DOI:10.20033/j.1003-7241.(2025)02-0071-05.

数字孪生技术下物联网智能终端数据安全交换方法

郭敬东，刘文亮，吴 飞，何德明，李 明
（国网福建省电力有限公司，福建 福州 350003）

摘 要：为实现智能终端数据的安全交换以及数据可视化，提出数字孪生技术下物联网智能终端数据安全交换方法。感知设备获取智能终端的实体数据，将数据清洗、融合处理后，存储至数据库中；利用数字孪生技术构建信息空间中智能终端的虚拟平面仿真模型；采用孪生运行机制和三维场景渲染技术对虚拟平面仿真模型进行处理，生成智能终端数字孪生体三维模型；并采用轻量化身份标识认证协议模型，完成不同智能终端数字孪生体之间进行数据交换的身份认证，抵御终端数据交换时受到的攻击，得到交换结果。测试结果显示方法可有效生成智能终端数字孪生体以及数字孪生体三维场景，实现终端数据交换时滞短，数据交换安全系数高，能够实现不同物联网终端的数据安全交换。

关键词：数字孪生技术；物联网；智能终端数据
中图分类号：TP391.92；TP311.13 文献标识码：A 文章编号：1003-7241(2025)02-0071-05

Data Security Exchange Method of Internet of Things Intelligent Terminal under Digital Twin Technology

GUO Jing-dong, LIU Wen-liang, WU Fei, HE De-ming, LI Ming
(State Grid Fujian Electric Power Co., Ltd., Fuzhou 350003 China)

Abstract: In order to realize the secure exchange and data visualization of intelligent terminal data, a secure exchange method of intelligent terminal data of the Internet of Things under the digital twin technology is proposed. The sensing device obtains the physical data of the intelligent terminal, cleans and fuses the data, and stores it in the database. The virtual plane simulation model of intelligent terminal in information space is constructed by digital twinning technology. The twinning operation mechanism and 3D scene rendering technology are used to process the virtual plane simulation model and generate the intelligent terminal digital twinning 3D model. The lightweight identity authentication protocol model is adopted to complete the identity authentication of data exchange between digital twins of different intelligent terminals, resist the attack of terminal data exchange, and obtain the exchange results. The test results show that the method can effectively generate the digital twins of intelligent terminals and the 3D scene of the digital twins, realize the terminal data exchange with short time delay, high data exchange security coefficient, and can realize the data security exchange of different Internet of Things terminals.

Keywords: digital twin technology; the Internet of things; intelligent terminal data

0 引言

物联网智能终端是物联网中的关键设备，其主要具有数据采集、初步处理、加密以及传输等功能。如果网络中没有该设备，则物联网采集的传感数据则无法进行传送[1]，“物”的联网将不复存在，直接导致智能终端之间的数据无法互联、交换。数据交换指的是两个智能终端设备之间，通过数据通信链路实现各个制备设备之间的互联，实现数据的交互、共享等[2]。数字孪生技术以数字化方式实现一个物理对象的映射，模拟对象在实际环境中的行为，对其运行状态、生产情况、运行数据等进行虚拟仿真以及可视化，以此了解对象的详细信息，并实现物理对象和数字对象之间动态、物理对象和物理对象之间、数字对象和数字对象之间的互动和数据交换。

智能终端数据在交换过程中的安全性以及可视化效果，是保证数据互联的核心，因此，领域内的诸多学者对此展开相关研究。如胡亨汶等提出基于RESTful Web Services的相关交换方法[3]，该方法主要是利用网络的模块化组件实现物联网终端数据的跨平台交换；李超等主要针对物联网终端数据交换过程中的安全性，提出基于可信计算相关交换方法[4]，它们能够实现物联网终端数据交换，但是无法确保数据交换过程中的安全性以及可视化效果。因此，本文提出数字孪生技术下物联网智能终端数据安全交换方法，实现智能终端数据的安全可视化交换。

*基金项目：国网福建省电力有限公司2020年科技项目(52130419002F)
收稿日期：2023-08-08

1 智能终端数据安全交换方法设计

1.1 智能终端数据安全交换方法框架

整体框架如图1所示。采用5层结构：物理层、数据层、业务逻辑层、数组孪生层以及交互层，物理层通过感知身边获取智能终端实体信息的高效采集，并将数据传输至数据层；数据层对数据实行清洗、融合预处理后，存储到数据库中；业务逻辑层依据存储数据，利用数字孪生技术对智能终端的位置、几何、传输行为等进行映射，构建信息空间中智能终端的实体、运行状态、参数的虚拟仿真平面模型后；数字孪生层采用数字孪生运行机制和三维场景渲染，处理智能终端虚拟仿真平面模型后，生成数字孪生体，并保证其和实际智能终端对应，并依据物联网终端安全认证体系实现不同物理对象孪生体之间的数据交换，最后在交互层的交互界面中呈现数据交换结果，并且用户可通过该层中的不同用户端口，进行交换结果查询。

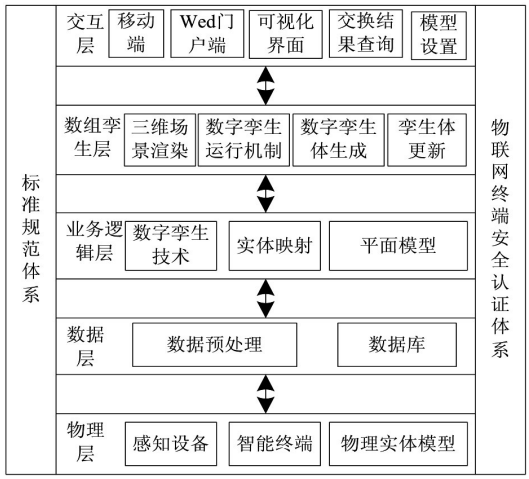

图1 智能终端数据安全交换方法框架

1.2 智能终端数字孪生体生成

1.2.1 智能终端数字孪生体运行机制

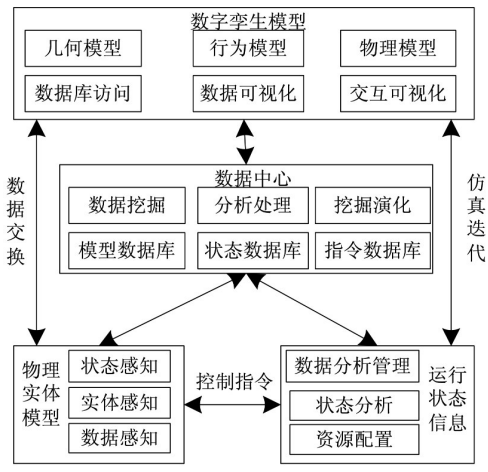

图2 数字孪生数据驱动运行机制

智能终端孪生数据是连接物理控制和虚拟空间的桥梁，同时也是驱动智能终端数字孪生体的核心。因此，智能终端数字孪生体在运行过程中，需满足一定的孪生运行机制。为了实现智能终端数据交互以及生成智能终端数字孪生体生成，需保证物理对象和虚拟对象以及物理对象运行信息之间的可进行两两交互[5-6]。因此，采用深度融合的数字孪生数据驱动运行机制，运行数字孪生体。该运行机制如图2所示。

运行机制包含智能终端和其运行状态信息间的交互机制、虚拟对象和智能终端运行状态信息之间的交互机制、智能终端物理实体和数字孪生体之间的交互机制。

(1) 智能终端和自身运行状态信息间的交互机制

智能终端在进行数据传输过程中，需按照传输需求生成传输方案，如果在传输过程中，数据和传输方案之间存在冲突时，可及时进行传输方案的调整，按照新的方案进行数据传输；并且将相关数据则于数字孪生体[7-9]的生成。

(2) 数字孪生模型和智能终端运行状态信息之间的交互机制

虚拟对象是基于智能终端的几何、运行状态以及规则等，在数据传输和交换前，对该传输过程实行仿真、分析以及评估等，及时发现数据传输过程中会存在的问题，具有一定的预见性。依据虚拟对象的仿真分析结果，可对智能终端物理实体传输方案的效果实行判断，并进行传输方案调整。将数据结果用于智能终端数字孪生体中，为孪生体提供可靠数据依据和驱动。

(3) 智能终端物理实体模型和数字孪生模型之间的交互机制

智能终端物理实体数字孪生体生成时，需依据上述两个机制为基础实现，除此之外，数字孪生体在生成过程中，可通过不断地仿真模拟，判断智能终端的实时数据传输结果与理想结果是否吻合，如果结果的偏差超过允许范围，则依据历史数据、实时数据以及虚拟仿真数据对智能终端的数据传输过程实行优化，保证最佳的传输效果。

1.2.2 智能终端数字孪生体三维场景渲染

智能终端数字孪生体三维场景渲染流程如图3所示。三维场景渲染是智能终端数字孪生体生成的重要步骤，其主要是模拟真实环境，对生成的智能终端平面虚拟模型实行渲染绘制，实现智能终端三维场景构建，并最终呈现给用户。依据该渲染流程即可完成智能数字终端孪生体的生成，通过交互界面进行呈现。

1.3 智能终端数据安全交换实现

1.3.1 物联网终端安全认证体系

孪生体在生成过程中，需依据物理对象和数字对象之间、物理对象和物理对象之间、数字对象和数字对象之间的互动和数据交换完成。为保证交换的安全性，采用

物联网终端认证体系对交换过程实行安全认证，结构如图4所示。应用侧模块能够对用户身份实行统一管理，网络侧通过安全认证网关对对象间的互动和数据交换实行安全认证，终端侧对物联网的边缘网关进行安全认证。3个模块协作，实现物理对象和数字对象之间动态、物理对象和物理对象之间、数字对象和数字对象之间的互动和数据交换时的安全。

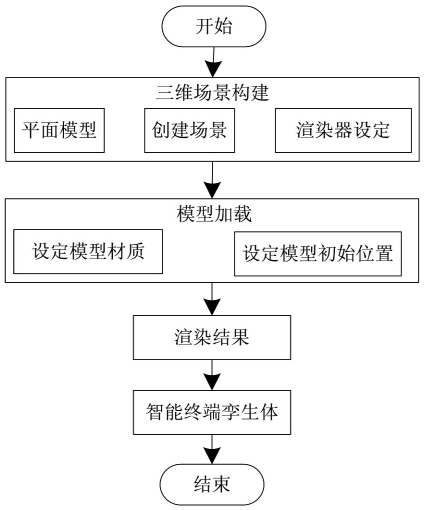

图3 智能终端数字孪生体三维场景渲染流程

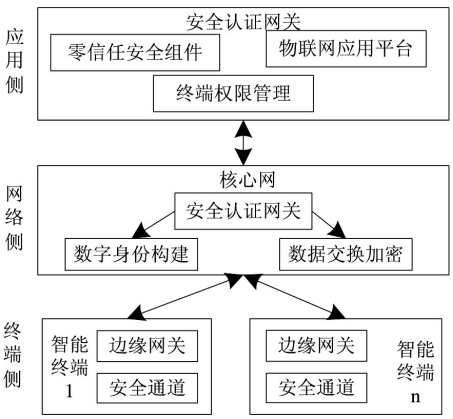

图4 物联网终端安全认证体系结构

1.3.2 数据交换身份认证和数据交换加密

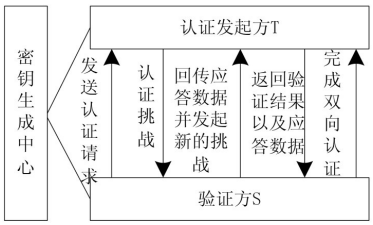

图5 轻量化身份标识认证协议模型结构

物联网终端安全认证体系在进行不同智能终端设备数据交换安全认证过程中，需先通过安全认证网关，构建不同智能终端数字孪生体的数字身份，并进行身份认证后，实现数据安全交换。采用轻量化身份标识认证协议模型完成不同智能终端数字孪生体身份认证，可有效抵御不同终端数据交换过程中受到的攻击。该模型结构如图5所示。

该模型共分为3个阶段，第一个阶段是初始化阶段：该阶段是在安全认证网关中的密钥生成中心中完成，密钥的生成是通过概率多项式时间算法完成，并且生成的密钥保存在生成中心中；第二个阶段是密钥生成阶段：该阶段是在安全认证网关中的密钥生成中心中完成，该阶段中的公钥采用智能终端数字孪生体身份标识表示，以此生成对应的私钥，通过安全信道将该私钥返回给智能终端数字孪生体；第三个阶段是双向身份认证阶段：该阶段以挑战应答机制为主，认证发起方(智能终端1数字孪生体)和验证方(智能终端2数字孪生体)之间通过多次数据交换，完成智能终端数据交换的身份合法性认证。

(1) 初始化阶段

该阶段是在安全认证网关中的私钥生成中心(PKG)完成，PKG会选择两种循环群，分别为加法和乘法，用F_1和F_2表示，两者均为素数，且阶数均为q；E表示任意生成元，且属于F_1中，F_1和F_2双线性对的计算公式为：

$$e:F_1\times F_2\to F_2 \tag{1}$$

如果1^k表示给定的安全参数，选取随机数$\eta_u\in Z_q^*$，则主密钥为η_u，主公钥E_b的计算公式为：

$$E_b=\eta_u E \tag{2}$$

设置PKG中的哈希函数γ_1和γ_2：

$$\begin{cases}\gamma_1:\{0,1\}^*\to F_1\\ \gamma_2:\{0,1\}^*\times F_2\to Z_q^*\end{cases} \tag{3}$$

主密钥不可对外公开，仅由PKG进行保存，上述初始化设置的PKG系统参数：F_1、F_2、e、q、E、E_b、γ_1和γ_2，可向进行过身份认证的所有智能终端数字孪生体公布。

(2) 密钥生成阶段

以构建的数字身份为依据，确定智能终端数字孪生体的唯一身份标识ID结果，并在PKG中生成密钥，同时计算身份标识ID对应的公钥B_{ID}，其计算公式为：

$$B_{ID}=\gamma_1(ID) \tag{4}$$

依据η_u生成智能终端数字孪生体对应的私钥η_{ID}，其计算公式为：

$$\eta_{ID}=\eta_u B_{ID} \tag{5}$$

PKG生成η_{ID}后，将智能终端密钥对(B_{ID},η_{ID})发送给对应的智能终端数字孪生体。

(3) 双向身份认证阶段

该阶段是实现T和S之间的双向身份认证，在该阶段中，T选择自身随机数$r_T\in Z_q^*$、时间戳t_T以及哈希函数γ_2，以此进行交互数据加密计算，则有：

$$c_T=\gamma_2(r_T,t_T) \tag{6}$$

完成c_T的计算后，向S发送身份认证请求，S接受c_T后并实行解密，在解密过程中，需先对t_T的有效性实行验证，如果为有效，S则选择自身的随机数$r_s \in Z_q^*$，在此基础上完成下述公式的计算：

$$\begin{cases} u_s = (r_s + r_T)\eta_s \\ c_s = \gamma_2(r_s, t_s) \\ B_T = \gamma_1(ID_T) \end{cases} \tag{7}$$

式中：u_s表示交换私钥，B_T表示T的公钥，c_s表示解密秘钥，完成上述计算后，向T发送身份认证挑战信息。

T接收数据后，需要解密c_s，对t_s的有效性t_s实行验证，如果有效，则通过式(8)运算S的公钥：

$$B_S = \gamma_1(ID_S) \tag{8}$$

对该公式是否成立进行检验，检验公式为：

$$e\left[u_s, -(r_s + r_T)E\right] = e(B_S, E_b) \tag{9}$$

如果该等式不成立，则表明T和S之间的双向认证失败，则断开两者之间的连接；如果等式成立，则表示T和S之间的双向认证成功，此时计算智能终端数字孪生体的交换私钥u_T：

$$u_T = (r_T + r_S)\eta_T \tag{10}$$

完成u_T的计算后，将应答信息回传给S。S接收验证信息后，并验证时间戳，同时完成验证信息解密，同时检验等式是否成立，其检验公式为：

$$e\left[u_T, -(r_T + r_S)E\right] = e(B_T, E_b) \tag{11}$$

如果该等式不成立，则表明T和S之间的双向认证失败，则断开两者之间的连接，拒绝两者之间的数据交互；如果等式成立，则表示T和S之间的双向认证成功，此时返回认证结果，并接受T传送的数据。

上述分析的数据安全交换过程，同样适用于智能终端和智能终端数字孪生体之间的数据安全交换过程，也适用于不同智能终端之间的数据安全交换过程。

2 测试结果与分析

以某工业生产企业作为测试对象，企业内通过部署物联网智能终端，包含环境传感器(型号FT-H30)、RFID(型号ZK-RFID909)、红外感应器(型号SN913-F)3种智能终端。传感器采集企业的运行信息、环境数据等，并传送至场站的监控中心，实现整个生产的运行监控。为保证数据传输过程中的安全性，并且提升设备的监控效果，获取最佳的数据传输和交换效果，将方法部署在该企业监控中心的原有服务器上，以此实现物联网智能终端数字孪生体的生成，模拟智能终端在实际环境中的数据的传输行为。

获取智能终端数字孪生体可视化结果以及三维场景的三维渲染效果如图6和图7所示。分析图6可得，本文方法可生成不同物联网终端的数字孪生体，呈现出不同终端进行数据交换的交换链路CPU使用率以及网络流量结果。分析图7可得，本文方法能生成实验生产企业的数字孪生体三维场景，并且生成的数字孪生体可进行不同角度的旋转和查看，应用性较好。

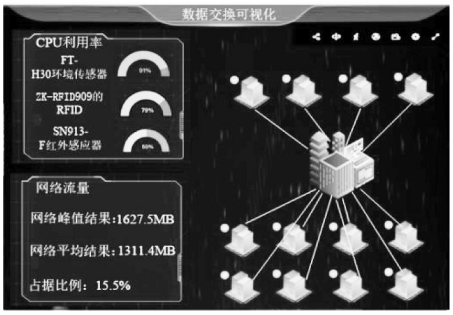

图6 智能终端数字孪生体可视化结果

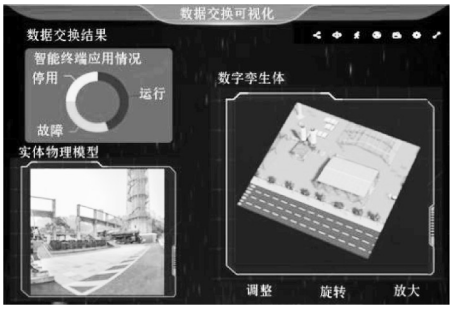

图7 数字孪生体的三维场景渲染结果

为验证本文方法在进行智能终端数据交换过程中，密钥交换结果，获取FT-H30环境传感器和SN913-F红外感应器两种智能终端设备之间的密钥交换结果，如图8所示。对图8的测试结果实行分析后可知：本文方法可完成不同智能终端设备的安全认证，实现不同智能终端设备数据密钥安全交换。

图8 智能终端设备数据安全交换结果

为验证数据交换性能，采用时滞效应作为评价指标，计算公式为：

$$\vartheta = \frac{q_r}{l_e \eta_l} \varepsilon_{loss} \tag{12}$$

式中：q_r表示智能终端服务信息的鲁棒性，l_e表示数据传输

(下转第79页)