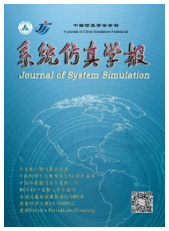

系统仿真学报
Journal of System Simulation
ISSN 1004-731X,CN 11-3092/V

《系统仿真学报》网络首发论文

题目：网络空间安全中的数字孪生技术研究
作者：任乾坤，熊鑫立，刘京菊，姚倩
DOI：10.16182/j.issn1004731x.joss.23-0853
收稿日期：2023-07-06
网络首发日期：2023-11-23
引用格式：任乾坤，熊鑫立，刘京菊，姚倩. 网络空间安全中的数字孪生技术研究[J/OL]. 系统仿真学报. https://doi.org/10.16182/j.issn1004731x.joss.23-0853

网络空间安全中的数字孪生技术研究

任乾坤[1,2]，熊鑫立[1,2]，刘京菊[1,2*]，姚倩[1,2]
（1.国防科技大学电子对抗学院，合肥 230037; 2. 网络空间安全态势感知与评估安徽省重点实验室, 合肥 230037）

摘要：网络数字孪生技术将数字孪生和网络空间建模与仿真技术相结合，通过深入研究网络数字孪生技术的内涵及其关键技术，可以更好地利用网络空间建模与仿真技术赋能网络空间安全未来的发展。概述了网络数字孪生的基础理论和研究现状，提出了网络数字孪生的分类法并对网络数字孪生的应用进行了总结，归纳出面向网络空间安全的网络数字孪生模型，论述了网络数字孪生内在安全问题与赋能网络安全技术的方法，展望了对网络数字孪生在网络空间安全领域的应用前景与挑战机遇。

关键词：数字孪生；网络空间建模与仿真；网络空间安全；网络防御；网络评估
中图分类号：TP393　　文献标志码：A
DOI: 10.16182/j.issn1004731x.joss.23-0853

Reserach on Digital Twins Technology in Cyberspace Security

Ren Qiankun[1,2], *Xiong Xinli*[1,2], *Liu Jingju*[1,2*], *Yao Qian*[1,2]

(1. College of Electronic Engineering, National University of Defense Technology, Hefei 230037, China;
2. Anhui Province Key Laboratory of Cyberspace Security Situation Awareness and Evaluation, Hefei 230037, China;)

Abstract: Combined with digital twins and cyber-space modeling and simulation, the network digital twins (NDT) technology with in-deep research can enable the development of diverse techniques of cyber security. The basic concept and research history of NDT are summarized, and a taxonomy is proposed to survey applications of NDT. A security-oriented network digital twin model (CyS-NDT) is concluded through the literature. The relationship between the internal security problem of NDT and the method of enabling network security technology is discussed to prospect further challenges and opportunities.

Keywords: digital twins; cyberspace modeling and simulation; cyberspace security; cyber defense; cyber evaluation

0　引言

随着物联网、云计算和人工智能等高新技术的飞速发展，管理和运维物理系统变得日益复杂。数字孪生技术通过将物理系统与数字模型相互映射，提供了解决管理和运维问题的新途径。在网络空间也存在复杂的网络信息系统和物理信息系统，将数字孪生技术引入网络空间可以准确映射网络拓扑，实时监测网络设备状态，提高管理和运维效率。同时，随着网络攻击呈现多元化、全球化、智能化等特点，网络空间安全面临着更加严峻的挑战。网络数字孪生作为一项新兴的技术，能够为网络提供快速的备份和恢复能力，保障了业务的连续性和安全性，在增强网络空间安全保护方面具有重要的意义。

收稿日期：2023-07-06　修回日期：2023-10-24
第一作者：任乾坤(1998-)，男，硕士研究生，研究方向为网络空间建模与仿真。E-mail：renqiankun@nudt.edu.cn
通讯作者：刘京菊(1974-)，女，博士，教授，研究方向为网络空间安全与机器学习。E-mail：jingjul@aliyun.com

数字孪生（digital twins，DT）的概念可以追溯到 2003 年美国密歇根大学教授 Michael Grieves 针对产品生命周期管理提出的镜像空间模型。此后，数字孪生逐渐成为航空、能源、医疗等领域的研究热点。随着网络数字化仿真技术的发展，数字孪生技术的研究开始迈向网络信息领域。网络数字孪生（network digital twins，NDT）作为典型的网络空间建模技术，旨在建立准确、可实时运行并具有交互反馈功能的网络空间模型。从而实现网络通信时延的降低以及网络行为的精准预测等，提升网络可用性和安全性。针对目前网络数字孪生技术发展及其在网络空间安全中的应用问题，本文的主要贡献是：

（1）根据网络数字孪生研究内容，提出了基于典型应用的分类法，对网络数字孪生技术进行了合理分类。

（2）总结了数字孪生技术在网络空间安全中的应用，归纳了网络数字孪生的基本框架：物理系统和孪生系统之间可以基于云边协同计算进行实时快速数据交互的网络模型。

（3）分析了网络数字孪生内在安全防护问题及其赋能的网络安全技术方面的应用，为数字孪生技术应用到网络空间安全领域提供了参考。

（4）分析了网络数字孪生在网络空间安全领域的新的挑战和机遇，为未来的研究发展提供了方向。

1 数字孪生概述与发展

数字孪生是以数字化方式创建物理实体的虚拟模型，借助数据模拟物理实体在现实环境中的行为，通过虚实交互反馈、数据融合分析、决策迭代优化等手段，为物理实体增加或扩展新的能力[1]。数字孪生先后历经了概念发展期、应用探索期、应用领先期、标准制定期和全域覆盖期，如图 1 所示。在概念发展期，美国国家航天局将数字孪生定义为：一种集成化了的多种物理量、多种空间尺度的系统仿真，利用物理模型、传感器数据的更新等，镜像出孪生对象的生存状态。在应用探索期，数字孪生技术快速发展，并逐渐应用到航空、医疗、能源等领域[2]。在应用领先期，数字孪生技术首次实现了对战斗机组件生命周期的预测，IBM、微软、谷歌等公司也先后进入数字孪生市场。在标准制定期，部分行业先后制定了数字孪生相关的标准，如工业领域的数字孪生 OPC 标准，各种行业白皮书的发布推动了数字孪生的标准化。在全域覆盖期，数字孪生技术逐步应用到全新领域，如：兵棋推演、网络建模、6G 设施等，为新一代网络发展和军事建设提供重要支撑。

图 1 数字孪生发展历程

2 网络数字孪生技术分析与应用

网络空间建模与仿真既是将物理实体转化为数字孪生体的核心，也是实现网络数字孪生应用需求的关键[3]。同时，网络防御技术的进步也需要网络数字孪生模型的支持，传统的故障诊断和检测评估方法无法保证新的防御措施在实际攻击中的有效性。利用网络数字孪生模型，可以模拟各种攻击场景，对新的防御策略进行测试和验证，提前发现潜在的安全问题[4]。

2.1 网络数字孪生技术概述

目前关于网络数字孪生的定义有许多种，其中 lmasan P[5]等将网络数字孪生定义为一个构建可以实时运行、数据精确驱动的网络模型，Tao F 等[6]则认为网络数字孪生是一个允许在不造成网络中断的情况下对网络进行安全分析和监控的网络模型。本文从网络空间安全的角度将网络数字孪生做出如下定义：网络数字孪生是一种与真实网络环境相互映射的、能够模拟网络安全威胁行为的物理网络数字化表征。

目前已有一些学者对网络数字孪生技术进行了研究，如 Rui Dong 等[7]基于深度学习架构设计了移动边缘计算框架，减少了物理设备在本地服务器处理的时间，实现了超高可靠性和超低延迟的网络数字孪生。Quan Yu 等[8-9]基于下一代网络体系结构提出了一种云端的网络数字孪生架构，通过云运营商为孪生网络中的实体提供服务。并在此基础上基于以云为中心的网络体系结构和无线接入网络体系结构提出了网络数字孪生的 6G 架构，并将控制基站和数据基站分离，更好的保护用户隐私，降低了网络能耗。

本文对现有网络数字孪生已有的关键技术进行了分析汇总，如表 1 所示。虽然网络数字孪生

技术在网络安全领域具有广阔的应用前景，但其发展也面临着一些挑战。首先，网络数字孪生系统的构建和维护成本较高，需要大量的技术支持和专业人才。其次，网络数字孪生系统需要实时同步物理模型和网络模型之间的状态信息，因此对数据传输速度和实时性要求较高。最后，网络数字孪生系统中保存了大量敏感数据，如何合法的使用这些数据并规范对隐私的保护也是一个重要问题。

表 1 现有网络数字孪生架构总结

技术实现方法	相关文献	主要研究	优点	缺点与不足
云计算	[9- 14] [38-40]	数据所有者从物理资产中生成数据并将其发送到云服务器，在虚拟空间中模拟数字孪生，将模拟结果与所有者共享，用户访问数据可以不受时间和地点的约束	提供按需服务、计算资源、无处不在的网络接入，拥有高性能的计算和存储服务	很难找到一种安全的方式来共享数据、存在隐私泄露问题
边缘计算	[15-23]	将数字孪生与边缘计算结合，建立一个数字孪生授权的边缘网络模型，解决了自适应边缘关联问题	减少了系统延迟，提高用户的实用性，解决了终端用户和服务器之间的不可靠、远距离通信的问题	边缘网络中接入点多且分散，边缘终端的防护能力不足，数据量大、网络不稳定等
网络切片	[24-27]	数字孪生技术通过创建支持切片的网络虚拟表示，以数字方式模拟其行为并预测时变性能，可以捕获不同切片之间的关系，并监控不同网络切片的端到端实时数据	对网络的安全状态进行分析和预测，对安全策略进行模拟、验证和优化，能够预测一些未知的安全问题	配置切片安全功能涉及到对大量网络功能和资源的管理和编排，动态管理的成本和复杂性相对较高，难以找到最佳的网络威胁解决方案
区块链	[28-31]	基于区块链的数据安全共享架构应用于数字孪生物联网系统，解决物理系统、数字孪生系统和物联网应用系统之间的数据安全传输问题	拥有一个安全且保护用户隐私的身份验证协议，允许用户验证数据的安全性	无法抵御离线密码攻击、匿名属性攻击、临时信息攻击等各种攻击行为
知识图谱	[32-34]	提出了一种基于知识图谱构建的数字孪生网络，用知识图谱描述复杂的数字孪生网络，不仅可以表示网络的物理属性，而且可以从不同的维度挖掘网络关系	增强了数字孪生内部链接和引用、知识补全、错误检测、集体推理和语义查询能力，可以基于历史数据和推理结果使用知识图谱进行决策	孪生数据之间的关系难以确立，仅仅通过知识图谱很难做到数据的全面映射，且对于数据之间的关系没有判定过程
云边协同	[35-37]	基于数字孪生的云边缘协同架构描述了数字孪生驱动下实时可视化监控和云边缘协同控制的关键技术，验证了基于数字孪生的云边协同系统的有效性	解决了设备层与云端直接通信时传输实时性差、带宽不足、安全性低的问题	仅仅考虑了单一设备使用，没有利用多个设备同时构建孪生模型，效率较低

2.2 网络数字孪生的分类

现有文献大都基于系统架构对网络数字孪生进行分类，如三维模型（物理实体、虚拟空间和连接接口）、五维模型（物理部分、虚拟部分、连接、数据和服务）、三层三域双闭环[38]（物理层、孪生层和应用层、）和四层架构（物理层、数据层、网络层和应用层，数据域、模型域和管理域，外层循环和内层循环）等。本文在网络数字孪生应用需求的基础之上分别从系统分析、系统维护和系统优化三个方面对网络数字孪生进行分类，如图 2 所示。

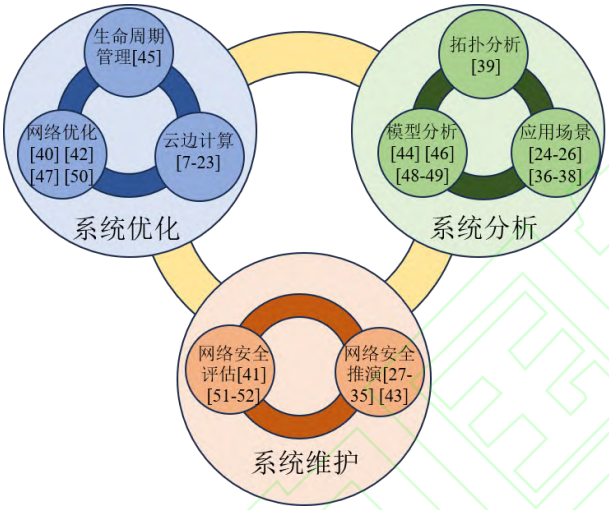

图 2 面向应用需求的网络数字孪生分类法

在网络数字孪生中，系统分析是指通过分析网络运行状态，对网络进行优化和改进的过程，主要用于拓扑优化[39]、模型分析、场景分析等方面[40]。通过综合运用基于系统分析的网络数字孪生技术，可以更好的优化网络性能。系统维护是指对系统进行即时的更新和修复等操作，用于解决网络安全问题，提高可靠性和安全性，防止网络攻击和信息泄露。基于系统维护的网络数字孪生技术主要包括两类：网络安全评估[41]和网络安全推演。系统优化是指通过设计和实施一系列改进措施，提升系统性能和效率的过程。在网络数字孪生中，系统优化的主要目的是解决网络传输速度和稳定性等问题，主要包括网络优化[42]、生命周期管理和云边计算服务等[43]。

2.3 网络数字孪生的应用

网络在应对日益增长的数据流量和用户需求等方面面临着数据计算成本高、物理系统维护困难和网络状态配置不安全的问题。通过合理的利用网络数字孪生技术，建立虚拟仿真模型，可以对网络的运行特点、演化规律和风险隐患等进行更加精确和全面的分析[44]。因此网络数字孪生被广泛应用于动态网络管理和控制、网络故障预测与诊断、网络无损检测等方面，为突破制约网络技术发展的瓶颈提供了有效的解决方案。

2.3.1 网络动态管理与控制

通过网络数字孪生，能够控制孪生系统和物理系统保持同步变化，实现网络动态管理和控制，可用于网络系统优化和维护。其实现过程依赖于网络数字孪生的高精度网络以及数据实时反馈等技术[45]。网络数字孪生以当前网络状态和流量等作为输入，以预测结果作为输出，目标是获取最佳的网络性能。网络数字孪生中优化后的参数可以直接使用在物理网络中，并可与物理网络中采集的数据进行比对验证孪生数据的正确性。当孪生网络检测到数据不一致时，会将更新后的数据反馈给物理网络，物理网络会及时更新当前数据，通过物理网络和孪生网络之间的数据闭环交互动态地实现了网络管理和控制。

2.3.2 网络故障预测与诊断

网络故障预测和诊断能够基于目前物理网络所处的状态推演出将来可能出现的故障，并给出解决方案。为了防止网络发生大规模故障，Tzanis N 等[50]提出一种数字孪生混合体系结构对智能电网进行实时故障诊断，旨在处理由智能电表生成的大规模连续数据流中的信息，辨识即将发生故障的网络位置。

Centomo S 等[51]通过收集网络数据，并使用机器学习算法进行分析和预测网络可能存在的故障，孪生网络根据预测结果对参数进行更新并下发到物理网络中，避免物理网络发生故障，从而可以节约大量纠错时间。利用网络数字孪生进行网络故障预测和诊断的方法可以比传统方法更快、更准确地定位网络故障，为网络提供最佳的快速恢复解决方案。

2.3.3网络无损检测与评估

网络数字孪生技术将物理网络映射至虚拟网络中，能够在不中断网络运行和不改变当前网络状态的条件下进行网络检测和评估[52]。将机器学习等技术融入到网络数字孪生中是构建无损检测与评估的关键方法。通过使用真实网络数据训练模型，可以提高模型准确性，并在网络数字孪生中对大量的网络数据进行分析和处理，自动发现网络运行问题，提前预警并采取相应的措施，在不改变网络运行状态的条件下更加精确地检测和评估网络状态。通过无损检测与评估，可以及时发现潜在网络安全问题，优化网络结构，提高可靠性和安全性。

3 面向网络空间安全的数字孪生

随着网络规模的不断扩大以及层出不穷的各种安全威胁，在网络空间安全中利用数字孪生的需求越来越大。数字孪生在网络安全中的应用是基于实体网络环境构建一个网络数字孪生模型来模拟网络拓扑、数据流量、漏洞利用等，使安全人员能够提前预测潜在的网络安全威胁，并采取相应的预防措施和应对策略[53]。数字孪生技术与网络安全结合起来有很大的优势，如复现更真实的网络攻击情景、模拟潜在的网络安全威胁、降低网络安全实验的成本和风险、对验证各类设备的性能和可靠性等。其主要应用领域如图 3 所示。

图 3 网络数字孪生应用领域

3.1 面向网络空间安全的网络数字孪生模型

根据网络数字孪生对物理网络实时映射的特点，基于现有文献所提的各类模型，本文归纳了面向网络空间安全的网络数字孪生模型（CyS-NDT），该模型主要由两大系统和两大模块组成，两大系统包括物理系统和孪生系统，两大模块包括攻击模拟模块和防御制定模块，如图 4 所示。其中物理系统接收来自物理网络的数据，用户对物理数据进行筛选并通过虚实交互接口映射至孪生系统。孪生系统根据接收到的物理系统的数据，经过决策中心处理后将结果再次反馈至物理系统。物理系统再根据反馈及时更新自身网络配置，并将更新后的数据重新映射到孪生系统，直至达到最优网络配置[5]。

同时为了降低外部恶意攻击对物理系统造成的风险，在 CyS-NDT 中引入了攻击模拟模块和防御制定模块。攻击模拟模块能够模拟大多数攻击行为，首先将攻击行为依次发送给孪生系统，孪生系统接收到来自外部的攻击信号时，将攻击信息发送至决策中心。决策中心根据接收到的攻击信息，并结合云计算和边缘计算等方法，制定相应的防御策略，包括网络配置调整、网络流量过滤、入侵检测系统更新等。其次决策中心会将制定的决策结果反馈给防御制定模块，该模块负责制定防御措施并将新配置下发至物理系统，物理系统根据孪生系统的数据及时更新自身的网络配置。

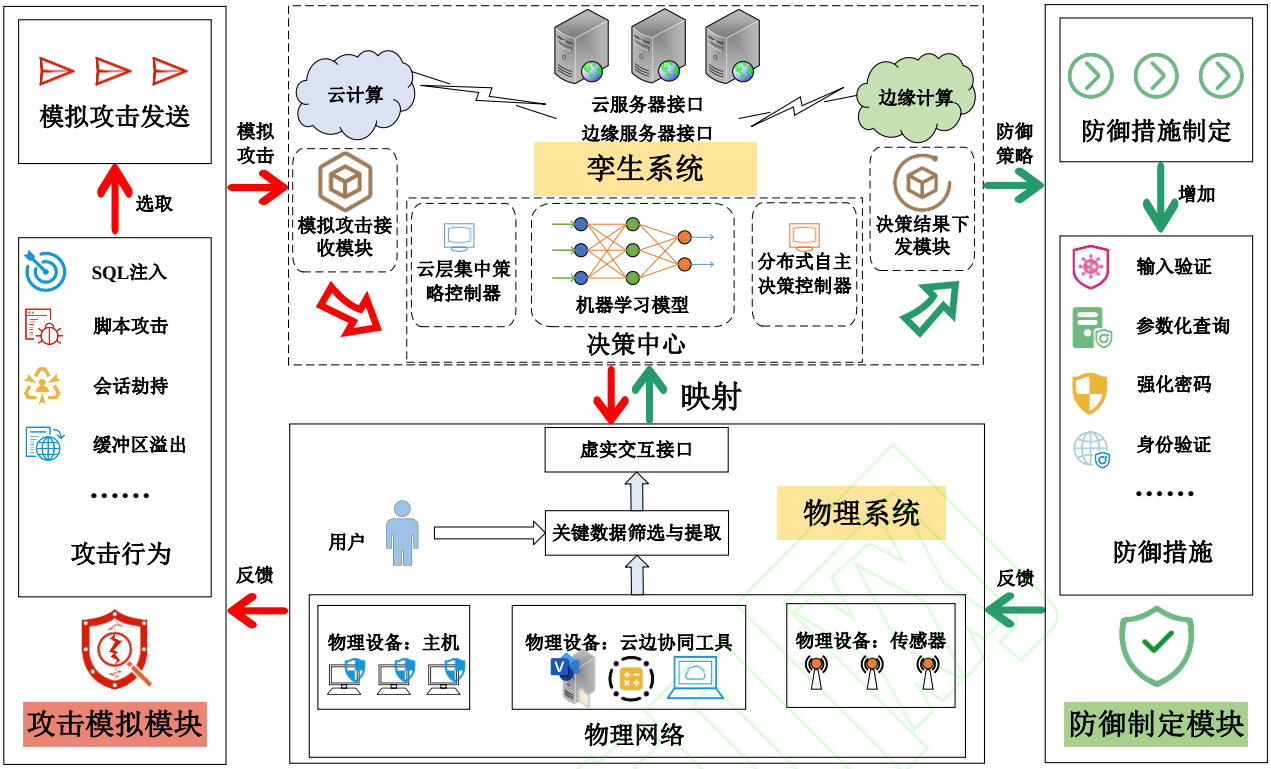

图 4 面向网络空间安全的网络数字孪生模型

3.1.1 物理系统

物理系统是构建网络数字孪生模型的实体基础，包含物理设备、关键数据筛选与提取、用户、虚实交互接口等关键组件。

物理设备在物理系统重扮演着重要角色，包括主机、网络设备、传感器等，它们收集并传输关于网络状态、设备运行情况以及环境数据等信息[45]。

关键数据筛选与提取是在物理系统中进行的重要步骤，用于提取与网络状态描述相关的关键数据。通过对物理系统产生的原始数据进行分析，并根据用户的需求和场景要求进行筛选，选取具有代表性的网络配置数据。

用户在物理系统中起着决策和控制的作用。根据不同的场景需求和目标，用户可以选择合适的数据映射至孪生系统。这些数据可以包括实时的网络状态信息、设备指标、传感器数据等。通过将数据提供给孪生系统，用户能够获得对网络性能、安全风险等方面的深入理解，并基于孪生系统提供的分析结果，进行决策制定和优化调整。

虚实交互接口是实现物理系统与孪生系统之间相互通信和数据交换关键组件。通过虚实交互接口，物理系统可以将经过筛选和提取的数据上传至孪生系统，以便进行建模、分析和优化。同时，孪生系统也可以将决策结果和优化策略反馈给物理系统，用于优化物理系统的运行。

3.1.2 孪生系统

孪生系统是实现网络数字孪生模型的重要基础，包含决策中心、云计算与边缘计算服务、模拟攻击接收模块和决策结果下发模块等关键组件。

决策中心在孪生系统中扮演着核心角色，它基于物理系统输入的网络配置、网络拓扑、网络路由以及调度策略等网络状态信息，利用机器学习算法进行建模和分析[54]。

云计算与边缘计算等技术为孪生系统提供了强大的计算和存储能力。通过接入云服务器和边缘服务器，孪生系统可以充分利用分布式计算资

源，提高对物理系统数据的处理速度，更好地满足实时监测、建模和分析的需求[13]。

通过引入模拟攻击接收模块和决策结果下发模块，并将其融入到孪生系统的迭代循环中，CyS-NDT 能够实现网络的动态更新和自我优化。在每一轮迭代结束后，物理系统会及时更新网络配置方案，并将更新后的数据重新映射至孪生系统，以实现更优的网络配置。

3.1.3攻击模拟模块

攻击模拟模块扮演着模拟物理系统网络安全威胁的关键角色，可模拟如 SQL 注入、脚本攻击、会话劫持、缓冲区溢出等多种攻击行为，可用于评估现有网络的脆弱性和防御机制的有效性[55]。各种攻击行为被输入到孪生系统中，以模拟实际网络环境中的攻击情况，同时可以评估网络系统在面临各种攻击时的表现，并寻找潜在的安全漏洞。当孪生系统接收到外部攻击信息时，会将攻击信息发送至决策中心。决策中心通过分析攻击模拟模块接收到的攻击数据，并结合预定义的策略和规则，制定出最佳的应对措施，并发送至防御措施制定模块。

3.1.4防御制定模块

防御制定模块接收来自孪生系统中的策略，根据防御策略制定相应的防御措施，如输入验证、参数化查询、强化密码、身份验证等，同时将防御措施下发至物理系统，物理系统接收到信息后及时更新自身的网络配置，并将防御措施反馈至攻击模拟模块，攻击模拟模块开始新一轮的攻击行为。通过进行循环地测试和评估用于优化防御措施的有效性，提高网络系统的安全性[56]。

3.2 网络数字孪生内在安全防护问题

CyS-NDT 在构建和使用过程中涉及到大量真实系统的关键技术和敏感数据，并且攻击者可以通过对 CyS-NDT 的攻击获取这些技术和数据，因此构建一个安全的 CyS-NDT 至关重要。为了保障 CyS-NDT 的安全性，需要加强访问控制、数据保护、安全通信等方面的措施。在访问控制方面，CyS-NDT 采用身份认证、网络隔离等方式来防止未经授权的访问，确保只有经过授权的用户才能访问和操作网络数字孪生系统；在数据保护方面，CyS-NDT 使用身份认证等方式来保护数据的安全性。确保关键技术和敏感数据的完整性、真实性和机密性，防止数据被篡改或未经授权的访问，从而增强 CyS-NDT 系统的安全性；在安全通信方面，CyS-NDT 使用安全的通信协议如非对称加密技术保护数据传输，以防止中间人攻击和数据篡改。CyS-NDT 还强化网络防火墙规则，限制对系统的未授权访问，设置安全策略和访问规则以保护系统免受来自外部网络的攻击。

3.2.1访问控制

访问控制是一种基础的安全机制，通过限制用户与资源之间的访问，确保只有授权的用户能够访问和操作 CyS-NDT。目前的数字孪生框架不允许安全的数据共享，为了弥合这一差距，Holmes D 等提出了一个框架，在 DT 数据共享中通过引入了身份认证机制来保护数据的传输安全。身份认证是访问控制的核心，使用密码、生物特征识别、双因素认证等方式，确保只有经过身份验证的用户才能够登录和使用网络数字孪生系统。这防止了未经授权的用户或攻击者获得访问权限，从而降低了系统被入侵的风险。此外网络隔离也是提升访问控制的重要措施之一，通过将 CyS-NDT 与其他网络环境隔离开来，比如使用虚拟专用网络或网络分割技术，可以减少攻击者的攻击面。这样可以降低潜在的安全漏洞和风险，确保 CyS-NDT 不受未经授权的访问和攻击。

3.2.2数据保护

CyS-NDT 通过运用高效的数据加密与保护技术，确保了数据的完整性与安全性，避免数据被干扰或破坏，影响 Cys-NDT 的正常运行。Hearn

等[58]提出任何将被共享的数字孪生都应该被加密并免受第三方的侵害，以解决通过中间人利用供应链进行攻击的问题。通过使用各种类型的数据保护技术和加固的 API，将软件和数据锁定到特定的设备，使软件不可操作或使数据只能在一台机器上访问，从而防止不同设备之间的数据的传播。Saif E 等[59]和 Dietz M 等[60]指出身份验证和完整性是保护数字孪生系统免受数据篡改和攻击等潜在风险的基本安全措施。

3.2.3安全通信

使用加密协议和安全通信通道是保护 CyS-NDT 数据在传输过程中安全性的重要手段。可以有效防止数据在传输过程中被窃取、篡改或伪造，确保数据的机密性、完整性和真实性。当数据从源到目标进行传输时，通过加密协议对数据进行加密，并确保只有授权的接收方能够解密数据。同时，安全通信通道将提供身份认证机制，确保通信双方的真实性和合法性，防止恶意第三方冒充身份进行攻击。并且，安全通信通道还将提供数据完整性验证，以检测数据是否被篡改或伪造。此外，为了保证数据传输的安全性，Jun Liu 等[61]还提出了一种采用非对称加密的数据传输安全方案，同时减少了数据加解密的时间消耗。

3.3 网络数字孪生赋能的网络安全技术

网络数字孪生技术在赋能网络安全技术方面可以发挥关键作用，Suhail S 等[62]指出首先可以通过威胁建模与仿真能够模拟各种网络威胁，帮助安全团队识别系统的薄弱点，进而制定更有效的防护策略。其次，网络数字孪生技术还可用于漏洞分析与修复，在不影响系统正常运行的情况下及时发现潜在漏洞，有助于提高系统的整体安全性。最后，还能够实时监测系统的网络流量和行为，一旦检测到异常行为或潜在威胁，能够立即触发警报并采取必要的防御措施，以降低潜在风险，保护系统免受恶意攻击和漏洞利用的威胁。

3.3.1威胁建模与仿真

在网络空间威胁建模与仿真领域，网络靶场作为一种用于模拟真实网络环境的安全测试平台发挥了重要作用。但传统的网络靶场仿真能力有限，将网络数字孪生技术应用于现有的网络靶场，可以增强其仿真能力和实用性[56]。

传统网络靶场建设的成本高、数据处理复杂，很难在短时间内将其部署到实际系统中。为了解决这些问题，利用数字孪生技术从传统网络靶场中提取关键数据[63]，可以模拟实际系统中的网络威胁，如漏洞利用和拒绝服务攻击等等，并能够在短时间内进行大规模的实验和测试。通过 CyS-NDT，安全团队可以进一步分析不同类型的威胁，更好地了解攻击者的意图和手法，能够更准确地评估系统的风险，识别潜在的攻击路径，并优化安全策略，更好地保护系统安全。

3.3.2漏洞分析与修复

网络数字孪生技术也可以用于漏洞分析与修复，及时发现和修复潜在漏洞对于保护实际系统的安全至关重要[64]。一旦发现潜在漏洞，CyS-NDT 可以通过脆弱性分析来评估漏洞的潜在威胁，通过与自动化脚本工具的集成，可以帮助系统管理员快速部署修复措施，减少漏洞被滥用的时间窗口。CyS-NDT 的漏洞分析与修复功能不仅有助于及时发现和解决漏洞，还支持组织建立坚固的网络安全基础，确保实际系统的安全性和可靠性。这种综合的方法对于保护敏感数据、维护业务连续性以及防范恶意攻击至关重要。

3.3.3实时监测与响应

网络数字孪生可以直接融入实际系统中，实时监测网络流量和系统行为，能够实时监测系统中的异常情况和潜在威胁[65-66]。一旦 CyS-NDT 探测到异常或潜在威胁，它可以自动触发警报或执行事先设定的防御措施，以减轻潜在风险，保障系统的安全。通过实时监测和快速响应，CyS-

NDT 为系统安全提供了强大的保障，使其能够迅速识别和应对潜在威胁。不仅确保了系统的稳定运行，还维护了重要数据的安全。CyS-NDT 提供了一种高效的安全防护机制，可以应对不断变化的网络安全挑战。

4 网络数字孪生的挑战与机遇

4.1 存在的挑战

由于网络数字孪生刚刚起步，将其应用在实际场景中仍面临一些不可避免的挑战，解决这些挑战可进一步推动网络数字孪生系统的深入发展、充分利用和广泛部署。

数据的高效与安全同步：在孪生数据的高效采集和安全同步方面面临着多重挑战。首先，数据来源众多，涵盖了各种不同类型的信息，包括不同的设备、传感器和应用系统。其次，这些数据往往使用不同的数据格式和通信协议，这导致了数据的异构性。最后，孪生系统和物理系统之间的数据同步要求采用高速、可靠和安全的数据传输技术。

资源管理与安全利用：在网络数字孪生系统中，资源管理和安全利用是至关重要的，由于物理网络的动态性，网络中的流量、应用程序、资源利用率和拓扑结构不断变化此外不同的网络用户可能具有不同的行为模式，使网络资源使用情况难以预测。同时由于网络的开放性和复杂性，以及网络用户的行为模式和意图难以控制，对于系统中的潜在漏洞和威胁难以发现，无法做到安全的利用网络资源。

4.2 未来的机遇

网络数字孪生模型提供了物理模型的虚拟表示，加快了数据交互速率，根据当前研究进展，接下来值得关注的研究方向有：网络数字孪生内在安全增强与基于网络数字孪生的网络防御等。

4.2.1网络数字孪生内在安全增强

网络数字孪生通过模拟网络设备、通信流量、应用程序和用户行为对网络进行管理、监控和安全评估。将数据隔离与虚拟网络拓扑、孪生日志审计和行为分析、孪生数据加密技术等经典的安全技术与网络数字孪生结合起来可以进一步增强网络的安全性，提高对潜在威胁的防御能力。

在数据隔离与虚拟网络拓扑方面，在孪生网络中创建多个虚拟网络拓扑，将不同的网络区域隔离开来，每个网络拓扑都有特定的数据隔离策略，以确保敏感数据不会跨越虚拟边界传播，可以防止横向移动攻击。在孪生日志审计和行为分析方面，孪生网络通过使用孪生日志来监控孪生网络的状态，模拟物理网络的日志信息，并使用行为分析技术来检测异常行为，可以实时监控孪生网络中潜在的安全问题。在孪生数据加密技术方面，由于网络数字孪生中会涉及大量的数据传输和存储，将虚拟化加密技术与之结合可以快速加密和解密孪生网络中的数据，确保数据在传输和存储过程中的安全性。

将经典的安全技术与网络数字孪生进行集成，可以更好地评估和应对网络威胁，提高网络数字孪生系统的整体安全性。

4.2.2基于网络数字孪生的网络防御

除了其自身的安全性之外，网络数字孪生在网络防御方面的能力也是未来的主要研究方向，如增强系统的响应能力、防御评估与演练、智能化防御、威胁情报分析和共享等。

在增强系统的响应能力方面，通过建立快速响应机制，如采用智能化的威胁检测和分析技术，以及自主学习的能力识别和拦截恶意活动，并迅速采取防御措施。在防御评估与演练方面，网络数字孪生系统通过模拟各种攻击场景，对系统的脆弱性进行评估，并验证系统修复效果。在智能化防御方面，引入人工智能和机器学习等技术，通过分析网络攻击的模式和行为，能够自动学习并改进防御策略，以适应不断变化的攻击方式，

增强自身的智能化防御能力。在威胁情报分析和共享方面，将网络数字孪生系统与外部的威胁情报源建立连接，强化威胁情报的收集、分析和共享机制，有助于快速识别和应对新的攻击手法，提高系统的安全性。

5 结束语

本文通过对现有网络数字孪生文章的总结，首先对网络数字孪生的应用进行了分析，主要讨论了数字孪生技术应用，如动态网络管理和控制、网络故障预测与诊断和网络无损检测；其次，介绍了网络数字孪生的基础理论，提出了基于系统分析、系统维护和系统优化的网络数字孪生的分类法；接着，归纳了面向安全的网络数字孪生模型（CyS-NDT），并分析了数字孪生技术在网络空间安全中的应用，从访问控制、数据保护和安全通信层面对网络数字孪生内在安全防护问题进行了详细阐述，又在威胁建模与仿真、漏洞分析与修复、实时监测与响应三个方面对网络数字孪生赋能网络安全技术的方法进行了探讨；最后指出了网络数字孪生存在的现实挑战和发展机遇。。

目前作者团队正在进行网络空间智能化对抗技术研究，旨在利用网络数字孪生技术构建智能化、精确化的网络虚拟环境，用于智能化对抗技术的训练、测试和验证。数字孪生作为一项新兴技术，其对网络空间建模的优势不断显现。未来，数字孪生技术将在网络架构设计、安全稳定运行和高效管理中发挥更加重要的作用，随着数字孪生技术的不断发展和完善，将进一步提升网络空间的安全性。

参考文献

[1] 陶飞,刘蔚然,刘检华等.数字孪生及其应用探索[J].计算机集成制造系统,2018,24(1):1-18.
Tao Fei, LIU Weiran, LIU Jianhua et al. Digital Twin and Its Application[J]. Computer Integrated Manufacturing Systems,2018,24(1):1-18.

[2] Bot ń-Sanabria D M, Mihaita A S, Peimbert-Garc á R E, et al. Digital twin technology challenges and applications: A comprehensive review[J]. Remote Sensing, 2022, 14(6): 1335.

[3] D. Chen, H. Yang, C. Zhou, L. Lu, P. L ü and T. Sun, "Classification, Building and Orchestration Management of Digital Twin Network Models," 2022 IEEE 22nd International Conference on Communication Technology (ICCT), 2022:1843-1846.

[4] Pirbhulal S, Abie H, Shukla A. Towards a novel framework for reinforcing cybersecurity using digital twins in IoT-based healthcare applications[C].2022 IEEE 95th Vehicular Technology Conference:(VTC2022-Spring). IEEE, 2022: 1-5.

[5] lmasan P, Ferriol-Galm és M, Paillisse J, et al. Network Digital Twin: Context, Enabling Technologies, and Opportunities[J]. IEEE Communications Magazine, 2022, 60(11): 22-27.

[6] Tao F, Zhang H, Liu A, et al. Digital twin in industry: State-of-the-art[J]. IEEE Transactions on industrial informatics, 2018, 15(4): 2405-2415.

[7] Dong R, She C, Hardjawana W, et al. Deep learning for hybrid 5G services in mobile edge computing systems: Learn from a digital twin[J]. IEEE Transactions on Wireless Communications, 2019, 18(10): 4692-4707.

[8] Yu Q, Ren J, Fu Y, et al. Cybertwin: An origin of next generation network architecture[J]. IEEE Wireless Communications, 2019, 26(6): 111-117.

[9] Yu Q, Ren J, Zhou H, et al. A cybertwin based network architecture for 6G[C].2020 2nd 6G Wireless Summit (6G SUMMIT). IEEE, 2020: 1-5.

[10] Thakur G, Kumar P, Deepika ., Jangirala S, Das AK, Park Y. An Effective Privacy-Preserving Blockchain-Assisted Security Protocol for Cloud-Based Digital Twin Environment. IEEE Acces. 2023;11:26877-26892.

[11] Wang H, Jin G. Digital Twin Model Construction and Management Method of Workshop Based on Cloud Platform[C].2022 11th International Conference of Information and Communication Technology (ICTech). IEEE, 2022: 28-32.

[12] Durgin G D, Varner M A, Patwari N, et al. Digital Spectrum Twinning for Next-Generation Spectrum Management and Metering[A]. 2022 IEEE 2nd International Conference on Digital Twins and Parallel Intelligence (DTPI).IEEE. 2022: 1–6.

[13] Alam K M, El Saddik A. C2PS: A digital twin architecture reference model for the cloud-based cyber-physical systems[J]. IEEE Access, 2017, 5: 2050-2062.

[14] Zhang G, MacCarthy B L, Ivanov D. The cloud, platforms, and digital twins—Enablers of the digital supply chain[M],The Digital Supply Chain. Elsevier, 2022: 77-91.

[15] Lu Y, Huang X, Zhang K, et al. Communication-efficient federated learning and permissioned blockchain for digital twin edge networks[J]. IEEE Internet of Things Journal, 2020, 8(4): 2276-2288.

[16] Lu, Y., S. Maharjan, and Y. Zhang. Adaptive Edge Association for Wireless Digital Twin Networks in 6G[J]. IEEE Internet of Things Journal,2021,8(22): 16219–30.

[17] Sun Y, Xu X, Qiang R, et al. Research on security management and control of power grid digital twin based on edge computing[C].2021 2nd International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT). IEEE, 2021: 606-610.

[18] Lu Y, Huang X, Zhang K, et al. Communication-efficient federated learning and permissioned blockchain for digital twin edge networks[J]. IEEE Internet of Things Journal, 2020, 8(4): 2276-2288.

[19] Tang F, Chen X, Rodrigues T K, et al. Survey on digital twin edge networks (DITEN) toward 6G[J]. IEEE Open Journal of the Communications Society, 2022, 3: 1360-1381.

[20] Zhang Z, Zhou, and H, Zhao L, et al. Digital Twin Assisted Computation Offloading and Service Caching in Mobile Edge Computing[C].2022 IEEE 42nd International Conference on Distributed Computing Systems (ICDCS). IEEE, 2022: 1296-1297.

[21] Zhang K, Cao J, Maharjan S, et al. Digital twin empowered content caching in social-aware vehicular edge networks[J]. IEEE Transactions on Computational Social Systems, 2021, 9(1): 239-251.

[22] Lu Y, Huang X, Zhang K, et al. Low-latency federated learning and blockchain for edge association in digital twin empowered 6G networks[J]. IEEE Transactions on Industrial Informatics, 2020, 17(7): 5098-5107.

[23] Xu X, Shen B, Ding S, et al. Service offloading with deep Q-network for digital twins-empowered internet of vehicles in edge computing[J]. IEEE Transactions on Industrial Informatics, 2020, 18(2): 1414-1423.

[24] Naeem F, Kaddoum G, Tariq M. Digital twin-empowered network slicing in B5G networks: Experience-driven approach[C].2021 IEEE Globecom Workshops (GC Wkshps). IEEE, 2021: 1-5.

[25] Granelli F, Capraro R, Lorandi M, et al. Evaluating a digital twin of an IoT resource slice: An emulation study using the ELIoT platform[J]. IEEE Networking Letters, 2021, 3(3): 147-151.

[26] H. Yang, Y. Li, K. Yao, T. Sun and C. Zhou, "A Systematic Network Traffic Emulation Framework for Digital Twin Network," 2021 IEEE 1st International Conference on Digital Twins and Parallel Intelligence (DTPI), Beijing, China, 2021, pp. 94-97.

[27] Wang H, Wu Y, Min G, et al. A graph neural network-based digital twin for network slicing management[J]. IEEE Transactions on Industrial Informatics, 2020, 18(2): 1367-1376.

[28] Zheng Q, Wang J, Shen Y, et al. Blockchain based trustworthy digital twin in the internet of things[C].2022 International Conference on Information Processing and Network Provisioning (ICIPNP). IEEE, 2022: 152-155.

[29] Pittaras I, Polyzos G C. Secure and Efficient Web of Things Digital Twins using Permissioned Blockchains[C].2022 7th International Conference on Smart and Sustainable Technologies (SpliTech). IEEE, 2022: 1-5.

[30] Dong W, Yang B, Wang K, et al. A dual blockchain framework to enhance data trustworthiness in digital twin network[C].2021 IEEE 1st International Conference on Digital Twins and Parallel Intelligence (DTPI). IEEE, 2021: 144-147.

[31] Takahashi K, Kanai K, Nakazato H. Performance Evaluation of Blockchains Towards Sharing of Digital Twins[C].2022 IEEE 4th Global Conference on Life Sciences and Technologies (LifeTech). IEEE, 2022: 128-129.

[32] Lv Z, Lou R. Edge-Fog-Cloud Secure Storage with Deep-Learning-Assisted Digital Twins[J]. IEEE Internet of Things Magazine, 2022, 5(2): 36-40.

[33] Chang X, Yang C, Wang H, et al. KID: Knowledge Graph-Enabled Intent-Driven Network with Digital Twin[C].2022 27th Asia Pacific Conference on Communications (APCC). IEEE, 2022: 272-277.

[34] Braun D, Müller T, Sahlab N, et al. A graph-based knowledge representation and pattern mining supporting the Digital Twin creation of existing manufacturing systems[C]. 2022 IEEE 27th International Conference on Emerging Technologies and Factory Automation (ETFA). IEEE, 2022: 1-4.

[35] Guo L, Cheng Y, Zhang Y, et al. Development of cloud-edge collaborative digital twin system for FDM additive manufacturing[C].2021 IEEE 19th International Conference on Industrial Informatics (INDIN). IEEE, 2021: 1-6.

[36] Xue Y, Shen Y, Duan H, et al. Digital twin system for transformer station based on cloud-edge collaboration architecture[C].2022 International Conference on Information Processing and Network Provisioning (ICIPNP). IEEE, 2022: 111-115.

[37] Lai G, Zhang X, Lu C, et al. The architecture and key technologies of the digital twin system of helicopter based on cloud-edge-end integration[C].2022 4th International Conference on Intelligent Control, Measurement and Signal Processing (ICMSP). IEEE, 2022: 1069-1072.

[38] Tao S, Cheng Z, Xiao-Dong D, et al. Digital twin network (DTN): concepts architecture and key technologies[J]. Acta Automatica Sinica, 2021, 47(3): 569-582.

[39] Y. Zhu, D. Chen, C. Zhou, L. Lu and X. Duan, "A knowledge graph based construction method for Digital Twin Network," 2021 IEEE 1st International Conference on Digital Twins and Parallel Intelligence (DTPI), Beijing, China, 2021, pp. 362-365.

[40] 杨俊皓. 大规模数字孪生网络拓扑快速构建方法研究[D].电子科技大学,2022.
Yang Junhao. Research on Rapid Construction Method of large-scale Digital twin network topology [D]. University of Electronic Science and Technology of China,2022.

[41] 贝太周,施冬明,李方舟,陈博,袁月.基于数字孪生的智能网络安全评估方案研究[J].山东电力技术,2022,49(6):25-30+80.
Bei Taizhou, Shi Dongming, Li Fangzhou, Chen Bo, Yuan Yue. Research on Intelligent Power Grid Security Assessment Scheme Based on Digital Twin[J]. Shandong Electric Power Technology, 2022, 49(6): 25-30+80.

[42] 王奇奇,莫皓颖,户江民等.基于数字孪生的网络优化方法研究[J].电声技术,2021,45(1):52-54.

Wang Qiqi, Mo Haoying, Hu Jiangmin, et al. Research on Network Optimization Method Based on Digital Twin[J]. Audio Engineering, 2021, 45(1): 52-54.

[43] 李欣,刘秀,万欣欣.数字孪生应用及安全发展综述[J].系统仿真学报,2019,31(3):385-392.
Li Xin, Liu Xiu, Wan Xinxin. An Overview of Application and Secure Development of Digital Twin[J]. Journal of System Simulation, 2019, 31(3):385-392.

[44] 张霖,陆涵.从建模仿真看数字孪生[J].系统仿真学报,2021,33(5):995-1007.
Zhang Lin, Lu Han. A View on Digital Twin from the Perspective of Modeling and Simulation[J]. Journal of System Simulation, 2021, 33(5):995-1007.

[45] Shu M, sun, zhang, et al. Digital-twin-enabled 6G network autonomy and generative intelligence: Architecture, technologies and applications[J]. Digital Twin, 2022, 2: 16.

[46] H. Yang, Y. Li, K. Yao, T. Sun and C. Zhou, "A Systematic Network Traffic Emulation Framework for Digital Twin Network," 2021 IEEE 1st International Conference on Digital Twins and Parallel Intelligence (DTPI), Beijing, China, 2021, pp. 94-97.

[47] Z. Zhao et al., "Design of a Digital Twin for Spacecraft Network System," 2022 IEEE 5th International Conference on Electronics and Communication Engineering (ICECE), Xi'an, China, 2022, pp. 46-50.

[48] M. Polverini, F. G. Lavacca, J. Galán-Jiménez, D. Aureli, A. Cianfrani and M. Listanti, "Digital Twin Manager: A Novel Framework to Handle Conflicting Network Applications," 2022 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Phoenix, AZ, USA, 2022, pp. 85-88.

[49] Z. Wei, S. Wang, D. Li, F. Gui and S. Hong, "Data-Driven Routing: A Typical Application of Digital Twin Network," 2021 IEEE 1st International Conference on Digital Twins and Parallel Intelligence (DTPI), Beijing, China, 2021, pp. 1-4.

[50] N. Tzanis, N. Andriopoulos, A. Magklaras, E. Mylonas, M. Birbas and A. Birbas, "A Hybrid Cyber Physical Digital Twin Approach for Smart Grid Fault Prediction," 2020 IEEE Conference on Industrial Cyberphysical Systems (ICPS), Tampere, Finland, 2020, pp. 393-397.

[51] Centomo S, Dall'Ora N, Fummi F. The design of a digital-twin for predictive maintenance[C],2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA). IEEE, 2020, 1: 1781-1788.

[52] Bagrodia R. Using network digital twins to improve cyber resilience of missions[J]. The Journal of Defense Modeling and Simulation, 2023, 20(1): 97-106.

[53] Pokhrel A, Katta V, Colomo-Palacios R. Digital twin for cybersecurity incident prediction: A multivocal literature review[C],Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops. 2020: 671-678.

[54] M. Van Den Brand, L. Cleophas, R. Gunasekaran, B. Haverkort, D. A. M. Negrin and H. M. Muctadir, "Models Meet Data: Challenges to Create Virtual Entities for Digital Twins," 2021 ACM/IEEE International Conference on Model Driven Engineering Languages and Systems Companion (MODELS-C), Fukuoka, Japan, 2021, pp. 225-228.

[55] 马宇威,杜海涛,粟栗等.基于数字孪生的 5G 网络安全推演[J/OL].计算机工程与应用,2023:1-10.
Ma Yuwei, Du Haitao, Su Li et al. 5G Network security Inference based on Digital twin [J/OL]. Computer Engineering and Applications,2023:1-10.

[56] 方滨兴,贾焰,李爱平,等.网络空间靶场技术研究[J].信息安全学报,2016,1(3):1-9.
Fang Binxing, Jia Yan, Li Aiping, et al. Research on cyberspace firing range technology [J]. Journal of Information Security,2016,1(3):1-9.

[57] Holmes D, Papathanasaki M, Maglaras L, et al. Digital Twins and Cyber Security–solution or challenge?[C],2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM). IEEE, 2021: 1-8.

[58] Hearn M, Rix S. Cybersecurity considerations for digital twin implementations[J]. IIC J. Innov, 2019, 10: 107-113.

[59] Nouma S E, Yavuz A A. Post-Quantum Hybrid Digital Signatures with Hardware-Support for Digital Twins[J]. arXiv preprint arXiv:2305.12298, 2023.

[60] Dietz M, Putz B, Pernul G. A distributed ledger approach to digital twin secure data sharing[C],Data and Applications Security and Privacy XXXIII: 33rd Annual IFIP WG 11.3 Conference, 2019: 281-300.

[61] Liu J, Zhang L, Li C, et al. Blockchain-based secure communication of intelligent transportation digital twins system[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(11): 22630-22640.

[62] Suhail S , Malik S U R , Jurdak R ,et al.Towards situational aware cyber-physical systems: A security-enhancing use case of blockchain-based digital twins[J].Computers in Industry, 2022(141-):141.

[63] 郑轶, 胡志锋, 王路路, 等. 信息域与物理域融合的孪生仿真网络靶场[J]. 信息安全研究, 2022, 7(E1): 98.
Zheng Yi, Hu Zhifeng, Wang Lulu, et al. Twin simulation network target range with fusion of information domain and physical domain [J]. Information Security Research, 2022, 7(E1): 98

[64] 郭凤昌,黄金涛,邓雷升等.网络安全数字孪生研究[J].信息安全与通信保密,2023(6):29-39.
Guo Suchang, Huang Jintao, Deng Leisheng et al. Research on Digital twin of Network Security [J]. Information Security and Communication Security,2023(6):29-39.

[65] Gao C, Park H, Easwaran A. An anomaly detection framework for digital twin driven cyber-physical systems[C].Proceedings of the ACM/IEEE 12th International Conference on Cyber-Physical Systems. 2021: 44-54.

[66] Masi M, Sellitto G P, Aranha H, et al. Securing critical infrastructures with a cybersecurity digital twin[J]. Software and Systems Modeling, 2023, 22(2): 689-707.