DOI：10.7652/xjtuxb201504013

信息物理融合系统中恶意软件传播动力学研究

谢文军[1]，付晓[1,2]，于振华[1]，韩林[1]
（1.空军工程大学信息与导航学院，710077，西安；
2.中航工业西安飞行自动控制研究所飞行器控制一体化技术重点实验室，710065，西安）

摘要：针对恶意软件在信息物理融合系统(cyber-physical system，CPS)中的传播机理难以描述的问题，提出了一种自适应 SIQRS(susceptible-infected-quarantined-recovered-susceptible)传播动力学模型。该模型采用节点隔离机制描述 CPS 的感知和控制能力，引入链路重连机制刻画 CPS 的自适应性，进一步分析了恶意软件在 CPS 中的传播规则，并依据平均场理论建立了相应的微分动力学方程。不同参数条件下的仿真结果表明：当感染率小于存在阈值时，恶意软件无法在 CPS 内传播；当感染率大于存在阈值且小于传播阈值时，CPS 发生滞后分岔并出现双稳态现象；当感染率大于传播阈值时，CPS 稳定在地方病平衡状态；当参数满足特定条件时，CPS 会发生 Hopf 分岔。研究表明，所提模型能够准确刻画恶意软件在 CPS 中的传播机理。

关键词：信息物理融合系统；恶意软件；非线性动力学；自适应性
中图分类号：TP311.5 **文献标志码**：A **文章编号**：0253-987X(2015)04-0078-06

The Spreading Dynamics of Malicious Softwares in Cyber-Physical System

XIE Wenjun[1]，FU Xiao[1,2]，YU Zhenhua[1]，HAN Lin[1]
(1. School of Information and Navigation，Air Force Engineering University，Xi'an 710077，China；2. Science and Technology on Aircraft Control Laboratory，AVIC Xi'an Flight Automatic Control Research Institute，Xi'an 710065，China)

Abstract：An adaptive SIQRS(susceptible-infected-quarantined-recovered-susceptible) spreading dynamics model is proposed to solve the problem that it is difficult to describe the spreading mechanism of malicious softwares in cyber-physical system (CPS). The quarantined mechanism is employed to describe the perception and control abilities of CPS，and the link rewired mechanism is introduced to depict the adaptability of CPS. The spreading rules of malicious softwares are analyzed，and their differential dynamic equations are presented based on the mean field theory. Numerical simulation results with different parameters show that when the infection rate is less than the epidemic persistence threshold，malicious softwares cannot spread in CPS；when the infection rate is larger than the epidemic persistence threshold and less than the epidemic threshold，a backward bifurcation occurs which causes the bistability；when the infection rate is larger than the epidemic threshold，CPS is stable at the endemic equilibrium；and a Hopf bifurcation occurs when the parameters satisfy a specific condition. It is concluded that the adaptive SIQRS model can accurately describe the spreading mechanism of malicious softwares in CPS.

Keywords：cyber-physical system；malicious software；nonlinear dynamics；adaptability

收稿日期：2014-07-07。 作者简介：谢文军(1991—)，男，硕士生；于振华(通信作者)，男，副教授。 基金项目：国家自然科学基金资助项目(61202128，61401499)；航空科学基金资助项目(20125896020)；陕西省工业攻关资助项目(2012GY2-40)。
网络出版时间：2015-02-10 网络出版地址：http://www.cnki.net/kcms/detail/61.1069.T.20150210.0924.001.html

信息物理融合系统（cyber-physical system，CPS）是一种集成计算、通信与控制能力的新型智能系统[1]，CPS 中计算进程与物理进程持续交互、深度融合，具备自主感知、自主判断、自主调节等特性，具有较高的自治能力。目前 CPS 已广泛应用于国防、航空航天、智能交通、智能电网等关键领域[2-5]，成为学术界和工业界共同关注的热点。

CPS 所处环境复杂多变，易遭受病毒、木马、蠕虫等恶意攻击。一旦 CPS 发生故障甚至失效，将给国防安全和人民生命财产带来巨大损失。因此，CPS 必须可信且可控，必须确保其动态行为过程和结果与人们的预期相符。恶意软件攻击是导致 CPS 不可信的重要因素之一，其通常首先感染 CPS 中单个或数个节点，随后进行扩散性传播，导致更多节点功能受损，使得 CPS 可信性降低，因此有必要对恶意软件的传播过程进行建模和分析，这对有效控制恶意软件在 CPS 中的传播具有重要意义。

近年来，恶意软件传播动力学已成为计算机安全领域的研究热点，目前已提出 SIS（susceptible-infected-susceptible）、SIRS（susceptible-infected-recovered-susceptible）等多种静态传播模型[6-7]，并得到了广泛应用。文献[8]提出了一种蠕虫病毒传播模型；文献[9]提出了考虑隔离与防护措施的 SEIQV（susceptible-exposed-infected-quarantined-vaccinated）模型；文献[10]提出了一类具有非单调传染率的 SIQR（susceptible-infected-quarantined-recovered）模型；文献[11]研究了恶意软件在网络上的传播模型中的分岔、振荡等动力学行为。然而，CPS 是一个分布式复杂系统，具有动态性、自适应性等动力学行为特征，系统行为难以预测。因此，上述静态模型难以准确描述恶意软件在 CPS 中的实际传播过程，也无法充分解释振荡、灭绝[12]等重要随机动力学现象。

本文在 SIQR[13] 模型的基础上，结合 CPS 的特性，建立了恶意软件在 CPS 中的自适应 SIQRS（susceptible-infected-quarantined-recovered-susceptible）传播模型，对其动力学行为进行分析，从而研究恶意软件在 CPS 中的传播机理，并通过数值仿真进行了分析和验证。

1　信息物理融合系统中恶意软件传播动力学建模

1.1　动力学模型构建

根据 CPS 的感知、控制能力，作如下假设：①CPS中健康节点具有主动识别与其相连的节点是否健康的能力；②若某健康节点发现与其相连的另一节点被感染，则将通知周边所有未感染节点断开与该感染节点的链接，将其隔离，称此规则为节点隔离机制。

可将 CPS 中的节点划分为 4 种状态：易感染节点（susceptible node）、感染节点（infected node）、隔离节点（quarantined node）及恢复节点（recovered node），分别简称为 S 态节点、I 态节点、Q 态节点及 R 态节点，其状态转化过程如图 1 所示。各状态节点间转化规则如下：

（1）S 态节点以感染率 a 转化为 I 态节点，$a=pN_I$，其中 p 为单个 I 态节点沿着 I-S 边感染 S 态节点的能力，称其为单边感染率，N_I 表示与该 S 态节点相连的 I 态节点的数目；

（2）I 态节点以治愈率 r 被 CPS 自主“治愈”并获得暂时免疫能力，转化为 R 态节点；

（3）I 态节点被发现后将以隔离率 b 转化为 Q 态节点，且 Q 态节点有一定概率被治愈并获得免疫能力，从而转化为 R 态节点，其治愈率为 c；

（4）R 态节点经过一段时间后丧失免疫能力，并以转化率 q 转化为 S 态节点。

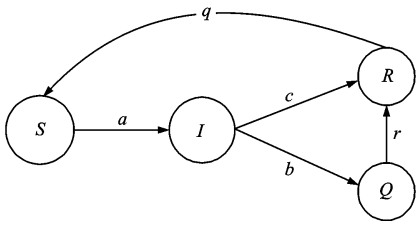


图 1　CPS 各状态节点转化过程示意图

为了刻画 CPS 的自适应性，在上述模型中添加如下规则：若某 S 态/R 态节点与 I 态节点相连，该节点能够以重连率[12] m 断开此 S-I/R-I 边，并与另一个 S 态或 R 态节点建立一条新的链接，此规则称为链路重连机制。该机制结合了节点动力学与拓扑动力学[14]，反映了拓扑结构和节点状态间的反馈现象，能更好地描述 CPS 节点状态演化过程及其动力学现象。

恶意软件开始传播时，CPS 拓扑同时开始自适应重构。设 P_s、P_i、P_r、P_q 分别表示网络中 S 态、I 态、R 态及 Q 态节点的分布密度，网络节点总数为 N，无向链接总数为 L。根据上述节点状态转化规则及平均场理论，可得恶意软件在 CPS 中的自适应 SIQRS 模型如下

$$P'_s(t)=qP_r(t)-pLP_{si}(t)/N \tag{1}$$

$$P'_i(t) = pLP_{si}(t)/N-(b+r)P_i(t) \quad (2)$$

$$P'_q(t) = bP_i(t)-cP_q(t) \quad (3)$$

$$P'_r(t) = rP_i(t)+cP_q(t)-qP_r(t) \quad (4)$$

式中：$P_{si}(t)$指 t 时刻 S-I 边的分布密度。虽然该模型较好地描述了 S 态节点、I 态节点、R 态节点的演化过程，但 $P_{si}(t)$仍是未知量。为进一步完善模型，基于自适应 SIRS 模型[12]，引入 5 个平均场量 P_{ss}、P_{sr}、P_{ii}、P_{ir}、P_{rr}，分别表示 S-S、S-R、I-I、I-R、R-R 边的分布密度。根据平均场理论，假设 $P_{ABC}\approx P_{AB}\cdot P_{BC}/P_B$，可得上述 6 种边分布密度的微分动力学方程[12]为

$$P'_{ss}(t) = qP_{sr}(t)+mP_s(t)P_{si}(t)/(P_s(t)+P_r(t))-2pLP_{ss}(t)P_{si}(t)/NP_s(t) \quad (5)$$

$$P'_{si}(t) = 2pLP_{ss}(t)P_{si}(t)/NP_s(t)+qP_{ir}(t)-rP_{si}(t)-mP_{si}(t)-p(P_{si}(t)+LP_{si}^2(t)/NP_s(t)) \quad (6)$$

$$P'_{ii}(t) = p(P_{si}(t)+LP_{si}^2(t)/NP_s(t))-2rP_{ii}(t) \quad (7)$$

$$P'_{rr}(t) = mP_r(t)P_{ir}(t)/(P_s(t)+P_r(t))+rP_{ir}(t)-2qP_{rr}(t) \quad (8)$$

$$P'_{sr}(t) = rP_{si}(t)+mP_r(t)P_{si}(t)/(P_s(t)+P_r(t))+mP_s(t)P_{ir}(t)/(P_s(t)+P_r(t))+2qP_{rr}(t)-qP_{sr}(t)-pLP_{si}(t)P_{sr}(t)/NP_s(t) \quad (9)$$

$$P'_{ir}(t) = 2rP_{ii}(t)+pLP_{si}(t)P_{sr}(t)/NP_s(t)-qP_{ir}(t)-rP_{ir}(t)-mP_{ir}(t) \quad (10)$$

1.2 动力学模型物理意义

根据以上动力学模型，在式(1)中，由于每个 R 态节点都以转化率 q 转化为 S 态节点，因此由 R 态节点转化引发的 S 态节点增加的速率为 $qP_r(t)$；由于 S 态节点被 I 态节点沿着 I-S 边感染的概率为 p，而每个 S 态节点平均接触 $LP_{si}(t)/N$ 个 I 态节点，因此由感染事件引发的 S 态节点减少的速率为 $pLP_{si}(t)/N$。

式(2)中，由于每个 I 态节点都以概率 r“痊愈”为 R 态节点或以隔离率 b 被隔离，因此 I 态节点减少的速率为 $(b+r)P_i(t)$。

式(3)中，由于每个 Q 态节点都以隔离治愈率 c“痊愈”为 R 态节点，因此由隔离节点恢复引发的 Q 态节点减少的速率为 $cP_q(t)$。

式(5)中，部分 R 态节点转化为 S 态节点，与其相连的原 R-S 边随之转化为 S-S 边，因此由 R 态节点转化引发的 S-S 边增加的速率为 $qP_{sr}(t)$；在重连事件中，S 态节点以重连率 m 断开与 I 态节点的链接，同时随机选择一个健康节点生成新的链接，在新生成的链接中 S-S 边所占百分比为 $P_s(t)/(P_s(t)+P_r(t))$，因此由重连引发的 S-S 边增加的速率为 $mP_s(t)P_{si}(t)/(P_s(t)+P_r(t))$；在一个 S-S-I 节点组中，若中间的 S 态节点被感染为 I 态节点，则与其相连的原 S-S 边将变为 S-I 边，而该节点组的分布密度为 $P_{ssi}(t)\approx P_{ss}(t)P_{si}(t)/P_s(t)$，且由于一条 S-S 边连接 2 个 S 态节点，平均每个 S 态节点产生 $2P_{ss}(t)/P_s(t)$ 条 S-S 边，由此引发的 S-S 边减少的速率为 $2pLP_{ss}(t)P_{si}(t)/NP_s(t)$。

式(6)中，部分 R 态节点转化为 S 态节点，与其相连的原 R-I 边随之转化为 S-I 边，由此引发的 S-I 边增加速率为 $qP_{ir}(t)$；部分 I 态节点“痊愈”为 R 态节点，与其相连的原 I-S 边随之转化为 R-S 边，由此引发的 S-I 边减少的速率为 $rP_{si}(t)$；在链路重连机制的作用下，S-I 边以重连率 m 转化为 S-S 边或 S-R 边，由此引发的 S-I 边减少的速率为 $mP_{si}(t)$；在一次感染事件中，I 态节点沿着 I-S 边以单边感染率 p 将 S 态节点感染为 I 态节点，原 I-S 边随之以速率 $pP_{si}(t)$转化为 I-I 边，若此前有另一 I 态节点与该 S 态节点相连，则两者之间的 I-S 边也将转化为 I-I 边，此事件仅发生在 I-S-I 节点组中，该节点组的分布密度为 $P_{isi}(t)\approx P_{si}^2(t)/P_s(t)$，因此 S-I 边减少的速率为 $p(P_{si}(t)+LP_{si}^2(t)/NP_s(t))$。

式(7)中，部分 I 态节点“痊愈”为 R 态节点，与其相连的原 I-I 边随之转化为 R-I 边，且每个 I 态节点平均产生 $2P_{ii}(t)/P_i(t)$ 条 I-I 边，因此原 I-I 边转化为 I-R 边的速率为 $2rP_{ii}(t)$。

式(8)中，在重连事件中，R 态节点断开与 I 态节点的链接并与另一个 R 态节点相连的概率为 $mP_r(t)/(P_s(t)+P_r(t))$，由此引发的 R-R 边增加的速率为 $mP_r(t)P_{ir}(t)/(P_s(t)+P_r(t))$。

式(9)中，在链路重连机制的作用下，部分 S 态节点断开与 I 态节点的链接并与 R 态节点相连，且部分 R 态节点断开与 I 态节点的链接并与 S 态节点相连，由此引发的 S-R 边增加的速率为 $mP_r(t)\cdot P_{si}(t)/(P_s(t)+P_r(t))+mP_s(t)P_{ir}(t)/(P_s(t)+P_r(t))$；部分 R 态节点转化为 S 态节点，与其相连的原 R-R 边随之转化为 S-R 边，且每个 R 态节点平均产生 $2P_{rr}(t)/P_r(t)$ 条 R-R 边，由此引发的 R-R 边减少的速率为 $2qP_{rr}(t)$；在一次感染事件中，S 态节点以概率 pL/N 被感染为 I 态节点，若此前有一个 R 态节点与该 S 态节点相连，则原 S-R 边将转化为 I-R 边，此事件仅发生在 I-S-R 节点组中，该节点

组的分布密度为 $P_{isr}(t)\approx P_{si}(t)P_{sr}(t)/P_s(t)$，由此引发的 S-R 边减少的速率为 $pLP_{si}(t)P_{sr}(t)/NP_s(t)$。

式(10)中，因为部分 R 态节点转化为 S 态节点，与其相连的原 R-I 边随之转化为 S-I 边，由此引发的 I-R 边减少的速率为 $rP_{ir}(t)$；因为原 I-R 边以重连率 m 断开重连，由此引发的 I-R 边减少的速率为 $mP_{ir}(t)$。

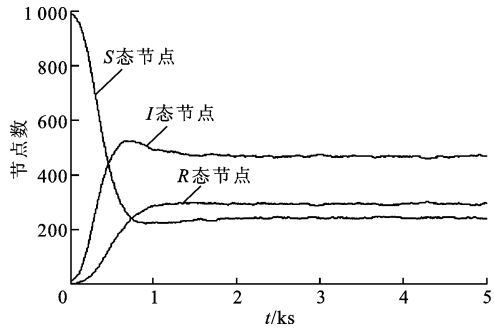
2　信息物理融合系统中恶意软件传播过程仿真与分析

为了形象地描述恶意软件在 CPS 中的传播机理，下面将其与恶意软件在一般系统中的传播过程进行对比。

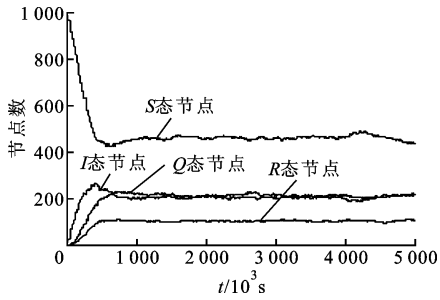
与 CPS 相比，一般系统通常不具备控制链接及自适应重构的能力，因此可将恶意软件在一般系统上的传播模型简化为经典 SIRS 模型[7]。

利用增长和优先连接机制[15]生成一般系统的拓扑图，在该拓扑图上加入节点隔离机制及链路重连机制，可获得 CPS 拓扑图。在此基础上对恶意软件在 CPS 与一般系统中的传播过程进行仿真对比、分析。

设初始时刻 S 态节点的密度 $P_s(0)=0.99$，I 态节点的密度 $P_i(0)=0.01$，Q 态节点的密度 $P_q(0)=0$，R 态节点的密度 $P_r(0)=0$，单边感染率 $p=0.002$，治愈率 $r=0.002$，转化率 $q=0.003\ 2$，网络中节点数 $N=10^3$，总边数 $L=3\ 000$，在一般系统上进行 1 000 次仿真实验，得出各状态节点分布演化曲线及度分布曲线；然后取相同参数在 CPS 上进行 1 000 次仿真实验，其中重连率 $m=0.002$，隔离率 $b=0.04$，隔离治愈率 $c=0.003\ 2$，进行同样操作，结果如图 2、图 3 所示。

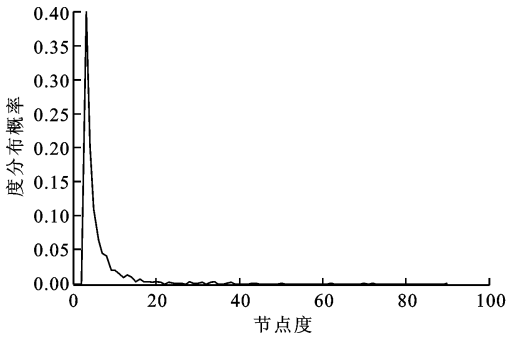


(a)一般系统

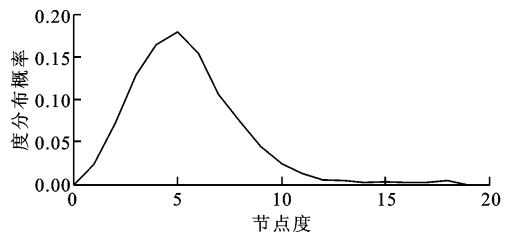


(b)CPS

图 2　各状态节点数量演化



(a)一般系统



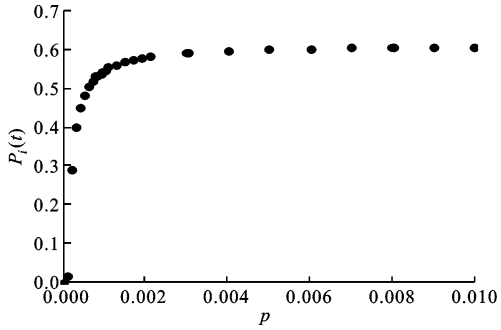
(b)CPS

图 3　稳定状态时节点度分布

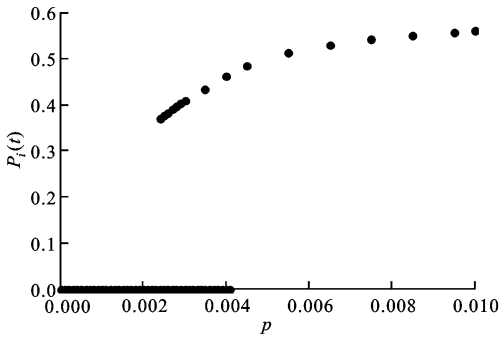
由图 2 可知，CPS 中恶意软件传播规模显著低于一般系统中的恶意软件传播规模，节点隔离机制与链路重连机制一定程度地抑制了恶意软件的传播，降低了损失；由图 3 可知，达到稳态后，一般系统中节点度数大多集中在 3～5 之间，同时存在较多大度数节点，而在 CPS 中，节点度分布相对均匀，网络中大度数节点消失，且出现了个别度数为 0 的孤立节点，显然这将增大恶意软件在 CPS 中的传播难度。

上述仿真仅考虑了固定参数情况下的恶意软件在 CPS 中的传播过程，而实际情况中系统参数往往是可变的，因此还需对变参数情况下恶意软件在 CPS 中的传播过程进行研究。本文采用 Runge-Kutta 法对变参数模型进行数值分析，以进一步了解其传播动力学特征。

首先考虑单边感染率 p 可变的情况。假设 CPS 中节点总数 $N=10^4$，总边数 $L=10^5$，治愈率 $r=0.002$，隔离率 $b=0.04$，隔离治愈率 $c=0.003\ 2$，转化率 $q=0.003\ 2$，单边感染率 p 不定，重连率取为 $m=0$ 及 $m=0.1$。对这两种情况分别进行数值仿真，得出感染率 p 与感染节点密度 $P_i(t)$ 的关系，如

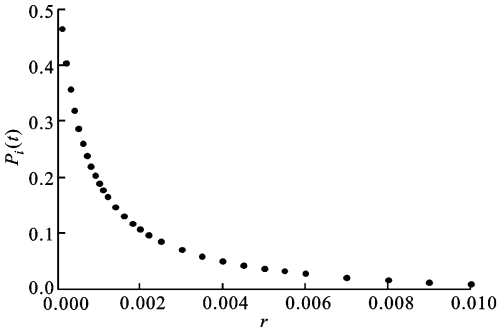


(a)$m=0$

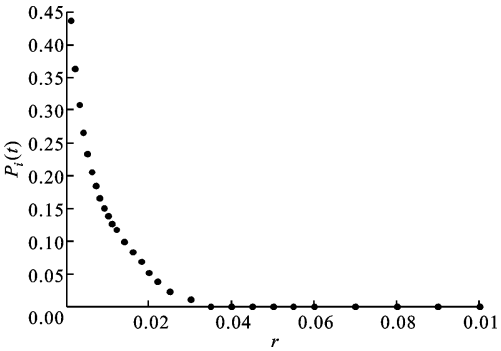


(b)$m=0.1$

图 4 CPS 中单边感染率 p 与感染节点密度 $P_i(t)$的关系



(a)$m=0$



(b)$m=0.05$

图 5 CPS 中治愈率 r 与感染节点密度 $P_i(t)$的关系

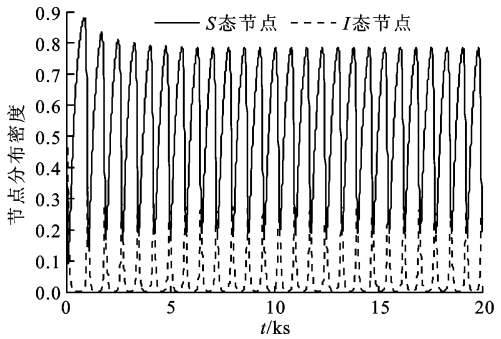
图 4 所示。

从图 4a 中可观察到当 $m=0$ 时，CPS 仅在单边感染率 p 取极小值时存在无病毒平衡状态，且在 $p\approx0.000\ 1$ 处发生了一个连续相变，之后稳定状态下的感染节点密度迅速上升，CPS 进入地方病平衡状态，该点即为传播阈值；在图 4b 中，当 $m=0.1$ 时，可观察到除传播阈值外，还出现了一个新的阈值，可称其为存在阈值，该阈值对应系统的鞍结分岔，当 p 大于存在阈值时，已感染的节点可持续存在。值得注意的是，这两个阈值间为不连续相变，两者间存在一个双稳态区域。在此区域内，CPS 发生滞后分岔，其无病毒平衡点和地方病平衡点都是稳定的，CPS 既有可能处于无病毒状态，也有可能处于地方病状态。随着 m 的增大，链路重连机制使得恶意软件的传播阈值显著增加，且地方病状态下的最终感染规模有所下降，大幅降低了恶意软件爆发的概率，有效提高了 CPS 对恶意软件的抵抗力。

其次考虑治愈率 r 可变的情况。假设 CPS 中节点总数 $N=10^4$，总边数 $L=10^5$，单边感染率 $p=0.008$，隔离率 $b=0.001$，隔离治愈率 $c=0.002$，转化率 $q=0.003\ 2$，治愈率 r 不定，重连率为 $m=0$ 及 $m=0.05$。对这两种情况进行数值仿真，得出治愈率 r 与感染节点密度 $P_i(t)$的关系，如图 5 所示。

由图 5 可知，随着 m 的增大，完全抑制恶意软件传播所需的治愈率降低。在链路重连机制的作用下，系统可在较低治愈率的情况下完全抑制恶意软件的传播，使其趋于消亡，减轻系统防护压力。

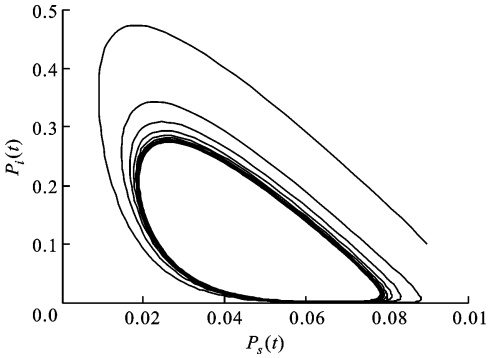
如图 6、图 7 所示，以单边感染率 p 为分岔参数，在其传播阈值处 CPS 将发生 Hopf 分岔，各状态节点的分布密度随之剧烈振荡，系统稳定性大幅下降。



$p=0.008$；$r=0.02$；$q=0.003\ 2$；$m=0.1$；$b=0.001$；$c=0.002$

图 6 CPS 中临界状态附近节点分布密度演化

综合上述仿真可知，虽然 CPS 中的节点隔离机制与链路重连机制难以彻底阻止恶意软件在 CPS 中的传播，但其可以提高恶意软件在 CPS 中的传播阈值，控制传播规模，对恶意软件在 CPS 中的传播过程有一定的抑制作用。



$p=0.008$；$r=0.02$；$q=0.003\ 2$；$m=0.1$；$b=0.001$；$c=0.002$

图 7　CPS 中 S 态-I 态节点相轨道

3　结　论

本文通过构建恶意软件在 CPS 中的自适应 SIQRS 传播模型，给出恶意软件在 CPS 中的传播规则，对其传播机理进行了研究，并进行了数值仿真。仿真结果表明，与一般系统相比，CPS 在节点隔离机制及链路重连机制的作用下能够更好地抵抗恶意软件的入侵，且这一抵抗能力随着重连率 m 的增大而加强。Hopf 分岔的出现表明所建自适应 SIQRS 模型可以较好地描述恶意软件在 CPS 中传播的复杂动力学行为特征，能够准确反映其动力学行为，便于对其展开进一步研究。

本文所建立的自适应 SIQRS 传播模型可预测恶意软件的传播趋势，有助于选择有效的控制方案，具有重要的理论意义与实践价值。此外，由该模型得出的各状态节点分布密度演化曲线可获知最佳介入时机，从而制订相应策略，以最小代价实现主动防御，最大限度地降低潜在风险。

参考文献：

[1] National Science Foundation of the United States. Cyber-physical system (CPS) program solicitation [EB/OL]. (2013-01-14) [2014-05-29]. http://www.nsf.gov.

[2] RAJKUMAR R, LEE I, SHA L. Cyber-physical systems: the next computing revolution [C]// Proceedings of the 47th ACM/IEEE Conference on Design Automation. Piscataway, NJ, USA: IEEE, 2010: 731-736.

[3] SAMPIGETHAYA K, POOVENDRAN R. Aviation cyber-physical systems: foundations for future aircraft and air transport [J]. Proceedings of the IEEE, 2013, 1010(8): 1834-1855.

[4] 何积丰. Cyber-physical Systems [J]. 中国计算机学会通讯，2010，6(1)：25-29.
HE Jifeng. Cyber-physical systems [J]. Communications of the China Computer Federation, 2010, 6(1): 25-29.

[5] LEE I, SOKOLSKY O, CHEN Sanjian, et al. Challenges and research directions in medical cyber-physical systems [J]. Proceedings of the IEEE, 2012, 100(1): 75-90.

[6] PASTOR-SATORRAS R, VESPIGNANI A. Epidemic spreading in scale-free networks [J]. Physical Review Letters, 2001, 86(14): 3200-3203.

[7] BUONOMO B, RIONERO S. On the Lapunov stability for SIRS epidemic models with general nonlinear incidence rate [J]. Applied Mathematics and Computation, 2010, 217(8): 4010-4016.

[8] TOUTONJI O A, YOO S, PARK M. Stability analysis of VEISV propagation modeling for network worm attack [J]. Applied Mathematical Modelling, 2012, 36(6): 2751-2761.

[9] WANG Fangwei, ZHANG Yunkai, WANG Changguang, et al. Stability analysis of a SEIQV epidemic model for rapid spreading worms [J]. Computers and Security, 2010, 29(4): 410-418.

[10] 叶志勇，刘原，吴用. 具有非单调传染率的 SIQR 传染病模型的稳定性分析 [J]. 生物数学学报，2014，29(1)：105-112.
YE Zhiyong, LIU Yuan, WU Yong. Stability of a SIQR model with nonmonotone incidence rate [J]. Journal of Biomathematics, 2014, 29(1): 105-112.

[11] 任建国. 计算机病毒的网络传播机制：三个新型的动力系统模型 [D]. 重庆：重庆大学，2012.

[12] SHAW L B, SCHWARTZ I B. Fluctuating epidemics on adaptive networks [J]. Physical Review: E, 2008, 77(6): 248-262.

[13] HERBERT H, MA Zhien, LIAO Shengbing. Effects of quarantine in six endemic models for infectious diseases [J]. Mathematical Bioscience, 2002, 180(1): 141-160.

[14] 鲁延玲，蒋国平，宋玉蓉. 自适应网络中病毒传播的稳定性和分岔行为研究 [J]. 物理学报，2013，62(13)：1-9.
LU Yanling, JIANG Guoping, SONG Yurong. Stability and bifurcation of epidemic spreading on adaptive network [J]. Acta Physica Sinica, 2013, 62(13): 1-9.

[15] BARABASI A L, ALBERT R. Emergence of scaling in random networks [J]. Science, 1999, 286(5439): 509-512.

（编辑　武红江）