针对物理访问控制的拟态防御认证方法

周清雷，班绍桓，韩英杰，冯峰
（郑州大学信息工程学院，河南 郑州 450001）

摘 要：针对传统物理访问控制系统的认证方法易受攻击的安全问题，基于拟态防御技术及其动态异构冗余架构（DHR）原理，以移动端二维码为接口、以动态口令为内核设计了一种拟态防御认证方法。首先，构建认证服务器的执行体池；然后，利用由输入分发代理、选调器和表决器等功能模块组成的中心控制器，实现从执行体池中动态调度异构冗余执行体；最后，表决器对异构冗余执行体输出进行多模裁决决定认证结果。实验结果表明，对比传统物理访问控制系统的认证方法，所提认证方法具有更高的安全性和可靠性。此外，所提认证方法能与其他认证方法组合使用。

关键词：访问控制；QR 码；异构冗余；拟态防御
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2020115

Mimic defense authentication method for physical access control

ZHOU Qinglei, BAN Shaohuan, HAN Yingjie, FENG Feng
School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China

Abstract: To address the security problem of the vulnerability of the authentication methods of traditional physical access control systems, a mimic defense authentication method was designed based on the principle of mimic defense technique and its dynamic heterogeneous redundant architecture (DHR), using mobile 2D code as the interface and dynamic password as the core. First, the actuator pool of the authentication server was constructed. Then, a central controller consisting of functional modules such as input distribution agent, selector and voter was used to dynamically schedule heterogeneous redundant actuators from the actuator pool. Finally, a multimode ruling on the heterogeneous redundant actuator output to determine the authentication result was made by the voter. The experimental results show that the proposed authentication method has higher security and reliability compared to the traditional physical access control system authentication method, and at the same time, it can be used in combination with other authentication methods.

Key words: access control, QR code, heterogeneous redundancy, mimic defense

1 引言

访问控制包括认证、控制策略实现和审计 3 个方面的内容[1]，而安全的身份认证方法是保证访问控制等安全机制有效实施和增强用户安全感的关键。目前，物理访问控制系统应用的传统身份认证技术有静态口令认证、智能卡认证和生物特征认证。静态口令认证是一种最原始、最简单的认证方式，容易被暴力破解，是一种极不安全的认证方式[2]。智能卡认证存在可复制、易丢失的风险，并且智能卡不方便携带和管理[3]。生物特征认证的识别率取决于采集条件，不但存在设备造价高、

收稿日期：2019−12−16；**修回日期**：2020−05−01
通信作者：班绍桓，banshaohuan@163.com
基金项目：国家重点研发计划基金资助项目（No.2016YFB0800100）；“公共安全风险防控与应急技术装备”重点专项基金资助项目
Foundation Items: The National Key Research and Development Program of China (No.2016YFB0800100), “Public Security Risk Prevention and Control and Emergency Technical Equipment” Key Special Fund

体型大等缺点，而且现已出现指纹膜等复制手段来破坏其安全性[4]。

针对目前物理访问控制系统中认证技术存在的问题，本文提出了一种基于拟态防御技术、以移动端 QR（quick response）码技术为接口、以动态口令认证为内核且应用于物理访问控制系统的认证架构。该认证架构不仅拥有高可靠、高可用等优点，还可与其他认证方案组合使用。

2　基础知识

本文所提认证架构的实现主要采用了 QR 码、动态口令和拟态防御等技术，下面对相关技术进行简要介绍。

2.1　QR 码

在多种二维码中，最常用的是由日本公司 Denso-Wave 于 1994 年创建的 QR 码，如图 1 所示，其结构由空白区、功能图形和编码区域组成。功能图形包括 4 个部分：位置探测图形、位置探测图形分隔符、定位图形和校正图形。编码区域包括 3 个部分：格式信息、版本信息、数据和纠错码字。

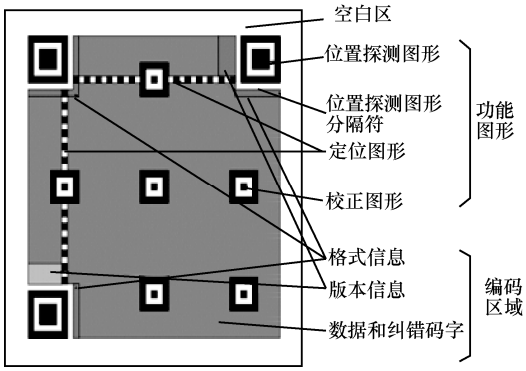

图 1　QR 码结构

QR 码与普通条形码相比具有支持中文字符及图像等多种文字信息、存储密度大、数据存储量高、纠错能力强和多角度高速识别等优点[5]。随着移动互联网技术的发展和智能终端的普及，将移动端作为载体，以 QR 码标准为核心而发展的编码、译码和识别相结合的移动端 QR 码技术已经广泛应用到移动支付、高校信息管理系统、身份识别、数据交换等方面[6-7]。

2.2　动态口令

动态口令又被称为一次性密码（OTP, one time password），它是一种随机生成、不断变换且仅一次有效的口令技术，用于应对静态口令的各种缺陷。动态口令根据“动态因子”的不同可分为同步认证技术和异步认证技术。同步认证技术主要包括时间同步和事件同步 2 种方式；异步认证方式主要包括挑战/响应认证技术。由美国研制的基于时间同步的动态口令认证系统 RSASecurID 较成熟，已被广泛应用在银行、证券等各种业务的关键型行业[8]。QR 码与动态口令的结合使用已应用在物理访问控制[9]、网银安全系统[10]等方面。

2.3　拟态防御

拟态防御（MD, mimic defense）是由邬江兴院士提出的一种在非相似余度架构的基础上增加策略调度和负反馈控制机制的新型主动防御技术[11]。这种防御技术具有的动态性、多样性和随机性等特性，能够非线性地提升系统安全性，其基本原理是动态异构冗余（DHR, dynamic heterogeneous redundancy）结构[12]，如图 2 所示。

首先，从异构元素池中选择合适的构件元素来组成不同的异构执行体集；然后，调度模块从这些异构执行体集中选择出奇数个执行体来处理由输入代理分发的相同输入信息；最后，表决模块对所有处理结果进行多模裁决以获得最终的输出，同时将这些执行体运行时所产生的信息反馈给调度模块，而调度模块根据反馈信息适时选择新的执行体来替换当前活跃的执行体集。如果执行体个数为 1 且去除表决模块，拟态防御就变成移动目标防御（MTD, move target defense）[13]。

目标防御的静态性和确定性因拟态防御技术的异构执行体集、动态调度等机制而发生改变，从而破坏了攻击对平台、环境的可依赖性。同时，拟态防御技术还利用多模裁决机制来应对未知的安全威胁。因此，拟态防御技术能够大大降低对目标系统攻击成功的概率。

到目前为止，基于 DHR 架构的拟态防御技术被广泛应用于网络安全领域。例如拟态 Web 服务器[14]、拟态域名系统（DNS, domain name system）框架[15]、拟态网络操作系统[16]、拟态路由器[17]等。

3　方案设计与分析

针对物理访问控制系统中传统认证方法所遇到的威胁，本节从拟态防御原理出发，给出一种以移动端 QR 码为接口、以动态口令技术为内核的认证方法，应用于物理访问控制系统的实现方案

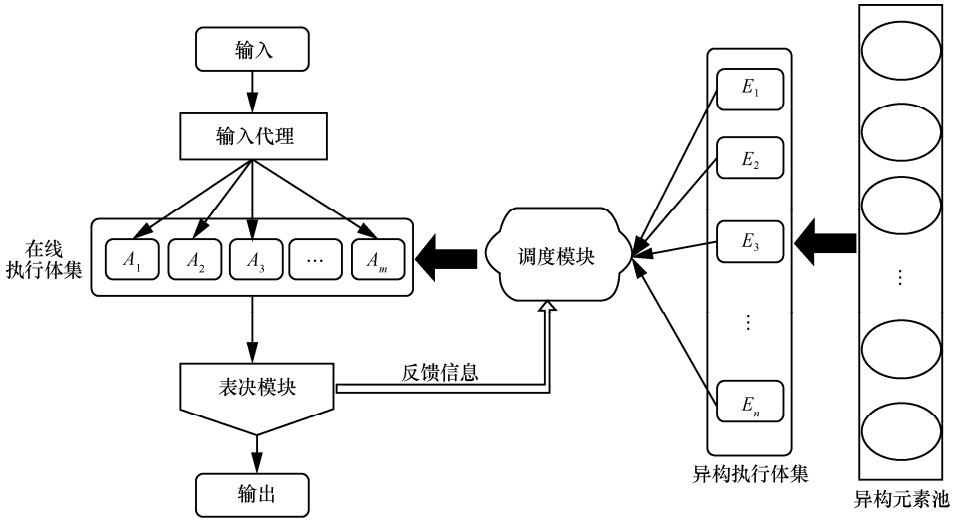

图 2　DHR 结构

（MD-PAC, MD-based physical access control），用拟态防御系统特有的内生安全机制来对抗未知病毒木马或漏洞后门等不确定性安全隐患。

3.1　MD-PAC 架构

MD-PAC 架构由认证服务器资源池、认证服务器执行体池和中心控制器组成（如无另外说明，下文提到的认证服务器皆为实现动态口令认证的服务器），如图 3 所示。其中，从认证服务器资源池选出异构冗余的认证服务器组成的执行体池是实现拟态防御的基本条件。中心控制器又分为选调器、输入分发代理和表决器 3 个基本模块，中心控制器是实现拟态防御技术核心模块。下面对这 3 个核心模块进行简要介绍。

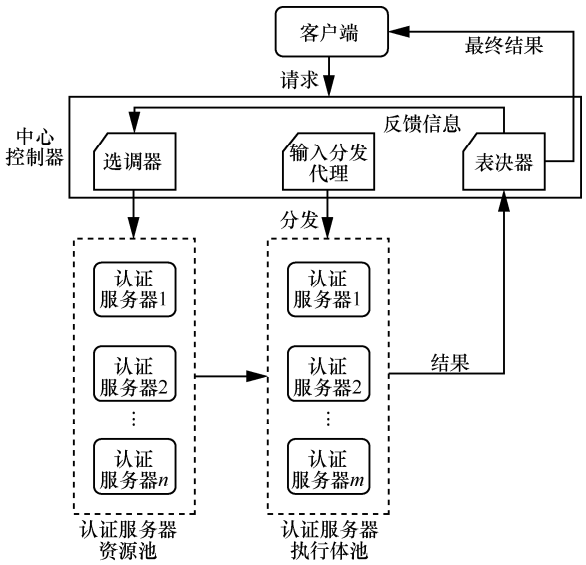

图 3　MD-PAC 架构

1) 选调器

策略调度作为 DHR 负反馈控制机制中的重要一环，其实现主要靠选调器来完成。选调器的调度策略可分为两类：第一类是定时替换在线认证服务器执行体，即在规定的工作时间结束后，从 n 个认证服务器组成的资源池中选出 m 个认证服务器以替换当前的在线执行体；第二类是异常情况发生时强制替换，即当表决器判定在线执行体的处理结果存在不一致问题时，表决器将异常信息反馈给选调器，选调器会根据规定的调度策略选择相应认证服务器以替换当前的在线执行体。

选调策略的具体设计应遵循问题规避而不是问题归零的原则，根据实际问题场景而定，以期实现执行体资源的最大限度利用。从资源池中随机选取认证服务器作为在线执行体集是最简单的一种调度策略，复杂的调度策略有定义执行体的置信度以选择高置信度的执行体，这为动态调度的研究进展提供了更丰富的调度策略[18]。

2) 输入分发代理

输入分发代理的功能是对客户端发来的输入进行预处理，并分发给各个在线的异构认证服务器执行体。其中，预处理主要包括规范输入序列语法语义、适配各执行体通信信道等标准化或归一化处理，以屏蔽拟态防御场景的对外差异，这是实现该架构的必要步骤。

3) 表决器

表决器负责实现多模裁决机制，即对在线执行体的处理结果进行表决，并将得到的最终表决结果

返回给客户端；同时，如果出现异常情况，则将反馈信息传输至选调器。

表决器的裁决策略决定了 DHR 架构对未知攻击的感知能力，常见的裁决策略有简单的大数表决，以及复杂的、高防御等级的一致性比较、策略参数组合比较和迭代判决等。

3.2　可行性分析

MD-PAC 架构的应用离不开移动端 QR 码技术、动态口令认证技术和拟态防御技术的实现。

移动端 QR 码已经广泛应用在移动支付等领域，移动端 QR 码的生成与智能终端的识别等配套设备也非常完善，并且，相较于移动端 QR 码在类似硬件交互系统中所带来的便利性，其经济成本很低，甚至可以忽略。

动态口令认证技术也十分成熟，并成功地应用在银行、证券等关键业务领域。

拟态防御技术的实现是 MD-PAC 架构提升安全性能的重点。如 2.3 节所述，拟态防御技术已成功应用于 Web 服务器、DNS 服务器和路由器等互联网相关领域。多样化的市场环境提供的大量标准化的商用现成（COTS, commercial off-the-shelf）级软硬件产品保障了认证服务器的异构性。同时，虚拟化技术的灵活性不仅能提高全局效益，还降低了部署拟态防御认证架构所需的费用。

从表 1 可以看出，由多层不同元素组成的认证服务器具有异构冗余特性，其具体体现在如下几个方面。

表 1　　认证服务器异构池元素

异构层级	异构元素
处理器层	Intel、AMD、ARM、IBM
操作系统层	Windows(Windows 7, Windows 8, Windows 10; Windows Server 2003, Windows Server 2008)
	Linux(Debian、RedHat、Ubuntu)
虚拟化层	VMware、VirtualBox、MiWorkspace
编译器层	GNU、Cygwin、MSVC、Borland

1) 处理器层。认证服务器可以使用由 Intel、AMD、ARM、IBM 等不同厂商生产的不同型号的处理器。

2) 操作系统层。每个认证服务器的底层操作系统可以选择 Windows、Linux 等。

3) 虚拟化层。常见的虚拟化软件有 VMware、VirtualBox、MiWorkspace 等。

4) 编译器层。通过多样化的编译工具可生成不同的执行文件，以获得软件层面的异构功能等价体。具体的编译工具有 GNU、Cygwin、MSVC、Borland 等。

动态性可在异构冗余认证服务器池的基础上，由选调器的动态调度策略和表决器的裁决功能共同建立的负反馈控制机制来实现。

此外，MD-PAC 架构还需要如下假设前提，这些假设不失一般性。

1) 对于一个输入，系统必须有一个输出与之对应。

2) 在线异构执行体安全的情况下，对于同一输入，每个异构执行体都有与之对应的处理结果。

3) 允许异构的认证服务器之间有不同的处理时延。

4) 若执行体被攻击，则被攻击执行体的处理结果与正常执行体的处理结果不一致。

3.3　工作原理

正常情况下，拟态防御认证系统通过在线认证服务器执行体对请求进行处理，然后执行体将处理结果传输到表决器，表决器对处理结果进行裁决，并将最终结果返回给客户端，同时向选调器传输反馈信息。而选调器则根据反馈信息和定时任务 2 种机制动态地替换在线认证服务器执行体。

MD-PAC 架构的具体工作流程如图 4 所示，具体介绍如下。

1) 用户进行注册操作并与 MD-PAC 认证系统进行绑定。

2) 选调器从异构认证服务器资源池中选择 m 个认证服务器进行初始化操作，在线执行体等待任务。

3) 认证开始时，用户移动端的应用程序产生动态口令并生成相应认证 QR 码。

4) 智能硬件终端识别二维码并将识别内容作为输入传输给中心控制器。

5) 中心控制器中的输入分发代理对输入进行相应预处理后向在线的认证服务器执行体分发任务处理请求。

6) 在线的认证服务器执行体进行本次认证任务，并将处理结果发送至中心控制器中的表决器。

7) 表决器对返回的处理结果进行多模裁决。

① 若处理结果一致，则认为认证成功，并将认证成功的信息传输给客户端中的智能硬件终端。

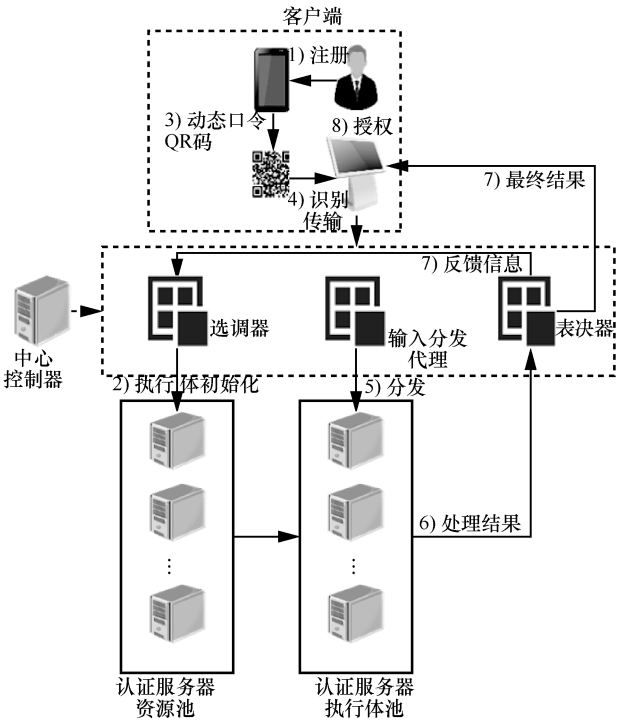

图 4　MD-PAC 架构的具体工作流程

② 若处理结果不一致，则按照裁决策略判定认证是否成功，并将最终结果传输给客户端中的智能硬件终端，同时将处理结果、执行体状态等信息反馈给选调器，选调器按照相关选调策略对执行体进行后续替换、清洗等操作。

8) 智能硬件终端根据最终返回结果判定用户是否有权进行访问控制等操作。

3.4　安全性分析

移动端 QR 码技术已经十分成熟，并广泛应用于扫码支付、扫码乘车、门禁等方面，其安全性已满足绝大多数场景。对于拥有更高安全需求的应用场景，可将普通 QR 码换成基于拟态防御思想加密的 QR 码（M-QR, mimic QR code）。M-QR 拥有更高的安全性和可靠性，是本文作者的前期研究成果，在此不做赘述。

拟态防御的异构冗余性、动态性、不确定性等特性使 MD-PAC 架构具备良好的入侵容忍能力，即使半数以上执行体被成功攻击，也会因为当前在线执行体在下一调度周期被替换而使 MD-PAC 架构能继续提供高可靠服务（当然，在成功攻击周期内，MD-PAC 架构可能无法提供可靠服务）。异常执行体会因拟态多模裁决机制而被实时地下线清洗。因此，上述特性非线性地提升了 MD-PAC 架构的安全性。

MD-PAC 架构中，中心控制器的选调器、输入分发代理和表决器作为认证服务的前端，更容易受到攻击者的青睐。因此，需对其进行较严格的配置，例如使中心控制器独立于任何认证服务器、使用单向传递信息机制、使用执行体内部随机性信息作为调度策略中的参数、对反馈控制算法和调度算法严格保密等。

MD-PAC 架构与文献[9]所述架构 OQAS（OPT QR-code authentication system）以及传统动态口令认证架构在抗穷举攻击等多方面抗攻击性的对比如表 2 所示。其中，MD-PAC 架构的认证任务采用动态口令认证，所以该架构保留了动态口令认证带来的良好的抗攻击性能。同时，MD-PAC 架构与 OQAS 架构都可对动态口令进行哈希加密，从而使穷举攻击无效。借助拟态防御系统特有的内生安全机制来对抗未知攻击则是 MD-PAC 架构所独有的特性。

表 2　　所涉及认证架构的抗攻击性对比

架构	穷举攻击	撞库攻击	重放攻击	中间人攻击	未知攻击
MD-PAC 架构	是	是	是	是	是
OQAS 架构	是	是	是	是	否
传统动态口令认证架构	否	是	是	是	否

4　仿真实验

本节对 MD-PAC 架构在安全性能和时间性能方面进行仿真实验验证。三模冗余是目前最常见、易实现的有效 DHR 架构[14]，因此本文所做实验与分析的对象均为三模冗余的 MD-PAC 架构。

4.1　安全性能

参考文献[12]，本节在离散模型的基础上使用 MATLAB R2016a 对 MD-PAC 架构和 OQAS 架构（不使用 DHR 架构进行防御）在安全性能上进行仿真对比与分析。

根据 DHR 结构的性能评估模型假设，攻击者的攻击能力随着时间而不断增强。参考该模型，非冗余异构的静态认证服务器随时间的推移被未知攻击威胁，攻击成功的概率可表示为

$$P_i = \int_0^{T_i} \lambda \mathrm{e}^{-\lambda t} \mathrm{d}t, i = \{1,2,\cdots,n\} \tag{1}$$

其中，T_i 为第 i 个请求服务周期的结束时间，λ 为常系数。

假设 MD-PAC 架构采取了动态的随机调度策略，认证服务器执行体会发生周期性的动态变化，从而向外表现出一种随机性。因此，在每个周期中，攻击成功的概率还会因在线执行体间的异构性不同而产生折扣，该折扣因子（设为 μ ）可以通过冗余执行体间的相异度来计算。执行体间异构性越大，相异度的值越大，攻击成功的概率就越低，即折扣因子的值越小。折扣因子与相异度的关系可表示为

$$\mu_i = \frac{\xi}{\alpha_i}, i = \{1,2,\cdots,n\} \tag{2}$$

其中，$\alpha_i(\alpha_i \in (0,1])$ 为第 i 个周期内在线执行体之间的平均相异度，ξ 为常系数。

假设每个在线认证服务器执行体被成功攻击的概率都相等，同时假设使用大数表决算法作为表决器中的拟态裁决策略。一个周期内在线执行体不会发生变化，所以系统在一个周期内被成功攻击的概率是一定的。在第 i 个周期内 MD-PAC 架构被成功攻击的概率可表示为

$$P_i = \mu_i \sum_{u=\frac{m+1}{2}}^{m} C_m^u p_i^u (1-p_i)^{m-u}, i = \{1,2,\cdots,n\} \tag{3}$$

其中，$\mu_i(\mu_i \in (0,1])$ 为第 i 个周期内的折扣因子；C_m^u 表示 m 个执行体中有任意 u 个被成功攻击，m 为第 i 个周期内在线执行体的数量，$u>\frac{m}{2}$ 为第 i 个周期内在线执行体被成功攻击的数量；p_i 为第 i 个周期内在线执行体被成功攻击的概率。

到目前为止，从技术方法上还无法准确测量异构冗余执行体之间的相异度。由于相异度与相似度必然相关联，因此利用相似度来计算相异度，即

$$\alpha_i = \frac{\delta}{\beta_i}, i = \{1,2,\cdots,n\} \tag{4}$$

其中，$\beta_i(\beta_i \in (0,1])$ 为相似度，δ 为常系数。

将文献[19]中的相似度矩阵作为本节认证服务器执行体之间相似度矩阵的数据来源，当 λ=0.5、ξ=0.8、δ=0.6，且 m=3 时，MD-PAC 架构与 OQAS 架构的安全性能对比如图 5 所示。由图 5 可知，拟态防御机制显著提升了 MD-PAC 架构的安全性。

冗余度对 MD-PAC 架构安全性能的影响如图 6 所示。从图 6 可以看出，随着架构冗余度的增加，同一周期内架构被成功攻击的概率降低。

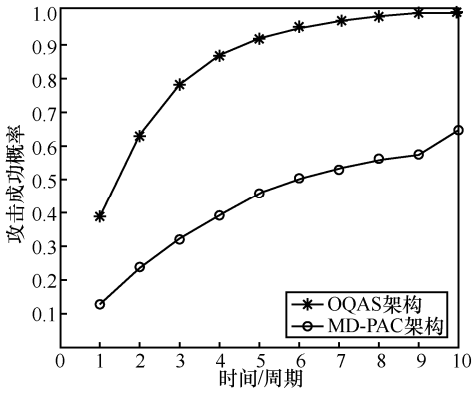

图 5　MD-PAC 架构与 OQAS 架构的安全性能对比

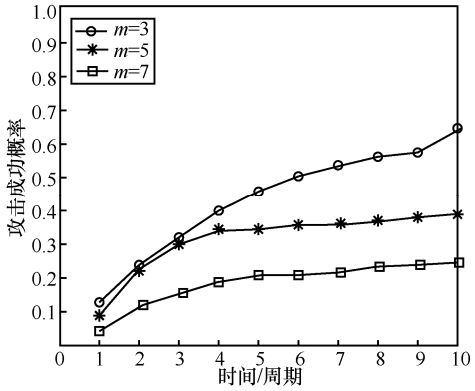

图 6　冗余度对 MD-PAC 架构安全性能的影响

4.2　时间性能

本节对 MD-PAC 架构与 OQAS 架构在时间性能上进行理论对比分析并用仿真实验进行验证，所涉及的符号如表 3 所示。

表 3　　符号定义

符号	含义
T_{G_QR}	移动端生成含相关信息 QR 码耗时
T_{I_QR}	智能硬件终端识别 QR 码耗时
$T_{transfer}$	输入从客户端传输到一个执行体耗时
$T_{max\_transfer}$	输入从客户端传输到执行体中最长耗时
T_{AP}	一个执行体处理任务耗时
T_{max_AP}	所有执行体中处理任务中最长耗时
T_{SA}	选调器处理耗时（调度执行体）
T_{voter}	表决器处理耗时

由于认证服务器的异构性，每个服务器对同一任务的处理在时间上有所差异，并且在线认证服务器执行体之间是相互独立的，因此可用服务器处理任务的最长耗时来代表整个在线执行体集的处理耗时。同理，也可用最大传输时延来代表整个传输过程耗时。MD-PAC 架构的一个请求服务周期耗时为

$$T_{\text{MD-PAC}}=T_{\text{G\_QR}}+T_{\text{I\_QR}}+T_{\text{max\_AP}}+T_{\text{SA}}+T_{\text{voter}}+2T_{\text{max\_transfer}} \quad (5)$$

OQAS 架构只有一个静态认证服务器，所以不存在任务处理耗时和传输耗时的不同，也不存在选调器处理耗时和表决器处理耗时，因此该架构的一个请求服务周期耗时为

$$T_{\text{OQAS}}=T_{\text{G\_QR}}+T_{\text{I\_QR}}+T_{\text{AP}}+2T_{\text{transfer}} \quad (6)$$

本文假设 MD-PAC 架构所用服务器的最大处理时延与 OQAS 架构的服务器处理时延相等，MD-PAC 架构的最大传输时延与 OQAS 架构的传输时延大约相同。所以，与 OQAS 架构相比，MD-PAC 架构一个请求服务周期的额外增加时延为

$$T_{\text{addition}} \approx T_{\text{SA}}+T_{\text{voter}} \quad (7)$$

即 MD-PAC 架构与 OQAS 架构相比需要耗费额外的时间，而额外增加时延体现在选调器调度耗时与表决器处理耗时上。

在本次验证实验中，为实现 MD-PAC 架构的多样性和异构性，MD-PAC 实验对象的 3 个执行体（三模冗余）使用了不同的操作系统、编程语言版本和异构化处理脚本。另一方面，为方便对比，选取 MD-PAC 实验对象中的一个执行体作为 OQAS 的实验对象，且该实验对象使用的脚本未进行异构化处理。2 种实验对象的组成配置如表 4 所示。

表 4 测试对象配置

实验对象	操作系统	编程语言	脚本
MD-PAC	Windows 10	Python 3.6.2	异构化处理
	Ubuntu 16.04	Python 3.7.4	
	CentOS 7（VMware）	Python 3.7.0	
OQAS	CentOS 7（VMware）	Python 3.7.0	未异构化处理

此外，2 种实验对象都使用基于时间同步的动态口令认证技术，且都用电脑识别 QR 码的过程模拟智能终端读取 QR 码。

根据 2 种实验对象配置进行多组重复实验，记录每次实验的耗时，计算 2 种实验对象耗时的最小值、平均值和最大值，如图 7 所示。根据实验结果的对比可以得出，MD-PAC 实验对象在耗时的最小值、平均值和最大值上均高于 OQAS 实验对象，这是由于三模冗余的 MD-PAC 架构在对异构执行体进行拟态裁决、对冗余执行体进行动态调度时需要耗费额外的时间。因此，该验证实验符合理论分析结果。

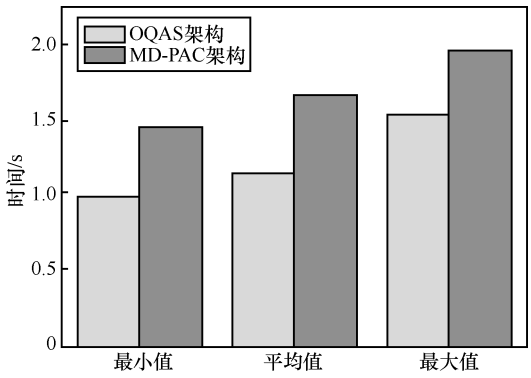

图 7 时间性能对比

5 结束语

本文针对现有物理访问控制架构无法有效应对未知威胁的问题，提出了基于拟态防御思想、以移动智能端二维码为接口、以动态口令为内核的 MD-PAC 架构。仿真实验表明，该架构具有的动态性、异构性和不确定性提升了物理访问控制中认证服务的安全性。对比以动态口令为认证方法的传统物理访问控制架构和 OQAS 架构，所提架构具有更高的安全性能。时间开销增大、经济成本增加是所提架构带来的不足之处。因此，接下来的研究重点为优化调度算法和裁决策略等，以提升时间性能；与虚拟化和云服务等技术结合使用，以降低经济成本。

参考文献：

[1] 贾铁军, 侯丽波, 宋少婷, 等. 网络安全实用技术[M]. 北京: 清华大学出版社, 2011.
JIA T J, HOU L B, SONG S T, et al. Practical network security technology[M]. Beijing: Tsinghua University Press, 2011.

[2] 李小燕. 网络可信身份认证技术演变史及发展趋势研究[J]. 网络空间安全, 2018, 9(11): 6-18.
LI X Y. Study on evolution history and development trend of network trusted identity authentication technology[J]. Information Security and Technology, 2018, 9(11): 6-18.

[3] 常玲, 赵蓓, 薛姗, 等. 基于网络安全的身份认证技术研究[J]. 电信工程技术与标准化, 2019, 32(2): 37-42.
CHANG L, ZHAO P, XUE S, et al. Research on identity authentication technology in network security[J]. Telecom Engineering Technics and Standardization, 2019, 32(2): 37-42.

[4] 安迪, 杨超, 姜奇, 等. 一种新的基于指纹与移动端协助的口令认证方法[J]. 计算机研究与发展, 2016, 53(10): 2400-2411.
AN D, YANG C, JIANG Q, et al. A new password authentication method based on fingerprint and mobile phone assistance[J]. Journal of Computer Research and Development, 2016, 53(10): 2400-2411.

[5] 周庆, 黄党志. 基于 Ising 模型的 QR 码加密算法[J]. 计算机应用, 2013, 33(10): 2861-2864.

ZHOU Q，HUANG D Z. Encryption algorithm for QR code based on Ising model[J]. Journal of Computer Applications, 2013, 33(10): 2861-2864.

[6] 韩林, 张春海, 徐建良. 基于二维码的内外网物理隔离环境下的数据交换[J]. 计算机科学, 2016, 43(S2): 520-522.
HAN L, ZHANG C H, XU J L. Data exchange based on QR code in physically isolated internal and external network environment[J]. Computer Science, 2016, 43(S2): 520-522.

[7] 古晓艳, 夏志强. 基于二维码的高校教学设备管理系统的设计与实现[J]. 计算机科学, 2017, 44(S1): 523-525.
GU X Y, XIA Z Q. Design and implementation of teaching equipment management system based on two-dimensional code[J]. Computer Science, 2017, 44(S1): 523-525.

[8] MOHAN P, CHELLIAH S. An authentication technique for accessing de-duplicated data from private cloud using one time password[J]. International Journal of Information Security and Privacy, 2017, 11(2): 1-10.

[9] KAO Y, LUO G, LIN H, et al. Physical access control based on QR code[C]//2011 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. Piscataway: IEEE Press, 2011: 285-288.

[10] 于英政. QR 二维码相关技术的研究[D]. 北京: 北京交通大学, 2014.
YU Y Z. Research on related technologies of the QR 2-dimensional code[D]. Beijing: Beijing Jiaotong University, 2014.

[11] 邬江兴. 网络空间拟态防御导论[M]. 北京: 科学出版社, 2017.
WU J X. Introduction to cyberspace mimic defense[M]. Beijing: Science Press, 2017.

[12] 扈红超, 陈福才, 王禛鹏. 拟态防御 DHR 模型若干问题探讨和性能评估[J]. 信息安全学报, 2016, 1(4): 40-51.
HU H C, CHEN F C, WANG Z P. Performance evaluations on DHR for cyberspace mimic defense[J]. Journal of Cyber Security, 2016, 1(4): 40-51.

[13] ZHUANG R, DELOACH S A, OU X. Towards a theory of moving target defense[C]//Proceedings of the First ACM Workshop on Moving Target Defense. New York: ACM Press, 2014: 31-40.

[14] 仝青, 张铮, 张为华, 等. 拟态防御 Web 服务器设计与实现[J]. 软件学报, 2017, 28(4): 883-897.
TONG Q, ZHANG Z, ZHANG W H, et al. Design and implementation of mimic defense Web server[J]. Journal of Software, 2017, 28(4): 883-897.

[15] 王禛鹏, 扈红超, 程国振. 一种基于拟态安全防御的 DNS 框架设计[J]. 电子学报, 2017, 45(11): 2705-2714.
WANG Z P, HU H C, CHENG G Z. A DNS architecture based on mimic security defense[J]. Acta Electronica Sinica, 2017, 45(11): 2705-2714.

[16] 王禛鹏, 扈红超, 程国振. MNOS:拟态网络操作系统设计与实现[J]. 计算机研究与发展, 2017, 54(10): 2321-2333.
WANG Z P, HU H C, CHENG G Z. Design and implementation of mimic network operating system[J]. Journal of Computer Research and Development, 2017, 54(10): 2321-2333.

[17] 马海龙, 伊鹏, 江逸茗, 等. 基于动态异构冗余机制的路由器拟态防御体系结构[J]. 信息安全学报, 2017, 2(1): 29-42.
MA H L, YI P, JIANG Y M, et al. Dynamic heterogeneous redundancy based router architecture with mimic defenses[J]. Journal of Cyber Security, 2017, 2(1): 29-42.

[18] OUELHADJ D, PETROVIC S. A survey of dynamic scheduling in manufacturing systems[J]. Journal of Scheduling, 2009, 12(4): 417.

[19] 刘勤让, 林森杰, 顾泽宇. 面向拟态安全防御的异构功能等价体调度算法[J]. 通信学报, 2018, 39(7): 188-198.
LIU Q R, LIN S J, GU Z Y. Heterogeneous redundancies scheduling algorithm for mimic security defense[J]. Journal on Communications, 2018, 39(7): 188-198.

[作者简介]

周清雷（1962– ），男，河南新乡人，博士，郑州大学教授、博士生导师，主要研究方向为信息安全、自动机理论及计算复杂性理论。

班绍桓（1996– ），男，河南永城人，郑州大学硕士生，主要研究方向为信息安全。

韩英杰（1976– ），女，黑龙江密山人，郑州大学讲师，主要研究方向为信息安全、自动机与模型检测等。

冯峰（1990– ），男，河南新乡人，郑州大学硕士生，主要研究方向为信息安全和高性能计算。