

基于离散马尔可夫链的不同抗干扰系统模型分析

任权, 贺磊, 邬江兴

(国家数字系统工程技术研究中心, 河南 郑州 450001)

摘要: 区块链、非相似冗余以及拟态防御技术已在网络空间不同安全领域得到迅速发展, 然而, 目前针对这3类创新型技术缺乏有效的模型进行统一描述和分析。采用离散时间马尔可夫链模型进行建模, 并对3类系统抵抗攻击或干扰时的性能进行分析, 结果表明, 拟态防御系统采用动态异构冗余架构与负反馈控制机制能保证系统的高可用性。区块链系统利用高冗余共识机制在一定时间内具有优于拟态防御系统和非相似冗余系统的抗干扰性能, 但随后性能会快速衰减。非相似冗余系统性能随着冗余度的增加会快速趋于高冗余度区块链, 系统的抗干扰性能衰减相对缓慢。

关键词: 网络安全; 区块链; 非相似冗余; 拟态防御; 离散时间马尔可夫链; 抗干扰性

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018035

Analysis of different anti-interference system models based on discrete time Markov chain

REN Quan, HE Lei, WU Jiangxing

National Digital Switching System Engineering & Technological R&D Center, Zhengzhou 450001, China

Abstract: Block chain, dissimilar redundancy and mimic defense technology have developed rapidly in different security fields of cyberspace. However, there is a lack of effective models to describe and analyze these three kinds of innovative technologies currently. The DTMC (discrete time Markov chain) was used to model and analyze the anti-interference of the three kinds of systems. The results show that mimic defense system which adopts dynamic heterogeneous redundancy architecture and negative feedback control mechanism can ensure the high availability of the system. The block chain system uses high redundancy consensus mechanism to have a higher anti-interference performance than mimic defense system and dissimilar redundancy system in a certain time, but its performance will decrease quickly after that. With the increase of redundancy, the anti-interference performance of the dissimilar redundancy system will tend to the high redundancy block chain rapidly. Compared with block chain, the anti-interference performance falling of dissimilar redundancy system will be relatively slower.

Key words: cyberspace security, block chain, dissimilar redundancy, mimic defense, DTMC, anti-interference performance

收稿日期: 2018-02-26; 修回日期: 2018-03-28

通信作者: 任权, 13218013361@163.com

基金项目: 国家网络安全专项基金资助项目 (No.2017YFB0803201); 国家高技术研究发展计划 (“863” 计划) 基金资助项目 (No.2015AA016102); 国家自然科学基金群体创新资助项目 (No.61521003)

Foundation Items: The National Specific Issues of Cyberspace Security (No.2017YFB0803201), The National Hi-Tech Research and Development (863 Program) (No.2015AA016102), The Innovative Research Groups of the National Natural Science Foundation of China (No.61521003)

1 引言

随着信息化和工业化的深层次融合，网络技术被广泛运用于金融、航空航天、电子交通运输等核心基础设施。然而，各类信息安全事件层出不穷，网络空间安全已成为信息时代最严峻的挑战之一。目前，网络空间架构具有典型的静态性、确定性和相似性，如 Windows 操作系统、谷歌搜索引擎以及思科路由器占据着市场大部分份额，一旦攻击方成功控制系统，将可持续对整个网络空间造成破坏性的影响^[1,2]。此外，漏洞的不可避免性使攻击方处于不对称优势地位，而防守方总处于被动。为增强网络空间的防御能力，动态化、多样化、冗余化技术被广泛运用。区块链技术、非相似冗余度技术以及拟态防御技术依据不同场景的需求被用来提高网络可靠性和安全性。区块链系统（BCS, block chain system）采用强大的非对称加密算法链接交易块以使记录可回溯且不可篡改，区块链的共识机制则借助分布式系统各节点的共识算法来构建防篡改网络环境，抵抗不确定性干扰^[3]。非相似冗余度系统（DRS, dissimilar redundancy system）采用冗余度异构容错技术和多模表决机制有效抑制共态故障，将不确定的随机故障转化为概率可控的事件，相比单冗余度系统大大提高了系统的可靠性^[4]。网络空间拟态防御系统（CMDS, cyberspace mimic defense system）融合了动态多维重构和负反馈控制特性，利用动态异构冗余架构和多模裁决机制将网络空间不确定的和确定性的攻击或干扰转化为概率可控的可靠性事件^[5]。因此，如何结合动态化、异构化、高冗余和共识特性建立 3 大系统的统一数学模型以及分析系统的可用性成为本文的研究重点。

在传统的可靠性模型分析中，主要采用可靠性框图和故障树法描述系统的结构和组成^[6,7]，Jin 等^[8]基于可靠性框图法对仪表系统建模，并分析了系统的可靠性和可用性。Hurdle 等^[9]扩展了传统使用故障树进行故障检测和识别的能力，通过减少故障发生时恢复系统工作状态所需的时间以适应动态变化系统的应用。然而，基于故障树和可靠性框图模型只能描述系统元素失效的逻辑组合（如处理器、软件、硬件等），无法反映系统

的动态特性以及构件之间的相互作用。Ranjbar 等^[10]采用马尔可夫动态模型来描述基于正常和失败 2 个假设状态和行为之间的关系。Shi 等^[11]利用广义随机 Petri 网对非相似冗余度系统进行了可靠性建模，并结合同构的连续时间马尔可夫链分析了系统的性能以及故障覆盖率和监测误报警率的影响。Cai 等^[12]提出了一个广义抽象的绩效评估模型，利用广义随机 Petri 网（GSPN）理论分析了移动目标防御系统的性能。尽管连续时间马尔可夫链和广义随机 Petri 网能更加细致地反映复杂系统可靠性的动态变化特性以及分析在部件失效情况下系统状态变化过程中的可靠性。但这 2 种方法对多状态复杂系统建模和求数值解比较困难。Yeon^[13]采用离散时间马尔可夫链方法，在给定道路的拥堵和畅通状态条件下，分析了状态转移概率变化情况和高速公路出行时间。为解决高冗余带来的状态空间爆炸问题，以及简化数值求解复杂问题，本文采用离散时间马尔可夫模型为 3 大系统建立统一数学模型，对 3 类系统的抗干扰性能进行分析。

2 3 类抗干扰系统架构描述

2.1 区块链系统

区块链是一个分布式共享账本数据库，其中每个数据块使用密码学相关联而产生，其本质是通过去中心化的方式维护一个可靠数据库的方案，即区块链中数据的验证、记账、存储、维护和传输等过程均基于分布式系统结构，采用数学方法而不是中心代理机构来建立节点之间的信任关系，如每笔交易的达成需通过系统大多数节点达成共识，从而形成去中心化的可信分布式系统^[14,15]。区块链网络拓扑如图 1 所示。

区块链的核心特征包括 3 个方面。一是去中心化。区块链系统由大量节点构成一个分布式对等网络，不存在中心化的管理机构，系统中所有节点均可参与数据的记录与验证，并将计算结果广播给其他节点，去中心化机制实现了部分节点异常情况下系统仍能正常运行。二是共识机制。在传统的互联网模式中，节点与节点之间通过第三方可信机构进行正常交易，而区块链则通过共识的数学算法在节点间建立可信的网络。这样

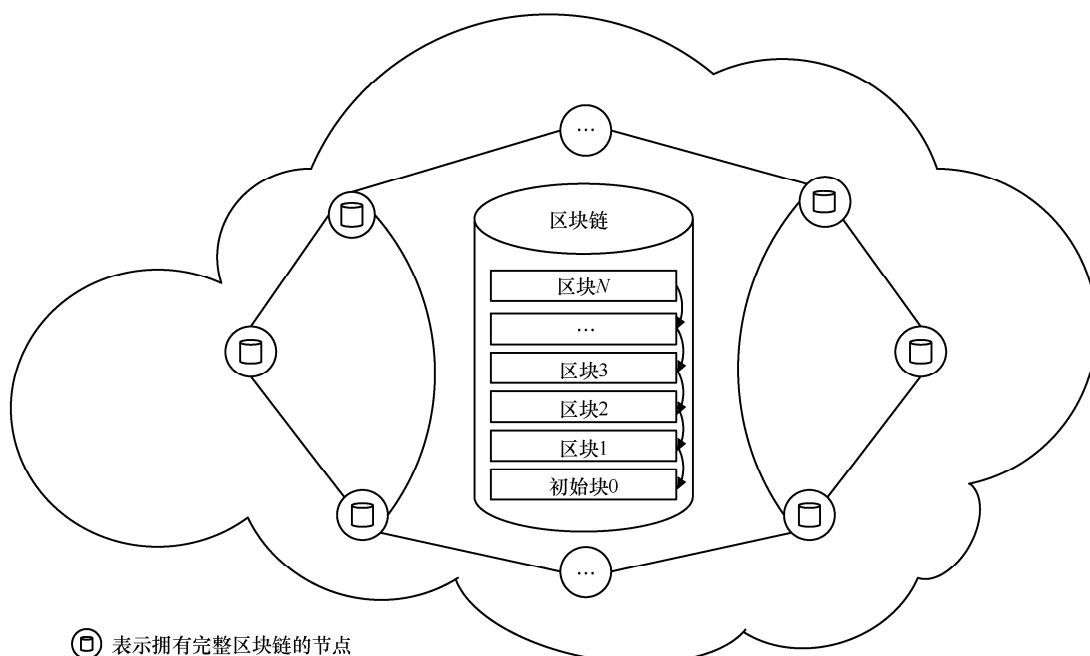


图1 区块链网络拓扑

参与方不必知道交易方是谁，更不需要借助第三方机构进行交易。三是数据不可篡改性。区块链技术采用非对称式密码学对数据进行加密处理，通过分布式系统中的共识算法来抵抗不确定性扰动，确保数据的不可篡改和伪造。原则上，要想篡改历史信息需同时控制大规模网络中超过 50% 的节点。

2.2 非相似余度系统

作为常用的容错方法之一，余度技术随着计算机系统对可靠性的迫切需求而产生并快速发展，其实质是利用“余度”思想来容忍故障的影响，提高系统的可靠性，即当计算机系统中一部分（或全部）部件出现故障时，可以由冗余的部件替代故障部分来保证系统在规定的时间内正常完成指定的工作。非相似余度系统架构如图2所示。

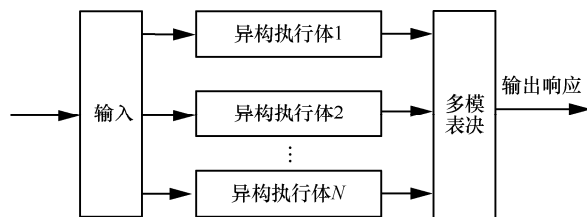


图2 非相似余度系统架构

为提高系统的可靠性和安全性，非相似余度技术被广泛运用于飞行控制系统、高铁行车系统、

核电站系统等，其目的是避免设计缺陷导致的共态故障，如系统、软硬件的规范错误，软硬件的设计和实现错误，通过采用不同版本的开发语言、开发工具，构建不同的运行环境来增大各个功能等价体之间的相异性。非相似余度系统利用余度之间交叉通道监控的方法来检测隔离这类同态故障，有效提高目标系统的可靠性^[16]。

2.3 网络空间拟态防御系统

拟态安全防御(MSD, mimic security defense)的基本思想是在各执行体功能等价条件下，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，以防御者可控的方式在多样化环境间实施主动跳变或快速迁移，对攻击者则表现为难以观察和预测的目标环境变化，从而大幅增加攻击难度和成本，大幅降低安全风险^[17]。拟态防御系统架构如图3所示。

拟态防御系统主要包括输入代理、可重构的异构执行体、负反馈控制器、拟态裁决机制等。多维动态重构意味着执行体可以在空间上形成串行、并行，或串并联组合的重构形态；在时间上，执行体可以是静态、动态、伪随机态；在策略上，可以考虑干扰环境、历史信息以及结构性能；在

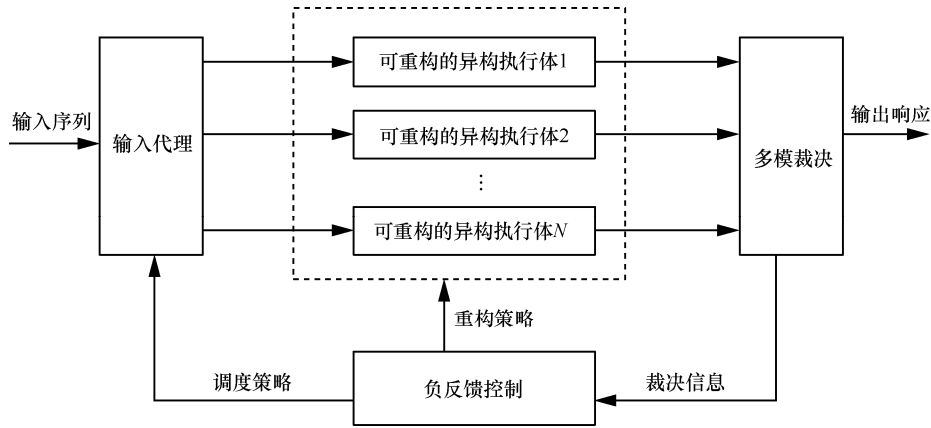


图3 拟态防御系统架构

生成方式上，可以是重构、重组和重定义。拟态防御系统利用执行体在时空维度上的异构性来打破静态、确定性和相似性的网络技术架构。因此，拟态系统可以容忍基于未知的漏洞和后门的外界扰动以及基于未知木马和病毒的渗透扰动，实现内外防护一体化。

3 离散马尔可夫模型分析

3.1 模型假设

假设1 为简化区块链、非相似余度和网络空间拟态防御系统模型建立时由大量节点数产生的状态复杂度，本文考虑输出矢量长度为1且离散时间段内未知攻击或扰动至多使一个执行体输出异常，清洗或重构至多使一个执行体恢复正常的情况。

假设2 针对区块链系统，系统每个节点分布式存在，在受到特定干扰时不可修复；针对非相似余度和网络空间拟态防御系统，执行体集中式存在，在受到特定干扰时DRS在多数执行体未同时出现异常时可重启修复，而CMDS在系统多数执行体异常后仍可通过动态重构进行修复。

假设3 针对3类抗干扰系统，传统的防御技术如入侵检测、防火墙和特定感知等不被应用，系统干扰平均到达时间为1 min，该系统可通过拟态裁决或共识机制感知输出不一致的执行体或节点。

3.2 定义

定义1 随机过程 $\{X_n, n \in T\}$ 为具有状态空间 I 的离散时间马尔可夫链（DTMC, discrete-time Markov Chain），其中， X_n 的离散状态集 $I = \{i_0, i_1, \dots, i_{n+1} \in T\}$ ， $T = \{0, 1, 2, \dots\}$ 是离散时间

集合，如果对任意 $n \geq 1$ 和 $i_0, i_1, \dots, i_{n+1} \in I$ 有

$$\begin{aligned} P\{X_{n+1} = i_{n+1} | X_0 = i_0, X_1 = i_1, \dots, X_n = i_n\} \\ = P\{X_{n+1} = i_{n+1} | X_n = i_n\} \end{aligned} \quad (1)$$

定义2 条件概率

$$p_{ij}^{(n)} = P\{X_{m+n} = j | X_m = i\}, i, j \in I, m \geq 0, n \geq 1 \quad (2)$$

$p_{ij}^{(n)}$ 为时间齐次的DTMC $\{X_n, n \in T\}$ 的 n 步转移概率，并称 $\mathbf{P}^{(n)} = p_{ij}^{(n)}$ 为 n 步转移矩阵。

定义3 稳态概率

$$\begin{aligned} \pi_i &= \lim_{n \rightarrow \infty} P\{X(n) = k | X(0) = i\} \\ &= \lim_{n \rightarrow \infty} P\{X(n) = k\} \end{aligned} \quad (3)$$

其中， $i=1, 2, \dots, m$ ，于是

$$\begin{cases} \pi_k = \sum_{i=1}^m \pi_i p_{ik} \\ \sum_{i=1}^m \pi_i = 1 \end{cases} \quad (4)$$

定理1 时间齐次的DTMC $\{X_n, n \in T\}$ 由转移概率矩阵 $\mathbf{P}$ 和初始概率分布 $A = (a_i)_{i \in I}$ 确定，即

$$\begin{aligned} P\{X_1 = i_1, \dots, X_{n-1} = i_{n-1}, X_n = i_n\} \\ = a_{i_1} p_{i_1 i_2} \cdots p_{i_{n-1} i_n} \end{aligned} \quad (5)$$

对于 n 步转移概率矩阵有

$$\mathbf{P}^{(n)} = \mathbf{P}^n \quad (6)$$

3.3 3类抗干扰系统建模

单个执行体存在状态转移概率 $s_{00}, s_{01}, s_{10}, s_{11}$ ，分别表示单个执行体在一段离散时间内由响应正常到响应正常，响应正常到响应异常，响应异常恢复到响应正常，响应异常保持响应异常。当系统存

在 n 个执行体时, 系统整体的状态转移矩阵为

$$\mathbf{S} = \mathbf{S}_1 \otimes \mathbf{S}_2 \otimes \cdots \otimes \mathbf{S}_k \otimes \cdots \otimes \mathbf{S}_n \quad (7)$$

这里 $\mathbf{S}_k$ 是执行体 k 的一步转移概率矩阵。因此, 系统整体的状态由单个执行体的状态共同决定。当系统一步转移时仅存在一个执行体出现异常或恢复正常, 可以得到系统整体的转移概率简化矩阵 $\mathbf{P}$, 有

$$\begin{cases} P_{kk-1} = s_{00}s_{10} \\ P_{kk} = s_{00}s_{11} + s_{01}s_{10}, 1 \leq k \leq n-1 \\ P_{kk+1} = s_{01}s_{11} \end{cases} \quad (8)$$

其中, $P_{00} = s_{00}$, $P_{nn} = s_{11}$, P_{kk} 代表系统从 k 个异常输出响应转移到 k 个异常输出响应的概率; $P_{k(k+1)}$ 代表系统从 k 个异常输出响应转移到 $k+1$ 个异常输出响应的概率; $P_{k(k-1)}$ 代表系统从 k 个异常输出响应恢复到 $k-1$ 个异常输出响应的概率。

于是系统的可用度为

$$p = a_0 \mathbf{PI} \quad (9)$$

其中, a_0 为初始可靠度, $\mathbf{I}=(1,1,\cdots,1,0,\cdots,0)$ 为 k 个执行体处于正常状态时的矢量 ($k=\frac{n}{2}+1$ 代表多数执行体正常, 正常执行体的矢量相关位取 1, 异常执行体的矢量相关位取 0)。于是根据式(6),

可以得到不同抗干扰系统的可用性随离散时间的变化情况。

以 $n=9\ 999$ 节点的区块链系统为例, 根据区块链系统分布式特性建立 DTMC 模型, 如图 4 所示。该模型共存在 10 000 个状态, 其中, 状态 k 表示存在 k 个同时异常的输出响应。对于区块链, 单个执行体受未知扰动后不可修。图 4 给出区块链系统离散时间马尔可夫链, 表 1 给出了单个执行体受扰动后状态转移概率设置。

对于非相似余度系统 (小余度静态异构冗余系统), 单个执行体在系统裁决正常条件下可修, 因此在执行体受干扰异常后的参数设置存在 2 种情况 (可修和不可修状态)。图 5 给出非相似余度系统离散时间马尔可夫链, 表 2 给出了单个执行体受扰动后状态转移概率设置。其中, 参数 $s_{10}()$ 括号外表示少数执行体异常后的状态转移概率值, $s_{11}()$ 括号内表示多数执行体异常后的状态转移概率值。

对于拟态系统 (小余度动态异构冗余系统), 执行体异常可修复。图 6 给出拟态防御系统离散时间马尔可夫链, 表 3 给出了单个执行体受扰动后状态转移概率设置。

4 3 大系统抗干扰性能对比分析

对不同冗余度的拟态系统、非相似余度系统

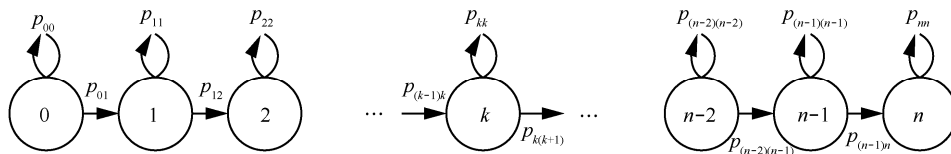


图4 区块链系统离散时间马尔可夫链模型

表1 区块链节点受未知扰动后状态转移概率设置

参数	值	含义
s_{00}	0.9	执行体受干扰后处于初始状态的概率
s_{01}	0.1	执行体受干扰后响应异常的概率
s_{10}	0	执行体受干扰异常后响应恢复正常的概率
s_{11}	1	执行体受干扰异常后响应保持异常的概率

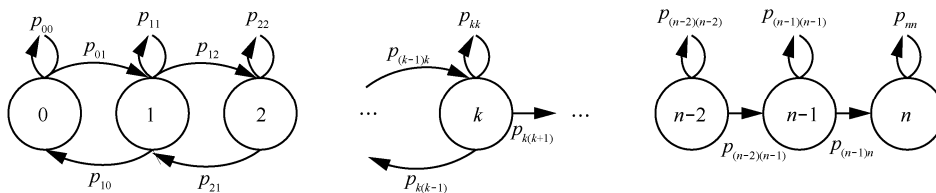


图5 非相似余度系统离散时间马尔可夫链模型

表 2 非相似余度系统单个执行体受未知扰动后状态转移概率设置		
参数	值	含义
s_{00}	0.9	执行体受干扰后处于初始状态的概率
s_{01}	0.1	执行体受干扰后响应异常的概率
s_{10}	0.9 (0)	执行体受干扰异常后响应恢复正常的概率
s_{11}	0.1 (1)	执行体受干扰异常后响应保持异常的概率

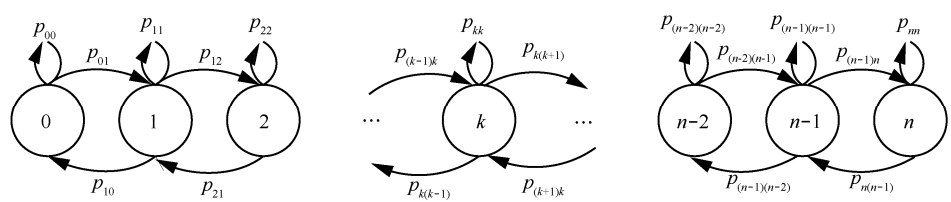


图 6 网络空间拟态防御系统离散时间马尔可夫链模型

表 3 网络空间拟态系统单个执行体受未知扰动后状态参数设置		
参数	值	含义
s_{00}	0.9	执行体受干扰后处于初始状态的概率
s_{01}	0.1	执行体受干扰后响应异常的概率
s_{10}	0.9	执行体受干扰后响应恢复正常的概率
s_{11}	0.1	执行体受干扰异常后响应保持异常的概率

和区块链系统，通过求解上述随机过程矩阵，可以分析各系统的可用概率与状态转移步数（min）的关系。

根据图 7 仿真结果，网络空间拟态防御系统能时刻保持高稳定可用性（抵抗攻击或扰动的能力）；区块链系统会在较短时间范围内保持高稳定可用性，随后快速衰减至 0；非相似余度系统的可用性会在较长一段时间内缓慢衰减为 0。

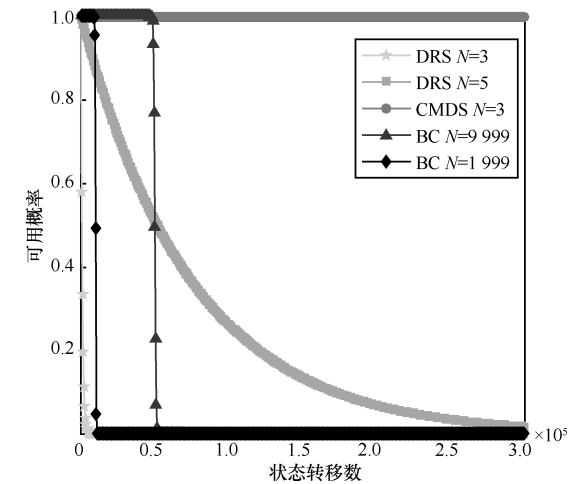


图 7 不同余度的 DRS、CMDS 和区块链系统可用概率与状态转移数（时间）的关系

图 8 通过比较 3 余度拟态防御系统和不同余度的非相似余度系统表明，随着余度数的增多，非相似余度系统的性能在一定时间内会趋于拟态防御系统。

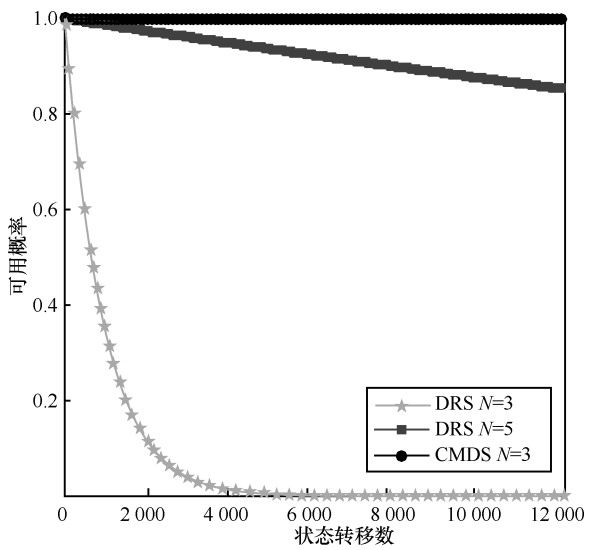


图 8 不同余度的 DRS 和 CMDS 可用概率与状态转移数（时间）的关系

图 9 通过比较非相似余度系统和区块链系统表明，非相似 3 余度系统的抗干扰性能高于同余

度区块链系统但低于实际高冗余 $N=1\ 999$ 的区块链系统。此外,随着冗余数的增加,非相似冗余系统的性能会快速趋于高冗余度区块链系统。

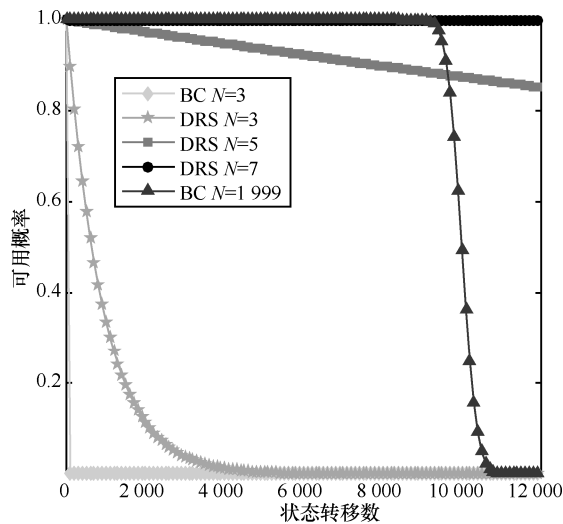


图9 不同冗余度的DRS和区块链系统可用概率与状态转移数(时间)的关系

图10通过比较3冗余度拟态防御系统和高冗余度 $N=9\ 999$ 的区块链系统表明,在初始一段时间范围内高冗余度区块链系统的可用性更优于拟态系统,但区块链系统抗干扰性能在之后的较短时间内会快速衰减。

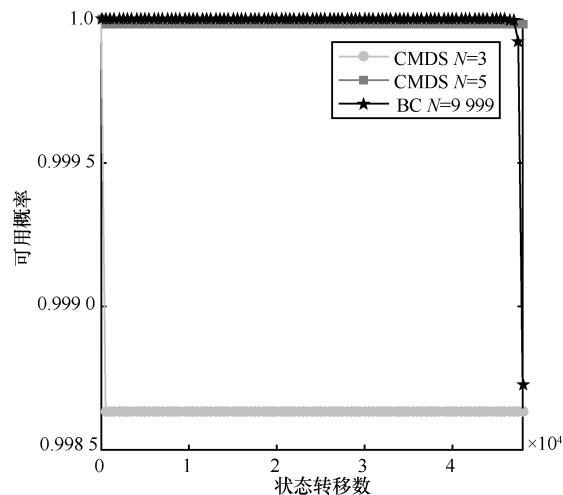


图10 不同冗余度的CMDS和区块链系统可用概率与状态转移数(时间)的关系

5 结束语

本文基于离散时间马尔可夫链模型对区块链系统、非相似冗余系统以及拟态防御系统进行建模,对比分析了3大系统在遭受攻击或干扰时的

可用性。本文的主要贡献如下。

1) 在一定时间范围内,较低冗余度的网络空间拟态防御系统、非相似冗余系统以及高冗余度的区块链系统都具有高稳定可用性和高可靠性。

2) 3冗余度拟态系统抵抗未知攻击或扰动性能具有时间稳定性;非相似冗余系统抵抗未知攻击性能随时间缓慢下降,非相似冗余系统适用于动态性需求较弱但抗随机性异常较大的场景。

3) 在一定时间范围内(中等攻击, $1 \times 10^5 \text{ min}$),高冗余度区块链系统能够维持很高的抗攻击或扰动性能,并优于3冗余度拟态系统(可用概率相差0.1%左右);但在超出该时间范围后快速下降,此时,拟态系统抗攻击或扰动性能显著高于区块链系统。

4) 在一定时间范围内(中等攻击, $1 \times 10^5 \text{ min}$),随着冗余数的增加,非相似冗余系统的抗攻击性能会快速拟合于高冗余度区块链系统;超过该时间范围,非相似冗余系统抗攻击性能显著高于区块链系统。

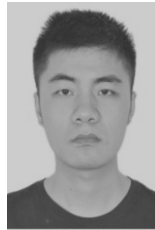
根据以上结果可以得出:根据不同干扰场景的抗干扰性能需求以及不同抗干扰系统自身的特性(区块链系统的高冗余特性、非相似冗余的异构弱动态性、拟态防御系统的动态异构低冗余特性),可以采用相应抗干扰系统的优势来综合考虑达到安全需求的代价。

参考文献:

- [1] VOAS J, GHOSH A, CHARRON F, et al. Reducing uncertainty about common-mode failures[C]//The Eighth International Symposium on Software Reliability Engineering. 1997:308-319.
- [2] LEVITIN G. Optimal structure of fault-tolerant software systems[J]. Reliability Engineering & System Safety, 2005, 89(3):286-295.
- [3] SWAN M. Blockchain: blueprint for a new economy[M]. O'Reilly Media, Inc. 2015.
- [4] 安金霞, 朱纪洪, 王国庆, 等. 多冗余度飞行计算机系统分级组合可靠性建模方法[J]. 航空学报, 2010, 31(2):301-309.
AN J X, ZHU J H, WANG G Q, et al. Hierarchical combination reliability modeling method for multiple redundancy flight control computer system[J]. Acta Aeronautica Et Astronautica Sinica, 2010, 31(2):301-309.
- [5] 郭江兴. 网络空间拟态防御研究[J]. 信息安全学报, 2016, 1(4):1-10.
WU J X. Research on cyber mimic defense[J]. Journal of Cyber Security, 2016, 1(4):1-10.
- [6] DISTEFANO S, XING N L. A new approach to modeling the system reliability: dynamic reliability block diagrams[C]// Reliability and Maintainability Symposium(Rams '06). 2006:189-195.
- [7] NYSTROM B, AUSTRIN L, ANKARBACK N, et al. Fault tree analysis of an aircraft electric power supply system to electrical ac-

- tuators[C]// International Conference on Probabilistic Methods Applied To Power Systems. 2006:1-7.
- [8] JIN J, PANG L, ZHAO S, et al. Quantitative assessment of probability of failing safely for the safety instrumented system using reliability block diagram method[J]. Annals of Nuclear Energy, 2015, 77: 30-34.
- [9] HURDLE E E, BARTLETT L M, ANDREWS J D. Fault diagnostics of dynamic system operation using a fault tree based method[J]. Reliability Engineering & System Safety, 2009, 94(9):1371-1380.
- [10] RANJBAR A H, KIANI M, FAHIMI B. Dynamic Markov Model for reliability evaluation of power electronic systems[C]// International Conference on Power Engineering, Energy and Electrical Drives. 2011:1-6.
- [11] SHI J, MENG Y, WANG S, et al. Reliability and safety analysis of redundant vehicle management computer system[J]. Chinese Journal of Aeronautics, 2013, 26(5):1290-1302.
- [12] CAI G, WANG B, LUO Y, et al. A model for evaluating and comparing moving target defense techniques based on generalized stochastic Petri net[M]//Advanced Computer Architecture. 2016: 184-197.
- [13] YEON J, ELEFTERIADOU L, LAWPHONGPANICH S. Travel time estimation on a freeway using discrete time Markov Chains[J]. Transportation Research Part B Methodological, 2008, 42(4): 325-338.
- [14] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报 2016,4 (42): 481-494.
YUAN Y, WANG F Y. Blockchain the state of the art and future trends[J]. Zidonghua Xuebao/Acta Automatica Sinica, 2016, 42(4): 481-494.
- [15] 林晓轩. 区块链技术在金融业的应用[J]. 中国金融 2016 (8): 17-18.
LIN X X. Application of block chain technology in financial industry[J]. China Finance, 2016(8):17-18.
- [16] 陈宗基, 秦旭东, 高金源. 非相似余度飞控计算机[J]. 航空学报, 2005, 26(3): 320-327.
CHEN Z J, QIN X D, GAO J Y. Dissimilar redundant flight control computer system[J]. Acta Aeronautica Et Astronautica Sinica, 2005.
- [17] 邬江兴. 拟态计算与拟态安全防护的原意和愿景[J]. 电信科学 2014, 30 (7):1-7.
WU J X. Meaning and vision of mimic computing and mimic security defense[J]. Telecommunications Science, 2014, 30 (7):1-7.

[作者简介]



任权（1994-），男，湖南常德人，国家数字交换系统工程技术研究中心硕士生，主要研究方向为网络安全防御、鲁棒网络体系结构。



贺磊（1974-），男，河南郑州人，国家数字交换系统工程技术研究中心副研究员，主要研究方向为网络安全防御、网络体系结构。



邬江兴（1953-），男，浙江嘉兴人，中国工程院院士，国家数字交换系统工程技术研究中心教授、博士生导师，主要研究方向为信息通信网络、网络安全。