

数字孪生在核心网络安全中的 创新应用研究

Research on Applications of Digital Twins in Core Network Security

李延斌, 穆佳, 邢天齐 (中国联通研究院, 北京 100048)

Li Yanbin, Mu Jia, Xing Tianqi (China Unicom Research Institute, Beijing 100048, China)

摘要:

分析了核心网安全的重要性和现状,结合数字孪生技术的特点,给出了数字孪生技术应用在网络安全领域中的场景和作用。提出了数字孪生网络安全体系架构和关键技术,分析了网络安全领域面临的挑战,并给出相应的解决方案,为后续研究提供借鉴和参考。

关键词:

核心网安全;数字孪生;安全体系架构

doi:10.12045/j.issn.1007-3043.2026.09.004

文章编号:1007-3043(2026)09-0019-07

中图分类号:TN918

文献标识码:A

开放科学(资源服务)标识码(OSID):



Abstract:

The importance and current status of core network security are analyzed. Combined with the characteristics of digital twin technology, the scenarios and roles of digital twin technology application in the field of network security are presented. The architecture and key technologies of digital twin network security system are proposed, the challenges in the field of network security are analyzed, and corresponding solutions are given, which provides reference and guidance for subsequent research.

Keywords:

Core network security; Digital twin; Architecture of network security

引用格式:李延斌,穆佳,邢天齐. 数字孪生在核心网络安全中的创新应用研究[J]. 邮电设计技术,2026(9):19-25.

0 引言

随着信息技术的飞速发展,网络空间已成为人类不可或缺的“第二生存空间”,其安全性直接关系到国家的安全、经济的稳定以及社会的和谐。网络空间安全形势的严峻性不仅在于攻击次数的增加和技术的复杂性,还在于新的技术如5G和数字孪生技术带来的安全挑战。因此,需要采取新的策略和技术来应对这些挑战,确保网络空间的安全与稳定。在这一背景下,运营商核心网作为通信网络的中枢神经系统,其安全性更是牵一发而动全身,对整个网络系统的稳定

运行和用户数据的安全负有重大责任。网络安全技术的发展,不仅是技术层面的挑战,更是国家安全战略的重要组成部分。

数字孪生技术作为实现数字化、智能化、服务化等先进理念的重要使能技术,当前备受学术界和工业界的关注。它通过在信息世界对物理世界进行等价映射,为物理实体创建虚拟的数字副本,实现物理世界与数字世界的无缝对接和高度融合。数字孪生技术的应用,不仅限于产品的设计和制造,还扩展到了网络空间安全领域,为网络安全提供了新的解决方案。数字孪生技术在核心网安全中的应用潜力巨大,它通过构建精确的虚拟网络模型,实现安全策略的模拟、测试和优化,有效预测和防御网络威胁,提升网络

收稿日期:2026-08-03

的韧性和安全性。同时还能够促进网络安全产品的研发、建、用、维等全环节使能闭环,创造出颠覆性技术机遇。

本文旨在探讨运营商核心网网络安全与数字孪生技术结合的可能性和实践路径,分析网络安全面临的新挑战,探讨数字孪生技术在网络安全领域的应用前景,并提出相应的策略和建议。期望本研究能为运营商核心网网络安全的未来发展提供新的思路和技术支持,以应对日益复杂的网络威胁,保障网络空间的安全与稳定。

1 核心网安全概述

1.1 核心网安全的重要性

5G 核心网引入了网络功能虚拟化、边缘计算^[1]、服务化架构等新技术,使得网络架构发生重大变化,也带来了新的安全挑战。

一方面,用户及产业对网络的要求越来越高,对网络的依赖性越来越强,使得网络承担了更多的使命和责任;另一方面,运营商自身的建设投资及运维压力较之前显著增大。如何既保证业务体验,又降低成本,既保证网络的安全可靠,又可以灵活部署,降低压力,是当前运营商面临的重大课题之一。

5G 核心网容灾本质上是对网络运营成本和网络服务质量的平衡把控。对运营商网络安全和健壮性的考量不仅是要求核心网应用层网元具备相应功能流程要求,而是一种基于网络整体的综合能力评估。

移动通信网络经过多年的演进,逐渐形成了一张四代共存(2G/3G/4G/5G)、三网并存(CS/PS/IMS)的超级复杂网络,不同代际与不同业务网之间存在多种不同组合。再叠加几乎同步演进的承载网、终端和基站,整个电信网的复杂程度趋于极致。此外,5G 核心网引入了服务化架构,在实现简化部署和配置的同时也带来了集中注册和状态管理的风险。

1.2 核心网安全面临的挑战

5G 核心网逐步采用大区化部署,单大区数据中心规划容量过亿,发生故障时影响巨大。5G 核心网多省份共享大区数据中心,两两容灾,单数据中心规模增长 2~3 倍,用户容量达到千万级规模,未来将超过 1 亿。

从应用层视角来看,由于 APP 要求永远在线,现代智能终端在不能连接数据网络时会不断重试^[2]。由于大区数据中心集中,加剧了信令浪涌风险,大区间容灾倒换信令流量是平时的 200 倍以上,而业界重大

恶性事故大多跟信令浪涌有关。

基站到大区控制面距离超千公里,中间经过几十个传输路由设备,容易发生故障。如果省干路由器故障,将影响全省业务,业界已经出现过影响全省语音业务的严重事故。传输距离长导致传输时延大,容易出现通信亚健康,导致业务受损。

电信领域首次大规模采用云存储、SDN 等云化技术^[3],新技术带来架构解耦和配置简化的同时,也带来网络高稳风险。集中部署或集中控制容易导致通信网络整体故障。

此外,在多代、多网络、多协议并存的背景下,电信设备及系统本身的业务复杂度和实现难度已经大幅提高。此时,再叠加异厂家集成,系统可靠性不可控度增高。

5G 网络被广泛应用于垂直行业,需要大量的设备来实现其功能,这些设备在运行过程中可能出现故障或异常。如果设备的安全性能不足或维护不当,可能导致生产事故。同时,5G 网络中传输的数据量巨大且种类繁多,包括生产数据、用户信息等敏感数据。如果这些数据没有得到妥善保护,将面临泄露的风险。一旦数据泄露,将对企业的生产运营和用户的隐私安全造成威胁^[4]。因此,加强对数据的安全管理和保护也是 5G 在垂直行业应用时必须重视的问题^[5-6]。

2 数字孪生关键技术

2.1 定义

数字孪生是充分利用物理模型、传感器更新、运行历史等数据,集成多学科、多物理量、多尺度、多概率的仿真过程,它在虚拟空间中完成映射,从而反映相对应的实体装备的全生命周期过程。简单来说,数字孪生就是为真实世界的物理对象创建一个数字副本,这个副本和物理对象之间可以实现数据的双向流通,并且实时反映物理对象的状态、行为等诸多特性。

2.2 建模技术

建模技术是数字孪生的基础,包括几何建模和物理建模。几何建模用于精确构建物理实体的外观形状,例如对一个复杂的机械装备进行三维建模,从外壳到内部的各个零部件都能通过三维建模软件进行精细构建。物理建模侧重于描述物理实体的物理特性,如材料属性、力学特性等。以汽车发动机为例,物理建模可以模拟发动机在不同工况下的热传导、流体流动和应力分布等情况。

2.3 数据采集与传输技术

要实现数字孪生,大量的数据采集是必不可少的。通过传感器可以获取物理实体的各种数据,如温度传感器、压力传感器、位移传感器等。例如在一个智能工厂中,生产设备上安装的温度传感器可以实时采集设备关键部位的温度数据。这些数据通过网络传输技术,如5G、工业以太网等,快速、稳定地传送到数据处理中心,为数字孪生模型的更新提供原始数据。

2.4 数据处理与分析技术

采集到的数据往往是海量且复杂的。数据处理技术包括数据清洗,用于去除数据中的噪声和错误数据。例如,在采集环境监测数据时,可能会由于传感器故障等原因产生异常数据,通过数据清洗可以将这些无效数据剔除。数据分析技术则可以挖掘数据中的潜在规律,例如通过对设备运行数据的分析,预测设备发生故障的概率,为设备的维护提供依据。

2.5 仿真技术

仿真技术利用数学模型和计算机算法对物理实体的行为进行模拟。在航空航天领域,通过对飞机飞行过程的仿真,可以在虚拟环境中测试飞机在不同气象条件、飞行姿态下的性能,从而优化飞机的设计和飞行控制策略。同时,仿真技术还可以用于模拟生产流程,提前发现生产过程中的瓶颈和问题,提高生产效率。

3 数字孪生在核心网安全中的应用

3.1 安全风险识别与预测

3.1.1 数据收集

从运营商核心网的各个设备和系统中收集数据,包括网络拓扑结构信息(如路由器、交换机的连接关系)、设备配置参数(如防火墙规则、接入控制列表)、流量数据(包括源IP、目的IP、端口号、协议类型等)、设备性能指标(如CPU利用率、内存使用率)和安全日志(记录入侵检测系统、防火墙等的安全事件)。

这些数据可以通过网络管理系统(NMS)、安全信息和事件管理系统(SIEM)等工具进行收集。例如,利用简单网络管理协议(SNMP)从网络设备中获取设备状态和性能数据。

3.1.2 构建数字孪生模型

根据收集到的数据构建核心网的数字孪生模型,包括网络的物理架构和逻辑架构。物理架构模型描

绘了设备的位置、连接线缆等物理特征;逻辑架构模型则展示了网络的IP地址分配、虚拟局域网(VLAN)划分、路由策略等。

例如,使用图形化建模工具,以节点的形式表示核心网中的网元(如基站控制器、移动交换中心等),以边来表示它们之间的连接,构建出一个与实际核心网拓扑结构一致的图模型。同时,在模型中为每个网元关联其相应的配置参数和性能指标等数据属性。

3.2 威胁建模与仿真

3.2.1 攻击场景重现

数字孪生^[7]可以构建一个与真实网络系统完全相同的虚拟模型。通过对以往网络攻击事件数据的收集,如攻击类型(如DDoS攻击、SQL注入攻击等)、攻击路径、攻击者利用的漏洞等,可在虚拟模型中重现这些攻击场景。例如,对于DDoS攻击,数字孪生模型可以模拟大量虚假流量涌入服务器的情况,包括流量的大小、来源IP分布等细节。

攻击场景重现有助于安全团队深入了解攻击是如何发生的,以及攻击对系统各个组件(如服务器、网络设备等)的具体影响。通过观察虚拟模型中系统在攻击下的性能变化,如响应时间的延长、资源的过度占用等,可提前制定针对性的防范策略。

3.2.2 测试安全策略和工具

利用数字孪生模型^[8],安全人员可以在虚拟环境中测试各种网络安全策略和工具的有效性。例如,可在虚拟模型中部署入侵检测系统(IDS)或防火墙,然后模拟不同类型的网络攻击,观察这些安全工具是否能够准确地检测和阻止攻击。

可以对比不同品牌或配置的安全工具的性能,从而选择最适合真实网络环境的安全解决方案。同时,还可以对安全策略进行优化,比如调整防火墙的访问控制规则,测试规则的变化对抵御攻击的影响,以确保真实网络系统的安全性。

3.3 态势感知与威胁情报

a) 精确建模与实时反映。数字孪生可创建网络系统的虚拟副本,包含网络拓扑、设备配置、资产清单和历史事件等信息,且能实时同步网络环境的动态变化,为态势感知提供准确基础。例如,通过数字孪生模型,安全人员能清晰了解网络中各设备的连接关系、运行状态及数据流向,当有新设备接入或网络配置更改时,虚拟副本也会相应更新。

b) 异常检测与威胁辨识。基于机器学习和人工

智能算法,数字孪生模型可持续监测网络环境,收集流量数据、系统日志和安全事件等,分析识别偏离正常基线行为的异常事件。如在发现某段时间内某服务器的流量突然异常增大,或用户登录出现异地频繁登录等异常情况时,可及时发出警报,促使安全团队采取响应措施。

c) 安全风险评估与态势预测。借助数字孪生模型,综合分析历史数据和当前网络状态,评估网络安全风险并预测潜在威胁。比如,根据以往攻击事件数据和当前网络漏洞情况,预测未来可能遭受的攻击类型、攻击目标及影响范围,协助安全团队制定主动安全策略,优先处理高风险问题,提前做好防范准备。

d) 场景模拟与决策支持^[9]。利用数字孪生模型模拟各种网络攻击场景,安全团队可直观看到攻击对网络系统的影响,评估不同应对措施的有效性。在面对实际安全事件时,能快速做出明智决策,选择最优的应对策略,提高应急响应的效率和准确性。

e) 情报收集与整合。数字孪生模型能够收集来自网络中各种设备、系统和应用程序的安全数据,包括漏洞信息、恶意软件活动、异常流量等,并将这些分散的威胁情报进行整合和关联分析。例如,将防火墙的访问日志、入侵检测系统的警报信息以及终端设备的安全报告等进行综合分析,形成更全面、准确的威胁情报视图^[10]。

f) 威胁情报共享。作为一个共享平台,数字孪生模型^[11]可以促进不同安全团队、组织之间的威胁情报共享与协作。各团队可将自己发现的威胁情报上传至数字孪生模型,其他团队则能及时获取并了解最新的威胁动态,实现信息的互联互通,提高整体的威胁应对能力。例如,企业的不同部门或不同企业之间,通过数字孪生模型共享威胁情报,共同应对跨部门、跨企业的网络安全威胁。

g) 预测新兴威胁。通过对大量历史数据和实时数据的分析^[12],数字孪生技术可以挖掘潜在的威胁模式和趋势,对新兴威胁进行预测。例如,分析网络流量中的异常模式、恶意软件的演变趋势等,及时发现可能出现的新型攻击手段或未知威胁,为安全团队提供预警,使其能够提前采取预防措施,降低潜在风险。

h) 基于威胁情报的防御优化。根据收集到的威胁情报,数字孪生模型可以自动调整网络安全防御策略和配置,优化防御机制。如发现某种新型恶意软件正在传播,数字孪生模型可自动更新防火墙规则、调

整入侵检测系统的检测策略等,以增强网络对该威胁的抵御能力,实现主动、动态的防御。

3.4 安全事件溯源与取证

3.4.1 事件重建与过程还原

数字孪生技术可以精确地重建网络安全事件发生的场景。它通过记录网络系统中各个组件(如服务器、网络设备、应用程序等)的状态变化、数据流动和操作记录,构建一个完整的事件时间线。例如,在遭受数据泄露事件后,数字孪生模型可以重现从攻击者首次尝试入侵(可能是通过发送恶意软件或利用系统漏洞)到数据被窃取并传输出网络的整个过程。

对于复杂的多阶段攻击,如高级持续性威胁(APT),数字孪生能够详细地展示攻击者每一步的操作,包括如何在网络中横向移动、利用哪些内部系统和账户权限来获取敏感数据等。这有助于安全团队深入了解事件的全貌,分析攻击者的意图和策略。

3.4.2 数据溯源与追踪

数字孪生提供了强大的数据溯源功能。在网络环境中,数据的流动和转换非常复杂,而数字孪生模型可以跟踪数据的起源、传播路径和所有的修改记录。例如,当发现敏感数据被篡改时,通过数字孪生可以追溯到数据最初的来源,是从哪个数据库表中提取的,经过了哪些中间处理环节(如应用程序的计算、传输过程中的加密/解密等)。

此外,能精确追踪数据访问者的身份,结合用户认证和授权系统的记录,确定是哪个用户账户或者外部实体访问了数据,以及他们具有何种权限级别。这对于确定数据泄露的责任和攻击的源头非常关键。

3.4.3 证据收集与保全

数字孪生模型本身可作为一个可靠的证据存储库,它所记录的网络系统状态、事件日志、数据操作记录等都可以作为网络安全事件的法律证据。这些记录具有时间戳,并且由于是在数字孪生环境下系统自动收集和保存的,其真实性 and 完整性相对较高。

与传统的证据收集方式相比,数字孪生避免了人为因素(如误操作、篡改)导致证据丢失或损坏的风险。例如,在涉及网络犯罪的法律诉讼中,数字孪生提供的详细事件记录和数据溯源信息可为起诉方提供有力支持,证明攻击者的犯罪行为 and 造成的损害程度。

3.4.4 协助调查与分析

安全人员可以利用数字孪生进行深度调查和分

析。通过在数字孪生模型中模拟不同的假设情况,如假设攻击者采用了另一种入侵手段,或者假设在某个时间点采取了不同的安全措施,来验证这些假设对事件结果的影响。

这有助于总结经验教训,评估现有安全策略和措施的有效性。例如,如果在数字孪生模型中发现提前修补某个系统漏洞可以阻止大部分攻击行为,那么就可以明确后续安全加固的重点方向,同时也为制定更完善的应急预案提供参考依据。

3.5 应急响应与处置

3.5.1 培训环境创建

数字孪生提供了一个安全、高度仿真的网络环境用于安全培训。培训人员可以在数字孪生模型中设置各种网络安全场景,涵盖从基础网络钓鱼到复杂APT攻击等多种威胁情境。

新入职的网络安全人员可以在这个虚拟环境中学习如何识别不同类型的安全威胁以及如何使用安全工具进行检测和应对。例如,在模拟网络钓鱼场景中,培训人员可以学习如何识别钓鱼邮件的特征,如发件人地址异常、邮件内容中的可疑链接等,并进行实际的操作,如点击链接后观察系统的反应,以及如何采取正确的措施来清除可能入侵的恶意软件。

3.5.2 应急演练平台

数字孪生作为应急演练的平台,可以模拟真实的网络安全事件。不同的安全团队(如应急响应团队、系统运维团队等)可以在这个虚拟环境中进行协同演练。

例如,在模拟大规模数据泄露事件时,应急响应团队可以练习如何快速封锁受影响的网络区域,收集证据;系统运维团队可以演练如何恢复受损的系统和数据。通过多次演练,可以提高各团队之间的协作效率和应对真实网络安全事件的能力。

3.6 信令风暴解决方案

3.6.1 信令拓扑

基于网元配置数据自动生成网络拓扑图,基于网络性能指标数据在拓扑图中实时呈现信令流量数据。

网络拓扑功能支持逐层下钻,可分别展示逻辑网元视图、容灾组拓扑连线视图和单网元拓扑连接视图。同时,支持查看单网元告警。

3.6.2 信令冲击仿真

该方案提供面向各信令风暴冲击场景的网络信令冲击仿真能力,覆盖5GC的关键信令网元,并输出

评估数据,以辅助网络容灾前的风险评估。其中,网元包括AMF、SMF和UDM,场景包括DC级故障和AMF故障等,评估数据包括用户恢复曲线、网络起控时间以及各网元在冲击过程中的起控表现(信令冲击曲线、起控时间)。

3.6.3 流控参数核查

对核心网中网元的流量控制(流控)参数配置进行检查。通过分析当前设置与预定义策略之间的差异,帮助网络管理维护人员识别并修正可能导致的性能问题或安全风险的配置错误。这一功能确保了网络资源的有效管理和合理分配,以维持稳定的服务质量和防止潜在的信令风暴。

3.7 应用实例

3.7.1 工业物联网数字孪生

通过数字孪生实现对工厂全生产流程的实时监控和故障预测^[13],以预防突发设备故障、降低维护成本并提升生产效率。该方案利用6G网络提供的超高上行数据速率(100 Gbit/s)和毫秒级低时延(<1 ms),将装配线上的大量传感器数据及超高清视频实时同步给数字孪生系统。数字孪生系统利用这些数据模拟物理环境,通过分析振动等异常模式来预测未来可能发生的故障,并辅助维护团队进行维修方案的模拟演练。

3.7.2 AI运维数字孪生

通过数字孪生实现物理网络实体(如基站)中AI/ML模型的自适应优化,解决预训练模型无法适应真实复杂网络环境的问题,从而确保障碍物遮挡等变化环境下的精准波束管理。该方案在边缘或云端创建一个物理基站的数字孪生,该孪生系统实时接收物理基站回传的波束测量、信道状态等数据。当发现模型效果不佳时,数字孪生利用实时数据对AI模型进行重训练和仿真验证,确认有效后将优化好的模型下发回物理基站执行。

4 网络安全数字孪生体系架构

4.1 体系架构

如图1所示,网络安全数字孪生体系架构包含物理网络^[14]、工具中台、网络孪生引擎以及上层应用4层体系,其中网络孪生引擎又包含了孪生模型、孪生服务以及孪生管理。

4.2 关键技术要素

网络安全数字孪生体系架构关键技术包含概念、

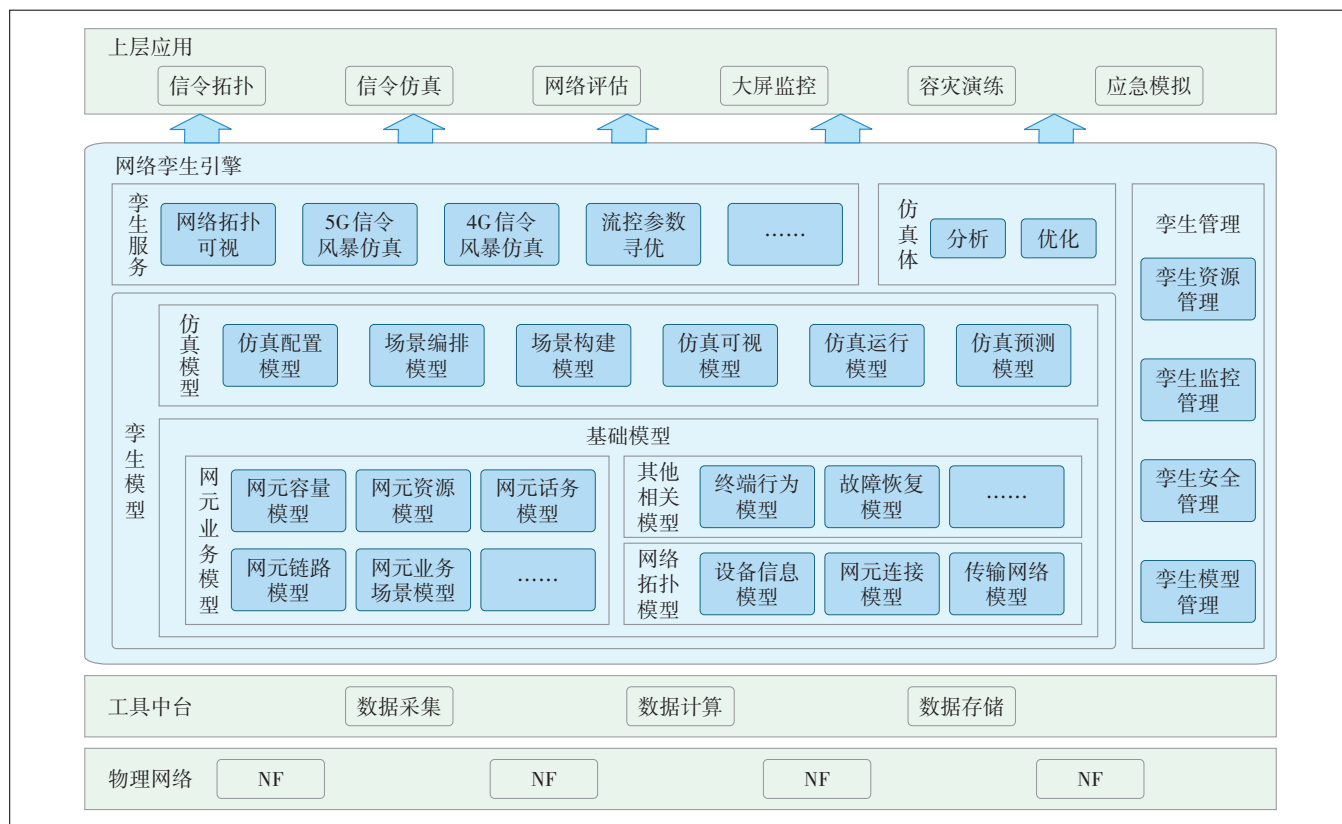


图1 网络安全数字孪生体系架构

特点以及使用场景,具体如图2所示。

5 面临的挑战与解决方案

5.1 技术挑战

a) 数据安全和隐私保护。数字孪生数据通常是时延敏感和任务关键(Mission-Critical)的,需要在其生命周期中跨越多个网络、软件和应用以提供服务,

这使得全方位的安全保护和全过程的信任建立成为挑战。

b) 个人数据收集和滥用。在IoDT中,通过普遍存在的物联网设备收集的个人数据可能处于空前细粒度水平和高同步频率,这为私人数字孪生相关数据的犯罪和滥用开辟了新机会。

c) 新兴技术的安全威胁继承。由于IoDT是建立

分类	机理模型	数据模型
概念	在运行环境上执行物理实体逻辑的完全模拟,目的是尽可能准确地复制仿真对象的业务逻辑,取得更精确的结果输出	利用数学模型、算法、传递函数等手段建立物理实体的工作模型,生成特定行为的预测
特点	- 运行平台和物理实体一样,具备物理实体运行能力 - 所建模型需要和物理实体相同的运行平台,成本高 - 无需为物理对象所有组件建立数学模型,构建方法相对简便 - 精度较高,可以捕获更准确和更广泛细节行为	- 采用数据模型和算法对物理对象进行建模 - 无需和物理实体一样的运行平台,建设成本低 - 对物理实体特定行为进行了简化和抽象化,构建方法相对复杂 - 精度低,物理实体的部分细节无法捕获
适用场景	- 潜在影响精准分析 - 网络优化精准评估 - 支撑机器学习的训练 - 基于CI/CD的网络功能验证 - 紧急准备(预案验证,人员培训) - 配置验证	- 潜在影响定性分析 - 网络优化粗略评估 - 故障预测 - 信令风暴分析 - 故障分析 - 紧急准备(风险评估) - 网络可视(拓扑,流量) - 网络规划设计支撑 - 业务运营(业务保障)

图2 网络安全数字孪生体系关键技术

在各种新兴技术之上提供各类智慧服务,所有这些技术的安全威胁和缺陷(例如窃听、僵尸网络、欺诈和网络钓鱼)可能被 IoDT 所继承。

d) 新的和意想不到的威胁。由于业务功能上的多样性和系统复杂性的不断增长,新的和意想不到的威胁,如语义数据/知识污染和虚实融合式威胁等,可能新的 IoDT 生态系统中滋生。

5.2 解决方案

a) 构建网络安全数字孪生体系架构。需要将数字孪生技术纳入网络安全综合保障体系之中,并针对数字孪生技术特点和应用发展趋势制定其安全发展的整体路线图。

b) 强化网络安全数字化建模。构筑数字孪生发展牢固根基,强化网络安全数字化建模,为数字孪生提供基础的模型支撑。

c) 核心技术壁垒突破。加快突破核心技术壁垒,推进数字孪生尽快落地;加强网络安全数字孪生基础理论创新研究,加快推动网络安全虚实映射技术^[15]、智能演进模型构建、自动推演与实时反馈等关键技术实现突破。

d) 加强数字孪生自身安全设计。确保数字孪生安全运行,加强数字孪生自身安全设计,包括同步、软件、网络隔离和抗 DoS 攻击能力等。

e) 基于区块链的数据安全。在 IoDT 中,传统的基于云/雾的孪生通常因为云/雾服务器的故障而出现典型的敏感信息泄露、数据篡改和数据可靠性问题。为解决上述问题,提出了一种新颖的基于区块链的数字孪生螺旋框架,其中设计了一种新的区块链变体,称为 twinchain,以抵抗量子攻击并提供即时交易确认。

f) 深度学习和博弈论的应用。深度学习技术可以协助提供安全可调的数字孪生体服务,而基于博弈论的方法可用于攻击防御、服务拥塞治理和长期激励设计,以增强数字孪生网络的安全性。

6 结论与展望

数字孪生技术在网络安全方面面临新的挑战,需从网络安全综合保障体系、核心技术研究、网络安全风险预警和应急处理技术等方面进行研究和建设。网络安全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。

数字孪生技术与核心网安全结合的未来发展方向是多维度的,涉及技术融合、产业升级、标准化、网络安全等多个层面,通过技术创新和协同合作,推动数字孪生技术在更广泛领域的应用,并确保其安全性和可靠性。

参考文献:

- [1] 杨红梅,王亚楠. 5G 边缘计算安全关键问题及标准研究[J]. 信息安全研究,2021,7(5):390-395.
- [2] 孙侃. 面向融合媒体应用的 5G 安全风险分析与对策研究[J]. 广播电视信息,2022(增刊1):159-164.
- [3] 郝梓其. 5G 新技术面临的安全挑战及应对策略[J]. 信息安全研究,2020,6(8):694-698.
- [4] 全国信息安全标准化技术委员会,通信安全标准工作组. 5G 网络安全标准化白皮书(2021 版)[R/OL]. <http://www.chuangze.cn/attached/file/20210515/20210515135519081908.pdf>.
- [5] 中兴通讯. 5G 行业应用安全白皮书[R/OL]. <https://www.doc88.com/p-85929371011161.html>.
- [6] 中兴通讯. 5G 安全白皮书:安全让 5G 走得更远[R/OL]. 2019-05-29. https://www.zte.com.cn/content/dam/zte-site/res-www-zte-com-cn/mediares/zte/files/pdf/white_book/201905291835_5G_Security_White_Paper_CN.pdf.
- [7] 孙滔,周铨,段晓东,等. 数字孪生网络(DTN):概念、架构及关键技术[J]. 自动化学报,2021,47(3):569-582.
- [8] 中国移动通信有限公司研究院. 基于数字孪生网络的 6G 无线网络自治白皮书[R/OL]. <https://www.vzkoo.com/document/2022072665e4dfec16e96b8ba922a9f.html>.
- [9] 中国联通研究院,浪潮通信信息系统有限公司,亚信科技(中国)有限公司,等. 中国联通数字孪生网络白皮书[R/OL]. https://13115299.s21i.faiusr.com/61/1/ABUIABA9GAAG6firpAYopo6_ngM.pdf.
- [10] 王达,孙滔,孙晓文,等. 数字孪生在网络全生命周期管理中的研究[J]. 电信科学,2022,38(4):138-145.
- [11] 陶飞,张贺,戚庆林,等. 数字孪生模型构建理论及应用[J]. 计算机集成制造系统,2021,27(1):1-15.
- [12] 刘大同,郭凯,王本宽,等. 数字孪生技术综述与展望[J]. 仪器仪表学报,2018,39(11):1-10.
- [13] 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.
- [14] ITU-T Y.3090 Digital twin network - requirements and architecture[S].
- [15] 高志华. 基于数字孪生的智慧城市建设发展研究[J]. 中国信息化,2021(2):99-100.

作者简介:

李延斌,高级工程师,主要从事移动核心网安全相关的工作;穆佳,高级工程师,主要从事移动核心网的研究工作;邢天齐,工程师,主要从事移动核心网标准相关工作。