

基于信息安全强度的路侧设备任务调度优化策略

苏北坡^{1,2}, 代亮^{1,2}, 巨永锋¹

(1. 长安大学电子与控制工程学院, 陕西 西安 710064; 2. 长安大学车联网教育部-中国移动联合实验室, 陕西 西安 710018)

摘要: 车路协同系统中, 车辆由于自身计算资源局限性将任务卸载至路侧设备(RSU)进行执行, 然后由RSU考虑在本地处理任务或将任务卸载至云端的“车-边-云”架构, 是近年来受到广泛关注的边缘计算新模式。由于“边-云”侧无线信道的开放接入以及不确定性, 需要增加安全机制来保证数据传输的可靠性, 然而增加安全机制会使RSU的计算负载增加, 进而使得RSU的能耗增加。针对如何在满足任务时延约束条件下优化路侧设备能耗及信息安全效用, 提出了车路协同系统下路侧设备基于能耗-队列均衡的联合任务调度及加密优化(EPTS), 并建立车速状态模型、任务加密模型、数据缓存队列模型、任务计算模型及优化目标函数。利用李雅普诺夫优化理论将优化问题模型进行转化, 并将转化后的模型描述为背包问题进行求解, 仿真结果验证了所提出的EPTS具有较好的收敛性和有效性, 平均目标价值优于平均分配策略17%, 优于任务队列长度加权分配策略21%。

关键词: 车路协同系统; 路侧设备; 能耗; 信息安全效用; 李雅普诺夫

中图分类号: TN92

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2024027

Task scheduling optimization strategy for roadside unit based on security strength

SU Beipo^{1,2}, DAI Liang^{1,2}, JU Yongfeng¹

1. School of Electronics and Control Engineering, Chang'an University, Xi'an 710064, China

2. The Joint Laboratory for Internet of Vehicles, Ministry of Education-China Mobile Communications Corporation, Chang'an University, Xi'an 710018, China

Abstract: In the context of cooperative vehicle-infrastructure systems (CVIS), vehicles often offload computational tasks to roadside units (RSUs) for execution due to their own constrained computing resources. A novel approach that has garnered increased attention involves the “vehicle-edge-cloud” framework, wherein RSUs decide whether

收稿日期: 2023-11-10; 修回日期: 2024-03-19

通信作者: 代亮, ldai@chd.edu.cn

基金项目: 国家重点研发计划项目 (No.2021YFB2601401); 长安大学中央高校基本科研业务费专项资金 (No.300102323201)

Foundation Items: The National Key Research and Development Program of China (No.2021YFB2601401), Special funds for basic Research Operations in Central Universities of Chang'an University (No.300102323201)

引用格式: 苏北坡, 代亮, 巨永锋. 基于信息安全强度的路侧设备任务调度优化策略[J]. 网络与信息安全学报, 2024, 10(02): 106-120.

Citation Format: SU B P, DAI L, JU Y F. Task scheduling optimization strategy for roadside unit based on security strength[J]. Chinese Journal of Network and Information Security, 2024, 10(02): 106-120.

to process tasks locally or to offload them to the cloud. The open and unpredictable nature of the wireless channels on the “edge-cloud” interface necessitates the incorporation of a security mechanism to safeguard the integrity of information transmission. However, integrating such a security mechanism can escalate the energy consumption of RSUs. Addressing the challenge of jointly optimizing roadside energy consumption and information security utility, without compromising task delay constraints, is a complex issue. To tackle this, an energy-packets queue tradeoff of task scheme and encryption strategy (EPTS) was introduced. This approach involved the development of a vehicle speed state model, a task encryption model, a data cache queue model, and a task calculation model, along with the formulation of an optimization objective function. The optimization model was subsequently transformed using Lyapunov optimization theory and was reformulated as a knapsack problem for resolution. The simulation results confirm the EPTS's commendable convergence and effectiveness. The average objective value achieved by the proposed EPTS was found to be 17% superior to that of the Equal Allocation Strategy (EAS) and 21% superior to the queue-weighted strategy (QS).

Keywords: cooperative vehicle-infrastructure system, roadside units, energy consumption, information security utility, Lyapunov

0 引言

随着车联网 (Internet of vehicle, IoV) 技术的发展, 车载端所产生的数据量以及数据类型也日趋复杂^[1]。然而, 车辆自身计算资源有限, 无法满足计算密集型车载应用的计算要求, 从而导致交通事故、用户体验质量降低等问题^[2-3]。为解决上述问题, “车一边一云”架构被提出, “车一边一云”架构通过云端和路边单元为智能车辆提供所需计算资源, 云端和路边单元联合处理车载任务, 保证了任务的实时性^[4-5]。车路协同系统作为未来智慧城市建设的重要组成部分之一^[6-7], 配备计算资源的路侧设备可以将接收到的车载应用数据卸载至与基站相连的云端处理, 也可以在本地处理后通过实时通信进行信息交互, 提高了车辆与基础设施之间的协同性, 以此保证系统资源的高效利用, 提高道路交通效率以及增强道路交通安全等^[8-10]。

“车一边一云”架构的提出, 极大地缓解了车载端的计算压力, 然而由于“车一边一云”架构下, 无线信道的开放接入及不确定性, 车辆和路侧设备 (roadside unite, RSU) 在进行任务传输的过程中可能会发生隐私泄露等安全风险^[11-12]。道路上的车辆中可能会存在潜在的恶意攻击者^[13-15]。车辆及RSU卸载的任务中可能包含车辆的上下文信息, 如位置、速度、方向等。一些恶意攻击者窃听收集到这些信息后可以精准攻击, 导致车辆相撞甚至造成人员伤亡。而且收集

到的数据可能会被提供或发布给第三方, 以供数据收集者挖掘数据的潜在商业价值^[16]。当车辆为RSU以及云端提供的有偿资源服务进行付费时, 用户ID以及账户密码等私密信息的泄露会导致财产安全问题。因此, 应在“车一边一云”架构下增加安全机制, 以保证信息传输的保密性、真实性、完整性等安全防护。

在“车一边一云”架构下, 控制中心需要决策任务应在RSU进行本地处理或将任务卸载至云端处理, 任务仅在本地处理时, RSU的计算资源及能耗约束可能会导致任务处理时延较长。卸载至云端处理可以减轻RSU端的计算负载, 然而无线信道的不确定性可能会使RSU卸载任务所需能耗及时延更大, 且增加的安全机制消耗了额外的计算资源及能耗, 对联合优化路侧端能耗及信息安全效用提出了更大的挑战。本文考虑通过动态时变应用场景下的任务调度及加密优化决策来解决上述问题。本文主要贡献如下。

(1) 考虑一个联合优化路侧端能耗以及信息安全效用问题。该问题可以拆解为对任务处理调度、信道分配、加密块长度的优化问题, 对上述问题进行联合优化以获得最优的信息安全效用以及路侧端能耗。任务的处理时延约束应考虑车辆在RSU通信范围的驻留时间。

(2) 针对多RSU的联合优化问题, 提出了一种最小化目标价值的任务调度及加密策略EPTA。该策略通过多个RSU的数据缓存队列状态、任务到达状态、信道状态及通信环境状态得

到任务调度及加密决策,根据多个RSU的队列状态、任务到达状态、信道状态及通信环境状态的变化,动态地决定路侧端本地处理及卸载至云端的任务数量和加密块长度。最小化路侧端能耗以及最大化信息安全效用,从而保证系统性能。

(3) 将任务调度及加密问题解耦为3个子问题,并分别对其求解,从而得到原问题的最优解,仿真实验结果验证了该算法的有效性,与其他方案相比,本文所提出的方案具有较大的性能优势。

1 相关工作

联网车辆基础设施内的路侧设备容易受到安全和接入控制挑战。RSU可能与不可靠的服务供应商(service providers, SP)共享资源,不安全的消息传递基础设施可能会导致信息泄露。为了缓解这些问题,Albouq等^[17]引入了一种自动服务提供机制,该机制支持使用分布式安全框架(distributed security framework, DSF)的受控消息传递基础设施。服务提供是通过为RSU提供发布/订阅代理来完成的,这些发布/订阅代理使授权的SP能够将其服务作为主题分发,并通过DSF定义访问权限。DSF充当由雾计算节点托管的安全中间层,以确保与RSU非常接近,能够处理资源授权,并提供RSU和SP的身份验证。

在车辆通信网络(vehicle to everything, V2X)范围内,交换的安全/警告消息的性质使其本身高度依赖于位置,因此它通常用于事件报告。如车辆需要定期交换包括速度、时间和位置信息的信标消息。报告的位置信息必须准确、真实。为了减轻位置欺骗/伪造攻击带来的潜在风险,将多天线RSU作为雷达和无线收发器。Abdelaziz等^[18]集成RSU中的雷达功能使其利用到达角估计作为物理层身份验证方案,以交叉验证检验所报告的位置信息的准确性、真实性。

Narayanadoss等^[19]考虑了一种被称为交叉火力攻击的新型安全攻击,它涉及大量受危害的节点,这些节点以时间协调的方式产生低强度的流量,使得目标链路或主机(受害者)与网络的其余部分断开连接。由于攻击流量与合法流量难以区分,因此检测此类攻击具有挑战性。在支持动态网络监控和流量特征提取的软件定义网络下,

作者开发了一个机器学习模型,该模型可以学习流经智能交通系统(intelligent transportation system, ITS)网络流量之间的时间相关性,从而区分合法流量和攻击流量。为了保证时间敏感型信息的安全计算和事件驱动消息的快速处理,Gupta等^[20]提出了基于车载边缘计算的层次化框架。安全分析表明,该框架可以显著提高功耗,缓解可追溯性、身份隐私保护、重放攻击、拒绝服务攻击、冒充攻击等安全问题。Chang等^[21]提出了一种新的Sybil攻击检测机制,该机制在保留车辆位置隐私的同时,利用车辆的轨迹进行识别。Sybil攻击是指利用社交网络中的少数节点控制多个虚假身份,从而利用这些虚假身份控制或影响网络中大量正常节点。

在车载自组织网(vehicular ad hoc network, VANET)中,为了提高车辆的安全性和保障位置隐私,确定事件消息的可信度近年来受到了极大的关注。在这些研究中,可信度决策的准确性和时延都是重要的议题。Wei等^[22]提出了一个基于路侧设备和信标的信任管理系统,该系统旨在快速地按比例分配消息意见,并阻止内部攻击者在隐私增强的VANET中发送或转发伪造的消息。Kumar等^[23]提出了一种VANET通信的安全方法,以抵御使用RSU的恶意操作或攻击。随着VANET的发展,RSU间通信网络的可靠性和稳定性已成为一个关键问题。Tang等^[24]利用级联故障模型来模拟网络的级联故障过程,同时利用进化算法对网络进行进化,从而可以获得综合性能相对最好的网络。Ashritha等^[25]提出了一种车载到RSU、车载到车载的轻量级认证方案,构建了一个安全的通信系统。在该系统中,作者利用了时间戳的方法,降低了在高密度交通区域进行认证的计算代价。车辆的隐私是通过不透露其真实身份来保护的。

随着新兴的通信和计算技术的出现,IoV已成为一种新的范式,使车辆能够与RSU以及其他车辆进行通信,以收集或交换信息。然而,IoV的固有特性,如车辆的高机动性和边缘节点有限的存储容量,给开发缓存方案带来了许多困难。因此,Safavat等^[26]提出了一种新的改进的多项式回归神经网络分类器和2CK-ECC(caesar combined key-based elliptic curve cryptography)算法

来预测IoV的车辆移动性、安全性和内容缓存。

在IoV中, 由于车辆计算能力是有限的, 为了保证低响应延迟, 任务卸载是必要的^[27]。为了有效地卸载任务, 互联车辆 (connected vehicles, CV) 需要将速度、位置等上下文信息上传到RSU和基站, 这给CV的隐私安全带来了巨大的威胁和风险。针对上述问题, Wang等^[16]提出了一种隐私保护的车辆边缘计算系统架构。CV可能会受到黑洞攻击, 即通过伪造到目的地节点的有吸引力的路线来欺骗合法节点。当攻击者向源节点发送确认存在新路由的数据包时, 就会发生以上这种情况。Albouq等^[28]提出了一种黑洞检测协议, 该协议工作在分成簇的高速公路上, 并由RSU监控, 以检测单个和合作的黑洞攻击。每个RSU的任务是在合法节点报告的身份验证违规和可疑路线建立活动之后, 对各自的高速公路路段执行黑洞攻击的检测和隔离。

随着IoV的发展, 物联网 (Internet of things, IoT) 与人工车辆的融合已成为ITS的必然选择。在ITS中, IoT使用开放的通道互联网与其他IoV、RSU和云服务器进行无线通信。上述参与实体及其通信技术的开放性带来了参与实体之间安全漏洞、数据隐私、透明度、可验证性、可扩展性和数据完整性等挑战。为了应对这些挑战, Kumar等^[29]提出了一个基于隐私保护的车联网安全框架 (privacy-preserving based secured framework for Internet of vehicles, P2SF-IoV)。P2SF-IoV融合了区块链和深度学习技术来克服上述挑战, 并在这两个模块上工作。

智慧城市车载通信中的信息安全传输仍是一项具有挑战性的任务。大多数相关工作采用了公钥基础设施, 即证书吊销列表 (certification revocation lists, CRL), 以确保车载通信中的安全性和隐私性。然而, 这些工作遇到了一些问题, 如: 检查过程耗时长, CRL庞大; 通过链接未加密的基本安全消息进行可追溯性攻击; 攻击者从停放的车辆或RSU的存储中提取密钥。为了解决上述问题, Othman等^[30]提出了一种使用物理不可克隆函数的物理安全的隐私保护消息认证协议——秘密共享。该协议即使在内存泄露的情况下也能保证车载通信中的安全性、隐私性不

受被动和主动攻击。

安全广播信息的低延迟和高可靠性对于未来的ITS至关重要。Thota等^[31]首先提出一种新的安全广播系统模型, 以满足车间通信 (vehicle to vehicle, V2V) 应用的延迟和可靠性要求。其次, 基于一个真实的系统级模拟器, 使用该模型对不同车联网技术 (C-V2X和IEEE 802.11p) 下的不同车辆密度在城乡场景中的性能进行了综合评估。与其他提出的标准重复码相比, 使用应用层Raptor Q码进一步提高了系统性能。Zhang等^[32]提出了一种车辆移动和信道动态感知方案, 以适应车载网络并提高学习性能。这一新方案使RSU能够选择合适的车辆, 并对本地模型进行加权平均。

从上述相关研究可知, 大多数研究工作主要是考虑在V2V的通信环境中, 提高信息安全性, 并解决在动态环境中的信息泄露问题。然而, 很少有学者考虑联合优化路侧设备的能量消耗和信息安全效用问题、车辆车速的不确定性以及不同车辆到达率对系统性能的影响。因此本文提出了基于能耗—队列均衡的联合任务调度及加密优化策略, 能够实时在线优化算法以解决上述问题。

2 系统模型

车路协同系统下多RSU研究场景如图1所示, 在一段高速路段沿途均匀部署了 N 个路侧设备和一个基站, 路侧设备配备了数据收发装置、处理单元、存储单元。考虑到计算资源受限的车辆难以处理计算密集型任务, 路侧设备可以接收途经车辆的计算任务, 并将任务存入缓存区。任务可以交给路侧端的处理单元进行处理, 也可以卸载至与基站相连的云端进行处理, 将处理结果存储至存储单元并发送至车辆, 以此保障车辆的智能驾驶安全性, 提高交通运行效率。

在“车一边一云”架构中, 由于网络的动态 $s_n(t)$ 拓扑、信道时变等特性, 任务信息的传输存在一定的安全风险, 可能会遭受恶意攻击, 产生信息泄露 (如车辆位置信息、车辆与用户的私密信息) 等问题, 因此保证网络的安全性是十分有必要的。

将系统时间离散为等长的时隙 τ , 每个时隙开始时, RSU将到达的任务数据存入缓存区。任

务调度控制器根据多个 RSU 的队列状态、信道状态、车辆到达率做出任务处理决策。

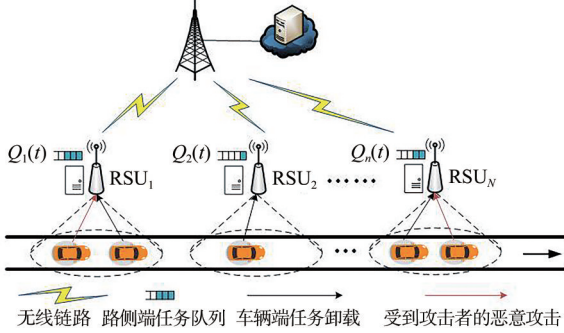


图1 车路协同系统下多RSU研究场景
Figure 1 Research scenario of Multi-RSUs in CVIS

路侧设备本地处理任务及卸载任务至云服务器都会消耗能量，且将多个 RSU 的本地处理单元计算功率设定为相同的固定值。当路侧设备仅在本地处理单元处理任务时，能量开销较低，信息安全等级高。随着车辆到达率的增加，由于本地计算资源有限，数据缓存队列产生积压，排队时延变长，任务处理可能不及时。当路侧设备卸载任务至云服务器时，能够有效降低任务队列长度，缓解本地计算压力，但考虑信道状态以及通信环境状态的不确定性，任务的传输可能会导致较大的能量消耗以及较高的信息泄露风险，因此在满足长期平均队列长度约束及任务时限要求下，联合优化长期平均能耗及信息安全效用是本文关注的问题，目的是提高能量效率，以保证在

有限的能量以及更安全的信息传输环境下可以有更多的计算任务被处理。针对上述问题本文提出基于能耗—队列均衡的联合任务调度及加密优化策略。

如图2所示，在每个时隙开始时，任务调度控制器根据多个 RSU 的任务队列状态和信道状态来决定任务分组的处理方式以及加密方式。多 RSU 任务调度与加密决策模型如图2所示，由通信环境状态 $K_n(t)$ 、任务到达状态 $h_n(t)$ 、数据缓存队列状态 $Q_n(t)$ 、信道状态 $r_n(t)$ 、传输调度决策变量 $d_n(t)$ 及加密决策 $s_n(t)$ 组成。

2.1 车速状态模型

设定车辆行驶在高速公路上，在单一车道的车辆到达服从参数为 λ 的泊松分布，推导得到相邻车辆到达时间间隔 Δt 服从负指数分布，其概率密度函数如下：

$$f(t) = \lambda e^{-\lambda t} (t > 0) \quad (1)$$

根据概率密度函数推导可得：

$$F(t) = P(\Delta t \leq t) = 1 - e^{-\lambda t} (t > 0) \quad (2)$$

因此，在 τ 时隙内至少有一辆车到达该路段的概率为：

$$P_v = P(\Delta t \leq \tau) = 1 - e^{-\lambda \tau} (\tau > 0) \quad (3)$$

给出在 τ 时隙内没有车辆到达该路段的概率为 $1 - P_v$ 。

设定 $v(t)$ 为车辆在 t 时隙到达时的速度，并假设车辆在路段内的行驶速度恒定。在自由流交

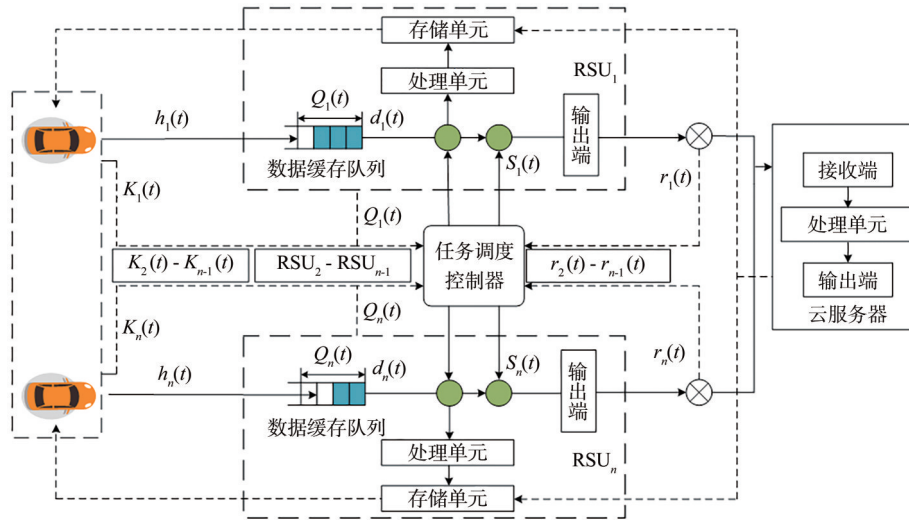


图2 多RSU任务调度与加密决策模型
Figure 2 RSUs task scheduling and encryption decision model

通状态下, 车速 $v(t)$ 服从均值为 $\bar{V}$, 标准差为 σ 的正态分布, 其概率密度函数为:

$$f_v(v) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\left(\frac{v-\bar{V}}{\sigma\sqrt{2}}\right)^2} \quad (4)$$

高速的限速区间表示为 $[V_{\min}, V_{\max}]$, 则车速分布的截断概率密度函数为:

$$f'_v(v) = \frac{2f_v(v)}{\operatorname{erf}\left(\frac{V_{\max}-\bar{V}}{\sigma\sqrt{2}}\right) - \operatorname{erf}\left(\frac{V_{\min}-\bar{V}}{\sigma\sqrt{2}}\right)} \quad (5)$$

将连续的车速离散为 $X+1$ 个车速状态^[33]。其状态向量表示为 $V = [V_1, \dots, V_{X+1}]$, 其中 $V_1 = V_{\min}$ 和 $V_{X+1} = V_{\max}$ 分别表示高速的最低限速和最高限速, 且满足 $V_x < V_{x+1}$ ($x = 1, 2, \dots, X$)。 $y_n(t)$ 表示在 t 时隙车辆到达 RSU_n 的车速状态, $y_n(t) = x$ ($1 \leq x \leq X$) 表示 $v(t) \in [V_{x+1}, V_x]$, 此外, $y_n(t) = X+1$ 表示 t 时隙 RSU_n 内没有车辆到达。

令 δ_x 表示车辆处于车速状态 x 的概率, 其概率密度函数表达式为:

$$\delta_x = P\{y_n(t) = x\} = \begin{cases} P_v \int_{V_{x+1}}^{V_x} f'_v(v) dv, & 1 \leq x \leq X \\ 1 - P, & x = X+1 \end{cases} \quad (6)$$

2.2 任务加密模型

在开放接入的信道条件下, 路侧设备将任务卸载至云端时, 可能会有来自车辆的恶意攻击, 使得任务数据泄露, 造成不必要的安全隐患, 因此采取有效的加密算法对任务信息进行加密, 能够有效提高任务传输的私密性及安全性。相较于非对称加密算法, 对称加密算法简单、高效且快速, 更适用于“车一边一云”架构场景。

针对不同的加密算法, 可能存在多种不同方式的恶意攻击, 因此如何量化信息安全性, 使得其具备普适性是一项挑战。从另一个角度出发, 通过攻击者破解加密块的能力(攻击强度)来衡量信息安全级别。准确来说, 攻击者破解一定长度加密块的能力与概率质量函数(PMF)有关。攻击强度参数为 γ , $\Pr(\gamma = L)$ 表示攻击者破解块长度为 L 的加密块密码的概率。攻击强度为 γ 的攻击者能够在有效时间内以较小的代价破解任何长度小于 γ 的加密块密码。因此, $\Pr(\gamma = L)$ 同样能够表示加密帧被破解从而导致信息泄露的概

率。信息泄露的概率可以看作帧脆弱性, 则帧脆弱性的概率为 $\vartheta = \Pr(\gamma = L) = \Pr(\gamma \geq L)$ 。

在时隙 t , 控制器决策 RSU_n 以 $s_n(t)$ 的块长度进行加密传输, 将任务卸载至云端。其中 $s_n(t) \in \{L_0, \dots, L_i, \dots, L_I\}$, L_i , L_0 分别表示加密系统中最大和最小可用块长度。攻击车辆的攻击强度可以描述为: $1/(L_I - L_0)$, 且攻击车辆处于 RSU_n 通信范围内且成功破解长度为 $s_n(t)$ 加密块密码的概率服从均匀分布, 可以得到在时隙 t , RSU_n 卸载任务时帧脆弱性的概率表达式为:

$$\vartheta_n(t) = \Pr(\gamma \geq L) = \frac{L_I - s_n(t)}{L_I - L_0} \quad (7)$$

由此可知, 帧脆弱性的概率越低, 信息传输越安全, 即信息安全的强度越高, 因此信息的安全性可以被量化为 $1 - \vartheta_n(t)$ ^[34]。当路侧设备的通信范围内车辆密度较大时, 可能会有多个攻击车辆, 因此在时隙 t , RSU_n 卸载任务至云端的信息安全强度可以表示为:

$$U_n(t) = (1 - \vartheta_n(t))^{\nu_n^a(t)} = \left(\frac{s_n(t) - L_0}{L_I - L_0} \right)^{\nu_n^a(t)} \quad (8)$$

$\nu_n^a(t) = K_n(t) \cdot \rho$, 其中 ρ 表示路侧设备通信范围内攻击车辆密度, $K_n(t)$ 表示在时隙 t , RSU_n 通信环境状态。且 $K_n(t) \in [I_{\min}, I_{\max}]$, 并将其划分为 Y 个状态, 表示为 $I_{\max} = K_{n,1} > K_{n,2} > \dots > K_{n,Y-1} > K_{n,Y} = I_{\min}$ 。 $K_n(t) = y$ 表示信道状态为 y , 即可通信车辆数量处于区间 $[K_{n,y-1}, K_{n,y}]$ 。根据文献[35], 推导得到通信环境状态的概率密度函数为:

$$\begin{aligned} P\{K_n(t) = y\} &= \sum_{k=y}^{\infty} C_y^k [p_k(t)]^y [1 - p_k(t)]^{k-y} \cdot \frac{(\lambda t)^k e^{-(\lambda t)}}{k!} \quad (9) \\ &= \frac{[\lambda t \cdot p_k(t)]^y e^{-(\lambda t) \cdot p_k(t)}}{y!} \end{aligned}$$

为优化信息安全性及服务质量(QOS), 提出信息安全效用模型如下:

$$\psi_n(t) = \frac{r_n^{\text{trans}}(t)}{8s_n(t)} \lg(8s_n(t)) \cdot U_n(t) \quad (10)$$

$r_n^{\text{trans}}(t)$ 表示在时隙 t , RSU_n 卸载任务至云端的传输速率。

2.3 任务缓存队列调度模型

车辆途经 RSU_n 通信范围时, 会将一部分难

以处理的计算任务卸载至路侧设备, 考虑车辆能源充足, 为保证信息安全性及较短的传播时延, 采用较大的发射功率向路侧设备卸载任务。RSU_n将接收到的计算任务存入任务缓存队列后, 控制器作出任务调度及处理决策。设决策变量 $d_n(t) = \{d_n^l(t), d_n^o(t)\}$ 。

$d_n^o(t)$ 表示在时隙 t , RSU_n 是否将数据缓存队列中的任务卸载至云服务器。 $d_n^o(t) \in \{0, 1\}$, $d_n^o(t) = 1$ 表示在时隙 t , RSU_n 将卸载一个任务至云服务器, $d_n^o(t) = 0$ 表示在时隙 t , RSU_n 在本地处理任务, 且满足 $\sum_{n=1}^N d_n^o(t) \leq 1$ 。

$d_n^l(t)$ 表示在时隙 t , RSU_n 本地处理任务的数量。由于路侧端的计算资源是有限的, 因此在一个时隙内可以处理的最大任务数量可以表示为 $S = \lceil \tau/T_l \rceil$ 。同时任务处理数量不应超过任务队列长度 $Q_n(t)$, 定义 $T_n(t) = \min\{S, Q_n(t)\}$, 可得出系统的任务处理数量应满足如下关系:

$$0 \leq d_n^l(t) \leq T_n(t), 1 \leq n \leq N \quad (11)$$

考虑车路协同系统中存在多个 RSU 同时处理任务的情况, 综合考虑车路协同系统中所有 RSU 的任务处理持续时间约束, 给出系统总体的任务处理持续时间约束条件为:

$$\sum_{n=1}^N d_n^l(t) \leq N \cdot S \quad (12)$$

考虑路侧设备的数据队列的最大缓存容量为 J 个任务分组, 每个任务的大小为 Z , 令 $Q_n(t+1)$ 表示 RSU_n 在 $t+1$ 时隙的任务队列长度, 给出其队列更新表达式如下:

$$Q_n(t+1) = \max\{Q_n(t) - B_n(t) + h_n(t), 0\} \quad (13)$$

$h_n(t)$ 表示在时隙 t , 到达 RSU_n 的任务分组数。考虑到车速较快的车辆在路侧设备通信范围内的驻留时间较短, 车辆能够卸载的任务量较少, 因此车辆卸载的任务数量与车速具有相关性。根据车速状态模型, 在时隙 t 的任务到达状态 $h_n(t)$ 被划分为 $X+1$ 个状态, 且满足 $h_x < h_{x+1}$, $x \in \{1, 2, \dots, X+1\}$, 其中 $h_{X+1} = 0$ 表示没有车辆到达且没有任务被卸载。

$B_n(t)$ 为 RSU_n 在 t 时隙处理的业务数量, 其表达式为:

$$B_n(t) = d_n^o(t) + d_n^l(t) \quad (14)$$

任务队列过长会产生较大的任务排队时延, 因此系统给定 ϖ 作为长期平均任务缓存队列长度的上限。其表达式如下:

$$\lim_{T \rightarrow \infty} \frac{1}{T} \sum_{t=0}^{T-1} E\{Q_n(t)\} \leq \varpi \quad (15)$$

2.4 任务计算模型

根据任务处理的场景不同, 将任务计算模型分为本地处理模型和云处理模型。

本地处理模型。已知本地计算资源的计算频率为 f_l , 处理单元的运算功率为 P_l , 处理任务所要求的处理密度为 c , 即单位数据量所需 CPU 周期数, 则路侧端在本地处理一个任务所需的处理时延可表示为:

$$T_l = \frac{8Z \cdot c}{f_l} \quad (16)$$

本地处理一个任务所需能耗 $e^l = P_l \cdot T_l$ 。

云处理模型。路侧设备通过无线传输的方式将任务卸载至附近与基站相连的云服务器, 云服务器计算完毕后将任务结果传回至路侧设备。

考虑卸载任务至云端时, 路侧设备需要对任务进行加密处理, 加密频率为 f_l^{en} , 加密所需运算功率为 P_l^{en} , 则路侧设备在本地对一个任务进行加密处理所需时延可表示为:

$$T_l^{\text{en}} = \frac{8Z \cdot c}{f_l^{\text{en}}} \quad (17)$$

加密所需能耗可表示为:

$$e^{\text{en}} = P_l^{\text{en}} \cdot T_l^{\text{en}} \quad (18)$$

信道状态通过块衰落模型进行量化表示, 考虑信道状态在一个时隙内保持不变, 且在不同时隙独立同分布。考虑到 RSU_n 的地理位置以及环境因素, 假定信道路径增益 $r_n(t) \in [R_{\min}, R_{\max}]$, 并将其划分为 W 个状态, 表示为 $R_{\max} = r_{n,1} > r_{n,2} > \dots > r_{n,W-1} > r_{n,W} = R_{\min}$ 。 $r_n(t) = w$ 表示信道状态为 w , 即信道增益处于区间 $[r_{n,w-1}, r_{n,w}]$ 。信道状态的概率密度函数表示为:

$$\Pr\{r_n(t) = w\} = \theta_w, w \in \{1, \dots, W\} \quad (19)$$

其中 $\theta_w \in [0, 1]$, 且 $\sum_{w=1}^W \theta_w = 1$ 。

令 P_r 表示在时隙 t , RSU_n 卸载任务至云端所需传输功率。已知带宽为 B , 噪声功率为 N_0 , 基

于香农公式推导出RSU_n的传输速率为：

$$r_n^{\text{trans}}(t) = B \lg \left(1 + \frac{P_r \cdot r_n(t)}{N_0} \right) \quad (20)$$

则传输能耗可表示为：

$$e_n^{\text{trans}}(t) = P_r \cdot \frac{8Z}{r_n^{\text{trans}}(t)} \quad (21)$$

路侧端任务卸载所需能耗为：

$$e_n^{\text{off}}(t) = e_n^{\text{trans}}(t) + e^{\text{en}} \quad (22)$$

系统通过任务调度优化策略得到RSU_n任务处理数量 $d_n^l(t)$ 以及卸载决策 $d_n^o(t)$ 。RSU_n的计算功率 P_l 已知，因此可以推导出RSU_n在时隙 t 的能量消耗，进而得到所有RSU在时隙 t 消耗的总能量 $E(t)$ ，其表达式为：

$$E(t) = \sum_{n=1}^N [e^l \cdot d_n^l(t) + e_n^{\text{off}}(t) \cdot d_n^o(t)] \quad (23)$$

本文的优化目标是联合优化路侧端平均能耗及信息安全效用，即在路侧端能耗最小化的同时能够最大化信息安全效用。

目标函数如下：

$$O(t) = \varepsilon_1 E(t) - \varepsilon_2 d_n^o(t) \psi_n(t) \quad (24)$$

最终的优化目标如下：

$$\begin{aligned} \min_{d_n^l(t), d_n^o(t), s_n(t)} O(t) \\ \text{s.t.} \quad & \begin{cases} s_n(t) \in \{L_0, \dots, L_i, \dots, L_I\} & C_1 \\ d_n^o(t) \in \{0, 1\} & C_2 \\ \sum_{n=1}^N d_n^o(t) \leq 1 & C_3 \\ 0 \leq d_n^l(t) \leq T_n(t), 1 \leq n \leq N & C_4 \\ \sum_{n=1}^N d_n^l(t) \leq N \cdot S & C_5 \\ \lim_{T \rightarrow \infty} \frac{1}{T} \sum_{t=0}^{T-1} E\{Q_n(t)\} \leq \varpi & C_6 \end{cases} \end{aligned} \quad (25)$$

3 基于李雅普诺夫优化的任务调度模型

李雅普诺夫优化是一种具有自主学习能力的控制算法，能够根据当前时隙的状态实时进行判定和自适应网络状态，并实时地制定动态卸载策略。由于第2部分所提出优化问题的决策变量较多，而且维度较大，在线优化的计算复杂度很高，为降低模型的计算复杂度，需要基于李雅普诺夫优化理论将优化问题模型进行转换。设定向量矩阵 $\mathbf{G}(t) = [Q_n(t)]$ 。通过该矩阵定义李雅普

诺夫函数：

$$L(G(t)) = \frac{1}{2} \sum_{n=1}^N Q_n(t)^2 \quad (26)$$

由式(26)可知数据队列长度和 $L(G(t))$ 的数值呈正相关，将系统时隙 t ， $t+1$ 时的数据队列动态变化过程描述为系统在两时隙前后的李雅普诺夫函数差值，即李雅普诺夫漂移量 $\Delta(G(t))$ ，其表达式如下：

$$\Delta(G(t)) = E\{L(G(t+1)) - L(G(t)) | G(t)\} \quad (27)$$

此外，为了在虚拟队列稳定的条件下，解决优化问题，增加了漂移加惩罚函数，则式(27)可以被改写为：

$$\Delta(G(t)) + VE\{O(t) | G(t)\} \quad (28)$$

其中， $V > 0$ ，作为数据队列长度和目标函数之间的tradeoff参量，若 V 数值增加，则目标函数在李雅普诺夫漂移参量中的权重就增加，对系统的漂移性影响也随之增大。所以系统可以通过调节 V 的数值，达到系统目标优化的作用。优化思路为推导李雅普诺夫漂移量的上界，通过最小化上界，达到系统优化目的。

根据定理对于 $\forall a, b, c > 0$ ，有 $\{\max[(a - b + c), 0]\}^2 \leq (a - b + c)^2$ 成立，由式(13)得出如下不等式：

$$\frac{1}{2} Q_n(t+1)^2 \leq \frac{1}{2} Q_n(t)^2 + \frac{1}{2} (h_n(t) - B_n(t))^2 + Q_n(t)(h_n(t) - B_n(t)) \quad (29)$$

根据式(26)，可以推导出如下关系：

$$\begin{aligned} \Delta(G(t)) &\leq \frac{1}{2} \sum_{n=1}^N E\{(h_n(t) - B_n(t))^2 | G(t)\} + \\ &\sum_{n=1}^N Q_n(t) E\{(h_n(t) - B_n(t)) | G(t)\} \end{aligned} \quad (30)$$

令 $h^{\max}$ 表示 $h_n(t)$ 的最大值， $B^{\max}$ 表示 $B_n(t)$ 的最大值，可以得到如下关系式：

$$\begin{aligned} \sum_{n=1}^N E\{(h_n(t) - B_n(t))^2 | G(t)\} &\leq \\ \sum_{n=1}^N \max\{(h^{\max})^2, (B^{\max} - h^{\max})^2\} \end{aligned} \quad (31)$$

将参量 $\text{Cons} = N \max\{(h^{\max})^2, (B^{\max} - h^{\max})^2\} / 2$

代入式(31)中，可以得到如下关系式：

$$\begin{aligned} \Delta(G(t)) + VE\{E'(t)|G(t)\} \leq \text{Cons} + \\ \sum_{n=1}^N Q_n(t) E\{(h_n(t) - B_n(t))|G(t)\} + \\ VE\{[\varepsilon_1 e^l \cdot d_n^l(t) + \varepsilon_1 d_n^o(t) e_n^{\text{off}}(t) - \\ \varepsilon_2 d_n^o(t) \psi_n(t)]|G(t)\} \end{aligned} \quad (32)$$

系统可以通过最小化式 (32) 的右侧来解决目标函数最小化问题, 其中, 不等式右端即李雅普诺夫漂移函数值的上界, 令该上界最小化即可实现在系统稳定的前提下, 通过任务调度决策 $d_n(t)$ 及加密决策 $s_n(t)$ 求得优化模型的最优临界点。系统的优化模型如下:

$$\begin{aligned} \min_{d_n^l(t), d_n^o(t), s_n(t)} \text{Cons} + \sum_{n=1}^N Q_n(t) (h_n(t) - B_n(t)) + \\ V \sum_{n=1}^N [\varepsilon_1 e^l \cdot d_n^l(t) + \varepsilon_1 d_n^o(t) e_n^{\text{off}}(t) - \varepsilon_2 d_n^o(t) \psi_n(t)] \end{aligned} \quad (33)$$

其中, Cons, $h_n(t)$ 在每个时隙内均为常量, 系统结果不受其影响, 因此可将其省略, 式 (33) 简化后如下:

$$\begin{aligned} \min_{d_n^l(t), d_n^o(t), s_n(t)} \sum_{n=1}^N d_n^l(t) (V \varepsilon_1 e^l - Q_n(t)) + \\ \sum_{n=1}^N d_n^o(t) (V \varepsilon_1 e_n^{\text{off}}(t) - V \varepsilon_2 \psi_n(t) - Q_n(t)) \end{aligned} \quad (34)$$

3.1 最优信道分配决策

考虑多个 RSU 的信道状态是动态变化的, 不同信道状态下路侧设备卸载任务所需能耗不同, 为权衡多个 RSU 的队列与能耗, 以保证在长期平均队列约束的条件下最小化路侧端长期平均能耗。首先假定一个合理的加密决策向量 $\mathbf{S} = \{s'_n(t)\}$, 令 $\Omega_n(t) = Q_n(t) + V \varepsilon_2 \psi_n(t, s'_n(t)) - V \varepsilon_1 e_n^{\text{off}}(t)$, 将信道分配问题描述为:

$$\begin{aligned} \max_{d_n^o(t)} \sum_{n=1}^N d_n^o(t) \cdot \Omega_n(t) \\ \text{s.t.} \begin{cases} d_n^o(t) \in \{0, 1\}, 1 \leq n \leq N \\ \sum_{n=1}^N d_n^o(t) \leq 1 \end{cases} \end{aligned} \quad (35)$$

式 (35) 的最优解可以表示为:

$$d_n^o(t) = \begin{cases} 1, & \Omega = \arg \max_{n \in N} \Omega_n(t) \\ 0, & \text{其他} \end{cases} \quad (36)$$

3.2 最优加密决策

为保证在开放通信环境下, RSU 在信息安全

等级较高的条件下卸载更多的有用信息至云端处理。已知最优信道分配决策向量, 将信息加密问题描述为:

$$\begin{aligned} \max_{s_n(t)} \sum_{n=1}^N d_n^o(t) \cdot \psi_n(t) \\ \text{s.t. } s_n(t) \in \{L_0, \dots, L_i, \dots, L_I\} \end{aligned} \quad (37)$$

式 (37) 的最优解可以表示为:

$$s_n(t) = \begin{cases} L_i, & \psi = \arg \max_{i \in I} \psi_n(t), d_n^o(t) = 1 \\ 0, & d_n^o(t) = 0 \end{cases} \quad (38)$$

3.3 最优本地任务处理决策

将本地任务处理决策问题描述为:

$$\min_{d_n^l(t)} \sum_{n=1}^N d_n^l(t) \cdot (V \varepsilon_1 e^l - Q_n(t)) \quad (39)$$

令 $\sigma_n(t) = Q_n(t) - V \varepsilon_1 e^l$, 则系统优化模型被描述为:

$$\begin{aligned} \max_{d_n^l(t)} \sum_{n=1}^N d_n^l(t) \cdot \sigma_n(t) \\ \text{s.t.} \begin{cases} 0 \leq d_n^l(t) \leq T_n(t), 1 \leq n \leq N \\ \sum_{n=1}^N d_n^l(t) \leq N \cdot S \\ \lim_{T \rightarrow \infty} \frac{1}{T} \sum_{t=0}^{T-1} E\{Q_n(t)\} \leq \varpi \end{cases} \end{aligned} \quad (40)$$

该优化模型的目的是在有限的资源空间下 (任务处理数量受约束), 实现模型的价值最大化。因此背包问题适用于解决该条件下的问题。

在背包问题中, 系统优化模型的系统价值由 $\sigma_n(t)$ 表示, 系统首先将 $\sigma_n(t)$ 的值降序排列, 再按顺序依次放入 “背包” 中。该过程可以被中断, 根据其中断时的系统状态即可获得系统优化问题的最优解。

定义 φ 为系统背包问题的中断指标参数, 且 $\varphi = \{\phi_1, \phi_2\}$, 其中 ϕ_1, ϕ_2 满足如下关系式:

$$\begin{cases} \phi_1 = \arg \min_n \sum_{j=1}^n T_j(t) \geq N \cdot S \\ \phi_2 = \arg \min_n \sigma_n(t) < 0 \end{cases} \quad (41)$$

任务调度决策 $d_n^l(t)$ 最优解如下:

$$d_n^l(t) = \begin{cases} T_n(t) & , n < \varphi \\ \min \left\{ N \cdot S - \sum_{n=1}^{\varphi-1} T_n(t), T_\varphi(t) \right\} & , n = \varphi \\ 0 & , \text{其他} \end{cases} \quad (42)$$

4 仿真分析

本节通过 MATLAB 仿真软件对实际环境进行模拟仿真实验与分析,对本文基于能耗—队列均衡的联合任务调度及加密优化策略进行仿真实验。首先根据系统模型分别绘制出系统平均目标价值,任务分组队列长度以及信息安全效用随着参数变化的曲线图像;其次,为了验证算法的有效性,通过建立消融实验,来研究各个决策变量对模型产生的影响;最后在仿真参数不变的情况下,将本文策略模型与目前较为常用的两种任务调度策略:平均分配策略(equal allocation strategy, EAS)和任务队列长度加权分配策略(queue-weighted strategy, QS),在系统平均目标价值以及任务分组排队方面进行仿真对比。本文策略模型的高速公路参数遵循 3GPP TR 36.885 中的设置,车辆到达 RSU 通信范围的数量服从泊松分布,车辆移动速度服从高速限速区间的高斯分布。仿真参数设置如表 1 所示。

表 1 仿真参数
Table 1 Simulation parameter

参数名称	符号/单位	参数值
本地计算频率	f_i/GHz	2.5
加密计算频率	f_i^{en}/GHz	5.1
处理密度	$c/(\text{gigacycles}/\text{Mbits})$	0.15
本地 CPU 功率	P_i/W	70
CPU 加密运行功率	P_i^{en}/W	75
传输功率	P_r/W	100
带宽	$B/\text{Mbit}\cdot\text{s}^{-1}$	8
限速区间	$[V_{\min}, V_{\max}]/(\text{m}\cdot\text{s}^{-1})$	$[16.67, 33.33]$
速度期望	$\bar{V}/(\text{m}\cdot\text{s}^{-1})$	25
速度标准差	σ	5.56
时隙长度	τ/s	1
任务大小	Z/MB	1

另外,系统时间 T 设置为 1 500 s,攻击车辆密度 ρ 为 0.1,数据队列最大缓存容量 J 为 100 个,RSU 的数量 N 设置为 5 个。

系统性能指标为平均目标价值以及任务队列长度,平均目标价值为路侧设备能耗与信息安全

效用的差值。上述性能指标代表系统的优劣性。指标越低代表系统性能越好,信息安全效用则代表密码性能的优劣性,数值越高密码性能越好。

本文考虑与长期目标价值相比,系统长期平均目标价值上下浮动较为稳定,能更好地衡量调度策略的性能。在保证长期平均队列稳定的条件下,降低系统长期平均目标价值能够显著提升系统性能。

在 4.3 节对比实验中,平均分配策略指所有 RSU 在本地的任务处理时长是相等的,且该策略能够使卸载任务至云端的概率相等;任务分组排队长度加权分配策略指系统根据 RSU 中任务分组排队长度来分配在本地的任务处理时长以及卸载任务至云端的权重,RSU 任务分组排队长度越长,则权重越大,RSU 将任务卸载至云端的概率越大。

4.1 系统性能仿真实验

图 3 显示了在不同权重 V 下系统平均目标价值的变化。通过仿真结果可以得到,当权重 V 增加时,系统平均目标价值降低,这是因为随着权重 V 的增加,平均目标价值对系统性能的影响逐渐增大,因此为了得到更好的系统性能,系统会自适应地降低平均目标价值。图 4 显示了任务队列长度在不同权重 V 下的变化,权重 V 的增加会相对降低队列长度对系统性能的影响。为了保证系统平均目标价值更低,系统倾向不处理或少处理任务。然而,这样决策产生的结果即任务队列长度增加。

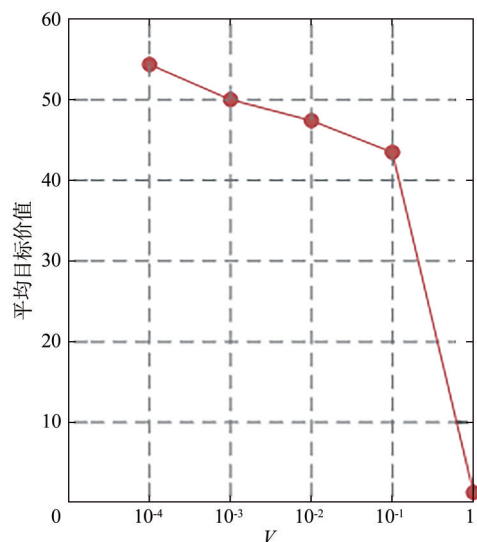


图 3 平均目标价值随权重变化趋势

Figure 3 The trend of average objective value changing with weight

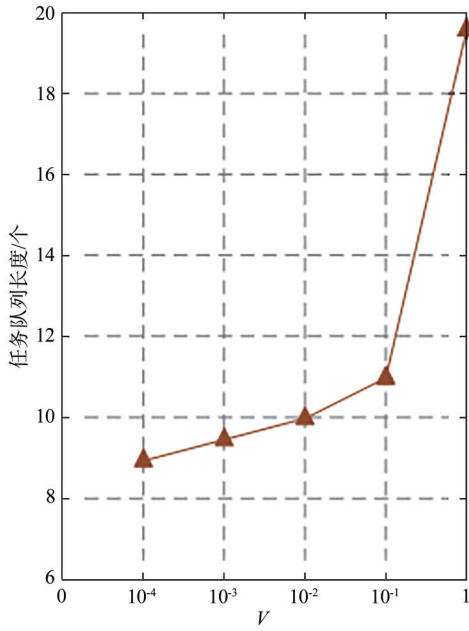


图4 任务队列长度随权重变化趋势

Figure 4 The trend of task queue changing with weight

当系统所处环境不同时, 车辆到达率也会出现相应的变化, 考虑到车辆到达率与RSU的任务到达以及通信环境状态具有相关性, 更多的车辆到达会使得RSU的任务队列以及通信环境保持在一个较高的状态。因此需要对本系统的任务调度及加密优化策略能否在不同车辆到达率的条件下自适应进行任务调度及加密优化进行验证, 以保证该策略具有在线优化的能力以及鲁棒性。具体实验方案及结果分析如下。

实验方案给出车辆到达率不同时, 平均目标价值以及任务队列长度的相应变化, 设置权重 $V = 0.01$ 。实验结果如图5~图6所示, 由图6可知, 随着车辆到达率的增加, 系统的平均任务队列长度增加, 则平均排队时延会相应地增加, 因此系统需要消耗能量处理更多的任务分组以及卸载任务至云端。更多的车辆到达会产生较多的攻击车辆, 使得信息安全效用下降, 因此长期平均目标价值相应增加。

当任务队列过长时, 系统处理任务会产生很高的排队时延, 并且过高的排队时延会降低任务处理效率, 从而造成任务处理超时和任务处理失败等问题。因此系统设定队列长度不应超过阈值

$$\varpi = \alpha_0 \frac{t_d}{0.5 \cdot (T_i + Z/\bar{r}_n^{\text{trans}})}, \quad \text{即} \quad \lim_{T \rightarrow \infty} \frac{1}{T} \sum_{t=0}^{T-1} E\{Q_n(t)\} \leq$$

ϖ 。其中 t_d 为任务截止时限, 为保证冗余量给出权重系数 α_0 。由图5~6可知, 系统在不同的车辆到达率下, 系统平均目标价值和任务队列长度能够进行动态调整, 且最终呈收敛趋势, 该结果表明本文提出的基于能耗——队列均衡的联合任务调度及加密优化策略 (energy-packets queue length tradeoff of task scheme and encryption algorithm, EPTA) 能够根据任务到达率的变化, 动态调整任务调度策略, 从而保证系统的稳定性。

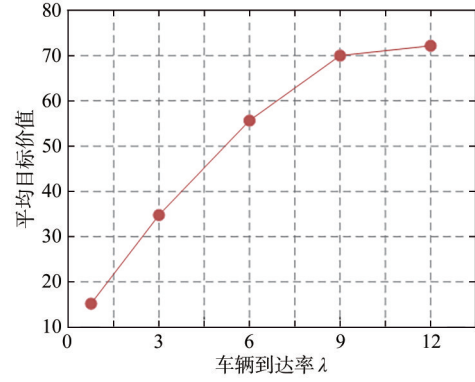


图5 平均目标价值随车辆到达率变化趋势

Figure 5 The trend of average objective value with vehicle arrival rate

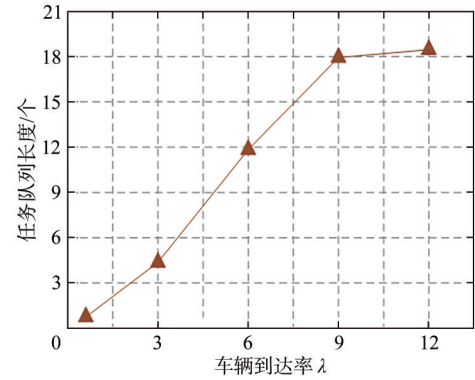


图6 任务队列随车辆到达率变化趋势

Figure 6 The trend of task queue with vehicle arrival rate

为了验证系统在动态的环境变化条件下, 加密算法在不同参数变化下对系统性能产生的影响。在最大加密块长度、权重 V 和车辆到达率变化的条件下, 对平均目标价值及信息安全效用进行仿真实验, 具体实验。实验结果如图7~9所示, 由图7可知, 随着最大加密块长度的增加, 系统的信息安全强度 $U_n(t)$ 会降低, 因此长期平均目标价值相应地增加。系统在不同的最大加密块长度条件下, 通过任务调度及加密优化策略进

行动态调整,使得平均目标价值最终呈收敛趋势。由图8可知,信息安全效用随着权重 V 的增大而降低。这是由于随着权重 V 不断降低,系统更倾向于不处理或少处理任务。使得任务很少卸载至云端,触发任务加密机制的次数较少,因此信息安全效用也会随之降低。图9显示随着车辆到达率的不断提高,信息安全效用会逐渐下降。由此可知,随着车辆到达率提高,RSU通信范围内的攻击车辆数量增加,攻击强度的增加会使得信息安全效用降低,而本文提出的策略能够在车辆到达率成倍上升的情况下,保证信息安全效用的下降幅度较小,因此该策略具备一定的鲁棒性。

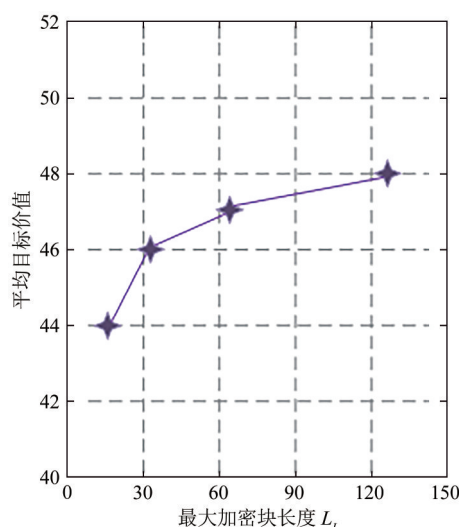


图7 平均目标价值随最大加密块长度变化趋势

Figure 7 The trend of average objective value with the maximum encryption block length

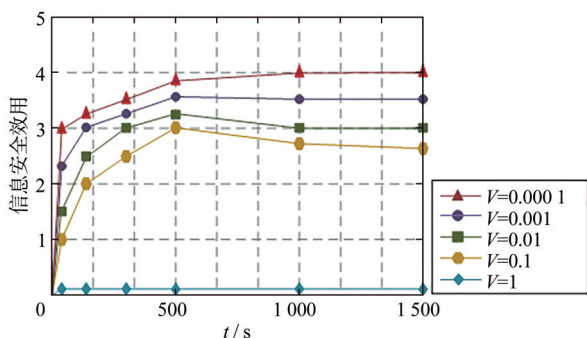


图8 信息安全效用随权重 V 变化曲线

Figure 8 Variation curve of information security utility with weight V

4.2 消融实验

本文根据提出的3个模块进行了3组消融实验。3个模块分别为信道分配决策 (channel allo-

cation decision, CAD) 模块、加密决策 (encryption decision, ED) 模块以及本地任务处理决策 (local task processing decision, LTPD) 模块,每个模块将对应的决策算法替换为基准算法。通过对3个模块与原模型进行对比实验,验证各改进决策的有效性。对比结果如图10~图11所示。

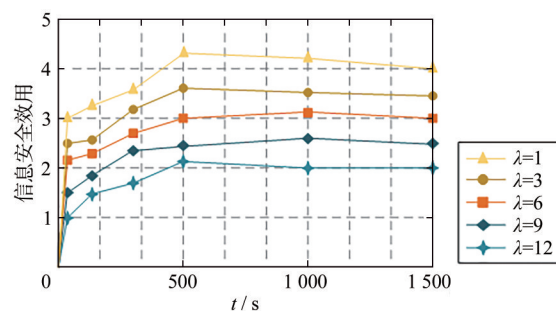


图9 信息安全效用随车辆到达率变化曲线

Figure 9 Variation curve of information security utility with vehicle arrival rate

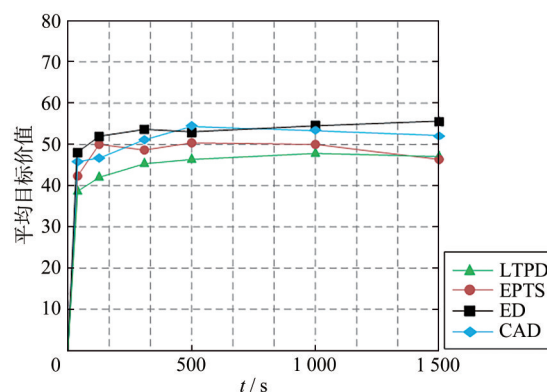


图10 平均目标价值在不同模块下的对比

Figure 10 Comparison result diagram of average objective value under different modules

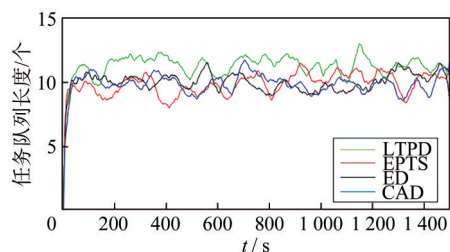


图11 任务队列长度在不同模块下的对比

Figure 11 Comparison result diagram of task queue length under different modules

由图10~图11可知,原模型与CAD模型相比,任务队列长度差距较小,而平均目标价值降低了10%,因此信道分配决策算法相较于基准算法能够有效地降低平均目标价值;原模型与ED模

型相比,任务队列长度差距较小,而平均目标价值降低了 19%,因此加密决策算法相较基准算法,有效降低了平均目标价值;原模型与 LTPD 模型相比,平均目标价值相差较小,而任务队列长度降低了约 18%,因此本地任务处理决策算法相较基准算法能够有效降低任务队列长度。

4.3 对比实验

本文将 EPTS 与 EAS、QS 进行对比仿真实验,证明 EPTS 的优势。实验设置权重 $V = 0.01$ 。对比仿真实验结果如图 12~图 15 所示。

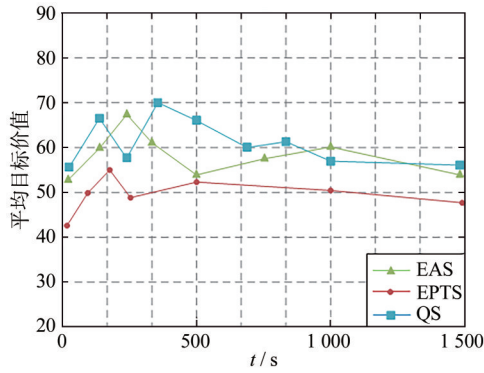


图 12 平均目标价值在不同算法下的对比
Figure 12 Comparison result diagram of average objective value under different algorithms

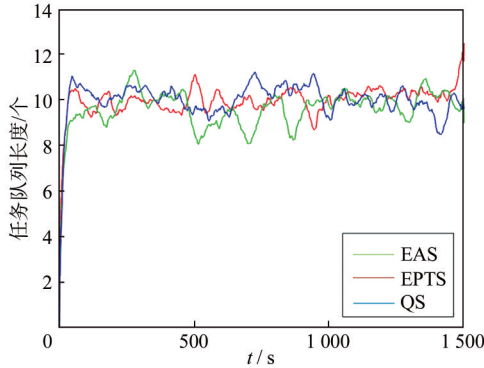


图 13 任务队列长度在不同算法下的对比
Figure 13 Comparison result diagram of task queue length under different algorithms

由图 12~13 可知,相较其他策略,在任务队列长度差距较小的情况下, EPTS 的系统平均目标价值是最低的。图 14 显示了随着车辆到达率的增加, EPTS 得出的结果始终处于最优,而通过图 15 可以看到在不同 RSU 工作功率的条件下, EPTS 得出的平均目标价值均低于其他两种策略。因为 EPTS 策略能够根据经过车辆的到达率、信道状态以及任务队列的长度动态地调整本地处理

任务数量、信道选择以及加密块长度决策,从而提高系统的工作效率。而 EAS 在面对复杂环境中信道状态以及任务队列长度时,无法及时调整决策,从而对其性能造成了影响。QS 也仅从队列长度对系统进行了优化。因此本文提出的 EPTS 相较于这两种策略具有较为明显的优势。

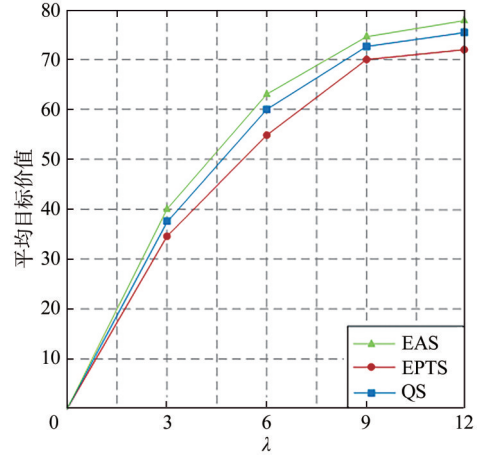


图 14 平均目标价值在不同算法下随车辆到达率变化的对比
Figure 14 Comparison of average objective value with vehicle arrival rate under different algorithms

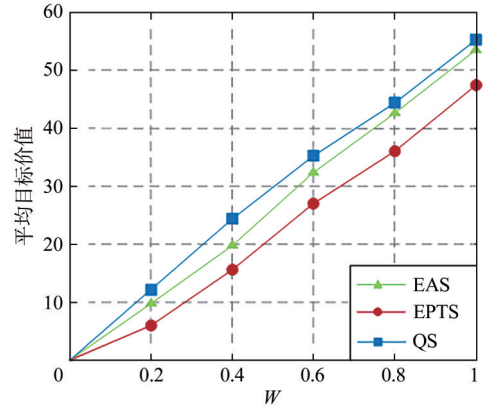


图 15 平均目标价值在不同算法下随 RSU 工作功率变化的对比
Figure 15 Comparison of average objective value with RSU working power under different algorithms

5 结束语

本文研究了车路协同系统下的多 RSU 分布式任务调度及加密优化问题,提出了一种使得路侧端能耗最小及信息安全效用最大的任务调度及加密策略。该策略根据高速路段上的多个 RSU 的车辆到达概率、缓存队列长度、信道状态和通信环境状态作出任务调度及加密决策。本文基于李雅普诺夫优化理论对该问题进行转化,并引入

李雅普诺夫漂移参量及权重来权衡系统平均目标价值和任务队列长度, 最后将其转化为“背包”问题进行求解。该方法能够通过多个RSU车辆到达概率、缓存队列长度、信道状态以及通信环境状态的实时变化, 动态地调整任务调度及加密策略, 从而保证任务结果在截止日期前下发至车辆, 且实现任务调度过程中路侧端长期平均能耗最小化、信息安全效用最大化。本文的假设中, 车辆到达在高速路段的单个车道服从到达率为 λ 的泊松分布, 考虑车辆的到达率在多个车道独立同分布, 即多车道的车辆到达数量可以表示为单个车道的多次叠加。在仿真实验中, 本文提出的EPTA在到达率较高时, 系统性能变化较小, 因此EPTS同样适用于多车道场景。仿真结果表明本文提出的EPTS在任务队列长度与EAS及QS接近的情况下, 路侧端平均目标价值优于EAS 17%, 优于QS 21%。

在下一步的研究中, 会考虑更多环境变化因素对任务调度算法造成的影响, 目的是还原更加现实的研究场景。

参考文献:

- [1] GARG S, KAUR K, KADDOUM G, et al. Sec-IoV: a multi-stage anomaly detection scheme for Internet of vehicles[C]//Proceedings of the ACM MobiHoc Workshop on Pervasive Systems in the IoT Era. New York: ACM, 2019: 37-42.
- [2] 李兴华, 钟成, 陈颖, 等. 车联网安全综述[J]. 信息安全学报, 2019, 4(3): 17-33.
LI X H, ZHONG C, CHEN Y, et al. Survey of Internet of vehicles security[J]. Journal of Cyber Security, 2019, 4(3): 17-33.
- [3] 梁广俊, 王群, 辛建芳, 等. 移动边缘计算资源分配综述[J]. 信息安全学报, 2021, 6(3): 227-256.
LIANG G J, WANG Q, XIN J F, et al. Survey of mobile edge computing resource allocation[J]. Journal of Cyber Security, 2021, 6(3): 227-256.
- [4] XUN Y J, QIN J M, LIU J J. Deep learning enhanced driving behavior evaluation based on vehicle-edge-cloud architecture[J]. IEEE Transactions on Vehicular Technology, 2021, 70(6): 6172-6177.
- [5] 张伟成, 卫红权, 刘树新, 等. 5G移动边缘计算场景下的快速切换认证方案[J]. 网络与信息安全学报, 2022, 8(3): 154-168.
ZHANG W C, WEI H Q, LIU S X, et al. Fast handover authentication scheme in 5G mobile edge computing scenarios[J]. Chinese Journal of Network and Information Security, 2022, 8(3): 154-168.
- [6] 陈超, 吕植勇, 付姗姗, 等. 国内外车路协同系统发展现状综述[J]. 交通信息与安全, 2011, 29(1): 102-105, 109.
CHEN C, LYU Z Y, FU S S, et al. Overview of the development in cooperative vehicle-infrastructure system home and abroad[J]. Journal of Transport Information and Safety, 2011, 29(1): 102-105, 109.
- [7] CAO D P, WANG X, LI L X, et al. Future directions of intelligent vehicles: potentials, possibilities, and perspectives[J]. IEEE Transactions on Intelligent Vehicles, 2022, 7(1): 7-10.
- [8] 贾鹏, 冯明月, 张志超. 智能车路协同系统发展现状与趋势[J]. 军事交通学院学报, 2014, 16(2): 39-42.
JIA P, FENG M Y, ZHANG Z C. Survey on intelligent vehicle and road cooperation system[J]. Journal of Military Transportation University, 2014, 16(2): 39-42.
- [9] 郭戈, 许阳光, 徐涛, 等. 网联共享车路协同智能交通系统综述[J]. 控制与决策, 2019, 34(11): 2375-2389.
GUO G, XU Y G, XU T, et al. A survey of connected shared vehicle-road cooperative intelligent transportation systems[J]. Control and Decision, 2019, 34(11): 2375-2389.
- [10] CHEN C, YAO G R, LIU L, et al. A cooperative vehicle-infrastructure system for road hazards detection with edge intelligence[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(5): 5186-5198.
- [11] 陈璐, 汤红波, 游伟, 等. 移动边缘计算安全防御研究[J]. 网络与信息安全学报, 2021, 7(1): 130-142.
CHEN L, TANG H B, YOU W, et al. Research on security defense of mobile edge computing[J]. Chinese Journal of Network and Information Security, 2021, 7(1): 130-142.
- [12] 沈剑, 周天祺, 王晨, 等. 面向边缘计算的隐私保护密钥分配协议[J]. 网络与信息安全学报, 2021, 7(1): 93-100.
SHEN J, ZHOU T Q, WANG C, et al. Privacy protection key distribution protocol for edge computing[J]. Chinese Journal of Network and Information Security, 2021, 7(1): 93-100.
- [13] GAO C, WANG G, SHI W S, et al. Autonomous driving security: state of the art and challenges[J]. IEEE Internet of Things Journal, 2022, 9(10): 7572-7595.
- [14] HALEEM M, MATHUR C, CHANDRAMOULI R, et al. Opportunistic encryption: a trade-off between security and throughput in wireless networks[J]. IEEE Transactions on Dependable and Secure Computing, 2007, 4(4): 313-324.
- [15] 邓慧娜, 叶阿勇, 刘燕妮, 等. 移动边缘计算中隐私感知的在线任务卸载机制[J]. 信息安全学报, 2023, 8(4): 126-138.
DENG H N, YE A Y, LIU Y N, et al. Privacy-aware online task offloading mechanism in mobile edge computing[J]. Journal of Cyber Security, 2023, 8(4): 126-138.
- [16] WANG S P, LI J, WU G J, et al. Joint optimization of task offloading and resource allocation based on differential privacy in vehicular edge computing[J]. IEEE Transactions on Computational Social Systems, 2022, 9(1): 109-119.
- [17] ALBOUQ S S, FREDERICKS E M. Securing communication between service providers and road side units in a connected vehicle infrastructure[C]//Proceedings of the 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA). Piscataway: IEEE Press, 2017: 1-5.
- [18] ABDELAZIZ A, EMRE KOKSAL C, BURTON R, et al. Beyond PKI: enhanced authentication in vehicular networks via MIMO[C]//Proceedings of the 2018 IEEE 19th International Work-

- shop on Signal Processing Advances in Wireless Communications (SPAWC). Piscataway: IEEE Press, 2018: 1-5.
- [19] NARAYANADOSS A R, TRUONG-HUU T, MOHAN P M, et al. Crossfire attack detection using deep learning in software defined ITS networks[C]//Proceedings of the 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring). Piscataway: IEEE Press, 2019: 1-6.
- [20] GUPTA S, GUPTA S, GUPTA N, et al. Delay-tolerant and prioritized batch verification system using efficient RSU scheduling in VANET[C]//Proceedings of the ICC 2022-IEEE International Conference on Communications. Piscataway: IEEE Press, 2022: 5706-5711.
- [21] CHANG S, QI Y, ZHU H Z, et al. Footprint: detecting sybil attacks in urban vehicular networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 23(6): 1103-1114.
- [22] WEI Y C, CHEN Y M. An efficient trust management system for balancing the safety and location privacy in VANETs[C]//Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications. Piscataway: IEEE Press, 2012: 393-400.
- [23] KUMAR A, GUPTA N. A secure RSU based security against multiple attacks in VANET[C]//Proceedings of the 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS). Piscataway: IEEE Press, 2020: 1156-1163.
- [24] TANG W Z, SHAN X Y, TIAN D X, et al. Optimizing RSUs network against cascading failure[C]//Proceedings of the 2015 IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom). Piscataway: IEEE Press, 2015: 1670-1675.
- [25] ASHRITHA M, SRIDHAR C S. RSU based efficient vehicle authentication mechanism for VANETs[C]//Proceedings of the 2015 IEEE 9th International Conference on Intelligent Systems and Control (ISCO). Piscataway: IEEE Press, 2015: 1-5.
- [26] SAFAVAT S, RAWAT D B. Improved multiresolution neural network for mobility-aware security and content caching for Internet of vehicles[J]. IEEE Internet of Things Journal, 2023, 10(20): 17813-17823.
- [27] CHEN C, ZENG Y N, LI H, et al. A multihop task offloading decision model in MEC-enabled Internet of vehicles[J]. IEEE Internet of Things Journal, 2023, 10(4): 3215-3230.
- [28] ALBOUQ S S, FREDERICKS E M. Lightweight detection and isolation of black hole attacks in connected vehicles[C]//Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW). Piscataway: IEEE Press, 2017: 97-104.
- [29] KUMAR R, KUMAR P, TRIPATHI R, et al. P2SF-IoV: a privacy-preservation-based secured framework for Internet of vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(11): 22571-22582.
- [30] OTHMAN W, MIAO F Y, XUE K P, et al. Physically secure lightweight and privacy-preserving message authentication protocol for VANET in smart city[J]. IEEE Transactions on Vehicular Technology, 2021, 70(12): 12902-12917.
- [31] THOTA J, ABDULLAH N F, DOUFEXI A, et al. V2V for vehicular safety applications[J]. IEEE Transactions on Intelligent Transportation Systems, 2020, 21(6): 2571-2585.
- [32] ZHANG X R, CHANG Z, HU T, et al. Vehicle selection and resource allocation for federated learning-assisted vehicular network[J]. IEEE Transactions on Mobile Computing, 2023(99): 1-12.
- [33] 代亮, 张亚楠, 钱超, 等. 基于车辆载带中继的路边单元突发业务分组调度最优策略[J]. 自动化学报, 2021, 47(5): 1098-1110.
- DAI L, ZHANG Y N, QIAN C, et al. Optimal packet scheduling strategy for roadside units' bursty traffic based on relaying vehicles[J]. Acta Automatica Sinica, 2021, 47(5): 1098-1110.
- [34] XIAO H Z, ZHAO J, FENG J, et al. Joint optimization of security strength and resource allocation for computation offloading in vehicular edge computing[J]. IEEE Transactions on Wireless Communications, 2023, 22(12): 8751-8765.
- [35] DAI L, CHEN T Q, ZHAI Y M, et al. Energy-efficient distributed packet scheduling optimization strategy in cooperative vehicle infrastructure systems[J]. Wireless Communications and Mobile Computing, 2021, 2021: 6661623.

[作者简介]



苏北坡 (1996-) 男, 陕西渭南人, 长安大学博士生, 主要研究方向为车路协同系统下的任务调度, 网络信息安全。



代亮 (1981-) 男, 陕西安康人, 长安大学教授, 博士生导师, 主要研究方向为车路协同系统理论与工程应用, 低碳智能交通系统, 网络安全。



巨永锋 (1962-) 男, 陕西周至人, 长安大学教授, 博士生导师, 主要研究方向为模式识别与智能系统, 机器人控制与智能控制, 道路交通控制与管理, 网络安全。