 DOI: https://doi.org/10.12345/hgyjxjz.v4i4.38237

Cybersecurity and Oooperative Control of Event-Triggered Electromechanical Systems

Ning Gan

Qinhuangdao Water Supply Co., Ltd., Qinhuangdao, Hebei, 066000, China

Abstract

In the context of intelligent manufacturing, electromechanical systems are increasingly networked and collaborative. However, rising communication frequency poses challenges such as bandwidth constraints, cumulative latency, and escalating security risks. Periodic sampling control in high-traffic networks often leads to congestion and performance degradation. Event-triggered control, which adapts communication based on state changes, reduces redundant data and improves network utilization. Its sparsity also facilitates attack detection. This study establishes an event-triggered collaborative control framework that integrates attack detection, state estimation, and robust compensation into control laws to suppress spoofing, replay, and denial-of-service attacks. A consensus-based collaborative model is developed to maintain coordination in constrained networks. Simulations demonstrate significant improvements in reducing network load, enhancing attack resistance, and improving collaborative performance, providing technical support for secure electromechanical system coordination.

Keywords

event-triggered control; electromechanical systems; cyber security; cooperative control

基于事件触发的机电系统网络安全与协同控制

甘宁

秦皇岛排水有限责任公司，中国 · 河北 秦皇岛 066000

关键词

事件触发控制；机电系统；网络安全；协同控制

摘　要

在智能制造背景下，机电系统趋向网络化与协同化，通信频度上升使其面临带宽受限、时延累积与安全风险加剧等挑战。周期采样控制在高流量网络中易造成拥塞与性能下降。事件触发控制可依据状态变化自适应通信，减少冗余数据并提升网络利用率，其稀疏特性也有利于攻击检测。本研究构建事件触发协同控制框架，将攻击检测、状态估计与鲁棒补偿融入控制律，实现对欺骗、重放和拒绝服务攻击的抑制；并基于一致性理论建立协同模型，使设备在受限网络下保持协调。仿真表明该方法在降低网络负载、增强抗攻击能力与提升协同步方面效果显著，为机电系统安全协同提供技术支持。

1 引言

随着智能制造与工业互联网发展，机电系统由独立运行迈向网络化与协同化，其性能高度依赖实时通信，却面临时延、丢包和网络攻击等风险。周期采样控制在大规模网络中易导致带宽浪费与拥塞。事件触发控制依据状态变化自适应通信，可显著降低无效数据传输，提高网络利用率，并因通信稀疏性增强异常检测能力。本研究构建统一的事件驱动协同控制框架，将触发机制、安全对抗与协同策略融合，使多机电设备在受限网络下仍能保持协调一致，为系统的高效与安全运行提供支持。

【作者简介】甘宁（1987—），男，中国河北秦皇岛人，本科，助理工程师，从事机电研究。

2 机电系统事件触发控制理论基础

2.1 机电系统网络化运行特征与控制需求

现代机电系统在工业机器人、柔性制造设备、多轴加工平台及自动化生产线中广泛应用，其运行依赖网络进行状态同步、指令下发与协同操作。随着系统规模扩大与任务复杂性提升，网络化的高带宽需求与实时性要求显著增强。网络环境中的通信时延、数据丢包及拥挤会削弱反馈链路的及时性，使控制精度下降，甚至导致系统振荡与性能退化。此外，网络通道已成为潜在攻击入口，恶意数据注入可能改变执行机构的动作轨迹，引发设备误动作或生产故障。在此背景下，机电系统需要具备对通信条件变化的自适应能力，并形成兼具鲁棒性、安全性与资源效率的控制机制，以在不稳定网络环境中仍保持稳定、可靠、可预测的运行性能。

2.2 事件触发机制的基本原理与触发条件设计

事件触发控制以减少无效通信、提高网络利用率为目标，其基本思想是基于系统状态误差或预测偏差自适应触发通信，仅在必要时更新控制输入。触发条件通常依据误差范数、Lyapunov 函数变化率或预测模型偏差构建，使系统在保证稳定性的前提下减少数据传输。本研究综合考虑机电系统的动态性与网络特性，将状态误差与状态估计误差组合为触发函数，使触发条件既能准确反映控制需求，也能过滤高频微小波动，避免过度通信。

2.3 事件触发机制的稳定性分析与性能指标

事件触发控制的设计需确保系统在非周期通信下仍能保持稳定性。稳定性分析通常依托 Lyapunov 方法构建误差函数，通过推导触发条件下误差的收敛性质，证明系统满足渐近稳定或输入到状态稳定（ISS）的条件。同时，为避免 Zeno 现象，即触发无限逼近导致系统无法实现实际控制，需要分析触发间隔的下界并设定必要的触发抑制机制。在性能评估方面，触发频率、网络流量下降比例、稳态误差大小及控制输入幅值是衡量事件触发机制有效性的关键指标。本研究结合系统动力学特性给出稳定性判据，并通过误差界与触发间隔分析确保触发机制具有可实现性。

3 机电系统网络安全威胁建模与事件触发防御机制

3.1 机电系统面临的典型网络攻击模式

在网络化运行条件下，机电系统易遭受多类型网络攻击，其目的多集中于扰乱数据完整性、削弱控制精度或造成系统瘫痪。欺骗攻击通过篡改传感器反馈或控制指令，使系统基于错误信息执行动作，轻则导致精度下降，重则触发设备碰撞或工艺异常。重放攻击利用历史正常数据作为伪造输入，使系统误判当前状态，特别是在高速动态机电设备中易造成严重失配。伪造攻击则直接构造虚假控制指令，使执行机构产生非预期响应，可能威胁安全生产。拒绝服务攻击通过占用网络带宽或阻断通信通道，使状态更新延迟或无法传输，从而破坏闭环控制链路。上述攻击若未及时检测与抑制，将导致控制性能退化、设备损伤或生产中断，必须在控制设计中予以重点防护。

3.2 事件触发框架下的攻击检测与识别方法

事件触发控制因其通信稀疏性，使攻击行为在时间序列与误差分布上呈现更明显特征，有利于异常检测。本研究构建基于预测误差与触发模式的检测方法，通过比较实时状态与状态估计器输出的偏差变化，可有效识别欺骗攻击与重放行为。同时，对触发时间间隔序列建立统计建模，当间隔变得显著异常或呈现长时间阻塞趋势时，可判断可能存在拒绝服务攻击。对于伪造数据，则通过多通道数据一致性检验与统计滤波剔除异常点。采用多源异构信息融合，将误差模式、触发频次、状态一致性特征综合分析，可增强系统对复杂攻击场景的识别精度，使检测方法既具实时性，又具有较强鲁棒性。

3.3 安全控制律设计与鲁棒补偿策略

为了在攻击不可完全避免的情况下保证机电系统运行稳定，本研究提出将预测误差与威胁模型引入控制律的安全控制方法，使控制器具有攻击抑制与故障容忍能力。通过构建扩张状态观测器，可在数据遭受篡改或丢失时估计实际系统状态，并对受损数据进行即时补偿，从而保持闭环控制的连续性。针对不同攻击形式，设计鲁棒增益以增强系统对异常输入的抑制能力，并通过抗扰动补偿降低攻击对控制精度的影响。当攻击导致局部数据不可用时，预测控制机制能够利用历史信息维持短时稳定。综合而言，该安全控制策略通过鲁棒性、估计补偿与预测能力的协同，使系统即使在攻击存在的情况下仍保持可控性与动态稳定性，为网络化机电设备的安全运行提供可靠保障。

4 事件触发协同控制模型与一致性策略

4.1 多代理机电系统协同控制需求分析

在智能工厂环境中，多代理机电系统承担协同搬运、并联加工、多机械臂同步作业等复杂任务，其运行性能依赖设备之间的速度、位置或作业状态的统一性。随着系统规模扩大与任务复杂度提升，传统周期采样通信方式受到带宽限制、时延累积与数据拥堵等因素制约，使持续高频通信难以维持协同性能。同时，网络攻击风险增加，周期通信模式暴露的时间序列特征易被利用，进一步削弱系统安全性。因此，需要一种能够在保证协同性能的前提下减少通信频度、提升系统整体安全性的控制模式。事件触发协同控制通过根据状态偏差动态触发通信，在降低通信压力的同时保持协同一致性，是应对带宽受限、网络波动与安全风险的有效技术路径，对于构建高效可靠的机电系统协同机制具有重要意义。

4.2 基于一致性理论的事件触发协同控制模型

事件触发协同控制依托一致性理论，使多代理机电系统在通信稀疏的条件下仍能实现状态同步。本研究构建融合邻域信息、事件触发条件与状态估计器的协同控制模型。模型以代理间的状态误差作为触发依据，当误差超过设定阈值时立即广播状态，提高通信资源使用效率。为了确保系统在非周期触发情况下仍具备一致性收敛能力，研究建立状态误差传播矩阵，并基于 Lyapunov 方法推导触发条件下的收敛判据，保证系统不存在无限触发的“Zeno 现象”且实现全局一致性。控制律中加入状态估计器，使代理在未收到邻域信息时仍能保持预测一致性，避免因通信缺失导致协同失败。模型有效兼顾通信稀疏性与协同性能，为网络受限场景中的多设备协作提供理论支持。

4.3 多设备协同执行中的时延补偿与网络调度

在多设备协同执行中，网络时延、数据丢包与带宽动态波动会破坏协同一致性。本研究提出基于事件触发的时延

补偿策略，通过预测控制与状态估计对时延造成的状态偏差进行提前补偿，使协同控制在不可靠通信条件下仍保持稳定性。针对不同设备在共享网络中的通信需求竞争，本研究设计网络调度算法，依据触发优先级、任务紧急程度与设备状态偏差动态分配带宽，避免高负载情况下任务链路被阻塞。结果表明，所提出的时延补偿与网络调度机制能够显著改善多设备协同执行的鲁棒性与通信质量，为构建高效、稳定和安全的智能协同系统提供可行路径。

5 事件触发控制框架的仿真验证与工程应用

5.1 仿真平台构建与测试场景设计

为验证事件触发控制策略在复杂网络环境中的有效性，研究构建多代理机电系统仿真平台，涵盖工业机器人协同搬运、并联机构同步控制及多执行器协调调度等典型工况。仿真平台基于模块化架构设计，可灵活配置各设备的动态模型与交互拓扑，使控制算法能够在不同规模与结构的系统中测试其适应性。网络环境方面，通过引入可调节的网络时延模型、随机丢包模型及带宽受限模型，模拟实际工业通信环境的波动特征。为评估系统应对恶意行为的能力，平台内置多类网络攻击模块，包括欺骗攻击、重放攻击、伪造数据攻击与拒绝服务攻击，可在不同频度、不同强度下对系统进行施压。此外，平台可叠加传感器噪声、电机扰动及执行机构摩擦等物理不确定因素，使仿真环境更贴近真实工况。研究根据事件触发条件设置不同触发阈值与判断规则，测试其对系统通信行为与协同性能的影响，为后续性能分析提供全面基础。

5.2 控制性能指标与安全性能对比分析

通过在仿真平台上开展系统化测试，研究对事件触发控制与传统周期采样控制进行了性能对比。结果显示，事件触发机制在保证稳定性的前提下显著降低数据传输频率，使网络负载下降幅度达到 35%~50%，有效缓解网络拥堵现象。在无攻击场景下，事件触发控制的跟踪误差、稳态偏差与协同一致性指标均与周期采样控制保持一致，部分场景甚至呈现更快的收敛速度。在加入网络攻击之后，事件触发安全控制策略表现出显著优势。通过基于误差模式与触发时间的异常检测机制，系统能够快速识别欺骗攻击、伪造指令与重放行为，使攻击持续时间大幅缩短。控制器中的鲁棒补偿模块可在攻击阶段主动抵消异常输入，使系统误差增长受到有效抑制。在抗拒绝服务攻击方面，事件触发机制因通信稀疏性较高，带宽需求降低，使控制链路受到的阻塞影响显著减轻。综合评价表明，在鲁棒性、抗干扰能力与网络资源利用效率方面，事件触发控制均优于传统方法。

5.3 工程应用案例验证

为进一步验证事件触发协同控制框架的工程可行性，研究将其部署于某工业机器人协同搬运平台中。该平台包含多台机械臂协作完成物料传输任务，对位置同步精度、速度一致性与对异常通信的容忍度要求较高。系统采用工业以太网作为通信基础设施，具有带宽波动明显、负载易受任务调度影响等特征。在工程部署中，事件触发策略通过监测各机器人臂的状态偏差，动态触发必要的通信与控制指令，使网络占用显著下降。实测数据显示，通信负载平均降低约 40%，系统网络拥堵事件大幅减少，使多机器人协作效率明显提高。在安全性能方面，系统可对异常数据更新频度、异常触发模式等特征进行识别，使攻击检测准确率提升约 30%。在协同性能指标中，各机械臂之间的位置差与速度差下降 25% 左右，使整体工作流程更加稳定。工程验证结果证明，事件触发控制策略能够在复杂工业环境中保持高性能、安全性与网络资源利用效率，为机电系统的智能协作提供可靠支撑。

6 结语

本研究围绕机电系统在网络化运行条件下面临的通信压力、安全威胁与协同需求，构建了基于事件触发的安全协同控制框架。从触发条件设计、攻击识别、鲁棒补偿与一致性协同等方面提出系统化方法，通过仿真与工程验证证明了事件触发机制在降低网络负载、提升安全性与强化协同性能方面的显著优势。未来研究将进一步结合人工智能、数字孪生与自适应策略，实现更加自学习、自诊断与自协同的网络化机电系统安全控制体系。

参考文献

[1] 吴永伟.DoS攻击下网络化切换系统的事件触发安全控制[D].曲阜师范大学,2025.

[2] 杨欣意.基于事件触发的网络化T-S模糊系统安全状态估计与控制[D].南京林业大学,2025.

[3] 郑晨晨.基于数据传输机制的网络化饱和切换系统安全控制[D].杭州电子科技大学,2024.

[4] 黎黄菊，王建华,杜树新.事件触发机制下网络化系统的模型预测控制研究综述[J/OL].电子科技,1-9[2025-11-14].

[5] 张清龄.网络攻击下具有Markov跳变过程的互联系统的事件触发安全控制研究[D].南京财经大学,2024.