获取, 采样时间为 2 s.

参考输入值设置为 8 cm 和 10 cm. 另外在控制器中引入积分状态, 为了实现参考输入的跟踪. 积分状态控制器如下:

$$\boldsymbol{x}_c(k+1)=\boldsymbol{x}_c(k)+\boldsymbol{r}(k)-C_c\boldsymbol{y}(k) \tag{35}$$

$\boldsymbol{x}_c$ 是控制器积分状态, $C_c=[0\quad 1]$, 极小极大控制器用在新的增广系统上, 状态为 $\xi(k)=[\boldsymbol{x}(k)\quad \boldsymbol{x}_c(k)]^{\mathrm{T}}$, 控制输入如下:

$$\boldsymbol{u}(k)=K_\xi\hat{\xi}(k) \tag{36}$$

其中, K_ξ 和 $\hat{\xi}(k)$ 由式 (22) 和式 (21) 给出. 下面设 $D=0.1\,[B\quad B\quad B\quad 0\quad 0\quad 0]$, $E=0.1\,[0\quad 0\quad 0\quad I\quad I\quad I]$: 另外, 选择矩阵 $Q=Q_K=Q_0=0.1I$.

3.2 LQG 控制仿真结果

对系统加入数据包时序攻击和未受攻击的系统进行仿真对比, 如图 8 和图 9 所示, 其中虚线为受攻击后的系统响应, 实线为未受攻击的系统响应.

3.3 基于博弈论的极大极小控制器仿真结果

首先需先求得满足约束条件的衰减因子 γ, 对于可变延迟, 设置最大延迟时长 $\tau=4$, 本文采用粒子群搜索算法, 求得 $\gamma^*=2.317$, 然后代入求得其他各参数. $K_\xi=[K_u\quad K_c]$, 由增广的状态估计方程求得. 另外, $K_1=A\Lambda(k)C^{\mathrm{T}}N^{-1}$, $K_2=A\Lambda(k)\gamma^{-2}Q$. 则没有受到攻击时的仿真结果如图 10 和图 11 所示. 受到数据包时序攻击下的仿真结果如图 12 和图 13 所示.

通过仿真结果可看出, LQG 控制在遭到攻击时, 控制器已失去稳定控制, 而本文所设计的极大极小控制器在遭到数据包时序攻击时, 虽然有小幅度的波动, 但最终仍实现了稳定, 可明显说明所设计的控制器是可行的, 并具有很好的控制性能. 并且在系统稳定时, 水箱的水位跟踪参考输入变化而变化, 并在较短时间内达到稳定, 对干扰也有较大程度的抑制.

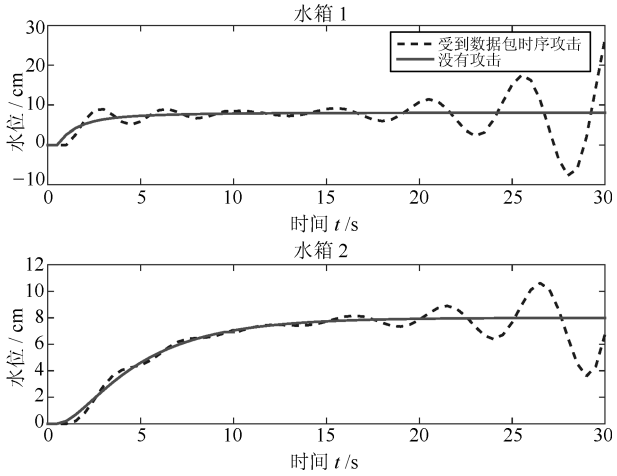


图 8　LQG 控制输出图

Fig. 8　LQG control output diagram

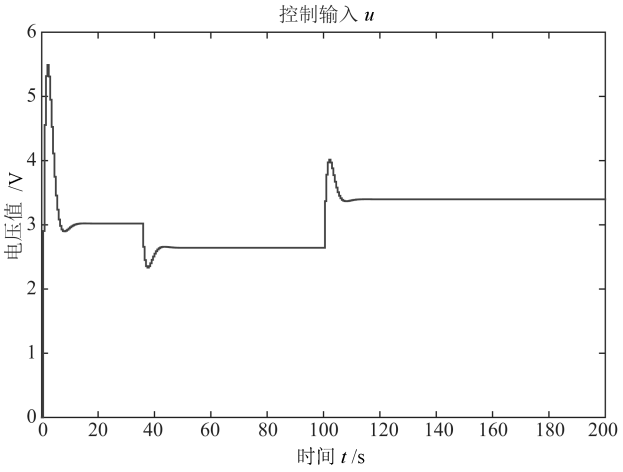


图 11　极大极小控制器的输入值

Fig. 11　The input value of the minimax controller

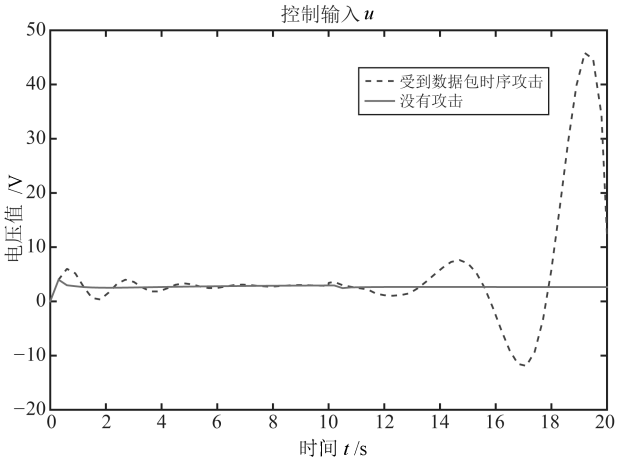


图 9　LQG 控制的输入值

Fig. 9　Input value of LQG control

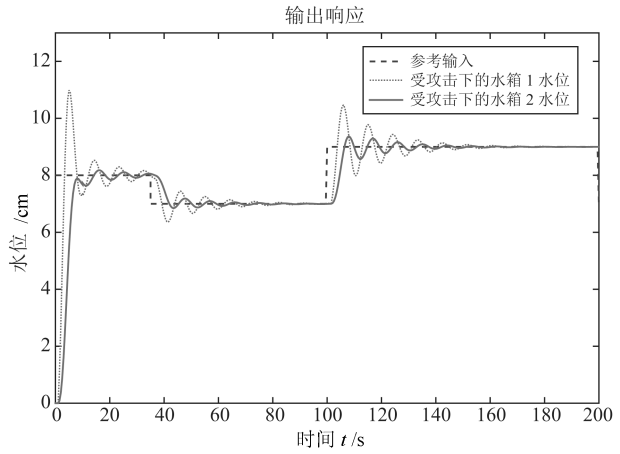


图 12　受攻击下的极大极小控制器输出响应

Fig. 12　Output response of minimax controller under attack

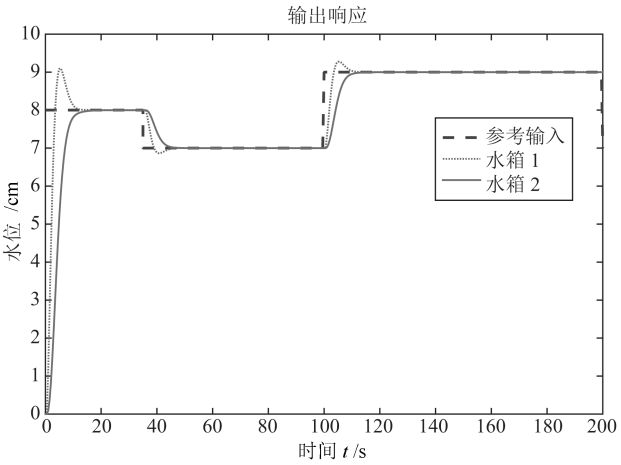


图 10　极大极小控制器的输出图

Fig. 10　The output diagram of the min-max controller

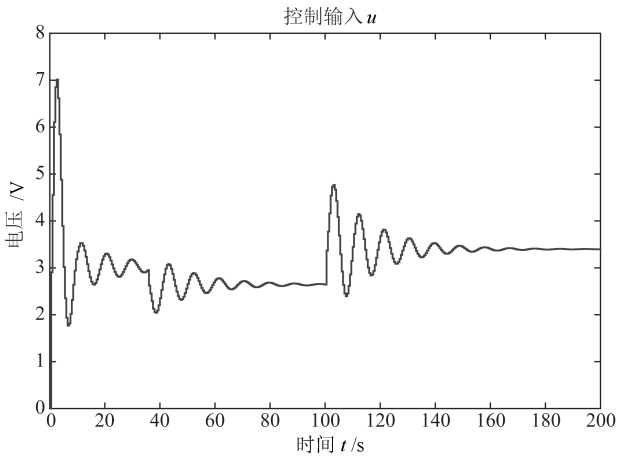


图 13　受攻击下的极大极小控制器输入值

Fig. 13　Input value of the min-max controller under attack

4 结论

随着传感、通信技术和控制理论的进一步综合发展, 以及物联网研究和开发的成熟化, CPS 将成为各国未来科技发展的一个研究热点[25]. 本文根据最优控制的理论, 将信息物理系统的攻击防御模型作为二人零和动态博弈问题, 设计了在网络控制系统中对数据包的时序攻击具有弹性的鲁棒输出反馈控制器. 运用极大极小值原理并将其和黎卡提微分方程的解相结合给出了最优控制策略的控制律. 并与随机系统的线性二次型最优控制即 LQG 控制器进行对比, 结果显示本文所设计的极大极小控制器具有更好的控制效果.

受攻击下的信息物理融合系统的安全性问题, 是系统决策者与网络攻击者之间的博弈与对抗, 随着无线网络的普及及智能系统的发展, 无线通讯网络与物理实体之间信息交互的安全性将显得尤为重要. 如果在完全信息状态下, 也就是攻击者能够获取受控系统信息的状态下, 攻击将会有策略性. 因此对于具有策略性的外部干扰和攻击, 如何使受控系统不受影响或降低其带来的影响, 也就是如何使系统具有更好的弹性控制或鲁棒控制性能将会是今后重点研究的方向和解决的问题.

References

1 Guan X P, Yang B, Chen C, Dai W, Wang Y. A comprehensive overview of cyber-physical systems: from perspective of feedback system. *IEEE/CAA Journal of Automatica Sinica*, 2016, **3**(1): 1−14

2 Wang Zhong-Jie, Xie Lu-Lu. Cyber-physical systems: a survey. *Acta Automatica Sinica*, 2011, **37**(10): 1157−1166
(王中杰, 谢璐璐. 信息物理融合系统研究综述. 自动化学报, 2011, **37**(10): 1157−1166)

3 Hespanha J P, Naghshtabrizi P, Xu Y. A survey of recent results in networked control systems. *Proceedings of the IEEE*, 2007, **95**(1): 138−162

4 Cetinkaya A, Ishii H, Hayakawa T. Networked control under random and malicious packet losses. *IEEE Transactions on Automatic Control*, 2017, **62**(5): 2434−2449

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

6 Jiang Y, Yin S. Recursive total principle component regression based fault detection and its application to vehicular cyber-physical systems. *IEEE Transactions on Industrial Infoslatics*, 2018, **14**(4): 1415−1423

7 Wang E K, Ye Y M, Xu X F, Chow K P. Security issues and challenges for cyber physical system. In: Green Computing and Communications (GreenCom), 2010 IEEE/ACM Int′l Conference on and Int′l Conference on Cyber, Physical and Social Computing (CPSCom). New York, USA: IEEE, 2010. 733−738

8 Peng Chao-Yu. Research on Security of Model Checking-based Cyber-Physical Systems [Master thesis], Nanjing University of Posts And Telecommunications, 2015
(彭超宇. 基于模型检验的信息物理融合系统安全性研究 [硕士学位论文], 南京邮电大学, 2015)

9 Ding Chao, Yang Li-Jun, Wu Meng. Security architecture and key technologies for IoT/CPS. *ZTE Technology Journal*, 2011, **17**(1): 11−16
(丁超, 杨立君, 吴蒙. IoT/CPS 的安全体系结构及关键技术. 中兴通讯技术, 2011, **17**(1): 11−16)

10 Amin S, Cárdenas A A, Sastry S S. Safe and secure networked control systems under denial-of-service attacks. In: Proceedings of International Conference on Hybrid Systems: Computation and Control. Heidelberg, Berlin, Germany: Springer, 2009. 31−45

11 Gupta A, Langbort C, Basar T. Optimal control in the presence of an intelligent jammer with limited actions. In: Proceedings of the Decision and Control (CDC) 49th IEEE Conference. New York, USA: IEEE, 2010. 1096−1101

12 Pang Z H, Liu G P, Dong Z. Secure networked control systems under denial of service attacks. In: Proceedings of the 18th IFAC World Congress, Milano, Italy: 2011. 8908−8913

13 Sinopoli B, Schenato L, Franceschetti M, Poolla K, Jordan M I, Sastry S S. Kalman filtering with inteslittent observations. *IEEE Transactions on Automatic Control*, 2004, **49**(9): 1453−1464

14 Li X, Sun S. Robust H_∞, Control for networked systems with random packet dropouts and time delays. *Procedia Engineering*, 2012, **29**: 4192−4197

15 Moon J, Basar T. Control over TCP-like lossy networks: A dynamic game approach. In: Proceedings of the American Control Conference. New York, USA: IEEE, 2013. 1578−1583

16 Shi Ming-Guang, Chen Wu-Wei. Mixed H_2/H_∞ control based on game theory and its application to the vehicle active suspension system. *Control Theory and Applications*, 2005, **22**(6): 882−888
(史明光, 陈无畏. 基于博弈论的 H_2/H_∞ 混合控制及其在汽车主动悬架中的应用. 控制理论与应用, 2005, **22**(6): 882−888)

17 Zhu Chao-Qun, Guo Ge. Optimal control for event- triggered networked control systems. *Control and Decision*,

2014, **29**(5): 802−808
(祝超群, 郭戈. 事件驱动的网络化系统最优控制. 控制与决策, 2014, **29**(5): 802−808)

18 Li Hai-Tao, Tang Gong-You, Ma Hui. Optimal control for a class of networked control systems with data packet dropout. *Control and Decision*, 2009, **24**(5): 773−776
(李海涛, 唐功友, 马慧. 一类具有数据包丢失的网络控制系统的最优控制. 控制与决策, 2009, **24**(5): 773−776)

19 Shoukry Y, Araujo J, Tabuada P, Srivastava Me, Johansson K H. Minimax control for cyber-physical systems under network packet scheduling attacks. In: Proceedings of the 2nd ACM International Conference on High Confidence Networked Systems. New York, USA: ACM, 2013. 93−100

20 Basar T, Bernhard P. *H_∞-optimal Control and Related Minimax Design Problems: a Dynamic Game Approach*. Springer Science and Business Media, Birkhäuser Boston, 2008.

21 Zhang Fen. Research The Problem of Differential Games Based on The Optimal Control [Master thesis], Yunnan Normal University, 2015.
(张芬. 基于最优控制的微分博弈问题研究 [硕士学位论文], 云南师范大学, 2015.)

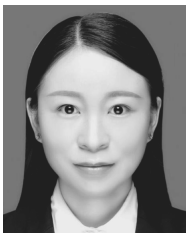
22 Araújo J. Design, Implementation and Validation of Resource-Aware and Resilient Wireless Networked Control Systems [Ph. D. dissertation], KTH Royal Institute of Technology, 2014.

23 Garone E, Sinopoli B, Goldsmith A, Casavola A. LQG control for MIMO systems over multiple erasure channels with perfect acknowledgment. *IEEE Transactions on Automatic Control*, 2012, **57**(2): 450−456

24 Changela M, Kumar A. Designing a controller for two tank interacting system. *International Journal of Science and Research (IJSR)*, 2015, **5**(4): 589−593

25 Wen Jing-Rong, Wu Mu-Qing, Su Jing-Fang. Cyber-physical System. *Acta Automatica Sinica*, 2012, **38**(4): 507−517
(温景容, 武穆清, 宿景芳. 信息物理融合系统. 自动化学报, 2012, **38**(4): 507−517)

庞 岩 大连理工大学航空航天学院副教授. 主要研究方向为混杂系统与非线性系统控制, 信息物理融合系统弹性控制. E-mail: ypang@dlut.edu.cn
(**PANG Yan** Associate professor at the School of Aeronautics and Astronautics, Dalian University of Technology. Her research interest covers control of hybrid and nonlinear systems, and resilient control of CPSs.)



王 娜 上海飞机设计研究院助理工程师. 2018 年于大连理工大学航空航天学院获得硕士学位. 主要研究方向为信息物理融合系统的安全控制, 飞机控制律设计. E-mail: wangna1@comac.cc
(**WANG Na** Assistant engineer at Shanghai Aircraft Design and Research Institute. She received her master degree from the School of Aeronautics and Astronautics, Dalian University of Technology in 2018. Her research interest covers secure control of cyber-physical systems, and aircraft control law design.)

夏 浩 大连理工大学控制科学与工程学院教授. 主要研究方向为控制器评价, 过程控制. 本文通信作者.
E-mail: hao.x.xia@dlut.edu.cn
(**XIA Hao** Professor at the School of Control Science and Engineering, Dalian University of Technology. His research interest covers control system performance assessment and advance process control. Corresponding author of this paper.)