DOI:10.11918/202101035

融合节点信誉度和路径跳数的 WSNs 虫洞攻击检测策略

滕志军[1,2],杜春秋[2],孙汇阳[3],李 梦[2],王艳娇[1,2]

(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.北京电子科技学院 密码科学与技术系,北京 100070)

摘 要:为抵御无线传感器网络中的虫洞攻击,提高网络性能。本文根据虫洞攻击下节点邻居数目出现的异常情况,对邻居数目超出阈值的可疑节点进行筛选,然后令其专有邻居集中的节点相互通信,记录路径跳数,将跳数超出虫洞阈值的路径标记为待测路径;借助贝叶斯信誉模型计算该待测路径上中间节点的直接信任值,并结合邻居数目、处理延时、节点能量、包转发率等信任因素对节点的间接信任值进行评判,进而获得该节点的综合信任值;通过将路径跳数与中间节点的综合信任相结合,计算待测路径的路径信任评价量,并依据受虫洞攻击节点的路径特性合理设定信任阈值,提出一种融合节点信誉度和路径跳数的虫洞攻击检测策略(wormhole attack detection strategy integrating node creditworthiness and path hops,WADS-NC&PH),以检测无线传感器网络中的虫洞攻击。仿真结果表明,WADS-NC&PH 对虫洞攻击的检测具有显著效果,即使面对高攻击度的网络,该策略仍能有效检出虫洞攻击并移除虚假链路,提高无线传感器网络的安全性和可靠性。

关键词:无线传感器网络;虫洞攻击;路径跳数;虫洞阈值;信誉模型;信任阈值
中图分类号:TN92 **文献标志码**:A **文章编号**:0367-6234(2021)08-0064-08

A wormhole attack detection strategy integrating node creditworthiness and path hops in WSNs

TENG Zhijun[1,2], DU Chunqiu[2], SUN Huiyang[3], LI Meng[2], WANG Yanjiao[1,2]

(1. Key Laboratory of Modern Power System Simulation and Control & Renewable Energy Technology (Northeast Electric Power University), Ministry of Education, Jilin 132012, Jilin, China; 2. School of Electrical Engineering, Northeast Electric Power University, Jilin 132012, Jilin, China; 3. Department of Cryptography Science and Technology, Beijing Electronic Science and Technology Institute, Beijing 100070, China)

Abstract: To resist the wormhole attacks in wireless sensor networks (WSNs) and improve network performance, a wormhole attack detection strategy integrating node creditworthiness and path hops (WADS-NC&PH) was proposed. Based on the abnormal situations of the neighbor number of the nodes under wormhole attacks, the suspicious nodes whose neighbor number exceeded the threshold were screened, and the nodes in their exclusive neighbor set were allowed to communicate with each other. The number of path hops was recorded, and the path whose number of hops exceeded the wormhole threshold was marked as the path to be tested. The Bayesian trust model was utilized to calculate the direct trust value of the intermediate node on the path to be tested, and combined with the trust factors such as the number of neighbors, processing delay, node energy, and packet forwarding rate, the indirect trust value of the node was judged, thereby obtaining the comprehensive trust value of the node. By integrating the number of path hops with the comprehensive trust of intermediate nodes, the path trust evaluation of the path to be tested was calculated. Based on the path characteristics of the nodes attacked by wormholes, the trust threshold was set reasonably, and WADS-NC&PH was proposed to detect wormhole attacks in WSNs. Simulation results show that WADS-NC&PH had a significant effect on the detection of wormhole attacks. Even in the face of highly attacked networks, this strategy could still effectively detect wormhole attacks and remove false links, improving the security and reliability of WSNs.

Keywords: wireless sensor networks (WSNs); wormhole attack; path hops; wormhole threshold; trust model; trust threshold

近年来,随着无线传感器网络(wireless sensor networks,WSNs)的飞速发展,其在军事领域和民用领域都得到了广泛的应用[1],因此保证网络的安全运行具有重要意义。由于传感器节点通常部署在无

收稿日期:2021-01-11
基金项目:国家自然科学基金青年科学基金(61501107)
作者简介:滕志军(1973—),男,教授,硕士生导师
通信作者:杜春秋,2912289944@qq.com

人监管的区域，各节点随机分布，且能量有限，因此很容易受到各种恶意攻击[2-4]。其中，虫洞攻击就是一种常见的恶意攻击形式，其由至少两个相距较远的虫洞节点合谋发起，通过私有信道互相发送信息，从而破坏路由的建立、更新与维护过程[5-7]，对 WSNs 的安全产生严重威胁。

为有效检测虫洞攻击，降低其对网络的影响，国内外专家学者们相继展开研究。董晓梅等[8]提出了一种 WSNs 中针对虫洞攻击的 SMRSA 检测算法。该算法主要根据受攻击节点间通信路径明显变短来定位感染节点所在的可疑路径，然后对可疑路径上的节点进行邻居数目的检查，将邻居数目出现异常的节点视为受攻击节点。Hayajneh 等[9]提出了 SECUND 算法，主要通过检查互斥邻居之间的跳数是否超过预定义的阈值来检测虫洞攻击。Luo 等[10]提出一种 CREDND 检测算法。将虫洞攻击分为外部攻击和内部攻击两种，针对外部攻击利用节点邻居数目和路径跳数进行检测，针对内部攻击则利用邻居监测的方式进行检验。Amish 等[11]基于 RTT 机制和虫洞攻击的数据传输特征，将 AOMDV 路由协议融入了这些方法中，通过比较端到端的时延，筛选出虫洞攻击节点。胡蓉华等[12]提出了一种 SenLeash 虫洞攻击检测机制，主要依据节点的消息传输距离受限特性来检测虫洞攻击。韩挺等[13]提出了一种基于多属性决策的 MANET 路由动态信任模型来判断节点性质。该模型通过引入推荐信任度和推荐节点搜索算法检测网络中的恶意节点。周治平等[14]提出一种改进的贝叶斯信誉模型，根据节点的信任值来检测恶意攻击。另外，针对虫洞攻击对 DV-HOP 定位过程的影响，许多改进的虫洞攻击检测算法相继被提出来[15-16]，这些算法能有效识别虫洞攻击，降低其对定位过程的影响。

上述检测方案为虫洞攻击的研究提供了扎实的理论基础，但仍存在以下几点问题：1）在利用节点间距离进行攻击检测时，需要用到 GPS 等硬件设施，这使得检测过程更加复杂，网络成本较高；2）在根据节点路径跳数进行检测时，未对虫洞链路进行避让，使得检测效率大大降低；3）如果仅利用信誉模型进行攻击检测，则很容易出现虫洞节点漏检的情况；4）若利用传输时延来检测，则节点间需要精准的时钟同步，不仅能耗高且数据的可用性无法得到保证。针对上述问题，本文提出一种融合节点信誉度和路径跳数的虫洞攻击检测策略（WADS-NC&PH）。该策略主要基于网络受攻击后节点邻居数目及路径跳数的变化特点，结合信誉模型，计算可疑节点的路径信任评价量，以判定网络中是否存在虫洞攻击。

1　系统模型

1.1　网络模型

本文假设 WSNs 中节点数目为 N，各节点近似均匀地分布在面积为 S 的整个网络中，每个节点的通信半径为 r，传感器节点的分布密度如下：

$$\rho = \frac{N}{S} \tag{1}$$

节点平均邻居数目 n'的计算方式见式(2)。

$$n' = \rho\pi r^2 = \frac{N\pi r^2}{S} \tag{2}$$

1.2　虫洞攻击模型

WSNs 中的虫洞攻击通常由两个恶意节点合谋发起，二者分别位于网络两端，一般相距较远，节点的配置信息不会出现在路由表中，在网络中处于一种“隐身”的状态。进行数据转发时，一端的虫洞节点将收到的信息通过私有链路传递给位于网络另一端的合谋节点，该合谋节点再将收到的信息以广播的方式发送给周围邻居节点，从而扰乱数据的正常传输，影响网络性能。

本文假设虫洞链路的长度远大于正常节点的通信半径。图 1 为两个虫洞节点 M_1、M_2协同发动虫洞攻击的示意图。其中，源节点 O 到达目的节点 D 的原始路径有两条，路径跳数最少是 6 跳。然而，当网络受到虫洞攻击时，源节点 O 发送的消息会通过虫洞链路直接传送至目的节点 D，该条路径的跳数仅为 1 跳。此时，节点 O、D 会将彼此误认为邻居节点，严重影响网络的正常通信和数据传输。

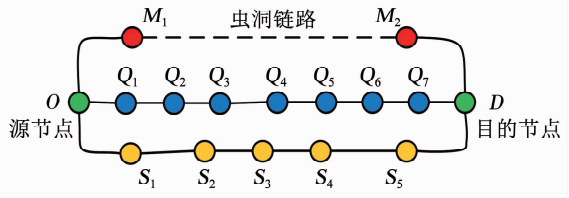

图 1　虫洞攻击模型

Fig. 1　Wormhole attack model

2　虫洞攻击检测

由于虫洞节点的转发特性，导致原本不属于彼此通信范围内的节点间建立连接，使得被攻击节点的邻居数目大量增多。本文根据虫洞攻击这一特性对网络中的可疑节点进行筛选，这样既可以避免针对所有节点启动检测的能量消耗，又可以高效率、有针对性地检测出虫洞攻击。

首先，网络中各节点更新邻居列表，并统计邻节点数目，将各节点的邻居数目记为 G_i，然后将 G_i 与

节点平均邻居数目 n' 相比，设定邻居阈值比为 W，若 $G_i/n' \geqslant W$，说明该节点的邻居数目超出阈值，可能受到虫洞攻击，那么将该节点列入可疑节点名单，准备进行下一阶段的检测。邻居阈值比 W 的大小由后文仿真进行确定。

2.1 路径跳数的计算

如图 2 所示，节点 A、B 为被筛选出的可疑节点，M_1、M_2 为一对虫洞攻击节点，二者通过私有链路相互连接。节点 M_1 将收到的数据包经由虫洞链路直接传递给节点 M_2，然后 M_2 广播相同的数据包，使得其覆盖区域中的每个节点都能接收到该包。假设将节点 A 的 1 跳邻居集表示为 N_A，节点 B 的 1 跳邻居集表示为 N_B，虫洞节点 M_1，M_2 的 1 跳邻居集分别表示为 N_{M1}，N_{M2}。那么在虫洞攻击影响下，节点 A 的原始邻居集 $\{C,D,E,P,Q\}$ 中添加了 N_{M2} 中的所有节点，此时，A 的邻居集合可表示为 $N_A = \{P,Q,C,D,E,R,S,I,J,K,B\}$。同理，节点 B 的邻居集 $N_B = \{R,S,L,N,O,P,Q,F,G,H,A\}$。

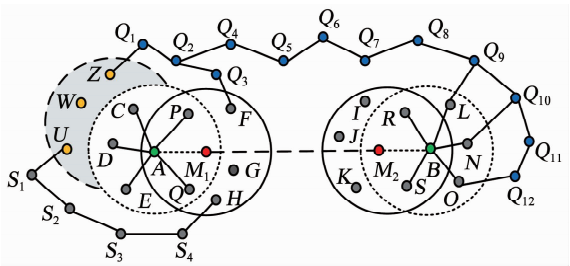

图 2 虫洞攻击检测模型

Fig. 2 Wormhole attack detection model

将公有邻居集定义为节点 A、B 邻居集中相同节点所组成的集合。将 $A(B)$ 的专有邻居集定义为只包含在节点 $A(B)$ 邻居集内而不在节点 $B(A)$ 邻居集内的节点所组成的集合。用 N_{com} 表示节点 A、B 的公有邻居集，$N_{A'}$、$N_{B'}$ 分别表示 A、B 的专有邻居集，则有 $N_{\text{com}} = N_A \cap N_B = \{P,Q,R,S\}$，$N_{A'} = N_A - N_{\text{com}} - \{B\} = \{C,D,E,I,J,K\}$，$N_{B'} = N_B - N_{\text{com}} - \{A\} = \{L,N,O,F,G,H\}$。对于节点 A、B 而言，A 的专有邻节点 C、D、E 与 B 的专有邻节点 L、N、O 相距很远，实际跳数比在虫洞攻击下的跳数高得多。

为了更加准确的检测出虫洞攻击，首先要避开虫洞路径。在计算专有邻居节点间的路径跳数时，本文选择不在节点 A、B 及虫洞节点 M_1、M_2 通信范围内的其他节点作为中间节点，将选定的路径标记为参考路径，并将路径跳数与虫洞阈值相比，判断当前路径类型。参考路径的选取步骤如下。

Step1 节点 C 广播一个 HELLO 消息，根据收到消息的回复情况建立其邻居集合 N_C；

Step2 节点 C 检测其邻居集 N_C 中是否含有与节点 A、B 邻居集 N_A、N_B 中相同的节点，若有，则从其邻居集中删除这些节点，从而获得新的纯净邻居集 $N_{C'}$，否则更新集合 N_C 为 $N_{C'}$，转到 Step3；

Step3 节点 C 再次发送一个数据包 Q，路径目标为网络中的节点 X，选择 $N_{C'}$ 中的某节点 Y 作为下一跳节点进行数据转发；

Step4 节点 Y 重复 Step1 ~ 3，以相同的方式选择下一跳节点，并转发该数据包，依此类推，直至数据包到达目的节点 X；

Step5 搜索出所有从节点 C 到节点 X 的路径，选择跳数最少的有效路径作为参考路径。

2.2 虫洞阈值的选取

如图 3(a) 所示，节点 A、B 为真实邻居，二者通信范围内不存在虫洞攻击节点，通信距离 $d < r$。令节点 A 专有邻居集中的某节点与节点 B 专有邻居集中的所有节点进行通信，那么距离最远的两个节点的位置如图中 C、G 所示。节点 C 发送一个数据包，目标为网络中的节点 G(选取不在 N_A、N_B 中的节点作为中间节点)，极限情况下的最短路径为图中 $C-D-E-F-G$，此时 C、G 间的通信路径长度为 $d_1+d_2+d_3+d_4$($d_i \leqslant r, i=1,2,3,4$)，路径跳数 $l = (d_1+d_2+d_3+d_4)/r \leqslant 4$。当节点 A、B 间的通信距离达到最大通信半径 r 时，如图 3(b) 所示，节点 C、G 间最短通信路径长度为 $4r$，此时路径跳数 $l = 4r/r = 4$。

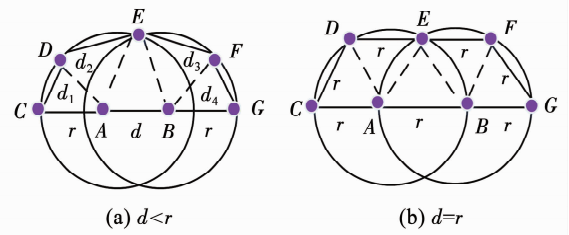

图 3 节点通信模型

Fig. 3 Node communication model

通过上述分析可知，当节点 A、B 受到虫洞攻击时，按本文参考路径选取方式得到的专有邻居节点间的最小跳数应不低于 4 跳。因而，本文将虫洞阈值 ε 设置为：$\varepsilon = 4 + \tau$。若 $N_{A'}$ 中的节点到 $N_{B'}$ 中所有节点的路径跳数均低于虫洞阈值，则节点 A、B 为正常节点，二者通信范围内不存在虫洞攻击；若存在跳数高于虫洞阈值的路径，则节点 A、B 很可能受到虫洞攻击。考虑到 WSNs 的数据传输特征，某些路径上的节点剩余能量低，不参与协作或是提前死亡，导致路径跳数的判断存在误差，使得误检率升高。因此，本文为降低这种情况带来的不利影响，将跳数超出阈值的路径标记为待测路径，对其进一步进行路径信任评价量的检测。

2.3　信任模型

信任是衡量节点可靠性的重要依据，本文通过建立信任模型，计算待测路径上中间节点的信任值，然后对该路径的合理性进行评判，从而检测网络中的虫洞攻击。节点信任值的计算方式如下。

2.3.1　直接信任

根据 WSNs 贝叶斯信任评估模型[17]（beta reputation system）对节点的直接信任值进行计算。假设在时间 T 内节点 i 与节点 j 一共完成了（$\alpha_{ij}+\beta_{ij}$）次通信任务，其中通信成功的次数为 α_{ij} 次，通信失败的次数为 β_{ij} 次。直接信任值的计算公式可表示为

$$D_{ij}(t)=\frac{\alpha_{ij}+1}{\alpha_{ij}+p_{\mathrm{acf}}\times\beta_{ij}+2}\times r_{\mathrm{wwf}} \tag{3}$$

式中：p_{acf}表示异常修正因子，用来削弱由于非入侵因素的存在导致节点交互失败次数增加的影响，r_{wwf}为节点的行为约束函数，主要对通信失败次数增加的节点实施相应处罚。二者表达式为：

$$p_{\mathrm{acf}}=\frac{\sum_{t=1}^{T}E_t}{\sum_{t=1}^{T}R_t} \tag{4}$$

$$r_{\mathrm{wwf}}=1-\frac{\alpha_{ij}}{\sum_{t=1}^{T}W_t} \tag{5}$$

式中：R_t表示在某一时段 T 内，网络中检测到的节点通信受影响的总次数，E_t表示网络通信异常时，节点由于网络攻击所引起异常行为的次数。W_t表示节点具有影响力的通信总次数，即节点成功转发数据包，且相同数据包只转发一次的通信次数。

2.3.2　间接信任

节点的间接信任可以看作是第三方推荐节点对待评价节点行为做出的评估。假设节点 i 和节点 j 拥有的共同邻居数为 L 个，满足模糊评判条件的节点数为 k'。由于信任具有传递性，则间接信任可由源节点 i 与推荐节点 k 的直接信任 D_{ik}和推荐节点 k 与目的节点 j 的直接信任 D_{kj}共同决定，那么节点 i,j 的间接信任可表示为

$$I_{ij}(t)=\left(1-\frac{N_{\mathrm{fail}}}{N_{\mathrm{tol}}}\right)\frac{\sum_{k=1}^{k'}B_{\mathrm{qte}}D_{ik}D_{kj}}{k'} \tag{6}$$

由于推荐节点并非都是可信的，因此对选中的推荐节点进行了相应限制。N_{fail}表示节点 i 和节点 k 的直接信任值 D_{ik}低于 0.3 的节点数目，N_{tol}表示被选中的推荐节点总数。B_{qte}表示模糊信任评判结果。

由于网络中节点存在个体化差异，且在负载动态变化时，可能会对节点间的信任造成一定影响。因此本文采用模糊综合评判模型[18]对推荐节点的各信任因素进行分析。考虑到虫洞攻击下的网络通信特性及节点自身物理属性，将推荐节点信任因素指标集定义为{邻居数目，处理延时，节点能量，包转发率}，记作 $X=\{X_1,X_2,X_3,X_4\}$，相应权重集合可表示为 $A=\{a_1,a_2,a_3,a_4\}$，$a_1+a_2+a_3+a_4=1$。由于各信任因素的性质不同，对评估过程的影响差异较大，因此本文采用层次分析法[19]（analytic hierarchy process，AHP）来建立各评价因素的信任模型，通过引用 AHP 的 1－9 标度法[19]计算得到信任因素的权重为：$a_1=0.787$，$a_2=0.172$，$a_3=0.034$，$a_4=0.007$。

定义评价集合 $V=\{V_1,V_2,V_3,V_4\}$，V_m表示评价等级，当 $m=1,2,3,4$ 时分别表示不可信、低可信、中可信和高可信。对 X 中每一因素根据评价集中的等级指标进行模糊评判，得到隶属度矩阵 $\boldsymbol{R}$ 为

$$\boldsymbol{R}=\begin{bmatrix}r_{11}&r_{12}&r_{13}&r_{14}\\r_{21}&r_{22}&r_{23}&r_{24}\\r_{31}&r_{32}&r_{33}&r_{34}\\r_{41}&r_{42}&r_{43}&r_{44}\end{bmatrix} \tag{7}$$

r_{nm}表示各信任因素指标对评价等级的隶属度。接下来将隶属度矩阵 $\boldsymbol{R}$ 与评价权重集合 A 做模糊合成运算，得到信任因素集 X 的评价结果为

$$\boldsymbol{Y}=A\cdot\boldsymbol{R}=\begin{bmatrix}a_1&a_2&a_3&a_4\end{bmatrix}\cdot\begin{bmatrix}r_{11}&r_{12}&r_{13}&r_{14}\\r_{21}&r_{22}&r_{23}&r_{24}\\r_{31}&r_{32}&r_{33}&r_{34}\\r_{41}&r_{42}&r_{43}&r_{44}\end{bmatrix}=\begin{bmatrix}y_1&y_2&y_3&y_4\end{bmatrix} \tag{8}$$

式中“·”为加权平均型模糊合成算子，这种算子的特点是可均衡评价因素间的差异，防止异常因素的干扰。综合程度高，效果显著。依据 $\boldsymbol{M}=(\cdot,\oplus)$ 算子的计算方式，y_m的计算公式为

$$y_m=\min\left(1,\sum_{n=1}^{4}a_n r_{nm}\right),\ m=1,2,3,4 \tag{9}$$

根据各影响因素的等级评价结果，当 $y_1/\sum_{m=1}^{4}y_m\geqslant 0.5$ 时，说明该节点评价等级过低，不被接受，在选定的推荐节点集中将该节点删去。否则，选取该节点作为推荐节点，B_{qte}的表达式如下：

$$B_{\mathrm{qte}}=\frac{y_2+y_3+y_4}{\sum_{m=1}^{4}y_m} \tag{10}$$

2.3.3　综合信任

节点当前的综合信任值可通过直接信任和间接信任加权获得，即

$$T_{ij}(t)=\varphi D_{ij}(t)+\mu I_{ij}(t) \tag{11}$$

式中:φ 代表直接信任的权重,μ 代表间接信任的权重,且 $\varphi+\mu=1$。由于此时对网络的情况不了解,直接信任和间接信任对综合信任的影响视为同等重要,二者权重被均等分配,即 $\varphi=\mu=0.5$。

2.4 路径信任评价量

在对待测路径进行信任评价量的检测时,考虑受攻击节点专有邻居集中的节点相距较远,实际转发跳数很高,因此对每条路径的信任评价量通过分组计算[20],每两跳为一组。将待测路径的总跳数表示为 H,分组方式如下

$$h=\begin{cases}\dfrac{H}{2}, & H\text{ 为偶数跳}\\ \mathrm{int}\left(\dfrac{H}{2}\right)+1, & H\text{ 为奇数跳}\end{cases} \tag{12}$$

式中:h 表示路径分组结果,当 H 为偶数跳时,路径组数为 $H/2$;为奇数跳时,路径组数为 $H/2$ 的整数部分加 1,最后一组的路径信任值按一跳计算。S^z_{tru} 应满足条件:1)信任区间为[0,1],且随着跳数的增加信任值逐渐减小;2)各组路径信任为中间节点综合信任的乘积;3)源节点为可信节点且初始信任度为 1,包括源节点在内的第一组路径信任无衰减,从第二组开始逐渐衰减。则该路径第 x 组信任值衰减系数 δ 的表达式为

$$\delta=\exp(-0.5(x-1)) \tag{13}$$

式中衰减系数 δ 的扩展矩阵 $\boldsymbol{\delta}_{\mathrm{del}}$ 可表示为

$$\boldsymbol{\delta}_{\mathrm{del}}=\begin{bmatrix}1\\ \mathrm{e}^{-0.5}\\ \mathrm{e}^{-0.5\times2}\\ \vdots\\ \mathrm{e}^{-0.5(x-1)}\\ \vdots\\ \mathrm{e}^{-0.5(h-1)}\end{bmatrix} \tag{14}$$

分组路径信任的矩阵表达式为

$$\boldsymbol{T}_{\mathrm{tru}}=\begin{bmatrix}T^{11}_{\mathrm{tru}} & T^{12}_{\mathrm{tru}} & T^{13}_{\mathrm{tru}} & \cdots & T^{1x}_{\mathrm{tru}} & \cdots & T^{1h}_{\mathrm{tru}}\\ T^{21}_{\mathrm{tru}} & T^{22}_{\mathrm{tru}} & T^{23}_{\mathrm{tru}} & \cdots & T^{2x}_{\mathrm{tru}} & \cdots & T^{2h}_{\mathrm{tru}}\\ T^{31}_{\mathrm{tru}} & T^{32}_{\mathrm{tru}} & T^{33}_{\mathrm{tru}} & \cdots & T^{3x}_{\mathrm{tru}} & \cdots & T^{3h}_{\mathrm{tru}}\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ T^{z1}_{\mathrm{tru}} & T^{z2}_{\mathrm{tru}} & T^{z3}_{\mathrm{tru}} & \cdots & T^{zx}_{\mathrm{tru}} & \cdots & T^{zh}_{\mathrm{tru}}\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ T^{h1}_{\mathrm{tru}} & T^{h2}_{\mathrm{tru}} & T^{h3}_{\mathrm{tru}} & \cdots & T^{hx}_{\mathrm{tru}} & \cdots & T^{hh}_{\mathrm{tru}}\end{bmatrix} \tag{15}$$

将衰减系数与分组路径信任合成得到每条路径的信任评价量 S^z_{tru},其展开式如式(16)所示,式中"。"为因素累乘型合成算子。

$$\begin{bmatrix}T^{11}_{\mathrm{tru}} & T^{12}_{\mathrm{tru}} & T^{13}_{\mathrm{tru}} & \cdots & T^{1x}_{\mathrm{tru}} & \cdots & T^{1h}_{\mathrm{tru}}\\ T^{21}_{\mathrm{tru}} & T^{22}_{\mathrm{tru}} & T^{23}_{\mathrm{tru}} & \cdots & T^{2x}_{\mathrm{tru}} & \cdots & T^{2h}_{\mathrm{tru}}\\ T^{31}_{\mathrm{tru}} & T^{32}_{\mathrm{tru}} & T^{33}_{\mathrm{tru}} & \cdots & T^{3x}_{\mathrm{tru}} & \cdots & T^{3h}_{\mathrm{tru}}\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ T^{z1}_{\mathrm{tru}} & T^{z2}_{\mathrm{tru}} & T^{z3}_{\mathrm{tru}} & \cdots & T^{zx}_{\mathrm{tru}} & \cdots & T^{zh}_{\mathrm{tru}}\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ T^{h1}_{\mathrm{tru}} & T^{h2}_{\mathrm{tru}} & T^{h3}_{\mathrm{tru}} & \cdots & T^{hx}_{\mathrm{tru}} & \cdots & T^{hh}_{\mathrm{tru}}\end{bmatrix}\circ\begin{bmatrix}1\\ \mathrm{e}^{-0.5}\\ \mathrm{e}^{-0.5\times2}\\ \vdots\\ \mathrm{e}^{-0.5(x-1)}\\ \vdots\\ \mathrm{e}^{-0.5(h-1)}\end{bmatrix}=\begin{bmatrix}S^1_{\mathrm{tru}}\\ S^2_{\mathrm{tru}}\\ S^3_{\mathrm{tru}}\\ \vdots\\ S^z_{\mathrm{tru}}\\ \vdots\\ S^h_{\mathrm{tru}}\end{bmatrix} \tag{16}$$

S^z_{tru} 的计算公式如式(17)所示

$$S^z_{\mathrm{tru}}=\prod_{x=1}^{h}T^{zx}_{\mathrm{tru}}\mathrm{e}^{(-0.5(x-1))} \tag{17}$$

设定信任阈值为 K,当 $S^z_{\mathrm{tru}}\leqslant K$ 时,说明节点 A、B 专有邻居节点间不满足实际的通信关系,二者受到虫洞攻击。此时 A、B 向除其专有邻居之外的所有节点广播休眠数据包,使包括虫洞节点在内的部分节点进入休眠状态,不参与网络通信。算法流程见图 4。

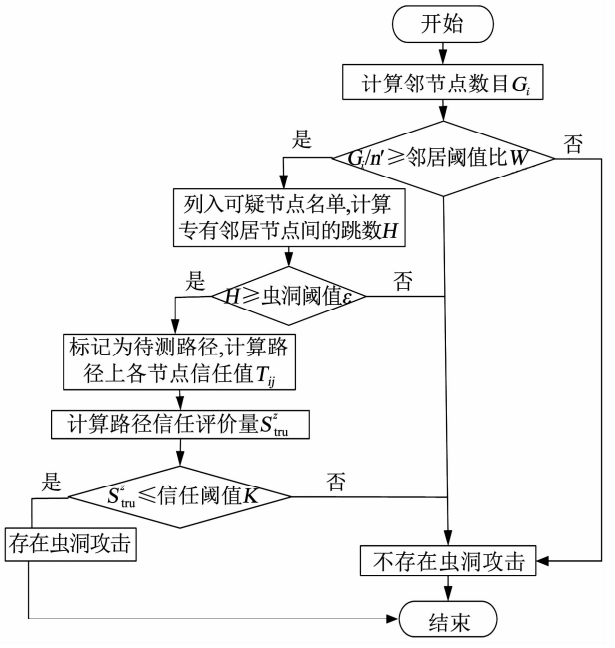

图 4 算法流程图

Fig. 4 Algorithm flow chart

3 仿真分析

假设无线传感器网络尺寸为 100 m × 100 m 的正方形区域,在其中部署 100 个静态传感器节点,各节点近似均匀分布,通信半径为 10 m,均可百分百响应通信请求。仿真参数见表 1。

3.1 WSNs 虫洞攻击模型

图 5 表示 WSNs 在虫洞攻击下的网络模型,虫洞节点集合分别为{98,97},{40,35,22},{80,82,

表 1　仿真参数

Tab. 1　Simulation parameters

节点总数/个	通信半径/m	初始能量/J	数据包大小/bit	数据分组发送间隔/s	虫洞节点数目/个
100	10	2	800	3	2 ~ 5

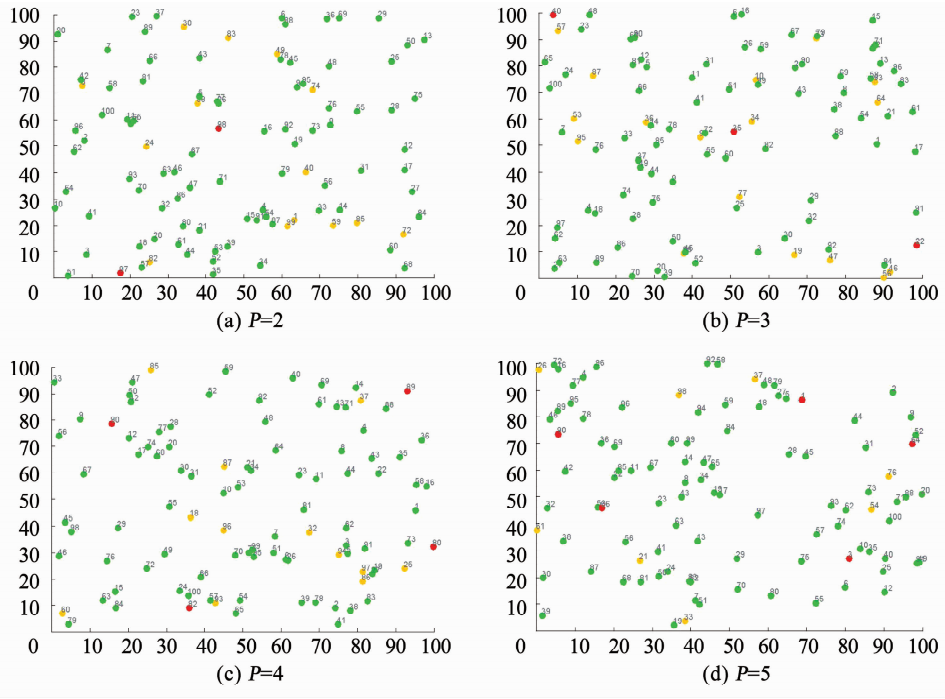

图 5　WSNs 虫洞攻击模型

Fig. 5　Wormhole attack model in WSNs

89,90},{90,1,64,66,3},这些虫洞节点信息不会出现在路由表中,在网络中处于一种“隐身状态”。针对以上网络分别进行仿真分析。P 表示虫洞节点数目。

3.2　邻居阈值比的选取

可疑节点覆盖率与邻居阈值比、虫洞节点数目三者的整体关系见图 6。从图中可以看出,随着邻居阈值比的增加,可疑节点覆盖率在逐渐减小,这是因为邻居阈值越大,WSNs 对处于虫洞攻击下节点的邻居数目要求就越高,满足条件的节点越来越少,存在受虫洞影响节点漏检的情况。只有当邻居阈值相对较小时,对网络中受攻击节点的检测才更加全面,可疑节点覆盖率更高。由于邻居阈值比在1.1 ~ 1.5 之间的检测率相差很小,考虑到网络能耗,本文邻居阈值比 W 取 1.5。

3.3　虫洞阈值的选取

在邻居阈值比为 1.5 的前提下对网络中的节点进行筛查,并进一步检测可疑节点的通信路径,得到在不同数目虫洞节点攻击下,虚假链路检测率和正常链路误检率随虫洞阈值 ε 的变化曲线。

从图 7 可以看出,随着虫洞阈值的增加,虚假链路检测率在逐渐减小。当阈值超过 6 时,检测率的下降幅度增大,这是因为虫洞阈值越高,WADS-NC&PH 越无法检测到路径相对较短的虫洞攻击。

图 8 为正常链路误检率随虫洞阈值 ε 的变化曲线。从图中可以看出,随着阈值的增加,误检率在逐渐降低,这是因为在未受攻击时正常邻居节点间的路径跳数都较短。因此,当阈值升高时,正常链路被误检的概率会越来越小。结合图 7 的仿真结果,在虫洞阈值超过 6 时,网络中虚假链路的检测率和正常链路的误检率变化幅度都较为明显。

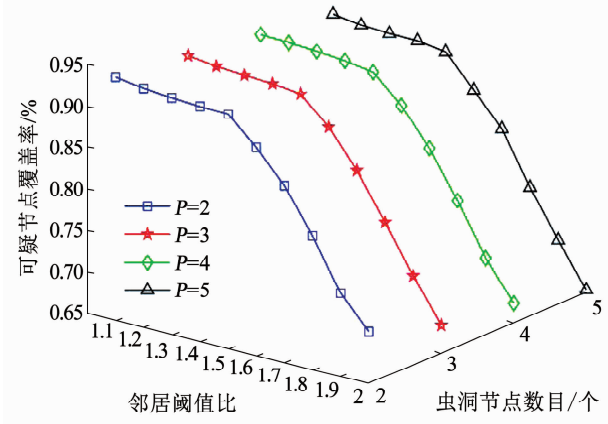

图 6　可疑节点覆盖率与邻居阈值比和虫洞节点数目的关系

Fig. 6　Relation between suspicious node coverage, neighbor threshold ratio, and number of wormhole nodes

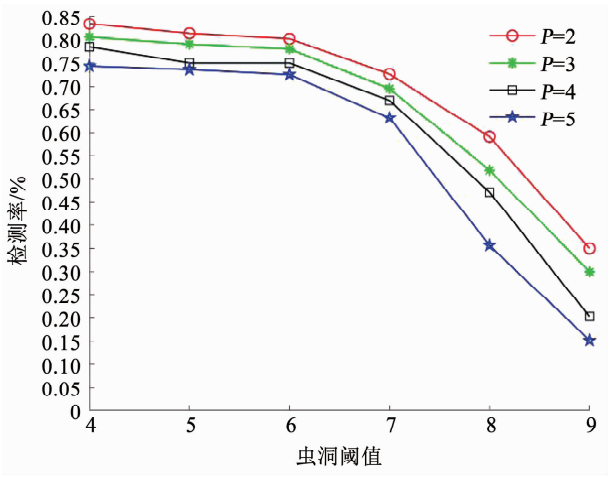

图 7 检测率与虫洞阈值的关系

Fig. 7 Relation between detection rate and wormhole threshold

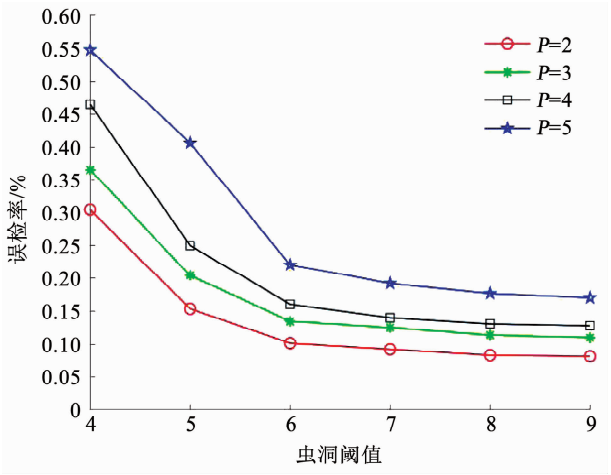

图 8 误检率与虫洞阈值的关系

Fig. 8 Relation between false detection rate and wormhole threshold

3.4 信任阈值的选取

对跳数高于虫洞阈值的路径进行路径信任评价量的检测,仿真结果见图 9。其中 P 表示虫洞节点数目,b 表示网络中的虚假链路总数。从图中可以看出,当信任阈值 K 由 0 至 0.02 变化时网络中虚假链路的数目在逐渐降低,后续随着信任阈值的增长,虚假链路的数目基本保持不变。

3.5 性能分析

为验证本文策略的有效性,将 WADS-NC&PH 与 SMRSA[8]、SECUND[9]、CREDND[10] 进行实验对比。WADS-NC&PH 的邻居阈值比设置为 1.5,虫洞阈值设置为 6,信任阈值设置为 0.02。

从图 10、11 中可以看出,随着虫洞节点个数的增加,3 种方案运行后网络中虚假链路数目及正常链路的误检率均有所升高,但 WADS-NC&PH 的检测效果优于其他几种算法。对 SMRSA 而言,由于该算法对网络节点的布置情况进行了较多的规范和

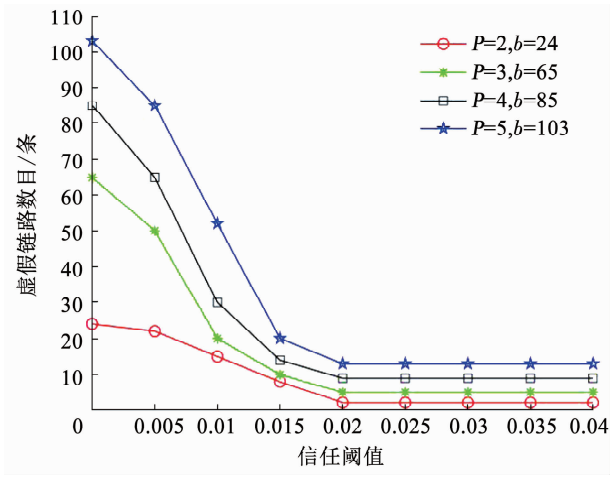

图 9 虚假链路数目与信任阈值的关系

Fig. 9 Relation between the number of false links and trust threshold

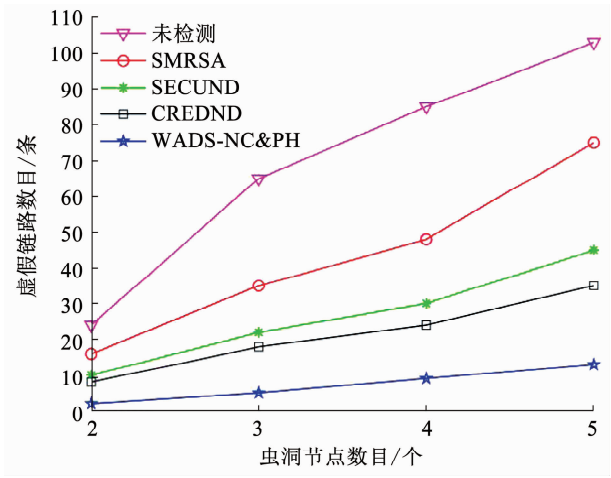

图 10 不同算法下网络中虚假链路数目比较

Fig. 10 Comparison of the number of false links in the network under different algorithms

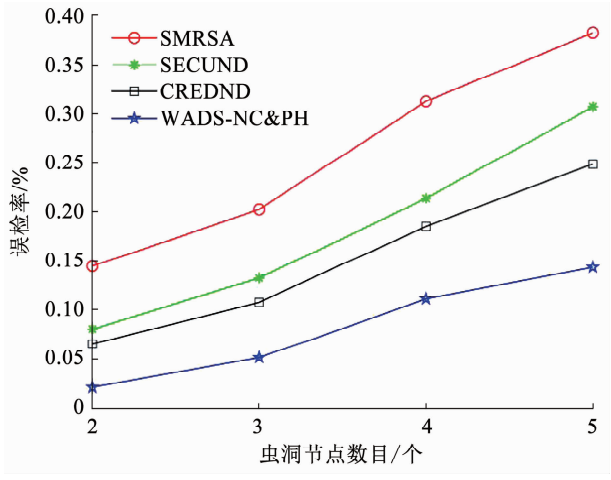

图 11 不同算法的误检率比较

Fig. 11 Comparison of false detection rates of different algorithms

限制在面对受攻击度较高的网络时,算法的适应能力较弱,检测效果有所下降。SECUND 算法和

CREDND 算法都利用了路径跳数进行检测，但 SECUND 算法对链接相对较短的虫洞攻击检测效果不佳。而 CREDND 算法在路径跳数的统计过程中未对虫洞路径进行避让，导致虚假链路的漏检，虫洞攻击检测率有所下降。WADS-NC&PH 在检验节点邻居数目的基础上，对待测节点的通信路径进行了限制，选择未受攻击节点作为中间节点，规避了虫洞链路，并利用路径信任评价量对可疑节点进行最终检验，因此在面对受攻击度较高的网络时，网络性能更加可靠。

为进一步验证本文算法的可扩展性，在 500 m × 500 m 的网络中随机布置 300 ~ 800 个传感器节点，各节点通信半径设置为 30 m，得到不同数目虫洞节点攻击下网络中虚假链路数与节点平均邻居数的关系曲线见图 12。从图中可以看出，面对不同节点密度的网络，本文策略对虫洞攻击仍具有较好的检测效果。

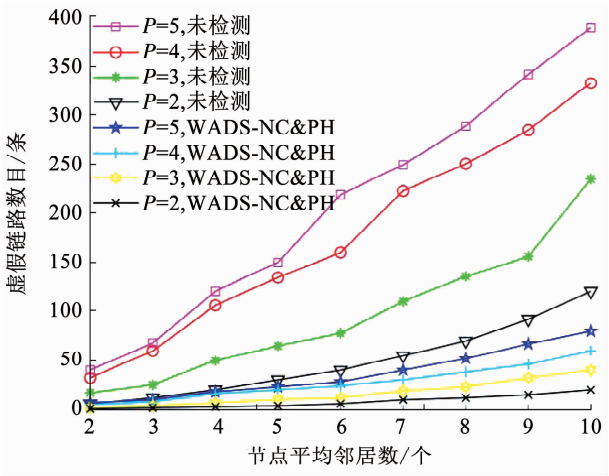

图 12　节点密度对检测效果的影响

Fig. 12　Influence of node density on detection effect

4　结　论

分析了无线传感器网络中虫洞攻击的研究现状，并为抵御攻击提出了一种融合节点信誉度和路径跳数的虫洞攻击检测策略。该策略首先对网络中的节点进行邻居数目的筛查，将超出阈值的节点列入可疑节点名单，然后令可疑节点的专有邻居集进行通信，记录每对通信节点间的路径跳数，将跳数超出阈值的路径标记为待测路径，并对该条路径进行路径信任评价量的检验。WADS-NC&PH 是一种本地化协议，无需任何特殊的硬件支持，且在检测过程中对虫洞路径进行了规避，通过与节点信任相结合，可提高虫洞攻击的检测效率，降低节点能耗。仿真结果表明，该策略对虫洞攻击的检测及虚假链路的移除具有明显效果，保障了无线传感器网络安全可靠运行。无线传感器网络在虫洞攻击检测方面还有很多问题有待研究和解决，下一阶段将重点研究依据网络节点实际分布的随机性及数据传输情况，自适应调节信任权重以提高算法鲁棒性。

参考文献

[1] 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): 92
WANG Shuopeng. Prediction and analysis of systemic network security model based on data mining[J]. Journal of Northeast Electric Power University, 2019, 39(6): 92. DOI: 10.19718/j.issn.1005-2992.2019-06-0091-03

[2] PADMANABHAN J, MANICKAVASAGAM V. Scalable and distributed detection analysis on wormhole links in wireless sensor networks for networked systems[J]. IEEE Access, 2018, 6: 1755. DOI: 10.1109/ACCESS.2017.2780188

[3] 滕志军, 许媛媛, 庞宝贺, 等. 合作博弈下无线传感器网络功率控制策略[J]. 哈尔滨工业大学学报, 2019, 51(11): 90
TENG Zhijun, XU Yuanyuan, PANG Baohe, et al. Power control strategy of wireless sensor network under cooperative game[J]. Journal of Harbin Institute of Technology, 2019, 51(11): 90. DOI: 10.11918/j.issn.0367-6234.201905173

[4] 叶波. 基于负载均衡度的云计算任务调度算法[J]. 东北电力大学学报, 2019, 39(1): 94
YE Bo. Task scheduling algorithm for cloud computing based on load balance degree[J]. Journal of Northeast Electric Power University, 2019, 39(1): 94. DOI: 10.19718/j.issn.1005-2992.2019-01-0088-08

[5] 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(7): 607. DOI: 10.1016/j.future.2019.02.004

[6] ELSHRKAWEY M, ELSHERIF S, 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): 261. DOI: 10.1016/j.jksuci.2017.04.002

[7] SAHOO 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): 231. DOI: 10.1007/s13369-017-3052-7

[8] 董晓梅, 杨洁. 一种无线传感器网络中的虫洞攻击检测算法[J]. 东北大学学报(自然科学版), 2012, 33(9): 1253
DONG Xiaomei, YANG Jie. A wormhole attack detection algorithm in wireless sensor networks[J]. Journal of Northeastern University (Natural Science Edition), 2012, 33(9): 1253

[9] HAYAJNEH T, KRISHNAMURTHY P, TIPPER D, et al. Secure neighborhood creation in wireless ad hoc networks using hop count discrepancies[J]. Mobile Networks & Applications, 2012, 17(3): 415. DOI: 10.1007/s11036-011-0334-2

[10] LUO Xiao, CHEN Yanru, LI Miao, et al. CREDND: a novel secure neighbor discovery algorithm for wormhole attack[J]. IEEE Access, 2019, 7: 18194. DOI: 10.1109/ACCESS.2019.2894637

[11] AMISH P, VAGHELA V B. Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol[J]. Procedia Computer Science, 2016, 79: 700. DOI: 10.1016/j.procs.2016.03.092

(下转第 131 页)