工程科学学报
Chinese Journal of Engineering

基于EtherCAT总线的七自由度机械臂的隐蔽攻击技术

汪世鹏 解仑 李连鹏 孟盛 王志良

Covert attack technology of EtherCAT based 7 degrees of freedom manipulator

WANG Shi-peng, XIE Lun, LI Lian-peng, MENG Sheng, WANG Zhi-liang

引用本文:
汪世鹏, 解仑, 李连鹏, 孟盛, 王志良. 基于EtherCAT总线的七自由度机械臂的隐蔽攻击技术[J]. 工程科学学报, 2020, 42(12): 1653-1663. doi: 10.13374/j.issn2095-9389.2019.12.07.002
WANG Shi-peng, XIE Lun, LI Lian-peng, MENG Sheng, WANG Zhi-liang. Covert attack technology of EtherCAT based 7 degrees of freedom manipulator[J]. *Chinese Journal of Engineering*, 2020, 42(12): 1653-1663. doi: 10.13374/j.issn2095-9389.2019.12.07.002

在线阅读 View online: https://doi.org/10.13374/j.issn2095-9389.2019.12.07.002

工程科学学报, 第 42 卷, 第 12 期: 1653−1663, 2020 年 12 月
Chinese Journal of Engineering, Vol. 42, No. 12: 1653−1663, December 2020
https://doi.org/10.13374/j.issn2095-9389.2019.12.07.002; http://cje.ustb.edu.cn

基于 EtherCAT 总线的七自由度机械臂的隐蔽攻击技术

汪世鹏，解　仑✉，李连鹏，孟　盛，王志良

北京科技大学计算机与通信工程学院, 北京 100083
✉通信作者, E-mail: xielun@ustb.edu.cn

摘　要　针对七自由度机械臂控制系统提出了一种七自由度机械臂隐蔽攻击模型. 首先基于推导的机械臂逆运动学方程, 对基于 EtherCAT 总线的七自由度机械臂进行运动规划与建模; 其次, 根据粒子群算法的研究与分析, 提出了基于混沌理论的多种群粒子群优化的七自由度机械臂系统 PID 参数辨识算法; 最后搭建了七自由度机械臂的攻击实验平台并使用辨识的参数结合隐蔽攻击原理开展了机械臂系统的攻击实验, 并且将所提出的隐蔽攻击技术与其他传统攻击技术进行了比较. 结果表明, 所提出的七自由度机械臂隐蔽攻击方法可以破坏机械臂系统的数据完整性和准确性, 并且具有很好的隐蔽性, 验证了所建立的攻击模型的有效性和可行性.

关键词　EtherCAT; 运动学; 隐蔽攻击; 机械臂; 粒子群
分类号　TP309.3

Covert attack technology of EtherCAT based 7 degrees of freedom manipulator

WANG Shi-peng, *XIE Lun*✉, *LI Lian-peng*, *MENG Sheng*, *WANG Zhi-liang*

School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China
✉ Corresponding author, E-mail: xielun@ustb.edu.cn

ABSTRACT　While the industrial robotic manipulator is a kind of multi-input and multi-output human-like operation and highly autonomous control system. It is widely used in medical care, home service, industrial manufacturing and other fields. With the integration of cyber-physical system networks and the Internet in recent years, the control commands of the industrial robotic arm control system can be totally exposed to the Internet. Under these circumstances, the chances of successful attacks by attackers to systems are increasing year by year. Compared to the security of traditional cyber physical system, the security of manipulator control system is a very challenging problem. In this paper, a covert attack method of 7 degrees of freedom (7-DOF) manipulator control system was proposed. Firstly, based on the inverse kinematics equation of the manipulator, the motion planning and modeling of 7-DOF manipulator, which communicated by EtherCAT, was carried out. Secondly, according to the research and analysis of particle swarm optimization method, a 7-DOF manipulator system PID parameter identification algorithm based on chaotic theory for multi- swarm particle swarm optimization was proposed. Parameter identification mainly identified the PID parameters of each joint. The principle and derivation process of the algorithm were described in detail. Finally, the experimental platform of manipulator control system was built and the identified parameters were used in combination with the covert attack principle to conduct the experiment. The proposed method was compared with other traditional attack methods, such as state machine attack and traditional sine attack. The results show that the covert attack model of the proposed 7-DOF manipulator can destroy the data integrity and accuracy of the manipulator system, and has a good concealment, which verifies the effectiveness and feasibility of the established attack model. The attack experiment platform constructed in this paper provides the physical basis for the attack and defense experiment of the manipulator, and it has certain reference

收稿日期: 2019−12−07
基金项目: 国家重点研发计划重点资助专项(2017YFB1302104); 国家自然科学基金面上资助项目(61672093); 智能机器人与系统高精尖创新中心开放基金资助项目(2018IRS01)

significance for similar researchers.

KEY WORDS EtherCAT; kinematics; covert attack; manipulator; particle swarm optimization

工业机械臂是一种多输入多输出的类人的作业、高度自主的控制系统,广泛应用于医疗护理、家庭服务、工业制造等领域. 近年来, 随着信息物理系统网络与互联网的融合, 机械臂控制系统的安全暴露于互联网中, 使得攻击者攻击成功的几率逐年增加. Stuxnet 和 Duqu 恶意病毒已经证明了信息物理系统是能够被攻击而且造成的后果极其严重[1−2].

攻击者通常选择现场总线和机械臂控制模型作为入侵对象. 机械臂系统中以太网总线种类很多, 常用的有 Profinet IO[3−5]、Modbus[6−7]、EtherCAT[8−9]等. 相较于其他总线而言, EtherCAT 总线实时性更高、具有更灵活的网络拓扑结构、可无缝集成现有的总线系统. 因此, EtherCAT 总线在工业控制领域中备受关注. 然而, 该总线缺少像身份认证等安全上的保障, Granat 等[10] 指出 EtherCAT 总线暴露于 DoS/DDoS,中间人攻击等常见的攻击. 与可达空间受限的六自由度机械臂相比, 七自由度机械臂(7-DOF manipulator)能保持末端机构在平面上位置不变的情况下, 实现构型的变换, 而且七自由度机械臂在设计上和人体手臂的模型相类似, 因此具有更好的灵活性[11].

在信息物理攻击方法及模型研究等方面, 隐蔽攻击(Covert attacks, CA)又称为错误数据注入攻击(False data injection attacks, FDI), 是一类比较有意义的攻击方式[12−13]. Xie 等[14] 提出了一种基于错误数据注入的攻击方法, 攻击者如果获得了当前电力系统相关配置信息, 便有可能注入干扰智能电网状态估计过程的恶意攻击包, 从而绕开系统中已有的不良数据检测方法. 隐蔽攻击模型的思路是篡改当前控制系统的传感器测量值, 并且使修改后的数值仍处于合法运行范围之内, 从而避免被标准的入侵检测方法检测到, 实现对控制系统的影响. 相较于普通攻击, 隐蔽攻击更难被发现, 造成的损失也比其他类型的攻击更严重. de Sá等[15] 提出了一种针对化工生产过程的隐蔽攻击模型, 并对攻击的影响进行了评估. Krotofil 和 Larsen[16] 提出了一种新的化工过程仿真模型, 并实施了隐蔽攻击. Quarta 等[17] 对工业机器人控制系统进行了相关的分析, 提出了一个攻击者模型, 并将其与工业机器人应该遵守的最低要求相对应: 精确感知环境, 执行控制逻辑的正确性以及人类操作员的安全性; 展示了攻击者如何利用软件漏洞等破坏这些需求, 从而导致机器人领域独有的严重后果. Lagraa 等使用 ROS 对机器人摄像机进行了结构化安全评估, 并使用一些安全漏洞接管了从机器人摄像机传入的视频流, 针对此提出了一种入侵检测系统来检测异常流量[18]. Vilches 等着重于创建一个开放和免费访问的机器人漏洞评分系统, 主要考虑了机器人技术当中的相关安全问题[19]. 虽然已经有研究人员开始关注机械臂安全相关的研究, 但是针对机械臂控制系统的隐蔽攻击的文章还很少. 因此, 研究基于 EtherCAT 总线的隐蔽攻击技术对提高机械臂控制系统安全十分必要.

本文提出了一种基于混沌理论的多种群粒子群优化的七自由度机械臂系统 PID 参数辨识算法; 然后使用该算法对 EtherCAT 总线下的七自由度机械臂进行了系统辨识, 得到的参数作为隐蔽控制器的参数; 最后根据提出的隐蔽攻击方法展开隐蔽攻击. 实验结果表明了在七自由度机械臂上实施隐蔽攻击的可行性. 本研究的新颖之处在于提出了一种针对部署在 EtherCAT 总线上的机械臂隐蔽攻击方法并搭建了实验测试平台. 作为探索性的研究, 对 EtherCAT 总线的安全性以及机械臂控制系统的稳定性作出了贡献.

1 七自由度机械臂模型

机械臂运动规划是保障机械臂在符合设定的约束以及避障条件下, 依据规划的路径完成位置和姿态的转换. 正向运动学通过机械臂各个关节的实际转动或伸缩值, 求解其末端的位置和姿态; 对应的逆运动学是已知末端的姿态和位置, 求解各个关节转动或伸缩量, 通常运动规划都是以逆运动学为基础[20].

1.1 运动规划模型

Denavit 和 Hartenberg[21] 为了表示机械臂相邻连杆间的运动规则, 针对各个关节的连杆建立坐标系, 该坐标系被称为 D-H 坐标系. 按照机械臂连杆和关节的分布情况、依据 D-H 坐标系的创建规则和各个连杆的长度, 建立如图 1 所示的七自由度机械臂 D-H 坐标系, 可得到如表 1 所示的机械臂连杆结构参数.

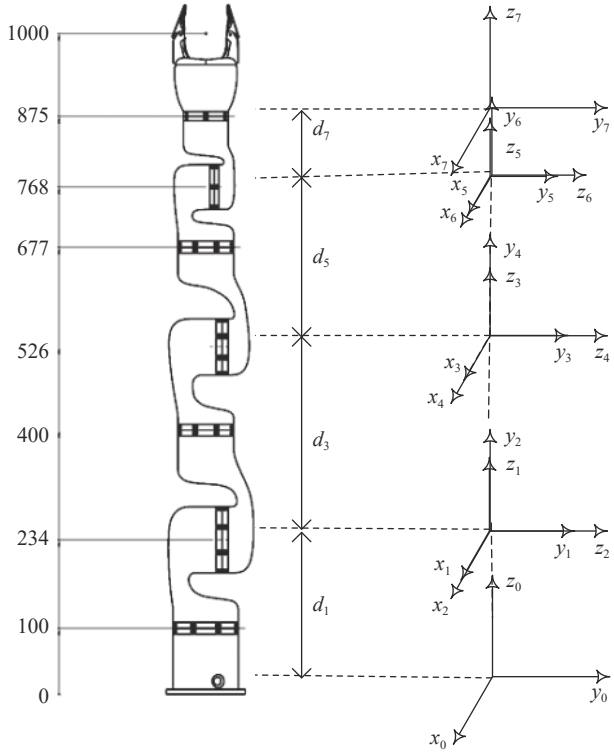


图 1 七自由度机械臂 D-H 坐标系

Fig.1 7-DOF manipulator D-H coordinate system

坐标系{i}相对于坐标系{i–1}的坐标变换矩阵如下

$$
{}_{i}^{i-1}\boldsymbol{T}=\begin{bmatrix}
\cos\theta_i & -\sin\theta_i & 0 & a_{i-1} \\
\sin\theta_i\cos\alpha_{i-1} & \cos\theta_i\cos\alpha_{i-1} & -\sin\alpha_{i-1} & -\sin\alpha_{i-1}d_i \\
\sin\theta_i\sin\alpha_{i-1} & \cos\theta_i\sin\alpha_{i-1} & \cos\alpha_{i-1} & \cos\alpha_{i-1}d_i \\
0 & 0 & 0 & 1
\end{bmatrix} \tag{1}
$$

已知目标位姿$(x_t,y_t,z_t,\alpha,\beta,\gamma)$,则建立逆运动学求解等式

$$
{}_{7}^{0}\boldsymbol{T}={}_{1}^{0}\boldsymbol{T}_{2}^{1}\boldsymbol{T}_{3}^{2}\boldsymbol{T}_{4}^{3}\boldsymbol{T}_{5}^{4}\boldsymbol{T}_{6}^{5}\boldsymbol{T}_{7}^{6}\boldsymbol{T}=\begin{bmatrix}
n_x & o_x & a_x & x_{\mathrm{t}} \\
n_y & o_y & a_y & y_{\mathrm{t}} \\
n_z & o_z & a_z & z_{\mathrm{t}} \\
0 & 0 & 0 & 1
\end{bmatrix} \tag{2}
$$

式(2)中，$[n_x, n_y, n_z]^{\mathrm{T}}$、$[o_x, o_y, o_z]^{\mathrm{T}}$、$[a_x, a_y, a_z]^{\mathrm{T}}$为机械臂末端的俯仰角、偏航角和滚转角，$[x_{\mathrm{t}}, y_{\mathrm{t}}, z_{\mathrm{t}}]^{\mathrm{T}}$为机械臂末端的位移. 依据所建立的 D-H 坐标系对七自由度机械臂逆运动学模型求解[22]. 由于构型设计上符合存在封闭解的 Pieper 准则[23]，可求解出各个关节角的解析解方程，得到解析的运动学模型.

1.2 机械臂 PID 控制器模型

机械臂的运动规划需要各个关节的控制器依据模型的参数进行计算才能实施. 机械臂运动控制是依靠各个关节执行器来达到目标位姿. 本文所用机械臂的关节控制器是采用 PID 进行调节的. 具体 PID 控制框图如图 2 所示.

图 2 中，y表示七自由度机械臂期望的末端位置，$\dot{y}$表示七自由度机械臂期望的末端速度，$\ddot{y}$表示七自由度机械臂期望的末端加速度；P_{d} 表示规划轨迹的期望位置；$\omega_i(i=1\cdots7)$表示关节位置，$\dot{\omega}_i$ $(i=1\cdots7)$表示关节速度，$\ddot{\omega}_i(i=1\cdots7)$表示关节加速度；$x$、$\dot{x}$、$\ddot{x}$分别表示七自由度机械臂末端期望位置、期望速度和期望加速度.

图 2 所示关节控制器采用三闭环的位置随动系统，位置环使得各个关节到达指定的位置，速度环使得各个关节的速度能够按照要求的量进行转动，电流环可以防止速度过载从而提升系统稳定性.

关节位置控制器是位置式 PID 控制器为

$$
\begin{cases}
O(k)=\hat{K}_{\mathrm{p}}\left[e(k)+\dfrac{T_{\mathrm{s}}}{T_{\mathrm{I}}}\displaystyle\sum_{i}^{n}e(i)+\dfrac{T_{\mathrm{d}}}{T_{\mathrm{s}}}(e(k)-e(k-1))\right] \\
\hat{K}_i=\hat{K}_{\mathrm{p}}\dfrac{T_{\mathrm{s}}}{T_{\mathrm{I}}} \\
\hat{K}_{\mathrm{d}}=\hat{K}_{\mathrm{p}}\dfrac{T_{\mathrm{d}}}{T_{\mathrm{s}}}
\end{cases} \tag{3}
$$

式中，$O(k)$表示第k次的关节转动输出，$\hat{K}_{\mathrm{p}}$表示可调

表 1 机械臂 D-H 坐标系参数

Table 1 D-H coordinate system parameters of manipulator

Joint, i	Twist angle, α_{i-1}/(°)	Link length, a_{i-1}	Joint angle, θ_i	Offset of connecting rod, d_i/mm	Range/(°)
1	0	0	θ_1	234	±180
2	–90	0	θ_2	0	±135
3	90	0	θ_3	292	±180
4	–90	0	θ_4	0	±135
5	90	0	θ_5	242	±180
6	–90	0	θ_6	0	±135
7	90	0	θ_7	107	±180

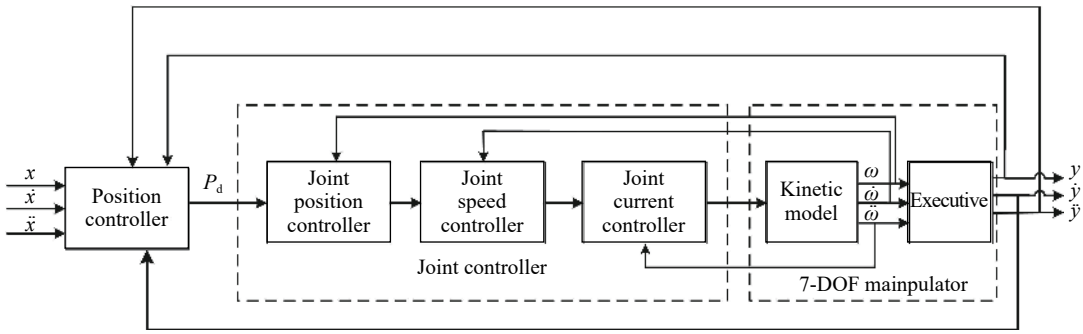


图 2　机械臂 PID 控制框图

Fig.2　Manipulator PID control block diagram

节的比例系数, T_I表示控制器的积分常数, $\hat{K}_i$表示可调节的积分系数, T_s表示采样周期, T_d表示微分常数, $\hat{K}_d$表示可调节的微分系数, $e(k)$表示第k次的关节转动偏差.

2　多种群粒子群的 PID 参数辨识

在对机械臂控制系统进行隐蔽攻击时, 需要获得足够的先验知识, 由于通常只能获取部分机械臂相关的知识, 在这种情况下是几乎不能够实施隐蔽攻击, 因此需要通过一些措施获取机械臂控制系统模型. 本文将群智能优化算法引入到七自由度 PID 参数辨识过程中, 利用多种群粒子群优化系统辨识算法得到七自由度机械臂最佳匹配模型参数, 并将其应用到隐蔽攻击方法中.

2.1　多种群粒子群优化算法

混沌粒子群算法(Chaotic particle swarm optimization, CPSO)[24]以及基本粒子群算法(Particle swarm optimization, PSO)[25]等随着算法的搜索空间的维度增加其获取全局最优值的效率会大大降低. 多种群粒子群优化算法(Multi-swarm particle swarm optimization, MPSO)[26]是在 PSO 上进化而来的一种优化算法, 其核心思想是将种群随机划分成几个子群, 子群内部按照 PSO 算法的流程进行迭代更新, 并且子群之间共享信息从而帮助整个种群更好地寻优.

多种群粒子群优化算法采取的是主从策略, 按照种群之间的竞态关系可以将多种群粒子算法分为竞争型和合作型. 合作型多种群粒子群优化算法相对于竞争型而言少了一个迁移因子. 本文采用竞争型多种群粒子群算法中主种群的更新策略如下:

$$\begin{cases} V_i = wV_i + c_1 r_1\left(P_i^{\mathrm{M}} - X_i\right) + \varphi c_2 r_2\left(P_{\mathrm{g}}^{\mathrm{M}} - X_i\right) + (1-\varphi)\cdot \\ c_3 r_3\left(P_{\mathrm{g}}^{\mathrm{S}} - X_i\right) \\ X_{i+1} = X_i + V_i \cdot \mathrm{d}t \end{cases} \tag{4}$$

式中, $1 \leqslant i \leqslant n$; X_i及V_i为第i次迭代位置与速度; w是惯性权重, c_1, c_2, c_3是主种群和从种群中粒子的学习权重; r_1, r_2, r_3是主种群和从种群中粒子随机真值, 取值为$0 \leqslant r_1, r_2, r_3 \leqslant 1$; P_i^{M}, $P_{\mathrm{g}}^{\mathrm{M}}$分别是主种群的局部最优位置和全局最优位置; $P_{\mathrm{g}}^{\mathrm{S}}$是从种群的全局极值位置; φ是迁移因子, 如果从种群中的全局最优位置大于主种群中的全局最优位置, 则$\varphi = 1$, 如果从种群中的全局最优位置和主种群中的全局最优位置处于同等水平, 则$\varphi = 0.5$, 如果从种群中的全局最优位置低于主种群中的全局最优位置, 则$\varphi = 0$. 由从种群和主种群的全局最优位置来搜索整个种群的最优.

2.2　多种群粒子群的 PID 参数辨识

基于前述机械臂 PID 控制模型可知, 每个关节都有 6 个参数需要辨识, 因此使用多种群粒子群系统辨识对七自由度机械臂进行辨识的参数为 42 个. 实现基于多种群粒子群算法的七自由度机械臂运动控制模型的系统参数辨识方法的详细步骤如下:

1)将群体中的 n 个粒子随机初始化到解空间中. 根据七自由度机械臂系统模型参数待辨识的个数设置粒子的维度为 42, 并在随机初始化粒子的起始位置和起始速度. 这些初始化了的粒子构成了七自由度机械臂的系统参数解集合并设定好学习权重c_1, c_2, c_3的初始值以及惯性权重w的初始值等.

2)划分群体为多个种群. 将种群划分成多个群体, 群体的个数为s, 划分的方式如下: 对所有的粒子进行编号, 编号为 1 的粒子划分进 1 号子群体中, 2 号粒子划分进 2 号子群体中, i号粒子划分进s号子群体中, $i+1$号粒子被划分进 1 号子群体中, 以此类推, 通过这种方式将整个种群划分成多个子群. 划分完毕的种群中选择全局最优位置所在的子种群为主群, 其余子群为从子群.

3)通过适应度函数来计算每个子群中粒子对

应的适应值和更新的学习因子c_{1i},c_{2i},c_{3i}及权重w_i.

4)主种群更新. 主群根据迭代方程更新群体中粒子的速度和位置, 更新公式如下:

$$\begin{cases} V_i = w_i V_i + c_{1i} r_1 \left(P_i^{\mathrm{M}} - X_i\right) + \varphi c_{2i} r_2 \left(P_{\mathrm{g}}^{\mathrm{M}} - X_i\right) + (1-\varphi)\cdot \\ c_{3i} r_3 \left(P_{\mathrm{g}}^{\mathrm{S}} - X_i\right) \\ X_{i+1} = X_i + V_i \cdot \mathrm{d}t \end{cases} \tag{5}$$

5)从子群更新. 在更新从子群的时候采用下面的步骤进行.

a)确定从子群参数的可行域$[a,b]$, 设置混沌算法初始化参数.

b)通过 Logistic 映射引入混沌变量, Logistic 映射公式为$z=\mu z(1-z)$, 其中, z 表示混沌域并且$z\in(0,1)$, μ为 Logistic 参数, 取值范围为$\mu\in[3.5699456,4]$. 对于粒子位置向量 x 映射到 Logistic 方程定义域上得

$$z_i = \frac{x-a}{b-a} \tag{6}$$

c)从子群更新粒子的位置以及速度, 使用的方程为

$$\begin{cases} V_i = w_i V_i + c_{1i} r_1 (P_i - X_i) + c_{2i} r_2 \left(P_{\mathrm{g}} - X_i\right) \\ X_{i+1} = X_i + V_i \cdot \mathrm{d}t \end{cases} \tag{7}$$

搜索过程中将混沌序列使用方程

$$x = a + (b-a)z \tag{8}$$

将粒子逆映射到原来的空间中去.

6)计算从子群中每个粒子的适应度函数值. 对这些粒子的位置和粒子历史最优值进行比较, 如果优于的话则更新粒子的主种群以及从种群中的粒子最优值, 分别得到P_i^{M}, $P_{\mathrm{g}}^{\mathrm{M}}$, P_i^{S}以及$P_{\mathrm{g}}^{\mathrm{S}}$.

7)判断当前位置是否为优于全局最优值. 如果是的话, 则将当前位置赋给全局最优值P_{g}.

8)判断迭代是否符合终止要求. 将设定的迭代次数值和算法当前的迭代次数进行比较, 如果达到了则算法终止, 否则, 算法将跳转到步骤 4 继续执行.

七自由度机械臂的多种群粒子算法系统辨识的基本流程图如图 3 所示.

3 设计与实验

3.1 系统整体架构

本文在工业以太网 EtherCAT 总线上搭建了七自由度机械臂控制和攻击测试平台, 该平台主要包含了 EtherCAT 主站、工业交换机、EtherCAT 从

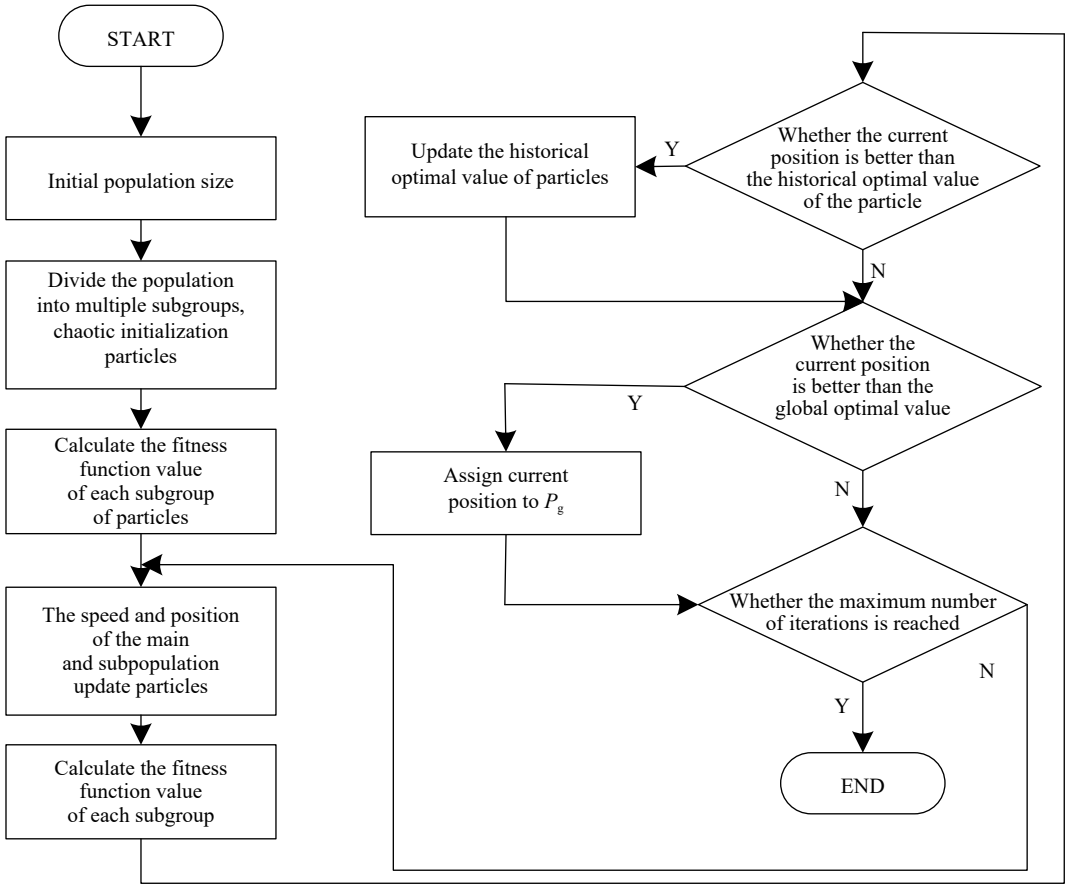


图 3 七自由度机械臂的多种群粒子算法系统辨识基本流程图

Fig.3 Basic flow chart of MPSO system identification for 7-DOF manipulator

站、七自由度机械臂以及攻击者. 提出的平台中各个设备之间的关系如图 4 所示.

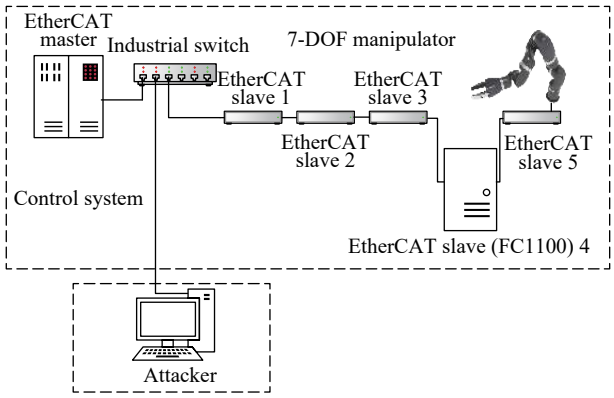


图 4　系统整体架构图

Fig.4　System architecture

EtherCAT 主站采用 EtherCAT 主站软件架构, 在 Linux 原有的任务调度的基础上移植 xenomai, 扩展 Linux 操作系统的在严格通信要求上的任务调度. 采用改进的开源主站 SOME 连接 EtherCAT 从站读取机械臂的状态信息并向机械臂控制系统中写入命令字.

工业交换机在工业控制系统中用于将工业以太网数据转发到各个受控对象, 但同时也提供给攻击者一种入侵方式. 在本文中通过工业型交换机攻击七自由度机械臂.

EtherCAT 从站主要包含了基于 lan9252 设计的 EtherCAT 从站多协议网关以及插入 FC1100 PCI 卡的主机组成的标准 EtherCAT 从站系统. 本文中设计的 EtherCAT 从站多协议网关用于连接机械臂等多种实验设备, 该网关电路上主要包含了 EtherCAT 从站专用控制芯片 LAN9252、标准以太网接口电路、电源管理电路、STM32 的外围设备电路及调试电路等, 如图 5 所示.

攻击者由标准计算机搭载 Kali Linux 系统, 通过工业交换机接入 EtherCAT 通信网络中. EtherCAT 协议在设计的时候并没有考虑连接的安全性来保护主站和从站之间的通信. 因此, 很容易受到媒体访问控制(Media access control, MAC)欺骗. 本文采用了 MAC 地址欺骗的方法, 由于该方法的实施效果取决于工业交换机整体性能, 本文在实施实验时不进行相应的研究. EtherCAT 协议实施中间人攻击的流程如图 6 所示.

图中 MAC_S 表示 EtherCAT 从站的 MAC 地址, MAC_M 表示 EtherCAT 主站的 MAC 地址, MAC_A 表示攻击者根据主站和从站通信获得的主站以及从站伪造地址, 根据欺骗的过程进行修改, Src 表示通信过程中数据的源地址, Dst 表示通

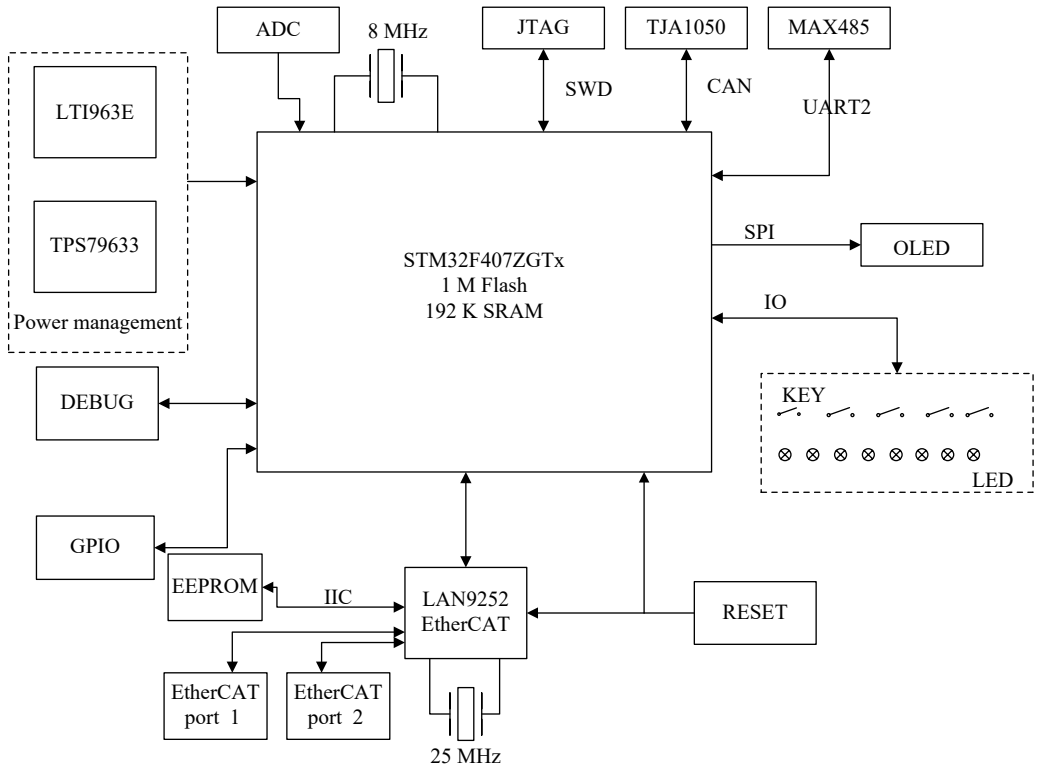


图 5　EtherCAT 从站多协议网关硬件结构图

Fig.5　EtherCAT slave multi-protocol gateway hardware structure diagram

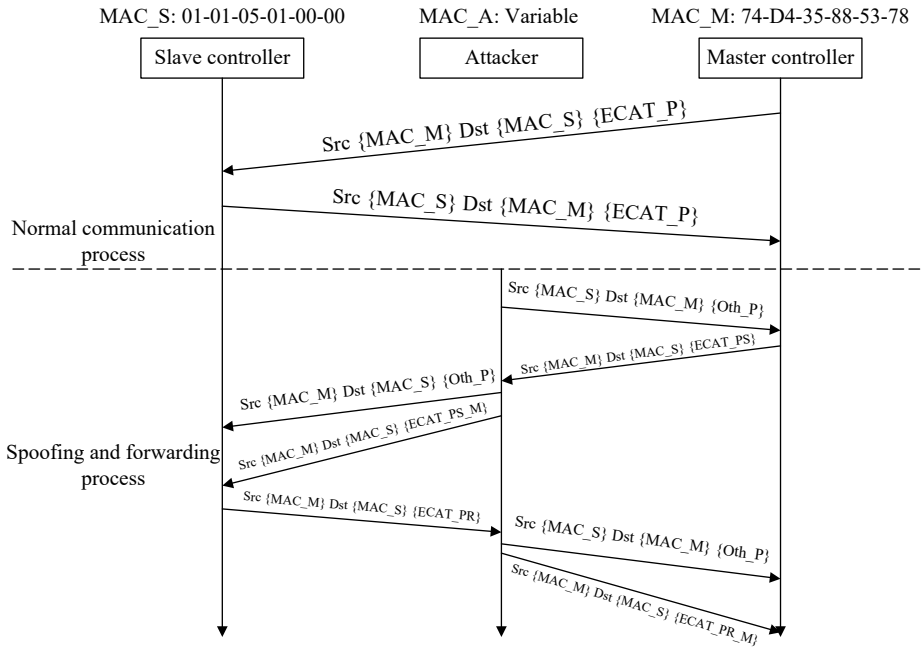


图 6 EtherCAT 中间人攻击示意图

Fig.6 EtherCAT man-in-the-middle attack diagram

信过程中数据的目的地址，ECAT_P, ECAT_PS, ECAT_PR 表示数据包中的EtherCAT 帧,ECAT_PS_M, ECAT_PR_M 表示修改后的 EtherCAT 帧，oth_表示为了实施中间人构建的其他包. 攻击者采用持续的发送数据包来充当主站从站来进行数据的篡改与转发.

3.2 实验

根据系统整体架构搭建的工业以太网下的七自由度机械臂平台如图 7 所示. 其中工业型交换机是整个系统的连接枢纽，工作人员通过工业型交换机可以远程控制 ROS-EtherCAT 主站；ROS-EtherCAT 主站通过工业交换机线性连接 FC1100 以及 4 块 EtherCAT 从站多协议网关，构成 EtherCAT 总线通信系统，并且有 1 块 EtherCAT 从站多协议网关通过 CAN 总线连接七自由度机械臂. 攻击者通过工业型交换机接入整个通信网络中，在图中并未展示出来.

本文提出的七自由度机械臂隐蔽攻击原理如图 8 所示.

图中攻击者主要通过对被攻击的机械臂运动学模型知识以及机械臂关节的控制模型知识构建一个类似于机械臂控制器的隐蔽控制器，其中隐蔽控制器的参数通过前面章节所提出的基于混沌理论的多种群粒子群的 PID 参数辨识算法获得. 使用构造的 PID 攻击函数对控制器的输出 $u_k^i(i=1,2,\cdots,7)$ 添加一个偏差$\hat{u}_k^i(i=1,2,\cdots,7)$，对机械臂的各个关节的实际输出造成影响，然后对各个

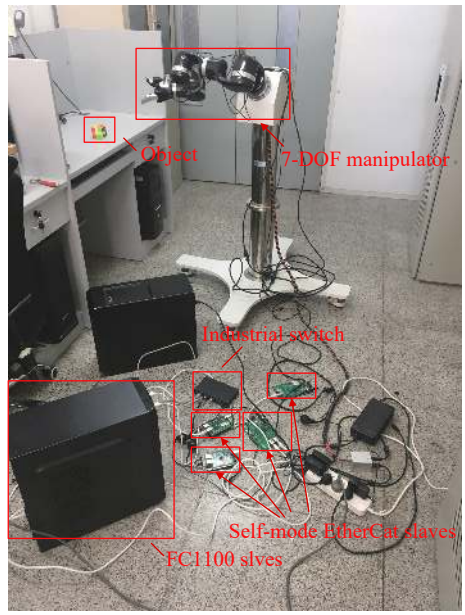


图 7 七自由度机械臂系统平台

Fig.7 7-DOF manipulator system platform

关节的反馈值减去添加偏差应该产生的影响值，从而欺骗控制器，让机械臂系统认为当前机械臂的执行已经到达了目标位置及姿态，从而完成隐蔽攻击的目的. 机械臂的运动规划模型主要在攻击的时候让机械臂的位姿到达指定的攻击姿态，达到预期的攻击效果. $\left[\begin{array}{cccc} u_k^1+\hat{u}_k^1 & u_k^2+\hat{u}_k^2 & \cdots & u_k^n+\hat{u}_k^n \end{array}\right]$ 为各个关节的实际输出值，其中 $n=7$, $\left[\begin{array}{cccc} y_k^1-\hat{y}_k^1 & y_k^2-\hat{y}_k^2 & \cdots & y_k^n-\hat{y}_k^n \end{array}\right]$为各个关节的反馈欺骗值，其中$n=7$.

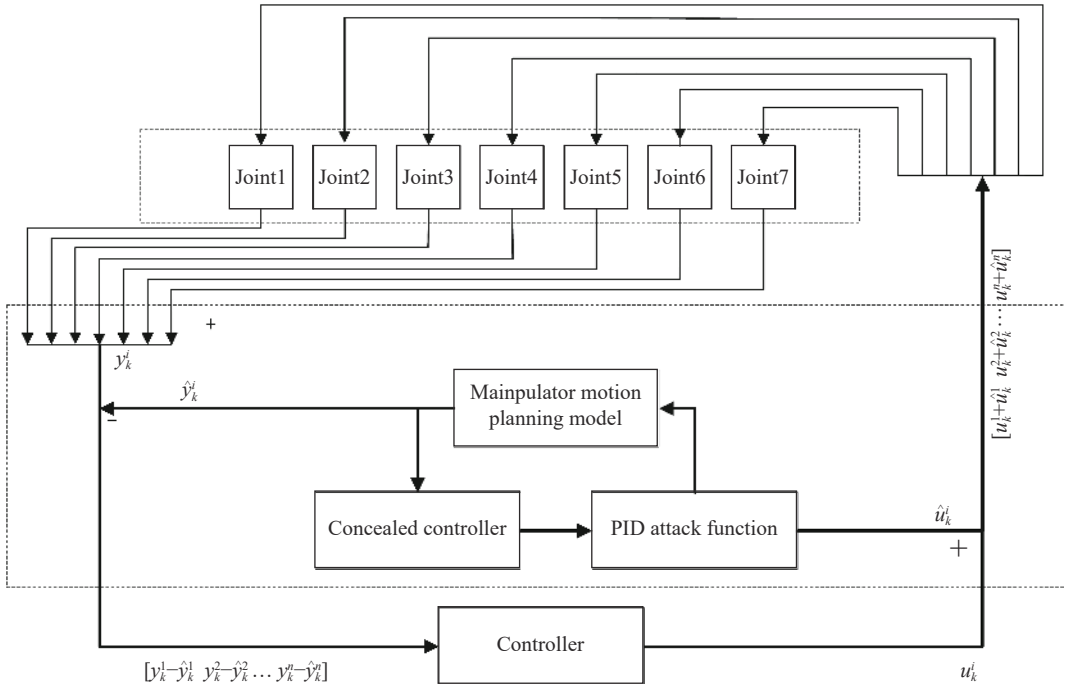


图 8　七自由度机械臂隐蔽攻击原理图

Fig.8　7-DOF manipulator covert attack schematic

首先从协议的角度对七自由度机械臂展开攻击, 因为 EtherCAT 协议对于拒绝服务攻击(Denial of service, DoS)没有任何抵抗措施, 因此本文进行 EtherCAT 协议攻击的部署相对简单. EtherCAT 协议在部署过程中, 只有主站能够修改从站的状态机状态, 而 EtherCAT 从站只有在运行状态才能进行周期性通信过程, 因此对 EtherCAT 从站状态机进行攻击会导致机械臂无法进行正常工作, 这种攻击很容易被操作人员发现或者被入侵检测系统检测到. 本文根据 EtherCAT 主从通信过程编写了一个可以攻击同一网段下的任一从站的状态机攻击程序, 攻击过程及效果如图 9 所示.

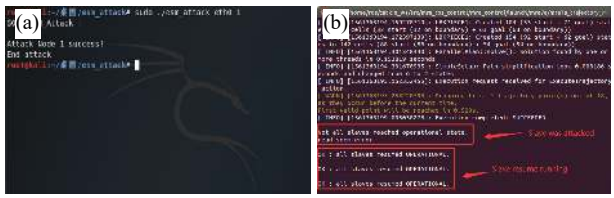


图 9　状态机攻击. (a)状态机攻击执行图; (b) ROS-EtherCAT 主站状态检测

Fig.9　State machine attack: (a) state machine attack execution diagram; (b) ROS-EtherCAT master status detection

从图中可以看到攻击期间, ROS-EtherCAT 主站检测到了有从站没有进入运行状态, 主站读取从站中的映射值出现了错误, 当停止了状态机攻击之后, 主站将从站的状态由错误状态恢复至正常运行状态, 这种攻击方式可以直接造成机械臂系统无法进行正常的操作而保持上次正常规划执行完的位姿, 但很容易被操作人员发现.

正弦攻击具有较好的隐蔽性, 一般的入侵检测系统很难检测到正弦攻击造成的异常. 正弦攻击的幅度值以及频率值都能够改变, 对其进行傅里叶变换分析可以发现其能量分布极其集中, 因此能造成更强的攻击后果, 本文在七自由度机械臂上同样构建了正弦攻击. 正弦攻击下的效果图如图 10 所示.

从正弦攻击与正常工作下的机械臂的速度曲线上可以看到, 正弦攻击下速度出现明显的频率变化以及幅度变化, 在位置曲线上有明显的波动出现, 而正常工作下的速度曲线以及位置曲线都很平滑. 并且在 ROS-EtherCAT 主站上可以看到控制系统报出执行出错的重大错误, 机械臂并未按照正常的轨迹规划去执行.

由于 EtherCAT 通信网络上有多个 EtherCAT 从站设备, 导致数据量相比单个设备来说要多很多, 因此, 需要分析数据结构, 找出七自由度机械臂相应数据, 对于机械臂数据的分析假设攻击者已经获得了部分关于机械臂控制器的知识, 如图 11 所示, 从抓取的网络包中, 分析属于机械臂的通信数据, 其中红色方框中为七自由度机械臂通信时的一帧数据.

从数据的传输格式来看, EtherCAT 上传输的

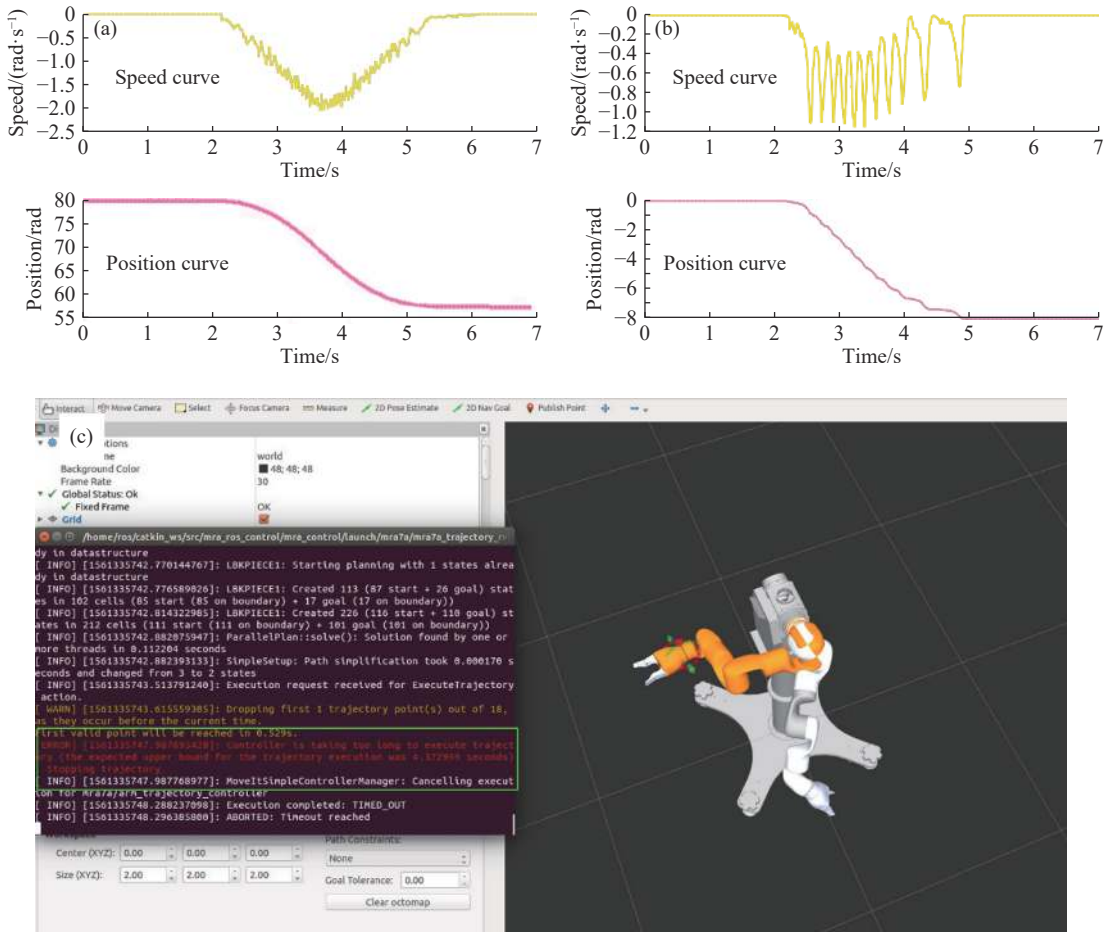


图 10 正弦攻击. (a)正常工作下的速度位置曲线; (b)正弦攻击下的速度位置曲线; (c) ROS-EtherCAT 主站状态

Fig.10 Sinusoidal attack: (a) speed position curve under normal working; (b) speed position curve under sinusoidal attack; (c) ROS-EtherCAT master status

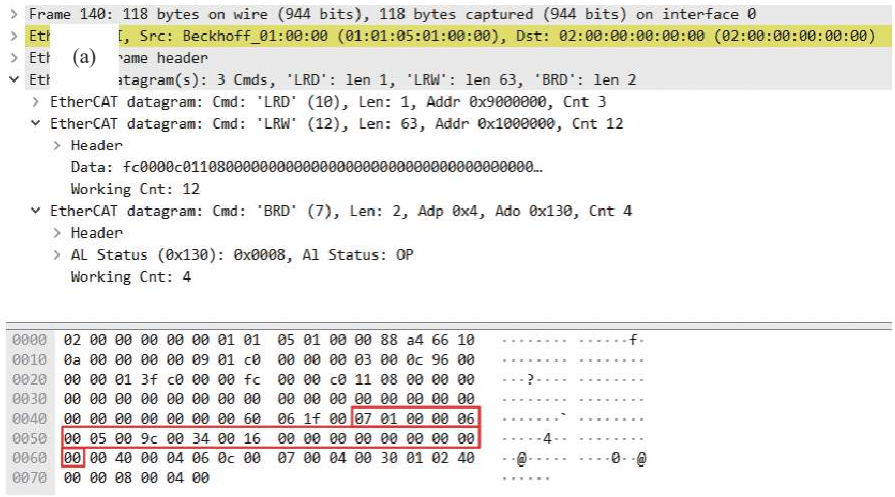
数据采用的是大端模式, 七自由度机械臂上 CAN 总线数据按照帧格式可以看到数据为帧 ID, 为 0x107, 数据长度(Data length count, DLC)为 0x06, 接下来的为数据区, 数据分别为 0x05、0x9c、0x34、0x16、0x00、0x00、0x00、0x00. 基于图 11(a)分析得到的 EtherCAT 总线传输的数据格式, 结合关节控制器内存控制表信息(图 11(b)), 根据提出的多种群粒子群的七自由度系统辨识算法对七自由度机械臂系统进行参数辨识. 首先, 根据上述得到的传输数据将群体中的 n 个粒子随机初始化到解空间, 划分群体为多个种群, 通过适应度函数来计算每个子群中粒子对应的适应值, 然后主种群、从子群更新, 计算从子群中每个粒子的适应度函数值, 判断当前位置是否为优于全局最优值. 需要辨识的参数有 42 个, 通过上述过程得到相应的最优值. 表 2 列出了关节 6 和关节 7 参数辨识结果, 其中位置 PID 参数为外环控制关键参数, 速度 PID 为内环控制关键参数, 位置外环参数是速度内环的输入. 从真实值和辨识值之间的对比, 可以看到本文提出的系统辨识算法辨识效果良好.

根据本文提出的七自由度机械臂隐蔽攻击模型, 七自由度系统辨识参数以及七自由度机械臂的运动学模型构建出的攻击, 攻击函数采取正弦攻击函数, 攻击效果如图 12 所示. 从图 12(a)中可以看到 ROS-EtherCAT 主站在攻击者进行隐蔽攻击时并未检测到任何异常, 并且认为机械臂已经到达了目标位姿, 而图 12(b)是机械臂的真实位姿状态, 和图 12(a)中显示的位姿有明显差异, 从而验证了本文提出的七自由度机械臂隐蔽攻击技术的实施具有良好的隐蔽性, 根据需要造成的破坏大小构造出攻击函数能够造成很严重的后果.

从不同的角度对比上述攻击, 如表 3 所示. 本文提出的七自由度机械臂隐蔽攻击技术在实施上比较复杂, 但是在保证破坏性的情况下具有较好的隐蔽性.

4 结论

本文提出了基于七自由度机械臂的隐蔽攻击



(b)

Address		Explanation	Authority	Initial value
0x00		Header (MODULE_TYP<<8) |0x50	R	(MODULE_TYP<<8) |0x50
0x01	SYS_ID	Grasp_ID	R/W	0x02
0x02	SYS_MODEL_TYPE	Drive MODEL: 0x10−M14 0x20−M17, 0x21−M17E, 0x30−M20, 0x80−Gripper	R	0x80
0x03	SYS_SW_VERSION	Firmware version	R	_HW_VWESION
0x04	SYD_ERROR	Error code Bit0: overpressure Bit1: undervoltage Bit2: over temperature Bit3: servo error	R	0

图 11　七自由度机械臂通信数据. (a)通信数据格式; (b)机械臂部分内存表信息

Fig.11　7-DOF manipulator communication data: (a) communication data format; (b) part of memory table information of the robot arm

表 2　部分辨识值和真实值

Table 2　Partially recognized value and true value

Joint	Parameter name	Actual value	Identification value
6	Position P	500	498.937
6	Position I	0	0.2045
6	Position D	100	102.382
6	Velocity P	400	401.586
6	Velocity I	300	297.926
6	Velocity D	0	–0.1052
7	Position P	800	799.428
7	Position I	0	–0.3054
7	Position D	150	151.313
7	Velocity P	200	202.479
7	Velocity I	11	10.582
7	Velocity D	0	–0.2043

方法. 对七自由度机械臂进行了运动学规划建模, 并对粒子群算法进行了研究; 提出了基于混沌理论的多种群粒子群优化的七自由度 PID 参数辨识

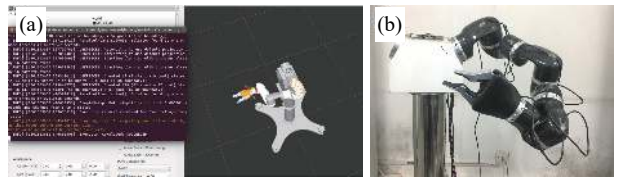


图 12　隐蔽攻击. (a) ROS-EtherCAT 主站状态; (b) 机械臂真实状态

Fig.12　Covert attack: (a) ROS-EtherCAT master status; (b) manipulator real state

表 3　机械臂攻击对比

Table 3　Manipulator attack comparison

Attack category	Difficulty of implementation	Destructive	Concealment
State machine attack	Simple	Weak	Weak
Sinusoidal attack	Medium	Stronger	Weaker
Covert attack	Complexity	Strong	Strong

算法. 设计了隐蔽攻击系统架构并搭建了实验平台, 利用所提出的算法对本文中的机械臂控制系统的参数进行辨识, 使用辨识的参数结合隐蔽攻击原理进行了攻击实验, 并且将所提出的隐蔽攻击技术与协议的状态机攻击以及传统的正弦攻击

进行了比较. 实验表明所提出的七自由度机械臂的系统辨识算法能够较好的辨识系统参数，并且能很好的应用于机械臂的隐蔽攻击中，验证了所提方法的可行性. 本文所构建的攻击实验平台为机械臂的攻防试验提供了物理基础，该平台对于类似研究者有一定的借鉴意义.

值得注意的是，本文在机械臂的隐蔽攻击实验中，仍然存在许多不足:机械臂的控制中由于传感器的精度问题，导致控制精度不是很高；本文并未对七自由度机械臂的动力学进行研究，因此提出的基于混沌优化多种群粒子群七自由度机械 PID 参数辨识算法并未对机械臂的动力学进行辨识.

参 考 文 献

[1] Bencsath B, Pek G, Buttyan L, et al. The cousins of stuxnet: Duqu, flame, and gauss. *Future Internet*, 2012, 4(4): 971

[2] Langner R. Stuxnet: dissecting a cyberwarfare weapon. *IEEE Secur Privacy*, 2011, 9(3): 49

[3] Wu X P, Xie L H. Performance evaluation of industrial Ethernet protocols for networked control application. *Control Eng Pract*, 2019, 84: 208

[4] Sestito G S, Turcato A C, Dias A L, et al. A method for anomalies detection in real-time Ethernet data traffic applied to PROFINET. *IEEE Trans Ind Inform*, 2018, 14(5): 2171

[5] Dias A L, Sestito G S, Brandao D. Performance analysis of Profibus DP and Profinet in a motion control application. *J Control Autom Electr Syst*, 2017, 28(1): 86

[6] Chen C H, Lin M Y, Guo X C. High-performance fieldbus application-specific integrated circuit design for industrial smart sensor networks. *J Supercomput*, 2018, 74(9): 4451

[7] Jiang B, Liu Y C, Sun F J, et al. Design of industrial control network based on Modbus/TCP. *Low Volt Apparat*, 2007(13): 30
(姜斌, 刘彦呈, 孙凡金, 等. 基于Modbus/TCP的工业控制网络设计. 低压电器, 2007(13): 30)

[8] Eramo V, Lavacca F G, Listanti M, et al. Definition and performance evaluation of an Advanced Avionic TTEthernet Architecture for the support of Launcher Networks. *IEEE Aerospace Electron Syst Mag*, 2018, 33(9): 30

[9] Langlois K, van der Hoeven T, Cianca D R, et al. EtherCAT tutorial: an introduction for real-time hardware communication on windows. *IEEE Robot Autom Mag*, 2018, 25(1): 22

[10] Granat A, Hofken H, Schuba M. Intrusion detection of the ICS protocol EtherCAT//*International Conference on Computer, Network Security and Communication Engineering* (*CNSCE*2017). Pennsylvania, 2017: 52

[11] Perry J C, Rosen J. Design of a 7 degree-of-freedom upper-limb powered exoskeleton//*The First IEEE/RAS-EMBS International Conference on Biomedical Robotics and Biomechatronics*, BioRob 2006. Pisa, 2006: 805

[12] Akpinar K O, Ozcelik I. Development of the ECAT preprocessor with the trust communication approach. *Secur Commun Networks*, 2018, 2018: 1

[13] Li W Z, Xie L, Wang Z L. Two-loop covert attacks against constant value control of industrial control systems. *IEEE Trans Ind Inform*, 2019, 15(2): 663

[14] Xie L, Mo Y L, Sinopoli B. False data injection attacks in electricity markets//2010 *First IEEE International Conference on Smart Grid Communications*. Gaithersburg, 2010: 226

[15] de Sá A O, Carmo L F R d C, Machado R C S. Covert attacks in cyber-physical control systems. *IEEE Transactions on Industrial Informatics*, 2017, 13(4): 1641

[16] Krotofil M, Larsen J. Rocking the pocket book: hacking chemical plants//*DefCon Conference*. DEFCON, 2015: 1

[17] Quarta D, Pogliani M, Polino M, et al. An experimental security analysis of an industrial robot controller//2017 *IEEE Symposium on Security and Privacy* (*SP*). San Jose, 2017: 268

[18] Lagraa S, Cailac M, Rivera S, et al. Real-time attack detection on robot cameras: a self-driving car application//2019 *Third IEEE International Conference on Robotic Computing* (*IRC*). Naples, 2019: 102

[19] Vilches V M, Gil-Uriarte E, Ugarte I Z, et al. Towards an open standard for assessing the severity of robot security vulnerabilities, the Robot Vulnerability Scoring System (RVSS). *arXiv preprint* (2018-05-16)[2019-12-07] arXiv: 1807.10357, 2018. http://arxiv.org/abs/1807.10357

[20] D 'Souza A, Vijayakumar S, Schaal S. Learning inverse kinematics//*Proceedings* 2001 *IEEE/RSJ International Conference on Intelligent Robots and Systems. Expanding the Societal Role of Robotics in the the Next Millennium* (*Cat. No.* 01*CH*37180). IEEE, 2001: 298

[21] Denavit J, Hartenberg R S. A kinematic notation for lower pair mechanisms based on matrices. *J Appl Mech*, 1955, 22: 215

[22] Sui D L, Xie L, Li L P, et al. Coupling planning control algorithm of redundant manipulator. *Comput Integr Manuf Syst*, 2019, 25(12): 3226
(眭东亮, 解仑, 李连鹏, 等. 一种冗余机械臂耦合规划控制算法. 计算机集成制造系统, 2019, 25(12): 3226)

[23] CRAIG J J. *Introduction to Robotics*. Beijing: China Machine Press, 2005

[24] Yue Y G, Cao L, Hu J, et al. A novel hybrid location algorithm based on chaotic particle swarm optimization for mobile position estimation. *IEEE Access*, 2019, 7: 58541

[25] Tharwat A, Elhoseny M, Hassanien A E, et al. Intelligent Bézier curve-based path planning model using Chaotic Particle Swarm Optimization algorithm. *Cluster Comput*, 2019, 22(2): 4745

[26] Nagra A A, Han F, Ling Q H, et al. An improved hybrid method combining gravitational search algorithm with dynamic multi swarm particle swarm optimization. *IEEE Access*, 2019, 7: 50388