基于拟态防御原理的分布式多接入边缘计算研究

朱泓艺，陆肖元，李毅
（上海宽带技术及应用工程研究中心，上海 200436）

摘　要：多接入边缘计算在网络边缘提供高性能的网络资源，但由于其位置管理分散，所以对安全性能要求较高。基于拟态防御原理提出了分布式多接入边缘计算的拟态防御架构，通过分割数据与校验填充，转发至多个边缘节点处理，并根据校验分析实现了多模裁决与动态调度的拟态防御机制。仿真结果表明，在增加时延成本的情况下，该架构可有效降低数据被篡改和被泄露的概率。提出了基于置信度与时延成本的边缘节点调度策略，提升了系统的效率与安全性能。

关键词：多接入边缘计算；业务编排；拟态安全防御；动态异构冗余
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.2096−3750.2019.00122

Research on distributed multi-access edge computing based on mimic defense theory

ZHU Hongyi, LU Xiaoyuan, LI Yi
Shanghai Engineering Research Center for Broadband Technologies and Applications, Shanghai 200436, China

Abstract: The highly efficient network resources are provided by multi-access edge computing at the edge of the network, but high security capability is required also due to its distributed position and organization. Based on mimic defense theory, mimic defense structure for distributed multi-access edge computing was proposed. By segmenting data, padding check data and processing data at multiple edge node, dynamic scheduling and decision-making functions according to checksum were implemented. The simulation results show that with the increase of delay cost, the data manipulation and leak rates can be reduced effectively by the proposed structure. The edge node scheduling strategy based on trust and cost is proposed to improve the efficiency and security of the system.

Key words: multi-access edge computing, task orchestration, mimic security defense, dynamic heterogeneous redundancy

1　引言

随着大数据研究的深入推进，其应用逐步渗透到社会的各行各业中，对大数据的关注点逐渐聚焦到如何有效利用采集的数据服务于产业的创新与发展上。挖掘、分析和利用大数据，对当今科技的创新具有重要的实践指导意义。在物联网应用场景中，由于数据的规模远超出终端用户的计算处理能力，因此，目前的大数据处理模式仍以将处理任务迁移至远程云计算中心为主，但是这样的处理模式引发了 3 种问题：1) 将大数据集中到云计算中心进行处理，占用了通信网络的回传带宽，导致网络拥塞情况严重；2) 对于部分智能化业务应用的要求无法满足，如无人驾驶的高可靠性、低时延要求；3) 传输、缓存链路过长，则更容易遭受各种类型的网络攻击与威胁。因此，在实践中由海量传感器或物联

收稿日期：2019−06−11；修回日期：2019−07−12
通信作者：朱泓艺，hyzhu@bnc.org.cn
基金项目：国家重点研发计划项目（No.2017YFB0803205）；上海市科学技术委员会科研计划项目（No.18DZ1100503）
Foundation Items: The Key Research and Development Program of China (No.2017YFB0803205), Science Research Program of Shanghai Scientific and Technology Committee (No.18DZ1100503)

网设备采集的大数据，无法经网络传至数据中心进行有效利用。

边缘计算是指在靠近终端用户或数据源的网络边缘侧，集网络、计算和存储于一体的分布式开放平台。作为云计算和移动边缘计算的补充，欧洲电信标准化协会（ETSI，European Telecommunications Standards Institute）于 2018 年提出了多接入边缘计算（MEC，multi-access edge computing）[1]。MEC 扩展了边缘计算的定义和应用，在网络边缘节点提供各种类型的 IT 业务，能够同时为固定用户和移动用户提供边缘计算服务，将部分数据和计算任务迁移至 MEC 节点进行处理，可大幅度降低回传至远程数据中心的带宽占用。同时，由于缩短了通信路径，端到端的时延和安全问题都能获得有效解决。MEC 作为 5G 大数据时代的核心技术之一，近几年受到国内外学术界与产业界的广泛关注，但对 MEC 的研究仍处于起步阶段，相关研究主要侧重于边缘节点资源建模[2]、资源优化管理与业务编排[3]、边缘网络安全等方面。

尽管 MEC 可以有效解决大数据处理模式引发的 3 个问题，但为了将理论付诸于实践，仍然有多项技术难点亟待研究和攻破[4]，如边缘计算任务迁移策略[5]。相较于云计算中心，MEC 服务器的计算、缓存和传输等网络资源有限，在业务处理过程中，需要应用边缘与云、边缘与边缘的协作，根据业务数据量、时延要求等特征，分别分配至本地 MEC、临近 MEC 或远程数据中心进行处理。在任务迁移过程中，由于传输链路和各节点的安全性能不同，数据安全的风险程度也不同。目前，MEC 服务器在安全性能上具有以下 3 个特点：1) 应用的软/硬件多种多样，其中，大部分软/硬件具有无法预知的安全缺陷和漏洞后门；2) 网络结构和端口等主要应用独立静态配置，攻击者持续的探测攻击使得系统安全性能随时间的增长而下降；3) 服务器中应用的防御技术大部分为被动防御如防火墙等，无法对未知的漏洞和威胁提供有效预防措施。因此，“动态防御”成为网络安全领域的主要研究课题。在国外，研究者提出移动目标防御（MTD，moving target defense），为系统的各项配置引入动态随机性，使得系统在多方面呈现出不可预知的特点，从而有效阻止攻击者对目标系统的分析和攻击，大幅度提高了攻击难度和成本。在我国，由邬江兴院士提出的拟态防御策略不仅考虑了动态与随机性[6]，并引入了动态异构冗余（DHR，dynamic heterogeneous redundancy）的理念，为目标系统创建同功能异构的执行空间。在运行期间，动态调用多个异构执行体，在输出端进行一致性判决，并使用反馈控制模块对异构执行体进行重新调度和清洗等。拟态防御思想已被应用于多种网络设备[7]及软件[8]设计中，为系统提供内生的安全防护性能。

在 MEC 方案中，由于各个 MEC 都独立采用异构的服务器架构、软/硬件设施，可视作具有相同功能的异构体。因此，为了提高 MEC 方案的安全性能，本文提出了一种基于拟态防御理论的分布式 MEC 方案架构。传统的边缘计算体系仅考虑了端—边—云之间的协同，被称为“边云协同”。而在本文所考虑的系统架构中，多个 MEC 通过有线通信方式如电缆、光缆或无线通信方式如 Wi-Fi、4G/5G 等互相连接，并且可以互相协同处理业务。为了提升边缘计算体系的内生网络安全防护性能，在用户端设置一个转发/接收代理设备，提供数据切割、校验填充和数据转发等功能，将数据处理业务交由多个 MEC 处理。不同 MEC 的通信模式、硬件架构和软件系统分别由各自的供应商独立构建，呈现天然的高度异构性，因此，交由不同 MEC 进行的分布式数据处理可被视为异构执行体。在接收数据时，收发设备通过分析数据的校验部分，获取各个 MEC 受网络攻击的情况，并且基于 MEC 置信度实现拟态防御的多模裁决与动态调度等机制。针对异构、多样、动态以及随机的网络环境，提出了面向拟态防御系统的信息安全模型[9]，在应用层按照功能对业务进行切片分割并引入 DHR 架构，并提出拟态安全等级评估方案对其进行分析[10]。上述研究均以普适的网络架构为着眼点，没有针对分布式计算网络模型的拟态防御安全评估。与基于拟态防御的高安全分布式存储系统[11]不同，本文侧重于 MEC 架构中的数据在迁移与处理过程中的拟态防御安全分析与评估，通过模型建立、优化权衡与模拟仿真，定量分析该 MEC 架构中资源消耗与安全增益的权衡关系。仿真结果表明，拟态防御思想在 MEC 架构中，能够通过增加一定时延提供高度可靠的内生安全，有效降低了 MEC 进行数据处理时被泄露与被篡改的风险。

2　基于拟态防御原理的分布式 MEC 方案

区别于传统的孤立边缘计算架构，本文所提

的 MEC 方案支持有线与无线不同模式的多种接入方式，并且将多个临近且互连的 MEC 服务器划分为一个合作域，称为 MEC 合作域。任意一个固定或移动用户不仅可以访问最近的 MEC 服务器（以下称为“主 MEC 服务器”），还可以由主 MEC 服务器调用整个 MEC 合作域中多个 MEC 服务器的计算资源。

2.1 MEC 系统结构与工作流程

MEC 系统结构如图 1 所示，待处理的数据源由数据采集器提供如监控摄像，并交由收发代理设备进行数据分割、校验填充与转发处理。收发代理设备可以为内置于传感器的单元模块，也可以为一个独立设备，但在本架构中，该设备需处于用户控制范围内，其安全性能才可以由用户掌控。数据经过初步分割处理后，由收发代理交给 MEC 合作域内的多个 MEC 服务器进行数据处理，其中，主 MEC 服务器为直连，其余多个服务器则由主 MEC 服务器以及 MEC 互连的旁路进行通信传输，路径中的 MEC 服务器仅进行数据转发而不对数据进行分组与计算。

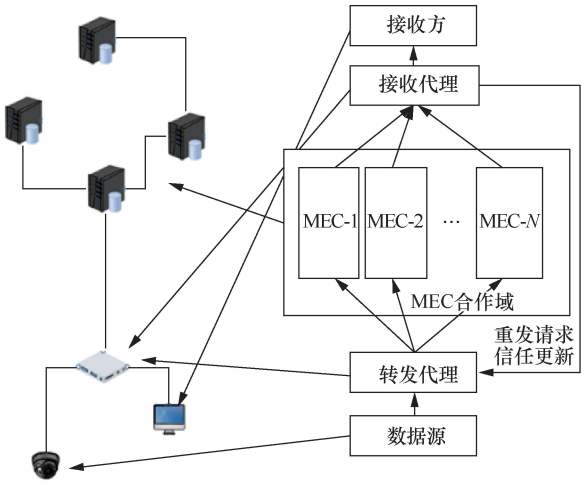

图 1 MEC 系统结构

当每个 MEC 服务器完成各自的数据处理计算后，将处理结果由原路传回至收发代理进行校验分析。收发代理根据校验分析结果，将正确处理的数据传递至数据接收方，将产生错误信息的 MEC 服务器标记为不可信，直至其经过重置、清洗等手段恢复正常工作为止，同时，将校验信息错误的数据重发至其他 MEC 服务器进行处理。

2.2 基于 DHR 的 MEC 架构

DHR 架构作为拟态安全防御的核心思想与理念，旨在为需要网络安全防御的目标系统引入多个功能等价的异构执行体，并采取动态化的调度策略，以在系统中加入冗余为代价，使得原本静态的系统在功能、执行模式等方面变得不确定且难以识别。在目标系统受网络攻击时，DHR 架构可以为系统提供内生的安全防护，并与其他静态防御手段如加密、防火墙等协同联防，从而成倍提升系统的安全性能。在本文所提的多 MEC 服务器协作的分布式数据处理架构中，异构、冗余与动态分别由多 MEC 分布式处理、校验数据填充与基于反馈信息的动态 MEC 调度提供。

2.2.1 分布式数据处理

在 MEC 架构中，不同的 MEC 服务器通常由不同的供应商提供，则各个 MEC 服务器的系统架构包括硬件（CPU、GPU 和缓存等）与软件（操作系统、身份验证系统和加密方式等）各不相同，整体呈现高度的异构性。通过将来自同一个数据源的数据处理任务交由多个异构的 MEC 服务器分别独立处理，使得即使在数据处理过程中受网络攻击且被攻击方成功篡改或窃取数据，也不会出现由于单一 MEC 服务器被入侵，导致其余 MEC 服务器被连锁攻破的情况，有效提高了系统的安全防御能力。

2.2.2 校验填充与裁决

在本文所提的架构体系中，由收发代理设备对来自数据源的流数据进行分割，并将分割后的数据段转发至不同 MEC 服务器进行处理。为了提高数据的安全性能，收发代理在各数据段中填充一定数量的校验数据，各个 MEC 服务器对真实数据与校验数据不作区分，进行同样的数据处理。在接收数据时，收发代理提取各个 MEC 服务器返回数据结果中的校验部分，并进行离群异常值检测和裁决。通过校验填充与裁决的方式，一方面，如果某个 MEC 服务器在执行过程中被篡改数据，由于校验数据同样被篡改而在检测中呈现离群异常特征，则收发代理会将该 MEC 服务器标记为不可信，并将被攻击篡改的数据段发送至其他可信的 MEC 服务器重新处理；另一方面，由于加入了校验填充，有效数据被窃取的概率也会随之降低。

2.2.3 调度与信任管理

通过对返回数据的校验部分进行离群异常值检测，收发代理可以有效检测出被攻击并被篡改了

数据的 MEC 服务器，通过该反馈信息，收发代理的决策模块可将该 MEC 服务器标记为不可信，在下一次传输中选择其他可信的 MEC 服务器作为转发目标。同时，收发代理可以通过记录历史受攻击情况，维护并管理各个 MEC 服务器的实时置信度。在每次传输过程中，调度置信度较高的数个 MEC 服务器，并为置信度较低的 MEC 服务器填充更多校验数据。

2.3　拟态防御 MEC 架构在监控视频图像处理中的应用

以监控视频图像处理的应用场景为例，监控系统将拍摄的视频交由收发设备后，将视频分割为图片集合，并插入一定数量的校验图片，这些校验图片由 MEC 服务器识别处理后的结果为确定值，并且 MEC 服务器不被告知校验图片的索引位置。完成校验图片的插入工作后，收发设备将所有图片分割为集合片段，转发至合作域内的多个 MEC 服务器进行图像识别处理，如摄像中出现人员的脸部识别。在 MEC 服务器完成处理后，将结果反馈至收发设备，收发设备首先提取校验图片的处理结果进行拟态裁决，然后判定是否存在导致图像处理结果失效的受攻击 MEC 服务器，最后将通过裁决的处理结果进行反馈，将受攻击影响的图片数据片段重发至可信的 MEC 服务器再次进行处理。

在执行图像识别处理的过程中，可能遭受的网络攻击包括：1) 攻击者窃取 MEC 服务器缓存的图片集合片段；2) 攻击者为了抹去图片中可能被识别出的可疑人员，为所有图片附加噪声以影响机器识别算法。对于第一种攻击方式，由于图片数据被转发至多个 MEC 服务器处理，数据的窃取缺乏连贯性；对于第二种攻击方式，由于攻击者无法确定校验图片的位置，攻击影响将同时作用于数据图片与校验图片，使得校验图片的处理结果出错，这点会在拟态裁决阶段被检测发现。因此，基于拟态防御原理的 MEC 架构在监控视频图像处理应用中能够有效提高图像数据的安全性。

3　系统模型

为了定量分析本文所提的 MEC 系统性能，将从资源开销与安全性能两个方面对系统进行数学建模。对于大数据处理应用场景而言，最主要的资源开销为时延成本，包括计算时延和传输时延两部分；而在安全性能方面，数据则面临被泄露与被篡改两方面的威胁，分别以泄露比率与逃逸概率进行量化。

3.1　资源模型

定义一个数据源产生的数据量为 D，假设整个 MEC 合作域（定义为 $\mathcal{E}_N$）中有 N 个可以协作的 MEC 服务器，由于每个 MEC 服务器的架构、性能以及需要并行处理的任务数量不同，可以分配的计算与传输资源也不同。对于第 $n\in\{1,2,\cdots,N\}$ 个 MEC 服务器，在第 k 次传输过程中，为该数据源分别分配 $c_k[n]$ 的计算资源与 $r_k[n]$ 的链路传输码率。

在第 k 次传输过程中，收发代理对数据进行分割后，基于一个预设方案（随机选择或基于置信度选择）选择其中 M 个 MEC 服务器（定义被选的服务器集合为 $\mathcal{C}_M\subseteq\mathcal{E}_N$）进行数据转发与处理。如果第 n 个 MEC 服务器被选中，则为其分配数据量 $s_k[n]$ 的片段，其中，真实数据为 $d_k[n]$、校验填充数据为 $p_k[n]$，否则不分配任何数据，即

$$s_k[n]=\begin{cases} d_k[n]+p_k[n], & n\in\mathcal{C}_M \\ 0, & \text{其他} \end{cases} \tag{1}$$

在本文所提的系统架构中，单次传输的总时延成本可以归纳为计算时延与传输时延两个部分。根据定义的资源模型，对于第 n 个 MEC 服务器在第 k 次数据传输过程中，用于计算收发代理分配的数据片段所消耗的时间为 $\tau_k^{cp}[n]=\dfrac{s_k[n]}{c_k[n]}$。为了最大程度保证数据校验的正确性，假定所有被选择的 M 个 MEC 服务器都完成数据处理并返回至收发代理进行校验后，再进行下一次数据传输。由于拟态裁决对各个 MEC 服务器的同步要求，每个 MEC 服务器传输时延成本都需要考虑双向传输信道，即 $\tau_k^{cm}[n]=2\dfrac{s_k[n]}{r_k[n]}$。系统单次传输的整体时延成本为

$$\begin{aligned} T_k &= \max\left\{\tau_k^{cp}[n]+\tau_k^{cm}[n]\right\} \\ &= \max\left\{\frac{s_k[n]}{c_k[n]}+2\frac{s_k[n]}{r_k[n]}\right\} \end{aligned} \tag{2}$$

3.2　安全模型

由于网络攻击手段繁复多样并且攻击复杂度日益增加，目前，对网络攻击的模型缺乏统一的标

准。假定一个以等概率攻击 MEC 合作域 $\mathcal{E}_N$ 内所有 MEC 服务器的攻击者，在第 k 次传输过程中，第 n 个 MEC 服务器受到该攻击者成功攻击的概率为 $\alpha_k[n]\in[0,1]$。

本文考虑两种数据攻击方式，具体包括：1) 数据篡改，根据拟态校验原理，对数据的篡改需要使得超过半数的 MEC 服务器同时被攻击成功且输出相同的错误校验结果；2) 数据泄露，如果攻击者攻击成功后仅窃取数据而不对数据作任何改动，则校验无法检测该类型攻击。由于收发代理每次传输都会动态选择不同的 MEC 集合，并且传输的数据中存在一定比例的填充数据，因此，泄露的数据比例将减少。

对于第一种攻击方式，将一次成功地、使超过半数 MEC 服务器输出相同的错误校验结果称为逃逸成功，即 $\{\text{逃逸成功}\}\triangleq\{\text{攻击成功数}\geqslant\left\lfloor\frac{M}{2}\right\rfloor+1\}$，则该事件的概率可以由式(3)获得。

$$\Pr\{\text{逃逸成功}\}=\sum_{j=\left\lfloor\frac{M}{2}\right\rfloor+1}^{M}\Pr\{\text{攻击成功数}=j\} \tag{3}$$

其中，定义任选 j 个 MEC 服务器的集合为 $\mathcal{Z}_j$，则在单次传输过程中，成功进行 j 次攻击的概率为

$$\Pr\{\text{攻击成功数}=j\}=\sum_{\mathcal{Z}_j\subseteq\mathcal{C}_M}\prod_{n\in\mathcal{Z}_j}\alpha_k[n]\prod_{n\notin\mathcal{Z}_j}(1-\alpha_k[n]) \tag{4}$$

特别地，如果攻击成功概率 $\alpha_k[n]=p_a$ 为定值，则式(4)可化简为 $C_M^j p_a^j(1-p_a)^{M-j}$，其中，C_M^j 为组合数。综合上述等式，最终得到在第 k 次传输过程中，攻击者进行一次逃逸成功的概率为

$$P_k^{\text{escape}}=\sum_{j=\left\lfloor\frac{M}{2}\right\rfloor+1}^{M}\sum_{\mathcal{Z}_j\subseteq\mathcal{C}_M}\prod_{n\in\mathcal{Z}_j}\alpha_k[n]\prod_{n\notin\mathcal{Z}_j}(1-\alpha_k[n]) \tag{5}$$

对于第二种攻击方式，攻击者在第 k 次传输过程中对所有目标发起攻击，可以窃取到的数据量为

$$R_k^{\text{leak}}=\sum_{n\in\mathcal{C}_M}\alpha_k[n]d_k[n] \tag{6}$$

对于产生数据量为 D 的数据源，系统整体数据泄露比率为

$$P^{\text{leak}}=\frac{1}{D}\sum_{k=1}^{K}R_k^{\text{leak}} \tag{7}$$

4 问题描述

基于上述系统资源开销与安全性能模型，讨论本文所提的系统架构相较于单个 MEC 服务器在无校验填充状态下的资源开销与安全性能的增益。由于在边缘计算领域的多个服务质量需求中，时延成本与安全可靠性为两个重要指标，本节将在时延开销与安全性能之间寻求优化权衡。

4.1 开销增益

在本文所提的架构中，系统的开销描述为处理数据源的全部数据量 D 所需要的时间。在仅考虑上述第一种攻击方式的情况下，舍去校验出错误的结果，并重传数据，则第 k 次传输过程中成功传输的平均数据量为

$$R_k^{\text{success}}=\sum_{n\in\mathcal{C}_M}(1-\alpha_k[n])d_k[n] \tag{8}$$

因此，完成全部数据处理所需要的传输次数 K 可以由式(9)得到

$$\sum_{k=1}^{K}R_k^{\text{success}}=D \tag{9}$$

对于选择的 M 个服务器，完成数据量 D 的数据处理所需要的合计时延成本为

$$\mathcal{T}=M\sum_{k=1}^{K}T_k \tag{10}$$

尽管用于对照的系统同样处于 MEC 服务器数量为 N 的 MEC 合作域，但仅将数据传输至主 MEC 服务器进行处理，则单 MEC 系统的数据处理时延成本定义为

$$\mathcal{T}'=\sum_{k=1}^{K'}T_k' \tag{11}$$

其中，由于单 MEC 系统没有校验填充（即 $s_k[1]=d_k[1]$）与拟态校验系统，传输时延开销仅需要考虑上行链路信道，则单次传输需要的时延为

$$T_k'=\frac{d_k[1]}{c_k[1]}+\frac{d_k[1]}{r_k[1]} \tag{12}$$

整体传输次数则由式(13)获得

$$\sum_{k=1}^{K'}d_k[1]=D \tag{13}$$

特别地，如果每次传输主 MEC 服务器分配给该任务的传输与计算资源相同，即 $c_k[1]=c_1$，$c_r[1]=r_1$，则单 MEC 系统的数据处理时间开销可以化简为

$$\mathcal{T}^{'}=\frac{r_1+c_1}{r_1c_1}\cdot\frac{D}{M} \tag{14}$$

最终开销增益定义为

$$\eta^{\text{cost}}=\frac{\mathcal{T}}{\mathcal{T}^{'}} \tag{15}$$

4.2　安全增益

多 MEC 架构相较于单 MEC 系统的安全增益同样从数据篡改与数据泄露两个方面进行讨论。对于单 MEC 系统，由于仅有一个 MEC 目标且没有校验填充，单次成功攻击即为成功逃逸，则对于数据篡改安全增益为

$$\eta^{\text{escape}}=\frac{1-\overline{P_k^{\text{escape}}}}{1-\overline{\alpha_k[1]}}=\frac{1-\dfrac{1}{K}\displaystyle\sum_{k=1}^{K}P_k^{\text{escape}}}{1-\dfrac{1}{K^{'}}\displaystyle\sum_{k=1}^{K^{'}}\alpha_k[1]} \tag{16}$$

从数据泄露角度来看，系统安全增益为

$$\eta^{\text{leak}}=\frac{1-\dfrac{1}{D}\displaystyle\sum_{k=1}^{K}R_k^{\text{leak}}}{1-\dfrac{1}{D}\displaystyle\sum_{k=1}^{K^{'}}\alpha_k[1]d_k[1]} \tag{17}$$

4.3　优化权衡

4.3.1　时延优化

根据系统模型中关于时延成本的讨论可知，单次传输的整体时延取决于被选择的 M 个服务器中计算传输链路时延最大值。因此，为了降低整体时延，收发设备分配给不同 MEC 服务器的数据片段长度应与其单位数据时延消耗成反比。若以主 MEC 服务器（即 n=1）为基准，则各个 MEC 服务器分配的数据长度可以通过式(18)获得

$$\begin{aligned}&\frac{s_k[n]}{c_k[n]}+2\frac{s_k[n]}{r_k[n]}=\frac{s_k[1]}{c_k[1]}+2\frac{s_k[1]}{r_k[1]}\\&\Rightarrow s_k[n]=\frac{r_k[n]c_k[n]}{r_k[1]c_k[1]}\frac{r_k[1]+2c_k[1]}{r_k[n]+2c_k[n]}s_k[1]\\&=\gamma_k[n]s_k[1]\end{aligned} \tag{18}$$

其中，$\gamma_k[n]=\dfrac{r_k[n]c_k[n]}{r_k[1]c_k[1]}\dfrac{r_k[1]+2c_k[1]}{r_k[n]+2c_k[n]}$ 为各个 MEC 服务器的相对单位数据时延消耗比。

4.3.2　安全优化

对网络攻击环境的分析基于以下 3 个假设：1) 在整个 MEC 合作域中，每个 MEC 服务器都时刻承受着被攻击的风险；2) 当一个 MEC 服务器被攻击后，其安全性能可以视为 0；3) 在经过清洗与重置等处理后，由于系统的架构不变，其安全性能可恢复至受攻击前的水平。

为了优化系统的安全性能，假设收发设备基于历史数据维护各个 MEC 服务器的信任参数，则设定置信度 $\beta_k[n]=1-\alpha_k[n]$，其中，$\alpha_k[n]$的估测基于经验数据。收发设备以置信度与相对时延消耗比乘积（$\beta_k[n]\gamma_k[n]$）最高作为策略，动态调度 MEC 服务器分发数据，同时根据置信比对每个数据片段填充校验数据。分发给各个 MEC 服务器数据片段中的有效数据长度为

$$d_k[n]=\beta_k[n]s_k[n]=(1-\alpha_k[n])\gamma_k[n]s_k[1] \tag{19}$$

5　仿真结果与分析

通过对多 MEC 架构进行仿真模拟，并以单 MEC 系统作为参照，针对时延成本与安全性能两方面进行分析。仿真所使用的数据源产生的数据量为 10^5 MB，交由合作域内多个 MEC 服务器处理，可协同的 MEC 服务器数量范围为[10,30]，且各个 MEC 服务器的计算能力在 5~10 Mbit/s 内随机分布，分配给该数据处理任务的传输码率则在 2~20 Mbit/s 内随机分布。为了便于对比，将单次传输中分配给主 MEC 服务器的片段数据量设定为 200 MB，同时，每次传输过程中 MEC 服务器的选择与分配数据量基于前文提出的最优策略。

时延开销与被选择 MEC 服务器数量 M 的关系如图 2 所示，蓝色线为系统时延开销，红色线为完成所有数据处理所需要的传输次数，实线为多 MEC 系统架构（可协同 MEC 服务器数量 $N=30$），虚线所表示的单 MEC 系统则作为参照。由图 2 可知，随着被选择 MEC 服务器数量 M 的增加，时延开销与传输次数都随之增加。由于拟态裁决需要等待数据回传到收发设备，所以计算了两倍的传输时延。同时，加入的校验数据与重传机制导致有效传输比例下降，需要更多的传输次数。

安全性能与被选择 MEC 服务器数量 M 的关

系如图 3 所示，蓝色线表示逃逸概率，红色线表示泄露比率，黑色虚线表示作为参照的单 MEC 系统。随着 M 的增加，多 MEC 系统的泄露比率稳步下降，而逃逸概率在 M 达一定数量后无限趋近于 0。由于仿真数据量的限制，当 M 为 6 时，系统几乎不会漏判被篡改的数据，安全性能得到大幅度提升。因此，多 MEC 系统在增加 40%~50% 的时延成本下，可以大幅度提升数据处理的安全可靠性。

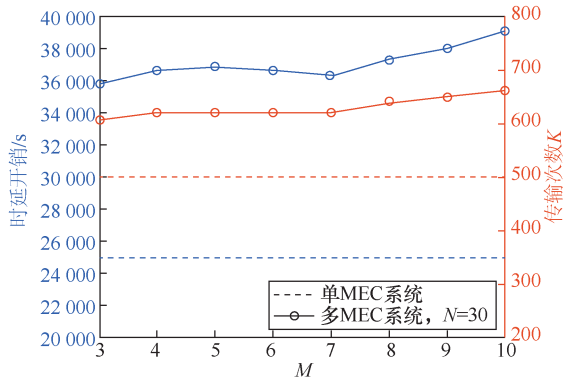

图 2　时延开销与被选择 MEC 服务器数量 M 的关系

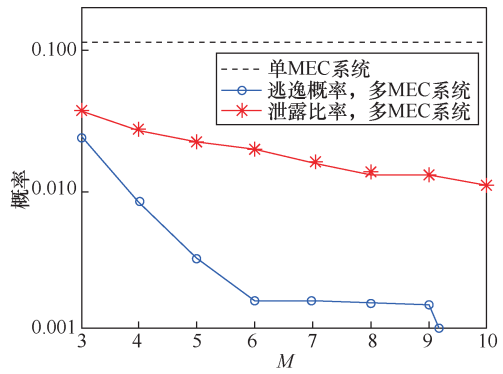

图 3　安全性能与被选择 MEC 服务器数量 M 的关系

可协同 MEC 服务器数量 N 对系统的影响如图 4 所示，蓝色线表示时延开销，两条红色线则分别表示系统的逃逸概率与数据泄露比率。设定被选择的 MEC 服务器数量 M 为 5，而可协同的 MEC 服务器数量 N 则从 10 增加到 30。由图 4 可知，当 M 不变时，随着 N 的增加，系统时延开销、安全性能没有明显变化。因此，当 MEC 合作域内有足够可协同的 MEC 服务器数量 N 时，则 N 的增加不会对数据处理业务产生影响，业务的性能主要取决于每次传输过程中选择协作的 MEC 服务器数量。

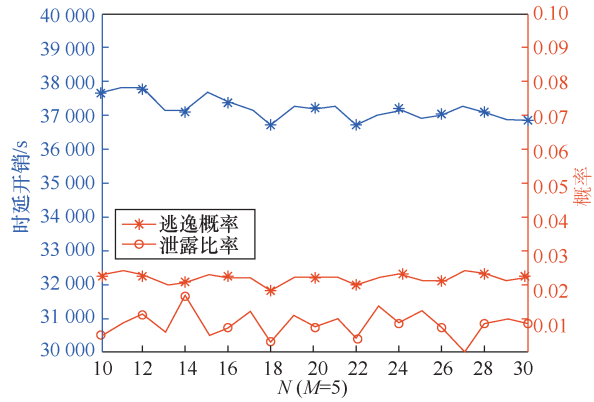

图 4　可协同 MEC 服务器数量 N 对系统的影响

6　结束语

针对多 MEC 服务器协同处理大数据业务的应用场景，提出了基于拟态防御原理的分布式数据处理方案，给出了合理的系统架构与执行步骤，并对系统的资源消耗与安全性能进行了数学建模与优化权衡分析，通过仿真模拟对该系统架构的开销与性能进行验证与分析。仿真结果表明，随着被选择 MEC 服务器数量 M 的增加，系统的逃逸概率大幅度下降，数据泄露比率也稳步下降，并且该安全性能的提升所增加的时延成本在可接受的范围内。因此，所提出的分布式处理方案可以在增加一定时延成本的情况下，有效提升系统的安全性能，从而保证 MEC 服务器进行大数据处理业务的安全性与可靠性。此外，整个 MEC 合作域内可协同的 MEC 服务器数量对系统性能没有显著影响，业务的处理主要取决于每次传输过程中选择协同的 MEC 服务器数量。在未来的工作中，将针对监控视频边缘图像处理等实际应用进行理论研究与系统开发实践，把该分布式数据处理方案落于实处。

参考文献：

[1] KEKKI S, FEATHERSTONE W, FANG Y, et al. MEC in 5G networks[S]. 2018.

[2] NDIKUMANA A, TRAN N H, HO T M, et al. Joint communication, computation, caching, and control in big data multi-access edge computing[J]. IEEE Transactions on Mobile Computing, 2019: 1.

[3] TALEB T, SAMDANIS K, MADA B, et al. On multi-access edge computing: a survey of the emerging 5G network edge cloud architecture and orchestration[J]. IEEE Communications Surveys &Tutorials, 2017, 19(3): 1657-1681.

[4] SHI W, CAO J, ZHANG Q, et al. Edge computing: vision and challenges[J]. IEEE Internet of Things Journal, 2016, 3(5): 637-646.

[5] CESELLI A, FIORE M, FURNO A, et al. Prescriptive analytics for MEC orchestration[C]//2018 IFIP Networking Conference (IFIP Networking) and Workshops. IEEE, 2019: 1-9.

[6] 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.
WU J X. Research on cyber mimic defense[J]. Journal of Cyber Security, 2016, 1(4): 1-10.

[7] 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.

[8] 庞建民, 张宇嘉, 张铮, 等. 拟态防御技术结合软件多样化在软件安全产业中的应用[J]. 中国工程科学, 2016, 18(6): 74-78.
PANG J M, ZHANG Y J, ZHANG Z, et al. Applying a combination of mimic defense and software diversity in the software security industry[J]. Engineering Science, 2016, 18(6): 74-78.

[9] 常箫, 张保稳, 张莹. 一种面向网络拟态防御系统的信息安全建模方法[J]. 通信技术, 2018, 51(1): 165-170.
CHANG X, ZHANG B W, ZHANG Y. Information security modeling method for CMD systems[J]. Communications Technology, 2018, 51(1): 165-170.

[10] 李宁波, 赫凌俊, 谢彬, 等. 基于主动防御的高安全分布式存储系统研究[J]. 信息技术与信息化, 2018(8): 185-188.
LI N B, HAO L J, XIE B, et al. Research on high security distributed storage system based on active defense[J]. Information Technology & Informatization, 2018(8): 185-188.

[11] 周清雷, 冯峰, 朱维军. 基于功能切片的拟态防御体系结构及安全等级评估方法[J]. 通信学报, 2018, 39(z2): 99-109.
ZHOU Q L, FENG F, ZHU W J. Mimic defense organization structure based on functional slice and method of evaluating security level[J]. Journal on Communications, 2018, 39(z2): 99-109.

[作者简介]

朱泓艺（1990– ），男，上海人，博士，上海宽带技术及应用工程研究中心助理研究员，主要研究方向为下一代无线通信技术、边缘计算及信息安全技术。

陆肖元（1975– ），男，上海人，教授级高级工程师，上海宽带技术及应用工程技术研究中心副主任、上海浦东临港智慧城市发展中心主任，主要研究方向为宽带网络与智慧城市应用等相关领域。

李毅（1965– ），男，浙江绍兴人，博士，博士生导师，上海宽带技术及应用工程研究中心主任，主要研究方向为宽带网络与大数据技术及应用等相关领域。