# 基于 TrueTime 的网络控制系统 DoS 攻击仿真

曹航瑞[1]　陆馨宇[1]　苏芷蔓[2]　邬晶[2]　龙承念[2]
（1. 上海交通大学密西根学院，2. 上海交通大学自动化系，上海，200240）

**摘要**　随着工业互联网的不断开放及普及，针对网络控制系统(NCS)的恶意网络攻击不断发生，攻击下的网络控制系统研究成为了当前的研究热点，并获得一定的研究成果。本文介绍了一种基于实时仿真工具箱 TrueTime 的拒绝服务式攻击(DoS)仿真，以倒立摆系统为被控对象，研究了网络控制系统中 DoS 攻击对系统稳定性的影响，并通过设计合理的 PID 控制器保证系统的一定性能。仿真结果表明 DoS 攻击对系统的性能会产生不良影响，甚至破坏系统的稳定性。该仿真工具箱能模拟不同网络环境的实时网络控制系统，在研究 NCS 性能方面具有方便性和灵活性。

**关键词**　网络控制系统；TrueTime 工具箱；倒立摆；DoS 攻击

# Simulation of DoS Attack in Networked Control System Using TrueTime

Hangrui Cao[1], Xinyu Lu[1], Zhiman Su[2], Jing Wu[2], Chengnian Long[2]
(1. UMJI – Shanghai Jiao Tong University, 2. Department of Automation, Shanghai Jiao Tong University, Shanghai, 200240)

**Abstract**　*With the openness and popularization of the industrial networks, there are more and more malicious network attack aiming at decreasing the performance of networked control system (NCS), which has become the research hotspot recently. This paper introduces a Denial-of-Service (DoS) attack simulation based on the real-time simulation toolbox TrueTime. The influence of DoS attack on the system stability of NCS has been discussed and corresponding PID controller is designed to ensure the certain performance of the system under attacks. An inverted pendulum system is used to show that DoS attack will have negative effect on the performance of the system, and even damage the stability of the system. This way we used in simulation are flexible and can be extended to other real-time NCSs with different network environment.*

**keywords**　*Networked Control System; TrueTime Toolbox; Inverted Pendulum; DoS Attack*

## 0　引言

网络化控制系统(NCS)是由传统物理基础架构与信息基础架构共同组成[1]，借助先进的传感量测系统和灵活的通信基础设施，可以获取更加全面详细的系统实时运行数据[2]。其管理机制由传统的“采集+集中控制”向“采集+控制+区域自治”转变，提升了智能化管理水平。信息侧作为通信的支撑性部分，在 NCS 的正常运行中有着重要地位，但近年来利用信息通信网络存在的漏洞和安全缺陷对系统本身或资源进行的恶意攻击不断发生[3]，严重破坏了系统的保密性、完整性和可用性[4]。传统的只对 NCS 进行数值仿真的方法已无法保证其在攻击情形下仿真分析的准确性和实时性[5]，而网络控制系统的实时仿真平台能再现信息通信网络环境，以实际的物理流-信息流交互方式精确地满足各类仿真需求，是学者研究网络攻击对通信网络性能影响的重要平台。

实际上，国内外已建的网络化控制仿真平台有很多，目前常用的实时仿真软件有

收稿日期：2020-8-31
基金项目：国家自然科学基金（61873166，62073215）
作者简介：曹航瑞，男，上海交通大学密西根学院本科生，研究方向为网络控制系统的建模与分析，email: caohangrui@sjtu.edu.cn；陆馨宇，女，上海交通大学密西根学院本科生，研究方向为网络控制系统的建模与分析，email: xinyu_lu@sjtu.edu.cn；苏芷蔓，女，上海交通大学自动化系本科生，研究方向为网络控制系统的建模与分析，email: 17827776760@sjtu.edu.cn；邬晶，女，上海交通大学自动化系副教授，主要研究方向为信息物理系统的建模、分析与安全控制等，email: jingwu@sjtu.edu.cn （通讯作者）；龙承念，男，上海交通大学自动化系教授，主要研究方向为物联网、信息物理系统、区块链等，email：longcn@sjtu.edu.cn。

TrueTime、NS2/NS3、OPNET、PowerSim、RTLAB、Pscad、Jitterbug 等。如 Martin Lévesque 等人展示了基于 OMNeT++和 OpenDSS 的新型通信和配电网络协同仿真器的实现细节[6]；东南大学研究团队实现了基于 OPNET 和 RTLAB 的主从式 CPS 协同仿真平台[7]；浙江大学提出了基于 RTLAB、DSP 控制器、OPNET 和主站的半实物实时仿真架构[8]。此外，基于TrueTime工具箱，文献[9]对比了不同通信网络协议下的时延分布规律和时延大小对 NCS 动态性能响应的影响；文献[10]研究了具有干扰攻击和网络延迟补偿的无线控制系统的稳定性；文献[11]利用 TrueTime2.0 搭建了网络控制系统的时延补偿策略模型。然而，上述文献主要是针对网络本身对系统的影响进行了仿真验证，没有考虑恶意攻击对系统带来的影响。

本文将基于 TrueTime 工具包，研究拒绝服务攻击下 NCS 系统的性能变化。通过搭建的网络化控制系统，设计了攻击下的 PID 控制器，最后，仿真验证了所设计控制器的有效性。

# 1 问题描述

网络控制系统(Networked Control System, NCS)是通过一系列有线或无线网络、网络节点构成的闭环控制系统，本文考虑如图1所示的网络控制系统。

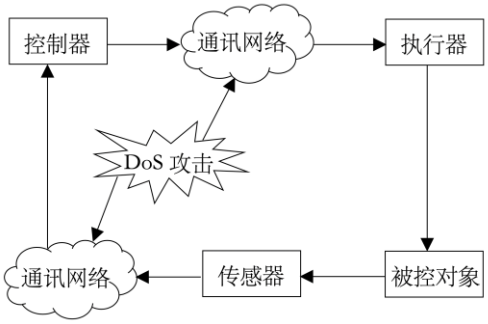


**图 1 DoS 攻击下的网络控制系统结构图**

其中传感器，控制器，执行器和被控对象通过通信网络进行实时的数据通信。被控对象可由如下线性非时变的系统模型表示：

$$\begin{cases}\dot{x}(t) = Ax(t) + Bu(t) \\ y(t) = Cx(t) + Du(t)\end{cases} \quad (1)$$

其中，$x(t)$是系统的状态向量，$y(t)$是输出向量，$u(t)$是系统的控制输入向量，$A, B, C, D$是适当维数的已知矩阵。传感器的工作方式为时间驱动，周期性采样并发送来自被控对象的输出信息，当该时刻为采样时间点时，传感器进行一次采样并处理数据，发送给控制器；控制器接受到来自传感器的输出后与参考输入作比较并计算控制信息，将控制量发送给执行器；执行器接收并处理来自控制器的控制量，发送信息给被控对象来执行命令。本文对该网络控制系统采取的攻击方式为 DoS 攻击，通过发送大量干扰数据占用网络节点的信息处理时间，造成控制器或执行器在一定时间内无法接收到有效信息或接收到的信息因干扰而失真[12]。

本文利用 TrueTime 工具箱进行仿真，验证 DoS 攻击对网络控制系统性能的影响。

# 2 仿真模型搭建

## 2.1 TrueTime 工具箱

Matlab/Simulink 能反应控制系统的性能，TrueTime 是基于 Matlab 的实时网络控制仿真工具箱，用于仿真网络特性，其包括 TrueTime Kernel 和 TrueTime Network 模块[13]。

### 2.1.1 Truetime Kernel

TrueTime Kernel 模块主要用于仿真 NCS 的网络节点，即传感器、控制器、执行器和干扰节点，其模块图如图2所示。该模块的接口中，A/D 和 D/A 用于实现数字信号和模拟信号的转换。传感器采用 ttAnalogIn()函数接收来自系统的信号，并用 ttSendMsg()函数发送至控制器。控制器使用 ttGetMsg()接收信号，然后使用 ttSendMsg()发送信号至执行器。执行器使用 ttGetMsg()接收信号并使用 ttAnalogOut()发送信号至系统，由此构成闭环回路。其中，攻击者使用 ttSendMsg()函数向通信网络发送干扰信息。

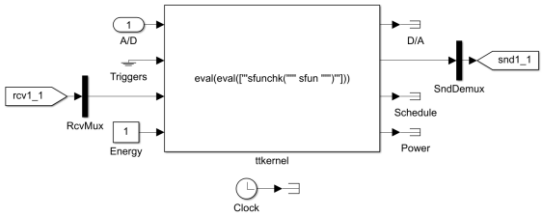


**图 2 TrueTime Kernel 模块示意图**

### 2.1.2 Truetime Network

TrueTime Network 模块用于网络节点之间的通信，采用事件驱动的方式工作，即当信息到达网络时模块运作。模块中 Rcv 口接收 Kernel 模块发送来的信号，信号经网络传输后由 Snd 口向 Kernel 模块发出。本文中的 Network 模块包含 3 个网络节点，如图 3 所示，其中节点 1 是攻击模块发送攻击干扰信号的通道，传感器发出的采样信号经节点 2 传输至控制器，控制器发出的控制信号经节点 3 传输至执行器。

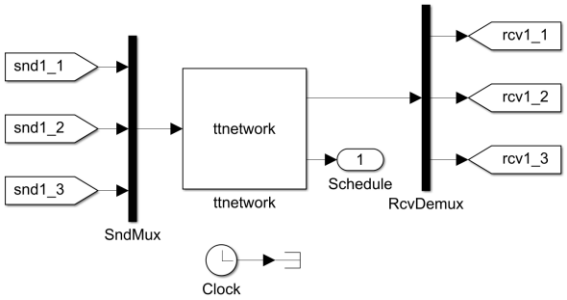


**图 3 TrueTime Network 模块示意图**

## 2.2 基于 TrueTime 网络系统模型的建立

利用上一部分所介绍的 TrueTime 工具，建立图 4 所示的网络模型：

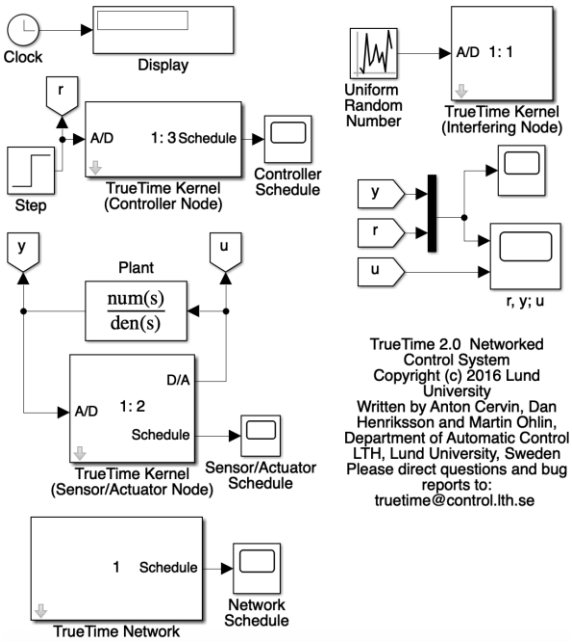


**图 4 基于 TrueTime 2.0 的网络仿真模型**

该网络模型由 Network Kernel, Controller, Sensor, Actuator, Plant 及攻击的 Interference Kernel 组成。各部分之间的信号传输时通过 TrueTime 中的函数

1. 在网络模块(TrueTime Network)中配置网络协议，传输率，最小帧长；可支持 CSMA/CD， CSMA/AMP 等六种网络模型。

2. Plant 部分是所研究系统的传递函数，如 DC Servo, 倒立摆，电网系统等模型。

3. 传感器采用时间驱动，以定常采样周期 h 对系统状态进行采样。

4. 控制器内部算法通过在 Controller 的对应的初始化函数中，创建对应计算的任务实现。

5. 攻击具有一定的能量约束，且能持续一定的周期，它将干扰真实数据使其失真或拥塞网络传输信道，导致系统接收的信号噪声太大而主动丢掉或接收不到信号。设计合理的控制器，保证系统的稳定性。

## 2.3 控制器设计

控制器采用离散下 PID 的控制算法。其中，比例项 P 对应比例控制，积分项 I 是与误差的时间积分成比例的控制，用于调节稳态误差，导数项 D 正比于控制误差的时间导数，用于调节达到稳态时间。对各控制信号表达式如下:

$$P(k) = K\big(br(t_k) - y(t_k)\big) \tag{2}$$

$$I(k+1) = I(k) + \frac{Kh}{T_i}\big(r(t_k) - y(t_k)\big) \tag{3}$$

$$D(k) = a_d D(t_{k-1}) + b_d\big(y(t_{k-1}) - y(t_k)\big) \tag{4}$$

$$u(k) = P(k) + I(k) + D(k) \tag{5}$$

$$a_d = \frac{T_d}{Nh + T_d},\ b_d = \frac{NKT_d}{Nh + T_d} \tag{6}$$

其中，$P(k)$为比例单元，$I(k)$为积分单元，$D(k)$为微分单元，$r(t_k)$为参考信号，$y(t_k)$为输出信号，$u(k)$为控制信号，$K$为比例增益系数，$b$为比例设定点权重，$t_k$为采样时刻，$T_i$为积分时间常数，$T_d$为微分时间常数，$h$为采样周期，$N$为每秒经过零点的平均次数。引入参数$K_d = T_d * K_p, K_i = K_p/T_i$ ，则其传递参数的形式可以写为：

$$G(s) = \frac{K_d s^2 + K_p s + K_i}{s}$$

通过调节参数$K_p, K_i, K_d$保证系统的稳定性。

# 3 仿真验证

本文以一级倒立摆系统为例，对攻击下的倒立摆系统进行性能测试及相应的 PID 控制器。首先，考虑系统在没有 DoS 攻击下的情况系统的性能，其次，验证加入 DoS 攻击后系统的稳定性是否被破坏，若 DoS 攻击明显影响系统性能，则需设计攻击下的控制器参数，保证系统在 DoS 攻击下也可稳定。

系统的初始设置如下，网络模块中网络协议为 CSMA/AMP(CAN), 传输率为 80000bit/s, 最小帧长为 80bits, 丢包率为 0, 各模块内时延为 0.0005s.

## 3.1 倒立摆模型

直线型倒立摆结构图如图 5 所示：

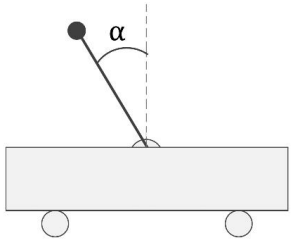


**图 5 直线型一级倒立摆系统**

其系统模型满足式(1)，状态变量为

$$x(t)=\begin{bmatrix} z(t) \\ \dot{z}(t) \\ \alpha(t) \\ \dot{\alpha}(t) \end{bmatrix}$$

其中，$z(t)$表示小车位移，$\dot{z}(t)$为小车的加速度，$\alpha(t)$表示摆杆与法线方向的夹角，$\dot{\alpha}(t)$是夹角的加速度。系统矩阵满足如下形式：

$$A=\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & -\frac{b(J+mL^2)}{K} & \frac{m^2L^2g}{K} & -\frac{mLc}{K} \\ 0 & 0 & 0 & 1 \\ 0 & -\frac{mLb}{K} & \frac{mLg(K+m^2L^2)}{K(J+mL^2)} & -\frac{c(m^2L^2+K)}{K(J+mL^2)} \end{bmatrix}$$

$$\mathrm{B}=\begin{bmatrix} 0 \\ \frac{J+mL^2}{K} \\ 0 \\ \frac{mL}{K} \end{bmatrix},\ C=\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},\ D=0$$

其中，$m$为摆杆质量，$J$为转动惯量，$b$为小车滑动摩擦系数，$c$为摆杆转动摩擦系数，$L$为摆杆转动轴心到质心的长度。

取 $m=2,\ J=10,\ b=0.1,\ c=0.1,\ L=0.3$ 该系统的传递函数为：

$$G(s)=\frac{8s^2}{448.1s^4+4.401s^3-960s^2+8s}$$

显见，该连续系统存在两位于右半平面零点，该倒立摆系统开环不稳定，需要设计合适的控制器使得系统稳定。将该倒立摆系统用 Transfer Function 模块接入网络模型中作为 Plant.

### 3.2 无网络攻击下的控制器设计

当不存在网络攻击时，利用劳斯判据可得 PID 参数为$K_p=520, K_i=1000, K_d=240$, 使得系统稳定。其阶跃信号的响应曲线如图6所示。

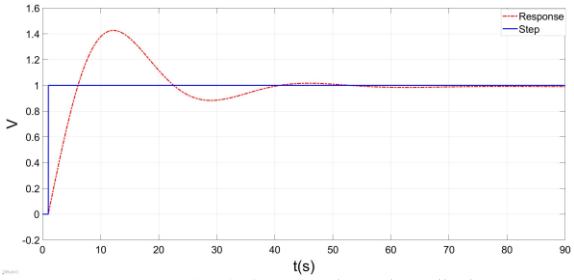


**图 6 无网络攻击下的阶跃响应曲线**

由图6可知，闭环系统稳定，且能跟踪上单位阶跃输入信号。

### 3.3 不同网络协议下的输出响应曲线

假设攻击的幅值$\gamma \le 0.05$，攻击频率为$\omega=24000\ bit/s$，对 CSMA/CAN(CAN)，Roundrobin、FDMA 和 CSMA/CD(Eternet) 四种网络协议分别进行了测试。对应的阶跃信号响应曲线分别如图 7-10 所示。

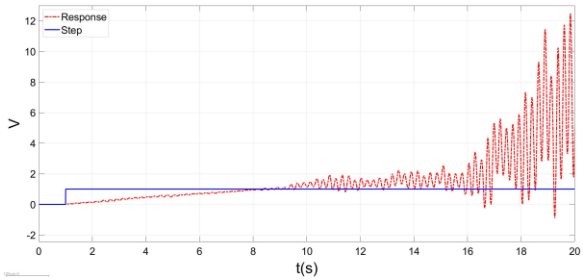


**图 7 CSMA/CAN(CAN)协议下的攻击阶跃响应**

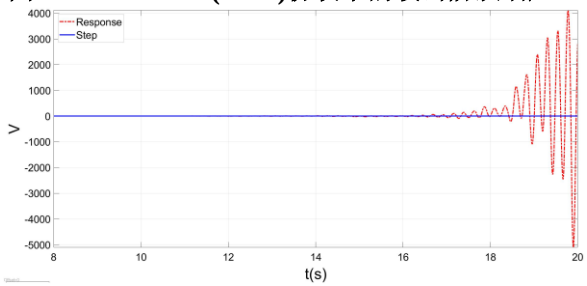


**图 8 Roundrobin 协议下的攻击阶跃响应**

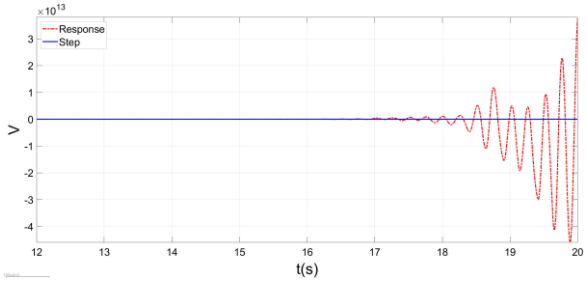


**图 9 FDMA 协议下的攻击阶跃响应**

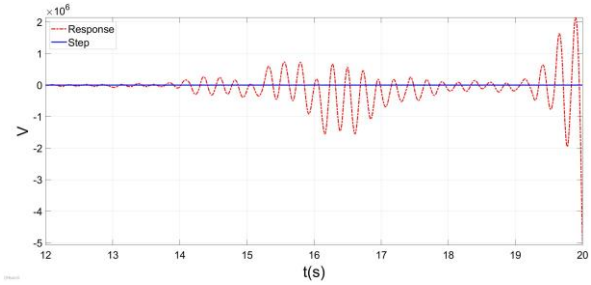


**图 10 CSMA/CD(Ethernet)协议下的攻击阶跃响应**

由图 7-10 可知，闭环系统均不稳定，说明 DoS 攻击能够对系统的性能产生影响，并且，没有考虑攻击影响下的控制器设计不一定能保证系统的性能。实际上，我们还对系统不存在攻击但有纯延时情形做了测试，测试结果表明无攻击情形下的控制器设计可以保证在最大容忍延时范围内系统依然稳定。此外，四种协议在相同的攻击下，CAN 协议最不敏感，发散速度缓慢。FDMA 协议和 Ethernet 协议较为敏感，发散速度较快。

### 3.4 网络攻击下的控制器优化

在考虑攻击的约束下，我们重新设计了 PID 控制器，其相应的参数为$K_p=1000, K_i=$

$2000, K_d = 180$，四个网络协议下的阶跃响应曲线如图 11-14 所示。

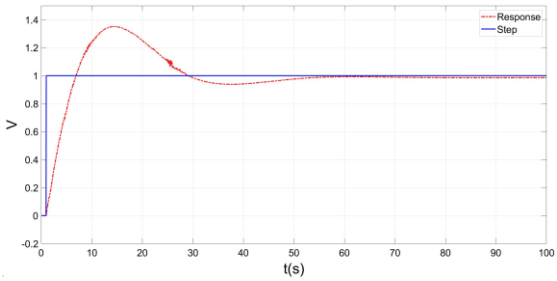


**图 11 攻击下的系统闭环响应曲线(CAN)**

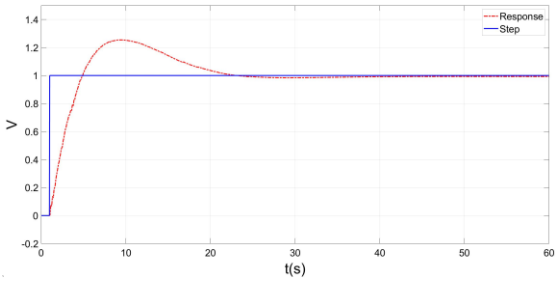


**图 12 攻击下的系统闭环响应曲线(Roundrobin)**

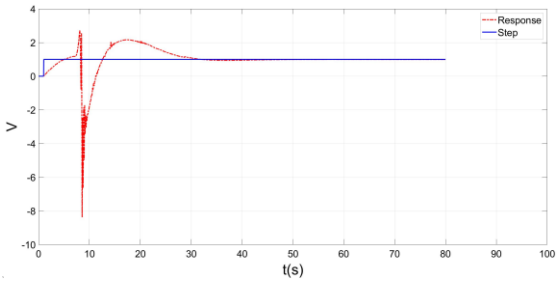


**图 13 攻击下的系统闭环响应曲线(Ethernet)**

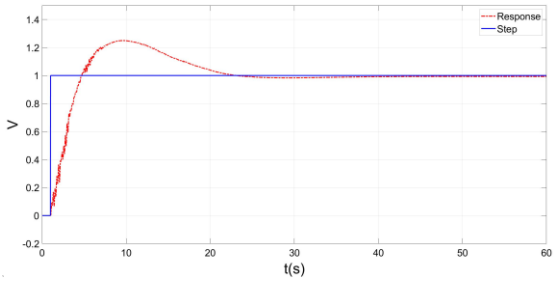


**图 14 攻击下的系统闭环响应曲线(FDMA)**

由图 11-14 可知，在考虑攻击情形下设计的 PID 控制器可以使系统最终达到稳定。其中，CAN 协议下的调整时间较长，FDMA 协议和 Ethernet 协议下的动态特性都有较多的振荡，尤其是 Ethernet，在 9 秒的时候有一个较大的波动。

# 4 结论

本文主要利用 TrueTime 工具箱研究了网络控制系统在有网络攻击、无网络攻击下的响应。利用 TrueTime 工具箱，分别对四种不同协议下的攻击进行了模拟，分析了不同协议下攻击对网络控制系统性能的影响。并验证了考虑攻击的控制器设计的重要性。

## 参考文献


[1] 李中伟, 佟为明, 金显吉. 智能电网信息安全防御体系与信息安全测试系统构建乌克兰和以色列国家电网遭受网络攻击事件的思考与启示[J]. 电力系统自动化,2016,40(08):147-151.

[2] 安宇,刘东,陈飞,徐玮韡.考虑信息攻击的配电网信息物理运行风险分析[J].电网技术,2019,43(07):2345-2352.

[3] 汤奕, 陈倩, 李梦雅, 王琦, 倪明, 梁云. 电力信息物理融合系统环境中的网络攻击研究综述[J]. 电力系统自动化, 2016,40(17):59-69.

[4] 王琦, 李梦雅, 汤奕, 倪明. 电力信息物理系统网络攻击与防御研究综述(一)建模与评估[J]. 电力系统自动化, 2019,43(09):9-21.

[5] 孙平远, 刘科研, 齐冬莲. 基于电力信息物理系统实时仿真平台的网络安全仿真[J].电力建设,2020,41(02):40-46.

[6] Lévesque M, Xu D Q, Joós G, et al. Communications and power distribution network co-simulation for multidisciplinary smart grid experimentations[C]//Proceedings of the 45th Annual Simulation Symposium. 2012: 1-7.

[7] 周力,吴在军,孙军,苏晨,顾伟,施玉祥.融合时间同步策略的主从式信息物理系统协同仿真平台实现[J].电力系统自动化,2017,41(10):9-15+91.

[8] 裴涤. 配电网 CPS 信息系统异常检测与半实物仿真研究[D].浙江大学,2018.

[9] 许超. 具有长时延的网络控制系统时延补偿与调度研究[D].大连交通大学,2019.

[10] Liu Y, Sun Z. Delay compensation for interference attacks in IWSN-based Wireless Control System[C]//2019 Chinese Control Conference (CCC). IEEE, 2019: 3491-3496.

[11] 韩建伟.基于 TrueTime 的网络控制系统时延补偿策略的研究[D].哈尔滨理工大学,2018.

[12] Zhang H, Cheng P, Shi L, et al. Optimal dos attack scheduling in wireless networked control system[J]. IEEE Transactions on Control Systems Technology, 2016, 24(3): 843-852.

[13] 王俊杰,孙君曼.基于 TrueTime 的网络化控制系统仿真平台的构建[J].郑州轻工业学院学报(自然科学版), 2011,26(1):79-82. DOI:10.3969/j.issn.1004-1478.2011.01.020.