DOI:10.11918/202305018

WSN 中计及信誉度的人工蜂群恶意节点识别策略

滕志军[1,2],谷金亮[2],崔瑶瑶[2],朱思安[2],庞宝贺[3]

(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 吉林 132012;
2.东北电力大学 电气工程学院,吉林 吉林 132012;3.哈尔滨工程大学 信息与通信工程学院,哈尔滨 150000)

摘 要:在无线传感器网络(WSN)复杂的应用环境中,为抵御恶意节点发起的选择性转发攻击和不诚实建议攻击、提高网络安全性能,在人工蜂群(ABC)算法的基础上,提出一种计及信誉度的人工蜂群无线传感器网络恶意节点识别策略(CR-ABC)。借助模糊信任模型,融合模糊综合评价机制,综合通信特征、数据属性、物理属性3个方面的影响因素计算节点综合信任值,提高信誉模型的检测精度;引入建议偏差值函数和交互指数偏差值函数,利用ABC算法优化模糊信任模型,确保在恶意节点数量较多时,系统仍保持较高的识别率和较低的误判率。仿真结果表明,CR-ABC对选择性转发攻击的识别率可达90%以上,对正常节点误判率低于6%;对于不诚实建议攻击,即使不诚实节点的数量占比达到50%,CR-ABC仍能保持优异的识别性能,可有效提高复杂环境下WSN的安全性和可靠性。

关键词:无线传感器网络;信誉度;人工蜂群算法;选择性转发攻击;不诚实建议攻击
中图分类号:TN92 **文献标志码**: **文章编号**:0367-6234(2026)03-0181-09

Malicious node identification strategy based on artificial bee colony considering reputation in WSN

TENG Zhijun[1,2], GU Jinliang[2], CUI Yaoyao[2], ZHU Si'an[2], PANG Baohe[3]

(1. Key Laboratory of Modern Power System Simulation and Control & Renewable Energy Technology, Ministry of Education (Northeast Electric Power University), Jilin 132012, Jilin, China; 2. School of Electrical Engineering, Northeast Electric Power University, Jilin 132012, Jilin, China; 3. College of Information and Communication Engineering, Harbin Engineering University, Harbin 150000, China)

Abstract: In the complex application environment of wireless sensor networks (WSN), in order to resist the selective forwarding attack and dishonest recommendation attack launched by malicious nodes and improve the safety performance of the network, this paper proposes a malicious node identification strategy based on artificial bee colony (ABC) considering reputation (CR-ABC) in WSN. By utilizing a fuzzy trust model (FTM) and integrating a fuzzy comprehensive evaluation mechanism, the paper calculates the comprehensive trust value of nodes based on three influencing factors: communication features, data attributes, and physical attributes to improve the detection accuracy of the reputation model. The paper introduces the suggested deviation function and the interaction index deviation function and uses the ABC algorithm to optimize the FTM, aiming to ensure that the system still maintains a higher identification rate and a lower misjudgment rate when there are too many malicious nodes. The simulation results show that the identification rate of CR-ABC for selective forwarding attacks can reach over 90%, and the misjudgment rate for normal nodes can be reduced to less than 6%. For dishonest recommendation attacks, even if the number of dishonest nodes reaches 50%, CR-ABC still maintains a high identification performance, which can effectively improve the security and reliability of WSN in complex environments.

Keywords: wireless sensor network; reputation; artificial bee colony algorithm; selective forwarding attack; dishonest recommendation attack

随着物联网技术的发展,无线传感器网络(wireless sensor network,WSN)已被广泛应用于多个领域[1]。由于传感器节点暴露于开放环境,且通过无线信道通信,易受到恶意攻击,给WSN的安全带来了严峻挑战[2]。其中,选择性转发攻击是WSN中最基础且最难检测的攻击类型之一,与其他攻击

收稿日期:2023-05-06;**录用日期**:2023-07-06;**网络首发日期**:2023-11-08
网络首发地址:https://link.cnki.net/urlid/23.1235.t.20231107.1525.002
基金项目:国家自然科学基金青年科学基金项目(61501107)
作者简介:滕志军(1973—),男,教授,硕士生导师
通信作者:谷金亮,1963631427@qq.com

协同作用时,会对整个网络造成更严重的危害。

在 WSN 中,每个节点既是数据采集终端,也是数据转发路由器,正常工作时需转发所有需要的数据信息。选择性转发攻击的核心特征是:攻击者在数据转发过程中,故意丢弃部分或全部数据包,或间歇性转发接收的消息,常见形式包括丢弃特定类型的消息、拒绝转发至特定节点的数据等。

不诚实建议攻击是一种基于选择性转发攻击、并针对信誉安全模型发起的协同攻击。这种攻击模式中,恶意节点通过伪造信誉值,提供不诚实的反馈建议,隐藏自身与同伙的攻击身份,常见类型包括诽谤攻击、塞选票攻击和串谋攻击等。

针对选择性转发攻击,国内外专家学者开展了大量研究。Ren 等[3]提出了一种具有自适应检测阈值的信道感知信誉模型,根据检测到的丢包率与估计的正常丢包率的偏差,对节点的数据转发行为进行评估,可精准检测 WSN 中的选择性转发攻击;尹荣荣等[4]提出基于多跳确认和信任评估的选择性转发攻击检测方法,利用基于源节点的请求响应形式的多跳确认方案,解决了路径上多恶意节点误警率高和静态信任阈值适应性差等问题;Liu 等[5]采用数据聚类算法筛选恶意节点,确保在恶劣环境下节点不会被误判;马吉等[6]通过设置独立的监督网络,实现选择性转发攻击节点的有效检测。然而,多数现有信任和信誉模型未充分考虑恶意节点针对评估系统本身的攻击,而实际网络攻击往往是多种攻击方式共同发起,攻击范围更广、隐蔽性更强[7-8]。

不诚实建议攻击具有攻击范围大、协同性强、隐蔽性好等 特点,传统的信誉模型难以有效识别与防御。孙子文等[9]提出了一种改进的信任评估模型,通过推荐信任可靠度阻止恶意节点对其他节点的群体诽谤;张琳等[10]在传统信誉阈值判断模型的基础上,结合曼哈顿度量和 DPAM 算法,提出基于密度的聚类算法,结合簇间和簇内距离均衡化的目标函数,提高了恶意节点的识别效率;王出航等[11]在遗传算法的基础上,以网络能耗最小以及负载均衡为目标,构建适应度函数,通过寻找最优簇头集,优化安全路径选择;滕志军等[12]引入信誉维护函数、异常弱化因子、模糊评判方法和贴近度理论,提出融合多指标的 WSN 动态信任评估预测模型,提高模型识别的准确性;Anwar 等[13]提出基于信任评估机制的贝叶斯信誉模型,通过将恶意节点与信任节点隔离,防御多种攻击,提高了信誉模型的稳定性。然而,以上方法仅根据节点之间的转发行为来评估节点的直接信任和间接信任,导致误判率居高不下。

群体智能属于计算智能范畴,灵感来源于蚂蚁、白蚁和蜜蜂等群居昆虫的集体行为,为智能信息处理提供了有效的元启发式工具[14]。这类算法应用在 WSN 中,展现出稳健性强、灵活性高、复杂度低等优势[15]。Farah Khedim 等[16]提出了基于生物启发的 WSN 信任模型(BTS),应用模糊控制算法过滤掉不诚实的建议,引入认知计时参数来检测攻击源,解决偏差检验引起的假阳性和假阴性问题,以区分不诚实的建议和错误的建议;Raghav 等[17]提出了一种基于生物启发的安全路由方案,在信任安全机制中引入 ABC 算法,利用侦察蜂优化路径和聚类选择,用于处理泛洪攻击、欺骗干扰和女巫攻击等 WSN 攻击。

现有的防御选择性转发攻击和不诚实建议攻击的方法,仍存在 2 个关键问题亟待解决。第一,节点之间的信任度具有主观性和不确定性,会受到环境等多种因素的影响,在低信任节点中,很难区分恶意节点和由于链路质量差导致的错误节点;第二,当恶意节点数量过多时,信誉保障机制易失效。这两个问题都会引发攻击识别率降低、正常节点误判率升高等不良后果。

为了解决上述问题,本文提出了一种 WSN 中计及信誉度的人工蜂群恶意节点识别策略(CR-ABC)。首先,构建模糊信任模型(fuzzy trust model, FTM),计算相邻节点之间的间接信任,利用模糊综合评价机制,综合多个影响因素计算综合信任值,实现恶意节点和错误节点的有效区分;其次,引入建议偏差值函数和交互指数偏差值函数,通过 ABC 算法优化 FTM 模型,确保在恶意节点数量较多时,系统仍保持较高的识别率和较低的误判率。

1 系统模型

一个节点在与陌生的节点交互之前,需要评估陌生节点的信誉度,请求节点与陌生节点之间的信任值依赖于请求节点(跟随蜂)对目标节点(食物源)的直接观察,以及第三方节点(雇佣蜂)的推荐信息。同时,请求节点还需对第三方推荐节点进行评估,判断是否存在不诚实的推荐行为。CR-ABC 模型可计算交互节点间的直接信任和间接信任。

如图 1 所示,CR-ABC 的工作原理如下:请求节点先在网络中向邻居节点广播信誉查询请求;邻居节点收到请求后,计算待评估节点的直接信任值和间接信任值,并将建议信息反馈给请求节点;请求节点根据多个推荐者(雇佣蜂)发送的数据信息,通过适应度函数和概率计算识别不诚实推荐节点(说谎者),并将其添加到黑名单;剔除不诚实推荐节点后,请求节点计算待评估节点的综合信任值,判断其

是否为恶意节点,若确定为恶意节点,请求节点会将其列入黑名单并全网广播,随后寻找下一个目标节点重复上述流程。

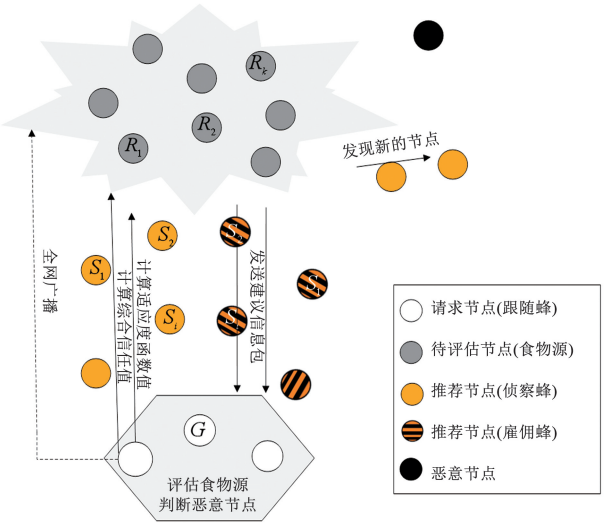

图 1　CR-ABC 模型

Fig. 1　CR-ABC model

2　信誉模型

根据 CR-ABC 模型,节点进行通信时先计算节点的直接信任值和间接信任值,再将信任结果与阈值进行比较,以识别选择性转发攻击。

参考 WSN 贝叶斯信誉评价模型(beta reputation system,BRS)[18],节点 S_i 对待评估节点 R_k 的直接信任值 $\mathrm{DT}_{S_i \to R_k}$ 为:

$$\mathrm{DT}_{S_i \to R_k} = \frac{\mu\alpha + \Delta\alpha}{\mu(\alpha+\beta) + \Delta\alpha + \Delta\beta} \tag{1}$$

$$\mu = \frac{\theta}{\Delta\alpha + \Delta\beta} \tag{2}$$

式中:α 是节点历史正常通信次数;β 是节点历史非正常通信次数;$\Delta\alpha$ 是在阶段时间 t 内节点正常通信次数;$\Delta\beta$ 是在阶段时间 t 内节点非正常通信次数;μ 是信誉维护函数,用于强化现阶段节点行为对信誉值的影响,降低历史行为的影响;θ 是一个固定维护值,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。

在 CR-ABC 模型中,利用模糊综合评判机制分析通信特征、数据属性和物理属性等影响因素,完成对各推荐者的多维度评估。

1)建立信任因素集 M 和信任评判集 E:$M = \{m_1, m_2, m_3\}$,其中 m_1 为能量因素(节点剩余能量),m_2 为转发行为因素(一段时间内节点发送数据包的速率),m_3 为邻节点环境因素(节点的一跳邻居数量);$E = \{e_1, e_2, e_3\}$,其中 e_1 代表不可信,e_2 代表中可信,e_3 代表高度可信。各信任等级对应的隶属度函数分别为 $e_1(t)$、$e_2(t)$ 和 $e_3(t)$,同时 $e_1(t) + e_2(t) + e_3(t) = 1$,如图 2 所示。

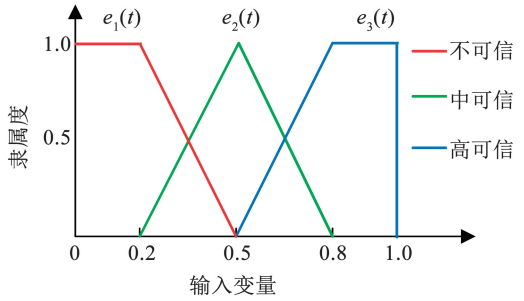

图 2　隶属度函数

Fig. 2　Membership function

2)建立隶属度矩阵 $\boldsymbol{X}$:隶属度矩阵 $\boldsymbol{X}$ 是节点信任因素集 M 中各因素与评判集 E 中各信任等级的关系矩阵。将 3 种评价因素 $M = \{m_1, m_2, m_3\}$ 作为输入变量,代入隶属度函数,可以得到隶属度矩阵 $\boldsymbol{X}$ 为

$$X = \begin{bmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{bmatrix} \tag{3}$$

具体计算流程:将 3 种评价因素集 $M = \{m_1, m_2, m_3\}$ 进行归一化后作为输入变量代入隶属度函数中。例如:计算 x_{11} 时,将归一化后的 m_1 值作为输入变量代入隶属度函数,在 $e_1(t)$ 曲线上找到输入为 m_1 值时,对应的隶属度取值。矩阵 $\boldsymbol{X}$ 的各元素即为相应信任因素指标的隶属度,即第 i 行第 j 列元素 x_{ij},表示从信任因素 m_i 来看,节点对评价集第 j 个评判等级 e_j 的隶属程度。例如,x_{12} 表示节点的能量因素在"中可信"模糊子集范围内的隶属度。

3)确定模糊权重矢量:$z = (z_1, z_2, z_3)$,z_i 为因素集 M 中各评判因素 m_i 的权重,即 z_1 为能量因素的权重,z_2 为转发行为因素的权重,z_3 为邻节点因素的权重,且 $z_1 + z_2 + z_3 = 1$。参考三标度法[19],计算各因素的重要程度,计算得 $z_1 = 0.105$,$z_2 = 0.637$,$z_3 = 0.258$。

4)通过计算模糊权重矢量与隶属度矩阵,得到对各信任因素的模糊综合评价结果向量 P 为

$$P = Z \circ X = (z_1, z_2, z_3) \circ \begin{bmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{bmatrix} = (p_1, p_2, p_3) \tag{4}$$

式中,$\circ$ 为模糊合成算子,p_j 为被评价节点从整体上对模糊子集 e_j 的隶属程度。

利用模糊综合评价机制,通过加权平均法计算节点 S_i 对待评估节点 R_k 的间接信任值 $\mathrm{IT}_{S_i \to R_k}$ 为

$$\mathrm{IT}_{S_i\to R_k}=\frac{\sum_{j=1}^{3}p_j e_j}{\sum_{j=1}^{3}p_j} \tag{5}$$

3 适应度函数

3.1 建议偏差值函数

请求节点整合推荐节点发送的信息包生成建议信息域,并对各节点直接推荐值进行偏差分析,以检测不诚实建议。推荐节点 S_i 与其他 $m-1$ 个推荐者对待评估节点 R_k 的直接推荐值之间的偏差值为

$$d_{T_{S_i}}=\frac{1}{m-1}\sum_{\substack{j=1,\\ j\neq i}}^{m}\left|\mathrm{DT}_{S_i\to R_k}-\mathrm{DT}_{S_j\to R_k}\right| \tag{6}$$

式中,$d_{T_{S_i}}$ 被视为建议偏差值适应度函数,m 是推荐者节点的数量。

3.2 交互指数偏差值函数

串谋节点间会保持密切合作与频繁通信,但与正常节点几乎无交互。不同的信任值导致串谋节点和历史交互节点之间发生指标偏差。用 AI_{S_i} 表示推荐者 S_i 的交互指标,如公式(7);$d_{I_{S_i}}$ 是 S_i 的交互指标偏差值,如公式(8)。

$$\mathrm{AI}_{S_i}=\mathrm{W}_{S_i\leftrightarrow R_k}-\mathrm{RN}_{S_i\to R_k} \tag{7}$$

$$d_{I_{S_i}}=\left|\mathrm{AI}_{S_i}-\mathrm{mean}(\mathrm{AI})\right| \tag{8}$$

式中:$\mathrm{W}_{S_i\leftrightarrow R_k}$ 为 S_i 和 R_k 之间的交互次数;$\mathrm{RN}_{S_i\to R_k}$ 为节点 S_i 推荐节点 R_k 的次数;mean(AI) 为所有雇佣蜂交互指数的平均值。$d_{I_{S_i}}$ 也可作为交互指数偏差值适应度函数。

通过最小化加权法计算两个偏差函数,将多目标问题转化为单目标问题,如等式(9)所示:

$$\min f_{S_i}=\varepsilon d_{T_{S_i}}+\sigma d_{I_{S_i}} \tag{9}$$

式中:f_{S_i} 为推荐者 S_i 的适应度函数,是建议偏差值函数与交互指数偏差值函数的加权和;ε 和 σ 分别为两个适应度函数的权重,$\varepsilon+\sigma=1$。

根据 ABC 算法,每个推荐者 S_i 对应的加权线性适应度函数 fit_{S_i} 为

$$\mathrm{fit}_{S_i}=\frac{1}{1+f_{S_i}} \tag{10}$$

4 CR-ABC 算法实现步骤

4.1 雇佣蜂阶段

推荐者相当于雇佣蜂,其数量由请求节点(跟随蜂)确定。推荐者向请求节点发送建议信息包 $\{\mathrm{ID}_{S_i},\mathrm{Pos}_{S_i},\mathrm{Pos}_{R_k},\mathrm{DT}_{S_i\to R_k},\mathrm{IT}_{S_i\to R_k}\}$,$\mathrm{ID}_{S_i}$ 为推荐者自身的标识码;Pos_{S_i} 为位置信息;Pos_{R_k} 为待评估节点 R_k 最后一次交互时的位置信息;$\mathrm{DT}_{S_i\to R_k}$ 为节点 S_i 对 R_k 的直接信任值,$\mathrm{IT}_{S_i\to R_k}$ 为间接信任值。

4.2 跟随蜂阶段

请求节点根据与每个推荐者相关的概率值 P_{S_i} 对推荐者进行分类,若概率值小于阈值,判定该推荐者为不诚实建议节点。参考 ABC 算法,概率 P_{S_i} 计算公式为

$$P_{S_i}=\frac{\mathrm{fit}_{S_i}}{\sum_{\substack{j=1,\\ j\neq i}}^{m}\mathrm{fit}_{S_j}} \tag{11}$$

剔除不诚实建议节点后,请求节点根据不属于黑名单中的推荐者提供的信息计算待评估节点的综合信任值,即

$$\mathrm{CT}_{S_i\to R_k}=\frac{\sum_{\substack{j=1,\\ j\neq i}}^{m}\left[\mathrm{fit}_{S_j}\times\mathrm{IT}_{S_j\to R_k}\times\exp\left(-d_{T_{S_j\to R_k}}\Big/\sum_{\substack{j=1,\\ j\neq i}}^{m}d_{T_{S_i\to R_k}}\right)\right]}{\sum_{\substack{j=1,\\ j\neq i}}^{y}\mathrm{fit}_{S_j}} \tag{12}$$

式中 $\exp\left(-d_{T_{S_j\to R_k}}\Big/\sum_{\substack{j=1,\\ j\neq i}}^{m}d_{T_{S_i\to R_k}}\right)$ 为具有较小偏差值的推荐节点的间接信任值赋予更大的权重。

4.3 侦察蜂阶段

如果节点 R_k 的综合信任值 $\mathrm{CT}_{S_i\to R_k}$ 大于系统阈值,则在节点 S_i 和节点 R_k 之间建立可信链路用以转发信息。侦察蜂观察并记录节点 R_k 的交互行为,并通过 FTM 更新其直接信任值和间接信任值;如果节点 R_k 的综合信任值 $\mathrm{CT}_{S_i\to R_k}$ 小于阈值,请求节点将把恶意节点添加到黑名单中,通过 WSN 进行广播,随后开始接收另一评估节点的请求信息并进入新的循环。

4.4 CR-ABC 算法的主要步骤

Step1:设置全局节点数量为 N,推荐节点数量为 m,邻节点间相互观察统计,根据公式(1)计算待评估节点的直接信任值;

Step2:依据模糊综合评判机制,利用公式(5)计算待评估节点的间接信任值;

Step3:请求节点收集所有的建议信息包后,利用公式(6)计算建议偏差值函数,再根据公式(7)和(8)计算交互指数偏差值函数;

Step4:根据公式(9)和(10)计算推荐者的适应度函数值,剔除不诚实建议节点,再根据公式(12)计算待评估节点的综合信任值,结果低于阈值判断为恶意节点,并将其列入黑名单;

Step5:拉黑恶意节点并全网广播,发起下一轮请求或等待新一轮请求信息。

CR-ABC 算法伪代码如表 1 所示。

表 1　CR-ABC 算法伪代码

Tab. 1　CR-ABC algorithmic pseudocode

CR-ABC 算法描述
Begin
1. 请求节点 G 发送一个请求
2. ＊＊＊＊＊侦察蜂阶段＊＊＊＊＊
3. 邻居节点 S_i 接收到请求信息
4. 计算待评估节点 R_k 的直接信任值 $DT_{S_i \to R_k}$
5. 计算待评估节点的间接信任值 $IT_{S_i \to R_k}$
6. ＊＊＊＊＊雇佣蜂阶段＊＊＊＊＊
7. 发送建议信息包 $\{ID_{S_i}, Pos_{S_i}, Pos_{R_k}, DT_{S_i \to R_k}, IT_{S_i \to R_k}\}$ 给请求节点 G
8. ＊＊＊＊＊跟随蜂阶段＊＊＊＊＊
9. 请求节点计算适应度函数值
10. 计算待评估节点 R_k 的综合信任值 $CT_{S_i \to R_k}$
11. 判断待评估节点 R_k 是否为恶意节点
12. 拉黑恶意节点并向全网广播
13. ＊＊＊＊＊侦察蜂阶段＊＊＊＊＊
14. 更新恶意节点黑名单并向全网广播
End

5　仿真实验及分析

为对比 CR-ABC 模型与文献[16]的 BTS 模型、文献[20]的信任聚类模型(TBCS)、文献[21]的信任系统攻击防御模型(DTSA)的安全性能,参考文献[18]中的参数设置,在 MATLAB 中搭建仿真环境。实验初始设定所有的正常节点都能完全响应通信请求,详细参数如表 2 所示。

表 2　仿真参数

Tab. 2　Simulation parameters

参数	数值
仿真区域	100 m×100 m
节点总数	100 个
簇头节点个数	4 个
恶意节点个数	0~50 个
通信半径	10 m
初始信任值	0.5
节点初始能量	2 J
数据包大小	800 bit

在安全性能分析实验中,选择性转发攻击节点以 50% 的概率随机丢弃数据包。网络模型评估指标包括恶意节点识别率(RP)和正常节点误判率(FPP),如公式(13)和公式(14)所示:

$$RP = \frac{\text{已识别恶意节点数}}{\text{恶意节点总数}} \times 100\% \tag{13}$$

$$FPP = \frac{\text{正常节点被误判数}}{\text{正常节点总数}} \times 100\% \tag{14}$$

5.1　信任值分析

如图 3 所示,本文信任评价模型对恶意行为的变化更加敏感。当节点与其他节点良好协作时,信任值在 25 秒内缓慢增长,30 秒后趋于稳定,约为 0.9。然而,如果节点不合作,模型将迅速降低其信任值,3 秒后信任值低于 0.2,此后 8 秒内信任值降低至接近 0.1,随后被拉入黑名单。这是因为本文在信任值计算中引入历史评价,正常节点的信任值无回落趋势,利用人工蜂群算法优化信任模型识别不诚实节点,快速收敛恶意节点的信任值,10 秒内全网节点将不再与该恶意节点通信,使得恶意节点的信任值无回升趋势。

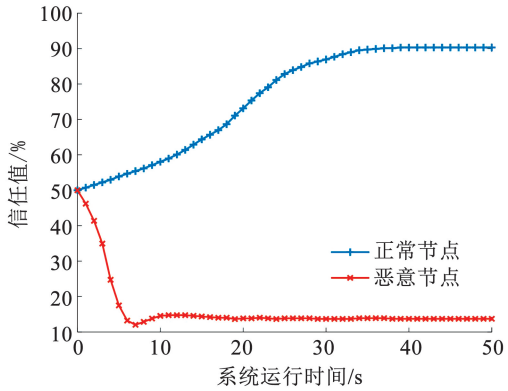

图 3　信任值收敛情况

Fig. 3　Trust value convergence

5.2　选择性转发攻击场景分析

如图 4 所示,CR-ABC 算法运行在 5 秒之后,当恶意节点超过 5 个时,识别率达到 85% 以上。这是因为较少的恶意节点隐蔽性较好,而模型在初始运行阶段需要更多的时间收集数据信息;随着系统运行,节点运行状态数据增加,模型计算节点综合信任值的准确性也随之提升。当运行时间超过 20 秒后,识别率保持在 90% 以上。恶意节点数量的增加对识别率影响不大,原因在于本模型通过多个节点的推荐值计算评估节点的信任程度,并对这些推荐节点进行评估,剔除建议偏差值较大的信息,从而在选择性转发攻击节点数量增加的情况下,系统仍可以保持安全性和稳定性。

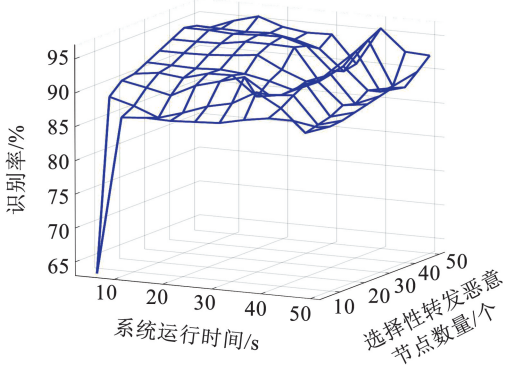

图 4　选择性转发攻击节点识别率

Fig. 4　Identification rates of nodes under selective forwarding attacks

图 5 中 CR-ABC 算法运行 5 秒后，当恶意节点超过 5 个时，误判率低于 8%。20 秒后，误判率低于 5%。恶意节点数量的增加导致误判率略有上升，但总体趋势可控。这是因为本模型在计算适应度函数时，考虑了通信链路、工作环境等非恶意因素对节点建议偏差值的影响，综合了节点的通信特性、数据属性和物理属性 3 个因素，通过模糊综合评判算法再次评估推荐节点，因此在恶意节点数量增加后，系统仍可保持误判率无明显增长。仿真结果验证了该模型在选择性转发攻击下恶意节点识别的准确性和有效性。

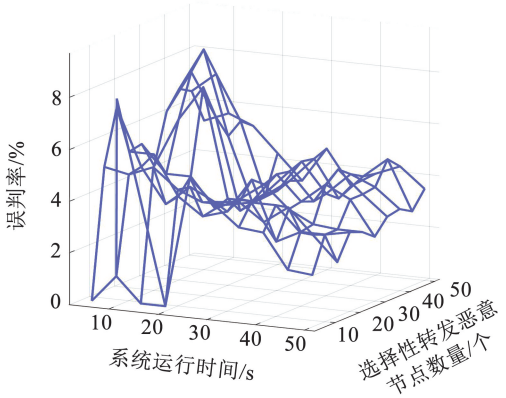

图 5 选择性转发攻击节点误判率

Fig. 5 Misjudgment rates of nodes under selective forwarding attacks

图 6 反映了 4 种模型在不同恶意节点数量下的识别率变化情况。当恶意节点数量超过 5 个时，CR-ABC 的 RP 大于 90%，与其他 3 种模型相比，CR-ABC 的识别率总体提高了约 2%，且在恶意节点数量较大的情况下仍能保持稳定。

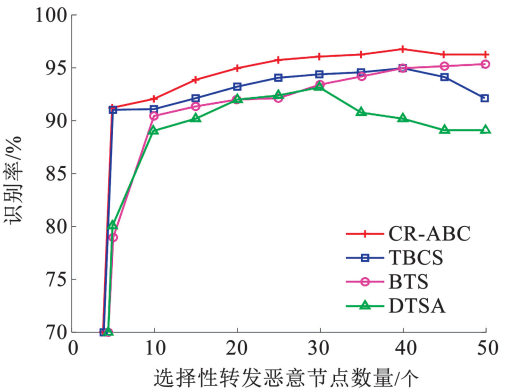

图 6 选择性转发攻击下不同模型识别率比较

Fig. 6 Comparison of identification rates of different models under selective forwarding attacks

图 7 是 4 种模型在不同恶意节点数量下的误判率对比。与其他 3 种模型相比，CR-ABC 的 FPP 总体降低了约 2%。当 WSN 中恶意节点数量增加时，各安全模型的压力也会增大，本文算法误判率略有上升，但趋势相对平缓，主要原因在于利用 ABC 算法优化信任模型，并应用智能模糊规则检测异常值。

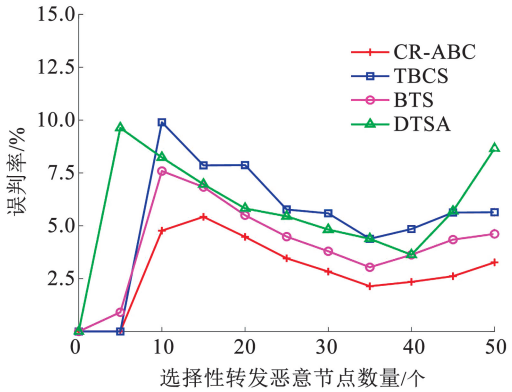

图 7 选择性转发攻击下不同模型误判率比较

Fig. 7 Comparison ofmisjudgment rates of different models under selective forwarding attacks

5.3 不诚实建议攻击场景分析

1）诽谤攻击场景分析

在诽谤攻击下，恶意推荐者故意提供邻居节点的负面建议值。如图 8 所示，CR-ABC 算法的识别率保持在 86% 以上。当建议偏差值较低时，模型识别率偏低，这是因为此时恶意节点提供的不诚实建议值变化不明显。例如：建议偏差值为 0.1，节点真实信任值为 0.8，则恶意节点提供的不诚实建议值为 0.72(0.8 × (1 − 0.1) = 0.72)。随着建议偏差值的提高，恶意节点提供的不诚实建议值变化更加明显，模型识别率不断提高。例如：建议偏差值为 0.5，节点的真实信任值为 0.8，则恶意节点提供的不诚实建议值为 0.4(0.8 × (1 − 0.5) = 0.4)。当恶意节点数不断增加后，模型的识别率会有所降低，这是因为恶意节点的数量较多时，系统需要更多的时间来选择可信任节点进行交互。

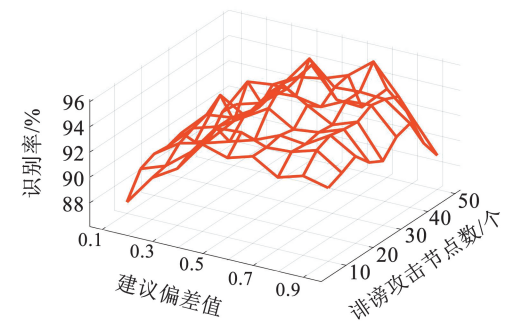

图 8 诽谤攻击下的识别率

Fig. 8 Identification rates under defamation attacks

如图 9 所示，CR-ABC 算法的误判率保持在 13% 以下，当建议偏差值较低时，模型误判率偏高；随着建议偏差值的提高，模型的误判率不断降低。当网络中恶意节点数量增加时，模型的误判率会有所升高，但网络仍能保持正常通信。

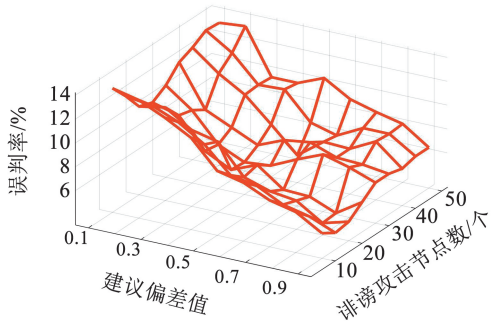

图 9　诽谤攻击下的误判率

Fig. 9　Misjudgment rates under defamation attacks

2)塞选票攻击场景分析

针对塞选票攻击,恶意推荐者为其他恶意节点提供更高建议值,影响信誉评估的结果。CR-ABC 算法融合模糊综合评价机制,综合多因素计算待评估节点综合信任值,提高信誉模型的检测精度。如图 10 所示,CR-ABC 算法的识别率保持在 82% 以上,引入建议偏差值函数和交互指数偏差值函数,确保在恶意节点数量过多时,系统仍保持较高的识别率和较低的误判率。

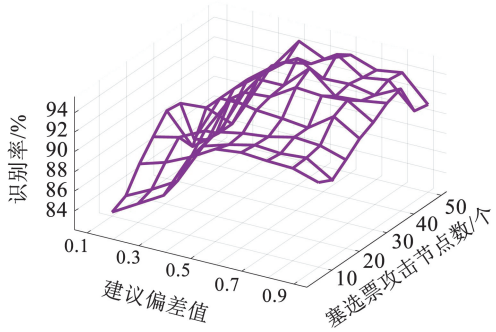

图 10　塞选票攻击下的识别率

Fig. 10　Identification rates under ballot stuffing attacks

CR-ABC 基于模糊综合评判机制计算节点的间接信任,同时利用 ABC 算法优化信誉模型,使模型可以在恶意节点数量较多时仍保持安全性和准确性。如图 11 所示,CR-ABC 算法的误判率保持在 13% 以下。

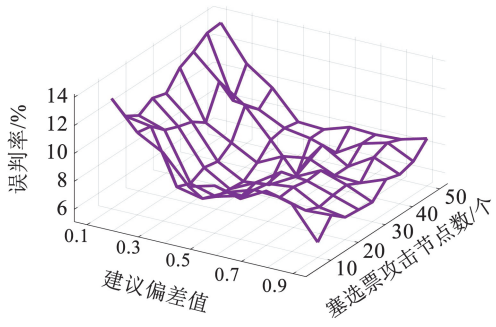

图 11　塞选票攻击下的误判率

Fig. 11　Misjudgment rates under ballot stuffing attacks

3)串谋攻击场景分析

诽谤攻击和塞选票攻击结合即为串谋攻击。图 12 显示了当建议偏差值为 0.5 时,恶意节点数量与性能之间的关系曲线。CR-ABC 的识别率约为 90%,比 FTM 高 3% 左右,误判率稳定在 10% 左右,比 FTM 低 11% 左右,且 CR-ABC 的性能受串谋节点数量变化影响较小。

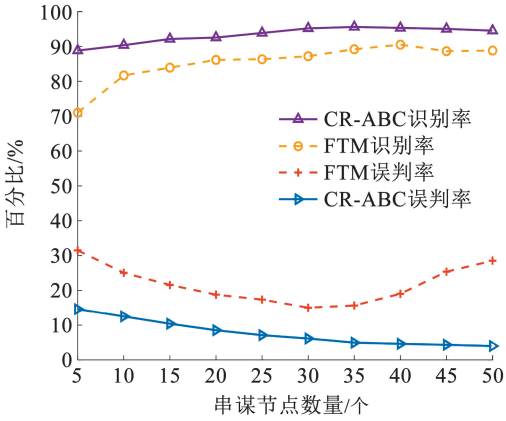

图 12　改变串谋节点数量的 CR-ABC 性能分析

Fig. 12　Performance analysis of CR-ABC with varying number of collusion nodes

图 13 显示了当存在 25 个串谋节点时,建议偏差值与性能之间的关系曲线。当建议偏差值≤0.4 时,CR-ABC 的识别率从 82% 升至 90%,FTM 的识别率在71% ~85% 之间,FTM 的误判率始终高于 CR-ABC。这是因为在没有 ABC 算法优化的情况下,FTM 更难区分虚假推荐和小的恶意偏差。当建议偏差值达到 0.5 后,CR-ABC 仍保持较高的识别率和较低的误判率。

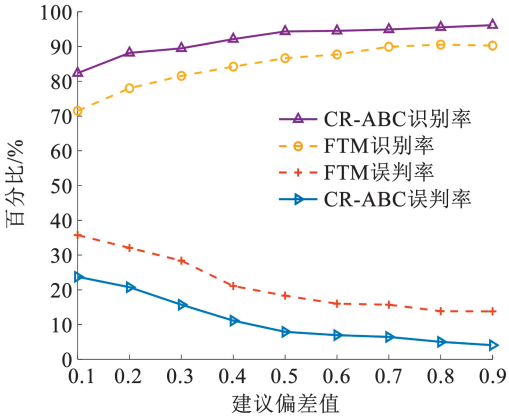

图 13　改变建议偏差值的 CR-ABC 性能分析

Fig. 13　Performance analysis of CR-ABC with varying recommended deviation value

5.4　不同模型实时性分析

传输延时会随着恶意节点的增加而增加。恶意节点不合作、拒绝转发数据包等行为均会造成传输延时的增加。图 14 是不同模型的实时性比较,当恶意节点数量在 0 ~30 时,3 种对比模型的毫秒级端到端延时差别不大,本文 CR-ABC 模型的端到端延时低于对比模型。这是因为 CR-ABC 模型综合通信

特征、数据属性、物理属性 3 个方面的影响因素计算综合信任值,提高了信誉模型的检测精度。当恶意节点数量超过 30 时,CR-ABC 模型的传输延时仍优于与其他 3 种模型。这是因为 TBCS 模型和 DTSA 模型仅基于模糊综合评判机制提升信任评估的准确性;BTS 模型仅利用 ABC 算法优化信任模型。当恶意节点数量过多时,信任评估准确性均有所下降。相比之下,本文提出的 CR-ABC 模型利用 ABC 算法优化信任模型,同时应用智能模糊规则检测异常值,保证了在恶意节点数量过多时信任评估仍然有效,减缓了端到端延时的增长速度。

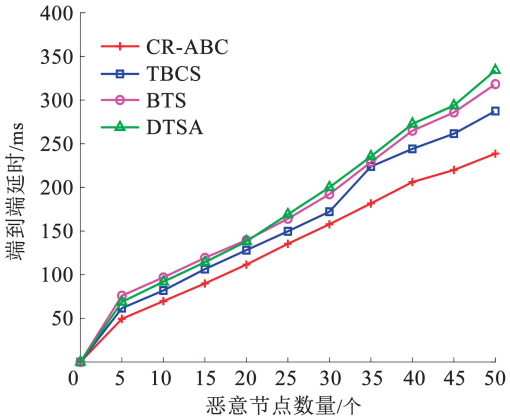

图 14 不同模型实时性分析

Fig. 14 Real-time analysis of different models

5.5 算法复杂度分析

表 3 算法复杂度分析

Tab. 3 Algorithm complexity comparison

	时间复杂度 $T(n)$	空间复杂度 $S(n)$
CR-ABC	$O(n)$	$O(1)$
TBCS	$O(n^2)$	$O(n)$
BTS	$O(n)$	$O(n)$
DTSA	$O(n)$	$O(1)$

算法的时间复杂度通常用时间复杂度函数 $T(n)$ 表示,是指执行算法所需要的计算工作量随问题规模 n(本文中 n 为网络节点数)变化的函数关系。本文提出的 CR-ABC 算法中,核心操作(如遍历节点、计算信任值与偏差值)是对问题规模 n 的线性遍历,其时间复杂度函数 $T(n)$ 由 n 决定,因此该算法的时间复杂度为 $O(n)$,即具有线性时间复杂度。

算法的空间复杂度用空间复杂度函数 $S(n)$ 表示,是指运行过程中所需存储空间随问题规模 n 变化的函数关系。本文提出的 CR-ABC 的存储空间仅用于存储建议信息包 $\{\mathrm{ID}_{S_i}, \mathrm{Pos}_{S_i}, \mathrm{Pos}_{R_k}, \mathrm{DT}_{S_i \to R_k}, \mathrm{IT}_{S_i \to R_k}\}$,其空间消耗不随 n 增大而增加。因此本文算法的空间复杂度为 $S(n) = O(1)$,即常数阶。

6 结 语

由于环境的开放性和资源的有限性,WSN 节点容易受到各种攻击,传统的信誉模型难以有效抵御不诚实建议攻击等协同式攻击。本文提出一种 WSN 计及信誉度的人工蜂群恶意节点识别策略,用于防御选择性转发攻击和不诚实建议攻击。该策略基于模糊信誉模型,依据节点的多属性状态评判推荐节点,引入建议偏差值函数和交互指数偏差值函数计算适应度值,通过 ABC 算法优化模糊信誉模型,使系统在恶意节点数量较多时,仍能保持较高的识别率和较低的误判率。仿真实验结果表明,CR-ABC 模型在选择性转发攻击和不诚实建议攻击下均能保证准确性和有效性,在恶意节点数量较多时仍能稳定安全运行。未来的工作将侧重于研究自适应阈值和权重设置对系统性能的影响。

参考文献

[1]王天荆, 李秀琴, 白光伟, 等. 无线传感器网络中基于自适应网格的多目标定位算法[J]. 通信学报, 2019, 40(7):197
WANG Tianjing, LI Xiuqin, BAI Guangwei, et al. Multi-target localization algorithm based on adaptive grid in wireless sensor network[J]. Journal of Communications, 2019, 40(7): 197. DOI: 10.11959/j.issn.1000-436x.2019129

[2]张丹,张悦,藏晓鑫. 基于自组织数学模型的监控视频异常入侵检测方法[J]. 东北电力大学学报,2022, 42(4): 63
ZHANG Dan, ZHANG Yue, ZANG Xiaoxin. An abnormal intrusion detection method of surveillance video based on self-organizing mathematical model [J]. Journal of Northeast Electric Power University, 2022, 42(4): 63. DOI:10.19718/j.issn.1005-2992.2022-04-0063-07

[3]REN J, ZHANG Y, ZHANG K, et al. Adaptive and channel-aware detection of selective forwarding attacks in wireless sensor networks [J]. IEEE Transactions on Wireless Communications, 2016, 15(5): 3718. DOI:10.1109/TWC.2016.2526601

[4]尹荣荣, 张文元, 杨绸绸, 等. 一种基于多跳确认和信任评估的选择性转发攻击检测方法[J]. 控制与决策, 2020, 35(4): 949
YIN Rongrong, ZHANG Wenyuan, YANG Chouchou, et al. A selective forwarding attacks detection approach based on multi-hop acknowledgment and trust evaluation [J]. Control and Decision, 2020, 35(4): 949. DOI:10.13195/j.kzyjc.2018.0608

[5]LIU Y, WU Y. Employ DBSCAN and neighbor voting to screen selective forwarding attack under variable environment in event-driven wireless sensor networks [J]. IEEE Access, 2021, 9: 77090. DOI:10.1109/access.2021.3083105

[6]马吉,杜永文,夏金棕. 基于独立监督网络的选择性转发攻击检测[J]. 传感技术学报,2022,35(4):538
MA Ji, DU Yongwen, XIA Jinzong. Selective forwarding attack detection based on independent supervised networks[J]. Chinese Journal of Sensors and Actuators, 2022, 35(4): 538. DOI:10.3969/j.issn.1004-1699.2022.04.017

[7]李建坡,张庆华,张展图,等. 基于拥塞控制的无线传感器网络能耗优化路由算法[J]. 东北电力大学学报,2020,40(4):69
LI Jianpo, ZHANG Qinghua, ZHANG Zhantu, et al. Optimized

routing algorithm for energy consumption of wireless sensor networks based on congestion control[J]. Journal of Northeast Electric Power University, 2020, 40(4): 69. DOI:10.19718/j.issn.1005-2992.2020-04-0069-06

[8] GABER T, ABDELWAHAB S, ELHOSENY M, et al. Trust-based secure clustering in WSN-based intelligent transportation systems [J]. Computer Networks, 2018, 146: 151. DOI: 10.1016/j.comnet.2018.09.015

[9] 孙子文, 吴平. 基于信任评估模型的 IWSN 安全路由研究[J]. 传感技术学报, 2019, 32(6): 858
SUN Ziwen, WU Ping. Research on secure routing of IWSN based on trust evaluation model[J]. Chinese Journal of Sensors and Actuators, 2019, 32(6): 858

[10] 张琳, 尹娜, 王汝传. 无线传感网中基于 DPAM-MD 算法的恶意节点识别研究[J]. 通信学报, 2015, 36(S1): 53
ZHANG Lin, YIN Na, WANG Ruzhuan. Research of malicious nodes identification based on DPAM-MD algorithm for WSN[J]. Journal of Communications, 2015, 36(S1): 53. DOI:10.11959/j.issn.1000-436x.2015281

[11] 王出航, 王雪, 胡黄水, 等. 基于改进 GA 和信任感知的无线传感器网络安全分簇路由协议[J]. 吉林大学学报(理学版), 2021, 59(5): 1237
WANG Chuhang, WANG Xue, HU Huangshui, et al. Secure clustering routing protocol based on improved GA and trust-aware for wireless sensor networks[J]. Journal of Jilin University (Science Edition), 2021, 59(5): 1237. DOI:10.13413/j.cnki.jdxblxb.2020197

[12] 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. A dynamic trust evaluation and prediction model for WSN based on multiple indexes [J]. Journal of Zhengzhou University (Engineering Science), 2023, 44(3): 76. DOI:10.13705/j.issn.1671-6833.2022.06.014

[13] ANWAR R W, ZAINAL A, OUTAY F, et al. BTEM: Belief based trust evaluation mechanism for wireless sensor networks[J]. Future Generation Computer Systems, 2019, 96: 605. DOI: 10.1016/j.future.2019.02.004

[14] GAMBHIR A, PAYAL A, ARYA R. Performance analysis of artificial bee colony optimization based clustering protocol in various scenarios of WSN[J]. Procedia Computer Science, 2018, 132: 183. DOI:10.1016/j.procs.2018.05.184

[15] ARI A A A, LABRAOUI N, YENKE B O, et al. Clustering algorithm for wireless sensor networks: The honeybee swarms nest-sites selection process based approach[J]. International Journal of Sensor Networks, 2018, 27(1): 1. DOI:10.1504/IJSNET.2018.092101

[16] KHEDIM F, LABRAOUI N, ARI A A A. A cognitive chronometry strategy associated with a revised cloud model to deal with the dishonest recommendations attacks in wireless sensor networks[J]. Journal of Network and Computer Applications, 2018, 123: 42. DOI:10.1016/j.jnca.2018.09.001

[17] RAGHAV R S, THIRUGNANSAMBANDAM K, ANGURAJ D K. Beeware routing scheme for detecting network layer attacks in wireless sensor networks[J]. Wireless Personal Communications, 2020, 112: 2439. DOI:10.1007/s11277-020-07158-9

[18] 滕志军, 杜春秋, 孙汇阳, 等. 融合节点信誉度和路径跳数的 WSNs 虫洞攻击检测策略[J]. 哈尔滨工业大学学报, 2021, 53(8): 64. DOI:10.11918/202101035
TENG Zhijun, DU Chunqiu, SUN Huiyang, et al. WSNs wormhole attack detection strategy combining node reputation and path hop count[J]. Journal of Harbin Institute of Technology, 2021, 53(8): 64. DOI:10.11918/202101035

[19] DONG H. Computationally efficient higher-order three-scale method for nonlocal gradient elasticity problems of heterogeneous structures with multiple spatial scales[J]. Applied Mathematical Modelling, 2022, 109: 426. DOI:10.1016/j.apm.2022.05.010

[20] SINGH K, VERMA A K. TBCS: A trust based clustering scheme for secure communication in flying Ad-Hoc networks[J]. Wireless Personal Communications, 2020, 114: 3173. DOI: 10.1007/s11432-010-0050-8

[21] 陶洋, 潘蕾娜, 王进, 等. 防御信任攻击的无线传感器网络安全信任评估模型[J]. 传感技术学报, 2018, 31(12): 1876
TAO Yang, PAN Leina, WANG Jin, et al. Security trust evaluation model for wireless sensor networks against trust attacks[J]. Chinese Journal of Sensors and Actuators, 2018, 31(12): 1876

(编辑　丁晓清)