基于博弈论的网络攻防行为建模与态势演化分析

刘小虎[①] 张恒巍*[①] 张玉臣[①] 胡 浩[①] 程 建[②]

[①](战略支援部队信息工程大学 郑州 450001)

[②](国防科技大学 武汉 430000)

摘 要：网络安全本质在对抗。针对现有研究缺乏从博弈视角分析网络攻防行为与态势演化关系的问题，该文提出一种网络攻防博弈架构模型(NADGM)，借鉴传染病动力学理论以不同安全状态网络节点密度定义网络攻防态势，分析网络节点安全状态转移路径；以网络勒索病毒攻防博弈为例，使用NetLogo多Agent仿真工具开展不同场景下攻防态势演化趋势对比实验，得出增强网络防御效能的结论。实验结果验证了模型方法的有效性和可行性。

关键词：网络攻防；博弈论；态势演化；传染病动力学；勒索病毒

中图分类号：TN915.08; TP393 **文献标识码**：A **文章编号**：1009-5896(2021)12-3629-10

DOI: 10.11999/JEIT200628

Modeling of Network Attack and Defense Behavior and Analysis of Situation Evolution Based on Game Theory

LIU Xiaohu[①] ZHANG Hengwei[①] ZHANG Yuchen[①] HU Hao[①] CHENG Jian[②]

[①](*Strategic Support Force Information Engineering University*, *Zhengzhou* 450001, *China*)

[②](*National University of Defense Technology*, *Wuhan* 430000, *China*)

Abstract: The essence of network security is confrontation. In view of at the problem that the existing research lacks to analyze the relationship between network attack and defense behavior and situation evolution from the perspective of game, a Network Attack And Defense Game architecture Model (NADGM) is proposed, the theory of infectious disease dynamics is used to define the network attack and defense situation with the density of network nodes in different security states, and the network node security state transition path is analyzed; The network blackmail virus attack and defense game is taken as an example, and NetLogo multi-agent simulation tools is used to carry out comparative experiments of attack and defense situation evolution trend in different scenarios, and the conclusion of enhancing network defense effectiveness is obtained. The experimental results verify the effectiveness and feasibility of the model method.

Key words: Network attack and defense; Game theory; Situation evolution; Infectious disease dynamics; Extortion virus

1 引言

网络空间的安全性是一种涌现属性[1]。微观层面网络攻防对抗行为推动了宏观层面网络攻防态势的不断演化[2]。有效刻画网络攻防行为、准确预测网络攻防态势演化趋势成为亟需研究解决的关键问题。网络攻防与博弈论在目标对立、策略依存和关系非合作等特征方面具有相似性[3]。博弈论被认为是网络空间安全学科的基础理论之一[4]。基于博弈论建模网络攻防行为，分析网络攻防态势演化趋势，日益成为当前网络安全领域的研究热点[5]。

根据攻防双方掌握的行为信息和收益信息的完备程度，可将网络攻防博弈模型划为完全信息博弈模型和不完全信息博弈模型[6]。例如文献[7]针对网络安全测评和最优主动防御问题，提出了网络攻防完全信息博弈模型以及一种攻防策略分类及量化方法；文献[8]针对军事信息网络的安全风险评估问题，基于完全信息博弈模型提出了一种网络安全风险评估方法，并从安全属性角度量化攻防收益。由于网络对抗过程中，攻防双方一般仅能掌握己方信息和部分对方信息。因此，不完全信息博弈模型更符合网络攻防特点。例如文献[9]针对网络防御决策方法中未考虑攻击方的类型、防御方的反击行为等问题，建立了网络攻防不完全信息博弈模型，结合攻击者类型、防御者反击行为和攻击成功率改进收益量化方法；文献[10]针对网络防御决策方法仅考虑

收稿日期：2020-07-29；改回日期：2021-05-28；网络出版：2021-07-13

*通信作者： 张恒巍 zhw11qd@163.com

攻击方类型未考虑防御方类型、策略选取可操作性差等问题，提出了一种攻防双方均具有多种类型的不完全信息博弈模型，并用数学方法证明了攻防双方采用混合策略的可信性。

现有研究在建立网络攻防博弈模型后，大多通过案例推演或者数值仿真方式加以验证，存在着难以刻画展示网络攻防态势、无法有效分析网络攻防行为与态势演化趋势之间的联系等问题，在分析和解释网络安全涌现现象方面存在一定不足。博弈论与仿真是研究社会复杂系统的两个互补方法[11]，能够为研究网络安全问题提供可行途径。将网络攻防节点视为智能体，在建立网络攻防行为博弈模型后，利用NetLogo多智能体仿真工具动态模拟网络攻防态势随时间演化趋势，可从微观网络攻防行为层面分析宏观攻防态势演化现象，增强对网络攻防态势演化规律的认识，提高网络防御的针对性和有效性[12]。同时，网络攻防态势演化分析涉及网络节点数量众多，采用智能体仿真方法可解决攻防实验环境部署难度大、可扩展性差、灵活性不足等问题，并提供较好的动态展示效果。

针对网络攻防行为与态势演化关系的问题，本文将网络攻防节点的决策行为视为逻辑上的同时决策，采用不完全信息静态博弈建模网络攻防行为，借鉴传染病动力学理论定义网络攻防态势，以网络勒索病毒攻防博弈为例开展仿真实验，分析不同攻防场景下网络攻防态势演化趋势。主要贡献在于：(1)基于不完全信息静态博弈理论构建了网络攻防博弈模型，攻防双方均具有多种类型，采用两次海萨尼转换求解贝叶斯纳什均衡，更加符合网络攻防信息不完备的实际；(2) 借鉴传染病动力学理论，以不同安全状态网络节点密度定义网络攻防态势，分析网络节点的4条安全状态转移路径，便于从网络攻防行为层面解释态势演化现象；(3)采用NetLogo多智能体仿真工具动态模拟网络攻防态势随时间演化趋势，具有计算量小、直观性强、扩展性好等优点。

2 网络攻防博弈模型构建与均衡求解

2.1 博弈模型构建

为有效构建网络攻防博弈模型，一般假设攻击方和防御方都受能力、资源和偏好等条件约束，攻击策略和防御策略均是有限的，攻防双方目标均是通过适当的策略组合实现自身收益最大化[13]。

定义1 网络攻防博弈模型(Network Attack-Defense Game Model, NADGM)是一个非合作不完全信息静态博弈模型，包括7元组$\mathrm{NADGM}=(N,S,\Theta,P,T,x(t),U)$，其中

(1)$N=(N_{\mathrm{D}},N_{\mathrm{A}})$是局中人空间。$N_{\mathrm{D}}$表示防御方局中人；$N_{\mathrm{A}}$表示攻击方局中人。局中人具有自主决策能力。

(2)$S=(S_{\mathrm{D}},S_{\mathrm{A}})$是局中人的策略空间。$S_{\mathrm{D}}$表示防御方策略集，$S_{\mathrm{D}}=\{D_g\,|g=1,2,\cdots,m\}$；$S_{\mathrm{A}}$表示攻击方策略集，$S_{\mathrm{A}}=\{A_h\,|h=1,2,\cdots,n\}$。其中，$1\le(m,n)<+\infty,(m,n)\in Z$。

(3)$\Theta=(\Theta_{\mathrm{D}},\Theta_{\mathrm{A}})$是局中人的类型空间。$\Theta_{\mathrm{D}}$表示防御方类型，$\Theta_{\mathrm{A}}$表示攻击方类型。由于不完全信息性，攻防双方类型都不少于1种。

(4)$P=(P_{\mathrm{D}},P_{\mathrm{A}})$是局中人的概率空间，描述攻防双方类型的不确定性。$P_{\mathrm{D}}$表示防御方的概率空间，$P_{\mathrm{A}}$表示攻击方的概率空间。

(5)T代表时间。网络攻防博弈及态势演化是一个动态连续的对抗过程，需要从时间维度进行建模和分析。

(6)$x(t)$表示t时刻的网络攻防态势，$0\le t\le T$。本文采用网络中具有不同安全状态的网络节点的密度刻画网络攻防态势，详细分析见第3节定义2。

(7) $U=(U_{\mathrm{D}},U_{\mathrm{A}})$是收益函数。$U_{\mathrm{D}}$表示防御方收益函数，$U_{\mathrm{A}}$表示攻击方收益函数。收益是博弈双方策略选取的结果、策略调整的依据。

2.2 博弈均衡求解

收益量化和计算是博弈均衡求解的基础与前提[14]。基于博弈论的网络攻防研究中，攻防收益量化和计算较多借鉴姜伟等人[15]提出的方法。例如，文献[12]定义了系统损失代价(System Damage Cost, SDC)、攻击代价 (Attack Cost, AC)、攻击回报(Attack Reward, AR)、防御代价(Defense Cost, DC)、防御回报(Defense Reward, DR)等概念。其中，系统损失代价SDC受攻防策略组合影响，记为$\mathrm{SDC}(D_g,A_h)$，代表当防御策略为D_g、攻击策略为A_h时目标系统遭受损失的值；防御回报DR为采用防御措施后系统免于遭受的损失，可用SDC正值表示；攻击回报AR为攻击方对目标系统造成的损失，用系统损失代价SDC正值表示。但由于攻防双方实施策略的成本不相同，网络攻防博弈模型NADGM属于非零和博弈。不同攻防策略组合(D_g,A_h)下，收益函数$U_{\mathrm{D}}(D_g,A_h)$和$U_{\mathrm{A}}(D_g,A_h)$的计算方法由式(1)给出。

$$\left.\begin{aligned}&U_{\mathrm{D}}(D_g,A_h)=\mathrm{DR}-\mathrm{DC}\\&U_{\mathrm{A}}(D_g,A_h)=\mathrm{AR}-\mathrm{AC}\\&\mathrm{AR}=\mathrm{SDC}(D_g,A_h)\\&\mathrm{DR}=\mathrm{SDC}(D_g,A_h)\end{aligned}\right\}\tag{1}$$

网络攻防对抗中攻防策略集都是有限的而非无限的，网络攻防博弈NADGM是有限非合作博弈。

纳什根据不动点定理证明了有限非合作博弈均衡的存在性[16]。网络攻防博弈模型NADGM均衡为贝叶斯纳什均衡，其存在性定理及证明见文献[17]。

不完全信息静态博弈均衡的求解，需要利用海萨尼转换，引入虚拟局中人“自然”(Nature)，将不完全信息静态博弈均衡求解问题转化为完全但不完美信息静态博弈均衡求解问题。为便于推理和分析，设定防御方为3种类型，各自拥有不同强度的策略，即$\Theta_{\mathrm{D}}=\{\Theta_{\mathrm{D1}},\Theta_{\mathrm{D2}},\Theta_{\mathrm{D3}}\}$，分别对应概率$P_{\mathrm{D}i}=\{P_{\mathrm{D1}},P_{\mathrm{D2}},P_{\mathrm{D3}}\}$，且有$\sum_{i=1}^{3}P_{\mathrm{D}i}=1$，$\Theta_{\mathrm{D1}}=\{D_1,D_2,D_3\}$，$\Theta_{\mathrm{D2}}=\{D_4,D_5,D_6\}$，$\Theta_{\mathrm{D3}}=\{D_7,D_8,D_9\}$。同理，对于攻击方有$\Theta_{\mathrm{A}}=\{\Theta_{\mathrm{A1}},\Theta_{\mathrm{A2}},\Theta_{\mathrm{A3}}\}$，分别对应概率$P_{\mathrm{A}j}=\{P_{\mathrm{A1}},P_{\mathrm{A2}},P_{\mathrm{A3}}\}$，且$\sum_{i=1}^{3}P_{\mathrm{A}j}=1$，$\Theta_{\mathrm{A1}}=\{A_1,A_2,A_3\}$，$\Theta_{\mathrm{A2}}=\{A_4,A_5,A_6\}$，$\Theta_{\mathrm{A3}}=\{A_7,A_8,A_9\}$。

运用2次海萨尼转换得出不完全静态贝叶斯博弈树如图1所示。

此时，防御方收益$U_{\mathrm{D}}(D(t),A(t))$(简称$U_{\mathrm{D}}(t)$)为

$$U_{\mathrm{D}}(t)=\sum_{\Theta_{\mathrm{D}}}P_{\mathrm{D}i}\cdot P_{\mathrm{A}j}\cdot U_{\mathrm{D}}(D_g,A_h) \tag{2}$$

同理，攻击方收益$U_{\mathrm{A}}(D(t),A(t))$(简称$U_{\mathrm{A}}(t)$)为

$$U_{\mathrm{A}}(t)=\sum_{\Theta_{\mathrm{A}}}P_{Di}\cdot P_{\mathrm{A}j}\cdot U_{\mathrm{A}}(D_g,A_h) \tag{3}$$

设定$\mathrm{EQ}_t=(U_{\mathrm{D}}^{*}(t),U_{\mathrm{A}}^{*}(t))$为网络攻防博弈模型NADGM的贝叶斯纳什均衡解，则满足式(4)

$$\left.\begin{aligned}U_{\mathrm{D}}^{*}(t)&=\max\sum\{P(A_h|D_g)U_{\mathrm{D}}[(D(t),A^{*}(t));\\&\qquad D_g,A_h]\}\\U_{\mathrm{A}}^{*}(t)&=\max\sum\{P(D_g|A_h)U_{\mathrm{A}}[(A(t),D^{*}(t));\\&\qquad A_h,D_g]\}\end{aligned}\right\} \tag{4}$$

联立式(2)、式(3)和式(4)组成方程组，利用线性规划方法可求解网络攻防博弈模型NADGM的贝叶斯纳什均衡。为避免在实际计算过程中面临的求解过程复杂、计算量大等问题，可利用博弈分析和计算工具Gambit[18]进行求解。对于攻击方和防御方，贝叶斯纳什均衡解为双方最优策略，双方均不会因单方面改变策略而增加收益。

3　网络攻防态势定义与演化分析

涌现性是网络安全的天然属性。文献[19]指出传染病模型和基于智能体仿真是研究网络安全涌现性的有效途径。传染病模型SIR将人群状态分为易感者、感染者和康复者，不同状态人群在一定条件下可以相互转化，与网络攻防对抗所引起的节点安全状态转移具有一定相似性，已在网络安全研究领域得到了一定应用。例如，文献[20]将传染病模型应用于无线传感网络节点通信协议设计中，提出了Discard算法；文献[21]在“易感-感染-移除-易感”SIRS病毒传播模型的基础上建立了零日病毒传播模型，运用劳斯稳定性判据分析了系统平衡点的局部稳定性，并开展了仿真实验。文献[22]在传染病模型的基础上提出了网络安全状态演化模型，通过求解模型的鞍点策略给出最优防御策略选取方法。

网络攻防对抗中，攻击方试图将攻击策略部署到更多的网络节点，扩大攻击的影响范围；防御方试图将防御策略部署至更多的网络节点。从涌现性视角理解，微观层面网络攻防对抗行为会导致网络节点状态发生改变，进而在宏观层面引起网络攻防态势演化现象。文献[23]指出网络攻防行为主要引起两方面变化：一是单个网络节点安全状态不断迁移变化；二是不同安全状态网络节点数量持续动态变化。因此，借鉴传染病动力学理论[24]，将网络节点的安全状态划分为3类，分别是攻击感染节点、正常用户节点和防御部署节点。

攻击感染节点(Infectious Node, IN)：攻击方在网络节点部署有攻击策略，拥有该节点的控制权，对应于网络攻防博弈模型中N_{A}; IN(t)表示t时刻攻击感染节点IN的数量。

防御部署节点(Recovered Node, RN)：防御方在网络节点部署有防御策略，拥有该节点的控制权，对应于网络攻防博弈模型中N_{D}; RN(t)表示t时刻防御部署节点RN的数量。

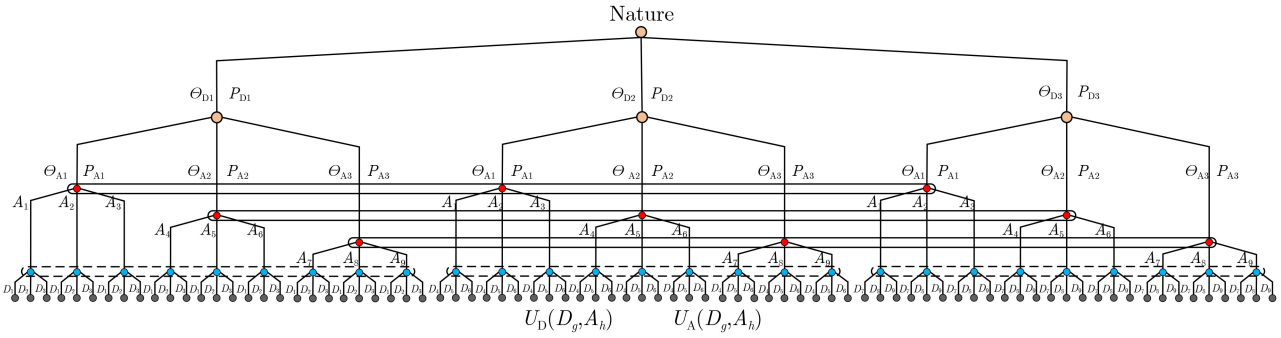

图 1 不完全信息静态贝叶斯博弈树

正常用户节点(Susceptible Node, SN)：网络节点未部署攻击策略和防御策略，正常用户拥有该节点的控制权。攻击方和防御方在付出一定策略代价后，相应地可使其转化为攻击感染节点ID和防御部署节点RN。SN(t)表示t时刻正常用户节点SN的数量。

网络攻防博弈研究中，一般假设所研究的网络攻防系统是确定的，则可认为系统中网络节点的总数量保持不变，记为QN。网络节点的攻防博弈结果引发节点安全状态转移，导致不同类型节点数量动态变化。但无论网络节点安全状态如何转移，t时刻3类安全状态节点数量之和保持不变，即

$$\mathrm{IN}(t)+\mathrm{RN}(t)+\mathrm{SN}(t)=\mathrm{QN} \tag{5}$$

刘小虎等人[12]给出了网络攻防策略对抗结果判定方法，将攻击方和防御方分别视为智能体，采用不同类型的智能体数量表示网络攻防态势，改进NetLogo 模型库中“狼-羊-草”模型开展了仿真实验。但是，仅依靠某一类型智能体数量无法直观反映网络攻防态势。网络节点密度指某类型节点占网络节点总数量的比例。网络节点密度越高，则该类型智能体在攻防中越占优。特定时刻，不同类型网络节点密度反映了攻击感染节点、正常用户节点和防御部署节点在网络系统的整体分布情况，刻画了网络攻防态势。

定义2 网络攻防态势(Network Attack and Defense Situation, NADS)由3类网络节点密度组成$x(t)=(\rho_{\mathrm{IN}},\rho_{\mathrm{SN}},\rho_{\mathrm{RN}})$。其中，攻击感染节点IN密度$\rho_{\mathrm{IN}}(t)=\dfrac{\mathrm{IN}(t)}{\mathrm{QN}}$，防御部署节点RN密度$\rho_{\mathrm{RN}}(t)=\dfrac{\mathrm{RN}(t)}{\mathrm{QN}}$，正常用户节点SN密度$\rho_{\mathrm{SN}}(t)=\dfrac{\mathrm{SN}(t)}{\mathrm{QN}}$，$\rho_{\mathrm{IN}}(t)+\rho_{\mathrm{RN}}(t)+\rho_{\mathrm{SN}}(t)=1$。则$t$时刻网络攻防态势NADS($t$)用式(6)表示。

$$\mathrm{NADS}(t)=\begin{cases}x(t)=(\rho_{\mathrm{IN}},\rho_{\mathrm{SN}},\rho_{\mathrm{RN}})\\ \rho_{\mathrm{IN}}(t)=\dfrac{\mathrm{IN}(t)}{\mathrm{QN}}\\ \rho_{\mathrm{RN}}(t)=\dfrac{\mathrm{RN}(t)}{\mathrm{QN}}\\ \rho_{\mathrm{SN}}(t)=\dfrac{\mathrm{SN}(t)}{\mathrm{QN}}\\ \rho_{\mathrm{IN}}(t)+\rho_{\mathrm{RN}}(t)+\rho_{\mathrm{SN}}(t)=1\end{cases} \tag{6}$$

将网络节点视为智能体，通过微观层面攻防智能体间博弈行为，分析宏观层面网络攻防态势演化现象。与经典传染病SIR模型不同的是，由于攻击方和防御方的博弈行为，存在4条网络节点智能体安全状态转移路径，如图2所示：

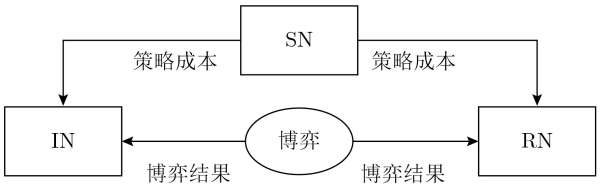

图 2 网络节点智能体安全状态转移路径

(1) SN→IN：攻击方付出一定策略成本后，可将攻击策略部署至SN节点，使其变为IN节点；若攻击方无法负担部署攻击策略的代价，则不能实现安全状态转移。

(2) SN→RN：防御方付出一定策略成本后，可将防御策略部署到SN节点，使其变为RN节点；若防御方无法负担部署防御策略的代价，则不能实现安全状态转移。

(3) RN→IN：攻击方策略强度比防御方策略强度高，网络节点无法有效抵御攻击，节点变为IN节点。

(4) IN→RN：防御方策略强度比攻击方策略强度高，网络节点成功清除攻击策略，节点变为RN节点。

4 网络勒索病毒攻防案例仿真分析

4.1 网络勒索病毒攻防行为分析

勒索病毒是常见的网络攻击形式之一，近两年呈持续高发态势，影响较大的有WannCry, Bad-Rabbit, GandCrab和Sodinokibi等[25]。勒索病毒主要以利用系统漏洞或社会工程学方式发送邮件、布设木马等形式进行传播，一旦感染用户主机，则加密其存储的数据，理论上不可破解，用户需支付赎金才能获得解密密钥。勒索病毒类型多、变种快，若不及时升级防御措施则无法有效免疫。防御勒索病毒需要从技术和管理两方面做起，防御策略主要包括安装反病毒软件并更新病毒库、及时安装系统漏洞补丁、关闭非必需的共享功能以及端口、使用高强度密码并动态更换、定期备份关键数据等。我们以勒索病毒的攻击与防御为例，建立网络攻防博弈模型并进行态势演化分析。

勒索病毒攻防博弈模型中，攻防局中人分别为勒索病毒攻击方N_{A}和网络安全防御方N_{D}；将防御方划分为两种类型$\Theta_{\mathrm{D}}=(\Theta_{\mathrm{DH}},\Theta_{\mathrm{DL}})$，分别表示增强型防御和普通型防御。防御方为增强型防御类型时，网络安全意识较强，防御能力相对较高；防御方为普通型防御类型时，网络安全意识薄弱，防御能力相对较低。例如，早在2017年3月，微软公司就已经公布了针对MS17-010漏洞的补丁包，5月12日WannCry全球爆发，一部分用户升级了系统，可认为属于增强型防御类型，另一部分用户没有升级系统，可认为属于普通型防御类型。防御方

属于以上两种类型的概率分别是P_{DH}和P_{DL}。将攻击方划分为两种类型$\Theta_{\mathrm{A}}=(\Theta_{\mathrm{AH}},\Theta_{\mathrm{AL}})$，分别表示增强型攻击和普通型攻击。勒索病毒种类较多、版本不同，攻击能力有所区别。例如，GandCrab自2018年年初出现，从1.0版本逐步升级到5.2版本，低版本的病毒逐渐被防御方破解和查杀。将攻击能力强、熟练运用组合式漏洞扫描和深度社会工程学工具的用户视为增强型攻击类型，攻击能力弱、勉强运用简单漏洞扫描和一般社会工程学工具的用户视为普通型攻击类型。攻击方属于以上两种类型的概率分别是P_{AH}和P_{AL}。参考美国麻省理工学院(MIT)林肯实验室攻防行为数据库[26]的分级方法，将攻击策略划分为$S_{\mathrm{A}}=\{A_1,A_2,A_3,A_4\}$，将防御策略划分为$S_{\mathrm{D}}=\{D_1,D_2,D_3,D_4\}$，勒索病毒攻防类型及策略划分如表1所示。

表 1　勒索病毒攻防类型及策略划分

攻防类型	攻防策略	策略含义
Θ_{DH}	D_1	安全意识强，及时升级系统和病毒库等
	D_2	安全意识强，及时修补漏洞等
Θ_{DL}	D_3	安全意识弱，延迟升级系统和病毒库等
	D_4	安全意识弱，延迟修补漏洞等
Θ_{AH}	A_1	攻击能力强，熟练运用漏洞扫描攻击等
	A_2	攻击能力强，熟练运用社会工程学攻击等
Θ_{AL}	A_3	攻击能力弱，勉强运用漏洞扫描攻击等
	A_4	攻击能力弱，勉强运用社会工程学攻击等

根据3.2节分析，采用两次海萨尼转换，得出勒索病毒攻防贝叶斯博弈树如图3所示。

攻击回报AR主要包括被用户支付赎金、攻击方影响力的提升等，感染主机数量越多，攻击回报越大；攻击成本AC主要包括制作和释放勒索病毒的代价，以及若在传播病毒过程中被发现，存在被反制和惩罚的代价等。防御回报DR主要包括因实施勒索病毒防御策略而免于遭受的损失，以及被感染后成功修复所带来的回报等；防御成本DC主要包括实施勒索病毒防御策略代价、安全管理代价，以及若被感染进行数据修复的代价等。依据勒索病毒攻防实际，基于历史数据统计和回归分析，并结合安全专家经验，分别给出系统损失代价SDC、攻击代价AC、防御代价DC，然后利用式(1)计算得出不同策略组合下防御收益$U_{\mathrm{D}}(D_g,A_h)$、攻击收益$U_{\mathrm{A}}(D_g,A_h)$，如表2所示。

采用Gambit15.0制作勒索病毒攻防博弈模型的工程实例，如图4所示。通过运行工程实例求解得出勒索病毒攻防博弈模型的贝叶斯纳什均衡解。

4.2　网络勒索病毒攻防态势仿真

网络信息系统由大量节点组成，单个网络攻防节点博弈行为无法展示网络攻防态势，仿真是解决该问题行之有效的途径。NetLogo是一款开源的多智能体仿真工具，能够同时模拟大量节点的智能交互行为[27]。仿真实验中设置网络信息系统节点总数为1000个，平均节点度为6，IN节点个数为10，生

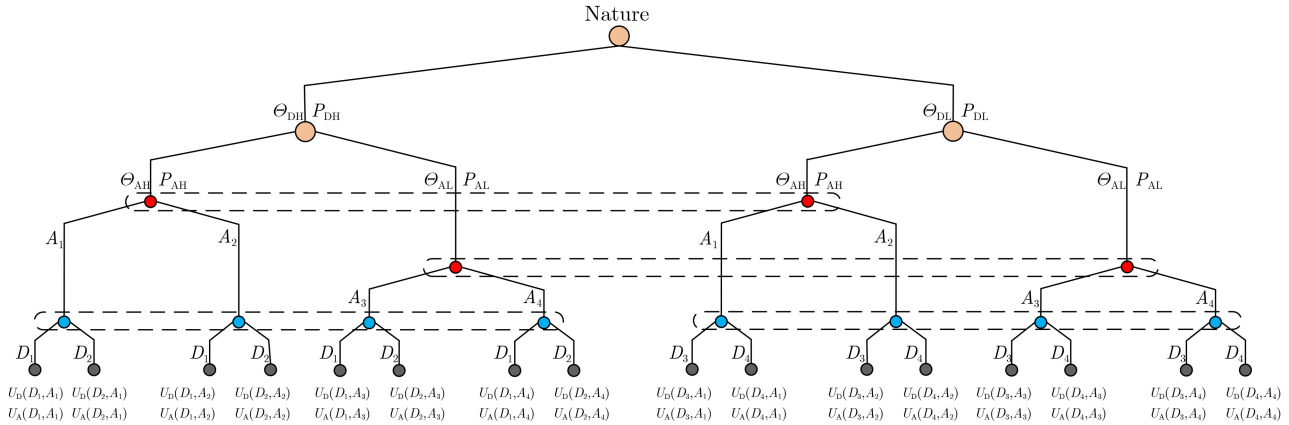

图 3 勒索病毒贝叶斯博弈树

表 2　不同策略组合下攻防收益

防御策略	攻击策略			
	A_1	A_2	A_3	A_4
D_1	(530,800)	(550,780)	(800,360)	(820,330)
D_2	(410,910)	(420,890)	(780,380)	(800,350)
D_3	(120,1580)	(130,1560)	(240,770)	(260,740)
D_4	(100,1820)	(110,1940)	(210,810)	(220,780)

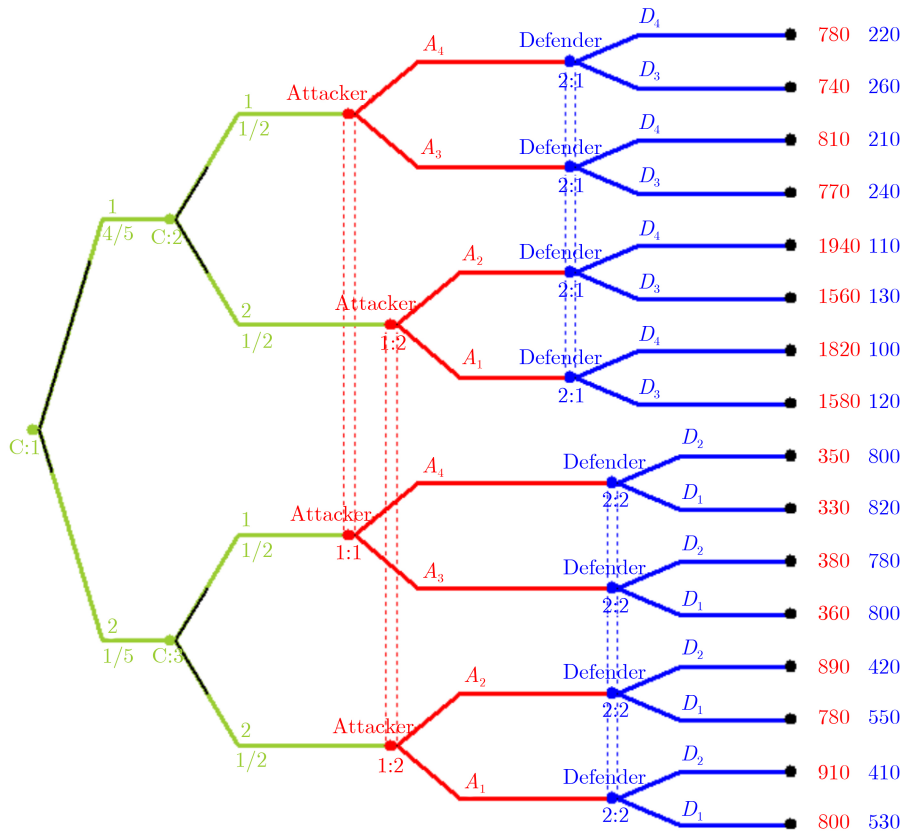

图 4 勒索病毒攻防博弈模型Gambit工程实例

成初始网络攻防态势如图5所示，其中红色节点表示攻击感染节点IN，蓝色节点表示增强型防御节点RN，灰色节点表示普通型防御节点SN。

通过设置不同的仿真参数，动态模拟不同场景下网络攻防态势演化趋势，如图6—图11所示。图中横坐标均为仿真时间，纵坐标均为不同类型节点数占网络节点总数的比例。从网络信息系统的机密性、完整性和可用性等方面综合考虑，设定当攻击感染节点IN比例峰值大于5%时，则可认为勒索病毒大规模爆发，当攻击感染节点IN比例峰值大于50%时，则认为由于勒索病毒攻击造成网络信息系统瘫痪。

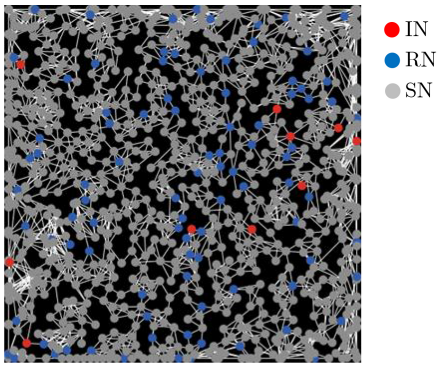

图 5 初始网络攻防态势

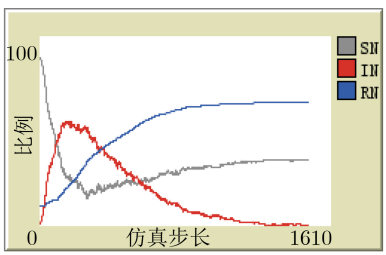

图 6 RN=100时攻防态势演化

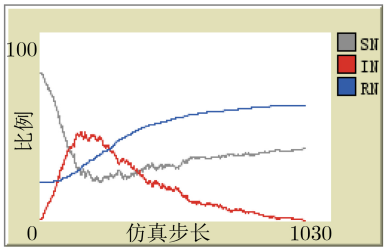

图 7 RN=200时攻防态势演化

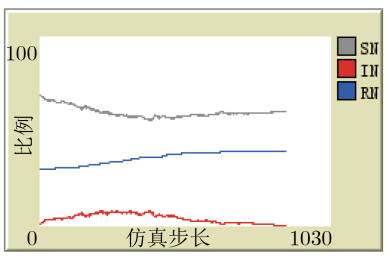

图 8 RN=300时攻防态势演化

场景1(图6)：初始RN节点100个，模拟防御方属于增强型防御类型概率为0.1的情况。经Gambit工程实例计算，博弈均衡时攻防收益$(U_{\mathrm{A}}, U_{\mathrm{D}}) = (1115.5, 228.5)$。通过观察可得，当$t$=198时，IN节点比例的峰值达到了51.2%。该场景下网络攻防态势演化趋势是，勒索病毒在较短时间内大规模爆发，并可能引起网络信息系统瘫痪。

场景2(图7)：初始RN节点200个，模拟防御方属于增强型防御类型概率为0.2的情况。经Gambit工程实例计算，博弈均衡时攻防收益$(U_{\mathrm{A}}, U_{\mathrm{D}}) = (1056, 277)$。通过观察可得，当$t$=127时，IN节点比例的峰值达到了39.4%。该场景下网络攻防态势演化趋势是，勒索病毒在一定时间内大规模爆发，并可能对网络信息系统造成重大损害。

场景3(图8)：初始RN节点300个，模拟防御方属于增强型防御类型概率为0.3的情况。经Gambit工程实例计算，博弈均衡时攻防收益$(U_{\mathrm{A}}, U_{\mathrm{D}}) = (996.5, 325.5)$。通过观察可得，当$t$=322时，IN节点比例的峰值达到了8.7%。该场景下网络攻防态势演化趋势是，勒索病毒在一定规模爆发，并可能对网络信息系统造成一定损害。

场景4(图9)：初始RN节点363个，模拟防御方属于增强型防御类型概率为0.363的情况。经Gambit工程实例计算，博弈均衡时攻防收益$(U_{\mathrm{A}}, U_{\mathrm{D}}) = (959.0, 356.1)$。通过观察可得，当$t$=81时，IN节点比例的峰值达到了5.0%。该场景下网络攻防态势演化趋势是，勒索病毒并未大规模爆发，对网络信息系统造成较小损害。

场景5(图10)：初始RN节点400个，模拟防御方属于增强型防御类型概率为0.4的情况。经Gambit工程实例计算，博弈均衡时攻防收益$(U_{\mathrm{A}}, U_{\mathrm{D}}) = (937.0, 374.0)$。通过观察可得，当$t$=221时，IN节点比例的峰值达到了3.8%。该场景下网络攻防态势演化趋势是，勒索病毒感染范围较小，并没有大规模爆发，且在一段时间内得到清除。

场景6(图11)：初始RN节点500个，模拟防御方属于增强型防御类型概率为0.5的情况。经Gambit工程实例计算，博弈均衡时攻防收益$(U_{\mathrm{A}}, U_{\mathrm{D}}) = (877.5, 422.5)$。通过观察可得，IN节点比例的峰值没有出现。该场景下网络攻防态势演化趋势是，勒索病毒难以爆发，并且可在较短时间内(相对于场景1-场景5)得到清除。

通过对比不同场景下的仿真结果，可得出两条结论：

(1) 微观层面网络攻防博弈行为影响宏观层面态势演化趋势。网络攻防对抗中，不同的攻防行为产生不同的博弈结果。对比图6—图11可知，若网络攻防博弈均衡时防御方收益越高、攻击方收益越低，则IN节点比例的峰值越来越低，表示勒索病毒存活的时间和扩散的范围相对越小，网络攻防态势演化趋势越有利于防御方。因此，从微观层面的网络攻防行为入手，量化和计算博弈收益，通过不同的博弈均衡分析宏观层面网络攻防态势演化现象，能够提高对攻防态势演化规律的认识，有助于指导防御策略选取，增强防御效能。

(2) 增强单个节点防御能力是扭转网络攻防态势的关键。对比图6、图7、图8可知，当防御方属于增强型防御类型概率小于等于0.363时，IN节点比例出现峰值，勒索病毒能够在网络中大规模爆发，甚至在图6中比例峰值超过了50%，造成网络信息系统瘫痪；对比图9、图10、图11可知，当防御方属于增强型防御类型概率超过0.363时，IN节点比例峰值较低，甚至在图10中没有出现，表明勒索病毒不能够在网络中大规模爆发。因此，应增强对网络安全的重视程度，提高网络节点防御能力。同时，加大对网络攻击的事先检测和事后惩治力

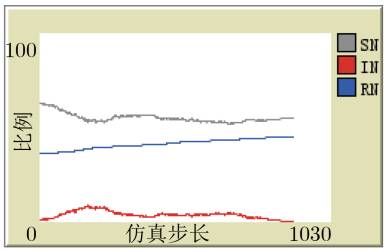

图 9 RN=363时攻防态势演化

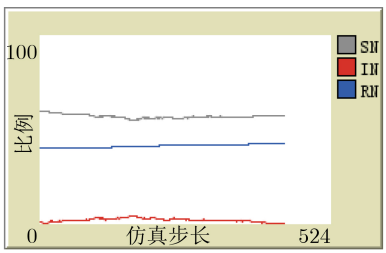

图 10 RN=400时攻防态势演化

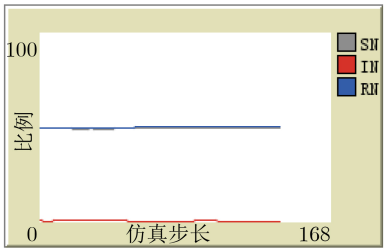

图 11 RN=500时攻防态势演化

度。一方面有力震慑攻击方，另一方面增大攻击方的攻击成本和复杂度，降低预期收益，从而扭转网络攻防态势。

将研究成果与相关文献进行对比，结果如表3所示。

在博弈信息方面，本文基于不完全信息博弈分析网络攻防对抗行为，攻防双方均具有多种类型；在态势演化分析方面，本文借鉴传染病动力学理论，提出了一种网络攻防态势定义及演化分析方法；在网络攻防实验场景方面，本文采用NetLogo多智能体仿真工具动态模拟网络攻防态势随时间演化趋势，仿真场景中网络节点规模大。相比于相关文献，本文方法更加符合网络攻防双方所拥有信息不完备的实际，能够从微观网络攻防行为层面分析和解释宏观态势演化趋势，具有适用于大规模场景、态势展现直观等优势。

表 3 研究成果对比

文献	博弈信息	态势演化分析	网络攻防实验场景	网络节点规模	态势展现效果
文献[7]	完全信息	缺乏	实物攻防环境	节点数≤10	无
文献[8]	完全信息	缺乏	实物攻防环境	节点数≤10	无
文献[9]	不完全信息	缺乏	实物攻防环境	节点数≤10	无
文献[12]	不完全信息	不详细	NetLogo多Agent仿真	节点数≥1000	直观
本文	不完全信息	传染病动力学	NetLogo多Agent仿真	节点数≥1000	直观

5 结论

本文从博弈视角研究网络攻防行为建模与态势演化问题。基于不完全信息静态理论构建了网络攻防博弈模型，给出攻防收益计算量化和博弈均衡求解方法；借鉴传染病动力学理论，采用不同安全状态节点密度定义网络攻防态势，分析网络节点状态转移路径；以网络勒索病毒攻防博弈为例对方法进行了应用，采用NetLogo多Agent仿真工具动态模拟不同场景下网络攻防态势随时间演化趋势。通过分析仿真结果，给出两条关于网络攻防态势演化的认识。

参 考 文 献

[1] 屈蕾蕾, 肖若瑾, 石文昌, 等. 涌现视角下的网络空间安全挑战[J]. 计算机研究与发展, 2020, 57(4): 803–823. doi: 10.7544/issn1000-1239.2020.20190379.

QU Leilei, XIAO Ruojin, SHI Wenchang, *et al*. Cybersecurity challenges from the perspective of emergence[J]. *Journal of Computer Research and Development*, 2020, 57(4): 803–823. doi: 10.7544/issn1000-1239.2020.20190379.

[2] LIU Xiaohu, ZHANG Hengwei, ZHANG Yuchen, *et al*. Optimal network defense strategy selection method based on evolutionary network game[J]. *Security and Communication Networks*, 2020, 2020: 5381495. doi: 10.1155/2020/5381495.

[3] TAN Jinglei, LEI Cheng, ZHANG Hongqi, *et al*. Optimal strategy selection approach to moving target defense based on Markov robust game[J]. *Computers & Security*, 2019, 85: 63–76. doi: 10.1016/J.COSE.2019.04.013.

[4] 张焕国, 杜瑞颖. 网络空间安全学科简论[J]. 网络与信息安全学报, 2019, 5(3): 4–18. doi: 10.11959/j.issn.2096-109x.2019021.

ZHANG Huanguo and DU Ruiying. Introduction to cyberspace security discipline[J]. *Chinese Journal of Network and Information Security*, 2019, 5(3): 4–18. doi: 10.11959/j.issn.2096-109x.2019021.

[5] PAWLICK J, COLBERT E, and ZHU Quanyan. A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy[J]. *ACM Computing Surveys*, 2019, 52(4): 82. doi: 10.1145/3337772.

[6] 徐瑨, 吴慧慈, 陶小峰. 5G网络空间安全对抗博弈[J]. 电子与信息学报, 2020, 42(10): 2319–2329. doi: 10.11999/JEIT200058.

XU Jin, WU Huici, and TAO Xiaofeng. 5G cyberspace security game[J]. *Journal of Electronics & Information Technology*, 2020, 42(10): 2319–2329. doi: 10.11999/JEIT200058.

[7] 姜伟, 方滨兴, 田志宏, 等. 基于攻防博弈模型的网络安全测评和最优主动防御[J]. 计算机学报, 2009, 32(4): 817–827. doi: 10.3724/SP.J.1016.2009.00817.

JIANG Wei, FANG Binxing, TIAN Zhihong, *et al*. Evaluating network security and optimal active defense based on attack-defense game model[J]. *Chinese Journal of Computers*, 2009, 32(4): 817–827. doi: 10.3724/SP.J.1016.2009.00817.

[8] 王增光, 卢昱, 李玺. 基于攻防博弈的军事信息网络安全风险

评估[J]. 军事运筹与系统工程, 2019, 33(2): 35–40, 47. doi: 10.3969/j.issn.1672-8211.2019.02.007.

WANG Zengguang, LU Yu, and LI Xi. Risk assessment of military information network security based on attack defense game[J]. *Military Operations Research and Systems Engineering*, 2019, 33(2): 35–40, 47. doi: 10.3969/j.issn.1672-8211.2019.02.007.

[9] 王晋东, 余定坤, 张恒巍, 等. 基于不完全信息攻防博弈的最优防御策略选取方法[J]. 小型微型计算机系统, 2015, 36(10): 2345–2348. doi: 10.3969/j.issn.1000-1220.2015.10.033.

WANG Jindong, YU Dingkun, ZHANG Hengwei, *et al*. Defense strategies selection based on incomplete information attack-defense game[J]. *Journal of Chinese Computer Systems*, 2015, 36(10): 2345–2348. doi: 10.3969/j.issn.1000-1220.2015.10.033.

[10] 王晋东, 余定坤, 张恒巍, 等. 静态贝叶斯博弈主动防御策略选取方法[J]. 西安电子科技大学学报: 自然科学版, 2016, 43(1): 144–150. doi: 10.3969/j.issn.1001-2400.2016.01.026.

WANG Jindong, YU Dingkun, ZHANG Hengwei, *et al*. Active defense strategy selection based on the static Bayesian game[J]. *Journal of Xidian University*, 2016, 43(1): 144–150. doi: 10.3969/j.issn.1001-2400.2016.01.026.

[11] 张烙兵, 阮启明, 邱晓刚. 研究社会复杂系统的两种互补方法: 仿真与博弈论[J]. 系统仿真学报, 2019, 31(10): 1960–1969. doi: 10.16182/j.issn1004731x.joss.19-0513.

ZHANG Laobing, RUAN Qiming, and QIU Xiaogang. Two complementary methods for studying complex social systems: Simulation and game theory[J]. *Journal of System Simulation*, 2019, 31(10): 1960–1969. doi: 10.16182/j.issn1004731x.joss.19-0513.

[12] 刘小虎, 张恒巍, 张玉臣, 等. 基于博弈模型与NetLogo仿真的网络攻防态势研究[J]. 系统仿真学报, 2020, 32(10): 1918–1926. doi: 10.16182/j.issn1004731x.joss.20-fz0290.

LIU Xiaohu, ZHANG Hengwei, ZHANG Yuchen, *et al*. Research on network attack and defense situation based on game theory model and NetLogo simulation[J]. *Journal of System Simulation*, 2020, 32(10): 1918–1926. doi: 10.16182/j.issn1004731x.joss.20-fz0290.

[13] LIU Xiaohu, ZHANG Hengwei, ZHANG Yuchen, *et al*. Active defense strategy selection method based on two-way signaling game[J]. *Security and Communication Networks*, 2019, 2019: 1362964. doi: 10.1155/2019/1362964.

[14] 谭晶磊, 张恒巍, 张红旗, 等. 基于Markov时间博弈的移动目标防御最优策略选取方法[J]. 通信学报, 2020, 41(1): 42–52. doi: 10.11959/j.issn.1000-436x.2020003.

TAN Jinglei, ZHANG Hengwei, ZHANG Hongqi, *et al*. Optimal strategy selection approach of moving target defense based on Markov time game[J]. *Journal on Communications*, 2020, 41(1): 42–52. doi: 10.11959/j.issn.1000-436x.2020003.

[15] 姜伟, 方滨兴, 田志宏, 等. 基于攻防随机博弈模型的防御策略选取研究[J]. 计算机研究与发展, 2010, 47(10): 1714–1723.

JIANG Wei, FANG Binxing, TIAN Zhihong, *et al*. Research on defense strategies selection based on attack-defense stochastic game model[J]. *Journal of Computer Research and Development*, 2010, 47(10): 1714–1723.

[16] FUDENBERG D and TIROLE J. Game Theory[M]. Boston: Massachusetts Institute of Technology Press, 2019.

[17] ZHANG Hengwei, YU Dingkun, WANG Jindong, *et al*. Security defence policy selection method using the incomplete information game model[J]. *China Communications*, 2015(S2): 123–131.

[18] MCKELVEY R D, MCLENNAN A M, and TUROCY T L. Gambit: Software tools for game theory, version 16.0.1[EB/OL]. http://www.gambit-project.org, 2016.

[19] HUSTED N and MYERS S. Emergent properties & security: The complexity of security as a science[C]. Proceedings of the 2014 New Security Paradigms Workshop, Victoria, 2014: 1–14. doi: 10.1145/2683467.2683468.

[20] SHASHIDHAR N, KARI C, and VERMA R. The efficacy of epidemic algorithms on detecting node replicas in wireless sensor networks[J]. *Journal of Sensor and Actuator Networks*, 2015, 4(4): 378–409. doi: 10.3390/jsan4040378.

[21] 孟庆微, 仇铭阳, 王刚, 等. 零日病毒传播模型及稳定性分析[J]. 电子与信息学报, 2021, 43(7): 1849–1855. doi: 10.11999/JEIT200519.

MENG Qingwei, QIU Mingyang, WANG Gang, *et al*. Zero-day virus transmission model and stability analysis[J]. *Journal of Electronics & Information Technology*, 2021, 43(7): 1849–1855. doi: 10.11999/JEIT200519.

[22] ZHANG Hengwei, JIANG Lv, HUANG Shirui, *et al*. Attack-defense differential game model for network defense strategy selection[J]. *IEEE Access*, 2018, 7: 50618–50629. doi: 10.1109/ACCESS.2018.2880214.

[23] 张恒巍, 李涛, 黄世锐. 基于攻防微分博弈的网络安全防御决策方法[J]. 电子学报, 2018, 46(6): 1428–1435. doi: 10.3969/j.issn.0372-2112.2018.06.023.

ZHANG Hengwei, LI Tao, and HUANG Shirui. Network defense decision-making method based on attack-defense differential game[J]. *Acta Electronica Sinica*, 2018, 46(6): 1428–1435. doi: 10.3969/j.issn.0372-2112.2018.06.023.

[24] VARGAS-DE-LEÓN C. On the global stability of *SIS*, *SIR* and *SIRS* epidemic models with standard incidence[J]. *Chaos*, *Solitons* & *Fractals*, 2011, 44(12): 1106–1110. doi: 10.1016/j.chaos.2011.09.002.

[25] SHARMEEN S, AHMED Y A, HUDA S, *et al*. Avoiding future digital extortion through robust protection against ransomware threats using deep learning based adaptive approaches[J]. *IEEE Access*, 2020, 8: 24522–24534. doi: 10.1109/ACCESS.2020.2970466.

[26] GORDON L, LOEB M, LUCYSHYN W, *et al*. 2015 CSI/FBI computer crime and security survey[C]. The Computer Security Institute, San Francisco, USA, 2015: 48–64.

[27] TISUE S and WILENSKY U. NetLogo: A simple environment for modeling complexity[C]. The 5th International Conference on Complex Systems, Trieste, Italy, 2004: 16–21.

刘小虎：男，1989年生，博士生，讲师，研究方向为网络攻防博弈、网络建模仿真.

张恒巍：男，1978年生，博士，副教授，研究方向为网络攻防博弈.

张玉臣：男，1977年生，博士，副教授，研究方向为网络空间安全战略.

胡 浩：男，1989年生，博士，讲师，研究方向为网络态势感知.

程 建：男，1990年生，硕士，讲师，研究方向为网络建模仿真.

责任编辑：马秀强