

良性与恶性蠕虫模型在气象物联网中的应用分析

陈建云, 林建滨

(福建省福州市气象局, 福建 福州 350008)

摘要:根据气象物联网的特征,结合生物学传染病动力学模型,考虑多个现实影响因素,如节点的出生率、自然死亡率、因病死亡率以及节点的移动性,构建了一个新颖的混合良性蠕虫对抗双恶性蠕虫的传播模型。针对气象物联网的传播特性,研究良性蠕虫对抗恶性蠕虫的技术,提出了一个新颖的在气象物联网中混合良性蠕虫对抗双恶性蠕虫的传播模型。依托物联网平台,利用研究和刻画蠕虫传播机理的有效工具数学模型分析了多蠕虫在气象物联网上的传播机理,基于传染病动力学理论分析了网络系统在达到不同平衡状态下的平衡点。理论和数值仿真结果表明,该模型可较为准确地刻画良性蠕虫与双蠕虫在网络上的对抗传播过程。

关键词:气象物联网;动力学模型;良性蠕虫;数值仿真

中图分类号:TP309

文献标识码:A

文章编号:1673-629X(2019)06-0116-03

doi:10.3969/j.issn.1673-629X.2019.06.024

Application and Analysis of Interactions of Hybrid Benign Worm and Two Malicious Worms in Meteorological Internet of Things

CHEN Jian-yun, LIN Jian-bin

(Meteorological Bureau of Fuzhou City, Fujian Province, Fuzhou 350008, China)

Abstract:Based on the characteristics of meteorological internet of things (IoT) and the dynamic model of biologic infectious diseases, we construct a novel propagation model of mixed benign worms against double malignant worms in consideration of the birth rate of nodes, natural mortality and mobility of nodes. In view of the propagation of meteorological IoT, the technology of benign worms against the malignant worms is studied, and a novel propagation model of a benign worm against double malignant worms in the IoT is proposed. Based on the platform of IoT, we analyze the propagation mechanism of multiple worms in the weather network according to the mathematical model of studying and characterizing the mechanism of worm propagation, and analyze the equilibrium point of the network system in different equilibrium states based on the theory of infectious disease dynamics. The results of theory and numerical simulation show that the model can accurately depict the communication process between benign worms and double worms on the network.

Key words:meteorological internet of things; dynamic model; benign worm; numerical simulation

0 引言

气象物联网是采用无线传感网络、云计算、移动网络等多项技术,依托物联网平台构建的气象网络,在气象监测、气象服务、气象灾害预警、农业种植等方面具有广泛的应用。国内也正在加快气象物联网的建设步伐,力争向“智慧气象”迈进。随着气象物联网的发展,网络蠕虫成为气象物联网的主要安全隐患之一。

依托物联网平台,世界任何地方可联网的通信设备都可以获得气象物联网中的数据,也可以采集气象数据并上传数据。携带恶意蠕虫的联网设备将对气象物联网的安全构成极大威胁,良性蠕虫是根据蠕虫的

传播机理编译的安全防护代码,利用良性蠕虫对抗技术已成为现有控制蠕虫传播的有效方法之一^[1-2]。

数学模型是研究和刻画蠕虫传播机理的有效工具,有助于制定防御策略,并检验控制策略的有效性。基于网络病毒与生物病毒传播的相似性,许多学者利用传染病动力学建模方法提出了很多良性蠕虫对抗模型,对蠕虫的交互动力学行为进行分析研究,取得了许多研究成果^[3-5]。

然而现有的良性蠕虫对抗模型主要研究良性蠕虫与单蠕虫的交互行为,而实际网络中存在的蠕虫类型多种多样,而各类蠕虫之间又存在合作或竞争等复杂

收稿日期:2018-07-20

修回日期:2018-11-21

网络出版时间:2019-03-06

基金项目:福建省自然科学基金社会发展引导性(重点)项目(2017Y-008);气象预报业务关键技术发展专项(YBGJXM201703-06)

作者简介:陈建云(1984-),男,硕士,工程师,研究方向为网络安全。

网络出版地址: <http://kns.cnki.net/kcms/detail/61.1450.TP.20190306.0952.066.html>

的交互关系,目前还没有文献针对良性蠕虫与多类恶性蠕虫的交互传播进行建模。文中将根据气象物联网的传播特性,考虑多个现实影响因素,包括新节点的加入、节点的自然死亡率、节点因病毒感染的故障死亡率等,在研究良性蠕虫对抗技术的基础上,提出一个新颖的混合良性蠕虫对抗双恶性蠕虫的传播模型,并进行动力学理论分析和数值仿真实验验证,以提出有效的蠕虫控制策略^[6-9]。

1 良性蠕虫与双恶性蠕虫交互模型

模型中存在三类蠕虫,其中一类为合作型恶性蠕虫,记为 Worm-1,会有助于另一类非合作型恶性蠕虫 Worm-2 的入侵;还有一类为混合型良性蠕虫,既可以修复易感状态的节点,也可以修复被 Worm-1 感染的节点。 t 时刻易感状态的节点数目记为 $S(t)$,被上述三类蠕虫分别感染的节点数目分别记为 $I_1(t)$ 、 $I_2(t)$ 、 $U(t)$,被 Worm-1 和 Worm-2 同时感染的节点数目记为 $I_{12}(t)$,被修复成为免疫状态的节点数目记为 $R(t)$ 。为了便于书写,分别简记为 S 、 I_1 、 I_2 、 I_{12} 、 R 、 U ^[7,10]。

因气象物联网中存在大量的移动和静止节点,移动节点的动态特性会很大程度上影响蠕虫的传播。移动节点在移动过程中接触到的节点数目与节点的移动速度 v 、节点的通信半径 r 、节点的分布密度 ρ 及节点的平均通信列表 n 相关,文中利用气象物联网中所有节点的平均连接度 k 来刻画节点的移动性。假设所有节点是均匀分布的,若所有节点都是静止的,则节点平均连接度为 $\rho\pi r^2 - 1 + n$;一个移动节点在时间 t 内的有效通信面积为 $s = 3\Delta t v / \sqrt{r^2 - 0.25(\Delta t)^2 v^2} + 2r^2 \arccos(0.5\Delta t v / r)$ 。设网络中移动节点的比率为 θ ,则气象物联网中所有节点的平均连接度为 $\bar{k} = \rho s \theta + \rho\pi r^2(1 - \theta) - 1 + n$ 。

此外,结合气象物联网特征,考虑多个现实影响因素使模型更加精确,包括新节点的加入、节点的自然死亡率、节点因感染的故障死亡率等。具体地, A 代表 t 时刻网络中新增的 S 类节点数目, β_1 、 β_2 、 β_3 分别表示 Worm-1、Worm-2 和良性蠕虫的感染率,由于用户的抗病毒措施使得 S 、 I_1 、 I_2 、 I_{12} 、 U 类节点成为 R 类节点的速率分别为 ε 、 γ_1 、 γ_2 、 γ_3 、 γ_4 , R 类节点变为 S 类节点的速率为 α , d 为节点的自然死亡率, Worm-1 使得 Worm-2 的感染率提高 μ 倍,由于蠕虫感染作用使得 I_1 、 I_2 、 I_{12} 、 U 类节点发生故障死亡率分别为 η_1 、 η_2 、 η_3 、 η_4 ^[10-11]。

2 数值仿真模拟

为了验证该模型的有效性,利用 MATLAB 进行

仿真分析。

实验 1:设置模型参数 $N(0) = 10^6$, $R(0) = 0$, $\beta_1 = \beta_2 = \beta_3 = 3 \times 10^{-8}$, $\gamma_1 = \gamma_2 = \gamma_4 = 0.03$, $\eta_1 = \eta_2 = \eta_4 = 0.001$, $k = 10$, $\varepsilon = 0.02$, $\alpha = 0.06$, $d = 0.0002$, $A = 200$,使得基本再生数 $G_1 < 1$, $G_2 < 1$, $G_3 < 1$,仿真结果如图 1 所示。网络中各类节点达到全局渐进稳定状态,此结果验证了定理 1,证明了当 $G_1 < 1$, $G_2 < 1$, $G_3 < 1$ 时,模型 1 的无病平衡点 $E_1 \leftarrow (S^1, 0, 0, 0, R^1, 0)$ 是全局渐进稳定的^[12-13]。

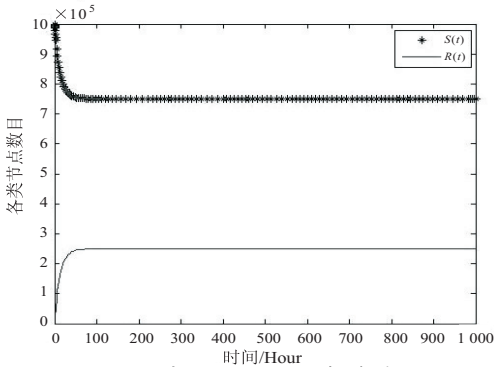


图 1 无病平衡点全局渐进稳定

实验 2:检验 Worm-1 流行态的稳定性。设置参数 $I_1(0) = 1\,000$, $A = 300$,其余参数同实验 1,仿真结果如图 2 所示。验证了 Worm-1 流行平衡点 E_2 是全局渐进稳定的,此时网络中恶性感染节点占据绝大部分。

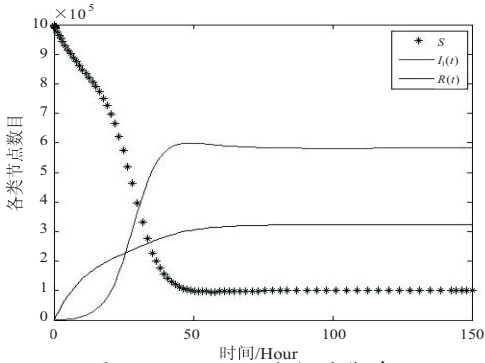


图 2 Worm-1 流行平衡态

实验 3:检验 Worm-1 和良性蠕虫共存平衡态。设置参数 $U(0) = 1\,000$,其余参数同实验 2,数值仿真结果如图 3 所示。图 3 证明了 Worm-1 和良性蠕虫共存平衡点 E_4 是全局渐进稳定的。图 3 显示网络中被 Worm-1 感染的节点数目最终趋于 0,恶性蠕虫爆发的峰值被大大降低,与图 3 对比结果表明混合型良性蠕虫可以有效地修复网络中的脆弱节点和被 Worm-1 感染的节点,增强网络的安全性。

实验 4:检验 Worm-1、Worm-2 和良性蠕虫共存平衡态。在实验 3 的基础上变动参数 $A = 1\,000$, $U(0) = 5$, $\mu = 1.5$,另外设置 k 分别为 5 和 10,仿真结果如图 4 和图 5 所示。对比图 4 和图 5 可知,网络中节点的平均连接度 k 越大,即节点的移动速度、通信半径

和密度越大,恶性蠕虫在网络中的传播速度也越快,并且提高了蠕虫爆发的峰值。气象物联网中大量移动节点的存在加快了网络中蠕虫传播速度,因此如何综合性地根据网络中节点的平均连接度调整良性蠕虫的引入数量是控制气象物联网中蠕虫传播的一个关键点。

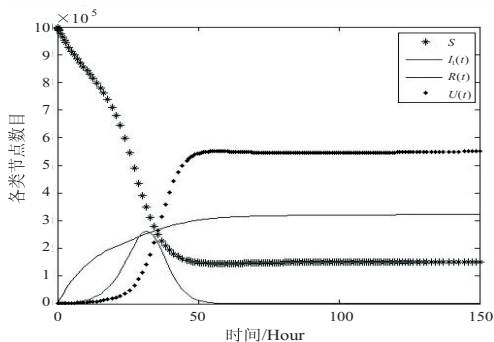


图 3 Worm - 1 和良性蠕虫共存平衡态

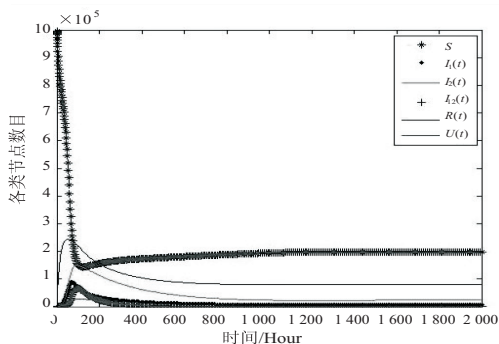


图 4 Worm - 1、Worm - 2 和良性蠕虫共存平衡态($k = 5$)

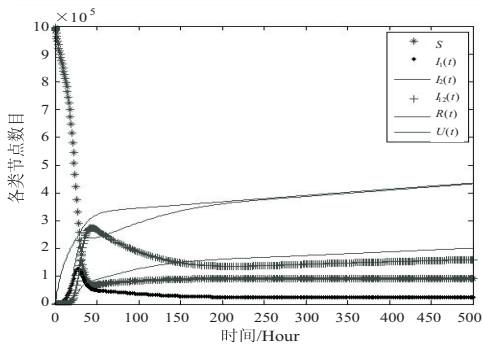


图 5 Worm - 1、Worm - 2 和良性蠕虫共存平衡态($k = 10$)

3 结束语

针对气象物联网的传播特性,研究良性蠕虫对抗恶性蠕虫的技术,提出了一个新颖的在气象物联网中混合良性蠕虫对抗双恶性蠕虫的传播模型。基于传染病动力学理论,在理论上分析了网络系统在达到不同平衡状态下的平衡点,数值仿真结果证明了理论结果的正确性和模型的准确性。研究结果表明,节点的平均连接度越大就越有利于网络中蠕虫的传播,因此根据气象物联网中节点的平均连接度合理地控制引入网络中良性蠕虫的数目,使得良性蠕虫在有效保护网络

安全的同时,不过多地占用网络的有限带宽,不附加给网络额外的压力,是控制气象物联网中恶性蠕虫传播的有效策略。未来将结合更多气象物联网的特性,如考虑良性蠕虫引入时延性,增强模型的精准性,寻找更优的蠕虫防御策略。

参考文献:

- [1] CASTANEDA F, SEZER E C, XU J. WORM vs. WORM: preliminary study of an active counter-attack mechanism [C]//Proceedings of the 2004 ACM workshop on rapid malware. Washington DC, USA: ACM, 2004: 83-93.
- [2] WANG Yini, WEN Sheng, XIANG Yang, et al. Modeling the propagation of worms in networks: a survey [J]. IEEE Communications Surveys & Tutorials, 2014, 16(2): 942-960.
- [3] ZHENG Xufei, LI Tao, FANG Yonghui. Strategy of fast and light-load cloud-based proactive benign worm countermeasure technology to contain worm propagation [J]. The Journal of Supercomputing, 2012, 62(3): 1451-1479.
- [4] 严博, 吴晓平, 廖巍, 等. 基于随机进程代数的 P2P 网络蠕虫对抗传播特性分析 [J]. 电子学报, 2012, 40(2): 293-299.
- [5] TOUTONJI O, YOO S M. Passive benign worm propagation modeling with dynamic quarantine defense [J]. KSII Transactions on Internet and Information Systems, 2009, 3(1): 96-107.
- [6] XIAO Xi, FU Peng, DOU Changsheng, et al. Design and analysis of SEIQR worm propagation model in mobile internet [J]. Communications in Nonlinear Science and Numerical Simulation, 2017, 43: 341-350.
- [7] 周翰逊, 赵宏, 闻英友. 分而治之的混合型良性蠕虫的建模与分析 [J]. 计算机研究与发展, 2009, 46(7): 1110-1116.
- [8] 王超, 卿斯汉, 何建波. 基于混合对抗技术的对抗性蠕虫 [J]. 通信学报, 2007, 28(1): 28-34.
- [9] 唐浩坤, 刘宴兵, 黄俊, 等. 基于形式化逻辑矩阵的结构化 P2P 蠕虫对抗模型 [J]. 计算机科学, 2013, 40(5): 141-146.
- [10] MISHRA B K, PANDEYSK. Dynamic model of worms with vertical transmission in computer network [J]. Applied Mathematics and Computation, 2011, 217(21): 8438-8446.
- [11] WANG Fangwei, ZHANG Yunkai, WANG Changguang, et al. Stability analysis of an e-SEIAR model with point-to-group worm propagation [J]. Communications in Nonlinear Science and Numerical Simulation, 2015, 20(3): 897-904.
- [12] MA J, CHEN Z, WU W, et al. Influences of removable devices on the anti-threat model: dynamic analysis and control strategies [J]. Information, 2015, 6(3): 536-549.
- [13] MA J, CHEN Z, LIU J, et al. Analysis of two-worm interaction model in heterogeneous M2M network [J]. Information, 2015, 6(4): 613-632.