面向恶意程序传播的传感网可靠度评估

沈士根[1,2],范 恩[1],胡珂立[1],刘建华[2],曹奇英[3]
(1. 绍兴文理学院计算机科学与工程系,浙江绍兴 312000; 2. 嘉兴学院数理与信息工程学院,浙江嘉兴 314001;
3. 东华大学计算机科学与技术学院,上海 201620)

摘 要: 为评估恶意程序传播环境中的传感网可靠度,引入"死亡"状态扩展了传统的 SEIR 传染病模型,采用马尔可夫链确切地描述了传感节点的状态动态变化过程. 利用随机博弈,提出了传感网恶意程序传播检测模型来预测恶意程序的传播行为概率,再将得到的结果整合到马尔可夫链的状态转换矩阵,实现了恶意程序传播故意性和马尔可夫链随机性的关联. 建立了利用马尔可夫链计算恶意程序传播环境中传感节点可靠度的公式,分别给出了具有星形和簇状拓扑结构的传感网可靠度评估方法. 实验给出了恶意程序传播对传感节点可靠度的影响,结果表明所提出的方法能有效评估整个传感网的可靠度.

关键词: 传感网; 恶意程序; 传染病模型; 随机博弈; 可靠度
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112 (2018)01-0075-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.01.011

Reliability Evaluation for WSNs with Malware Spread

SHEN Shi-gen[1,2], FAN En[1], HU Ke-li[1], LIU Jian-hua[2], CAO Qi-ying[3]
(1. *Department of Computer Science and Engineering, Shaoxing University, Shaoxing, Zhejiang* 312000, *China*;
2. *College of Mathematics, Physics and Information Engineering, Jiaxing University, Jiaxing, Zhejiang* 314001, *China*;
3. *College of Computer Science and Technology, Donghua University, Shanghai* 201620, *China*)

Abstract: To evaluate the reliability of WSNs (Wireless Sensor Networks) in the malware spread scenario, the traditional epidemic model SEIR was extended by introducing a state "Dead" and the dynamic change process of sensor node states was exactly described by a Markov chain (MC). Using the stochastic game, a malware spread detection model for WSNs was proposed to predict the probability of malware adopting the spread behavior. The prediction results attained were integrated into the MC's state transition matrix in order to relate the malware intention to the MC randomness. An equation to compute a sensor node's reliability in the malware spread scenario was constructed via the MC, and reliability evaluation methods for WSNs with star or cluster topology were given. Experiments have shown the influence of malware's spread on sensor nodes' reliability and illustrated that the proposed method can efficiently evaluate the WSNs reliability.

Key words: wireless sensor networks; malware; epidemic model; stochastic game; reliability

1 引言

在我国,物联网已被正式列为国家五大新兴战略性产业之一,带动了传感网在智慧城市、智慧健康、智慧交通、智慧安防等应用领域的迅猛发展. 而要实现物联网多元与异构的复杂应用环境,保证传感节点的可靠度是前提. 实际上,这种传感节点可靠度反映了传感节点在规定条件下和规定时间内完成数据感知、数据传输、数据汇聚等规定功能的能力,是评估整个传感网可靠度的基础. 实现传感节点的可靠度评估能预测整个传感网性能,指导整个传感网的设计、优化、部署和维护,从而为实现具有高可靠度的传感网奠定基础.

研究[1-4]表明,恶意程序在由大量传感节点组成的传感网中容易传播流行. 例如,Giannetsos 等人[2]给出了基于 Von Neumann 结构的传感节点中如何注入恶意程序并传播恶意程序的方法. Gu 等人[3]通过实验说明了在传感网中传播恶意程序的方便性. 这些恶意程序一旦利用传感节点的漏洞在传感网中广泛传播后,它们就能窃听传感节点感知的数据,甚至可以采用耗尽传感节点能量的方法使传感节点完全处于瘫痪状态,从

收稿日期:2016-06-23;修回日期:2016-11-24;责任编辑:李勇锋
基金项目:国家自然科学基金(No. 61272034, No. 61572014, No. 61603258);浙江省自然科学基金(No. LY16F020028)

而严重影响整个传感网的可靠度和整个网络工作的稳定性.

为了理解恶意程序的传播机制,越来越多的研究者利用传染病理论、元胞自动机、排队论等理论工具建立了不同的恶意程序传播模型[5].典型的主要包括:传统的 SEIR(Susceptible-Exposed-Infectious-Removed)传播模型[6,7]、基于二维元胞自动机的 SIR(Susceptible-Infectious-Removed)传播模型[8]、扩展传统传染病理论的 SEIRS-V (Susceptible-Exposed-Infectious-Removed-Susceptible-Vaccination)模型[9]、扩展传统传染病理论的 SID(Susceptible-Infectious-Dead)模型[10]、基于排队论的 SIS(Susceptible-Infectious-Susceptible)模型[11]、分别具有指数分布和幂律分布规律的两阶段 SIS 模型[12]、以及针对移动传感网的反应扩散方程模型[13,14]、脉冲微分方程模型[15]等.

当前,国内外研究者针对传感网及传感节点的可靠度评估已提出了一些方法.邹青丙等人[16]综述了包括传感网在内的无线多跳网络可靠度评估方法,并结合物联网应用环境,对无线多跳网络可靠性研究的发展趋势进行了展望.黄旭等人[17]提出了一种在实验中向传感网人为注入模拟故障后再评估网络可靠度的方法.郭志强等人[18]基于模糊逻辑设计了一个综合性链路质量指标,对传感网的无线链路质量进行了有效的评估和预测.聂晨华等人[19]基于动态故障树给出了传感网可靠度评估方法.Guo 等人[20]基于证据理论(evidence theory)评估传感节点的可靠度.Yang 和 Chen[21]针对具有线性关系的传感网,在改进 Monte Carlo 方法基础上提出了一种递归方差缩减(recursive variance reduction)评估方法.Silva 等人[22]给出了利用故障树评估工业应用场景下传感网可靠度的方法.

本文根据传感节点自身特性,在扩展传统的 SEIR 传染病模型基础上,基于随机博弈和马尔可夫链提出了一种面向恶意程序传播的传感网可靠度评估方法.首先,通过分析传感节点的实际状态,引入"死亡"状态得到一个更能确切反映传感节点在恶意程序传播环境中状态动态变化的模型,并以马尔可夫链形式给出了各个状态之间的动态变化关系.其次,由于马尔可夫链是一种随机过程,不能直接表达出恶意程序逐步传播的故意性,为解决该问题,利用随机博弈来预测恶意程序的传播行为概率,并将得到的结果整合到马尔可夫链的状态转换矩阵,从而实现恶意程序传播故意性和马尔可夫链随机性的关联.最后,利用马尔可夫链计算恶意程序传播环境中一个传感节点的平均无故障时间 MTTF(Mean Time to Failure),推理得到一个传感节点的可靠度,从而可推理得到具有星形和簇状拓扑结构的传感网可靠度评估方法.

2 基于扩展 SEIR 的传感节点状态转换模型

对一个传感节点而言,在感染恶意程序前后具有不同的状态.当节点存在系统漏洞但未被恶意程序感染时,可将其划分为"易感"(Susceptible,S)状态;当节点已被恶意程序感染但恶意程序未处于活动期,即被感染的节点不会向外传播恶意程序时,可将其划分为"潜伏"(Exposed,E)状态;当节点已被恶意程序感染且恶意程序通过传输数据等方式传播自身时,可将其划分为"传染"(Infectious,I)状态;当节点新安装了安全补丁从而对当前恶意程序具有免疫力时,可将其划分为"恢复"(Removed,R)状态;当节点损坏或因为恶意程序故意破坏导致失去所有的功能时,可将其划分为"死亡"(Dead,D)状态.因此,本文针对传感节点的实际情况,通过引入"死亡"状态扩展传统的 SEIR 模型得到一个新的 SEIRD(Susceptible-Exposed-Infectious-Removed-Dead)模型,从而能确切地反映一个传感节点在受恶意程序传播时的动态状态变化.各状态的动态变化以马尔可夫链表示,如图 1 所示.

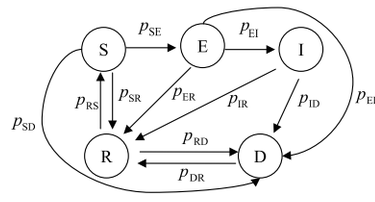


图1 以马尔可夫链表示的传感节点状态转换图

在图 1 中,每个状态转换实际上由传感网系统和恶意程序采取的行动触发.对一个传感节点而言,最初都处于 R 状态,当恶意程序通过扫描传感节点并发现传感节点具有安全漏洞时,传感节点的状态从 R 转换为 S.恶意程序接下来会利用扫描到的安全漏洞对传感节点继续攻击,若攻击成功,则使传感节点的状态从 S 转换为 E.由于恶意程序频繁地发动攻击容易被传感网系统成功检测,因此,恶意程序可能会采取隐藏自己的方式,从而使受恶意程序感染的传感节点长期处于 E 状态.而当恶意程序利用已感传感节点传播恶意程序时,传感节点的状态即从 E 转换为 I.通常,安装安全补丁并清除已知的恶意程序是目前弥补系统安全漏洞并使传感节点免受已知恶意程序感染的常用措施,实行这些措施将使传感节点的状态从 S、E 或 I 转换为 R.另外,任何一个传感节点都可能出现软硬件故障或者能量耗尽等情况,使得传感节点的状态从 S、E、I 或 R 转换为 D.对于已"死亡"的节点,由于传感节点一般都有不可修复性,所以通常采用直接更换传感节点的方式,此时,将使传感节点的状态从 D 转换为 R.值得说明的是,状态从 D 转换为 R 的传感节点已不再是原来的传

感节点.

在上述状态转换过程中,从状态 R 转换为 S 和从状态 S 转换为 E 都是由于恶意程序逐步传播造成的. 虽然恶意程序在何时发动传播行为是随机的,但具体实施传播行为是故意的. 而马尔可夫链作为一种随机过程,不能直接表达出恶意程序逐步传播的故意性. 又由于恶意程序使传感节点从状态 R 转换为 S 再转换为 E 涉及多个状态,且这两个状态转换具有相关性,因此,本文将通过引入随机博弈模型来预测传感节点分别处于状态 R 和 S 时恶意程序的传播行为,并把得到的恶意程序传播行为预测概率整合到马尔可夫链的状态转换矩阵中,从而解决如何关联恶意程序传播故意性和马尔可夫链随机性的问题.

3　基于随机博弈的传感网恶意程序传播检测模型

定义 1　基于随机博弈的传感网恶意程序传播检测模型是一个五元组$\mathbb{G}=\langle \Delta,\Phi,\Gamma,\Omega,\gamma\rangle$,其中:

- $\Delta=\{$传感网系统,恶意程序$\}$为参与者集合;
- $\Phi=\{\Phi_{\mathrm{R}},\Phi_{\mathrm{S}},\Phi_{\mathrm{E}}\}$为状态博弈集合,其中,$\Phi_{\mathrm{R}}$、$\Phi_{\mathrm{S}}$ 和 Φ_{E} 分别为传感节点分别处于状态 R、S 和 E 时的状态博弈;
- $\Gamma=\Gamma_W\times\Gamma_M$ 为传感网系统可采取的动作集合与恶意程序可采取的动作集合的迪卡尔积,其中,$\Gamma_W=\{\text{detect}(\delta),\text{not-detect}(\beta)\}$为传感网系统可采取的动作集合,$\Gamma_M=\{\text{spread}(\eta),\text{not-spread}(\varphi)\}$为恶意程序可采取的动作集合;
- $\Omega=\{\boldsymbol{Q}_{\mathrm{RS}},\boldsymbol{Q}_{\mathrm{SE}}\}$为各状态博弈之间的转移矩阵集合. 其中,$\boldsymbol{Q}_{\mathrm{RS}}$为状态博弈 Φ_{R} 转换到状态博弈 Φ_{S} 的转移矩阵,$\boldsymbol{Q}_{\mathrm{SE}}$ 为状态博弈 Φ_{S} 转换到状态博弈 Φ_{E} 的转移矩阵;
- $\gamma=\{\boldsymbol{U}_{\mathrm{R}},\boldsymbol{U}_{\mathrm{S}},\boldsymbol{U}_{\mathrm{E}}\}$为各状态博弈的支付矩阵集合. 其中,$\boldsymbol{U}_{\mathrm{R}}$ 为状态博弈 Φ_{R} 的支付矩阵,$\boldsymbol{U}_{\mathrm{S}}$ 为状态博弈 Φ_{S} 的支付矩阵,$\boldsymbol{U}_{\mathrm{E}}$ 为状态博弈 Φ_{E} 的支付矩阵.

定义 1 中的参与者分别为传感网系统和恶意程序,这是根据传感网恶意程序传播环境来确定的. 其中,传感网系统对应了传感网中实际部署的入侵检测系统 IDS(Intrusion Detection System),恶意程序对应了传感网中各种各样企图窃听传感数据、干扰传感网通信甚至破坏传感节点的恶意程序.

虽然图 1 给出的传感节点总共有 R、S、E、I 和 D 五种状态,但由于状态 I 和 D 分别表示“传染”和“死亡”状态,所以恶意程序关注的是传感节点的 R、S 和 E 状态. 也就是说,传感网系统和恶意程序之间的博弈是在传感节点的 R、S 和 E 状态下进行的. 因此,定义 1 中的整个随机博弈包含了 Φ_{R}、Φ_{S} 和 Φ_{E} 三个状态博弈.

对每个状态 $k\in\{\mathrm{R},\mathrm{S},\mathrm{E}\}$,记 $\rho^k=(\rho_\delta^k,\rho_\beta^k)$ 和 $\sigma^k=(\sigma_\eta^k,\sigma_\varphi^k)$分别为传感网系统和恶意程序在状态博弈 Φ_k 采取的混合策略,其中 ρ_δ^k 为传感网系统在状态博弈 Φ_k 采取动作 δ 的概率,ρ_β^k 为传感网系统在状态博弈 Φ_k 采取动作 β 的概率,σ_η^k 为恶意程序在状态博弈 Φ_k 采取动作 η 的概率,σ_φ^k 为恶意程序在状态博弈 Φ_k 采取动作 φ 的概率. 显然,对 $\forall k\in\{\mathrm{R},\mathrm{S},\mathrm{E}\}$,满足条件

$$\rho_\delta^k+\rho_\beta^k=1 \tag{1}$$

$$\sigma_\eta^k+\sigma_\varphi^k=1 \tag{2}$$

接下来分析各状态博弈之间的转移矩阵. 在整个随机博弈中,由于最初恶意程序未发现传感节点的漏洞,所以传感网系统和恶意程序从状态博弈 Φ_{R} 开始进行博弈过程. 而当恶意程序通过选择动作 η 发现传感节点存在软硬件漏洞并且未被传感网系统成功检测时,状态博弈即从 Φ_{R} 转换到 Φ_{S}. 记 $\sigma_\eta^{\mathrm{R}*}$ 为恶意程序在状态博弈 Φ_{R} 采取动作 η 的最优策略,则可以得到

$$p_{\mathrm{RS}}=\sigma_\eta^{\mathrm{R}*} \tag{3}$$

另外,每个传感节点都可能硬件损坏或者能量耗尽导致其状态转换为 D. 记 ξ 为一个传感节点的硬件损坏率,则可以得到

$$p_{\mathrm{RD}}=\xi \tag{4}$$

由式(3)和式(4),可以得到状态博弈 Φ_{R} 转换到 Φ_{S} 的转移矩阵 $\boldsymbol{Q}_{\mathrm{RS}}$的元素为

$$\lambda_{ij}^{\mathrm{RS}}=\begin{cases}\dfrac{\sigma_\eta^{\mathrm{R}*}}{\sigma_\eta^{\mathrm{R}*}+\xi}, & \text{若 } i=\beta \text{ 且 } j=\eta\\ 0, & \text{其他}\end{cases} \tag{5}$$

恶意程序然后会针对发现的漏洞继续选择动作 η,若仍未被传感网系统成功检测,则将恶意程序传染到传感节点,使得状态博弈 Φ_{S} 从转换到 Φ_{E}. 记 $\sigma_\eta^{\mathrm{S}*}$ 为恶意程序在状态博弈 Φ_{S} 采取动作 η 的最优策略,τ 为恶意程序成功传播的概率,则可以得到

$$p_{\mathrm{SE}}=\sigma_\eta^{\mathrm{S}*}\tau \tag{6}$$

记 ϑ 为一个传感节点安全补丁的修复率,则可以得到

$$p_{\mathrm{SR}}=\vartheta \tag{7}$$

由式(4)、(6)和式(7),可以得到状态博弈 Φ_{S} 转换到 Φ_{E} 的转移矩阵 $\boldsymbol{Q}_{\mathrm{SE}}$的元素为

$$\lambda_{ij}^{\mathrm{SE}}=\begin{cases}\dfrac{\sigma_\eta^{\mathrm{S}*}\tau}{\sigma_\eta^{\mathrm{S}*}\tau+\vartheta+\xi}, & \text{若 } i=\beta \text{ 且 } j=\eta\\ 0, & \text{其他}\end{cases} \tag{8}$$

最后分析各状态博弈的支付矩阵集合. 在每个状态博弈 $\Phi_k(k\in\{\mathrm{R},\mathrm{S},\mathrm{E}\})$,因为恶意程序和传感网系统各有两种纯策略可供选择,所以共有四种纯策略对:(δ,η)、(δ,φ)、(β,η)、(β,φ). 其中,纯策略对(δ,η)表示传感网系统正检测恶意程序的传播行为,这将使恶意程序遭受损失;纯策略对(δ,φ)表示传感网系统对恶

意程序的正常行为误判为传播行为,也就是说,入侵检测系统产生误报;纯策略对(β,η)表示传感网系统对恶意程序的传播行为未作检测,这与实际入侵检测系统中存在的漏报相对应;纯策略对(β,φ)表示传感网系统和恶意程序均未采取相应的动作. 值得说明的是,在整个随机博弈中,每个状态博弈的效用包括两部分,一部分为当前状态博弈中各参与者取得的瞬时效用,另一部分为转移到下一个状态博弈的预期效用. 记 $\varepsilon_{ij}^{k}(k\in\{\mathrm{R},\mathrm{S},\mathrm{E}\},i\in\{\delta,\beta\},j\in\{\eta,\varphi\})$为恶意程序在状态博弈 $\boldsymbol{\Phi}_k(k\in\{\mathrm{R},\mathrm{S},\mathrm{E}\})$中得到的瞬时效用(instantaneous utility),ν_{S} 和 ν_{E} 分别为支付矩阵 $\boldsymbol{U}_{\mathrm{S}}$ 和 $\boldsymbol{U}_{\mathrm{E}}$ 的值,则由随机博弈累积效用的定义,可以得到支付矩阵 $\boldsymbol{U}_{\mathrm{R}}$、$\boldsymbol{U}_{\mathrm{S}}$ 和 $\boldsymbol{U}_{\mathrm{E}}$ 的元素 ψ_{ij}^{R}、ψ_{ij}^{S}和 ψ_{ij}^{E}分别为

$$\psi_{ij}^{\mathrm{R}}=\begin{cases}\varepsilon_{ij}^{\mathrm{R}}+\lambda_{ij}^{\mathrm{RS}}\nu_{\mathrm{S}}, & \text{若 } i=\beta \text{ 且 } j=\eta\\ 0, & \text{其他}\end{cases}\tag{9}$$

$$\psi_{ij}^{\mathrm{S}}=\begin{cases}\varepsilon_{ij}^{\mathrm{S}}+\lambda_{ij}^{\mathrm{SE}}\nu_{\mathrm{E}}, & \text{若 } i=\beta \text{ 且 } j=\eta\\ 0, & \text{其他}\end{cases}\tag{10}$$

$$\psi_{ij}^{\mathrm{E}}=\varepsilon_{ij}^{\mathrm{E}}\tag{11}$$

式(9)中,$\varepsilon_{ij}^{\mathrm{R}}$表示恶意程序在状态博弈 $\boldsymbol{\Phi}_{\mathrm{R}}$ 中得到的瞬时效用,$\lambda_{ij}^{\mathrm{RS}}\nu_{\mathrm{S}}$ 表示转移到下一个"状态博弈"$\boldsymbol{\Phi}_{\mathrm{S}}$ 时恶意程序得到的预期效用,其中

$$\nu_{\mathrm{S}}=\sum_{i\in\{\delta,\beta\}}\sum_{j\in\{\eta,\varphi\}}\rho_i^{\mathrm{S}*}\sigma_j^{\mathrm{S}*}\psi_{ij}^{\mathrm{S}}\tag{12}$$

式(10)中,$\varepsilon_{ij}^{\mathrm{S}}$表示恶意程序在状态博弈 $\boldsymbol{\Phi}_{\mathrm{S}}$ 中得到的瞬时效用,$\lambda_{ij}^{\mathrm{SE}}\nu_{\mathrm{E}}$ 表示转移到下一个"状态博弈"$\boldsymbol{\Phi}_{\mathrm{E}}$ 时恶意程序得到的预期效用,其中

$$\nu_{\mathrm{E}}=\sum_{i\in\{\delta,\beta\}}\sum_{j\in\{\eta,\varphi\}}\rho_i^{\mathrm{E}*}\sigma_j^{\mathrm{E}*}\psi_{ij}^{\mathrm{E}}\tag{13}$$

式(11)中,$\varepsilon_{ij}^{\mathrm{E}}$表示恶意程序在状态博弈 $\boldsymbol{\Phi}_{\mathrm{E}}$ 中得到的瞬时效用.

至此,通过计算传感网恶意程序传播检测模型在状态博弈 $\boldsymbol{\Phi}_{\mathrm{R}}$ 和 $\boldsymbol{\Phi}_{\mathrm{S}}$ 的纳什均衡,就可以得到恶意程序在这两个状态博弈中选择传播行为的最优概率 $\sigma_\eta^{\mathrm{R}*}$ 和 $\sigma_\eta^{\mathrm{S}*}$,再通过式(3)和式(6)实现与马尔可夫链状态转换概率的关联.

算法1 计算传感网恶意程序传播检测模型中恶意程序选择传播行为的最优概率

步骤1 由式(11)初始化支付矩阵 $\boldsymbol{U}_{\mathrm{E}}$.

步骤2 计算状态博弈 $\boldsymbol{\Phi}_{\mathrm{E}}$ 的纳什均衡分别得到传感网系统和恶意程序的最优混和策略$(\rho_\delta^{\mathrm{E}*},\rho_\beta^{\mathrm{E}*})$和$(\sigma_\eta^{\mathrm{E}*},\sigma_\varphi^{\mathrm{E}*})$.

步骤3 设置 $\nu_{\mathrm{E}}\leftarrow\sum_{i\in\{\delta,\beta\}}\sum_{j\in\{\eta,\varphi\}}\rho_i^{\mathrm{E}*}\sigma_j^{\mathrm{E}*}\psi_{ij}^{\mathrm{E}}$.

步骤4 由式(10)计算支付矩阵 $\boldsymbol{U}_{\mathrm{S}}$.

步骤5 计算状态博弈 $\boldsymbol{\Phi}_{\mathrm{S}}$ 的纳什均衡分别得到传感网系统和恶意程序的最优混和策略$(\rho_\delta^{\mathrm{S}*},\rho_\beta^{\mathrm{S}*})$和$(\sigma_\eta^{\mathrm{S}*},\sigma_\varphi^{\mathrm{S}*})$.

步骤6 设置 $\nu_{\mathrm{S}}\leftarrow\sum_{i\in\{\delta,\beta\}}\sum_{j\in\{\eta,\varphi\}}\rho_i^{\mathrm{S}*}\sigma_j^{\mathrm{S}*}\psi_{ij}^{\mathrm{S}}$.

步骤7 由式(9)计算支付矩阵 $\boldsymbol{U}_{\mathrm{R}}$.

步骤8 计算状态博弈 $\boldsymbol{\Phi}_R$ 的纳什均衡分别得到传感网系统和恶意程序的最优混和策略$(\rho_\delta^{\mathrm{R}*},\rho_\beta^{\mathrm{R}*})$和$(\sigma_\eta^{\mathrm{R}*},\sigma_\varphi^{\mathrm{R}*})$.

步骤9 返回恶意程序选择传播行为的最优概率 $\sigma_\eta^{*}=\{\sigma_\eta^{\mathrm{E}*},\sigma_\eta^{\mathrm{S}*},\sigma_\eta^{\mathrm{R}*}\}$.

4 恶意程序传播环境中的传感网可靠度评估

4.1 评估传感节点的可靠度

记 Θ 为传感节点在恶意程序传播环境中的状态集合,由图1可得到

$$\Theta=\{\mathrm{R},\mathrm{S},\mathrm{E},\mathrm{I},\mathrm{D}\}\tag{14}$$

记

$$\boldsymbol{Z}(t)=[Z_{\mathrm{R}}(t)\ \ Z_{\mathrm{S}}(t)\ \ Z_{\mathrm{E}}(t)\ \ Z_{\mathrm{I}}(t)\ \ Z_{\mathrm{D}}(t)]\tag{15}$$

为一个传感节点在时刻 t 的状态概率向量,其中 $Z_i(t)$ $(i\in\Theta)$表示一个传感节点在时刻 t 处于状态 i 的概率. 记 $\boldsymbol{P}$ 为包含元素 $p_{ij}(i,j\in\Theta)$的传感节点状态转换矩阵,可以得到描述各状态动态变化的微分等式为

$$\frac{\mathrm{d}\boldsymbol{Z}(t)}{\mathrm{d}t}=\boldsymbol{Z}(t)\boldsymbol{P}\tag{16}$$

记

$$\boldsymbol{Z}=[Z_{\mathrm{R}}\ \ Z_{\mathrm{S}}\ \ Z_{\mathrm{E}}\ \ Z_{\mathrm{I}}\ \ Z_{\mathrm{D}}]\tag{17}$$

为一个传感节点的马尔可夫链状态稳态概率向量,则其值可通过解由

$$\boldsymbol{Z}\boldsymbol{P}=0\tag{18}$$

得到的五个等式中的任意四个等式联合

$$\sum_{i\in\Theta}Z_i=1\tag{19}$$

形成的方程组得到.

得到一个传感节点的马尔可夫链状态稳态概率向量后,接下来即可计算恶意程序传播环境中一个传感节点的 MTTF. 记 Θ_{Use}为一个传感节点能正常工作的状态集合,Θ_{Disuse}为一个传感节点不能正常工作的状态集合,则由式(14)可以得到

$$\Theta_{\mathrm{Use}}=\{\mathrm{R},\mathrm{S},\mathrm{E}\}\tag{20}$$

$$\Theta_{\mathrm{Disuse}}=\{\mathrm{I},\mathrm{D}\}\tag{21}$$

这样,传感节点状态转换矩阵 $\boldsymbol{P}$ 相应地可表示为

$$\boldsymbol{P}=\begin{bmatrix}\boldsymbol{P}_1 & \boldsymbol{P}_2\\ \boldsymbol{P}_3 & \boldsymbol{P}_4\end{bmatrix}\tag{22}$$

其中,

$$\boldsymbol{P}_1=\begin{bmatrix}p_{\mathrm{RR}} & p_{\mathrm{RS}} & p_{\mathrm{RE}}\\ p_{\mathrm{SR}} & p_{\mathrm{SS}} & p_{\mathrm{SE}}\\ p_{\mathrm{ER}} & p_{\mathrm{ES}} & p_{\mathrm{EE}}\end{bmatrix}\tag{23}$$

$$\boldsymbol{P}_2=\begin{bmatrix}p_{\mathrm{RI}} & p_{\mathrm{RD}}\\ p_{\mathrm{SI}} & p_{\mathrm{SD}}\\ p_{\mathrm{EI}} & p_{\mathrm{ED}}\end{bmatrix}\tag{24}$$

$$\boldsymbol{P}_3=\begin{bmatrix}p_{\mathrm{IR}} & p_{\mathrm{IS}} & p_{\mathrm{IE}}\\ p_{\mathrm{DR}} & p_{\mathrm{DS}} & p_{\mathrm{DE}}\end{bmatrix} \tag{25}$$

$$\boldsymbol{P}_4=\begin{bmatrix}p_{\mathrm{II}} & p_{\mathrm{ID}}\\ p_{\mathrm{DI}} & p_{\mathrm{DD}}\end{bmatrix} \tag{26}$$

类似地,记 $\boldsymbol{Z}_{\mathrm{Use}}$ 和 $\boldsymbol{Z}_{\mathrm{Disuse}}$ 分别为一个传感节点能正常工作和不能正常工作的状态稳态概率向量,则

$$\boldsymbol{Z}_{\mathrm{Use}}=[Z_{\mathrm{R}}\quad Z_{\mathrm{S}}\quad Z_{\mathrm{E}}\quad] \tag{27}$$

$$\boldsymbol{Z}_{\mathrm{Disuse}}=[Z_{\mathrm{I}}\quad Z_{\mathrm{D}}] \tag{28}$$

记 θ 为恶意程序传播环境中一个传感节点的 MTTF,则

$$\theta=\boldsymbol{Z}_{\mathrm{Use}}(0)(-\boldsymbol{P}_{\mathrm{I}})^{-1}\boldsymbol{I} \tag{29}$$

其中,

$$\boldsymbol{Z}_{\mathrm{Use}}(0)=\frac{\boldsymbol{Z}_{\mathrm{Use}}}{\boldsymbol{Z}_{\mathrm{Use}}\boldsymbol{I}} \tag{30}$$

$$\boldsymbol{I}=[l\quad l\quad l]^{-1} \tag{31}$$

至此,恶意程序传播环境中一个传感节点在时刻 t 的可靠度 $\mu(t)$ 可表示为

$$\mu(t)=\exp\left(-\frac{1}{\theta}t\right) \tag{32}$$

4.2　评估整个传感网的可靠度

4.2.1　星形拓扑结构

图 2 给出了一种具有星形拓扑结构的传感网,其中包含一个汇聚节点和多个传感节点. 在这种拓扑结构中,每个传感节点都与汇聚节点直接通信,并且每个传感节点互不影响,即一个传感节点的损坏不会影响到其他传感节点的运行. 因此,以可靠性理论的角度来看,这属于一个并行系统. 所以,可得到具有星形拓扑结构的整个传感网的可靠度 ω_{Star} 为

$$\omega_{\mathrm{Star}}=1-\prod_{i=1}^{X}(1-\mu(t)) \tag{33}$$

其中,X 表示整个传感网中传感节点的数量.

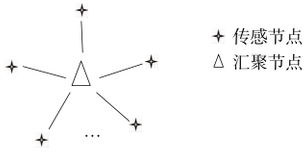


图2　具有星形拓扑结构的传感网

4.2.2　簇状拓扑结构

图 3 给出了一种具有簇状拓扑结构的传感网,其中包含一个汇聚节点和多个簇头节点. 在这种拓扑结构中,每个传感节点先与簇头节点通信,再由簇头节点进行数据处理后发送到汇聚节点. 以可靠性理论的角度来看,每个传感节点与簇头节点的通信可以看成是一个并行系统,而从一个传感节点到汇聚节点的一条路由可以看成是一个串行系统,不同的路由又可以看成一个并行系统,因此,具有簇状拓扑结构的整个传感网可以看成一个“并-串-并”系统. 所以,可得到具有簇状拓扑结构的整个传感网的可靠度 $\omega_{\mathrm{Cluster}}$ 为

$$\omega_{\mathrm{Cluster}}=1-\prod_{j=1}^{Y}\left(1-\left(1-\prod_{i=1}^{N}(1-\mu(t))\right)\mu(t)\right) \tag{34}$$

其中 N 表示一个簇中包含的传感节点数,Y 表示整个传感网包含的路由数.

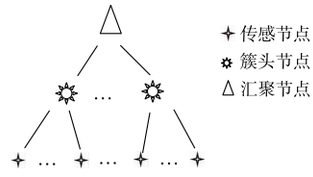


图3　具有簇状拓扑结构的传感网

5　实验

实验首先分析恶意程序传播对传感节点可靠度的影响,然后在恶意程序传播环境中分别评估具有星形和簇状拓扑结构的传感网可靠度. 由式(29)和(32)可知,传感节点可靠度值决定于传感节点状态转换矩阵和恶意程序在不同状态博弈中选择传播行为的最优概率. 根据传感网特点,实验参数设置 $\xi=1/300$,$\vartheta=7/10$,$\tau=0.5$.

5.1　恶意程序传播对传感节点可靠度的影响

由式(23)、(29)、(32)可知,在恶意程序传播环境中的传感节点可靠度跟传感节点状态转换矩阵密切相关,其中的元素 p_{RS} 和 p_{SE} 分别决定于由算法 1 得到的恶意程序采取传播行为的最优概率 $\sigma_\eta^{\mathrm{R}*}$ 和 $\sigma_\eta^{\mathrm{S}*}$,而其他元素主要决定于传感网部署后的拓扑结构,是相对固定的参数. 因此,实验首先探究恶意程序采取传播行为的概率 σ_η^{R} 和 σ_η^{S} 对传感节点可靠度的影响,如图 4 所示.

从图 4 可以看出,恶意程序在传感节点处于状态 R 时增大选择传播行为的概率对传感节点的可靠度影响较大,而在传感节点处于状态 S 时增大选择传播行为的概率对传感节点的可靠度影响微乎其微. 例如,当 $\sigma_\eta^{\mathrm{S}}=0.6$ 时,随着 σ_η^{R} 值从 0.2 变化到 1,传感节点的可靠度从约 0.8607 变化到约 0.7999,降低了约 7.1%;而当 $\sigma_\eta^{\mathrm{R}}=0.6$ 时,随着 σ_η^{S} 值从 0.2 变化到 1,传感节点的可靠度从约 0.8179 变化到约 0.8128,仅降低了约 0.6%. 这些实验结果反映出在传感节点处于状态 R 时增大选择传播行为的概率对传感节点的可靠度影响比传感节点处于状态 S 时要大,所以,在传感节点处于状态 R 时积极防御恶意程序的传播行为更能延长传感节点的可靠度,从而增强整个传感网的可靠性.

5.2　评估整个传感网的可靠度

图 5 给出了具有星形拓扑结构的处于恶意程序传播环境中的传感网可靠度评估结果,其中整个传感网中传感节点的数量分别为 10、20 和 30. 从中可以看出,

整个传感网的可靠度随着传感节点数量的增加而增加. 例如,当传感节点的数量分别为 10、20 和 30 时,整个传感网的可靠度从 1 降到 0.5 大约需要 15 天、19 天和 21 天. 实验结果反映出在实际构建具有星形拓扑结构的传感网时,根据需要适当增加传感节点的数量能提高处于恶意程序传播环境中的整个传感网可靠度.

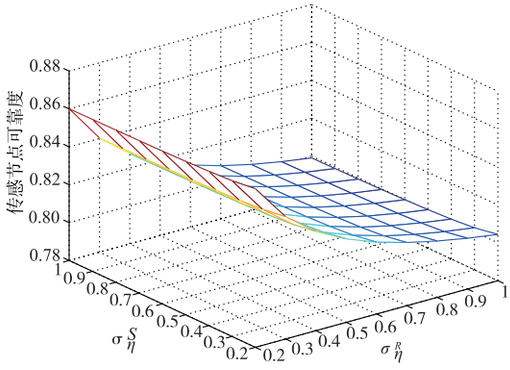


图4 σ_η^S和σ_η^R跟传感节点可靠度之间的关系

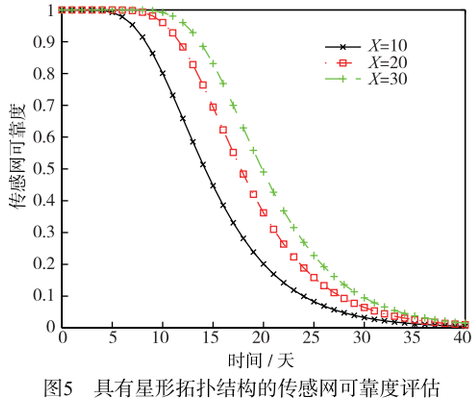


图5 具有星形拓扑结构的传感网可靠度评估

图 6 给出了具有簇状拓扑结构的处于恶意程序传播环境中的传感网可靠度评估结果,其中,一个簇中包含的传感节点数和整个传感网包含的路由数各分别设置为 2、4 和 6. 从中可以看出,整个传感网的可靠度随着簇中传感节点数的增加而增加,同时随着整个传感网包含的路由数的增加而增加,但变化的趋势不一样. 例如,当簇中传感节点数为 4,整个传感网包含的路由数从 2 变化到 6 时,整个传感网的可靠度从约 0.2292 变化到约 0.5420,增加了约 136.47%;而当整个传感网包含的路由数为 4,簇中传感节点数从 2 变化到 6 时,整个传感网的可靠度从约 0.1414 变化到约 0.6407,增加了约 353.11%. 实验结果表明,在实际构建具有簇状拓扑结构的传感网时,增加一个簇中的传感节点数比增加整个传感网的路由数更能提高处于恶意程序传播环境中的整个传感网可靠度.

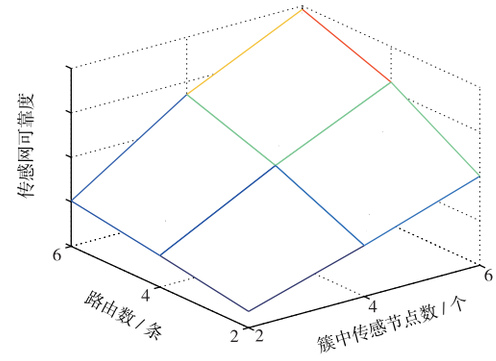


图6 具有簇状拓扑结构的传感网可靠度评估

6 结束语

本文根据传感节点的实际情况,通过引入“死亡”状态扩展的 SEIRD 模型能确切地描述传感节点的状态,以马尔可夫链表示的传感节点状态转换图阐明了传感网系统和恶意程序采取不同行动时导致的状态动态变化过程. 基于随机博弈的传感网恶意程序传播检测模型能预测恶意程序的传播行为概率,给出的算法详细描述了在不同状态计算最优传播概率的过程,将这些最优传播概率整合到马尔可夫链状态转换矩阵后,解决了如何关联恶意程序传播故意性和马尔可夫链随机性的问题. 基于马尔可夫链建立的评估方法能实现对具有星形和簇状拓扑结构的传感网进行可靠度评估,为设计和部署在恶意程序传播环境下高可靠度的传感网提供了理论依据.

参考文献

[1] ILLIANO V P,LUPU E C. Detecting malicious data injections in wireless sensor networks:A survey[J]. ACM Computing Surveys,2015,48(2):Article ID 24.

[2] GIANNETSOS T,et al. Arbitrary code injection through self-propagating worms in Von Neumann architecture devices[J]. Computer Journal,2010,53(10):1576 – 1593.

[3] GU Q,FERGUSON C,NOORANI R. A study of self-propagating mal-packets in sensor networks:Attacks and defenses[J]. Computers and Security,2011,30(1):13 – 27.

[4] 沈士根,刘建华,曹奇英. 博弈论与无线传感器网络安全[M]. 清华大学出版社,2016.
SHEN Shi-gen,LIU Jian-hua,CAO Qi-ying. Game Theory Meets Wireless Sensor Networks Security[M]. Tsinghua University Press,2016. (in Chinese)

[5] WANG Y,WEN S,XIANG Y,et al. Modeling the propagation of worms in networks:A survey[J]. IEEE Communications Surveys and Tutorials,2014,16(2):942 – 960.

[6] 王超,杨旭颖,等. 基于 SEIR 的社交网络信息传播模型[J]. 电子学报,2014,42(11):2325 – 2330.

WANG Chao, YANG Xu-ying, et al. SEIR-based model for the information spreading over SNS[J]. Acta Electronica Sinica, 2014, 42(11): 2325 – 2330. (in Chinese)

[7] 冯朝胜,秦志光,袁丁,等. P2P 网络中被动型蠕虫传播与免疫建模[J]. 电子学报,2013,41(5):884 – 889.
FENG Chao-sheng, QIN Zhi-guang, YUAN Ding, et al. Modeling propagation and immunization of passive worms in peer-to-peer networks [J]. Acta Electronica Sinica, 2013, 41(5): 884 – 889. (in Chinese)

[8] 苏晓萍,宋玉蓉,申情,等. 一种具有 GAF 分簇结构的无线传感器网络中恶意软件传播模型[J]. 电信科学,2011,27(8):33 – 38.
SU Xiao-ping, SONG Yu-rong, SHEN Qing, et al. A malware propagation model with GAF-based clustering in wireless sensor network [J]. Telecommunications Science, 2011, 27(8): 33 – 38. (in Chinese)

[9] MISHRA B K, KESHRI N. Mathematical model on the transmission of worms in wireless sensor network[J]. Applied Mathematical Modelling, 2013, 37(6): 4103 – 4111.

[10] 沈士根,黄龙军,等. 基于微分博弈的在线社交网络恶意程序传播优化控制方法[J]. 电信科学, 2015(10), 2015215.
SHEN Shi-gen, HUANG Long-jun, et al. Differential game-based optimal control method for preventing malware propagation in online social network[J]. Telecommunications Science, 2015(10), 2015215. (in Chinese)

[11] KARYOTIS V, PAPAVASSILIOU S. Macroscopic malware propagation dynamics for complex networks with churn[J]. IEEE Communications Letters, 2015, 19(4): 577 – 580.

[12] YU S, GU G, 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, HE Z, et al. Reaction-diffusion modeling of malware propagation in mobile wireless sensor networks [J]. Science China Information Sciences, 2013, 56(9): 1 – 18.

[14] ZHU L, ZHAO H, WANG X. Stability and bifurcation analysis in a delayed reaction-diffusion malware propagation model[J]. Computers and Mathematics with Applications, 2015, 69(8): 852 – 875.

[15] WANG X, 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.

[16] 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 Qing-bing, HE Ming, WANG Yan, et al. Survey on reliability evaluating method of wireless multi-hop networks[J]. Computer Engineering and Applications, 2015, 51(5): 88 – 91, 192. (in Chinese)

[17] 黄旭,陈冬岩,李会,等. FIPES:一种新的故障注入评测无线传感器网络及其可靠性方法[J]. 仪器仪表学报,2012,33(2):369 – 376.
HUANG Xu, CHEN Dong-yan, LI Hui, et al. FIPES: A new fault injection method for wireless sensor network reliability evaluation[J]. Chinese Journal of Scientific Instrument, 2012, 33(2): 369 – 376. (in Chinese)

[18] 郭志强,等. 基于综合性评估的无线链路质量分类预测机制[J]. 计算机研究与发展,2013,50(6):1227 – 1238.
GUO Zhi-qiang, et al. A classification prediction mechanism based on comprehensive assessment for wireless link quality[J]. Journal of Computer Research and Development, 2013, 50(6): 1227 – 1238. (in Chinese)

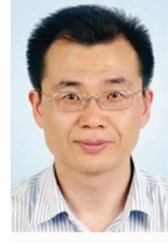
[19] 聂晨华,高西,等. 可修复节点无线传感器网络可靠性符号计算[J]. 计算机工程与设计,2015,36(8):2033 – 2039,2113.
NIE Chen-hua, GAO Xi, et al. Symbolic computation method for reliability evaluation of wireless sensor network with repairable node[J]. Computer Engineering and Design, 2015, 36(8): 2033 – 2039, 2113. (in Chinese)

[20] GUO H, SHI W, DENG Y. Evaluating sensor reliability in classification problems based on evidence theory[J]. IEEE Transactions on Systems, Man, and Cybernetics (Part B: Cybernetics), 2006, 36(5): 970 – 981.

[21] YANG Q, CHEN Y. Monte Carlo methods for reliability evaluation of linear sensor systems[J]. IEEE Transactions on Reliability, 2011, 60(1): 305 – 314.

[22] SILVA I, GUEDES L A, et al. Reliability and availability evaluation of wireless sensor networks for industrial applications[J]. Sensors, 2012, 12(1): 806 – 838.

作者简介



沈士根　男,1974 年生,浙江桐乡人,绍兴文理学院计算机科学与工程系教授,东华大学博士,研究方向为无线传感器网络、博弈论.
E-mail:shigens@126.com

范　恩　男,1982 年生,湖北武汉人,绍兴文理学院计算机科学与工程系讲师,西安电子科技大学博士,研究方向为智能信息处理、数据融合、无线传感器网络.
E-mail:efan@usx.edu.cn