基于简化云与K/N投票的选择性转发攻击检测方法

尹荣荣*①② 张文元①② 杨绸绸① 李曦达①

①(燕山大学信息科学与工程学院 秦皇岛 066004)

②(燕山大学河北省特种光纤与光纤传感重点实验室 秦皇岛 066004)

摘 要：针对无线传感器网络中恶意节点产生的选择性转发攻击行为，该文提出一种有效的攻击检测方法。该方法将简化云模型引入信任评估中，结合改进的K/N投票算法确定目标节点的信任值，将目标节点信任值与信任阈值比较，进行选择性转发攻击节点的判定。仿真结果表明，当信任阈值为0.8时，经过5个时间段后，该方法能够有效地检测出网络中的选择性转发攻击节点，具有较高的检测率和较低的误检率。

关键词：选择性转发攻击；简化云；改进的K/N投票算法；信任评估模型；信任阈值

中图分类号：TN915.08; TP393 **文献标识码**：A **文章编号**：1009-5896(2020)12-2841-08

DOI: 10.11999/JEIT190274

A Selective Forwarding Attack Detection Method Based on Simplified Cloud and K/N Voting Model

YIN Rongrong①② ZHANG Wenyuan①② YANG Chouchou① LI Xida①

①(*School of Information Science and Engineering, Yanshan University, Qinhuangdao* 066004, *China*)

②(*Key Laboratory for Special Fiber and Fiber Sensor of Hebei Province, Yanshan University, Qinhuangdao* 066004, *China*)

Abstract: For the selective forwarding attack behavior generated by malicious nodes in wireless sensor networks, an efficient detection method is proposed. The simplified cloud model is introduced into the trust evaluation model, and the improved K/N voting algorithm is used to obtain the trust value of the target node. Then, the trust value of the target node is compared with the trust threshold to identify the attack node. The simulation results show that when the trust threshold is 0.8 and after 5 time periods, the proposed method can effectively detect the selective forwarding attack nodes, and it has high detection rate and low fault rate.

Key words: Selective forwarding attack; Simplified cloud; Improved K/N voting algorithm; Trust evaluation model; Trust threshold

1 引言

随着无线传感器网络广泛的实际应用，其安全性显得越来越重要[1]。与其他类型的复杂网络一样，无线传感器网络容易遭受各种安全攻击的威胁[2]，尤其是内部攻击。选择性转发攻击作为多种内部攻击中危害最严重的攻击形式之一，攻击者将他们的错误行为隐藏在正常的数据包丢失中，以混淆检测，具有很强的隐蔽性和破坏性[3]。因此，将发起选择性转发攻击的恶意节点剔除网络是当前广大学者研究的热点。

针对选择性转发攻击检测问题，文献[4–6]引入了信任机制，建立了节点的信任模型，对恶意节点的检测起到了很好的作用，但这些网络中的许多应用需求和特性并不都适应于无线传感器网络。针对无线传感器网络的选择性转发攻击问题，有学者开始了无线传感器网络的信任管理研究[7]。Zawaideh等人[8]提出了基于公平信任的恶意节点检测和隔离方案，该方案可以有效地降低正常节点被误判为恶意节点的比例，但是需要经过不断更新信誉列表才能逐渐找出恶意节点。Ozcelik等人[9]提出了混合入侵检测系统，该方案可以集中检测恶意节点，但存在主观权重的局限性。周治平等人[10]提出了ITEM检测方案，运用贝叶斯和熵的信任评估模型构建直

收稿日期：2019-04-22；改回日期：2020-05-28；网络出版：2020-11-13
*通信作者： 尹荣荣 yrr@ysu.edu.cn
基金项目：国家自然科学基金(61802333)，国家留学基金(201808130258)，河北省高等学校科学技术研究项目(QN2018029)
Foundation Items: The National Natural Science Foundation of China (61802333), The State Scholarship Fund of China (201808130258), The Science and Technology Research Project of Colleges and Universities in Hebei Province (QN2018029)

接信任值，该模型在一定程度上克服了主观分配权重带来的局限性，但是对于决定节点正常和恶意的信任阈值没有给出明确的求解方式。与此同时，Sajjad等人[11]提出的NeTMids检测方案，Prabhakar等人[12]提出的SGHA检测方案和Ahmad等人[13]提出的RBMND检测方案，都是通过直接信任值和间接信任值加权求和得出综合信任值，然后和信任阈值比较来检测恶意节点。其中NeTMids方案可以检测泛洪、干扰和选择性转发攻击，但是对于选择性转发攻击的检测是通过简单的节点转发率大小进行判别的，误检率较高。SGHA方案对于接近网关节点的恶意节点检测率较高，而远离网关的恶意节点检测率较低，导致总体检测率下降。RBMND方案则通过使用Merkle树哈希算法来计算节点转发率，忽略了环境因素对网络造成的丢包影响。可见，以上选择性转发攻击恶意节点的信任评估思想多是通过监测或者计算邻居节点转发率进行直接信任值的判定，而转发率具有一定的随机性和不确定性，需要找一种方法对节点转发率的模糊性评估进行精确化。

云模型是在统计数学和模糊数学的基础上，能够实现定性概念与其数值表示之间不确定性转换的模型，由于其良好的数学性质，可以表示现实生活中大量的不确定现象[14]，将信任机制和云模型融合起来，可以实现信任的准确性评估[15–17]。蔡绍滨等人[15]构建了基于云理论的信任模型，该模型用云模型计算节点的一次信任值，将云理论和信任计算有效结合起来，但未能解决入侵识别敏感度与入侵容忍之间的矛盾问题。徐晓斌等人[16]采用轻量云的二元组表示各信任指标，以期望作为整体信任情况，熵作为信任的不确定性，克服了敏感度和入侵容忍的矛盾问题，但存在针对节点单一攻击的决策困难问题。肖云鹏等人[17]通过对直接信任和间接信任进行加权综合后再利用简化逆向云算子进行计算，解决了单一攻击的信任决策困难问题，但没有兼顾评估个体的信任状况，降低了评估精度。本文在讨论目标节点的信任评估时，将简化云的优点和改进K/N投票算法相结合，利用简化云对节点进行信任评价，能够量化评估节点信任的不确定性，既可以保证信任情况的相对稳定，又可以实现较敏感的异常行为发现。同时利用改进K/N投票算法可以兼顾邻居节点对目标节点信任评估的个体差异性。综合两者进行目标节点的信任计算，使得评估结果更为准确。

基于上述考虑，本文提出了基于简化云和改进K/N投票的信任评估模型，并将其运用于选择性转发攻击恶意节点识别中，给出了一种新的选择性转发攻击检测方法，该方法将简化云理论引入信任建模研究，通过监视邻居节点的转发率构建简化云模型，将简化云模型关联度作为直接信任值，通过信任值的传递性计算间接信任值，进而运用改进的K/N投票算法得到目标节点的最终信任值，最后和信任值阈比较来检测恶意节点，提升了网络中恶意节点的检测率，降低了误检率。

2 基于简化云和K/N投票的信任评估模型

2.1 简化云模型的建立

转发率作为判断选择性转发攻击的重要依据，会受到环境等众多因素的影响，因此，节点的转发率具有随机性和不确定性。云模型用云的3个数字特征，期望Ex、熵En和超熵He表示定量数据的定性特征，用以表示数据的整体水平、离散程度及不确定度。考虑到无线传感器网络中节点计算能力有限，应避免较复杂的计算，故继承徐晓斌等人[16]的轻量优点，只采用2个数字特征，即期望Ex和熵En来表示简化云特征。

网络在部署完成后，各个节点开始进行数据的传输，设m个节点同时在n个连续的时间片段Δt内对邻居节点的转发率进行监听，为了提高检测效率，加快恶意节点的排查速度，本文借助计算简单高效，且性能与云模型接近的简化逆向云算法[17]对邻居节点的转发率进行精确分析。

设第m个节点在n个连续的时间片段Δt内对邻居节点的转发率信息集为$X_{mn}=\{x_1,x_2,\cdots,x_n\}$，可以建立该邻居节点的简化云模型LC(Ex,En)，其中Ex表示信息集期望，即该邻居节点在n个Δt时间内转发率的均值；En表示信息集的熵，即该邻居节点转发率相对转发率均值的偏离程度，呈现一定的随机性和模糊性。

$$\mathrm{Ex}=\overline{X}=\frac{1}{n}\sum_{i=1}^{n}x_i \tag{1}$$

$$\mathrm{En}=\sqrt{\frac{\pi}{2}}\times d=\sqrt{\frac{\pi}{2}}\times\frac{1}{n}\sum_{i=1}^{n}\left|x_i-\overline{X}\right| \tag{2}$$

其中，x_i和$\overline{X}$分别表示该邻居节点在第i个时间片段内的转发率和n个时间片段内转发率的均值。

由于云由大量云滴组成，一个云滴是定性概念上的一次实现，用(x_i,y_i)来表示云模型中的一个云滴，这里y_i为该邻居节点在第i个Δt时间内的转发率对应的云隶属度[18]

$$y_i=\mathrm{e}^{-(x_i-\mathrm{Ex})^2/2\mathrm{En}^2} \tag{3}$$

2.2 基于简化云的信任值确定

通过上面节点转发率构建出云滴，形成简化云模型进行节点i对邻居节点j的直接信任评估，能够

兼顾转发率的随机性和不确定性。在正态云中，有99.74%的云滴落在(Ex–3En, Ex+3En)，因此，可以用{(Ex–3En, Ex+3En)}表示云滴落在(Ex–3En, Ex+3En)区间的集合。那么，节点N_i和节点N_j在n个Δt时间的转发率构建的云模型相交的云滴集合为N，节点N_i和节点N_j在n个Δt时间的转发率构建的云模型合并的云滴集合为M，则节点N_i和邻居节点N_j在n个Δt时间片段的转发率构建的云模型的关联度[19]k_{ij}，即节点i对邻居节点j的直接信任值t_{ij}^{dir}表示为

$$t_{ij}^{\mathrm{dir}} = k_{ij} = \frac{|N|}{|M|} \tag{4}$$

节点i对邻居节点j进行信任评估时，还需要从其他邻居节点处获得节点j的可信度，根据信任值的传递性[20]，节点i对邻居节点j的间接信任评估，可以通过共同邻居节点的推荐信任值进行衡量，故间接信任值t_{ij}^{indir}的计算为

$$t_{ij}^{\mathrm{indir}} = \frac{\sum\limits_{k\in M_k} t_{ik} \times t_{kj}}{|M_k|} \tag{5}$$

其中，M_k表示节点i和节点j之间共同信任推荐节点的集合。

为了解决主观信任值局限性的问题，节点i对邻居节点j的综合信任值由直接信任值和间接信任值加权求和得到，综合信任值的计算公式如式(6)所示

$$T_{ij} = \alpha t_{ij}^{\mathrm{dir}} + (1-\alpha) t_{ij}^{\mathrm{indir}} \tag{6}$$

其中，α为直接信任的权重。

2.3 基于改进K/N投票算法的信任评估模型

按照以往的K/N投票算法，对网络中目标节点的信任值的评判只是简单地依靠其它度量节点判定值的线性相加，这种投票方法将中和掉相互冲突的票，没有考虑到投票个体的差异性。基于此，在K/N投票算法的基础上，本文利用改进的K/N投票算法进行最终的信任评估建模，其表示方法如下：目标节点的信任值取决于邻居节点的度量权重和邻居节点对目标节点的度量结果两个方面。在不确定度非常大的信任评价情况下，普通的K/N投票算法很容易因为数量方面的优势而导致评估失误，改进的K/N投票算法通过引入度量节点权重，反映了投票个体差异对评估结果的影响，增强了统计分析的鲁棒性，有效地实现了对目标节点的信任判断。

邻居节点的度量权重由这些节点的信任值大小决定，则邻居节点i的信任值归一化后的度量权重为

$$\delta_i = \frac{T_i}{\sum\limits_{i\in \mathrm{Nei}} T_i} \tag{7}$$

其中，Nei为目标节点的邻居节点集合。因此，可以得到m个邻居节点对应的度量权重矩阵为

$$\mathbf{NW} = \begin{bmatrix} \delta_1 & \delta_2 & \cdots & \delta_m \end{bmatrix} \tag{8}$$

根据式(6)将m个邻居节点对目标节点j的综合信任值作为度量结果，对应的度量结果矩阵为

$$\mathbf{CTV} = \begin{bmatrix} T_{1j} & T_{2j} & \cdots & T_{mj} \end{bmatrix} \tag{9}$$

那么，由邻居节点对应的度量权重和邻居节点对目标节点的度量结果，可以得到目标节点j的最终信任值

$$T_j = \mathbf{NW} \cdot \mathbf{CTV}^{\mathrm{T}} \tag{10}$$

目标节点j的信任值T_j越大，表明节点越不容易产生恶意攻击，当目标节点j的信任值T_j大于信任阈值T时，目标节点为正常节点，否则认为目标节点为选择性转发攻击节点。因此，信任阈值T是限定网络中节点为正常节点和恶意节点的关键性因素，本文的信任阈值T优化确定在仿真部分给出。

3 基于信任评估模型的选择性转发攻击检测方法

基于信任评估模型的选择性转发攻击检测方法的核心是利用简化云模型将具有随机性和模糊性的节点转发率精确化，综合直接信任和间接信任，获取节点的综合信任值，并利用改进的K/N投票算法兼顾评估个体的差异性，融合综合信任值和节点信任值权重，确定目标节点的最终信任值，算法流程如图1所示。

检测方法具体步骤如下：

步骤 1：网络中每个节点监听邻居节点的转发率，建立邻居节点转发率矩阵，并从转发率矩阵中提取每个节点的信息集X_{mn}，构建简化云模型。

步骤 2：根据云滴的分布状态，计算邻居节点对目标节点的云模型关联度，即邻居节点对目标节点的直接信任值t_{ij}^{dir}。

步骤 3：计算邻居节点对目标节点的间接信任值t_{ij}^{indir}，由直接信任值和间接信任值加权求和得到邻居节点对目标节点的综合信任值T_{ij}。

步骤 4：由邻居节点对目标节点的综合信任值和邻居节点所占权重，作为邻居节点对目标节点的一次信任评估，所有邻居节点信任评估的和得到目标节点的最终信任值T_j。

步骤 5：将目标节点的最终信任值T_j和信任阈

值T比较，大于信任阈值的目标节点为正常节点，否则为选择性转发攻击节点。

步骤 6：完成网络中所有节点的信任评估，找出网络中选择性转发攻击的节点。

4 仿真实验

为了验证本文选择性转发攻击检测方法的性能，本实验参考文献[17]情况设定仿真参数，采集节点交互通信情况进行信任计算，在半径为100 m的圆形监测区域内随机布置200个传感器节点，每个节点的通信半径均为30 m，节点转发率分布范围为0.9～1.0，初始每个节点的信任值为0.5，每运行一个时间段t后进行一次节点信任值的评估，将每个时间段分为n个Δt时间片段，每个Δt时间片段进行一次转发率的记录，随机选取一定比例的恶意节点进行性能的分析。具体仿真参数如表1所示。

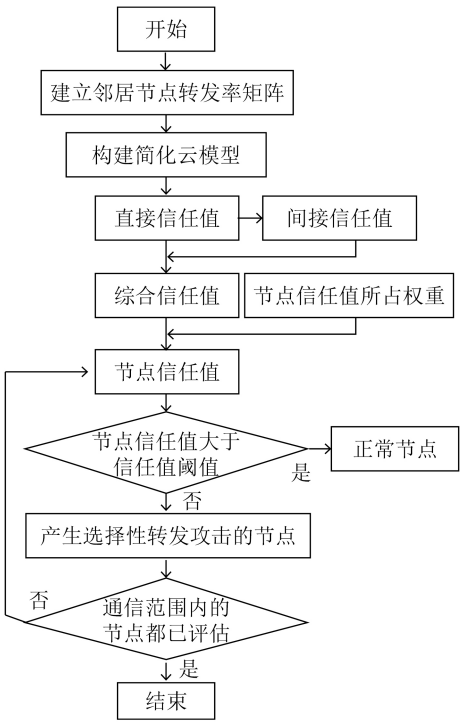


图 1 基于信任评估模型的选择性转发攻击检测方法流程图

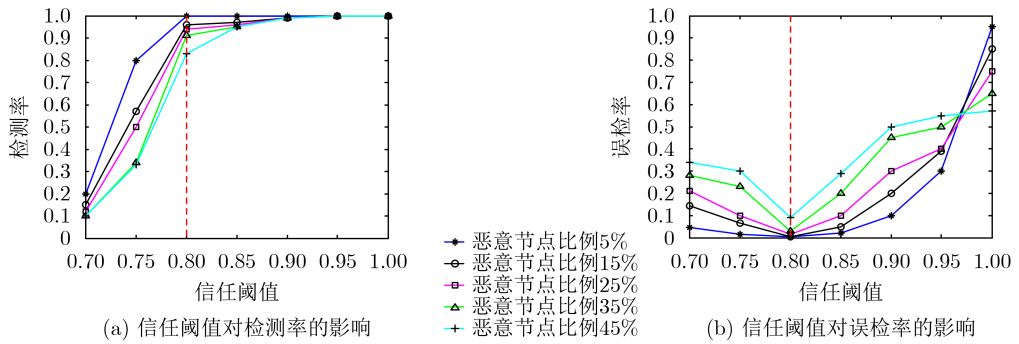
4.1 本文检测方法有效性验证

(1) 信任阈值的分析：信任阈值T是限定节点为正常节点和恶意节点的关键性因素，其取值大小是决定节点是否为正常节点的分界线，下面对于信任阈值T的取值进行实验确定。在不同的恶意节点比例场景下，将实验运行5个时间片段后，信任阈值对检测率(检测出的恶意节点个数比恶意节点的总个数)和误检率(正常节点被判定为恶意节点和恶意节点被判定为正常节点的个数和比节点总数)的影响如图2所示。

由图2(a)可以看出随着信任阈值的增加，恶意节点检测率在逐渐增加。这是由于被判定为恶意节点的个数随之增加，恶意节点被检测出来的个数也随之增加，当阈值达到1.0时，恶意节点都被检测出来，检测率达到100%。由图2(b)可以看出随着信任阈值的增加，误检率呈现先降后增的趋势，在信任阈值为0.8时，误检率达到最低。这是因为在信任阈值小于0.8时，正常节点被判定为恶意节点的个数变化不大，而恶意节点被判定为正常节点的个数在减少。而当信任阈值大于0.8时，恶意节点被判定为正常节点的个数变化不大，而正常节点被判断为恶意节点的个数在不断增加。并且恶意节点比例越小，意味着正常节点个数越多，出现正常节点被判断为恶意节点的误检率的增加速度就越快，当阈值为1.0时，恶意节点都被检测出来，而正常节点都被判定为恶意节点。从而，综合两者选取0.8作为本文信任评估模型的信任阈值T。

表 1 仿真参数

参数	值
时间段t	1000 s
直接信任值权重α	0.6
云滴个数w	100
包的大小s	64 bit
包传输速率v	640 bit/s



(a) 信任阈值对检测率的影响　(b) 信任阈值对误检率的影响

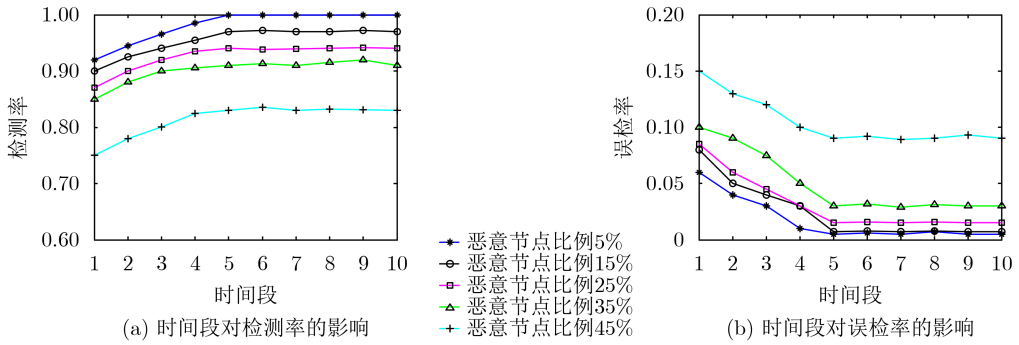
图 2 信任阈值对检测率和误检率的影响

(2) 时间段的分析：在不同恶意节点比例下，考察随网络运行时间段的递增网络检测率和误检率的变化情况，如图3所示。

由图3(a)和图3(b)可以看出随着时间段的增加，检测率是先增加后趋于稳定，而误检率是先减小后趋于稳定。这主要是因为随着时间段的增加，邻居节点的度量权重开始发生变化，邻居节点对目标节点的信任值的影响也开始变化，当经过5个时间段后，各个目标节点的信任值趋于稳定，因此，邻居节点对目标节点的信任值影响趋于稳定，网络的检测率和误检率也趋于稳定。此外，当时间段一定时，检测率和恶意节点比例呈反比，主要是因为恶意节点比例越小，目标节点的邻居节点中正常节点占比越大，对恶意节点的判定越准确；而误检率和恶意节点呈正比，主要是因为恶意节点比例越大，目标节点的邻居节点中恶意节点占比越大，对正常节点的判定误差越大。从而，根据时间段对检测率和误检率的影响，选取5个时间段作为本文信任评估模型的监测时间段n。

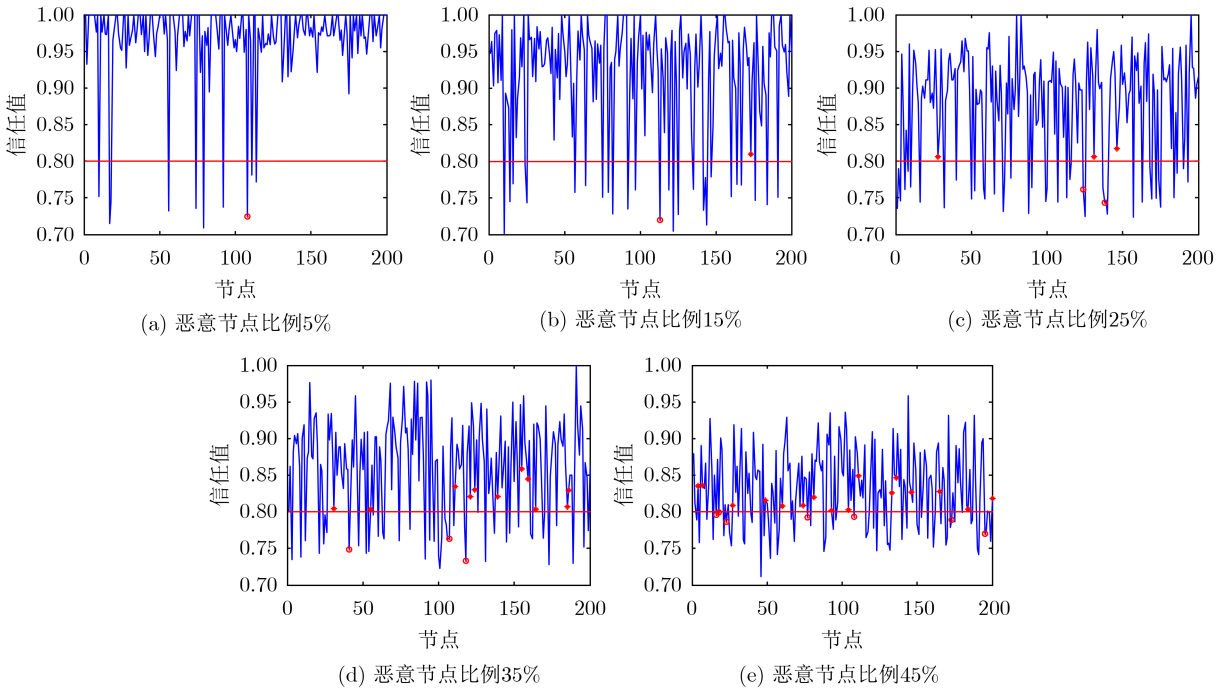
(3) 节点信任值分析：图4更直观地展示了当网络运行5个时间段，在不同恶意节点比例下节点信任值的变化情况，包括正常节点被判断为恶意节点(用红色o表示)的个数和恶意节点被判断为正常节点(用红色*表示)的个数。信任值恒等于0.8的直线是本文信任评估模型判定节点是否为正常节点的分界线，即节点的信任阈值T。节点的信任值在该分界线的上半部分，则被判定为正常节点，否则被判定为恶意节点。

由图4可见随着恶意节点比例增加，正常节点信任值呈下降趋势，因为目标节点的邻居节点中的恶意节点比例随之增加，邻居节点对目标节点的恶意评估就会增加，导致总体节点信任值呈下降趋



(a) 时间段对检测率的影响　　(b) 时间段对误检率的影响

图 3 时间段对检测率和误检率的影响



(a) 恶意节点比例5%　(b) 恶意节点比例15%　(c) 恶意节点比例25%

(d) 恶意节点比例35%　(e) 恶意节点比例45%

图 4 恶意节点比例对节点信任值的影响

势。另外，正常节点被判断为恶意节点和恶意节点被判断为正常节点的个数在逐渐增加，因为目标节点的邻居节点中的恶意节点比例随之增加，如果目标节点是正常节点，则其邻居节点增加的恶意节点对目标节点信任值的恶意评估会使其信任值降低，导致低于信任阈值的正常节点增加。如果目标节点是恶意节点，则其邻居节点减少的正常节点对恶意节点的信任值评估会使其信任值增加，导致高于信任阈值的恶意节点增加。

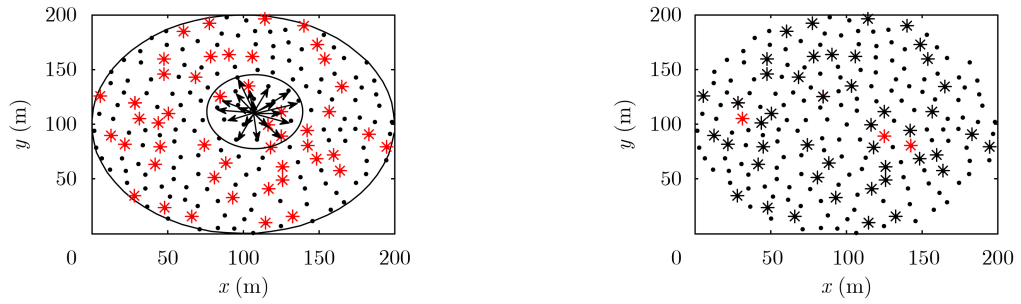
4.2 本文检测方法与其他方法的性能对比分析

(1) 检测前后本文网络拓扑的分析：为了更直观地体现本文检测方法的效果，在恶意节点比例为25%的情况下，图5(a)为网络部署时的仿真场景图，黑色“●”表示正常节点，红色“*”表示恶意节点，大圆为节点分布区域，小圆为节点的通信范围，箭头指向的节点为该节点的邻居节点。在圆形区域内正常节点和恶意节点都是随机部署的，每个节点都有多个邻居节点，每两个邻居节点都有多个相交的邻居节点。图5(b)为当信任值阈为0.8时，经过5个时间段时本文检测方法的仿真场景图，黑色“*”表示被检测出来的恶意节点，红色“*”表示未被检测出来的恶意节点。

从图5(b)运行本文检测方法后的结果可以看出，恶意节点的检测率可以达到94%左右，直观地表明本文检测方法可以很好地识别出恶意节点。

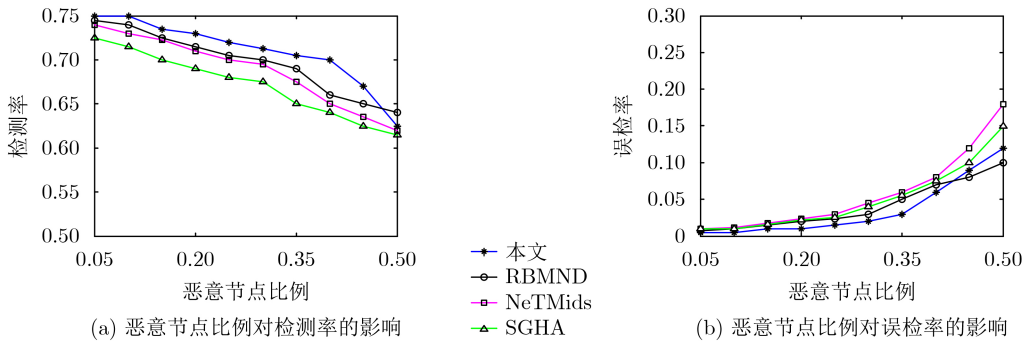
(2) 检测率和误检率的对比分析：最后给出本文方法、NeTMids方法[11]、SGHA方法[12]和RBMND方法[13]，在不同恶意节点比例下的网络检测率和误检率的变化关系对比图，如图6所示。

由图6(a)可以看出随着恶意节点比例的增加，4种方法的检测率都呈下降趋势，但在恶意节点比例小于48%的范围内，本文方法的检测率均比其他方法要高。这是由于本文方法以转发率构建简化云模型，并通过改进K/N投票算法获取节点的最终信任值，可以将转发率具体化同时兼顾评估个体差异，使得检测结果更加准确，而其他方法都是通过监测或者计算邻居节点的转发率直接构建信任值，没有解决转发率随机性和评估个体差异带来的局限性。然而当恶意节点比例大于48%时，RBMND方法的检测率要比本文方法的检测率高，因为RBMND使用Merkle树哈希技术进行恶意节点检测，减小了恶意节点所占比重大对信任值决定大的影响。进一步由图6(b)可以看出随着恶意节点比例的增加，4种方法的误检率都呈上升趋势，但在恶意节点比例小于42%的范围内，本文方法的误检率低于其他方法，这是因为由云滴构建的简化云模型可以很好地将正常节点和恶意节点区分开，而其他方法通过监测计算转发率来求解信任值，误差较大。当恶意节点比例大于42%时，RBMND方法的误检率要低于本文方法，主要是因为RBMND方法会经过多次评估判断出恶意节点，对于多恶意节点的场景误检率较低。



(a) 检测前网络　　(b) 检测后网络

图 5 检测结果对比图



(a) 恶意节点比例对检测率的影响　　(b) 恶意节点比例对误检率的影响

图 6 恶意节点比例对检测率和误检率的影响

5　结束语

本文将简化云模型和改进的K/N投票算法引入信任评估模型中，兼顾了转发率的随机性和评估个体的差异性，使得选择性转发攻击节点的检测率和误检率达到更好的效果。运用实验性的信任阈值T和时间段n求解方式可知，当信任阈值为0.8时，经过5个时间段后，本文方法可以有效地检测出网络中的选择性转发攻击节点。仿真结果表明，当恶意节点比例较小时，本文方法的性能要优于最新的NeTMids, SGHA和RBMND检测方法，当恶意节点比例较大时，本文方法性能开始下降，这是本文方法的不足之处。为此，在恶意节点比例较大的场景下，进一步提高恶意节点的检测率，是我们下一步的研究工作。

参 考 文 献

[1] 周伟伟, 郁滨. WSNs多阶段入侵检测博弈最优策略研究[J]. 电子与信息学报, 2018, 40(1): 63–71. doi: 10.11999/JEIT170323.
ZHOU Weiwei and YU Bin. Optimal defense strategy in WSNs based on the game of multi-stage intrusion detection[J]. *Journal of Electronics & Information Technology*, 2018, 40(1): 63–71. doi: 10.11999/JEIT170323.

[2] IOANNOU C, VASSILIOU V, and SERGIOU C. An intrusion detection system for wireless sensor networks[C]. The 24th International Conference on Telecommunications, Limassol, Cyprus, 2017: 253–259. doi: 10.1109/ICT.2017.7998271.

[3] KALKHA H, SATORI H, and SATORI K. Preventing black hole attack in wireless sensor network using HMM[J]. *Procedia Computer Science*, 2019, 148: 522–561. doi: 10.1016/j.procs.2019.01.028.

[4] SHABUT A M, DAHAL K P, BISTA S K, *et al*. Recommendation based trust model with an effective defence scheme for MANETs[J]. *IEEE Transactions on Mobile Computing*, 2015, 14(10): 2101–2115. doi: 10.1109/TMC.2014.2374154.

[5] 赵明, 闫寒, 曹高峰, 等. 融合用户信任度和相似度的基于核心用户抽取的鲁棒性推荐算法[J]. 电子与信息学报, 2019, 41(1): 180–186. doi: 10.11999/JEIT180142.
ZHAO Ming, YAN Han, CAO Gaofeng, *et al*. Robust recommendation algorithm based on core user extraction with user trust and similarity[J]. *Journal of Electronics & Information Technology*, 2019, 41(1): 180–186. doi: 10.11999/JEIT180142.

[6] 李致远, 王汝传. 一种移动P2P网络环境下的动态安全信任模型[J]. 电子学报, 2012, 40(1): 1–7. doi: 10.3969/j.issn.0372-2112.2012.01.001.
LI Zhiyuan and WANG Ruchuan. A dynamic secure trust model for mobile P2P networks[J]. *Acta Electronica Sinica*, 2012, 40(1): 1–7. doi: 10.3969/j.issn.0372-2112.2012.01.001.

[7] 荆琦, 唐礼勇, 陈钟. 无线传感器网络中的信任管理[J]. 软件学报, 2008, 19(7): 1716–1730. doi: 10.3724/SP.J.1001.2008.01716.
JING Qi, TANG Liyong, and CHEN Zhong. Trust management in wireless sensor networks[J]. *Journal of Software*, 2008, 19(7): 1716–1730. doi: 10.3724/SP.J.1001.2008.01716.

[8] ZAWAIDEH F, SALAMAH M, and Al-BAHADILI H. A fair trust-based malicious node detection and isolation scheme for WSNs[C]. The 2nd International Conference on the Applications of Information Technology in Developing Renewable Energy Processes & Systems (IT-DREPS), Amman, Jordan, 2017: 1–6. doi: 10.1109/IT-DREPS.2017.8277813.

[9] OZCELIK M M, IRMAK E, and OZDEMIR S. A hybrid trust based intrusion detection system for wireless sensor networks[C]. 2017 Networks, Computers and Communications (ISNCC), Marrakech, Morocco, 2017: 1–6. doi: 10.1109/ISNCC.2017.8071998.

[10] 周治平, 邵楠楠. 基于贝叶斯的改进WSNs信任评估模型[J]. 传感技术学报, 2016, 29(6): 927–933. doi: 10.3969/j.issn.1004-1699.2016.06.023.
ZHOU Zhiping and SHAO Nannan. An improved trust evaluation model based on Bayesian for WSNs[J]. *Chinese Journal of Sensors and Actuators*, 2016, 29(6): 927–933. doi: 10.3969/j.issn.1004-1699.2016.06.023.

[11] SAJJAD S M, BOUK S H, and YOUSAF M. Neighbor node trust based intrusion detection system for WSN[J]. *Procedia Computer Science*, 2015, 63: 183–188. doi: 10.1016/j.procs.2015.08.331.

[12] PRABHAKAR A and ANJALI T. Mitigating selective Gray Hole Attack in wireless multi-hop network[C]. 2017 International Conference on Wireless Communications, Signal Processing and Networking, Chennai, India, 2017: 1223–1227. doi: 10.1109/WiSPNET.2017.8299958.

[13] AHMAD A, ALAJEELY M, and DOSS R. Reputation based malicious node detection in OppNets[C]. The 13th International Joint Conference on Computer Science and Software Engineering, Khon Kaen, Thailand, 2016: 1–6. doi: 10.1109/JCSSE.2016.7748925.

[14] 李德毅, 刘常昱. 论正态云模型的普适性[J]. 中国工程科学, 2004, 6(8): 28–34. doi: 10.3969/j.issn.1009-1742.2004.08.006.
LI Deyi and LIU Changyu. Study on the universality of the normal cloud model[J]. *Engineering Science*, 2004, 6(8): 28–34. doi: 10.3969/j.issn.1009-1742.2004.08.006.

[15] 蔡绍滨, 韩启龙, 高振国, 等. 基于云模型的无线传感器网络恶意节点识别技术的研究[J]. 电子学报, 2012, 40(11): 2232–2238. doi: 10.3969/j.issn.0372-2112.2012.11.015.

CAI Shaobin, HAN Qilong, GAO Zhenguo, *et al*. Research on cloud trust model for malicious node detection in wireless sensor network[J]. *Acta Electronica Sinica*, 2012, 40(11): 2232–2238. doi: 10.3969/j.issn.0372-2112.2012.11.015.

[16] 徐晓斌, 张光卫, 王尚广, 等. 基于轻量云模型的WSN不确定性信任表示方法[J]. 通信学报, 2014, 35(2): 63–69. doi: 10.3969/j.issn.1000-436x.2014.02.009.

XU Xiaobin, ZHANG Guangwei, WANG Shangguang, *et al*. Representation for uncertainty trust of WSN based on lightweight-cloud[J]. *Journal on Communications*, 2014, 35(2): 63–69. doi: 10.3969/j.issn.1000-436x.2014.02.009.

[17] 肖云鹏, 姚豪豪, 刘宴兵. 一种基于云模型的WSNs节点信誉安全方案[J]. 电子学报, 2016, 44(1): 168–175. doi: 10.3969/j.issn.0372-2112.2016.01.025.

XIAO Yunpeng, YAO Haohao, and LIU Yanbing. A WSNs node reputation security scheme based on cloud model[J]. *Acta Electronica Sinica*, 2016, 44(1): 168–175. doi: 10.3969/j.issn.0372-2112.2016.01.025.

[18] 李德毅. 知识表示中的不确定性[J]. 中国工程科学, 2000, 2(10): 73–79. doi: 10.3969/j.issn.1009-1742.2000.10.018.

LI Deyi. Uncertainty in knowledge representation[J]. *Engineering Science*, 2000, 2(10): 73–79. doi: 10.3969/j.issn.1009-1742.2000.10.018.

[19] 胡涛, 王树宗, 杨建军. 基于云模型的物元综合评估方法[J]. 海军工程大学学报, 2006, 18(1): 85–88. doi: 10.3969/j.issn.1009-3486.2006.01.018.

HU Tao, WANG Shuzong, and YANG Jianjun. Matter-element integration evaluation method based on cloud model[J]. *Journal of Naval University of Engineering*, 2006, 18(1): 85–88. doi: 10.3969/j.issn.1009-3486.2006.01.018.

[20] 李慧, 马小平, 施珺, 等. 复杂网络环境下基于信任传递的推荐模型研究[J]. 自动化学报, 2018, 44(2): 363–376. doi: 10.16383/j.aas.2018.c160395.

LI Hui, MA Xiaoping, SHI Jun, *et al*. A recommendation model by means of trust transition in complex network environment[J]. *Acta Automatica Sinica*, 2018, 44(2): 363–376. doi: 10.16383/j.aas.2018.c160395.

尹荣荣：女，1985年生，副教授，研究方向为无线传感器网络、网络安全.

张文元：男，1991年生，硕士生，研究方向为无线传感器网络攻击检测.

杨绸绸：女，1974年生，副研究员，研究方向为无线传感器网络攻击防御.

李曦达：女，1977年生，副教授，研究方向为无线传感器网络资源优化.

责任编辑：陈 倩