基于半马尔可夫过程的异质 WSNs 可用度评估

杨淑敏[1] 吴国文[1] 张 红[1] 沈士根[2] 曹奇英[1*]

[1](东华大学计算机科学与技术学院 上海 201620)

[2](绍兴文理学院计算机科学与工程系 浙江 绍兴 312000)

摘 要 为评估异质无线传感器网络(HWSNs)的可用性,提出一种异质传感器节点状态更契合实际情况的 SEQIRD(Susceptible Exposed Quarantined Infected Recovered Dead)新模型。使用半马尔可夫过程描述节点各状态之间的动态转换过程,得到各个状态的稳态概率,并计算得出不同拓扑结构下整个 HWSNs 稳态可用度。最后进行数值分析,以验证初始感染率、感染变化率和恢复率对 HWSNs 稳态可用度的影响。

关键词 无线传感器网络 半马尔可夫过程 异质 可用度

中图分类号 TP311.52 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2024.03.019

AVAILABILITY MEASUREMENT FOR HETEROGENEOUS WSNS BASED ON SEMI-MARKOV PROCESS

Yang Shumin[1] Wu Guowen[1] Zhang Hong[1] Shen Shigen[2] Cao Qiying[1*]

[1](*College of Computer Science and Technology, Donghua University, Shanghai 201620, China*)

[2](*Department of Computer Science and Engineering, Shaoxing University, Shaoxing 312000, Zhejiang, China*)

Abstract In order to measure the availability of heterogeneous wireless sensor networks (HWSNs), a new Susceptible Exposed Quarantined Infected Recovered Dead (SEQIRD) model with heterogeneous sensor node states is proposed, which is more suitable for the actual situation. The semi-Markov process was utilized to depict states of the node's dynamic transition process, and the steady-state probability of each state was obtained. The entire HWSNs steady-state availability under different topologies could be computed. Numerical analyses were performed to verify the influence of the initial infection rate, infection change rate and recovery rate on the steady-state availability of HWSNs.

Keywords Wireless sensor networks Semi-Markov process Heterogeneous Availability

0 引 言

无线传感器网络(Wireless Sensor Networks,WSNs)备受军事[1]、医疗[2]、环境[3]等领域研究人员的关注。传感器网络的连通性、节能性[4-5]和网络的覆盖率[6]等几大方面依旧是目前 WSNs 的研究热点。由于在实际的应用场景中,传感器节点拥有不同的采集数据能力和安全等级,还可能因为被架设在不同的拓扑结构中而具有不同的链路通信能力和数据转发能力,因此异质无线传感器网络(Heterogeneous WSNs,HWSNs)更能满足广泛的异质世界对多元网络模型的要求。

节点在采集、传输、处理数据时根据一定的条件能够达到稳定状态且提供正常服务的概率表示了 HWSNs 节点稳态可用度,是评估 HWSNs 节点性能的重要指标之一。

在 HWSNs 中,恶意程序攻击节点使其感染病毒并在网络中传播病毒的方式和传染病在人群中传播的方式类似,所以在构建恶意程序传播模型[7-10]时通常借鉴传染病模型[11-13]。

国内外学者提出的物联网体系结构评估模型以及方法的综述为 HWSNs 可生存性、可用性、可靠性和稳定

收稿日期:2021-01-11。国家自然科学基金项目(61772018)。**杨淑敏**,硕士生,主研领域:无线传感器网络。**吴国文**,副教授。**张红**,博士生。**沈士根**,教授。**曹奇英**,教授。

性等性能评估提供了很好的借鉴作用。赵金皓等[14]通过构建 SEIRD(Susceptible Exposed Infected Recov ered Dead)模型,提出了一种关于节点状态的时空动力学方法。Shen 等[15-16]通过传感器节点的通信连通性体现节点异质性,提出了恶意软件在异质传感网中的传播模型。沈士根等[17]通过扩展传统 SIR(Susceptible In fected Recovered)传染病模型,得到了 HSI-ORD(Heterogeneous Susceptible Infected-is-Olated Removed Deceased)模型,以异质传感节点与其通信的节点数反映其异质性特征,并计算出该模型的稳定点。Lalropuia 等[18]通过贝叶斯博弈模型对 5G 无线通信网进行了可用性分析。沈士根等[19]通过引入随机博弈并利用马尔可夫链对 WSNs 进行了可靠性评估。苏玉泽等[20]引入半马尔可夫理论,给出了网络状态转移概率矩阵并进行了可生存性评估。Chen 等[21]提出了一种新的基于半马尔可夫过程的无线传感网生存性评估方法。Shakya 等[22]在对 WSNs 进行稳定性分析的时候考虑了空间相关性并引入了强相关节点和弱相关节点的概念。

本文提出一种基于半马尔可夫过程的 HWSNs 可用度评估方法,并考虑了攻击相关性对节点脆弱性的影响。首先,通过增加潜伏状态和隔离状态构建 SEQIRD(Susceptible Exposed Quarantined Infected Recovered-Dead)模型。其次,根据协作入侵理论[23,24]可知,异质传感器节点在受到多个感染了恶意程序的节点攻击的时候,节点的感染概率会随着攻击的次数改变,造成节点的脆弱性发生变化,由此定义了感染率函数。然后,在考虑半马尔可夫过程的基础上,建立异质传感器节点各个状态间的状态转移概率矩阵,得到传感器节点各个状态的稳态分布。最后,计算得到单个异质传感器节点的稳态可用度,考虑不同拓扑结构的影响,分别得到星型、簇型和 Mesh 型 HWSNs 稳态可用度。

1　异质传感器节点 SEQIRD 状态转换模型

HWSNs 中的异质传感器节点在被恶意程序攻击而感染前后状态会发生一系列变化。本文提出了一种包含 S、E、Q、I、R、D 六种状态的新模型。当异质传感器节点因为安全等级较低而存在漏洞,具备被感染风险的时候所处的状态称为易感状态 S;处于易感状态的传感器节点被恶意程序感染,但是恶意程序还没有被激活的状态称为潜伏状态 E;当传感器节点存在休眠期恶意程序被安全系统发现而隔离提供时间来恢复时属于隔离状态 Q;被恶意程序感染的异质传感器节点在与其他节点通信的过程中传播恶意程序将达到感染状态 I;当传感器节点中的恶意程序被安全查杀系统消除,以后不会再受该恶意程序攻击时就变为恢复状态 R;异质传感器节点会因为环境影响和能量消耗等因素而不能提供正常服务时所处的状态为死亡状态 D。图 1 建模了 HWSNs 中的异质传感器节点在受到恶意程序攻击后状态动态转换过程。

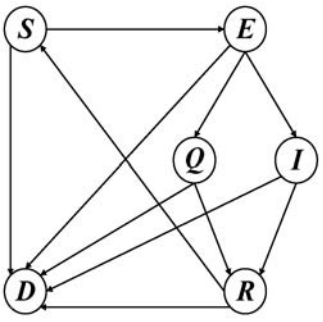

图 1　异质传感节点 SEQIRD 状态转换模型

假设在 HWSNs 通信范围内均匀部署异质传感器节点。那么:

$$N_i \approx \mathrm{int}(\rho \pi r_i^2) \tag{1}$$

式中:int 函数表示取整函数;ρ 表示部署节点的密度;π 表示圆周率;r_i 表示异质传感器节点 i 与其他节点通信的半径;N_i 表示与异质传感器节点 i 直接通信的节点数量。

在 t 时刻,异质传感器节点 i 处于状态 $x(x \in \{S, E, Q, I, R, D\})$ 的概率记为 $p_i^x(t)$,从状态 x 转换到状态 $y(y \in \{S, E, Q, I, R, D\})$ 的概率记为 $q_i^{xy}(t)$。由于 HWSNs 中异质传感器节点都处于初始状态 R,所以 $p_i^{\mathrm{R}}(0) = 1$,而 $p_i^{\mathrm{S}}(0) = p_i^{\mathrm{E}}(0) = p_i^{\mathrm{Q}}(0) = p_i^{\mathrm{I}}(0) = p_i^{\mathrm{D}}(0) = 0$。

S 状态的异质传感器节点由于自身安全等级较低,其通信范围内处于感染状态的节点成功传播恶意程序,导致其被恶意程序感染,由于刚刚受到感染,恶意程序还没达到活跃期,因此该异质传感器节点由 S 状态转换为 E 状态的转换概率可表示为:

$$q_i^{\mathrm{SE}} = 1 - \prod_{j=1}^{N_i} [1 - \alpha p_j^I(t-1)] \tag{2}$$

式中:α 表示与该 S 状态节点直接通信的 I 状态节点对其发起成功攻击的概率。节点还可能由于环境影响、零件老化和物理损坏使其从状态 S 转换为状态 D,记这种自然死亡概率为 φ,则 $q_i^{\mathrm{SD}} = \varphi$。

处于状态 E 的异质传感器节点被恶意程序持续攻击,而且这些攻击具有一定的关联性,导致节点脆弱性降低。因此,该节点从 E 状态到 I 状态的转变对应于

被恶意程序成功感染并受恶意程序控制的过程,根据宋明秋等[25]在文章中对攻击相关性的设定,E 状态到 I 状态的状态转换概率可表示为:

$$q_i^{\mathrm{EI}} = \beta_0 + \Delta\beta \sum_{m=1}^{n} \left[m \frac{C_m^n \alpha^m (1-\alpha)^{n-m}}{q_i^{\mathrm{SE}}} \right] \tag{3}$$

式中:β_0 表示初始感染率;$\Delta\beta$ 为感染变化率;n 表示与该 E 状态节点直接通信的感染状态节点个数;m 表示节点受到恶意程序攻击感染的数目($1 \leqslant m \leqslant n$),且 m 是一个服从二项分布的随机变量。

处于 E 状态的异质传感器节点存在恶意程序传播风险而被隔离时将使其状态转变为 Q,该概率表示为 μ,则 $q_i^{\mathrm{EQ}} = \mu$。该状态的节点存在被恶意程序感染而加快能量消耗致不能提供正常服务的概率记为 θ,同样存在自然死亡概率,因此,E 状态到 D 状态的转换可表示为 $q_i^{\mathrm{ED}} = \varphi + \theta$。

对于在状态 Q 和状态 I 的异质传感器节点,通过查杀恶意程序或者打补丁的方式使其状态转换为 R,记这种恢复率为 λ,故从 Q 状态和 I 状态转换为 R 状态的转换概率可分别表示为 $q_i^{\mathrm{QR}} = \lambda$、$q_i^{\mathrm{IR}} = \lambda$,根据以上分析可得 $q_i^{\mathrm{QD}} = \varphi + \theta$、$q_i^{\mathrm{ID}} = \varphi + \theta$。

当在状态 R 的异质传感器节点具有新的安全漏洞时其状态会达到 S,记该概率为 δ,则 $q_i^{\mathrm{RS}} = \delta$。该状态节点同样存在因电池耗尽等自然死亡因素,故 $q_i^{\mathrm{RD}} = \varphi$。

2 异质传感器节点可用度计算

HWSNs 中传感器节点所处的状态是决定其能否正常工作的重要因素,而异质传感器节点状态转换过程是随机的,也就是现在所处的状态决定下一个状态的改变,和之前所处的状态无关。但是,马尔可夫过程(Markov Process,MP)和半马尔可夫过程(Semi Markov Process,SMP)相比较,SMP 的节点状态持续时间可以服从任意分布而 MP 只能服从指数分布,因此基于 SMP 对异质无线传感器节点动态转换过程建模更加客观,使得 HWSNs 可用度评估更符合实际情况。

在半马尔可夫过程中,从一种状态到另一种状态的过渡可以看作是逻辑上的两步过渡。在第一阶段,该过程在 $T_i(t)$ 给出的一定时间内保持在状态 x 中,其中 $T_i(t)$ 是状态 x 的停留时间分布。在下一阶段,该过程以转换概率 p_{xy} 将其状态从 x 更改为 y。记转移时间 t_n 下的状态为 x_n,我们可以得到:

$$P_r(X_{n+1} = x_{n+1} \mid X_0 = x_0, \cdots, X_n = x_n) = P_r(X_{n+1} = x_{n+1} \mid X_n = x_n) \tag{4}$$

其中,$x_i \in G$,$G = \{S, E, Q, I, R, D\}$,$0 \leqslant i \leqslant n+1$。因此通常使用一个 $SMP\{Z(t), t \geqslant 0\}$ 来表示一个节点的转换行为,且满足:

$$Z(t) = X_n \quad \forall\, t_n \leqslant t \leqslant t_{n+1} \tag{5}$$

式中:$\{X_n\}$ 表示过程 $\{Z(t)\}$ 的内嵌马尔可夫链;t 是描述异质传感器节点处于各状态的离散时间序列。定义 t_x 是传感器节点在状态 x 的持续时间,$\boldsymbol{v}_x$ 是传感器节点在状态 x 的转移概率矢量。定义稳态概率是异质传感器节点达到各个状态并驻留的时间和传感器节点驻留的总时间比值,记 $\boldsymbol{\pi}_x$ 是传感器节点的稳态概率矢量,即:

$$\boldsymbol{\pi}_x = \frac{\boldsymbol{v}_x t_x}{\sum_{y \in G} \boldsymbol{v}_y t_y} \quad x \in G \tag{6}$$

根据异质无线传感器网络状态转移模型构建状态转移矩阵 $\boldsymbol{P}$,可得:

$$\boldsymbol{P} = \begin{bmatrix} 0 & p_{\mathrm{SE}} & 0 & 0 & 0 & p_{\mathrm{SD}} \\ 0 & 0 & p_{\mathrm{EQ}} & p_{\mathrm{EI}} & 0 & p_{\mathrm{ED}} \\ 0 & 0 & 0 & 0 & p_{\mathrm{QR}} & p_{\mathrm{QD}} \\ 0 & 0 & 0 & 0 & p_{\mathrm{IR}} & p_{\mathrm{ID}} \\ p_{\mathrm{RS}} & 0 & 0 & 0 & 0 & p_{\mathrm{RD}} \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{7}$$

根据离散马尔可夫性质可得:

$$\begin{cases} \boldsymbol{v}_x = \boldsymbol{v}_x \boldsymbol{P} \\ \sum_{x \in C} \boldsymbol{v}_x = 1 \end{cases} \tag{8}$$

综上可得:

$$\boldsymbol{v}_{\mathrm{S}} = \frac{\delta}{1-(\chi+\mu)\lambda(1-\omega)\delta} \tag{9}$$

$$\boldsymbol{v}_{\mathrm{E}} = \frac{(1-\omega)\delta}{1-(\chi+\mu)\lambda(1-\omega)\delta} \tag{10}$$

$$\boldsymbol{v}_{\mathrm{Q}} = \frac{(1-\omega)\delta\mu}{1-(\chi+\mu)\lambda(1-\omega)\delta} \tag{11}$$

$$\boldsymbol{v}_{\mathrm{I}} = \frac{(1-\omega)\delta\chi}{1-(\chi+\mu)\lambda(1-\omega)\delta} \tag{12}$$

$$\boldsymbol{v}_{\mathrm{R}} = \frac{1}{1-(\chi+\mu)\lambda(1-\omega)\delta} \tag{13}$$

$$\boldsymbol{v}_{\mathrm{D}} = \frac{\varphi(1+\delta) + (\varphi+\theta)(1-\omega)\delta(1+\chi+\mu)}{1-(\chi+\mu)\lambda(1-\omega)\delta} \tag{14}$$

代入式(6)可得:

$$\boldsymbol{\pi}_{\mathrm{S}} = \frac{\delta t_{\mathrm{S}}}{[1-(\chi+\mu)\lambda(1-\omega)\delta]\boldsymbol{\pi}_{\mathrm{sum}}} \tag{15}$$

$$\boldsymbol{\pi}_{\mathrm{E}} = \frac{(1-\omega)\delta t_{\mathrm{E}}}{[1-(\chi+\mu)\lambda(1-\omega)\delta]\boldsymbol{\pi}_{\mathrm{sum}}} \tag{16}$$

$$\boldsymbol{\pi}_{\mathrm{Q}} = \frac{(1-\omega)\delta\mu t_{\mathrm{Q}}}{[1-(\chi+\mu)\lambda(1-\omega)\delta]\boldsymbol{\pi}_{\mathrm{sum}}} \tag{17}$$

$$\boldsymbol{\pi}_{\mathrm{I}} = \frac{(1-\omega)\delta\chi t_{\mathrm{I}}}{[1-(\chi+\mu)\lambda(1-\omega)\delta]\boldsymbol{\pi}_{\mathrm{sum}}} \tag{18}$$

$$\boldsymbol{\pi}_{\mathrm{R}}=\frac{t_{\mathrm{R}}}{[1-(\chi+\mu)\lambda(1-\omega)\delta]\boldsymbol{\pi}_{\mathrm{sum}}} \tag{19}$$

$$\boldsymbol{\pi}_{\mathrm{D}}=\frac{[\varphi(1+\delta)+(\varphi+\theta)(1-\omega)\delta(1+\chi+\mu)]t_{\mathrm{D}}}{[1-(\chi+\mu)\lambda(1-\omega)\delta]\boldsymbol{\pi}_{\mathrm{sum}}} \tag{20}$$

式中:

$$\boldsymbol{\pi}_{\mathrm{sum}}=\boldsymbol{\pi}_{\mathrm{s}}t_{\mathrm{s}}+\boldsymbol{\pi}_{\mathrm{E}}t_{\mathrm{E}}+\boldsymbol{\pi}_{\mathrm{Q}}t_{\mathrm{Q}}+\boldsymbol{\pi}_{\mathrm{I}}t_{\mathrm{I}}+\boldsymbol{\pi}_{\mathrm{R}}t_{\mathrm{R}}+\boldsymbol{\pi}_{\mathrm{D}}t_{\mathrm{D}},$$

$$w=\prod_{j=1}^{N_i}[1-\alpha p_j^l(t-1)];$$

$$\chi=\beta_0+\Delta\beta\sum_{m=1}^{n}\left[m\frac{C_m^n\alpha^m(1-\alpha)^{n-m}}{1-w}\right]。$$

处于状态 I 和 D 的异质传感器节点无法正常工作,而节点的稳态可用度描述了节点受到损坏或者恶意程序攻击之后继续提供可用服务的能力,故单个异质传感器节点的稳态可用度公式计算如式(21)所示。

$$A=1-\boldsymbol{\pi}_{\mathrm{I}}-\boldsymbol{\pi}_{\mathrm{D}} \tag{21}$$

3　HWSNs 可用度计算

3.1　星型 HWSNs

图 2 展现了由单个 Sink 节点和一些普通异质传感器节点构成的具有星型拓扑结构的 HWSNs。普通异质传感器节点直接将采集到的数据和 Sink 节点进行通信,只有可以提供正常服务的普通异质传感器节点达到一定数量的情况下,星型 HWSNs 才能维持正常运转,因此,可以得到具有星型拓扑结构的整个 HWSNs 稳态可用度计算公式,如式(22)所示。

$$A_{\mathrm{Star}}=\sum_{i=k}^{n}\left[\binom{n}{i}\cdot\prod_{j=i}^{k}A\cdot\prod_{j=i+1}^{n}(1-A)\right] \tag{22}$$

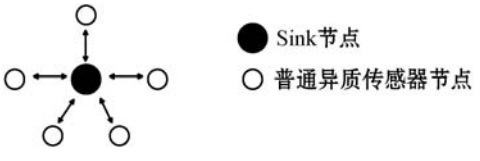

图 2　星型 HWSNs 拓扑结构

3.2　簇型 HWSNs

图 3 展示了由 Sink 节点、簇头节点和普通异质传感器节点三种类型的节点组成的簇型 HWSNs,它的工作流程是普通异质传感器节点先和相应的簇头节点通信,然后簇头节点再和 Sink 节点通信。在同一个簇内,所有普通异质传感器节点与簇头节点之间的通信都是并行的,且普通异质传感器节点通过簇头与 Sink 节点之间的路由是串行的,这些路由构成了簇型 HWSNs 的一个并行系统。因此,一个簇的稳态可用度计算公式可表示为:

$$A_c=1-\prod_{i=1}^{N_c}(1-A) \tag{23}$$

图 3　簇型 HWSNs 拓扑结构

式中:N_c 表示簇 c 中普通异质传感器节点数。一条路由的稳态可用度可表示为:

$$A_{router}=A_c\cdot A_{cn,router}=\left[1-\prod_{i=1}^{N_c}(1-A)\right]\cdot A_{cn,router} \tag{24}$$

式中:$A_{cn,router}$ 表示簇头 cn 的稳态可用度。整个簇型 HWSNs 的稳态可用度可表示为:

$$A_{Cluster}=1-\prod_{router=1}^{Router}(1-A_{router})=1-\prod_{router=1}^{Router}\left[1-\left(1-\prod_{i=1}^{N_c}(1-A)\right)A_{cn,router}\right] \tag{25}$$

式中:$Router$ 表示整个簇型 HWSNs 的路由数。

3.3　Mesh 型 HWSNs

如图 4 所示,一个 Mesh 型 HWSNs 通常包含若干 Sink 节点,每个 Sink 节点管理若干普通异质传感器节点。当一个普通异质传感器节点感知到数据后,发送到对应的 Sink 节点,再由 Sink 节点发送到基站。所有 Sink 节点形成了一个 Mesh 网络。

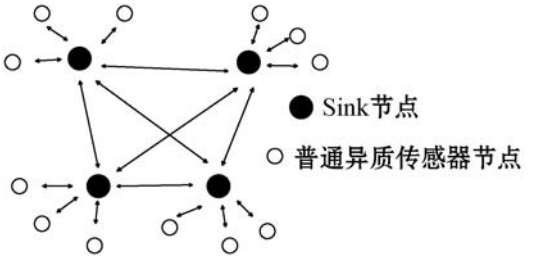

图 4　Mesh 型 HWSNs 拓扑结构

图 4 展示了一个 Sink 节点到所属该节点子网内的所有普通异质传感器节点的通信是并行的,而要使一个 Mesh 网络成功运行,其中至少需要有一定数量的 Sink 节点能正常工作。记 Sink 节点总数为 n,要求能正常工作的 Sink 节点数为 k。因此一个子网的稳态可用度可表示为:

$$A_m=1-\prod_{i=1}^{X_m}(1-A) \tag{26}$$

式中:X_m 表示子网中普通异质传感器节点数。整个 Mesh 型 HWSNs 的稳态可用度可由式(27)表示。

$$A_{\mathrm{mesh}}=\sum_{i=k}^{n}\left[\binom{n}{i}\cdot\prod_{j=i}^{k}A_m\cdot\prod_{j=i+1}^{n}(1-A_m)\right] \tag{27}$$

4 实验仿真及分析

从式(15)－式(20)可以看出,多个因素影响传感器节点 i 的稳态可用度,其中感染初始概率 β_0、感染变化率 $\Delta\beta$ 和恢复率 λ 是变化的,其他因素与节点所处的拓扑结构、使用的传感器节点种类和所要部署的环境等有关。所以,实验使用 MATLAB R2016a 先分析 β_0、$\Delta\beta$、λ 和单个异质传感器节点稳态可用度的关系,然后评估具有不同拓扑结构的 HWSNs 稳态可用度。

4.1 初始感染率和感染变化率对异质传感器节点可用度的影响

如图 5 所示,实验设定初始感染率 β_0 的变化范围为 10% ~60%,感染变化率 $\Delta\beta$ 分别为 0.05、0.1、0.15。可以看出,异质传感器节点的稳态与初始感染率、感染变化率相关,当初始感染率低且感染变化慢的时候异质传感器节点的可用度高。例如,当初始感染率从 0.1 升高到 0.6 时,对于 $\Delta\beta=0.05$、$\Delta\beta=0.1$ 和 $\Delta\beta=0.15$ 等三种情况,异质传感器节点的稳态可用度分别从 0.812 7、0.808 3、0.804 0 降低至 0.757 1、0.753 3、0.740。通过实验可以反映初始感染率越高,初始网络状态下异质传感器节点就越脆弱,更容易被恶意程序成功攻击,感染概率也随之升高,因而可用度就随之降低;感染变化率越高,异质传感器节点对恶意程序发起攻击的行为越敏感,其更容易被恶意程序感染并大范围传播恶意程序。所以,初始感染率和感染变化率越低,都将使异质传感器节点的稳态可用度越高。

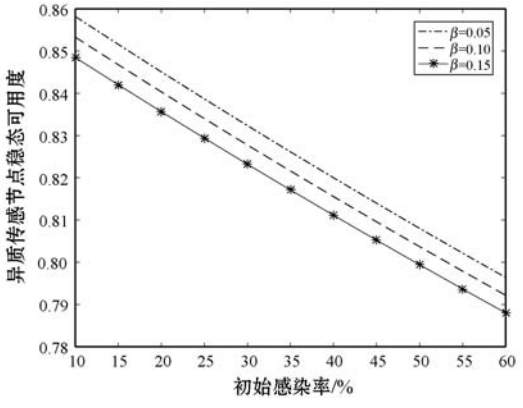

图 5 初始感染率和感染变化率对异质传感器节点稳态可用度的影响

4.2 感染率和恢复率对异质传感器节点可用度的影响

由式(3)可知,异质传感器节点的感染率和周围与其直接通信的已经被恶意程序感染的节点数量密切相关。通过实验来进一步说明它们之间的关系,实验设定恢复率 λ 的变化范围为 80% ~98%,周围与其直接通信的感染状态的异质传感器节点个数分别为 2、4、6。如图 6 所示,减少周围与其直接通信的感染状态的异质传感器节点个数和提高恢复率都能使异质传感器节点的稳态可用度提升。例如,当恢复率从 0.8 升高到 0.98 时,对于 $n=2$、$n=4$、$n=6$ 等三种情况,异质传感器节点的稳态可用度分别从约 0.820 1 升高到 0.824 6、从约 0.815 6 升高到 0.820 2 和从约 0.811 0 升高到 0.815 7。因为周围与其直接通信的已经被恶意程序感染的节点数量越多,该节点受到恶意程序的攻击就会越多,节点就会变得十分脆弱,更容易被恶意程序感染。

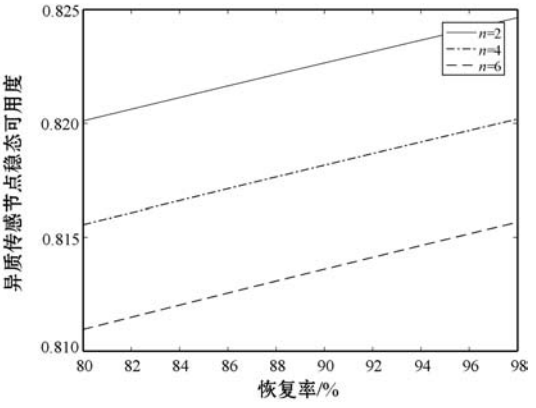

图 6 感染状态节点个数和恢复率对异质传感器节点稳态可用度的影响

4.3 星型 HWSNs 的可用度

图 7 给出了具有星型拓扑结构的 HWS-Ns 可用度评估结果。实验设定整个 HWSNs 中传感器节点总数变化范围为 20 ~30,可以提供正常服务的异质传感器节点数量变化范围为 5 ~25。实验结果反映出具有星型拓扑结构的 HWSNs 稳态可用度会升高因为异质传感器节点总数增加了,但是增加能够提供正常服务的异质传感器节点数量会使 H-WSNs 的稳态可用度降低。因此,在实际构建具有星型拓扑结构的 HWSNs 过程中,需要根据实际情况适当增加冗余的异质传感器节点的数量来提高整个 HWSNs 稳态可用度。

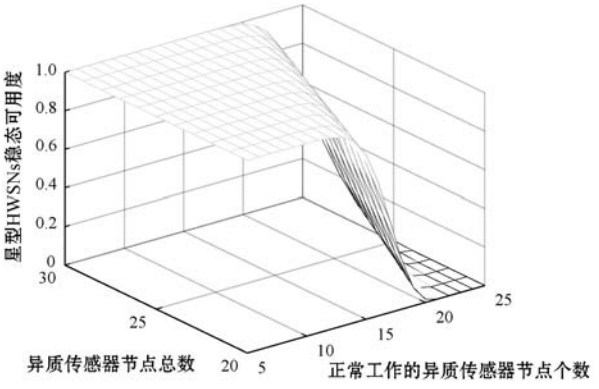

图 7 星型 HWSNs 的稳态可用度

4.4　簇型 HWSNs 的可用度

图 8 给出了具有簇型拓扑结构的 HWS-Ns 可用度评估结果,实验设定同一个簇中普通异质传感器节点个数 N_c 的变化范围为 1 ~ 8,整个 HWSNs 中路由数量分别为 1、2、3。例如,当同一个簇中普通异质传感器节点的数量从 1 增加到 8 时,对于 *Router* = 1、*Router* = 2 和 *Router* = 3 等三种情况,异质传感器节点的稳态可用度分别从 0.859 6、0.977 4、0.996 6 均升高至 1。通过对实验结果的分析,我们发现在实际构建簇型 HWSNs 的拓扑结构过程中,需要根据实际情况适当增加同一簇中异质传感器节点的数量来提高整个 HWSNs 稳态可用度,整个 HWSNs 稳态可用度的提高还可以通过路由数量的增加来实现。

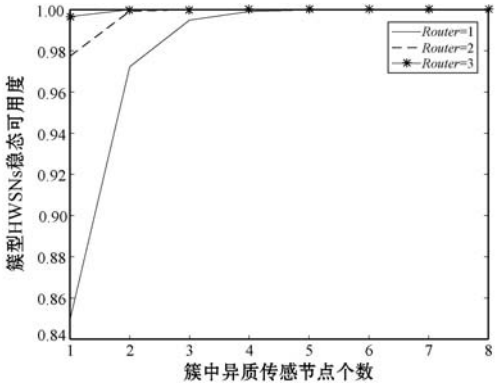

图 8　簇型 HWSNs 的稳态可用度

4.5　Mesh 型 HWSNs 的可用度

图 9 给出了具有 Mesh 型拓扑结构的 H-WSNs 可用度评估结果,实验设定整个子网中普通异质传感器节点数量变化范围为 2 ~ 6,Mesh 网中正常工作的异质传感器节点个数变化范围为 2 ~ 6。可以看出,具有 Mesh 型拓扑结构的 HWSNs 稳态可用度的升高是因为子网中异质传感器节点个数的增加,但是增加 Mesh 网中提供正常数据服务的异质传感器节点数量,整个 HWSNs 的稳态可用度会降低。实验结果反映出在实际构建具有 Mesh 型拓扑结构的 HWSNs 过程中,需要根据实际情况适当增加子网中冗余的异质传感器节点的数量来提高整个 HWS-Ns 稳态可用度。

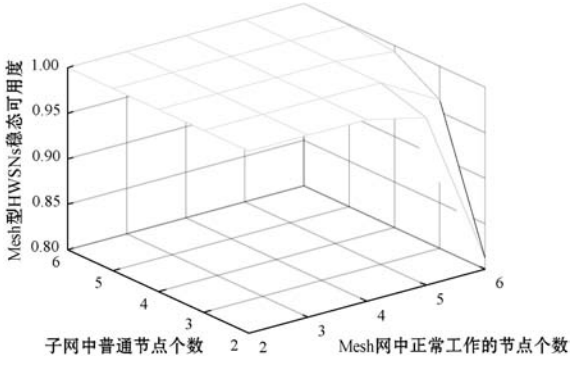

图 9　Mesh 型 HWSNs 的稳态可用度

5　结　语

本文在 SIRD 模型的基础上,通过设立潜伏状态和隔离状态来分别描述异质传感器节点被恶意程序感染而潜伏同时不具备感染其他节点能力的情况和被安全程序检测到存在恶意程序而被隔离提供时间来恢复服务的情况。考虑在恶意程序感染节点后不断对正常节点发起攻击的情况下,基于半马尔可夫过程建立的评估方法能实现对具有星型、簇型和 Mesh 型拓扑结构的异质无线传感器网络进行稳态可用度评估,为设计、部署和维护高可用度的 HWSNs 提供了理论基础保障。

参　考　文　献

[1] 郑力明,王黎. 军事物联网背景下的通信抗干扰技术探究[J]. 通信电源技术,2020,37(8):147 - 148.

[2] Gardašević G, Katzis K, Bajić D, et al. Emerging wireless sensor networks and internet of things technologies-foundations of smart healthcare[J]. Sensors,2020,20(13):3619.

[3] 戴天虹,赵永政,张佳薇,等. 林业环境监测中无线传感网信号传播特性[J]. 福建农林大学学报(自然科学版),2020,49(2):199 - 205.

[4] Mu D, Sha M, Kang K D, et al. Radio selection and data partitioning for energy-efficient wireless data transfer in real-time IoT applications[J]. Ad Hoc Networks, 2020, 107: 102251.

[5] Bengheni A, Didi F, Bambrik I. EEM-EHWSN: Enhanced energy management scheme in energy harvesting wireless sensor networks[J]. Wireless Networks,2019,25(6):3029 - 3046.

[6] Wei W, Sun Z Y, Song H B, et al. Energy balance-based steerable arguments coverage method in WSNs[J]. IEEE Access,2018,6:33766 - 33773.

[7] 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.

[8] 周海平,沈士根,冯晟,等. 基于微分博弈的无线传感器网络恶意程序传播模型[J]. 传感技术学报,2019,32(6):931 - 939.

[9] 周海平,沈士根,黄龙军,等. 攻防博弈驱动下的无线传感器网络病毒传播模型[J]. 计算机应用研究,2019,37(3):847 - 850.

[10] Zhou H P, Shen S G, Liu J H. Malware propagation model in wireless sensor networks under attack-defense confrontation[J]. Computer Communications,2020,162:51 - 58.

[11] Wang Y Q, Yang X Y. Virus spreading in wireless sensor networks with a medium access control mechanism[J]. Chinese Physics B,2013,22(4):40206.

(下转第 133 页)

4　应用实践

本文所设计实现的网络性能监控系统是在国产麒麟操作系统下借助 Python、Django、JQuery、Highcharts 等多个开源工具包开发实现的,具有网络拓扑管理、流量监测、设备状态监测等多项功能,图 7 是其进行网络流量监测的效果图。鉴于篇幅原因,其余不再赘述。

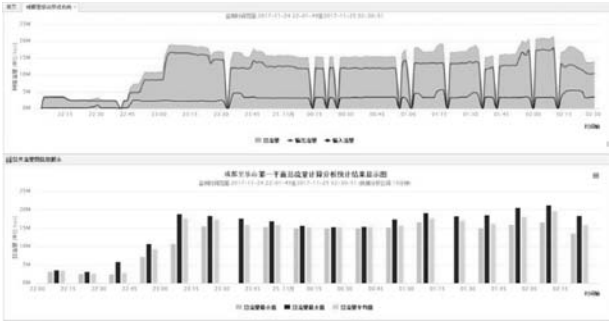

图 7　系统应用实例示意图

5　结　语

本文在对网络性能管理在网络运维中的积极作用及国产麒麟操作系统在政府、交通、金融、军队等关键部门大规模部署应用背景进行阐述分析的基础上,设计出一种基于 Django 框架的集数据采集、存储、封装、分析、显示及管理于一体的高性能网络性能管理系统,并对整个系统实现的关键细节结合具体实现技术进行了详细说明,给出了该系统运行的具体实例。应用实践表明,文章所述方法可靠可行,具有一定的应用推广价值。

参　考　文　献

[1] Django Software Foundation. Django Documentation[EB/OL]. (2021-01-01). https://www.djangoproject.com/.

[2] Ilya Etingof. Pysnmp Documentation[EB/OL]. (2021-01-01). https://github.com/etingof/pysnmp.

[3] Joe Kuan. Learning Highcharts 4[M]. Birmingham UK: Packt Publishing,2015: 321 - 328.

[4] 曹丹阳,霍然,孙凌,等. 卫星可见光波段观测模拟与分析系统设计与开发[J]. 软件,2018,39(3):1 - 7.

[5] 常佳宁,李阳齐. 基于 Django 的个人博客系统设计开发[J]. 中国科技信息,2021(2):75 - 77.

[6] 牛作东,李捍东. 基于 Python 与 flask 工具搭建可高效开发的实用型 MVC 框架[J]. 计算机应用与软件, 2019,36(7):21 - 25.

[7] 林刚,文全刚,傅晓阳,等. 解析 MIB 文件的 API 设计与应用[J]. 计算机应用与软件,2018,35(2):141 - 144.

[8] 赵鹏,褚剑等. 基于开源硬件平台的分布式网络性能测量系统研究[J]. 软件,2015,36(8):150 - 154.

(上接第 129 页)

[12] Yu S, Gu G F, Barnawi A, et al. Malware propagation in large-scale networks[J]. IEEE Transactions on Knowledge and Data Engineering,2015,27(1):170 - 179.

[13] Wang X M, He Z, Zhang L. A pulse immunization model for inhibiting malware propagation in mobile wireless sensor networks[J]. Chinese Journal of Electronics,2014,23(4):810 - 815.

[14] 赵金皓,曹奇英,沈士根. 受到恶意程序攻击的 MWSNs 节点状态时空动力学分析[J]. 计算机应用与软件,2018,35(6):122 - 128.

[15] Shen S G, Zhou H P, Feng S, et al. SNIRD: Disclosing rules of malware spread in heterogeneous wireless sensor networks[J]. IEEE Access,2019,7:92881 - 92892.

[16] Shen S G, Zhou H P, Feng S, et al. HSIRD: A model for characterizing dynamics of malware diffusion in heterogeneous WSNs[J]. Journal of Network and Computer Applications,2019,146:102420.

[17] 沈士根,周海平,黄龙军,等. 基于扩展传染病模型的异质传感网恶意程序传播建模与分析[J]. 传感技术学报,2019,32(6):923 - 930.

[18] Lalropuia K C, Gupta V. A Bayesian game model and network availability model for small cells under denial of service (DoS) attack in 5G wireless communication network[J]. Wireless Networks,2020,26(1):557 - 572.

[19] 沈士根,范恩,胡珂立,等. 面向恶意程序传播的传感网可靠度评估[J]. 电子学报,2018,46(1):75 - 81.

[20] 苏玉泽,孟相如,康巧燕,等. 基于半马尔可夫过程的虚拟网络生存性模型[J]. 科学技术与工程,2019,19(24):260 - 267.

[21] Chen H S, Zhuang H Y, Shan Z G, et al. A novel SMP-based survivability evaluation metric and approach in wireless sensor network[J]. Computer Science and Information Systems,2019,16(3):733 - 751.

[22] Shakya R K, Rana K, Gaurav A, et al. Stability analysis of epidemic modeling based on spatial correlation for wireless sensor networks[J]. Wireless Personal Communications, 2019,108(3):1363 - 1377.

[23] 罗宁. 基于因果关联攻击场景重构的方法研究[D]. 武汉:华中科技大学,2005.

[24] 经小川,胡昌振,谭惠民. 基于关联序列分析的协同攻击检测方法研究[J]. 武汉理工大学学报,2004,26(6):78 - 81.

[25] 宋明秋,李艳博. 考虑攻击相关性的蠕虫传播模型[J]. 运筹与管理,2020,29(1):79 - 85.