基于激励机制的网络攻防演化博弈模型研究

徐晓桐,王高才,胡锦天

(广西大学 计算机与电子信息学院,南宁 530004)
E-mail:wanggcgx@163.com

摘　要: 随着网络信息系统的日益复杂化,网络的安全性和用户隐私性引起了人们的高度重视,寻找能够维护网络安全、分析和预判网络攻防形式的新技术尤为重要.由于演化博弈理论的特性与网络攻防的特性较为契合,因此,本文对网络环境进行了分析,构建网络攻防场景,并在惩罚机制的基础上引入激励机制,提出了基于激励机制的攻防演化博弈模型.通过给出群体不同的问题情境,利用复制动态方程对局中人的策略选取进行演化分析.另外,在第三方监管部门对局中人管理的基础上,分析不同攻击时长时攻击群体的演化规律,证明攻击具有时效性.通过激励机制对防御群体策略选取的影响以及引入防御投资回报,来进一步证明增加激励机制的可行性.根据实验验证表明,本文提出的攻防演化博弈模型在不同的问题情境下均可达到稳定状态并获得最优防御策略,从而有效减少防御方的损失,遏制攻击方的攻击行为.

关 键 词: 演化博弈;激励机制;网络攻防;最优防御策略
中图分类号: TP309　　**文献标识码:** A　　**文 章 编 号:** 1000-1220(2020)01-0104-07

Research on Evolutionary Game Model of Network Attack and Defense Based on Incentive Mechanism

XU Xiao-tong, WANG Gao-cai, HU Jin-tian
(School of Computer and Electronic and Information, Guangxi University, Nanning 530004, China)

Abstract: With the increasing complexity of network information system, people attach great importance to network security and user privacy. It is especially important to find new technologies that can maintain network security, analyze and predict the form of network attack and defense. Because the characteristics of evolutionary game theory are similar to those of network attack and defense, this paper analyses the network environment, constructs the network attack and defense scenarios, and introduces incentive mechanism on the basis of punishment mechanism, and proposes an evolutionary game model of attack and defense based on incentive mechanism. By giving the different problem situations of the group, the replication dynamic equation is used to analyze the evolution of the strategy selection of the player. In addition, on the basis of the management of players in the third-party supervision department, the evolution law of attack groups in different attack time is analyzed, which proves that the attack is time-sensitive. The feasibility of the incentive mechanism is further proved by the impact of incentive mechanisms on the selection of defense group strategies and the introduction of defense investment returns. According to the experimental verification, the attack and defense evolutionary game model proposed in this paper can achieve the steady state and obtain the optimal defense strategy under different problem situations, thus effectively reducing the loss of the defender and curbing the attack behavior of the attacker.

Key words: evolutionary game; incentive mechanism; network attack-defense; optimal defense strategy

1 引　言

随着互联网规模的扩大,网络的安全性和用户隐私性受到了极大地干扰,网络安全问题在现代社会中也引起了人们的高度注视,网络的安全性已经变成阻碍信息技术发展的重要因素之一.针对网络环境以及攻击手段的日趋复杂化,仅仅依靠一些被动的防御措施已无法保障网络空间的安全.因此,寻找能够对网络环境进行检测,并能及时预判是否安全进而积极采取防御手段的新技术尤为必要.

博弈论的研究最早出现于经济学研究领域,1944 年冯·诺依曼(von Neumann)和摩根斯坦(Morgenstern)提出了"博弈论与经济学",受到了人们的广泛关注[1].演化博弈理论是一种将博弈理论与动态演化过程相结合的理论,它是在传统博弈论的基础之上引进了生物学的进化理论.演化博弈论能够在各个不同的领域获得极大的发展应归功于史密斯(Smith,1973)与普瑞斯(Price,1974)[2],他们提出了演化博弈理论中的基本概念:演化稳定策略(Evolutionary Stable Strategy ESS).其中,参与者将不再是完全理性的个体,而是介于完全理性和非完全理性之间的、在一定限制条件下的有限理性.群体之间的局中人在演化过程中不断地纠错、模仿和

收稿日期:2019-03-15　收修改稿日期:2019-04-15　基金项目:国家自然科学基金项目(61562006)资助;广西自然科学基金项目(2016GXNSFBA380181)资助.　作者简介:**徐晓桐**,女,1995 年生,硕士研究生,研究方向为网络安全主动防御、计算机网络;**王高才**,男,1976 年生,博士,教授,博士生导师,CCF 高级会员,研究方向为计算机网络、系统性能评价和随机方法;**胡锦天**,男,1992 年生,硕士研究生,研究方向为移动边缘计算、无线网络.

改进,一步步趋向于某种稳定策略,最终达到一种博弈的平衡状态,从而获得最优策略以最大化自身利益的问题.

在网络攻防中,入侵者做出某些行为来实施入侵以及一个计算机网络做出某些行为来防止或抵抗攻击的过程与演化博弈的过程具有相似之处,因此,相当多的研究通过建立网络攻防博弈模型,来更加直观的选取最优策略[3-6]. 在网络安全领域,典型的演化博弈模型包括两个对抗的参与者:攻击者和防御者. 攻击者会试图在防御者的控制下破坏或摧毁网络环境,防御者可以通过增加自身的安全投资来增强网络环境的防御能力. 基于局中人的有限理性原则,攻防双方通过结合历史经验来改进各自的策略选择. 通过不断地学习和改进体制,攻防双方逐渐演变为稳定状态,有效提高了防御方选取最优策略的可靠性和准确性,保障了网络空间的安全.

本文的组织结构如下:第 2 节介绍相关研究工作;第 3 节介绍网络攻防演化博弈模型及相应概念;第 4 节讨论演化博弈最优策略算法的描述;第 5 节进行仿真实验并对实验结果进行分析;最后第 6 节对全文进行了总结.

2　相关研究工作

博弈论在网络安全方面的应用已经成为最近几年的一个研究热潮,由于传统的博弈理论需要满足太多的前提条件,比如完全信息条件等等,这与实际网络环境有较大的出入,从而削弱了博弈模型的实际应用范围. 因此,研究人员开始将演化博弈理论引入网络安全的研究中. 关注方向主要有以下三个方面:一是关于网络环境脆弱性的分析;二是信息安全的防御投资策略;三是关于网络群体行为的研究.

在对网络环境的脆弱性分析时,王元卓等人建立了基于随机 Petri 网的攻防博弈模型[7],可以对目标网络的攻击成功率、平均攻击时间、脆弱节点以及潜在攻击路径等方面进行安全分析与评价. J Liu 等人提出了一种博弈理论方法制定了涉及多个检测和防御决策的问题[8],以此来优化入侵检测策略、降低能耗以及减少了报警信息,提高了传感器云中数据的安全性. Alabdel Abass 等人使用演化博弈理论分析了云存储的 APT(Advanced Persistent Threat 高级持续性威胁)攻击/防御策略[9],利用复制动态方程来研究云存储系统的动态稳定性,以表征局部渐近稳定的均衡策略,并显示其间的关系渐近稳定性和演化稳定性. Yezekael Hayel 等人构建了演化泊松博弈模型[10],并设计了控制软件用户行为以实现系统目标的机制. 为了寻求最优策略集,Liu 等认为在研究基本协同演化方法上,鲁棒性是一个重要指标,并且他们研究了群体协同攻击规则对合作博弈攻击的鲁棒性[11]. 然而该模型仍局限于需要完全信息. 事实上,由于不同的参与者具有不同的认知能力以及非对称的信息,策略演化的过程将不可避免地缺乏远见. 因此,探索非确定性策略演化分析具有重要意义. Hu 等人利用复制动态方程来描述攻防行为[12],总结了不同类型参与者采取不同策略的演化过程,并通过计算演化稳定均衡给出了最优的防御策略. 张云等人提出一种基于不完全信息的攻防博弈模型[13],使用证据理论来描述信息的模糊性,更加全面的寻求最优防御策略. 文献[14]在博弈论的基础上,优化了网络安全评估机制. 文献[15]在非合作演化博弈的基础上,提出了具有不对称信息的演化博弈模型,并利用系统动力学对模型进行演化分析,通过引入第三方惩罚机制来进一步解决网络安全问题.

由于演化博弈研究的范围和应用范围正在不断扩大,Wang 等人在研究信息安全时使用演化博弈论来寻求长期最优安全投资策略,分别考虑了针对性和机会性两种类型的攻击的最优信息安全投资问题[16]. Zhang 等人利用演化博弈理论[17],解决网络安全攻防交互中的决策问题,并为防御者提供量化的方法来计算安全收益. 通过这种量化方式,可以为网络制定合适的安全策略. Pan 等人提出了一种动态的非对称信息演化博弈模型[18],从微观角度分析了参与者的决策动机,提出了最优投资策略.

另外,在研究网络群体行为时,文献[19]探讨了网络群体中用于隐私保护的群体结构演化博弈,它可以改进网络群体用户之间的隐私保护行为,并促进整个网络中隐私保护行为的传播;王元卓等人在介绍网络群体行为评估标准时[20],利用演化博弈模型讨论其群体行为的可行性. 文献[21]利用系统动力学对多个网络群体系统进行实验,评估了群体演化状态的稳定性,为特定策略的演化稳定性提供了相应的条件.

针对已有的研究结果,本文研究并提出了一种引入第三方激励机制的网络攻防演化博弈模型,将激励机制与惩罚机制相结合,并根据网络攻防场景对网络攻防群体的行为策略演化趋势进行分析,在此基础上寻求最优防御策略. 有效的提高了防御者的收益,抑制了攻击者的攻击行为.

3　基于激励机制的演化博弈模型

在网络攻防中,由于攻击者和防御者的有限理性致使攻防群体会选择不同的策略进行博弈. 双方在攻防过程中通过不断地试错、调整和改进自己的决策手段,从而形成新的攻防博弈局面.

3.1　模型定义

由于实际网络环境较为复杂,且攻防群体策略选择是有限理性行为,因此,本文在不完全信息的条件下定义了网络攻防演化博弈模型 *NADEGM*(Network Attack-Defense Evolution Game Model).

定义 1. 将网络攻防演化博弈模型定义为一个三元组 $NADEGM=(N,S,U)$,其中:

① $N=(N_A,N_D)$ 代表攻防演化博弈的局中人,即在博弈过程中采取某种策略的参与者. 参与者在不同的环境下具有不同的意义,它能够代表个体,也能够代表一个团队,个体或者团队组成的群体叫做局中人策略集. 这里 N_A 是攻击者,N_D 是防御系统.

② $S=(S_A,S_D)$ 表示局中人的策略集合,是局中人进行博弈的工具和手段. 其中 $S_A=(S_{A1},S_{A2},\cdots,S_{Am})$ 代表攻击策略集合,$S_D=(S_{D1},S_{D2},\cdots,S_{Dn})$ 代表防御策略集合.

③ $U=(U_A,U_D)$ 是局中人的收益函数集合. 其中,$U_A=(U_A^0,U_A^1)$,U_A^0 代表攻击方不进行攻击时所得到的收益,U_A^1 代表攻击方攻击成功时所得到的收益. $U_D=(U_D^0,U_D^1)$,其中,U_D^0 代表防御方不进行防御投资时的期望收益,U_D^1 代表防御方进行防御投资后的期望收益. 对于攻击方来说,攻击方的

攻击策略可以有 m 种可能;对于防御方来说,防御方的防御策略有 n 种可能性.因此,该收益函数集合也可以用 $M\times N$ 阶矩阵的形式表示:

$$U=\begin{pmatrix} U_{A11}U_{D11} & \cdots & U_{A1n}U_{D1n} \\ \vdots & \ddots & \vdots \\ U_{Am1}U_{Dm1} & \cdots & U_{Amn}U_{Dmn} \end{pmatrix}=$$

$$\begin{pmatrix} (U_{A11}^0,U_{A11}^1)(U_{D11}^0,U_{D11}^1) & \cdots & (U_{A1n}^0,U_{A1n}^1)(U_{D1n}^0,U_{D1n}^1) \\ \vdots & \ddots & \vdots \\ (U_{Am1}^0,U_{Am1}^1)(U_{Dm1}^0,U_{Dm1}^1) & \cdots & (U_{Amn}^0,U_{Amn}^1)(U_{Dmn}^0,U_{Dmn}^1) \end{pmatrix}$$

3.2 参数量化

在分析攻防演化博弈时,我们首先需要给出一些相关定义,便于量化攻防双方收益.

定义 2. 攻击成本 C_A(Attack Cost):表示攻击方实施攻击所需要损耗的财力、物力等.

对于防御方而言,在采取和不采取防御投资策略时,防御方所拥有的抗攻击能力是不同的.相应地,攻击方在此时攻击成功的概率和时间也是不同的.设防御方未投资防御策略时,攻击方攻击成功的概率为 P_0,此时攻击成功所用时间为 t_0,则攻击成本为 $C_A^0=t_0\times P_0$;设防御方投资防御策略时,攻击方攻击成功的概率为 P_1,此时攻击成功所用时间为 t_1,则攻击成本为 $C_A^1=t_1\times P_1$(显然 $C_A^0<C_A^1$).

定义 3. 激励机制酬劳 R(Incentive Mechanism Reward):表示第三方监管部门给予防御方的奖励.

在如今的信息时代,信息资源的占有程度和垄断程度决定了自身的收益.由于目标网络被攻击的原因大多是因为信息的不公开、不透明,导致攻击方想要通过攻击获取一定的信息.因此,社会想要通过激励机制来激励防御方,在不伤害自身利益的前提下适当的公开信息,实现信息共享,为此而受益的社会将会给予防御方一定的奖励,也降低了攻击方攻击所带来的损失.为了降低防御系统被攻击的可能性,防御方选择适当的公开信息得到社会的奖励,公开的信息越有利于社会,激励机制所产生的奖励就会越丰厚.用 R 表示激励机制酬劳,设 $R=\alpha I$(I 表示公开的信息量,α 表示社会受益度).因此,当防御方没有进行防御投资时,设此时防御方公开的信息量为 I_0,则 $R_0=\alpha I_0$;当防御方进行防御投资时,设此时防御方公开的信息量为 I_1,则 $R_1=\alpha I_1$.

定义 4. 惩罚成本 G(Penalty Cost):表示第三方监管部门对攻击方实施攻击的惩罚.

互联网攻击会引发一系列的网络安全问题,用户数据遭遇泄露,网络服务被迫中断,影响了人们的日常工作生活,严重时甚至影响国家安危.因此,第三方监管部门有责任对攻击方违反网络安全的不法行为进行惩治.用 G 表示监管部门对攻击方的惩罚,设惩罚力度系数为 β.因此,当防御方未采取防御投资策略时,攻击方受到的惩罚为 $G_0=\beta P_0$;当防御方采取防御投资策略时,攻击方受到的惩罚为 $G_1=\beta P_1$.

定义 5. 总回报 E(Total Earning)表示攻击方从一次成功攻击中可获得的总回报.

当防御方采取防御投资策略时,攻击方成功攻击的收益为 $P_1E-C_A^1-G_1$;当防御方未采取防御投资策略时,攻击方成功攻击的收益为 $P_0E-C_A^0-G_0$.

防御方作为目标网络本身也具有一定的防御能力,但为了更好的抵抗外来攻击以及保护自身网络环境的稳定状态,防御方可选择增加自身的防御投资来抵抗网络攻击,设防御方增加的投资成本为 V_{add}.设防御方原有的防御能力为 V_0,攻击方攻击成功所带来的损失为 L.所以,当防御方采取防御投资策略时,防御方的损失为 P_1L;防御方未采取防御投资策略时的损失为 P_0L.由公开信息带来的社会奖励分别为 R_0 和 R_1.当攻击方采取攻击策略并攻击成功时,防御方采取防御投资策略的期望收益为 $V_0-V_{add}-P_1L+R_1$;当攻击方采取攻击策略并攻击成功时,防御方未采取防御投资策略的期望收益为 $V_0-P_0L+R_0$.当攻击方没有采取任何攻击行为时,攻击方的期望收益为 0,防御方采取防御投资策略前后的期望收益为 V_0+R_0,$V_0-V_{add}+R_1$.

整理上述涉及的主要参数及意义如表 1 所示.

表 1 主要参数及意义

Table 1 Main parameters and meaning

变量	意义	变量	意义
C_A^0	防御方防御投资前,攻击方所需攻击成本	R	社会对防御方公开信息行为的奖励
C_A^1	防御方防御投资后,攻击方所需攻击成本	G	攻击方由攻击行为所受到的惩罚
P_0	防御方防御投资前,攻击方攻击成功的概率	L	防御方被攻击后遭受的损失
P_1	防御方防御投资后,攻击方攻击成功的概率	E	攻击方一次成功攻击带来的总回报
I_0	防御方防御投资前,防御方公开的信息量	V_0	防御方原有的防御能力(原有资产)
I_1	防御方防御投资前,防御方公开的信息量	V_{add}	防御方增加的防御能力(防御投资)
t_0	防御方防御投资前,攻击方攻击成功的时长	α	公开信息对社会的受益程度系数
t_1	防御方防御投资后,攻击方攻击成功的时长	β	惩罚力度系数

3.3 复制动态方程

假设在攻防博弈过程中,攻击方群体中采取攻击策略的比例为 x,采取不攻击策略的比例为 $1-x$;防御方群体中采取防御策略和不采取防御投资策略的比例分别为 y,$1-y$.利用上述参数设定,得出网络攻防演化博弈模型的收益矩阵如表 2 所示.

表 2 演化博弈期望收益矩阵

Table 2 Evolutionary game expectation return matrix

防御方/攻击方	攻击	不攻击
投资	$V_0-V_{add}-P_1L+R_1$, $P_1E-C_A^1-G_1$	$V_0-V_{add}+R_1$, 0
不投资	$V_0-P_0L+R_0$, $P_0E-C_A^0-G_0$	V_0+R_0, 0

用 U_D^1 表示防御方选择投资防御策略时防御方的期望收益,U_D^0 表示防御方不投资防御策略时防御方的期望收益,由上述收益矩阵可知:

$$\begin{aligned} U_D^1&=x(V_0-V_{add}-P_1L+R_1)+(1-x)(V_0-V_{add}+R_1)\\ &=-xP_1L+V_0-V_{add}+\alpha I_1 \end{aligned}\tag{1}$$

$$U_D^0 = x(V_0 - P_0L + R_0) + (1-x)(V_0 + R_0)$$
$$= -xP_0L + V_0 + \alpha I_0 \quad (2)$$

用$\overline{U_D}$表示防御方的平均收益,则可由公式(1)和公式(2)得.

$$\overline{U_D} = yU_D^1 + (1-y)U_D^0 = y[xL(P_0 - P_1) + \alpha(I_1 - I_0) - V_{add}] - xP_0L + V_0 + \alpha I_0 \quad (3)$$

相应地,用 U_A^1 表示攻击方采取攻击策略时攻击方的期望收益,U_A^0 表示攻击方采取不攻击策略时攻击方的收益,即得出.

$$U_A^1 = y(P_1E - C_A^1 - G_1) + (1-y)(P_0E - C_A^0 - G_0) =$$
$$-y[(P_0 - P_1)(E-\beta) + t_1P_1 - t_0P_0] + P_0(E - t_0 - \beta) \quad (4)$$
$$U_A^0 = 0 \quad (5)$$

用$\overline{U_A}$表示攻击方的平均收益,由公式(4)和公式(5)可得.

$$\overline{U_A} = xU_A^1 + (1-x)U_A^0 =$$
$$-xy[(P_0 - P_1)(E-\beta) + t_1P_1 - t_0P_0] + xP_0(E - t_0 - \beta) \quad (6)$$

根据以上分析得到攻防演化博弈模型的复制动态方程.由公式(4)和公式(6)可得攻击方复制动态方程为.

$$\frac{dx}{dt} = x(U_A^1 - \overline{U_A}) =$$
$$x(1-x)\{-y[(P_0 - P_1)(E-\beta) + t_1P_1 - t_0P_0]P_0(E - t_0 - \beta)\} \quad (7)$$

由公式(1)和公式(3)可得防御方复制动态方程为.

$$\frac{dy}{dt} = y(U_D^1 - \overline{U_D}) = y(1-y)[xL(P_0 - P_1) + \alpha(I_1 - I_0) - V_{add}] \quad (8)$$

4　攻防演化博弈最优策略选取

在网络攻防博弈过程中,攻击方与防御方对立的进行博弈,每一个局中人都是通过在博弈中不断地试错、调整和改进来促使自己的期望收益最大化.在这种原则的指导下,无论是攻击方的攻击策略还是防御方的防守策略,均会逐渐趋向于一种平衡.未趋向平衡的一方所换来的代价就是减少收益,所以任何一方都不会去尝试改变这种策略,即此时达到平衡的策略为最优策略.具体算法描述如下:

算法.最优防御策略选取算法

输入:参与攻防博弈的局中人 N_A,N_D 及主机节点信息

输出:攻击策略 S_A^*,最优防御策略 S_D^*

Begin

1. 初始化 $ADEGM = (N, S, U)$　/* 初始化攻防演化博弈模型 */

2. 构建 x, y　/* 构建攻防双方所选策略集的群体概率 */

3. 构建基于激励机制的不完全信息博弈树

4. 构建攻防双方演化博弈矩阵

5. 计算攻击方的复制动态方程{

5.1. $\overline{U_A} = xU_A^1 + (1-x)U_A^0$　/* 利用攻击群体选择某一策略的概率不同,计算攻击方的($S_{A1}, S_{A2}, \cdots, S_{Am}$)种攻击策略的平均收益 */

5.2. $\frac{dx}{dt} = x(U_A^1 - \overline{U_A})$　/* 由此得到攻击方复制动态方程 */

}

6. 计算防御方的复制动态方程

{

6.1. $\overline{U_D} = yU_D^1 + (1-y)U_D^0$　/* 利用防御群体选择某一策略的概率不同,计算防御方的($S_{D1}, S_{D2}, \cdots, S_{Dn}$)种防御策略的平均收益 */

6.2. $\frac{dy}{dt} = y(U_D^1 - \overline{U_D})$　/* 由此得到防御方复制动态方程 */

}

7. 求得演化均衡 ESS　/* 根据第 6 步、第 7 步所得复制动态方程,求解 $\frac{dx}{dt} = 0$ 和 $\frac{dy}{dt} = 0$ */

8. 返回 S_A^*, S_D^*

End

分析以上算法步骤可知,第 1 步-第 6 步的时间复杂度为 $O(m+n)$,第 7 步-第 8 步的时间复杂度为 $O((m+n)^2)$.综上所述,求解最优防御策略的选取的时间复杂度不超过 $O((m+n)^2)$.

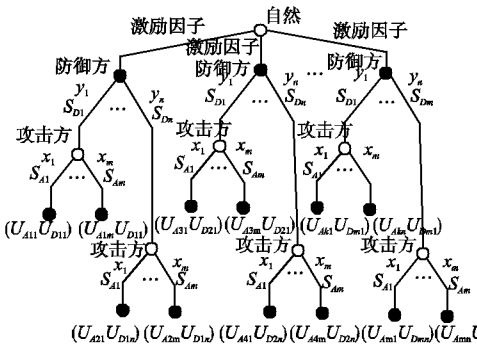

图 1　基于激励机制的不完全信息树

Fig. 1　Incomplete information tree based on incentive mechanism

针对上述建立的网络攻防演化博弈模型、参数设定及算法描述,构建了基于激励机制的不完全信息博弈树,利用博弈树我们可以更直观的分析演化博弈模型的所有信息.在本文提出的模型中,第三方监管部门是演化博弈中自然的身份,并不是参与者,在激励因子的作用下,防御方群体有($S_{D1}, S_{D2}, \cdots, S_{Dn}$)种防御策略,攻击方群体有($S_{A1}, S_{A2}, \cdots, S_{Am}$)种攻击策略,攻防双方群体均以不同的概率选取不同的策略并产生不同的收益,如图 1 所示.

5　应用实例与分析

在本节中,我们部署了网络拓扑环境对本文所提出的网络攻防演化博弈模型进行仿真实验.通过分析演化稳定策略,证明模型的有效性;通过分析攻击时间对攻击群体策略选取的影响,证明攻击具有时效性;通过激励机制对攻防群体策略选取的影响以及引入防御投资回报方程,证明激励机制的适用性.

在网络拓扑环境中,攻击主机 A 位于外部网络,内网中包含三台服务器,分别为 MySQL 服务器 B、web 服务器 C 和 FTP 服务器 D;由防火墙将内部网络与外部网络隔离开.如图 2 所示.

其中,防火墙用于将内网和外网隔开,是维护网络环境安全的一道屏障.外部主机只能通过网络访问 web 服务器 C 和

FTP 服务器 D. 在内网中,MySQL 服务器 B、web 服务器 C 和 FTP 服务器 D 之间可以利用 user 权限互相访问. 利用 Nessus

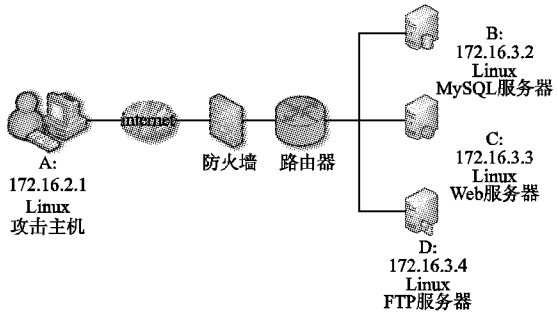

图 2 网络拓扑环境

Fig. 2 Network topology environment

脆弱点扫描器对网络中三台服务器节点进行弱点扫描,其服务器节点信息如表 3 所示.

表 3 服务器节点信息

Table 3 Server node information

Host/IP	OS	服务	脆弱点 ID
B 172. 16. 3. 2	Linux	MySQL	CVE-2018-10757
C 172. 16. 3. 3	Linux	ssh	CVE-2016-10012
D 172. 16. 3. 4	Linux	ftp	CVE-2016-9499

通过对网络中各主机节点脆弱性和攻击行为的分析,并结合国家信息安全漏洞库(CNNVD)信息,在实验中设计网络攻击策略 S_{A1}、S_{A2}(S_{A1} 策略成本高,攻击有效性高,针对性强;S_{A2} 策略成本低,攻击有效性低,可看作不采取攻击). 对抗外来攻击时,防御方可增加成本采取防御投资,也可依靠现有防御能力被动防守,设计防御策略为 S_{D1}、S_{D2}. 如表 4 和表 5 所示.

表 4 原子攻击信息

Table 4 Atomic attack information

编号及名称	网络攻击策略	
	S_{A1}	S_{A2}
1 Remote buffer overflow		
2 Buffer error	√	
3 install Web Linstener program		√
4 install delete Trojan	√	
5 Trying to steal account		√
6 FTP server information disclosure	√	
7 Homepage attack	√	
8 Check Point ZoneAlarm		
9 LPC to LSASS process		√
10 SQL injection vulnerability	√	

根据上述网络环境,构建基于激励机制的不完全信息博弈树,在社会第三方监管部门的激励下,攻防群体选择不同的攻防策略,形成攻防收益集合,如图 3 所示.

5.1 演化稳定策略

下面根据 x 和 y 的问题情境不同,对构建的网络环境进行多次模拟实验. 利用仿真实验,可以直观的分析攻击方 x 和防御方 y 的群体演化规律,实现对攻击策略的预测,并最终寻求到演化稳定策略,即此状态下的最优防御策略.

表 5 防御策略信息

Table 5 Defense strategy information

编号及名称	网络攻击策略	
	S_{D1}	S_{D2}
1 Install MySQL patches	√	
2 Uninstall delete Trojan		√
3 Install sshd patches	√	
4 Limit packets from ports		
5 Delete suspicious account		√
6 Restart Database server	√	√
7 Install ftp patches	√	
8 Repair database		
9 Close Homepage		√
10 Add physical recourse	√	

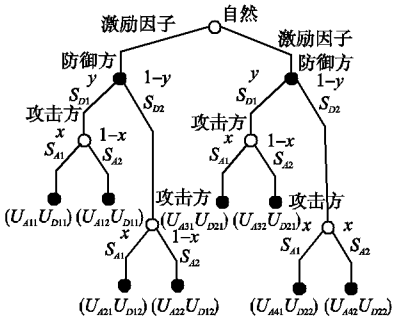

图 3 基于激励机制的不完全信息树

Fig. 3 Incomplete information tree based on incentive mechanism

当问题情境为 $x=0.2, y=0.6$ 时,即群体中攻击方以{0.2,0.8}的概率选取混合策略$\{S_{A1}, S_{A2}\}$,防御方以{0.6,0.4}的概率选取混合策略$\{S_{D1}, S_{D2}\}$. 通过不断演化,攻击方选取策略 S_{A1} 的几率逐步趋向于 0,防御方选取防御策略 S_{D1} 的几率逐步趋向于 1,二者均达到演化稳定状态,此时的最优防御策略为 S_{D1}. 如图 4 所示.

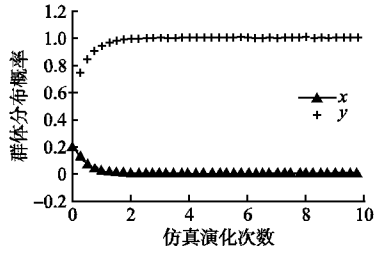

图 4 $x=0.2, y=0.6$ 时群体演化趋势

Fig. 4 Group evolution trend when $x=0.2, y=0.6$

分析可知,在此时的情境下,防御方属于较为积极的防备状态,并且愿意针对自身脆弱点采取投资防御策略的防御群体呈逐步增加趋势,攻击方群体逐渐转向不采取攻击的被动状态,此时网络环境较为安全.

当问题情境为 $x=0.7, y=0.3$ 时,即群体中攻击方以{0.7,0.3}的概率选取混合策略$\{S_{A1}, S_{A2}\}$,防御方以{0.3,0.7}的概率选取混合策略$\{S_{D1}, S_{D2}\}$,经过不断演化,攻击方

最终选取攻击策略 S_{A1} 的概率逐步趋向于 1,防御方选取防御策略 S_{D1} 的概率逐步趋向于 0,二者均达到演化稳定状态,此时的最优防御策略为 S_{D2}. 如图 5 所示.

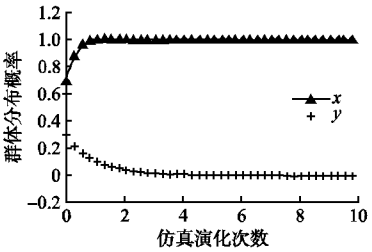

图 5　$x=0.7, y=0.3$ 时群体演化趋势

Fig. 5　Group evolution trend when $x=0.7, y=0.3$

分析此时的情景可知,由于防御方选择投资防御策略的群体概率较小,在攻防对抗中较为被动,攻击方群体逐渐采取有效的攻击策略进行攻击,整体网络环境瘫痪.

5.2　激励机制对攻防群体策略的影响

当防御方采取防御策略后,攻击方想要攻击成功的时间就会延长. 我们可以发现,本文所构建的模型在仿真实验环境下,在第 1min 至第 3min 时,攻击群体逐渐趋向于选择高成本的攻击策略,在第 4min 时攻击群体中选择高成本攻击策略者基本保持原有概率不变,如图 6(a)所示. 当超过 4min 之后,由于攻防双方长时间僵持导致攻击成本过高,攻击方逐渐趋向于消极状态,最终演化为不采取攻击,如图 6(b)所示. 因此,当防御方以较为积极的状态采取防御策略致使攻击时间过长时,可以有效遏制攻击方的攻击积极性.

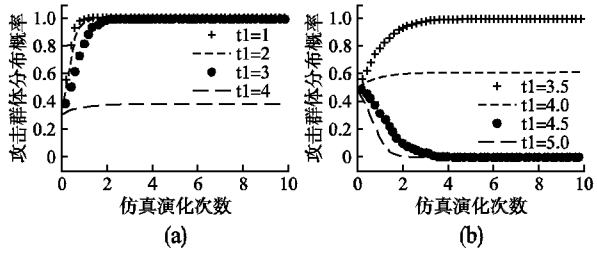

图 6　攻击时长对攻击群体的影响趋势

Fig. 6　Impact of attack duration on attack groups

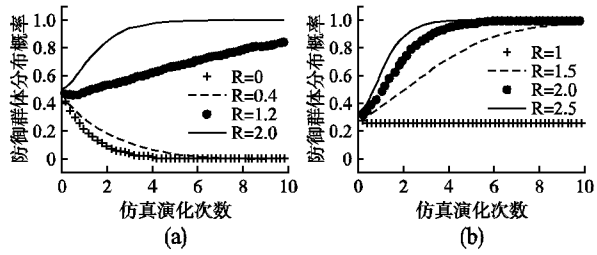

图 7　激励机制对防御群体的影响趋势

Fig. 7　Influence of incentive mechanism on defense groups

为了分析增加激励机制对防御群体的影响,我们将 R 分别取不同值观测防御群体的演化规律. 将图 7(a)、图 7(b)结合分析可知,无论选择投资防御策略的初始群体的概率是多少,当社会不给予防御方激励或者激励程度较小时,防御群体逐渐趋向于被动防御的消极状态,这样对于整个网络环境是十分不利的;当社会给予防御方足够丰厚的激励时,防御群体逐渐趋向于采取投资防御策略的积极状态,更有利于建设和谐文明的互联网空间.

5.3　激励机制对防御收益的影响

此外,为了更直观的看出增加激励机制的优势,我们引入投资回报(Return on Security Investment)的概念[16]. 可得到防御投资回报 $ROSI$:

$$ROSI=\frac{L(P_0-P_1)-(V_{add}-\alpha I)}{V_{add}-\alpha I}$$

通过对比我们可以看出增加激励机制可以明显提高防御方的收益,有效降低了攻击方攻击对网络环境所造成的损失. 如图 8 所示.

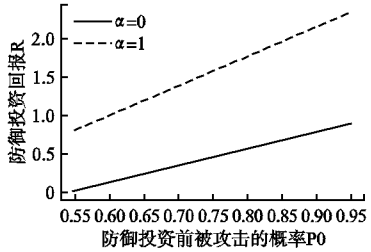

图 8　激励机制对防御方收益的影响

Fig. 8　Impact of incentives on the benefits of defenders

6　总　结

如今,网络攻防对抗正朝着快速、实时、多元化的方向迅猛发展,基于传统动态博弈的分析方法已经不能满足现实需求. 本文构建了基于激励机制的网络攻防演化博弈模型,在不同的问题情境下,系统通过不断演化,最终将会趋向于某个稳定状态,防御方经过不断的修正和改进自己的行为,最终获得此情境下的最优防御策略. 此外,本文在惩罚机制的基础上引入激励机制,通过第三方监管部门对局中人进行管理,可以有效提高防御方的总体收益,促进防御方投资防御策略的积极性. 通过分析攻击时长可以发现,增加防御策略投资会导致攻击时间变长、攻击成本过高,从而遏制了攻击者的攻击积极性,便于构建更加安全稳定的网络环境. 通过对比可以很直观的发现本文演算得出的理论分析与仿真实验得出结论保持一致,证明了本文提出的攻防演化博弈模型的实际意义. 将其应用在实际网络环境下,可以对外来攻击者及时进行预判和检测,并为自身最优防御策略的选取提供一定的依据,对网络环境的维护有一定的积极作用.

References:

[1] Schmidt C. Game theory and economics: an historical survey[J]. Revue d'économie politique, 1990, 100(5): 589-618.

[2] Balkenborg D, Schlag K. On the interpretation of evolutionary stable sets in symmetric and asymmetric games [R]. Mimeo, Bonn University Economics Department, 1994.

[3] Herbert Gintis. Game theory evolving [M]. Boston: Princeton University Press, 2015.

[4] Ron N Borkovsky, Doraszelski U, Kryukov Y. A user's guide to solving dynamic stochastic games using the homotopy method[J]. Operations Research, 2017, 58(4): 1116-1132.

[5] Taylor P D, Jonker L B. Evolutionary stable strategies and game dynamics [J]. Mathematical Biosciences, 1978, 40(1-2): 145-156.
[6] Huang J, Wang J, Zhang H, et al. Network defense strategy selection based on best-response dynamic evolutionary game model[C]//IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference(IAEAC), IEEE, 2017: 2611-2615.
[7] Wang Yuan-zhuo, Lin Chuang, Cheng Xue-qi, et al. Analysis for network attack-defense based on stochastic game model[J]. Chinese Journal of Computers, 2010, 33(9): 1748-1762.
[8] Liu J, Yu J, Shen S. Energy-efficient two-layer cooperative defense scheme to secure sensor-clouds[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(2): 408-420.
[9] Abass A A A, Xiao L, Mandayam N B, et al. Evolutionary game theoretic analysis of advanced persistent threats against cloud storage[J]. IEEE Access, 2017, 5: 8482-8491.
[10] Hayel Y, Zhu Q. Epidemic protection over heterogeneous networks using evolutionary poisson games[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(8): 1786-1800.
[11] Liu P, Liu J. Robustness of coevolution in resolving prisoner's dilemma games on interdependent networks subject to attack[J]. Physica A: Statistical Mechanics and its Applications, 2017, 479: 362-370.
[12] Hu H, Liu Y, Zhang H, et al. Optimal network defense strategy selection based on incomplete information evolutionary game[J]. IEEE Access, 2018, 6: 29806-29821.
[13] Zhang Yun, Wei Cheng-jian, Shen Hang. Ambiguous game based on minimax regret in uncertain information system[J]. Journal of Chinese Computer Systems, 2017, 38(9): 2045-2050.
[14] Zhu Jian-ming, Raghunathan S. Evaluation model of information security technologies based on game theoretic[J]. Chinese Journal of Computers, 2009, 32(4): 828-834.
[15] Zhu Jian-ming, Song Biao, Huang Qi-fa. Evolution game model of offense-defense for network security based on system dynamics [J]. Journal on Communications, 2014, 35(1): 54-61.
[16] Wang Q, Zhu J. Optimal information security investment analyses with the consideration of the benefits of investment and using evolutionary game theory[C]//2nd International Conference on Information Management(ICIM), IEEE, 2016: 105-109.
[17] Zhang C, Pan R, Chaudhury A, et al. Effect of security investment on evolutionary games[J]. Journal of Information Science and Engineering, 2014, 30(6): 1695-1718.
[18] Pan R, Xu C. Research on decision of cyber security investment based on evolutionary game model[C]//International Conference on Multimedia Information Networking and Security, IEEE, 2010: 491-495.
[19] Du J, Jiang C, Chen K C, et al. Community-structured evolutionary game for privacy protection in social networks[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(3): 574-589.
[20] Wang Yuan-zhuo, Yu Jian-ye, Qiu Wen, et al. Evolutionary game model and analysis methods for network group behavior[J]. Chinese Journal of Computers, 2015, 38(2): 282-300.
[21] Zhang J, Zhu Y, Chen Z. Evolutionary game dynamics of multiagent systems on multiple community networks[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2018, (99): 1-17.

附中文参考文献：

[7] 王元卓，林 闯，程学旗，等. 基于随机博弈模型的网络攻防量化分析方法[J]. 计算机学报，2010，33(9)：1748-1762.
[13] 张 云，蔚承建，沈 航. 一种信息不确定系统的模糊安全博弈模型[J]. 小型微型计算机系统，2017，38(9)：2045-2050.
[14] 朱建明，Raghunathan S. 基于博弈论的信息安全技术评价模型[J]. 计算机学报，2009，32(4)：828-834.
[15] 朱建明，宋 彪，黄启发. 基于系统动力学的网络安全攻防演化博弈模型[J]. 通信学报，2014，35(1)：54-61.
[20] 王元卓，于建业，邱 雯，等. 网络群体行为的演化博弈模型与分析方法[J]. 计算机学报，2015，38(2)：282-300.