文章编号:1007-5321(2025)05-0069-07 **DOI**:10.13190/j.jbupt.2024-171

融合 IF 和 GBO 算法的 Sinkhole 攻击识别与安全路径选择策略

余修武[1,2,3], 晋诗琪[1], 张 可[1]

(1. 南华大学 资源环境与安全工程学院, 衡阳 421001; 2. 湖南省铀尾矿库退役治理技术工程技术研究中心, 衡阳 421001;
3. 铀矿冶放射性控制技术湖南省工程研究中心, 衡阳 421001)

摘要: 为了有效应对无线传感器网络(WSN)中的 Sinkhole 攻击,提出了一种融合孤立森林(IF)和梯度优化算法(GBO)的 Sinkhole 攻击识别与安全路径选择策略(IF-GBO)。首先,通过设定检测阈值以触发 IF-GBO 入侵检测机制,减少网络开销,提高检测效率。其次,结合 Sinkhole 攻击的特点以及 WSN 数据的动态实时性,设计了包含节点跳数、能耗、数据包接收/转发率和时延等多维特征的数据集,并采用滑动窗口采样的方式进行模型训练,不仅提高了算法的运行效率,还增强了识别异常节点的精确度。最后,建立多目标路径选择函数,利用 GBO 算法帮助节点快速寻找新的传输路径以应对 Sinkhole 攻击,有效保证了数据的可靠传输,延长了网络寿命,并解决了异常检测结果无法及时传输至真实 Sink 节点的问题。实验结果表明,相较于支持向量机(SVM)、K 最近邻(KNN)、局部异常因子(LOF)等经典的异常检测模型,IF-GBO 能够准确识别出恶意节点,且具有更低的误判率和更强的泛化能力。与基于跳数的 Sinkhole 攻击检测算法(HCODESSA)和最小跳数选择的随机路径检测算法(RMHSD)相比,GBO 防御策略能有效缓解 Sinkhole 攻击对网络的破坏,确保了路由的安全性和可靠性。

关 键 词: 无线传感器网络; 网络安全; Sinkhole 攻击; 入侵检测系统; 孤立森林算法

中图分类号: TP393.0 **文献标志码**: A

Sinkhole Attack Identification and Secure Path Selection Strategy Integrating IF and GBO Algorithms

YU Xiuwu[1,2,3], JIN Shiqi[1], ZHANG Ke[1]

(1. School of Resource and Environment and Safety Engineering, University of South China, Hengyang 421001, China;
2. Hunan Engineering Research Center for Uranium Tailings Decommission and Treatment, Hengyang 421001, China;
3. Hunan Province Engineering Research Center of Radioactive Control Technology in Uranium Mining and Metallurgy, Hengyang 421001, China)

Abstract: To effectively mitigate Sinkhole attacks in wireless sensor networks (WSN), this paper proposes a novel Sinkhole attack detection and defense strategy (IF-GBO) that integrates isolation forest (IF) and gradient-based optimizer (GBO). First, a detection threshold is established to trigger the IF-GBO intrusion detection mechanism, thereby reducing network overhead and improving detection efficiency. Second, considering the characteristics of Sinkhole attacks and the dynamic real-time nature of WSN data, a multidimensional feature dataset is designed, incorporating node hop count, energy consumption, packet reception/forwarding rate, and time delay. The model is trained using a sliding window sampling approach, which not only enhances the algorithm's operational efficiency but also improves the accuracy of malicious node identification. Finally, a multi-objective path selection function

收稿日期: 2024-08-21
基金项目: 湖南省自然科学基金项目(2024JJ5338)
作者简介: 余修武(1976—), 男, 教授, 硕士生导师, 邮箱:yxw2008xy@163.com。

is developed, leveraging the GBO algorithm to assist nodes in rapidly identifying alternative transmission paths to counter Sinkhole attacks. This approach effectively ensures reliable data transmission, extends network lifetime, and resolves the issue of delayed delivery of anomaly detection results to the legitimate sink node. Experimental results demonstrate that compared to conventional anomaly detection models such as support vector machine (SVM), k-nearest neighbors (KNN) and local outlier factor (LOF), IF-GBO achieves higher accuracy in identifying malicious nodes with lower false positive rates and superior generalization capability. Furthermore, when compared to dedicated Sinkhole attack detection algorithms like hop count-based detection scheme for Sinkhole attack (HCODESSA) and a Sinkhole detection algorithm based on the random routes selected by minimum hop (RMHSD), the GBO-based defense strategy significantly mitigates the disruptive effects of Sinkhole attacks on the network, ensuring routing security and reliability.

Key words: wireless sensor network; network security; Sinkhole attack; intrusion detection algorithm; isolation forest algorithm

无线传感器网络(WSN, wireless sensor network)是一种由分布式传感器组成的无线网络[1],在灾后应急救援等领域均得到了广泛的应用[2-3],但由于其通常部署在资源有限的开放环境,易遭受各种网络攻击,而安全的路由机制是防止内外部攻击的重要技术之一[4]。目前,常见的攻击方式主要包括选择性转发攻击、虫洞攻击、Sinkhole 攻击等[5-7]。其中,Sinkhole 攻击通过广播虚假信息,声称自己是汇聚节点或伪装成通往基站的最短路径,吸引周围节点的数据流量,并随意篡改或丢弃数据,具有很强的破坏性[8]。

入侵检测系统(IDS, intrusion detection system)作为第2层网络防御机制,通过实时动态的监控来识别网络中潜在的异常行为[9-10]。早期 WSN 入侵检测主要是通过关注节点行为来实现,随着网络规模扩大,检测方法拓展到利用信任模型来判断节点行为是否异常[11-13]。近年来,学者们认为将机器学习(ML, machine learning)应用于 IDS 具有广阔的研究前景,ML 算法能够自动学习数据间的关系,提取有用信息并进行分析预测[9]。

针对 Sinkhole 攻击,Lanka 等[14]提出了一种基于跳数的 Sinkhole 攻击检测方案(HCODESSA, hop count-based detection scheme for Sinkhole attack),通过计算每个节点在遭受 Sinkhole 攻击前后的跳数变化来识别恶意节点,但对于跳数改变不明显但是仍处于攻击区域内的这类边缘节点,该算法难以精准识别。Zhang 等[15]提出了一种最小跳数选择的随机路径检测算法(RMHSD, a Sinkhole detection algorithm based on the random routes selected by minimum hop),通过统计不同路径中每个节点出现的次数,并计算节点与邻居节点间的跳数差,去评估节点的异常度,有效提高了识别率。但当恶意节点部署在远离 Sink 节点的区域时,则很难检测到。Prathapchandran 等[16]提出了一种基于低功耗和不可靠网络路由协议(RPL, routing protocol for low-power and lossy networks)下的随机森林信任感知安全机制(RFTrust, random forest trust)算法,该算法结合了随机森林和主观逻辑来识别 Sinkhole 攻击,有效抵御了 Sinkhole 攻击。Mohammed 等[17]提出了一种基于增强信誉的 IDS。所有节点根据自身能耗与簇内平均能耗的差距计算间接信任值,直接信任值则依据节点的数据包投递率,基站建立包含所有节点信息的信任矩阵,并利用人工蜂群算法识别恶意节点。但基站可以收到所有节点任意时刻的信息是不符合实际的,因为恶意节点很大概率会在下一轮竞选中成为簇首,将簇内收集的信息直接丢弃或篡改后发送给基站。

目前,现有研究仍存在一些需要解决的问题。所提方法只能检测是否存在 Sinkhole 攻击,而不能定位攻击者的坐标,且大多没有具体的防御措施,仅关注恶意节点的识别率。因此,提出了一种融合孤立森林(IF, isolation forest)和梯度优化(GBO, gradient-based optimizer)算法的 Sinkhole 攻击识别与安全路径选择策略。首先,设定入侵检测阈值以降低能耗开销;利用滑动窗口对多维数据进行采样,提高算法的运行效率和异常节点识别的精确度。最后,为有效抵御 Sinkhole 攻击对网络的破坏,构建了一个多目标路径选择函数。利用 GBO 算法帮助节

点迅速找到一条避开恶意节点并到达真实 Sink 的最优路径。

1　系统模型与相关假设

1.1　网络模型

WSN 模型主要包含以下几点：

1）网络由若干传感器节点和 1 个 Sink 节点组成，所有节点随机部署后，选择最短路径建立多跳路由，Sink 节点的能量不受限；

2）所有节点均为同一型号的传感器，有相同的存储容量、计算能力、通信半径 r 和初始能量 E_0；

3）每个节点都可以与通信半径内的邻居节点双向通信，并建立路由表。

1.2　能量模型

节点向距离为 d 的另一节点或基站发送 k bit 数据的能耗为

$$E_{\mathrm{TX}}(k,d)=\begin{cases}kE_{\mathrm{elec}}+k\varepsilon_{\mathrm{fs}}d^2, & d<d_0\\ kE_{\mathrm{elec}}+k\varepsilon_{\mathrm{amp}}d^4, & d\geqslant d_0\end{cases}\tag{1}$$

其中：$\varepsilon_{\mathrm{fs}}$ 和 $\varepsilon_{\mathrm{amp}}$ 分别为自由空间模型和多路径衰减模型中的功率放大特性常数，E_{elec} 为每比特数据传输的能耗，通过比较 d 与阈值 d_0 的大小来选择信道模型，d_0 的计算如下：

$$d_0=\sqrt{\frac{\varepsilon_{\mathrm{fs}}}{\varepsilon_{\mathrm{amp}}}}\tag{2}$$

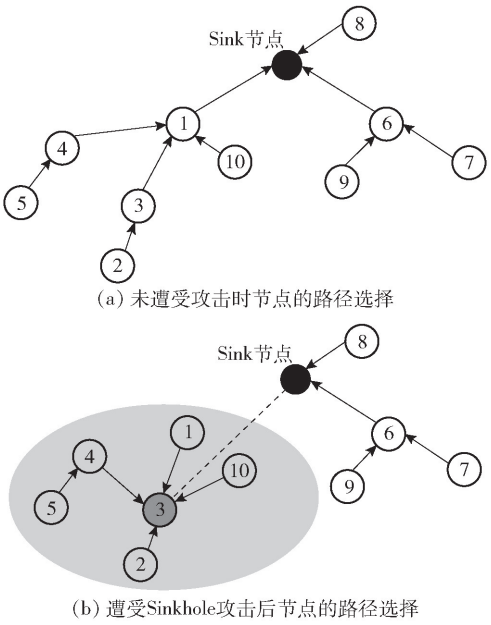
d_0 通常设为 87 m，节点接受 k bit 数据的能耗为

$$E_{\mathrm{RX}}(k)=kE_{\mathrm{elec}}\tag{3}$$

1.3　Sinkhole 攻击模型

定义受到 Sinkhole 攻击的节点称为恶意节点，在恶意节点的影响下，改变传输路径的节点为被污染节点，2 者统称为异常节点。为了便于后续的实验验证，假设恶意节点有 50% 的概率选择直接丢弃数据包，50% 的概率选择篡改数据后再发送给 Sink 节点。

Sinkhole 攻击的原理示意图如图 1 所示。



（a）未遭受攻击时节点的路径选择

（b）遭受Sinkhole攻击后节点的路径选择

图 1　Sinkhole 攻击模型

2　基于 IF 算法识别异常节点

2.1　IF 算法

IF 是一种高效的异常检测算法，通过随机选择特征和分割点构建孤立树（iTree），利用叶子节点到根节点的路径长度来判断数据是否异常。IF 不依赖标签数据，且 iTree 的构建过程相互独立，易于实现并行化，适应分布式计算环境[18]。路径长度是指从根节点遍历 iTree 直到外部节点处终止，其所经历的边长，记为 $h(x)$。数据 x 的路径长度计算如下：

$$c(\psi)=\begin{cases}2H(\psi-1)-2(\psi-1)/\psi, & \psi>2\\ 1, & \psi=2\\ 0, & \text{其他}\end{cases}\tag{4}$$

其中：ψ 为叶子节点数，$H(i)=Ln(i)+\gamma$ 为谐波数，γ 为欧拉常数，$C(\psi)$ 为给定 ψ 的路径长度的平均值，用于标准化 $h(x)$。数据 x 的异常分数计算式如下：

$$s(x,\psi)=2^{\frac{E(h(x))}{c(\psi)}}\tag{5}$$

其中：$E(h(x))$ 是 $h(x)$ 在 iTree 集合上的平均值，当 $E(h(x))\to c(\psi)$，$s\to 0.5$，说明该样本中可能没有明显的异常点；当 $E(h(x))\to 0$，$s\to 1$，x 被认为是异常点；$E(h(x))\to n-l$，$n\geqslant 1$，$s\to 0$，x 被认为是正常点。

2.2　入侵检测阈值

网络受到 Sinkhole 攻击后，网络吞吐量会明显下降。数据包传递率（PDR，packet delivery ratio）表示成功传递到 Sink 节点的数据包数量与源节点发送的数据包总数的比例。因此，设置 1 个启动入侵检测的阈值 w_{th}，若某一时间段内的 $P_{\mathrm{DR}}<w_{\mathrm{th}}$，说明网络可能遭受了 Sinkhole 攻击，需要开启 IDS。

2.3　滑动窗口采样

滑动窗口采样是一种广泛应用于时间序列数据预处理的技术，能够有效捕捉数据的局部特征和时间依赖性。定义多维数据集为 $[x_1,x_2,\cdots,x_l]$，l 为特征维度个数，通过设置合适的窗口大小 m 和步长

s,生成一系列包含时间序列信息的子序列,从而更好地捕捉数据中的动态变化和局部模式。滑动窗口采样多维特征数据的更新过程如图2所示。

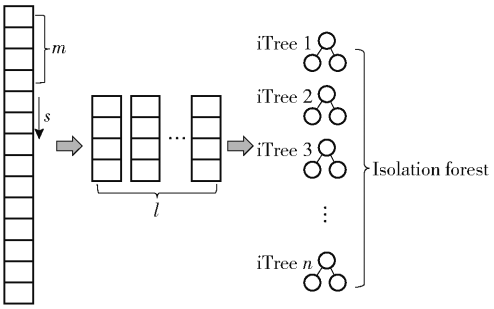


图2 滑动窗口采样过程

3 基于梯度优化算法的路径选择

WSN亟须一种能够快速应对Sinkhole攻击的防御策略,正常节点可以在排除异常节点的前提下,选择一条较优路径,将数据传输给真正的Sink节点,从而减少能耗。GBO是一种元启发式的数学优化算法,主要使用2个算子:梯度搜索规则(GSR, gradient search rule)和局部逃逸算子(LEO, local escaping operator)以及1组向量来探索搜索空间。GSR采用基于梯度的方法来增强搜索趋势,加快收敛速度,以获得更好的搜索空间中的位置,LEO则帮助GBO逃离局部最优[19-20]。

初始阶段,每个节点与通信半径 r 内的邻居节点建立路由信息表,存储邻居节点的相关信息,包括节点的标识符(ID, identity)、坐标、异常分数 v、节点剩余能量 E_r 和节点与Sink间的距离 d_{toSink}。遭受攻击后,需重新建立多跳路由,节点下一跳的选择需要综合考虑邻居节点的异常分数 v、剩余能量和与Sink间的距离等因素。因此,采用权重的思想,将多目标优化问题转化为单目标优化问题,定义GBO算法更新节点路径的目标函数如下:

$$F_{\text{obj}} = \alpha v + \beta \left(\frac{E_{\max} - E_r}{E_{\max} - E_{\min}} + \frac{d_{\text{toSink}} - d_{\min}}{d_{\max} - d_{\min}} \right) \quad (6)$$

其中:v 是节点的异常分数,数值分布在0~1之间,v 越接近1,表示数据点越可能是异常点,$E_{\max}$ 和 $E_{\min}$ 分别为网络中节点剩余能量的最大值和最小值。$d_{\max}$ 和 $d_{\min}$ 分别为网络中距离Sink节点最远和最近的节点距离。α 和 β 是权重因子,且满足 $\alpha + 2\beta = 1$。节点的异常分数始终是所有节点优先考虑的因素,因此设定 $\alpha = 0.70$,$\beta = 0.15$。

综上所述,IF-GBO算法的工作流程如图3所示。

4 实验仿真分析

实验的开发环境为PyCharm 2021.2.4,编程语言为Python。实验设计主要分为3个部分:1)参数优化实验;2)模型性能验证实验,将IF-GBO与经典的异常检测分类模型进行对比,包括支持向量机(SVM, support vector machine),K 最近邻(KNN, k-nearest neighbors),局部异常因子(LOF, local outlier factor);3)网络性能对比试验,将IF-GBO与HCODESSA[14]和RMHSD[15]进行对比。

设定区域面积为100 m×100 m,传感器节点数 $n = 80$,初始能量为1 J,通信半径 $r = 14$ m,Sink节点在区域中心位置,恶意节点比例为10%,网络运行10 s后,恶意节点开始发动攻击,IDS检测周期为100 ms,数据包每跳的传输时间为10 ms,恶意节点篡改数据需要耗费200 ms,仿真持续时间为30 s。引入准确率(Accuracy)、真正率(TPR, true positive rate)、精确度(Precision)、F_1 和假正率(FPR, false

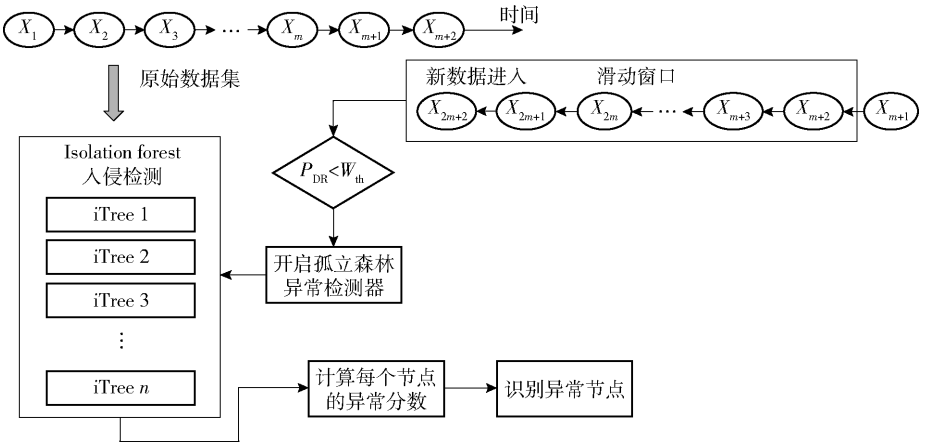


图3 IF-GBO流程图

positive rate)、接收者操作特征(ROC, receiver operating characteristic)曲线和 ROC 曲线下的面积(AUC, area under curve)等异常检测指标。

4.1　参数优化实验

1)图 4 为 w_{th}对于 AUC 的影响。当 w_{th}为 0.8, AUC 越接近 1.00,说明 IF-GBO 在此阈值下的综合性能上表现越好。

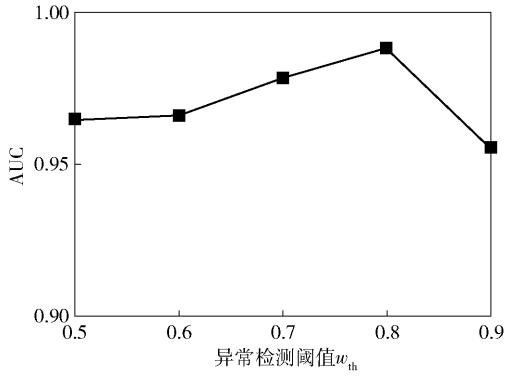


图 4　入侵检测阈值对 AUC 的影响

2)图 5 为不同参数组合下对 AUC 值的影响。当采样规模 $\psi=150$ 且孤立树数量 $t=60$ 时,IF-GBO 的 AUC 值最接近 1.00。

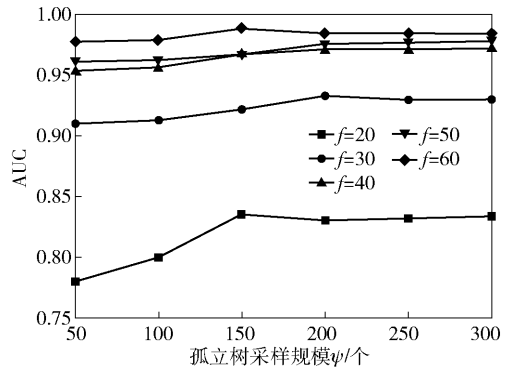


图 5　不同参数组合对于 AUC 的影响

3)图 6 是 IF-GBO 经训练后得到的异常分数直方图,正常数据与异常数据的得分有显著差异,证明了滑动窗口采样可以有效帮助模型分割出正常与异常数据,提高检测效果。

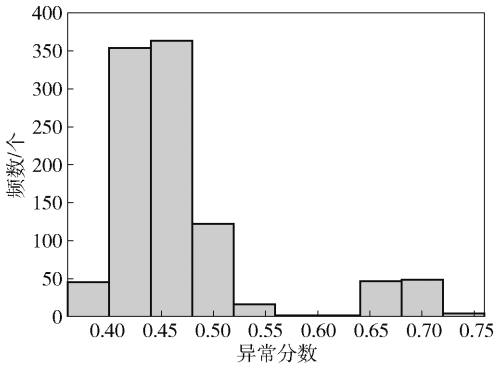


图 6　异常分数直方图

4.2　模型性能验证实验

1)不同模型的 ROC 曲线如图 7 所示,IF-GBO 最接近左上角,说明分类器的性能越好,可以在较低的 FPR 下,就能达到较高的 TPR,优于其他模型。

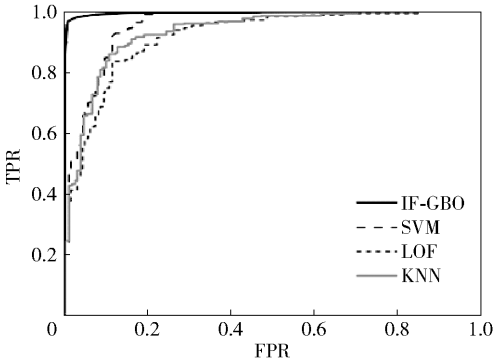


图 7　不同模型的 ROC 曲线

2)为了评估 IF-GBO 模型的泛化能力,设计了 2 组实验:1)节点数 $n=80$ 不变(恶意节点数为 8),仅改变监测区域的面积,实验结果如表 1 所示;2)监测区域面积保持 100 m × 100 m 不变,节点数改变,恶意节点数仍为 8,实验结果如表 2 所示。

从表 1 可以看出,随着区域面积增加,4 种模型的准确率、F_1 和 AUC 均呈现出下降的趋势,这是由于区域面积的增加会导致节点分布稀疏,数据传输路径变长,异常数据的样本不足,但 IF 在处理高维数据时表现良好,所以 IF-GBO 表现的性能是最好

表 1　区域面积改变时不同模型的性能指标数据对比　%

模型	100 m × 100 m				150 m × 150 m				200 m × 200 m			
	SVM	LOF	KNN	IF-GBO	SVM	LOF	KNN	IF-GBO	SVM	LOF	KNN	IF-GBO
准确率	93.51	87.44	88.04	98.13	89.04	84.55	85.04	95.13	86.88	79.87	80.26	92.25
F_1	90.42	86.33	87.12	98.09	85.42	80.12	82.12	95.09	82.42	72.12	77.33	92.09
AUC	90.10	85.81	87.30	99.41	85.88	81.21	83.21	94.41	83.88	70.21	75.61	91.41

表2 传感器节点数改变时不同模型的性能指标数据对比 %

模型	$n=80$				$n=100$				$n=120$			
	SVM	LOF	KNN	IF-GBO	SVM	LOF	KNN	IF-GBO	SVM	LOF	KNN	IF-GBO
准确率	93.23	88.10	88.87	99.05	94.04	88.55	89.40	99.13	94.28	86.11	86.01	99.25
F_1	91.23	87.37	86.80	98.66	90.23	85.32	85.12	97.09	89.77	83.12	82.55	94.41
AUC	92.05	87.21	87.69	98.75	91.88	85.41	86.21	97.41	89.45	84.21	83.43	95.22

的。此外,对于KNN和LOF而言,相较于准确率的变化趋势,F_1和AUC的下降速度更快,说明在节点分布稀疏的情况下,KNN和LOF模型的节点误判率较高,会影响后续正常节点的路径选择。从表2可以看出,随着节点数增加,虽然数据量增多,但样本的分布会更加不均衡,IF-GBO和SVM的准确率均有所提高,而KNN和LOF则呈现先升高后略有下降的趋势。虽然4种模型的F_1和AUC均有所下降,但IF-GBO的F_1和AUC始终保持在93%以上,说明了IF-GBO具有较强的分类和更高的鲁棒性。

4.3 网络性能对比实验

图8~10分别是从P_{DR}、节点的平均剩余能量和端到端时延3个角度去评估路由协议的性能。从图8可以看出,由于IF、HCODESSA和RMHSD算法均没有防御措施,并没有实质缓解Sinkhole攻击对路由性能的破坏,导致P_{DR}下降,数据大量丢失,在网络运行至20 s时,网络基本处于瘫痪状态。从图9可以看出,节点因数据丢失而重复向下一跳节点发送数据,会造成能耗的增加,而IF-GBO利用GBO收敛速度快、不容易陷入局部最优的优势,建立目标函数进行路径选择,保证了数据可靠传输。从图10可以看出,恶意节点丢弃数据或篡改数据都会导致时延大大增加,若采取防御措施,平均端到端时延仅增加200 ms左右。

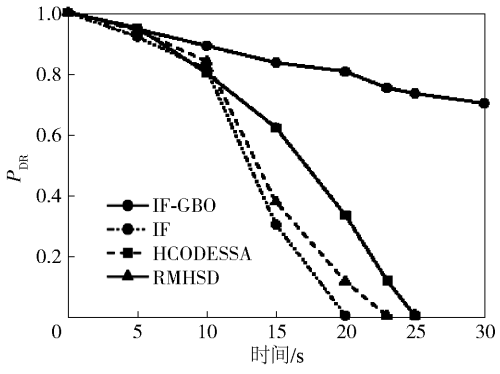


图8 不同算法的P_{DR}

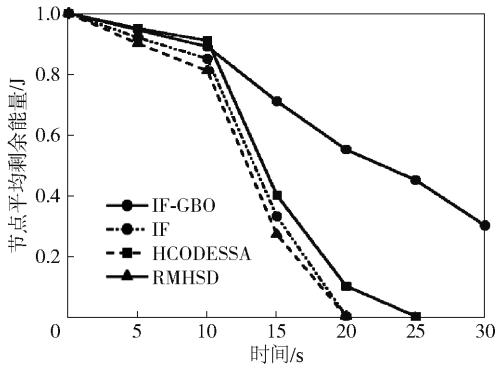


图9 不同算法的节点平均剩余能量对比

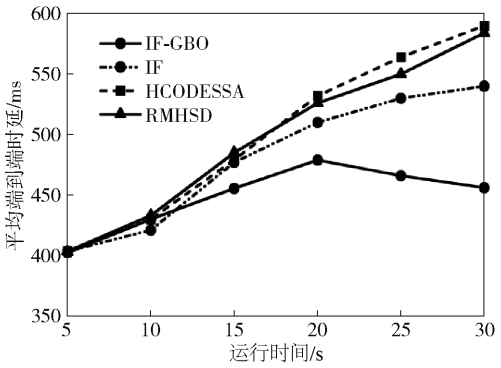


图10 不同算法的平均端到端时延对比

5 结束语

为提高WSN路由协议的安全性,应对Sinkhole攻击对网络造成的威胁,提出了一种融合IF和GBO算法的Sinkhole攻击检测与防御策略。Sinkhole攻击能够破坏网络的拓扑结构,阻碍数据传输,异常增加节点的能耗,攻击节点会诱导大量正常节点改变数据传输路径,致使这些节点的能耗、数据包接收率、转发率、跳数和时延等关键性能指标发生显著变化。IF作为一种高效的异常检测算法,具备快速捕捉离群数据点的显著优势,能够有效识别异常节点,而利用滑动窗口采样多维数据,能够进一步增强算法的精确度。路径选择目标函数则综合考虑了节点异常分数、剩余能量和节点间距离3个关键因素,采用GBO算法帮助节点快速寻找新的传输路径,有效

抵御 Sinkhole 攻击。通过这种方式，不仅能够有效保证数据的可靠传输，延长网络寿命，还巧妙解决了异常检测结果无法及时传输至真实 Sink 节点的难题。

在未来的研究工作中，计划将该算法进一步拓展，应用于检测 WSN 中的其他类型网络攻击，并对其可行性进行全面验证，为 WSN 的安全防护提供更为全面且有效的解决方案。

参考文献：

[1] LI J E, LU Q Y, LIU J, et al. Communication service priority in smart substation and its queue scheduling method[J]. Journal on Communications, 2021, 42(7): 25-40.

[2] 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.

[3] LV C, WANG R, ZHAO M. Application research of wireless sensor networks and the Internet of things[J]. Journal of Electronic Research and Application, 2025, 9(4): 283-289.

[4] TENG Z J, DU C Q, SUN H Y, et al. A wormhole attack detection strategy integrating node creditworthiness and path hops in WSNs[J]. Journal of Harbin Institute of Technology, 2021, 53(8): 64-71.

[5] WANG C H, WANG X, HU X S, 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): 1237-1244.

[6] PEI Y H, SHEN Y L, MA J F. Survey of wireless sensor network security techniques[J]. Journal on Communications, 2007(8): 113-122.

[7] TENG Z J, DU C Q, SUN H Y, et al. A wormhole attack detection strategy integrating node creditworthiness and path hops in WSNs[J]. Journal of Harbin Institute of Technology, 2021, 53(8): 64-71.

[8] PRAMITARINI Y, PERDANA R H Y, et al. A hybrid price auction-based secure routing protocol using advanced speedand cosine similarity-based clustering against Sinkhole attack in VANETs [J]. Sensors, 2022, 11(15): 5811-5833.

[9] AQEEL-UR R, SADIQ U R, HARIS R. Sinkhole attacks in wireless sensor networks: A survey[J]. Wireless Personal Communications, 2019, 106(4): 2291-2313.

[10] JIANG L W, GU H Y, XIE L X, et al. Research on the application of machine learning to intrusion detection in WSN[J]. Journal of Xidian University, 2024, 51(4): 206-225.

[11] KHAH P Y, SHIRVANI H M, MOTAMENI H. A hybrid machine learning approach for feature selection in designing intrusion detection systems (IDS) model for distributed computing networks[J]. The Journal of Supercomputing, 2024, 81(1): 254-265.

[12] THEN Z J, GU J L, CUI Y Y, et al. Artificial bee colony malicious node identification strategy considering reputation in WSN[J]. Journal of Harbin Institute of Technology, 2025: 1-11. [2025-09-08]. https://link.cnki.net/urlid/23.1235.t.20231107.1525.002.

[13] TENG Z J, LI M, GU J L, 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): 76-82.

[14] LANKA C S, MTHULISI V. The design of a defense mechanism to mitigate Sinkhole attack in software defined wireless sensor cognitive radio networks[J]. Wireless Personal Communications, 2020, 113(2): 1-17.

[15] ZHANG Z, LIU S, BAI Y, et al. *M* optimal *r*-outes hops strategy: Detecting Sinkhole attacks in wireless sensor networks[J]. Cluster Computing, 2019, 22(3): 7677-7685.

[16] PRATHAPCHANDRAN K, JANANI T. A trust aware security mechanism to detect Sinkhole attack in RPL-based IoT environment using random forest-RFTRUST [J]. Computer Networks, 2021, 198: 10198.

[17] MOHAMMED A A, MEKKY M M. Sinkhole attack detection by enhanced reputation-based intrusion detection system[J]. IEEE Access, 2024, 12: 86985-86996.

[18] YANG X H, ZHANG S C. Anomaly detecti-on model based on multi-grained cascade iso-lation forest algorithm[J]. Journal on Communications, 2019, 40(8): 133-142.

[19] AHMADIANFAR I, BOZORG-HADDAD O, CHU X. *G*-radient-based optimizer: A new metaheuristic optimization algorithm[J]. Information Sciences, 2020, 540: 131-159.

[20] EWEES A A. Solving optimization problems using an extended gradient-based optimizer[J]. Ma-Thematics, 2023, 11(2): 378-393.