加密传输在工控系统安全中的可行性研究

梁 耀 [1] 冯冬芹 [1] 徐珊珊 [1] 陈思媛 [2] 高梦州 [1]

摘 要 针对需要对现场数据加密的工业控制系统 (Industrial control system, ICS), 基于稳定性判据设计一种加密传输机制的可行性评估模型, 结合超越方程 D-subdivision 求解法, 提出一种数据加密长度可行域求解算法. 改进 IAE (Integral absolute error) 并提出 Truncated IAE (TIAE)-based 指标, 用于评估可行域内不同数据长度对系统实时性能的影响. 利用嵌入式平台测定的加密算法执行时间与数据长度的关系, 评估了两种对称加密算法应用在他励直流电机控制系统中的可行性, 验证了可行域求解算法的准确性, 并获得了实时性能随数据长度的变化规律.

关键词 工业控制系统, 加密传输, 稳定性, 数据加密长度可行域, 实时性能, TIAE-based 指标

引用格式 梁耀, 冯冬芹, 徐珊珊, 陈思媛, 高梦州. 加密传输在工控系统安全中的可行性研究. 自动化学报, 2018, **44**(3): 434−442

DOI 10.16383/j.aas.2018.c160399

Feasibility Analysis of Encrypted Transmission on Security of Industrial Control Systems

LIANG Yao[1] FENG Dong-Qin[1] XU Shan-Shan[1] CHEN Si-Yuan[2] GAO Meng-Zhou[1]

Abstract For those industrial control systems (ICS) whose field data need to be encrypted, a model, based on stability criterion is designed to assess the feasibility of the encrypted transmition mechanism. Combined with D-subdivision solution to transcentdental equation, a method to solve the feasible region of the length of encrypted data quantitatively is proposed. Integral absolute error (IAE) is improved to introduce the truncated IAE (TIAE)-based index, which is designed for evaluating the real-time performance influenced by the length in the feasible region. In terms of the relationship between execute time of encryption algorithm and length measured on embedded platform, two symmetric encryption algorithms for the control system of separately excited DC motor are evaluated, the accuracy of solution to the feasible region is verified, and the change law between real-time performance and length is obtained.

Key words Industrial control system (ICS), encrypted transmission, stability, feasible region of length of encrypted data, real-time performance, truncated integral absolute error (TIAE)-based index

Citation Liang Yao, Feng Dong-Qin, Xu Shan-Shan, Chen Si-Yuan, Gao Meng-Zhou. Feasibility analysis of encrypted transmission on security of industrial control systems. *Acta Automatica Sinica*, 2018, **44**(3): 434−442

随着技术发展和管理决策的需要, 通用的通信网络和多样化的 IT 组件与工控系统 (Industrial control system, ICS) 不断融合, 原本封闭的工控系统开始更多地与外部企业网络互联, 使得 ICS 更容易受到来自网络的安全威胁[1]. 仅 2015 年, ICS-CERT 公布的发生在美国的工控系统安全问题多达 295 起[2], 工控系统遭受到网络攻击的威胁日趋严峻.

收稿日期 2016-05-16 录用日期 2016-12-27
Manuscript received May 16, 2016; accepted December 27, 2016
国家自然科学基金 (61223004) 资助
Supported by National Natural Science Foundation of China (61223004)
本文责任编委 陈积明
Recommended by Associate Editor CHEN Ji-Ming
1. 浙江大学工业控制技术国家重点实验室 杭州 310027 中国 2. 多伦多大学计算机与电子工程学院 多伦多 M4Y1M7 加拿大
1. State Key Laboratory of Industrial Control Technology, Zhejiang University, Hangzhou 310027, China 2. Engineering at Electrical and Computer Engineering Department, University of Toronto M4Y1M7, Canada

工业通信网络中存在着严重的数据安全隐患, 容易遭受到破坏数据完整性的攻击, 如错误数据注入攻击[3]、重放攻击[4] 等, 而数据加密作为一种保护数据完整性和机密性的手段, 可以有效地阻止上述攻击. Zijlstra[5] 基于异步事件驱动方法, 设计了一种单比特加密传输方案, 用于控制系统的防窃听和数据篡改攻击. Zhang 等[6] 基于 DES (Data encryption standard) 加密和改进灰色预测模型设计了一种抗 DoS (Denial of service) 和欺骗攻击机制. 尽管如此, 目前国内外针对密码学在工控系统中的应用研究仍处于起步阶段, 实际上, 对于工控系统中的一些工控设备而言, 其资源总量和处理速度有限, 引入加密传输后会影响通信网络中控制数据交互的实时性, 甚至严重干扰系统的稳定性. Wei 等[7] 在小规模电网平台上测试发现, 加密传输带来的延时会造成断路器动作不及时, 会导致电压波动幅度超过 20 %. 正是由于工控系统的特殊性, 使得目前

缺少一种有效的加密传输应用的可行性评估方法.

加密传输应用在工控系统中的前提是不破坏原系统的稳定性, 在该前提下才能进一步研究如何评估加密传输对实时性能的影响. 控制系统稳定性分析的研究成果相对成熟[8], 但直接用于加密传输稳定性分析的成果仍然较少. Sipahi 等[9] 基于特征根聚类分析的方法, 提出了二维延时空间内稳定域的数值解法. Olgac 等[10] 利用 D-subvision 超越方程求解法, 给出了稳定延时的精确数值解, 对于加密传输的稳定性分析具有参考意义. 而 Lyapunov 不等式、谱分析等稳定性判定方法, 由于不能给出精确的参数稳定域, 不具有定量分析价值.

实时性评估方法主要分成两类: 随机性评估方法和确定性评估方法. 随机性评估方法主要基于 Harris[11] 提出的最小方差控制 (Minimum variance controller, MVC) 指标, 该指标利用最小方差控制下的系统性能作为评价基准, 以此衡量当前系统的性能. 但是 Eriksson 等[12] 指出, MVC 并不能保证满意的动态性能, 而且该指标没有以加密传输之前系统的性能作为评价基准. 确定性评估方法主要利用上升时间、超调量、稳定时间等指标. Gupta 等[13] 通过简单的归一化加权, 综合超调量 $\sigma\,\%$ 和稳定时间 t_s 两个因素作为 DES 加密后系统实时性能评估值, 该评估值的优点在于可以灵活调整权重, 但同时各指标之间的相对权重难以确定, 评估结果存在主观性差异. Zeng 等[14] 设计了一种基于确定性指标的评估框架, 权衡考虑了 AES 加密后系统的性能指标与安全指标, 并基于协同演化算法求解了加密长度的最优解. 但该框架直接以跟踪误差的均方值作为性能指标, 没有给出采样个数 K 的选取规则, 也没有对该指标合理性论证, 最后没有对最优解的存在性进行验证. Yu 等[15] 通过计算跟踪误差的无穷积分, 提出了绝对误差积分 (Integrated absolute error, IAE) 指标, 用于分析闭环系统的跟踪性能, 但是 IAE 指标中不仅包含了动态跟踪信息, 也包含了稳态跟踪信息, 而且 IAE 需要对时间进行无穷积分, 计算复杂度高.

针对上述文献中性能评估方法的不足, 本文提出了一种加密传输应用在工控系统中的可行性研究方法. 首先, 分析通用的工控系统加密传输框架, 以及数据加密造成的直接影响. 其次, 基于稳定性判据提出多输入多输出控制系统中加密传输机制的评估模型, 利用加密算法执行时间与数据加密长度的映射关系 (后文统一称为 “时间长度关系”), 设计一种求解长度可行域的算法. 然后, 借鉴 IAE 的思想, 提出了一种用于评估系统实时性能的指标, 即 Truncated IAE (TIAE)-based, 并在指标合理性论证中给出了一个合理的充分条件. 最后, 在嵌入式平台上测试了两种对称加密算法的时间长度关系, 并应用在他励直流电机控制系统仿真平台上, 计算并验证了系统稳定下的长度可行域, 获得了长度对实时性能的影响规律. 结果表明, 相比 Zeng 的结论, 利用长度可行域来判断长度的存在性将更加严谨. 相比 Harris 的随机性评估方法, TIAE 能提供更加合理、确定的分析指标. 相比 Gupta 的确定性评估方法, TIAE 则避免了主观赋值造成的差异. 因此, 本文提出的可行性研究方法可以为加密传输在工控系统的应用提供科学的依据.

1　问题描述

1.1　工业控制系统加密传输框架

在工业控制系统中, 控制器与执行器之间的前向通道、传感器与控制器之间的反馈通道的交互数据是进行加密保护的主要对象. 图 1 所示为通用的基于加密传输的工控系统分析框架, 包括控制器、控制网络、执行器、被控对象、传感器等.

1.2　加密算法执行时间分析

加密算法分为对称加密和非对称加密两种. 一方面, 非对称加密需要更多的计算资源和存储空间, 使其在工业控制领域应用受限. 另一方面, 尽管对称加密中的块加密相对流加密速度慢, 但安全性更高, 更容易实现数据保密性和加密速度之间的权衡. 因此, 本文讨论的加密传输机制中主要采用对称加密算法中的块加密算法, DES 和 AES (Advanced encrytion standard) 加密.

文献 [13] 及后文的实验数据表明, 采用对称加密的执行时间主要与加密平台、加密算法种类、 密

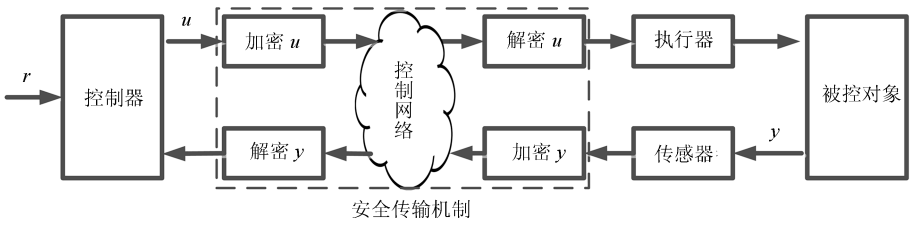

图 1　基于加密传输机制的工控系统框架图

Fig. 1　Frame diagram of industrial control system under encrypted transmission

钥长度和数据加密长度有关, 并且近似为式 (1) 的线性关系:

$$\begin{cases} \tau_{enc} = a_1 \cdot l_1 + b_1 \\ \tau_{dec} = a_2 \cdot l_2 + b_2 \end{cases} \tag{1}$$

其中, τ_{enc} 和 τ_{dec} 分别为加密、解密执行时间, l_1 和 l_2 分别为需要加密、解密的数据长度, a_i 和 b_i $(i = 1, 2)$ 表征了执行时间与除了数据长度外的因素的关系, 需要实验数据来标定.

根据工控网络中通信协议规定, 网络中传输的数据长度需要满足一定的范围, 即 $l_i \in L$, $L = [l_{\min}, l_{\max}]$. 那么, 加密和解密执行时间也限定在范围 $\Gamma_i = [\tau_{\min}, \tau_{\max}]$ 内,

$$\begin{cases} \tau_{\min} = a_i \cdot l_{\min} + b_i \\ \tau_{\max} = a_i \cdot l_{\max} + b_i \end{cases} \tag{2}$$

在图 1 所示的加密传输框架中, 系统延时主要包括两个部分, 前向通道延时 τ^{ca} 和反馈通道延时 τ^{sc}. 为了方便分析加密传输执行时间产生的延时对系统稳定性的影响, 根据单一变量原则, 暂不考虑通信网络固有延时. 此时, 系统延时主要集中在加解密过程中, 对应为

$$\begin{cases} \tau^{ca} = \Delta \cdot (\tau^{ca}_{enc} + \tau^{ca}_{dec}) \\ \tau^{sc} = \Delta \cdot (\tau^{sc}_{enc} + \tau^{sc}_{dec}) \end{cases} \tag{3}$$

其中, τ^{ca}_{enc} 和 τ^{ca}_{dec} 分别表示前向通道的加密延时和解密延时. τ^{sc}_{enc} 和 τ^{sc}_{dec} 分别表示反馈通道的加密延时和解密延时. 不同应用场合下的工控系统, 数据传输通道对于数据机密性和完整性的需求不同, Δ 定义为

$$\Delta = \begin{cases} 0, & \text{通道未加密} \\ 1, & \text{通道加密} \end{cases}$$

1.3 主要问题

一方面, 除了引入加密传输机制造成的延时外, 影响系统稳定性的因素还包括原系统的固有属性, 如控制结构、控制器类别、被控对象特征等. 因此, 如何综合这些因素建立一种基于加密传输的工控系统分析模型, 并在系统稳定的约束下求解数据加密长度 l_i 的可行域, 是首要解决的问题.

另一方面, 在上述可行域存在的前提下, 如何建立一种合理的实时性评估指标, 并分析该指标与可行域内不同长度的变化规律, 是其次要解决的问题.

2 系统稳定性分析

2.1 基于加密传输的工控系统分析模型

大型工业生产过程或被控对象都是多输入多输出 (Multiple input and multiple output, MIMO) 的, 以 MIMO 模型作为研究对象符合实践规律, 图 2 所示为基于加密传输机制的工控系统结构图.

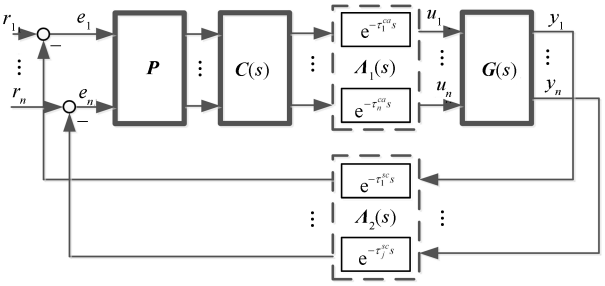

图 2 基于加密传输机制的 MIMO 控制系统结构图

Fig. 2 Structure diagram of MIMO control system under encrypted transmission

假设图 2 中 n 输入 n 输出对象的数学模型可以用有理传递函数矩阵 $G(s)$ 表示:

$$Y(s) = G(s) \cdot U(s) = \begin{pmatrix} g_{11}(s) & \cdots & g_{1n}(s) \\ \vdots & \ddots & \vdots \\ g_{n1}(s) & \cdots & g_{nn}(s) \end{pmatrix} \cdot U(s) \tag{4}$$

根据变量配对规则, 选择配对矩阵为 P, P 为同维单位矩阵经过初始行变换得到. 控制器为有理传递函数矩阵 $C(s)$. 根据对加密算法执行时间的分析, 在引入加密传输机制后, 前向通道和反馈通道的传递函数用 $\Lambda_1(s)$ 和 $\Lambda_2(s)$ 表示:

$$\Lambda_1(s) = \mathrm{diag}\{\mathrm{e}^{-\tau_1^{ca}s}, \mathrm{e}^{-\tau_2^{ca}s}, \cdots, \mathrm{e}^{-\tau_n^{ca}s}\}$$
$$\Lambda_2(s) = \mathrm{diag}\{\mathrm{e}^{-\tau_1^{sc}s}, \mathrm{e}^{-\tau_2^{sc}s}, \cdots, \mathrm{e}^{-\tau_n^{sc}s}\}$$

其中, $\boldsymbol{u} \in \mathbf{R}^n$ 和 $\boldsymbol{y} \in \mathbf{R}^n$ 分别是 MIMO 对象的输入、输出向量, $U(s) = \mathscr{L}[\boldsymbol{u}]$, $Y(s) = \mathscr{L}[\boldsymbol{y}]$, $\boldsymbol{u} = [u_1, u_2, \cdots, u_n]^{\mathrm{T}}$, $y = [y_1, y_2, \cdots, y_n]^{\mathrm{T}}$. τ_j^{ca}、τ_j^{sc} 分别为第 j 个前向、反馈通道总延时, $j = 1, \cdots, n$. 该系统的闭环特征方程为

$$CE(s; \tau_j^{sc}, \tau_j^{ca}) = \det\left(I + G(s)\Lambda_1(s)C(s)P\Lambda_2(s)\right) = 0 \tag{5}$$

显然式 (5) 的闭环特征根 $s^*(\tau_j^{sc}, \tau_j^{ca})$ 是关于未知参数 τ_j^{sc} 和 τ_j^{ca} 的函数. 当图 2 所示的工控系统中引入加密传输机制后, 闭环特征根在复平面上的分布, 即系统的稳定性, 将受到这些参数影响. 因此, 可以利用基于特征根分析的稳定性判据, 提出在系统稳定性的约束下, 加密传输机制的可行性评估模型, 即定理 1 的描述.

定理 1. 图 2 所示加密传输机制是可行的, 当且仅当式 (5) 所示的特征方程的全部特征根在复平面

的左半平面上, 即

$$\begin{cases} CE(s^*;\tau_j^{sc},\tau_j^{ca})=0 \\ \mathrm{Re}[s^*(\tau_j^{sc},\tau_j^{ca})]<0 \end{cases} \tag{6}$$

因为长度 l_i 直接影响加解密执行时间, 即未知参数 τ_j^{sc} 和 τ_j^{ca}, 为了单独研究长度对系统稳定性的影响, 暂不考虑不同通道内加密算法和长度的差异性. 在此基础上, 有推论 1 的描述,

推论 1. 如果所有前向通道采用的加密算法和数据加密长度相同, 所有反馈通道的加密算法和数据加密长度也相同时, 那么式 (5) 的评估模型可以表示为

$$\begin{aligned} CE(s;\tau)=c_n(s)\mathrm{e}^{-n\tau s}+c_{n-1}(s)\mathrm{e}^{-(n-1)\tau s}+\cdots+ \\ c_0(s)=\sum_{k=0}^{n}c_k(s)\mathrm{e}^{-k\tau s}=0 \end{aligned} \tag{7}$$

其中, $c_k(s)$ 表示只含变量 s 的有理多项式, $k=0,1,\cdots,n$.

证明. 此时 $\Lambda_1(s)=\mathrm{e}^{-\tau^{ca}s}I$, $\Lambda_2(s)=\mathrm{e}^{-\tau^{sc}s}I$, 闭环多项式转化为

$$\begin{aligned} &CE(s;\tau^{sc},\tau^{ca})= \\ &\quad \det[I+G(s)\Lambda_1(s)C(s)P\Lambda_2(s)]= \\ &\quad \det[I+\mathrm{e}^{-(\tau^{sc}+\tau^{ca})s}G(s)C(s)P]= \\ &\quad \det[I+\mathrm{e}^{-\tau s}K(s)]=0 \end{aligned} \tag{8}$$

其中, $K(s)=G(s)C(s)P$, $K(s)$ 为 n 维有理矩阵, 将式 (7) 展开即可转化为式 (6) 所示的多项式形式. □

2.2 数据加密长度可行域求解算法

长度是实施加密传输的一个重要参数, 综合式 (1) 和式 (7), 长度也是影响可行性评估模型中的一个重要因素. 对控制系统设计者而言, 可以采用试凑法来确定合适的长度, 即选取固定的长度分别代入式 (1) 和式 (7), 通过求解所有特征根来判断该长度合适与否. 但试凑法盲目性明显, 需要花费大量的时间和计算资源来求解式 (7) 的特征值. 另外, 还可以采用解析法, 在获得使式 (7) 稳定的参数集合之后, 在式 (2) 的约束下, 利用式 (1) 的线性关系求取长度的可行域. 解析法可以描述为:

定理 2. 假设线性映射 $f:x\to y$ 的映射关系为

$$y=f(x)=2\sum_{i=1}^{2}(a_ix+b_i)$$

如果两个集合 Φ 和 Θ 也满足该映射关系 $f:\Phi\to\Theta$, 其中

$$\begin{aligned} \Theta=&\{\tau\in[2\tau_{\min},2\tau_{\max}]| \\ &\mathrm{Re}[s^*(\tau)]<0;\forall s^*,CE(s^*;\tau)=0\} \end{aligned}$$

那么, 集合 Φ 即为使式 (7) 系统稳定的数据加密长度可行域.

在文献 [10] 中介绍了 D-subdivision 法, 可以利用超越方程 (7) 来求解参数 τ 的集合 Θ, 其主要思想包括两点: 在式 (7) 系统的临界稳定状态下, 参数 τ 必定使式 (7) 产生至少一对纯虚根. 求取该虚根和 τ 值, 判断在所有 τ 值处纯虚根穿越虚轴的移动趋势, 进一步求取稳定的集合 Θ.

基于定理 2 和 D-subdivision 求解方法, 可以设计如下所示的长度可行域求解算法:

1) 变量代换: 直接求超越方程 (7) 的纯虚根存在困难, 利用变量代换 $\mathrm{e}^{-\tau s}=(1-Ts)/(1+Ts)$, $T\in\mathbf{R}$, 将式 (7) 转化为有理多项式方程,

$$CE(s;\tau)=\sum_{k=0}^{n}c_k(s)\left(\frac{1-Ts}{1+Ts}\right)^k=0 \tag{9}$$

$$\begin{aligned} \Leftrightarrow&\sum_{k=0}^{n}c_k(s)(1-Ts)^k(1+Ts)^{n-k}= \\ &\sum_{p=0}^{\mu}b_p(T)s^p=0 \end{aligned} \tag{10}$$

其中, $\mu=\max\{\deg[c_j(s)]\}+n$.

2) 求解虚根: 式 (7) 和式 (10) 的纯虚根完全相同, 而式 (10) 的纯虚根可以利用劳斯表中的辅助多项式求解, 定义纯虚根的有限集合为 S,

$$S=\{s^*|s^*=\mp\omega_c i,\omega_c=\omega_{c1},\omega_{c2},\cdots,\omega_{cm}\}$$

同时能求解出所有纯虚根对应的参数 T 的集合 Ψ,

$$\Psi=\{T\in\mathbf{R}|T=T_{c1},T_{c2},\cdots,T_{cm}\}$$

根据变量代换的等价原则, 进一步求出每个参数 T_{ck} 对应的参数 τ 集合 $\Omega_k(\tau;\omega_{ck})$, $k\in\{1,2,\cdots,m\}$,

$$\begin{aligned} \Omega_k(\tau;\omega_{ck})=&\left\{\tau|\tau=\frac{2\tan(\omega_{ck}T_{ck})+2p\pi}{\omega_{ck}},\right. \\ &\left.p=1,\cdots,\infty\right\} \end{aligned}$$

将所有的集合 $\Omega_k(\tau;\omega_{ck})$ 合并, 按照元素大小排序, 并结合参数 τ 的实际取值范围, 可得使式 (7) 系统临界稳定的参数 τ 集合 Ω,

$$\Omega=\left\{\bigcup_{k=1}^{m}\Omega_k(\tau;\omega_{ck})\right\}\cap[2\tau_{\min},2\tau_{\max}]$$

3) 求解集合 Θ: 当参数 τ 等于集合 Ω 中的某一元素 $\tau_{k,l}$ 时, 式 (7) 的系统存在一对虚根 $s^* = \mp\omega_{ck}i$, 并且随着 τ 在 $[\tau_{k,l}, \tau_{k,l}+\varepsilon]$ 内变化, 该对虚根穿越虚轴的移动趋势为

$$\mathrm{RT}\left|_{s=\omega_{ck}i,\tau=\tau_{k,l}}\right. = \mathrm{sgn}\left[\mathrm{Re}\left(\frac{\mathrm{d}s(\tau)}{\mathrm{d}\tau}\left|_{r=\omega_{ck}i,\tau=\tau_{k,l}}\right.\right)\right]$$

将式 (7) 对参数 τ 进行求导, 即可求出移动趋势的值,

$$\begin{aligned}\mathrm{RT}\left|_{s=\omega_{ck}i,\tau=\tau_{k,l}}\right. = &\\ \mathrm{sgn}\left[\mathrm{Im}\left(\frac{\sum\limits_{j=0}^{n}\frac{\mathrm{d}a_j}{\mathrm{d}s}\mathrm{e}^{-\mathrm{j}\tau s}}{\sum\limits_{j=0}^{n}ja_j\mathrm{e}^{-\mathrm{j}\tau s}}\left|_{s=\omega_{ck}i,\tau=\tau_{k,l}}\right.\right)\right] = &\\ \mathrm{sgn}\left[\mathrm{Im}\left(\frac{\sum\limits_{j=0}^{n}\frac{\mathrm{d}a_j}{\mathrm{d}s}\left(\frac{1-Ts}{1+Ts}\right)^j}{\sum\limits_{j=0}^{n}ja_j\left(\frac{1-Ts}{1+Ts}\right)^j}\left|_{s=\omega_{ck}i,T=T_{ck}}\right.\right)\right]&\end{aligned} \tag{11}$$

该趋势只取决于 ω_{ck} 和 T_{ck}, 即虚根在 $\Omega_k(\tau;\omega_{ck})$ 中所有元素处的移动趋势相同. 趋势值为正表示系统增加两个不稳定极点, 反之表示减少两个不稳定极点. 令 $\mathrm{NU}(\tau)$ 表示不稳定极点个数, 则集合 Θ 可以按如下定义求解,

$$\Theta = \{\tau \in \Omega | \mathrm{NU}(\tau) = 0\}$$

4) 求解数据加密长度可行域 Φ: 确定前向和反馈通道采用的加密算法, 通过实验法测定式 (1) 的参数, 利用定理 2 的映射关系求取使系统稳定性的数据加密长度可行域 Φ.

3 系统实时性能分析

在获得长度可行域后, 进一步研究工控系统实时性能与可行域内长度的关系. 本文借鉴 IAE 计算的思想, 直接从系统的跟踪误差考虑, 确定了 TIAE 指标的核心: 在稳定时间到达之前, 累计的跟踪误差越小, 则系统的实时性能越好.

3.1 实时性指标建立

定义 1. 绝对误差积分 IAE[15]: 将输出跟踪误差的绝对值在 0 到无穷时间域内进行广义积分, 记为

$$\mathrm{IAE} = \int_0^\infty |r(t)-y(t)|\,\mathrm{d}t = \int_0^\infty |e(t)|\,\mathrm{d}t = T_s\sum_{i=0}^{\infty}|e(t_i)| \tag{12}$$

其中, $r(t)$ 是参考输入, $y(t)$ 是系统的单个输出, $e(t)$ 是跟踪误差, T_s 是测量采样周期.

为了克服 IAE 的缺点, 对 IAE 指标进行改进, 有定义 2 的描述,

定义 2. 截断的绝对误差积分 (Truncated integrated absolute error, TIAE): 将输出跟踪误差的绝对值在 0 到调整时间 t_s 内进行定积分, 记为

$$\mathrm{TIAE} = \int_0^{t_s} |r(t)-y(t)|\,\mathrm{d}t = \int_0^{t_s} |e(t)|\,\mathrm{d}t = T_s\sum_{i=0}^{m}|e(t_i)| \tag{13}$$

其中, $m = t_s/T_s$.

对比 IAE, 用 TIAE 指标来分析系统当前实时性能的优势在于, TIAE 对稳定时间内的跟踪误差进行累计, 综合考虑了动态响应过程中的传统实时性因素, 不需要人为主观赋权值, 也克服了 IAE 的上述两个缺点. 利用 TIAE 进一步得到系统实时性能的评价指标,

定义 3. TIAE-based 指标定义为: 在引入加密传输机制前后, 系统 TIAE 的比值, 记为

$$\eta_{\mathrm{TIAE}} = \frac{\mathrm{TIAE}_0}{\mathrm{TIAE}_{enc}} \tag{14}$$

当 $\eta_{\mathrm{TIAE}} = 1$, 表明引入加密传输机制之后系统实时性能与原系统相同, 可以达到满意的性能要求. 当 $0 < \eta_{\mathrm{TIAE}} < 1$, 表明引入加密传输机制之后系统实时性能比原系统差, 且 $\eta_{\mathrm{TIAE}} \to 0$ 表明实时性能已经极度恶化, 不适合引入加密传输机制. 假设可行域内的边界点 l_{cri} 正好使系统震荡不稳定, 此时 $\mathrm{TIAE}_{enc}(l_{cri}) \to +\infty$, 令 $\eta_{\mathrm{TIAE}}(l_{cri}) = 0$, 保证 η_{TIAE} 值域的连续性.

3.2 η_{TIAE} 合理性说明

对于工控系统设计者而言, 上升时间 t_r、超调量 $\sigma\,\%$、稳定时间 t_s 都属于越小越优型指标, 因此,

定理 3. 如果在长度可行域 Φ 内, η_{TIAE} 与 t_r、$\sigma\,\%$、t_s 关系的单调性一致, 并且严格单减, 那么 η_{TIAE} 能作为系统实时性能的综合评估值, 且 η_{TIAE} 越大则实时性能越优.

证明. 假设 η_{TIAE} 随 t_r 并不是严格单调的, 因为积分保证了 η_{TIAE} 在可行域 Φ 内的连续性, 那么在 $\eta_{\mathrm{TIAE}} \sim t_r$ 关系曲线中必存在两点 $t_{r,1}$ 和 $t_{r,2}$, 使得 $\eta_{\mathrm{TIAE}}(t_{r,1}) = \eta_{\mathrm{TIAE}}(t_{r,2})$, 显然这一点违背了越小越优常识, 假设不成立.

同理, 假设 $\eta_{\mathrm{TIAE}} \sim t_r$ 是严格单调, 但单调性与 $\eta_{\mathrm{TIAE}} \sim \sigma\,\%$、$\eta_{\mathrm{TIAE}} \sim t_s$ 不一致, 不妨设为

$$\begin{cases} \operatorname{sgn}\left\{\dfrac{\partial\left[\eta_{\mathrm{TIAE}}(l)\right]}{\partial\left[t_r(l)\right]}\right\} = 1 \\ \operatorname{sgn}\left\{\dfrac{\partial\left[\eta_{\mathrm{TIAE}}(l)\right]}{\partial\left[\sigma\,\%(l)\right]}\right\} = -1 \\ \operatorname{sgn}\left\{\dfrac{\partial\left[\eta_{\mathrm{TIAE}}(l)\right]}{\partial\left[t_s(l)\right]}\right\} = -1 \end{cases}$$

从 $\eta_{\mathrm{TIAE}} \sim \sigma\,\%$、$\eta_{\mathrm{TIAE}} \sim t_s$ 的单调性可以看出, 如果 $\eta_{\mathrm{TIAE}}(\sigma_1\,\%) > \eta_{\mathrm{TIAE}}(\sigma_2\,\%)$, 则 $\sigma_1\,\% < \sigma_2\,\%$, 实时性能在 $\sigma_1\,\%$ 更优, 即 η_{TIAE} 越大则实时性能越优. 在 $\eta_{\mathrm{TIAE}} \sim t_r$ 关系曲线中必存在两点 $t_{r,3}$ 和 $t_{r,4}$ $(t_{r,3} < t_{r,4})$, 使得 $\eta_{\mathrm{TIAE}}(t_{r,3}) < \eta_{\mathrm{TIAE}}(t_{r,4})$, 说明实时性能在 $t_{r,4}$ 更优, 显然违背了越小越优常识. 定理 3 得证. □

定理 3 给出了 η_{TIAE} 合理性的一个充分条件, 原因在于, 直接求解 η_{TIAE} 对 t_r 的单调性并不方便,

$$\operatorname{sgn}\left\{\frac{\partial\left[\eta_{\mathrm{TIAE}}(l)\right]}{\partial\left[t_r(l)\right]}\right\} = \operatorname{sgn}\left\{\frac{\partial\left[\dfrac{\mathrm{TIAE}_0}{\mathrm{TIAE}_{enc}(l)}\right]}{\partial\left[t_r(l)\right]}\right\} = \frac{\operatorname{sgn}\left\{-\dfrac{\mathrm{TIAE}_0}{\mathrm{TIAE}_{enc}^2(l)} \cdot \dfrac{\partial\left[\mathrm{TIAE}(l)\right]}{\partial l}\right\}}{\operatorname{sgn}\left\{\dfrac{\partial t_r(l)}{\partial l}\right\}} = -\frac{\operatorname{sgn}\left\{\dfrac{\partial\left[\mathrm{TIAE}(l)\right]}{\partial l}\right\}}{\operatorname{sgn}\left\{\dfrac{\partial t_r(l)}{\partial l}\right\}}$$

如果能获得 $t_r(l)$ 和 $\mathrm{TIAE}(l)$ 的解析式, 那么在可行域内, η_{TIAE} 对 t_r 的单调性是可以解析求解的. Yu 等[15] 提出利用泰勒级数近似 $\mathrm{e}^{-\tau s} \approx 1 - \tau s$, 从而求出系统输出的时域表达式, 但该近似必须要求 $\tau s \to 0$ 才能满足, 即要求极点全部分布在 0 附近, 当条件不满足时, 近似结果会导致错误的结论.

实际上, 在加密传输引入延时后, 闭环特征方程出现超越项 $\mathrm{e}^{-\tau s}$, 不能通过简单地近似来求取时域内系统输出、$t_r(l)$、$\mathrm{TIAE}(l)$ 的解析式. 可以采用数值计算的方法, 利用式 (13) 的离散表达式定量计算出 $\mathrm{TIAE}(l)$ 的变化规律, 然后再验证是否满足定理 3.

4　实验结果及仿真

根据加密传输可行性评估的分析步骤, 实验包括两个部分: 实验测定式 (1) 的参数、加密传输下系统的性能验证.

4.1　对称加密算法执行时间测试

为了判断加密平台、算法种类等因素对加密传输可行性的影响, 首先应测定这些因素与加解密执行时间的关系. 本文在嵌入式平台 (AT91SAM9XE512QU, MCU 32 bit, 180 MHz) 上分别运行 DES 和 AES 加密算法. 其中, DES 密钥长度为 8 字节, AES 密钥长度为 16 字节, 填充方式为报文长度对 8 或 16 取模, 并用该值将报文长度填满至 8 或 16 的整数倍. 实验记录加解密执行时间与长度的关系如表 1 所示, 将表 1 的测试数据通过最小二乘法进行拟合, 如式 (15) 和 (16) 所示, 拟合曲线如图 3 所示.

$$\begin{cases} \tau_{enc}(\mathrm{AES}) = 0.4673 \cdot l + 0.0492 \\ \tau_{dec}(\mathrm{AES}) = 0.5850 \cdot l - 0.2272 \end{cases} \tag{15}$$

$$\begin{cases} \tau_{enc}(\mathrm{DES}) = 0.5726 \cdot l - 2.3579 \\ \tau_{dec}(\mathrm{DES}) = 0.4466 \cdot l - 1.3557 \end{cases} \tag{16}$$

4.2　系统性能研究

为了研究加密传输机制对实时性要求高的系统的影响, 本文采用文献 [16] 中的他励直流电机控制系统作为仿真平台. 该直流电机控制系统采用恒定励磁控制, 在励磁电流达到额定电流后, 通过控制电枢电压 U_a 来调节转速 n, 电压转速环转化为如下线性模型,

表 1　加密算法执行时间与数据加密长度测试数据

Table 1　Test data between the execute time of encryption algorithms and the length of plaintext

长度 (B)		16	144	272	400	528	656	784	912	1040
时间 (ms)	AES 加密	7.48	67.21	127.18	187.24	246.88	306.46	366.37	426.42	485.94
	AES 解密	9.32	83.99	158.81	233.46	308.88	383.58	458.43	533.18	608.33
	DES 加密	8.83	79.72	150.59	228.22	300.12	372.94	445.34	517.98	595.94
	DES 解密	6.97	62.46	117.91	178.22	234.84	291.86	348.74	405.94	462.94

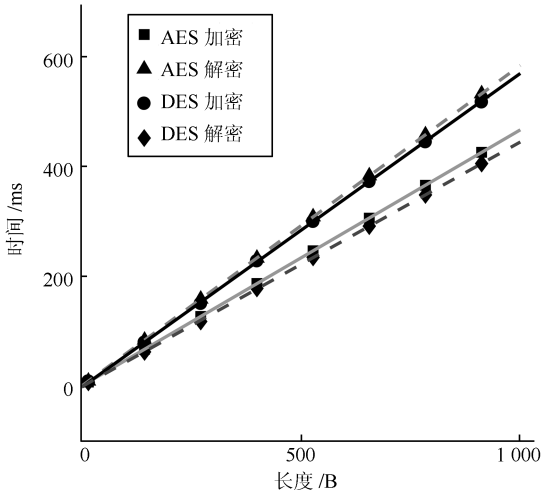

图 3 加密算法执行时间与数据加密长度关系曲线

Fig. 3 Relationship curve between the execute time of encryption algorithms and the length of encrypted data

$$\begin{cases} \dfrac{\mathrm{d}I_a}{\mathrm{d}t} = -120I_a - 120\omega + 100U_a \\ \dfrac{\mathrm{d}\omega}{\mathrm{d}t} = -0.055\omega + 0.06I_a - 5T_L \\ n = \dfrac{30}{\pi}\omega \end{cases}$$

因负载转矩不属于电机的固有属性, 不影响闭环特征方程, 只分析输入 U_a 对输出 n 的影响, 其开环传递函数为

$$G(s) = \frac{6}{s^2 + 120s + 13.8} \cdot \frac{30}{\pi}$$

电压转速环采用 PI 控制器, 调节 PI 参数使得闭环控制系统稳定, $C(s) = 10 + 1/s$. 在 $t > 10\,\mathrm{s}$ 后, 给定 $n_{ref} = 500\,\mathrm{r/min}$ 的阶跃转速.

4.2.1 稳定性分析

根据推论 1 的场景描述, 在上述电压转速环控制系统中引入加密传输机制, 前向和反馈通道采用相同的数据加密算法, 数据加密长度均为 l, 则系统的闭环特征方程为

$$c_1(s)\mathrm{e}^{-\tau s} + c_0(s) = 0$$

其中, $c_1(s) = 573 \cdot s + 57.3$, $c_0(s) = s^3 + 120s^2 + 13.8s$, $q = \max\{\deg(c_j(s))\} + n = 4$. 式 (10) 转化为

$$b_4(T)s^4 + b_3(T)s^3 + b_2(T)s^2 + b_1(T)s + b_0(T) = 0$$

根据劳斯判据, 可以依次求出集合 $\Psi = \{0.201867\}$, $S = \{4.775\}$, $\Omega_k = \{0.321, 1.637, \cdots\}$, 及虚根的变化趋势 RT $= \mathrm{sgn}\left[\mathrm{Im}\left(0.3905 + 0.4126\mathrm{i}\right)\right] = 1$. 得出系统不稳定极点个数随参数 τ 的关系如表 2 所示, 闭环系统稳定下的集合 Θ 为

$$\Theta = \{\tau | \tau \in (0, 0.321)\} \tag{17}$$

表 2 集合 Θ 判定表格

Table 2 Judging form of Θ

τ	ω	T	RT	NU(τ)
(0, 0.321)				0
0.321	4.775	0.201867	1	
(0.321, 1.637)				2
1.637	4.775	0.201867	1	
(1.637, 2.953)				4
2.953	4.775	0.201867	1	
···	···	···	···	6

根据实际测得的加密算法参数及集合 Θ, 考虑工业以太网的数据长度范围为 64～1 518 字节, 则加密传输应用在该直流电机控制系统时, 长度可行域分别为

$$\begin{cases} \Phi(\mathrm{AES}) = \{l | l \in [64, 153]\} \\ \Phi(\mathrm{DES}) = \{l | l \in [64, 161]\} \end{cases} \tag{18}$$

因此, 基于 AES 和 DES 对称加密算法的加密传输机制应用在该控制系统中是可行的.

4.2.2 实时性能分析

以 AES 加密算法分析, 分别选取可行域 Φ(AES) 内部的不同参数, 代入系统进行验证, 记录每个长度下系统的输出响应, 如图 4 所示.

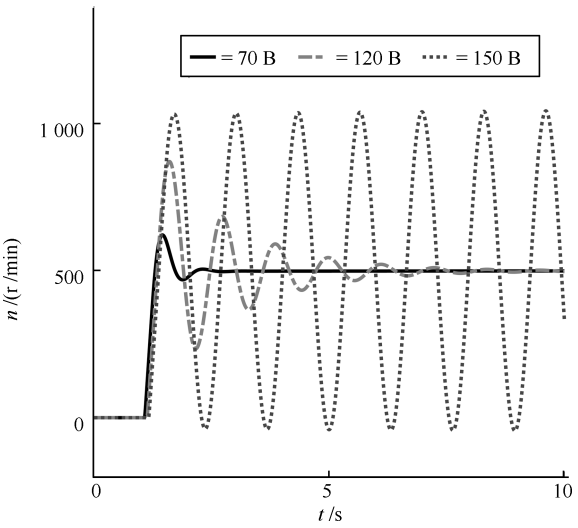

图 4 不同 AES 加密数据长度下实际转速变化曲线

Fig. 4 Timely varying curves of the actual speed under different length of AES encrypted data

从图 4 中实际转速变化曲线来判断, 当数据加密长度接近临界长度 153 B 时, 输出响应接近等幅

震荡, 进一步验证了集合 Φ(AES) 求解算法的正确性, 同样也可以验证 Φ(DES) 的正确性.

为了验证 $\eta_{\rm TIAE}$ 指标的合理性, 通过数值计算得到不同长度下的各实时性指标值, 如表 3 所示.

表 3　实时性指标与数据加密长度测试数据

Table 3　Test data between the real-time performance index and the length of encrypted data

l (B)	t_r (s)	σ %	t_s (s)	TIAE	$\eta_{\rm TIAE}$
0	20	0	1.618	99.2545	1
70	1.301	0.2438	1.972	130.2633	0.7620
80	1.305	0.3453	2.118	161.8826	0.6131
90	1.312	0.4396	2.596	206.0987	0.4816
100	1.323	0.544	3.209	274.6412	0.3614
110	1.333	0.639	4.311	372.4369	0.2665
120	1.344	0.7434	5.676	541.5546	0.1833
130	1.354	0.8383	8.749	846.1615	0.1173
140	1.365	0.9427	17.231	1.73E+03	0.0573
150	1.375	1.0376	80.985	8.52E+03	0.0117

首先判断 $\eta_{\rm TIAE}$ 与 t_r、σ %、t_s 之间的单调关系是否一致. 分别绘制 $\eta_{\rm TIAE}\sim t_r$、$\eta_{\rm TIAE}\sim\sigma$ %、$\eta_{\rm TIAE}\sim t_s$ 关系曲线, 如图 5 所示. 显然, $\mathrm{sgn}\left\{\frac{\partial[\eta_{\rm TIAE}(l)]}{\partial[t_r(l)]}\right\}$、$\mathrm{sgn}\left\{\frac{\partial[\eta_{\rm TIAE}(l)]}{\partial[\sigma\,\%(l)]}\right\}$、$\mathrm{sgn}\left\{\frac{\partial[\eta_{\rm TIAE}(l)]}{\partial[t_s(l)]}\right\}$ 在可行域 Φ(AES) 内的值均为 -1, 单调性为负并且都一致, 因此, $\eta_{\rm TIAE}$ 可以作为系统实时性能的综合评估值, 且 $\eta_{\rm TIAE}$ 越大则实时性能越优.

绘制表 3 中的测试数据, 得到各实时性指标随数据加密长度的变化关系曲线, 如图 6 和 7 所示,

对图 6 分析, 当系统引入加密传输机制之后, 传统的性能指标 t_r、σ % 与 l 近似成正的线性关系, 而 t_s、TIAE 与 l 近似成反比例关系, 长度可行域 Φ 的临界值即为渐近线.

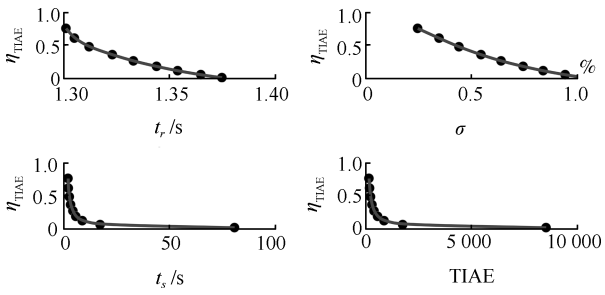

图 5　$\eta_{\rm TIAE}$ 随 t_r、σ %、t_s、TIAE 变化曲线

Fig. 5　Curves of the index $\eta_{\rm TIAE}$ under different t_r, σ %, t_s, TIAE

对图 7 分析, 实时性能 $\eta_{\rm TIAE}$ 是单调的, 并且随着数据加密长度增加而衰减, 在长度可行域 Φ 的临界值下, $\eta_{\rm TIAE}$ 收敛到 0, 表明此时系统的实时性能已经严重退化, 设计加密传输时应避免在该临界值附近选取数据加密长度. 图 6 和 7 中的变化规律也验证了 $\eta_{\rm TIAE}$ 指标提出的有效性.

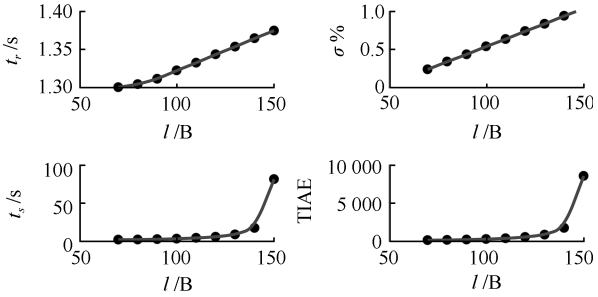

图 6　t_r、σ %、t_s、TIAE 随数据加密长度 l 变化曲线

Fig. 6　Curves of the index t_r, σ %, t_s, TIAE under different length of AES encrypted data

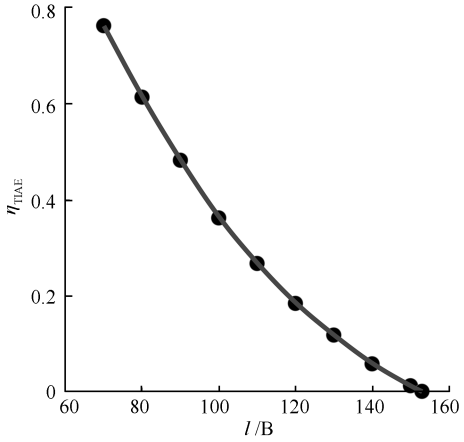

图 7　$\eta_{\rm TIAE}$ 随数据加密长度 l 变化曲线

Fig. 7　Curves of the index $\eta_{\rm TIAE}$ under different length of AES encrypted data.

5　结论

针对加密传输机制如何影响工控系统性能的问题, 本文从影响加密算法执行时间的主要因素: 数据加密长度出发, 依次提出了分析系统稳定性和实时性能的指标和方法.

关于加密传输机制的可行性研究中存在的一些问题, 还需要深入研究. 首先, 研究密钥长度、加密模式等因素对加解密的影响, 即与式 (1) 中参数 a_i、b_i 的关系. 其次, 有没有可能求出指标 $\eta_{\rm TIAE}$ 关于长度 l 的解析式, 或者将定理 3 完善成一个充要条件. 另外, 针对 MIMO 控制系统中存在的多个输出, 如何将实时性指标向量 $\boldsymbol{\eta}$ 中的各个分量 $\eta_{\rm TIAE}$ 综合考虑. 最后, 还要考虑将本文的可行性分析方法应用在真实的物理平台上进行论证.

References

1 Knowles W, Prince D, Hutchison D, Disso J F P, Jones K. A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection*, 2015, **9**: 52−80

2 ICS-CERT. ICS-CERT Monitor [Online], available: https://ics-cert.us-cert.gov/monitors/ICS-MM201512, May 3, 2016.
3 Pang Z H, Liu G P, Zhou D H, Hou F Y, Sun D H. Two-channel false data injection attacks against output tracking control of networked systems. *IEEE Transactions on Industrial Electronics*, 2016, **63**(5): 3242−3251
4 Tang B X, Alvergue L D, Gu G X. Secure networked control systems against replay attacks without injecting authentication noise. In: Proceedings of the 2015 American Control Conference (ACC). Chicago, USA: IEEE, 2015. 6028−6033
5 Zijlstra P. Cryptography for a Networked Control System using Asynchronous Event-Triggered Control [Master dissertation], Delft University of Technology, Netherlands, 2016.
6 Zhang L Y, Xie L, Li W Z, Wang Z L. Security solutions for networked control systems based on des algorithm and improved grey prediction model. *International Journal of Computer Network and Information Security (IJCNIS)*, 2013, **6**(1): 78−85
7 Wei M K, Wang W Y. Safety can be dangerous: secure communications impair smart grid stability under emergencies. In: Proceedings of the 2015 IEEE Global Communications Conference (GLOBECOM). San Diego, USA: IEEE, 2015. 1−6
8 Sipahi R, Niculescu S I, Abdallah C T, Michiels W, Gu K Q. Stability and stabilization of systems with time delay. *IEEE Control Systems*, 2011, **31**(1): 38−65
9 Sipahi R, Olgac N. A unique methodology for the stability robustness of multiple time delay systems. *Systems & Control Letters*, 2006, **55**(10): 819−825
10 Olgac N, Sipahi R. An exact method for the stability analysis of time-delayed linear time-invariant (LTI) systems. *IEEE Transactions on Automatic Control*, 2002, **47**(5): 793−797
11 Harris T J. Assessment of control loop performance. *The Canadian Journal of Chemical Engineering*, 1989, **67**(5): 856−861
12 Eriksson P G, Isaksson A J. Some aspects of control loop performance monitoring. In: Proceedings of the 3rd IEEE Conference on Control Applications. Scotland, UK: IEEE, 1994. 1029−1034
13 Gupta R A, Chow M Y. Performance assessment and compensation for secure networked control systems. In: Proceedings of the 34th Annual Conference of IEEE Industrial Electronics. Orlando, USA: IEEE, 2008. 2929−2934
14 Zeng W T, Chow M Y. Optimal tradeoff between performance and security in networked control systems based on coevolutionary algorithms. *IEEE Transactions on Industrial Electronics*, 2012, **59**(7): 3016−3025
15 Yu Z P, Wang J D, Huang B, Bi Z F. Performance assessment of PID control loops subject to setpoint changes. *Journal of Process Control*, 2011, **21**(8): 1164−1171
16 Smith R S. Covert misappropriation of networked control systems: presenting a feedback structure. *IEEE Control Systems*, 2015, **35**(1): 82−92

梁 耀 浙江大学控制科学与工程学院硕士研究生. 2014 年获得山东大学控制科学与工程学院学士学位. 主要研究方向为工控系统安全脆弱性分析与建模.
E-mail: liangyaoxp@zju.edu.cn
(**LIANG Yao** Master student at the College of Control Science and Engineering, Zhejiang University. He received his bachelor degree from Shandong University in 2014. His research interest covers vulnerability analysis and modeling of ICS security.)

冯冬芹 浙江大学工业控制技术国家重点实验室、浙江大学智能系统与控制研究所教授. 主要研究方向为现场总线, 实时以太网, 工业无线通信技术, 工业控制系统安全, 网络控制系统的研发与标准化工作. 本文通信作者.
E-mail: fengdongqin@zju.edu.cn
(**FENG Dong-Qin** Professor at the State Key Laboratory of Industrial Control Technology, Institute of Cyber-Systems and Control, Zhejiang University. His research interest covers field bus, real-time ethernet, industrial wireless communication technology, security of industrial control system, and network control system. Corresponding author of this paper.)

徐珊珊 浙江大学控制科学与工程学院硕士研究生. 2013 年获得华东理工大学学士学位. 主要研究方向为工业控制轻量级数据加密传输.
E-mail: lqxssxss@163.com
(**XU Shan-Shan** Master student at the College of Control Science and Engineering, Zhejiang University. She received her bachelor degree from East China University of Science and Technology. Her main research interest is lightweight encrypted data transmission for ICS.)

陈思媛 多伦多大学计算机与电子工程学院硕士研究生. 2015 年获得浙江大学学士学位. 主要研究方向为工控系统加密传输机制性能分析与补偿. E-mail: siyuansiyuan.chen@mail.utoronto.ca
(**CHEN Si-Yuan** Master student in the Department of Electrical and Computer Engineering, University of Toronto. She received her bachelor degree from Zhejiang University in 2015. Her research interest covers performance assessment and compensation for ICS based on cryptography.)

高梦州 浙江大学控制科学与工程学院博士研究生. 2012 年获得哈尔滨工业大学学士学位. 主要研究方向为工业控制系统网络安全.
E-mail: mzgao@zju.edu.cn
(**GAO Meng-Zhou** Ph. D. candidate at the Colledge of Control Science and Engineering, Zhejiang University. She received her bachelor degree from Harbin Institute of Technology in 2012. Her main research interest is network security of ICS.)