专题：面向6G的通感算一体化

基于通感算一体融合的5G风筝专网多源数据弹性安全分析方法

包海斌[1]，史健赟[1]，张建创[1]，王伟[1]，叶燕华[2]，王任[2]，从宇[3]，胡洋洋[3]
（1. 国能浙江北仑第一发电有限公司，浙江 杭州 315800；
2. 中国移动通信集团浙江有限公司宁波分公司，浙江 宁波 315000；
3. 北京科技大学，北京 100083）

摘　要：随着通信技术向6G演进，通感算一体化已成为新一代电力专网的关键特征。针对5G风筝专网接入电厂生产控制大区场景下，多源数据跨域关联难、动态关联规则挖掘适应性差、实时安全防护不足等问题，提出一种面向5G-Advanced通感算一体专网的多源数据弹性安全分析方法。该方法以5G专网为通信基础，融合传感器采集的感知数据，构建多源数据融合处理框架，实现跨域数据的计算分析。通过融合斯皮尔曼秩相关分析与时序FP-Growth算法，并引入指数衰减时间权重模型，实现了对包含时间约束的安全风险关联规则的挖掘。仿真结果表明，该方法对现有威胁的规则覆盖率有显著提升，且误报率明显下降，能够适配5G风筝专网的动态数据特征与通感算协同需求，为电力行业核心生产业务的安全连续运行提供技术支撑。

关键词：通感算一体融合；5G风筝专网；生产控制大区；关联规则挖掘；弹性安全
中图分类号：TM73；TN929.5
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2026002

Elastic security analysis method for multi-source data in 5G kite private network based on integration of communication, sensing and computation

Bao Haibin[1], Shi Jianyun[1], Zhang Jianchang[1], Wang Wei[1],
Ye Yanhua[2], Wang Ren[2], Cong Yu[3], Hu Yangyang[3]
1. Guoneng Zhejiang Beilun First Power Generation Co., Ltd., Hangzhou 315800, China
2. China Mobile Zhejiang Co., Ltd. Ningbo Branch, Ningbo 315000, China
3. University of Science and Technology Beijing, Beijing 100083, China

Abstract: With the advancement of communication technologies toward 6G, the integration of communication, sensing and computation has become a critical characteristic of next-generation power private networks. In scenarios

收稿日期：2025−10−02；修回日期：2026−01−05
通信作者：包海斌，12000885@ceic.com
基金项目：国家能源集团科技创新项目“基于5G风筝专网的弹性安全体系研究与实践项目”（No.E621000029）
Foundation Item: The Science and Technology Innovation Project of National Energy Group “Research and Practice Project on Elastic Security System Based on 5G Kite Private Network” (No.E621000029)

where 5G kite private networks are deployed in power plant production control areas, challenges including difficulties in cross-domain association of multi-source data, poor adaptability in dynamic association rule mining, and insufficient real-time security protection have been identified. To address these issues, an elastic security analysis method for multi-source data oriented to 5G-Advanced dvanced integrated sensing-communication-computation private networks was proposed. This method leveraged the 5G private network as the communication foundation, with perceptual data collected by sensors being integrated to construct a multi-source data fusion processing framework, enabling computational analysis of cross-domain data. By combining Spearman rank correlation analysis with time-series FP-Growth algorithms and incorporating an exponential decay time-weighted model, security risk association rules with time constraints were effectively mined. Simulation verification shows that this method significantly improves rule coverage for existing threats while effectively reducing the false alarm rate. The method well adapts to the dynamic data characteristics and integrated sensing-communication-computation synergy of 5G kite private networks, providing technical support for the secure and continuous operation of core production services in the power industry.

Key words: integration of communication, sensing and computation, 5G kite private network, production control area, association rule mining, elastic security

0 引言

随着5G-Advanced（5G-A）技术的规模部署及其向6G的持续演进，通感算一体化已成为未来专网发展的核心趋势。在电力行业，5G风筝专网作为6G理念的先导实践，依托高可靠、低时延的通信能力，结合智能仪表等感知终端，构建了覆盖电厂全域的“通感算”协同数据采集与分析体系，成为火电企业构建智慧电厂数字化应用的关键支撑。然而，在电力生产控制场景中，5G技术的引入使得核心生产系统与外部管理系统的数据交互量激增，生产控制大区的业务安全面临全新挑战[1]。网络流量数据、工控系统风险等海量数据直接关联到发电机组控制、故障保护等核心生产环节，从而对安全数据的细粒度分析提出了更高要求。

随着电厂规模的扩大与系统复杂度的提升，传统电厂数据分析方法，如规则引擎和静态基线分析等，局限性日益显现[2]。这些方法依靠人工经验和基础统计工具，侧重于事后分析、局部优化和规则判断，已难以适应现代电厂对数据处理的实时性、整体性与智能化要求。具体而言，传统方法主要存在以下3个方面不足：一是在数据存储层面，跨域融合与实时处理能力不足。传统方法缺乏有效的跨域数据融合机制，导致生产控制大区、管理信息大区及物联网终端的数据孤立存储，无法实现跨域关联与全局分析，无法全面反映网络安全态势。在通感算一体专网中，安全态势的刻画需要综合网络流量、终端感知数据、业务指令等多源异构数据。二是在数据分析层面，动态关联与未知威胁挖掘能力薄弱。传统方法主要依赖预定义的静态规则和已知攻击签名库，难以有效挖掘数据中隐含的动态关联特征，面对利用专网特性或针对通感算融合架构的未知攻击时，基于静态匹配的检测机制往往无法及时发现并作出响应。三是在网络适应层面，缺乏对动态环境的自调节能力。5G通感算专网的网络拓扑、业务负载及接入设备可能频繁变化，传统静态分析方法参数固定、模型更新缓慢，难以适应这种动态性，易造成误报或漏报。当网络遭遇攻击而引发中断或重构时，传统方法难以应对动态网络攻击下的业务连续性保障问题，导致安全监测出现盲区，无法为核心业务的连续性提供有效保障。因此，亟须研究面向电网数据的弹性安全分析方法，其核心内涵是系统在遭受攻击、发生故障或面临不确定性扰动时，仍能够持续保障

核心业务功能、快速适应威胁变化，并恢复至正常运行状态。

目前，电力系统数据分析的相关研究主要有：文献[3]通过采集并预处理电网实时数据，利用机器学习算法构建故障预警模型，并结合逻辑回归分析关键特征与故障模式的关联，实现了对电网故障的高精度预测；文献[4]设计了一种基于数据挖掘技术的计算机网络异常入侵检测系统，利用Min-Max归一化、主成分分析等技术处理网络流量数据，并借助支持向量机、*K*-means聚类等算法构建检测模型，有效提升了网络安全防护能力；文献[5]针对新型电力系统中多源异构设备接入导致电网数据缺失率高、传统方法填补精度不足的问题，提出了一种基于波动互相关分析（fluctuation cross-correlation analysis，FCCA）算法与Wasserstein生成对抗网络的电网缺失数据填补方法，有效提升了电网量测数据的完整性与可用性；文献[6]通过深度语义学习技术挖掘运维文本中的设备状态信息，实现了多源异构数据的融合和对电网数据的有效挖掘，提升了电网设备的智能运维效率。

上述研究为电力系统数据分析提供了重要借鉴，但大多聚焦于独立的、相对静态的电力信息系统，尚未充分考虑5G-A/6G通感算一体专网环境下，多源异构数据的实时、跨域、动态关联挖掘需求。因此，在5G风筝专网构建的“通感算”协同新架构下，如何实现对多源安全数据的弹性、精准和自适应分析，已成为保障电力核心生产业务安全连续运行的关键挑战[7]。针对该问题，本文提出一种基于关联规则挖掘的5G风筝专网多源数据弹性安全分析方法。该方法依托一体化安全管理平台，融合斯皮尔曼秩相关分析与时序FP-Growth算法，构建双向动态反馈机制与时间权重模型，实现对设备状态与安全风险的深度关联挖掘，通过识别潜在的威胁信息并发出预警，持续保障核心业务功能，为通感算一体专网环境下的电厂安全提供弹性支撑能力。本文的主要研究内容与创新点如下。

（1）构建面向5G-A通感算一体专网的多源异构数据处理框架，支持跨域数据的融合分析。

（2）提出斯皮尔曼-时序FP-Growth双向动态反馈机制，实现参数动态适配与规则交叉验证。

（3）引入基于指数衰减函数的时间权重模型，提升时序关联规则的时效性与准确性。

（4）设计分层安全架构与本地容灾机制，确保分析系统与生产控制系统的安全隔离与业务连续性。

1　电网安全数据分析系统架构

基于电厂5G风筝专网多源数据，构建电网安全数据分析系统，其核心在于融合通信网络的实时性、感知数据的多样性、计算分析的智能性，形成能够自适应5G-A专网特性的安全分析闭环。该系统以“通感算一体”为设计理念，分为数据采集层、数据预处理层和融合分析层。其中，数据采集层包括无人机终端、业务终端、5G基站与传输设备，以及下沉UPF服务器，依托5G-A通信专网采集智能设备感知到的运行状态、网络日志、安全警报等多源异构数据，为后续分析提供原始输入。数据预处理层包括防火墙、安全网关、交换机、采集服务器等各类安全接入区设备，通过对采集的数据进行过滤、清洗和标准化等操作，消除冗余信息，为融合分析提供高质量数据。融合分析层依托一体化安全管理平台应用服务器和交换机等分析和存储交换设备，部署斯皮尔曼秩相关算法模块，并集成时序FP-Growth算法模块，实现对设备数据中安全关联规则的挖掘。所构建的电厂5G专网安全数据分析系统架构如图1所示。该系统通过分层设备与融合算法的有机结合，为电网设备多源异构数据的关联规则分析提供了有效解决方案，可保障设备安全管控的精准性和实时性。

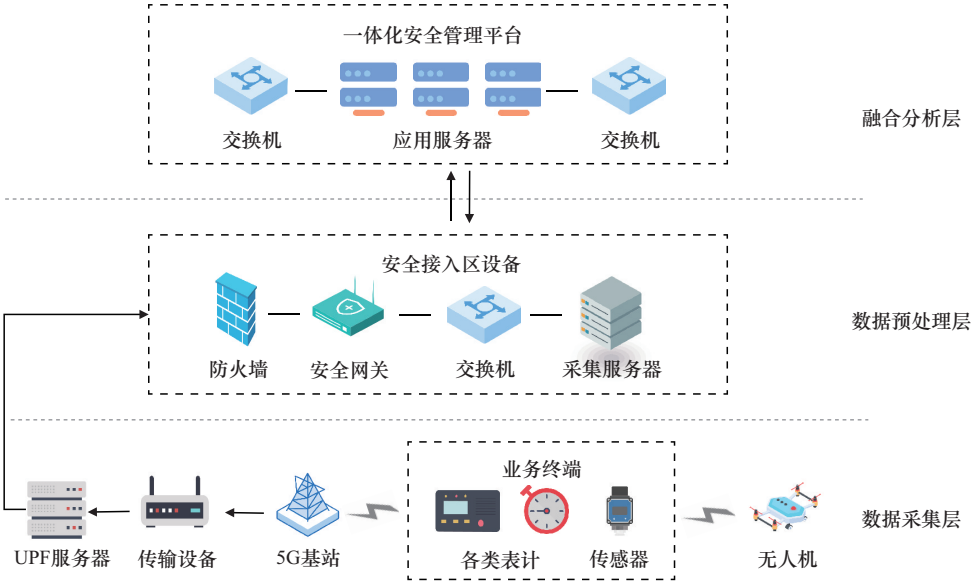

图1　电厂5G专网安全数据分析系统架构

2　基于关联规则挖掘的5G风筝专网多源数据弹性安全分析方法

2.1　多源数据相关性分析

针对通感算一体架构下电厂5G专网中多源异构安全数据的弹性分析需求，本文提出一种融合斯皮尔曼秩相关分析与时序FP-Growth挖掘算法的智能化分析方法。该方法以5G专网为通信基础，整合感知层采集的设备运行参数与安全指标，通过数据清洗、标准化和相关性分析，构建高质量特征集。在此基础上，采用斯皮尔曼秩相关系数衡量参数间的非线性关联，结合显著性检验筛选强关联特征，为时序关联规则挖掘提供输入。

本文方法首先将电网关键设备作为分析对象，聚焦于设备运行状态与安全风险的关联关系，明确包括设备运行参数、操作日志、故障记录等在内的定义分析目标。通过在目标设备上安装传感器及工控终端等数据采集装置，实时采集设备物理参数和运行日志。随后，利用5G通信终端接收业务终端数据，经由5G基站、传输设备、下沉UPF服务器传输至安全接入区。在安全接入区，工控防火墙和安全网关对非法访问进行过滤，确保数据安全传输至采集服务器。

在数据预处理阶段，对采集并接收到的系统配置、运行日志、网络空间威胁、工控系统风险数据以及防护工具的警报信息等实时运行数据进行数据清洗，剔除传感器异常值并填补缺失值[8]。

在异常值剔除方面，首先依据电网设备的物理特性和运行规律，设定合理的业务规则，界定参数正常范围，超出该设定区间的数值即判定为异常。同时结合统计方法辅助检测：对于服从正态分布的传感器数据，采用σ准则计算数据的均值和标准差σ，将偏离均值超过σ的数值标记为异常；对于非正态分布的数据，则通过四分位距法标记异常值。检测出的异常值优先采用备用传感器的同期数据进行替换。若无可替代数据，对于连续型参数，采用异常值前后正常数据的移动平均值进行修正，以平滑数据波动；对于离散型参数，则取同时间段内出现频率最高的数值进行填补，以确保数据的合理性。

在缺失值填补方面，根据字段重要性进行区分：对于关键参数，通过关联设备台账数据库或历史同期数据进行补全，或采用线性插值法计算

缺失的时序数据，即利用缺失值前后的已知数据，按时间间隔比例推算中间值。对于非关键参数，若缺失比例较低，可直接跳过填补而不影响整体分析；若缺失比例较高，则触发传感器故障告警，提示运维人员检查硬件状态。填补完成后，需通过业务逻辑校验确保数据一致性，最终形成完整、可靠的传感器数据集，为后续的关联分析提供高质量输入。

工控设备、网络等在运行过程中会产生量纲及格式不同的多源异构数据，需要将清洗后的数据进行标准化处理，以统一参数格式。由于各项指标数值分布在有限范围内，因此采用离差标准化的方法对数据进行归一化处理，其转换式为：

$$\bar{Z}=\frac{Z-Z_{\min}}{Z_{\max}-Z_{\min}} \tag{1}$$

其中，$\bar{Z}$为归一化处理后的数据，其范围为[0,1]；Z为原始数据；$Z_{\max}$为原始数据最大值；$Z_{\min}$为原始数据最小值。

基于输入预处理后的时序数据集，提取设备状态参数，如电压、温度、负荷以及故障次数等安全指标，利用斯皮尔曼相关系数分析计算参数间的秩相关系数$\rho_{\boldsymbol{X},\boldsymbol{Y}}$，其数学表达式为：

$$\rho_{\boldsymbol{X},\boldsymbol{Y}}=\frac{\sum_{i=1}^{N}\left(x_i-\bar{x}\right)\left(y_i-\bar{y}\right)}{\sqrt{\sum_{i=1}^{N}\left(x_i-\bar{x}\right)^2}\sqrt{\sum_{i=1}^{N}\left(y_i-\bar{y}\right)^2}} \tag{2}$$

其中，N表示观测值的总对数，即样本容量；$\boldsymbol{X}$表示第一类设备状态参数集；$\boldsymbol{Y}$表示第二类设备状态参数集；X_i表示第一类设备状态参数集的元素值；Y_i表示第二类设备状态参数集的元素值；将X_i的N个观测值x_i和Y_i的N个观测值y_i从小到大排序并赋予秩次，最小值秩次为1，最大值秩次为N；$\bar{x}$表示第一类设备状态参数观测值的x_i秩次的均值；$\bar{y}$表示第二类设备状态参数观测值的y_i秩次的均值；$\rho_{\boldsymbol{X},\boldsymbol{Y}}$表示将原始数据转换为秩次后计算得到的皮尔逊相关系数，即斯皮尔曼秩相关系数。

根据秩次的特性，对式（2）进行化简，用于计算两个安全指标的相关系数，如式（3）所示。

$$\rho_{\boldsymbol{X},\boldsymbol{Y}}=1-\frac{6\sum_{i=1}^{N}d_i^{\,2}}{N(N^2-1)} \tag{3}$$

其中，d_i表示x_i和y_i秩次的差值，即两个变量的秩次差。当相关系数计算结果为正时，表示各指标之间的单调性相同；当相关系数计算结果为负时，表示指标之间的单调性相反。相关系数越接近1，说明两个指标之间的相关性越强。

利用t检验判断相关系数是否具有统计显著性，如式（4）所示。

$$t=\rho_{\boldsymbol{X},\boldsymbol{Y}}\sqrt{\frac{N-2}{1-\rho_{\boldsymbol{X},\boldsymbol{Y}}^{\,2}}} \tag{4}$$

其中，t表示检验统计量，服从自由度$df=N-2$的t分布，用于判断相关系数是否显著。给定显著性水平α，若$|t|\geqslant t_{\alpha/2,df}$，则判定两个指标的关联具有统计显著性。

设定相关系数的阈值，结合显著性检验结果，筛选出满足条件的强关联对，并将其作为后续时序分析的核心输入。

2.2　基于时序 FP-Growth 算法的关联规则挖掘

在一体化安全管理平台服务器中部署时序FP-Growth算法模块，用于对核心安全数据的关联规则进行深入挖掘。该步骤在强关联参数基础上，挖掘具有时间约束的频繁安全模式，其核心是通过时序FP-Growth算法提取含时间信息的关联规则。

为适配算法对离散数据的需求，首先需将连续参数值离散化为时序项。通过将连续时间轴划分为若干时间窗口，每个窗口内的所有时序项构成一个时序事务，并标记事务的起止时间，从而构建时序事务数据库。

在时序FP-Growth算法中初始化参数，设置

最小支持度（min_sup）和最小置信度（min_conf）。支持度用于衡量关联规则的“普遍性”，即规则所描述的模式在整个数据集中出现的频率。置信度用于衡量关联规则的“可信度”，即当前件$\boldsymbol{A}$出现时，后件$\boldsymbol{B}$随之出现的概率[9]。对于规则$\boldsymbol{A}\to\boldsymbol{B}$，支持度$D_{\text{sup}}(\boldsymbol{A}\to\boldsymbol{B})$和置信度$D_{\text{conf}}(\boldsymbol{A}\to\boldsymbol{B})$的数学表达式分别如下[10-11]：

$$D_{\text{sup}}(\boldsymbol{A}\to\boldsymbol{B})=\frac{\text{Count}(\boldsymbol{A}\cup\boldsymbol{B})}{\boldsymbol{H}} \tag{5}$$

$$D_{\text{conf}}(\boldsymbol{A}\to\boldsymbol{B})=\frac{\text{Count}(\boldsymbol{A}\cup\boldsymbol{B})}{\text{Count}(\boldsymbol{A})} \tag{6}$$

其中，$\text{Count}(\boldsymbol{A}\cup\boldsymbol{B})$表示项集$\boldsymbol{A}$和$\boldsymbol{B}$同时出现的事务数；$\text{Count}(\boldsymbol{A})$表示项集$\boldsymbol{A}$出现的事务数；$\boldsymbol{H}$表示数据集的总事务数。

在时间窗口设置方面，考虑固定时间窗口未区分参数对安全的影响权重，易割裂关键的时序关联，且难以贴合电厂设备的实际运行周期。基于此，本文对时序FP-Growth算法的时间窗口划分与项权重处理进行了优化。一方面，依据5G专网实时采集的设备负荷数据动态划分窗口，时间窗口与滑动步长随设备运行状态动态切换。另一方面，参照行业相关规范，将设备参数按其安全影响等级赋予相应权重，并引入基于指数衰减函数的时间权重机制。对于一个在时间t_j产生的事务，其在当前时间T的权重w_j定义为$w_j=\mathrm{e}^{-\lambda\cdot(T-t_j)}$。其中，$\lambda$表示可调节的衰减率常数，直接影响历史数据权重的衰减速度，决定了模型对近期事件的敏感程度。λ值越大，权重衰减越快，模型越关注近期事件；λ值越小，历史数据的保留程度越高。电厂5G专网的安全事件通常具有短期爆发的特征，攻击行为的影响周期多在数小时至24 h内。基于这一业务特性，设定λ的初始候选范围，期望模型的“半衰期”（即权重衰减至50%所需时间）控制在12～24 h。在安全监测数据的验证集上，采用网格搜索策略，以加权关联规则挖掘的综合效能指数作为评价指标，系统评估不同λ值下模型的性能，从而确定最优的参数λ，以平衡模型对实时时间的敏感性与对历史有效模式的利用。

接下来，在构建FP树时，对时序项的加权支持度计数进行修正，并在生成规则时计算加权置信度。这一做法确保由核心安全指标主导的规则优先被筛选出来，从而克服静态时序处理方法的局限性。其中，加权支持度和置信度的计算式分别表示为：

$$W_{\text{sup}}(\boldsymbol{A})=\sum w_j\cdot I \tag{7}$$

$$W_{\text{conf}}(\boldsymbol{A}\to\boldsymbol{B})=\frac{W_{\text{sup}}(\boldsymbol{A}\cup\boldsymbol{B})}{W_{\text{sup}}(\boldsymbol{A})} \tag{8}$$

其中，I代表指示函数，如果项集$\boldsymbol{A}$出现在事务j中，则函数值为1，否则为0。$W_{\text{sup}}(\boldsymbol{A})$表示项集$\boldsymbol{A}$的加权支持度；$W_{\text{conf}}(\boldsymbol{A}\to\boldsymbol{B})$表示规则$\boldsymbol{A}\to\boldsymbol{B}$的加权置信度；$W_{\text{sup}}(\boldsymbol{A}\cup\boldsymbol{B})$表示项集$\boldsymbol{A}\cup\boldsymbol{B}$的加权支持度。

在算法协同深度方面，考虑固定的最小支持度和置信度参数难以适应5G专网环境下电厂设备的动态运行状态，本文构建了一种“斯皮尔曼–时序FP-Growth”双向动态反馈机制，其流程如图2所示。该机制计算得到的斯皮尔曼秩相关系数直接关联到时序FP-Growth的挖掘参数，同时将时序FP-Growth挖掘出的强关联规则反向输入斯皮尔曼模块，重新计算规则所覆盖时间区间内的动态相关系数，从而实现两种算法协同优化，以适配电厂5G专网数据的动态特性[12]。在此基础上，最小支持度和最小置信度的设置如下：

$$\text{min\_sup}=\alpha\times(1-|\rho_{\text{min}}|)+\beta \tag{9}$$

$$\text{min\_conf}=\gamma\times|\rho_{\text{avg}}|+\delta \tag{10}$$

其中，ρ_{min}表示强关联参数集中的最小相关系数，α表示调节系数，β表示基础支持度阈值，ρ_{avg}表示强关联参数集的平均相关系数，γ表示置信度调节系数，δ表示基础置信度阈值。

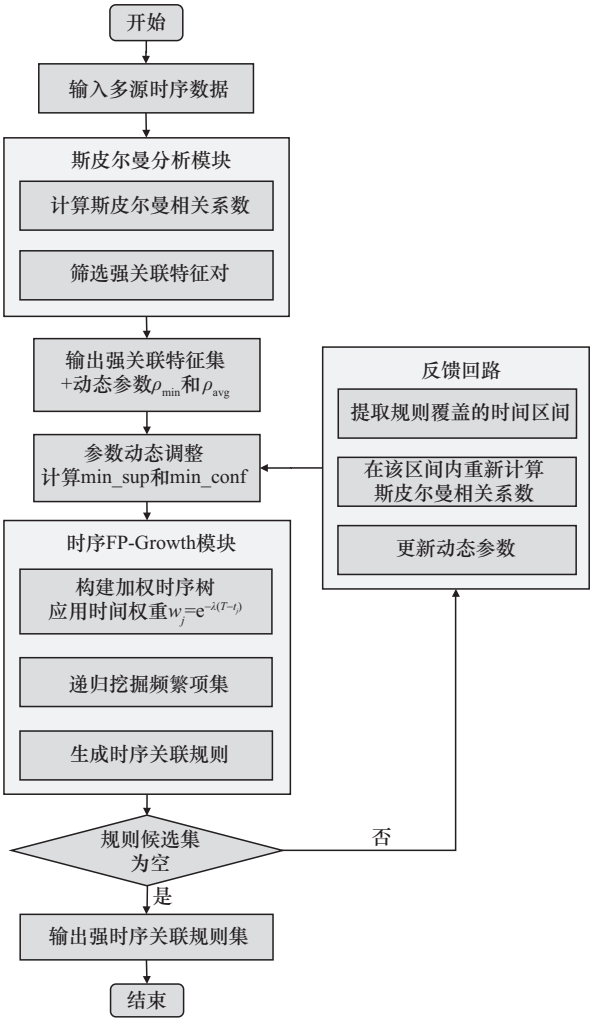

图2　斯皮尔曼-时序 FP - Growth 双向反馈机制流程

接下来构建时序 FP 树，即频繁模式树，以挖掘频繁项集与时序关联规则[13]。首先，扫描时序事务数据库，统计每个时序项的出现次数，筛选出满足最小支持度计数的频繁项集，并按支持度从高到低排序。接着，以排序后的项集为基础，从根节点开始逐条插入事务，相同路径共享节点，每个节点记录项名称、支持度计数及时间戳范围，同时更新项头表以记录项的位置指针。最后，通过递归挖掘时序 FP 树，提取所有满足最小支持度的频繁项集，并记录项集的时间约束。

基于最小支持度的频繁项集生成时序关联规则，规则形式为 $\boldsymbol{A}\rightarrow\boldsymbol{B}$，其中 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 为无交集的项集，且 $\boldsymbol{A}$ 的时间戳早于 $\boldsymbol{B}$ 的时间戳。筛选出支持度不低于 min_sup 且置信度不低于 min_conf 的规则，即强时序关联规则[14]。结合电厂设备特性，进一步提取安全模式，从而为电网安全数据分析及关联规则挖掘提供依据。

3　仿真验证

3.1　仿真设置

为验证本文所提出的基于数据挖掘的电厂 5G 专网弹性安全数据分析方法的有效性，本文研究依托火电厂真实运行数据构建了仿真实验环境，分别从多源数据融合与相关性分析、关联规则挖掘性能以及时间权重模型时效性 3 个维度，对上述核心算法进行验证与评估。

仿真环境基于 Python 3.8 搭建，实验数据来源于真实电厂 5G 专网安全管理子区一体化安全管理平台所采集的安全监测数据，涵盖系统配置、运行日志、网络空间威胁、工控系统风险以及防护工具告警信息等实时运行数据。

3.2　仿真结果与分析

3.2.1　多源数据融合与相关性分析

为验证多源数据经预处理后的可分性，基于标准化后的数值型特征进行 PCA 降维，将高维数据映射至二维空间，结果如图 3 所示。其中，标签“1”代表有安全警报，标签“0”代表无安全警报。从降维结果来看，有安全警报（深色点）与无安全警报（浅色点）的样本在二维空间中呈现明显的聚类趋势。该结果表明，多源数据融合与预处理有效提取了具有区分度的安全状态特征，高维数据的核心信息在降维后得到保留，验证了多源数据融合的必要性与有效性。相较而言，仅从网络、设备或系统中提取的单一维度特征往往难以充分刻画复杂的安全状态。本文提出的融合框架通过整合跨域数据，放大了安全状态在高维空间中的内在差异性，使降维后依然能观察到清晰的分离趋势。这表明融合后的数据蕴含了更丰富、更具判别性的安全状态信息。此外，

清晰的聚类趋势也表明不同安全状态下的数据模式具有较好的可区分性，这为后续时序FP-Growth算法进行关联规则挖掘提供了稳定、可靠的输入基础。

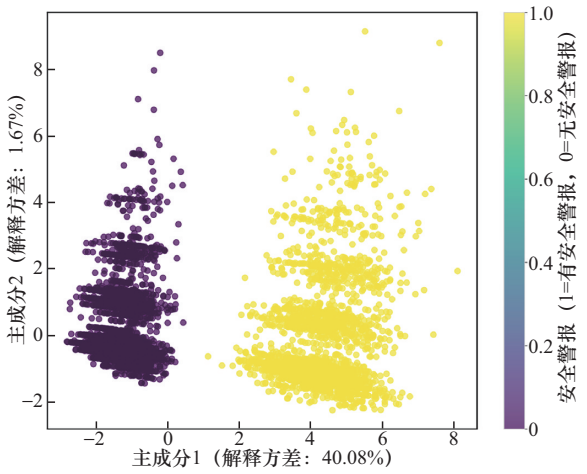

图3　多源数据PCA降维可视化

通过对预处理后的安全监测数据与告警数据进行斯皮尔曼秩相关分析，得到多源数据相关性分析热力图，如图4所示。图4直观反映了不同变量两两之间的非线性关联强度。其中，异常攻击（anomaly_attacks）次数与安全警报（security_alert）的相关系数达0.95，呈最强正相关。这是因为anomaly_attacks直接反映了攻击行为的发生频率，当攻击触发安全警报时，异常攻击次数也随之显著上升，从而验证了该特征作为安全风险预警指标的有效性。与此同时，正常流量（normal_traffic）与安全警报呈强负相关，这是由于攻击发生时恶意流量侵占5G传输带宽，正常业务流量受到挤压。斯皮尔曼分析能够预筛选出与安全目标高度相关的特征子集，确保时序FP-Growth算法的输入数据都是业务逻辑清晰的强关联特征。这显著减少了时序FP-Growth算法需要处理的项集空间，降低了计算复杂度，从而提升了挖掘效率。

取显著性水平为0.05，通过式（4）的显著性检验，上述相关系数对应的检验统计量t均满足条件，表明所有关联关系均具有统计显著性。该分析结果从多源特征中筛选出与安全风险密切相关的关键指标集，验证了斯皮尔曼相关性分析作为时序挖掘前序步骤的必要性和有效性[15]，为后续关联规则挖掘提供了可靠的核心特征集。

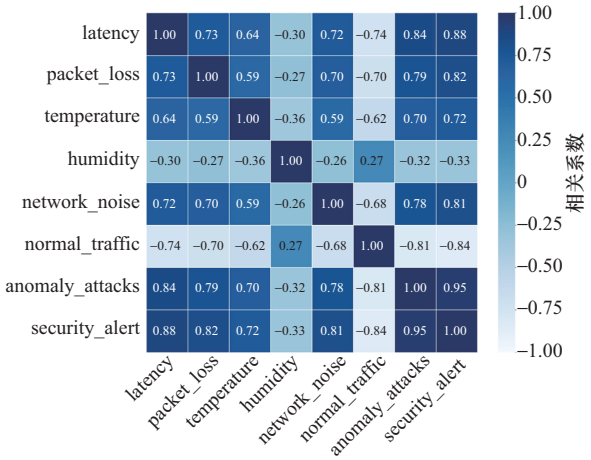

图4　多源数据相关性分析热力图

3.2.2　威胁类型与安全事件时间分布

对电厂5G专网安全监测数据中各类威胁进行统计分析可知，当前电厂网络面临的威胁呈现显著的场景化特征。威胁类型分布如图5所示。分布式拒绝服务攻击（distributed denial-of-service attack，DDoS）出现次数最多，其次分别为网络扫描与数据外泄，这与电厂5G专网的实际风险场景高度吻合。具体而言，DDoS攻击通过挤占5G传输带宽、阻塞核心控制指令通道，可直接干扰发电机组控制、故障保护等关键业务流程；而网络扫描作为攻击前的典型侦察行为，通过探测网络端口、设备漏洞等信息为后续攻击铺垫，是安全防护的重点方向。

每日安全事件数量分布如图6所示。在观测周期内，电厂每日安全事件数量呈现较大波动，符合实际电厂安全数据的动态规律。在设备负载高、数据交互频繁的时段，攻击方更易利用日常业务流量掩盖恶意行为，导致安全事件集中爆发；而在设备低负载、数据传输相对稳定的时段，安全事件则呈现相对平缓的态势。这种动态

波动的特征凸显了传统静态时序分析方法难以适应实际安全需求的局限性，进而验证了本文设计的时间权重模型的合理性。通过为安全事件高峰时段赋予更高的分析权重，该模型可针对性地提升实时检测的灵敏度，从而更好地适应电厂生产活动与攻击行为之间的动态关联特性。

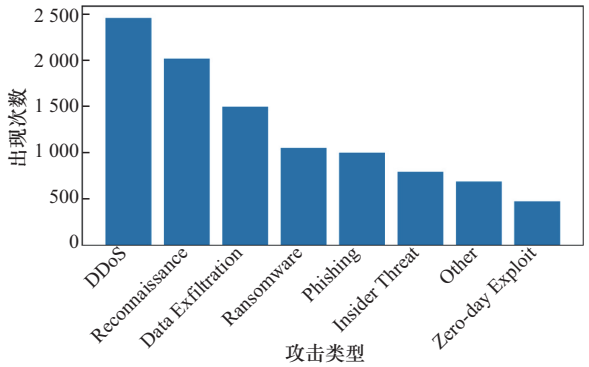

图5　威胁类型分布

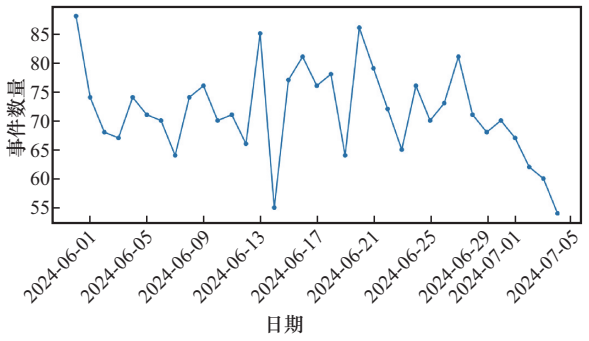

图6　每日安全事件数量分布

3.2.3　时序关联规则挖掘结果分析

基于斯皮尔曼与时序 FP-Growth 双向动态反馈机制，算法能够有效捕捉设备运行参数与安全风险间的动态关联模式。设定最小支持度为 0.15、最小置信度为 0.85，得到强时序关联规则挖掘分析结果，见表 1。

由表 1 可见，直接攻击规则聚焦于攻击行为与安全警报间的显性关联，主要表现为关键运行参数与安全警报在时序上的强联动特征。当异常攻击次数达到设定阈值且网络时延突破临界值时，触发安全警报的置信度极高。该规则可精准覆盖绝大多数攻击场景。例如，DDoS 攻击产生的恶意流量会造成传输链路拥堵，直接引起网络时延攀升，而异常攻击次数的激增则直观反映为持续高强度攻击。二者在时间维度上的协同变化，为安全风险的实时检测提供了可直接部署的量化判断依据。

间接风险规则主要用于发现传统防护手段对隐蔽性攻击的检测盲区，其核心在于挖掘非显性攻击特征之间的组合关联模式。以“正常流量下降且网络噪声升高时触发安全警报”为例，该规则精准捕捉了网络扫描等隐蔽攻击的典型行为特征。攻击方通过伪装流量实施网络探测时，虽未立即引发带宽拥堵等显性异常，但攻击数据包与正常流量的混杂会导致网络噪声升高。此类规则通过挖掘多维度非显性特征的关联关系，突破了传统防火墙仅依赖单一网络层特征的检测局限，实现了对网络扫描等侦察类攻击的提前识别与预警。

3.2.4　双向验证机制与时间权重模型的有效性

为验证双向动态反馈机制的优势，本文将其与传统静态 FP-Growth 算法进行对比分析。传统静态 FP-Growth 算法的支持度固定为 0.2，置信度固定为 0.9。不同算法的规则覆盖率对比如图 7 所

表 1　关联规则挖掘分析结果

规则前件	规则后件	支持度	置信度	核心覆盖场景
异常攻击次数高、时延高	安全警报	0.43	0.94	DDoS 攻击
异常攻击次数高、丢包率高	安全警报	0.36	0.92	高强度 DDoS 攻击
异常攻击次数高、噪声大	安全警报	0.22	0.89	数据外泄攻击前期
正常流量低且噪声大	安全警报	0.20	0.87	网络扫描攻击
正常流量低且丢包率高	安全警报	0.20	0.86	深度网络扫描
温度高、丢包率高	安全警报	0.18	0.83	设备过载

示。传统FP-Growth算法虽通过构建频繁模式树进行规则挖掘，但缺乏对网络安全多源特性的针对性优化。Apriori算法需要多次扫描数据集，且在网络安全高维稀疏数据中难以挖掘有效的关联规则。静态分析方法是基于固定阈值的检测方法的，虽然实现简单，但难以适应复杂多变的网络攻击模式，导致大量潜在威胁无法被有效识别。本文所提出的双向反馈机制借助斯皮尔曼相关系数动态调整挖掘参数，能有效适配5G专网的动态数据特性，从而显著提升关联规则挖掘的准确性和覆盖范围。本文方法的规则覆盖率达83.5%，远高于其他传统算法。这表明通过多源数据关联分析，从不同维度捕捉安全威胁的特征，本文方法能够有效识别并覆盖绝大多数网络安全威胁模式。

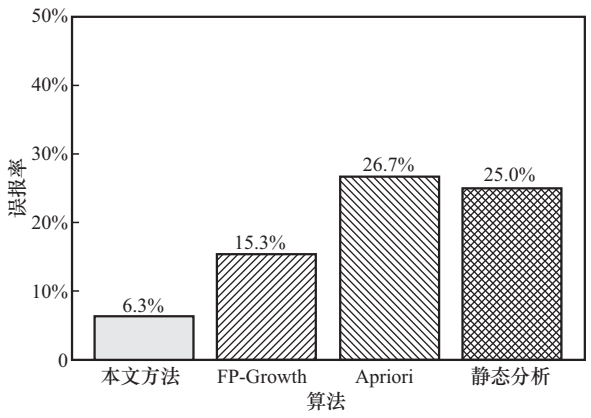

图7　不同算法的规则覆盖率对比

在安全监测系统中，误报率是衡量其实用性的关键指标。实验对比了不同算法的误报率，对比结果如图8所示。传统FP-Growth算法的误报率为15.3%，虽具有一定的检测准确性，但仍存在将正常网络波动误判为安全威胁的情况。Apriori算法由于生成的规则质量较差、实际意义有限，产生大量错误警报。静态分析方法误报率较高，主要原因是其基于固定阈值的检测机制缺乏灵活性，无法适应网络环境的动态变化，容易将正常的性能波动误判为安全事件。相比之下，本文所提方法的误报率仅为6.3%，体现了算法在准确性和可靠性方面的优势。通过多源数据融合和智能关联分析，本文方法能够有效区分正常网络行为与真实安全威胁，从而显著降低误判概率。

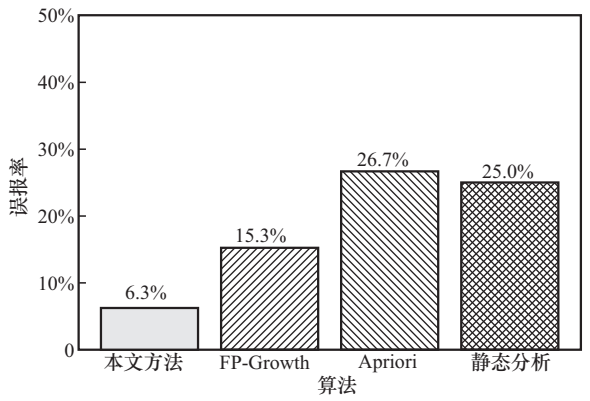

图8　不同算法误报率对比

为验证基于指数衰减函数的时间权重模型的有效性，实验对比了攻击事件发生后加权规则的置信度变化。攻击事件发生后置信度的变化如图9所示。在攻击事件发生后1 h内，加权规则的置信度比未加权规则高5.2%；而在事件发生24 h后，加权规则的置信度大幅降低，未加权规则基本不变。这一结果验证了本文所设计的时间权重模型的有效性。该模型通过显著提升近期安全事件的关联强度，降低历史事件的干扰，使挖掘出的规则更能反映当前网络的安全态势，符合电厂5G专网实时性优先的安全运维需求。

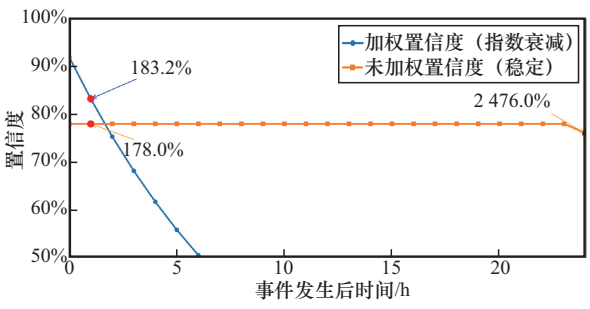

图9　攻击事件发生后置信度的变化

4　结束语

针对5G风筝专网通感算一体环境下多源数

据安全分析难题，本文提出一种面向5G-A通感算一体专网的多源数据弹性安全分析方法。该方法通过构建多源数据融合框架、斯皮尔曼与时序FP-Growth双向机制以及基于指数衰减的时间权重模型，实现了对电厂安全风险的精准挖掘与动态适配。多源数据融合框架突破了传统电厂系统中数据隔离的问题，通过斯皮尔曼秩相关分析实现了网络流量、工控系统风险等数据的跨域关联。在此基础上，斯皮尔曼–时序FP-Growth双向反馈机制与时间权重模型相结合，使方法能够依据动态特性自适应调整参数，从而更好地适配5G专网复杂时变的运行环境。该方法可直接部署于电厂现有的一体化安全管理平台，为5G专网核心业务的安全连续运行提供技术支撑。

基于当前研究成果与通信技术向6G演进的发展趋势，未来研究将重点探索面向6G的通感算深度融合机制。在通信层面，利用智能反射面、全双工等6G关键通信技术提升安全数据传输效率；在感知层面，利用6G网络的泛在感知能力增强感知数据维度，拓展信道状态信息等无线内生感知数据与传统工控数据的融合；在计算层面，构建云边端协同的分布式关联挖掘框架，实现计算资源的动态调配与高效利用。

通过在上述方向的持续探索，本文方法将能更好地适应未来6G通感算一体化电力专网的发展，为6G技术的进步与新型电力系统的构建提供有力的技术支撑。

参考文献：

[1] 肖勇, 费治军, 郑楷洪, 等. 电网运行状态可视化综述[J]. 计算机辅助设计与图形学学报, 2019, 31(10): 1750-1758.
Xiao Y, Fei Z J, Zheng K H, et al. Overview of visualization of power grid operation state[J]. Journal of Computer-Aided Design & Computer Graphics, 2019, 31(10): 1750-1758.

[2] 卢建昌, 樊围国. 大数据时代下数据挖掘技术在电力企业中的应用[J]. 广东电力, 2014, 27(9): 88-94.
Lu J C, Fan W G. Application of data mining technology in electric power enterprises in the era of big data[J]. Guangdong Electric Power, 2014, 27(9): 88-94.

[3] 邹昊凯, 董秋军, 吴布托. 基于大数据分析的特高压电网运行优化与故障预警研究[J]. 电脑编程技巧与维护, 2024(12): 111-113, 125.
Zou H K, Dong Q J, Wu B T. Research on operation optimization and fault early warning of UHV power grid based on big data analysis[J]. Computer Programming Skills & Maintenance, 2024(12): 111-113, 125.

[4] 潘大胜. 数据挖掘技术在计算机网络入侵检测中的应用[J]. 湖北科技学院学报, 2012, 32(12): 58-59.
Pan D S. Application of data mining technology in computer network intrusion detection[J]. Journal of Hubei University of Science and Technology, 2012, 32(12): 58-59.

[5] 蔡榕, 杨雪, 田江, 等. 基于相关性分析和生成对抗网络的电网缺失数据填补方法[J]. 电力工程技术, 2024, 43(1): 229-237.
Cai R, Yang X, Tian J, et al. Missing data filling method of power grid based on correlation analysis and generating countermeasure network[J]. Jiangsu Electrical Engineering, 2024, 43(1): 229-237.

[6] 蒋逸雯, 李黎, 李智威, 等. 基于深度语义学习的电力变压器运维文本信息挖掘方法[J]. 中国电机工程学报, 2019, 39(14): 4162-4171.
Jiang Y W, Li L, Li Z W, et al. Text information mining method of power transformer operation and maintenance based on deep semantic learning[J]. Proceedings of the CSEE, 2019, 39(14): 4162-4171.

[7] 彭小圣, 邓迪元, 程时杰, 等. 面向智能电网应用的电力大数据关键技术[J]. 中国电机工程学报, 2015, 35(3): 503-511.
Peng X S, Deng D Y, Cheng S J, et al. Key technologies of power big data for smart grid applications[J]. Proceedings of the CSEE, 2015, 35(3): 503-511.

[8] 康帅. 配电网大数据因果性和相关性分析方法研究[D]. 兰州：西北师范大学, 2024.
Kang S. Research on causality and correlation analysis methods for distribution network big data[D]. Lanzhou: Northwest Normal University, 2024.

[9] 黄剑湘, 林铮, 骆钊, 等. 基于关联规则算法的换流站SER事件集挖掘方法[J]. 科学技术与工程, 2022, 22(8): 3152-3159.
Huang J X, Lin Z, Luo Z, et al. Mining method of SER event set in converter station based on association rule algorithm[J]. Science Technology and Engineering, 2022, 22(8): 3152-3159.

[10] Hong J H, Li J B, Qiu X J, et al. Numerical correlation analysis of power grid construction project based on apriori algorithm[C]// Proceedings of the 2021 6th Asia Conference on Power and Electrical Engineering (ACPEE). Piscataway: IEEE Press,

2021: 361-364.

[11] Rao S, Gupta P. Implementing improved algorithm over APRIORI data mining association rule algorithm[J]. International Journal of Computer Science and Technology, 2012, 3(1): 489-493.

[12] 黄剑湘, 林铮, 刘可真, 等. 考虑换流站海量事件的关联规则挖掘分析方法[J]. 电力系统保护与控制, 2022, 50(12): 117-125.
Huang J X, Lin Z, Liu K Z, et al. Mining analysis method of association rules considering massive events of converter station [J]. Power System Protection and Control, 2022, 50(12): 117-125.

[13] Hipp J, Güntzer U, Nakhaeizadeh G. Algorithms for association rule mining: a general survey and comparison[J]. ACM SIGKDD Explorations Newsletter, 2000, 2(1): 58-64.

[14] 卢有飞, 冯国平, 卢宾宾. 基于关联规则挖掘技术的电网故障风险要素分析[J]. 武汉大学学报(工学版), 2024, 57(6): 792-797.
Lu Y F, Feng G P, Lu B B. Analysis of power grid fault risk factors based on association rule mining technology[J]. Engineering Journal of Wuhan University, 2024, 57(6): 792-797.

[15] Zhang L L, Wang W J, Zhang Y Q. Privacy preserving association rule mining: taxonomy, techniques, and metrics[J]. IEEE Access, 2019, 7: 45032-45047.

[作者简介]

包海斌（1984–），男，现就职于国能浙江北仑第一发电有限公司，主要从事电力生产工作。

史健赟（1982–），男，现就职于国能浙江北仑第一发电有限公司，主要从事电力生产工作。

张建创（1971–），男，现就职于国能浙江北仑第一发电有限公司，主要从事电力生产工作。

王伟（1983–），男，现就职于国能浙江北仑第一发电有限公司，主要从事电力企业信息化工作。

叶燕华（1989–），女，现就职于中国移动通信集团浙江有限公司宁波分公司，主要从事企业信息化工作。

王任（1982–），男，现就职于中国移动通信集团浙江有限公司宁波分公司，主要从事5G工业互联网工作。

从宇（1996–），男，北京科技大学博士生，主要研究方向为电力无线通信。

胡洋洋（2003–），女，北京科技大学硕士生，主要研究方向为电力无线通信。