计算机科学
COMPUTER SCIENCE

**物联网僵尸网络病毒的传播动力学模型与分析**

张翕然，刘万平，龙华

引用本文

张翕然，刘万平，龙华. 物联网僵尸网络病毒的传播动力学模型与分析[J]. 计算机科学, 2022, 49(6A): 738-743.

ZHANG Xi-ran, LIU Wan-ping, LONG Hua. Dynamic Model and Analysis of Spreading of Botnet Viruses over Internet of Things[J]. Computer Science, 2022, 49(6A): 738-743.

---

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.210300212

# 物联网僵尸网络病毒的传播动力学模型与分析

张翕然[1]　刘万平[1]　龙　华[2]
1 重庆理工大学计算机科学与工程学院　重庆 400054
2 重庆理工大学人工智能学院　重庆 400054
(xiranzhang@foxmail.com)

**摘　要**　随着信息技术的革新与进步,物联网技术在各个领域的应用呈现爆发式增长,然而大部分物联网设备却面临着黑客攻击的威胁。基于物联网设备的僵尸网络节点迅猛增长,导致了大规模DDoS攻击等网络安全事件,给物联网用户造成了极大损失。因此,研究以Mirai病毒为代表的一系列僵尸网络恶意威胁在物联网设备节点间的传播规律至关重要。首先,为了细致刻画物联网僵尸网络的形成过程,将物联网中的设备节点分为传输性设备节点和功能性设备节点,并通过对Mirai病毒感染机制的分析,提出了一个新颖的物联网病毒传播动力学模型——SDIV-FB模型。其次,从理论上计算了模型的传播阈值和平衡点,并对平衡点的稳定性进行了证明和分析。通过数值仿真实验验证了理论结果,并分析了模型参数对物联网病毒传播过程的影响。最后,确定了影响物联网僵尸网络病毒传播的重要参数,提出降低感染率和提高清除率可作为抑制物联网僵尸网络的有效控制策略。

**关键词**:物联网;Mirai病毒;僵尸网络;SDIV-FB模型;传播阈值
**中图法分类号**　TP393

## Dynamic Model and Analysis of Spreading of Botnet Viruses over Internet of Things

ZHANG Xi-ran[1],LIU Wan-ping[1] and LONG Hua[2]
1 School of Computer Science and Engineering,Chongqing University of Technology,Chongqing 400054,China
2 School of Artificial Intelligence,Chongqing University of Technology,Chongqing 400054,China

**Abstract**　With the innovation and progress of imformation technology,Internet of things(IoT) technology grows explosively growth in various fields. However,devices over these networks are suffering the threat of hackers. The rapid growth of IoT-Botnets in recent years leads to many security occurrences including large-scale DDoS attacks,which brings IoT users severe damages. Therefore,it is significant to study the spread of a group of botnets represented by Mirai virus among IoT networks. In order to describe the formation process of IoT botnet precisely,this paper classifies the nodes of IoT devices into transmission devices and function devices,and then proposes SDIV-FB,a novel IoT virus dynamics model,through the analysis of Mirai virus propagation mechanism. The spreading threshold and equiliabrium of the model system are calculated,and the stability of the equiliabria are proved and analyzed. Moreover,the rationality of the derived theories are proved through the numerical simulation experiments,and the effectiveness of the model parameters are verified as well. Finally,decreasing the infection rate and increasing the recovery rate are proposed in this paper as two effective strategies for controlling the IoT botnets.

**Keywords**　Internet of things (IoT),Mirai virus,Botnet networks,SDIV-FB model,Spreading threshold

## 1　引言

国际电信联盟于2005年正式提出了“物联网”(The Internet of Things,IoT)的概念[1],到如今其发展势头迅猛,已影响并渗透到社会生活的各个角落。物联网技术的广泛应用带来了极大的便利,然而其安全性问题也尤为突出。物联网设备大多是传感器交互型的,其数量庞大而且往往缺乏科学有效的管理,因此面临着网络攻击的威胁[1]。具有多连接能力的传输型节点也通常是恶意攻击的突破口,黑客能利用其极强的传输效率,迅速感染周围相连的设备。由于大多数IoT设备的初始配置相对简单,因此容易受到爆破攻击,而具有爆破攻击特性的僵尸网络病毒在物联网上的传播感染速度比传统互联网更快[2-5]。

分布式拒绝服务攻击(Distributed Denial of Service Attack)作为众多拒绝服务攻击方法中最强有力的方法之一,引起了无数互联网安全研究者的关注。如今,随着物联网的广泛部署和应用,由物联网设备节点引发的DDoS攻击更加频繁[6-8]。据2019物联网安全年报显示[9],物联网安全事件中超过50%都是IoT设备安全漏洞引起的,这些漏洞能被僵尸网络病毒恶意利用,从而造成严重后果。2016年,Mirai病毒在物联网上的爆发导致了数起物联网僵尸网络DDoS攻击事件[10]。美国计算机安全顾问网站Brian Krebs和法国云服务

基金项目:重庆市自然科学基金(cstc2021jcyj-msxmX0594);重庆市教委科学技术研究项目(KJQN201901101)
This work was supported by the Natural Science Foundation of Chongqing,China (cstc2021jcyj-msxmX0594) and Science and Technology Research Program of Chongqing Municipal Education Commission (KJQN201901101).
通信作者:刘万平(wpliu@cqut.edu.cn)

商 OVH 都先后受到 Mirai 病毒引发的大规模 DDoS 攻击，攻击流量最高达到 620Gbps 和 1.1Tbps[11]。特别是当 Mirai 源码被公开后，僵尸网络在线节点规模达到了 40 万[12]。此外，大规模 DDoS 攻击还阻塞了美国域名服务商，导致 Twitter，Netflix，GitHub 等上百个大型网站崩溃[13-15]。由此可见，物联网僵尸网络病毒具有极大的危害性。

物联网设备节点的 3 个显著特点非常有利于僵尸网络病毒的传播。

(1)设备脆弱性。一方面，随着物联网产业在近年来的井喷式发展，物联网设备供应商为抢占市场而忽视了设备安全性。另一方面，与传统互联网设备节点相比，由于物联网设备的硬件资源有限，因此部署的安全防护较弱。而且，不同类型物联网设备节点的功能具有较大差异，很难有统一的安全标准。

(2)设备持续在线。大部分 IoT 设备部署网络后会处于 24h 运行状态，特别是路由器、SD-WAN 设备、ADSL 调制解调器等传输性设备，这类设备在保证信息传输效率的同时，也更有利于恶意病毒的传播。

(3)缺乏合理的管理机制。物联网设备用户的安全意识较弱，通常设备不能正常工作后才会进行检查，使得物联网上的僵尸网络病毒更加顽固。

因此，需要构建相应的数学模型对物联网上的病毒传播进行仿真模拟研究，从而提出控制僵尸网络病毒的有效策略。近年来，许多学者通过借鉴经典的 SIR 仓室建模方法[16-18]，从不同角度了研究恶意代码在网络上的传播。Mishra 等提出了 SEIRS-V 模型[19]，模拟蠕虫病毒在无线传感器网络上的传播，该研究考虑了蠕虫病毒具有的自我复制、自动攻击等特点，与僵尸网络恶意代码的特点具有一定的相似性。Acarali 等在 WSNs 模型的基础上，提出了 IoT-SIS 模型[20]，将模型的适用范围推广到物联网设备。不同于传统的无线传感器设备，物联网设备具有更强的连接通信能力，因此在构建模型时，提出了全局随机扫描攻击是 IoT-WSNs 设备区别于传统 WSNs 设备的一种攻击方式，该攻击方式类似于 Mirai 病毒在物联网设备间的传播，即对设备的漏洞进行扫描并且暴力破解。

本文基于 Mirai 病毒的传播感染机制，借鉴无线传感器网络的节点分类特性，使用传播动力学建模方法，构建物联网僵尸网络恶意代码传播动力学模型。

## 2 物联网设备节点分类

本文将物联网设备节点分为两类，分别是功能性节点(Function Nodes)和传输性节点(Transmission Nodes)。一方面，功能性节点类似于无线传感器网络中的传感器节点(Sensor Nodes)，其作用是完成物联网与外界交互的各种功能，主要包括：网络摄像头、数字录像机、可穿戴设备、活动追踪器等。另一方面，传输性节点类似于无线传感器网络中的汇聚节点(Sink Nodes)，其主要作用是完成物联网节点间的信息存储与转发，包括：路由器、SD-WAN 设备、ADSL 调制解调器、部分 Linux 服务器等。

传输性节点是物联网中信息传输的主要节点，是物联网恶意代码传播和扩散的主要途径，因此一旦感染则具有很强的传染性。Mirai 病毒在传输性节点间的传播类似于蠕虫在无线传感网络上的传播。与此同时，物联网传输性节点具有的强通信能力使得 Mirai 病毒在物联网节点间的传播没有无线传感网络上的地域性和有限性。这使得平均场理论更适用于本文的研究。

为了与传输性节点间的感染方式进行区分，本文假设功能性节点的感染过程只受到与之接触的带有 Mirai 病毒的传输性节点的影响。除此之外，感染后的功能性节点不影响网络中恶意代码的传播，只作为潜伏态的僵尸网络节点，而不具有感染性。再结合功能性节点的特性，该类设备的连接具有随机性和任意性。因此我们将带有 Mirai 病毒传输性节点感染功能性节点的过程比作一类“易感染的种群”被网络环境中的“病毒因子”感染的过程[20]。

## 3 Mirai 僵尸网络病毒的感染机制

Mirai 病毒的传播过程包括 3 个部分：1)僵尸网络受控端(The Bot) 能够扫描周围的弱口令设备，同时也是僵尸网络中执行 DDoS 攻击的傀儡机；2)C&C 僵尸网络控制服务器(The Command and Control Server)对成功感染的僵尸节点进行监控和管理，同时也是下达 DDoS 攻击命令的控制端；3)Loader 加载服务器(Loader Server)登录被破解的物联网设备，加载和运行 Mirai 僵尸网络恶意代码。

僵尸网络感染、成型、攻击的过程大致可分为 4 步，如图 1 所示。

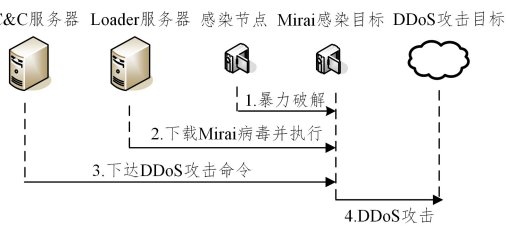


图 1 僵尸网络感染过程和攻击过程

Fig. 1 Botnet infection and attack process

(1)由 Bot 对扫描到的弱口令设备执行暴力破解，这一步被破解后的节点不具有感染性。

(2)由 Loader 服务器登录到被破解后的设备下载并运行 Mirai 病毒，完成该步骤的节点成为感染节点，具有传播恶意代码的能力。

(3)C&C 服务器下达 DDoS 攻击指令。

(4)收到攻击命令后的僵尸网络完成攻击。

## 4 模型的建立

传输性设备节点可分为 4 类：Susceptible nodes(易感染节点 $S$)、Delitescent nodes(潜伏态节点 $D$)、Infected nodes(感染态节点 $I$)和 Vaccinated nodes(免疫节点 $V$)，这样可用 SDIV 模型来描述传输性设备节点的状态转化。感染态 $I$-节点会对所有与之相连接的易感染 $S$-节点进行扫描和破解，我们假设平均每个感染态传输性设备对易感染态节点的破解成功率系数为 $\beta$，被成功破解后的易感染 $S$-节点将转化为不具有感染性的潜伏态 $D$-节点。由于 Mirai 病毒暴力破解的物联网设备不具有感染性，而只有在成功接收到 Loader 指令后，潜伏态设备才会从文件服务器上下载 Mirai 病毒，成功运行恶意代码后转化为感染态 $I$-节点，因此潜伏态 $D$-节点转化为感染态节点的概率记为 $\eta$。如果被感染的 $I$-节点被人为清除了恶意代码，并对该节点进行了重配置，则传输性 $I$-节点将变为免疫节点，记这个转化概率为 $\gamma$。当传输性设备处于免疫态时不具有传染性，该设备也不会被感染态传输设备再次

破解。然而，考虑到僵尸网络病毒具有更新换代的能力，传输型设备无法识别更新后的僵尸网络病毒。因此，免疫态 $V$-节点仍然会以概率 $\varepsilon$ 失去免疫，再次成为易感染 $S$-节点。

功能性设备节点可分为两类：Feeble nodes(易感染节点 $F$)和 Botnet nodes(潜伏节点 $B$)，这样可用 FB 模型描述功能性设备节点的状态转化。物联网的网络结构具有极强的不稳定性，特别是功能性节点的通信和连接具有随机性。为了与传输性设备间的连接方式进行区分，我们将易感染功能性 $F$-节点与感染态传输 $I$-节点的接触过程比作一类“易感染的种群”暴露在网络环境中的“病毒因子”之下的过程[21]，那么整个网络环境中的感染态传输性设备对易感染功能性设备的感染率系数为 $\lambda(1-e^{aI})$。功能性节点被感染后不具备感染性，但能潜伏作为僵尸网络中的一个僵尸节点。

考虑到模型中所有节点均表示物联网设备，因此在人为控制的情况下，我们假设所有节点有相同的出生率和死亡率 $b$，即网络上的总节点数保持不变，如图 2 所示。

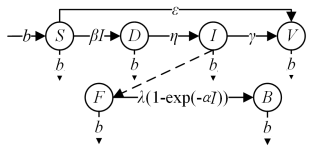


图 2 SDIV-FB 模型示意图

Fig. 2 Diagram of SDIV-FB model

在该模型中，用 6 个变量 $S(t)$，$D(t)$，$I(t)$，$V(t)$，$F(t)$ 和 $B(t)$ 分别表示 $S$ 节点、$D$ 节点、$I$ 节点、$V$ 节点、$F$ 节点和 $B$ 节点在传输节点数中的占比，则有以下关系式：

$$S(t)+D(t)+I(t)+V(t)=1 \tag{1}$$

$$\begin{cases}\dfrac{dS}{dt}=b+\varepsilon V-\beta SI-bS\\ \dfrac{dD}{dt}=\beta SI-\eta D-bD\\ \dfrac{dI}{dt}=\eta D-\gamma I-bI\\ \dfrac{dV}{dt}=\gamma I-\varepsilon V-bV\\ \dfrac{dF}{dt}=b-\lambda(1-e^{-aI})F-bF\\ \dfrac{dB}{dt}=\lambda(1-e^{-aI})F-bB\end{cases} \tag{2}$$

结合以上分析，虽然功能性节点对僵尸网络的形成有至关重要的作用，但 Mirai 病毒的传播过程是由传输性节点决定，系统(2)的动力学行为可以由以下子系统决定：

$$\begin{cases}\dfrac{dS}{dt}=b+\varepsilon V-\beta SI-bS\\ \dfrac{dD}{t}=\beta SI-\eta D-bD\\ \dfrac{dI}{dt}=\eta D-\gamma I-bI\\ \dfrac{dV}{dt}=\gamma I-\varepsilon V-bV\end{cases} \tag{3}$$

将式(1)带入式(3)，则式(3)可以转化为：

$$\begin{cases}\dfrac{dD}{dt}=\beta(1-D-I-V)I-(\eta+b)D\\ \dfrac{dI}{dt}=\eta D-(\gamma+b)I\\ \dfrac{dV}{dt}=\gamma I-(\varepsilon+b)V\end{cases} \tag{4}$$

其中系统(4)的初值属于集合：$\Omega=\{(D,I,V)\mid D,I,V\geqslant 0\cap D+I+V\leqslant 1\}$。令式(4)的右端为零，可以求得对应方程组的两个解，即系统(4)的两个平衡点：$(0,0,0)$ 和 $(D^*,I^*,V^*)$。其中：

$$\begin{cases}D^*=\dfrac{\gamma+b}{\eta}I^*=\dfrac{1-\dfrac{(\eta+b)(\gamma+b)}{\eta\beta}}{\dfrac{\eta}{\gamma+b}+\dfrac{\eta\gamma}{(\varepsilon+b)(\gamma+b)}+1}\\ I^*=\dfrac{1-\dfrac{(\eta+b)(\gamma+b)}{\eta\beta}}{\dfrac{\gamma+b}{\eta}+\dfrac{\gamma}{\varepsilon+b}+1}\\ V^*=\dfrac{\gamma}{\varepsilon+b}I^*=\dfrac{1-\dfrac{(\eta+b)(\gamma+b)}{\eta\beta}}{\dfrac{(\gamma+d)(\varepsilon+b)}{\eta\gamma}+\dfrac{\varepsilon+b}{\gamma}+1}\end{cases}$$

结合式(4)可以计算得到传播阈值为 $R_0=\eta\beta/(\eta+b)(\gamma+b)$，则当 $R_0>1$ 时非零平衡点在 $\Omega$ 内存在。

结合式(3)，整个传输型节点系统的平衡节点也有两个：无传播平衡点 $P(1,0,0,0)$ 和恶意代码存在平衡点 $Q(S^*,D^*,I^*,V^*)$，其中，$S^*=1-D^*-I^*-V^*$。

## 5 平衡点稳定性分析

**定理 1** 当 $R_0\leqslant 1$ 时，系统(3)的无传播平衡点 $P$ 是局部渐进稳定的。

证明：系统(4)的 Jacobi 矩阵为：

$$\begin{bmatrix}-\beta I-(\eta+b) & \beta(1-D-2I-V) & -\beta I\\ \eta & -(\gamma+b) & 0\\ 0 & \gamma & -(\varepsilon+b)\end{bmatrix}$$

代入平衡点 $P(0,0,0)$ 得到：

$$\begin{bmatrix}-(\eta+b) & \beta & 0\\ \eta & -(\gamma+b) & 0\\ 0 & \gamma & -(\varepsilon+b)\end{bmatrix}$$

其特征多项式为：

$$\lambda^3+(\theta_1+\theta_2+\theta_3)\lambda^2+(\theta_1+\theta_2+\theta_3+\theta_4+\theta_2\theta_3-\theta_4)\lambda+(\theta_1\theta_2\theta_3-\theta_1\theta_4)$$

其中：

$$\begin{cases}\theta_1=\varepsilon+b\\ \theta_2=\eta+b\\ \theta_3=\gamma+b\\ \theta_4=\eta\beta\end{cases}$$

根据劳斯判据得到 Routh 表：

$$\begin{array}{c|c}\lambda^3 & 1\\ \lambda^2 & \theta_1+\theta_2+\theta_3\\ \lambda^1 & \theta_1\theta_2+\theta_1\theta_3+[(\theta_2+\theta_3)(\theta_2\theta_3-\theta_4)]/(\theta_1+\theta_2+\theta_3)\\ \lambda^0 & \theta_1(\theta_2\theta_3-\theta_4)\end{array}$$

由 $R_0\leqslant 1$ 可得 $\eta\beta/(\eta+b)(\gamma+b)$，则有 $\theta_2\theta_3>\theta_4$。

根据劳斯判据，系统(4)的平衡点$(0,0,0)$是局部渐进稳定的，则系统(3)的无传播平衡点 $P(1,0,0,0)$ 也是局部渐进稳定的。定理 1 得证。

当系统(3)处于无毒平衡点状态时，感染态传输性节点的数量趋向于零，模型(1)中的被感染的功能性节点也趋向于零，僵尸网络将不再存在。

**定理 2** 当 $R_0>1$ 时，系统(3)的恶意代码存在平衡点 $Q$ 是局部渐进稳定的。

证明：非零平衡点$(E^*,I^*,R^*)$的 Jacobi 矩阵为：

$$\begin{bmatrix} -\beta I^* -(\eta+b) & \beta(1-D^*-2I^*-V^*) & -\beta I^* \\ \eta & -(\gamma+b) & 0 \\ 0 & \gamma & -(\varepsilon+b) \end{bmatrix}$$

其特征多项式为 $x^3+a_1x^2+a_2x+a_3=0$；多项式系数分别为：

$$\begin{cases} a_1=\Delta_1+\Delta_2+\Delta_3 \\ a_2=\Delta_1\Delta_2+\Delta_2\Delta_3+\Delta_1\Delta_3-\Delta_4 \\ a_3=\Delta_1\Delta_2\Delta_3-\Delta_2\Delta_4+\gamma\eta\beta I \end{cases}$$

其中：

$$\begin{cases} \Delta_1=\beta I^*+(\eta+b) \\ \Delta_2=\varepsilon+b \\ \Delta_3=\gamma+b \\ \Delta_4=\eta\beta(1-D^*-2I^*-V^*) \end{cases}$$

得到：

$$\begin{aligned} &a_1a_2-a_3 \\ &=(\Delta_1+\Delta_2+\Delta_3)(\Delta_1\Delta_2+\Delta_2\Delta_3+\Delta_1\Delta_3-\Delta_4)- \\ &\quad \Delta_1\Delta_2\Delta_3+\Delta_2\Delta_4-\gamma\eta\beta I^* \\ &=\Delta_1^2(\Delta_2+\Delta_3)+\Delta_2^2(\Delta_1+\Delta_3)+\Delta_3^2(\Delta_1+\Delta_2)+ \\ &\quad 2\Delta_1\Delta_2\Delta_3-\Delta_4(\Delta_1+\Delta_3)-\gamma\eta\beta I^* \\ &=(\beta I^*+\eta+b)^2(\varepsilon+\gamma+2b)+(\varepsilon+b)^2(\beta I^*+\eta+\gamma+ \\ &\quad 2b)+(\gamma+b)^2(\beta I^*+\eta+\varepsilon+2b)+2\beta I^*(\varepsilon+b)(\gamma+b)+ \\ &\quad 2(\varepsilon+b)(\eta+b)(\gamma+b)+\eta\beta I^*(\beta I^*-\eta-2b)+(\eta\beta^2 I^*+ \\ &\quad \eta^2\beta+\eta\beta\gamma+2b\eta\beta)*(I^*+D^*+V^*-1) \end{aligned}$$

整理简化后，结合式(1)可以得到 $a_1a_2-a_3>0$。

根据 Hurwitz 定理：

$$|a_1|>0,\ \begin{vmatrix} a_1 & 1 \\ a_3 & a_2 \end{vmatrix}>0,\ \begin{vmatrix} a_1 & 1 & 0 \\ a_3 & a_2 & 1 \\ 0 & 0 & a_3 \end{vmatrix}>0$$

可知系统(4)的平衡点$(D^*,I^*,V^*)$是局部渐进稳定的。因此系统(3)的恶意代码平衡点 $Q(S^*,D^*,I^*,V^*)$也具有局部渐进稳定性。同时，我们注意到，当恶意代码存在平衡点 $Q$ 且它是局部渐进稳定时，功能性节点的状态为$(F^*,B^*)$，于是由系统(2)可以获得：

$$F^*=\frac{b}{\lambda(1-e^{-aI^*})+b}$$

$$B^*=\frac{\lambda(1-e^{-aI^*})F^*}{b}$$

可知$(F^*,B^*)$的值被唯一确定下来，定理 2 得证。

当系统(4)处于有毒平衡态时，网络中存在稳定数量的感染态传输性节点，同时被感染的功能性节点的数量趋于稳定，僵尸网络将一直存在。

## 6 数值仿真实验

本节将对上述建立的数学模型进行数值仿真实验和分析，模拟 Mirai 病毒的传播过程。实验以传播阈值 $R_0$ 是否大于 1 作为切入点，验证第 5 节中结论的正确性，重点分析感染率 $\beta$ 和清除率 $\gamma$ 等参数对 Mirai 病毒传播的影响。同时结合系统(2)进行建模仿真，模拟僵尸网络的形成过程，重点分析 Mirai 病毒在传输性节点中的感染程度对僵尸网络最终规模的影响。为了验证各项参数对恶意代码传播的影响，设传输性节点共有 $N_1=10\,000$ 个；同时结合物联网的特性，假设功能性节点共有 $N_2=40\,000$ 个。设 $S(t),D(t),I(t),V(t)$分别是 $S,D,I,V$ 节点在所有传输性节点中的占比，即：$S(t)+D(t)+I(t)+V(t)=1$。同时令 $F(t),B(t)$分别表示 $F$ 节点和 $B$ 节点的占比。为了更好地模拟物联网设备节点间的状态转化，在没有特殊说明的情况下，默认初值分别为：$S(0)=0.6,D(0)=0.25,I(0)=0.15,V(0)=0$。

实验 1　默认初值情况下，取 $\beta=0.3,\varepsilon=0.4,\eta=0.6,\gamma=0.2,b=0.1$，计算得到 $R_0=0.856<1$。由图 3 可知，Mirai 病毒传播过程最终将趋近于无毒平衡点。同时可以注意到，在传播初期 I-节点增加速度极快，因为 Mirai 病毒在传输性节点中的潜伏期极短，即被暴力破解后的目标 IoT 设备会很快地从 Loader 服务器上下载 Mirai 病毒并在短时间内运行。但是，由于我们假设恶意代码的感染率较低，最终感染节点全部消亡。图 4 给出了不同初值情况下 $D(t),I(t),V(t)$的变化规律，它们均收敛于无毒平衡点。

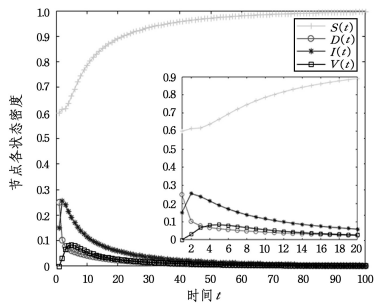


图 3　参数 $\beta=0.3,\varepsilon=0.4,\eta=0.6,\gamma=0.2,b=0.1$ 时，传输性节点系统的演化

Fig. 3　Evolution of transmission system when $\beta=0.3,\varepsilon=0.4,\eta=0.6,\gamma=0.2,b=0.1$

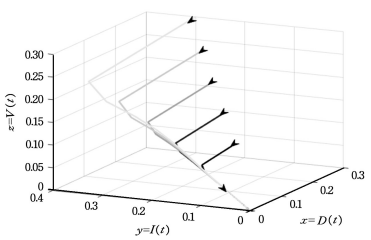


图 4　不同初值下$(D,I,V)$趋于无传播平衡点 $P$ 的演化过程

Fig. 4　Evolution of node system with different initial value$(D,I,V)$

实验 2　默认初值情况下，取 $\beta=0.7,\varepsilon=0.4,\eta=0.6,\gamma=0.2,b=0.1$，计算得到 $R_0=2>1$。由图 5 可知，模型将最终在有毒平衡点(0.50，0.13，0.26，0.11)处于稳定。可以注意到，当 Mirai 病毒的感染概率提升以后，$S$ 节点会在短时间内迅速减少。大约在时间 $t=20$ 后 $S$ 节点占比趋于稳定，而稳定后 $S$ 节点数大约为总节点数的 50%。这解释了一个重要的现实意义，即在 Mirai 病毒开始感染后，如果绝大部分物联网使用者和管理者没有提出相应的对策，那么近四成的传输性节点将在极短的时间内失去安全性，即恶意代码完成传播并形成稳定的过程会很快。

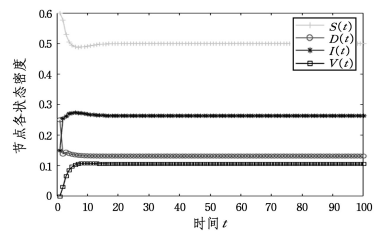


图 5　参数 $\beta=0.7,\varepsilon=0.4,\eta=0.6,\gamma=0.2,b=0.1$ 时，传输性节点系统的演化

Fig. 5　Evolution of transmission node system when $\beta=0.7,\varepsilon=0.4,\eta=0.6,\gamma=0.2,b=0.1$

图 6 给出了不同初值情况下 $D(t)$, $I(t)$, $V(t)$ 的变化规律，均收敛于有毒平衡点(0.50, 0.13, 0.26, 0.11)。

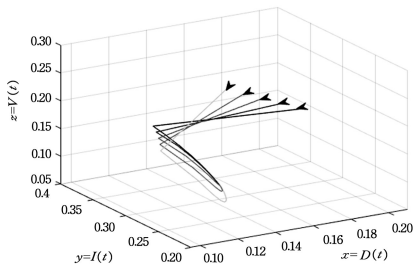


图 6 不同初值下 $(D, I, V)$ 恶意代码趋于存在平衡点 $Q$ 的演化

Fig. 6 Evolution of malicious codes tend to have equilibriun $Q$ with different initial values

实验 3 默认初值情况下，取参数 $\varepsilon=0.4$, $\eta=0.6$, $\gamma=0.2$, $b=0.1$，感染率 $\beta$ 作为变量。如图 7 所示，感染率的变化对于 Mirai 病毒的传播具有一定影响。从 $\beta=0.7$ 到 $\beta=0.3$ 的匀速减小过程中，$I$ 节点的数量变化明显。其现实指导意义在于，当我们为传输性节点设立防火墙网关时，能够有效限制恶意代码的传播，从而控制被感染节点的数量。再者，物联网设备在投入使用时，进行高强度的安全配置，而不是使用弱口令，也能有效减小恶意代码传播的范围。

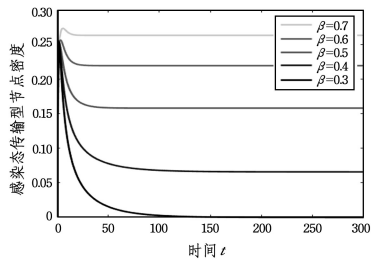


图 7 变量 $\beta$ 取不同值时感染态传输性节点的占比演化

Fig. 7 Evolution of transmission node proportion in infected state with different $\beta$

实验 4 默认初值情况下，取参数 $\beta=0.7$, $\varepsilon=0.4$, $\eta=0.6$, $b=0.1$，清除率 $\gamma$ 作为变量。如图 8 所示，清除率的变化对 Mirai 病毒的传播具有一定影响。从 $\gamma=0.2$ 到 $\gamma=0.8$ 的匀速增加过程中，$I$ 节点的数量占比明显减少。其中在 $\gamma$ 匀速增加的开始阶段，$I$ 节点的减少更为显著。其现实意义在于，当物联网用户面对僵尸恶意代码传播时，可以及时地重配置物联网设备节点或者在部分关键物联网设备上安装杀毒软件。这样能够有效地防止僵尸网络的形成。另外，普及物联网威胁的防控策略也是一种有效的预防方式。在一定范围内执行感染后的清除措施是高效的。同时，我们在实验过程中增加对比项 $\gamma=0$，揭示了在感染恶意代码后，若不加以行动，感染情况则会加剧。

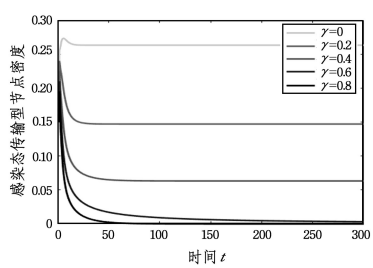


图 8 变量 $\gamma$ 取不同值时感染态传输性节点的占比演变过程

Fig. 8 Evolution of transmission nodes proportaion in infected state with different parameter $\gamma$

根据第 5 节对系统(2)的分析，在传输性节点的演化过程确定的基础上，模拟功能性节点的感染过程和僵尸网络的形成过程。用 $I$ 节点的个数加上 $B$ 节点的个数表示最终僵尸网络节点的个数。

实验 5 考虑 $F(0)=N_2=40000$, $B(0)=0$。取传输性节点对功能性节点的感染系数 $\lambda=0.9$, $a=0.01$, $b=0.1$。如图 9 所示，取实验 1 中的参数设置即 $\beta=0.3$, $\varepsilon=0.4$, $\eta=0.6$, $\gamma=0.2$, $b=0.1$。随着传播的进行，功能性节点的状态也趋于稳定，所有被感染节点数趋于 0，僵尸网络逐渐消亡。如图 10 所示，取实验 2 中的参数设置 $\beta=0.7$, $\varepsilon=0.4$, $\eta=0.6$, $\gamma=0.2$, $b=0.1$。随着 $I$ 节点的增加，$B$ 节点也迅速增加，可以看出，在感染出现后，僵尸网络成型速度极快，其规模高达 17000 个节点。综上，传输性设备的安全性是僵尸网络成型与否的关键所在。因此，对部分特殊的传输性设备节点(如路由器、SD-WAN 设备、ADSL 调制解调器)需要重点提升其安全性能。

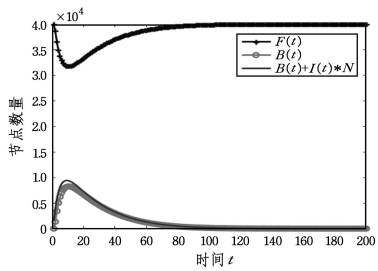


图 9 参数 $\beta=0.3$, $\varepsilon=0.4$, $\eta=0.6$, $\gamma=0.2$, $b=0.1$ 时，功能性节点系统的演化和僵尸网络的形成

Fig. 9 Evolution of function system and formation of botnet when $\beta=0.3$, $\varepsilon=0.4$, $\eta=0.6$, $\gamma=0.2$, $b=0.1$

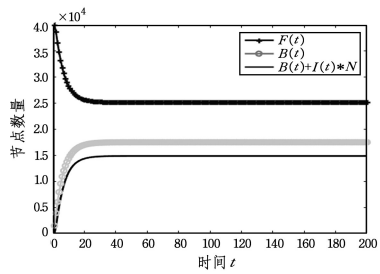


图 10 参数 $\beta=0.7$, $\varepsilon=0.4$, $\eta=0.6$, $\gamma=0.2$, $b=0.1$ 时，功能性节点系统的演变和僵尸网络的形成

Fig. 10 Evolution of function system and formation of botnet when $\beta=0.7$, $\varepsilon=0.4$, $\eta=0.6$, $\gamma=0.2$, $b=0.1$

**结束语** 本文首先探讨了 Mirai 僵尸网络病毒在物联网上的传播机制，进而利用数学建模法建立了 SDIV-FB 传播模型，计算出平衡点并分析了其稳定性。通过理论分析，得出了模型的传播阈值 $R_0$。通过 MATLAB 数值仿真实验验证了：传播阈值 $R_0 \leqslant 1$ 时，最终病毒将从物联网中消失，僵尸网络逐渐消亡；当传播阈值 $R_0 > 1$ 时，病毒的传播会一直存在于物联网中，僵尸网络也会一直存在。传播阈值 $R_0$ 的现实指导意义在于，物联网安全防御方需要尽可能地采取有效措施来降低传播阈值，才能有效遏制僵尸网络的形成。本文在实验阶段验证了降低传播阈值的有效方法是尽可能地降低感染率，并在一定范围内提高清除率。

从 $R_0$ 的表达式可以看出，当网络节点数量和僵尸网络病毒的种类固定时(出生率死亡率 $b$、节点转化率 $\eta$ 均为常数)，

影响病毒传播和僵尸网络形成速度的参数分别是感染率 $\beta$ 和清除率 $\gamma$。

(1)降低感染率 $\beta$

感染率越低，传播阈值就越小，也就越不利于物联网病毒的传播。结合实际，要抑止僵尸网络的形成，通常可以采取的有效策略是为每一个长时间持续在线的传输性节点配置网关和防火墙，并且，在接入网络前重新更改口令，关掉不必要的端口。这些方法极大地限制了感染态传输性节点传播恶意代码的能力，同时也提高了未感染的传输性节点的抗性，有效地降低了整个系统的传播阈值。

(2)提高清除率 $\gamma$

清除率越高，传播阈值也越小，使得物联网病毒趋于消亡。结合实验阶段的结果可知，当清除率在一定范围内提高时，感染态传输性节点的占比下降趋势加剧，当超过一定范围继续提高清除率，感染态传输性节点的占比下降趋势开始放缓。因此需要在一定合理的范围内提高清除率，例如：按一定策略周期性地对部分节点进行重配置，或者对最活跃的部分传输性节点进行更频繁的监测，而不必对每一个节点进行实时监控。这种提高清除率的方式在大规模物联网节点的情况下具有更高的性价比，同时也能有效地降低传播阈值。

本文的研究表明，物联网病毒的传播和僵尸网络形成的速度都极快，在短时间就能够达到稳定状态。传播阈值 $R_0$ 的大小直接影响着最终的稳定状态，而影响传播阈值大小的行为有降低感染率这类“预防”措施和提高清除率这类“治疗”措施。一方面，预防措施需要尽可能对所有传输性节点进行安全防护部署，确保在传播源头上得到有效遏制。另一方面，治疗措施则需要有针对性地对部分传输性节点进行监测和管理，确保能效地避免僵尸网络的形成。

## 参 考 文 献


[1] PEÑA-LÓPEZ I. ITU Internet report 2005:the Internet of things[R]. Geneva:ITU,2005.

[2] ANGRISHI K. Turning internet of things (iot) into Internet of vulnerabilities (iov):Iot botnets[J]. arXiv:1702.03681,2017.

[3] BERTINO E,ISLAM N. Botnets and internet of things security [J]. Computer,2017,50(2):76-79.

[4] KAMBOURAKIS G,KOLIAS C,STAVROU A. The mirai botnet and the iot zombie armies[C]// IEEE Military Communications Conference (MILCOM). 2017:267-272.

[5] JI Y,YAO L,LIU S,et al. The study on the botnet and its prevention policies in the internet of things[C]// 2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design (CSCWD). IEEE,2018:837-842.

[6] JERKINS J A,STUPIANSKY J. Mitigating IoT insecurity with inoculation epidemics[C]// Proceedings of the ACMSE 2018 Conference. 2018:1-6.

[7] JIAO D. Inventory of the most serious DDoS attacks in 2016 [J]. Computer and Network,2016,42(24):48-50.

[8] XIAO J C. Eight DDoS attacks affecting enterprise IoT security [J]. Computer and network,2017,43(10):56-57.

[9] WANG H L. DDoS attacks grew wildly in the first- half of 2017 [J]. Computer and Network,2017,43(23):53.

[10] ZHANG X,ZHANG K L,SANG H Q,et al. 2019 IoT Security Annual Report[J]. Information Security an-d Communication Confidentiality,2020(1):45-62.

[11] MMD-0055-2016-Linux/PnScan, ELF worm that still circles around[J/OL]. The MalwareMustDie Blog,2016. https://blog.malwaremustdie.org/2016/08/mmd-0054-2016-pnscan-elf-worm-that.html.

[12] GOODIN D. Record-Breaking DDoS Reportedly Delivered by > 145K Hacked Cameras[J/OL]. Ars Technica. http://arstechnica.com/security/2016/09/botnet-of-145K-cameras-reportedly-deliver-internets-biggest-ddos-ever.

[13] WILLIAMS C. You Can Now Rent a Mirai Botnet of 400,000 Bots[J/OL]. Bleeping Computer. https://www.bleepingcomputer.com/news/security/you-can-now-rent-a-mirai-botnet-of-400-000-bots.

[14] LIU W,ZHONG S. Web malware spread modelling and optimal control strategies[J]. Scientific Reports,2017,7(1):1-19.

[15] WILLIAMS C. Today the Web Was Broken by Countless Hacked Devices-Your 60-Second Summary [J/OL]. www.theregister.co.uk/2016/10/21/dyn_dns_ddos_explained.

[16] LI B S,CHANG A Q,ZHANG J X. IoT botnets seriously threaten network infrastructure security-analysis of Dyn company's botnet attack[J]. Information Security Research,2016,2(11):1042-1048.

[17] LIU W,ZHONG S. Modeling and analyzing the dynamic spreading of epidemic malware by a network eigenvalue method[J]. Applied Mathematical Modelling,2018,63:491-507.

[18] LIU W,WU X,YANG W,et al. Modeling cyber rumor spreading over mobile social networks:A compartment approach[J]. Applied Mathematics and Computation,2019,343:214-229.

[19] 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.

[20] ACARALI D,RAJARAJAN M,KOMNINOS N,et al. Modelling the spread of botnet malware in IoT-based wireless sensor networks[J]. Security and Communication Networks,2019.

[21] BREBAN R,DRAKE J M,STALLKNECHT D E,et al. The role of environmental transmission in recurrent avian influenza epidemics[J]. PLoS Comput. Biol.,2009,5(4):e1000346.


**ZHANG Xi-ran**, born in 1994, postgraduate. His main research interests include Internet of things virus and epidemic models.

**LIU Wan-ping**, born in 1986, Ph.D, associate professor, research supervisor, is a member of China Computer Federation. His main research interests include cyberspace security dynamics and information security.