边缘计算场景下无线传感器网络信息轻量级加密算法

邓 喆[1] 吴亚洁[1]
DENG Zhe WU Yajie

摘 要 边缘计算环境中的无线传感器网络通常在设备端附近产生的计算，直接面对大量原始涉及设备的敏感信息，面对海量信息当前加密方法没有区分信息种类，导致加密成本过高。提出边缘计算场景下无线传感器网络信息轻量级加密算法。利用贝叶斯网络结构，将边缘计算场景中的无线传感器网络海量信息划分为敏感信息和载体信息两种类型。设计一种轻量级加密算法，只对敏感信息进行加密，并将加密后的敏感信息随机嵌入载体信息中，实现无线传感器网络信息的智能隐藏。实验结果表明，利用所提算法将敏感信息嵌入载体信息后，载体信息的不可感知性较高，可以避免隐藏信息被恶意攻击者发现，保证了边缘计算场景中无线传感器网络信息的安全。

关键词 边缘计算；无线传感器网络；敏感信息；智能隐藏算法

doi：10.3969/j.issn.1672-9528.2024.01.034

0 引言

随着物联网技术的快速发展，无线传感器网络具有智能化、自组织化和低功耗等特点为各个领域带来了许多便利和优势，已经被广泛应用于环境监测、智能交通、智能家居、农业生产等领域。然而，随着无线传感器网络普及和应用范围的扩大，也带来了一些安全问题。恶意攻击者可能会窃取传感器节点采集的数据，甚至篡改网络的通信内容，造成信息泄露和拒绝服务攻击等威胁。为了解决上述问题，相关的信息隐藏技术引起了学者的广泛关注。如罗佳等人[1]利用量子生成对抗网络（quantum generative adversarial network，QGAN）设计一种信息隐藏方案，解决了量子图像信息检测过程的不安全问题。秦川等人[2]研究了一种构造式文本信息隐藏算法，可以在保证生成文本质量的基础上提升信息隐藏容量。张敏情等人[3]针对图像密文域可逆信息隐藏的嵌入率低等问题，采用多项式秘密共享技术设计信息隐藏方案，增强了图像的容灾性。

边缘计算场景中的无线传感器网络是指分布在边缘设备上的一组无线传感器节点，并通过边缘计算协同处理和存储其采集到的数据。由于该网络直接面对设备，结构中的不可控节点产生的信息众多，极易被外界恶意攻击者所攻击，导致网络中通信传输的信息出现泄露，进一步影响整个网络结构的数据安全，所以在无线传感器网络信息通信传输过程中，需要做好信息隐藏，避免有效信息被恶意篡改。无线传感器网络通常面临信道噪声、数据篡改等多种干扰和攻击威胁。为保证其在恶劣环境下依旧稳定运行，防止敌对方破解或修改隐藏数据，本文提出了一种边缘计算场景下无线传感器网络信息轻量级加密算法，为进一步推动无线传感器网络的广泛应用和发展做出贡献。

1 边缘计算场景下的无线传感器网络信息分类

无线传感器网络涉及大量的数据生成和传输。在边缘计算环境中，传感器节点会产生大量的数据，并将其传输给边缘设备进行处理和存储。面向庞大的数据量，为更好地管理和组织数据，提高隐藏算法的效率和性能，首先对无线传感器网络中通信传输的信息做分类处理，从而确定待隐藏的信息对象。

针对无线传感器网络中通信传输的信息特征，本文将其划分为敏感信息与常规信息这两种类型，其中以敏感信息为待隐藏信息，常规信息为载体信息。为实现无线传感器网络敏感信息与常规载体信息的准确、高效分类，本文引入了贝叶斯网络[4]，该网络结构是一种基于概率的分类器，假设 x、y 为两个随机无线传感器网络信息，当信息 y 出现的同时信息 x 出现的概率为 $P(x|y)$。在贝叶斯网络结构中[5]，如果信息 x 属于常规载体信息空间，信息 y 属于敏感信息空间，且这两种空间的全并集为无线传感器网络中通信传输的全部信息，则无线传感器网络信息分类的贝叶斯概率为：

$$P(y_i|x)=\frac{P(x|y_i)P(y_i)}{\sum_{i=1}^{I}P(x|y_i)P(y_i)} \quad (1)$$

1. 贵阳职业技术学院信息科学系 贵州贵阳 550081

式中：$P(y_i|x)$ 表示无线传感器网络信息分类的贝叶斯概率，也就是第 i 个随机信息 y_i 已经出现的基础上，随机信息 x 出现的概率；$P(y_i)$ 表示第 i 个随机信息 y_i 出现的概率；I 表示信息总量。

根据得到的贝叶斯概率 $P(y_i|x)$，设定一个分类阈值为 λ，根据阈值 λ，将后验概率大于或等于阈值的样本归为常规信息，而将后验概率小于阈值的样本归为敏感信息。具体判定的过程为：当 $P(y_i|x) \geq \lambda$ 时，将无线传感器网络信息判定为常规信息 a，当 $P(y_i|x) < \lambda$ 时，将无线传感器网络信息判定为敏感信息 b。

2 无线传感器网络敏感信息轻量级加密算法设计

边缘计算环境中的无线传感器网络包含的个人健康信息、用户位置等敏感信息，未经适当保护的敏感信息可能被滥用、泄露或用于非法活动，对个人造成严重损害 [6-7]。因此，为了保护隐私，本文设计了一种轻量级加密算法，在信息隐藏前对其进行加密处理。

轻量级加密算法主要通过一个由 S 盒替换层和 P 置换层组成的基础密码结构进行的加密，所以将第 1 部分分类信息中的无线传感器网络敏感信息加密主要分为三层。

第一层是与轮密钥异或，表达式为：

$$b_i \to b_i \oplus m_i \tag{2}$$

式中：b_i 表示第 i 个加密信息；m_i 表示第 i 个轮密钥；$\oplus$ 表示异或运算。

第二层是 S 盒替换层，即将上一层加密后的敏感信息进行 S 盒变换，变换后输入第三层。

第三层是 P 置换层，置换规则为：

$$W(j)=\begin{cases}\dfrac{j\cdot 16 \bmod 63}{b_i}, 0 \leq j \leq 62\\ 63, j=63\end{cases} \tag{3}$$

式中：$W(j)$ 表示无线传感器网络敏感信息经过 64 位置换后的新位置；j 表示加密数据的位数。经过以上三层的运算处理后，即可完成边缘计算场景下无线传感器网络敏感信息的轻量级加密，得到加密信息 $b_i^* = b_i \oplus W(j)$。

3 加密信息的智能隐藏

根据上述过程对边缘计算场景下无线传感器网络敏感信息进行加密后，可以防止敏感信息在传输、存储或处理过程中受到非法获取或窃听的风险。即使信息被加密 [8-9]，仍然可能有其他方法来破解或解密。因此，为了进一步降低信息泄露和风险，本文设计一种敏感信息随机嵌入的智能隐藏算法。具体流程如下文所示。

根据上述内容对无线传感器网络敏感信息进行了分类与加密后，利用阈值矩阵将加密后的敏感信息进行稀疏化处理，表达式为：

$$F_j^{'} = \frac{\gamma_{j\times j}\varepsilon F_j}{b_i^*} \tag{4}$$

式中：F_j、$F_j^{'}$ 分别表示稀疏化处理前、后的无线传感器网络载体信息第 j 个列向量；$\gamma_{j\times j}$ 表示大小为 $j\times j$ 的频域上的近似稀疏矩阵；ε 表示无线传感器网络节点生成的阈值矩阵。

在获得加密后无线传感器网络敏感信息的稀疏化处理结果后，经过简单的矩阵线性运算 [10]，即可将敏感信息嵌入到载体信息中，从而形成隐藏后的目标信息，表达式为：

$$B_j = F_j^{'} + \eta M_j \tag{5}$$

式中：B_j 表示无线传感器网络敏感信息隐藏后所得目标信息；η 表示尺度调节因子，主要用于规避敏感信息嵌入对载体信息的影响；M_j 表示加密后的无线传感器网络敏感信息。经过式（5）运算后，即可将无线传感器网络敏感信息加密嵌入常规的载体信息中，从而实现敏感信息的智能隐藏，降低敏感信息被外界攻击者发现的可能性。

4 实验与分析

4.1 实验准备

本章主要对边缘计算场景下无线传感器网络信息智能隐藏算法的性能进行评估，首先需要做好实验准备工作。在 TinyOS 平台环境下，采用 802.11 无线网络协议，搭建一个图 1 所示的边缘计算场景下无线传感器网络场景用于承载信息隐藏算法。

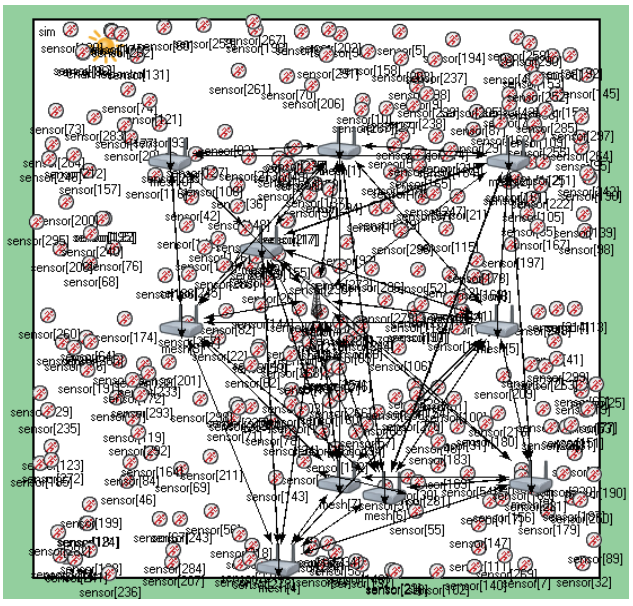

图 1 边缘计算场景下无线传感器网络场景

图 1 所示的无线传感器网络中设置了 110 个字节的广播数据包作为待隐藏的敏感信息，本次实验中，为避免实验结果的偶然性，对原始实验数据做分组处理，如表 1 所示。

表 1 实验隐藏信息分组

组别	敏感信息类型	字节数 / 个	一次信息长度 / 位
数据组 1	个人身份信息	2	8
数据组 2	银行账户信息	4	8
数据组 3	医疗健康信息	6	8
数据组 4	商业机密	8	8
数据组 5	企业财务信息	10	8
数据组 6	政府敏感信息	12	16
数据组 7	地理位置信息	14	16
数据组 8	工业控制系统信息	16	16
数据组 9	私人通信内容	18	16
数据组 10	媒体版权信息	20	16

基于上述实验数据，本章以所提信息隐藏算法为实验组，并以文献 [1] 基于量子生成对抗网络的信息隐藏算法、文献 [2] 的基于多项式秘密共享的信息隐藏算法为对照组。在模拟环境下，选用数值型数据作为无线传感器网络隐藏信息的载体信息，分别采用实验组与对照组算法将实验隐藏信息一一嵌入载体信息中，全部隐藏后统计并整理各算法下的嵌入结果，对比分析所提算法的性能。

4.2 保真度分析

保真度是衡量隐藏后无线传感器网络敏感信息的保持程度。在信息隐藏过程中，需要确保常规信息载体在隐藏秘密信息后仍然保持原始信息的相似性和质量，较高的保真度表示隐藏对信息产生的破坏较小。所提方法的保真度分析结果如图 2 所示。

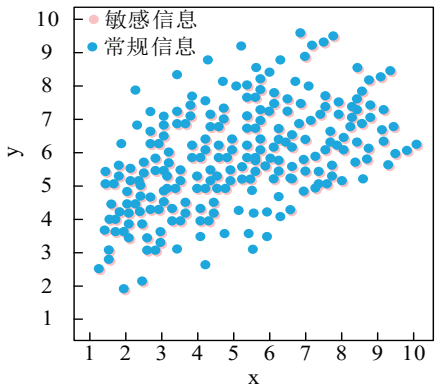

图 2 无线传感器网络信息隐藏保真度结果

由图 2 可知，所提方法可以将表 1 中不同数据组的无线传感器网络敏感信息嵌入到常规信息中，基本没有出现漏嵌入问题。

比特错误率（bit error rate，BER）是衡量无线传感器网络敏感信息隐藏后的数据包中与原始数据包不同的比特数量的指标。为了进一步量化保真度实验结果，以比特错误率为指标进行计算。依据公式 BER= 错误比特数 / 总比特数，得到所提方法的保真度结果为 0.4%，比特错误率较低，即接近于无误差的情况，证明了所提方法信息隐藏效果较好。

4.3 均方误差分析

考虑到在敏感信息嵌入边缘计算场景下无线传感器网络过程中，势必会影响载体信息的质量，所以该组实验主要以载体信息的不可感知性作为实验指标。该指标主要描述的是载体信息质量明显变化的特性，属于定性描述指标，而均方误差可以通过定量的方式来衡量无线传感器网络载体信息的失真程度，所以均方误差常被作为不可感知性的评价指标，其计算公式为：

$$MSE=\frac{1}{N}\sum_{n=1}^{N}\left(Z^{'}(n)-Z(n)\right)^{2} \tag{6}$$

式中：MSN 表示无线传感器网络中载体信息的均方误差；$Z(n)$、$Z^{'}(n)$ 分别表示无线传感器网络敏感信息嵌入前、后的载体信息数据值，其中 n=1,2,…,N；N 表示载体信息的字节数。

在利用实验组算法与对照组算法进行无线传感器网络信息隐藏之后，分别统计各算法下载体信息的不可感知性，具体实验结果如图 3 所示。

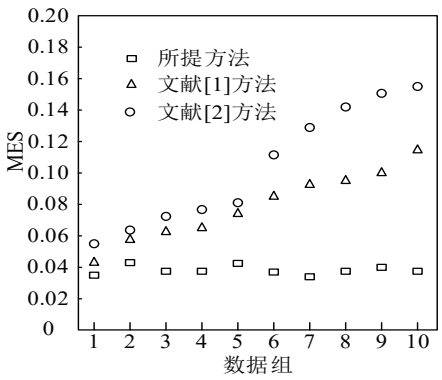

图 3 无线传感器网络信息隐藏均方误差对比结果

从图 3 中可以看出，在无线传感器网络载体信息中嵌入了敏感信息之后，无论是实验组算法还是对照组算法，载体信息的不可感知性均出现下降的现象，其中在对照组的两种算法下，载体信息不可感知性随数据规模的不断增大而显著下降，也就是嵌入的敏感信息规模越大，载体信息的失真程度越大，而在所提算法下，载体信息不可感知性一直处于较为稳定的状态，维持在可接受的范围内，利用所提算法将敏感信息嵌入隐藏在载体信息后，载体信息的均方误差小于 0.04，较对照组算法最小值更低。由此可以说明，采用所提算法将无线传感器网络的敏感信息嵌入到载体信息后，即使遭受到外界的恶意攻击，由于载体信息的不可感知性极高，信息质量未出现明显变化，所以恶意攻击者很难掌握敏感信息的具体数据值和嵌入位置，也就是无线传感器网络的敏感信息隐藏效果良好。

一种高性能 Web 内容安全监管系统

张 玲[1] 王 喜[1] 张 立[1]
ZHANG Ling WANG Xi ZHANG Li

摘 要 Web 内容安全保障主要是保护大型政府门户网站、新闻网站发布的公告和新闻等内容的安全。这类 Web 网站发布的内容是社会舆情引导的重要组成部分，如果被恶意篡改将会引发严重的后果。针对这一类问题，提出一种 Web 内容安全监管系统。系统从内容监管、权限审核、核心词表与关联模式定义三方面实现对 Web 内容审计与管控，融合了被动与主动两种安全保护的方式，并能与内容发动审核流程紧密联合。所提出的系统相对于其他同类系统具有高性能、高安全保障性的特点。

关键词 Web 内容安全；内容监管；高性能；监管系统；门户网站

doi：10.3969/j.issn.1672-9528.2024.01.035

0 引言

目前我国社会信息化程度已相对较高，绝大多数的政府部门、事业单位都有自己的门户网站。这些网站会发布一些非常重要的公众信息，包括各类公告、宣布事项等。这些网站是社会公众及时了解事态、权威信息的重要渠道，也是社会宣传、引导社会舆情的重要组成部分。这类网站发布的内容具有重要的社会意义，必须要保证其发布内容的权威性与可靠性。但是，经常看到这些网站受到黑客的攻击，或由于发布审核流程出现问题，引发舆情事故。分析这类事故产生的原因，主要有以下三个方面。

（1）内容未及时更新与维护。大部分门户网站经过长期的运营，积累了大量的信息内容，如果网站的内容没有建

1. 泰州市气象局 江苏泰州 225300

5 结语

无线传感器网络的信息隐藏算法是保护数据安全的重要手段之一，本文在边缘计算场景下研究了无线传感器网络信息轻量级加密算法。首先通过贝叶斯网络对网络信息进行分类，从而识别出敏感信息作为待隐藏信息；然后再利用轻量级加密技术对待隐藏信息进行了加密处理，并将加密后的信息嵌入到常规载体信息中；最后，设计了敏感信息随机嵌入的智能隐藏算法，使得敏感信息在正常情况下无法被察觉，有效防止了未经授权的访问和窃取。

参考文献：

[1] 罗佳，周日贵，李尧翀，等．基于量子生成对抗网络的信息隐藏方案 [J]. 计算机辅助设计与图形学学报，2021, 33(7): 983-990.
[2] 秦川，李蓉受，钱振兴，等．基于宋词生成的大容量构造式信息隐藏算法 [J]. 计算机学报，2023,46(1):17-30.
[3] 张敏情，王泽曦，柯彦，等．基于多项式秘密共享的图像密文域可逆信息隐藏 [J]. 电子与信息学报，2022,44(12):4337-4347.
[4] 龚健虎，张跃进．深度 AWB 结合改进 DIT 的高效大数据分类 [J]. 计算机工程与设计，2021,42(2):468-474.
[5] 吴家皋，郭亚航，蔡沈磊，等．基于多时间段优化贝叶斯网络的车载容迟网络路由算法 [J]. 通信学报，2021, 42(12): 109-120.
[6] 刘政，代培培，邢建平，等．面向嵌入式设备的轻量级 AES 加密通讯系统的设计与实现 [J]. 电子器件，2023, 46(1): 29-35.
[7] 李玮，刘春，谷大武，等 .Saturnin-Short 轻量级认证加密算法的统计无效故障分析 [J]. 通信学报，2023,44(4):167-175.
[8] 温文媜，邹孟雷，方玉明，等．面向医学图像加密域大容量信息隐藏与认证方法 [J]. 中国图象图形学报，2023, 28(3): 716-733.
[9] 吕海翠，郭玲．数据库敏感信息可变保序加密安全算法研究 [J]. 计算机仿真，2021,38(9):301-305.
[10] 罗宇，郭家松．大位宽情况下的回滚式循环冗余校验算法 [J]. 电子与信息学报，2021,43(4):1057-1063.

【作者简介】

邓喆（1989—），女，贵州铜仁人，硕士，讲师，研究方向：计算机应用技术、大数据技术、网络安全。

吴亚洁（1983—），女，天津蓟县人，硕士研究生，讲师，研究方向：电子信息。

（收稿日期：2023-10-17）