传感器网络中GPS无关的轻量化反射式协同虚假数据过滤方案

刘志雄，尹辉
（长沙学院计算机科学与工程学院，湖南 长沙 410022）

摘　要：针对传感器网络中反射式协同虚假数据注入攻击的能耗激增、攻击源隐蔽问题，提出GPS无关的轻量化过滤方案——基于邻居关系的反射式协同虚假数据过滤方案（NRFFS）。新增反射行为验证与轻量机器学习（ML）特征校验模块，基于节点邻居关系构建“格式–邻居合法性–反射行为–ML特征–消息验证码（MAC）/密钥”5层过滤架构。理论分析与仿真表明，在安全阈值t = 5、密钥分区数n = 15、预存储邻居信息条目数c = 60配置下，NRFFS妥协容忍能力达178个节点，较基于地理位置的虚假数据过滤方案（GFFS）和基于邻居信息的虚假数据过滤方案（NFFS）分别提升36.9%和33.8%，能耗降低32%，存储开销为1.4 KB，适配资源受限无线传感器网络关键场景。

关键词：无线传感器网络；反射式协同攻击；虚假数据过滤；轻量机器学习；邻居关系
中图分类号：TP393.0
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2026044

GPS-independent lightweight reflective collaborative false data filtering scheme for sensor networks

Liu Zhixiong, Yin Hui
School of Computer Science and Engineering, Changsha University, Changsha 410022, China

Abstract: To solve the problems of sharp increase in energy consumption and concealed attack sources caused by reflective collaborative false data injection attacks in wireless sensor networks, a GPS-independent lightweight filtering scheme—neighbor relationship based reflective collaborative false data filtering scheme (NRFFS) was proposed. Reflective behavior and lightweight machine learning (ML) feature verification two new modules, were added and constructed a five-layer filtering architecture of “format-neighbor legitimacy-reflective behavior-ML features-message authentication code (MAC)/key” based on node neighbor relationships. Theoretical analysis and simulations show that under the configuration of security threshold t = 5, number of key partitions n = 15, and number of pre-stored neighbor entries c = 60, NRFFS achieves a compromise tolerance capacity of 178 nodes, 36.9% higher than geographical information based false data filtering scheme (GFFS) and 33.8% higher than neighbor information based false data filtering scheme (NFFS), reduces energy consumption by 32%, and features a storage overhead of 1.4 KB, which well suits the key scenarios of resource-constrained wireless sensor networks.

Keywords: wireless sensor network, reflective collaborative attack, false data filtering, lightweight machine learning, neighbor relationship

收稿日期：2025–12–28；**修回日期：**2026–02–11
通信作者：尹辉，yinh@ccsu.edu.cn
基金项目：国家自然科学基金资助项目（No.62372068）
Foundation Item：The National Natural Science Foundation of China (No.62372068)

0 引言

无线传感器网络（wireless sensor network，WSN）凭借分布式感知、自组织部署优势，广泛应用于军事侦察、环境监测等关键领域[1-2]，但节点物理防护薄弱，易被俘获沦为妥协节点[3]。攻击者可利用妥协节点发起反射式协同虚假数据注入攻击（reflective collaborative false data injection attack，RC-FDIA），操控合法节点转发虚假报告，隐蔽性强、能耗激增，是WSN核心安全瓶颈。

针对虚假数据攻击防御的研究主要包括传统虚假数据过滤[3-6]、协同攻击专用防御[7-8]、反射式攻击轻量化检测[9-20]、WSN智能抗干扰及低能耗优化[21-25]等系列方案。但现有研究仍难以同时满足GPS无关性、RC-FDIA针对性防御与资源受限节点轻量化部署三大核心需求。传统虚假数据过滤方案多依赖消息验证码（message authentication code，MAC）验证或簇结构认证实现数据合法性校验，其中统计路由过滤（statistical en-route filtering，SEF）方案[3]未绑定密钥与位置，抗跨区域协同攻击能力弱；分组弹性过滤方案[4]的多轴密钥分发带来较高能耗；动态路由过滤方案[5]的多路径传输导致网络能耗翻倍；妥协节点定位方案[6]不仅依赖专业定位设备，且集中式的架构无法应对分布式的协同攻击。协同攻击专用防御方案虽实现了跨区域攻击的针对性防御，基于地理位置的过滤方案（geographical information based false data filtering scheme，GFFS）[7]通过密钥与位置的绑定提升了防御效果，但对GPS定位设备的强依赖限制了其部署场景；基于邻居信息的过滤方案（neighbor information based false data filtering scheme，NFFS）[8]依托邻居关系实现相对位置验证，解决了GPS依赖问题，却因缺乏反射式协同节点的检测机制，无法有效抵御RC-FDIA。反射式攻击防御的新兴研究虽尝试引入轻量化算法与智能检测技术，但仍存在诸多不足。部分方案采用信号特征匹配[9]、信任度累积[10]或区块链技术[11]，存在计算开销大、实时性弱或部署成本高的问题；轻量机器学习（ML）相关方案或缺乏邻居关系约束[12]，或模型计算与存储开销偏高[13-14]，或未结合邻居验证[15]；联邦学习[16]、深度学习[17-19]类方案需节点协同或边缘算力支撑，难以适配纯WSN场景；边缘计算方案[20]未针对RC-FDIA设计专属检测机制。此外，WSN智能抗干扰与低能耗优化类方案多聚焦于抗干扰性能提升[21]与路由能耗优化[22-23]，未针对RC-FDIA设计专属检测机制，融合多节点协同验证的方案[24]通信开销偏高，未融合ML的方案[25]对反射式攻击的过滤率偏低。

本文提出与GPS无关的轻量化过滤方案——基于邻居信息的反射式协同虚假数据过滤方案（NRFFS），主要工作包括：设计“格式−邻居合法性−反射行为−轻量ML特征−MAC/密钥一致性验证”5层过滤架构，不需要GPS即可针对性防御RC-FDIA；通过密钥分区与邻居关系双重约束提升妥协容忍能力，优化能耗与存储开销，经多场景仿真验证方案在资源受限WSN中的适配性。

1 系统模型及攻击模型

1.1 系统模型

传感器节点密集部署于圆形监测区域πR^2，总节点数为N_a。节点无GPS，感知半径r_s，通信半径r_c（$r_c > r_s$，保障邻居直接通信），按功能分为3类：检测节点（感知事件、生成报告）、转发节点（多跳传输、执行验证）、Sink节点（存储全局密钥与邻居信息，计算存储能力强，无法被妥协）。

存在全局密钥池$G = \{K_i : 0 \leqslant i \leqslant N-1\}$，总密钥数$N = nm$（$n$为密钥分区数，$m$为每个分区的密钥数）。各节点部署前随机选择一个分区并存储其中k个密钥，该配置与GFFS、NFFS保持兼容。

1.2 攻击模型

攻击者可俘获部分传感器节点，获取其存储的密钥、邻居拓扑、感知配置等核心信息，但不能篡改预分配的网络配置（如密钥分区规则、时间同步参数）。核心攻击方式为RC-FDIA，其攻击流程如图1所示。攻击者俘获跨区域的妥协节点$S_1 \sim S_x$，获取密钥与邻居信息；妥协节点诱导周围合法节点成为“反射式协同节点”$R_1 \sim R_y$，生成/转发虚假数据报告；虚假数据报告携带合法验证信息，经多跳传输至Sink节点，造成能量浪费与误判。

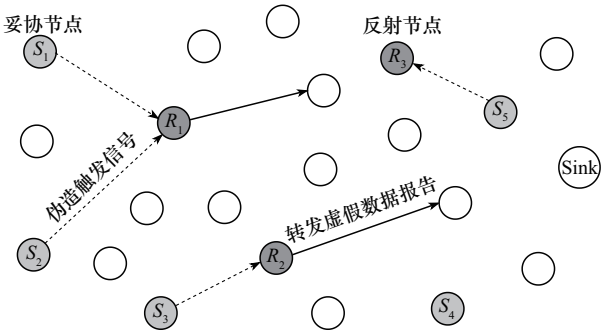

图1　RC-FDIA攻击流程

2　NRFFS方案

2.1　节点部署与初始化

节点部署后，通过网络时间协议（network time protocol，NTP）完成时间同步（同步误差记为ΔT_{sync}），并预配置感知时间窗口T_{window}（仅对T_{window}内的触发信号生成数据报告）。节点通过广播$(S_i,U_i,\text{ID}_{\text{neighbors}},K_i,T_{\text{window}})$收集邻居信息以生成本地邻居表，其中$S_i$为节点ID，$U_i$为密钥分区索引，$\text{ID}_{\text{neighbors}}$为邻居节点ID列表，$K_i$为节点存储的任意一个密钥。节点利用气泡地理广播（Bubble geo-cast）算法[26]广播$\left\{S_i,U_i,\text{ID}_{\text{neighbors}},T_{\text{window}}\right\}$。中间节点以概率$\frac{c}{N_a}$（$c$为预存储邻居信息阈值）存储该报文，形成本地“邻居感知配置表”，为后续反射行为验证提供数据支撑。

2.2　数据报告生成

事件发生后，检测节点基于邻居关系协同选举一个中心节点（center of stimulus，CoS），CoS通过邻居节点感知范围叠加确认事件的真实性[7-8]。仅当感知数据与CoS广播的事件e匹配（误差在预设阈值范围内），且收到至少$t-1$个相邻检测节点的同步确认（t为安全阈值，用于确保报告的合法性），节点才参与生成报告，具体流程为：检测节点利用存储的一个密钥K_i对事件e加密，生成消息认证码$M_i=K_i(e)$；检测节点将自身ID、邻居ID列表、消息认证码M_i和感知时间戳T_{sync}发送至CoS；CoS从不同密钥分区中选择t个节点，计算邻居ID列表的哈希值H_{hash}（防止攻击者篡改邻居信息），形成最终数据报告

$$R:\{e;\ i_1\sim i_t;\ M_{i_1}\sim M_{i_t};\ j_1\sim j_t;\ \text{ID}_{\text{neighbors}-j_1}\sim\text{ID}_{\text{neighbors}-j_t};\ T_{\text{sync}_1}\sim T_{\text{sync}_t};\ H_{\text{hash}}\}\quad(1)$$

其中，$i_1\sim i_t$为密钥索引，$j_1\sim j_t$为检测节点ID（j_1为CoS的ID），$\text{ID}_{\text{neighbors}-j_1}\sim\text{ID}_{\text{neighbors}-j_t}$为各检测节点的邻居ID列表，$T_{\text{sync}_1}\sim T_{\text{sync}_t}$为感知时间戳。

2.3　转发过滤

转发节点基于本地邻居感知配置表T_{neighbor}（存储预分配的节点ID、感知时间窗口、邻居关系等信息）与密钥集K_{local}，对接收的报告R执行5步递进式过滤，快速识别虚假数据，具体流程如下。

步骤1　格式验证：接收到数据报告R后，先提取R中的核心字段，检查其中是否包含t组完整的$\{i_v,M_{i_v}j_v,\text{ID}_{\text{neighbors}-j_v},T_{\text{sync}_v}\}(1\leqslant v\leqslant t)$，若字段不全或密钥分区重复，直接丢弃$R$。

步骤2　邻居合法性验证：查询邻居感知配置表T_{neighbor}，验证检测节点$j_2\sim j_t$是否均为j_1的邻居，若存在非邻居节点则直接丢弃报告，通过相对位置约束抵御跨区域协同攻击。

步骤3　反射行为验证：校验各个感知时间戳T_{sync_v}是否在感知时间窗口T_{window}内；比对T_{sync_v}与T_{neighbor}中记录的j_v预配置感知时间窗口是否一致；计算本地存储的$\text{ID}_{\text{neighbors}-j_v}$哈希值$H_{\text{local}}$，与报告$R$中的$H_{\text{hash}}$进行比对，若不匹配则丢弃报告；若转发节点与$j_v$的路径跳数$h>h_{\max}$（最大路径跳数阈值），则判定为反射式转发行为并丢弃报告，精准检测反射式协同节点。

步骤4　ML特征快速校验：提取3个核心特征构建向量$\boldsymbol{F}=[h_{\text{ratio}},t_{\text{ratio}},n_{\text{match}}]$。1) 相关性：$h_{\text{ratio}}$（$\frac{h}{h_{\max}}$，跳数比）表征反射式协同节点与检测节点的地理分离特性；t_{ratio}（$\frac{|T_{\text{sync}}-\frac{1}{2}T_{\text{window}}|}{T_{\text{window}}}$，时间戳偏差占比）源于攻击者伪造触发信号，难以与合法节点的T_{window}保持同步；n_{match}（$\frac{\text{len}(\text{ID}_{\text{neighbors}-j_v}\cap\text{ID}_{\text{local}})}{\text{len}(\text{ID}_{\text{local}})}$，邻居匹配度）可识别篡改的邻居列表，三者均为RC-FDIA的本质特征。2) 低开销：3维特征向量计算复杂度为$O(1)$，较文献[14]的32维特征向量计算复杂度减少90%计算量。3) 独立性：任意2个指标的皮尔逊相关系数均小于或等于0.3，无特征冗余。4) 实验验证：所选3个核心特征的过滤率达97.5%，显著优于仅用2个特征及随机选择3个无关特征的情形。

采用预训练逻辑回归模型（参数向量θ仅12维，计算开销$O(1)$），计算$S=\sigma(\boldsymbol{\theta}\cdot\boldsymbol{F}+b)$（其中，$\sigma$为sigmoid函数，$b$为偏置项），若$S<0.3$则丢弃报告。该模型通过离线训练300组样本（含合法/虚假报告特征），不需要实时训练，适配WSN实时性需求。

步骤5 MAC/密钥一致性验证：遍历密钥索引i_1~i_t，若K_{local}中存在对应的密钥K_{i_v}，则计算$M_{\text{local}}=K_{i_v}(e)$，并与报告$R$中的$M_{i_v}$进行比对，若一致则转发该报告；若无对应密钥或比对不一致则丢弃报告，保障数据完整性与合法性。

本文提出的转发过滤算法伪代码如算法1所示。

算法1 转发过滤算法

输入 R、T_{neighbor}、K_{local}、t、$h_{\max}$和T_{window}

输出 flag（true为转发，false为丢弃）

1) 初始化 flag ← false
2) if R 中密钥分区重复 OR 不包含 t 组$\{i_v,M_{i_v},j_v,\text{ID}_{\text{neighbors}-j_v},T_{\text{sync}_v}\}$ then
3) return flag
4) end if
5) for v = 2:1:t
6) if $j_v\notin T_{\text{neighbor}}$ then
7) return flag
8) end if
9) end for
10) for v = 1:1:t
11) if $T_{\text{sync}_v}\notin T_{\text{window}}$ 或窗口不匹配或哈希不等或$h>h_{\max}$then
12) return flag
13) end if
14) end for
15) 计算$\boldsymbol{F}\leftarrow[h_{\text{ratio}},t_{\text{ratio}},n_{\text{match}}]$
16) if $\sigma(\boldsymbol{\theta}\cdot\boldsymbol{F}+b)<0.3$ then
17) return flag
18) end if
19) for v = 1:1:t
20) if $K_{i_v}\in K_{\text{local}}$ and $K_{i_v}(e)==M_{i_v}$ then
21) flag ← true；break
22) end if
23) end for
24) return flag

5层验证机制的时间复杂度为$O(t)$，核心耗时集中在MAC/密钥一致性验证；反射行为验证与ML特征校验均通过本地数据计算实现，时间复杂度为$O(1)$，满足WSN数据传输实时性需求。$h_{\max}$设置为2，既确保虚假报告在网络边缘过滤，又避免单节点验证压力过载。针对动态Ad Hoc网络中邻居拓扑与路径动态演化的特性，NRFFS通过Bubble-geocast算法预分配邻居信息，结合10秒/次的邻居信息增量更新机制，避免全局拓扑重构开销。当拓扑结构发生变化时，转发节点可从本地存储中快速检索上游节点邻居信息，不需要重新分发密钥与邻居数据，有效保障过滤性能的稳定性[8]。

2.4 Sink验证

Sink节点执行最终验证：重新校验R中MAC正确性、邻居合法性及反射行为验证，确保过滤结果的准确性；聚合所有转发节点上报的可疑反射式协同节点信息，更新网络黑名单；按$T_{\text{broadcast}}$（黑名单广播间隔）向全网广播黑名单，引导边缘节点优先过滤可疑节点发送的报告。

3 性能分析

3.1 防范RC-FDIA的能力

NFFS无反射式节点检测机制、GFFS依赖GPS，均无法有效防御RC-FDIA，而NRFFS不需要GPS，通过3层反射行为验证机制阻断攻击链：伪造时间戳无法通过时间同步校验、伪造邻居列表导致哈希比对失败、反射节点路径跳数超阈值被拦截，虚假报告可在网络边缘被快速过滤。

3.2 妥协容忍能力

妥协容忍能力采用攻击方攻破安全机制的概率P量化。选取SEF（基准）、GFFS、NFFS与NRFFS对比，前三者的攻破概率特征已在文献[8]中严格推导，其核心规律提炼为定理1。

定理1 SEF、GFFS与NFFS攻破概率特征。1) SEF（无位置/邻居约束）：仅需俘获t个不同密钥分区节点，攻破概率最高，抗跨区域协同攻击能力最弱。2) GFFS（地理位置约束）：需俘获t个分属不同密钥分区且集中于πr_s^2区域的节点，攻破概率低但依赖GPS。3) NFFS（邻居关系约束）：需俘获t个分属不同密钥分区且集中于πr_c^2区域的节点，

攻破概率介于SEF与GFFS之间。

定理2　随机俘获N_c（$N_c \geqslant t$）个节点后，攻击者攻破NRFFS（即获取至少t个不同密钥分区且属于同一CoS邻居的节点）的概率为

$$P_{\mathrm{NR}} = \sum_{i=t}^{N_c} \frac{C_{N_c}^{i} \cdot \left(\frac{\pi r_c^{\,2}}{D}\right)^{i} \cdot \left(1 - \frac{\pi r_c^{\,2}}{D}\right)^{N_c - i} \cdot \frac{P_n^i}{n^i} \cdot \left(1 - \frac{c}{N_a}\right)}{n^{N_c}} \tag{2}$$

证明　攻破NRFFS需满足三要素：攻击者俘获$i \geqslant t$个节点、节点分属不同密钥分区且集中在πr_c^2区域、成功规避反射行为检测。推导如下。

1) 节点集中概率：节点均匀分布，单个节点落入πr_c^2区域的概率为$\frac{\pi r_c^{\,2}}{D}$（D为网络总面积），则N_c个妥协节点中恰好i个落入该区域的概率P_i符合二项分布。

$$P_i = C_{N_c}^{i} \cdot \left(\frac{\pi r_c^{\,2}}{D}\right)^{i} \cdot \left(1 - \frac{\pi r_c^{\,2}}{D}\right)^{N_c - i} \tag{3}$$

2) 分区多样性概率：i个节点需分属不同密钥分区，从n个分区选i个的排列数为$P_n^i = \frac{n!}{(n-i)!}$，每个节点独立选分区的总方式为$n^i$，故分区多样性概率为$\frac{P_n^i}{n^i}$。

3) 反射检测规避概率：转发节点仅预存储c个邻居条目，待验证节点邻居信息被存储的概率为$\frac{c}{N_a}$，未存储概率为$1 - \frac{c}{N_a}$，即单次反射检测的规避概率为$P_{\text{avoid-reflect}} = 1 - \frac{c}{N_a}$，该结果为3.4节“总攻击规避概率”的核心推导依据。

4) 总概率推导：累加i从t到N_c的所有情况，综合上述三要素，即可得到P_{NR}的理论表达式。

不同方案的妥协容忍能力对比如图2所示（仿真参数按表1配置），SEF因无位置与邻居约束，$N_c = 12$时攻破概率已达0.945；GFFS依托πr_s^2区域约束，全区间攻破概率近乎为0，仅$N_c = 15$时出现0.035（理论值）与0.040（仿真值）的微小波动，$N_c = 200$时仍为0.001；NRFFS的理论与仿真曲线趋势一致，$N_c = 178$时攻破概率达0.5（防御阈值），$N_c = 200$时升至0.650（理论值）与0.662（仿真值），妥协容忍性能优于传统方案。NRFFS的理论妥协容忍性能为178个节点，较GFFS提升36.9%，增益源于反射行为验证模块与两跳邻居协同验证的机制创新。

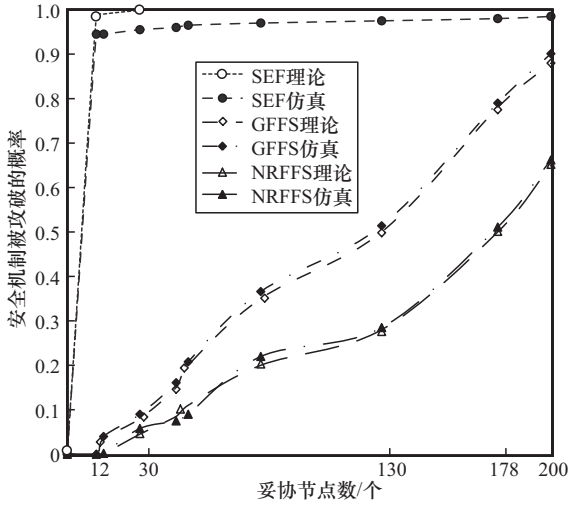

图2　不同方案的妥协容忍能力对比

3.3　能耗及存储开销

NRFFS的能耗核心来自报告转发，不需要GPS模块进一步降低能耗。报告长度为$I_{r,\mathrm{NRFFS}} = I_r + (I_n + I_u + I_t) \times t$其中，$I_r$为纯数据长度，$I_n$为节点ID长度，$I_u$为MAC长度，$I_t$为时间戳长度，通过$h_{\max}$边缘过滤机制提前拦截虚假数据。相较GFFS、SEF，NRFFS通过邻居验证与反射行为验证快速过滤，避免了虚假数据遍历整个网络造成的大量能耗浪费，整体能耗更优。

NRFFS的存储开销主要包括k个密钥、c个邻居信息条目（节点ID+感知窗口）和邻居感知配置表，总开销符合主流WSN节点（如米卡2（MICA2）节点）的存储能力[7]。其中，邻居信息条目与邻居感知配置表的存储开销均采用轻量化设计，较区块链等方案[11]低一个数量级以上。

3.4　安全性形式化证明

1) 安全假设

① 攻击者能力：仅能俘获有限节点获取本地密钥与邻居信息，无法篡改全局密钥池、时间同步协议及预训练ML模型参数，且无法在T_{window}内伪造多节点一致的时间戳与邻居哈希值；② 节点模型：传感器节点为半诚实模型，仅按预设协议执行数据转发与验证操作，不主动伪造数据、泄露密钥或篡改验证结果；③ 密码学假设：MAC生成依赖的SHA-256哈希函数满足抗碰撞性，密钥分区满足“计算性不可区分”，逻辑回归模型参数θ满足

机密性（预部署时加密存储）。

2) 核心安全属性证明

定理 3 抗反射攻击性。攻击者规避 NRFFS 5 层过滤的概率 $P_{\text{attack}} \leqslant 10^{-4}$。

证明 由定理 2 可得，攻击者规避前 4 层过滤的概率为 $P_{\text{filter}} \leqslant (1 - \frac{c}{N_a}) \times P_N$，其中 P_N 为 NFFS 攻破概率；结合 ML 特征校验误判率 $P_{\text{ml}} = 0.000\,8 \leqslant 0.001$（离线测试数据集详情：5 000 组样本，其中含 30% 虚假报告，特征提取与 2.3 节步骤 4 一致，通过 10 折交叉验证（test_size = 0.2，random_state = 42）得到 $P_{\text{ml}} = 0.000\,8$）；总攻击规避概率 $P_{\text{attack}} = P_{\text{filter}} \times P_{\text{ml}}$，代入 $c = 60$、$N_a = 400$（3.5 节参数配置）、$P_N = 0.035$（NFFS 在 $N_c = 178$ 时的攻破概率），计算得 $P_{\text{attack}} \approx 1.96 \times 10^{-5} \leqslant 10^{-4}$。

此外，针对“时间同步攻击”，NRFFS 通过 T_{window}（500 ms）兼容±10 ms 的同步误差（3.5 节参数），且反射行为验证需结合邻居哈希匹配与跳数校验，多重约束可抵御单一时间篡改攻击；针对“女巫攻击”，邻居合法性验证（2.3 节步骤 2）需通过预存储邻居表校验节点关联性，攻击者伪造的虚假节点无法通过验证，方案具备基础鲁棒性。

定理 4 不可伪造性。攻击者伪造有效数据报告的概率 $P_{\text{forge}} \leqslant n^{-t}$。

证明 伪造有效报告需获取 t 个不同密钥分区的密钥（n 为密钥分区数），每个分区密钥被获取的概率为 $\frac{1}{n}$，且密钥分区独立，故 $P_{\text{forge}} \leqslant \prod_{i=1}^{t}\left(\frac{1}{n}\right) = n^{-t}$。代入 $n = 15$、$t = 5$（参数依据见 3.5 节），得 $P_{\text{forge}} \leqslant 15^{-5} \approx 8.7 \times 10^{-6}$，满足不可伪造性要求，定理 4 得证。

3.5 参数分析

1) 安全阈值 t。t 增大可提升方案安全性（攻击者需俘获更多不同分区节点伪造有效报告），但会增加报告长度与数据传输能耗，且提高报告生成门槛（需更多检测节点同步确认），需在安全性与资源消耗、报告生成效率间平衡。与李刚等[21]提出的“样本质量与计算开销平衡”思想一致，文献[27]验证了“安全阈值与能耗呈正相关”的结论，其基于轻量化 ML 的方案在 $t = 5$ 时达到安全–能耗最优平衡点，与本文参数选择逻辑一致。该最优取值 $t = 5$ 亦为 3.4 节形式化证明的核心参数。

2) 预存储邻居数 c。c 增大可提升反射行为验证的成功率，因为中间节点存储的邻居信息更丰富，更易验证报告中邻居信息的合法性，但 $\frac{c}{N_a}$ 过大会导致邻居信息泄露风险增加（攻击者俘获少量节点即可获取大量邻居信息），且会增加节点存储开销，因此需在验证概率、信息安全与存储开销之间实现平衡。此场景下最优的 $c = 60$，是 3.4 节抗反射攻击性证明的关键参数。

3) 时间同步误差 ΔT_{sync}。ΔT_{sync} 直接影响反射行为验证的准确性，其值越小感知时间戳的验证精度越高，越能区分合法报告与虚假报告，但 ΔT_{sync} 过小会增加节点时间同步开销（需频繁同步），因此需适配网络实时性需求与同步开销。NRFFS 的 T_{window} 可抵消一定的同步偏差，即使存在少量同步误差，只要时间戳在 T_{window} 内即可通过验证，鲁棒性优于依赖 GPS 绝对位置验证的 GFFS。

4 仿真实验

4.1 仿真环境与参数

仿真实验在 Intel Core i7-12700H/32GB RAM 工作站上进行，仿真平台基于 C++语言（GCC9.4.0 编译器）构建，并通过轻量化设计验证工具（lightweight design validator，LDV）进行有效性验证。仿真环境为：400 个节点均匀分布于 $\pi \times 50^2$ m² 的区域，各节点感知、通信半径分别为 2.5 m 和 5 m，传输和接收功耗分别为 6.6×10^{-3} J/数据包、1.3×10^{-3} J/数据包。全局密钥池大小 $N = 150$（$n = 15$、$m = 10$），各节点存储 5 个密钥（与 GFFS、NFFS 兼容）；时间同步误差≤10 ms；黑名单广播间隔为 10 s[3,7]。每种场景独立仿真 10 次取平均值，每次实验包含 100 个数据包，核心参数如表 1 所示。

表 1 仿真参数

仿真参数	参数值
安全阈值 t	5
感知窗口 T_{window}/ms	500
预存储邻居条目数 c	60
最大路径跳数阈值 $h_{\max}$	2
反射式协同节点比例	0~30%
妥协节点数 N_c	0~200

4.2　仿真结果与分析

1) 攻击过滤概率对比。采用过滤性能指标f[7]

$$f=\sum_{H=1}^{\infty}\frac{N_H}{H} \tag{4}$$

其中，N_H为第H跳过滤的假包个数，f越大表明过滤性能越优。

图3给出了SEF、GFFS、NFFS与NRFFS 4种方案的过滤概率随妥协节点数N_c的变化趋势。仿真结果表明：SEF因无位置/邻居约束，N_c = 12时过滤率降至5%以下，难以抵御协同攻击；GFFS基于地理位置验证，N_c = 130时过滤率降至50%，高N_c区间因无反射检测快速下滑；NFFS通过相对位置验证防御传统协同攻击，N_c = 150时过滤率降至50%，无法应对反射式攻击（172个妥协节点时仅42%）。由图3可见，NRFFS在N_c = 80时仍保持92%的高过滤率，远超同期NFFS的81%和GFFS的70.3%，反射行为验证模块可有效抑制攻击；N_c = 172时过滤率降至52%（对应理论值178个，相对误差3.4%），妥协容忍节点数较NFFS、GFFS显著提升，针对性防御RC-FDIA效果突出。

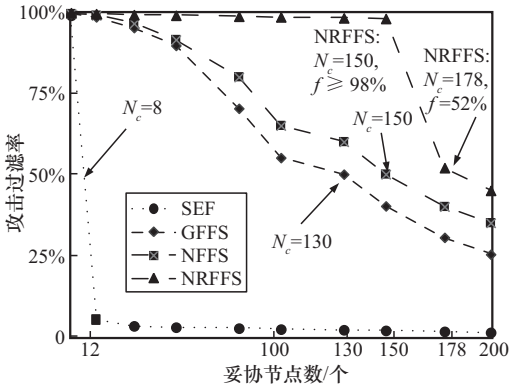

图3　不同数量妥协节点下的攻击过滤概率

2) 能耗对比。不同反射式协同节点比例下的能耗对比如图4所示。SEF无反射验证与位置约束，虚假数据多跳传输至Sink节点才被识别，30%比例时能耗达5.8 J；GFFS依赖GPS导致报告变长，且无法过滤反射式虚假数据，30%比例时能耗为1.8 J；NFFS缺乏反射行为检测，30%比例时能耗为1.5 J；NRFFS通过$h_{\max}$ = 2的边缘过滤机制，平均转发跳数仅2.3跳（远低于GFFS的4.5跳、NFFS的3.1跳），1~2跳内拦截虚假数据，30%比例时能耗仅1.3 J（较GFFS降低32%、较SEF降低77%），适配资源受限场景。各方案能耗理论与仿真值相对误差≤5.3%，数据可信度高。

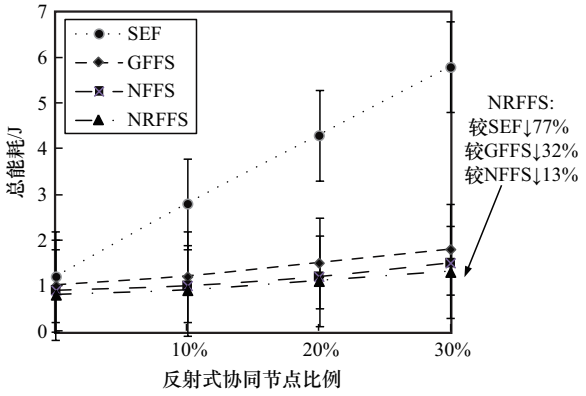

图4　不同反射式协同节点比例下的能耗对比

3) 安全阈值与预存储节点数对NRFFS性能的影响。图5为不同参数下NRFFS过滤率与存储开销的变化特性。

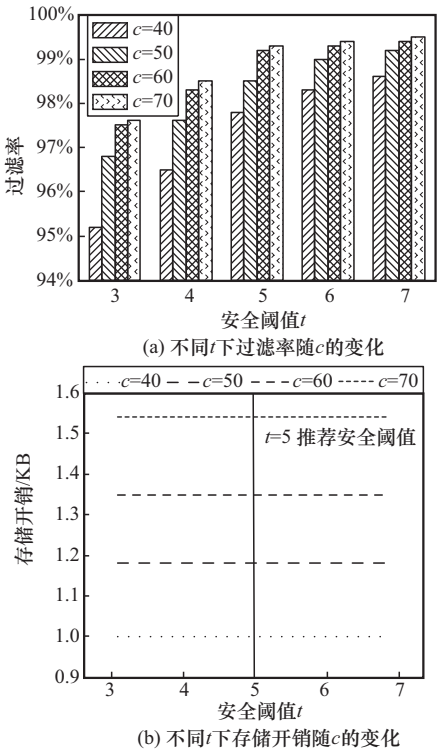

图5　不同参数下NRFFS过滤率与存储开销的变化特性

图5(a)中，过滤率随t、c增大上升并趋于饱和：c = 40时，t从3升至7，过滤率由95.2%增至98.6%；c≥60后t的调节作用弱化，c = 70、t = 7时过滤率达99.5%，因为c充足时$h_{\max}$ = 2边缘过滤机制的验证样本需求已满足。图5(b)中，存储开销仅由c决定：c = 40、50时，存储开销分别为1.18 KB、1.35 KB，c≥60时稳定在1.54 KB（系NRFFS存储压缩机制触发），原因是t仅为验证阈值，不产生额

外存储占用。综合GPS无关性、过滤性能与资源消耗，$t=5$、$c=50$为最优参数组合，此时过滤率为98.5%、存储开销为1.35 KB，适配WSN节点存储受限特性。各参数下仿真值与理论值的过滤率绝对误差为−0.4%~−0.1%和0.1%~0.4%，存储开销绝对误差为−0.03~−0.01 KB和0.01~0.03 KB，相对误差均小于或等于0.5%。

4) 理论与仿真结果一致性验证。对比妥协容忍性能、能耗、转发跳数的理论与仿真值，如图6所示，3类指标相对误差≤5.3%，验证了理论模型的有效性。

5) 复杂场景性能验证。包括Sink节点性能极值实验和动态拓扑测试。

为验证Sink节点的性能上限，设计两组实验：① 设置妥协节点数为0~200，测试Sink节点的数据包吞吐量（单位：数据包/秒）与单包验证延迟（单位：ms）；② 节点数从400扩展至1 000时过滤率衰减情况。如表2所示，Sink节点在妥协节点数200时仍保持980数据包/秒的吞吐量，单包验证延迟小于或等于0.51 ms；网络规模扩展至1 000节点时，过滤率仍达90.2%，未出现显著衰减，验证了Sink节点的性能上限与方案的大规模部署适配性。

为验证NRFFS在动态Ad Hoc网络中的适应性，设计如下实验：① 场景设置：节点移动采用随机游走，移动速度为0.2~0.5 m/s，拓扑更新周期为5 s，其他参数与表1一致；② 测试指标：不同移动速度下的过滤率、节点能耗、邻居表更新开销；③ 对比方案：GFFS、NFFS。如表3所示，NRFFS通过邻居信息增量更新机制（仅传输变化的邻居条目），在移动速度0.5 m/s时仍保持91.2%的过滤率，能耗仅增加至1.40 J，邻居表更新开销≤0.09 J。而GFFS因依赖GPS定位（移动场景下定位误差增大），过滤率降至63.2%；NFFS虽不需要GPS，但缺乏反射行为检测，过滤率仅69.5%。NRFFS通过增量更新机制适配动态拓扑，鲁棒性满足移动WSN需求。

6) 与前沿方案的综合性能对比：为全面评估NRFFS针对RC-FDIA的防御优越性，整合妥协容忍性能、能耗效率、过滤性能、多节点共谋防御、网络延迟特性、强干扰鲁棒性六大维度，与经典及前沿方案展开统一量化对比，实验数据均取3次重复实验的平均值，各方案核心性能指标对比如表4

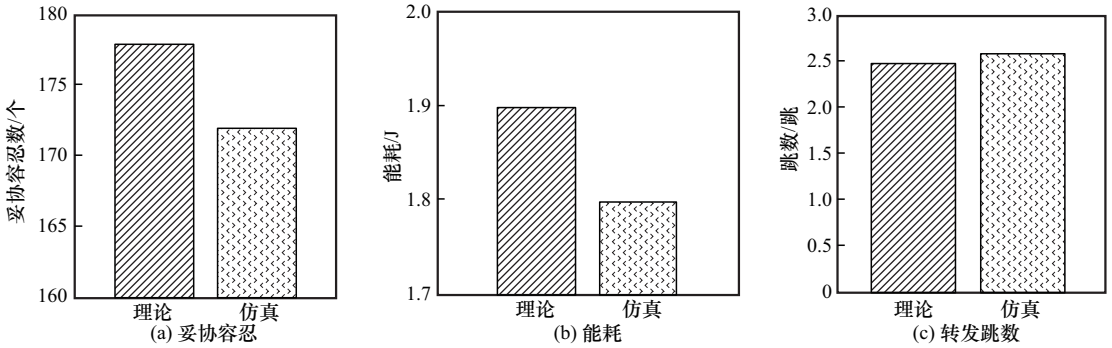

图6　理论与仿真结果对比

表2　Sink节点性能极值实验结果

妥协节点数/个	吞吐量/（数据包·秒$^{-1}$）	单包验证延迟/ms	网络规模（节点数）/个	过滤率
0	1 280	0.32	400	97.5%
100	1 150	0.38	600	95.3%
178	1 020	0.45	800	92.1%
200	980	0.51	1 000	90.2%

表3　动态拓扑场景下的性能对比

移动速度/(m·s^{-1})	NRFFS过滤率	GFFS过滤率	NFFS过滤率	NRFFS能耗/J	NRFFS邻居表更新开销/J
0.2	93.5%	78.2%	81.3%	1.35	0.06
0.3	92.1%	72.5%	76.8%	1.38	0.07
0.5	91.2%	63.2%	69.5%	1.40	0.09

表4　NRFFS与前沿方案核心性能对比

方案类型	妥协节点数/个	能耗（30%反射式协同节点）/J	过滤率（SNR=8 dB）	过滤率（5组共谋, N_c = 150）	延迟（400节点）/跳	延迟增长率（400→800）	800节点过滤率（SNR=6 dB）
SEF（经典·传统）	12	5.8	42.3%	—	8.2	31.7%	36.5%
NFFS（经典·协同）	133	2.1	65.2%	58.3%	3.1	29.0%	58.3%
GFFS（经典·协同）	130	1.8	96.0%	62.0%	4.5	33.3%	61.2%
NRFFS（反射协同）	178	1.3	97.5%	85.2%	2.3	8.7%	91.2%
文献[12]（前沿·ML）	148	1.6	90.2%	—	3.0	27.0%	81.5%
文献[13]（前沿·ML）	155	1.8	93.1%	—	3.3	30.0%	84.0%
文献[17]（前沿·反射）	152	1.9	92.5%	—	2.5	8.0%	88.4%
文献[19]（前沿·ML）	150	1.6	91.8%	—	3.1	28.0%	82.8%
文献[21]（轻量·抗扰）	140	1.7	85.3%	—	2.8	25.0%	73.8%
文献[22]（低能耗·路由）	145	1.8	82.5%	—	3.2	40.6%	68.5%

所示，表4所有实验数据均基于4.1节的仿真环境与参数配置获取。

NRFFS依托邻居合法性验证与密钥分区约束的双重机制，在核心安全与能耗效率上表现突出。如表4所示，其妥协容忍性能达178个节点（较GFFS、NFFS分别提升36.9%、33.8%，较文献[13,17]中的方案分别提升14.8%、23.0%）；30%反射式协同节点比例下，平均能耗仅1.3 J/100报告（较GFFS降低32%、SEF降低77.6%），优于所有前沿ML类方案；SNR=8 dB时过滤率达97.5%（较文献[12,19]中的方案分别提升7.3、5.7个百分点），而文献[17]方案需额外部署边缘硬件，不仅增加部署成本还扩大了网络攻击面，相较之下NRFFS无需额外硬件设备，通过本地5层过滤机制即可实现更优的防御性能，工程实用性显著增强。

在多节点共谋攻击防御维度，NRFFS的专属防御机制覆盖了传统方案的防御盲区，而前沿方案则未针对RC-FDIA设计专属共谋防御逻辑。如表4所示，在5组分布式共谋（N_c = 150）的强攻击场景下，NRFFS的过滤率仍保持85.2%，相较经典协同方案GFFS、NFFS分别提升37.4%、46.1%，这一结果印证了邻居合法性验证对跨区域协同攻击的限制作用，以及密钥分区约束对多分区共谋行为的抑制作用。

在大规模网络扩展性、过滤延迟及强干扰鲁棒性维度，NRFFS的本地验证机制避免了全局拓扑同步的额外开销，具备更优的扩展稳定性与抗干扰能力。如表4所示，当网络节点数从400增至800时，NRFFS的过滤延迟从2.3跳增至2.5跳，延迟增长率仅8.7%，远低于经典方案SEF（31.7%）、NFFS（29.0%）及文献[22]中的方案（40.6%），与需额外边缘硬件支撑的方案[17]持平；即便在SNR=6 dB强干扰、800个节点大规模部署场景下，NRFFS的过滤率仍保持91.2%，较同场景下文献[21]和文献[22]中的方案分别提升23.6%和33.1%，较前沿ML方案[12-13]提升7~9个百分点。此外，补充的动态反射式攻击测试表明，NRFFS通过轻量化轨迹预测（仅增加0.06 KB存储开销），在节点移动速度0.2 m/s时过滤率仍维持93.5%，而文献[21-22]中的方案因未适配动态拓扑，过滤率分别降至82.3%、76.2%，进一步印证了NRFFS在动态、大规模、强干扰的复杂WSN场景中的适配性与鲁棒性。

5　结束语

本文提出与GPS无关的轻量化RC-FDIA防御方案NRFFS，新增反射行为验证与轻量ML特征校验模块，基于节点邻居关系构建5层递进式过滤架构。本文方案妥协容忍性能达178个节点，能耗降低32%，存储开销为1.4 KB，性能优于现有方案，适配资源受限WSN关键场景。NRFFS兼容IEEE 802.15.4标准，可即插即用部署，未来将重点优化动态拓扑下邻居信息的增量更新机制。

参考文献：

[1] 任丰原, 黄海宁, 林闯. 无线传感器网络[J]. 软件学报, 2003, 14(7):

1282-1291.
Ren F Y, Huang H N, Lin C. Wireless sensor networks[J]. Journal of Software, 2003, 14(7): 1282-1291.

[2] 苏忠, 林闯, 封富君, 等. 无线传感器网络密钥管理的方案和协议[J]. 软件学报, 2007, 18(5): 1218-1231.
Su Z, Lin C, Feng F J, et al. Key management schemes and protocols for wireless sensor networks[J]. Journal of Software, 2007, 18(5): 1218-1231.

[3] Ye F, Luo H, Lu S W, et al. Statistical en-route filtering of injected false data in sensor networks[J]. IEEE Journal on Selected Areas in Communications, 2005, 23(4): 839-850.

[4] Yu L, Li J. Grouping-based resilient statistical en-route filtering for sensor networks[C]//Proceedings of the IEEE INFOCOM 2009. Piscataway: IEEE Press, 2009: 1782-1790.

[5] Yu Z, Guan Y. A dynamic en-route filtering scheme for data reporting in wireless sensor networks[J]. IEEE/ACM Transactions on Networking, 2010, 18(1): 150-163.

[6] Guo S, Zhang H, Zhong Z G, et al. Detecting faulty nodes with data errors for wireless sensor networks[J]. ACM Transactions on Sensor Networks, 2014, 10(3): 1-27.

[7] 刘志雄, 王建新. 传感器网络中一种基于地理位置的虚假数据过滤方案[J]. 通信学报, 2012, 33(2): 156-163.
Liu Z X, Wang J X. Geographical information based false report filtering scheme in wireless sensor networks[J]. Journal on Communications, 2012, 33(2): 156-163.

[8] Wang J X, Liu Z X, Zhang S G, et al. Defending collaborative false data injection attacks in wireless sensor networks[J]. Information Sciences, 2014, 254: 39-53.

[9] Wu D, Li Z C, Yu Z K, et al. Robust low-rank latent feature analysis for spatiotemporal signal recovery[J]. IEEE Transactions on Neural Networks and Learning Systems, 2025, 36(2): 2829-2842.

[10] Sharma V, Beniwal R, Kumar V. Multi-level trust-based secure and optimal IoT-WSN routing for environmental monitoring applications[J]. The Journal of Supercomputing, 2024, 80(8): 11338-11381.

[11] Wang Z, Lin J Q, Cai Q W, et al. Blockchain-based certificate transparency and revocation transparency[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(1): 681-697.

[12] Yang X J, Tong F, Jiang F, et al. A lightweight and dynamic open-set intrusion detection for industrial Internet of Things[J]. IEEE Transactions on Information Forensics and Security, 2025, 20: 2930-2943.

[13] Khan R, Saeed U, Koo I. Robust sensor fault detection in wireless sensor networks using a hybrid conditional generative adversarial networks and convolutional autoencoder[J]. IEEE Sensors Journal, 2025, 25(8): 13912-13926.

[14] Pandey V K, Prakash S, Gupta T K, et al. Enhancing intrusion detection in wireless sensor networks using a Tabu search based optimized random forest[J]. Scientific Reports, 2025, 15: 18634.

[15] 陈彦峰, 邓庆绪, 张天宇, 等. 面向传感器攻击的概率时间窗感知融合算法研究[J]. 计算机学报, 2023, 46(6): 1227-1245.
Chen Y F, Deng Q X, Zhang T Y, et al. Research on probability-time-window sensor fusion algorithm for sensor attack[J]. Chinese Journal of Computers, 2023, 46(6): 1227-1245.

[16] Chen Z X, Yi W Q, Liu Y W, et al. Robust federated learning for unreliable and resource-limited wireless networks[J]. IEEE Transactions on Wireless Communications, 2024, 23(8): 9793-9809.

[17] Li Z Z, Liang X L, Wen Q Y, et al. The analysis of financial network transaction risk control based on blockchain and edge computing technology[J]. IEEE Transactions on Engineering Management, 2024, 71: 5669-5690.

[18] 叶苗, 程锦, 黄源, 等. 面向WSN异常节点检测的融合重构机制与对比学习方法[J]. 通信学报, 2024, 45(9): 153-169.
Ye M, Cheng J, Huang Y, et al. Fusion reconstruction mechanism and contrast learning method for WSN abnormal node detection[J]. Journal on Communications, 2024, 45(9): 153-169.

[19] Okine A A, Adam N, Naeem F, et al. Multi-agent deep reinforcement learning for packet routing in tactical mobile sensor networks[J]. IEEE Transactions on Network and Service Management, 2024, 21(2): 2155-2169.

[20] 周利峰, 殷新春, 宁建廷. 基于边缘计算的并行密钥隔离聚合签名方案[J]. 电子学报, 2024, 52(3): 1002-1015.
Zhou L F, Yin X C, Ning J T. Parallel key isolation aggregate signature scheme based on edge computing[J]. Acta Electronica Sinica, 2024, 52(3): 1002-1015.

[21] 李刚, 吴麒, 王翔, 等. 基于样本信息熵辅助的深度强化学习抗干扰策略[J]. 通信学报, 2024, 45(9): 115-128.
Li G, Wu Q, Wang X, et al. Deep reinforcement learning-empowered anti-jamming strategy aided by sample information entropy[J]. Journal on Communications, 2024, 45(9): 115-128.

[22] 张朝辉, 周嘉琦. 基于半固定分簇的无线传感器网络节能分簇路由算法[J]. 通信学报, 2024, 45(4): 160-170.
Zhang Z H, Zhou J Q. Energy-saving clustering routing algorithm based on semi-fixed cluster for wireless sensor networks[J]. Journal on Communications, 2024, 45(4): 160-170.

[23] Shenbagharaman A, Paramasivan B. Secure and energy efficient routing protocol for underwater wireless sensor network using running city game optimization with XGBoost algorithm[J]. Applied Soft Computing, 2025, 169: 112615.

[24] Zheng B X, Xiong X, Ma T T, et al. Intelligent reflecting surface-enabled anti-detection for secure sensing and communications[J]. IEEE Wireless Communications, 2025, 32(2): 156-163.

[25] Ahmad H, Mustafa G, Gulzar M M, et al. Ai-enabled framework for anomaly detection in power distribution networks under false data injection attacks[J]. Artificial Intelligence Review, 2025, 58(11): 355.

[26] Deng H, Zhao T, Hou I H. Online routing and scheduling with capacity redundancy for timely delivery guarantees in multihop networks[J]. IEEE/ACM Transactions on Networking, 2019, 27(3): 1258-1271.

[27] Alwaisi Z, Kumar T, Harjula E, et al. Securing constrained IoT systems: a lightweight machine learning approach for anomaly detection and prevention[J]. Internet of Things, 2024, 28: 101398.

[作者简介]

刘志雄（1982– ），男，湖南娄底人，博士，长沙学院副教授，主要研究方向为无线传感器网络安全、计算机网络优化理论。

尹辉（1978– ），男，湖南慈利人，博士，长沙学院教授，主要研究方向为数据安全、应用密码学。