https://doi.org/10.1051/jnwpu/20203830634

基于环境参数优化和时间信誉序列的恶意节点识别模型

滕志军[1,2], 庞宝贺[2], 孙铭阳[3], 谢露莹[2], 郭力文[4]

(1.东北电力大学 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, 吉林 吉林 132012;
2.东北电力大学 电气工程学院, 长春 吉林 132012; 3.东北电力大学 自动化工程学院, 吉林 吉林 132012;
4.爱立信(西安)信息通信技术服务有限公司大连分公司, 辽宁 大连 116000)

摘 要:在复杂无线传感器网络环境中,为阻断恶意节点发动危及网络安全的中断攻击和选择性转发攻击,在 TS-BRS 信誉模型的基础上,搭建基于 MNRT-OEP&RS 的恶意节点识别模型,利用机器学习中的线性回归并结合节点能量、工作量、邻节点数量、节点疏松度等可确定参数求解环境参数,计算基准信誉序列与周期内的节点信誉序列的相似度;设定动态信誉双阈值,对节点的信息转发行为进行动态考量,以甄别恶意节点。仿真实验表明,改进后的算法对恶意节点的识别率可达 90%以上,对正常节点误判率降低到 8%以下,有效提高复杂环境下无线传感器网络的安全性。

关 键 词:无线传感器网络;网络安全;环境影响;线性回归;动态信誉双阈值
中图分类号:TN92 **文献标志码**:A **文章编号**:1000-2758(2020)03-0634-09

随着无线传感器网络(wireless sensor network, WSN)在军事、工业、医疗、商业等领域的广泛应用,用户对传感器节点的安全性要求日益提高[1]。然而,节点长期暴露于恶劣的部署环境中以及无线传感器网络自身的开放式特征决定了其节点从运行时刻开始,就处于一个节点可能随时被破坏或捕获的环境中[2-3]。传感器节点被捕获后,攻击者对节点进行解密、篡改程序,再次放回到网络中,这些被篡改节点就变成了恶意节点,它们以破坏 WSN 为目的,可以对网络发起几乎所有攻击[4-6]。因此,仅依靠基于密码学的安全机制无法防御恶意节点进入无线传感网络内部发起攻击行为,需要建立一种有效的安全模型来解决这些问题。

信任模型被看作为密码学的安全补充机制,可以进一步来防御恶意节点发起的内部攻击[7-8]。很多研究者从信任的角度对网络安全问题进行了深入的研究。Ganeriwal 等[9]提出一个典型的信誉框架 RFSN,将贝叶斯公式与 β 函数进行拟合作为节点的信誉值。该模型使贝叶斯理论在信誉评估中得到广泛应用,但 RFSN 模型只设定一个阈值来区别正常与恶意节点,在复杂环境下误判率较高。在文献[10-11]中,Ishmanov 等人提出了一种防御中断攻击和诽谤攻击的基于信任的 WSN 安全机制,通过联合观测值和推荐值评估节点的信誉值,并利用改进的聚类方法分析推荐值以检测诽谤攻击,在此基础上引入节点行为异常的权重来提高信任机制的适应性。文献[12]中的 TAR-MD 模型将异常节点区分为恶意节点和亚攻击节点,利用节点的信誉阈值时间序列进行相似度比较,通过聚类分析的方法,识别 WSN 中的亚攻击节点。文献[13]提出了 DPAM-MD 模型,是在传统信誉阈值判断模型的基础上,利用时序和相似度的概念结合曼哈顿度量和基于密度的聚类算法来识别亚攻击节点。文献[14]提出基于状态上下文和分层信誉机制,针对感知环境多变、节点状态多变的层次型无线传感器网络中,对簇头节点和普通节点分别进行三维信誉评估,最后根据

收稿日期:2019-07-08 **基金项目**:国家自然科学基金青年科学基金项目(61501107)及吉林省教育厅“十三五”科学研究规划项目(JJKH20180439KJ)资助

作者简介:滕志军(1973—),东北电力大学教授,主要从事无线通信技术与物联网网络安全研究。

综合评估检测恶意入侵。相似的是文献[15]提出了一种应用于大规模层次型 WSN 信任估计模型,利用聚类的方法来检测异常或自私节点。文献[16]引入了错误行为周期因子和信任值修复的方法,来区分选择性转发攻击节点和暂时性错误节点。文献[17]提出了应用于分簇 WSN 的轻量级的信任机制,但并不能防御选择性转发攻击。文献[18]针对恶意转发攻击提出了一种基于网络的移动代码驱动信任机制(MCTM),使用移动代码,根据预先定义的行程访问传感器节点,同时收集有关这些节点的必要信息,为评估其信任度做准备。文献[19]提出的 BLTM 模型是在信任值服从 β 分布基础上充分考虑 WSN 网络通信链路质量问题,直接信任包括通信信任、能量信任和数据信任,利用链接质量指标分析机制来保证该模型在链路质量较差的网络环境下识别网络攻击具有较好的收敛性。

上述文献为 WSN 网络安全领域的研究提供了扎实的理论基础,也可以发现以下几个问题:①传感器节点直接信任的计算主要基于通信交互信息,由于内部攻击的种类繁多,这类方法还不够安全。因此,需要考虑节点的能量、工作量和分布密度等状态信息。②实际的 WSN 环境中的通信质量并不理想,质量较差的链接可能会损害通信行为,并对正常节点的信任值产生不利影响。因此需要区分处在劣势环境中的正常节点与选择性攻击等一类的亚攻击节点。③通过设定单一信誉阈值判断识别恶意节点的方法,只能粗略地对异常节点进行甄别,精度较低。需要寻找自适应的阈值判定方法结合节点的状态来识别恶意节点。为解决以上问题,本文提出基于环境参数优化和时间信誉序列的恶意节点识别技术(malicious node recognition technology based on optimizing environmental parameter & time reputation sequence,缩写为 MNRT-OEP&RS)。在评估信誉值计算中,考虑节点的历史信誉值和状态参数,以实现对不同环境状态下节点进行有效公平的评估,同时,本模型设定动态信誉双阈值,可有效甄别亚攻击性恶意节点并解决以往信任模型中单一阈值设定造成的误判率较高的问题。

1　构建多维参数信誉模型

无线传感器网络中,节点经常携带不同类型的传感器部署在不同的环境以感知环境数据,为提高识别恶意节点的精度,需要对每一个节点的信誉行为进行动态考量。本文通过选取节点信誉值、节点能量、节点数据量、邻节点数量和分布疏松度等相关参数构建环境模型。

1.1　节点信誉模型

本文引用基于时序信息分析的 WSN 贝叶斯信誉评价模型(Time-series WSN hierarchical beta reputation system,缩写为 TS-BRS)[20],对网络内部的节点的信誉值进行计算。在成簇式分层 WSN 中,TS-BRS 模型,能在较短时间内降低中断攻击性恶意节点的信誉值,并优化信道占用问题对通信行为的影响。其节点信誉值计算公式如下

$$T_{\text{tru}} = \frac{\mu\alpha + \Delta\alpha}{\mu(\alpha + \beta) + \Delta\alpha + \Delta\beta} \tag{1}$$

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

式中:T_{tru} 为节点的信誉值;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 Δt 内节点正常通信次数;$\Delta\beta$ 是在阶段时间 Δt 内节点非正常通信次数;μ 是信誉维护函数,维护现阶段节点行为对信誉值影响,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,本文参考 TS-BRS 模型将参数 θ 取值为 150。

1.2　信誉时间序列

TS-BRS 无线传感器网络安全模型中,每个节点的信誉值以相同的时间间隔 Δt 进行周期性更新。节点 N 的信誉值可写为 $\{T^N_{\text{tru}_{t1}}, T^N_{\text{tru}_{t2}}, T^N_{\text{tru}_{t3}}, T^N_{\text{tru}_{t4}} \cdots\}$。每 n 个时间间隔的节点信誉构成一个信誉序列,如图 1 所示。

$$\underbrace{\{T^N_{\text{tru}_{t1}}, T^N_{\text{tru}_{t2}}, \cdots, T^N_{\text{tru}_{tn}}}_{n}, \underbrace{T^N_{\text{tru}_{t(n+1)}}, T^N_{\text{tru}_{t(n+2)}}, \cdots, T^N_{\text{tru}_{t(n+n)}}, \cdots\}}_{n}$$

图 1　信誉序列选取

定义 1　信誉矩阵。$A^N_i = \{T^N_{\text{tru}_t(in)}, T^N_{\text{tru}_t(in+1)}, \cdots, T^N_{\text{tru}_t(in+n-1)}\}$ 为节点 N 的第 i 组时间序列,则节点下一组信誉时间序列为 $A^N_{i+1} = \{T^N_{\text{tru}_t(in+n)}, T^N_{\text{tru}_t(in+n+1)}, \cdots, T^N_{\text{tru}_t(in+2n-1)}\}$,以此类推,信誉序列 A^N_i 可以定义信誉矩阵 $\boldsymbol{T}(A^N_i)$。

$$\boldsymbol{T}(A^N_i) = \begin{bmatrix} T^N_{\text{tru}_t(in)} \\ T^N_{\text{tru}_t(in+1)} \\ T^N_{\text{tru}_t(in)+2} \\ \vdots \\ T^N_{\text{tru}_t(in+n-1)} \end{bmatrix} \tag{3}$$

1.3 状态矩阵

定义 2 状态矩阵。网络中不同的节点处于不同环境状态具有不同的工作状态,本文中节点的状态考虑 4 个维度:剩余能量 E_{res},数据量 W_{job},邻节点数量 M_{nei} 以及节点分布疏松度 D_{den},即 $s=\{E_{\text{res}},W_{\text{job}},M_{\text{nei}},D_{\text{den}}\}$。

当节点更新信誉值时,记录下节点当前状态,联系其信誉矩阵可构建节点 N 相关状态时间矩阵为

$$\boldsymbol{S}_i^N=\begin{bmatrix}S_{t(in)}^N\\S_{t(in+1)}^N\\S_{t(in+2)}^N\\\vdots\\S_{t(in+n-1)}^N\end{bmatrix}=\begin{bmatrix}E_{\text{res}_{t(in)}}^N & W_{\text{job}_{t(in)}}^N & M_{\text{nei}_{t(in)}}^N & D_{\text{den}_{t(in)}}^N\\E_{\text{res}_{t(in+1)}}^N & W_{\text{job}_{t(in+1)}}^N & M_{\text{nei}_{t(in+1)}}^N & D_{\text{den}_{t(in+1)}}^N\\E_{\text{res}_{t(in+2)}}^N & W_{\text{job}_{t(in+2)}}^N & M_{\text{nei}_{t(in+2)}}^N & D_{\text{den}_{t(in+2)}}^N\\\vdots & \vdots & \vdots & \vdots\\E_{\text{res}_{t(in+n-1)}}^N & W_{\text{job}_{t(in+n-1)}}^N & M_{\text{nei}_{t(in+n-1)}}^N & D_{\text{den}_{t(in+n-1)}}^N\end{bmatrix} \tag{4}$$

1.3.1 节点剩余能量

其中,节点的剩余能量 E_{res} 为节点预设能量减去节点发送、接收和处理单位数据所需能耗。当节点能量资源不足时,表现出自私行为,放弃协作或只接收不发送数据[21-22],与选择性转发攻击的表现相似。因此,在对节点的信誉值进行评估时,需要考量节点的剩余能量。该能耗模型参考经典的无线射频模块模型[23]得出,如公式(5)所示。

$$E_{\text{T}}(l,d)=\begin{cases}E_{\text{elec}}\times l+\varepsilon_{\text{fs}}\times l\times d^2, & d<d_{\text{crossover}}\\E_{\text{elec}}\times l+\varepsilon_{\text{mp}}\times l\times d^4, & d<d_{\text{crossover}}\end{cases}$$

$$E_{\text{R}}(l,d)=E_{\text{elec}}\times l$$

$$E_{\text{res}}=E_{\text{tot}}-E_{\text{T}}(l,d)-E_{\text{R}}(l,d) \tag{5}$$

式中:$E_{\text{T}}(l,d)$,$E_{\text{R}}(l,d)$ 分别为发送和接受数据所需能耗;E_{tot} 为节点总能量;E_{elec} 为收发电路处理单位数据所消耗的能量;l 为节点准备发送的数据量;ε_{fs} 为在自由空间模型下,发送单位数据发射放大电路所消耗的能量;ε_{mp} 为在多径衰减模型下,发送单位数据发射放大电路所消耗的能量;d 为该节点与目的节点之间的距离,可以通过节点功率模型计算得出;$d_{\text{crossover}}$ 为自由空间模型和多径衰减模型的距离临界值,其计算方式为

$$d_{\text{crossover}}=\frac{4\pi\sqrt{L}h_rh_t}{\lambda} \tag{6}$$

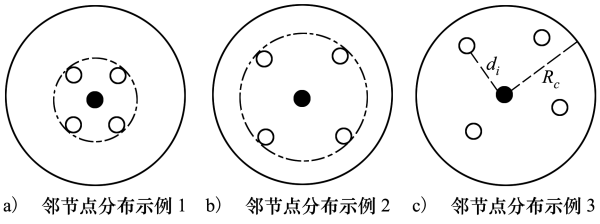
式中:$L\geqslant 1$ 为系统损耗因子;h_r 为接收天线的高度;h_t 为发送天线的高度;λ 为波长。

1.3.2 节点数据量

节点数据量可以用 2 种方式表示,第一种方法是统计节点在阶段 Δt 内收发数据包的大小,第二种方法是对节点在 Δt 内收发数据包进行计算,次数记为 W_{job}。因为本文仿真实验设定的数据包大小相同,为节省计算开销,采用第二种计量方法。

1.3.3 邻节点数量和节点分布疏松度

邻节点数量 M_{nei} 代表在以节点的通信半径为圆的区域内其他节点的数量;节点分布疏松度 D_{den} 是该区域节点分布呈现的疏松程度。如图 2 所示,在相同的通信半径和邻节点数量下,节点分布的密集度差别很大,而不同疏密程度的节点分布会对信息的有效传输造成影响。



a) 邻节点分布示例 1 b) 邻节点分布示例 2 c) 邻节点分布示例 3

图 2 邻节点分布图

用目标节点和邻节点的距离来描述节点疏松度,即

$$D_{\text{den}}=\frac{\sum_{i=1}^{M_{\text{nei}}}d_i}{M_{\text{nei}}R_{\text{c}}} \tag{7}$$

式中:d_i 表示各邻居节点与目标节点的距离;R_{c} 表示节点的通信半径。当节点的通信半径一定时,节点分布越密集,D_{den} 越小。

1.4 环境参数

定义 3 环境因素矩阵。将环境因素矩阵 $\boldsymbol{Q}_{\text{env}}$ 与节点的状态时间矩阵和信誉时间序列的关系定义为

$$\boldsymbol{S}\boldsymbol{Q}_{\text{env}}=\boldsymbol{T} \tag{8}$$

节点 N 第 i 组时间序列展开关系式可表示为

$$\begin{bmatrix} E^N_{\mathrm{res}_{t(in)}} & W^N_{\mathrm{job}_{t(in)}} & M^N_{\mathrm{nei}_{t(in)}} & D^N_{\mathrm{den}_{t(in)}} \\ E^N_{\mathrm{res}_{t(in+1)}} & W^N_{\mathrm{job}_{t(in+1)}} & M^N_{\mathrm{nei}_{t(in+1)}} & D^N_{\mathrm{den}_{t(in+1)}} \\ E^N_{\mathrm{res}_{t(in+2)}} & W^N_{\mathrm{job}_{t(in+2)}} & M^N_{\mathrm{nei}_{t(in+2)}} & D^N_{\mathrm{den}_{t(in+2)}} \\ \vdots & \vdots & \vdots & \vdots \\ E^N_{\mathrm{res}_{t(in+n-1)}} & W^N_{\mathrm{job}_{t(in+n-1)}} & M^N_{\mathrm{nei}_{t(in+n-1)}} & D^N_{\mathrm{den}_{t(in+n-1)}} \end{bmatrix} \cdot \begin{bmatrix} q^N_E \\ q^N_W \\ q^N_M \\ q^N_D \end{bmatrix} = \begin{bmatrix} T^N_{\mathrm{tru}_{t(in)}} \\ T^N_{\mathrm{tru}_{t(in+1)}} \\ T^N_{\mathrm{tru}_{t(in+2)}} \\ \vdots \\ T^N_{\mathrm{tru}_{t(in+n-1)}} \end{bmatrix} \tag{9}$$

$\boldsymbol{Q}_{\mathrm{env}}$ 的计算可以使用机器学习中的线性回归求解。该矩阵的均方误差 G_{MSE} 公式如下

$$G_{\mathrm{MSE}} = \frac{1}{n}\sum_{j=0}^{n-1}\left(s^N_{t(in+j)} \cdot Q_{\mathrm{env}} - T^N_{\mathrm{tru}_t(in+j)}\right)^2 \tag{10}$$

当均方误差 G_{MSE} 达到最小时,所得即为环境因素矩阵 $\boldsymbol{Q}_{\mathrm{env}}$ 的最优解。采用正定方程对 $\boldsymbol{Q}_{\mathrm{env}}$ 进行求解,即

$$\boldsymbol{Q}_{\mathrm{env}} = (\boldsymbol{S}^{\mathrm{T}} \cdot \boldsymbol{S})^{-1} \cdot \boldsymbol{S}^{\mathrm{T}} \cdot \boldsymbol{T} \tag{11}$$

2　基于 MNRT-OEP&RS 的恶意节点识别

在网络中恶意节点为躲避安全机制的检测会表现亚攻击性,选择性的丢弃数据包,间接的转发数据,以隐藏攻击者的身份,延长生存周期[24-25]。而无线传感器网络中节点随机布撒,各个节点所处环境各不相同,恶劣的环境也会导致网络信息传输异常。因此,如何区分环境状况影响还是恶意攻击造成的非成功通信,是信誉安全模型中亟须解决的难题。本文联系环境参数 $\boldsymbol{Q}_{\mathrm{env}}$,对网络中每一个节点设定适应于节点状态和环境的判定方法。

2.1　基准信誉序列

在无线传感器网络成功部署后,网络中各节点都可视为正常节点。网络中节点信誉值以 n 为周期,更新出第一组时间序列 $\boldsymbol{T}(A^N_1)$,结合公式(11)计算出节点第一个周期的环境参数 $\boldsymbol{Q}_{\mathrm{env}_{t1}}$。当节点的信誉值更新出第二组时间序列 $\boldsymbol{T}(A^N_2)$ 和节点状态矩阵 $\boldsymbol{S}^N_2$,可利用公式(12)计算出节点当前环境下的基准信誉序列 $\boldsymbol{T}'(A^N_2)$。

$$\boldsymbol{T}'(A^N_2) = \boldsymbol{S}^N_2 \boldsymbol{Q}_{\mathrm{env}_{t1}} \tag{12}$$

根据节点周期内的信誉序列和节点当前的基准信誉序列的相似度进行判定点在某一阶段是否有恶意行为。

2.2　相似度计算

考虑到贝叶斯信誉评价模型的无线传感器网络节点的信誉值分布情况近似服从高斯分布的特性,在本文算法中,序列相似度工具采用简化的高斯径向基函数,其具体公式如下

$$k^N_2 = \mathrm{E}\left[\sum_{j=0}^{n-1}\exp\left\{-\frac{\left(\boldsymbol{T}^N_{\mathrm{tru}_{t(2n+j)}} - \boldsymbol{T}'^N_{\mathrm{tru}_{t(2n+j)}}\right)^2}{\sigma^2}\right\}\right] \tag{13}$$

$$p^N_2 = \begin{cases} 1 & \text{if} \quad \mathrm{sum}\boldsymbol{T}(A^N_2) > \mathrm{sum}\boldsymbol{T}'(A^N_2) \\ -1 & \text{if} \quad \mathrm{sum}T(A^N_2) < \mathrm{sum}T'(A^N_2) \end{cases} \tag{14}$$

$$K^N_2 = k^N_2 p^N_2 \tag{15}$$

式中:σ 为调整参数,调节函数的径向作用范围,大小需要参考节点信誉值分布的跨度范围;σ 取值为 1。k 的取值范围在[0,1] 之间,如果相似度结果趋近于 1,则表明两条序列相似程度越大;相似度结果趋近于 0,则表明 2 条序列相似程度越小。同时定义 p 为信誉的变化方向,如果实际信誉高于基准信誉则 p 等于 1,如果实际信誉低于基准信誉则 p 等于 -1。最终得到相似度 K^N_2 若是大于 0,则称为正相似度,否则,为负相似度。

2.3　恶意节点识别

传统的信誉模型中只设定一个较低的阈值,若节点的信誉值低于这个阈值就判定为恶意节点。本文设定双阈值 δ 和 ψ,如图 3 所示,0 到 δ 为低信誉区间,δ 到 ψ 为中信誉区间,ψ 到 1 为高信誉区间。本文主要侧重于识别低信誉区间内的正常节点和中信誉区间的亚攻击性恶意节点。

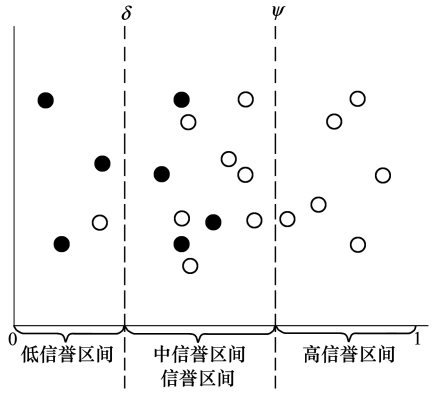


图 3　节点信誉分布

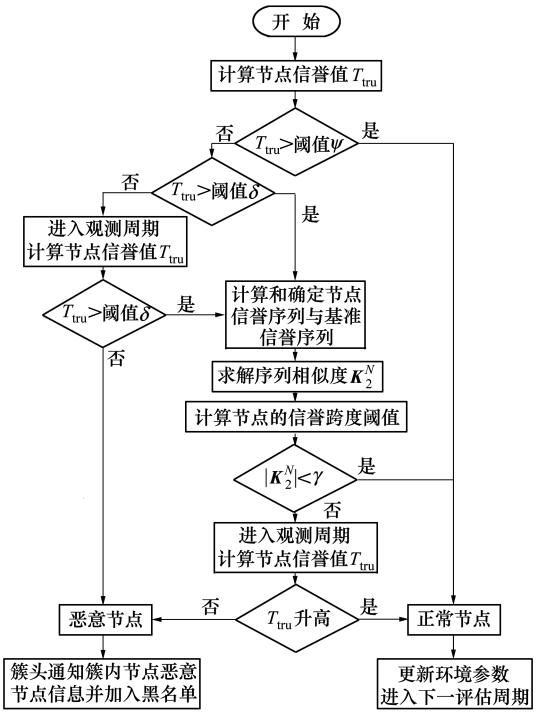


图 4 MNRT-OEP&RS 工作流程图

恶意节点识别流程图如图 4 所示。考虑到网络环境中的小区域突发状况,设 f 为一个节点观察周期参数。

①节点信誉序值在高信誉区间,则节点可直接视为正常节点。

②节点信誉值在连续 f 个观察周期仍处在低信誉区间,则判定为恶意节点。

③ 节点信誉值处在中心信誉区间,结合公式(15)判断节点当前序列与基准序列的相似度大小和方向。这里定义节点可容忍信誉跨度阈值为 γ。如果节点信誉序列相似度为正相似或$|K_2^N|<\gamma$,则判定节点为正常节点,同时根据公式(11)更新环境参数 Q_{env};如果节点信誉序列相似度为负且$|K_2^N|>\gamma$,节点将进入观察期,如果经过 f 个观察周期节点的信誉值依旧没有升高,则判定节点为恶意节点。节点的信誉跨度阈值 γ 公式如下

$$\gamma=\eta\exp\left\{\frac{\mathrm{E}[\,\mathrm{sum}T'(A_2^N)\,]}{\psi-\delta}-\frac{\delta}{\psi-\delta}\right\} \tag{16}$$

式中,η 为超级参数,用来调节信誉跨度阈值 γ 的大小,本文参考文献[22],使得 $\eta\in(0,1)$,η 越小,信誉阈值跨度范围越小。当基准信誉序列的期望越高,则相似度允许的跨度阈值越高;当基准信誉序列的期望越低,则相似度允许的跨度阈值越低。

3 仿真及分析

采用 MATLAB2016a 搭建仿真环境,仿真环境设置:100 m×100 m~200 m×200 m 的正方形区域随机分布 100~300 个节点,分 4 个簇,节点通信半径为 20 m。仿真初始全部为正常节点,均可百分百响应通信请求,在更新 3 个信誉序列后产生恶意节点数量占总节点的 10%,各恶意节点以 0.5~0.1 的概率丢弃数据包。

表 1 仿真参数

参数	数值
仿真区域/(m×m)	100×100~200×200
节点总个数	100~300
簇头节点个数	4
恶意节点占比/%	10
通信半径/m	20
节点初始能量/J	2
传输和接收能耗/(nJ·bit^{-1})	50
自由空间模型 ε_{fs}/(pJ·bit^{-1}·m^2)	10
多径衰减模型 ε_{mp}/(pJ·bit^{-1}·m^2)	100
数据包大小/bit	80

3.1 网络性能评价指标

本文引用 2 种指标对模型的性能进行判定,分别为恶意节点识别率 Y 和正常节点误判率 Z,公式如下

$$Y=\frac{\text{已识别恶意节点数}}{\text{恶意节点总数}} \tag{17}$$

$$Z=\frac{\text{正常节点被误判数}}{\text{正常节点总数}} \tag{18}$$

3.2 阈值 δ 和 ψ 的设定

为确定阈值 δ 和 ψ 的大小,在 100 m×100 m 区域随机分布 100 个节点,其中 10 个为恶意节点,以 50%~100%的概率丢弃数据包。首先设定 ψ 为 1,用 TS-BRS 信誉模型识别恶意节点,阈值 δ 从 0 到 1 变化,记录低信誉区域存在的可信节点数,结果如图 5 所示。然后,在相同的仿真环境下,将阈值 δ 设定为 0,阈值 ψ 从 0 到 1 变化,记录出现在高信誉区域的恶意节点数量,结果如图 6 所示。

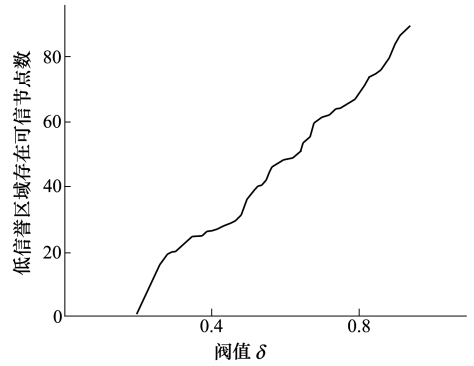


图 5　阈值 δ 与低信誉区域存在可信节点个数之间的关系

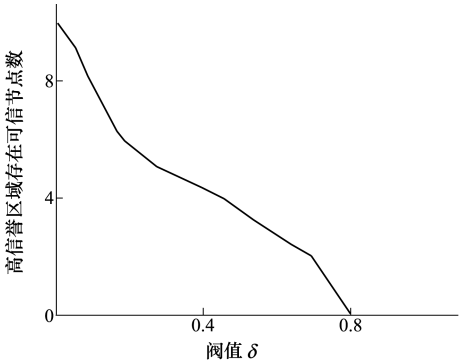


图 6　阈值 ψ 与高信誉区域存在恶意节点个数之间的关系

由图 5 可知,当阈值 δ 移动在 0.2 左右时,低信誉区域存在第一个可信节点,意味着阈值 δ 取值越大,误判率将越大。在图 6 中可看出,将阈值 ψ 设为 0.8 时,高信誉区域不再存在恶意节点。由此,本文将阈值 δ 和 ψ 分别设置为 0.2 和 0.8。

3.3　时间序列的长度 n 和参数 η 的设定

在 MNRT-OEP&RS 算法中还有 2 个重要的参数,一个是时间序列的长度 n,另一个为公式(16)中影响信誉跨度阈值 γ 的超级参数 η。本文预设的实验环境状况下,仿真分析 2 个可控参数与模型的恶意节点识别率和正常节点误判率的关系,时间序列长度取从 50 到 300,参数 η 的取值从 0.1 到 0.5。

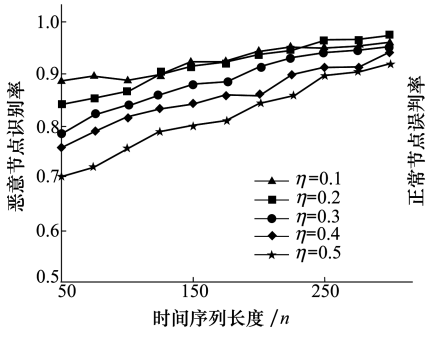


图 7　不同参数与恶意节点识别率的关系

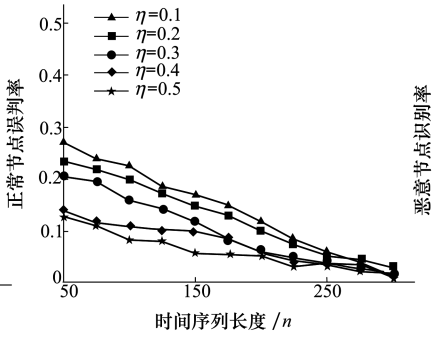


图 8　不同参数与正常节点误判率的关系

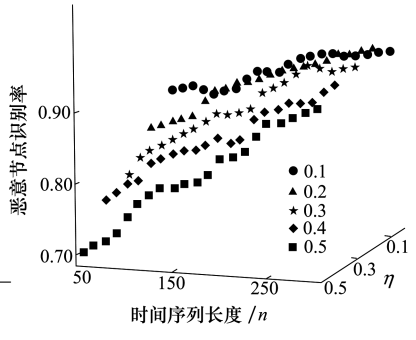


图 9　不同参数与恶意节点识别率的关系

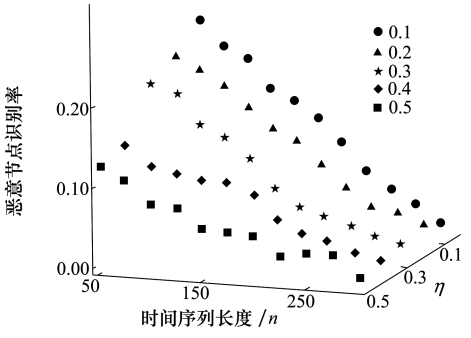


图 10　不同参数与正常节点误判率的关系

由图 7 至 10 可知,当时间序列长度越小,对当前节点的行为特征提取的有效信息量越少,因此在采用较短的时间序列情况下模型的恶意节点识别率和正常节点误判率的结果并不理想。随着时间序列长度的增加,模型对网络的检测准确率越高;但是如果时间序列过长,会增加计算开销使节点负担加重,并且周期变长使得恶意节点有更多的生存时间,对网络造成更大的破坏影响。若选用较小的参数 η,虽然能提升对恶意节点的识别的能力,但是 η 判定过于敏感,以至于细小的环境波动也会造成对正常节点的误判;而过大的参数 η 对恶意节点的识别能力不足。权衡之后将时间序列长度设置为 250,参数 η 为 0.3。

3.4 安全性能分析

当传感器网络中,恶意节点数量增多,各安全模型的压力都会增加。同为建立节点的信誉序列,TAR-MD 模型和 DPAM-MD 模型首先设定一个阈值将节点分为恶意节点和正常节点,然后通过聚类方法在正常节点中识别亚攻击性节点,在相对理想环境下效果较好。BLTM 模型结合直接信任值和推荐信任值识别异常节点。本文将与 BLTM 模型、TAR-MD 模型和 DPAM-MD 模型进行复杂环境下的恶意节点识别率对比和正常节点误判率对比。

图 11 反映了 4 种模型在不同数量的恶意节点的攻击下的识别率。从图中可以看出,MNRT-OER&RS 模型的识别率大于 0.9(即 90%)且稳定上升,而 BLTM 模型、DPAM-MD 模型和 TAR-MD 模型的识别率较低。这是因为在相对复杂环境下,更有利于亚攻击节点的伪装,而不便于正常节点的信息传输。BLTM 算法考虑到通信链路质量对信誉值的影响,但没有考虑推荐节点成为恶意节点会减低识别率的情况。

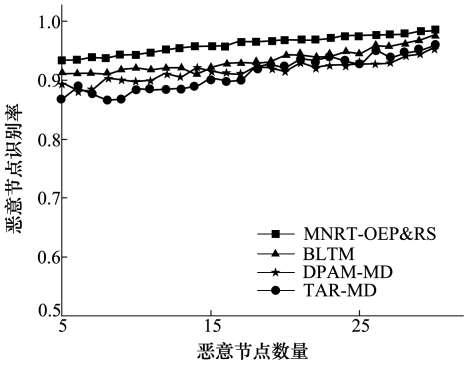


图 11 不同模型的恶意节点识别率比较

如图 12 所示,MNRT-OER&RS 模型的误判率均在 0.08(即 8%)以下,低于其他 3 个模型的误判率,这是因为设定单一阈值的安全模型会受环境因素的影响而产生安全性能波动,导致误判率有所升高,而本文算法是对每个节点都设置灵活的判定阈值区间,充分考虑环境的影响,所以模型整体效果具有小幅提高且表现相对平稳。

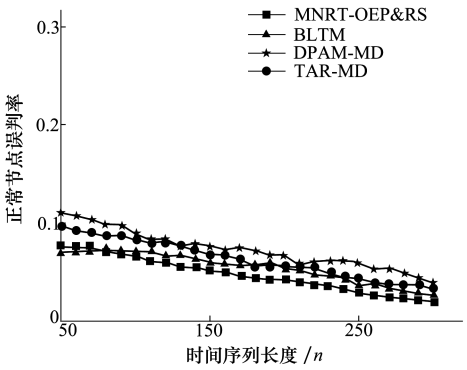


图 12 不同模型的误判率比较

3.5 算法复杂度分析

表 2 算法复杂度比较

算法	时间复杂度 $T(m)$	空间复杂度 $S(m)$
MNRT-OEP&RS	$O(m)$	$O(1)$
DPAM-MD	$O(m)$	$O(m)$
TAR-MD	$O(m)$	$O(m)$
BLTM	$O(m^2)$	$O(1)$

假设问题的大小是 m,本文提出的 MNRT-OEP&RS 的时间复杂度是由时间序列长度 n 决定的,因此,这个算法可以在 $O(m)$ 时间内完成。

对于 MNRT-OEP&RS,需要存储参数 α 和 β,分别代表节点正常和异常通信次数,$s = \{E_{\text{res}}, W_{\text{job}}, M_{\text{nei}}, D_{\text{den}}\}$,表现节点的状态信息等。因此本文算法的空间复杂度为 $S(m) = O(1)$。

4 结 论

本文是在传统贝叶斯信誉评价模型基础上,搭建了一种基于环境参数优化和信誉序列的恶意节点识别模型。该模型通过获取节点的时间信誉序列,融合多环境因素,对网络中各节点设定相应的信誉阈值区间,以识别选择性转发攻击型和中断攻击型的恶意节点。仿真实验表明,该模型能够有效的识别恶意节点,并可对单一阈值的信誉模型进行较好的补充。无线传感器网络在安全方面还有很多问题有待研究和解决,下一阶段将重点研究节点剩余能量、转发数据量、分布状态等因素对信息传输的影响及如何设置各参数在环境参数中的权重等问题。

参考文献:

[1] 王夙喆,李勇,程伟, 等. 传感器网络定位中节点攻击类型的分布式识别算法[J]. 西北工业大学学报, 2016, 34(1): 85-91
WANG Suzhe, LI Yong, CHENG Wei, et al. Distributed Localization Attack Type Recognition Algorithm for Malicious Nodes in Wireless[J]. Journal of Northwestern Polytechnical University, 2016, 34(1): 85-91 (in Chinese)

[2] 韩挺,罗守山,辛阳,等. 面向 MANET 路由的多属性动态信任模型[J]. 北京邮电大学学报, 2013, 36(5): 86-89,104
HAN Ting, LUO Shoushan, XIN Yang, et al. Dynamic Trust Model with Multiple Decision Factors in MANET[J]. Journal of Beijing University of Posts and Telecommunications, 2013, 36(5): 86-89, 104 (in Chinese)

[3] OSANAIYE O, ALFA A S, HANCKE G P. Denial of Service(DoS) Defence for Resource Availability in Wireless Sensor Networks[J]. IEEE Access, 2018, 6: 6975-7004

[4] 王硕鹏. 基于数据挖掘系统网络安全模型预测分析[J]. 东北电力大学学报, 2019, 39(6): 91-93
WANG Shuopeng. Prediction and Analysis of Systemic Network Security Model Based on Data Mining[J]. Journal of Northeast Electric Power University, 2019, 39(6):91-93 (in Chinese)

[5] ELSHRKAWEY M, ELSHERIF S M, ELSAYED WAHED M. An Enhancement Approach for Reducing the Energy Consumption in Wireless Sensor Networks[J]. Journal of King Saud University-Computer and Information Sciences, 2018, 30(2): 259-267

[6] YU Y, LI K, ZHOU W, et al. Trust Mechanisms in Wireless Sensor Networks: Attack Analysis and Countermeasures[J]. Journal of Network and Computer Applications, 2012, 35(3): 867-880

[7] 徐晓斌,张光卫,王尚广, 等. 基于群体信任的 WSN 异常数据过滤方法[J]. 通信学报, 2014, 35(5): 108-117,123
XU Xiaobin, ZHANG Guangwei, WANG Shangguang, et al. Abnormal Data Filtering Approach Based on Collective Trust for WSN[J]. Journal on Communications, 2014, 35(5):108-117 (in Chinese)

[8] 曲朝阳,宋晨晨,任有学,等. 结合用户活跃度的协同过滤推荐算法[J]. 东北电力大学学报, 2017, 37(5):74-79
QU Zhaoyang, SONG Chenchen, REN Youxue, et al. Recommendations Based on Collaborative Filtering by User Activity[J]. Journal of Northeast Electric Power University, 2017, 37(5):74-79 (in Chinese)

[9] GANERIWAL S, SRIVASTAVA M. Reputation-Based Framework for High Integrity Sensor Networks[C]// Proceeding of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, New York, 2004: 66-77

[10] ISHMANOV F, KIM S, NAM S. A Secure Trust Establishment Scheme for Wireless Sensor Networks[J]. Sensors, 2014, 14(1): 1877-1897

[11] ISHMANOV F, KIM S, NAM S. A Robust Trust Establishment Scheme for Wireless Sensor Networks[J]. Sensors, 2015, 15(3): 7040-7061

[12] OUYANG Xi, TIAN Bin, LI Dong, et al. A Novel Hierarchical Reputation Model for Wireless Sensor Networks[J]. International Journal of Digital Content Technology and its Applications, 2012, 6(10): 61-69

[13] 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(增刊 1): 53-59
ZHANG Lin, YIN Na, WANG Ruchuan. Research of Malicious Nodes Identification Based on DPAM-DM Algorithm for WSN[J]. Journal on Communications, 2015, 36(suppl 1):53-59 (in Chinese)

[14] ZHANG Z, ZHU H, LUO S, et al. Intrusion Detection Based on State Context and Hierarchical Trust in Wireless Sensor Networks[J]. IEEE Access, 2017, 5(99): 12088-12102

[15] TAYYAB Khan, KARAN Singh, LE Hoang Sona, et al. A Novel and Comprehensive Trust Estimation Clustering Based Approach for Large Scale Wireless Sensor Networks[J]. IEEE Access, 2019, 7: 58221-58240

[16] SAHOO R R, RAY S, SARKAR S, et al. Guard Against Trust Management Vulnerabilities in Wireless Sensor Network[J]. Arabian Journal for Science & Engineering, 2018, 43(12): 7229-7251

[17] SINGH M, SARDAR A R, MAJUMDER K, et al. A Lightweight Trust Mechanism and Overhead Analysis for Clustered WSN[J]. IETE Journal of research, 2017, 63(3): 297-308

[18] TARIQ N, ASIM M, MAAMAR Z, et al. A Mobile Code-Driven Trust Mechanism for Detecting Internal Attacks in Sensor Node-Powered IOT[J]. Journal of Parallel and Distributed Computing, 2019, 134: 198-206

[19] WU X, HUANG J, LING J, et al. BLTM: Beta and LQI Based Trust Model for Wireless Sensor Networks[J]. IEEE Access, 2019, 7: 43679-43690

[20] 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, 2019, 40(1): 38-43
TENG Zhijun, GUO Liwen, LYU Jinling, et al. WSN Bayes Reputation Evaluation Model Based on Time Series Information Analysis[J]. Journal of Zhengzhou University, 2019, 40(1): 38-43 (in Chinese)

[21] 李云,于季弘,尤肖虎. 资源受限的机会网络节点激励策略研究[J]. 计算机学报, 2013, 36(5): 947-956
LI Yun, YU Jihong, YOU Xiaohu. An Incentive Protocol for Opportunistic Networks with Resources Constraint[J]. Chinese Journal of Computers, 2013, 36(5): 947-956 (in Chinese)

[22] 杨静,李无忧,闫俊杰,等. 串谋行为识别的间断连接无线网络数据转发机制[J]. 系统工程与电子技术, 2017, 39(11): 2571-2579
YANG Jing, LI Wuyou, YAN Junjie, et al. Collision Behavior Recognizing Data Forwarding for Intermittently Connected Wireless Network[J]. Systems Engineering and Electronics, 2017, 39(11): 2571-2579 (in Chinese)

[23] HEINZELMAN W R, CHANDRAKASAN A, BALAKRISHNAN H. Energy-Efficient Communication Protocol for Wireless Microsensor Networks[C]// Proceedings of the 3rd Annual Hawaii International Conference on System Sciences, Hawaii, USA, 2000: 1-10

[24] SIDDIQUI S, GHANI S, KHAN A A. PD-MAC: Design and Implementation of Polling Distribution-Mac for Improving Energy Efficiency of Wireless Sensor Networks[J]. International Journal of Wireless Information Networks, 2018, 25(1): 1-9

[25] BAO F, CHEN I R, CHANG M J, et al. Hierarchical Trust Management for Wireless Sensor Networks and Its Applications to Trust-Based Routing and Intrusion Detection[J]. IEEE Trans on Network & Service Management, 2012, 9(2): 169-183

Model for Malicious Node Recognition Based on Environmental Parameter Optimization and Time Reputation Sequence

TENG Zhijun[1,2], PANG Baohe[2], SUN Mingyang[3], XIE Luying[2], GUO Liwen[4]

(1.Northeast Electric Power University, Key Laboratory of Modern Power System Simulation and Control & Renewable Energy Technology, Ministry of Education, Jilin 132012, China;
2.School of Electrical Engineering, Northeast Electric Power University, Jilin 132012, China;
3.School of Automation Engineering, Northeast Electric Power University, Jilin 132012, China;
4.Ericsson(Xi'an) Information and Communication Technology Service Co., Ltd. Dalian Branch, Dalian 116000, China)

Abstract: Wireless sensor network (WSN) works in a complex environment. To interdict the malicious nodes which attacks the safety of network, such as interrupt attacks and selective forwarding attacks, based on TS-BRS reputation model, a model for malicious node identification based on MNRT-OEP&RS algorithm is constructed. Using the linear regression of machine learning and combining the energy of nodes, data volume, number of adjacent nodes, the node sparsity and other deterministic parameters can solve environmental parameters. Then the similarity of between the benchmark reputation sequence and cycle reputation sequence sets the dynamic reputation double threshold are calculated in order to identify the malicious nodes by dynamically considering the information forwarding behavior. The simulated results show that the improved algorithm can guarantee the security of wireless sensor networks in complex environments effectively with above 90% recognition of malicious nodes and below 8% false positive rate.

Keywords: wireless senor network; network security; environmental impact; linear regression; dynamic reputation double threshold