DOI:10.11918/202504063

融合信任值和身份标识验证的节点复制攻击检测策略

滕志军[1,2],苗润升[2],孙铭阳[3],李纪奇[2],赵立权[1,2]

(1.现代电力系统仿真控制与绿色电能新技术教育部重点实验室(东北电力大学),吉林 132012;
2.东北电力大学 电气工程学院,吉林 132012;3.中国电信股份有限公司吉林分公司,长春 130022)

摘 要:为抵御无线传感器网络中的节点复制攻击,保障网络的安全与稳定,本文提出了一种融合信任值和身份标识验证的节点复制攻击检测策略(node replication attack detection strategy integrating node creditworthiness and identity authentication, NRADS-NC&IA)。该方法首先建立模糊综合信任评价模型,在直接信任模块中引入信誉维护函数、异常弱化因子及奖惩因子,综合通信属性、数据属性、网络属性和物理属性影响因素计算待评估节点的直接信任值,并采用滑动时间窗口机制实现节点信任值的动态更新,有效提升评估的时效性与准确性,在此基础上应用支持度函数评估节点可信度,从而有效过滤节点的欺骗行为得到更为可靠的节点间接信任值,最终的节点综合信任值由直接信任值与间接信任值加权求和得到;采用动态自适应阈值筛选可疑节点,并在可疑节点中进行节点ID比对,以确定副本节点。仿真实验表明,NRADS-NC&IA在无需依赖节点空间位置信息的情形下,静态和移动无线传感器网络的检测率保持在97%和94%以上,具有较强的环境适应性,可有效应对复杂动态环境中的无线传感器网络安全问题。

关键词:无线传感器网络;信任值;身份标识验证;节点复制攻击;模糊权重
中图分类号:TN92 **文献标志码**:A **文章编号**:0367-6234(2026)05-0063-10

Node replication attack detection strategy integrating node creditworthiness and identity authentication

TENG Zhijun[1,2], MIAO Runsheng[2], SUN Mingyang[3], LI Jiqi[2], ZHAO Liquan[1,2]

(1. Key Laboratory of Modern Power System Simulation and Control & Renewable Energy Technology, Ministry of Education (Northeast Electric Power University), Jilin 132012, China;
2. School of Electrical Engineering, Northeast Electric Power University, Jilin 132012, China;
3. China Telecom Corporation Limited Jilin Branch, Changchun 130022, China)

Abstract: To defend against node replication attacks in wireless sensor networks and maintain network security and stability, this paper proposes a node replication attack detection strategy integrating node creditworthiness and identity authentication (NRADS-NC&IA). The approach begins by establishing a fuzzy comprehensive trust evaluation model. In the direct trust module, reputation maintenance function, anomaly attenuation factor and reward and punishment factor are introduced. The direct trust value of the node to be evaluated is calculated by comprehensively considering the influencing factors of communication attributes, data attributes, network attributes and physical attributes. A sliding time window mechanism is adopted to dynamically update node trust value, significantly enhancing the timeliness and accuracy of the evaluation. On this basis, a support function is applied to evaluate the credibility of nodes, effectively filtering out the deceptive behaviors of nodes and obtaining more reliable indirect trust values of nodes. The final comprehensive trust value of nodes is derived from the weighted summation of its direct and indirect trust values. Dynamic adaptive thresholds are adopted to screen suspicious nodes, and node ID comparisons are conducted among the suspicious nodes to obtain the determined replica nodes. Simulation results show that NRADS-NC&IA achieves detection rates of over 97% and 94% in static and mobile wireless sensor networks without relying on the spatial position information of nodes. The strategy exhibits strong environmental adaptability and can effectively deal with the security problems of wireless sensor networks in complex dynamic environments.

Keywords: wireless sensor network; trust value; identity verification; node replication attack; fuzzy weight

收稿日期:2025-04-22;**录用日期**:2025-09-04;**网络首发日期**:2025-10-11
网络首发地址:https://link.cnki.net/urlid/23.1235.T.20251010.1333.002
基金项目:国家自然科学基金青年科学基金(61501107)
作者简介:滕志军(1973—),男,教授,硕士生导师
通信作者:赵立权,230666801@qq.com

21 世纪开始,无线通信、集成电路、传感器和数字电子等技术的发展促进了基于大量传感器节点协同工作组成的无线传感器网络(wireless sensor networks,WSNs)的快速发展[1],其广泛用于环境监测、灾害预警、智慧城市等物联网的数据感知阶段。无线传感器网络具有无标度特性,传感器节点通常被部署在开放且无人监管的环境中[2],极易遭受攻击,造成整个网络瘫痪[3],需要通过识别及检测不可信节点来确保自身安全,应对各种潜在攻击,并进行准确数据分析和预测[4]。节点复制攻击是一种常见的攻击方式,攻击者试图捕获传感器节点并提取加密信息,生成副本节点后进一步引入内部攻击,而这些副本很难去除,对整个网络造成巨大威胁[5]。

针对节点复制攻击的检测机制,目前大多集中在静态网络中,基于位置信息和身份信息采用分布式检测法或混合检测法进行识别。周晖等[6]提出基于分簇的节点复制攻击入侵检测方案,结合集中检测和分布检测,在分簇网络中利用簇头和基站传递节点的地理位置和 ID 信息。马锐等[7]提出了基于位置声明信息的分布式节点复制攻击检测方案,通过多重映射机制实现对单一证人节点的验证,但若副本节点不产生声明信息则无法检测该副本节点。Rani 等[8]提出基于唯一身份和定位的副本节点检测,其采用定位技术检测副本节点,需要精准的节点地理位置信息,具有自身局限性。

无线传感器网络并非始终保持静态,对于移动网络中的节点复制攻击检测,Mojtaba 等[9]提出基于看门狗节点的三步机制检测副本节点,看门狗节点监视网络流量并侦听信道,利用邻居信息进行副本节点检测,存在检测效率与资源消耗的矛盾。李峰等[10]提出了一种针对移动异构无线传感器网络的密钥管理策略,利用节点移动前后的位置数据、时间戳及速度上限等识别节点复制攻击。Ebrahim 等[11]提出了一种分布式签名协议,使用签名生成、交换和验证机制来检测移动网络中具有相同 ID 的副本节点,但其检测效率可能受网络规模和节点密度的限制,导致较大的通信开销和延迟。

在利用信任模型检测节点复制攻击方面,Rikli 等[12]提出了一种基于信任的集中式模型检测异常行为,收集与邻居通信相关的统计数据以执行信任功能。Amudha 等[13]提出了一种结合位置信息和信任的检测方法,用于识别无线传感器网络中的节点复制攻击。Anitha 等[14]提出了 SACOP 算法,利用直接和间接信任评估模型对节点的信任值进行估计,从而识别出网络中的副本节点,但间接信任评估模型中无过滤欺骗节点。

目前,对于节点复制攻击的检测方案存在以下问题:1)在实际应用场景中,准确获取每个节点的位置信息难度较大,且采用定位算法及 GPS 定位存在能耗,应设计不依赖节点位置信息的检测方案;2)对于移动网络的节点复制攻击检测存在显著的资源消耗及对位置信息的高依赖性等;3)信任体现主观看法,而现存方案在评判指标体系的构建上多存在单一性,针对复杂的攻击后果需要更客观全面的评判指标体系。

针对上述问题,本文提出了一种融合信任值和身份标识验证的节点复制攻击检测策略 NRADS-NC&IA。建立了模糊综合信任评价模型,计算待评估节点的直接信任值并引入滑动时间窗口动态更新,采用支持度函数衡量节点可信度得到间接信任值,加权求和得到综合信任值,用动态自适应阈值筛选可疑节点并进行节点 ID 比对。

1 系统模型

节点复制攻击网络拓扑图如图 1 所示,黑色实线为正常路径,红色线是节点复制攻击引发的路径和数据流变化。其中红色“·”线表示副本节点之间的虫洞隧道,红色“–”线表示副本节点吸引周围节点流量,红色粗实线表示选择性丢弃数据包、篡改数据包等异常数据流。副本节点可能引发黑洞攻击、虫洞攻击、DOS 攻击、选择性转发攻击以及数据异常等,而对于这些攻击后果可以通过转发指数、邻居节点数、数据发送率、处理延迟、剩余能量、信号强度等指标来检测。

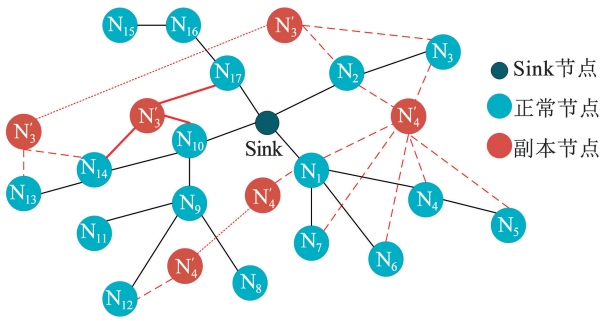

图 1 节点复制攻击网络拓扑图

Fig. 1 Topology of the node replication attack network

检测节点复制攻击的核心思想是确定哪些节点拥有相同 ID,而检查所有节点会消耗大量能量且效率低。因此,本文采用经典的无线传感器网络架构,其中 Sink 节点作为信息汇总中心,资源充裕且具备高度安全性,可保障与网络中节点通信而不受干扰。普通节点则在其通信覆盖范围内实现双向交互通信,利用最短路径算法将采集的数据高效传输至

Sink 节点[15]，建立信任模型并基于节点信任阈值筛选出可疑节点，最终在可疑节点名单中进行身份验证，拥有相同 ID 的节点即被判定为副本节点。

2　信任评估模型

2.1　直接信任

2.1.1　通信行为信任

由于 WSN 部署环境特殊，网络中存在一定的入侵因素，Ganeriwal 等[16]提出了一种适用于资源受限无线传感器网络的信誉评估机制（reputation-based framework for sensor networks，RFSN），利用贝叶斯公式与 Beta 分布对信誉分布进行拟合，通过计算其期望值来得到节点的信任值。然而原始的贝叶斯信任模型忽略了节点故障、环境干扰等异常因素的影响，可能导致很高的误检率。为解决这一问题，引入异常弱化因子，以减少因网络内部故障触发的误报行为检测；加入信任维护函数和奖惩因子，并在直接信任中对异常数据进行过滤，对原有信任模型进行调整。

利用 Beta 分布[17]对节点的信任进行拟合，信任分布符合 Beta($\alpha+1,\beta+1$)。用信任分布的统计期望来表示节点的通信行为信任 $\mathrm{DTB}_{ij}(t)$，其计算公式为：

$$\mathrm{DTB}_{ij}(t)=\frac{\omega\alpha_{ij}+1}{\omega\alpha_{ij}+\lambda\omega\beta_{ij}+2}\times\mathrm{RP} \tag{1}$$

$$\omega=\frac{\theta}{\alpha_{ij}+\beta_{ij}} \tag{2}$$

$$\lambda=\frac{F_i}{F_{\mathrm{d}}} \tag{3}$$

$$\mathrm{RP}=\frac{\alpha_{ij}}{\alpha_{ij}+\varepsilon\beta_{ij}} \tag{4}$$

$$\varepsilon=\frac{\alpha_{ij}+\rho_{ij}}{\alpha_{ij}} \tag{5}$$

式中：α_{ij}为节点 i 与节点 j 的历史正常通信次数；β_{ij}为节点 i 与节点 j 的历史异常通信次数；ω 为信任维护函数，作用是维护现阶段节点行为对信任值的影响，并削弱历史行为；θ 为固定维护值，用来设定维护函数的作用范围，参考 TS-BRS 模型将参数 θ 取值为 150[18]。$\lambda\in[0,1]$为异常弱化因子；F_i为因入侵因素导致的节点异常通信次数；F_{d}为网络中异常通信总次数。RP 为奖惩因子，用于激励正面行为，惩罚负面行为；与静态网络相比，移动网络多存在突发性异常，$\varepsilon(\varepsilon>1)$为突发性异常惩罚权重，对突发性异常行为设置额外惩罚权重，其中 ρ_{ij}为节点 i 与节点 j 的历史突发性异常通信次数，使其均适用于静态和移动网络。

分析节点收集的数据，基于数据的一致性和相关性采用异常数据筛选机制过滤异常数据[19]，若某节点收集数据 x_i 与其邻节点收集数据 x_j 的差值小于数据异常允许误差阈值 A_{th}，则该节点被视为正常；反之，则视为异常。节点数据异常允许误差阈值 A_{th} 的计算公式为

$$A_{\mathrm{th}}=\frac{1}{|N_i|}\sum_{j\in N_i}\left|x_j-\frac{x_i+\sum_{j\in N_i}x_j}{|N_i|+1}\right| \tag{6}$$

式中：N_i为节点 i 邻居节点的集合，$|N_i|$为节点 i 邻居节点个数。若通信行为正常且数据误差在允许范围则为成功交互，否则为异常交互。

2.1.2　模糊权重

由于节点复制攻击中的副本节点会进一步引入许多内部攻击，因此需要更客观全面的评判指标体系。本文在信任模型的输入中综合考虑了多种因素，其权重采用层次分析法及模糊综合评价[3]加以确定，旨在对复杂的攻击后果进行全面评估。为确保评判指标体系的客观性，对多种信任要素进行分层处理，以减少单次权重涉及的信任要素数目，并可防止因信任要素过多而引起权重分配系数偏低的情况。

结合无线传感器网络的特点，建立系统的梯阶层次结构，使用多层级模糊综合评价机制分析每个信任因素，实现对每个节点信任评估的准确性和公平性的多维评价，信任要素层次结构如图 2 所示。

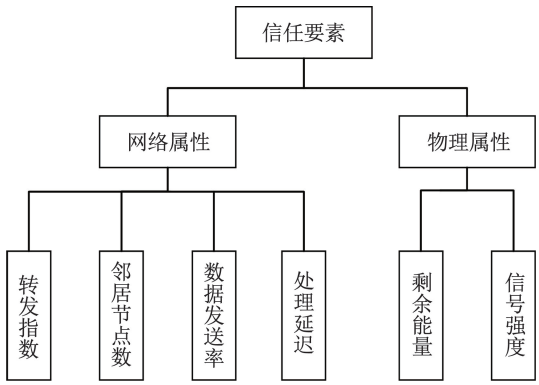

图 2　信任要素层次结构

Fig. 2　Hierarchy structure of trust factors

建立信任因素集：一级信任因素集 $U=\{U_1,U_2\}$，其中 U_1 和 U_2 分别表示网络属性和物理属性；二级信任因素集 $U_1=\{U_{11},U_{12},U_{13},U_{14}\}$，其中 U_{1m}（$m=1,2,3,4$）分别表示转发指数、邻居节点数、数据发送率、处理延迟，$U_2=\{U_{21},U_{22}\}$，其中 U_{2p}（$p=1,2$）分别表示剩余能量和信号强度；建立信任评判集 $E=\{e_1,e_2,e_3,e_4\}$，e_n（$n=1,2,3,4$），其中 e_1 代表不可信，e_2 代表低可信，e_3 代表中可信，e_4 代表高可信。

建立权重分配模糊向量：一级权重分配模糊向量 $\boldsymbol{A}=\{a_1,a_2\}$，且 $a_1+a_2=1$，采用三标度法[3]判断各节点信任要素的相对重要性，建立判断尺度表，可求得 $a_1=0.75$，$a_2=0.25$；建立二级权重分配模糊向量 $\boldsymbol{A}_1=\{a_{11},a_{12},a_{13},a_{14}\}$，$\boldsymbol{A}_2=\{a_{21},a_{22}\}$，采用三标度法建立判断尺度表，可求得 $a_{11}=0.564$，$a_{12}=0.263$，$a_{13}=0.118$，$a_{14}=0.055$，$a_{21}=0.75$，$a_{22}=0.25$。

各因素归一化到[0,1]后，将评价因素作为输入变量，代入梯形隶属度函数，得到隶属度矩阵 $\boldsymbol{R}$，图 3 展示了梯形隶属度函数。

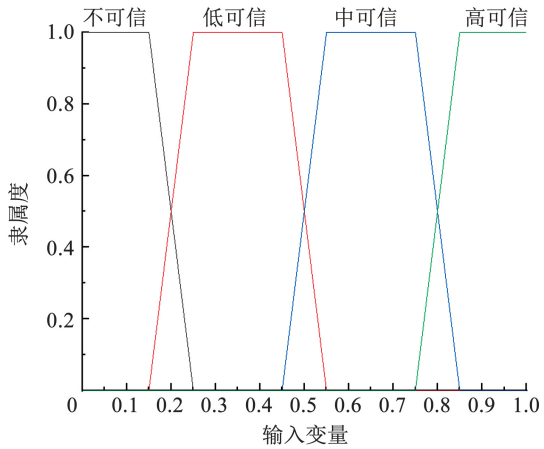

图 3 梯形隶属度函数图

Fig. 3 Ladder membership function diagram

二级模糊综合评判：建立单因素评价矩阵，对网络属性 U_1 和物理属性 U_2 的二级因素进行模糊评判，分别得到隶属度矩阵 $\boldsymbol{R}_1$ 和 $\boldsymbol{R}_2$，如公式(7)、(8)所示。

$$\boldsymbol{R}_1=\begin{bmatrix} r_{111} & r_{112} & r_{113} & r_{114} \\ r_{121} & r_{122} & r_{123} & r_{124} \\ r_{131} & r_{132} & r_{133} & r_{134} \\ r_{141} & r_{142} & r_{143} & r_{144} \end{bmatrix} \tag{7}$$

$$\boldsymbol{R}_2=\begin{bmatrix} r_{211} & r_{212} & r_{213} & r_{214} \\ r_{221} & r_{222} & r_{223} & r_{224} \end{bmatrix} \tag{8}$$

式中：r_{1mn} 为网络属性 U_1 中的第 m 个二级指标对评价集 E 中 e_n 的隶属度，r_{2pn} 为物理属性 U_2 中的第 p 个二级指标对评价集 E 中 e_n 的隶属度。

分别将隶属度矩阵 $\boldsymbol{R}_1$ 和 $\boldsymbol{R}_2$ 与评价权重集合 $\boldsymbol{A}_1$ 和 $\boldsymbol{A}_2$ 做模糊合成运算，得到的二级模糊综合评价结果向量 $\boldsymbol{B}_1$ 和 $\boldsymbol{B}_2$ 分别为：

$$\boldsymbol{B}_1=A_1\circ\boldsymbol{R}_1=(b_{11}\quad b_{12}\quad b_{13}\quad b_{14}) \tag{9}$$

$$\boldsymbol{B}_2=A_2\circ\boldsymbol{R}_2=(b_{21}\quad b_{22}\quad b_{23}\quad b_{24}) \tag{10}$$

式中：“∘”为模糊综合评判中的合成算子，b_{1n} 为网络属性 U_1 对评价集 E 中 e_n 的隶属度，b_{2n} 为物理属性 U_2 对评价集 E 中 e_n 的隶属度。

一级模糊综合评判：合成 $\boldsymbol{B}_1$ 和 $\boldsymbol{B}_2$，并与一级权重分配模糊向量 $\boldsymbol{A}$ 做模糊合成运算，得到一级模糊综合评价结果向量 $\boldsymbol{B}$ 为

$$\boldsymbol{B}=A\circ\begin{pmatrix}\boldsymbol{B}_1\\ \boldsymbol{B}_2\end{pmatrix}=(b_1\quad b_2\quad b_3\quad b_4) \tag{11}$$

式中 b_n 为被评价节点整体对评价集 E 中 e_n 的隶属度。

节点的直接信任 $\mathrm{DT}_{ij}(t)$ 计算公式为

$$\mathrm{DT}_{ij}(t)=\frac{\sum_{n=1}^{4}c_nb_n}{\sum_{n=1}^{4}b_n}\mathrm{DTB}_{ij}(t) \tag{12}$$

式中 c_n 为信任等级，根据模糊向量单值法将评价集 E 中 e_1、e_2、e_3、e_4 的 4 个信任等级进行定义[17]，分别为 $c_1=0.1$，$c_2=0.35$，$c_3=0.65$，$c_4=0.9$。

2.1.3 信任值更新

为了突显信任值本身具有的动态性和时效性，增强节点近期交互结果对整体信任评估的影响，采用时间滑动窗口机制[20]更新节点信任值。如图 4 所示，时间窗口的大小设为 d 个交互周期，用于记录节点近期的交互数据。

图 4 时间滑动窗口

Fig. 4 Time sliding window

使用指数衰减函数对时间窗内的每一个时间槽赋予权值，得到新的信任值：

$$\mathrm{DT}_{ij}(t\_\mathrm{new})=\sum_{h=1}^{d}\chi_h\mathrm{DT}_{ij}(t\_h) \tag{13}$$

式中：χ_h 为以 h 为时间槽索引的权重，$\mathrm{DT}_{ij}(t\_h)$ 为相对应时间槽的信任值，$h=1,2,\cdots,d$。权重 χ_h 的计算公式为

$$\chi_h=\frac{\mathrm{e}^{-\kappa(d-h)}}{\sum_{h=1}^{d}\mathrm{e}^{-\kappa(d-h)}} \tag{14}$$

式中：κ 为指数衰减系数，$(d-h)$ 为时间槽 h 相对于窗口终止点的偏移量。

2.2 间接信任

节点 i 为了得到被评估节点 j 的间接信任值，向两者的公共邻居节点(即推荐节点)广播查询信息。而推荐节点本身也可能存在不可信的现象，为了提高推荐信任评估的可靠性和准确性，本文利用支持

度函数计算推荐节点传递数值的偏差情况，并为各推荐节点分配相应的权重。当节点 i 收到来自多个推荐节点的直接信任值时，根据每个推荐节点的权重对这些信任值进行加权平均，从而得到对节点 j 的间接信任值。

支持度函数用于量化两个节点之间的相似性或接近程度，由于 Sigmoid 函数的平滑性和可调整性，本文选择 Sigmoid 函数作为支持度函数 sup 的具体形式，原始 Sigmoid 函数为

$$\sup(\mathrm{DT}_{fj}(t),\mathrm{DT}_{gj}(t)) = 2\times e^{\frac{-1}{|\mathrm{DT}_{fj}(t)-\mathrm{DT}_{gj}(t)|+c}} - 1 \tag{15}$$

其中推荐节点 = {节点 1、…、节点 f、节点 g、…、节点 q}，参数 c 是一个足够小的正常数，用于避免分母为零导致的计算中断。两个推荐节点得到的直接信任差异越大，支持度绝对值越小；直接信任差异越小，支持度绝对值越大。因此推荐节点 f 的综合支持度 $\sup_f$ 计算公式为

$$\sup_f = \sum_{l=1}^{q}\sup(\mathrm{DT}_{fj}(t),\mathrm{DT}_{lj}(t)) \tag{16}$$

推荐节点的综合支持度越小，信任程度就越低，计算间接信任时将此类推荐节点筛掉，因此设置阈值 τ_{th}，将综合支持度 $\sup_f$ 大于 τ_{th} 的推荐节点滤除，设筛掉此类节点后的推荐节点集合为集合 C，推荐节点 f 仍属于集合 C。

根据综合支持度计算归一化权重 w_f 计算公式为

$$w_f = \frac{\sup_f}{\sum_{f\in C}\sup_f} \tag{17}$$

综合上述公式，计算间接信任值 $\mathrm{IT}_{ij}(t)$ 为

$$\mathrm{IT}_{ij}(t) = \sum_{f\in C} w_f \times \mathrm{DT}_{if}(t) \times \mathrm{DT}_{fj}(t) \tag{18}$$

2.3　信任积聚

为得到更客观且全面的信任评估，本文采用基于权重的积聚方式[21]计算综合信任，并采用变异系数法分别为直接信任和间接信任分配动态权重 φ_1、φ_2。基于数据的内在变异性（即离散程度）自动调整权重，数据离散程度越大，权重越高。综合信任 $\mathrm{CT}_{ij}(t)$ 计算公式为

$$\mathrm{CT}_{ij}(t) = \varphi_1\mathrm{DT}_{ij}(t) + \varphi_2\mathrm{IT}_{ij}(t) \tag{19}$$

假设有 n 个节点，分别计算变异系数 $\mathrm{CV_d}$、$\mathrm{CV_{ind}}$，计算公式如下：

$$\mathrm{CV_d} = \frac{\sqrt{\frac{1}{n}\sum_{j=1}^{n}\left(\mathrm{DT}_{ij}(t) - \frac{1}{n}\sum_{j=1}^{n}\mathrm{DT}_{ij}(t)\right)^2}}{\frac{1}{n}\sum_{j=1}^{n}\mathrm{DT}_{ij}(t)} \tag{20}$$

$$\mathrm{CV_{ind}} = \frac{\sqrt{\frac{1}{n}\sum_{j=1}^{n}\left(\mathrm{IT}_{ij}(t) - \frac{1}{n}\sum_{j=1}^{n}\mathrm{IT}_{ij}(t)\right)^2}}{\frac{1}{n}\sum_{j=1}^{n}\mathrm{IT}_{ij}(t)} \tag{21}$$

采用 Softmax 函数，通过参数 τ 控制权重的平滑程度。为了既不过于尖锐地放大变异系数的差异，也不过于平滑地抹平差异，选择 $\tau = 0.5$ 作为适中的缩放程度，有助于在综合信任计算中保持不同信任源的相对重要性，得到 φ_1、φ_2 计算公式如下：

$$\varphi_1 = \frac{e^{\frac{\mathrm{CV_d}}{\tau}}}{e^{\frac{\mathrm{CV_d}}{\tau}} + e^{\frac{\mathrm{CV_{ind}}}{\tau}}} \tag{22}$$

$$\varphi_2 = \frac{e^{\frac{\mathrm{CV_{ind}}}{\tau}}}{e^{\frac{\mathrm{CV_d}}{\tau}} + e^{\frac{\mathrm{CV_{ind}}}{\tau}}} \tag{23}$$

最终得到综合信任值 $\mathrm{CT}_{ij}(t)$ 为

$$\mathrm{CT}_{ij}(t) = \frac{e^{\frac{\mathrm{CV_d}}{\tau}}}{e^{\frac{\mathrm{CV_d}}{\tau}} + e^{\frac{\mathrm{CV_{ind}}}{\tau}}}\mathrm{DT}_{ij}(t) + \frac{e^{\frac{\mathrm{CV_{ind}}}{\tau}}}{e^{\frac{\mathrm{CV_d}}{\tau}} + e^{\frac{\mathrm{CV_{ind}}}{\tau}}}\mathrm{IT}_{ij}(t) \tag{24}$$

2.4　动态阈值

为提高信誉模型在不同环境和条件下的适应性和准确性，本文采用基于聚类分析的动态阈值调整反馈机制。利用基于划分的聚类方法划分节点群体，根据节点综合信誉度划分为 k 簇，并明确 k 为 2，将节点划分为正常类和异常类。为避免局部最优和副本节点异常信誉的干扰，使用 k-mediods 来选择初始聚类中心[22]，$\mathrm{CT_{malicious}}$ 为恶意节点综合信任值，$\mathrm{CT_{normal}}$ 为正常节点综合信任值，将两类边界节点信任值的平均值作为初始阈值，初始阈值 $K_1(t)$ 计算公式为

$$K_1(t) = \frac{1}{2}\{\max[\mathrm{CT_{malicious}}(t)] + \min[\mathrm{CT_{normal}}(t)]\} \tag{25}$$

统计实际副本节点数 M 与评估副本节点数 M'，计算两者之间差值 $|M-M'|$，当差值 $|M-M'|$ 与实际副本节点数的比值大于 ξ（ξ 取极小值）时，启动反馈机制来动态优化模型的阈值设置。得到最终阈值 $K(t)$ 后，当 $\mathrm{CT}_{ij}(t) \leqslant K(t)$ 时，节点被判定为可疑节点并列入可疑节点名单，反之则为正常节点。

3　NRADS-NC&IA 算法

在可疑节点名单中进行 ID 身份验证，有相同 ID 的节点为副本节点，NRADS-NC&IA 算法流程图如图 5 所示。

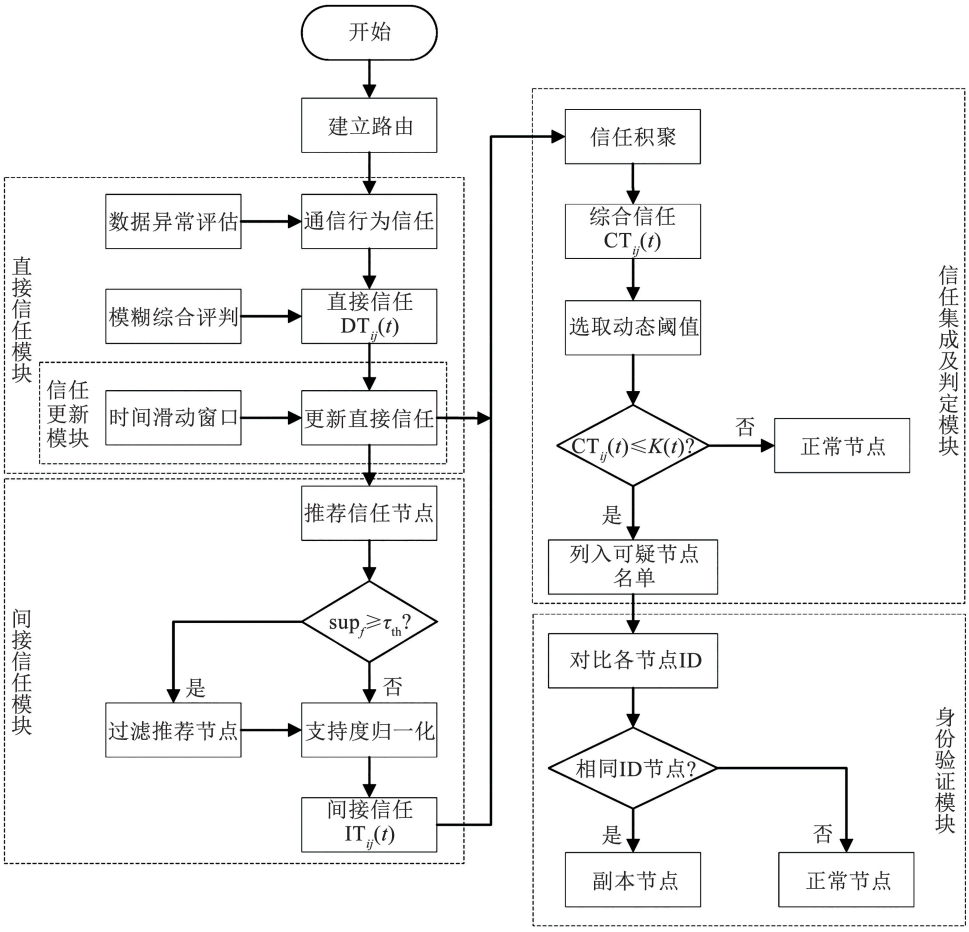

图 5 NRADS-NC&IA 算法流程图

Fig. 5 NRADS-NC&IA algorithm flow chart

NRADS-NC&IA 算法运行的主要步骤如下：

Step 1：利用最短路径算法构建全局路由，并进行通信，为后续的信任评估体系建立基础网络；

Step 2：利用 Beta 分布对节点信任进行拟合，根据公式(1)计算节点通信行为信任 $DTB_{ij}(t)$，并采用异常数据筛选机制进行数据异常评估；

Step 3：在信任模型的输入中综合考虑网络属性中的转发指数、邻居节点数、数据发送率、处理延迟和物理属性中的剩余能量及信号强度，结合层次分析法和模糊综合评判法计算直接信任 $DT_{ij}(t)$，并通过利用指数衰减函数的时间滑动窗口机制更新节点信任值；

Step 4：选定邻居节点和推荐节点，利用支持度函数计算推荐节点传递数值的偏差情况得到推荐节点的综合支持度，根据公式(18)计算节点间接信任；

Step 5：采用变异系数法分别为节点的直接信任和间接信任分配动态权重，根据公式(19)积聚信任得到综合信任 $CT_{ij}(t)$，全域综合信任发送给 Sink 节点；

Step 6：Sink 节点根据基于聚类分析的动态阈值调整反馈机制评估各节点是否可信，节点综合信任值大于阈值时被判定为正常节点，反之则为可疑节点被广播全网并列入可疑节点名单；

Step 7：筛选不受信节点加入可疑节点列表，列表内节点通过比对 ID 验证是否为副本节点。

4 仿真实验与分析

本文采用 MATLAB 来搭建仿真环境，假设无线传感器网络的覆盖范围为边长 100 m 的正方形区域，随机部署近似均匀分布的 100 个传感器节点，通信半径为 10 m，网络中普通节点正常转发数据包，副本节点以 50% ~90% 概率丢弃数据包，以 60% ~80% 概率篡改数据包，每迭代一次更新节点信任值，详细仿真参数见表 1。

表 1 仿真参数

Tab. 1 Simulation parameters

仿真区域/m	节点总数/个	通信半径/m	初始能量/J	初始信任值	数据包大小/bit	迭代次数
100 × 100	100	10	2	0.5	800	50

在网络中随机抽取不同比例的正常节点，模拟节点复制攻击场景，被捕获节点复制出多个 ID 相同副本节点，当副本节点集合为{3,6,30,45,79}，即占比 5% 时的模型图如图 6 所示。

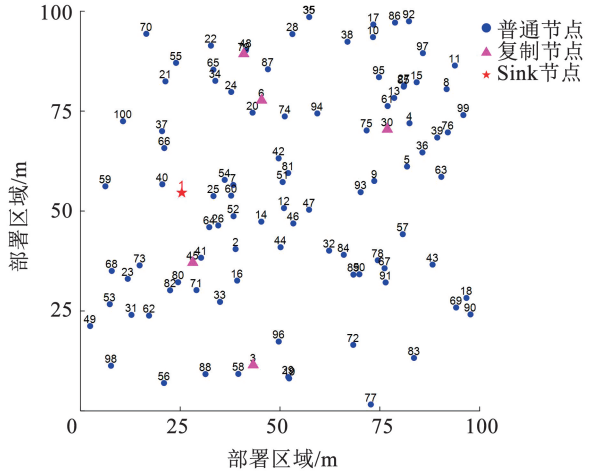

图 6　节点复制攻击模型(副本节点占比 5%)

Fig. 6　Node replication attack model (5% proportion of replica nodes)

4.1　节点信任值分析

如图 7 所示，将全域副本节点信任值在每个时间段取平均值进行可视化分析。随着迭代次数的增加(即恶意行为次数随之增加)，副本节点信任值整体呈现下降趋势，同时，随着恶意节点比例的增加，信任值的下降速度加快。

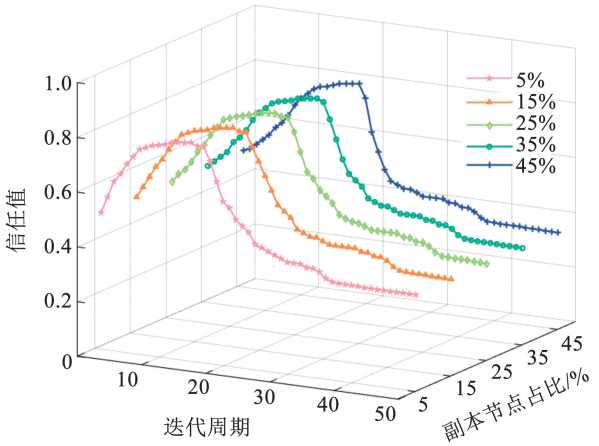

图 7　副本节点信任值变化曲线

Fig. 7　Trust value evolution curve of replica nodes

将本文提出的信任模型与 DTAM 算法[19]、ETERS 算法[23]、TSRP 算法[24]所提信任模型作比较，分析不同信任模型对正常节点和副本节点的信任值影响。

如图 8、图 9 所示，本文信任模型与文献[19]、文献[23]中信任模型均加入奖惩因子，激励正向行为、惩罚恶意行为，信任值变化速度相比文献[24]更快，而本文引入信任维护函数和异常弱化因子，是为保护节点信任值不受偶发性非入侵因素影响，给予节点信任值一定的“缓冲”，起到防止其因个别不良表现遭受过重惩罚，因此信任值下降速度较缓慢。

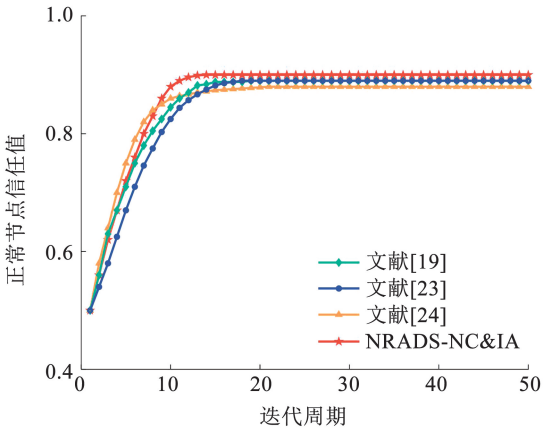

图 8　正常节点信任值对比

Fig. 8　Comparison of trust values of normal nodes

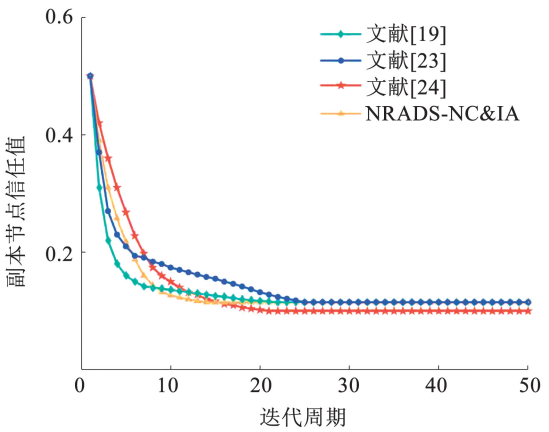

图 9　副本节点信任值对比

Fig. 9　Comparison of trust values of replica nodes

4.2　不同算法性能对比分析

4.2.1　静态网络中算法性能对比分析

将本文的 NRADS-NC&IA 算法与 SACOP 算法[14]、DTAM 算法[19]、ETERS 算法[23]、TSRP 算法[24]和组合加权 k 近邻分类算法[25]对比，证明本文算法在静态网络中的有效性。

由图 10 和图 11 结果可知，由于本文算法对副本节点行为后果有较全面的分析，在不依赖节点位置信息的同时加入欺骗过滤、异常维护等机制，使得副本节点占比增加到 45% 时检测率仍能够保持在 97% 以上，而文献[14]、[19]、[23]、[24]较为单一的评判指标在检测率和误检率方面均表现较差。文献[25]因加入节点空间位置信息，而检测率相较本文算法略高，但未考虑通信过程中的欺骗节点行为，误检率随副本节点占比增加而升高。

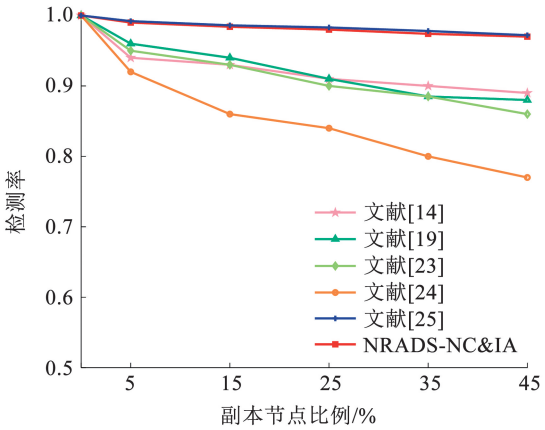

图 10 副本节点检测率

Fig. 10 Detection rate of replica nodes

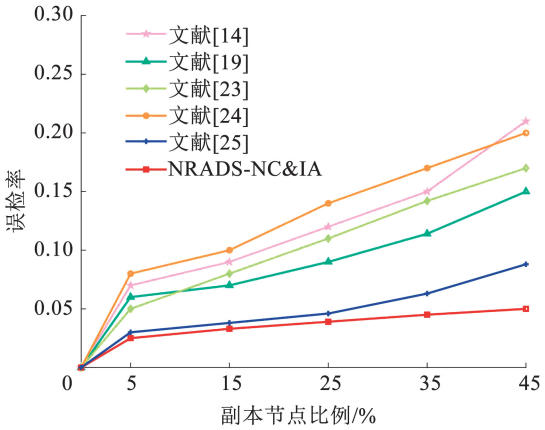

图 11 副本节点误检率

Fig. 11 False detection rate of replica nodes

图 12 为不同算法下的丢包率对比，可以看到，节点复制攻击导致的网络丢包率随副本节点占比增加而增加，由于本文提出的 NRADS-NC&IA 算法对副本节点具有高检测率，可实现较低丢包率，因而可保障网络数据包的稳定传输，有效降低了数据丢失的可能性。

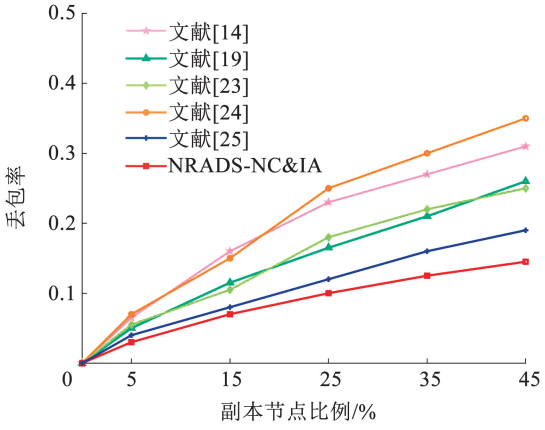

图 12 不同算法丢包率对比

Fig. 12 Comparison of packet loss rate of different algorithms

图 13 为不同算法端到端时延比较，随着网络中副本节点占比增加，副本节点发起的攻击频次增多，文献[14]、[19]、[23]、[24]检测性能下降，进而引发端到端时延的大幅上升；文献[25]虽检测率与本文算法相近，但端到端时延性能表现亦不及本文算法。

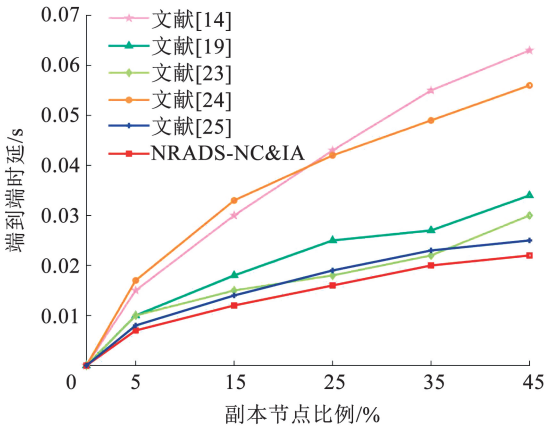

图 13 不同算法端到端时延比较

Fig. 13 Comparison of end-to-end delay of different algorithms

4.2.2 移动网络中算法性能对比分析

将本文的 NRADS-NC&IA 算法与基于邻居信息的检测算法[9]、移动异构密钥管理算法[10]和 FEC 算法[26]对比，证明本文算法在移动网络中的有效性。

由图 14 和图 15 可知，由于本文算法不依赖节点位置信息、节点速度等，因此，在移动网络能够保持较高检测率和较低误检率。

文献[9]中，若节点由于环境因素或能量消耗而减少移动，其被看门狗节点遇到的机会也会减少，导致算法对副本节点的检测率下降。若因看门狗节点的不均匀分布而频繁遇到某些节点，那么这些节点可能会被错误地认为是副本节点，导致误检率增加。文献[10]因对节点位置信息进行加密，副本节点的检测率较高，故误检率较低。文献[26]依赖节点位置信息计算节点移动速度，在检测率和误检率方面均表现较差。

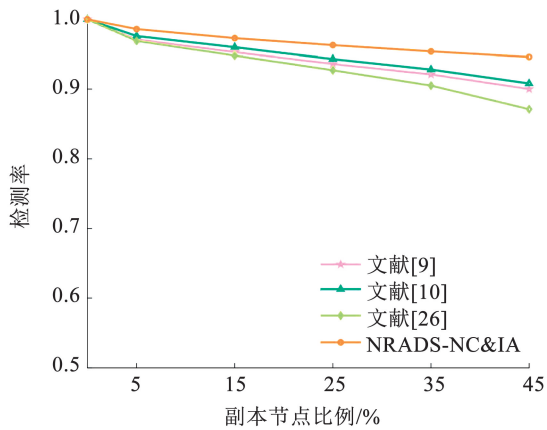

图 14 移动网络中的副本节点检测率

Fig. 14 Detection rate of replica nodes in mobile networks

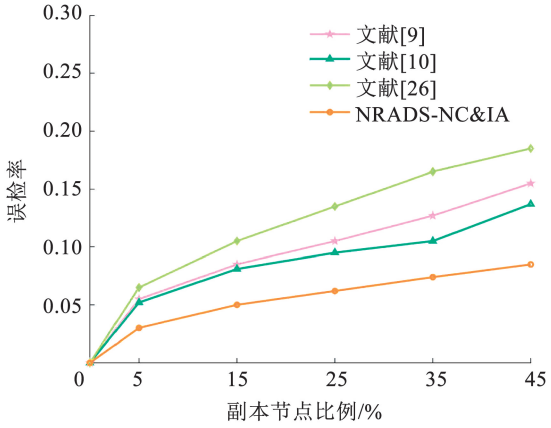

图 15　移动网络中的副本节点误检率

Fig. 15　False detection rate of replica nodes in mobile networks

图 16 和图 17 为移动网络中不同算法下的丢包率和平均剩余能量对比，可以看到，文献[9]需要看门狗节点持续监控网络流量和信道，文献[10]采用加密算法上传移动节点位置信息，文献[26]依赖节点实时的位置信息计算节点移动速度，因此在能耗方面均表现较差。本文算法通过信誉模型先筛选再判定，在移动网络中能耗较低，对副本节点具有高检测率且可实现较低丢包率。

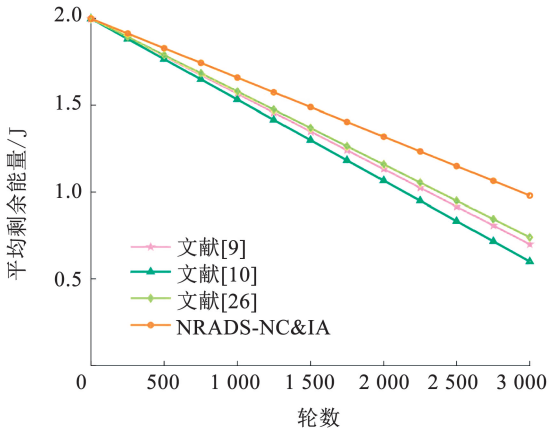

图 16　移动网络中的不同算法平均剩余能量对比

Fig. 16　Comparison of average residual energy of different algorithms in mobile networks

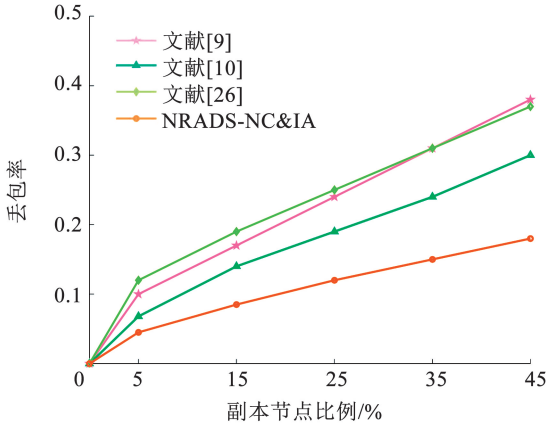

图 17　移动网络中的不同算法丢包率对比

Fig. 17　Comparison of packet loss rate of different algorithms in mobile networks

5　结　语

本文提出了一种融合信任值和身份标识验证的节点复制攻击检测策略，建立模糊综合信任评价模型，计算待评估节点的直接信任值并引入滑动时间窗口动态更新直接信任值；采用支持度函数衡量节点可信度得到间接信任值，加权求和得到综合信任值；采用动态自适应阈值筛选可疑节点并进行节点 ID 比对，从而确定副本节点。仿真实验表明，本文提出的 NRADS-NC&IA 算法建立了更客观全面的评判指标体系，在无需依赖难以获取的节点空间位置信息情形下，静态和移动网络的检测率保持在 97% 和 94% 以上，可有效应对复杂动态环境中的无线传感器网络安全问题。检测无线传感器网络节点复制攻击仍存在挑战，下一阶段将重点研究分簇式结构网络，提高副本节点识别速度，进一步降低节点能耗，优化算法性能。

参考文献

[1] ZHANG Yong, ZHANG Zhen, LIU Dengzhi, et al. Adaptive learning FOA algorithm with energy consumption balancing for coverage optimization in WSNs[J]. Ad Hoc Networks, 2025, 178: 103958. DOI :10.1016/j.adhoc.2025.103958

[2] 火久元, 杨继广, 穆聪, 等. 基于多目标徒步旅行优化的 WSN 安全成簇路由算法[J]. 兰州交通大学学报, 2025, 44(3): 29
HUO Jiuyuan, YANG Jiguang, MU Cong, et al. WSN secure clustering routing algorithm based on multi-objective hiking optimization[J]. Journal of Lanzhou Jiaotong University, 2025, 44(3): 29. DOI: 10.3969/j.issn.2096-9066.2025.03.004

[3] 姚雷, 王东豪, 梁璇, 等. 无线传感器网络多层次模糊信任模型研究[J]. 仪器仪表学报, 2014, 35(7): 1606
YAO Lei, WANG Donghao, LIANG Xuan, et al. Research on multi-level fuzzy trust model of wireless sensor network[J]. Chinese Journal of Scientific Instrument, 2014, 35(7): 1606. DOI: 10.19650/j.cnki.cjsi.2014.07.022

[4] 王晨宇, 张钊, 侯佳龙, 等. 基于密度峰值聚类和改进 LWLR 的短期电力负荷预测[J]. 东北电力大学学报, 2024, 44(4): 113
WANG Chenyu, ZHANG Zhao, HOU Jialong, et al. Short-term power load forecasting based on density peak clustering and improved LWLR[J]. Journal of Northeast Electric Power University, 2024, 44(4): 113. DOI: 10.19718/j.issn.1005-2992.2024-04-0113-08

[5] LUO Shiyao, LAI Yingxu, LIU Jing. Selective forwarding attack detection and network recovery mechanism based on cloud-edge cooperation in software-defined wireless sensor network[J]. Computers & Security, 2023, 126: 103083. DOI: 10.1016/j.cose.2022.103083

[6] 周晖, 朱立庆, 杨振, 等. 基于分簇的节点复制攻击入侵检测方法[J]. 传感器与微系统, 2014, 33(5): 129
ZHOU Hui, ZHU Liqing, YANG Zhen, et al. Intrusion detection method for node replication attacks based on clustering[J]. Transducer and Microsystems Technologies, 2014, 33(5): 129. DOI:10.13873/j.1000-97872014.05.029

[7]马锐，朱天保，马科，等. 基于单证人节点的分布式节点复制攻击检测[J]. 清华大学学报(自然科学版)，2017，57(9)：909
MA Rui，ZHU Tianbao，MA Ke，et al. Detection of distributed node replication attacks based on document holder nodes[J]. Journal of Tsinghua University (Natural Science Edition)，2017，57(9)：909. DOI：10.16511/j.cnki.qhdxxb.2017.26.039

[8]RANI T P，JAYAKUMAR C. Unique identity and localization based replica node detection in hierarchical wireless sensor networks[J]. Computers & Electrical Engineering，2017，64：148. DOI：10.1016/j.compeleceng.2017.08.010

[9]JAMSHIDI M，SHEIKH ABOOLI POOR S，ARGHAVANI A，et al. A simple，lightweight，and precise algorithm to defend against replica node attacks in mobile wireless networks using neighboring information[J]. Ad Hoc Networks，2020，100，102081. DOI：10.1016/j.adhoc.2020.102081

[10]李峰，李亚平，张志军，等. 移动场景下异构无线传感器网络密钥管理方法[J]. 数据采集与处理，2021，36(5)：1020
LI Feng，LI Yaping，ZHANG Zhijun，et al. Key management method for heterogeneous wireless sensor networks in mobile scenarios[J]. Data Acquisition and Processing，2021，36(5)：1020. DOI：10.16337/j.1004－9037.2021.05.017

[11]ALRASHED E A，KARAATA M H，HAMDAN A A. Malicious replica quarantining protocol for Mobile Wireless Sensor Networks using replica detection and identification[J]. Internet of Things，2024，27，101289. DOI:10.1016/j.iot.2024.101289

[12]RIKLI N E，ALNASSER A. Lightweight trust model for the detection of concealed malicious nodes in sparse wireless ad hoc networks[J]. International Journal of Distributed Sensor Networks，2016，12(7)：1. DOI：10.1177/1550147716657246

[13]AMUDHA G，NARAYANASAMY P. Distributed location and trust based promising detection in wireless sensor networks[J]. Wireless Personal Communications，2018，102：3303. DOI：10.1007/s11277－018－5369－2

[14]ANITHA S，JAYANTHI P，LALITHA K，et al. Secured ant colony optimization based on energy trust system for replica node attack detection[J]. International Journal on Emerging Technologies，2020，11(2)：104

[15]滕志军，于沥博，李明哲，等. 融合交互信誉度与RSSR的WSNs女巫攻击检测策略[J]. 吉林大学学报(工学版)，2025，55(7)：2455. DOI:10.13229/j.cnki.jdxbgxb.20230919
TENG Zhijun，YU Libo，LI Mingzhe，et al. WSNs witch attack detection strategy integrating interactive reputation and RSSR[J]. Journal of Jilin University (Engineering and Technology Edition)，2025，55(7)：2455. DOI:10.13229/j.cnki.jdxbgxb.20230919

[16]GANERIWAL S，BALZANO L K，SRIVASTAVA M B. Reputation-based framework for high integrity sensor networks[J]. ACM Transactions on Sensor Network，2008，4(3)：15：1. DOI：10.1145/1362542.1362546

[17]滕志军，李梦，谷金亮，等. 融合多指标的WSN动态信任评估预测模型[J]. 郑州大学学报(工学版)，2023，44(3)：76
TENG Zhijun，LI Meng，GU Jinliang，et al. Dynamic trust evaluation and prediction model for WSN integrating multiple indicators[J]. Journal of Zhengzhou University (Engineering and Technology Edition)，2023，44(3)：76. DOI：10.13705/j.issn.1671－6833.2022.06.014

[18]滕志军，郭力文，吕金玲，等. 基于时序信息分析的WSN贝叶斯信誉评价模型[J]. 郑州大学学报(工学版)，2019，40(1)：38
TENG Zhijun，GUO Liwen，LV Jinling，et al. Bayesian reputation evaluation model of WSN based on time series information analysis[J]. Journal of Zhengzhou University (Engineering and Technology Edition)，2019，40(1)：38. DOI：10.13705/j.issn.1671－6833.2019.01.007

[19]朱子豪，刘光杰. 一种面向物联网节点的动态信任评估模型[J]. 重庆理工大学学报(自然科学)，2022，36(7)：188
ZHU Zihao，LIU Guangjie. A dynamic trust evaluation model for internet of things nodes[J]. Journal of Chongqing University of Technology (Natural Science)，2022，36(7)：188. DOI:10.3969/j.issn.1674－8425(z).2022.07.024

[20]李莉，王小龙，张之欣，等. 新型电力系统分布式家庭光伏采集场景下的信任评估模型[J]. 通信学报，2023，44(7)：197
LI Li，WANG Xiaolong，ZHANG Zhixin，et al. Trust evaluation model in distributed household photovoltaic collection scenarios of the new power system[J]. Journal of Communications，2023，44(7)：197. DOI:10.11959/j.issn.1000－436x.2023137

[21]王田，张广学，蔡绍滨，等. 传感云中的信任评价机制研究进展[J]. 通信学报，2018，39(6)：37
WANG Tian，ZHANG Guangxue，CAI Shaobin，et al. Research progress of trust evaluation mechanism in sensor cloud[J]. Journal of Communications，2018，39(6)：37. DOI：10.11959/j.issn.1000－436x.2018098

[22]CHEN Xiying，LIU Caihui，LIN Bowen，et al. AHA-3WKM：The optimization of K-means with three-way clustering and artificial hummingbird algorithm[J]. Information Sciences，2024，672：120661. DOI：10.1016/j.ins.2024.120661

[23]KHAN T，SINGH K，HASAN M H，et al. ETERS：A comprehensive energy aware trust-based efficient routing scheme for adversarial WSNs[J]. Future Generation Computer Systems，2021，125：921. DOI：10.1016/j.future.2021.06.049

[24]韩优佳，胡黄水，姚美琴. 基于信任感知的无线传感器网络安全路由协议[J]. 计算机工程，2021，47(9)：145
HAN Youjia，HU Huangshui，YAO Meiqin. Trust-aware secure routing protocol for wireless sensor networks[J]. Computer Engineering，2021，47(9)：145. DOI：10.19678/j.issn.1000－3428.0058217

[25]赵晓峰，王平水. 基于组合加权k近邻分类的无线传感网络节点复制攻击检测方法[J]. 传感技术学报，2024，37(6)：1056
ZHAO Xiaofeng，WANG Pingshui. Detection method of node replication attack in wireless sensor networks based on combined weighted k-nearest neighbor classification[J]. Journal of Sensor Technology，2024，37(6)：1056. DOI:10.3969/j.issn.1004－1699.2024.06.016

[26]SUJIHELEN L，SENTHILSINGH C. Detect the replica node in mobile wireless sensor networks[C]//2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS). Piscataway：IEEE，2021：265. DOI：10.1109/ICICCS51141.2021.9432285

(编辑　吕雪梅)