基于定性微分博弈的网络安全威胁预警方法

黄世锐[1]，张恒巍[1,2]，王晋东[1]，窦睿彧[1]
（1.信息工程大学三院，河南 郑州 450001；2.信息保障技术重点实验室，北京 100093）

摘 要：目前，基于博弈理论的网络安全研究大多采用静态博弈或多阶段动态博弈模型，不符合实际网络攻防连续对抗、实时变化的特点，为了更加贴近攻防实际进行安全威胁预警，借鉴传染病动力学模型分析安全威胁传播过程，基于定性微分博弈理论构建网络攻防博弈模型，推演安全威胁动态变化趋势。在此基础上，提出攻防定性微分博弈求解方法，构造攻防界栅以及捕获区和躲避区；引入多维欧氏距离，度量不同安全状态的威胁严重程度；进而设计预警算法，实现对网络安全威胁的动态预警，且具有更好的准确性和时效性。仿真实验结果表明，所提模型和算法有效且可行。

关键词：网络安全威胁；网络攻防；威胁预警；定性微分博弈；预警算法
中图分类号：TP309
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2018134

Network security threat warning method based on qualitative differential game

HUANG Shirui[1], ZHANG Hengwei[1,2], WANG Jindong[1], DOU Ruiyu[1]
1. The Third Institute, Information Engineering University, Zhengzhou 450001, China
2. Science and Technology on Information Assurance Laboratory, Beijing 100093, China

Abstract: Most current network security research based on game theory adopts the static game or multi-stage dynamic game model, which does not accord with the real-time change and continuity of the actual network attack-defense process. To make security threats warning more consistent with the attack-defense process, the threat propagation process was analyzed referring to the epidemic model. Then the network attack-defense game model was constructed based on the qualitative differential game theory, by which the evolution of the network security state could be predicted. Based on the model, the qualitative differential game solution method was designed to construct the attack-defense barrier and divide the capture area. Furthermore, the threat severity in different security states were evaluated by introducing multidimensional Euclidean distance. By designing the warning algorithm, the dynamic warning of the network security threat was realized, which had better accuracy and timeliness. Finally, simulation results verify the effectiveness of the proposed algorithm and model.

Key words: network security threat, network attack and defense, threat warning, qualitative differential game, warning algorithm

收稿日期：2018−03−13；**修回日期**：2018−07−17
通信作者：张恒巍，zhw11qd@126.com
基金项目：国家自然科学基金资助项目（No.61303074, No.61309013）；河南省科技攻关计划基金资助项目（No.182102210144）；信息保障技术重点实验室开放基金资助项目（No.KJ-15-110）
Foundation Items: The National Natural Science Foundation of China (No.61303074, No.61309013), The Science and Technology Research Project of Henan Province (No.182102210144), The Opening Foundation of Sciense and Technology on Information Assurance Laboratory (No.KJ-15-110)

1 引言

传统网络安全威胁分析方法[1-2]忽视了安全威胁的基本属性是在网络攻击和防御措施的对抗竞争中不断变化的，在准确性和可靠性上存在不足。网络安全的本质在于攻防对抗，而博弈论是研究博弈方发生直接作用时决策及其均衡问题的理论[3]，与网络攻防的基本特征高度吻合[4]。因此，采用博弈论分析推演攻防对抗行为及其相互影响，进而提出网络安全威胁预警方法，具有重要的借鉴意义和理论价值，已成为近年来的研究热点。

目前，运用博弈理论进行网络安全研究已经取得部分成果。但随着网络技术的不断发展，网络对抗过程趋于动态化、高频化、连续化，传统博弈模型[5-7]仅能分析一次攻防过程或时间间断、离散的多阶段攻防过程，已经难以满足网络安全威胁预警的时效性要求。定性微分博弈理论是在借助微分方程描述连续时间内的状态转移并分析博弈方连续决策过程的基础上，研究在攻防对抗中某一目标结局能否实现的理论工具[8]。将定性微分博弈引入安全威胁预警研究，一方面，利用微分方程分析连续时间内的网络安全威胁传播行为和安全状态迁移过程[9-10]，采用含有时间变量的连续路径表示攻防策略选取轨迹，更符合实际网络攻防行为的高频变化性和时间连续性，使威胁预警方法更具动态性和时效性；另一方面，利用该理论构造界栅面，将网络安全状态空间分为捕获区和躲避区，分别表示攻击方和防御方的优势区域，据此可以对安全威胁状态演化趋势进行动态预测与度量。但是，定性微分博弈是多维相空间中的连续变化过程[11]，网络攻防模型构建和分析难度大，据我们所知，目前尚未有公开文献对上述方法予以讨论。

本文在定性微分博弈理论的基础上，为更加准确、有效地预测网络威胁状态演化情况，将网络系统划分为不同功能的子网络，借助传染病动力学模型描述网络威胁传播过程；在此基础上，构建网络攻防定性微分博弈（NSDG, network security qualitative differential game）模型，分析攻防实时变化条件下的网络安全威胁动态变化过程；进而提出攻防定性微分博弈求解方法，构造攻防界栅划分捕获区和躲避区，并引入多维空间欧氏距离计算不同安全状态的威胁严重程度，设计安全威胁预警算法。与现有成果相比，本文方法更加符合实际情况，能够研究连续实时攻防对抗下的网络安全威胁演化趋势，并对安全威胁进行动态预警，准确性和时效性更强。

2 网络攻防定性微分博弈模型

2.1 网络安全威胁传播过程分析

借鉴传染病动力学理论[12]，本文将网络节点的安全状态分为正常状态 N 和感染状态 I，并用 $N(t)$ 和 $I(t)$ 分别表示 t 时刻网络中正常节点和感染节点的数量。同时，本文借鉴经典传染病模型 SEM 描述网络安全威胁传播过程[9]。假设网络节点总数 Q 保持不变，用 $\rho(t)$ 表示 t 时刻网络中感染节点的密度，用 $1-\rho(t)$ 表示 t 时刻网络中正常节点的密度，并且 $\rho(t)=\dfrac{I(t)}{Q}$，用 $\nu_a(t)$ 和 $\nu_d(t)$ 分别表示在攻防对抗中，正常节点转化为感染节点的感染速率和感染节点成功修复为正常状态的修复速率。根据传染病模型理论，可以得到网络安全威胁传播方程为

$$\frac{\mathrm{d}\rho(t)}{\mathrm{d}t}=\nu_a(t)\theta(t)[1-\rho(t)]-\nu_d(t)\rho(t) \tag{1}$$

其中，$\theta(t)$ 表示 t 时刻正常节点与感染节点相连的概率。若假设网络节点数量较大且感染节点相互距离较远，忽略感染节点影响范围的重叠效应，则 $\theta(t)=1-(1-\rho(t))^{\beta}$，$\beta$ 为节点连通度。

结合攻防实际情况进行分析可知，由于节点安全状态的转化是由攻防策略相互作用共同决定的，式(1)中的感染速率 $\nu_a(t)$ 可以由 t 时刻的攻击效用 $a(t)$ 表示，而修复速率 $\nu_d(t)$ 则由防御效用 $d(t)$ 表示。以一个攻防实例进行简要说明，假设攻击方可能采取高、中、低这 3 种强度类型的攻击行为，用 $e_{\mathrm{A}}^{\mathrm{H}}$、$e_{\mathrm{A}}^{\mathrm{M}}$、$e_{\mathrm{A}}^{\mathrm{L}}$ 分别表示其平均攻击强度；防御方采取的平均防御行为强度分别表示为 $e_{\mathrm{D}}^{\mathrm{H}}$、$e_{\mathrm{D}}^{\mathrm{M}}$、$e_{\mathrm{D}}^{\mathrm{L}}$。则 t 时刻攻击效用和防御效用可以分别表示为 $a(t)=p_{\mathrm{A}}^{\mathrm{H}}(t)e_{\mathrm{A}}^{\mathrm{H}}+p_{\mathrm{A}}^{\mathrm{M}}(t)e_{\mathrm{A}}^{\mathrm{M}}+p_{\mathrm{A}}^{\mathrm{L}}(t)e_{\mathrm{A}}^{\mathrm{L}}$ 和 $d(t)=p_{\mathrm{D}}^{\mathrm{H}}(t)e_{\mathrm{D}}^{\mathrm{H}}+p_{\mathrm{D}}^{\mathrm{M}}(t)e_{\mathrm{D}}^{\mathrm{M}}+p_{\mathrm{D}}^{\mathrm{L}}(t)e_{\mathrm{D}}^{\mathrm{L}}$。其中，$\boldsymbol{P}_{\mathrm{A}}(t)=(p_{\mathrm{A}}^{\mathrm{H}}(t),\ p_{\mathrm{A}}^{\mathrm{M}}(t),p_{\mathrm{A}}^{\mathrm{L}}(t))$ 和 $\boldsymbol{P}_{\mathrm{D}}(t)=(p_{\mathrm{D}}^{\mathrm{H}}(t),p_{\mathrm{D}}^{\mathrm{M}}(t),p_{\mathrm{D}}^{\mathrm{L}}(t))$ 均为概率向量，分别表示攻防双方在 t 时刻的混合策略。根据上述分析，网络安全威胁传播方程可以进一步表示为

$$\begin{cases}\dfrac{\mathrm{d}\rho(t)}{\mathrm{d}t}=-d(t)\rho(t)+a(t)\theta(t)[1-\rho(t)]\\ a(t)=p_{\mathrm{A}}^{\mathrm{H}}(t)e_{\mathrm{A}}^{\mathrm{H}}+p_{\mathrm{A}}^{\mathrm{M}}(t)e_{\mathrm{A}}^{\mathrm{M}}+p_{\mathrm{A}}^{\mathrm{L}}(t)e_{\mathrm{A}}^{\mathrm{L}}\\ d(t)=p_{\mathrm{D}}^{\mathrm{H}}(t)e_{\mathrm{D}}^{\mathrm{H}}+p_{\mathrm{D}}^{\mathrm{M}}(t)e_{\mathrm{D}}^{\mathrm{M}}+p_{\mathrm{D}}^{\mathrm{L}}(t)e_{\mathrm{D}}^{\mathrm{L}}\\ \theta(t)=1-(1-\rho(t))^{\beta}\end{cases} \tag{2}$$

由于应用场景和服务需求的不同，大型网络往往由多个业务子网构成，本文以网络功能和拓扑为边界将网络划分为多个功能子网络，利用上述网络安全威胁传播方程分析各子网络感染节点的密度状态，进而刻画整体网络中安全威胁的影响范围和严重程度，预测网络安全威胁动态变化过程并实现预警。

2.2　构造网络攻防定性微分博弈模型

定义 1　网络攻防定性微分博弈模型可以用八元组表示，即 $NSDG=\left(N,B,S,t,X,P,f,G\right)$，各变量定义如下。

1) $N=(N_{\mathrm{D}},N_{\mathrm{A}})$ 表示网络攻防定性微分博弈的参与者空间，N_{D} 表示防御者，N_{A} 表示攻击者。

2) $B=(DS,AS)$ 表示攻防行动空间，其中，$DS=\{DS_j\,|1\leqslant j\leqslant n\}$，$DS_j$ 表示防御方的可选防御策略；$AS=\{AS_i\,|1\leqslant i\leqslant m\}$，$AS_i$ 表示攻击方的可选攻击策略。

3) $S=\{S_k\,|k=1,\cdots,K\}$ 表示网络系统根据功能和拓扑划分而成的子网络集合，其中，K 表示子网络数目，S_k 表示第 k 个子网络，并用 β_k 表示子网络 S_k 的平均连通度。

4) $t\in[t_{\mathrm{bin}}\,,t_{\mathrm{end}}]$ 表示网络攻防定性微分博弈的时刻。

5) $X(t)=\{(\rho_1(t),\cdots,\rho_k(t),\cdots,\rho_K(t))\ |0\leqslant\rho_k(t)\leqslant1,\ k=1,\cdots,K\}$ 表示 t 时刻的网络安全状态变量，是由各个子网络感染节点密度 $\rho_k(t)$ 组成的 K 维状态空间。由于 $\rho_k(t)$ 是由网络中感染节点的数量决定的，因此安全状态在 K 维状态空间中是离散分布的。

6) $P=\{\boldsymbol{P}_{\mathrm{D}}(t),\boldsymbol{P}_{\mathrm{A}}(t)\}$ 表示攻防双方在 t 时刻的控制策略，是以时间为变量的控制轨迹。$\boldsymbol{P}_{\mathrm{D}}(t)=\{p_{\mathrm{D}}^j(t)\,|1\leqslant j\leqslant n\}$ 表示防御者在 t 时刻选取的混合策略，$\sum_{j=1}^{n}p_{\mathrm{D}}^j(t)=1$；$\boldsymbol{P}_{\mathrm{A}}(t)=\{p_{\mathrm{A}}^i(t)\,|1\leqslant i\leqslant m\}$ 表示攻击者在 t 时刻选取的混合策略，$\sum_{i=1}^{m}p_{\mathrm{A}}^i(t)=1$。

7) $f=\{f_k\,|k=1,\cdots,K\}$ 表示网络安全状态迁移函数，是每个子网络感染节点密度 $\rho_k(t)$ 随时间变化的函数，即 2.1 节中的网络安全威胁传播方程。其中，$f_k=\dfrac{\mathrm{d}\rho_k(t)}{\mathrm{d}t}$，具体分析参见 2.1 节。

8) $G=\{(\overline{\rho_1}(t),\cdots,\overline{\rho_K}(t))\,\big|(\overline{\rho_1}(t),\cdots,\overline{\rho_K}(t))\in X,\ \varphi(\overline{\rho_1}(t),\cdots,\overline{\rho_K}(t))\leqslant\Theta\}$ 表示攻击目标集，也是网络安全风险高危区域。在网络对抗中，攻击方试图通过一系列攻击行为，使网络安全状态迁移至目标集内，从而达成攻击目标，而防御方则采取防御措施避免这一结果发生。

基于博弈模型定义和 2.1 节的分析结论，考虑各子网络功能拓扑的差异性，参考文献[10]，将 NSDG 模型中的攻防博弈目标集边界函数定义为

$$\partial G=\Theta=e_1\rho_1'(t)+\cdots+e_K\rho_K'(t)=\sum_{k=1}^{K}e_k\rho_k'(t)\quad(3)$$

其中，Θ 表示达到网络功能瘫痪阈值时的感染节点总数[10]，e_k 表示子网络 S_k 的节点数量且 $e_1+e_2+\cdots+e_K=Q$，$\rho_k'(t)$ 表示达到瘫痪阈值时子网络 S_k 的感染节点密度。

3　博弈求解分析与威胁预警算法设计

3.1　网络攻防定性微分博弈求解

在网络攻防定性微分博弈模型的基础上，根据定性微分博弈理论，可将网络安全多维状态空间划分为捕获区和躲避区[8]。若当前网络安全状态 X 位于捕获区内，则攻击方通过采取恰当的攻击策略总能使安全状态到达目标集内，实现预期目标；若位于躲避区内，则防御方采取恰当的防御措施总能抵御威胁的进一步传播，防止安全状态迁移至目标集内。因此，攻防双方都将采取最优策略进行连续对抗，避免落入对方的优势区域内，使网络安全状态在 2 个区域的分界面上不断迁移。而捕获区和躲避区的分界面则称为攻防定性微分博弈的攻防界栅。

定义 2　攻防界栅。在网络攻防定性微分博弈模型中，攻防界栅就是攻防双方最优控制策略 $(P_{\mathrm{D}}^*(t),P_{\mathrm{A}}^*(t))$ 对应的网络安全状态轨迹 $X^*(t)$，是区分捕获区（攻击者优势区域）和躲避区（防御者势区域）的界线。

求解网络攻防定性微分博弈问题的本质就是计算网络攻防界栅 $X^*(t)$ 并对多维状态空间进行划分，确定捕获区和躲避区。通过对第 2 节的分析和定义，结合定性微分博弈理论，给出求解网络攻防定性微分博弈问题的具体过程和步骤如下。

1)令向量 $\boldsymbol{\lambda}^{\mathrm{T}}=(\lambda_1,\lambda_2,\cdots,\lambda_K)^{\mathrm{T}}\in R^K$，构建 Hamilton 函数 $H\left(X,\boldsymbol{P}_{\mathrm{D}}(t),\boldsymbol{P}_{\mathrm{A}}(t),\boldsymbol{\lambda}\right)$ 表示网络安全状态的变化率，即

$$\begin{aligned}&H\left(X(t),\boldsymbol{P}_{\mathrm{D}}(t),\boldsymbol{P}_{\mathrm{A}}(t),\boldsymbol{\lambda}\right)=\boldsymbol{\lambda}^{\mathrm{T}}f\left(X(t),\boldsymbol{P}_{\mathrm{D}}(t),\boldsymbol{P}_{\mathrm{A}}(t)\right)\\&=\sum_{k\in K}\lambda_k\left\{-d(t)\rho_k(t)+a(t)[1-(1-\rho_k(t))^{\beta_k}]\left(1-\rho_k(t)\right)\right\}\end{aligned}\tag{4}$$

2)根据双边极值定理[8]，求出最优控制策略 $(\boldsymbol{P}_{\mathrm{D}}^*(t),\boldsymbol{P}_{\mathrm{A}}^*(t))$，使其满足

$$\begin{aligned}&\max_{\boldsymbol{P}_{\mathrm{D}}(t)}\min_{\boldsymbol{P}_{\mathrm{A}}(t)}H\left(X(t),\boldsymbol{P}_{\mathrm{D}}(t),\boldsymbol{P}_{\mathrm{A}}(t),\boldsymbol{\lambda}\right)\\&=\min_{\boldsymbol{P}_{\mathrm{A}}(t)}\max_{\boldsymbol{P}_{\mathrm{D}}(t)}H\left(X(t),\boldsymbol{P}_{\mathrm{D}}(t),\boldsymbol{P}_{\mathrm{A}}(t),\boldsymbol{\lambda}\right)\\&=H\left(X^*(t),\boldsymbol{P}_{\mathrm{D}}^*(t),\boldsymbol{P}_{\mathrm{A}}^*(t),\boldsymbol{\lambda}\right)\end{aligned}\tag{5}$$

其中，$X^*(t)$ 表示由最优控制策略 $(\boldsymbol{P}_{\mathrm{D}}^*(t),\boldsymbol{P}_{\mathrm{A}}^*(t))$ 所确定的最优轨迹。

3)计算伴随方程组 $\dot{\boldsymbol{\lambda}}=-\nabla_X H(X(t)^*,\boldsymbol{P}_{\mathrm{D}}^*(t),\boldsymbol{P}_{\mathrm{A}}^*(t),\boldsymbol{\lambda})$，对于 $\forall\dot{\lambda}_k\in\dot{\boldsymbol{\lambda}}$，$\dot{\lambda}_k=-\dfrac{\partial H\left(X(t),\boldsymbol{P}_{\mathrm{D}}(t),\boldsymbol{P}_{\mathrm{A}}(t),\boldsymbol{\lambda}\right)}{\partial\rho_k(t)}$。其中，$\rho_k(t)$ 表示子网络 S_k 的感染节点密度。

4)构建攻防博弈目标边界集 $X(t)\big|_{\partial G}$ 为

$$\begin{aligned}X(t)\big|_{\partial G}=\varphi(c_1,c_2,\cdots,c_{k-2})=(&\varphi_1(c_1,c_2,\cdots,c_{k-2}),\\&\varphi_2(c_1,c_2,\cdots,c_{k-2}),\cdots,\varphi_k(c_1,c_2,\cdots,c_{k-2}))\end{aligned}\tag{6}$$

其中，$c_1,c_2,\cdots,c_{k-2}$ 表示辅助参数，$\varphi_k(c_1,c_2,\cdots,c_{k-2})$ 对应边界集 $X(t)\big|_{\partial G}$ 上 $\rho_k(t)$ 的参数表达式。

5)据单位法向量具体定义，计算如下方程组确定攻防博弈目标边界集 $X(t)\big|_{\partial G}$ 上的单位法向量 $\boldsymbol{\lambda}\big|_{\partial G}$。

$$\begin{cases}\displaystyle\sum_{i=1}^{K}\lambda_i\frac{\partial\varphi_i(c_1,c_2,\cdots,c_{k-2})}{\partial c_j}=0\ ,\ j=1,2,\cdots,k-2\\ \boldsymbol{\lambda}\boldsymbol{\lambda}^{\mathrm{T}}\big|_{\partial G}=1\end{cases}\tag{7}$$

6)根据半透曲面[8]的必要条件，令 $H(X^*(t),\boldsymbol{P}_{\mathrm{D}}^*(t),\boldsymbol{P}_{\mathrm{A}}^*(t),\boldsymbol{\lambda})\big|_{\partial G}=0$，求出在攻防博弈目标边界集 G 上的最优攻防策略 $\boldsymbol{P}_{\mathrm{D}}^*(t)$ 和 $\boldsymbol{P}_{\mathrm{A}}^*(t)$ 以及目标集上的可用部分边界 BUP（目标边界集上 H=0 的部分）[8]，即攻防界栅初始状态位置集合 $X(t)\big|_{\partial BUP}$。

7) 以 BUP 上的点 $X(t)\big|_{\partial BUP}$ 为初始点，倒向积分伴随方程组和网络安全状态迁移方程组可以求出网络安全最优轨迹 $X^*(t)$，即为网络攻防界栅。

联立式(5)~式(7)，计算如下方程组

$$\begin{cases}\dot{\boldsymbol{\lambda}}=-\nabla_X H(X(t),\boldsymbol{P}_{\mathrm{D}}^*(t),\boldsymbol{P}_{\mathrm{A}}^*(t),\boldsymbol{\lambda})\\ \dot{X}(t)=f\left(X(t),\boldsymbol{P}_{\mathrm{D}}^*(t),\boldsymbol{P}_{\mathrm{A}}^*(t)\right)\\ X(0)=X(t)\big|_{\partial BUP}=\varphi(c_1,c_2,\cdots,c_{k-2})\\ \boldsymbol{\lambda}(0)=\boldsymbol{\lambda}\big|_{\partial G}\\ \boldsymbol{\lambda}\boldsymbol{\lambda}^{\mathrm{T}}\big|_{\partial G}=1\\ \displaystyle\sum_{i=1}^{K}\lambda_i\frac{\partial\varphi_i(c_1,c_2,\cdots,c_{k-2})}{\partial c_j}=0,j=1,2,\cdots,k-2\end{cases}\tag{8}$$

其中，对伴随方程组进行倒向积分时，初始值为攻防博弈目标边界集上的单位法向量 $\boldsymbol{\lambda}\big|_{\partial G}$；对安全状态迁移方程组进行倒向积分时，初始值为 BUP 上的安全状态变量 $X(t)\big|_{\partial G}$。

3.2 基于攻防界栅的网络安全威胁预警分析

在网络攻防定性微分博弈中，攻防界栅实质上是攻防双方采取最优策略对 $(\boldsymbol{P}_{\mathrm{D}}^*(t),\boldsymbol{P}_{\mathrm{A}}^*(t))$ 时网络安全状态的迁移轨迹 $X^*(t)$，将网络安全状态空间划分为捕获区和躲避区，分别对应攻击方和防御方的优势空间[13]。基于此，网络安全状态与攻防界栅之间的距离可以度量安全威胁的严重程度。考虑到网络安全状态是由各子网络感染节点密度共同决定的，因此安全状态在多维空间中离散分布，本文引入多维空间欧几里得距离（Euclidean distance，简称欧氏距离），以安全状态到攻防界栅的最小欧氏距离评估其所处威胁程度。

定义 3 网络安全威胁程度 T。网络安全状态空间是一个有限离散的 K 维空间 V，攻防界栅 $X^*(t)$ 将多维状态空间划分为躲避区和捕获区，区域内的安全状态分别表示为 $Y_{\mathrm{D}}=\left(\rho_{\mathrm{D}}^1,\rho_{\mathrm{D}}^2,\cdots,\rho_{\mathrm{D}}^k\right)\in V_{\mathrm{D}}$ 和 $Y_{\mathrm{A}}=\left(\rho_{\mathrm{A}}^1,\rho_{\mathrm{A}}^2,\cdots,\rho_{\mathrm{A}}^k\right)\in V_{\mathrm{A}}$。对于任意安全状态 $x=\left(\rho_i^1,\rho_i^2,\cdots,\rho_i^k\right)\in V_i$，其安全威胁程度 $T(x)$ 为

$$T(x)=\begin{cases}-\min\limits_{Y_{\mathrm{A}}}\mathrm{O}(x,Y_{\mathrm{A}})=\\ -\min\limits_{Y_{\mathrm{A}}}\sqrt{\left(\rho_1-\rho_{\mathrm{A}}^1\right)^2+\left(\rho_2-\rho_{\mathrm{A}}^2\right)^2+\cdots+\left(\rho_k-\rho_{\mathrm{A}}^k\right)^2}\\ \min\limits_{Y_{\mathrm{D}}}\mathrm{O}(x,Y_{\mathrm{D}})=\\ \min\limits_{Y_{\mathrm{D}}}\sqrt{\left(\rho_1-\rho_{\mathrm{D}}^1\right)^2+\left(\rho_2-\rho_{\mathrm{D}}^2\right)^2+\cdots+\left(\rho_k-\rho_{\mathrm{D}}^k\right)^2}\end{cases}\tag{9}$$

其中，$\mathrm{O}(x,Y_i)$ 表示 K 维空间中网络安全状态 x 与 Y_i 之间的欧氏距离。

当 t 时刻网络系统安全状态 $x(t)$ 处于躲避区时，

其安全威胁程度 $T(x)$ 根据与捕获区安全状态的最小距离评估确定；当网络系统安全状态 $x(t)$处于捕获区时，其安全威胁程度 $T(x)$ 根据与躲避区安全状态的最小距离评估确定。为方便分析，本文参考文献[13]的威胁等级划分标准，结合历史数据和专家经验，将威胁程度 T 划分为五级进行预警，如表 1 所示。

表 1　威胁预警等级划分标准

威胁预警等级 TL	威胁程度 T
一级	$[-1,-0.6)$
二级	$[-0.6,-0.2)$
三级	$[-0.2,0.2)$
四级	$[0.2,0.6)$
五级	$[0.6,1]$

3.3　网络安全威胁预警算法设计

基于定性微分博弈的网络安全威胁预警算法如算法 1 所示。

算法 1　基于定性微分博弈的网络安全威胁预警算法

输入　网络攻防定性微分博弈模型

输出　威胁预警等级 TL

begin

1) initialize　$(NSDG=(N,B,S,t,X,P,f,G))$；//初始化模型参数

2) initialize　$(AS=(\delta_1,\delta_2,\cdots,\delta_g),DS=(\varphi_1,\varphi_2,\cdots,\varphi_k))$；//构建攻击行为空间和防御行为空间

3)　initialize　$(\{S_1\cdots S_k\cdots S_K\},X(t)=(\rho_1(t),\cdots,\rho_k(t),\cdots,\rho_K(t)))$；//构建子网络集合并初始化网络安全状态变量

4) initialize　$(G,\{\beta_1\cdots\beta_k\cdots\beta_K\},\{f_1\cdots f_k\cdots f_K\})$；//初始化攻防博弈目标集、常量系数及网络安全状态迁移函数

5)　$H(X,\boldsymbol{P}_{\mathrm{D}}(t),\boldsymbol{P}_{\mathrm{A}}(t),\boldsymbol{\lambda})=\boldsymbol{\lambda}^{\mathrm{T}}f(X(t),\boldsymbol{P}_{\mathrm{D}}(t),\boldsymbol{P}_{\mathrm{A}}(t))$；//构造攻防微分博弈的 Hamilton 函数

6)　solve　$(\max\limits_{\boldsymbol{P}_{\mathrm{D}}(t)}\min\limits_{\boldsymbol{P}_{\mathrm{A}}(t)}H(X(t),\boldsymbol{P}_{\mathrm{D}}(t),\boldsymbol{P}_{\mathrm{A}}(t),\boldsymbol{\lambda})=\min\limits_{\boldsymbol{P}_{\mathrm{A}}(t)}\max\limits_{\boldsymbol{P}_{\mathrm{D}}(t)}H(X(t),\boldsymbol{P}_{\mathrm{D}}(t),\boldsymbol{P}_{\mathrm{A}}(t),\boldsymbol{\lambda}))$ //根据式(5)，计算最优控制策略 $(\boldsymbol{P}_{\mathrm{D}}^{*}(t),\boldsymbol{P}_{\mathrm{A}}^{*}(t))$

7) create　$(X(t)\big|_{\partial G}=\varphi(c_1,c_2,\cdots,c_{k-2}))$；//根据式(6)，参数化表示博弈目标集 G

8)　calculate　$(\sum\limits_{i=1}^{K}\lambda_i\dfrac{\partial\varphi_i(c_1,c_2,\cdots,c_{k-2})}{\partial c_j}=0$ $\&\&\ \boldsymbol{\lambda}\boldsymbol{\lambda}^{\mathrm{T}}\big|_{\partial G}=1)$；//根据式(7)，计算求解目标边界上的单位法向量 $\boldsymbol{\lambda}\big|_{\partial G}$

9) solve　$(H(X,\boldsymbol{P}_{\mathrm{D}}^{*}(t),\boldsymbol{P}_{\mathrm{A}}^{*}(t),\boldsymbol{\lambda}\big|_{\partial G})=0)$；//计算得到攻防界栅初始状态位置集合 $X\big|_{\partial BUP}$

10) dynamic programming($X^{*}(t)$)；//利用倒向积分方程组(8)，采用动态规划方法计算得到攻防界栅

11) create　$(V_{\mathrm{A}}=\{y_{\mathrm{A}}^{1},y_{\mathrm{A}}^{2},\cdots,y_{\mathrm{A}}^{m}\},V_{\mathrm{D}}=\{y_{\mathrm{D}}^{1},y_{\mathrm{D}}^{2},\cdots,y_{\mathrm{D}}^{n}\})$；//根据攻防界栅划分捕获区和躲避区，并构建捕获区安全状态空间和躲避区安全状态空间

12) for ($x\in X$)

{

13) calculate ($T(x)$)；//根据式(9)，计算求解各安全状态所处威胁程度

14) output (TL)；输出网络安全预警等级

}

end

将本文方法和其他文献进行对比，结果如表 2 所示。模型的时效性是指攻防分析和威胁预警的有效时间。相比其他文献，本文基于定性微分博弈模型分析攻防过程预测网络安全威胁的动态变化，充分考虑了攻防双方在对抗过程中行为的动态变化性以及时间连续性，预警效果更具准确性和时效

表 2　本文方法和其他文献方法对比

方法	博弈类型	博弈者类型	攻防过程	时效性	模型通用性	均衡求解	具体应用
文献[5]	不完全信息动态	2	单阶段	未考虑	差	无	效能评估
文献[7]	不完全信息动态	n	离散多阶段	未考虑	较好	详细	威胁评估
文献[14]	不完全信息静态	1	-	未考虑	差	详细	策略选取
文献[15]	不完全信息动态	2	单阶段	未考虑	差	简单	机制分析
本文	定性微分博弈	n	时间连续	好	较好	详细	威胁预警

性。同时，本文模型中的博弈方类型集合和策略集合可以扩展至 n，具有较好的通用性，且本文给出了博弈均衡求解的详细计算过程，实用性较强。

4 仿真实验与分析

4.1 实验环境描述

通过仿真实验验证本文模型和方法的有效性。服务器使用Linux操作系统、32 GB内存、主频3.2 GHz四核 CPU，并采用广泛使用的仿真工具 Scalable Simulation Framework (SSFNet)，通过设定不同的网络参数模拟不同功能拓扑和规模的网络攻防场景。参考文献[16]，并结合 2.1 节中的网络安全攻防演化分析，从 Route Views Project 中得出自治系统连接数据集，用于设计实验系统的拓扑结构，采用 2018 年 1 月 26 日的数据（NetTF Data 20180126113000）构建网络场景，其中，综合实验平台运算能力设置网络节点总数为 Q=1 200。为了采用三维图进行直观的演示分析，结合实验网络功能拓扑将网络划分为 3 个子网络，分别为数据子网、接入子网和业务子网，并设置其节点数量均为 400。

结合国家信息安全漏洞库（CNNVD）数据和文献[17-18]中的漏洞信息分析方法，参照美国 MIT 攻防行为数据库[19]，构建网络安全攻防策略集，如表 3 和表 4 所示。

表 3 攻击策略集

序号	攻击动作名称	攻击强度	攻击类型	平均攻击效用
1	Http LQ-sniffer	0.75		
2	Install Trojan	0.80	A_H	0.73
3	CF-exploit attack	0.65		
4	THS chunk overflow	0.42		
5	Attack SSH on Web Sever	0.40	A_M	0.40
6	Shutdown Database server	0.40		
7	Ssh buffer overflow	0.30		
8	Ftp rhost attack	0.30	A_L	0.27
9	Apache chunk overflow	0.21		

4.2 攻防仿真与分析

设置模型常量系数 β_1、β_2、β_3 为各子网络的平均连通度，用于计算分析网络安全状态的演化过程，具体分析见 2.1 节。根据参考文献[16]，按照不同功能子网络的节点分布情况以及拓扑结构特点，采用统计平均值设定 $\beta_1=6$、$\beta_2=4$、$\beta_3=8$。为了便于

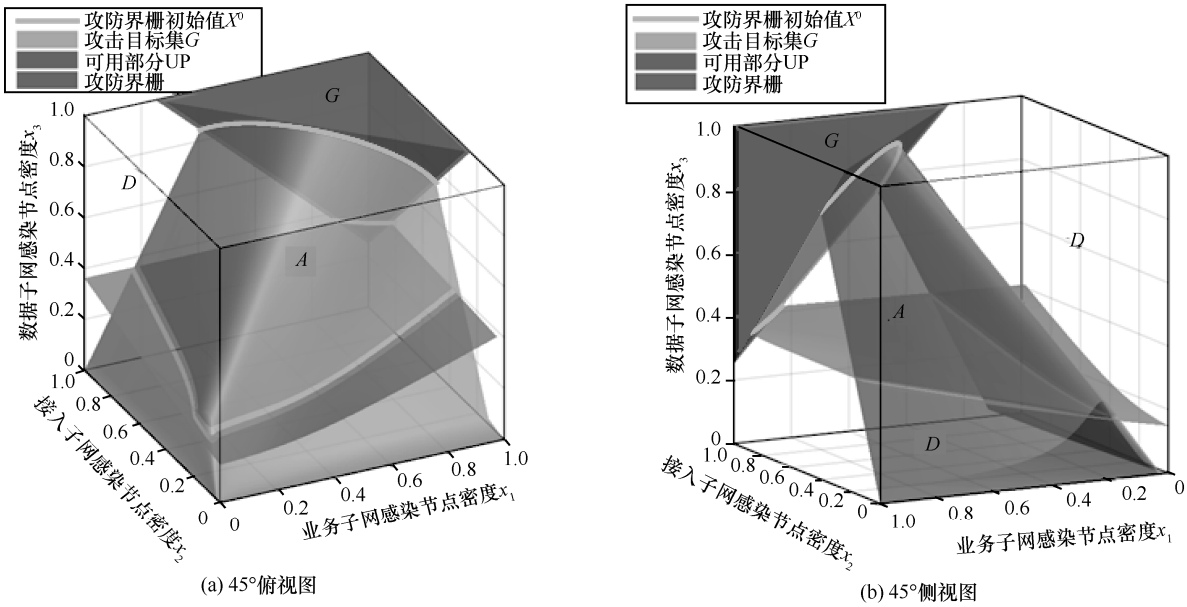
表 4 防御策略集

序号	防御动作名称	防御强度	防御类型	平均防御效用
1	Limit packets from ports	0.80		
2	Install Oracle patches	0.85	D_H	0.78
3	Reinstall Listener program	0.75		
4	Uninstall delete Trojan	0.70		
5	Renew root data	0.60		
6	Restart Database server	0.50	D_M	0.48
7	Limit SYN/ICMP packets	0.45		
8	Add physical resource	0.40		
9	Correct homepage	0.35		
10	Delete suspicious account	0.30	D_L	0.29
11	filtrate malicious packets	0.30		

实验分析，根据历史经验和专家建议，假设攻防定性微分博弈的目标集 $D=\{N_1\rho_1+N_2\rho_2+N_3\rho_3\geqslant 900\}$，即网络中感染节点总体数量超过 900 个。利用 Matlab R2016 仿真工具实现 3.3 节的网络安全威胁预警算法，计算求解攻防界栅并将网络安全状态空间划分为捕获区和躲避区，实验结果分别如图 1 和图 2 所示，算法运算用时 12.6 s。

如图 1 所示，网络安全状态三维空间由业务子网、接入子网和数据子网的感染节点密度 x_1、x_2、x_3 构成，其中，四面体所包含的深色三维区域为实验初始设置的攻击目标区域 G。通过构建网络攻防定性微分博弈模型并利用均衡求解算法，可以计算目标集区域边界面上的 BUP 状态集合，即攻防界栅初始值 X^0（如图 1 边界上 2 条线灰色曲线所示），并根据定性微分博弈理论[8]，将目标集边界面划分为可用部分 UP（初始值曲线所围成的边界面区域）和不可用部分 NUP（边界面上其余区域）。BUP 是 UP 和 NUP 的分界，同时又是攻防界栅 $X^*(t)$ 的起点。进一步通过 3.1 节方法可以求出攻防界栅 $X^*(t)$，如图 1 中由初始值曲线延伸的灰色三维曲面所示，网络安全三维空间被划分为捕获区 A 和躲避区 D。其中，捕获区 A 是由攻防界栅曲面与 UP 围成的区域空间，而躲避区 D 是由攻防界栅曲面与 NUP 围成的区域空间，两者分别表示网络攻防过程中攻防双方各自的优势区域。

如图 2 所示，以网络系统当前安全状态 x=（0.1,0.8,0.78）进行分析说明。依据 3.3 节的威胁预警算法，计算安全状态 x 与界栅曲面之间的欧氏



(a) 45°俯视图　　(b) 45°侧视图

图 1　攻防界栅曲面图（为更好地展示实验结果，(a)和(b)分别为不同视角下的攻防界栅）

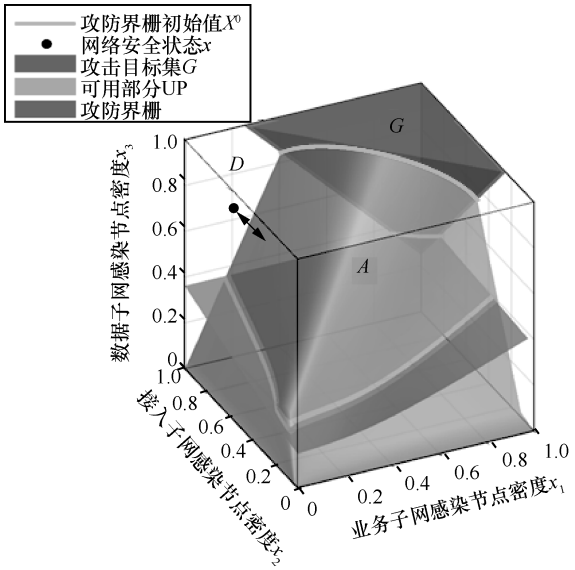


图 2　安全状态 x 与攻防界栅之间多维空间距离

距离，得到网络系统所处安全威胁程度 $T(x)$ 为

$$T(x)=-\min_{Y_A}\mathrm{O}(x,Y_A)$$

$$=-\min_{Y_A}\sqrt{\left(0.1-\rho_A^1\right)^2+\left(0.8-\rho_A^2\right)^2+\left(0.78-\rho_A^k\right)^2}$$

$$=-\sqrt{(0.1-0.36)^2+(0.8-0.65)^2+(0.78-0.58)^2}$$

$$=-0.1301$$

依据表 1，网络系统当前处于安全威胁三级预警，安全状态距离攻防界栅较近，此时，网络防御方应保持高度警戒状态，开展攻击行为实时监测，并采用针对性防御策略加强安全防护程度，以防攻击方加大攻击强度造成网络安全状态进一步恶化，突破安全“红线”。

进一步根据网络安全威胁预警算法，可以确定安全状态空间内不同状态所处的安全威胁程度及对应的预警等级，并以此为依据制定不同的防御预案，提高网络系统的主动防御能力和应急处置能力。由于安全状态数量较大，本节仅展示部分威胁预警结果，如表 5 所示。

5　结束语

目前，基于单阶段或多阶段动态博弈模型的网络安全分析方法难以分析实时变化、连续对抗的攻防过程。本文对连续时间的网络攻防过程进行研究分析，针对威胁预警需求，提出网络攻防定性微分博弈模型，构造攻防界栅划分捕获区及躲避区，引入多维空间欧氏距离评估威胁程度；在此基础上，设计网络安全威胁预警算法，确定安全状态所处威胁预警等级并根据预警等级对网络防御提出针对性建议，仿真实验验证了所提模型和算法的有效性。研究成果为分析预测动态变化的网络安全威胁状态、实现实时安全威胁预警提供了有效的模型方法，并能够为防御方制定（选取）针对性的防御预案（策略）提供指导。

未来工作主要包括进一步研究网络功能和拓扑结构等参数对威胁动态变化的影响，提升威胁预警算法的精确性和自适应性。在结合微分博弈与多目标决策

表 5　　**部分网络安全状态所处威胁预警等级**

安全状态	威胁程度	预警等级	安全状态	威胁程度	预警等级
（0.24, 0.23, 0.29）	0.041	三级预警	（0.41, 0.49, 0.23）	−0.033	三级预警
（0.37, 0.42, 0.25）	0.095	三级预警	（0.49, 0.47, 0.42）	0.256	四级预警
（0.14, 0.24, 0.64）	−0.454	二级预警	（0.61, 0.43, 0.41）	0.189	三级预警
（0.12, 0.15, 0.83）	−0.712	一级预警	（0.72, 0.84, 0.08）	−0.677	一级预警
⋮	⋮	⋮	⋮	⋮	⋮

理论的基础上，研究威胁预警—防御决策一体化方法。

参考文献：

[1] HERMANOWSKI D. Open source security information management system supporting IT security audit[C]// IEEE International Conference on Cybernetics. 2015: 336-341.

[2] KATIPALLY R, GASIOR W, CUI X, et al. Multistage attack detection system for network administrators using data mining[C]// BMJ. 2015: 1-4.

[3] FUDENBERG D, TIROLE J. Game theory[M]. Boston: Massachusettes Institute of Technology Press, 2015.

[4] 朱建明, 王秦. 基于博弈论的网络空间安全问题分析[J]. 通信学报, 2017, 32(10): 43-49.
ZHU J M, WANG Q. Analysis of cyberspace security based on game theory[J]. Journal on Communications, 2017, 32(10): 43-49.

[5] WHITE J, PARK J S, KAMHOUA C A, et al. Game theoretic attack analysis in online social network (OSN) services[C]//IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. 2013: 1012-1019.

[6] 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, 2015, 33(9): 1748-1764.
WANG Y Z, LIN C, CHENG X Q, et al. Analysis for network attack-defense based on stochastic game model[J]. Chinese Journal of Computers, 2015, 33(9): 1748-1764.

[7] 张恒巍, 余定坤, 韩继红, 等. 基于攻防信号博弈模型的防御策略选取方法[J]. 通信学报, 2016, 37(5): 51-61.
ZHANG H W, YU D K, HAN J H, et al. Defense policies selection method based on attack-defense signaling game model[J]. Journal on Communications, 2016, 37(5): 51-61.

[8] DAVID W K Y, LEON A P. Differential games theory[M]. New York: Springer Press, 2015.

[9] 张恒巍, 李涛. 基于攻防微分博弈的网络安全防御决策方法[J]. 电子学报, 2017,45(2): 431-439.
ZHANG H W, LI T. Defense strategy selection method based on attack-defense differential game model[J]. Acta Electronica Sinica, 2017,45(2): 431-439.

[10] NILIM A, GHAOUI L E. Active defense strategy selection based on differential game[J]. Operations Research, 2016, 43(12): 163-169.

[11] 范红旗, 王胜, 付强. 二人微分对策问题信息模式的数学描述[J]. 电子学报, 2015, 42(2): 1355-1361.
FAN H Q, WANG S, FU Q. Mathematical description for information pattern of stochastic differential games[J]. Acta Electronica Sinica, 2015, 42(2): 1355-1361.

[12] NOWAK M A. Evolutionary dynamics: exploring the equations of life[M]. Boston: Harvard University Press, 2015.

[13] ROESCH M. Snort-lightweight intrusion detection for networks[C]//The 13th System Administration Conference and Exhibition. 2015: 229-238.

[14] 余定坤, 王晋东, 张恒巍. 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, 2016, 43(1): 163-169.
YU D K, WANG J D, ZHANG H W. Active defense strategy selection based on static Bayesian game[J]. Journal of Xidian University, 2016, 43(1):163-169.

[15] 石乐义, 赵俊楠, 李芹, 等. 基于信令博弈的网络诱骗防御策略分析与仿真[J]. 系统仿真学报, 2016, 28(2):348-353.
SHI L Y, ZHAO J N, LI Q, et al. Signaling game analysis and simulation on network decoy defense strategies[J]. Chinese Journal of System Simulation, 2016, 28(2): 348-353.

[16] 林闯, 王元卓, 汪洋. 基于随机博弈模型的网络安全分析与评价[M]. 北京: 清华大学出版社, 2014.
LIN C, WANG Y Z, WANG Y. Analysis and evaluation for network security based on stochastic game model[M]. Beijing: Tsinghua University Press, 2014.

[17] LIU F M, DING Y S. Dynamics analysis of stochastic game based trust computing for networks[J]. Application Research of Computers, 2016, 33(2): 460-463.

[18] SUN W, KONG X W, HE D Q, et al. Research on attack and deference in information security based on stochastic game[J]. ACM Information security Science and technology, 2016, 27(9): 1408-1412.

[19] GORDON L, LOEB M, LUCYSHYN W, et al. 2016 CSI/FBI computer crime and security survey[C]//The 2016 Computer Security Institute. 2016: 48-66.

[作者简介]

黄世锐（1994−），男，广东汕头人，信息工程大学工程师，主要研究方向为网络安全预警与防御决策。

张恒巍（1978−），男，河南洛阳人，博士，信息工程大学副教授，主要研究方向为网络安全与攻防对抗、信息安全风险评估。

王晋东（1966−），男，山西洪桐人，信息工程大学教授，主要研究方向为网络与信息安全、云资源管理。

窦睿彧（1981−），女，江苏江都人，信息工程大学讲师，主要研究方向为网络信息安全。