面向协议规避与数据操控的工业控制系统隐蔽攻击载荷生成与无感注入机制研究

彭祥贞[1,2]，史建宇[1,2]，刘运祺[1,2]，郑承良[3]，崔晓晖[1,2]
（1.武汉大学国家网络安全学院，湖北 武汉 430072；2.数据智能湖北省重点实验室，湖北 武汉 430072；
3.香港科技大学土木及环境工程学系，香港 999077）

摘　要：针对工业控制系统（ICS）通信协议固有的认证与校验缺陷，提出一种面向协议规避与数据操控的工业控制系统隐蔽攻击载荷生成及无感注入机制。载荷生成层面，设计“时间序列生成对抗网络–长短期记忆网络（TimeGAN-LSTM）”模型，在低维空间解耦正常流量的静/动态特征，集成长短期记忆网络（LSTM）强化长程依赖建模，以生成符合原始时序、分布及物理规律的攻击载荷。无感注入层面，利用原创ICS通信协议漏洞，在协议、连接与时序上深度模拟合法通信，实现权限绕过与协议规避，并结合SQL注入和数据库接管工具（SQLmap）构建对历史数据库的隐蔽操控渠道。实验表明，生成载荷能有效绕过通用及ICS专用检测模型；攻击途径能够有效规避工业协议校验，为载荷提供了隐蔽注入途径。

关键词：工业控制系统；工业协议攻击；生成式人工智能；数据注入；渗透攻击
中图分类号：TP390
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025209

Research on covert attack payload generation and insensitive injection mechanism for industrial control systems for protocol evasion and data manipulation

PENG Xiangzhen[1,2], SHI Jianyu[1,2], LIU Yunqi[1,2], ZHENG Chengliang[3], CUI Xiaohui[1,2]
1. School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China
2. Hubei Provincial Key Laboratory of Data Intelligence, Wuhan 430072, China
3. Department of Civil and Environmental Engineering, The Hong Kong University of Science and Technology, Hongkong 999077, China

Abstract: Addressing authentication and verification flaws in industrial control system protocols, a covert attack payload generation and stealth injection method was proposed. A TimeGAN-LSTM model decoupled static and dynamic features of normal traffic in a latent space, generating high-fidelity payloads that preserved temporal patterns and physical constraints. By exploiting a novel protocol vulnerability and mimicking legitimate behaviors, the unauthorized access and protocol evasion was achieved. Integrated with SQLmap, a covert channel was established to manipulate historical databases. Experiments show the payloads bypass both general and ICS-specific detection models, evading protocol verification to enable stealthy data manipulation.

Keywords: industrial control system, industrial protocol attack, generative artificial intelligence, data injection, penetration attack

收稿日期：2025–08–07；修回日期：2025–11–10
通信作者：崔晓晖，xcui@whu.edu.cn
基金项目：湖北省重点研发计划基金资助项目（No.2025BAB018）
Foundation Items：The Key Research and Development Project of Hubei Province (No.2025BAB018)

0　引言

工业控制系统（ICS, industrial control system）作为关键基础设施的核心，运营技术（OT，operational technology）与信息技术（IT，information technology）融合进程的加快，正在从传统的封闭式机电系统向基于网络的数字系统演进[1]。这打破了OT数据的孤岛效应，提升了ICS对实时数据流的分析、监控、追溯等能力。但IT系统的引入，同样给ICS的安全性与可靠性带来了新的挑战[2]。2010年，震网病毒作为首例针对工业控制系统设计的蠕虫病毒，对ICS的物理设备层进行攻击，感染了全球超过20万台计算机，摧毁了伊朗浓缩铀工厂五分之一的离心机，给工业基础设施安全带来了巨大的威胁。在国内，据贵州省通信管理局监测数据显示，截至2024年年底，工业互联网攻击总量达102.62万次，环比增幅达97.1%。

现有针对工业控制系统的攻击手段主要分为了恶意代码攻击、网络入侵、拒绝服务攻击、跨站脚本攻击、中间人攻击以及物理攻击等[3-5]。攻击位置包含外部网络边界、IT-OT网络桥接点、工业物理设备以及外围物理接口或移动介质[6-11]。为了应对这些威胁，研究人员和工业界提出了多种攻击检测方法，包括基于签名的检测、基于异常的检测以及基于数据驱动的检测方法。基于签名的检测方法依赖于已知的攻击特征库，对已知攻击（如特定恶意软件、漏洞利用）的检测精准率高，误报率低，能够有效防御已知恶意代码、协议攻击、未授权访问行为等ICS攻击行为[12]。基于异常的检测方法通过学习ICS的正常行为模式，能够发现偏离正常行为的异常活动，从而对设备故障、参数篡改、高级持续性威胁以及违反操作规范的行为实现有效的检测与防御[13-14]。近年来，基于数据驱动的检测方法，特别是深度学习技术，因其强大的特征学习能力，在ICS安全领域展现出巨大的潜力，该类方法能够融合设备传感器数据、网络流量、操作日志，发现隐蔽攻击链[15-16]。但上述检测方法无法对基于ICS正常流量伪造的数据进行有效的防御，因为精心制造的攻击向量可以绕过深度学习算法（随机森林、支持向量机（SVM）、决策树等[17]）的检测机制，使其被识别为正常的数据。

恶意替换ICS数据库（涵盖实时与历史数据库）中的数据，构成一种针对关键基础设施“数字基石”的系统性攻击范式。其破坏性后果所呈现的“多层级耦合、跨时空传导”等复杂特性，使其危害程度远超传统网络攻击的范畴[18]。此类攻击能够精准污染ICS的核心数据存储层[19]。ICS的实时数据库作为控制逻辑执行的即时决策依据，历史数据库承载着过程追溯、性能优化与合规审计的长期记忆。因此，此类攻击能够从根本上瓦解工业自动化赖以维系的“感知–决策–执行–记录”闭环链条的完整性与可信性。在实时操作层面，恶意篡改实时数据库将直接诱发控制逻辑紊乱与物理过程失稳。例如，在化工生产场景中，伪造反应器温度实时读数可导致冷却剂阀门错误关闭，触发放热反应失控链；在电网调度中，注入虚假的母线频率实时数据会误导自动发电控制系统发出错误调频指令，引发区域电网振荡甚至级联停电[20]。实时数据库污染具有即时性，可在秒级时间内将数字攻击转化为物理世界的灾难性后果。在历史数据维度，恶意替换则表现为隐蔽的认知战与系统欺诈。历史数据库作为工业知识沉淀与决策优化的基础，其真实性是构建精准数字孪生、实施预测性维护及合规审计的前提。系统性伪造设备运行历史将导致维护策略偏离实际：掩盖渐进故障可能引发灾难性设备失效，扭曲能效数据则会使优化算法收敛于虚假最优解，造成长期资源错配与经济损耗[21]。历史数据的污染具备时空扭曲效应，通过伪造过去事件的时间戳或序列，可干扰事故原因分析，使调查人员构建错误的故障时间线，最终导致责任误判与安全改进措施失效。从监管视角看，对ICS数据库完整性的系统性篡改将直接解构合规性证据链，引发监管处罚及运营许可风险[22]。

基于深度学习算法的检测模型对攻击载荷的检测能力日益加强，同时ICS边界防御也愈发严密。针对这一挑战，本文提出一种面向协议规避与数据操控的工业控制系统隐蔽攻击载荷生成与无感注入机制。该机制的核心是利用ICS通信协议固有的认证与校验缺陷，构建一个完整的、以高隐蔽性污染ICS数据为目标的攻击链。具体而言，该攻击链包含3个关键环节：首先，利用时间序列生成对抗网络–长短期记忆网络（Time-GAN-LSTM，time-series generative adversarial net-

work-long short-term memory）模型深度学习正常工控流量的数据特征，打造高保真的“正常行为”攻击载荷。该模型通过学习ICS的真实正常流量，在低维潜在空间中解耦ICS静态与动态特征，并集成长短期记忆（LSTM，long short-term memory）网络门控单元强化对ICS数据长程依赖的精确建模能力，从而生成符合原始流量时序特征、分布特征以及物理规律的攻击载荷。此类载荷因其微小的参数变异特性从而具有高隐蔽性与潜伏性，这使其不仅能对物理设备造成破坏，更能有效规避依赖“正常–异常”特征学习的检测模型。其次，针对“震网”事件后企业普遍采用的防火墙与协议加固等边界防护措施，本文从ICS通信协议漏洞出发，设计了隐蔽的攻击途径。以施耐德可编程逻辑控制器（PLC，programmable logic controller）为例，本文利用一个原创高危漏洞（证书编号：CNVD-YCGN-202504007625），劫持统一消息传递应用程序服务（UMAS，unified messaging application service）协议会话ID，并通过协议逆向以及会话逻辑重构，在协议、连接与时序层面深度模拟合法通信行为，实现未授权的权限绕过以及协议规避，为上述特意打造的攻击载荷提供新型隐蔽攻击途径。最后，通过特定的SQL注入和数据库接管工具（SQLmap，SQL injection and database takeover tool），将前述高隐蔽性载荷经由该攻击途径秘密注入ICS历史数据库，以实现长期潜伏，并等待时机造成关键性破坏。

本文的主要贡献总结如下。

1) 通过设计TimeGAN-LSTM模型工业控制系统的正常样本生成符合原始流量时序特征以及分布特征的攻击载荷，旨在绕过传统的ICS检测机制，实现攻击载荷的隐蔽性以及潜伏性，实验证明了本文生成的攻击载荷能够100%绕过基于逻辑回归、随机森林、支持向量机以及决策树的检测。

2) 通过本文团队的原创高危漏洞（证书编号：CNVD-YCGN-202504007625）对工程师站与PLC之间的通信协议进行攻击，实现协议的检测规避，用于辅助攻击载荷对实时数据库的无感注入。

3) 通过SQLmap工具对ICS历史数据库进行注入攻击，实现攻击载荷的隐蔽式注入，实验验证了本文能够有效对ICS的历史数据库进行隐蔽式的数据操纵。

1 相关工作

1.1 面向ICS的TimeGAN算法

TimeGAN算法在工业控制系统安全领域近年来受到越来越多的关注，它通过结合生成对抗网络和时间序列分析，为ICS安全提供了新的解决方案[23]。TimeGAN能够学习ICS正常运行状态下的时间序列数据分布，从而生成与真实数据高度相似的合成数据。这些合成数据通常用于异常检测以及数据增强领域，在ICS异常检测研究领域，通过比较真实数据与TimeGAN生成的正常数据之间的差异，可以有效地检测ICS中的异常行为。例如，可以利用生成对抗网络–长短期记忆（GAN-LSTM，generative adversarial network-long short-term memory）网络构建智能入侵检测系统，生成攻击模式，提高检测器性能[24]。此外，还可以结合变分自编码器来提高异常检测的准确性[25]。在数据增强研究领域，ICS中恶意攻击数据通常难以获取，而TimeGAN可以生成大量的合成攻击数据，用于训练和评估入侵检测系统，提高其泛化能力和鲁棒性[26]。特别是在数据不平衡的情况下，TimeGAN可以通过生成少数类样本来缓解数据偏斜问题，提高检测性能[27]。本文主要关注其在攻击样本生成方面的优势，使用TimeGAN生成伪造的真实样本用于绕过ICS的检测机制，实现高隐蔽性的注入。

1.2 面向ICS的LSTM算法

LSTM是一种常用于处理时间序列数据的循环神经网络（RNN）架构[28]。它通过引入记忆单元和门控机制解决传统RNN中的梯度消失问题，从而能够学习长期依赖关系[29]。LSTM在ICS中的核心应用领域包含网络入侵检测以及工业异常检测等。在网络入侵检测研究领域LSTM能够分析网络流量模式，识别潜在的网络攻击，例如，Jiang[30]提出了一种基于卷积神经网络–长短期记忆（CNN-LSTM，convolutional neural network-long short-term memory）网络的网络异常流量检测方法可以有效检测异常网络流量。Danladi等[31]混合GAN-LSTM模型用于预测网络威胁情报和实时异常检测。在工业异常检测研究领域，LSTM可以用于检测各种时间序列数据中的异常模式，例如自然气管道数据、航天器遥测数据[32]。本文利用LSTM与TimeGAN进行融合，用于生成符合ICS正常流量

静态分布以及保留工业数据中的因果关联和动态演化模式的高质量攻击样本。

1.3　面向ICS的SQLmap渗透工具

SQLmap 是一款自动化结构化查询语言（SQL，structured query language）数据库注入漏洞检测和利用的渗透测试工具[33]。它通过多种技术识别 SQL 注入漏洞，并可用于获取数据库信息、访问数据库模式、转储表数据以及执行权限提升等操作。SQLmap 通过多种攻击技术来利用 SQL 注入漏洞，其常见技术包括布尔盲注、时间盲注、联合查询注入以及报错注入等[34]。利用这些技术，SQLmap 不仅能自动完成数据库指纹识别、数据提取、数据库枚举，还能够在权限允许的情况下读取/写入文件，甚至执行操作系统命令[35]。本文针对 ICS 数据库的弱保护性，在攻击链注入环节，利用 SQLmap 渗透工具对精心制造的攻击载荷进行隐蔽式注入，实现对 ICS 核心数据的操控。

2　面向工业控制系统的隐蔽式持久性高级威胁模型

本文设计了面向 ICS 的隐蔽式持久性高级威胁模型，如图 1 所示。该威胁模型通过 TimeGAN-LSTM 算法对 ICS 真实的正常样本进行生成，用于构造“合法”攻击向量绕过检测机制。并从协议规避角度以及数据操纵角度设计了 2 种定制化的数据注入方案，用于对 ICS 的实时数据库以及历史数据

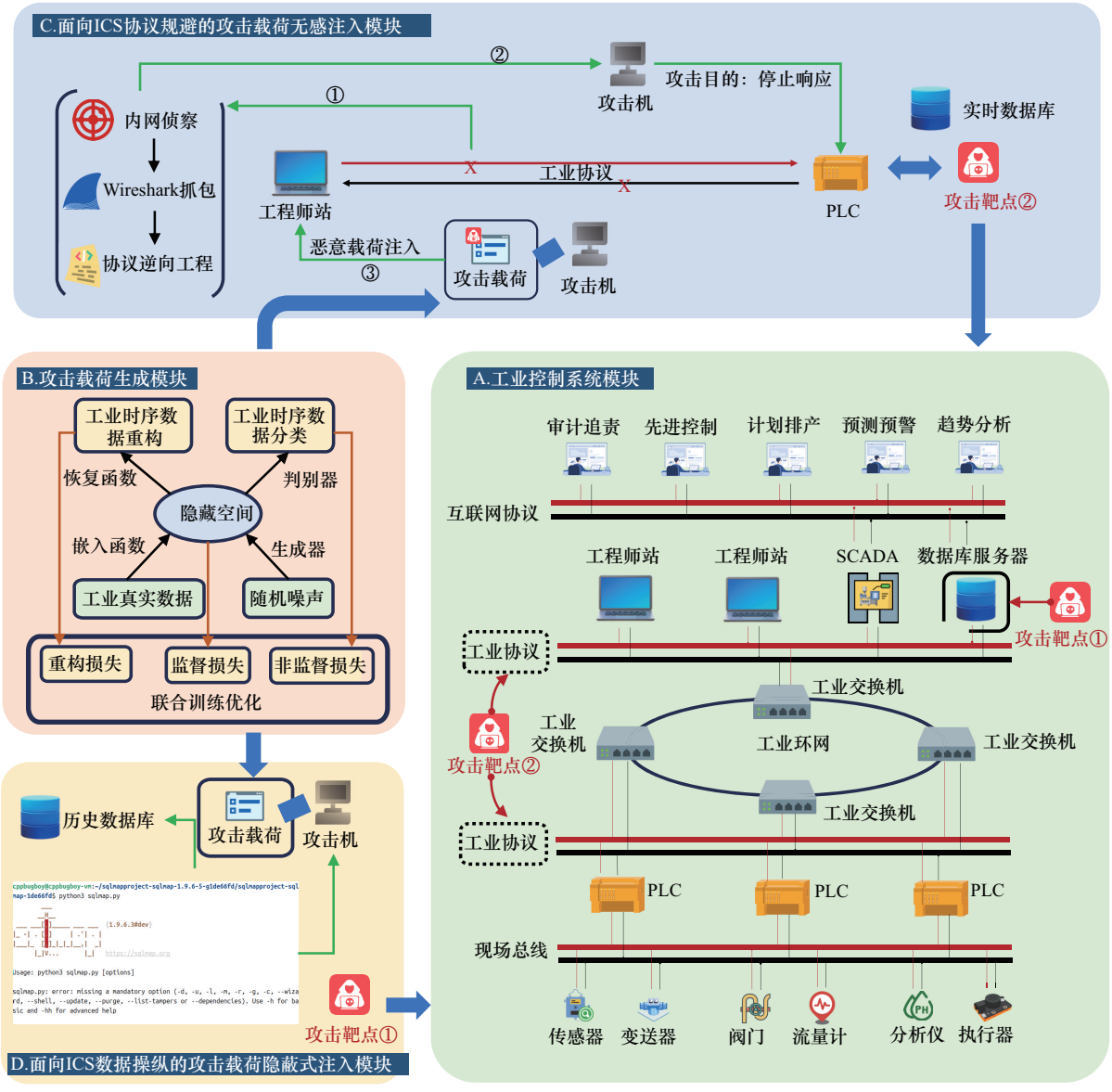


图 1　面向 ICS 的隐蔽式持久性高级威胁模型

库进行污染。模型分为工业控制系统模块、攻击载荷生成模块、面向ICS协议规避的攻击载荷无感注入模块以及面向ICS数据操纵的攻击载荷隐蔽式注入模块。

面向ICS的隐蔽式持久性高级威胁模型攻击流程如下。

阶段1（目标与准备）：以工业控制系统模块为攻击靶点，利用数据库服务器的检测机制缺陷以及工业协议缺乏身份认证、访问授权等设计缺陷确定攻击目标为可编程逻辑控制器、工程师站、PLC与工程师站之间的通信协议、实时数据库以及历史数据库。

阶段2（载荷生成）：在攻击载荷生成模块中，部署TimeGAN-LSTM模型，其核心任务是基于真实的ICS正常流量样本，合成具有高隐蔽性的“正常行为”攻击载荷。首先，在低维潜在空间中对ICS数据的静态属性与动态时序特性进行有效解耦；其次，集成LSTM门控单元强化对数据长程依赖关系的精确捕捉能力。最后，生成符合真实流量时序特征、数据分布以及内在物理规律的攻击载荷。

阶段3（协议规避与无感注入）：在阶段二的攻击载荷生成模块中获得攻击载荷后，面向ICS协议规避的攻击载荷无感注入模块利用原创漏洞在协议、连接与时序层面深度模拟合法通信行为，实现未授权的权限绕过以及协议规避，将载荷注入实时通信，即时篡改工业控制系统模块呈现的实时数据库。

阶段4（数据操控与攻击载荷潜伏）：面向ICS数据操纵的攻击载荷隐蔽式注入模块利用SQL注入漏洞作为渗透入口，利用SQLmap获取数据库服务器的访问与操纵权限。将阶段二中生成的高隐蔽性攻击向量作为“合法”数据，隐蔽地注入工业控制系统模块历史数据中，规避基于数据特征的传统检测机制，实现攻击载荷的长期潜伏。

上述4个模块的详细介绍如下。

工业控制系统模块：典型工业控制系统在架构上分为计划管理层、制造执行层与工业控制层。计划管理层集成审计追踪、先进控制、排产计划、预测预警及趋势分析等高级应用，并通过互联网协议与制造执行层进行数据交互。制造执行层包括工程师站、数据采集与监视控制（SCADA，supervisory control and data acquisition）系统、数据库服务器及人机界面（HMI，human machine interface）等设备，借助Modbus、Profibus等工业协议与工业控制层的PLC通信。PLC进一步通过现场总线连接底层传感器与执行器。面向ICS的隐蔽式持久性高级威胁模型针对数据库服务器的检测机制缺陷以及工业协议在身份认证与访问授权方面的设计弱点展开攻击，攻击靶点具体位置如图1所示。

攻击载荷生成模块：ICS中的实时与历史数据属于时序数据。为规避攻击样本检测机制，本文基于正常ICS流量设计了TimeGAN-LSTM算法以生成攻击载荷。其中，LSTM用于增强攻击向量生成过程中对历史长期信息与当前信息的依赖关系；TimeGAN则结合无监督与有监督学习，以解决攻击向量在时序数据中的生成与自回归问题。

面向ICS协议规避的攻击载荷无感注入模块：为实现隐蔽且有效的攻击载荷注入，本文针对工程师站与PLC之间的工业通信协议，设计了定制化的无感注入机制。首先，通过内网侦察、网络封包分析软件（Wireshark）抓包与协议逆向，提取工业协议中的IP、通信协议、功能码等关键信息，筛选数据采集指令，为攻击实施奠定基础。随后，利用攻击机伪装成工程师站，发送恶意指令使目标PLC停止响应。最后，伪造目标PLC身份，并基于攻击载荷模型生成的攻击向量构造响应数据包，实现对ICS实时数据库的无感注入。

面向ICS数据操纵的攻击载荷隐蔽式注入模块：ICS历史数据库多采用SQL Server、Oracle等系统。本文借助SQLmap工具，利用SQL注入漏洞获取数据库服务器权限，并对攻击向量进行注入，以实现对历史数据的隐蔽操纵。SQLmap支持包括MySQL、Oracle、SQL Server等在内的30多种数据库，能够有效绕过传统检测机制，确保注入过程不被发现。

2.1 基于TimeGAN-LSTM的攻击载荷生成机制

攻击载荷生成模块旨在生成与ICS原始真实样本高度相似的攻击样本用于绕过ICS的检测机制。ICS原始真实样本具有长序列、时序性、特征维度高等特性。TimeGAN通过对抗训练生成符合ICS原始真实样本分布的时间序列，LSTM的遗忘门、输入门和输出门机制能精准捕捉长期依赖关系（如设备状态趋势、周期性波动）。本文对TimeGAN与LSTM进行融合，能够生成覆盖ICS原始真实样本

静态分布以及保留工业数据中的因果关联和动态演化模式的攻击样本。LSTM 支持多变量输入（如温度、压力、流量等并行传感器数据），而 TimeGAN 的生成器可通过条件变量（如设备状态标签）控制输出，更适用于特征维度高的 ICS 原始真实样本数据，生成更符合物理规律的攻击样本。TimeGAN-LSTM 的攻击载荷生成机制示意如图 2 所示。

攻击载荷生成模块包含自编码子模块以及对抗子模块，自编码子模块包含嵌入器和恢复器，对抗子模块包含生成器和判别器。嵌入器将工业真实数据的静态特征和动态特征转化为隐藏状态，并映射到一个低维的潜在空间，用于提高原始工业数据的关键信息的捕捉能力，同时降低数据的维度，嵌入器如式(1)所示。

$$e{:}\beta \times \prod_t \phi \rightarrow H_\beta \times \prod_t H_\phi \tag{1}$$

其中，β为静态特征的空间，$\prod_t \phi$为时间序列特征在时间步 t 上的笛卡尔积，H_β和H_ϕ分别表示静态特征和时间序列特征的潜在空间。

恢复器的作用是将隐藏空间的特征重新转换为静态和动态特征，获得工业数据的重构时间序列数据，如式(2)所示。

$$\begin{aligned} r{:}H_\beta \times \prod_t H_\phi \rightarrow \beta \times \prod_t \phi, \\ \forall \tilde{\beta} = r_\beta(h_\beta), \tilde{\phi}_t = r_\phi(h_t) \end{aligned} \tag{2}$$

其中，静态特征恢复网络 r_β 将隐藏空间的 ICS 原始数据静态特征 h_β 恢复回 $\tilde{\beta}$，动态特征恢复网络 r_ϕ 将隐藏空间的 ICS 原始数据动态特征 h_t 恢复回 $\tilde{\phi}_t$，ϕ_t 为动态特征序列。重构损失定义如式(3)所示。

$$\mathcal{L}_R = \mathbb{E}_{\beta,\phi_{1:T}\sim p}\left[\| \beta - \tilde{\beta} \|_2 + \sum_{t=1}^{T} \| \phi_t - \tilde{\phi}_t \|_2\right] \tag{3}$$

在潜在空间引入监督器用于保持时间动态，其中监督损失用于增强生成器捕捉数据中的逐步条件

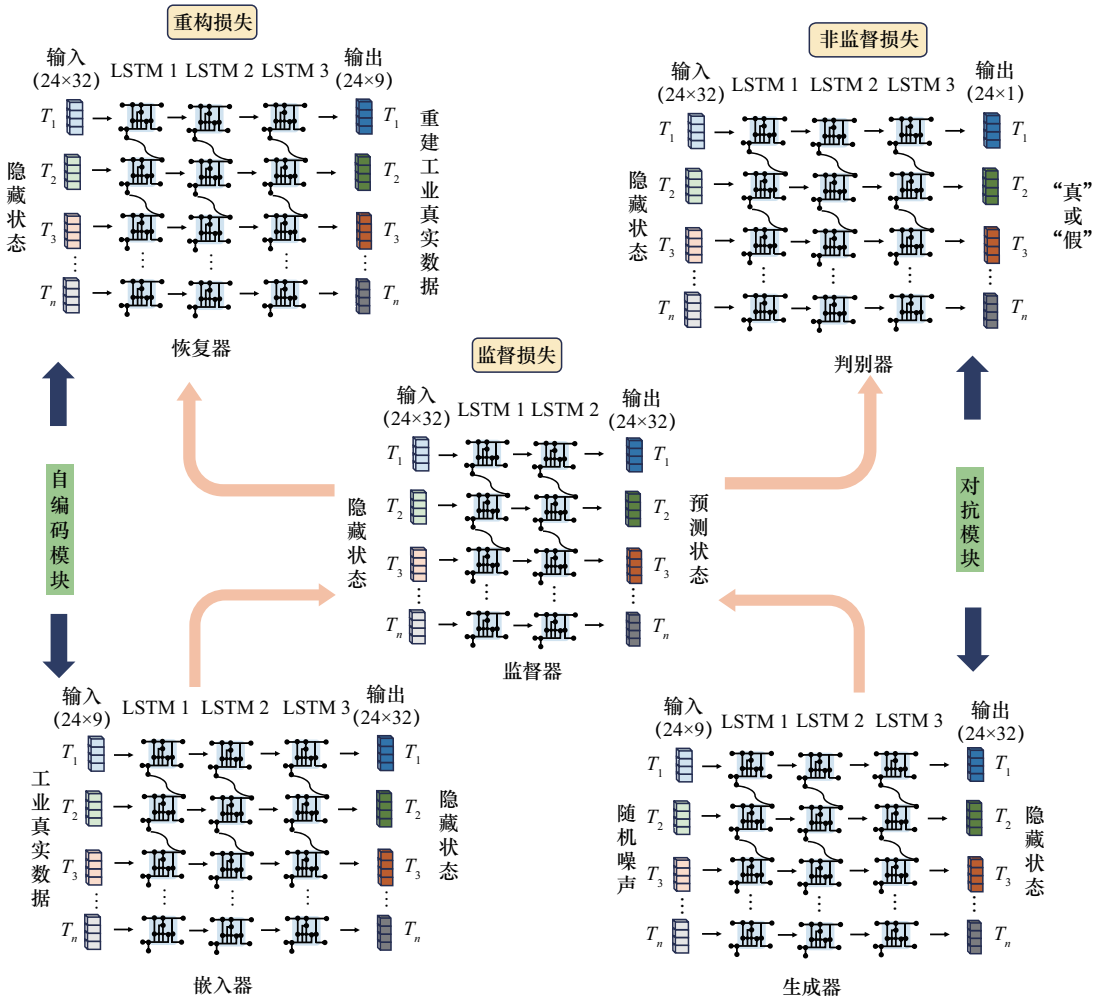


图 2　TimeGAN-LSTM 的攻击载荷生成机制示意

分布，并应用最大似然得到的监督损失评估生成器对真实数据特征和潜在特征的学习能力，如式(4)所示，其中g_β表示预测状态，h_ϕ表示时间序列特征，z_t表示随机噪声向量。

$$\mathcal{L}_S = \mathbb{E}_{\beta,\phi_{1:T}\sim p}\left[\sum_t \left\| h_t - g_\beta(h_\phi, h_{t-1}, z_t) \right\|_2\right] \tag{4}$$

对抗子模块包含生成器和判别器，生成器用于在潜在空间生成序列数据，初始输入一个与原始工业数据相同分布特征的随机噪声，生成函数如式(5)所示，用于获得由静态和动态特征组成的隐藏特征。

$$g: z_\beta \times \prod_t z_\phi \to H_\beta \times \prod_t H_\phi \tag{5}$$

其中，z_β和z_ϕ为随机噪声的已知分布的向量空间。

判别器用于对潜在空间的隐藏特征进行分类。其接受静态和时间序列的隐藏特征，通过双向递归网络区分真实数据和生成数据的潜在表示，尽可能准确地判别数据是真实的还是合成的，如式(6)所示。非监督损失的定义如式(7)所示。

$$d: H_\beta \times \prod_t H_\phi \to [0,1] \times \prod_t [0,1] \tag{6}$$

$$\mathcal{L}_U = \mathbb{E}_{\beta,\phi_{1:T}\sim p}\left[\ln y_\beta + \sum_t \ln y_t\right] + \mathbb{E}_{\beta,\phi_{1:T}\sim \hat{p}}\left[\ln(1-\hat{y}_\beta) + \sum_t \ln(1-\hat{y}_t)\right] \tag{7}$$

嵌入器、恢复器、监督器、生成器以及判别器的核心模型采用LSTM。LSTM是一种特殊的循环神经网络，通过设计门控机制解决传统RNN的梯度消失与长期依赖问题。其核心在于引入3个门控单元（遗忘门、输入门、输出门）和一个记忆单元（Cell State），形成对信息流的精细化控制。遗忘门决定历史记忆的保留比例，由Sigmoid函数输出0~1的值，如式(8)所示。

$$f_t = \sigma\left(\boldsymbol{W}_f \cdot [h_{t-1}, x_t] + b_f\right) \tag{8}$$

其中，σ为Sigmoid激活函数，$\boldsymbol{W}_f$为遗忘门的权重矩阵，$[h_{t-1}, x_t]$将前一时刻的隐藏状态h_{t-1}与当前输入x_t拼接作为输入，b_f为偏置项。当时丢弃历史记忆，$f_t \approx 1$时完全保留。

输入门控制新信息的写入强度，如式(9)所示，其中i_t表示输入门的输出，b_i表示输入门的偏置项。同时，候选记忆生成待存储的新信息，如式(10)所示，其中$\boldsymbol{W}_C$表示候选记忆的权重矩阵，b_C表示候选记忆的偏置项。

$$i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i) \tag{9}$$

$$\tilde{C}_t = \tanh(\boldsymbol{W}_C \cdot [h_{t-1}, x_t] + b_C) \tag{10}$$

其中，$\tilde{C}_t$为候选细胞状态，用于捕捉序列中的长期依赖信息。tanh为双曲正切激活函数，对输入做非线性变换。

记忆单元用于融合遗忘与新增信息如式(11)所示。

$$C_t = f_t \odot C_{t-1} + i_t \odot \tilde{C}_t \tag{11}$$

其中，$\odot$表示逐元素乘法，实现历史记忆C_{t-1}与新信息$\tilde{C}_t$的加权融合。

输出门用于调节当前记忆的对外暴露量，即t时刻的输出，如式(12)所示，最终输出如式(13)所示。

$$o_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o) \tag{12}$$

$$h_t = o_t \odot \tanh(C_t) \tag{13}$$

通过TimeGAN与LSTM的融合适用于高动态、强时序依赖的ICS原始数据，其核心价值在于能够基于正常的ICS流量有效地生成时序、慢变的攻击样本，从而更有效地绕过ICS的数据检测机制，从而实现数据的无感注入。

2.2 面向ICS协议规避的攻击载荷无感注入机制

针对ICS常用的工业协议，本文提出一种面向ICS协议规避的攻击载荷无感注入机制，用于实现攻击数据对ICS上位机进行隐蔽式数据注入，目标在于对ICS的实时数据库进行数据污染，如图3所示。攻击链主要包含3个阶段，包含上位机与PLC之间的流量抓取与协议逆向、伪造上位机指令包对目标PLC进行主动攻击使其停止响应以及伪造目标PLC响应包进行协议检测机制规避，进而实现攻击数据的无感注入。

前期工作：通过物理接触或社会工程手段将预装Kali Linux的攻击终端接入目标ICS内网。使用网络映射器（Nmap，network mapper）进行隐蔽式拓扑测绘，确认网段划分及防火墙策略。部署Wireshark并配置伯克利包过滤器（BPF，Berkeley packet filter）实现协议级流量捕获，同时安装Scapy数据包操作库用于自定义报文构造。

上位机与PLC之间的流量抓取与协议逆向包含4个步骤。

步骤1：通过Wireshark工具对ICS内网进行扫描，并抓取工程师站与PLC之间的实时通信数据包。捕获会话，重点分析PLC端与工作站的IP漂

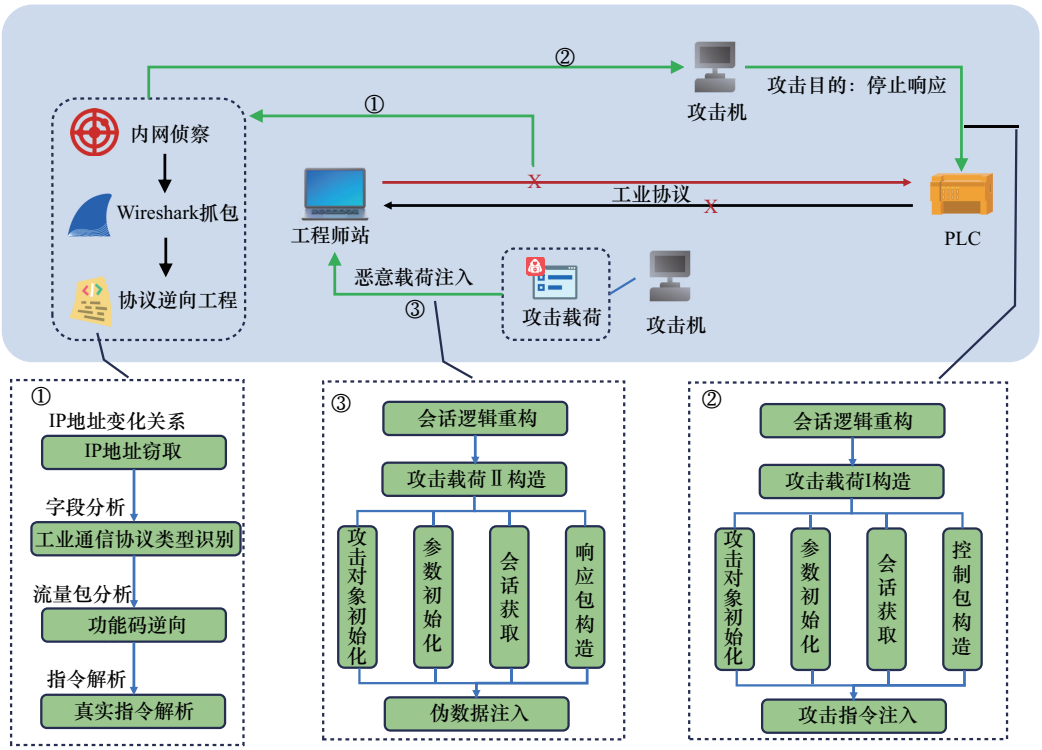


图 3　面向 ICS 协议规避的攻击载荷无感注入机制

移模式。其中，通过分析 Time 字段、Source 字段、Destination 字段，确定通信双方的 IP 地址变化、通信协议变化深入解析工程师站与 PLC 数量，对双方相应的 IP 地址进行窃取。

步骤 2：通过抓取的实时通信数据包进行数据包字段分析。首先进行工业通信协议识别，通过 Protocol 字段区分 Modbus 协议、Profibus 协议、UMAS 等。其次，对不同的描述符进行匹配，以进一步确定流量包抓取的完整性。最后，对不同描述符的值进行进一步分析，明确其具体含义。

步骤 3：功能码逆向工程，通过抓取到的实时通信数据包顺序以及时间关系，对“建立连接”等数据包进行协议逆向工程分析，通过与具体的工业协议格式对比分析，窃取并分析相应的功能码作用，包括初始化、读数据、请求响应等，具体为使用 TShark 执行深度协议解析，重点识别功能码分布特征。

步骤 4：真实指令解析，通过工程师站与 PLC 的响应，对数据采集指令进行解析，用于后续攻击载荷的构造，实现数据的无感注入。

伪造上位机指令包对目标 PLC 进行主动攻击使其停止响应，包含 3 个步骤。

步骤 1：会话逻辑重构，采用 Wireshark 的 Follow TCP Stream 功能重建完整会话时序，重点分析 3 次握手特征，包含初始化阶段、会话维持阶段以及异常检测阶段。

步骤 2：攻击载荷 I 构造，首先对攻击目标 PLC 进行初始化，设置目标 IP、端口、超时时间等参数。其次，创建套接字（Socket）连接，并检查设备是否在线，确认可达性后建立连接。最后，依据协议逆向构造攻击载荷。

步骤 3：对目标 PLC 进行指令注入，使其停止响应。伪造目标 PLC 响应包实现攻击数据的无感注入阶段核心在于攻击载荷Ⅱ的构造，核心方法为对响应包进行关键字段篡改进而进行深度伪造，实现伪造数据的无感注入。其中，功能码保持与原请求一致，数据域将生成的数据对线圈/寄存器中的值进行替换，并维持数据长度和类型避免语法异常。

2.3　面向 ICS 数据操纵的攻击载荷隐蔽式注入机制

ICS 的历史数据库多为 SQL Server、Oracle 等，SQLmap 能够发现并利用给定的统一资源定位符（URL）进行 SQL 注入。其核心功能包括数据库指纹识别、数据库枚举、数据提取、访问目标文件系统，并在获取完全的操作权限时执行任意命令。因此，本文基于 SQLmap 对 ICS 历史数据库进行污染，并设计了面向 ICS 数据操纵的攻击载荷隐蔽式注入机制，如图 4 所示。

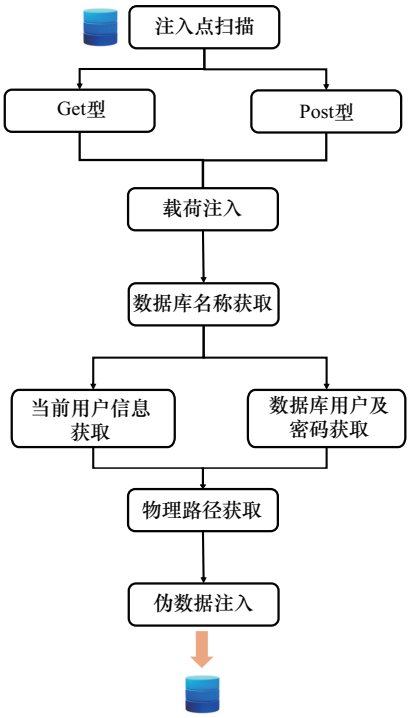


图 4　面向 ICS 数据操纵的攻击载荷隐蔽式注入机制

本文将注入过程分为了 5 个步骤。

步骤 1：注入点扫描。本步骤用于探测目标 URL 是否存在 SQL 注入漏洞。根据网站类型分别处理：对于不需要登录的 Get 型网站，直接指定 URL；需登录的 Get 型网站则先获取 Cookie 参数；Post 型网站需指定账号、密码等参数。随后在终端执行命令（如 Python SQLmap.py -u "http://example.com/page id=1" --batch）进行扫描，最终输出疑似盲注点及对应攻击载荷。

步骤 2：载荷注入。在识别到疑似注入点后，向目标参数自动注入测试载荷，方法包括布尔检测、时间延迟检测与错误响应检测。通过对比正常响应与注入响应的差异（如页面内容、响应时间、数据库报错），判定注入点是否有效及其具体类型。最终输出漏洞类型、数据库类型及可用注入技术。

步骤 3：数据库信息获取。确认注入点有效后，进一步获取数据库相关信息。首先通过 --dbs 命令列出所有可访问数据库名称；再借助 --current-user 与 --current-host 提取当前用户及主机信息。若当前账户权限较高，则使用 --users --passwords 发起凭证提取攻击，获取用户权限范围及密码哈希状态。

步骤 4：物理路径获取。利用数据库的文件操作功能探测服务器路径结构，例如执行 --file-read 指令读取服务器文件。通过数据库错误信息或内置函数推断路径，并在具备文件权限时直接读取目标文件。

步骤 5：伪数据注入。将 2.1 节基于正常流量构造的攻击数据，注入 ICS 历史数据库中，完成隐蔽的数据操纵。

3　结果与分析

本文对面向协议规避与数据操控的工业控制系统隐蔽攻击载荷生成与无感注入机制进行了研究，包含通过 TimeGAN-LSTM 算法设计了基于 ICS 正常流量的攻击样本。设计了面向 ICS 实时数据库以及历史数据库的双路径攻击载荷隐蔽式注入机制。本节对上述设计进行了实际验证与分析。

3.1　攻击载荷生成验证与分析

安全水处理（SWaT）数据集产生于一个真实的工业水处理测试平台长达 11 天的数据采集，其中前 7 天系统处于正常运行状态，后 4 天施加了多种物理与网络攻击，如图 5 所示。数据集记录了每秒的传感器读数和执行器状态、SCADA 与 PLC 之间的网络通信，具有高时间分辨率。该数据集结合了真实工业环境的物理属性数据与网络流量数据，同时提供了精确标注的攻击与正常数据。

SWaT 数据集是一个 6 阶段（原水入住、化学投药、超滤、脱氯、反渗透、反冲洗）的水处理平台，包含 51 个特征，946 722 条数据。特征方面，Ahmed 等[36] 指出 FIT101、LIT101、AIT201、AIT202、AIT203、FIT201、LIT301、FIT301、DPIT301、LIT401、FIT401、FIT501、PIT501、FIT502、PIT502、FIT503、PIT503、FIT601 这 18 个特征都是连续值属性，其余的都是离散属性。本文实验注重于原水注入、化学投药、超滤 3 个阶段共 9 个特征的正常数据生成攻击样本，并于脱氯、反渗透、反冲洗 3 个阶段的正常数据混合用于增强攻击载荷的隐蔽性。数据层面，包含传感器和执行器状态等物理属性数据以及“SCADA-PLC”网络通信数据。由于本文的攻击载荷依赖于 ICS 的原始正常流量，因此，本文主要关注 SWaT 数据集前 7 天采集到的正常数据，具体时间段为 2015 年 12 月 22 日 16:30:00 至 2015 年 12 月 28 日 9:59:59，包含 495 000 条数据。后 4 天的攻击数据被用于训练检测模型，以评估模型在攻击载荷检测与规避方面的性能。

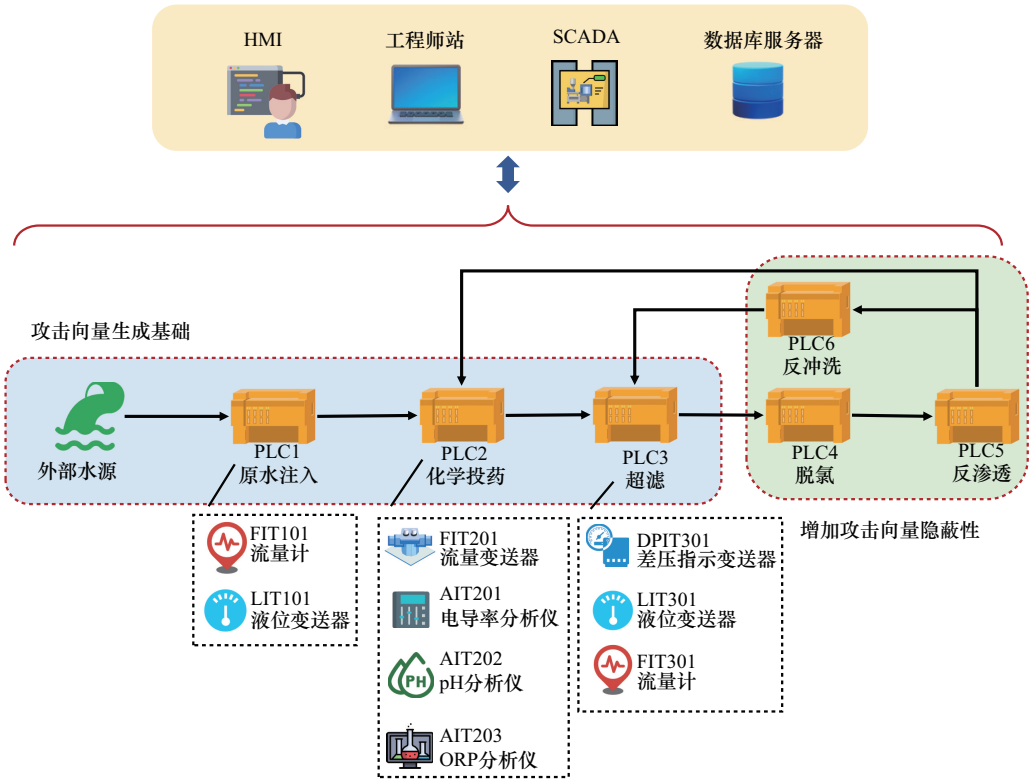


图 5　工业水处理测试平台示意

TimeGAN-LSTM超参数设置如表1所示，TimeGAN-LSTM的组件输入输出如表2所示。本文采用TimeGAN-LSTM生成了与原始样本数量一致的攻击样本数量，为了直观展示生成数据与真实数据在特征分布上的相似性，本文从完整数据集中随机选取了250个样本，分别采用主成分分析（PCA, principal component analysis）和t-分布随机邻域嵌入（t-SNE, t-distributed stochastic neighbor embedding）2种经典的降维算法进行特征可视化，如图6所示。

表1　TimeGAN-LSTM超参数设置

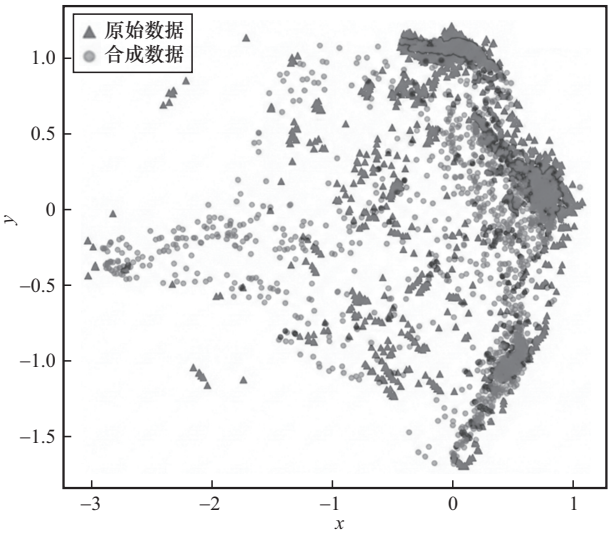
配置	参数	说明
序列长度	24	每个样本的时间步数
特征数量	9	SWaT传感器数量
隐藏层维度	32	LSTM单元数
噪声维度	32	生成器输入噪声维度
批大小	128	训练批次大小
学习率	5×10^{-4}	Adam优化器学习率
训练步数	1 000	每个训练阶段的迭代次数
网络深度	3层	主要组件的LSTM层数
γ参数	1	判别器损失权重

表2　TimeGAN-LSTM的组件输入输出

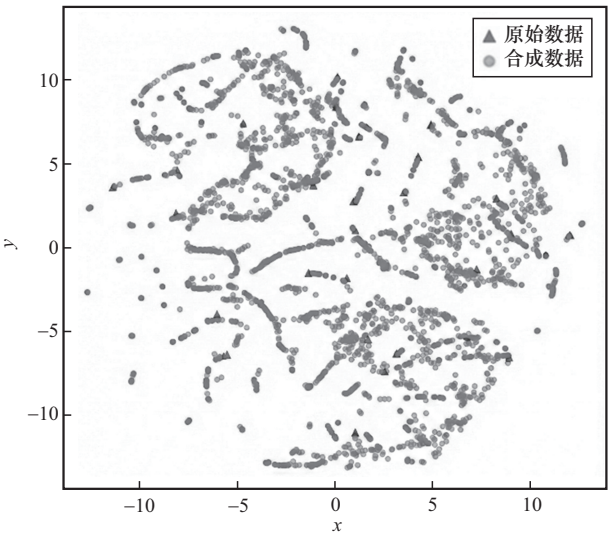
组件	输入维度	输出维度	功能
嵌入器	(batch, 24, 9)	(batch, 24, 32)	数据→隐藏表示
恢复器	(batch, 24, 32)	(batch, 24, 9)	隐藏表示→数据
生成器	(batch, 24, 9)	(batch, 24, 32)	噪声→隐藏表示
监督器	(batch, 24, 32)	(batch, 24, 32)	保持时间动态
判别器	(batch, 24, 32)	(batch, 24, 1)	区分真实/合成
完整生成器	(batch, 24, 9)	(batch, 24, 9)	噪声→合成数据

图6(a)为基于PCA的降维结果，其中，三角形表示原始数据，圆形表示TimeGAN-LSTM生成的合成数据。可以观察到，尽管存在部分边缘样本的离散分布，整体而言两类数据在二维投影空间中呈现出较好的重叠和分布一致性，特别是在主要的数据密集区域，合成数据能够较好地覆盖原始数据的分布模式。这说明生成模型在保留数据主成分特征方面表现出良好的重构能力。图6(b)为t-SNE降维后的可视化结果，该算法更关注局部结构的保持，因此更能反映ICS正常流量样本间的非线性关系。从图6可以看出，合成数据在高维特征空间的投影中与原始数据存在高度的聚

类一致性，多个局部簇结构几乎被完全复现，进一步验证了TimeGAN-LSTM在捕捉复杂时序数据分布特性方面的能力。局部邻域结构的高度重合提供了有效的视觉证据支持生成数据的真实性与判别性。



(a) 基于PCA的降维结果



(b) t-SNE降维后的可视化结果

图6　合成数据（攻击样本）与原始数据PCA与t-SNE降维后的可视化对比

为了验证本文使用TimeGAN-LSTM生成的合成数据的攻击检测绕过能力，对正常数据、合成数据以及（SWaT）数据集后3天的攻击样本数据进行了PCA，如图7所示。可以观察到，合成数据与正常数据高度重叠，且分布一致。合成数据能够有效地伪造成正常样本对ICS检测机制进行绕过。

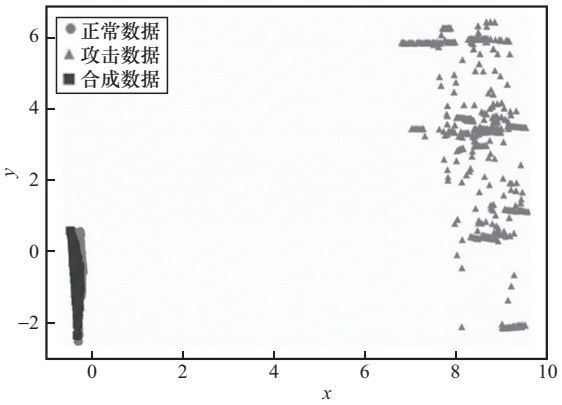


图7　ICS正常数据、攻击数据与合成数据的PCA降维可视化对比

在此基础上，为了评估生成攻击载体的整体效果，使用逃逸率（ER, evasion rate）作为核心评估指标，具体定义如式(14)所示。其中，ER为攻击载荷的逃逸能力。

$$\mathrm{ER} = 1 - \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}} \tag{14}$$

其中，TP表示被成功检测为攻击的真实攻击样本数量，FN表示被误判为正常的真实攻击样本数量。较高的ER说明攻击载荷对检测器的绕过能力更强。检测器采用TMANomaly[37]、AT-DCAEP[38]、TTA-Transformer[39]、STL-ConvTransformer[40]、RGA-nomaly[41]进行测试。图8为生成攻击载荷与真实攻击载荷对检测器的绕过能力测试。

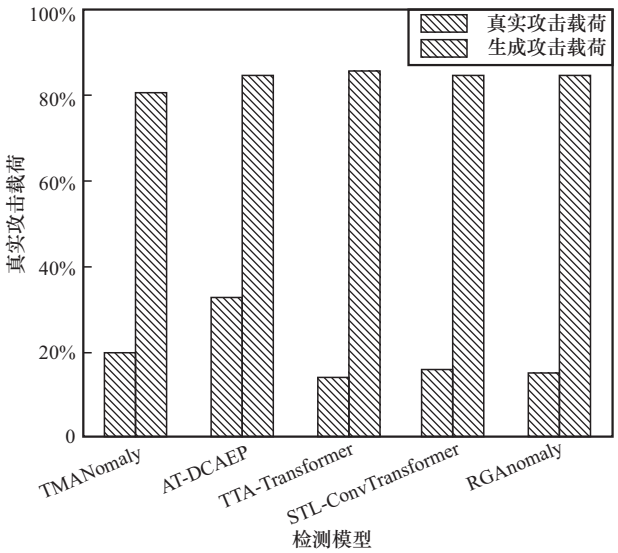


图8　生成攻击载荷与真实攻击载荷对检测器的绕过能力测试

由图8可以看出，本文的生成攻击载荷对不同的检测器的逃逸率均在80%以上，相较于真实攻

击载荷逃逸率在5倍以上。对于真实攻击载荷，由图7可以观察到，真实攻击数据与真实的正常数据存在明显的特征不一致情况，因此，检测器对真实的攻击样本的检测率在70%~80%，攻击数据的逃逸率极低。而本文的攻击载荷为TimeGAN-LSTM基于真实的正常样本生成的攻击载荷，攻击载荷的特征相较于正常样本一致性更高，因此相较于真实的攻击样本ER更高，对检测器的检测规避能力更强。

进而，本文对TimeGAN[23]、GAN-LSTM[31]利用ICS真实的正常数据生成相应的攻击载荷，并在上述检测器进行测试，测试结果如图9所示。

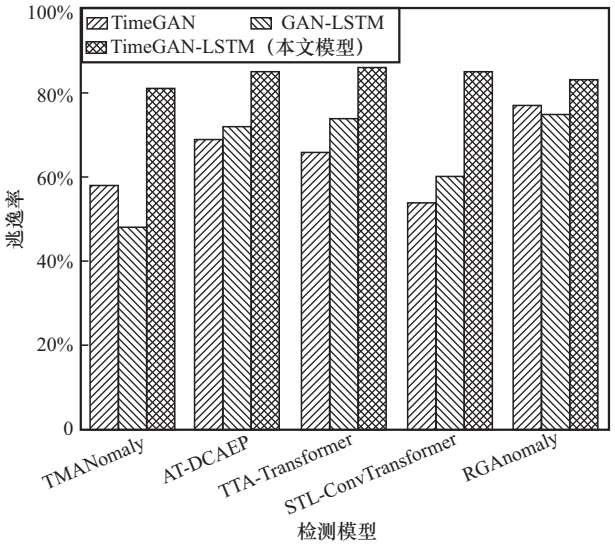


图9　不同攻击载荷生成模型的逃逸率测试

由图9可以看出，本文设计的TimeGAN-LSTM相较于TimeGAN、GAN-LSTM生成的攻击载荷逃逸率更高，这是由于相较于GAN-LSTM，TimeGAN-LSTM采纳了TimeGAN的“嵌入–监督–生成”范式，在低维潜在空间中解耦了正常流量的静态与动态特征，用于提升高维数据训练的稳定性。相较于标准TimeGAN，集成的LSTM门控单元强化了对ICS数据中“慢变趋势”等长程依赖的精确建模能力。此外，TimeGAN-LSTM能够通过引入“设备状态标签”等条件变量，实现了“上下文感知”的可控生成，确保了生成的攻击载荷在统计分布与物理语义上均“逻辑自洽”，从而对检测模型进行规避。

综上，该实验结果提供了强有力的证据，表明基于TimeGAN-LSTM的合成数据在多种检测模型下具备高度伪装性，能够以极小的统计差异融入真实数据流中。

3.2　攻击载荷协议规避与无感注入验证与分析

本文使用Schneider Quantum 140 CPU 65150对所提方案进行了验证。该型号PLC搭载高性能处理器，适用于复杂工业自动化控制场景。基于2.2节的设计方法，本文团队在该设备上发现并申报了相关原创漏洞，已获得原创漏洞证书（证书编号：CNVD-YCGN-202504007625）。验证过程涉及的设备配置信息如表3所示，系统组态及现场设备连接情况如图10所示。

表3　　PLC设备配置信息

类别	配置
PLC组件	2块CPS 22400模块 1块CPU 65150模块 1块NOE77101模块 1块ACI04000模块 1块DDO35300模块 1块CRP31200模块 1块CRA31200模块
上位机	Unity Pro XL
IP地址	192.168.1.138
掩码地址	255.255.255.0
网关地址	192.168.1.1

图10　系统组态及现场设备连接情况

采用Wireshark对ICS内网进行扫描，并抓取工程师站与PLC之间的实时通信数据包，如图11所示。对数据包字段进行分析，Unity Pro XL与Schneider Quantum PLC首先通过TCP的3次握手

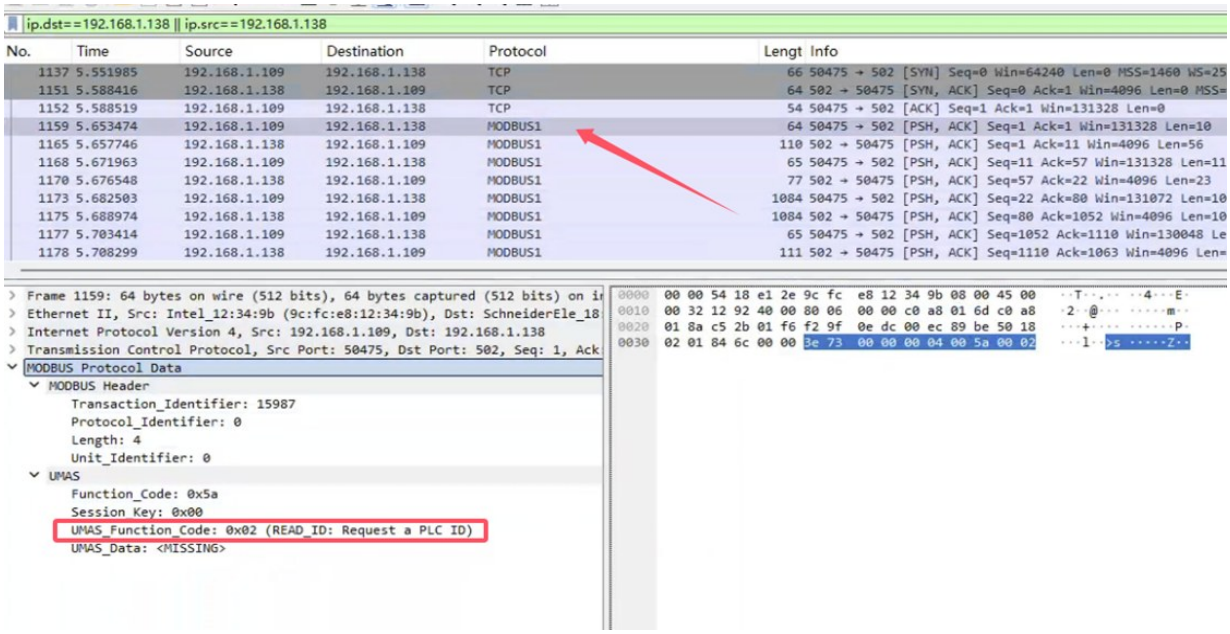


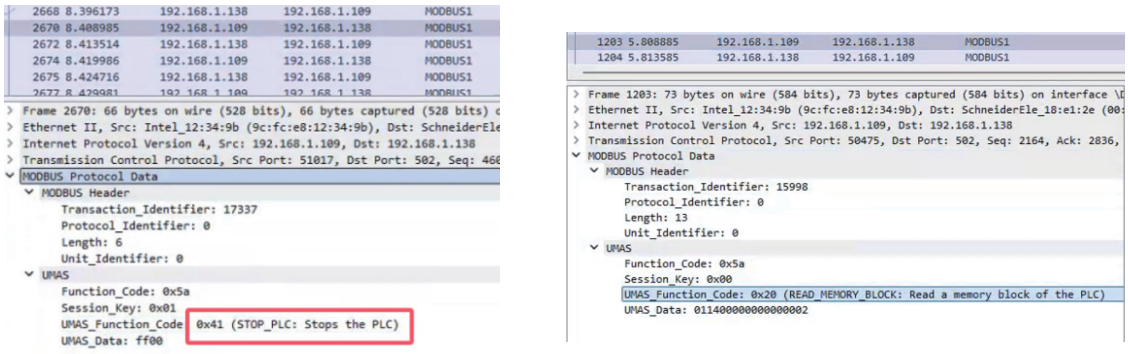
图 11　协议逆向示意

建立连接，双方通信 IP 为 192.168.1.138 与 192.168.1.138，通过 Protocol 字段确定通信协议为 Modbus 协议。

Modbus 报文头（Modbus Header）包含事务标识符（Transaction_Identifier），由客户端设置，用于将请求与响应关联起来。服务器在响应中会复制这个标识符，从而确保客户端能够识别对应的响应。协议标识符（Protocol_Identifier）通常设置为 0x0000，表示使用的是 Modbus 协议。长度（Length）表示从站地址（Unit_Identifier）到协议数据单元（PDU）末尾的总字节数。单元标识符（Unit_Identifier）用于区分网络中的不同设备。在 TCP/IP 网络中，通常设置为 0x00 或 0xFF。图 11 中，Unit_Identifier 为 0，表示目标设备的标识符为 0。功能码（Function_Code）定义了 Modbus 操作的类型，如读取线圈、寄存器等。会话密钥（Session_Key）在 UMAS 协议中，Session_Key 用于标识会话的密钥信息，用于加密或身份验证。UMAS 功能码（UMAS_Function_Code）定义了 UMAS 协议中的具体功能操作。图 11 中，UMAS_Function_Code 为 0x02，表示请求读取 PLC 的 ID。读取标识符（READ_ID）请求用于获取 PLC 的标识信息。

现已知通信协议为 Modbus 协议，其 0x01（读线圈）~0x10（写多寄存器），stop 数据包以及 read 数据包逆向解析结果如图 12 所示。其次，进行会话逻辑重构，采用 Wireshark 的跟踪 TCP 流（Follow TCP Stream）功能重建完整会话时序，基于 Python-socket 实现分层攻击框架：包含分为连接建立、会话获取、命令发送 3 个阶段。

攻击机配置及连接测试如图 13 所示，IP 地址



(a) stop数据包逆向解析结果　　(b) read数据包逆向解析结果

图 12　stop 数据包以及 read 数据包逆向解析结果

图 13　攻击机配置及连接测试

设置为192.168.1.113。

首先，设计攻击靶点为PLC的IP地址，端口为502端口，事务标识符起始值设置为0x3e73对应施耐德设备通信特征，并进行自增设计，确保符合协议连续性要求。其次，利用未授权内存读取允许获取会话ID。通过获取的会话ID，命令包携带有效会话令牌，使PLC误认为请求来自授权工程站，进行权限绕过。然后，设置5 s超时平衡工业网络延迟与攻击效率。整个攻击链使用同一个TCP连接，降低被IDS检测的风险。并设置0.5 s延时模拟合法操作间隔，规避基于报文速率的异常。最后，在发送攻击载荷前确认设备在线，避免触发大量失败日志。使用上下文管理器确保探测连接立即关闭，减少网络指纹。

图14展示了经Wireshark实时抓包，当捕获到Unity Pro XL向PLC发送的请求为读操作时，攻击机向目标PLC发送恶意的停止包，进而阶段②的攻击，使其停止响应。并将攻击载荷伪造成合法的响应，进行阶段③的攻击，实现攻击向量对实时数据库的无感注入。

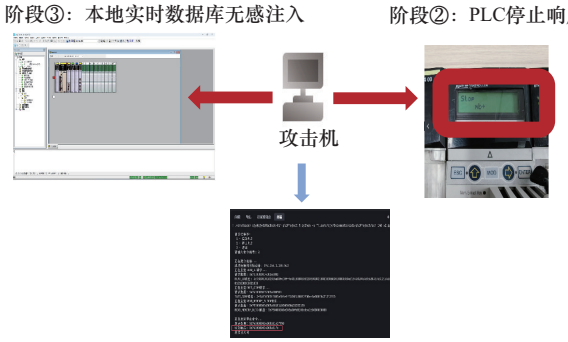


图 14　攻击结果示意

进而，本文进行了100次的协议规避攻击行为，攻击成功率测试结果如图15所示，攻击成功率为100%。

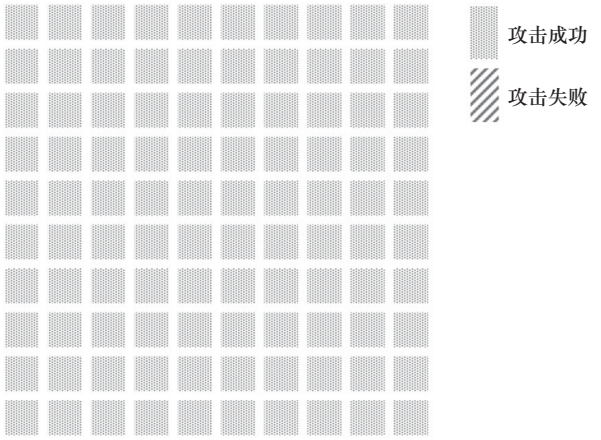


图 15　攻击成功率测试结果

如图15所示，本文基于自主挖掘的高危原创漏洞，对施耐德电气（中国）有限公司Quantum 140 CPU 65150型PLC实施了攻击。该设备通信协议中存在拒绝服务漏洞，利用此漏洞，本文实现了对PLC及上位机的攻击载荷无感知注入与协议级规避，从而达到了100%的攻击成功率。

3.3　基于SQLmap的攻击载荷隐蔽式数据注入验证与分析

本文使用SQLmap工具对ICS历史数据库进行攻击，已达到对ICS数据进行操控的目的，核心为将精心制作的攻击样本对原始数据进行替换。SQLmap的工作示意如图16所示。

本文采用MySQL仿真ICS的历史数据库，原始数据内容为SWaT数据集前7天的正常样本，共包含

图 16 SQLmap的工作示意

18个连续特征。攻击向量设置为原水注入、化学投药、超滤3个阶段共9个特征的正常数据生成攻击样本。图17展示了攻击后的数据库，通过SQLmap，实现了攻击向量的注入。通过脱氯、反渗透、反冲洗3个阶段正常9个特征相结合用于增加攻击向量的隐蔽性。由于攻击向量为使用TimeGAN-LSTM算法，并基于ICS原始流量生成，在特征以及分布层面存在高覆盖率，进一步增加了隐蔽性。

3.4 注入隐蔽性测试

为进一步验证TimeGAN-LSTM生成的合成数据在语义与统计分布上对真实工业控制系统正常流量的高保真度，本文设计了一组分类实验，评估合成样本在主流ICS流量检测模型中的“可伪装性”。具体而言，选取了4种常用于网络流量分类与异常检测的监督学习算法，包括逻辑回归、随机森林、支持向量机以及决策树。模型均基于原始正常数据进行训练，随后使用合成数据进行推理，以预测其被识别为正常样本的概率。图18为攻击样本绕过能力示意。

从图18可以看出，所有分类器对合成数据均

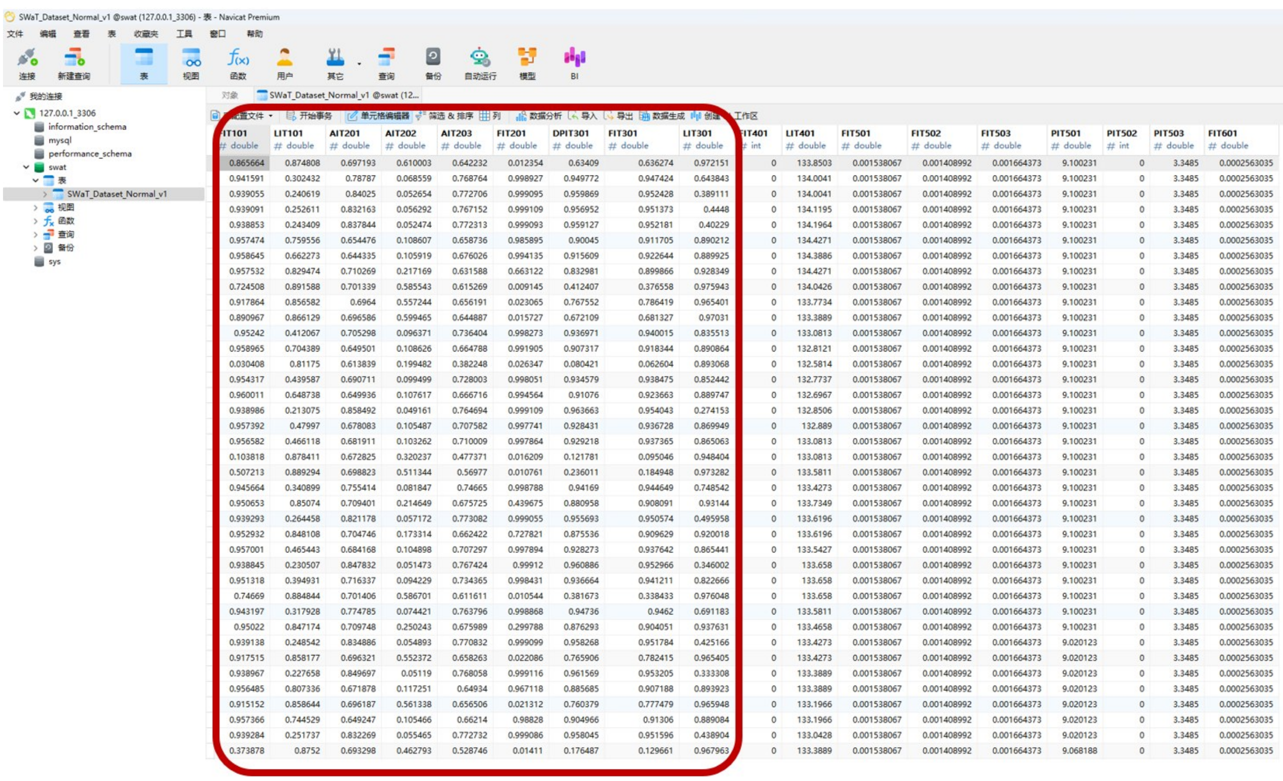


图 17 隐蔽数据注入

给出了极高的“正常”预测概率，几乎全部分布在0.999 5以上，甚至多数模型（如随机森林和SVM）输出的预测概率在1.0附近形成尖锐分布，显示出极低的模型不确定性。这一结果表明，合成数据在统计学意义上几乎无法与原始正常流量样本区分，能够成功“欺骗”这些训练于真实数据的分类器，使其判断合成样本为正常流量。尤其值得注意的是，即便在逻辑回归这种对特征线性可分性较敏感的模型下，合成数据依然表现出高置信度的“正常性”预测，进一步表明生成模型不仅捕捉了数据的非线性结构，也保留了其主要的线性判别特征。

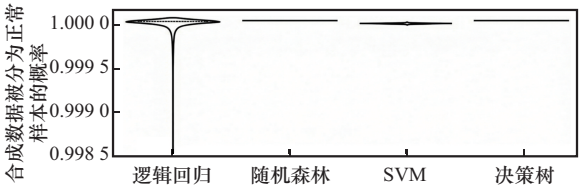


图 18　攻击样本绕过能力示意

4　对比与讨论

ICS攻击的研究中，文献[42]通过加密流量分析预测易受攻击的运行条件，进而实时编排对ICS系统的拒绝服务（DoS）攻击，从而显著放大其网络攻击的物理影响。文献[43]将远程启动或停止PLC的攻击扩展到最新的S7-1500 PLC。核心为将控制逻辑下载到远程PLC，实现了修改PLC的控制逻辑的同时保留PLC提供给工程站的源代码。文献[44]研究了一种嵌入在恶意软件中的攻击方法，能够通过恶意软件进行侦察、数据采集以及负载注入。文献[45]利用控制算法模块（例如PLC二进制逆向工程工具的比例积分微分模块）对过程的控制理论进行攻击，从而在工厂的运行范围内造成稳定或振荡偏差。本文对上述研究从攻击目标、攻击途径、协议规避能力以及数据检测规避能力4个层面进行了分析，如表4所示。

在攻击目标方面，本文研究攻击目标为PLC、工程师站以及数据库服务器，攻击面更广，抗防御能力更强。并且，本文攻击不涉及任何PLC逻辑的注入以及运行逻辑的篡改，文献[41-44]受限于PLC的内存大小，在实际的场景中的攻击能力受限。在攻击途径方面，本文的核心为对PLC与工程师站之间的通信进行攻击，用于实现本文精心制作的攻击向量对实时数据库的注入，以及对ICS的历史数据库进行注入。对协议检测的规避能力更强，具有更高的隐蔽性。在数据检测规避方面，本文定制化设计了TimeGAN-LSTM对伪造了真实的攻击数据，攻击向量的特征以及分布与ICS正常流量相符，具有高度的保真性。因此，本文相较于文献[42-45]具有较强的数据检测规避能力。

5　防御建议

本文是一种基于生成对抗网络与时序建模技术伪造正常样本以绕过检测系统，并进一步利用通信协议漏洞实施无感知攻击与历史数据篡改的高级攻击模式。在防御方面，传统基于流量签名或规则匹配的检测机制，在面对伪装为正常指令序列或合法通信行为的攻击载荷时往往失效，尤其当攻击行为通过对正常样本的深度学习建模生成，使得流量具备合法结构、合理统计特征，进一步削弱了传统异常检测的识别能力。为此，防御策略应从通信协议、物理过程一致性验证、数据完整性保障与智能行为分析4个维度协同构建纵深防御机制[46]。

在通信层，应引入协议语义解析与交互序列建模，通过构建协议状态机结合上下文行为约束，识别异常命令模式或字段组合；同时，基于控制系统动态响应模型，设计输出不可观测性分析，以判定通信控制信号是否引发了系统状态的物理响应，从而揭示潜在的伪装攻击行为。

在数据层面，针对历史数据库的注入攻击，应

表4　对比分析

文献	攻击目标	攻击途径	协议规避能力	数据检测规避能力
文献[42]	PLC	流量分析	弱	弱
文献[43]	PLC	上位机伪造	强	弱
文献[44]	PLC	恶意软件	弱	弱
文献[45]	PLC	ICS控制算法模块	弱	弱
本文	PLC+工程师站+数据库服务器	通信协议、数据库注入	强	强

强化数据写入路径的访问控制策略，引入完整性标签机制，并通过时间序列熵分析与交叉比对检测低熵、结构化异常伪数据，以防止长期潜伏与行为审计误导。此外，利用多副本存储与一致性校验机制可在写入环节前置异常数据隔离，从源头提高系统容忍性。并对工程师站、历史数据库接口与PLC通信路径实施最小权限原则与网络隔离设计，配合部署单向网闸与基于访问行为的零信任认证机制，实现访问路径的精细化控制与行为可追溯。

在智能检测方面，应引入对抗样本识别网络[47]，通过对正常与合成流量的微观特征差异进行特征学习（如频域波动性、自相关矩阵、熵变异指标等），构建基于GAN判别器结构的伪装攻击识别模型，提升对合成样本的分辨能力。

最后，在高风险接口（如历史数据库、控制指令通道）部署高交互工业蜜罐系统，可诱捕潜在攻击行为并提供溯源信息，为系统防御与响应策略优化提供关键情报。

6 结束语

针对工业通信协议、工业数据存储库等工业控制系统组件缺乏认证机制、校验机制不足等固有设计缺陷，本文设计了面向协议规避与数据操控的工业控制系统隐蔽攻击载荷生成与无感注入机制。通过TimeGAN-LSTM基于ICS正常流量生成覆盖ICS原始真实样本静态分布以及保留工业数据中的因果关联和动态演化模式的攻击样本。通过原创漏洞对ICS上位机与PLC进行的通信协议进行规避攻击，实现攻击样本对ICS实时数据库的无感注入。并利用SQLmap渗透工具，对ICS历史数据库进行数据的污染。实验结果表明，与现有工作相比，本文方案的攻击面更广、攻击途径更隐蔽，且实现了协议检测规避以及数据检测规避。后续研究将进一步评估该方案在真实工业场景下攻击的有效性，并探究相应的防御机制研究，为工控安全提供防御思路。

参考文献：

[1] 殷天野. 工业控制系统统入侵威胁与攻击模型研究[D]. 上海: 上海交通大学, 2017.
YIN T Y. Research on intrusion threats and attack models of industrial control systems[D]. Shanghai: Shanghai Jiao Tong University, 2017.

[2] 方栋梁, 刘圃卓, 秦川, 等. 工业控制系统协议安全综述[J]. 计算机研究与发展, 2022, 59(5): 978-993.
FANG D L, LIU P Z, QIN C, et al. Survey of protocol security of industrial control system[J]. Journal of Computer Research and Development, 2022, 59(5): 978-993.

[3] 韩冬松, 沙乐天, 赵创业. 基于蠕虫和代理的工控系统攻击建模[J]. 计算机与现代化, 2023(10): 107-114.
HAN D S, SHA L T, ZHAO C Y. Worm and agent-based attack modeling for industrial control systems[J]. Computer and Modernization, 2023(10): 107-114.

[4] ALAVI S A, MOGHADAM H P, JAHANGIR A H. Beyond botnets: autonomous firmware zombie attack in industrial control systems[J]. International Journal of Critical Infrastructure Protection, 2025, 48: 100729.

[5] 王航, 张帅, 杜君, 等. 工控系统认证绕过漏洞实证分析[J]. 网络空间安全, 2018, 9(3): 8-13.
WANG H, ZHANG S, DU J, et al. Analysis of industrial control system authtication bypass vulnerability[J]. Cyberspace Security, 2018, 9(3): 8-13.

[6] YAO W J, SUN Y B, WU G D, et al. AOIFF: a precise attack method for PLCs based on awareness of industrial field information[J]. IEEE Transactions on Sustainable Computing, 2025, 10(2): 232-243.

[7] HE J J, LI Y X, TANG J H, et al. An immune-knowledge-driven SCADA-based industrial virus propagation model[J]. IEEE Internet of Things Journal, 2024, 11(18): 29956-29970.

[8] 黄涛, 付安民, 季宇凯, 等. 工控协议逆向分析技术研究与挑战[J]. 计算机研究与发展, 2022, 59(5): 1015-1034.
HUANG T, FU A M, JI Y K, et al. Research and challenges on reverse analysis technology of industrial control protocol[J]. Journal of Computer Research and Development, 2022, 59(5): 1015-1034.

[9] 吕金虎, 任磊, 谭少林, 等. 工业互联网层级架构与安全: 复杂网络新视角[J]. 中国科学(技术科学), 2024, 54(10): 2042-2052.
LYU J H, REN L, TAN S L, et al. Hierarchical architecture and security of Industrial Internet: a new perspective from complex network[J]. Scientia Sinica (Technologica), 2024, 54(10): 2042-2052.

[10] 杨婷, 张嘉元, 黄在起, 等. 工业控制系统安全综述[J]. 计算机研究与发展, 2022(5): 1035-1053.
YANG T, ZHANG J Y, HUANG Z Q, et al. Summary of safety of industrial control system[J]. Journal of Computer Research and Development, 2022(5): 1035-1053.

[11] 赖英旭, 刘增辉, 蔡晓田, 等. 工业控制系统入侵检测研究综述[J]. 通信学报, 2017, 38(2): 143-156.
LAI Y X, LIU Z H, CAI X T, et al. Review on intrusion detection of industrial control system[J]. Journal on Communications, 2017, 38(2): 143-156.

[12] QIAN G Y, LI J Y, HE W, et al. An online intrusion detection method for industrial control systems based on extended belief rule base[J]. International Journal of Information Security, 2024, 23(4): 2491-2514.

[13] SAMIAH A, UMER M A, SIDDIQUI S. Decision tree based invariants for intrusion detection in industrial control system[J]. Computers & Security, 2025, 156: 104511.

[14] XU X Y, LAI Y X, ZHANG X, et al. Abnormal logical representation learning for intrusion detection in industrial control systems[J]. IEEE Transactions on Industrial Informatics, 2024, 20(8): 10624-10635.

[15] 刘奇旭, 陈艳辉, 尼杰硕, 等. 基于机器学习的工业互联网入侵检测综述[J]. 计算机研究与发展, 2022, 59(5): 994-1014.
LIU Q X, CHEN Y H, NI J S, et al. Survey on machine learning-based anomaly detection for industrial Internet[J]. Journal of Computer Research and Development, 2022, 59(5): 994-1014.

[16] 谭靖, 杨利刚, 李潇睿, 等. 深度强化学习及其在工业场景的应用与展望[J]. 工程科学学报, 2025, 47(4): 768-779.
TAN J, YANG L G, LI X R, et al. Deep reinforcement learning applications and prospects in industrial scenarios[J]. Chinese Journal of Engineering, 2025, 47(4): 768-779.

[17] YALÇıN N, ÇAKıR S, ÜNALDı S. Attack detection using artificial intelligence methods for SCADA security[J]. IEEE Internet of Things Journal, 2024, 11(24): 39550-39559.

[18] PU H Y, HE L, CHENG P, et al. CORMAND2: a deception attack against industrial robots[J]. Engineering, 2024, 32: 186-201.

[19] 赵猛猛. 面向工业控制系统的时间序列异常检测算法研究[D]. 北京: 北京邮电大学, 2025.
ZHAO M M. Research on time series abnormal detection algorithm for industrial control systems[D]. Beijing: Beijing University of Posts and Telecommunications, 2025.

[20] 沈克, 周志强, 付杨, 等. 面向石油装备制造企业的工业控制系统信息安全防护方法[J]. 信息网络安全, 2020, 20(S1): 107-110.
SHEN K, ZHOU Z Q, FU Y, et al. Information security protection method of industrial control system for petroleum equipment manufacturing enterprises[J]. Netinfo Security, 2020, 20(S1): 107-110.

[21] 尚文利, 石贺, 赵剑明, 等. 基于SAE-LSTM的工艺数据异常检测方法[J]. 电子学报, 2021, 49(8): 1561-1568.
SHANG W L, SHI H, ZHAO J M, et al. An anomaly detection method of process data based on SAE-LSTM[J]. Acta Electronica Sinica, 2021, 49(8): 1561-1568.

[22] 刘奇旭, 肖聚鑫, 谭耀康, 等. 工业互联网流量分析技术综述[J]. 通信学报, 2024, 45(8): 221-237.
LIU Q X, XIAO J X, TAN Y K, et al. Survey of industrial Internet traffic analysis technology[J]. Journal on Communications, 2024, 45(8): 221-237.

[23] YOON J, JARRETT D, VAN DER SCHAAR M. Time-series generative adversarial networks[J]. Proceedings of the 33rd International Conference on Neural Information Processing Systems. New York: ACM Press, 2019: 5508-5518.

[24] SIDDIQUE M S, KHAN M A R, AHAMMAD I, et al. An intelligent intrusion detection system for cyber-physical systems using GAN-LSTM networks[J]. Franklin Open, 2025, 11: 100281.

[25] LIAO S B, LIU C S, XIA Y X, et al. Time series anomaly detection based on GAN-VAE[J]. Data Science and Informetrics, 2024, 4(3): 126-136.

[26] CAI Z Y, DU H Y, WANG H Q, et al. One-dimensional convolutional Wasserstein generative adversarial network based intrusion detection method for industrial control systems[J]. Electronics, 2023, 12(22): 4653.

[27] DING H W, SUN Y, HUANG N N, et al. TMG-GAN: generative adversarial networks-based imbalanced learning for network intrusion detection[J]. IEEE Transactions on Information Forensics and Security, 2023, 19: 1156-1167.

[28] SCHMIDHUBER J, HOCHREITER S. Long short-term memory[J]. Neural Computation, 1997, 9(8): 1735-1780.

[29] DASH N, CHAKRAVARTY S, RATH A K, et al. An optimized LSTM-based deep learning model for anomaly network intrusion detection[J]. Scientific Reports, 2025, 15: 1554.

[30] JIANG L X. A network anomaly traffic detection method based on CNN-LSTM[J]. Security and Privacy, 2025, 8(3): e70033.

[31] DANLADI S K, SARITHA G, ANITHA ELAVARASI S, et al. A hybrid LSTM-GAN model for predictive cyber threat intelligence and anomaly detection[C]//Proceedings of the 2024 International Conference on Integrated Intelligence and Communication Systems (ICIICS). Piscataway: IEEE Press, 2024: 1-6.

[32] GITHINJI S, MAINA C W. Anomaly detection on time series sensor data using deep LSTM-autoencoder[C]//Proceedings of the 2023 IEEE AFRICON. Piscataway: IEEE Press, 2023: 1-6.

[33] OJAGBULE O, WIMMER H, HADDAD R J. Vulnerability analysis of content management systems to SQL injection using SQLMAP[C]//Proceedings of the SoutheastCon 2018. Piscataway: IEEE Press, 2018: 1-7.

[34] BITTON R, MAMAN N, SINGH I, et al. Evaluating the cybersecurity risk of real-world, machine learning production systems[J]. ACM Computing Surveys, 2023, 55(9): 1-36.

[35] SATTLER F, BÖHM S, SCHUBERT P D, et al. SEAL: integrating program analysis and repository mining[J]. ACM Transactions on Software Engineering and Methodology, 2023, 32(5): 1-34.

[36] AHMED C M, ZHOU J Y, MATHUR A P. Noise matters: using sensor and process noise fingerprint to detect stealthy cyber attacks and authenticate sensors in CPS[C]//Proceedings of the 34th Annual Computer Security Applications Conference. New York: ACM Press, 2018: 566-581.

[37] ZHANG L M, BAI W J, XIE X W, et al. TMANomaly: time-series mutual adversarial networks for industrial anomaly detection[J]. IEEE Transactions on Industrial Informatics, 2024, 20(2): 2263-2271.

[38] LIU W Q, YAN L, MA N N, et al. Unsupervised deep anomaly detection for industrial multivariate time series data[J]. Applied Sciences, 2024, 14(2): 774.

[39] KIM D, PARK S, CHOO J. When model meets new normals: test-time adaptation for unsupervised time-series anomaly detection[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2024, 38(12): 13113-13121.

[40] WU Y X, DAI B R. STL-ConvTransformer: series decomposition and convolution-infused transformer architecture in multivariate time series anomaly detection[C]//Advances in Knowledge Discovery and Data Mining. Berlin: Springer, 2024: 41-52.

[41] QIAN C, TANG W Z, WANG Y Y. RGAnomaly: Data reconstruction-based generative adversarial networks for multivariate time series anomaly detection in the Internet of Things[J]. Future Generation Computer Systems, 2025, 167: 107751.

[42] BEHDADNIA T, THOELEN K, ZOBIRI F, et al. Leveraging deep

learning to increase the success rate of DoS attacks in PMU-based automatic generation control systems[J]. IEEE Transactions on Industrial Informatics, 2024, 20(4): 6075-6088.

[43] LONGO G, LUPIA F, PUGLIESE A, et al. Physics-aware targeted attacks against maritime industrial control systems[J]. Journal of Information Security and Applications, 2024, 82: 103724.

[44] BIHAM E, BITAN S, CARMEL A, et al. Rogue7: rogue engineering-station attacks on s7 simatic PLCS[R]. 2019.

[45] SARKAR E, BENKRAOUDA H, MANIATAKOS M. I came, I saw, I hacked: Automated Generation of Process-independent Attacks for Industrial Control Systems[C]//Proceedings of the 15th ACM Asia Conference on Computer and Communications Security. New York: ACM Press, 2020: 744-758.

[46] PENG X Z, ZHENG C L, WANG Y D, et al. Double layer blockchain-assisted trusted data flow model for industrial control systems[J]. Reliability Engineering & System Safety, 2025, 260: 111013.

[47] LIU Y, OUYANG X, CUI X. GLEAM: Enhanced transferable adversarial attacks for vision-language pre-training models via global-local transformations[C]//Proceedings of the IEEE/CVF International Conference on Computer Vision. Piscataway: IEEE Press, 2025: 1665-1674.

[作者简介]

彭祥贞（1997– ），男，山东临沂人，武汉大学博士生，主要研究方向为工业控制系统安全、对抗攻击、区块链技术。

史建宇（1999– ），男，河南南阳人，武汉大学硕士生，主要研究方向为工业控制系统安全、漏洞挖掘、渗透攻击。

刘运祺（1992– ），男，河南许昌人，武汉大学博士生，主要研究方向为工业控制系统安全、渗透攻击、对抗攻击。

郑承良（1990– ），男，山东泰安人，博士，香港科技大学研究助理，主要研究方向为工业控制系统安全、去中心化AI等。

崔晓晖（1971– ），男，湖北武汉人，博士，武汉大学教授、博士生导师，主要研究方向为网络空间安全、工业控制系统安全、区块链技术等。