文章编号:1671-4598(2024)10-0326-07 DOI:10.16526/j.cnki.11-4762/tp.2024.10.046 中图分类号:TP391 文献标识码:A

态势感知技术下多传感器隐私数据防篡改方法

罗立芳
(中国石油大学(华东)信息技术中心应用平台室,山东 东营 257000)

摘要:多传感器运行环境复杂化,隐私信息的外界威胁度较高,为了有效实现多传感器隐私数据防篡改,提出了一种态势感知技术下多传感器隐私数据防篡改方法;结合隐私数据安全需求,确定密钥分存策略,设置隐私数据加密查询范围;基于多传感器隐私信息环境态势感知结果和隐私数据查询结果,制定动态防篡改机制,实现多传感器隐私数据防篡改;实验结果表明:该方法在不同节点环境下能够快速响应,防第三方篡改机制最小响应时间为1.8 s,单元块触发次数均较低,证实了该方法具备较好的隐私数据防篡改性能。

关键词:多传感器;防篡改;隐私数据;态势感知技术

Anti Tampering Method for Multi Sensor Privacy Data under Situation Awareness Technology

LUO Lifang
(Department of Information Technology Center Application Platform, China University of Petroleum (East China), Dongying 257000, China)

Abstract: It is of high external threat to privacy information for multiple sensors to operate in complex environments. In order to effectively achieve multi-sensor privacy data and prevent tampering, this paper proposes a method for preventing the tampering of multi-sensor privacy data under situational awareness technology. The security requirements of privacy data are combined to determine the key sharing strategy and set the range of the privacy data encryption query. Based on the situational awareness results of multi-sensor privacy information environments and privacy data query results, a dynamic anti-tamper mechanism is developed to achieve the anti tampering of multi-sensor privacy data. Experimental results show that this method has the characteristic of fast response in different node environments, with a minimum response time of 1.8 s for third-party tamper prevention mechanisms, and low triggering times for unit blocks. It is verified that this method has a good privacy data tamper prevention performance.

Keywords: multi-sensor ; anti tampering; privacy data; situation awareness technology

0 引言

单一传感器无法全面、准确地感知和描述复杂的空间环境状态,而多传感器可以通过温度、湿度、光照等传感器,定时或连续监测室内环境,获取空间环境中的多种信息,如温度、湿度、光照、空气质量等,及时反映空间环境的变化。但是多传感信息隐私数据的安全问题日益突出,给用户的隐私安全和财产安全带来威胁,同时也影响了人们对传感网络的信任度。因此,如何防止隐私数据篡改成为智能传感网络安全领域亟待解决的问题之一。

文献[1]应用数据挖掘技术提取信息隐私数据,对其之间的关系进行深入探究。通过同态加密算法与区块链技术对隐私数据进行加密与传输处理,从而实现隐私数据的防篡改传输;文献[2]利用数据挖掘方法对信息隐私数据定义进行精准地确定,对用户权限进行检验,引入数据加密算法实现隐私数据的防篡改性能;文献[3]设置了基础防御机制,判定用户的可信任度。利用分布式认证结构计算隐私数据的安全性增强函数,设计相应的隐蔽信道对隐私数据进行传输,完成了隐私数据防篡改方法的设计。上述3种隐私数据防篡改方法主要注重于隐私数据的加密,虽然能够实现隐私数据防篡改的目的,但是整体性能较差,例如防篡改成功率较低、响应时间较长等。

为了提高多传感器隐私数据防篡改的整体性能,提出态势感知技术下多传感器隐私数据防篡改方法。引入态势感知技术,获取多传感器信息环境的运行态势,通过对多传感器运行环境的评估和预测,提高了对隐私数据篡改的感知能力。通过深入分析隐私数据的特性,针对不同类型

收稿日期:2023-09-21; **修回日期**:2023-10-26。
作者简介:罗立芳(1975-),男,大学本科,高级工程师。
引用格式:罗立芳. 态势感知技术下多传感器隐私数据防篡改方法[J]. 计算机测量与控制,2024,32(10):326-332.

的隐私数据设计相应的查询程序，使得获取的隐私数据查询结果更加准确和可靠。

1　隐私数据防篡改方法设计

1.1　基于密钥分存策略的隐私密钥数据防篡改设计

常规情况下，用户码 u_i 主要是标识用户身份，而注册码 r_i 主要是验证用户身份，两者之间存在着一定的映射关系，以此为基础，对用户访问隐私数据权限进行判断。但是，上述用户权限判断方法存在着逻辑隐藏、错误率高等问题，所以此研究创新性地将密钥用户码 u 与注册码 r 进行分存处理，选取 Hash 函数构造密钥生成函数，以此来计算隐私数据的加密密钥，从而实现密钥的分存策略。

依据隐私数据的 Hash 加密算法，构造密钥生成函数 F_i，其表达式为：

$$M_i = F_i(u_i, r_i, H_i) \tag{1}$$

式中，M_i 为加密密钥空间；H_i 为隐私数据对应 Hash 数值，是隐私数据存储的关键参数[4]。一般情况下，隐私数据对应用户码 u_i 与注册码 r_i 以字符串形式存储，主要通过数值形式实现注册码 r_i 验证，故将用户码 u_i 与注册码 r_i 转换成数值形式，将其划分为多个数据段 $u_1, u_2, \cdots, u_v$ 与 $r_1, r_2, \cdots, r_v$，相应的隐私数据也被划分为多个单元块，并且每个单元块均处于加密的状态，还遵循着后一个单元块的 Hash 数值是在前一个单元块的 Hash 数值基础上得到的规律。该规律具体来说，即每个单元块都包含前一个单元块的 Hash 值，当一个新的单元块被添加到区块链中时，它的 Hash 值就会根据前一个区块的 Hash 值和自身的数据通过比特操作计算得到。这种机制确保了区块链的完整性和可追溯性，因为任何对区块链的修改都会被反映在新的区块的 Hash 值中。

依据上述描述得到隐私数据密钥分存结果如下式所示：

$$\begin{cases} M_1 = F_1(u_1, r_1, H_1) \\ M_2 = F_2(u_2, r_2, H_2) \\ \quad\vdots \\ M_v = F_v(u_v, r_v, H_v) \end{cases} \tag{2}$$

完成将密钥分散存储在不同的位置，以减少密钥被攻击者获取的可能性，从而提高数据的安全性和防止密钥泄露的风险。

1.2　多传感器运行隐私数据加密查询范围设计

上节将密钥进行了分散处理，为数据加密查询提供了必要的密钥保护。为了保护多传感器隐私数据，还需要对隐私数据的查询范围进行设置，只有获得授权的用户才能解密查询特定的隐私数据，确保对隐私数据查询在此范围内，从而保护数据的机密性。

对多传感器运行数据中的隐私部分加密，可以增加保护机制的破解难度，提高攻击者破解保护机制的代价，即可以增强该种保护机制有效性能[5]。以上述理论为基础，构建隐私数据加密查询范围，如图 1 所示。

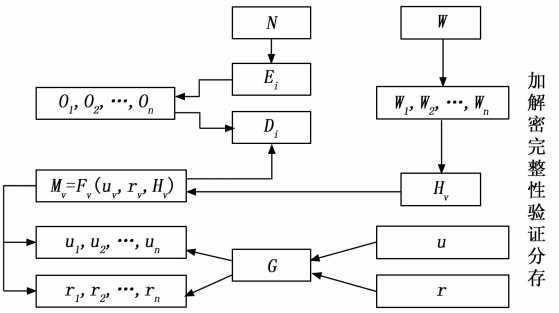

图 1　隐私数据加密查询范围示意图

如图 1 可知，构建隐私数据加密查询范围可以用一个九元组来描述，表达式为：

$$\psi = \{W, O, E, D, N, M, F, G, H\} \tag{3}$$

式中，ψ 为隐私数据加密查询范围设置结果；W 为明文空间，记为 $W = \{W_1, W_2, \cdots, W_n\}$；$O$ 为密文空间，记为 $O = \{O_1, O_2, \cdots, O_n\}$；$E$ 为隐私数据采取的加密算法，其能够生成相应的密文；D 为隐私数据采取的解密算法，其能够还原初始明文；N 为解密密钥空间；F 为密钥生成函数，是加密密钥计算的主要依据；G 为分解函数，承担着用户码 u_i 与注册码 r_i 分解的任务。

从图 2 来看，设置隐私数据加密查询范围不需要特殊硬件设备的支撑，也不需要对传感系统进行修改，并采用加密方式代替了验证与响应过程，加大了传感系统对于隐私数据的保护力度。通过隐私数据加密查询范围的设置，确定选择的加密算法和解密算法以保护隐私数据的安全性，为实现多传感器隐私数据防篡改功能提供了一个基础框架。

1.3　入侵态势感知下的隐私数据防篡改

多传感器隐私信息网络环境的入侵态势感知过程不是仅对某一刻的信息环境进行感知，而是要随时间变化对环境状态进行持续地感知和跟踪，根据上节设计的隐私数据加密查询范围，结合态势感知方法和隐私数据特性分析方法，制定动态防篡改机制，实时监测隐私数据的篡改行为和识别隐私数据，从而实现隐私数据防篡改。

1.3.1　多传感器隐私信息网络环境运行态势感知

为了及时发现异常行为和潜在的原始环境信息数据篡改风险，使用态势感知技术执行多传感器运行状态实时监控任务，通过多传感器运行态势要素信息获取、处理与分析，完成当前多传感器运行网络环境态势的全面评估，为后续隐私数据的防篡改奠定坚实的基础[6]。标准情况下，态势感知主要划分为 3 个阶段，分别为运行态势提取阶段、运行态势评估阶段与运行态势预测阶段，具体设计过程如下所示。

1）多传感器运行态势评估指标提取阶段：

多传感器运行态势提取阶段对数据完整性要求较高，此研究采用 Windows 平台中抓包软件 WireShark 对多传感

器运行数据包进行捕获[7]。抓包软件 WireShark 内部还包含多种协议自动解析器，可以完整显示不同数据包的细节信息[8]。首先，WireShark 在捕获的数据包中寻找协议标识，确定哪种协议解析器应该应用于该数据包。并将该数据包传递给对应的解析器进行解析。其次，协议自动解析器会将数据包中的二进制数据转换为可读格式，并提取出各个字段和信息。它会根据协议规范中定义的结构和字段格式，解析包头、包体和附加信息等。最后，解析器将解析得到的信息显示在 WireShark 界面上，以便用户查看和分析。这些信息可能包括源 IP 地址、目标 IP 地址、端口号、消息类型、有效载荷数据等。一般情况下，多传感器运行数据包解析后可以获得数据基本与内容属性特征，具体如表 1 所示。

表 1 多传感器运行态势数据基本内容与属性特征表

(a)多传感器运行态势数据基本属性特征

特征描述	特征代码	特征类型
目的端口号	Des_port	离散型
目的端口 IP	Des_ip	离散型
源端口号	Src_port	离散型
源端口 IP	Src_ip	离散型
协议类型	Protocol_type	离散型
连接持续时间	Duration	连续性
连接状态(正常或者错误)	Flag	离散型
源主机-目标主机字节数	Src_bytes	连续性
目标主机-源主机字节数	Dst_bytes	连续性
连接是否来自同一主机	Land	离散型

(b) 多传感器运行态势数据内容属性特征

特征描述	特征代码	特征类型
登陆是否成功	Logged_in	离散型
超级用户权限是否获得	Root_shell	离散型
Shell 命令使用次数	Num_shells	连续性
尝试失败次数	Failed_logins	连续性
Root 用户访问次数	Num_Root	连续性
隐私数据访问次数	Hot	连续性
目标主机连接百分比	Srv_diff_host－rate	连续性
服务连接百分比	Diff_srv_rate	连续性

以上述数据包字段解析后的数据基本与内容属性特征为基础，对多传感器运行态势数据进行清洗、集成、变换与融合等预处理，以此来提高多传感器运行态势数据整体质量。

初始多传感器运行态势评估指标数量较多，并且评估指标之间存在着重叠现象[9]，因此利用皮尔森相关系数对评估指标之间的相关性进行衡量，表达式为：

$$\rho(x_i,x_j)=\frac{\mathrm{cov}(x_i,x_j)}{\sigma(x_i)\sigma(x_j)} \tag{4}$$

式中，$\rho(x_i,x_j)$ 为多传感器运行态势评估指标 x_i 与 x_j 之间的皮尔森相关系数，其取值范围为－1～＋1。其中，当 $\rho(x_i,x_j)$ 取值为－1 时，表明评估指标 x_i 与 x_j 呈现显著的负相关关系；当 $\rho(x_i,x_j)$ 取值为 0 时，表明评估指标 x_i 与 x_j 没有相关性；当 $\rho(x_i,x_j)$ 取值为＋1 时，表明评估指标 x_i 与 x_j 呈现显著的正相关关系；$\mathrm{cov}(x_i,x_j)$ 为 (x_i,x_j) 的协方差数值；$\sigma(x_i)$ 与 $\sigma(x_j)$ 为评估指标 x_i 与 x_j 的标准差数值。

以公式（4）计算结果 $\rho(x_i,x_j)$ 绝对值为依据，对初始多传感器运行态势评估指标进行升序排列，选取前 20 个指标作为最终的多传感器运行态势评估指标[10]，具体如表 2 所示。

表 2 多传感器运行态势评估指标示意表

一级指标	二级指标	指标方向
稳定性	流量变化率	－
	平均故障时间	－
	关键设备存活时间	＋
	数据包分布比值变化率	－
	数据流总量变化率	－
脆弱性	漏洞数量	－
	漏洞等级	－
	安全设备数量	＋
	开放端口数量	－
	拓扑结构合理度	＋
威胁性	安全报警次数	－
	安全事件发生频率	－
	流入量增长率	－
	关键设备服务种类	＋
	资源利用率	＋
容灾性	带宽	＋
	支持并发线程数量	＋
	用户访问主流网站频率	－
	防火墙等级	＋
	安全设备防御性能等级	＋

至此完成了多传感器运行态势相关信息——评估指标的确定与提取，为后续多传感器运行态势评估提供支撑。

2）多传感器运行态势评估阶段：

以上述提取的多传感器运行态势评估指标为依据，利用层次分析法确定评估指标的权重系数，通过评估指标与权重系数乘积的累加求和获取多传感器运行态势评估结果。

基于层次分析法的多传感器运行态势评估指标权重系数计算步骤如下所示：

步骤一：依据表 2 所示多传感器运行态势评估指标层次结构构建判断矩阵，表达式为：

$$\boldsymbol{A}=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & a_{ij} & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{bmatrix} \tag{5}$$

式中，$\boldsymbol{A}$ 为判断矩阵；n 为评估指标的总数量，此研究 n 取值为 20；a_{ij} 为多传感器运行态势评估指标 x_i 相对于评估指

标 x_j 的相对重要程度，取值范围为 1～9，其具体取值规则如下所示：

（1）当评估指标 x_i 与评估指标 x_j 同等重要时，a_{ij} 取值为 1；

（2）当评估指标 x_i 比评估指标 x_j 稍微重要时，a_{ij} 取值为 3；

（3）当评估指标 x_i 比评估指标 x_j 明显重要时，a_{ij} 取值为 5；

（4）当评估指标 x_i 比评估指标 x_j 强烈重要时，a_{ij} 取值为 7；

（5）当评估指标 x_i 比评估指标 x_j 极端重要时，a_{ij} 取值为 9；

（6）当评估指标 x_i 与评估指标 x_j 的关系介于上述两种情况之间时，a_{ij} 取值为 2、4、6 或者 8。

步骤二：以步骤一构建的判断矩阵 $\boldsymbol{A}$ 为基础，获取其最大特征值，以此为基础计算一致性指标数值，验证判断矩阵是否符合一致性标准[11]。一致性指标计算公式为：

$$\Gamma=\frac{\lambda_{\max}(\boldsymbol{A})-n}{n-1} \tag{6}$$

式中，Γ 为一致性指标数值；$\boldsymbol{\lambda}_{\max}$（$\boldsymbol{A}$）为判断矩阵的最大特征值。

当公式（6）计算结果 Γ 大于或者等于 0.1 时，表明判断矩阵不符合一致性标准，需要对其进行一定的调整；当公式（6）计算结果 Γ 小于 0.1 时，表明判断矩阵符合一致性标准[12-13]。

步骤三：以通过一致性检验的判断矩阵为依据，计算多传感器运行态势评估指标的权重系数，表达式为：

$$\omega_i=\frac{\sum_{j=1}^{n}a_{ij}\rho(x_i,x_j)}{\Gamma\lambda_{\max}(A)}+\varepsilon_i \tag{7}$$

式中，ω_i 为多传感器运行态势评估指标 x_i 对应的权重系数；$\sum_{j=1}^{n}a_{ij}$ 为判断矩阵第 i 列元素的总和；ε_i 为权重系数调整项，决定着权重系数计算的精准度。

以上述评估指标权重系数的计算结果为依据，结合提取的多传感器运行态势评估指标数据，获取多传感器运行态势评估结果，表达式为：

$$\begin{cases}\zeta_t=\sum_{i=1}^{n}\omega_i\zeta x_i\\ \begin{cases}\zeta\leqslant\alpha^{\Delta} & \text{网络运行态势异常}\\ \zeta>\alpha^{\Delta} & \text{网络运行态势正常}\end{cases}\end{cases} \tag{8}$$

式（8）中，ζ 为多传感器运行态势评估结果；α^{Δ} 为多传感器运行态势判定阈值，需要根据研究多传感器的实际静态特性，如零点误差、灵敏度情况进行设定。

上述过程完成了多传感器运行态势的评估，为后续多传感器运行态势预测提供便利。

3）多传感器运行态势预测阶段：

多传感器运行态势预测阶段是态势感知技术的核心环节，选取支持向量机作为多传感器运行态势预测手段。基于支持向量机构建多传感器运行态势预测模型，具体如图 2 所示。

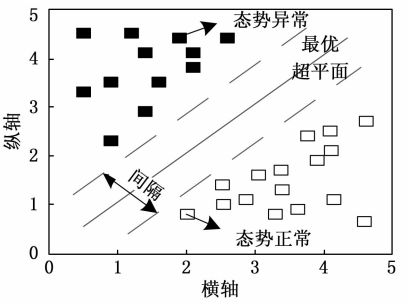

图 2　多传感器运行态势预测模型示意图

如图 2 所示，支持向量机中的最优超平面数学形式表示为

$$\beta^{\circ}\times\zeta_t+B=1 \tag{9}$$

式中，β° 为支持向量机最优超平面的斜率；B 为最优超平面最大分类间隔。

依据多传感器运行态势历史数据预测下一时刻的多传感器运行态势评估结果，表达式为：

$$\zeta'_{t+1}=\frac{b_1\zeta_1+b_2\zeta_2+\cdots+b_t\zeta_t}{t\times\chi^3} \tag{10}$$

式中，ζ'_{t+1} 为下一时刻多传感器运行态势评估数值预测结果；$\zeta_1,\zeta_2,\cdots,\zeta_t$ 为多传感器运行态势历史数据；$b_1,b_2,\cdots,b_t$ 为多传感器运行态势历史数据 $\zeta_1,\zeta_2,\cdots,\zeta_t$ 对应的系数；t 为历史数据对应的总时间；χ^3 为多传感器运行态势预测差分参量。

将公式（10）获得的下一时刻多传感器运行态势评估数值预测结果 ζ'_{t+1} 代入至支持向量机——公式（9）中，通过最优超平面的精准分类即可获得下一时刻多传感器态势感知结果（异常或者正常）[14]。

上述过程完成了多传感器态势感知技术的设计，能实时获得下一时刻多传感器态势感知结果（预测阶段），为隐私数据防篡改机制的控制提供依据，为隐私数据查询提供了必要的背景信息。

1.3.2　多传感器隐私数据识别与编码机制

通过多传感器态势感知技术提供的实时多传感器状态信息和背景信息，可以更好地理解和评估多传感器运行环境，为隐私数据查询提供依据，从而提高数据查询的准确性和安全性。在多传感器运行环境中，并不是每个数据均具备隐私属性，因此将多传感器信息划分为隐私数据与非隐私数据两个类别[15]。非隐私数据具备公开性，不需要对其篡改行为作出响应与管理。但是，多传感器运行环境中隐私数据与非隐私数据没有明显的分界线。为了方便后续隐私户数防篡改功能的实现，此节深入分析隐私数据特性，以此为基础，识别隐私数据，制定隐私数据查询编码，具体如下所示。

1）隐私数据特性分析：

从本质角度出发，多传感器态势信息隐私数据指的是用户（组织或者个人）在应用物联网、云计算、互联网等信息技术时，产生的信息或者数据，主要包括身份信息、证件信息、健康数据、客户信息、财务数据等。隐私数据若是发生被篡改的现象，会对用户个人、企业的生产与生活带来严重的不利影响[16]。

根据已有文献研究成果可知，度量隐私数据的 3 个特性分别为机密性、可用性与完整性。其中，机密性是隐私数据的关键特性，主要是按照数据拥有者需求对其进行一定的保密措施，其他用户在没有授权的背景环境下无法获取隐私数据。传感系统必须具有预防隐私数据非授权访问与获取的功能；可用性指的是隐私数据能够提供既定功能，不受时间、空间与传感系统故障、操作等影响，使得传感系统能及时响应用户需求的隐私数据服务；完整性指的是隐私数据必须保障自身信息的精确、安全与有效，其不受人为因素的影响，也不能接受未授权第三方的修改[17]。

为了方便后续隐私数据识别，将隐私数据特性——机密性、可用性与完整性数据化，明确隐私数据机密性、可用性与完整性的最小阈值，记为 $C_{\min}$ 、$U_{\min}$ 与 $I_{\min}$（由于研究篇幅的限制，不对隐私数据特性最小阈值确定过程进行过多的赘述），为后续隐私数据判定提供依据。

2）隐私数据查询程序制定：

基于上述确定的隐私数据机密性、可用性与完整性最小阈值 $C_{\min}$ 、$U_{\min}$ 与 $I_{\min}$ 为依据，结合多传感器态势感知信息实际情况，制定隐私数据识别程序，具体如下所示：

步骤一：将整个多传感器运行环境划分为 N 个识别单元，每个识别单元均由多个节点与一个存储节点构成。为每个隐私数据节点编码，使其具有唯一的 ID 号[18]。依据上述描述将识别单元记为：

$$Q=\{S_i,K,\zeta'_{t+1}\} \tag{11}$$

式中，S_i 为 ID 号为 i 的节点；K 为存储节点。

步骤二：节点时间保持松散同步，节点数据识别结果两次提交的时间间隔为 ΔT ，识别范围为 $[p,q]\in\psi$ ，则隐私数据一维识别结果表示为：

$$R_m=\{Q,\Delta T,[p,q]\} \tag{12}$$

步骤三：设置在时间间隔 ΔT 内节点识别多传感器数据次数为 m 次，即可获得 m 个一维多传感器隐私数据识别结果，表达式为：

$$S_i=\{\Delta T,(R_1,R_2,\cdots,R_m)\} \tag{13}$$

步骤四：获取一维多传感器数据识别结果中所有数据的特性数值，依据一维识别出的多传感器隐私数据结果 S_i 的总数量，制定隐私数据判定规则，去除成冗余和重叠信息，保留隐私数据，剔除非隐私数据，并对保留下的隐私数据进行重新整合，获得最终隐私数据识别结果，表达式为：

$$Y=\{S_iy_1,S_iy_2,\cdots,S_iy_l\} \tag{14}$$

式中，l 为最终识别结果中隐私数据 y 的总数量。至此实现了多传感器隐私数据的识别，以确保只有授权用户能够访问和查询特定的隐私数据，为隐私数据防篡改机制提供了精准的目标。

1.3.3 分段加密下实现隐私数据防篡改

为了确保数据在查询过程中没有被篡改，需要基于上节获得的隐私数据识别结果，制定动态防篡改机制，根据实际情况调整防篡改策略和措施，提高隐私数据的安全性。由于多传感器运行环境是处于实时变化的，制定的隐私数据防篡改机制也需要是动态的[19-20]。依据多传感器态势信息隐私数据的防篡改需求，制定动态防篡改机制，具体如下所示：

步骤一：实时获取多传感器态势感知结果 ζ'_{t+1} 。当多传感器运行态势正常时，关闭动态防篡改机制；当多传感器运行态势异常时，开启动态防篡改机制，转至步骤二；

步骤二：依据特性数值对多传感器态势信息的隐私数据进行查询，获取隐私数据查询结果 $Y=\{S_iy_1,S_iy_2,\cdots,S_iy_l\}$ ；

步骤三：获取隐私数据的用户码集合 u 与注册码集合 r ，采用分解函数 G 对其进行分段处理；

步骤四：应用第一组用户码、注册码与 Hash 数值对隐私数据第一个单元块进行加密处理，并将结果反馈给控制器；

步骤五：触发下一个单元块的加密程序，计算加密密钥，执行加密程序；

步骤六：重复执行步骤五，直至隐私数据所有单元块均执行完加密程序为止。当隐私数据出现被篡改现象时，及时发出警报并恢复被篡改内容，与此同时，加强隐私数据防篡改机制的强度。

通过上述过程实现了多传感器隐私数据的防篡改功能，最大限度地保护了隐私数据的安全，为传感系统的后续发展提供一定的帮助。

2 实验与结果分析

在 500 平方米的封闭厂房内，高度约 2.5 m，Tc-th-nb01 无线温湿度传感器测量范围 $-20\sim+50$ ℃，精度 ±0.5 ℃；Tc-th-11 温湿度传感器测量范围 0～100%，精度 ±3%；BH1750FVI 数字光强传感器测量范围 0～1 000 Lx，精度 ± 10 Lx；PMS1003 空气质量传感器测量范围 0～1 000 ppm，精度 ±10 ppm。

使用 Arduino UNO 板，Raspberry Pi 微控制器，温度传感器接口为 A0，湿度传感器接口为 A1，光传感器接口为 A2，空气质量传感器接口为 A3，每分钟采集 20 次数据。使用 Python 编程语言进行数据处理和统计分析。

选取改进区块链的防篡改方法、基于数据挖掘的防篡改方法与基于信息隐藏的数据防篡改方法作为对比方法 1、对比方法 2 与对比方法 3，联合提出方法共同进行多传感器隐私数据防篡改对比实验，以此来验证提出方法的应用

性能。

2.1　多传感器运行态势评估指标权重系数确定

提出方法引入了多传感器态势感知技术，其应用过程中需要多传感器运行态势评估指标权重系数具体数值的参与。为了方便后续实验的顺利进行，在实验进行之前确定 20 个最终多传感器运行态势评估指标的权重系数，具体如表 3 所示。

表 3　多传感器运行态势评估指标权重系数表

一级指标	权重系数	二级指标	权重系数
稳定性	0.24	流量变化率	0.02
		平均故障时间	0.05
		关键设备存活时间	0.07
		数据包分布比值变化率	0.04
		数据流总量变化率	0.06
脆弱性	0.31	漏洞数量	0.06
		漏洞等级	0.01
		安全设备数量	0.03
		开放端口数量	0.09
		拓扑结构合理度	0.13
威胁性	0.19	安全报警次数	0.02
		安全事件发生频率	0.03
		流入量增长率	0.06
		关键设备服务种类	0.03
		资源利用率	0.05
容灾性	0.26	带宽	0.09
		支持并发线程数量	0.04
		用户访问主流网站频率	0.02
		防火墙等级	0.06
		安全设备防御性能等级	0.05

如表 3 内容所示，多传感器运行态势评估指标权重系数计算结果符合 $\sum_{i=1}^{n}\omega_i = 1$ 规则，表明权重系数计算的精度较高，满足提出方法多传感器隐私数据防篡改实验进行需求。

2.2　实验环境搭建

选取某局域传感系统作为实验对象，包括计算机、TP-Link Archer C7 路由器和 Cisco Catalyst 2960 交换机。部署 Ethereum 区块链平台并配置节点和智能合约，使用 Weka 对多传感器隐私数据进行特征提取和分析，通过 OpenStego 对无线共享多传感器数据进行信息隐藏和提取。随机选取距离较近的 10 个节点作为多传感器信息获取入口，其具体环境如图 3 所示。

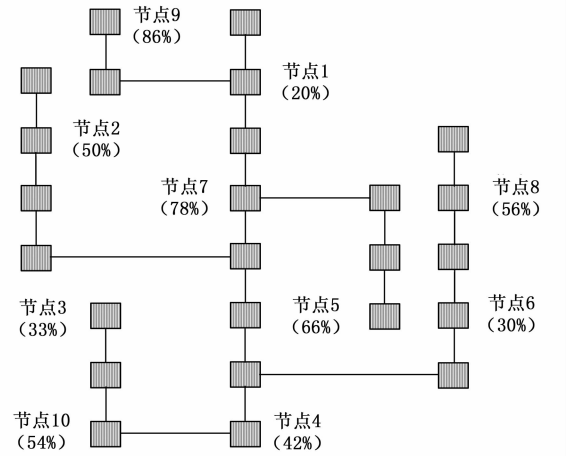

图 3　实验环境示意图

如图 3 所示，选取的 10 个节点位置是随机的，编号也是随机，后面标注的数值表示的是网路节点隐私数据的占比数值，表明每个节点隐私数据情况均不一致，满足提出方法应用性能测试需求。

2.3　实验结果分析

依据上述确定的多传感器运行态势评估指标权重系数与搭建的实验环境为基础，进行多传感器隐私数据防篡改对比实验。为了直观显示提出方法的应用性能，选取防第三方篡改机制响应时间与单元块触发次数作为评价指标，具体实验结果分析过程如下所示。

防第三方篡改机制响应时间指的是多传感器态势感知异常到防篡改机制开启之间的时间间隔，该时间越短，表明防第三方篡改机制响应速度越快，隐私数据防篡改性能越佳。通过实验获得防第三方篡改机制响应时间如图 4 所示。

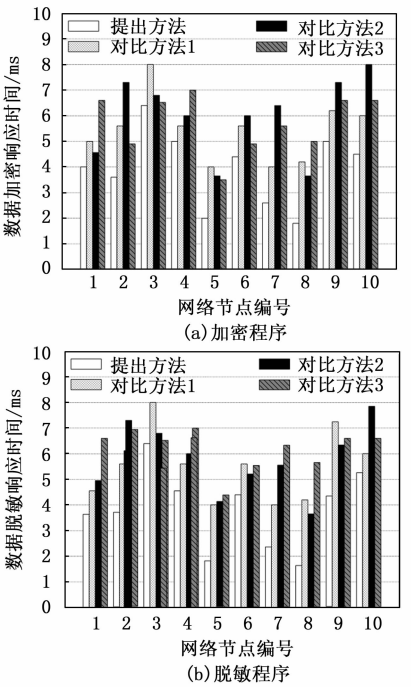

图 4　防第三方篡改机制响应时间示意图

如图 4 所示，在不同节点环境下，应用提出方法获得的防第三方篡改机制响应时间均低于对比方法 1、对比方法 2 与对比方法 3，说明在加密程序中，应用提出方法能够更快速地响应多传感器态势感知异常，提高了隐私数据的防篡改性能，而在节点 8 处，应用提出方法获得了最小的响

应时间为 1.8 s，进一步证实了该方法具备较好的响应速度。脱敏程序同理。这是因为通过提取、评估和预测多传感器运行态势，准确地获取下一时刻的多传感器态势感知结果。将该提前预测的结果应用于动态调整防篡改机制中，缩短了响应时间。

单元块触发次数指的是隐私数据出现被篡改现象时，单元块开启次数。通过实验获得单元块触发次数如图 5 所示。

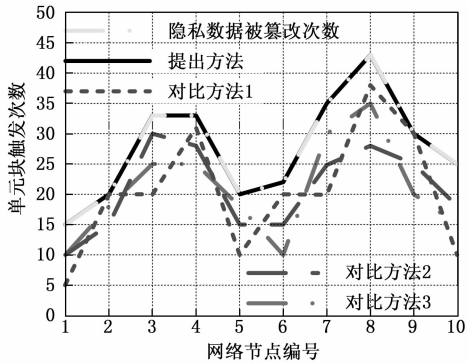

图 5 单元块触发次数示意图

如图 5 所示，在不同节点环境下，应用提出方法获得的单元块触发次数与隐私数据被篡改次数保持一致，说明每次隐私数据被篡改现象发生时，提出方法制定动态防篡改机制均会及时响应，最大限度保障隐私数据的安全。而对于对比方法 1、对比方法 2 与对比方法 3 获得的单元块触发次数均低于隐私数据被篡改次数，说明对比方法 1、对比方法 2 与对比方法 3 防篡改机制存在不响应现象，致使隐私数据被篡改。这是因为预测了多传感器运行态势结果后，深入分析了隐私数据的特性，保证在每次隐私数据被篡改时，动态防篡改机制都能够及时响应。

3 结束语

随着多传感器建设规模的加大和用户规模的扩大，多传感器病毒的种类和数量也在不断增长，隐私数据被篡改的风险急剧上升，成为制约多传感器发展的关键因素。故提出多传感器态势信息隐私数据防篡改方法研究，并得出以下结论：

1）缩短了隐私数据防篡改机制的响应时间，即在多传感器态势感知异常发生后，防篡改机制能够更快速地启动。说明系统能够更及时地检测到隐私数据的异常情况并做出相应的防护措施，减少了隐私数据被篡改的风险。

2）防篡改机制响应次数与隐私数据被篡改次数相同。说明每次隐私数据被篡改时，防篡改机制都能够及时响应并采取相应的措施，保护隐私数据的完整性和安全性。与对比方法相比，该方法的防篡改机制更加灵敏和准确，能够更好地应对隐私数据被篡改的风险。

提出方法能够及时发现并防止隐私数据的篡改，为多传感器态势信息隐私数据防篡改提供更加有效的方法保障，也为相关研究提供一定的借鉴作用。

参考文献：

[1] 高 珍，张国伟. 改进区块链的移动网络敏感数据防篡改仿真 [J]. 计算机仿真，2023，40 (3)：409－412.
[2] 杨修玮. 基于数据挖掘的网络隐私数据防篡改方法研究 [J]. 信息技术与信息化，2021，261 (12)：112－114.
[3] 刘淑艳，李丽芬. 基于信息隐藏的无线共享网络数据防篡改方法 [J]. 兵器装备工程学报，2022，43 (4)：265－270.
[4] 沈 逸，周纯杰，胡晓娅，等. 面向工业互联网中数据不透明性的隐私保护控制策略设计 [J]. 中国科学：技术科学，2022，52 (1)：152－164.
[5] 傅江辉. 基于云计算的社交网络安全隐私数据融合方法 [J]. 济南大学学报：自然科学版，2021，35 (1)：29－33.
[6] 王政辉. 计算机网络空间安全态势感知技术发展探索——评《网络空间安全防御与态势感知》 [J]. 中国安全科学学报，2021，31 (10)：199－199.
[7] 张 亮，屈 刚，李慧星，等. 智能电网电力监控系统网络安全态势感知平台关键技术研究及应用 [J]. 上海交通大学学报，2021，55 (s2)：103－109.
[8] 丁朝晖，张 伟，杨国玉，等. 工业控制系统网络攻击预测技术研究 [J]. 电子技术应用，2023，49 (1)：86－90.
[9] 杨 宇，谷宇恒. 网络安全态势感知综述 [J]. 科学技术与工程，2022，22 (34)：15011－15019.
[10] 徐 全，雷金勇，袁智勇. 基于同步量测的配网态势感知技术在新型电力系统中应用与展望 [J]. 南方电网技术，2023，17 (1)：136－143.
[11] 葛磊蛟，李元良，陈艳波，等. 智能配电网态势感知关键技术及实施效果评价 [J]. 高电压技术，2021，47 (7)：2269－2280.
[12] 赵振营. 意识形态视角下网络舆情态势感知方法研究 [J]. 情报科学，2023，41 (1)：152－157.
[13] 肖 白，周文凯，姜 卓. 基于孤立森林，模态分解和神经网络的空间负荷态势感知 [J]. 电力系统自动化，2022，46 (18)：190－198.
[14] 朱 骁，杨 庚. 横向联邦学习中 PCA 差分隐私数据发布算法 [J]. 计算机应用研究，2022，39 (1)：236－239.
[15] 潘 雪，袁凌云，黄敏敏. 主从链下的物联网隐私数据跨域安全共享模型 [J]. 计算机应用研究，2022，39 (11)：3238－3243.
[16] 贾若男，王晰巍，范晓春. 社交网络用户个人信息安全隐私保护行为影响因素研究 [J]. 现代情报，2021，41 (9)：105－114.
[17] 王 征，朱 光. 政务数据治理中的弱隐私信息追踪监测模型研究 [J]. 情报杂志，2022，41 (11)：151－156.
[18] 吉 斌，昌 力，朱丽叶，等. 区块链系统节点私钥泄露的电力数据防篡改方法与验证机制设计 [J]. 电力自动化设备，2021，41 (12)：87－94.
[19] 胡柏吉，张晓娟，李元诚，等. 支持多功能的 V2G 网络隐私保护数据聚合方案 [J]. 通信学报，2023，44 (4)：187－200.
[20] 夏秀峰，尹伯阳，刘向宇，等. 面向时空特性的社会网络个性化隐私保护算法 [J]. 小型微型计算机系统，2022，43 (10)：2200－2204.