工业互联网环境下电力设备网络安全风险评估

Network Security Risk Assessment of Power Equipment in Industrial Internet Environment

罗 进(解放军总医院,北京 100039)
Luo Jin(PLA General Hospital,Beijing 100039,China)

摘 要:
研究了工业互联网环境下电力设备的网络安全风险,通过仿真模拟和数值分析评估了不同算法对数据传输的影响。介绍了工业互联网环境设备组网算法,包括硬件基础、背景环境、协同组网聚类模式等内容,分析了协同组网节点数量对性能的影响,探讨了传输耗时、传输速度和状态预测方差等数据特征。结合关键节点设置,进一步考察了状态感知和短效通信设置对传输性能的影响,为工业互联网复杂网络环境下的安全支持提供保障。

关键词:
工业互联网;电力设备;网络安全评估
doi:10.12045/j.issn.1007-3043.2024.11.013
文章编号:1007-3043(2024)11-0075-07
中图分类号:TN915
文献标识码:A
开放科学(资源服务)标识码(OSID):

Abstract:
It studies the network security risk of power equipment in the industrial Internet environment, and evaluates the impact of different algorithms on data transmission through simulation and numerical analysis. It introduces the network algorithm of equipment in industrial Internet environment, including hardware foundation, background environment, collaborative network clustering mode, analyzes the influence of the number of nodes on the performance of collaborative network, and discusses the data characteristics such as transmission time, transmission speed and state prediction variance. Combined with the key node settings, it further analyzes the impact of state awareness and short-effect communication settings on transmission performance, so as to provide security support for the complex network environment of the industrial internet.

Keywords:
Industrial internet; Electric power equipment; Network security evaluation

引用格式:罗进. 工业互联网环境下电力设备网络安全风险评估[J]. 邮电设计技术,2024(11):75-81.

0 引言

随着工业互联网技术的快速发展,电力设备在网络中的应用日益广泛,随之而来的是网络安全风险的增加,这对电力系统的稳定运行和数据安全构成了威胁。Bian 等人(2021)研究了工业互联网环境下电气设备的智能物联网平台的实现和应用,探讨了智能物联网技术在电力设备中的具体应用,为工业互联网环境下电力设备的智能化提供了重要参考[1]。Zhang 等人(2020)提出了未来工业物联网开放生态系统的架构和应用,探讨了未来工业物联网的发展方向和应用领域,为行业内部数据共享和协作提供了新思路[2]。Zhao 和 Yue (2020)基于工业物联网技术进行了电力传输与变压设备的状态监测,为提高设备运行效率和安全性提供了新方法[3]。Bhattacharjee 和 Nandi (2019)探讨了如何将工业物联网技术应用于可再生能源行业,以促进清洁能源的发展和管理[4]。Alt 等人(2018)调查了在流体动力学领域中实施工业物联网所需的基本概念和要求,为流体动力学系统的智能化发展提供了指导[5]。Li 等人(2017)对工业互联网进行了启用技术、应用和挑战等方面的调查,探讨了工业互联网的相关技术、应用及面临的挑战,为理解工业

收稿日期:2024-09-10

互联网的发展趋势提供了重要参考[6]。Belahcen等人(2015)进行了有关电气机器状态监测与工业互联网关系的调查,探讨了两者之间的联系,为实现电气设备远程监测与维护提供了理论支持[7]。立足已有研究,本文旨在通过仿真模拟和数值分析,评估工业互联网环境下电力设备的网络安全风险,并提出相应的解决方案。

1 工业互联网环境设备组网算法

1.1 硬件基础与背景环境

受技术限制,目前传感器只能进行一些简单的程序计算。因此,在对整个网络进行开发时必须结合实际情况,避免传感器内部逻辑混乱。同时,传感节点通常部署在室外,条件恶劣。在某些传感器发生故障或供电不足无法继续工作时,需要保持整个传感网络的正常运行。

电力设备工业互联网组网环境UML类图如图1所示。在组网过程中,智能传感节点扮演着关键角色。这些节点通过相互交流和协作实现数据共享和处理,可在不同位置和环境中收集信息并形成整体数据视图。通过建立有效的通信机制和协议,智能节点能够共同完成监测任务,并及时响应任何异常情况或事件。在设计网络组网方案时,必须考虑编程逻辑的合理性和系统稳定性。合理设计节点之间的通信规则和数据处理流程是确保网络正常运行和数据准确性的关键。制定清晰明确的编程指导方针,并结合实际场景需求进行调整优化,可在保证系统稳定性的同时提高网络效率。为了应对因故障或供电问题导致的部分节点失效的情况,在组网过程中需要考虑容错设计方案,以确保整个网络持续运行。采用备用电源、自动切换机制或者故障自愈策略等是保证网络连续性和可靠性不可或缺的措施。

1.2 协同组网聚类模式

在工业传感器网络中进行簇内和簇间聚类分析时,本文采用了3种不同的聚类算法:K-means、DBSCAN(Density-Based Spatial Clustering of Applications with Noise)和贝叶斯网络。这些算法在处理数据聚类时有不同的特点和适用场景。

1.2.1 K-means算法

K-means算法是一种常见的聚类算法,旨在将数据点分配给k个簇中的最近中心,从而实现数据的聚类。该算法通过迭代优化数据点与簇中心之间的距离来不断调整簇的位置,直至达到最优聚类结果。具体而言,K-means算法步骤为:随机选择k个初始中心点,将每个数据点分配给距离最近的中心,根据每个簇内所有数据点的均值更新各自的中心。在算法重复分配和更新环节,直到达到收敛条件,如簇内误差平方和不再减小。因此,K-means算法过程是一种迭代优化过程,每次迭代都会不断更新簇中心以获得更好的聚类效果,能够有效地将数据点进行聚类分组。

由此,K-means算法要最小化每个数据点到其所属簇中心的距离之和,即:

$$y = \min \sum_{i=1}^{k} \sum_{x \in Si} \left\| x - \mu_i \right\|^2 \tag{1}$$

其中,y为最优解,c为数据点x到其最近中心μ_i的分配情况,S_i为第i个簇的数据点集合,μ_i是第i个簇的中心。

1.2.2 DBSCAN算法

DBSCAN是一种基于密度的聚类算法,相较于K-means等传统算法,它具有识别任意形状的簇的优势。DBSCAN通过数据点周围的密度来确定核心对象、边界对象和噪声点,从而实现对复杂数据集的聚类。

给定原始数据集为D,D如式(2)所示。

$$D = \left\{ x_1, x_2, \cdots, x_m \right\} \tag{2}$$

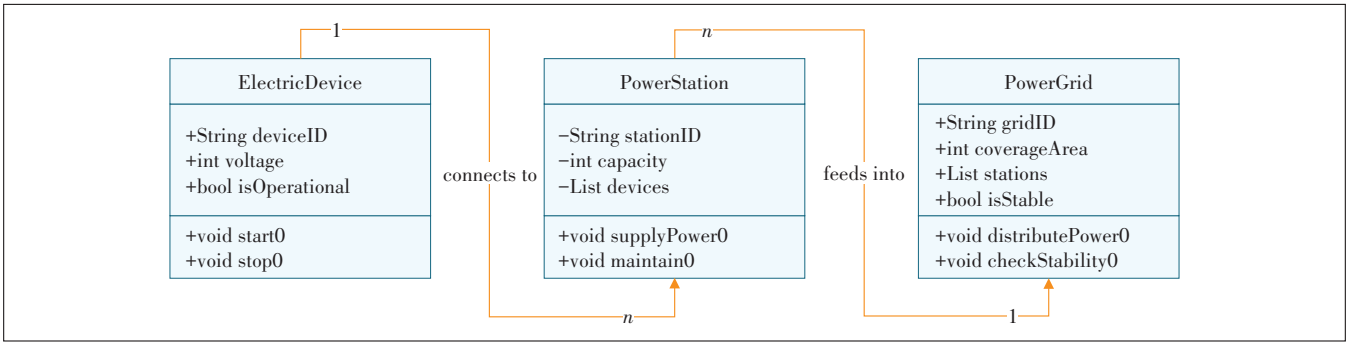

图1 电力设备工业互联网组网环境UML类图

定义ε为半径，MinPts为最小邻居数目，x_j为核心对象。如果在以x_j为中心、ε为半径的邻域内至少包含MinPts个点，即：

$$\left| N_\varepsilon\left(x_j\right) \right| \geqslant \text{MinPts} \tag{3}$$

对D中的元素x_j，其所有与x_j的距离不大于ε的点的集合为ε-领域，即：

$$N_\varepsilon\left(x_j\right) = \left\{ x_j \in D \left| \text{dist}\left(x_i, x_j\right) \leqslant \varepsilon \right. \right\} \tag{4}$$

本文基于此引入SOM模型。通过学习输入空间中任意输入模式下的数据，首先形成一个低维、离散的映射，然后维持其输入空间的拓扑结构，即将输入空间中相邻的样本映射到相邻的输出层神经元中。二维映射包含了数据点间的相对距离数据，以保持这一结构稳定。最后，利用邻域半径的概念界定优胜邻域中的各个节点，按照梯度下降的规律进行训练数据调整，计算相应更新幅度，其更新调整如式(5)所示。

$$m_i(t+1) = m_i(t) + \alpha(t) \times \exp\left[-\frac{\left\| r_c - r_i \right\|^2}{2 \times \delta(t)^2} \right] \times \left[x(t) - m_i(t) \right] \tag{5}$$

其中，t为迭代轮数，$m_i(t)$为第i个节点的初始向量，$\alpha(t)$是学习率函数，r_c为获胜节点的拓扑结构位置，r_i为第i个节点的拓扑结构位置。

算法不断迭代上述过程，直至t达到预期迭代轮数或结果收敛，输出相应结果。

1.2.3 贝叶斯网络

贝叶斯网络是一种概率图模型，被广泛应用于描述变量之间的概率依赖关系。在聚类分析中，贝叶斯网络被用来发现变量之间复杂的潜在关系，揭示数据背后的模式和规律。贝叶斯网络通过有向无环图表示变量之间的依赖关系，其中节点代表随机变量，边代表变量之间的依赖关系。这种图结构使我们能够直观地理解变量之间的联合分布，并通过概率推断进行预测和决策。在贝叶斯网络中，贝叶斯定理是其核心，该定理描述了在随机事件A发生的条件下，随机事件B发生的概率，即：

$$P\left(B \left| A\right.\right) = \frac{P\left(A \left| B\right.\right) \times P(B)}{P(A)} \tag{6}$$

其中，P为事件发生的概率，A、B为随机事件。

在贝叶斯网络中，利用贝叶斯定理来描述各个节点之间的条件依赖关系。通过观察数据集并利用统计方法，可以估计出这些先验和条件概率参数，从而构建完整的贝叶斯网络模型。一旦建立了模型，在给定部分节点值的情况下，可以利用贝叶斯推断来推断其他节点值的分布情况。

本文比较了这3种不同的聚类算法，可以根据具体应用场景和数据特征选择最适合的方法，进行工业传感器网络的数据聚类分析。

1.3 协同组网节点数量对性能影响分析

节点数量与模型选择对传输耗时的影响如图2所示。随着节点数量的增加，传输耗时逐渐增加。在所有算法中，贝叶斯网络的传输耗时相对较低，而K-means和DBSCAN的传输耗时则较高，这可能是因为贝叶斯网络能够更有效地利用节点间的概率依赖关系进行数据传输和处理。当测试节点为200个节点时，K-means算法的传输耗时为38.21 s，DBSCAN算法为34.00 s，而贝叶斯网络为32.08 s。当节点数量逐渐增加至2 000个节点时，贝叶斯网络的传输耗时均为最低。这可能是因为贝叶斯网络能够更好地利用节点间的概率依赖关系，并且在处理大量节点数据时保持了较高的效率。

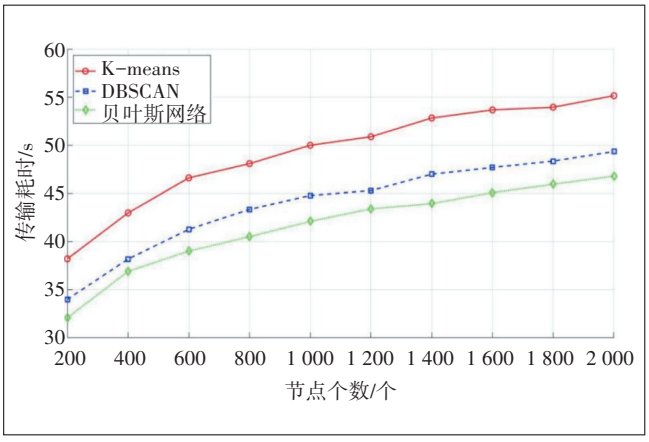

图2 节点数量与模型选择对传输耗时的影响

节点数量与模型选择对传输速度的影响如图3所示。随着节点数量的增加，传输速度呈下降趋势。在所有算法中，贝叶斯网络的传输速度最高，而K-means和DBSCAN的传输速度较低。这可能是因为贝叶斯网络能够更精确地对变量之间的概率关系进行建模，从而提高了数据处理效率。以200个节点为例，不同算法的传输速度分别为78.25 MB/s(K-means)、86.48 MB/s(DBSCAN)、96.82 MB/s(贝叶斯网络)。当节点数量增加到2 000个时，所有情况下贝叶斯网络的传输速度均最高。

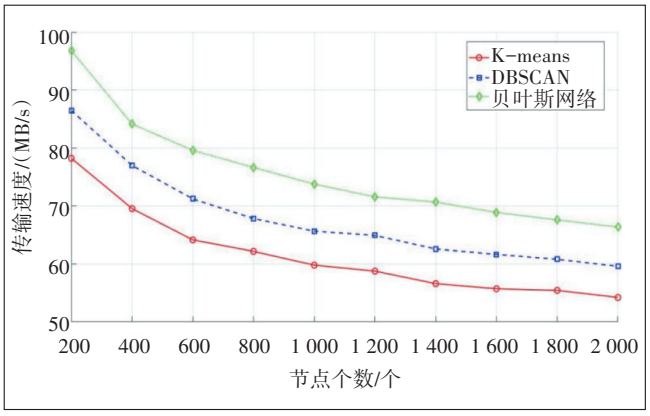

图3 节点数量与模型选择对传输速度的影响

2 聚类后节点信息交流算法

2.1 算法概述

通过智能传感节点之间的通信和协作，能够实现许多有益的功能。不同类型传感器之间的通信可以整合各自收集到的数据（见图4），从而提供更全面、准确的设备参数信息，这种综合性数据视角有助于更好地理解设备状态和性能。同时，不同位置传感器之间的协同工作使全面监测整体环境成为可能。通过跨位置传感器之间信息共享和协同操作，可以获得更全局、立体化的环境监测数据。

2.2 聚类内关键节点设置

对于复杂的电力设备网络连接，其组网需要通过前述聚类算法确定网络中簇的个数，并为每个簇分配一个关键节点。这一过程有：

$$T(n)=\begin{cases}\dfrac{p}{1-p\left[r\times \bmod\left(\dfrac{1}{p}\right)\right]}, & n\in G\\ 0, & n\notin G\end{cases} \tag{7}$$

其中，$T(n)$为节点n是否成为关键节点的阈值，p为其随机产生的0~1的随机数，G为节点n所属的簇，r为算法轮次，以使得迭代次数增长能够提高随机性而寻求更多解，mod为取余数操作。

确定簇首之后，所有簇首节点开始向外广播，并根据就近原则邀请自己的簇内节点成员。如果1个节点同时收到2个簇首的邀请，则根据就近原则选择加入自己意向的簇首。关键节点设置流程如图5所示。

通过将聚类方法与作业现场测试节点供电环境的能量级数相结合的方式来确定每个节点的能量级别。假设每个节点都有一定的初始能量，各节点根据各自的初始能量向外发送激活信号，并确定自己可感知周围节点数量。通过计算可感知距离最大值，可以发现节点初始能量之间的差异。此外，还使用了一种优化的簇内节点数调整策略。通过动态调整通信半径，可限制每个簇内的节点数，降低网络能耗，延长网络寿命。最后，提出了长效-短效混合通信策略，以应对临时增加节点数的情况，确保网络的正常运行。

通过合理设计系统架构和通信策略，可以提高监测效率、确保数据质量，并延长设备寿命，最大限度减少意外事件对网络的影响。

2.3 基于关键节点的性能影响分析

基于关键节点的节点数量与模型选择对传输耗时的影响如图6所示。在工业互联网环境中，每个节点都需要与其他节点进行通信和数据交换。当节点数量增多时，网络中需要处理的数据量也随之增加，这意味着更多的数据包需要在网络中进行传输和处理，导致整体传输耗时逐渐上升。即使在利用聚类算法将节点分类为不同簇并设置关键节点的情况下，每个簇仍然需要一定时间来完成内部通信和数据交换操作。关键节点虽然在簇内提供了局部通信和识别功能，但并未改变整体网络规模增大带来的通信负载增加。因此，在大规模工业互联网环境中，即使通过优化算法或设置关键节点来提高局部通信效率，整体传输耗时仍然会受到影响。

基于关键节点的节点数量与模型选择对传输速度的影响如图7所示。在工业互联网系统中，每个节

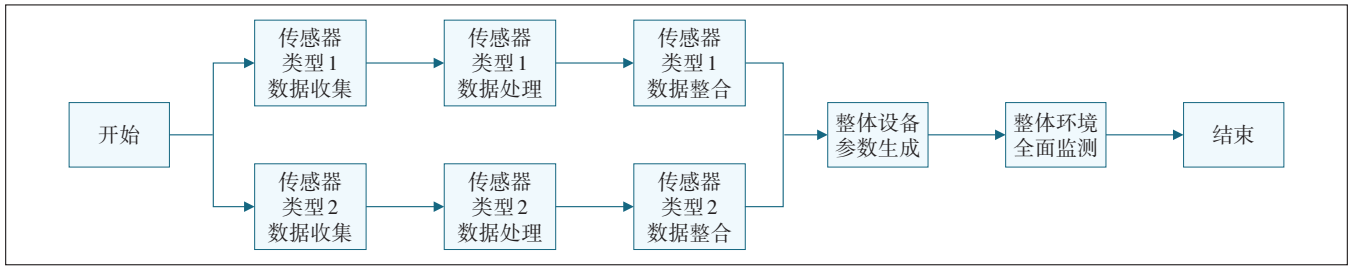

图4 协同组网传感器数据分散整合与全面检测

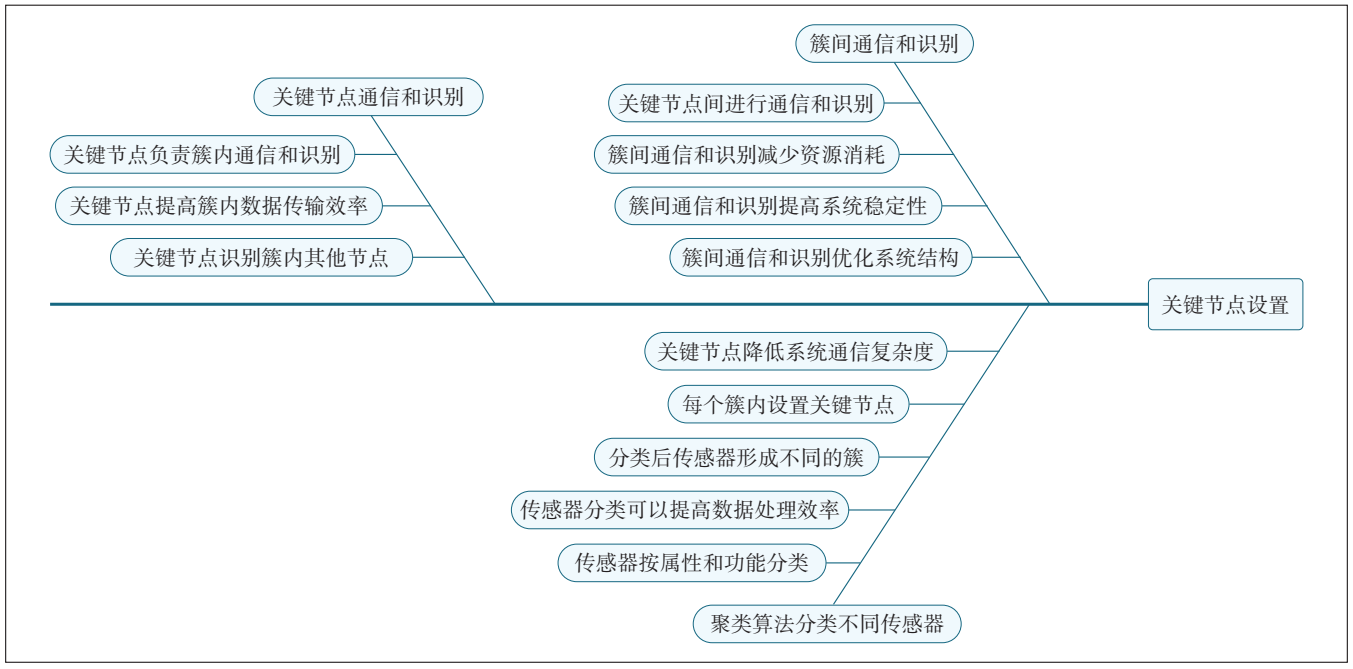

图5 关键节点设置流程

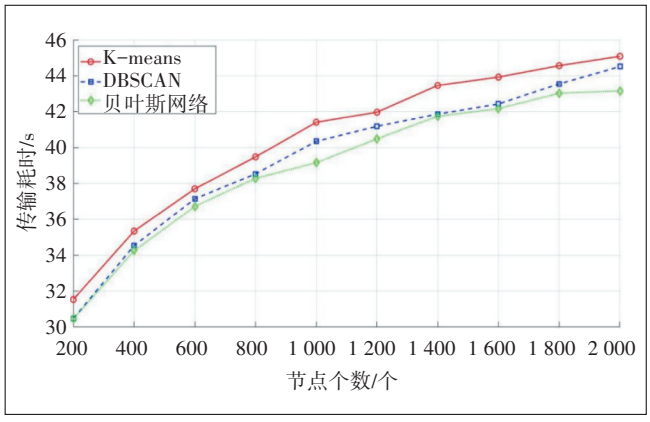

图6 基于关键节点的节点数量与模型选择对传输耗时的影响

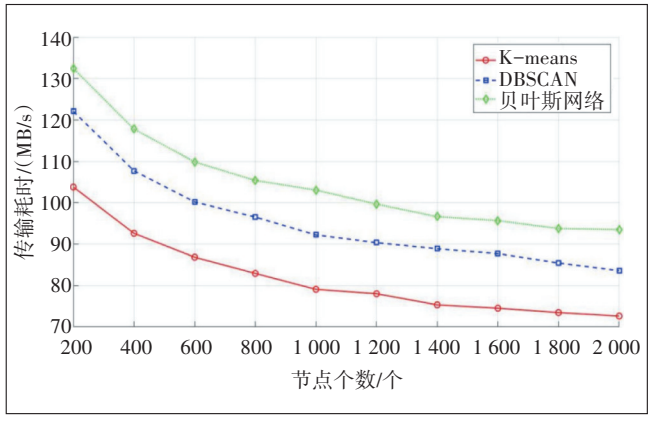

图7 基于关键节点的节点数量与模型选择对传输速度的影响

点都需要在网络中进行数据交换和通信。当节点数量增多时，网络中需要处理的数据量也相应增加，意味着更多的数据包需要在网络中进行传输和处理，导致整体传输速度逐渐下降。无论采用何种算法进行优化，在节点数量不断增加的情况下，网络负载都会随之增加，进而影响数据传输速度。即使通过设置关键节点来优化网络结构，簇内部仍存在大量的通信需求。随着节点数量的增加，簇内通信量也会相应增加，从而对整体传输速度产生负面影响。关键节点虽然可以提高局部通信效率和识别功能，但无法完全抵消整体网络规模增大带来的通信负载上升的影响。

因此，在大规模工业互联网环境中，即使通过算法优化或设置关键节点来提高局部通信效率，在节点数量不断增加的情况下，整体传输速度仍然会受到影响。这是由于随着节点数量的增多，网络负载不断上升，使得数据传输变得更为复杂和耗时。

3 状态感知和短效通信设置

3.1 传感器的簇内感知与识别

工业互联网环境中的电力系统设备数量和传感器需要进行动态感知，实时调度利用全部可用节点，以避免损坏、异常和恶意节点对系统造成干扰。这种动态感知的过程依赖于算法对传感节点的聚类结果的进一步分析，以识别和剔除非正常状态的节点。这

一过程中，首先利用聚类算法将不同传感器分类为不同的簇，然后在不同的簇内设置关键节点，每个关键节点都对簇内其他节点进行通信和识别，而簇间仅依赖于关键节点间的通信和识别。假设对于节点n，其所属簇为i，其可感知节点的数量为k，则计算距离有：

$$d_i = \frac{1}{k}\sum_{k}\mathrm{dist}(n,m),\ m \in i \tag{8}$$

其中，m为任一可感知节点。

为此，模型需相应判断感知范围内的各个节点是否处于工作状态，从而避免异常节点干扰计算和相应的信号传输，其主要利用已有的聚类算法进行对比分析。

此类动态感知和状态预测的性能测试结果如图8所示，状态预测方差表示了预测结果与实际结果之间的差异程度。从图8可以看出，在不同的算法下，随着节点数量的增加，状态预测方差逐渐减小。在所有算法中，贝叶斯网络具有最低的状态预测方差，表明其在状态预测任务中具有更好的准确性和稳定性。以200个节点为例，不同算法的状态预测方差分别为0.51（K-means）、0.44（DBSCAN）、0.38（贝叶斯网络）。当节点数量增加到2 000个时，所有情况下贝叶斯网络的状态预测方差均为最低。

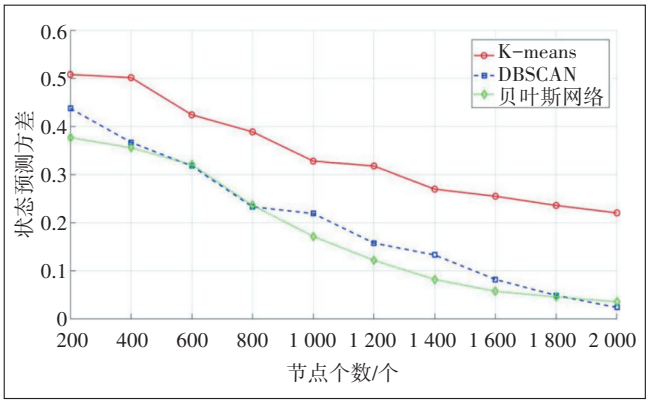

图8 节点数量与模型选择对状态预测能力的影响

在引入关键节点后，再次进行数据分析，其结果如图9所示。在工业互联网系统中，节点数量的增加会导致网络中需要处理的数据量急剧增加。此时，算法的数据处理效率和准确性就显得尤为重要。不同算法在应对大规模数据时可能表现出截然不同的特点，其中贝叶斯网络作为一种概率图模型，在处理大规模数据时展现出了更好的稳定性和准确性。

这种基于智能传感节点系统的感知网络架构为工业互联网环境下的电力设备网络带来了新的可能

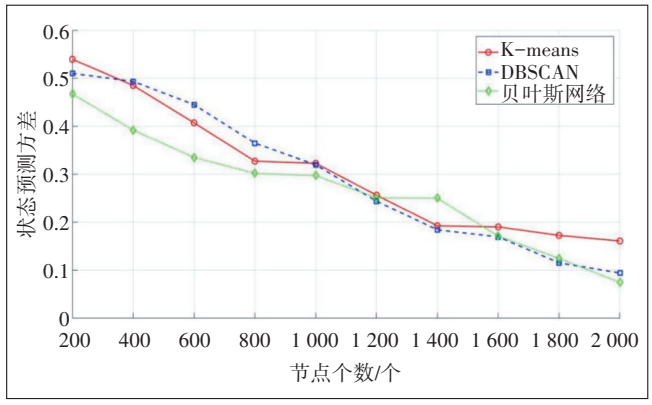

图9 基于关键节点的节点数量与模型选择对状态预测能力的影响

性和机遇。通过促进传感器之间更紧密、智能化地合作，可以更高效、精准地监测电力设备网络，并为未来智能化生产提供坚实基础。

3.2 分模式节点通信影响

通过计算可感知节点数量和平均距离，可以获得该传感器或其他类型设备的感知能力。利用这一指标，算法可以进一步区分不同感知距离的节点，避免感知距离过低、性能不足的节点承担过高的负载，也即构成能量消耗最小化的节点调整策略。

其中，对于特定的可用节点，其当下信号传输模式可以分为仅感受的短效信号传输模式和保持对外广播的长效信号传播模式。

在不设置关键节点时，模型选择与短效通信次数对传输耗时的影响如图10所示。从图10中可以观察到，随着短效通信次数的增加，传输耗时在不同算法下都呈现出逐渐增加的趋势。在处理短效信号传输模式时，随着通信次数的增加，K-means、DBSCAN和贝叶斯网络的传输耗时均逐渐增长。这可能是由于数据量增大导致算法计算复杂度上升，从而影响了传

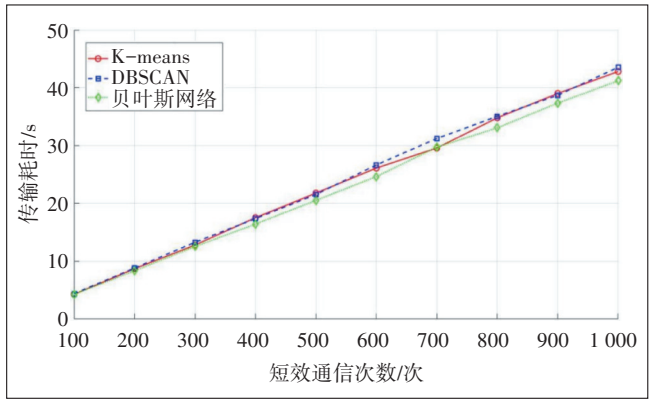

图10 模型选择与短效通信次数对传输耗时的影响

输速度。

相比不设置关键节点的情况，设置了关键节点的数据表现出了不同的特征（见图11）。随着短效通信次数的增加，虽然仍存在一定程度的耗时增长，但相比不设置关键节点来说，3种算法的传输耗时整体要低一些。这可能是由于关键节点参与后，数据传输时能够更有效地利用网络资源、优化路由选择。因此，在长效信号传播模式下，有关键节点参与可以降低整体传输耗时。

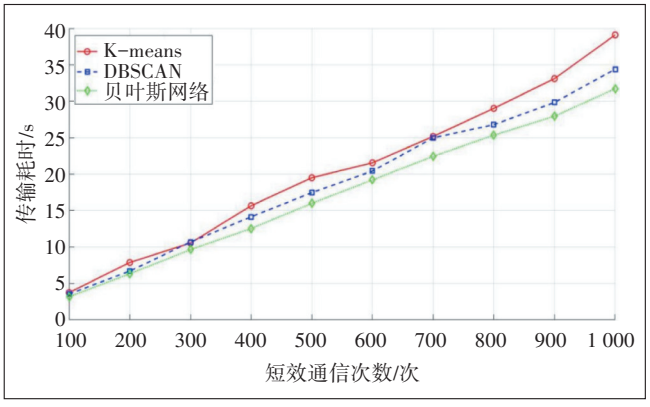

图11 基于关键节点的模型选择与短效通信次数对传输耗时的影响

4 结论

工业互联网的快速发展为电力设备的监测和管理提供了全新的可能性，然而随之而来的安全风险也日益凸显。本文旨在探讨在工业互联网环境下，通过加入关键节点来优化数据传输，提高传输速度和准确的状态感知，从而有效评估电力设备网络的安全风险。

研究对比了无关键节点和有关键节点设置下的数据特征，着重分析了传输耗时、传输速度以及状态预测方差这3个关键指标。传输耗时随着通信次数或节点数量的增加而略有增加，但相比无关键节点设置的情况，设置关键节点时整体传输耗时较低。这表明有关键节点参与时能够优化网络资源利用、改善路由选择等，从而提高数据传输效率。有关键节点设置下，尽管随着节点数量的增加，传输速度有所下降，但整体速度仍然较高。这意味着关键节点参与后能够保持较高的数据传输速度，从而有效应对大规模数据处理需求。在设置了关键节点时，状态预测方差相对较低。这表明关键节点参与后能够降低状态预测的不确定性，有效避免恶意节点对系统造成干扰，并形成对安全风险的有效评估。研究结果表明，在工业互联网环境下加入关键节点对电力设备网络安全风险评估具有积极影响。通过优化数据传输效率、提高传输速度以及准确的状态感知，可以有效评估系统中存在的安全风险，并采取相应措施。

未来，可进一步探讨不同类型电力设备在网络中的行为特征，并结合机器学习等技术手段实现更精准的安全风险评估。系统设计阶段应充分考虑加入关键节点以提升整体效率和稳定性，并在实践中不断完善工业互联网环境下电力设备网络安全防护体系。

参考文献：

[1] BIAN L J, ZHANG J W, CUI Q, et al. Research on the realization and application of intelligent IoT platform for electrical equipment under industrial Internet[J]. Journal of Physics: Conference Series, 2021, 1982(1): 012078.

[2] ZHANG P J, WU Y, ZHU H D, et al. Open ecosystem for future industrial Internet of things (IIoT): architecture and application[J]. CSEE Journal of Power and Energy Systems, 2020, 6(1): 1-11.

[3] ZHAO J D, YUE X Z, et al. Condition monitoring of power transmission and transformation equipment based on industrial Internet of things technology[J]. Computer Communications, 2020, 157: 204-212.

[4] BHATTACHARJEE S, NANDI C, et al. Implementation of industrial Internet of things in the renewable energy sector[M]//MAHMOOD Z. The Internet of Things in the Industrial Sector. Cham: Springer, 2019: 223-259.

[5] ALT R, MALZAHN J, MURRENHOFF H, et al. A survey of industrial Internet of things in the field of fluid power: basic concept and requirements for plug-and-produce[C]//BATH/ASME 2018 Symposium on Fluid Power and Motion Control. New York: American Society of Mechanical Engineers, 2018: V001T01A015.

[6] LI J Q, YU F R, DENG G Q, et al. Industrial Internet: a survey on the enabling technologies, applications, and challenges[J]. IEEE Communications Surveys & Tutorials, 2017, 19(3): 1504-1526.

[7] BELAHCEN A, GYFTAKIS K N, MARTINEZ J, et al. Condition monitoring of electrical machines and its relation to industrial Internet [C]//2015 IEEE Workshop on Electrical Machines Design, Control and Diagnosis (WEMDCD). Manhattan: IEEE, 2015: 233-241.

作者简介：

罗进，毕业于北京航空航天大学，硕士，解放军总医院服务保障中心室主任，主要从事工程类专业技术工作。