文章编号: 1001-0920(2019)04-0799-06 DOI: 10.13195/j.kzyjc.2017.1269

基于安全路径及丢包补偿的无线控制系统的丢包控制

孙子文[1,2†], 刘余辉[1]

(1. 江南大学 物联网工程学院，江苏 无锡 214122；
2. 物联网技术应用教育部工程研究中心，江苏 无锡 214122)

摘 要: 工业无线传感器网络(IWSN)可以为控制系统提供无线通信,然而,工业环境和攻击引发的数据包丢失等问题会显著降低IWSN控制系统的性能,甚至会破坏整个系统的稳定性. 对此,采用构造通信数据路由的安全路径以降低丢包率与改进的PID控制器进行丢包补偿的组合方案,减小攻击对IWSN控制系统稳定性的影响. 在OPNET和Simulink/TrueTime平台进行联合仿真实验,以倒立摆作为被控对象,模拟控制系统在具有不同攻击节点数目的IWSN中的系统稳定性能. 仿真结果表明,安全路由路径和改进的PID控制器能够极大地提高控制系统的稳定性.

关键词: 工业无线传感器网络；丢包控制；攻击；安全路由路径；改进的PID控制器；稳定性

中图分类号: TP14 **文献标志码:** A

Packet loss control of wireless control system based on security path and packet loss compensation

SUN Zi-wen[1,2†], *LIU Yu-hui*[1]

(1. School of Internet of Things，Jiangnan University，Wuxi 214122，China；2. Engineering Research Center of Internet of Things Technology Applications of Ministry of Education，Wuxi 214122，China)

Abstract: Industrial wireless sensor network (IWSN) can provide wireless communication for the control system. However, packet losses caused by industrial environments and attacks can significantly degrade the performance of IWSN and can even destabilize an entire system. Therefore, a security path of the communication data's routing to reduce the packet losses rate and a modified PID controller to compensate for packet losses are proposed to reduce the influence of the network attack on the stability of IWSN control system. The control system applying the two proposed programs is simulated under various number of attack nodes by using OPNET and Simulink/TrueTime. An inverted pendulum is used as the object of the controller. Simulation results show that the combination of the optimal path and the modified PID controller can greatly improve the stability of the control system.

Keywords: IWSN；packet loss control；attacks；security routing path；modified PID controller；stability

0 引 言

工业无线传感器网络(Industrial wireless sensor networks, IWSN)相比于有线系统具有许多优点,如易于部署、降低运营成本、易于扩展等[1]. 标准工业过程控制系统定期执行控制回路中的模块,即传感器以固定速率将采样数据馈送到控制模块,控制器对输入进行计算并以相同速率向执行器发送命令,这种范式适用于可靠的有线网络[2]. 然而,控制系统有线网络部分(控制器-执行器间或传感器-执行器间)正在被IWSN所取代. 无线网络作为信息传输的途径,暴露于室外环境中,不可避免地会受到攻击干扰,使在传感器、控制器和执行器之间传输的数据包丢失,引发控制系统的传输延迟和瞬时错误等问题,影响控制系统的性能,甚至造成控制系统不稳定[3]. 所以,IWSN控制系统必须严格遵守可靠性规范才能具有较好的性能,否则将会导致系统运行失误. 在设计IWSN控制系统时,必须考虑针对攻击引发数据包丢失的安全补偿控制策略.

已有许多文献针对无线网络控制系统(Wireless network control system, WNCS)的数据包丢失问题进

收稿日期: 2017-09-24；**修回日期:** 2017-12-30.
基金项目: 国家自然科学基金项目(61373126)；中央高校基本科研业务费专项资金项目(JUSRP51510).
责任编委: 李忠奎.
作者简介: 孙子文(1968−), 女, 教授, 博士, 从事模式识别、人工智能、无线传感网络理论与技术和信息安全等研究；刘余辉(1994−), 男, 硕士生, 从事工业无线传感器网络的研究.
†通讯作者. E-mail: sunziwen@jiangnan.edu.cn.

行了研究. 文献[4]采用无线控制倒立摆基本方法,分析了数据包丢失情况下对系统稳定性能的影响;文献[5]采用一种PIDPLUS控制器,通过对PID控制器的积分和微分环节改进,使系统在非周期性信号更新或通信信息丢失的情况下能够正常工作;文献[6]将灰色广义预测控制引入WNCS 中,并结合队列机制,提出了补偿策略,从而实现了对传感器节点-控制器节点、控制器节点-执行器节点两处网络传输的数据包丢失的补偿控制. 然而,WNCS采用的是基于802.11通信协议的控制网络(如工业以太网、基于令牌环或令牌总线传输的控制网)[7],而IWSN控制系统是基于802.15.4通信协议.

IWSN可以安装在化学环境或振动的环境中,相比于WNCS控制网络需要更强的抗干扰能力. 文献[8]采用一种预测补偿器和改进的线性二次型补偿器组合方案,通过补偿IWSN控制系统前向和后向通道中丢失的数据包,提高了IWSN控制系统的性能. 然而,该方案仅考虑正常工业环境下的干扰(如金属摩擦、振动等),而没有考虑到IWSN中存在异常攻击时的情况. 目前,已有文献开始研究针对IWSN中的攻击问题,如文献[9]提出的一种针对IWSN的高效攻击方法,攻击者通过监听网络中的通信,并利用已知的参数可以获取数据传输的下一个信道信息,然后通过发送大量的干扰数据包与正常数据包发生碰撞,造成正常数据包的丢失,而数据包丢失会造成网络结构和参数的改变,以及控制命令的丢失,使系统崩溃而失去稳定.

为解决IWSN控制系统在攻击干扰情况下数据包丢失造成的系统稳定性问题,本文采用一种基于802.15.4通信协议的通信数据路由的安全路径与改进的PID控制器的组合方案. 当网络受到攻击时,安全路径的作用是找到一条受攻击影响造成数据包丢失最少的路径传输通信数据;而改进的PID 控制器旨在补偿反向通道中丢失的数据包.

1 IWSN控制系统简介

1.1 IWSN控制系统基本模型

典型IWSN控制系统主要由控制模块和若干无线传感器节点组成,如图1所示. 在IWSN控制系统中,传感器节点可以检测被控对象的各种参数,执行器和传感器节点采用时间驱动方式,以固定周期将采样数据经由IWSN送达控制模块;控制器采用事件驱动方式,当传感器数据到达控制器时,控制器立刻计算控制值并发送给执行器.

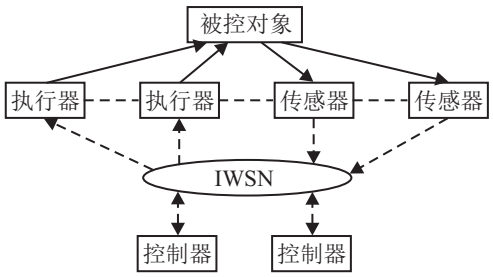


图1 IWSN控制系统基本模型

1.2 IWSN控制系统丢包时序模型

IWSN控制系统的通信丢失受工业设施多径衰落[10]和攻击的影响,无线网络会在传感器-控制器间和控制器-执行器间的信息传输中造成通信数据丢失,严重影响到控制系统的性能.

系统信息丢包时序模型如图2所示. 其中:$T_{\max}$是为接收数据包的节点设定的最大等待时间,如果超过$T_{\max}$时节点仍未接收到数据包,则可视为数据包丢失;k时刻执行器采样值y_k经控制器计算得到控制值为u_k.

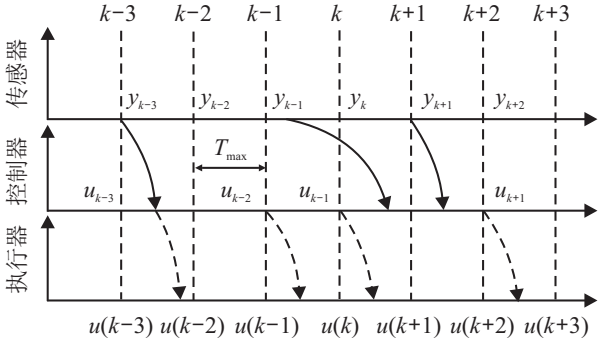


图2 系统信息丢包时序模型

IWSN中传输通信数据时存在两种造成数据包丢失的因素:

一是干扰引起数据包丢失[11]. 如在$[k-2,k-1]$区间无线网络受到外部信道干扰,数据包被全部丢弃,控制器没有收到来自传感器节点的测量信号,因此,$k-1$时刻会自动发出一个不确定的控制值.

二是攻击引起数据包丢失. 攻击节点为了达到攻击的目的,会发送大量恶意数据包,使网络产生拥塞[12]或选择性丢弃部分数据包[13]. 如在$[k-1,k]$区间无线网络产生拥塞,排队序列增加,增大正常数据包到达控制器的延迟,使正常数据包失效;或者在$[k+1,k+2]$区间,攻击节点随机丢弃部分重要信息,虽然部分数据包可以到达控制器,但控制器没能获得完整的数据. 这两种情况都使得控制器无法计算得到正确的控制值,因此,在k和$k+2$时刻控制器会自动发出一个不确定的控制值.

以上两种因素会不同程度地导致丢包的产生,使

系统控制器不能给出正确的控制值,如果不采取相应的措施,则可能会严重损坏控制系统的稳定性能.

2　提出方案

本文针对攻击造成的数据包丢失情况,研究如何提高IWSN控制系统稳定性问题. 为了解决该问题,采用组合解决方案:一是设计一条通信数据路由的安全路径,使这条路径受攻击影响的数据包丢失率最小;二是通过采用一种改进的PID控制器进行丢包补偿. 所采用组合方案的工业无线传感器网络控制系统丢包控制原理框图如图3所示.

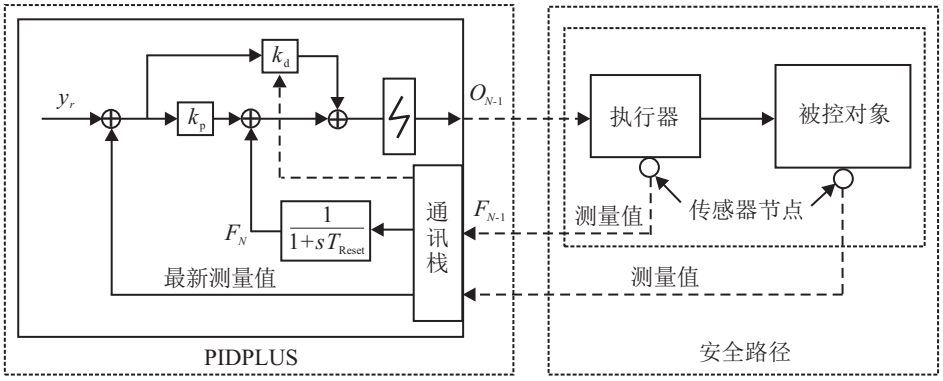


图 3　IWSN控制系统丢包控制原理框图

2.1　基于跟踪反馈机制的安全路由路径

2.1.1　安全路由路径构造策略

依据在源节点与网关节点间的数据包传输最短路由路径及最少丢包原则构造安全路由路径. 首先,源节点发送Hello数据包,将Hello数据包从源节点到网关节点的过程加入经过节点的ID号到标识符表H中,以跟踪数据包的流向. 然后,网关节点接收前n个到达的数据包并提取出标识符表H,采用反馈机制将H反向发送给源节点,获得时间延迟较小的几条路由路径. 最后,源节点按不同的路由路径发送相同数目的数据包,选择数据包丢失率最小的路径作为安全路由路径,用于后续发送测量数据包. 基于跟踪反馈机制的安全路由路径构造过程模型如图4所示,图中加粗虚线即为安全路由路径.

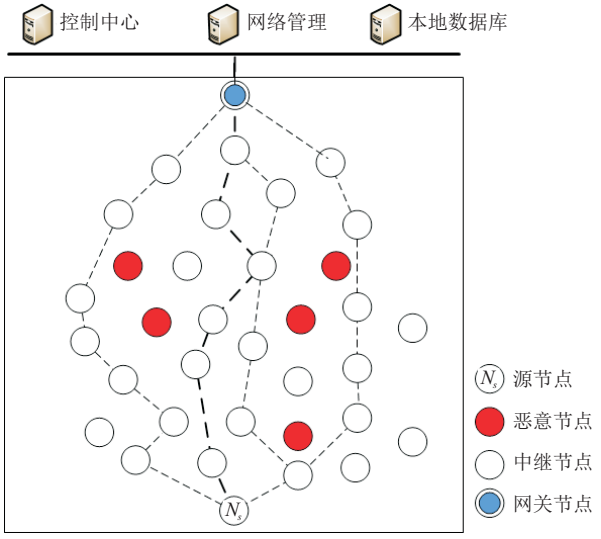


图 4　基于跟踪反馈机制的安全路由路径构造

2.1.2　安全路由路径构造算法

跟踪反馈机制安全路由路径的构造算法如下.

Step 1: 源节点N_s向周围节点发送Hello数据包,并在数据包内添加标识符表$H = \{l_1, l_2, \cdots, l_k\}$,其中$l_k$为第$k$个节点的ID,令其初始值为空;

Step 2: 当中继节点N_k接收到一个数据包时,如果N_k是正常节点,则N_k将自身标识l_k添加到H中;

Step 3: 当一个数据包P到达网关节点时,网关节点从数据包中抽取$H = \{l_1, l_2, \cdots, l_k\}$,将二元组$(N_s, H)$存储到本地数据库;

Step 4: 选择前n个到达网关节点的数据包经过的路径作为路由路径,可根据IWSN的范围、节点个数和传输速率判断n的大小;

Step 5: 网关节点将路由路径的标识符项H添加到一个广播消息中,利用路径反方向发送给源节点;

Step 6: 当广播消息到达源节点时,源节点抽取出路由路径$H_1, H_2, \cdots, H_n$,并按照不同的路由路径发送相同数目的数据包,比较每条路径的数据包丢失率,选择丢包率最小的路径作为安全路由路径.

2.2　控制器丢包补偿

当攻击节点数目较多时,安全路由路径并不能完全避免IWSN的数据包丢失,所以当发生数据包丢失时,必须考虑对数据包丢失的补偿控制.

PID控制器是控制系统中最常见的控制器,其比例部分使得系统响应迅速及时,积分部分可以消除余差,微分部分可以实现超前控制. 然而,当反馈值丢失时,标准PID控制存在两个主要问题:一是数据丢失期间控制器会继续执行,当数据丢失时,控制器会使

用最后一个测量值继续执行,输出将会根据最后一个测量值与设定值之间的误差继续动作;二是重新建立通信时输出出现突发变化,控制器在数据丢失后重新建立通信,新的控制值相比于反馈值丢失时的控制值差别很大,可能会使控制器的输出信号产生突变.

为了使控制系统在反馈值丢失时具有最佳控制,可以对PID进行重组. 本文中IWSN控制系统的控制器采用PIDPLUS控制器[5],如图3所示,通过将执行器反馈并入控制命令的计算中,并在通信建立时将积分和微分分量引入控制器输出的计算中来解决上述两个问题. 当传感器节点-控制器间的数据包丢失时,PIDPLUS控制器会根据过去的执行器和被控对象的测量值确定新的积分部分和微分部分的输出值,以确定控制器输出,从而在保证控制器输出不产生突发变化的同时控制执行器和被控对象继续动作.

积分部分由图3给出的滤波器$\dfrac{1}{1+sT_{\rm Reset}}$代替,滤波器同时接收有关执行器和被控对象的信息,执行器传达的测量信息用于计算滤波器的输出. 当正常通信时,滤波器的作用与常规积分部分的作用相同,且滤波器数据在新的测量值到达时被更新. 当数据包丢失时滤波器保持丢失前的最后一个输出(F_{N-1}),并且作为输入,用于计算新的滤波器输出(F_N). 滤波器的输出由下式计算:

$$F_N = F_{N-1} + (O_{N-1} - F_{N-1}) \times \left(1 - {\rm e}^{\frac{-\Delta T}{T_{\rm Reset}}}\right). \tag{1}$$

其中:F_N为新的滤波器输出,F_{N-1}为最后一次测量后的滤波器输出,O_{N-1}为控制器最后执行的输出值,ΔT为测量新值后经过的时间.

PIDPLUS控制器微分部分由下式给出:

$$O_D = k_d \cdot \frac{(e_N - e_{N-1})}{\Delta T}. \tag{2}$$

其中:e_N为当前误差,e_{N-1}为最后测量误差,ΔT为测量新值后经过的时间,O_D为控制器微分输出. 标准的PID控制器,其微分部分中的除数是信息传输的周期;而在PIDPLUS控制中,则是成功接收两次测量值之间经过的时间ΔT. 因此,PIDPLUS控制会比PID控制产生更小的微分动作.

2.3 被控对象的数学模型

采用一级直线型倒立摆作为被控对象,其结构如图5所示[14]. 倒立摆的控制目标是使摆杆始终保持在垂直状态. 为达到控制目的,控制器根据摆杆的角位移和其他参数确定作用于小车的力,控制小车前后移动,产生作用于摆杆的扭矩,使摆杆处于垂直状态.

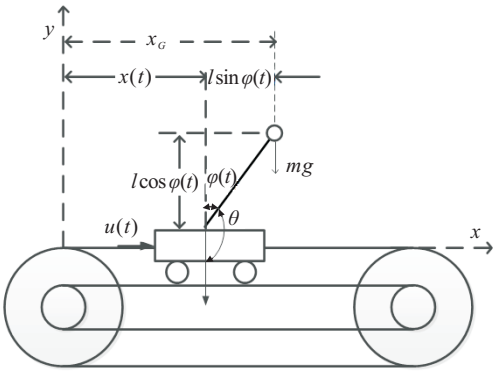


图5 倒立摆模型

忽略空气流动和各种摩擦,倒立摆系统可抽象成小车和匀质杆组成的系统. 假设小车质量和摆杆质量分别由M和m表示,b为小车摩擦系数,l为摆杆转动轴心到杆质心的长度,I为摆杆惯量,$u(t)$为控制小车沿着x坐标轴水平移动的力,$x(t)$和$\varphi(t)$分别为小车位置和摆杆与垂直向上方向的夹角,可由传感器节点实时检测,θ为摆杆与垂直向下方向的夹角. 应用牛顿定理得到系统运动方程

$$u(t) = (M+m)\ddot{x} + b\dot{x} + ml\ddot{\theta}\cos\theta - ml\dot{\theta}^2\sin\theta, \tag{3}$$

$$(I+ml^2)\ddot{\theta} + mgl\sin\theta = -ml\ddot{x}\cos\theta. \tag{4}$$

由式(3)和(4)可以得到传递函数

$$\frac{\phi(s)}{U(s)} = \frac{(ml/q)s^2}{s^4 + (b(I+ml^2)/q)s^3 - ((M+m)mgl/q)s^2 - (bmgl/q)s}. \tag{5}$$

其中:$q = [(M+m)(I+ml^2) - (ml)^2]$,$\phi(s)$是摆杆与垂直向上方向的夹角$\varphi(t)$的拉普拉斯函数,$U(s)$是作用力$u(t)$的拉普拉斯函数.

3 仿真与结果

运用Simulink/TrueTime进行IWSN控制系统仿真. 通过IWSN传输来自控制器的控制信号和来自传感器节点的反馈信号,同时通过使用PIDPLUS控制器稳定倒立摆系统.

由于Simulink/TrueTime工具箱没有对信道的建模过程,很难在无线网络中引入攻击节点并分析其对控制系统的影响[15]. 为了研究IWSN中的攻击对控制系统的影响,可以利用OPNET Modeler强大的无线信道建模功能分析攻击节点对IWSN控制系统稳定性的影响. 本文在控制系统中加入工业无线传感器网络,且只针对攻击造成数据包丢失的情况进行仿真. 通过联合仿真来分析数据包丢失对控制系统稳定性的影响.

3.1　安全路由路径对丢包的影响

使用OPNET进行网络仿真的参数配置如表1所示.

表 1　网络仿真参数

场景及参数设置	取值
仿真工具	OPNET14.5
MAC层	TDMA
传输速率/(Kbit/s)	250
工作频段/GHz	2.4
包大小/byte	256
仿真时间/s	400
仿真范围/m	500×500
通信距离/m	100
节点个数	30
路径个数	5

首先,依据数据包传输最短路由路径原则选择出在10个攻击节点下延迟相对较小的5条路由路径;然后,根据最少丢包原则选择丢包率最小的一条路由路径作为安全路径. 不同路由路径下的数据包丢失率如图6所示.

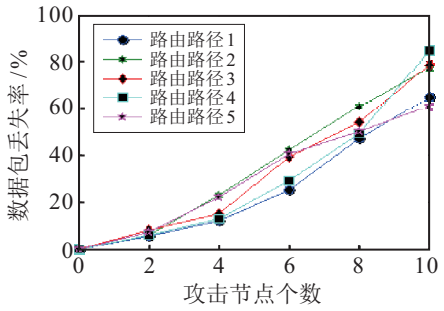


图 6　不同路由路径下的数据包丢失率

当攻击节点数目较少时,不同路由路径的数据包丢失率相差不大,且路径1受攻击影响造成的丢包率较少;然而,随着攻击节点数目的增加,不同路径的数据包丢失率都在上升,路径1受到的影响逐渐增大;当攻击节点数目为10时,路径5的丢包率低于路径1,因此,根据安全路由路径构造算法,选择路径5作为信息传输路径.

当攻击节点数目不同时,选取丢包率相对较小的一条路由路径作为传输路径. 所以,在不同攻击节点数目下,通过安全路由路径构造算法构造的传输路径是相对于其他几条路经丢包率最小的安全路径. 使用安全路由路径传输控制信息可以大大降低IWSN的数据包丢失率,当网络受到攻击时实现降低控制系统受到攻击影响的功能.

3.2　补偿控制对系统稳定性能的影响

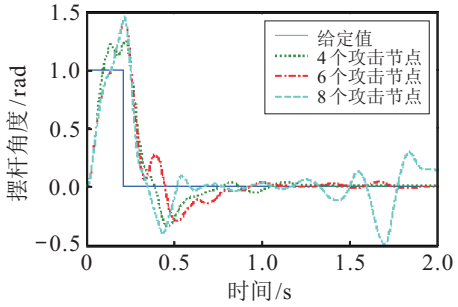
为了模拟PIDPLUS控制器对无线控制系统数据包丢失的补偿控制,以倒立摆作为无线网络控制系统的被控对象,以控制倒立摆模型的摆杆与垂直方向的夹角为目标. 倒立摆的参数设置如表2所示.

表 2　倒立摆参数

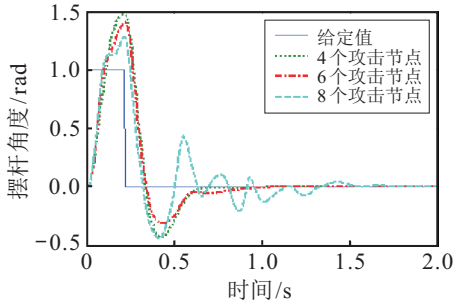
倒立摆参数设置	取值
小车质量 M/kg	1.096
摆杆质量 m/kg	0.109
摩擦系数 b	0.1
摆杆转动轴心到摆锤质心的长度 l/m	0.25
摆杆惯量 I/(kg·m^2)	0.003 4

忽略小车与摆杆转动轴心之间的摩擦系数. 利用参考临界比例度参数调节法,经过反复实时调整,确定当IWSN中不存在攻击节点时,系统超调量小于5%,调节时间为0.8 s时的PID控制参数为:比例增益为155,积分时间为0.35,微分时间为0.10.

IWSN控制系统在PID控制器控制下的摆杆的偏移角度随仿真时间的变化情况如图7(a)所示,初始时摆杆角度为0 rad,0时刻后小车受到作用力的干扰,摆杆角度发生偏移,且偏移角度受攻击节点个数的影响. 当IWSN中存在4个攻击节点时,摆杆轻微震荡,系统超调量大约为4%,且1.5 s后趋于稳定;当攻击节点个数增加到6个时,系统超调量变化不大,但摆杆震荡越来越剧烈,且在(0.9～1.7) s时角度在(−0.05～0.05) rad区间内摆动,1.7 s后才趋于稳定;当IWSN增加到8个攻击节点时,摆杆角度在(0.5～1.5) s时在(−0.1～0.1) rad范围内摆动,但在1.5 s后摆杆偏移角度增大,系统变得不稳定.



(a)　PID控制下的摆杆偏移角度



(b)　PIDPLUS控制下的摆杆偏移角度

图 7　不同控制器下的摆杆偏移角度

IWSN控制系统在PIDPLUS控制器作用下摆杆的偏移角度随仿真时间的变化情况如图7(b)所示. 当IWSN中存在4个攻击节点时, 系统超调量为4.5 %, 且在0.6 s后趋于稳定; 当攻击节点增加到6个时, 系统超调量减小但调节时间增大到1 s; 当IWSN增加到8个攻击节点时, 虽然摆杆震荡次数增大, 但仍然能在1.5 s趋于稳定.

通过比较图7所采用的PID和PIDPLUS控制器在不同的攻击节点个数下对IWSN控制系统稳定性的影响可知, 采用PIDPLUS控制器能改善IWSN控制系统在攻击造成无线通信数据丢失的情况下系统的稳定性能, 从而减小攻击对系统的影响.

4 结 论

基于IWSN的控制系统应能控制从控制中心到执行器的控制命令以及从传感器到控制中心的反馈信息的不可靠传输. 在本文中, 通过构造通信数据路由的安全路径来降低网络丢包率, 并且采用PIDPLUS控制器进行丢包补偿. 以倒立摆作为控制系统的被控对象, 采用OPNET和Simulink/TrueTime对所提出的方案进行联合仿真. 仿真结果表明, 采用安全路由路径与PIDPLUS控制器的组合方案, 不仅可以降低IWSN受到攻击时的数据包丢失率, 还能提高IWSN控制系统在数据包丢失时系统的稳定性.

参考文献(References)

[1] Sheela S J, Suresh K V, Tandur D. Security of industrial wireless sensor networks: A review[C]. Int Conf on Trends in Automation, Communications and Computing Technology. Bangalore: IEEE, 2016: 1-6.

[2] Song Jianping, Aloysius K Mok, Chen Deji, et al. Improving PID control with unreliable communications[C]. ISA EXPO Technical Conf. Houston, 2006: 17-19.

[3] Millán Y A, Vargas F, Molano F, et al. A wireless networked control systems review[C]. Robotics Symposium 2011 IEEE Ix Latin American and IEEE Colombian Conf on Automatic Control and Industry Applications[C]. Bogota: IEEE, 2011: 1-6.

[4] Bian Y, Jia J, Xu X, et al. Research on inverted pendulum network control technology[C]. The 3rd Int Conf on Measuring Technology and Mechatronics Automation. Shanghai: IEEE, 2011: 11-13.

[5] Kaltiokallio O, Eriksson L M, Bocca M. On the performance of the PIDPLUS controller in wireless control systems[C]. Control and Automation. Marrakech: IEEE, 2010: 707-714.

[6] 王天堃, 周黎辉, 韩璞, 等. 基于灰色广义预测控制的网络化控制系统丢包补偿[J]. 信息与控制, 2007, 36(3): 322-327.
(Wang T K, Zhou L H, Han P, et al. Compensation for packet dropout in networked control systems based on grey generalized predictive control[J]. Information and Control, 2007, 36(3): 322-327.)

[7] 张男. 基于无线传输的网络控制系统研究[D]. 秦皇岛: 燕山大学信息科学与工程学院, 2007.
(Zhang N. Research on network control system based on wireless transmission[D]. Qinhuangdao: School of Information Science and Engineering, Yanshan University, 2007.)

[8] Nguyen Vu-Anh-Quang. Packet loss compensation for control systems over industrial wireless sensor networks[J]. Int J of Distributed Sensor Networks, 2015, 2015(1): 1-9.

[9] Stojanovski S, Kulakov A. Efficient attacks in industrial wireless sensor networks[M]. ICT Innovations 2014. Cham: Springer, 2014: 289-298.

[10] Barac F, Gidlund M, Zhang T. PREED: Packet recovery by exploiting the determinism in industrial WSN communication[C]. Int Conf on Distributed Computing in Sensor Systems. Fortaleza: IEEE, 2015: 81-90.

[11] 孙业国, 秦世引. 网络控制系统研究进展[J]. 科技导报, 2010, 28(2): 109-115.
(Sun Y G, Qin S Y. Progress of networked control systems[J]. Science and Technology Review, 2010, 28(2): 109-115.)

[12] Zhuo S, Shokri-Ghadikolaei H, Fischione C, et al. Adaptive congestion control in cognitive industrial wireless sensor networks[C]. Int Conf on Industrial Informatics. Cambridge: IEEE, 2016: 900-907.

[13] Ju Ren. Adaptive and channel-aware detection of selective forwarding attacks in wireless sensor networks[J]. IEEE Trans on Wireless Communications, 2016, 15(5): 3718-3731.

[14] Wang Jia-Jun. Simulation studies of inverted pendulum based on PID controllers[J]. Simulation Modelling Practice and AMP Theory, 2011, 19(1): 440-449.

[15] 陈寅, 宋杨, 费敏锐. 基于Simulink和OPNET的NCS联合仿真平台的设计与开发[J]. 系统仿真学报, 2013, 25(7): 1518-1523.
(Chen Y, Song Y, Fei M R. Design and development of cosimulation platform for NCS based on Simulink and OPNET[J]. J of System Simulation, 2013, 25(7): 1518-1523.)

(责任编辑: 李君玲)