研究与开发

基于扩展传染病模型和马尔可夫链的物联网可用度评估方法

叶晓彤[1]，孙文飞[1,2]，沈士根[1]

（1. 绍兴文理学院计算机科学与工程系，浙江 绍兴 312000;
2. 浙江理工大学信息学院，浙江 杭州 310018）

摘　要：为反映恶意程序传播环境下物联网可用的状态，基于扩展的 SEIRD 传染病模型和马尔可夫链提出一种物联网可用度评估方法。根据物联网节点的实际状态，扩展经典传染病模型 SIR 建立 SEIRD 物联网节点状态转换模型。由物联网节点各个状态之间的动态变化过程，构建物联网节点处于 5 种状态的概率动力学方程，得到反映各状态转换的马尔可夫矩阵，进一步得到物联网节点的可用度计算方法。以典型的星形和簇形物联网拓扑结构为例，给出整个物联网可用度的评估方法。通过实验，为管理员如何合理部署正常工作节点数、路由数提供建议。研究成果对提高物联网可用度、促进物联网成功应用具有理论指导意义。

关键词：物联网；恶意程序；传染病模型；马尔可夫链；可用度

中图分类号：TP393

文献标识码：A

doi: 10.11959/j.issn.1000−0801.2021063

Availability evaluation method for extended epidemic model and Markov chain based IoT

YE Xiaotong[1], SUN Wenfei[1,2], SHEN Shigen[1]

1. Department of Computer Science and Engineering, Shaoxing University, Shaoxing 312000, China
2. School of Information Science and Technology, Zhejiang Sci-Tech University, Hangzhou 310018, China

Abstract: To reflect the availability status of the Internet of things (IoT) under malware diffusion, an availability evaluation method of IoT based on the extended epidemic model SEIRD and Markov chain was proposed. According to actual states of IoT nodes, the classic epidemic model SIR was extended to establish the node state transition model SEIRD. From the dynamic change process of each state of IoT nodes, the dynamic probability equations of IoT nodes belonging to five states were constructed, the Markov matrix reflecting the state transition was obtained, and an availability calculation method of an IoT node was achieved. Taking typical star and cluster IoT topologies as examples, the availability evaluation methods of the whole IoT with different topologies were given. Experiments provide suggestions for administrators how to reasonably deploy the number of normal working nodes and routes. The research results have theoretical significance for improving IoT availability and promoting the successful IoT applications.

Key words: IoT, malware, epidemic model, Markov chain, availability

---

收稿日期：2020−10−31；**修回日期**：2021−04−03

通信作者：沈士根，shigens@usx.edu.cn

基金项目：国家自然科学基金资助项目（No.61772018）

Foundation Item: The National Natural Science Foundation of China（No. 61772018）

1 引言

物联网与人们的生活息息相关，其安全问题是影响物联网应用的关键因素，而恶意程序传播[1-6]是影响物联网性能的诸多原因之一。当恶意程序感染物联网节点后，将通过物联网节点之间的通信传播到其他物联网节点，导致物联网节点数据丢失、通信阻断以及能量损耗等问题，甚至直接使整个物联网系统发生瘫痪。物联网可用度评估反映的是物联网在感知数据、数据通信、数据汇聚时该网络处于可用或可操作状态的概率，是反映物联网性能的重要指标之一。在恶意程序传播环境下，如何评估物联网可用度已成为物联网能否成功应用的关键问题。因此，面向恶意程序传播的物联网可用度评估得到了学术界和工业界的广泛重视。

当前，与网络可用度（availability）评估相关的有可靠度（reliability）、可信赖度（dependability）、可生存性（survivability）评估。邹青丙等[7]综述了无线多跳网络中的可靠度评估方法，并结合物联网展望可靠度评估发展趋势。何明等[8]较早研究了物联网可靠度评估问题，通过综合考虑感知层网络节点移动性和网络故障因素，给出了一种物联网中感知层网络可靠度评估方法。沈士根等[9]基于静态博弈预测恶意程序的传播行为，再将恶意程序传播的概率关联到马尔可夫链的随机性，实现了无线传感器网络的可生存性评估。沈士根等还使用“非合作非零和博弈”[10]和随机博弈[11]给出了无线传感器网络的可信赖度和可靠度评估方法，利用 SIRD 传染病模型和马尔可夫链[12]给出了面向恶意程序传播的异质无线传感器网络可用度评估方法。进一步地，金娟等[13]基于节点分布和脆弱性差异给出异质无线传感器网络节点异质模型，再进行节点可用度的分析。石琼等[14]利用连续时间马尔可夫链，考虑节点独立失效与相关失效，针对无线传感器网络可靠度、可用度及可生存性分别给出了评估方法。另外，基于连续时间马尔可夫链研究网络可生存性评估问题的文献还包括多种攻击并发下的无线传感器网络可生存性评估模型[15]、考虑节点移动的无线传感器网络可生存性评估模型[16]。Liu 等[17]提供了一种区域失效概率模型，以捕捉区域失效的关键特征，并将其应用于无线 Mesh 网络的可靠度评估。Huang 等[18]利用随机游走模型描述物联网节点间关系，提出了一种基于随机模型的物联网节点可信赖度评估方法。Yue 等[19] 针对工业无线传感器网络，给出了一种时间演化的 Monte Carlo（蒙特卡洛）可靠度评估方法。Ferraz 等[20]针对 IPv6 物联网，使用多元统计方法识别异常感知信息，给出了一种物联网可靠度评估模型。Huang 等[21]针对基于边缘计算的物联网环境，建立了表述物联网设备、边缘服务器和云服务器之间流量关系的网络模型，并给出了评估网络可靠度的算法。Andrade 等[22] 提出了一种基于 Petri 网的物联网基础设施灾难恢复建模与分析方法，实现了物联网基础设施的可用度评估。Xiang 等[23]考虑无线传感器网络的随机失效、能量消耗、环境随机性和干扰等方面，基于代数图论和 Monte Carlo 仿真提出了广义节点可靠度和平均广义节点可靠度评估指标，用于实现无线传感器网络的可靠度评估。

然而，在物联网恶意程序传播环境中，除参考文献[12-13]描述的易感状态（S）、感染状态（I）、免疫状态（R）、死亡状态（D）4 种状态外，还普遍存在潜伏状态（E）。该状态表示物联网节点被恶意程序感染后，隐藏自己并且不表现出传播恶意程序的行为。因此，本文为更好地反映物联网恶意程序传播环境下物联网节点的实际状态，建立 SEIRD 物联网节点状态转换模型。然后，构建物联网节点处于 5 种状态的概率动力学方程，得到各状态转换矩阵，进一步得到物联网节点可用度计算方法。最后，以典型的星形和簇形物联网拓扑结构为例，给出整个物联网可用度评估的方法。

2　恶意程序传播环境下的物联网节点状态转换模型

在物联网中，恶意程序通过被感染节点获取节点数据，并进行相邻节点的传播，这跟传染病的传播模式类似。因此，可以考虑基于传染病原理和马尔可夫链来描述物联网节点在恶意程序传播环境下的节点状态转换模型。

在物联网恶意程序传播过程中，易感状态（S）、潜伏状态（E）、感染状态（I）、免疫状态（R）、死亡状态（D）为物联网节点常见的 5 种状态，而这 5 种状态的节点存在相互转换关系，如图 1 所示。图 1 中，易感状态的节点指的是物联网系统内存在漏洞并有可能被感染的节点；潜伏状态的节点指的是该物联网节点已经被恶意程序感染但此时恶意程序未处于活动期，即此时该节点虽被感染但不会向外传播恶意程序；感染状态的节点指的是一个本来处于潜伏状态的物联网节点试图向其他节点传播恶意程序，此时处于潜伏状态的节点中的恶意程序被激活，从而由潜伏状态转换成感染状态；免疫状态的节点指的是处于易感状态、潜伏状态或感染状态的物联网节点通过安装系统安全补丁，从而达到类似于人体免疫力的效果，此时对已知的恶意程序可以起到抵抗的作用，从而保护节点不会被感染；死亡状态的节点指的是处于易感状态、潜伏状态、感染状态或免疫状态的物联网节点在恶意程序的代码攻击之下消耗殆尽节点内部的能量，从而导致该节点死亡的节点，也有可能是因为自身能量耗尽而死亡的节点。

3　恶意程序传播环境下的物联网节点状态转换动力学

对于任意一个物联网节点 i 而言，记其度为 k，即其周围有 k 个与之相邻且可以互相通信的节点。这 k 个与物联网节点 i 相邻的节点都有一定的可能

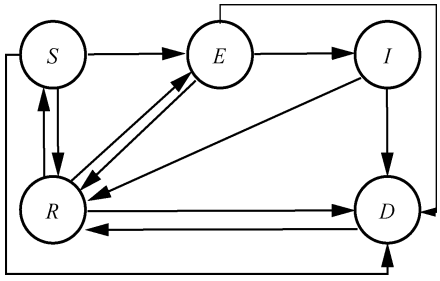

图 1　物联网节点 SEIRD 状态转换图

性对节点 i 进行攻击，从而使节点 i 由易感状态 S 转换到潜伏状态 E 再进一步由潜伏状态 E 转换到感染状态 I，所以，在 t 时刻节点 i 的状态与 $t-1$ 时刻该节点与其相邻节点的状态有密切关系。$P_i^S(t)$、$P_i^E(t)$、$P_i^I(t)$、$P_i^R(t)$、$P_i^D(t)$ 分别为节点 i 在 t 时刻处于易感状态、潜伏状态、感染状态、免疫状态和死亡状态的概率，$q_i^{xy}(t)$ 表示在 t 时刻节点由状态 x 转换到状态 y 的概率，其中，$x,y\in\{S,E,I,R,D\}$。显然，在一个刚建立的物联网中，各节点会被默认安装安全补丁对已知的恶意程序产生抵抗力，同时应对未来可能入侵的恶意程序，所以物联网内各节点的初始状态都处于免疫状态，即 $P_i^S(0)=P_i^E(0)=P_i^I(0)=P_i^D(0)=0, P_i^R(0)=1$。

部署于物联网中的入侵检测系统可以对节点进行安全检测和安装安全补丁，从而使节点获得抵抗恶意程序的免疫力。当入侵检测系统检测到节点存在安全漏洞时，可以为节点安装安全补丁，使该物联网节点从易感状态、潜伏状态或感染状态转换成免疫状态。记恶意程序感染节点的概率为 α，物联网入侵检测系统的检测率和误报率分别为 β 和 γ，一个节点由潜伏状态转换到感染状态的概率为 μ，被恶意程序杀死即进入死亡状态的概率为 ω，节点非恶意程序攻击下死亡的概率为 φ，单位时间内物联网管理员向物联网内部投放新的健康节点和清除死亡节点的概率均为 η，由于物联网节点存在漏洞导致其从免疫状态转换到易感状态的概率为 ζ，物联网节点 i 的相邻节点为 j。

对处于易感状态的物联网节点 i，在 t 时刻该节点和一个已经感染的节点通信时，其被恶意程序感染成功的概率可以表示为 $\alpha p_j^I(t-1)$，相应地，未被恶意程序感染的概率为 $1-\alpha p_j^I(t-1)$。进一步地，节点 i 可能与周围 k 个邻居节点通信。如果节点 i 的其中一个相邻节点处于感染状态，就有可能对节点 i 进行攻击，并且只要任意一个相邻节点对节点 i 攻击成功造成节点 i 的感染，都会使节点 i 的状态从易感状态变成潜伏状态。所以，节点 i 与 k 个相邻节点通信时不会被感染的概率为 $(1-\alpha p_j^I(t-1))^k$。此外，节点 i 有被物联网入侵检测系统安装安全补丁，使其以后面对已知恶意程序时存在不会再被攻击感染的可能性，也存在能量耗尽而变为死亡节点的可能性。因此，在 t 时刻处于易感状态的节点 i 的状态转换概率如式(1)所示。

$$\begin{cases} q_i^{SS}(t)=\left(1-\alpha p_j^I(t-1)\right)^k \\ q_i^{SE}(t)=1-\left(1-\alpha p_j^I(t-1)\right)^k-\beta-\varphi \\ q_i^{SI}(t)=0 \\ q_i^{SR}(t)=\beta \\ q_i^{SD}(t)=\varphi \end{cases} \tag{1}$$

当物联网节点 i 处于潜伏状态时，无法转换成易感状态，但是该节点内的恶意程序处于活动状态后将使该节点从潜伏状态转换为感染状态。当该节点经物联网入侵检测系统检测并安装安全补丁后，该节点将从潜伏状态变为免疫状态。当该节点因为物理原因死亡时，就会从潜伏状态转换为死亡状态。因此，在 t 时刻，处于潜伏状态的节点 i 的状态转换概率如式（2）所示。

$$\begin{cases} q_i^{ES}(t)=0 \\ q_i^{EE}(t)=1-\mu-\beta-\varphi \\ q_i^{EI}(t)=\mu \\ q_i^{ER}(t)=\beta \\ q_i^{ED}(t)=\varphi \end{cases} \tag{2}$$

对处于感染状态的物联网节点 i，当物联网入侵检测系统检测到恶意程序所攻击的安全漏洞时，通过安装安全补丁来弥补这个安全漏洞，从而使节点 i 由感染状态转换为免疫状态。也有可能在恶意程序的攻击下或者受物理原因影响，节点 i 由感染状态转换为死亡状态。另外，处于感染状态的节点不能转换为易感状态和潜伏状态。因此，在 t 时刻，处于感染状态的节点 i 的状态转换概率如式（3）所示。

$$\begin{cases} q_i^{IS}(t)=0 \\ q_i^{IE}(t)=0 \\ q_i^{II}(t)=1-\beta-\omega-\varphi \\ q_i^{IR}(t)=\beta \\ q_i^{ID}(t)=\omega+\varphi \end{cases} \tag{3}$$

对处于免疫状态的物联网节点 i，如果恶意程序发现了新的安全漏洞，则会使该节点又存在被攻击的可能性，使其从免疫状态转换成易感状态。而当物联网入侵检测系统误报时，会将物联网节点判断为潜伏状态。同时，节点 i 也存在非恶意程序攻击下死亡的可能。因此，在 t 时刻，处于免疫状态的节点 i 的状态转换概率如式(4)所示。

$$\begin{cases} q_i^{RS}(t)=\zeta \\ q_i^{RE}(t)=\gamma \\ q_i^{RI}(t)=0 \\ q_i^{RR}(t)=1-\varphi-\zeta-\gamma \\ q_i^{RD}(t)=\varphi \end{cases} \tag{4}$$

针对恶意程序传播和节点正常死亡导致物联网内部正常节点数量减少的问题，为了保障物联网的性能状态，一般采取向物联网内加入健康节点的办法。这种方法可以维持整个物联网中正常节点数量稳定。在实际操作中，加入健康节点的概率跟死亡节点的概率相同，并且，新加入节点的初始状态为免疫状态。因此，在 t 时刻，处于死亡状态的节点 i 的状态转换概率如式（5）所示。

$$\begin{cases} q_i^{DS}(t)=0 \\ q_i^{DE}(t)=0 \\ q_i^{DI}(t)=0 \\ q_i^{DR}(t)=\eta \\ q_i^{DD}(t)=1-\eta \end{cases} \tag{5}$$

结合图 1 可知，在 $t-1$ 时刻处于易感状态的物联网节点可以转换为潜伏状态、免疫状态或死亡状态；处于潜伏状态的节点可以转换为感染状态、免疫状态或死亡状态；处于感染状态的节点可以转换为免疫状态或死亡状态；处于免疫状态的节点可以转换为易感状态、潜伏状态或死亡状态；处于死亡状态的节点可以转换为免疫状态（实质是新加入的健康节点）。因此，物联网节点 i 在 t 时刻处于各个状态的概率如式（6）所示。

$$\begin{cases} p_i^S(t)=\left(q_i^{SS}(t)-q_i^{SE}(t)-q_i^{SR}(t)-q_i^{SD}(t)\right)p_i^S(t-1)+ \\ q_i^{RS}(t)p_i^R(t-1) \\ p_i^E(t)=\left(q_i^{EE}(t)-q_i^{EI}(t)-q_i^{ER}(t)-q_i^{ED}(t)\right)p_i^E(t-1)+ \\ q_i^{SE}(t)p_i^S(t-1) \\ p_i^I(t)=\left(q_i^{II}(t)-q_i^{IR}(t)-q_i^{ID}(t)\right)p_i^I(t-1)+ \\ q_i^{EI}(t)p_i^E(t-1) \\ p_i^R(t)=\left(q_i^{RR}(t)-q_i^{RS}(t)-q_i^{RE}(t)-q_i^{RD}(t)\right)p_i^R(t-1)+ \\ q_i^{SR}(t)p_i^S(t-1)+q_i^{ER}(t)p_i^E(t-1)+q_i^{IR}(t)p_i^I(t-1) \\ p_i^D(t)=\left(q_i^{DD}(t)-q_i^{DR}(t)\right)p_i^D(t-1)+q_i^{SD}(t)p_i^S(t-1)+ \\ q_i^{ED}(t)p_i^E(t-1)+q_i^{ID}(t)p_i^I(t-1)+q_i^{RD}(t)p_i^R(t-1) \end{cases} \tag{6}$$

将式（1）～式（5）代入式（6），化简可得物联网节点 i 在 t 时刻各个状态转换的动力学方程，如式（7）～式（11）所示。

$$\begin{cases} p_i^S(t)=\left(2\left(1-\alpha p_j^I(t-1)\right)^k-1\right)\cdot \\ p_i^S(t-1)+\zeta p_i^R(t-1) \\ p_i^S(0)=0 \end{cases} \tag{7}$$

$$\begin{cases} p_i^E(t)=(1-2\mu-2\beta-2\varphi)p_i^I(t-1)+ \\ \left(1-\left(1-\alpha p_j^I(t-1)\right)^k-\beta-\varphi\right)p_i^S(t-1) \\ p_i^I(0)=0 \end{cases} \tag{8}$$

$$\begin{cases} p_i^I(t)=(1-2\beta-2\omega-2\varphi)p_i^I(t-1)+\mu p_i^E(t-1) \\ p_i^I(0)=0 \end{cases} \tag{9}$$

$$\begin{cases} p_i^R(t)=(1-2\zeta-2\gamma-2\varphi)p_i^R(t-1)+\beta p_i^S(t-1)+ \\ \beta p_i^E(t-1)+\beta p_i^I(t-1) \\ p_i^R(0)=1 \end{cases} \tag{10}$$

$$\begin{cases} p_i^D(t)=(2\eta-1)p_i^D(t-1)+\varphi p_i^S(t-1)+ \\ \varphi p_i^E(t-1)+(\omega+\varphi)p_i^I(t-1)+\varphi p_i^R(t-1) \\ p_i^D(0)=0 \end{cases} \tag{11}$$

4　恶意程序传播环境下的物联网可用度

根据可靠性理论，一个物联网节点 i 在 t 时刻的可用度称为瞬时可用度，而当 t 趋于无穷时的可用度称为稳态可用度，该值能最终体现节点 i 和物联网的性能状况。记节点 i 在时刻 t 的瞬时可用度为 $\tau_i(t)$，稳态可用度为 $\tilde{\tau}_i(t)$，则该节点稳态可用度为：

$$\tilde{\tau}_i=\lim_{t\to\infty}\tau_i(t) \tag{12}$$

在实际计算物联网节点可用度时，通常经过计算表达物联网节点状态转换的马尔可夫矩阵的稳定点来得到具体值。记：

$$\tilde{\boldsymbol{p}}=\left[\tilde{p}_i^S,\tilde{p}_i^E,\tilde{p}_i^I,\tilde{p}_i^R,\tilde{p}_i^D\right] \tag{13}$$

为节点 i 的稳态可用度向量，其元素值可通过：

$$\tilde{p}_i\lim_{t\to\infty}\boldsymbol{M}_i(t)=\tilde{p}_i \tag{14}$$

进行求解，其中，在时刻 t 物联网节点 i 状态转换的马尔可夫矩阵 $\boldsymbol{M}_i(t)$ 由式（1）～式（5）得到：

$$\boldsymbol{M}_i(t)=\begin{bmatrix} \psi_1 & \psi_2 & 0 & \beta & \varphi \\ 0 & 1-\mu-\beta-\varphi & \mu & \beta & \varphi \\ 0 & 0 & 1-\beta-\omega-\varphi & \beta & \omega+\varphi \\ \zeta & \gamma & 0 & 1-\varphi-\zeta-\gamma & \varphi \\ 0 & 0 & 0 & \eta & 1-\eta \end{bmatrix} \tag{15}$$

$$\psi_1=\left(1-\alpha p_j^I(t-1)\right)^k \tag{16}$$

$$\psi_2=1-\left(1-\alpha p_j^I(t-1)\right)^k-\beta-\varphi \tag{17}$$

由式（14）进行矩阵乘法后的任意 4 个等式联合 $\tilde{p}_i^S+\tilde{p}_i^E+\tilde{p}_i^I+\tilde{p}_i^R+\tilde{p}_i^D=1$ 可得：

$$\begin{cases}\psi_3\tilde{p}_i^S+\zeta\tilde{p}_i^R=\tilde{p}_i^S\\ (1-\psi_3-\beta-\varphi)\tilde{p}_i^S+(1-\mu-\beta-\varphi)\tilde{p}_i^E+\gamma\tilde{p}_i^R=\tilde{p}_i^E\\ \mu\tilde{p}_i^E+(1-\beta-\omega-\varphi)\tilde{p}_i^I=\tilde{p}_i^I\\ \beta\left(\tilde{p}_i^S+\tilde{p}_i^E+\tilde{p}_i^I\right)+(1-\varphi-\zeta-\gamma)\tilde{p}_i^R+\eta\tilde{p}_i^D=\tilde{p}_i^R\\ \tilde{p}_i^S+\tilde{p}_i^E+\tilde{p}_i^I+\tilde{p}_i^R+\tilde{p}_i^D=1\end{cases} \tag{18}$$

式（18）中：

$$\psi_3=\lim_{t\to\infty}\left(1-\alpha p_j^I(t-1)\right)^k \tag{19}$$

求解式（18）可得：

$$\tilde{p}_i^S=\frac{\zeta}{1-\psi_3}\tilde{p}_i^R \tag{20}$$

$$\tilde{p}_i^E=\frac{(1-\psi_3-\beta-\varphi)\zeta+(1-\psi_3)\gamma}{(\mu+\beta+\varphi)(1-\psi_3)}\tilde{p}_i^R \tag{21}$$

$$\tilde{p}_i^I=\frac{\mu\left((1-\psi_3-\beta-\varphi)\zeta+(1-\psi_3)\gamma\right)}{(\beta+\omega+\varphi)(\mu+\beta+\varphi)(1-\psi_3)}\tilde{p}_i^R \tag{22}$$

$$\begin{cases}\tilde{p}_i^R=\eta/\Lambda\\ \Lambda=\varphi+\zeta+\gamma+\eta+(\eta-\beta)\left(\dfrac{\zeta}{1-\psi_3}+\right.\\ \left.\dfrac{(1-\psi_3-\beta-\varphi)\zeta+(1-\psi_3)\gamma}{(\mu+\beta+\varphi)(1-\psi_3)}+\right.\\ \left.\dfrac{\mu\left((1-\psi_3-\beta-\varphi)\zeta+(1-\psi_3)\gamma\right)}{(\beta+\omega+\varphi)(\mu+\beta+\varphi)(1-\psi_3)}\right)\end{cases} \tag{23}$$

$$\tilde{p}_i^D=1-\tilde{p}_i^S-\tilde{p}_i^E-\tilde{p}_i^I-\tilde{p}_i^R \tag{24}$$

最终，一个物联网节点 i 的稳态可用度为：

$$\tilde{\tau}_i=1-\tilde{p}_i^E-\tilde{p}_i^I-\tilde{p}_i^D \tag{25}$$

5 典型物联网拓扑结构下的物联网可用度评估

5.1 星形物联网拓扑结构

星形物联网拓扑结构以物联网网关节点为中心，所有物联网节点都与网关节点相连。当连接网关节点的物联网节点需要发送数据时都要通过网关节点，再由网关节点统一向上一级基站发送数据。因此，星形物联网拓扑结构中网关节点是网络成功运行的关键，容错率较低，所有物联网节点单独与网关节点进行通信。

在星形物联网拓扑结构下，要使物联网可以正常工作，除网关节点必须正常运行外，还需要正常工作的物联网节点。记整个星形物联网中节点数为 Y，能正常工作的节点数为 g，保证星形物联网正常工作的最小节点数为 X，则当 $g\in[X,Y]$ 时，该星形物联网可以正常运行。因此，整个星形物联网的可用度 τ_{star} 为：

$$\tau_{\text{star}}=\sum_{g=X}^{Y}\left(C_Y^g\prod_{i=1}^{g}\tilde{\tau}_i\prod_{i=g+1}^{Y}(1-\tilde{\tau}_i)\right) \tag{26}$$

其中，C_Y^g 表示组合数。

5.2 簇形物联网拓扑结构

簇形物联网拓扑结构较星形物联网增加了簇头节点，每个簇头节点与同一个簇中的物联网节点相连并且直接跟网关节点相连。当簇头节点出现故障时，通过簇头选举算法将选择同一个簇内其他物联网节点作为新的簇头。因此，每一个簇内的物联网节点与对应的簇头进行通信，属于并行系统，簇头节点跟网关节点的通信路由属于串行系统，所有的通信路由进一步组成了并行系统。

记一个簇中的物联网节点数为 Y_B，整个簇的可用度 $\tilde{\tau}_{cl}$ 可以表示为：

$$\tilde{\tau}_{cl}=1-\prod_{i=1}^{Y_B}(1-\tilde{\tau}_i) \tag{27}$$

把一个簇看作一个整体，记对应的簇头可用度为 $\tilde{\tau}_{cl,w}$，则由簇和簇头组成的一条通信路由的可用度 $\tilde{\tau}_w$ 为：

$$\tilde{\tau}_w=\tilde{\tau}_{cl}\tilde{\tau}_{cl,w} \tag{28}$$

记 W 为整个簇形物联网中所有路由的条数，则整个簇形物联网可用度 $\tilde{\tau}_{\text{Cluster}}$ 为：

$$\tilde{\tau}_{\text{Cluster}} = 1 - \prod_{w=1}^{W} (1 - \tilde{\tau}_w) \tag{29}$$

6　实验仿真与结果分析

6.1　物联网入侵检测系统检测率和误报率对物联网节点可用度的影响

物联网入侵检测系统的检测率 β 和误报率 γ 的变化会影响物联网节点可用度，为了分析其影响程度，根据物联网入侵检测系统的实际检测率和误报率变化情况，实验设置检测率 β 变化的范围为 80%～98%，误报率 γ 变化的范围为 2%～20%。实验结果如图 2 所示。

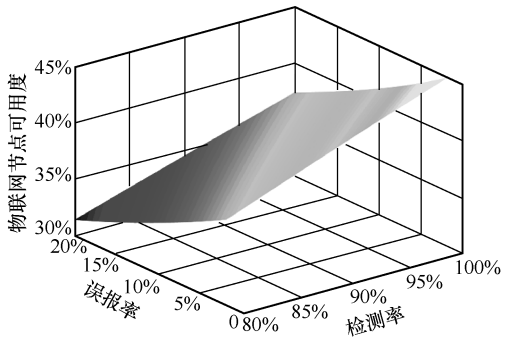

图 2　物联网入侵检测系统检测率和误报率变化下的物联网节点可用度

从图 2 可以看出，在误报率相同的情况下，物联网节点可用度随着检测率的增大而增大。例如，当误报率 $\gamma = 10\%$ 时，随着检测率从 80% 提高到 98%，物联网节点可用度从约 34.56% 提升到约 41.18%。而在检测率相同的情况下，物联网节点可用度随着误报率的减小而增大。例如，当检测率 $\beta = 90\%$ 时，随着误报率从 20% 降低到 2%，物联网节点可用度从约 34.44% 提升到约 41.28%。实验结果反映了在实际物联网应用中，为了提高物联网节点可用度，应尽量提高物联网入侵检测系统的检测率并且降低其误报率。

6.2　星形物联网可用度实验分析

由式（26）可知，星形物联网可用度主要与总的节点数和正常工作的节点数密切相关，因此，实验在设定物联网入侵检测系统检测率和误报率不变的情况下，分析物联网总节点数和正常工作节点数变化对整个星形物联网可用度的影响。实验结果如图 3 所示。

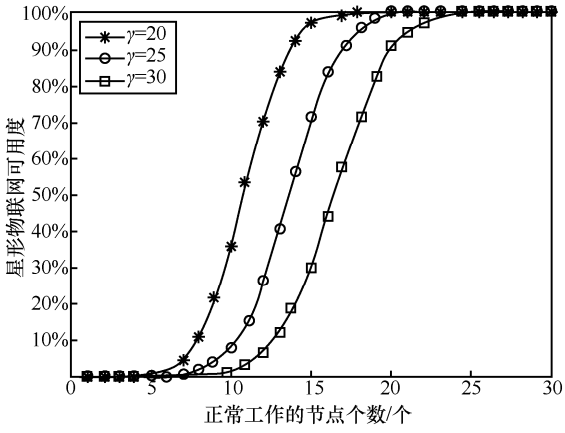

图 3　物联网总节点数和正常工作节点数变化下的星形物联网可用度

从图 3 可以看出，在物联网总节点数不变的情况下，增加正常工作节点数能显著提升星形物联网可用度。例如，当物联网总节点数 $Y = 25$ 时，若正常工作节点数小于 10，星形物联网可用度低于 10%，基本处于不可用状态；若正常工作节点数从 10 逐步增加到 20，星形物联网可用度从约 10%快速增加到约 100%。而在物联网正常工作节点数不变的情况下，增加物联网总节点数将降低整个星形物联网的可用度。例如，当物联网正常工作节点数 $g = 15$ 时，若物联网总节点数 Y 分别为 20、25、30，则整个星形物联网的可用度分别约为 97.40%、71.39%、30.19%。实验结果反映了在星形物联网中，保证合理的正常工作节点数是提高星形物联网可用度的关键，同时反映了提出的星形物联网可用度评估方法能给出合理的正常工作节点数建议，从而为提高星形物联网可用度提供理论指导。

6.3　簇形物联网可用度实验分析

由式（29）可知，簇形物联网可用度主要与路由数和簇中物联网节点数密切相关，因此，实

验在设定物联网入侵检测系统检测率和误报率不变的情况下，分析路由数和簇中物联网节点数变化对整个簇形物联网可用度的影响。实验结果如图 4 所示。

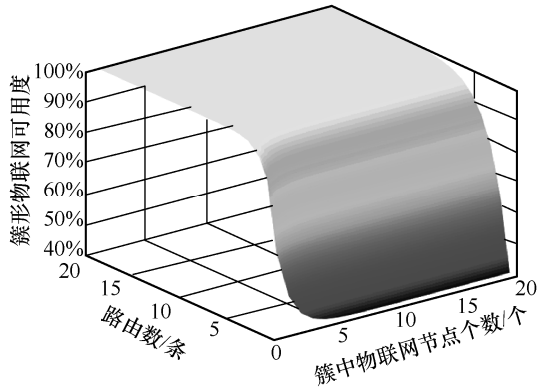

图 4　路由数和簇中物联网节点数变化下的簇形物联网可用度

从图 4 可以看出，在簇形物联网中，改变簇中物联网节点个数对整个簇形物联网可用度影响有限，而改变物联网中路由数对整个簇形物联网可用度影响巨大。例如，当簇中物联网节点个数 $Y_B=10$ 时，若物联网中路由数从 1 增加到 5，则簇形物联网可用度从约 40.02% 增加到约 92.23%；若物联网中路由数继续从 5 增加到 10，则簇形物联网可用度从约 92.23% 增加到100%。实验结果反映了在簇形物联网中，保证合理的路由数是提高簇形物联网可用度的关键，同时反映了提出的簇形物联网可用度评估方法能给出合理的路由数建议，从而为提高簇形物联网可用度提供理论指导。

7　结束语

本文通过扩展传统的传染病模型，基于能表达物联网节点状态转换的马尔可夫链，提出了一种恶意程序传播环境下的物联网可用度评估方法。经过扩展后得到的 SEIRD 物联网节点状态转换模型，能确切地反映恶意程序传播环境下的物联网节点状态。分析得到的物联网节点处于各个状态的概率动力学方程反映了物联网节点各个状态之间的动态变化过程，进一步得到的马尔可夫矩阵为计算物联网节点可用度奠定了基础。最终得到的星形和簇形物联网可用度评估方法能为管理员合理部署正常工作节点数、路由数提供建议，从而提高星形和簇形物联网的可用度，对促进物联网的成功应用具有理论指导意义。

参考文献：

[1] SHEN S, HUANG L, ZHOU H, et al. Multistage signaling game-based optimal detection strategies for suppressing malware diffusion in fog-cloud-based IoT networks[J]. IEEE Internet of Things Journal, 2018, 5(2): 1043-1054.

[2] SHEN S, ZHOU H, FENG S, et al. HSIRD: a model for characterizing dynamics of malware diffusion in heterogeneous WSN[J]. Journal of Network and Computer Applications, 2019(146): 14.

[3] ZHOU H, SHEN S, LIU J. Malware propagation model in wireless sensor networks under attack-defense confrontation[J]. Computer Communications, 2020(162): 51-58.

[4] 张红, 沈士根, 吴小军, 等. 基于元胞自动机和静态贝叶斯博弈的 WSN 恶意程序传染模型[J]. 电信科学, 2019, 35(6): 60-69.
ZHANG H, SHEN S G, WU X J, et al. WSN malware infection model based on cellular automaton and static Bayesian game[J]. Telecommunications Science, 2019, 35(6): 60-69.

[5] 周海平, 沈士根, 黄龙军, 等. 基于博弈论的无线传感器网络恶意程序传播模型[J]. 电信科学, 2018, 34(11): 67-76.
ZHOU H P, SHEN S G, HUANG L J, et al. Game theory-based malware propagation model for wireless sensor network[J]. Telecommunications Science, 2018, 34(11): 67-76.

[6] 沈士根, 冯晟, 周海平, 等. 基于云计算和动态贝叶斯博弈的 WSN 恶意程序传播优化抑制方法[J]. 电信科学, 2018, 34(9): 78-86.
SHEN S G, FENG S, ZHOU H P, et al. Optimal approach of suppressing WSN malware propagation based on cloud computing and dynamic Bayesian game[J]. Telecommunications Science, 2018, 34(9): 78-86.

[7] 邹青丙, 何明, 王琰, 等. 无线多跳网络可靠性评估方法研究[J]. 计算机工程与应用, 2015, 51(5): 88-91, 192.
ZOU Q B, HE M, WANG Y, et al. Survey on reliability evaluating method of wireless multi-hop networks[J]. Computer Engineering and Applications, 2015, 51(5): 88-91, 192.

[8] 何明, 陈国华, 赖海光, 等. 物联网感知层移动自组织网可靠性评估方法[J]. 计算机科学, 2012, 39(6): 104-106, 137.
HE M, CHEN G H, LAI H G, et al. Methods for evaluating reliability of mobile Ad hoc networks in the perception layer of IoT[J]. Computer Science, 2012, 39(6): 104-106, 137.

[9] 沈士根, 黄龙军, 范恩, 等. 受恶意程序传染的 WSNs 可生存性评估[J]. 传感技术学报, 2016, 29(7): 1083-1089.
SHEN S G, HUANG L J, FAN E, et al. Survivability evaluation for WSNs under malware infection[J]. Chinese Journal of Sensors and Actuators, 2016, 29(7): 1083-1089.

[10] SHEN S G, MA H, FAN E, et al. A non-cooperative non-zero-sum game-based dependability assessment of heterogeneous WSNs with malware diffusion[J]. Journal of Network and Computer Applications, 2017, 91: 26-35.

[11] 沈士根, 范恩, 胡珂立, 等. 面向恶意程序传播的传感器网络可靠度评估[J]. 电子学报, 2018, 46(1): 75-81.
SHEN S G, FAN E, HU K L, et al. Reliability evaluation for WSNs with malware spread[J]. Acta Electronica Sinica, 2018, 46(1): 75-81.

[12] 沈士根, 黄龙军, 周海平, 等. 面向恶意程序传播的异质 WSN 稳态可用度评估[J]. 传感技术学报, 2017, 30(7): 1100-1105.
SHEN S G, HUANG L J, ZHOU H P, et al. Steady-state availability evaluation for heterogeneous WSN under malware infection[J]. Chinese Journal of Sensors and Actuators, 2017, 30(7): 1100-1105.

[13] 金娟, 曹奇英, 沈士根, 等. 受恶意程序攻击的异质传感器网络节点可用度分析[J]. 计算机应用与软件, 2018, 35(9): 167-172.
JIN J, CAO Q Y, SHEN S G, et al. Nodes availability analysis of heterogeneous WSN attacked by malware[J]. Computer Applications and Software, 2018, 35(9): 167-172.

[14] 石琼, 丁英华, 秦丽, 等. 无线传感器网络可生存性评估研究[J]. 中北大学学报(自然科学版), 2020, 41(5): 418-430.
SHI Q, DING Y H, QIN L, et al. Survivability assessment for wireless sensor networks[J]. Journal of North University of China (Natural Science Edition), 2020, 41(5): 418-430.

[15] 刘志锋, 陈凯, 李雷, 等. 一种多种攻击并发下的 WSN 生存性评估模型[J]. 计算机科学, 2017, 44(8): 129-133.
LIU Z F, CHEN K, LI L, et al. Survivability evaluation model for wireless sensor network under multiple attacks[J]. Computer Science, 2017, 44(8): 129-133.

[16] 李化邓, 李雷, 施化吉, 等. 无线传感器网络的生存性评估[J]. 计算机应用研究, 2018, 35(8): 2450-2453.
LI H D, LI L, SHI H J, et al. Survivability evaluation in wireless sensor network[J]. Application Research of Computers, 2018, 35(8): 2450-2453.

[17] LIU J, JIANG X, NISHIYAMA H, et al. Reliability assessment for wireless mesh networks under probabilistic region failure model[J]. IEEE Transactions on Vehicular Technology, 2011, 60(5): 2253-2264.

[18] HUANG J, CHEN G, CHENG B. A stochastic approach of dependency evaluation for IoT devices[J]. Chinese Journal of Electronics, 2016, 25(2): 209-214.

[19] YUE Y, LI J, FAN H, et al. An efficient reliability evaluation method for industrial wireless sensor networks[J]. Journal of Southeast University (English Edition), 2016, 32(2): 195-200.

[20] FERRAZ JUNIOR N, SILVA A, GUELFI A, et al. IoT6Sec: reliability model for Internet of Things security focused on anomalous measurements identification with energy analysis[J]. Wireless Networks, 2019, 25(4): 1533-1556.

[21] HUANG C, HUANG D, LIN Y. Network reliability evaluation for a distributed network with edge computing[J]. Computers and Industrial Engineering, 2020(147): 106492.

[22] ANDRADE E, NOGUEIRA B. Dependability evaluation of a disaster recovery solution for IoT infrastructures[J]. Journal of Supercomputing, 2020, 76(3): 1828-1849.

[23] XIANG S, YANG J. Reliability evaluation and reliability-based optimal design for wireless sensor networks[J]. IEEE Systems Journal, 2020, 14(2): 1752-1763.

[作者简介]

叶晓彤（1978− ），男，绍兴文理学院计算机科学与工程系讲师，主要研究方向为无线传感器网络、物联网、网络空间安全、博弈论。

孙文飞（1999− ），男，浙江理工大学信息学院硕士生，主要研究方向为物联网、网络空间安全。

沈士根（1974− ），男，博士，绍兴文理学院计算机科学与工程系教授，主要研究方向为无线传感器网络、物联网、网络空间安全、博弈论。