物联网环境下多源异构数据融合与安全传输机制设计

王晗

河北科技学院，河北省邯郸市，056000；

摘要：随着物联网技术在工业制造、智慧城市、医疗健康及交通管理等领域的深入应用，系统中产生的数据呈现出来源多样、结构复杂与实时性强等特征。多源异构数据的融合利用成为提升系统智能化水平的重要路径，但在实际应用中，数据格式差异、语义不统一、传输过程易受攻击等问题制约了融合效率与安全性。围绕这一现实需求，本文对物联网环境下多源异构数据的融合机制与安全传输技术进行系统研究，分析其关键问题，并提出基于分层架构的数据融合与安全传输一体化设计方案。通过构建统一数据模型、引入边缘协同机制以及设计轻量级加密与动态密钥管理策略，实现数据融合效率与传输安全性的协同优化。研究表明，该机制能够在保证数据完整性与可信性的前提下，提高系统整体运行效率，对物联网应用的稳定发展具有积极意义。

关键词：物联网；多源异构数据；数据融合；安全传输；机制设计

DOI：10.69979/3041-0673.26.03.104

引言

物联网是新一代信息技术的重要组成，它依靠感知设备、通信网络和智能平台三者之间的配合工作，把物理世界同信息空间融合起来。随着应用场景的不断扩大，物联网系统所接入的设备数量越来越多，数据种类也越来越多样，不同的数据来源之间存在着很大的结构、格式和语义上的差别。传统的处理方式不能很好地解决复杂环境下数据整合的问题，造成信息利用效率低，甚至会影响系统的决策准确性。同时物联网系统具有开放性高、节点分布广、终端资源少等特性，在数据传输过程中存在数据被窃取、篡改、伪造等问题越来越严重。在这样的背景之下，对多源异构数据融合的方法以及安全传输机制进行研究，对于提高物联网系统可靠性和智能化程度有着十分重要的意义。本文从多源异构数据特征入手，分析目前存在的主要问题，建立融合和安全协同的设计框架，提出关键技术的实现途径，为相关领域的研究和实践提供一定的参考。

1 多源异构数据融合与安全传输的基础分析

1.1 多源异构数据的类型与特征

物联网环境下数据来源具有很强的分散性以及复杂性。传感器设备所采集的环境数据、终端设备产生的运行数据、系统平台所产生业务数据一起组成了多源数据体系。这些数据在结构上是结构化数据、半结构化数据和非结构化数据的混合体，在时间上是实时流数据、周期性数据和事件驱动数据的混合体，在表达方式上不同的设备使用不同的编码和通信协议，使得数据具有很强的异构性。另外由于设备制造标准和部署环境的不同，数据质量存在不一致的情况，即缺少的数据、噪声干扰以及异常波动等都会加大后面融合处理的难度。从上面的分析可以看出，多源异构数据还有很强的动态变化特点，不同的设备在运行过程中由于环境改变、设备老化或者网络状态的变化都会引起数据出现偏差，从而造成数据稳定性的降低。数据空间分布存在跨区域、跨网络现象，给数据汇聚与统一管理造成很大障碍。在一些应用场景中还会出现多种模态的数据一起被使用的情况，例如图像、语音以及传感器数值数据等都会参与到分析当中，这就对系统的处理能力提出了更高的要求。因此，在实际使用中要从数据结构、语义表达、质量控制等各方面着手，对多源异构数据实施系统化处理，从而提高数据的利用价值。

1.2 数据融合的内涵与实现方式

数据融合就是把来自各个地方的数据进行整合、处理和分析，从而得到更加全面、更加准确的信息的过程。在物联网环境之下，数据融合不是简单的数据层相加，而重视语义层与决策层的整合。根据融合层次的不同可以分为数据级融合、特征级融合和决策级融合。数据级融合直接对原始数据进行处理，适合于数据结构比较统一的场合；特征级融合通过提取关键特征来实现多源数据的关联分析；决策级融合是在各个子系统独立分析的基础上，再做综合判断。不同的融合方式适合不同的应用场景，要根据实际情况来选择。

1.3 安全传输在物联网中的作用

数据在传输过程中存在着诸多的安全隐患，在无线通信环境当中，攻击者会利用监听、篡改或者伪造数据的方式对系统产生影响。安全传输机制用加密、认证、完整性校验等方式保证数据在传输过程中机密性和可靠性。对于物联网来说，由于终端设备资源有限，传统的复杂安全算法不能直接使用，所以需要设计出轻量化、安全性好、适应性强的传输方式来满足实际的应用需求。从系统运行角度来讲，安全传输同数据本身的安危息息相关，它牵涉到整个系统的稳定状况。数据一旦在传输过程中被篡改或者伪造，就会造成错误的决策，进而引起连锁反应，影响整个系统的正常运转。除此之外，在物联网的环境下由于设备数目多、网络结构复杂、数据在多个节点之间来回流动，因此安全防护的工作就变得越来越难了。

2 物联网多源异构数据融合与传输面临的问题

2.1 数据异构性带来的融合难题

实际应用中各种设备所用的数据格式、通信协议不一样，造成数据不能直接兼容。缺少统一的数据标准造成融合过程中需要复杂的转换和映射，加大了系统的负担。另外数据语义不一致也会造成融合结果出现偏差，比如同一个指标在不同的系统中定义不同，进而影响到分析的准确性。就异构性而言，并不只是数据结构上的不同，还有时间尺度、空间维度上的一致性问题。比如一部分设备是以秒级频率采集数据的，而另一部分则是以分钟或者小时为周期来记录信息的，如果缺少有效的时序对齐机制的话，就无法进行关联分析。另外不同的设备部署位置分散，空间坐标表达方式也不同，都会影响到融合结果。数据质量参差不齐，由于设备受到环境影响或者硬件限制而产生的噪声数据或者缺失数据，会使得融合变得更加困难。对于上面的问题，只能依靠简单的数据转换来满足要求，不能达到统一建模和智能校正的目的，从而提高数据的一致性和可用性。

2.2 安全机制与系统架构的不匹配问题

目前很多物联网系统的设计中没有考虑到安全的需求，安全机制往往是作为附加模块存在的，并没有和数据融合的过程进行协同。部分设备使用简单的认证方式或者没有加密处理，很容易成为攻击的入口。不同的层次之间安全策略不统一，造成整体防护能力不够。安全问题还表现在防护措施零散化，各个安全组件没有统一的调度，不能形成一个完整的防护体系。感知层设备侧重身份认证，网络层侧重数据加密，但是缺少贯穿全流程的安全控制，造成链路中存在防护薄弱环节。另外一些系统在数据传输的时候没有对数据的完整性做有效的校验，从而给攻击者留下篡改数据的机会来影响系统的判断。更复杂的是，在物联网环境当中，设备数量众多并且分散，安全策略的统一部署和更新比较困难，一旦某个节点出现漏洞，就会成为攻击扩散的入口。因此建立与系统架构高度融合的安全机制，就成了提高整体安全性的主要方向。

3 多源异构数据融合与安全传输机制设计

3.1 分层架构设计

为了改善系统的性能，可以创建起以感知层、边缘层和平台层构成的分层架构。感知层完成数据采集和初步处理，边缘层做数据预处理和局部融合，平台层做深度分析和全局融合。分层设计可以有效地降低系统的负载，提高数据处理的效率。感知层除了完成数据采集的任务之外，还要对数据进行初步的筛选和格式规范，从而减少无效信息进入系统。边缘层是连接终端和平台的中间层，有一定的计算能力可以完成数据清洗、特征提取和局部融合，从而降低中心平台的压力。平台层把资源集中起来做复杂的分析和模型训练，可以实现跨区域的数据整合以及长期趋势的预测。合理划分各个层次的职责，可以达到资源最优配置的目的。分层架构给安全机制的部署提供了一条清晰的道路，不同的层次可以根据自身的特性来选择相应的安全策略，从而提高整个系统的稳定性和可扩展性。

3.2 统一数据模型与语义映射机制

利用统一的数据模型把各种不同的来源数据进行标准化表示。采用语义映射技术把各个系统中产生的数据做语义对齐，保证融合结果的一致性。该方法可以降低数据转换的成本，提高融合的效率。在实际使用中，统一的数据模型要兼顾到设备种类、数据属性以及业务需求，对数据加以结构化表述，而且还要确立起统一的字段规范和编码准则。语义映射机制就是建立数据之间的联系，把各个系统中不同的异构数据变成统一的语义表达。以创建领域知识库或者本体模型的方式，对设备的状态、环境参数等进行统一的定义，从而使得系统可以正确地理解数据的意义。另外语义映射可以结合上下文信息做动态调整，来满足不同的应用场合的要求。这样既可提高数据融合的准确性，又给后续智能分析打下良好的基础。

3.3 安全传输机制设计

就安全传输来说，可以采用轻量级的加密算法并结合动态密钥管理。对数据加以加密以防泄漏，使用身份认证手段保证通信双方的合法性，并且依靠完整性检验来防止数据在传送时发生更改。多种技术共同起作用可以形成稳定的数据传输环境。具体实现时，要依照设备资源情况来挑选恰当的加密办法，对计算能力较差的终端而言，可以选用低复杂度算法，从而减轻能耗负担。动态密钥管理可以提高系统的安全性，定时更换密钥可以减少由于密钥泄露造成的风险。另外在传输过程中加入双向认证，可以防止非法节点接入系统。利用安全日志记录和异常检测技术，可以对潜在的威胁进行及时发现和处理，从而构建起比较完善的系统安全防护体系。

4 关键技术实现与优化策略

4.1 边缘计算与融合优化技术

边缘计算可以在数据源附近完成部分处理任务，减少数据传输量，提高响应速度。在边缘节点上采用融合算法可以实现实时数据处理，降低中心平台的负担。并且用数据压缩、筛选技术提高系统的效率。边缘节点根据业务需求可以对数据进行分类处理，对于高实时性数据优先做本地分析，对于历史性数据则上传到平台做深度处理。另外边缘计算可以和缓存一起使用，在网络不稳定的时候暂时保存数据，防止数据丢失。采用智能调度算法可以针对网络状况以及计算负荷情况，对任务进行动态的分配，从而达到资源合理分配的目的。边缘计算应用可以加快系统响应速度，给大规模物联网系统稳定运行提供支持。

4.2 动态安全管理与风险控制策略

对于物联网环境下动态的变化可以创建自适应的安全管理机制，依照网络状况以及设备的行为来改变安全策略。利用异常检测技术找出隐藏的危险，从而迅速做出反应来加强系统的防护。另外，创建完备的日志记载和审计系统，有益于找出安全事件。在实际使用中可以利用行为分析技术，对设备的通信方式实行持续监控，当出现异常情况时，就会发出警报。同时利用风险评价模型给各个数据、节点设定不同的安全等级，从而达到差异化防护的目的。系统还可以加入自动响应机制，在检测到威胁的时候自动隔离异常节点或者改变访问权限，从而减小安全事件造成的损失。利用各种技术手段的配合使用，可以创建出灵活高效的、高效的防护体系。

5 结语

伴随着物联网技术的不断发展，多源异构数据融合以及安全传输的问题将会一直被人们所关注。本文从理论分析和机制设计两个方面给出面向物联网环境的融合与安全协同方案，采用分层架构、统一数据模型、轻量级安全机制的方式来达到数据处理效率和安全性之间的平衡。从另一方面来说，它既可以提高系统的稳定性，又可以提高数据应用的可靠性，给智慧城市、工业互联网等场景提供有力的支持。未来可以继续对智能融合算法、跨域数据共享、安全防护技术等进行研究，用人工智能的方法来改进融合策略，用区块链技术提高数据可信度，研究更高效的轻量级安全算法。不断改善有关的技术体系，可以促使物联网系统朝着更加智能、可靠、安全的方向前进。

参考文献

[1]张玮.农业企业数据资产赋能业财融合的价值提升策略[J].中国集体经济,2026,(11):29-32.DOI:10.20187/j.cnki.cn/11-3946/f.2026.11.015.

[2]刘兴隆.跨域感知环境下的物联网数据可信共享方法[J/OL].智能物联技术,1-7[2026-04-02].https://link.cnki.net/urlid/33.1411.TP.20260328.0910.002.

[3]徐文渊,程雨诗,陈艳姣,等.关键信息基础设施物联网安全发展态势及展望[J/OL].中国工程科学,1-12[2026-04-02].https://link.cnki.net/urlid/11.4421.G3.20260326.1457.012.

[4]张潮,陈祎飞,韩磊,等.静压桩施工数据自动采集系统的研发与实践[J/OL].施工技术(中英文),1-4[2026-04-02].https://link.cnki.net/urlid/10.1768.tu.20260325.1402.004.

[5]王艳.基于电子工程技术的农业大数据平台架构设计与关键技术[J].世界热带农业信息,2026,(03):139-141.

作者简介：王晗（2004.1），男，汉族，籍贯：河北省邯郸市，学历：本科(未毕业)，研究方向：物联网工程。