

基于时机博弈的网络安全防御决策方法

孙鹏宇^{1,2}, 张恒巍¹, 谭晶磊¹, 李晨蔚¹, 马军强¹, 王晋东¹

(1. 中国人民解放军战略支援部队信息工程大学 三院, 郑州 450001; 2. 中国人民解放军 91451 部队, 河北 邯郸 056000)

摘要: 现有的网络防御决策模型大多基于攻防行为进行建模分析, 忽视了攻防时机对网络安全产生的影响, 且对网络攻防时机的选取大多依赖经验和主观判断, 导致网络安全管理者在进行防御决策时难以提供可信的理论支撑。然而网络攻防的时机因素对网络防御决策意义重大, 在面对外部攻击时能否进行实时决策, 决定了网络在攻防对抗中能否掌握主动, 以最小的代价将攻击危害降到最低。针对网络安全中的时机策略选取问题, 提出一种网络安全防御决策方法, 基于 SIR 传染病模型并加以改进, 构造描述网络安全状态的微分方程, 实现对系统安全状态的实时度量。借鉴 FlipIt 博弈方法构建攻防时机博弈模型, 提出攻防收益量化与计算方法, 通过求解不同攻防周期策略下的纳什均衡, 获得最优防御时间策略。实验结果表明, 当攻击策略一定时, 使用该方法动态选择最优防御策略的平均收益为 0.26, 相比固定周期的防御方法, 平均防御收益提高了 23.81%。

关键词: 网络安全; 网络攻防; 传染病模型; 时机博弈; 最优防御策略

开放科学(资源服务)标志码(OSID):



中文引用格式: 孙鹏宇, 张恒巍, 谭晶磊, 等. 基于时机博弈的网络安全防御决策方法[J]. 计算机工程, 2022, 48(11): 145-151.

英文引用格式: SUN P Y, ZHANG H W, TAN J L, et al. Network security defense decision method based on time game [J]. Computer Engineering, 2022, 48(11): 145-151.

Network Security Defense Decision Method Based on Time Game

SUN Pengyu^{1,2}, ZHANG Hengwei¹, TAN Jinglei¹, LI Chenwei¹, MA Junqiang¹, WANG Jindong¹

(1. The Third Institute, Information Engineering University of the PLA Strategic Support Force, Zhengzhou 450001, China;
2. PLA 91451 Unit, Handan, Hebei 056000, China)

[Abstract] Currently major network assessment models focus on the intensity of attack and defense, often ignoring the impact of timing on network security. While selecting attack and defense timing, mostly relying on subjective experience and judgement, network managers lack quantitative analysis and credible theoretical support on making defense decisions. A key factor in network defense is timing decision against various attacks to seize the initiative with lower cost and damage, which is significant in protecting network resource. To effectively solve the problem of time strategy selection in network security, this study proposes a network security defense decision-making method, an improved Susceptible-Infectious-Removed (SIR) epidemic model that is used to characterize differential equations of network real-time security states. We present a method to quantify and calculate utilities of attack and defense with a FlipIt game method. An optimal defense time strategy is proposed via calculating the Nash equilibrium under different periodic strategies of attack and defense. The experimental results show that, when the attack strategy is constant, the dynamic optimal defense strategy in this study is 0.26. Compared with periodic defense strategy, the average utility is improved by 23.81%.

[Key words] network security; network attack and defense; epidemic model; time game; optimal defense strategy

DOI: 10.19678/j.issn.1000-3428.0063866

0 概述

近年来,随着信息技术的飞速发展,网络攻击事件频繁发生^[1],大到国际战略、国家安全,小到公司利益、个人隐私,普遍受到来自黑客攻击、蠕虫病毒、

木马程序等网络安全威胁。此外,随着计算机技术的快速发展,网络安全威胁和攻击的手段越来越灵活^[2-3],现有的漏洞检测、防火墙、病毒防护等静态防御技术已难以应对隐蔽性强、变化快的网络攻击。因此,提高网络安全威胁防控能力,增强网络防御效

基金项目:国家重点研发计划(2017YFB0801900)。

作者简介:孙鹏宇(1993—),男,硕士研究生,主研方向为网络与信息安全;张恒巍(通信作者),副教授、博士;谭晶磊,博士研究生;李晨蔚,硕士研究生;马军强,副教授;王晋东,教授。

收稿日期:2022-01-28 修回日期:2022-04-16 E-mail:zhw11qd@163.com

能已成为亟待解决的问题。

网络安全的本质在于对抗,对抗的本质在于攻防两端能力的较量^[4]。在网络攻防对抗中,双方行动彼此制衡、相互影响,对抗结果由双方策略共同决定,针对特定的攻击手段,不同的防御策略会产生不同的安全收益^[5]。由于网络攻防对抗中的基本特征与博弈理论相似,攻防双方的对抗过程可以抽象为双人博弈的过程,因此应用博弈模型分析网络攻防行为成为网络安全领域的热点研究方向^[6-7],已有诸多学者取得了较好的研究成果。

基于博弈模型分析网络攻防行为主要取决于决策行动的具体内容(即行为策略)及决策行动的时间(即时间策略)。基于行为策略的攻防博弈模型成果较多,行为策略的研究经历了由静态到动态、由完全信息到不完全信息、由完全理性到不完全理性的发展过程。近年来,研究人员陆续提出适用于不同网络场景的防御决策模型,主要包括攻防信号博弈模型^[8-10]、攻防微分博弈模型^[11-12]、攻防随机博弈模型^[13-15]以及攻防演化博弈模型^[16-17],但在现有成果中,对时间策略展开深入研究的网络攻防博弈模型则相对较少,而时间策略的选取对网络防御决策意义重大,因为即使选取的行为策略正确,但如果行动时机错误,依然会影响防御效能,给网络系统造成巨大的损失。

基于时间博弈^[18-19]的网络防御决策方法适用于描述对公共资源控制权交替变换的情况,优点是模型的拓展性较强,可以和现有的行为策略模型相结合,更好地贴合网络攻防实际场景,有效提高网络攻防策略的准确性和时效性,协助网络管理者作出最优决策。文献^[18]提出FlipIt博弈,这是一种经典的时间博弈方法,能够有效应对具有隐蔽性、针对性的攻击行为,以时间维度选取策略进行建模,动态刻画攻防双方对安全目标控制权的争夺过程,为研究安全策略最优时机问题提供了理论工具^[20]。此后,相关技术成果及扩展研究相继出现^[21-23]。

本文以FlipIt博弈为基础,参考SIR传染病模型^[24]对网络安全状态进行演化分析,将网络资源节点抽象为SIR模型中的个体,并把网络节点安全状态扩展为正常状态N(Normal)、感染状态I(Infected)、修复状态R(Restored)、受损状态M(Malfunctioned)NIRM4种状态,在此基础上建立微分方程,用于描述网络安全状态演化过程。此外,借鉴FlipIt博弈方法,构建攻防时机博弈模型研究网络对抗过程,并综合分析时机选取策略对攻防收益变化的影响,提出攻防决策收益函数,并以纳什均衡策略为依据设计最优防御策略选取算法。

1 网络攻防时机博弈模型分析

为应对网络攻击行为快速、隐蔽的特点,在攻防对抗中赢得主动,本文构建一种基于FlipIt模型的防御时机决策模型,分析攻防双方决策与行动时机的关系。FlipIt博弈的特点在于行动的隐蔽性,即双方可以随时发起行动控制资源且不被对方发现,并且

只有在对方行动之后,才能知道系统资源的当前状态(攻击或防御),攻防双方决策则根据博弈过程中反馈的信息确定。因此,本文从不完全信息角度构建基于时机博弈的攻防策略选取模型。

1.1 基于SIR模型的攻防过程演化分析

SIR模型是传播动力学中描述信息传递或行为传播的经典模型,主要应用于分析传染病在人群中的流行规律及其内在的动力学过程。模型将人群分为易感者、感染者和恢复者3类,并设置总人口恒定,其感染机制可以描述如下:流行病毒是传染的源头,通过一定的速率感染易感者,此时易感者变成感染者,成为新的传染源头;感染者可以通过治疗变成恢复者,同时获得免疫能力,使自身既不会感染病毒也不会传播病毒。

通过对SIR模型进行定量分析和数据模拟,能够预测传染病传播趋势并制定有效的防御措施。SIR模型具体表述如下:在初始阶段所有的节点均为易感节点,当接收到外界传递的信息后,相应的节点受到传染变成感染节点,紧接着感染节点继续传递信息给其他易感节点,同时有部分感染节点转为免疫节点,信息传递行为在免疫节点处终止。

在网络攻防对抗中,攻击方利用网络系统内部潜在的漏洞,对部分节点发起攻击,并渗透到网络系统中的其他节点,企图破坏整个网络系统。攻防行为的交互对抗,导致网络系统的安全状态发生迁移,相应状态网络节点的数量也随之动态变化,整个攻防过程与传染病的传播过程类似。本文借鉴SIR传染病模型模拟网络攻防过程,将网络资源节点抽象为SIR模型中的个体并扩展为NIRM4种状态,动态刻画网络节点的安全状态演化过程。本文用 $x_N(t)$ 、 $x_I(t)$ 、 $x_R(t)$ 、 $x_M(t)$ 分别表示在 t 时刻下正常节点N、感染节点I、免疫节点R和受损节点M的数量。

假设网络中节点总数量 Q 保持不变,则 $\forall t \in [t_0, T]$,有 $x_N(t) + x_I(t) + x_R(t) + x_M(t) = Q$ 。4种网络节点的状态转移路径具体如下所示:

1) $N \rightarrow I$: 网络节点处于正常工作状态,由于遭受到网络病毒入侵,被病毒成功入侵的网络节点将转变为感染节点I。

2) $N \rightarrow R$: 网络节点处于正常工作状态,当网络病毒开始入侵时,就立即被防御系统成功捕捉病毒信息并对其进行查杀,此时网络节点转变为对网络病毒免疫的节点R。

3) $I \rightarrow R$: 网络节点成功被病毒入侵并感染,防御系统采取定期系统检测或病毒筛查手段,有效识别并清除已感染的节点,成功修复安全漏洞,此时网络节点转变为对网络病毒免疫的节点R。

4) $I \rightarrow M$: 网络节点成功被病毒入侵并感染,防御系统利用病毒检测、系统升级等方法进行修复后,仍未能有效清除已感染的节点,导致节点受损严重,终止服务,并且无法继续感染其他节点,此时网络节点转变为终止服务的受损节点M。

4种网络节点的状态转换示意图如图1所示。

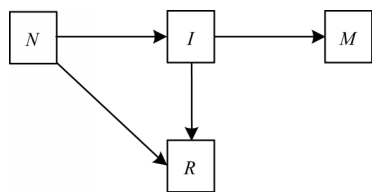


图1 网络节点状态转换示意图

Fig.1 Schematic diagram of network node state transition

根据上述网络节点状态的转移情况,本文重点围绕正常节点 N 和感染节点 I 进行分析,网络安全状态变化的微分方程可以表示为:

$$\begin{cases} x'_N = v_a \sigma \pi x_I(t) x_N(t) / Q - v_d x_N(t) \\ x'_I = v_a \sigma \pi x_I(t) x_N(t) / Q - v_a x_I(t) - v_d x_I(t) \\ x'_R = v_d x_N(t) + v_d x_I(t) \\ x'_M = v_a x_I(t) \end{cases} \quad (1)$$

假设网络病毒的传播只能感染渗透相邻的网络节点,不能感染其他网络节点。网络节点以密度 σ 进行分布, v_a 为感染速率,大小与网络中感染节点所占比例有关, v_d 为修复速率,大小与网络中正常节点和免疫节点所占的比例有关。

本节在改进SIR模型的基础上,构造描述网络安全状态变化的微分方程,实现对安全状态的实时度量,为后面时机博弈模型的构建与攻防收益的量化计算提供分析基础和度量方法的支撑。

1.2 基于时机博弈的最优防御策略模型

本文在1.1节的基础上构建攻防时机博弈模型,该模型为非自适应连续博弈模型,其中攻防双方均采用具有随机阶段的周期性策略,攻防双方的行动由博弈期间接收到的反馈确定。

定义1 攻防时机博弈模型(Attack-Defense Time Game, ADTG)可以表示为一个6元组 $A_{\text{ADTG}} = (N, T, x(t), B, P, U)$,并满足如下条件:

1) $N = (N_A, N_D)$ 是攻防博弈的参与人集合, N_A 代表攻击方, N_D 代表防御方。

2) $T = T_A + T_D \in [0, +\infty)$ 是攻防博弈的总时间,表示攻击方与防御方控制系统资源的总时间,其中 T_A 为攻击方控制系统资源的总时间, T_D 为防御方控制系统资源的总时间。

3) $x(t) = \{x_N(t), x_I(t), x_R(t), x_M(t)\}$ 是网络系统的状态变量。 $x_N(t), x_I(t), x_R(t), x_M(t)$ 分别表示 t 时刻网络系统中4种状态的节点数量, Q 代表节点总数量, $Q = x_N(t) + x_I(t) + x_R(t) + x_M(t)$ 。

4) $B = (AS, DS)$ 是攻防双方的行动空间,其中, $AS = (\beta_1, \beta_2, \dots, \beta_j)$, $DS = (\delta_1, \delta_2, \dots, \delta_k)$ 分别表示攻击方和防御方的行动集合,双方的行动次数均不小于1,即 $j, k \geq 1$ 。在任意 t 时刻,攻防双方都有可能采取行动控制资源。

5) $P = (P_A, P_D)$ 是攻防双方的周期策略空间,其中, P_A 表示攻击方时间策略,代表连续2次攻击行动的时间间隔, $P_A = \{P_A(t) | P_A(t) = (p_A^j(t)), 1 \leq j \leq m\}$ 为攻

击方的时间策略集合。同理, P_D 表示防御方时间策略, $P_D = \{P_D(t) | P_D(t) = (p_D^k(t)), 1 \leq k \leq n\}$ 表示防御方的时间策略集合。

6) $U = (U_A, U_D)$ 是攻防双方的收益函数集合,其中, U_A 和 U_D 分别表示攻击方和防御方的收益函数。

1.3 收益量化与计算方法

收益量化是求解博弈均衡并进行定量计算的基础,其作为攻防时机博弈模型ADTG的输入,直接影响攻防时机的选取结果,进而影响最优攻防策略的输出。这里将收益量化分为两部分,包括网络攻防对抗导致网络节点状态变化产生的收益及攻防双方实施行为策略消耗的成本。为有效计算攻防收益,本文将攻防双方控制目标资源的总时长作为收益的唯一指标,相关参数的定义、符号名称及具体含义如表1所示。

表1 相关符号的定义

Table 1 Definition of relevant symbols

符号	名称	具体含义
C_A	攻击成本	采取攻击行为造成的资源损失
C_D	防御成本	采取防御行为造成的资源损失
R_A	攻击回报	攻击方控制公共资源后获得的直接回报
R_D	防御回报	防御方控制公共资源后获得的直接回报
r_{AR}	攻击回报率	单位时间内攻击方控制资源后获得的直接回报
r_{DR}	防御回报率	单位时间内防御方控制资源后获得的直接回报
U_A	攻击收益	攻击方控制公共资源后获得的净收益
U_D	防御收益	防御方控制公共资源后获得的净收益
ω_{AU}	攻击收益率	单位时间内攻击方控制资源后获得的净收益
ω_{DU}	防御收益率	单位时间内防御方控制资源后获得的净收益

为简化计算,将攻防行为的回报率和收益率进行归一化处理,即 $r = r_{AR} + r_{DR} = 1$, $\omega = \omega_{AU} + \omega_{DU}$,其中,攻击方收益率 $\omega_{AU} = \liminf_{t \rightarrow \infty} \omega_{AU}(t)$,防御方收益率 $\omega_{DU} = \liminf_{t \rightarrow \infty} \omega_{DU}(t)$ 。

根据博弈论^[25]可知,在给定的攻防时机博弈模型 $A_{\text{ADTG}} = (N, T, x(t), B, P, U)$ 中,由于攻防双方的策略相互依存,存在最优的攻防策略组合 (P_A^*, P_D^*) 使攻防双方达到博弈平衡,满足:

$$\begin{aligned} \omega_{AU}(P_A^*, P_D) &\geq \omega_{AU}(P_A, P_D) \\ \omega_{DU}(P_A, P_D^*) &\geq \omega_{DU}(P_A, P_D) \end{aligned} \quad (2)$$

根据定义1的周期性博弈可知,攻防双方的行动是隐蔽的,无法准确掌握对手行动时间的完整信息,双方采取的博弈策略为非适应性策略,策略的时机选取是随机的。因此,本文借鉴FlipIt博弈方法,将相位随机化引入到周期性策略中,即攻防双方均采用具有随机特征的周期性策略,双方的行动时间在区间 $[0, P]$ 中随机选择,双方的周期性策略仅根据行动频率 $\frac{1}{P_A}$ 和 $\frac{1}{P_D}$ 的大小确定。在此将收益计算分为以下2种情况:

1) 当 $\frac{1}{P_D} \geq \frac{1}{P_A}$ 时, 令 $\xi = \frac{P_D}{P_A}$, 表示在给定防御方行动频率 $\frac{1}{P_D}$ 的情况下攻击方在防御周期区间内发起攻击的概率, 由于攻击方在单位防御周期区间仅行动1次, 相应周期区间内攻击方控制的时间预期为 $\frac{\xi}{2}$, 那么攻防双方的收益表达式如下:

$$U_A = R_A - C_A = \frac{\xi}{2} - \frac{C_A}{P_A} = \frac{P_D}{2P_A} - \frac{C_A}{P_A} \quad (3)$$

$$U_D = R_D - C_D = 1 - \frac{\xi}{2} - \frac{C_D}{P_D} = 1 - \frac{P_D}{2P_A} - \frac{C_D}{P_D} \quad (4)$$

2) 当 $\frac{1}{P_A} \geq \frac{1}{P_D}$ 时, 同理可得攻防双方的收益为:

$$U_A = R_A - C_A = 1 - \frac{\xi}{2} - \frac{C_A}{P_A} = 1 - \frac{P_A}{2P_D} - \frac{C_A}{P_A} \quad (5)$$

$$U_D = R_D - C_D = \frac{\xi}{2} - \frac{C_D}{P_D} = \frac{P_A}{2P_D} - \frac{C_D}{P_D} \quad (6)$$

根据文献[18]理论推导的结果可知, 在给定的攻防时机博弈模型 $A_{\text{ADTG}} = (N, T, x(t), B, P, U)$ 中, 双方都采用随机阶段的周期性策略, 达到如下纳什均衡:

$$\begin{aligned} \frac{1}{P_A} > \frac{1}{P_D}, P_A^* &= \frac{C_D}{2C_A}, P_D^* = \frac{1}{2C_A} \\ \frac{1}{P_A} &= \frac{1}{P_D}, P_A^* = P_D^* = \frac{1}{2C_A} \\ \frac{1}{P_A} < \frac{1}{P_D}, P_A^* &= \frac{1}{2C_A}, P_D^* = \frac{C_D}{2C_A} \end{aligned} \quad (7)$$

2 最优防御策略选取算法

依据博弈基本理论, 纳什均衡是博弈过程能够达到的最优稳定解^[26]。因此, 根据式(7)求解得到的纳什均衡策略可认定为攻防双方的最优策略, 任何一方背离均衡策略, 都会导致其博弈收益降低。依据纳什均衡策略, 本文设计的攻防时机博弈的最优防御策略选取算法如下。

算法1 攻防时机博弈的最优防御策略选取算法

输入 攻防时机博弈模型

输出 最优防御策略 P_D^*

1. 初始化 $A_{\text{ADTG}} = (N, T, x(t), B, P, U)$;

2. 构建攻防双方的行为空间: $AS = (\beta_1, \beta_2, \dots, \beta_j)$, $DS = (\delta_1, \delta_2, \dots, \delta_k)$;

3. 构建攻防双方的周期策略空间: $P_A = \{P_A(t) | P_A(t) = (p_A^j(t)), 1 \leq j \leq m\}$, $P_D = \{P_D(t) | P_D(t) = (p_D^k(t)), 1 \leq k \leq n\}$;

4. 初始化常量系数 C_A, C_D ;

5. 根据式(3)~式(6), 计算攻防双方的收益情况 $U = (U_A, U_D)$;

6. 根据式(7), 计算攻防双方最优策略对 (P_A^*, P_D^*) ;

7. Return P_D^* 。

3 实验结果与分析

3.1 实验环境

通过仿真实验验证本文 ADTG 模型的可行性和

有效性。本节搭建了如图2所示的实验网络拓扑环境。

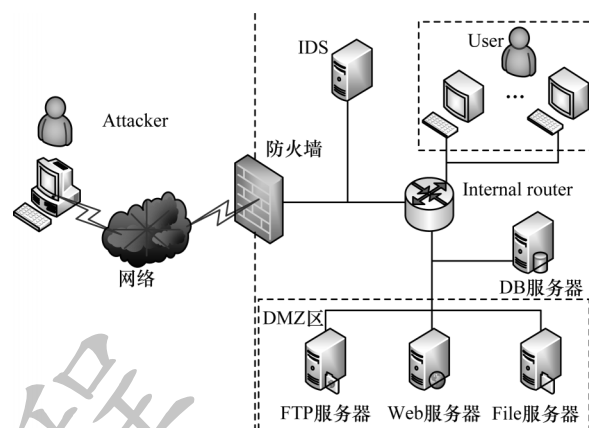


图2 仿真系统拓扑图

Fig.2 Topology diagram of simulation system

本文实验环境分为内部网络和外部网络2个部分, 攻击主机位于外部网络, 能够通过外网入侵内网中的任意节点, 目标信息系统为交换网络 and 用户主机。内部网络包括4台服务器, 分别为FTP服务器、Web服务器、File服务器和数据库服务器。根据防火墙的规则, 攻击方只能访问DMZ区的服务器, DMZ区的服务器可以访问数据库服务器, 但是无法访问局域网内用户主机。本文假设攻击方试图窃取数据库中储存的内部涉密敏感信息。根据国家信息安全漏洞库数据信息获得服务器和主机存在的漏洞信息, 如表2所示。

表2 服务器漏洞信息

Table 2 Vulnerability information of server

主机	操作系统	漏洞信息	漏洞编号
FTP服务器	Linux	缓冲区错误漏洞	CVE-2020-18077
Web服务器	Linux	跨站脚本漏洞	CVE-2021-46144
File服务器	Linux	信息泄露漏洞	CVE-2021-43224
Database服务器	Linux	路径遍历漏洞	CVE-2021-22028
User	Linux	权限许可和访问控制问题漏洞	CVE-2022-21838

参考林肯实验室攻防行为数据库^[27], 设计本文攻击和防御行为信息, 如表3和表4所示。

表3 攻击行为信息

Table 3 Attack behavior information

序号	攻击行为信息	攻击级别
1	安装侦听程序	高级
2	安装删除木马程序	高级
3	窃取帐户和密码	中级
4	FTP服务器上的SSH攻击	中级
5	远程代码注入	低级

表4 防御行为信息		
Table 4 Defense behavior information		
序号	防御行为信息	防御级别
1	安装 Oracle 补丁	高级
2	卸载删除木马程序	高级
3	更新根数据	中级
4	重启数据库服务器	中级
5	关闭服务	低级

3.2 防御收益的定量分析

本文通过设定不同参数,仿真网络节点不同的初始状态,并分析节点状态的演化过程,进而对防御收益进行定量分析。由于博弈模型为不完全信息博弈,攻防双方在行动之前都没有任何关于对手行为的信息,攻防收益仅与双方选取的策略有关。根据式(3)~式(6),将双方收益转化为行动频率,考虑到攻防双方的行动频率由行动成本决定,本文从行动周期和行动成本入手,进行仿真实验。设常量参数 P_A 、 P_D 、 C_A 、 C_D ,其中: P_A 、 P_D 分别为攻防双方的周期性策略,用于计算攻防博弈中的攻防回报; C_A 、 C_D 分别为攻防策略的成本,用于计算执行策略付出的代价,详细分析见1.3节。

本文依托 Matlab 软件为实验平台,验证所提出的最优防御策略选取算法。下面重点从求解最优防御收益 U_D^* 入手,分析防御收益 U_D 与攻防周期 P_A 、 P_D 以及防御成本 C_D 之间的关系。为简化计算,将攻击成本 C_A 设定为1,采用有限离散博弈时间,攻防双方的周期策略以0.5 s为最小行动时间单位进行实验。

图3所示为面对不同攻击周期时,防御收益 U_D 与防御周期 P_D 的关系。

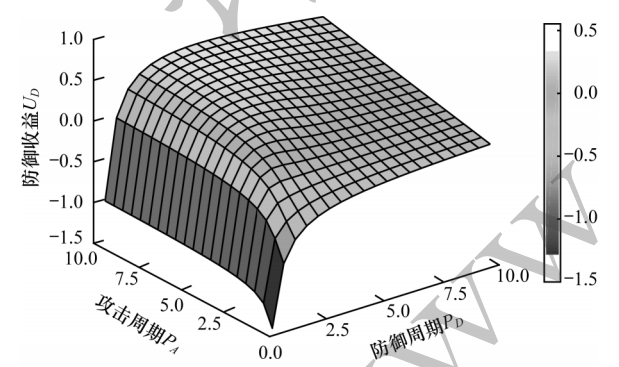


图3 防御收益与攻防周期的关系
Fig.3 Relationship between defense benefit and attack defense cycle

假设防御成本 $C_D=1$,由图3可知,当 $P_A=P_D$ 时,防御收益 U_D 随着攻防周期区间的增大而增加;当 $P_A<P_D$ 时,防御收益 U_D 随着攻击周期区间 P_A 的增大呈现上升趋势,随着防御周期区间 P_D 的增大,防御收益 U_D 继续保持上升;当 $P_A>P_D$ 时,防御收益 U_D 随着攻击周期区间 P_A 的增大同样呈现上升趋势,随着防御周期区间 P_D 的增大,防御收益 U_D 变化情况为先上升后下降。观察实验数据可得,当攻击周期 $P_A=3$

时,防御方的最佳防御周期 $P_D^*=2.5$,防御收益 $U_D^*=0.183$;当攻击周期 $P_A=5$ 时,防御方的最佳防御周期 $P_D^*=3$,此时防御收益 $U_D^*=0.367$ 。综合实验结果不难发现,此时的防御收益 U_D^* 既是局部最优解,又是全局最优解,说明面对不同攻击周期 P_A 时,存在与之对应的最优防御周期 P_D^* 使得防御收益 U_D^* 最大。以上实验验证了模型的合理性。

图4所示是在防御周期 P_D 一定的情况下,防御收益 U_D 与攻击周期 P_A 和防御成本 C_D 的关系。

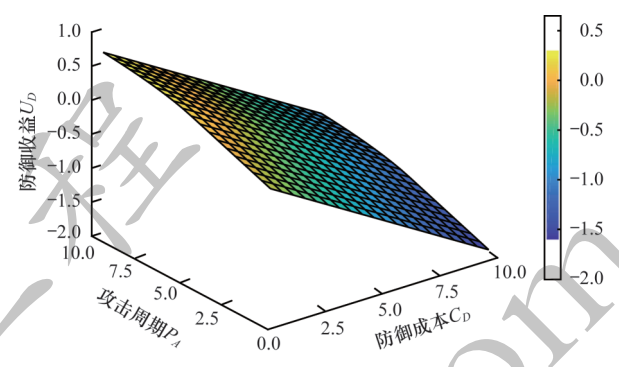


图4 防御收益与攻击周期和防御成本的关系
Fig.4 Relationship between defense benefit, attack cycle and defense cost

假设防御周期 $P_D=5$,由图4可知,防御收益 U_D 随着行动成本 C_D 的增加而减小,说明行动成本是制约防御收益 U_D 的1个关键因素。随着攻击周期区间 P_A 的增大,防御收益 U_D 总体呈现上升趋势,当 $P_A\leq 5$ 时,防御收益 U_D 与攻击周期 P_A 成正比;当 $P_A>5$ 时,防御收益 U_D 虽持续保持增长态势,但增长速度逐渐变缓,这是由于当攻防周期 $P_A=P_D$ 时,防御收益 U_D 会发生跳变,具体分析见式(4)和式(6),这侧面说明动态调整防御策略 P_D 对抵御不同类型的攻击周期 P_A 起到了关键作用。

图5所示是攻击周期 P_A 在一定条件下,防御收益 U_D 与防御周期 P_D 和防御成本 C_D 的关系。

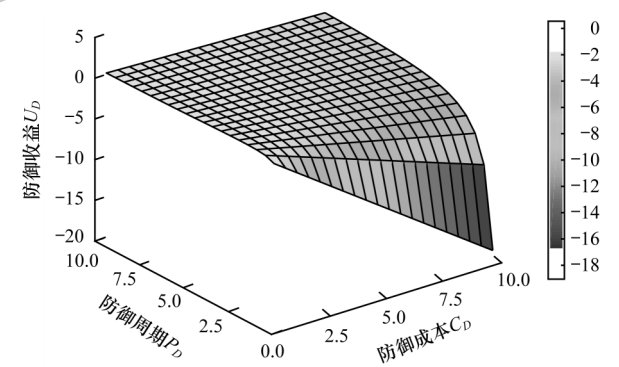


图5 防御收益与防御周期和防御成本的关系
Fig.5 Relationship between defense benefit, defense cycle and defense cost

假设攻击周期 $P_A=5$,由图5可知,防御收益 U_D 与防御成本 C_D 呈反比关系,随着防御周期区间 P_D 的增大,防御收益 U_D 呈现先上升后下降趋势,这再次验证了当攻击周期 P_A 一定,且付出的防御成本 C_D 相同时,存在

最优防御策略 P_D^* 使防御收益 U_D^* 最大化。

由上述仿真结果数据的分析可以发现,防御周期和攻防成本是决定防御收益的主要因素。

3.3 对比实验与分析

现有的网络安全防御决策研究主要针对攻防行为策略进行分析建模,忽视了行动时机对系统安全的重要影响,且系统设定的防御时机策略一般为固定的周期策略,如软件的定期杀毒、密码重置、密钥定期更新等,但静态被动的时间防御策略不能及时有效地抵御网络攻击行为。为此,将本文方法与已有的固定先验周期的防御方法进行对比,分析当攻击方的行动周期 P_A 固定时,不同的防御策略 P_D 对防御收益 U_D 的影响。由前述实验可知,成本是制约防御收益 U_D 的主要因素,为方便验证实验结论,排除其他无关干扰因素,本文假设每次攻防的行动成本均为1s(即行动成本为控制网络目标节点1s的所有权),实验收益设定为双方控制资源的总时间(s)减去行动的总次数(次数即秒数)。本文以攻击方固定周期策略 $P_A=3$ 和 $P_A=5$ 为例进行对比实验,探究当攻击周期 P_A 固定时,改变不同的防御周期策略 P_D 对防御收益 U_D 的影响,实验结果如图6和图7所示。

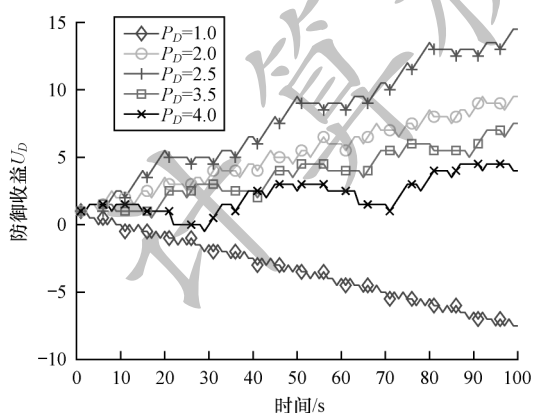


图6 攻击周期与防御收益随时间的变化关系($P_A=3$)

Fig.6 Relationship between attack cycle and defense benefit over time ($P_A=3$)

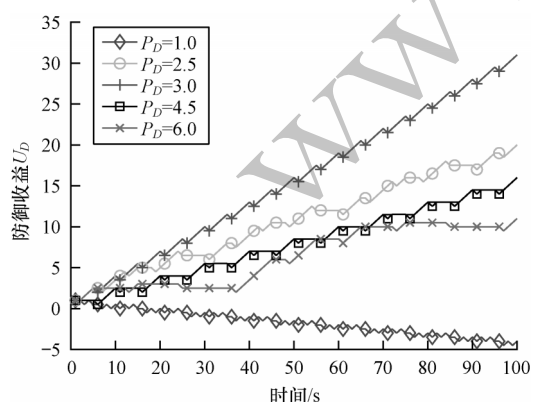


图7 攻击周期与防御收益随时间的变化关系($P_A=5$)

Fig.7 Relationship between attack cycle and defense benefit over time ($P_A=5$)

图6和图7分别表示当攻击周期固定为 $P_A=3$ 和 $P_A=5$ 时,通过调整不同的防御策略 P_D ,防御收益 U_D 随时间 t 的变化情况。由图可知,当攻防双方均采用周期策略时,产生的收益情况也呈现周期性变化。设定攻击方采取固定周期策略 $P_A=3$,当防御方采取防御策略 $P_D=1$ 时,防御收益 U_D 为负;当防御策略 $P_D=2, 2.5, 3, 4$ 时,防御收益 U_D 均为正,特别的,当防御策略 $P_D=2.5$ 时,防御收益 U_D 达到最大。设定攻击方采取固定周期策略 $P_A=5$,当防御方采取防御策略 $P_D=1$ 时,防御收益 U_D 仍为负;当防御策略 $P_D=2.5, 3, 4.5, 6$ 时,防御收益 U_D 持续增加,且当防御策略 $P_D=3$ 时,防御收益 U_D 最大。

由此说明,当攻击策略 P_A 一定时,选取不同的防御策略 P_D 会产生不同的防御收益 U_D 。如果防御策略 P_D 很小(即行动周期短),可能会因行动次数的增加导致防御收益 U_D 为负;随着防御策略 P_D 逐渐增大,防御收益 U_D 先增加后减小,而且随着时间 t 的增加,不同防御策略 P_D 产生的防御收益 U_D 之间的差距也愈加明显,即存在最优的防御策略 P_D^* 和最佳防御收益 U_D^* 。对比实验结果与仿真实验所得结果一致。以图6为例,当攻击策略一定时,采用固定防御策略的平均收益为0.21,动态调整防御策略的平均收益为0.26,防御收益提高了23.81%。实验数据表明相较于先验的固定周期防御策略,实时动态调整防御策略才是更有效的安全防御手段,验证了本文模型和算法有效且可行。

4 结束语

本文从网络攻防时机角度模拟攻防双方控制目标资源的状态,并基于FlipIt时间博弈理论,结合SIR模型传播规律,对实时变化的网络系统状态进行分析研究,最终构建攻防时机博弈模型。提出博弈双方收益计算方法、均衡求解方法和最优防御策略选取算法,从理论分析和数值仿真实验两方面验证本文模型和算法的有效性和科学性。在此基础上,与现有固定周期的防御方法进行对比,进一步说明动态调整时间策略的必要性。实验结果表明,当攻击策略一定时,使用本文方法动态选择最优防御策略的平均收益为0.26,相比传统固定防御方法,平均防御收益提高了23.81%。下一步将通过应用复杂网络理论,分析传播动力学模型在真实网络环境中的传播规律,从而设计应用于现实环境中大规模复杂网络的实时防御决策方法。

参考文献

- [1] WU Z N, TIAN L Q, WANG Y, et al. Network security defense decision-making method based on stochastic game and deep reinforcement learning[J]. Security and Communication Networks, 2021, 23(7): 1-13.
- [2] 方滨兴. 定义网络空间安全[J]. 网络与信息安全学报, 2018, 4(1): 1-5.

- FANG B X. Define cyberspace security[J]. Chinese Journal of Network and Information Security, 2018, 4(1): 1-5. (in Chinese)
- [3] 胡瑞钦,谭晶磊,彭心荷,等. 面向SDN数据层的双虚拟IP地址动态跳变技术[J]. 信息网络安全, 2022, 22(2): 76-85.
- HU R Q, TAN J L, PENG X H, et al. Dynamic hopping technology of double virtual IP address for SDN data layer[J]. Netinfo Security, 2022, 22(2): 76-85. (in Chinese)
- [4] 习近平. 在网络安全和信息化工作座谈会上的讲话[M]. 北京:人民出版社, 2016.
- XI J P. Speech at the symposium on network security and informatization[M]. Beijing: People's Publishing House, 2016. (in Chinese)
- [5] LI X T. Decision making of optimal investment in information security for complementary enterprises based on game theory[J]. Technology Analysis & Strategic Management, 2021, 33(7): 755-769.
- [6] ETESAMI S R, BAŞAR T. Dynamic games in cyber-physical security: an overview[J]. Dynamic Games and Applications, 2019, 9(4): 884-913.
- [7] LIU X H, ZHANG H W, ZHANG Y C, et al. Optimal network defense strategy selection method based on evolutionary network game[J]. Security and Communication Networks, 2020, 38(7): 1-11.
- [8] CHEN X Y, LIU X T, ZHANG L, et al. Optimal defense strategy selection for spear-phishing attack based on a multistage signaling game[J]. IEEE Access, 2019, 7: 19907-19921.
- [9] LIU X H, ZHANG H W, ZHANG Y C, et al. Active defense strategy selection method based on two-way signaling game[J]. Security and Communication Networks, 2019, 41(2): 1-14.
- [10] AYDEGER A, MANSHAEI M H, RAHMAN M A, et al. Strategic defense against stealthy link flooding attacks: a signaling game approach[J]. IEEE Transactions on Network Science and Engineering, 2021, 8(1): 751-764.
- [11] XU X T, WANG G C, HU J T, et al. Study on stochastic differential game model in network attack and defense[J]. Security and Communication Networks, 2020, 34(5): 1-15.
- [12] 孙岩,姬伟峰,翁江,等. 基于微分博弈的移动目标防御最优策略[J]. 计算机研究与发展, 2021, 58(8): 1789-1800.
- SUN Y, JI W F, WENG J, et al. Optimal strategy of moving target defense based on differential game[J]. Journal of Computer Research and Development, 2021, 58(8): 1789-1800. (in Chinese)
- [13] 杨峻楠,张红旗,张传富. 基于随机博弈与改进WoLF-PHC的网络防御决策方法[J]. 计算机研究与发展, 2019, 56(5): 942-954.
- YANG J N, ZHANG H Q, ZHANG C F. Network defense decision-making method based on stochastic game and improved WoLF-PHC[J]. Journal of Computer Research and Development, 2019, 56(5): 942-954. (in Chinese)
- [14] SAMIR M, AZAB M, SAMIR E. SD-CPC: SDN controller placement camouflage based on stochastic game for moving-target defense[J]. Computer Communications, 2021, 168: 75-92.
- [15] 金志刚,王新建,李根,等. 融合攻击图和博弈模型的网络防御策略生成方法[J]. 信息网络安全, 2021, 21(1): 1-9.
- JIN Z G, WANG X J, LI G, et al. The generation method of network defense strategy combining with attack graph and game model[J]. Netinfo Security, 2021, 21(1): 1-9. (in Chinese)
- [16] 张恒巍,黄健明. 基于Markov演化博弈的网络防御策略选取方法[J]. 电子学报, 2018, 46(6): 1503-1509.
- ZHANG H W, HUANG J M. Network defense strategy selection method based on Markov evolutionary game[J]. Acta Electronica Sinica, 2018, 46(6): 1503-1509. (in Chinese)
- [17] LIU Y H, CHEN H, ZHANG H, et al. Defense strategy selection model based on multistage evolutionary game theory[J]. Security and Communication Networks, 2021, 49(4): 1-15.
- [18] DIJK M, JUELS A, OPREA A, et al. FlipIt: the game of "stealthy takeover"[J]. Journal of Cryptology, 2013, 26(4): 655-713.
- [19] 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.
- TAN J L, ZHANG H W, ZHANG H Q, et al. Optimal strategy selection approach of moving target defense based on Markov time game[J]. Journal on Communications, 2020, 41(1): 42-52. (in Chinese)
- [20] NOCHENSON A, GROSSKLAGS J. A behavioral investigation of the FlipIt game[EB/OL]. [2021-12-05]. https://www.researchgate.net/publication/263606042_A_Behavioral_Investigation_of_the_FlipIt_Game.
- [21] LASZKA A, HORVATH G, FELEGYHAZI M, et al. Modeling targeted attacks with for multiple resources[C]// Proceedings of International Conference on Decision and Game Theory for Security. Berlin, Germany: Springer, 2014: 175-194.
- [22] JONES S, OUTKIN A, GEARHART J, et al. Evaluating moving target defense with PLADD[EB/OL]. [2021-12-05]. <https://www.osti.gov/servlets/purl/1222986/>.
- [23] 丁绍虎,齐宁,郭义伟. 基于M-FlipIt博弈模型的拟态防御策略评估[J]. 通信学报, 2020, 41(7): 186-194.
- DING S H, QI N, GUO Y W. Evaluation of mimic defense strategy based on M-FlipIt game model[J]. Journal on Communications, 2020, 41(7): 186-194. (in Chinese)
- [24] KERMACK W O, MCKENDRICK A. A contribution to the mathematical theory of epidemics[EB/OL]. [2021-12-05]. https://www.researchgate.net/publication/237076919_A_Contribution_to_the_Mathematical_Theory_of_Epidemics.
- [25] MYERSON R B. Game theory: analysis of conflict[EB/OL]. [2021-12-05]. https://www.researchgate.net/publication/220689692_Game_Theory_Analysis_of_Conflict.
- [26] 谢识予. 经济博弈论(第4版)[M]. 上海:复旦大学出版社, 2017.
- XIE S Y. Economic game theory (the 4th Edition)[M]. Shanghai: Fudan University Press, 2017. (in Chinese)
- [27] GORDON L, LOEB M, LUCYSHYN W, et al. CSI/FBI computer crime and security survey[EB/OL]. [2021-12-05]. https://www.researchgate.net/publication/243784811_CSI_FBI_Computer_Crime_and_Security_Survey.