移动无线网络
蠕虫传播与防御

陈志德　王　孟◎著

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

移动无线网络蠕虫传播与防御

陈志德　王　孟　著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书首先介绍了移动蠕虫与良性蠕虫相关研究背景、研究意义、蠕虫传播模型和良性蠕虫对抗等技术的研究现状，并阐述本书研究的必要性和重要性；其次，综合考虑节点地址隐藏技术、大量移动节点、网络异质性对蠕虫传播与对抗的影响等因素，提出无线网络双蠕虫交互的建模，并给出仿真分析；再次，提出 N 蠕虫和变异蠕虫的相关传播模型；最后，提出了基于移动良性蠕虫的控制修复机制，并采用划分的思想对移动社交网络中节点进行建模与分析。本书对移动无线网络蠕虫传播与防御机制研究具有一定借鉴意义。

本书可作为高等院校计算机等专业高年级教材，也可供相关专业和工程技术领域的从业及研究人员参考阅读。

图书在版编目（CIP）数据

移动无线网络蠕虫传播与防御 / 陈志德，王孟著. —北京：电子工业出版社，2017.3
ISBN 978-7-121-30576-4

Ⅰ. ①移… Ⅱ. ①陈… ②王… Ⅲ. ①计算机病毒—防治 Ⅳ. ①TP309.5

中国版本图书馆 CIP 数据核字（2016）第 296591 号

责任编辑：董亚峰　　特约编辑：刘广钦
印　　刷：三河市华成印务有限公司
装　　订：三河市华成印务有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：720×1 000　1/16　印张：10.75　字数：268 千字
版　　次：2017 年 3 月第 1 版
印　　次：2017 年 3 月第 1 次印刷
定　　价：39.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：（010）88254694。

前 言

蠕虫传播研究一直是我们很关注的一个课题，根据市场研究机构 Gartner 预计，全球联网设备的数量到 2020 年将增加至 260 亿台左右。全球每时每刻都发生着因为无线网络蠕虫攻击所造成的重大损失事件。如果恶意黑客入侵家庭智能系统，或在其攻克的网络中投入大量的病毒和恶意蠕虫，会直接或间接地造成难以估量的经济财产损失。

由于移动网络固有的共享、开放和广泛等特性，使得基于各类平台的系统本身的弱点得以暴露，随之出现越来越多的安全问题。移动智能设备的普及和移动网络的发展相互促进，传统的杀毒技术对具有移动特性的移动网络显得无能为力。如何预防和控制蠕虫随时可能带来的威胁，显得越来越重要。

趋势表明，在当前的移动网络安全形势下，企业和个人应该继续强化包括移动设备安全防护在内的网络安全措施，以保证网络环境的安全。

本书首先对移动蠕虫传播和良性蠕虫传播的相关研究背景和研究意义进行了简述，并介绍了蠕虫传播模型及良性蠕虫对抗等技术的研究现状，阐述本书研究的必要性和重要性；其次，综合考虑节点地址隐藏技术、大量移动节点、网络异质性对蠕虫传播与对抗的影响等因素，提出无线网络双蠕虫交互的建模，并给出仿真分析；再次，提出 N 蠕虫和变异蠕虫的相关传播模型；最后，根据社交网络的发展情况提出基于移动良性蠕虫的控制修复机制，并采用划分的思想对移动社交网络中节点进行建模与分析。

维护一个网络的安全性是一个长期的工程，需要对网络的信息有实时的了解，可结合良性蠕虫渗透测试原理与传播模型建模规律，来分析蠕虫传播的路径与可能存在的风险，为预防蠕虫产生危害做好准备。

作 者

2016 年 11 月 8 日

目 录

第 1 章

绪 论

1.1 研究背景与意义

随着计算机软、硬件技术和物联网技术的飞速发展，无线网络凭借灵活的移动性、方便的扩展性、良好的兼容性等优势，引起人们越来越多的关注和重视。近年来，随着无线网络技术的日益成熟，该技术已被广泛地应用到国防军事、灾害救援、环境监测、空间探索等众多领域，并且在各方面都提供了快捷的网络部署和业务承载方案，其重要性和意义已得到众多国家和团体的肯定。2003 年美国《技术评论》杂志将无线传感器网络评为将会给人类带来深远影响的十大新兴技术之首。我国国务院 2006 年发布的《国家中长期科学和技术发展规划纲要（2006—2020 年）》也指出要优先支持此类网络的研究和应用[1]。

由于无线网络在移动设备和传输介质方面的特殊性，相比传统的 Internet 及移动 IP 网络，无线网络更加脆弱，更容易遭到攻击。随着无线网络应用的越来越广泛，无线网络面临的安全问题也越来越凸显[2~4]。首先，由于无线网络不需要固定的基础设施，所以，典型的安全措施不再适用；开放的无线传输信号很容易受到窃听、伪造、篡改、拒绝式服务等攻击；暴露的无线节点很容易受到攻击者的控制和破坏；此外，大范围无规则移动的无线节点，使得无线网络的拓扑结构时刻发生变化，致使管理者很难定位移动节点。一旦移动节点被恶意病毒感染，其感染范围将无限扩大。这些现实状况使得无线网络的安全面临着越来越严峻的挑战。

根据市场研究机构 Gartner 的预计，全球联网设备的数量到 2020 年将增加至 260 亿台左右。全球每时每刻都发生着因为无线网络蠕虫攻击所造成的重大损失事件。如果恶意黑客入侵家庭智能系统，或在其攻克的网络中投入大量的病毒和恶意蠕虫，会直接或间接造成难以估量的经济财产损失。在无线网络技术飞速发展的今天，在享受无线网络技术带来的便捷生活的同时，我们应该清楚地意识到黑客的攻击技术也在快速发展着，并且各种各样的网络病毒及其变种正严重地威胁着无线网络的安全。防御无线网络中恶意蠕虫及其变种的攻击成为重要的研究问题。

移动网络是无线网络系统的重要组成部分，人们每天使用移动设备与他人通信。而近年来随着 3G/4G 网络和智能手机的应用普及，以及手机用户量的快速增加，手机病毒呈现泛滥的趋势，移动手机网络平台受到恶性蠕虫的威胁越来越严重。食人鱼（Cabir）蠕虫[5]是第一个智能手机蠕虫，在 2004 年 6 月被截获，该病毒会感染采用了 Symbian 手机操作系统的诺基亚手机。在手机被感染后，该病毒就会启用手机蓝牙对邻近的其他手机进行扫描，在发现漏洞手机后，该病毒就会复制自己并将其发送到该手机上。这意味着，智能手机也将成为病毒肆虐的新场所。

2009 年 11 月的第一个 iPhone 蠕虫和 iBotNet 蠕虫都是利用 SSH 默认密码的漏洞，自动将用户导向钓鱼网站，窃取用户的账号和密码；2015 年 4 月中旬，发现了影响全球数十亿台安卓手机的漏洞——“WiFi 杀手”。利用该漏洞，黑客可以远程攻击开启了 WiFi 的安卓手机。据调查，80%以上的网民会随意连接公共免费的 WiFi，其中接近四成用户会使用无密码的 WiFi 进行网络支付。根据 2014—2015 年中国互联网安全研究报告[6]，2014 年全球共有 2.8 亿部手机中安卓病毒，其中，仅中国就有近 1.2 亿部手机中毒，数量居全球第一。可见，网络的安全及广大用户的隐私与财产安全一直受到恶性蠕虫的威胁，且危害程度与日俱增。

无论是在传统的 Internet 网络上还是在移动无线网络上，蠕虫传播都是一个严重的威胁，而且这样的威胁还在不断增长。由于移动网络固有的共享、开放和广泛等特性，使得基于各类平台的系统本身的弱点得以暴露，随之出现越来越多的安全问题。移动智能设备的普及和移动网络的发展相互促进，传统的杀毒技术对具有移动特性的移动网络显得无力。如何预防和控制蠕虫随时可能带来的威胁，显得越来越重要。

2014 年 11 月，趋势科技发布中国区第三季度网络安全威胁报告及 2015 年移动安全威胁预测[7]。报告显示，2014 年第三季度，趋势科技中国区新增约 53

万条病毒码，客户终端检测并拦截恶意程序约 6988 万次，在中国地区拦截的恶意 URL 地址共计 1553 万余次，这些数据显示出网络安全威胁仍处于不断增长之中。同时，趋势科技还对 2015 年移动安全形势进行了展望，指出漏洞利用工具将重点针对 Android，而 Apple Pay 等新型支付方式也将给移动信息生活会带来新的风险[7,8]。移动智能设备被越来越多地用于网络应用之中，在“双十一”天猫 571.1 亿元的交易额中，移动端消费占比就达到了 42.6%。高额的收益预期驱使网络犯罪分子将移动设备作为重点攻击目标，移动安全威胁因此出现了迅速增长。为了对抗消费者的安全防护措施，网络犯罪分子不断寻求新的攻击方式，以提高攻击的成功率[7]。如图 1-1 所示是 2014 年安卓系统主要恶意程序类型。

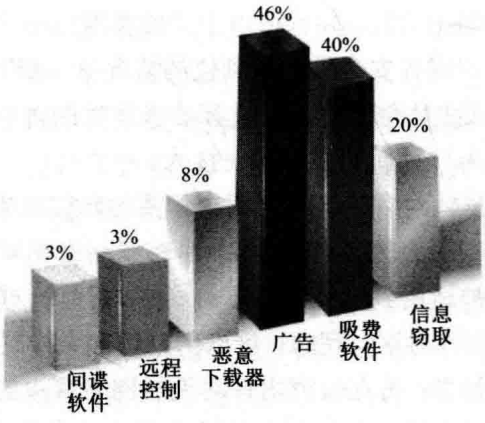

图 1-1　2014 年安卓系统主要恶意程序类型

趋势表明，在当前的移动网络安全形势下，企业和个人应该继续强化包括移动设备安全防护在内的网络安全措施，以保证网络环境的安全。

采用防火墙隔离技术可以将网络对外界保护起来，但是这种被动的防御措施对传统网络的效果相对明显，而对于开放式的无线网络来说，防火墙技术的防护效果就不甚理想。入侵检测作为防火墙之后网络的第二道安全闸门，是一种积极主动的安全防护技术，是目前加强无线网络安全性的有效方法之一。它可以对网络进行实时监护，当发现危害时，会主动拦截恶意攻击。然而，由于目前针对网络蠕虫的入侵检测技术仍不成熟，而网络蠕虫传播的隐蔽性、复杂性、多变性、突发性等特点，使得只有在网络中的蠕虫已经大规模感染并对网络的正常使用造成影响后才会被发现。传统的防御技术，如防火墙技术、杀毒软件、病毒检测技术等，在应对大量新型网络蠕虫攻击的能力上受到越来越多的限制，且它们不利

于研究蠕虫传播的特性和传播规律，不能帮助我们制定有效的防御策略。被动的防御治标不治本，因为在任何时候都有大量的用户连接网络，而大多数用户缺乏安全意识或者缺乏识别蠕虫的能力和技术，不能实现广泛有效的检测和防御。

根据文献[9]可知，良性蠕虫采用了恶性蠕虫的自动触发技术和传播技术的安全防护代码，其核心思想是将恶性蠕虫转变为良性蠕虫，去除恶性蠕虫不可控的传播特征，使得良性蠕虫在可控的方式下维护网络的安全。良性蠕虫能够像恶性蠕虫那样主动探测网络中存在漏洞的主机，当发现有漏洞的主机时就会主动修复这些脆弱主机或软件漏洞。为了避免良性蠕虫影响网络的正常使用，当网络中良性蠕虫达到一定比例时就会启动自销毁机制，释放占用的网络带宽和资源。

良性蠕虫防御策略是主动维护网络安全的防护技术之一，它可以有效地保护网络中数量庞大和脆弱的主机，并且可以主动修复网络中大量的漏洞主机。即使是在用户缺乏安全意识或者安全措施不到位的情况下，良性蠕虫策略也能改善主机的安全情况。良性蠕虫凭借高度可控性和非破坏性的优点，利用良性蠕虫对抗恶性蠕虫的传播正成为一种新的应急响应技术。

目前，已经有大量针对有线网络下蠕虫传播的研究成果，但是，由于有线网络和无线网络之间存在很大的差异，所以，在有线网络环境下针对蠕虫传播的许多研究成果不能直接被运用到无线网络中。并且，目前针对良性蠕虫的相关研究还处在起步阶段。本书针对这一现象，重点研究切合无线网络特征的良性蠕虫与恶性蠕虫交互的传播模型，旨在研究出针对无线网络蠕虫的有效防御策略。综上所述，本书研究切合无线网络特征的良性蠕虫对抗技术具有很大的现实意义。

1.2 国内外研究现状

近年来，随着无线网络技术的日益成熟，无线网络已被广泛地应用到国防军事、灾害救援、环境监测、空间探索等诸多重大领域，其重要性和意义已得到众多国家和团体的肯定，且对其安全性的关注和研究也越来越重视。然而，无线网络中各种蠕虫病毒及其变种带来的危害越来越大，各种恶意程序的相关研究工作已经受到国内外研究界的高度重视。根据文献[3]，为了更好地进行恶意程序方面的研究，2003 年美国政府投入 546 万美元在 Southern California 和 UC Berkeley 两所大学建设了拥有 1000 多台主机的网络攻击测试平台。在国内，相关方面的

研究工作虽然起步较晚，但是在国内众多研究者的努力下，研究工作同样也取得了很大的进展。随着恶意程序危害性的加剧，政府和国家安全部门都将极力推进针对无线网络恶意程序的研究和防治工作。

入侵检测技术是目前检测蠕虫入侵的主要技术之一，但是大多数的入侵检测技术只有在网络中病毒感染到一定程度时才会预警，防御工作相对滞后。防火墙和对漏洞打补丁依然是目前防治蠕虫感染的主要方法，然而，这些方法都太过于被动，防御效果不尽如人意。因为网络用户数量巨大，且不同用户的安全意识深浅不同，所采取的安全防护程度也不同。据统计，全网用户中每年将防火墙升级至最新版本的用户不足 1/5。可见，绝大多数网络用户安全意识比较低，不能及时升级防火墙或去检测设备的安全性，并且不能及时对受感染的设备打补丁或及时更新补丁库。其次，防火墙只是保护了单个主机，并不能主动去清除网络中的蠕虫，网络中依然有大量的蠕虫盛行。

防火墙或漏洞补丁的更新永远都是滞后的。因为网络中恶意蠕虫的传播速度与日俱增，越来越自主化和智能化，导致防火墙的防护工作不到位。恶意蠕虫从流行于网络到被发现需要一段时间，并且从发现恶意蠕虫到程序员编译出对应的补丁依然需要一段时间，使得操作系统和应用软件补丁的更新不及时。此外，广大用户对设备进行打补丁依然存在时间差，造成对蠕虫的防治工作不及时，恶意蠕虫对网络安全的威胁越来越严重。随着网络蠕虫技术的发展，在对抗传播迅速的恶意蠕虫的过程中，传统的抗病毒技术和防火墙技术的对抗效果越来越不理想。

常微分方程被广泛运用于生命科学领域，它可以用来研究各类流行病毒的传播机制，如流感、乙肝、AIDS 等。基于计算机病毒和传染病毒传播机理的相似性，研究人员提出了许多蠕虫传播模型。由于目前大多数的蠕虫传播模型都是在同质网络中构建的，本书将现有的模型分为三类：单蠕虫传播模型、蠕虫交互传播模型和异质网络中蠕虫传播模型。

1.2.1　单蠕虫传播模型

文献[10]提出了早期简单的传染病模型（Simple Epidemic Model），并给出了相关的微分方程。该类模型将个体分为两大类，即易感个体和感染个体。该模型没有考虑个体通过免疫措施可以恢复的情况，比如打补丁修复，考虑的网络因素比较少，显然不符合实际的病毒传播情况，不能准确地描述实际网络中病毒的传

播行为。

后来，在文献[11]中 Kephart 和 White 在考虑感染节点具有可恢复性的情况，提出了 SIS 模型。在该模型中，由于用户的免疫操作可以恢复被感染的节点。但是在该模型中用户只对病毒进行清理却并没有对主机进行打补丁，使得节点会以一定的概率转化为脆弱型节点。此外，该模型将网络抽象成有向的随机图，这一理念较符合当时网络的结构，较好地描述了早期网络中病毒的传播行为。在文献[12]中，Wierman 等人修改了 SIS 模型，他们将整个网络看做由许多局域网组成的一个大网络，考虑了节点的二次感染情况，并且考虑到新病毒的引入对已存在病毒传播的影响，使得模型更加符合实际情况。

由于 2001 年 7 月红色代码蠕虫的大肆传播，对网络的安全造成严重的危害。2002 年，Zou 等人在文献[13]中针对影响红色代码蠕虫传播的因素提出了双因素（Two-Factor）模型。因素一是网络服务提供者和网络用户所采取的免疫行为，因素二是考虑红色代码蠕虫的大肆传播引起网络拥塞和路由器发生故障，造成红色代码蠕虫后期的感染率下降。该模型可以作为一个通用的网络蠕虫传播模型。相比之前的一些模型，仿真和数值分析证明了双因素蠕虫模型更好地匹配了红色代码蠕虫的传播感染的真实数据。该模型为更好地了解和预测网络中大规模的蠕虫传播提供了参考。

接着，Kermack 和 Mckendrick 在文献[14]中提出了 SIR 模型，该类模型将个体分为三类，即易感染个体、感染个体和恢复个体，进一步改进了之前的传染病模型。Piqueira 等人在文献[15]提出了 SAIC（Susceptible-Antidotal-Infectious-Contaminated）模型，该模型考虑到感染节点具有潜伏期，节点虽然已经感染了恶意蠕虫，但是却并不表现出感染特性，该类节点不会感染其他的节点，该类恶性蠕虫自身的破坏性存在一定的时延。因此，将感染节点区分为具有恶性感染能力和没有恶性感染能力两类。此外，该模型还考虑了用户免疫策略的影响。实验结果证明该模型很好地拟合了实际网络中病毒传播的数据。文献[16]考虑了节点的免疫具有时效性，在一定的时间过后免疫节点会以一定的概率重新变为易感类节点。将时间延迟作为分歧参数，该文献研究了该模型的地方病平衡点的局部稳定性和霍普夫分岔。研究结果表明，不同免疫期的取值对病毒传播具有很大的影响，且当时间延迟达到一定值时该系统将出现周期解。这些研究结果都为后续的研究工作打下了基础。

基于上述模型，许多新的模型被提出，但这些模型研究的都是单蠕虫传播的情况。随着计算机网络技术的迅速发展，网络环境越来越复杂，网络蠕虫同样也在日趋复杂化，且网络蠕虫的种类也在迅猛增长。在复杂的网络环境下，多种蠕

虫之间的关系也越发复杂化。单蠕虫传播模型没有考虑到不同类别蠕虫之间的交互行为，所以，多蠕虫交互的传播模型应运而生。

1.2.2　蠕虫交互传播模型

根据网络中不同病毒之间的交互行为，Tanachaiwiwat 和 Helmy 在文献[17]中率先研究了双蠕虫交互的传播模型。针对随机扫描类蠕虫的特点，深入研究了存在竞争关系的两类蠕虫间的交互行为。竞争蠕虫会首先检测主机中是否存在另一种蠕虫，如果存在，就会自动删除该蠕虫，甚至有部分竞争蠕虫会对另一类蠕虫利用的漏洞打补丁，阻断该类蠕虫的传播通道。

受到竞争蠕虫的启发，文献[17]提出将竞争蠕虫替换为一类有益的蠕虫——良性蠕虫，利用良性蠕虫主动对抗恶性蠕虫，“以毒攻毒”。文献[17]建立了良性蠕虫与恶性蠕虫交互的传播模型，研究了利用最少的良性蠕虫遏制恶性蠕虫的传播。他们发现良性蠕虫策略的有效性不仅依赖于蠕虫的扫描速率，同时还依赖于网络的拓扑结构和恶性蠕虫采用的传播策略。文献[18]指出传统的对抗恶性蠕虫方法的缺陷，比如下载安装杀毒软件和打补丁都需要一定的时间，这样会导致防护工作的滞后，广大用户不能及时采取防护措施。并且提出修改现有的网络恶性蠕虫，使其变为良性蠕虫来对抗原始的恶性蠕虫。如利用“对抗型红色代码”修复“红色代码 2”留下的后门，利用 Nachi 良性蠕虫来消灭“冲击波”Blaster 恶性蠕虫。

文献[19]指出良性蠕虫的核心思想是将恶性蠕虫转变为良性蠕虫。良性蠕虫与恶性蠕虫具有相同的传播机制，借用了恶性蠕虫的扫描探测技术、自动触发技术和传播技术，同时添加了控制模块、修复功能模块和自动销毁模块。良性蠕虫功能模块如图 1-2 所示。

良性蠕虫的控制功能模块对良性蠕虫的传播、感染、复制进行完全控制。文献[20]指出良性蠕虫的控制指标包括指定可活动的时间、指定可扩散的范围、指定可繁殖的副本总数等。一旦违背了这三大控制指标中的一个或多个要求，良性蠕虫就会变得不受控制，就将转变为恶性蠕虫。例如，2001 年 5 月 Cheese“良性”蠕虫被用来对抗 Lion 恶性蠕虫，Cheese“良性”蠕虫利用与 Lion 恶性蠕虫相同的后门进行感染。当其扫描到被 Lion 恶性蠕虫感染的主机，就会利用其留下的后门感染该主机，当感染该主机后，Cheese“良性”蠕虫就会删除该后门，并继续扫描其他存在该类后门的主机。但是由于该 Cheese“良性”蠕虫的控制

指标没有设定好，使其在网络中不受控制地大规模传播，严重影响了网络的正常使用。

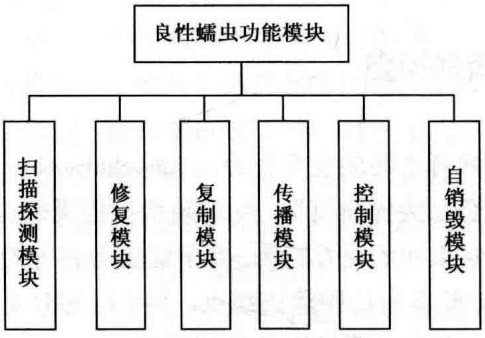

图 1-2　良性蠕虫功能模块

良性蠕虫的自销毁模块会检测当前网络中良性蠕虫的总数，当良性蠕虫生成的繁殖副本达到一个阈值时，就会触发自销毁模块对自身进行销毁，释放被自身占用的网络带宽，减少网络的负载。良性蠕虫凭借高度的可控性和非破坏性的优点，受到研究界越来越多的重视。

根据良性蠕虫的行为，良性蠕虫被分为三类：被动良性蠕虫、主动良性蠕虫和混合良性蠕虫。当被动良性蠕虫感染节点时，就会处于伺机待动的状态。只有当恶意蠕虫企图感染该节点时，才会触发该节点上被动良性蠕虫的防御响应机制，进而发起对恶性蠕虫的反击。主动良性蠕虫会主动扫描网络中的节点，感染节点并且修复被恶意蠕虫感染的节点。混合良性蠕虫是被动良性蠕虫和主动良性蠕虫的综合体，在伺机待命的同时，又可以主动发起进攻。可以根据实际需要，综合选用不同种类的良性蠕虫。

彭等人在文献[21,22]中对良性蠕虫的修复策略进行分类：查杀恶意蠕虫并修补主机漏洞、只查杀恶意蠕虫、仅修补易感主机的漏洞及修补所有脆弱主机漏洞并查杀恶意蠕虫。他们分别分析了良性蠕虫出现时间的早晚和在良性蠕虫采用不同修复策略的修复效果。分析结果表明，良性蠕虫越早引入和修复功能越强大，其对恶性蠕虫传播控制的效果就越好。Zhao 等人在文献[23]中基于双因素传播模型研究了主动良性蠕虫和混合良性蠕虫分别在感染有时间延迟和无时间延迟的情况下的传播情况。在文献[24]中 Toutonji 等人同样基于双因素传播模型研究了被动良性蠕虫的动态免疫策略对恶意蠕虫传播的影响。文献[25]创新性地提出了基于云良性蠕虫对抗策略，并分析了传播模型的动力学行为。文献[26]针对城市

车载物联网环境中蠕虫的传播问题，提出了基于速度分治的车载物联网良性蠕虫模型。针对 P2P 网络蠕虫传播的特点，文献[27,28]研究了利用良性蠕虫对抗 P2P 蠕虫的策略。

研究结果表明，良性蠕虫对抗恶性蠕虫的效果非常显著。然而，目前针对良性蠕虫的研究工作仍然处于起步阶段，如何编译出具有高可控性、无危害的良性蠕虫是良性蠕虫研究工作的重点和难点。此外，虽然现有研究结果证明良性蠕虫策略相比传统的防御措施具有很大的优势，但是，已有的许多研究成果是分别针对不同的应用环境，比如，P2P 对等网络、车载网、云技术等，在不同的应用环境中良性蠕虫的修复效果存在差异，即使是在同一个网络环境下相同的良性蠕虫也会有不同的修复效果。因此，目前针对良性蠕虫的许多研究成果也同样不能被直接运用于无线网络。

1.2.3　移动良性蠕虫的研究现状

随着移动网络的蓬勃发展，移动恶意代码也呈现出爆发的趋势。这些移动恶意代码大部分都是吸费软件或有高度风险的应用程序，它们以吸取或盗取隐私数据为目标，威胁极大。当前移动智能手机或者其他移动终端设备具有很大的脆弱性，这使得移动恶意蠕虫的爆发成为一种很大的潜在威胁[29,30,31]。

移动良性蠕虫的思想就是将恶意的蠕虫转化成良性的蠕虫，而且该良性蠕虫还可以运用相同的感染机制使得移动设备对恶意蠕虫免疫[18,33]。由于良性蠕具备的主动对抗恶意蠕虫和自动修复系统漏洞能力，对良性蠕虫的研究一直是蠕虫安全领域的一个重要课题，但现有的关于良性蠕虫修复网络对抗恶意蠕虫的模型在一定程度上忽略了良性蠕虫本身的传播特点与其所在网络环境等因素的影响。所以，如何正确运用良性蠕虫来控制恶意蠕虫并分析其传播特点一直是研究的热点。

1.2.4　蠕虫检测、防御、修复机制的研究现状

当前的蠕虫检测防御技术主要有以下几个方面[34,35,36,37]。

（1）基于网络数据包内容的检测应用：主要包括 IDS 蠕虫特征匹配 Autograph、EarlyBird 等。主要检测原理是先收集一些蠕虫恶意代码的特征值，