

基于 SEIPQR 模型的工控蠕虫防御策略

潘洁¹, 叶兰², 赵贺³, 张鑫磊³

(1. 中国移动通信集团设计院有限公司, 北京 100080; 2. 中国移动通信集团, 北京 100032;
3. 中国移动通信集团采购共享服务中心, 北京 100053)

摘要: 随着社会的发展和技术的进步, 计算机病毒也发生了进化, 变得越来越复杂, 越来越隐蔽。其中蠕虫病毒更是最早的计算机病毒发展进化成为可以在工控系统上感染并进行传播的工控蠕虫病毒, 极大影响工业生产的安全。单一的网络隔离或者打补丁免疫, 已经跟不上蠕虫病毒的传播速度。针对该现状, 分析蠕虫病毒在工控系统上的传播方式以及特点, 在原有网络隔离和补丁的基础上提出一种针对工控蠕虫的防御策略, 以达到有效防御蠕虫病毒的目的。该防御策略基于传染病模型的基本思想提出了一个模拟蠕虫传播趋势的数学模型 SEIPQR。该模型包含易感染 (susceptible) 状态、暴露 (exposed) 状态、打补丁 (patched) 状态、感染 (infected) 状态、隔离 (quarantine) 状态以及免疫 (recovered) 状态 6 种状态, 创建模型的 6 种状态转换图, 对状态转换图得到微积分方程组, 在系统设备数量一定的情况下, 对方程组进行变换, 通过求解基本再生数 R_0 的方法对方程组进行求解, 并分析当暴露主机和感染主机的数量为 0 时模型的 6 种方程表达式, 根据 Routh-Hurwitz 准则得出当 $R_0 < 1$ 时, 系统是渐进稳定的; 当 $R_0 > 1$ 时, 系统是不稳定的。通过数值仿真对比在不同打补丁概率、不同隔离率以及不同感染率 3 种情况下 SEIPQR 模型的动力学特性, 并得到模型的无病平衡点和地方病平衡点。数据仿真结果表明, 在整个系统感染蠕虫病毒时, 对易感染设备及时地打补丁以及进行网络隔离可以有效抑制工控蠕虫的传播。

关键词: 工业控制网络; 工控蠕虫; 传染病模型; 数值仿真

中图分类号: TP393

文献标志码: A

doi: 10.11959/j.issn.2096-109x.2022032

Defense strategy of industrial control worm based on SEIPQR model

PAN Jie¹, YE Lan², ZHAO He³, ZHANG Xinlei³

1. China Mobile Group Design Institute Co., Ltd., Beijing 100080, China

2. China Mobile Group, Beijing 100032, China

3. China Mobile Procurement Shared Service Center, Beijing 100053, China

Abstract: Computer viruses keep evolving with the development of society and progress of technologies, and they become more complex and hidden. The worm virus is the earliest computer virus, which has evolved to an industrial control worm virus and caused a great impact on the safety of the industrial system. Neither the single network iso-

收稿日期: 2021-07-05; 修回日期: 2022-03-04

通信作者: 叶兰, yelan@chinamobile.com

引用格式: 潘洁, 叶兰, 赵贺, 等. 基于 SEIPQR 模型的工控蠕虫防御策略[J]. 网络与信息安全学报, 2022, 8(3): 169-175.

Citation Format: PAN J, YE L, ZHAO H, et al. The defense strategy of industrial control worm based on SEIPQR model[J]. Chinese Journal of Network and Information Security, 2022, 8(3): 169-175.

lation nor the patching immunity is unable to keep up with the spreading of the worm virus. The propagation mode and characteristics of the worm virus in the industrial control system were analyzed. Based on the related works of network isolation and patching, a defense strategy against the worm virus was proposed. This strategy was originated from the fundamental infectious disease model, and then a mathematics model (SEIPQR) was proposed to simulate the trend of worm virus propagation. The model included six situations: Susceptible, Exposed, Infected, Quarantine and Recovered. The state transition diagrams of the model was created, and the calculus equations were obtained from the state transition diagrams. Under the condition that the number of system equipment is fixed, the equations were transformed. The equations were solved by solving the basic regeneration number R_0 , and six equation expressions of the model were analyzed when the number of exposed hosts and infected hosts is zero. According to the principle of the Routh-Hurwitz, the system is asymptotically stable when $R_0 < 1$, and unstable if $R_0 > 1$. Then the dynamic characteristics of the SEIPQR model under different patching probability, different isolation rate and different infection rate were compared by numerical simulation. Furthermore, the disease-free equilibrium point and endemic equilibrium point of the model were obtained. The simulation results showed that, when the whole system is infected with worm virus, timely patching the susceptible devices and isolating the network can effectively inhibit the spread of industrial control worm virus.

Keywords: industrial control network, industrial control worm, epidemic model, numerical simulation

0 引言

工业互联网作为新一代信息技术与工业经济深度融合形成的新兴业态和应用模式,是实现产业数字化转型的关键基础。随着工业化与信息化进程的不断交叉融合,越来越多的信息技术应用到了工业控制领域,使工业控制系统与信息网络联系更加紧密。工业控制系统已经成为国家关键基础设施的重要组成部分,工业控制系统的安全关系到国家的战略安全。由于两化融合和工业 4.0 的影响,工业控制系统的网络信息安全成为研究热点,其中如何主动防御黑客对工控系统或工控网络的攻击成为备受关注的焦点。随着工业控制系统的不断开放和互联互通,工业控制系统及工业互联网设备的安全脆弱性逐渐凸显。通用软硬件和网络设施的广泛使用,打破了传统工业控制系统与信息网络的“隔离”,在不断促进工业互联网发展和壮大的同时,传统互联网所面临的安全问题逐渐渗透到工业互联网中。和普通的互联网相比,工业互联网的特征更加复杂,不仅涉及的设备种类更多更复杂,其布置的网点也更加密集,所以对它构成安全威胁的因素更多。在社会的各个领域中,新技术的应用范围越来越广,这些新的计算机技术对社会生产和经济的发展起到了极大的推动作用,但同时埋下了不少安

全隐患。近年来,越来越多网络安全攻击的矛头指向了工业控制系统。2010 年,伊朗的布什尔核电站遭到了蠕虫病毒 Stuxnet 的攻击^[1]。此后,有许多针对工业互联网的病毒被发现,如 Night Dragon^[2]、Flame^[3]、Duqu/Duqu2.0^[4]、Blaster^[5]和 BlackEnergy^[6]等。其中典型的可编程逻辑控制器 (PLC, programmable logic controller) 蠕虫 Blaster 只能存在于 PLC,并且可以在不涉及任何计算机的情况下通过西门子 SIMATIC S7-1200 的控制系统进行传播,PLC Blaster 可以扫描工业互联网以寻找新目标,进而攻击 PLC 并在受感染的 PLC 中完成自我复制。2019 年,委内瑞拉电网工业控制系统遭受攻击导致全国大规模停电^[7]。这些攻击行为不仅对工控系统本身造成了破坏,而且严重影响了人们正常的生产生活。

目前,应用于工业互联网的安全防御方法主要是被动防御技术,如防火墙、入侵检测/预防系统、数据泄露预防系统等。此类安全防御方法大多部署于网络边界,且工业互联网所面临的安全威胁大多来源于 IT (Internet technology) 网络,因此其在工业互联网与 IT 网络的边界处仍能起到较好的威胁检测作用。然而,这些传统防御方法在防护能力的静态性、防护措施的被动性和对于新的网络攻击的不适用性等方面的不足,导致

其已无法应对日趋严峻的网络攻击形势。此外,工业互联网本身在安全防御方面存在诸多脆弱性和行业特殊要求。例如,工控协议和工业控制系统均缺乏内置安全机制;工业控制系统处理能力较弱,具有系统更新较为滞后等特点。基于上述情况,为了解决工业互联网安全领域所面临的问题,需要从根本上了解工控蠕虫在工业互联网中的传播规律并提出相应的抑制策略。因此,对于工业互联网中蠕虫的传播行为进行建模分析尤为必要。

网络隔离就是一旦发现被蠕虫感染的主机设备就对其进行隔离,再对其进行修复,这样能减少被感染的主机设备继续感染其他设备的可能性。补丁是在网络安全领域中使用的一种修复技术,它可以为易受攻击的主机设备提供临时保护,使其在更新软件的过程中免于蠕虫的攻击。在此基础上,本文提出了一个传染病模型来分析蠕虫可能的传播趋势。恶意软件的传播与传染病的传播极为相似^[8],20世纪80年代,Cohen等^[9]先后借鉴研究传染病传播的方法,建立了研究网络恶意软件的动力学模型。在Code Red事件发生后,Staniford等^[10]率先基于SEM(simple epidemic model)对Code Red的传播行为进行了分析,模型很好地匹配了观测到的蠕虫上升期数据。为了了解蠕虫的传播行为,Rey等^[11]基于随机复杂网络建立了恶意软件的传播模型,模型是基于个体的并通过元胞自动机进行描述;Hosseini等^[12]针对无标度网络对蠕虫病毒的传播建立了理论模型,并且提出了模型的新版本;Kupennan和Agiza研究了小世界效应对蠕虫传播行为的影响^[13-14];Yuan^[15]基于仿真系统对蠕虫在工业复杂网络中的传播进行了模拟;近年来,有学者利用SIS(Susceptible Infected Susceptible)模型研究了恶意软件在移动电话间的传播过程^[16];基于SIS模型提出了僵尸网络的优化传播策略^[17];建立了一种高级的混合式P2P僵尸网络的传播模型^[18];苏飞等^[19]分析了一种能够在IPv6网络中大规模传播的混合式恶意软件的传播模型。

目前,对工控网络蠕虫的研究较少,由于

真实工业控制系统的网络较为复杂,以往的一些传播模型难以准确描述工控蠕虫实际的传播过程,并且少有针对恶意软件提出有效的对抗策略。因此,本文通过数学建模方法研究工控网络中蠕虫的传播规律,确定其中关键因素,从而构建合理的传播模型。由于蠕虫的传播过程非常复杂,其传播参数的变化对其传播过程具有巨大影响。目前,在抑制策略的研究中多采用数学建模和传播仿真的方法。由于恶意软件传播的动力方程的分析和求解困难,恶意软件传播动力系统中各参数的演化规律难以量化和分析。这就使网络本身的多变性对于恶意代码抑制策略的影响无法得到有效的定量分析,导致无法对抑制策略进行有效的预测,严重的甚至会导致系统失稳,影响工控网络的正常运行。为了研究蠕虫在工控网络中的传播特点和抑制策略,本文基于传染病模型的基本思想,在SEM模型的基础上提出了网络隔离和补丁的措施,并建立了相应的传染病模型来分析工控蠕虫的传播趋势和防御策略。

1 SEIPQR 模型

为了抑制蠕虫在工控网络中的传播,减少被蠕虫感染的工控设备的数量,一般的做法是先识别已经被蠕虫感染的工控设备,然后对被感染的工控设备进行免疫。随着网络带宽的持续增加以及黑客技术的不断提升,蠕虫的传播速度越来越快,对感染节点进行免疫的速度已经无法跟上蠕虫感染的速度。本文提出集隔离保护和打补丁于一体的蠕虫抑制策略来限制蠕虫在工控耦合网络中的传播。

1.1 模型的建立

首先使用入侵检测方法,通过入侵检测系统发现被蠕虫感染的工控设备。当入侵检测系统发现其被蠕虫感染后,立即通过断电等方式将其从网络中隔离,这样能有效防止其继续感染网络中的其他工控设备。对于易感染和暴露的设备,通过及时打补丁使其具有免疫的效果。即使它们没有被蠕虫感染,也可提前对其进行保护,预防其将来可能被蠕虫感染。当设备被隔离和打补丁后,会变为免疫状态。

根据上述思想, 模型中的设备可以分为以下 6 种状态。

1) 易感染 (susceptible) 状态: 工控设备存在漏洞, 容易遭受蠕虫攻击, 当蠕虫扫描发现后, 该设备就会处于暴露状态。

2) 暴露 (exposed) 状态: 工控设备暴露在外部网络环境中, 处于感染状态的主机有概率会被蠕虫感染。

3) 打补丁 (patched) 状态: 对于易感染和暴露的设备, 及时对其打补丁。

4) 感染 (infected) 状态: 设备已经被蠕虫感染并能感染网络中其他工控设备。

5) 隔离 (quarantine) 状态: 将被蠕虫感染的设备进行隔离, 使其从网络中暂时离开。

6) 免疫 (recovered) 状态: 设备通过隔离打补丁等方式获得对蠕虫的免疫力。

此外, 各个设备有一定的概率接入网络和离开网络。其中接入网络的易感染设备概率为 p , 接入网络的免疫设备概率为 $1-p$, 离开网络的概率为 μ 。这样可以使模型计算中保持总设备数量不变, 方便对蠕虫传播的趋势进行分析。为了形象地表示 SEIPQR 模型的状态转换过程, 结合以上的设备状态描述得到 SEIPQR 模型的状态转换图, 如图 1 所示。

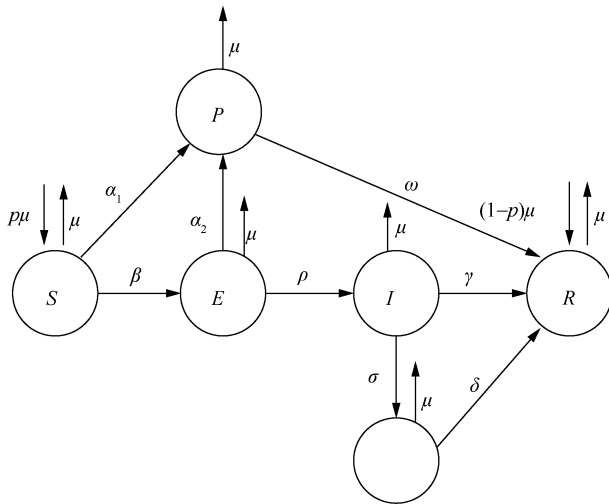


图 1 SEIPQR 模型状态转换图
Figure 1 State transition of the SIQMR model

根据状态转换过程, 可以得到 SEIPQR 模型的微分方程组。

$$\begin{cases} \frac{dS}{dt} = p\mu N - (\mu + \alpha_1)S(t) - \beta S(t)[E(t) + I(t)] \\ \frac{dP}{dt} = \alpha_1 S(t) + \alpha_2 E(t) - (\omega + \mu)P(t) \\ \frac{dE}{dt} = \beta S(t)[E(t) + I(t)] - (\alpha_2 + \rho + \mu)E(t) \\ \frac{dI}{dt} = \rho E(t) - (\sigma + \gamma + \mu)I(t) \\ \frac{dQ}{dt} = \sigma I(t) - (\mu + \delta)Q(t) \\ \frac{dR}{dt} = (1-p)\mu N + \gamma I(t) + \delta Q(t) + \omega P(t) - \mu R(t) \end{cases} \quad (1)$$

其中, N 为系统中总设备数量, β 为工控设备暴露的概率, α_1 和 α_2 分别是易感染设备和暴露设备成功打补丁的概率, ρ 为暴露设备被感染的概率, σ 为感染设备的隔离率, γ 为感染设备的免疫率, δ 表示隔离后设备变为免疫状态的概率, ω 表示打补丁后设备变为免疫状态的概率。

1.2 模型的平衡点

本节对模型的动力学特性进行推导, 进而分析蠕虫的传播特点。借鉴 Sen 等^[20]提出的求解基本再生数 R_0 的方法, 对本文模型的基本再生数进行求解并分析系统的无病平衡点。无病平衡点, 即暴露主机和感染主机的数量是 0。在无病平衡点状态下, 方程组(1)可以写成以下形式。

$$\begin{cases} \frac{dS}{dt} = p\mu N - (\mu + \alpha_1)S(t) - \beta S(t)[E(t) + I(t)] \\ \frac{dP}{dt} = \alpha_1 S(t) + \alpha_2 E(t) - (\omega + \mu)P(t) \\ \frac{dE}{dt} = \beta S(t)[E(t) + I(t)] - (\alpha_2 + \rho + \mu)E(t) \\ \frac{dI}{dt} = \rho E(t) - (\sigma + \gamma + \mu)I(t) \\ \frac{dQ}{dt} = \sigma I(t) - (\mu + \delta)Q(t) \end{cases} \quad (2)$$

令 $E(t) = I(t) = 0$, 代入上式中, 无病平衡点 $(S^*, E^*, I^*, Q^*, P^*)$ 可以表示为

$$\begin{cases} S^* = \frac{p\mu N}{\mu + \alpha_1} \\ E^* = I^* = Q^* = 0 \\ P^* = \frac{p\mu N \alpha_1}{(\mu + \omega)(\alpha_1 + \omega)} \end{cases} \quad (3)$$

定理 1 当基本再生数 $R_0 < 1$ 时, 系统(2)是渐近稳定的; 当 $R_0 > 1$ 时, 系统是不稳定的。

$$R_0 = \frac{\beta S^* (\mu + \gamma + \sigma + \rho)}{(\rho + \mu + \alpha_2)(\mu + \gamma + \sigma)} = \frac{pN\mu\beta(\mu + \gamma + \sigma + \rho)}{(\rho + \mu + \alpha_2)(\mu + \gamma + \sigma)(\mu + \alpha_1)} \quad (4)$$

证明 求出系统(2)的特征方程(5), 求解特征方程(5)可得其特征根有负实部, 即 $\lambda_1 = -(\mu + \alpha_1)$, $\lambda_2 = -(\mu + w)$ 和 $\lambda_3 = -(\mu + \delta)$, 以及 $(\lambda + \mu + \alpha_1) \cdot (\lambda + \mu + w)(\lambda + \mu + \delta)(\lambda^2 + c\lambda + d) = 0$ 的根。

$$\begin{pmatrix} \lambda + (\mu + \alpha_1) & 0 & \beta S^* & \beta S^* & 0 \\ -\alpha_1 & \lambda + (\mu + w) & \alpha_2 & 0 & 0 \\ 0 & 0 & \lambda + (\alpha_2 + \rho + \mu - \beta S^*) & \beta S^* & 0 \\ 0 & 0 & -\rho & \lambda + (\mu + \gamma + \sigma) & 0 \\ 0 & 0 & 0 & \sigma & \lambda + (\mu + \delta) \end{pmatrix} = 0 \quad (5)$$

其中

$$\begin{cases} c = \rho + 2\mu + \gamma + \sigma + \alpha_2 - \beta S^* \\ d = (\rho + \alpha_2 + \mu)(\mu + \gamma + \sigma) - \beta S^*(\mu + \gamma + \sigma + \rho) \end{cases} \quad (6)$$

当 $R_0 < 1$ 时, $d > 0$

$$\begin{aligned} \rho + \alpha_2 + \mu &> \frac{\beta S^* (\mu + \gamma + \sigma + \rho)}{(\mu + \gamma + \sigma)} > \beta S^* \\ c &= \rho + \alpha_2 + 2\mu + \gamma + \sigma - \beta S^* \\ c &> \rho + \alpha_2 + \mu - \beta S^* > 0 \end{aligned} \quad (7)$$

根据 Routh-Hurwitz 准则, 当且仅当特征根为负值时, 系统的无病平衡点是稳定的。可以得到, 当 $R_0 < 1$ 时, 系统(2)是渐进稳定的; 当 $R_0 > 1$ 时, 系统是不稳定的。

2 数值仿真实验

本节进行了数值实验以分析工控蠕虫的传播特点, 并展示了模型的动力学特性。在实验中, 不同的基本再生数 R_0 对应无病平衡点和地方病平衡点。仿真实验可以从动力学上验证推导的结果, 数值曲线和仿真曲线的拟合程度可以验证其准确性。为了

模拟蠕虫在网络中的传播, 实验中假设网络中节点总数为 $N = 1\,000\,000$ 。表 1 给出了无病平衡点的参数。

表 1 无病平衡点的参数
Table 1 Parameters for disease-free equilibrium

参数	数值
β	0.000 000 08
μ	0.000 5
p	0.2
γ	0.06
δ	0.000 000 1
σ	0.08
w	0.000 000 08

通过上文的推导可知, 当 $R_0 < 1$ 时, 系统存在无病平衡点。令 $\alpha_1 = 0.000\,6$, $\alpha_2 = 0.000\,01$, $\rho = 0.003$, 则 $R_0 < 1$ 。图 2 展示了系统的无病平衡状态, 即感染状态的主机数量为 0。图中实线是数值 (num) 结果, 虚线是仿真 (sim) 结果。可以看出二者的拟合程度较好, 这就可以验证上文推导结果的准确性。

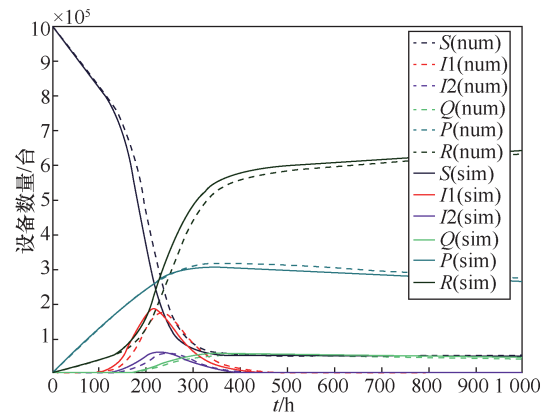


图 2 SEIPQR 模型的无病平衡点
Figure 2 The disease-free equilibrium of SEIPQR model

当 $R_0 < 1$ 时, 为了验证打补丁的效果, 分别令 $\alpha_1 = 0.001\,5$, $\alpha_1 = 0.002\,5$, $\alpha_1 = 0.003\,5$, 然后对相应的感染设备数量进行对比。在图 3 中可以看出, 当易感染设备成功打补丁的概率增大时, 感染设备的数量会明显下降。这说明对易感染设备打补丁可以有效抑制蠕虫的传播。

类似地, 实验还对比了参数 α_2 和隔离率 σ 变化时感染主机的数量。图 4 和图 5 分别展示了两组对比的结果, 从图中可以看出感染主机数量的变化不大, 这说明参数 α_2 和 σ 对于蠕虫传播的

影响并没有参数 α_1 大。由此可知, 在抑制蠕虫传播的过程中, 应当重点对易感染设备及时打补丁。

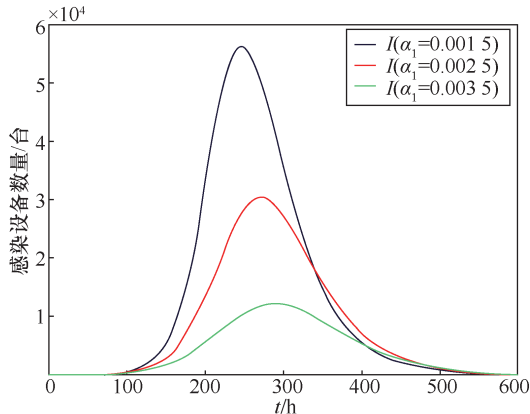


图 3 不同打补丁概率 α_1 的对比

Figure 3 Comparison of infected hosts with different parameter α_1

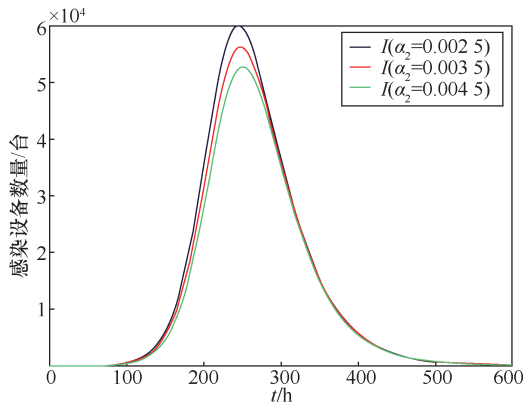


图 4 不同打补丁概率 α_2 的对比

Figure 4 Comparison of infected hosts with different parameter α_2

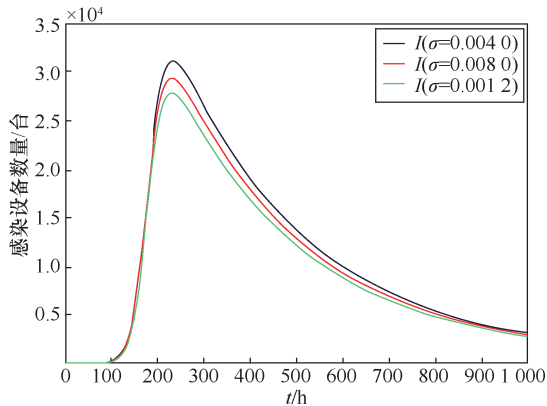


图 5 不同隔离率 σ 的对比

Figure 5 Comparison of infected hosts with different parameter σ

当 $R_0 > 1$ 时, 系统存在无病平衡点。令 $\alpha_1 = 0.0015$, $\alpha_2 = 0.0035$, $\rho = 0.023$, 则 $R_0 > 1$ 。图 6 展示了

模型的地方病平衡状态, 此时感染设备的数量不为 0。随后, 为了比较感染率 ρ 对蠕虫传播的影响, 分别令 $\rho = 0.002$, $\rho = 0.003$, $\rho = 0.004$ 进行对比实验。从图 7 中可以看出, 感染率越大, 感染设备的数量也就越多。这说明在蠕虫传播的过程中, 可以通过降低感染率来抑制蠕虫的传播。

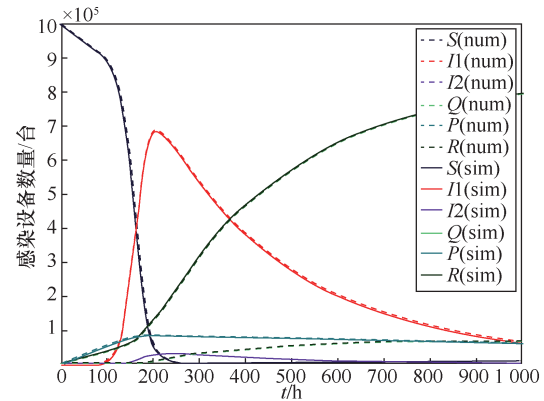


图 6 模型的地方病平衡点

Figure 6 The endemic equilibrium of SEIPQR model

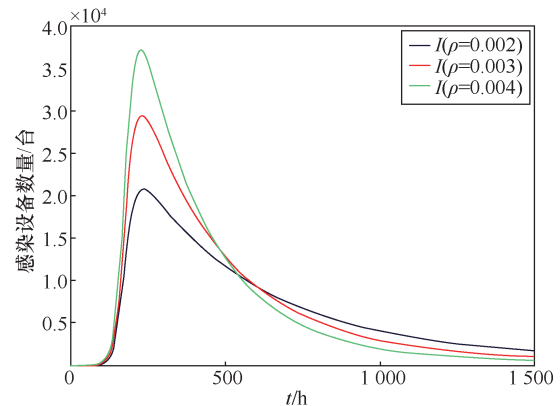


图 7 不同感染率 ρ 的对比

Figure 7 Comparison of infected hosts with different parameter ρ

根据以上实验结果和分析, 本文提出的 SEIPQR 模型可以准确地描述蠕虫在工控网络中的动力学特性。此外, 实验结果说明, 网络隔离和补丁策略可以有效抑制工控蠕虫的传播。本文在工控网络中, 通过建立基于网络隔离和补丁传播模型, 来分析影响蠕虫传播的关键因素, 可以准确地推测蠕虫攻击工控设施的过程, 从而有效地控制蠕虫的爆发。通过这种数学手段, 可以更加清晰地展示蠕虫的传播规律和全局性, 对蠕虫的了解更加深刻, 提出的对抗策略更具有实用性。在实际的防御过程中, 结合蠕虫传播模型, 决策者能够有效地提出蠕虫在工控

网络中的抑制策略。本文将传播动力学的研究方法应用到工控蠕虫传播与抑制的研究中, 为工业互联网安全领域的研究提供一种新的思路。

3 结束语

本文在工业互联网的背景中, 结合网络隔离和补丁提出了针对工控蠕虫传播的防御策略。在此基础上利用传染病模型的原理, 建立了 SEIPQR 模型。本文在该模型的基础上分析了工控蠕虫在工业互联网中的传播特点, 求解了动力系统的基本再生数, 并据此论证了蠕虫传播的无病平衡点。此外, 本文给出的数值仿真实验结果很好地验证了模型的准确性和防御策略的有效性, 参数对比实验也为如何更好地抑制工控蠕虫传播提供了可靠的参考。

参考文献:

- [1] TRAUTMAN L J, ORMEROD P C. Industrial cyber vulnerabilities: lessons from stuxnet and the Internet of Things[J]. Social Science Electronic Publishing, 2017, 72: 767-769.
- [2] GEWIRTZ D. Night dragon: cyberwar meets corporate espionage, J. Counterter[J]. Homeland Secur Int, 2011, 17(2): 6.
- [3] BENCATH B, PEK G, BUTTYAN L, et al. The cousins of stuxnet: Duqu, flame, and gauss, Future Int[J]. 2012, 4(4): 971-1003.
- [4] MAYNARD P, MCLAUGHLIN K, SEZER S. Modelling duqu 2.0 malware using attack trees with sequential conjunction[C]//Proceedings of the International Conference on Information Systems Security and Privacy. 2016: 465-472.
- [5] SPENNEBERG R, BRUGGEMANN M, SCHWARTKE H. Plc-blast: a worm living solely in the PLC[C]//Black Hat Asia 16, 2016.
- [6] RAVALL S. Blackenergy a threat to industrial control systems network security[J]. International Journal of Advanced Research in Engineering & Technologies. 2015, 2(12): 120-125.
- [7] 朱朝阳. 委内瑞拉大停电事故的背后[J]. 国家电网, 2019(5): 72-74.
ZHU C Y. Behind the blackout in Venezuela[J]. State Grid, 2019(5): 72-74.
- [8] LLOYD A L, MAY R M. Epidemiology: how viruses spread among computers and people[J]. Science, 2001, 292(5): 1316-1317.
- [9] COHEN F. Computer viruses: theory and experiments[J]. Computers & Security, 1987, 6(1): 22-35.
- [10] STANIFORD S, PAXSON V, WEAVER N. How to own the internet in your spare time[C]//USENIX Security Symposium. 2002: 14-15.
- [11] MARTÍN del R A, HERNÁNDEZ G, BUSTOS T A, et al. Advanced malware propagation on random complex networks[J]. Neurocomputing, 2021, 423: 689-696.
- [12] HOSSEINI S, ABDOLLAHI A M, RAHMANI T A. Agent-based simulation of the dynamics of malware propagation in scale-free networks[J]. Simulation, 2016, 92(7): 709-722.
- [13] KUPENNAN M, ABRAMSON G, NEWMAN M, et al. Small world effect in an epidemiological model[M]//The Structure and Dynamics of Networks. Princeton University Press, 2011: 489-492.
- [14] AGIZA H N, ELGAZZAR A S, Youssef S A. Phase transitions in some epidemic models defined on small-world networks[J]. International Journal of Modern Physics C, 2003, 14(6): 825-833.
- [15] YUAN L. The research on control strategy of worms spread in complex network in industry[J]. Advanced Materials Research, 2012, 487: 758-763.
- [16] JULI C M, LEGAND L B III, JOSEPH I Gill. Modelling the spread of mobile malware [J]. International Journal of Computer Aided Engineering and Technology, 2010, 2(1): 3-14.
- [17] SHANG Y. Optimal attack strategies in a dynamic botnet defense model[J]. Applied Mathematics & Information Sciences, 2012, 6(1): 29-33.
- [18] KALE A R, SHIRBHATE D D. An advanced hybrid peer-to-peer botnet[J]. International Journal of Wireless Communication, 2012, 2(1): 15-19.
- [19] 苏飞, 林昭文, 马严, 等. IPv6 网络环境下的蠕虫传播模型研究[J]. 通信学报, 2011, 32(9): 51-60.
SU F, LIN Z W, MA Y, et al. Research on worm propagation model in IPv6 networks[J]. Journal on Communications, 2011, 32(9): 51-60.
- [20] SEN M D L, NISTAL R, ALONSO-QUESADA S, et al. Some formal results on positivity, stability, and endemic steady-state attainability based on linear algebraic tools for a class of epidemic models with eventual incommensurate delays[J]. Discrete Dynamics in Nature and Society, 2019(7): 1-22.

[作者简介]



潘洁(1978—), 女, 浙江台州人, 中国移动通信集团设计院有限公司高级工程师、高级咨询设计师, 主要研究方向为通信网络安全。



叶兰(1979—), 女, 天津人, 中国移动通信集团工程师, 主要研究方向网络与数据安全。



赵贺(1982—), 男, 北京人, 中国移动通信集团采购共享服务中心工程师, 主要研究方向为网络与数据安全。



张鑫磊(1994—), 男, 北京人, 中国移动通信集团采购共享服务中心助理工程师, 主要研究方向为网络与数据安全。