网络空间拟态防御建模与量化评估技术研究

Modeling and Quantitative Evaluation of Cyberspace Mimic Defense

马海龙/MA Hailong，任权/REN Quan，伊鹏/YI Peng
（中国人民解放军战略支援部队信息工程大学，中国 郑州 450001）
(Information Engineering University, Zhengzhou 450001, China)

DOI：10.12142/ZTETJ.202206010
网络出版地址：https://kns.cnki.net/kcms/detail//34.1228.TN.20221221.1450.005.html
网络出版日期：2022-12-23
收稿日期：2022-10-17

摘要：针对网络空间未知漏洞后门等不确定性扰动问题，拟态防御技术基于动态异构冗余架构与拟态伪装机制实现了对随机或非随机扰动的有效管控。针对上述内生安全问题，首先采用Petri网、鞅以及概率论等理论与技术来评估与仿真系统的安全性，并对评估结果与实际部署进行了策略分析，同时对比了不同理论工具在量化可用性、攻击成功概率以及逃逸概率等指标时存在的优缺点。最后，针对现有理论与技术在不同场景适用性存在的不足以及实际部署量化问题，展望了后续拟态防御系统在定性与定量分析研究的主要方向。

关键词：网络空间内生安全；拟态构造；建模方法；评估

Abstract: For uncertain disturbances such as unknown vulnerabilities and backdoors in cyberspace, the mimic defense technology realizes effective control of random or non-random disturbances based on dynamic heterogeneous redundancy architecture and mimicry camouflage mechanism. For the above endogenous security problems, the Petri nets, martingales, probability theory, and other theories and technologies are used to evaluate and simulate the security of the system, and the evaluation results and actual deployment strategies are analyzed. At the same time, the advantages and disadvantages of different theoretical tools are compared in quantifying availability, attack success probability, escape probability, and other indicators. Finally, in view of the shortcomings of the applicability of the existing theories and technologies in different scenarios and the quantitative problems of the practical deployment, the main direction of the subsequent mimicry defense system in qualitative and quantitative analysis is discussed.

Keywords: cyberspace endogenous security; mimic structure; modeling methods; evaluation

随着信息化和工业化的高度融合，各类信息安全事件层出不穷，网络空间安全问题成为信息时代日益严峻的挑战[1]。为了应对各类网络安全事件，传统的网络防御是在系统上，通过防火墙、恶意检测等附加式防御手段来提高系统的抗攻击能力。尽管上述防护技术能在一定程度上减少网络攻击造成的危害，但逐年递增的网络安全事件却表明现有网络安全防御架构难以应对基于未知的漏洞后门发动的未知攻击，总体表现为：工程技术手段的局限性，任何软硬件厂家都无法确保网络设备中不存在任何设计缺陷；在全球开放式产业链条件下，任何厂商都不能确保生产链等环节未被蓄意植入后门；开源模式已经成为技术开发的主流趋势，现有的科技理论和方法尚不能彻查系统中的漏洞与后门；修补式的被动网络防御策略难以应对日新月异的网络攻击方法[2]。

为改变网络空间攻防不对称性的格局，提高网络系统应对攻击的能力，网络空间拟态防御[3]被提议作为网络安全“改变游戏规则”的研究主题之一。拟态防御技术是通过动态异构冗余构造与拟态伪装机制来规避网络空间广义不确定性扰动问题。2008年，邬江兴教授受生物界拟态现象启发，提出了“结构决定效能”的拟态计算，又从“结构决定功能与安全”思路入手，将动态异构冗余架构与广义鲁棒控制机制融合，创立拟态防御理论体系，逐步开辟了网络空间拟态防御（CMD）研究方向，期望通过架构设计赋予信息系统内生安全能力。内生安全是指借助系统本身的构造、机制、运行场景以及规律等内部属性，达成的安全功能或属性。拟态防御是基于功能等价的多个执行单元，以提供目标环境的动态性、非确定性、异构性、非持续性为目的，动态地构建网络、平台、环境、软件、数据等多样化的拟态环境。拟态防御基于动态异构冗余架构与拟态伪装机制实现了将随机或

基金项目：国家自然科学基金资助项目（61872382）

非随机扰动转化为概率可控的可靠性事件。

因此，本文将对网络空间拟态防御理论与技术发展展开研究，主要贡献包括：（1）对网络空间内生安全问题进行阐述，针对该问题探讨了现有防御架构存在的问题；（2）介绍拟态防御系统的基本要素与关键技术；（3）给出了现有拟态防御理论的系统建模方法，对比分析了不同模型的适用场景；（4）对拟态防御理论方向研究进行展望。

1 问题提出与解决

1.1 内生安全问题

“矛盾存在于一切事物之中，矛盾双方在一定条件下可以转化”。在信息网络空间中，如果一个软硬件实体的暗功能和副作用能被某种因素触发而影响到实体服务功能的可信性，这些副作用和暗功能则被称为“内生安全”问题[3]，即系统内部本征功能的内在性矛盾。以典型技术为例，大数据技术能够根据算法和数据样本发现未知的规律或特征，而被人为污染的数据样本以及恶意利用的算法缺陷同样可使人误解，结果的不可解释性是其内生安全问题。区块链技术采用了大于等于51%的共识机制，该机制却不能避免市场占有率大于51%的商用级产品中的漏洞后门问题。这是区块链1.0时代的内生安全问题。当前，计算技术的快速发展使人类步入了辉煌的信息时代，但计算技术本身的缺陷也使得网络空间充满了不确定性。因此，本文所提的内生安全问题主要是指网络空间各类信息服务功能实体中存在的未知漏洞后门等问题。显然，该类问题是系统内部本征功能所衍生出的副作用或暗功能，是伴随本征功能产生和发展的，因此无法从根本上彻查或者消除。

1.2 解决思路

从哲学原理上说，内生安全问题不可能彻底消除，只能在时空约束前提下实现条件规避或危害控制。传统的网络安全思维模式和技术路线主要采取挖漏洞、打补丁、查毒杀马或是设蜜罐、布沙箱等堆叠的附加式防护手段。该方式在引入安全功能的同时会不可避免地引入新的内生安全问题。内生安全问题源自系统结构本身，那么在功能等价条件下变换系统结构本身无疑能成为内生安全问题的解决之道。

2 拟态防御架构

动态异构冗余（DHR）架构以非相似余度架构为基础，融合了多模表决与策略裁决、负反馈控制策略、多维动态重构机制三大核心机理，实现了将广义不确定扰动管控在有效范围之内，从而确保DHR架构相对攻击方具有“熵不减”的广义鲁棒控制能力。

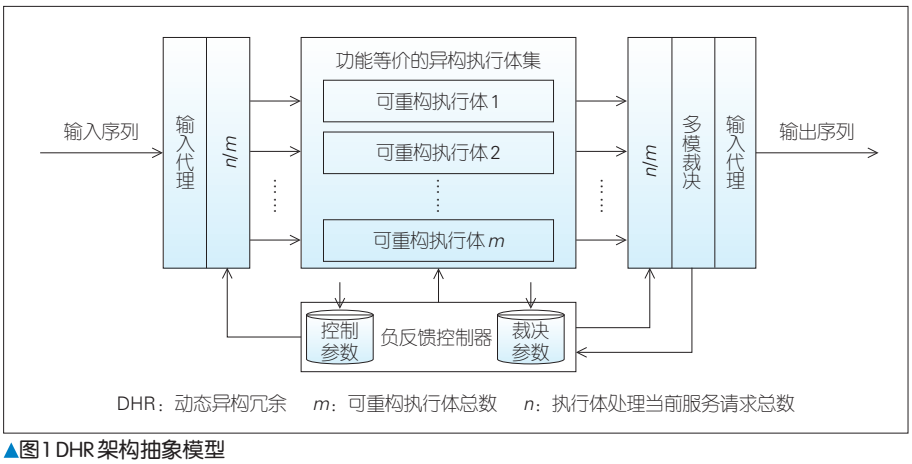
DHR架构抽象模型如图1所示，主要包括输入输出代理、功能等价的可重构执行体集、输出裁决模块以及负反馈控制器。输入代理模块负责接收负反馈控制器的指令，并将输入请求复制、分发到多个功能等价的可重构异构体；功能等价异构执行体集合中的可重构执行体能独立完成指定功能属大概率事件；输出裁决模块策略选取合适算法判决输出矢量，并将满足要求的输出响应转发给输出代理，若裁决结果不一致或未达要求则激活负反馈控制器；负反馈控制器通常会依据自身策略主动激活或受裁决结果被动激活，反馈控制器被激活后会依据控制参数和裁决参数执行功能等价的重组/重构/重配等操作。

3 拟态防御理论系统建模

拟态防御基于DHR架构与拟态伪装机制，将攻击造成的随机或非随机扰动转化为概率可控的可靠性事件，这使得定量分析架构的抗攻击能力成为可能。本节中，针对现有系统可用概率、攻击成功概率等通用指标，以及拟态构造特有逃逸概率指标，我们探讨拟态防御模型的抗攻击性。抗攻击性是系统在受到外部攻击出现不可见故障时，连续提供有效服务并在规定时间内恢复所有服务的能力。关于抗攻击性模型的假设与定义如下：

假设1：目标系统是3余度DHR系统，执行体中不包括入侵检测、防火墙等特异性感知和防御手段；

假设2：通过拟态裁决机制可以发现输出矢量与多数执



▲图1 DHR架构抽象模型

行体不同的情况，并能够对其进行包括动态重构等在内的恢复操作；

假设3：对于拟态裁决机制未能发现的错误，系统仍然能以一定的概率进行定期或不定期恢复。

定义1：可用概率。系统处于正常服务状态的概率。在3余度拟态防御系统中，可用概率是指系统全部执行体处于漏洞休眠状态或单个执行体处于故障状态的概率。

定义2：逃逸概率。攻击方通过协同多个执行体使输出结果出现一致错误，从而实现判决逃逸。

定义3：攻击成功概率。攻击成功执行的概率，如系统组件（或防御者）被破坏导致出错或目标被攻击者成功访问的概率。

下面我们主要针对集中式与分布式裁决场景、随机与非随机攻击场景对3个模型进行阐述。

3.1 基于广义随机Petri网的拟态构造评估模型

19世纪60年代，德国学者C. A. PETRI提出了Petri网的概念。Petri网适用于在逻辑层次上对事件离散的动态系统进行建模和分析。Petri网可用来描述系统中进程或部件的顺序、并发、冲突以及同步等关系。为了准确地描述整个拟态防御系统的结构、不同攻击扰动与拟态系统动态重构与负反馈控制防御特性，文献[4]和[5]以3余度动态异构冗余系统为例，依据拟态系统针对不同扰动表现出不同的行为，建立包括24个状态、42个变迁的广义随机Petri网（GSPN）模型（具体如图2所示）。

拟态构造扰动异常情况下的GSPN模型：

$$GSPN=(S,T,F,K,W,M_0,\Lambda), \tag{1}$$

其中，库所$S=\{P_1,P_2,\cdots,P_{24}\}$表示系统中状态元素的集合，变迁$T=\{T_1,T_2,\cdots,T_{42}\}$表示系统中状态迁移集合，$F$为模型中库所与变迁之间的有向弧集合，$W$是弧的权重集合，各弧的权重为1，$K=\{1,1,1,0,\cdots,0\}$定义了$S$中各元素的容量，状态标识$M=\{M_0,M_1,\cdots,M_{12}\}$。其中$M_0=\{1,1,1,0,\cdots,0\}$定义了模型的初始状态，$\Lambda=\{\lambda_1,\lambda_2,\cdots,\lambda_{15}\}$定义了与时间变迁相关联的平均实施速率集合。

设i，j表示马尔科夫链中任意实存状态，$i,j\in M_T$，r,s表示马尔科夫链中任意消失状态，$r,s\in M_v$。系统实存状态之间的转移概率矩阵为：

$$u_{ij}=f_{ij}+\sum_{r\in M_v}P_r\{r\to j\}, \tag{2}$$

其中，f_{ij}表示实存状态间的转移概率，$P_r\{r\to j\}$表示沿着一条全部由消失状态构成的中间状态的路径，从消失状态r转移到实存状态j的概率。其中，路径可以包括任意步数。

由马尔可夫链的转移概率建立转移速率矩阵如下：

$$q_{ij}=\begin{cases}\lim\limits_{\Delta t\to 0}\dfrac{u_{ij}(\Delta t)}{\Delta t}, i\neq j\\ \lim\limits_{\Delta t\to 0}\dfrac{u_{ij}(\Delta t)-1}{\Delta t}, i=j\end{cases}, \tag{3}$$

q_{ij}为由实存状态M_i到实存状态M_j的转移速率，其中$i,j\in[1,l],l=M_T$。Q矩阵是以q_{ij}为元素的转移速率矩阵。概率向量$P(t)=(P_1(t),P_2(t),\cdots,P_i(t),\cdots,P_l(t))$，其中$P_i(t)$为系统处于实存状态$M_i$的瞬时概率，则有微分方程（4）成立：

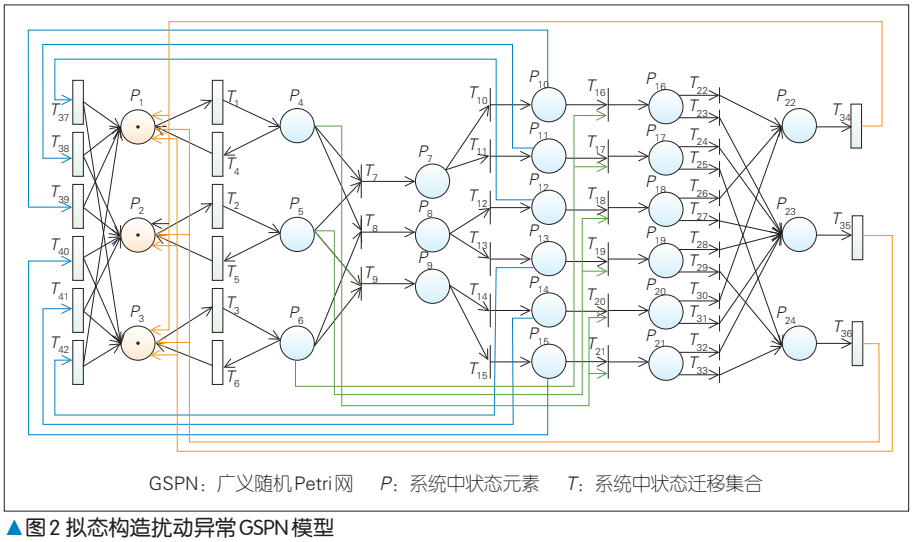
$$\begin{cases}P'(t)=P(t)Q\\ P(0)=(P_1(0),P_2(0),\cdots,P_l(0))。\end{cases} \tag{4}$$

通过上述方程组可求解可达标识的可用概率和逃逸概率。

文献[4]给出了各种防御策略所对应的安全性指标，因此可针对不同安全需求采用不同策略部署与系统构建来实现。

3.2 融合鞅与GSPN的二维拟态构造评估模型

拟态防御系统在联合判决和重配置过程中带来的资源消耗将大幅增加防御成本。存在判决时延的分布式拟态系统亟



▲图2 拟态构造扰动异常GSPN模型

需一种分析系统安全性的方法。文献[6]在单节点攻击层，根据博弈论思想对攻击者和防御者的行为分别建立模型，利用广义随机PN描述攻防动作对系统的影响，进而分析系统的安全性。在链路攻击层，使用马尔科夫链来刻画攻击者在链路中的位置变化，并结合随机过程的鞅理论，计算出攻击难度和网络配置间的量化关系。

假定攻击单个节点成功的概率为μ，攻击链的节点总数为Θ，节点被随机扰动的概率为ω。假设当前时刻攻击者停留在第k个节点，即已攻击成功k个节点，则攻击转移如图3。

定理1：构建一个随机序列$M_0,M_1,M_2,\cdots,M_n$，其中，$M_i=X_i-[(1-\omega)\mu-\omega]*i$，则$M_n$序列是关于$X_0,X_1,X_2,\cdots,X_n$的鞅。

为了求解攻击Θ步到达目标节点的步数，我们引入了鞅停时定理。在随机过程中，停时被定义为具有某种与将来无关性质的随机时刻。鞅停时满足：

（1）$P\{S<\infty\}=1$；

（2）$E[|M_S|]<\infty$；

（3）$\lim\limits_{n\to\infty}E[|M_S|I_{\{S>n\}}]=0$。

则有：

$$E[M_S]=E[M_0]。\tag{5}$$

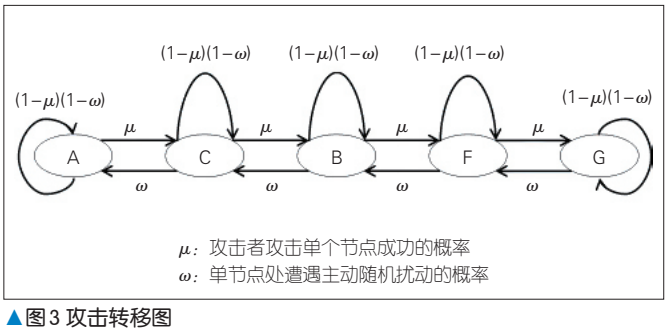
定理2：对于一条长度为Θ个节点的攻击链，如果攻击者攻击单个节点成功的概率为μ，单节点处遭遇主动随机扰动的概率为ω，那么攻击者成功攻击目标节点（即Θ点）需要的步数期望为：

$$E[S]=\frac{\theta}{(1-\omega)\mu-\omega}。\tag{6}$$

下面我们计算到达Θ点的步数期望。根据停时定理得：$E[M_S]=E[M_0]=E[X_0]=0$，

$$E[M_S]=E[X_S-[(1-\omega)\mu-\omega]S]=E[X_S]-[(1-\omega)\mu-\omega]E[S]。\tag{7}$$

又因为$E[X_S]=\Theta$，所以等式（6）成立。



▲图3 攻击转移图

根据上文，运算得到的攻击逃逸的稳态概率即为下一部分马尔科夫链的下行概率，攻击成功概率即为马尔科夫链的上行概率，即：$\mu=P(P_E)$，$\omega=\lambda(T_{E0})$。

该模型给出了二维拟态构造评估模型，在实际部署过程中可以通过改善动态清洗与重构能力来增大修复速率，通过改善节点品质等因素来改变单个节点的攻击成功概率[7-10]。

3.3 基于概率论与数理统计的拟态构造评估模型

针对系统的未知安全防范，大多数安全评估模型首先基于随机性攻击假设，进而基于攻击路径和漏洞分析方法来量化攻击难度。尽管这类攻击模型能有效反映攻防双方在随机条件下的博弈策略，但缺乏针对系统整体安全的有效性证明，即从理论上论证在一定的攻击条件，存在一种防御方案可保证任意小的系统差错概率。

文献[7]给出了一种证明方法，针对非随机扰动且执行体有记忆情况，DHR架构引入了反馈函数$f(t)$，在部署差模异构执行体（即在共模同构率ω可忽略）后，拟态构造执行体出错概率：

$$\forall t>0,P_e^i(t)\in[0,\max\{\frac{\lambda_{i+1}}{\lambda_{i+1}+\mu_{i+1}}(1-e^{-(\lambda_{i+1}+\mu_{i+1})T'_{i+1}}),e^{-\mu_{i+1}T'_{i+1}}\}]<1。\tag{8}$$

由此可见，执行体出错概率值随时间递增并处于与时刻T_{i+1}相关的确定范围（T_{i+1}在非随机扰动条件下为确定值），即执行体在DHR架构中出错概率$P_e^i(t)$随时间变化不趋于1。当引入反馈可控消记忆动作$f(t)$后，DHR构造信道容量C将处于防御方可控范围$[C_s,C_0]$。若非随机扰动到达与动态反馈修复时间服从负指数分布，那么整个DHR构造信道有可控的稳态分布。DHR构造信道稳态信道容量为C_s，初始信道容量为C_0，执行体i稳态信道容量记作C_s^i。

我们设DHR构造信道在t时刻的输入请求为$\boldsymbol{x}(t)$，$\boldsymbol{x}(t)\in X^n$，$\boldsymbol{x}(t)=(x_1(t),x_2(t),\cdots,x_n(t))$，输出响应为$\boldsymbol{y}(\boldsymbol{x}(t))\in Y^n$，$\boldsymbol{y}(\boldsymbol{x}(t))=(y_1(x_1(t)),y_2(x_2(t)),\cdots,y_n(x_n(t)))$。从编码空间$X^n$中随机选取$M=2^{nR(t)}$个编码序列作为请求发送，设$X$中所有元素以独立、等概率形式出现，那么就可以满足随机编码条件。给定与时刻t对应的输出响应$\boldsymbol{y}(\boldsymbol{x}(t))$，若存在唯一的$k\in[1,2^{nR(t)}]$，则有：

$$(\boldsymbol{x}_k(t),\boldsymbol{y}(\boldsymbol{x}(t)))\in T_{XY}(n,\varepsilon)。\tag{9}$$

$\boldsymbol{y}(\boldsymbol{x}(t))$判决为$\boldsymbol{x}_k(t)$，即$F(\boldsymbol{y}(\boldsymbol{x}(t)))=\boldsymbol{x}_k(t)$。其中，$T_{XY}(n,\varepsilon)$表示输入输出序列对$(\boldsymbol{x}(t),\boldsymbol{y}(\boldsymbol{x}(t)))$是联合$\varepsilon$典型序列。

若发送请求为$\boldsymbol{x}_m(t)$，响应序列为$\boldsymbol{y}(\boldsymbol{x}_m(t))$，则判决出错概率为：

$$P_{em}=P(\boldsymbol{x}_k(t)\neq\boldsymbol{x}_m(t)|\boldsymbol{y}(\boldsymbol{x}_m(t)))。\tag{10}$$

我们设发送端的第一个请求消息为$\boldsymbol{x}_1(t)$，令事件：

$$E_m(t)=\{(\boldsymbol{x}_m(t),\boldsymbol{y}(\boldsymbol{x}_m(t)))\in T_{XY}(n,\varepsilon)\},m\in[1,2^{nR(t)}]。\tag{11}$$

于是，判决出错可分为两种情况：

（1）发送编码序列$\boldsymbol{x}_1(t)$与响应序列$\boldsymbol{y}(\boldsymbol{x}_1(t))$不构成联合$\varepsilon$典型序列，令事件为$E_1^C(t)$；

（2）编码序列$\boldsymbol{x}_k(t),k\neq1$与响应序列$\boldsymbol{y}(\boldsymbol{x}_1(t))$构成联合$\varepsilon$典型序列，令事件为$E_k(t)$。

于是则有攻击成功概率：

$$P_e(t)=P(E_1^C(t)\cup E_2(t)\cdots\cup E_M(t))\leqslant P(E_1^C(t))+\sum_{k=2}^{M}P(E_k(t))。\tag{12}$$

第1部分攻击成功概率：

$$P(E_1^C(t))=1-P(E_1(t))\leqslant\varepsilon。\tag{13}$$

第2部分攻击成功概率：

$$\sum_{k\neq1}P(E_k(t))\leqslant2^{n[R(t)-C(t)+3\varepsilon]}。\tag{14}$$

我们取t时刻的DHR构造信道容量$C(t)=\min\{C_s^1,C_s^2,\cdots C_s^n\}$，于是：

$$\forall\eta=3\varepsilon>0,R(t)<C(t)-\eta,n\to\infty,\tag{15}$$

那么：

$$\sum_{k\neq1}P(E_k(t))\to0,$$

$$P_e(t)\leqslant\varepsilon,\tag{16}$$

即攻击成功概率$P_e(t)$为任意小。

该模型给出了内生安全构造具有任意小安全需求的存在性证明。在实际部署过程中，我们可通过编码与冗余度设计、执行体扰动消除以及反馈控制构造等来尽可能地接近该模型求解结果。

3.4 评估指标分析

表1比较了上述3个模型的优缺点。当前，拟态防御理论模型主要针对集中式与分布式裁决、扰动随机与非随机场景进行量化评估。GSPN模型在面向集中判决场景时能通过多个量化指标可以有效评估系统的抗攻击能力。然而，在面向分布式场景时，该模型需要进一步完善。文献[7]所提的模型则是通过优化资源与构造来仿真系统攻击可用性，该方法同样在一定余度与随机性攻击扰动条件下进行的。针对分布式裁决系统，文献[8]建立了融合鞅与GSPN的系统安全评估方法，该方法对裁决延时判决问题进行了进一步研究。针对基于拟态防御的云科学计算流，文献[9]提出了一种攻击评估模型。上述的可用性与攻击成功概率指标模型相关研究存在两方面不足：一方面，GSPN模型在执行体数量增多时会出现指数爆炸问题；另一方面，上述模型均是在攻击随机到达的情况下分析的系统安全性。在逃逸概率指标方面，文献[4]在GSPN模型的基础上提出用大系统拆分成小系统的方案来解决状态爆炸问题，从而实现逃逸概率的一般性求解。针对攻击非随机到达展开建模，文献[10]量化分析了拟态构造将非随机攻击转化为随机可靠性事件，从而借助概率论与数理统计方法对余度足够大的情况进行探讨，实现了对拟态构造安全的有效性论证。该论证过程主要以攻击成功概率指标进行推理，简化了攻防细节。由于文献[4]和[10]对攻击扰动与防御动作特性进行了整合与抽象，简化了量化指标。

因此，上述模型均能有效量化评估系统抗攻击能力，所

▼表1 现有拟态防御理论量化评估模型的优缺点

指标	优点	缺点
可用性	基于GSPN模型，文献[5]和[7]准确地描述拟态防御系统结构、不同攻击扰动与负反馈控制防御特性，量化分析攻击可用性和感知安全性；文献[8]提出一种感知调度算法与失效概率最小化模型来保证系统可用性最大化。	仅考虑扰动随机表现形式，均未分析非随机扰动情况；GSPN在多余度架构下状态复杂，抗攻击性评估也将异常复杂；失效概率最小化模型则是在一定余度下进行仿真分析，未考虑一般性。
攻击成功概率	针对存在判决时延的分布式拟态系统，文献[6]提出一种基于鞅与GSPN的系统安全评估方法，量化分析攻击扰动概率和逃逸概率。针对拟态构造的云科学计算流；文献[9]提出了一种攻击评估模型，能有效反应攻击次数与攻击成功率的关系。	仅考虑了扰动随机表现形式，且现有模型对多余度系统架构下的抗攻击性分析同样难以适用。
逃逸概率	针对大余度拟态防御系统提出了组合模型，文献[4]可将大规模复杂系统拆分成多个子系统，再对整个系统采用GSPN理论进行一般性求解；文献[10]基于概率论与数理统计方法，论证了系统整体的安全性，该论证具有一般性，适用多余度与非随机攻击场景。	通过组合子系统GSPN模型来建立系统整体模型，可以实现逃逸概率分析，但难以覆盖任意余度，因此具有一定局限性；概率与数理统计模型则是针对攻防动作特性进行整合与抽象，对安全防御有效性进行一般论证，简化了量化指标。

GSPN：广义随机Petri网

提数学模型在解决各自场景问题时均表现出一定的优越性。同时，现有的模型在应对不同拟态场景时仍有待进一步优化，如GSPN模型在面临大余度分布式网络场景[11]时如何量化分析，针对不同场景的非随机攻击评估量化指标如何选取等。此外，现有模型在针对异构性[12]量化评估方面仍存在不足，有待进一步研究。因此，后续拟态防御理论的发展将会进一步面向系统异构性与共模扰动的量化、面向系统裁决与异构归一化的量化、面向负反馈控制的动态重构与清洗策略制定等方面，从而有效解决拟态防御理论与实际部署结合存在的难题[12]。

4 结束语

作为未知漏洞后门等不确定性威胁的解决方案，网络空间拟态防御得到广泛应用。文章中，我们研究了网络空间拟态防御理论模型，阐述了网络空间内生安全以及现有防御架构所存在的问题，并指出了拟态防御系统的基本要素与关键技术。同时，我们对3种典型的建模方法进行了比较分析。随着拟态防御技术与各类技术的融合，拟态防御理论存在的挑战也逐步彰显，如拟态防御理论在攻防对抗定性分析方面有待完善；在网络通信理论方面如何研究基于概率论与数理统计的拟态构造安全可控性；对拟态构造的防御极限进行量化评估；如何研究拟态构造执行体的信息并行处理方式，构造高容量的执行体，减少裁决时延，实现高效的处理能力等。在网络计算理论方面，如何研究网络信息处理过程中存储、计算与控制单元存在的内生安全问题，并从整体上量化分析网络计算的安全可控性。因此，拟态防御的发展仍需大力推进理论与技术创新。

参考文献

[1] CONTEH N Y, SCHMICK P J. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks [J]. International journal of advanced computer research, 2016, 6(23): 31–38. DOI: 10.19101/ijacr.2016.623006

[2] JAJODIA S, GHOSH A K, SWARUP V, et al. Moving target defense [M]. Springer, New York, 2012

[3] 邬江兴. 网络空间拟态防御研究 [J]. 信息安全学报, 2016, 1(4): 1–10. DOI: 10.19363/j.cnki.cn10–1380/tn.2016.04.001

[4] 任权, 邬江兴, 贺磊. 基于GSPN的拟态DNS构造策略研究 [J]. 信息安全学报, 2019, 4(2): 37–52. DOI: 10.19363/J.cnki.cn10–1380/tn.2019.03.05

[5] REN Q, WU J X, HE L. Performance modeling based on GSPN for cyberspace mimic DNS [J]. Chinese journal of electronics, 2020, 29(4): 738–749. DOI: 10.1049/cje.2020.05.001

[6] 杨昕, 李挥, 邬江兴, 等. 融合广义随机Petri网的二维拟态安全评估模型 [J]. 中国科学: 信息科学, 2020, 50(12): 1944–1960

[7] REN Q, HU T, WU J, et al. Multipath resilient routing for endogenous secure software defined networks [J]. Computer networks, 2021, 194(2): 108134

[8] QI C, WU J X, CHENG G Z, et al. An aware–scheduling security architecture with priority–equal multi–controller for SDN [J]. China communications, 2017, 14(9): 144–154. DOI: 10.1109/CC.2017.8068772

[9] WANG Y W, WU J X, GUO Y F, et al. Scientific workflow execution system based on mimic defense in the cloud environment [J]. Frontiers of information technology & electronic engineering, 2018, 19(12): 1522–1536. DOI: 10.1631/FITEE.1800621

[10] 邬江兴. 网络空间内生安全: 拟态防御与广义鲁棒控制(下册) [M]. 北京: 科学出版社, 2020

[11] REN Q, GUO Z H, WU J X, et al. SDN–ESRC: a secure and resilient control plane for software–defined networks [J]. IEEE transactions on network and service management, 2022, 19(3): 2366–2381. DOI: 10.1109/TNSM.2022.3163198

[12] TONG Q, GUO Y F. A comprehensive evaluation of diversity systems based on mimic defense [J]. Science China information sciences, 2021, 64 (12): 1–2. DOI: 10.1007/s11432–020–3008–1

作 者 简 介

马海龙，中国人民解放军战略支援部队信息工程大学副研究员；主要研究领域为网络空间内生安全与智能威胁感知；先后主持和参加国家重点研发计划和自然基金项目10余项，获得6项科技进步奖；已发表论文40余篇，出版专著2部，授权专利10项。

任权，中国人民解放军战略支援部队信息工程大学助理研究员；主要研究领域为软件定义网络与网络内生安全架构。

伊鹏，中国人民解放军战略支援部队信息工程大学研究员；主要研究领域为网络空间内生安全与多模态网络。