Physical Layer Security Assisted Computation Offloading in Intelligently Connected Vehicle Networks

Yiliang Liu, Wei Wang, *Member, IEEE*, Hsiao-Hwa Chen, *Fellow, IEEE*, Feng Lyu, *Member, IEEE*, Liangmin Wang, *Member, IEEE*, Weixiao Meng, *Senior Member, IEEE*, and Xuemin Shen, *Fellow, IEEE*

***Abstract*— In this paper, we propose a secure computationoffloading scheme (SCOS) in intelligently connected vehicle (ICV) networks, aiming to minimize overall latency of computing via offloading part of computational tasks to nearby servers in small cell base stations (SBSs), while securing the information delivered during offloading and feedback phases via physical layer security. Existing computation offloading schemes usually neglected time-varying characteristics of channels and their corresponding secrecy rates, resulting in an inappropriate task partition ratio and a large secrecy outage probability. To address these issues, we utilize an ergodic secrecy rate to determine how many tasks are offloaded to the edge, where ergodic secrecy rate represents the average secrecy rate over all realizations in a time-varying wireless channel. Adaptive wiretap code rates are proposed with a secrecy outage constraint to match time-varying wireless channels. In addition, the proposed secure beamforming and artificial noise (AN) schemes can improve the ergodic secrecy rates of uplink and downlink channels even without eavesdropper channel state information (CSI). Numerical results demonstrate that the proposed schemes have a shorter system delay than the strategies neglecting time-varying characteristics.**

***Index Terms*— Computation offloading, intelligently connected vehicles, physical layer security, time-varying channels.**

Manuscript received January 4, 2020; revised August 25, 2020 and November 26, 2020; accepted January 1, 2021. Date of publication January 22, 2021; date of current version June 10, 2021. This work was supported in part by the National Natural Science Foundation of China under Grant U1764263 and Grant 61671186, in part by the Taiwan Ministry of Science and Technology under Grant 109-2221-E-006-175-MY3 and Grant 109-2221-E-006-182-MY3, and in part by the Natural Sciences and Engineering Research Council (NSERC) of Canada. The associate editor coordinating the review of this article and approving it for publication was S. Pollin.

Yiliang Liu and Weixiao Meng are with the School of Electronics and Information Engineering, Harbin Institute of Technology, Harbin 150001, China (e-mail: alanliuyiliang@gmail.com; wxmeng@hit.edu.cn).

Wei Wang is with the College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China (e-mail: wei_wang@nuaa.edu.cn).

Hsiao-Hwa Chen is with the Department of Engineering Science, National Cheng Kung University, Tainan 70101, Taiwan (e-mail: hshwchen@ieee.org).

Feng Lyu is with the School of Computer Science and Engineering, Central South University, Changsha 410083, China (e-mail: fenglyu@csu.edu.cn).

Liangmin Wang is with the School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China (e-mail: wanglm@ujs.edu.cn).

Xuemin Shen is with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: sshen@uwaterloo.ca).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TWC.2021.3051772.

Digital Object Identifier 10.1109/TWC.2021.3051772

I. Introduction

THE advancement in sensors, cloud computing, artificial intelligence (AI), and 5G technologies has pushed the evolution of traditional vehicle-to-vehicle (V2V) networks toward intelligently connected vehicle (ICV) networks [1]. Compared to safety or value-added services in V2V networks supported by IEEE 802.11p [2], 5G-enabled ICVs equipped with advanced computing modules can realize autonomous driving, driver-supervised driving, cooperative driving, high definition and three-dimensional (3D) map services, on-board working and entertainment, augmented reality (AR), etc. [3]–[5]. In addition to local computing, enabled by mobile edge computing (MEC) technologies, ICVs can offload part of computational tasks to nearby servers in SBSs to cut down vehicle cost. For example, in Tesla store [6], consumers should pay an extra 8,000∼10,000 US dollar for full self-driving hardware (Nvidia drive PX 2 platform), whose price could probably be reduced substantially if dedicated MEC services are available [1], [7]. Also, MEC can reduce computing and network latency when on-board computing capacity is insufficient [8]–[14].

MEC faces many security threats due to information exchanges between ICVs and SBSs. In order to guarantee information confidentiality, symmetric key agreements with authentication processes were proposed in the literature [15]–[17]. However, secret key establishment is controlled by centralized parties of cryptography management, such as authentication, authorization, and accounting (AAA) servers defined in the 3GPP standard, which requires ubiquitously available trusted third-party and tamper-proof devices [18]–[20], and therefore it may be not suitable for highly dynamic ICV networks. As an important security mechanism, physical layer security is capable to achieve confidential information transmission by exploring random characteristics of wireless medium, and is implemented via physical layer technologies (such as encoding, decoding, and resource allocation, etc.) without cryptography operations [21].

The issue of high mobility in vehicular networks should not be ignored for improving the performance of computation offloading schemes for vehicles. Task partition techniques divide computation tasks and determine which part of computation tasks to be offloaded, which is conducted before MEC

computation. The task partition requires satisfactory secrecy rates in uplink and downlink, and uses these rates to balance local and edge computations. Previous computation offloading schemes assumed that these rates are time-invariant during offloading duration [8]–[14]. However, the coherence time of vehicular channels is short due to high mobility (usually less than 1 ms), which means that uplink and downlink channels change rapidly, and thus data transmission in ICV networks suffers distortions due to varying wireless channels. In this case, task partition with a time-invariant rate may lead to a poor offloading performance when the rates of data transmission must be made different due to variations of wireless channels. Besides, high mobility also brings in more challenges in data transmissions. Fixed wiretap code rates[1] without considering time-varying secrecy rate may cause a large secrecy outage. Note that even we can keep a secrecy outage probability below a threshold, we still can not avoid a secrecy outage completely because the CSIs of eavesdroppers are unavailable during the entire transmission and computation phases. The unknown CSI of eavesdroppers is a typical issue and should not be ignored in physical layer security assisted offloading schemes. The other issue is a long latency caused by small secrecy rates. Existing computation offloading schemes use wiretap coding with single antenna technologies to achieve physical layer security [12]–[14]. When eavesdroppers have better channel conditions or more antennas, the secrecy rate can be very low and even equals to zero, causing a long delay if using a channel with a small secrecy rate to transmit data.

In order to address the aforementioned issues, we formulate a latency minimization problem with respect to a computation task partition ratio, where an ICV network uses ergodic secrecy rates of uplink and downlink for computation task partition. Although these time-varying CSIs and their secrecy rates are unavailable in the task partition phase as transmissions have not yet occurred in this phase, the ICV can calculate the ergodic secrecy rates of uplink and downlink by integral equations, considering that the CSIs are integral variables. In the follow-up transmission phases, the main CSIs between ICV and SBS in each transmission burst can be estimated, such that an adaptive wiretap code rate with secrecy outage constraints can be identified according to the main CSIs to avoid a large secrecy outage. In addition, SBS-assisted jamming, multi-antenna beamforming, and artificial noise (AN) technologies are used to improve secrecy rates, which do not require CSIs of eavesdroppers. The main contributions of this work are summarized as follows.

1) First, we formulate a secure computation offloading model of an ICV network, where joint AN-assisted beamforming and wiretap coding schemes are used to prevent a multi-antenna eavesdropper from wiretapping uplink and downlink information between the ICV and MEC server. Due to the latency requirement of computation services, the optimization problem is to minimize the total latency of transmission and computation.
2) In computation task partition phases, the exact expressions of uplink and downlink ergodic secrecy rates are deduced for task partition. The closed-form expressions of the lower bounds of these ergodic secrecy rates are given also to reduce complexity. In addition, computation task partition is solved in a closed-form.
3) To improve the secrecy rates of uplink, SBS receives uplink data via maximum ratio combining (MRC), while transmitting AN signals to confuse an eavesdropper without any self-interference at SBS. In downlink, SBS uses maximum ratio transmission (MRT) for message beamforming and sending AN signals in null spaces. To mitigate time-varying effects in wiretap coding, adaptive wiretap code rates are proposed, considering secrecy outage probabilities in both uplink and downlink.

The remainder of this paper can be outlined as follows. Section II surveys the related works. Section III describes the system model and problem formulation, together with the workflow of SCOS given in Section III-E. The computation task partition approach, uplink/downlink secure beamforming, and AN technologies are elaborated in Section IV. The schemes enabling adaptive secrecy rates are proposed in Section V. We show simulation results in Section VI, and conclude this paper in Section VII.

The major notations are defined as follows. Bold uppercase letters denote matrices and bold lowercase letters denote column vectors. $\mathbf{A}^{\dagger}$ represents the Hermitian transpose of $\mathbf{A}$. $\mathbf{I}_a$ is an identity matrix with its rank a. $\mathcal{CN}(\mu, \sigma^2)$ is a complex normal (Gaussian) distribution with mean μ and variance σ^2. $(\mathbf{A})^{-1}$ is an inverse function of $\mathbf{A}$. $|\mathbf{x}|$ is the Euclidean norm of $\mathbf{x}$. $\mathrm{E}[\cdot]$ is the expectation operator. $\binom{x}{y}$ is the combination between x and y such that $\binom{x}{y} = \frac{x!}{(x-y)!y!}$. $\mathrm{Rank}(\mathbf{A})$ calculates the rank of $\mathbf{A}$. $x!$ is the factorial of x. $e \simeq 2.7183$ is a constant. $\mathrm{diag}(\mathbf{x})$ is a diagonal matrix of vector $\mathbf{x}$. An $[a \times (b+c)]$ matrix $[\mathbf{A}, \mathbf{B}]$ denotes a combined matrix between an $(a \times b)$ matrix $\mathbf{A}$ and an $(a \times c)$ matrix $\mathbf{B}$.

II. Related Works

In this section, we briefly discuss about MEC and traditional AN-based physical layer security technologies considered in SCOS designs.

A. MEC Technologies

As mentioned in [7], network, communication, computation task partition, and security are the main technical challenges of MEC. Sardellitti *et al.* focused on the physical layer in network and communication aspects, where energy consumption of all users was minimized via beamforming and computation resources optimization [26]. The MEC/cloud access capacity was discussed in [11], which maximized the number of users that access to the cloud. Wang *et al.* proposed a routing algorithm based on deep reinforcement learning, which aimed to minimize routing delay and improve network bandwidth

[1]The wiretap code was introduced first by Wyner, which is a general code scheme to ensure that a coding rate (defined as a wiretap code rate) below the secrecy capacity can achieve both reliability and information-theoretic security [22]. The secrecy rate can be viewed as an inherent property of a given communication system, while the wiretap code rate is controlled by encoders. This paper uses Wyner's coding that is non-structured random codes based on cosets. Many efforts were dedicated to find practical codes based on Wyner's theory [23]–[25].

utilization [27]. Two classic task partition models were proposed as follows. Miettinen *et al.* considered a data-based model, where task-input data were bit-wise independent and can be arbitrarily divided into different groups and executed by different entities simultaneously [28]. Mahmoodi *et al.* proposed a taskcall graph-based model that decides whether a component completes processing on a mobile or edge server [29]. The taskcall graph has three typical dependency models, i.e., sequential, parallel, and general computation task dependency models. Cheng *et al.* considered a parallel computation task dependency model and assigned virtual machines (VMs) in an edge server to the tasks that can be executed in parallel [9].

The ICV computation tasks can be categorized into time-sensitive tasks and non-mission critical tasks. As mentioned in [4], time-sensitive ICV tasks include driver-supervised driving, cooperative driving, and autonomous driving, which can perform driving tasks in certain conditions while a driver should intervene whenever needed according to road conditions and system requests. Computation offloading of MEC is capable of reducing the cost of vehicle computing platforms and accelerate computation processes. Meanwhile, it can provide global information on road environments, and the models in an MEC server are more precise than that of vehicles in some machine learning-assisted applications [7]. The non-mission critical ICV tasks usually include on-board working and entertainment. Drivers and passengers can take full advantage of MEC to accelerate the processes and enjoy on-board entertainment as these require a large amount of computation power and storage.

To achieve confidentiality, Yang *et al.* first considered physical layer security in offloading, and used wiretap coding to protect uplink channels from users to MEC servers in a multi-user multi-server scenario [12]. Considering the security in terrestrial to air channels, Bai *et al.* used single-antenna jamming technologies to protect uplink channels between an MEC server and an unmanned aerial vehicles (UAV) against both active and passive eavesdroppers [14]. Zhou *et al.* extended jamming technologies further in a scenario with multiple UAVs, where task partition ratio, UAV locations, and transmission power were optimized jointly to maximize the minimum uplink secrecy capacity among multiple UAVs [30]. Likewise, Wang *et al.* considered energy efficiency in secure offloading systems with multiple legitimate users. They optimized radio resource allocation to minimize energy consumption [31]. The radio resources in the above investigations were assumed to be orthogonal. Wu *et al.* used secrecy outage-constrained wiretap coding to protect uplink channels in non-orthogonal multiple access (NOMA) assisted computation offloading systems, where an optimal computation task partition ratio was investigated to minimize energy consumption and secrecy outage probabilities [32]. Multiple antennas technologies were also used to improve the performance of secure offloading systems. He *et al.* used multiple antennas of SBS to generate AN signals to impede eavesdropping and leverage full-duplex communication technologies to suppress self-interference [33].

B. AN-Based Physical Layer Security Technologies

As shown in the literature, physical layer security is achieved by wiretap coding, where messages are reliably transmitted to destinations while the messages are kept confidential to eavesdroppers [22]. In order to make physical layer security more efficient, AN technologies allocate a part of transmission power for generating interference signals, which improve secrecy capacity/rate. The main AN technologies are summarized as follows. 1) Nullspace based AN technology was presented in [34], which does not require wiretap CSIs. AN signals are transmitted to the nullspace of main channels, such that they do not interfere desired users but only impair eavesdropped channels. 2) Eigenspace based AN technology can identify some appropriate eigenspaces reserved for messages to generate AN signals, instead of selecting nullspaces only for AN signals [35], [36]. The aforementioned AN technologies belong to linear precoding. 3) Semidefinite programming (SDP) based AN technology needs complex optimization processing to output the optimal beamforming vectors and AN signals, and it offers an optimal secrecy rate [37]. The limitation of the SDP based AN technology is the requirement of wiretap CSIs.

C. Discussion

The existing investigations on the AN methods did not give ergodic secrecy rate expressions of vehicle-to-infrastructure (V2I) links. Besides, high mobility issues should be considered in wiretap coding as discussed in Section I. Thus, in this work, we propose SCOS, which focuses on computation task partition and uplink/downlink AN-aided secure beamforming, followed by adaptive wiretap coding schemes.

III. System Model and Problem Formulation

A. System Model

Let us consider a secure ICV offloading system, which is equipped with a single antenna, an SBS with N_m antennas, an MEC server, and an eavesdropper (Eve) with N_e antennas, as shown in Fig. 1. For security purpose, N_m should be larger than N_e. If an ICV desires to establish wireless connection for uploading or feedback, it uses Uu interfaces supported by a cellular network with two operational modes on physical layer, i.e., frequency division duplex (FDD) and time division duplex (TDD) [38]. Here, we assume a TDD model because the characteristics of channel reciprocity in TDD avoid CSI feedback overhead. As aforementioned, four entities exist in this system, which are described as follows.

1) ICV is responsible for computation task partition and transmits a part of tasks to an MEC-assisted SBS confidentially.
2) SBS receives task data while sending AN signals as a cooperative jammer in uplink, and also uses AN-assisted technologies in downlink transmissions to provide feedback to the ICV.
3) MEC server executes computation tasks for the ICV, and is generally installed in an SBS or is located physically close to the SBS, such that the channel between the SBS and the MEC server is assumed to be secure.

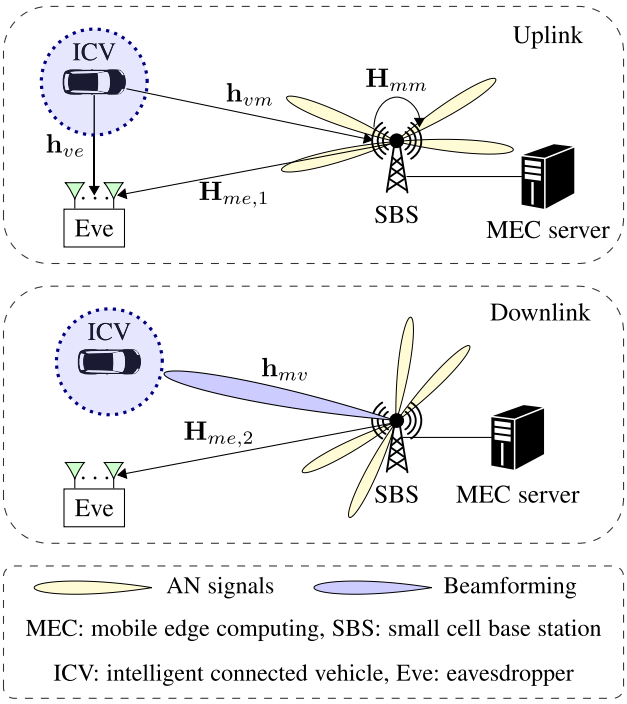


Fig. 1. A communication model with a multiple antenna eavesdropper. An uplink is to upload a part of computation tasks to a nearby SBS. After the MEC server obtains computation results, a downlink is used to download the computation results to the ICV. In addition, beamforming and AN schemes are illustrated in Section IV.

4) Eve is a passive eavesdropper that silently receives messages, and thus its CSIs are unavailable.

B. Computation Task Model

The ICV will perform a computation task with M-bits data with the assistance of an MEC server. Let us consider a task that has a full granular data-partition model and can be arbitrarily divided, as discussed in [7], [10], [11]. We define a variable η as a ratio of locally processed data to the total amount of data. Hence, in the first phase, ηM bits will be processed at the ICV and $(1-\eta)M$ bits should be uploaded to SBS. In the second phase, the MEC server of the SBS will complete the computation of $(1-\eta)M$ bits data, and then send the results to the ICV. In both phases, Eve aims to wiretap the information from uplink and downlink channels, and thus physical layer security schemes should be used to protect the uplink and downlink channels. Some investigations ignored the delay of downlink phases when little data need to be transmitted in feedback [11]. Considering diverse applications in ICVs, such as 3D map [4], [5] and remote diagnosis services [39], we should not ignore the delay in uplink or downlink phases.

C. Channel Model

Four channels are considered in the uplink process as shown in Fig. 1. The uplink channel between the ICV and the SBS is defined as an $N_m \times 1$ vector, i.e., $\mathbf{h}_{vm}$, and a wiretap channel between the ICV and Eve is defined as an $N_e \times 1$ vector, i.e., $\mathbf{h}_{ve}$. As the SBS works as a full-duplex cooperative jammer, the interference channel between the SBS and Eve is defined as an $N_e \times N_m$ matrix, i.e., $\mathbf{H}_{me,1}$. In addition, a self-interference channel incurred from AN signals at the SBS is defined as an $N_m \times N_m$ matrix, i.e., $\mathbf{H}_{mm}$.

Analogously, two channels are considered in the downlink process, as shown in Fig. 1. The downlink channel between the SBS and the ICV is defined as a $1 \times N_m$ vector, i.e., $\mathbf{h}_{mv}$, and the wiretap channel between Eve and the SBS is defined as an $N_e \times N_m$ matrix, i.e., $\mathbf{H}_{me,2}$.

The works in [40] showed that vehicular channels can be simplified by slow-fading Rayleigh models due to the effect of heavily built-up urban environments on radio signals. Also, vehicular CSIs are constant within coherence time, e.g., the coherence time is approximately 2 ms when the speed of vehicles is 10 m/s and the center frequency is 6 GHz. Thus, data delivery is done through multiple wireless channels. According to the aforementioned features, the CSIs of these six channels are assumed as follows.

1) Main CSIs: In the uplink and downlink, we assume that the CSIs of the main channels $\mathbf{h}_{vm}$, $\mathbf{H}_{mm}$, and $\mathbf{h}_{mv}$ are obtained via pilot-added estimation technologies [41] in each transmission burst, which do not require the location information of vehicles. In addition, as CSIs of the main channels are time-varying, they are unavailable in the computation task partition phase since offloading is a causal process, and the task partition ratio η will be determined based only on the channel distribution information (CDI), assuming that the main CSIs obey Rayleigh fading models.
2) Wiretap CSIs: Since Eve keeps silent, $\mathbf{h}_{ve}$, $\mathbf{H}_{me,1}$, and $\mathbf{H}_{me,2}$ are unavailable. For simplicity, all of these channels are assumed to obey Rayleigh fading channel models. Since $\mathbf{H}_{me,1}$ and $\mathbf{H}_{me,2}$ are independent and identically distributed, we simplify $\mathbf{H}_{me,1}$ and $\mathbf{H}_{me,2}$ as a complex Gaussian random matrix $\mathbf{H}_{me}$.

In this paper, we emphasize the secure computation offloading approach and assume that channel estimation is perfect, as what have been assumed in [12], [14], [30]–[33]. However, in practice, perfect CSIs may not be available due to channel estimation and feedback errors. The imperfect CSI leads to errors in precoding vectors and impairs wiretap code rates of the proposed scheme, and then further reduces the secrecy rates. For the case of imperfect CSI, many efforts have been independently conducted, such as imperfect CSI modeling, robust precoding, and wiretap coding with CSI uncertainty [21], [42], [43], which help to design secure computation offloading schemes under imperfect CSI conditions. We will consider the imperfect CSI in our future works.

D. Problem Formulation

Here, we first derive a latency expression before formulating a latency minimization problem. In this model, when ηM bits data are processed in an ICV, the local computing time is $T_v = \eta M/a_v$, and the computing time of the MEC server is $T_m = (1-\eta)M/a_m$, where a_v (bit/s) and a_m (bit/s) are the computing speeds of the ICV and the MEC

server, respectively. The transmission delays of uplink and downlink are expressed as $T_u = \beta(1-\eta)M/R_u$ and $T_d = \alpha(1-\eta)M/R_d$, respectively, where α accounts for the ratio of output to input bits offloaded to the MEC server, and β is the compression ratio of uploaded data as many data types, e.g. images and videos, should be compressed before uploading and decompressed in MEC server before data processing. R_u (bit/s) and R_d (bit/s) are the wiretap code rates of the uplink and downlink channels, respectively. Similar latency models can be seen in [10], [44]. In this case, the latency of this task computation can be formulated as

$$T_{\text{latency}}(\eta, R_u, R_d) = \max(T_v, T_m + T_u + T_d), \tag{1}$$

where $\max(x, y)$ is the maximum values of x and y. Note that $T_{\text{latency}}(\eta, R_u, R_d)$ is a function of η, R_u, and R_d. a_v and a_m are fixed computation parameters for the given ICVs and SBSs.

For vehicular tasks where the vehicle has a stringent requirement on the speed of computing feedback, it is preferred to shorten the latency as much as possible, which can be formulated as

$$\text{P1:} \quad \min_{\eta} \left\{T_{\text{latency}}(\eta, R_u, R_d)\right\}, \tag{2a}$$

$$\text{s.t. } 0 \le \eta \le 1. \tag{2b}$$

Constraint (2b) specifies the domain of offloading ratio. Due to the non-convexity of the objective function, P1 is a non-convex problem. In addition, it is imprecise to assume that R_u and R_d are time-invariant due to time-varying distortions. We adopt a practical method to solve P1 as follows. In Section IV, we optimize η with the ergodic secrecy rates of uplink and downlink, i.e., $\bar{R}_u$ and $\bar{R}_d$. In Section V, we establish uplink and downlink wiretap code rates, considering the secrecy outage probability.

E. Workflow of SCOS

The procedure of SCOS is sketched as follows.

1) **Setup:** The ICV handshakes with an SBS and loads the system parameters $\{a_v, a_m, N_m, N_e, P_m, P_v\}$ from the SBS, where P_m is the normalized SBS transmission power in both uplink and downlink. P_v is the normalized ICV transmission power.
2) **Computation task partition:** The ICV estimates the ergodic secrecy rates of uplink and downlink, i.e., $\bar{R}_u$ and $\bar{R}_d$, with corresponding physical layer security schemes. The ICV picks up a computation task partition based on $\{\bar{R}_u, \bar{R}_d, a_v, a_m\}$, and outputs η^*. The details are described in Section IV.
3) **Uplink transmission:** The ICV estimates the uplink CSI $\mathbf{h}_{vm}$ within coherence time, then adjusts the wiretap code rate R_u with the constraint of the secrecy outage probability, and sends $\beta(1-\eta^*)M$ data to the SBS at R_u. The details are described in Section V-A.
4) **Parallel computing:** The ICV and the SBS execute tasks simultaneously.
5) **Downlink transmission:** The SBS estimates the downlink CSI $\mathbf{h}_{mv}$ within coherence time, then adjusts the wiretap code rate R_d with the constraint of the secrecy outage probability, and sends the results to the ICV at R_d. The details are described in Section V-B.

In uplink phases, SBS uses a joint MRC and designed AN scheme; while in downlink phases, the SBS uses a joint MRT and nullspace-based AN scheme. We want to mention that SCOS just provides a theoretical guidance to optimize computation task partition and to design proper physical layer security approaches. However, in real-world communication systems, many factors, such as CSI estimation error, signal synchronization, and coding and modulation efficiency, will actually affect the deployment and performance of SCOS.

IV. Task Partition and An-Assisted Phy-Layer Security

An ICV uses parameters $\{\bar{R}_u, \bar{R}_d, a_v, a_m\}$ for computation task partition. In the setup process, the system parameters $\{a_v, a_m, N_m, N_e, P_m, P_v\}$ are given. Thus, we should first calculate the ergodic secrecy rates of uplink and downlink, i.e., $\bar{R}_u$ and $\bar{R}_d$, which depend on $\{N_m, N_e, P_m, P_v\}$, statistical CSI model (a Rayleigh fading channel), and the corresponding physical layer (PHY-layer) security schemes. The calculations of $\bar{R}_u$ and $\bar{R}_d$ do no require instantaneous CSIs of both main and wiretap channels.

A. Uplink Ergodic Secrecy Rate $\bar{R}_d$

The ICV transmits $\beta(1-\eta)M$ data to SBS. The SBS uses an MRC receiver, i.e., $\mathbf{w}_m = \mathbf{h}_{vm}^{\dagger}/|\mathbf{h}_{vm}|$ to gather the signals from different antennas simultaneously, and generates AN signals to confuse Eve. In this case, the received signals at the SBS and Eve are expressed as

$$\mathbf{y}_{vm} = \mathbf{h}_{vm}x_u + \mathbf{H}_{mm}\mathbf{G}_u\mathbf{z}_u + \mathbf{n}_{vm}, \tag{3a}$$

$$\mathbf{y}_{ve} = \mathbf{h}_{ve}x_u + \mathbf{H}_{me}\mathbf{G}_u\mathbf{z}_u + \mathbf{n}_{ve}, \tag{3b}$$

where x_u is the ICV uplink signal encoded by wiretap coding to satisfy $\mathrm{E}(|x_u|^2) = P_v$. $\mathbf{n}_{vm}$ and $\mathbf{n}_{ve}$ are AWGN vectors obeying $\mathcal{CN}(\mathbf{0}, \sigma_{vm}^2\mathbf{I}_{N_m})$ and $\mathcal{CN}(\mathbf{0}, \sigma_{ve}^2\mathbf{I}_{N_e})$, respectively. $\mathbf{G}_u$ is an $N_m \times (N_m - 1)$ matrix,[2] which lies in the nullspace of $\mathbf{h}_{vm}^{\dagger}\mathbf{H}_{mm}$. $\mathbf{z}_u$ is a complex Gaussian AN signal obeying $\mathcal{CN}(\mathbf{0}, \frac{P_m}{N_m-1}\mathbf{I}_{N_m-1})$.

The processed signals can be formulated as

$$\mathbf{w}_m\mathbf{y}_{vm} = \mathbf{w}_m\mathbf{h}_{vm}x_u + \mathbf{w}_m\mathbf{n}_{vm}. \tag{4}$$

Although the ICV can obtain $\mathbf{h}_{vm}$ via channel estimation in each uplink transmission burst, it is unavailable in the task partition phase. Thus, we will use the ergodic secrecy rate for task partition. With the proposed MRC and AN schemes, the real ergodic secrecy rate in uplink channel is expressed as

$$\ddot{R}_u = \mathrm{E}_{\mathbf{h}_{vm},\mathbf{h}_{ve},\mathbf{H}_{me}}[C_{v,u} - C_{e,u}]^+ \tag{5}$$

$$\ge \mathrm{E}_{\mathbf{h}_{vm}}[C_{v,u}] - \mathrm{E}_{\mathbf{h}_{vm},\mathbf{h}_{ve},\mathbf{H}_{me}}[C_{e,u}], \tag{6}$$

[2]Assume that the number of SBS antennas is larger than that of Eve, i.e., $N_m > N_e$, and Eve has $N_m - 1$ antennas. Thus, Eve can not separate the AN signals of SBS from the signals of ICV as the dimension of the spaces for AN signals $\mathbf{G}_u$ is $N_m - 1$.

where

$$C_{v,u} = B_1 \log_2 \Big(1 + \frac{P_v}{\sigma_{vm}^2}|\mathbf{h}_{vm}|^2\Big), \tag{7a}$$

$$C_{e,u} = B_1 \log_2 \det \left(\mathbf{I}_{N_e} + \frac{P_v \mathbf{h}_{ve}\mathbf{h}_{ve}^\dagger}{\sigma_{ve}^2 \mathbf{I}_{N_e} + \frac{P_m}{N_m - 1}\mathbf{H}_1\mathbf{H}_1^\dagger}\right), \tag{7b}$$

where B_1 is the uplink bandwidth and $\mathbf{H}_1 = \mathbf{H}_{me}\mathbf{G}_u \in \mathbb{C}^{N_e \times (N_m - 1)}$. $C_{v,u}$ is the uplink channel capacity between the ICV and the SBS that can be achieved via $\mathbf{w}_m$, and $C_{e,u}$ is the uplink capacity between the ICV and Eve. Note that P_v and P_m are normalized by the bandwidth.

The equality of Eqn. (6) holds if and only if $\{C_{v,u} - C_{e,u}\}$ is always nonnegative in all channel states. However, due to the lack of $\mathbf{H}_{me}$, we cannot determine whether an instantaneous secrecy rate is nonnegative or not, and thus we resort to derive a lower bound of the real ergodic secrecy rate as an ergodic secrecy rate. According to [36], we know $C_{v,u}$ is larger than $C_{e,u}$ with a high probability because of AN signals. The uplink ergodic secrecy rate can be written as

$$\bar{R}_u = \mathrm{E}_{\mathbf{h}_{vm}}[C_{v,u}] - \mathrm{E}_{\mathbf{h}_{vm},\mathbf{h}_{ve},\mathbf{H}_{me}}[C_{e,u}]. \tag{8}$$

Then, we will derive a theoretical expression of the ergodic secrecy rate $\bar{R}_u$ for task partition, i.e., use $\bar{R}_u$ in P1 instead of R_u, which is deduced in the following proposition.

Proposition 1: The ergodic secrecy rate of R_u, i.e., $\bar{R}_u$ is

$$\bar{R}_u = B_1\big\{\Phi(\rho_1) + C(\mathbf{H}_1, \rho_2) - \Psi(\mathbf{H}_2, \rho_2, P_v)\big\}, \tag{9}$$

where

$$\Phi(\rho) = \frac{1}{\ln(2)} \exp(\rho) \sum_{k=0}^{N_m - 1} E_{k+1}(\rho), \tag{10}$$

$$\rho_1 = \frac{\sigma_{vm}^2}{P_v}, \quad \rho_2 = \frac{P_m}{\sigma_{ve}^2(N_m - 1)}, \tag{11}$$

$\mathbf{H}_1 = \mathbf{H}_{me}\mathbf{G}_u \in \mathbb{C}^{N_e \times (N_m - 1)}$, $\mathbf{H}_2 = [\mathbf{h}_{ve}, \mathbf{H}_1] \in \mathbb{C}^{N_e \times N_m}$,

$$C(\mathbf{A}, \rho) = \frac{\exp(1/\rho)}{\ln(2)} \sum_{k=0}^{n-1} \sum_{l=0}^{k} \sum_{i=0}^{2l} \left\{ \frac{(-1)^i (2l)!(m - n + i)!}{2^{2k-i} l! i! (m - n + l)!} \times \binom{2k - 2l}{k - l} \binom{2l + 2m - 2n}{2l - i} \sum_{j=0}^{m-n+i} E_{j+1}(1/\rho) \right\}, \tag{12}$$

$n = \min(a, b)$, $m = \max(a, b)$ for any $\mathbf{A} \in \mathbb{C}^{a \times b}$, $E_\tau(z)$ is the exponential integral of order τ defined by

$$E_\tau(z) = \int_1^{+\infty} e^{-zx} x^{-\tau} dx, \quad \tau = 0, 1, \ldots, \mathrm{Re}(z) > 0, \tag{13}$$

and $\mathrm{Re}(z)$ is the real part of z. Finally, we have

$$\Psi(\mathbf{H}_2, \rho_2, P_v) = K \sum_{k=1}^{N_e} \det\{\mathbf{\Theta}(k, \mathbf{Q})\}, \tag{14}$$

where we have $N_m \times N_m$ matrix $\mathbf{Q} = \mathrm{diag}(P_v/\sigma_{ve}^2, \rho_2, \ldots, \rho_2)$. The i-th row and j-th column element of the $N_m \times N_m$ real matrix $\mathbf{\Theta}(k, \mathbf{Q})$ are defined as

$$\big[\mathbf{\Theta}(k, \mathbf{Q})\big]_{i,j} = \begin{cases} (-1)^{d_i}(j - 1 + d_i)!/\mu_{(c_i)}^{j+d_i}, & j = 1, \ldots, N_e,\ j \neq k, \\ \dfrac{(-1)^{d_i}}{\ln(2)} e^{\mu_{(c_i)}}(j - 1 + d_i)!\Omega, & j = 1, \ldots, N_e,\ j = k, \\ [N_m - j]_{d_i}\{\mu_{(c_i)}^{N_m - d_i - j}\}, & j = N_e + 1, \ldots, N_m, \end{cases} \tag{15}$$

where $[y]_x = y(y - 1)\ldots(y - x + 1)$, $[y]_0 = 1$,

$$\Omega = \sum_{t=0}^{j-1+d_i} \frac{\Gamma(t - j + 1 - d_i, \mu_{(c_i)})}{\mu_{(c_i)}^{t+1}}, \tag{16}$$

$$\Gamma(a, x) = \int_x^{+\infty} \exp(-z) z^{a-1} dz, \tag{17}$$

$$K = \frac{(-1)^{N_e(N_m - N_e)} \prod_{i=1}^{2} \mu_i^{\nu_i N_e}}{\Gamma_{N_e}(N_e) \prod_{i=1}^{2} \Gamma_{\nu_i}(\nu_i)(\mu_1 - \mu_2)^{\nu_1 \nu_2}}, \tag{18}$$

$\Gamma_\alpha(\beta) = \prod_{i=1}^{\alpha}(\beta - i)!$, and $\mu_1 > \mu_2$ are the distinct eigenvalues of $\mathbf{Q}^{-1}$, whose numbers are ν_1 and ν_2, respectively, so that $\sum_{i=1}^{2} \nu_i = N_m$. Let c_i denote a unique integer such that

$$\nu_1 + \ldots + \nu_{c_i - 1} < i \leq \nu_1 + \ldots + \nu_{c_i}, \tag{19}$$

and

$$d_i = \sum_{j=1}^{c_i} \nu_j - i. \tag{20}$$

Note that when $\mu_1 = \mu_2$, i.e., $\rho_2 = P_v/\sigma_{ve}^2$, we have $\Psi(\mathbf{H}_2, \rho_2, P_v) = C(\mathbf{H}_2, \rho_2)$.

Proof: See in Appendix A. ∎

Although Eqn. (9) has no integral expression except for several special functions, it is a complex equation, which yields a lot of computation overhead. We provide a closed-form expression of the lower bound of $\bar{R}_u$ in a high SNR region, i.e., when P_m/σ_{ve}^2 is high, as given in the following corollary. The lower bound is a common metric in security as it represents the worst case scenario.

Corollary 1: In a high SNR region, i.e., if P_m/σ_{ve}^2 is high, the lower bound of $\bar{R}_u$, i.e., $\tilde{R}_u$ is

$$\tilde{R}_u = B_1\Big\{\Phi(\rho_1) + \sum_{i=0}^{N_e - 1} \psi(N_m - 1 - i) - \log_2(\chi_1)\Big\}, \tag{21}$$

where

$$\psi(x) = \frac{1}{\ln(2)}\Big(-\xi + \sum_{r=1}^{x-1} \frac{1}{r}\Big), \tag{22}$$

$$\chi_1 = A_1 + \frac{P_v}{\sigma_{ve}^2 \rho_2} \times A_2, \tag{23}$$

$$A_1 = \sum_{i=1}^{N_e} \sum_{j=2}^{N_m} [N_m - i + 1]_i \binom{N_m - j}{i - 1} + 1, \tag{24}$$

$$A_2 = \sum_{i=1}^{N_e} [N_m - i + 1]_i \binom{N_m - 1}{i - 1}, \tag{25}$$

$\xi = 0.577215\ldots$ is the Euler's constant, $[y]_x = y(y-1)\ldots(y-x+1)$, $[y]_0 = 1$, $\Phi(\rho)$ is defined in Eqn. (10), and $\binom{x}{y} = \frac{x!}{(x-y)!y!}$. Note that when $N_m - j < i - 1$, we set $\binom{N_m-j}{i-1} = 0$ in A_1.

Proof: See in Appendix B. ∎

Remark 1 (Uplink Power Gain of SBS): P_m only affects $\log_2(\chi_1)$ in Eqn. (21). χ_1 will decrease and approach to A_1 with an increasing P_m. Thus, $\tilde{R}_u$ grows with an increasing P_m, and then approaches to a constant that equals to Eqn. (21) after replacing χ_1 with A_1.

B. Downlink Ergodic Secrecy Rate $\bar{R}_d$

For downlink security purpose, the SBS uses a joint MRT and nullspace-based AN technology. More specifically, the MRT vector is $\mathbf{w}_d = \mathbf{h}_{mv}^\dagger/|\mathbf{h}_{mv}|$, and the received signals at the ICV and Eve are formulated as

$$\begin{aligned} y_{mv} &= \mathbf{h}_{mv}\mathbf{w}_d x_d + \mathbf{h}_{mv}\mathbf{G}_d\mathbf{z}_d + n_{mv} \\ &= \mathbf{h}_{mv}\mathbf{w}_d x_d + n_{mv}, \end{aligned} \tag{26a}$$

$$\mathbf{y}_{me} = \mathbf{H}_{me}\mathbf{w}_d x_d + \mathbf{H}_{me}\mathbf{G}_d\mathbf{z}_d + \mathbf{n}_{me}, \tag{26b}$$

where $\mathbf{G}_d$ is an $N_m \times (N_m - 1)$ matrix that lies in the nullspace of $\mathbf{h}_{mv}$, $\mathbf{z}_d$ is a complex Gaussian AN signal obeying $\mathcal{CN}(\mathbf{0}, \frac{P_m}{N_m}\mathbf{I}_{N_m-1})$, and $\mathrm{E}[x_d x_d^\dagger] = P_m/N_m$. n_{mv} is an AWGN variable obeying $\mathcal{CN}(0, \sigma_{mv}^2)$, and $\mathbf{n}_{me}$ is an AWGN vector obeying $\mathcal{CN}(\mathbf{0}, \sigma_{me}^2\mathbf{I}_{N_e})$. Similar to the uplink phases, we will use ergodic secrecy rate for task partition, i.e., to use $\bar{R}_d$ in P1 instead of R_d. The real ergodic secrecy rate in downlink channel is

$$\ddot{R}_d = \mathrm{E}_{\mathbf{h}_{mv},\mathbf{H}_{me}}[C_{v,d} - C_{e,d}]^+, \tag{27}$$

where

$$C_{v,d} = B_2 \log_2\left(1 + \frac{P_m}{N_m\sigma_{mv}^2}|\mathbf{h}_{mv}|^2\right), \tag{28a}$$

$$C_{e,d} = B_2 \log_2 \det\left(\mathbf{I}_{N_e} + \frac{P_m\mathbf{h}_1\mathbf{h}_1^\dagger}{N_m\sigma_{me}^2\mathbf{I}_{N_e} + P_m\mathbf{H}_3\mathbf{H}_3^\dagger}\right), \tag{28b}$$

B_2 is the downlink bandwidth, $\mathbf{h}_1 = \mathbf{H}_{me}\mathbf{w}_d \in \mathbb{C}^{N_e\times 1}$, and $\mathbf{H}_3 = \mathbf{H}_{me}\mathbf{G}_d \in \mathbb{C}^{N_e\times(N_m-1)}$.

Similar to the uplink phases, the downlink ergodic secrecy rate is formulated as

$$\bar{R}_d = \mathrm{E}_{\mathbf{h}_{mv}}[C_{v,d}] - \mathrm{E}_{\mathbf{h}_{mv},\mathbf{H}_{me}}[C_{e,d}]. \tag{29}$$

We provide an exact expression of $\bar{R}_d$ to measure the downlink ergodic secrecy rate in the following proposition.

Proposition 2: The ergodic secrecy rate of R_d, i.e., $\bar{R}_d$ is

$$\bar{R}_d = B_2\{\Phi(\rho_3) + C(\mathbf{H}_3, \rho_4) - C(\mathbf{H}_4, \rho_4)\}, \tag{30}$$

where

$$\rho_3 = \frac{\sigma_{mv}^2 N_m}{P_m}, \quad \rho_4 = \frac{P_m}{\sigma_{me}^2 N_m}, \tag{31}$$

$\mathbf{H}_4 = [\mathbf{h}_1, \mathbf{H}_3] \in \mathbb{C}^{N_e\times N_m}$, and $C(\mathbf{A}, \rho)$ is defined in Eqn. (12).

Proof: The proof in [35, Th. 3] shows a general case, where the numbers of antennas in receivers and eavesdroppers are arbitrary. Proposition 2 is a special case that the number of antennas at receivers is one, which can be deduced from [35, Th. 3] via changing the variable of the number of antennas. ∎

Also, we provide a closed-form expression of the lower bound of $\bar{R}_d$ in a high SNR region, i.e., when P_m/σ_{me}^2 is high, as in the following corollary.

Corollary 2: In a high SNR region, i.e., when P_m/σ_{me}^2 is high, the lower bound of $\bar{R}_d$, i.e., $\tilde{R}_d$ is

$$\tilde{R}_d = B_2\{\Phi(\rho_3) + \sum_{i=0}^{N_e-1}\psi(N_m - 1 - i) - \log_2(\chi_2)\}, \tag{32}$$

where $\chi_2 = N_m!/(N_m - N_e)!$, $\psi(x)$ is defined in Eqn. (22), and $\Phi(\rho)$ is defined in Eqn. (10).

Proof: See in Appendix C. ∎

Remark 2 (Downlink Power Gain of SBS): P_m only affects $\Phi(\rho_3)$ in Eqn. (32). $\Phi(\rho_3)$ increases monotonically with an increasing P_m, so does $\tilde{R}_d$, meaning that the downlink power gain of P_m is larger than that of uplink.

C. Computation Task Partition With $\bar{R}_u$ and $\bar{R}_d$

The ICV will use $\{\bar{R}_u, \bar{R}_d, a_v, a_m\}$ for the computation task partition. First, we introduce an auxiliary function to represent estimated latency of the MEC server that processes $(1-\eta)M$ bits data as

$$T_{\mathrm{MEC}}(\eta) = T_m(\eta) + T_u(\eta) + T_d(\eta), \tag{33}$$

where $T_m(\eta) = \frac{(1-\eta)M}{a_m}$, $T_u(\eta) = \frac{\beta(1-\eta)M}{\bar{R}_u}$, and $T_d(\eta) = \frac{\alpha(1-\eta)M}{\bar{R}_d}$. As the descriptions given in the problem formulation, α accounts for a ratio of output to input bits offloaded to the MEC server, and β is a compression ratio of the uploaded data. Hence, with the auxiliary function and parameters $\{\bar{R}_u, \bar{R}_d, a_v, a_m\}$, P1 can be formulated as

$$\text{P2:} \min_{0\le\eta\le 1} \max\{T_v(\eta), T_{\mathrm{MEC}}(\eta)\}, \tag{34}$$

where $T_v(\eta) = \eta M/a_v$ is the computing time of the ICV. The optimal η has a closed-form solution, as seen in the following proposition.

Proposition 3: The optimal computation task partition ratio η^* can be expressed as

$$\eta^* = 1 - \frac{1}{a_v a_1 + 1}, \tag{35}$$

where

$$a_1 = \frac{1}{a_m} + \frac{\beta}{\bar{R}_u} + \frac{\alpha}{\bar{R}_d}. \tag{36}$$

Proof: See in Appendix D. ∎

Remark 3 (Advantage of Edge Computing): Since $a_v > 0$ and $a_1 > 0$, it is obvious that $0 < \eta^* < 1$ highlights the advantage of edge computing, i.e., the computation strategy of an ICV should offload a part of computation tasks to an SBS, while computing the rest of computation tasks in an on-board computer in parallel.

Remark 4 (Cask Principle): When $a_v \to 0$, we have $\eta^* \to 0$, which means that if the computing capacity of an ICV is very small, the total computation task will be uploaded to

the SBS. While $a_1 \to +\infty$, we have $\eta^* \to 1$, which means that the total computation task will be processed at the local ICV computer, and the ability of edge computing follows the "cask principle", where the smallest one of the metrics decides the capability of edge computing. That is, if any of $a_m \to 0$, $\bar{R}_u \to 0$, or $\bar{R}_d \to 0$ is achieved, we have $a_1 \to +\infty$ and total computation task will be processed at the local ICV computer.

V. Uplink/Downlink Adaptive Wiretap Coding

In the above section, we used ergodic secrecy rates of uplink and downlink for the task partition, because the ergodic secrecy rates can be calculated without instantaneous CSIs of the main and wiretap channels. The ergodic secrecy rate is just a global secrecy metric that can not be used for wiretap coding. In uplink and downlink transmissions, the instantaneous CSIs of the main channels, i.e., $\mathbf{h}_{vm}$, $\mathbf{h}_{mv}$, and $\mathbf{H}_{mm}$ can be obtained via channel estimation, while the instantaneous CSIs of wiretap channels are still unavailable since Eve is silent. With instantaneous CSIs of the main channels and statistical CSIs of wiretap channels, a common way in PHY-layer security is to consider the secrecy outage probability with wiretap coding [12], [22], i.e., to adaptively adjust the wiretap code rates for both uplink and downlink transmissions with the given secrecy outage probability constraints.

A. Uplink Adaptive Wiretap Code Rate

The ICV obtains $\mathbf{h}_{vm}$ and the SBS uses the MRC and AN schemes as described in Section IV-A. The instantaneous uplink secrecy rate can be written as

$$R_1 = [C_{v,u} - C_{e,u}]^+, \tag{37}$$

where $C_{v,u}$ and $C_{e,u}$ are formulated in Eqns. (7a) and (7b). Due to the fact that ICV cannot access Eve's CSI, it adopts secrecy outage probability as a performance metric for adaptive wiretap coding, which is defined as the probability that the target wiretap code rate of secure transmissions, i.e., R_u is larger than the secrecy rate R_1. From [22, Eq. (4)], we know that the secrecy outage probability is expressed as

$$\begin{aligned} P_{\text{out}}(R_u) &= P(R_1 \le R_u \big| \text{message transmission}) \\ &= P(C_{e,u} \ge C_{v,u} - R_u), \end{aligned} \tag{38}$$

which means that the secrecy outage probability is the conditional probability based on the reliability of transmitted codewords, i.e., SBS is able to decode correctly with the rate of transmitted codewords, where the rate can be up to $C_{v,u}$. Based on Wyner's coset based encoding theory, to achieve physical layer security, the encoder should choose two rates, namely, the rate of transmitted codewords of common messages ($C_{v,u}$), and the rate of confidential information, namely, wiretap code rate (R_u) [24]. Since we assume that ICV has perfect knowledge about the instantaneous CSI of $\mathbf{h}_{vm}$ within coherence time, it is possible to use an adaptive rate of transmitted codewords that equals to $C_{v,u}$. The remaining work is to find an appropriate R_u.

Based on the secrecy outage probability, we present an effective secrecy rate as a secrecy metric, which means an average rate secretly received at SBS over many transmission bursts with a wiretap code rate R_u, which is expressed as

$$\hat{R}_u(R_u) = \{1 - P_{\text{out}}(R_u)\}R_u. \tag{39}$$

We can emulate Eqn. (39) via Monte Carlo simulations over all realizations of $\mathbf{H}_{me}$. However, in order to adaptively adjust wiretap code rate R_u to maximize $\hat{R}_u$, it is necessary to deduce an effective secrecy rate $\hat{R}_u$. The expression is presented in Proposition 4.

Proposition 4: The effective secrecy rate of R_u, i.e., $\hat{R}_u$, can be expressed as

$$\hat{R}_u(R_u) = \{1 - F_{Z_1}(\phi_1)\}R_u, \tag{40}$$

where $\phi_1 = \frac{P_m}{P_v(N_m-1)}(2^{C_{v,u}-R_u} - 1)$,

$$\begin{aligned} F_{Z_1}(z) &= \exp(-a_1 z) \sum_{k=0}^{N_e-1} \frac{A_k(z)}{k!}(a_1 z)^k, \\ A_k(z) &= \frac{\sum_{n=0}^{N_e-k-1} \binom{N_m-1}{n} z^n}{(1+z)^{N_m-1}}, \end{aligned} \tag{41}$$

and $Z_1 = \mathbf{h}_{ve}^\dagger (a_1 \mathbf{I}_{N_e} + \mathbf{H}_1 \mathbf{H}_1^\dagger)^{-1} \mathbf{h}_{ve}$ represents a random variable, where $a_1 = \frac{\sigma_{ve}^2 (N_m-1)}{P_m}$. It is obvious that $F_{Z_1}(\phi_1)$ is the expression of secrecy outage probability of R_u.

Proof: See in Appendix E. ∎

Proposition 4 provides exact expressions of Eqn. (39) and $P_{\text{out}}(R_u) = F_{Z_1}(\phi_1)$. We can further simplify the expression if Eve has a very high SNR, i.e., $P_m/\sigma_{ve}^2 \to \infty$, as shown in Corollary 3.

Corollary 3: When $P_m/\sigma_{ve}^2 \to \infty$, the effective secrecy rate $\hat{R}_u$ can be expressed approximately as

$$\hat{R}_u(R_u) \simeq \{1 - Q_{Z_1}(\phi_1)\}R_u, \tag{42}$$

where $\phi_1 = \frac{P_m}{P_v(N_m-1)}(2^{C_{v,u}-R_u} - 1)$,

$$Q_{Z_1}(z) = \frac{\sum_{n=0}^{N_e-1} \binom{N_m-1}{n} z^n}{(1+z)^{N_m-1}}, \tag{43}$$

and $Z_1 = \mathbf{h}_{ve}^\dagger (\mathbf{H}_1 \mathbf{H}_1^\dagger)^{-1} \mathbf{h}_{ve}$ represents a random variable.

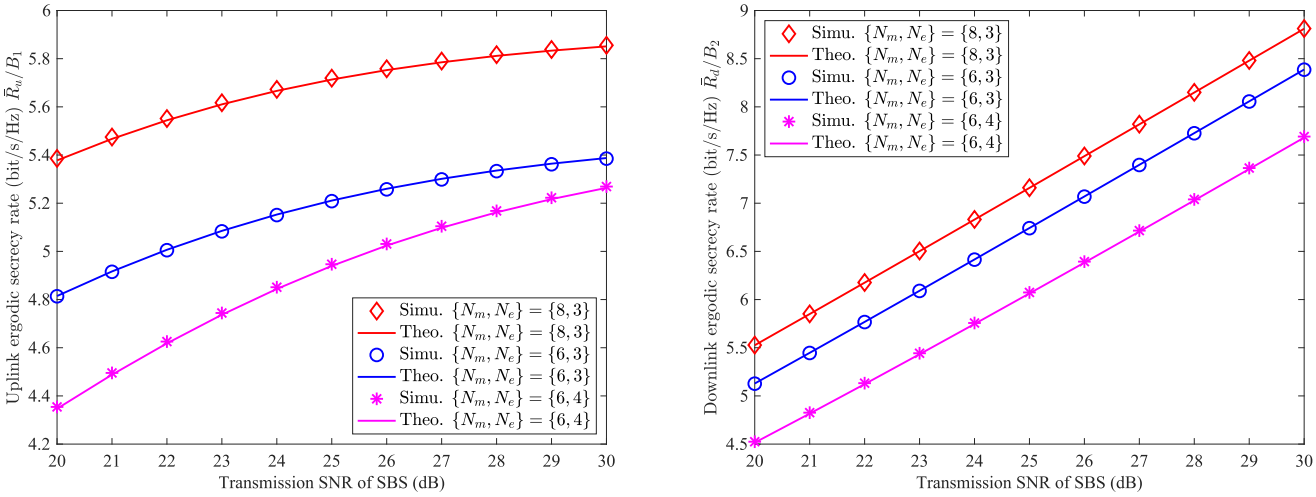
Proof: When $P_m/\sigma_{ve}^2 \to \infty$, we get $a_1 = 0$. Then, $Q_{Z_1}(z) = A_0(z)$, and thus it is easy to obtain Eqn. (42). An approximated expression of secrecy outage probability, i.e., Eqn. (43), is also given in [45, Eq. (45)]. ∎

1) Effective Secrecy Rate Maximization: Based on Proposition 4, we propose an adaptive wiretap coding scheme to maximize effective secrecy rate as follows.

$$(\hat{R}_u^*, R_u) = \max_{P_{\text{out}}(R_u) \le \varepsilon_u} \hat{R}_u(R_u), \tag{44}$$

where the optimal $\hat{R}_u$, i.e., $\hat{R}_u^*$, and the corresponding R_u can be obtained via one-dimensional search on the function $\hat{R}_u(R_u)$ with a secrecy outage probability constraint ε_u.

2) Secrecy Outage Limitation: An alternative adaptive wiretap coding scheme considers only secrecy outage probability. With a secrecy outage limitation $P_{\text{out}}(R_u) \le \varepsilon_u$, we can maximize R_u via the inverse operation of $\varepsilon_u = P_{\text{out}}(R_u)$ due to the fact that $P_{\text{out}}(R_u) = F_{Z_1}(\phi_1)$ is a decreasing function of R_u. The method is much simpler than that of effective secrecy rate maximization, which does not require any search algorithms.



(a) Uplink ergodic secrecy rates. (b) Downlink ergodic secrecy rates.

Fig. 2. Numerical results of uplink and downlink ergodic secrecy rates in terms of SBS transmission SNR, where ICV transmission SNR is 10 dB in uplink.

B. Downlink Adaptive Wiretap Code Rate

The SBS obtains $\mathbf{h}_{mv}$ and uses the MRT and AN schemes as described in Section IV-B. In this case, the instantaneous downlink secrecy rate can be formulated as

$$R_2 = [C_{v,d} - C_{e,d}]^+, \tag{45}$$

where $C_{v,d}$ and $C_{e,d}$ are formulated in Eqns. (28a) and (28b). Similar to Proposition 4, effective secrecy rate $\hat{R}_d$ can be expressed as

$$\hat{R}_d(R_d) = \{1 - P_{\text{out}}(R_d)\}R_d. \tag{46}$$

Proposition 5: The effective secrecy rate of R_d, i.e., $\hat{R}_d$, can be expressed as

$$\hat{R}_u(R_u, C_{v,u}) = \{1 - F_{Z_2}(\phi_2)\}R_u, \tag{47}$$

where $\phi_2 = 2^{C_{v,d}-R_d} - 1$,

$$P_{Z_2}(z) = \exp(-za_2) \sum_{k=0}^{N_e-1} \frac{A_k(z)}{k!}(za_2)^k,$$
$$A_k(z) = \frac{\sum_{n=0}^{N_e-k-1} \binom{N_m-1}{n} z^n}{(1+z)^{N_m-1}}, \tag{48}$$

$Z_2 = \mathbf{h}_1^\dagger(a_2\mathbf{I}_{N_e} + \mathbf{H}_3\mathbf{H}_3^\dagger)^{-1}\mathbf{h}_1$ represents a random variable, and $a_2 = \frac{N_m\sigma_{me}^2}{P_m}$. The adaptive channel coding with $C_{v,d}$ is used in SBS with the knowledge of $\mathbf{h}_{mv}$.

Proof: Similar to Proposition 4. ■

With effective secrecy rate $\hat{R}_d$ and secrecy outage probability $F_{Z_2}(\phi)$, an SBS can execute effective secrecy rate maximization or adaptive rate adjustment with the secrecy outage limitations, similar to that in the uplink phase.

C. Computation Complexity Analysis

Next, let us discuss about the computation complexity of the proposed scheme as follows.

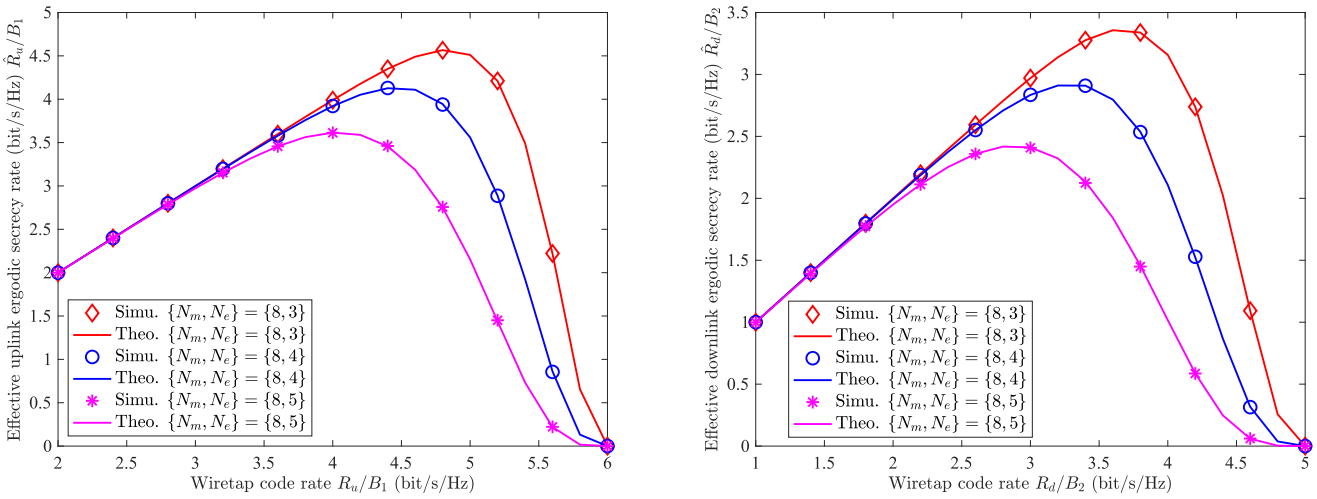
The precoding/coding process of PHY-layer security includes uplink/downlink precoding and adaptive wiretap coding. The computation complexity of the wiretap codebook encoding and decoding is $O(M)$, where M is the number of lattice points [24], [46]. As shown in Propositions 4 and 5, adaptive adjustment of wiretap coding rates can be achieved by Golden-section searching algorithm with its computation complexity $O\big(\log(1/\epsilon)\big)$, where ϵ is the required accuracy. For uplink precoding, SBS should generate the MRC receiver $\mathbf{w}_m = \mathbf{h}_{vm}^\dagger/|\mathbf{h}_{vm}|$ and the nullspace $\mathbf{G}_u$, which need $O(4N_m)$ and $O(3N_m^2 + 4N_m)$ time overhead, respectively. Similarly, for downlink precoding, SBS needs $O(4N_m)$ and $O(2N_m^2 + 3N_m)$ time overhead to generate the MRT vector $\mathbf{w}_d = \mathbf{h}_{mv}^\dagger/|\mathbf{h}_{mv}|$ and the nullspace $\mathbf{G}_d$, respectively [47]. In conclusion, the computation complexity of the precoding algorithms is polynomial and thus practical in 5G communication systems.

Note that computation task partition ratio is calculated by ergodic secrecy rates $\bar{R}_u$ and $\bar{R}_d$, which can be viewed as the given system parameters because $\bar{R}_u$ and $\bar{R}_d$ are determined by the pre-defined parameters $\{a_v, a_m, N_m, N_e, P_m, P_v\}$ as shown in Propositions 1 and 2, with no dependence on the instantaneous CSIs of both main and wiretap channels. Also, the optimal computation task partition ratio between onboard computers and MEC servers has been formulated in a closed-form solution, as shown in Proposition 3, which can be calculated with very little computation overhead.

VI. Numerical and Simulation Results

In this section, we first examine Propositions 1, 2, 4, and 5 in Figs. 2(a), 2(b), 3(a), and 3(b), respectively. These figures show the good agreements between theoretical results (Theo.) and Monte Carlo simulation results (Simu.) from 10^5 independent runs.

In particular, Fig. 2(a) illustrates the impact of transmission SNR of SBSs on uplink ergodic secrecy rates, where theoretical results were calculated from Proposition 1, and Monte Carlo simulations were done based on Eqn. (8). We can see that ergodic secrecy rates increase with an increasing transmission SNR of SBSs, and will reach to a constant,



(a) Uplink effective secrecy rates. (b) Downlink effective secrecy rates.

Fig. 3. Numerical results of uplink and downlink effective secrecy rates in terms of wiretap code rates, where transmission SNRs of ICV and SBS are 10 dB and 20 dB, $C_{v,u}/B_1 = 6$ bit/s/Hz, and $C_{v,d}/B_2 = 5$ bit/s/Hz.

which is consistent with the discussions in Remark 1. Also, more antennas at SBSs can yield a better performance, while an increasing number of Eve's antennas will reduce ergodic secrecy rates. Fig. 2(b) shows the impact of SNR on the downlink, where theoretical results were calculated from Proposition 2, and Monte Carlo simulations were based on Eqn. (29). We can see that ergodic secrecy rates grow almost linearly with SNR, which is also consistent with Remark 2. The ergodic secrecy rate is a representative performance index of the proposed scheme. As shown in Figs. 2(a) and 2(b), uplink and downlink ergodic secrecy rates are approximately 6 bit/s/Hz and 9 bit/s/Hz, respectively, i.e., 120 Mbps and 180 Mbps for secrecy transmission over a 20 MHz channel.

Theoretical results of Propositions 4 and 5 are verified in Figs. 3(a) and 3(b), respectively, where Monte Carlo simulations were done based on Eqns. (39) and (46), respectively. Here, we assume that the main capacities of uplink and downlink are 6 and 5 bit/s/Hz, respectively. The main capacities of uplink are higher than that of downlink channels, which is reasonable because the uplink transmission phases have the access to additional power offered by ICV. As shown in Fig. 3(a), we find that effective secrecy rate $\hat{R}_u$ increases with an increasing wiretap code rate R_u at the beginning, since instantaneous secrecy rate R_1 is larger than R_u with a large probability. Then, $\hat{R}_u$ will decrease with R_u because a large R_u will cause a large secrecy outage probability. The downlink phase in Fig. 3(b) shows a similar phenomenon in the uplink phase. Moreover, we find only one peak in each curve in Figs. 3(a) and 3(b), which is consistent with the results shown in [22], meaning that we can use unimodal function-aimed search algorithms, such as golden-section search.

The simulation results are provided to investigate joint impacts of computing capacities, transmission SNR, and the number of antennas on system latency. We assume that an autonomous control task has 610 KB images, in which these images are processed with full granular data-partition [7], [10], [11], and part of the data ($\eta^* \times 610$ KB) will be compressed and uploaded. We use 20 MHz bandwidth[3] for uplink and downlink as defined in 3GPP LTE-V2X [48], [49]. The compressed ratio of a file β is set to 0.4 [50]. The output to input data ratio in the MEC server α is set to 0.4. In addition, four different schemes, i.e., ICV alone, MEC server alone, SCOS, and the scheme that tasks are partitioned with CSIs obtained at the beginning of transmissions, are compared, which are described as follows.

1) ICV alone: The whole task is executed in an ICV.
2) MEC alone: The whole task is uploaded and executed in an MEC server. PHY-layer security schemes with effective uplink and downlink secrecy rate maximization are used.
3) SCOS: Simulations use ergodic secrecy rates for task partition, and use PHY-layer security schemes with effective secrecy rate maximization in both uplink and downlink.
4) Task partition with initial CSIs: Simulations use CSIs obtained at the beginning of uplink transmissions for task partition and also use PHY-layer security methods. That is, estimate $\mathbf{h}_{vm}$ before sending data to an SBS, with an assumption of $\mathbf{h}_{mv} = \mathbf{h}_{vm}$, which are constant during the entire process. We also assume that Eve's CSIs can be obtained, and then we calculate the corresponding secrecy rates of uplink and downlink phases for task partition. The assumption of constant initial CSIs was also used in the literature, such as [8]–[11].

In the simulations, we ignored the overhead of data compression/decompression and task partition because these customized functions can be decoupled from the data forwarding via software-defined network (SDN) technologies [15], [51],

[3]3GPP Release 16 supports 10, 20, 30, and 40 MHz bandwidth for New Radio (NR)-V2X [48], and will introduce new channel bandwidth for NR-V2X licensed bands for future applications.

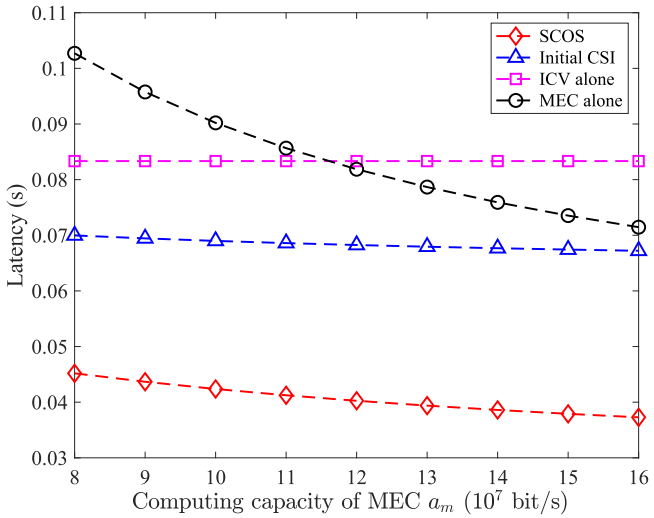


Fig. 4. Latency in terms of MEC server computing capacity, i.e., a_m, where we set $a_v = 6 \times 10^7$ bit/s, $N_m = 10$, $N_e = 4$, and transmission SNRs of SBS and ICV are 20 dB and 10 dB, respectively.

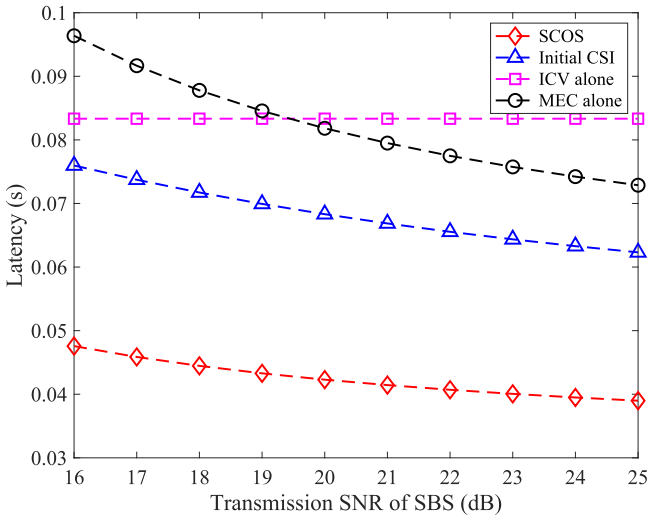


Fig. 6. Latency in terms of transmission SNR of SBS, where we set $a_m = 12 \times 10^7$ bits/s, $a_v = 6 \times 10^7$ bit/s, $N_m = 10$, $N_e = 4$, and transmission SNR of ICV is 10 dB.

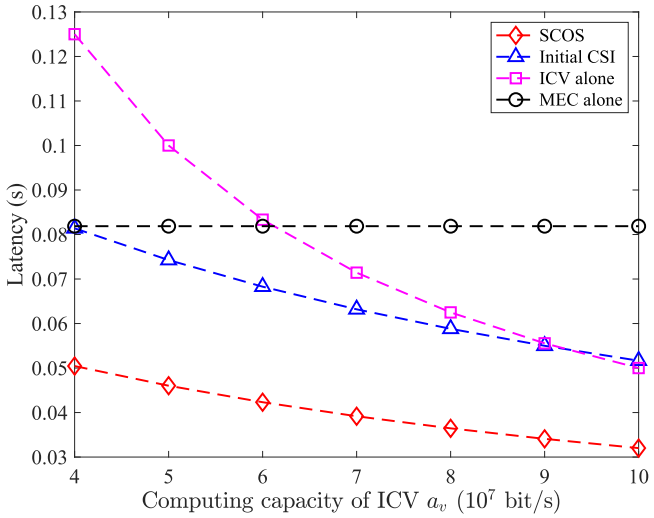


Fig. 5. Latency in terms of ICV computing capacity, i.e., a_v, where we set $a_m = 12 \times 10^7$ bit/s, $N_m = 10$, $N_e = 4$, and transmission SNRs of SBS and ICV are 20 dB and 10 dB, respectively.

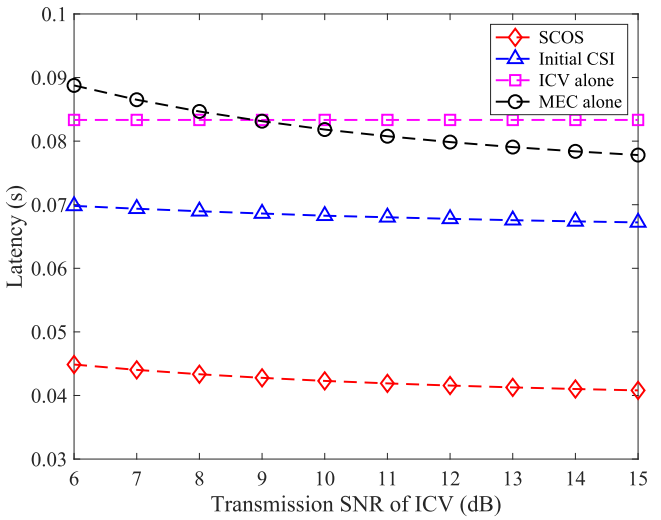


Fig. 7. Latency in terms of transmission SNR of ICV, where we set $a_m = 12 \times 10^7$ bits/s, $a_v = 6 \times 10^7$ bit/s, $N_m = 10$, $N_e = 4$, and transmission SNR of MEC server is 20 dB.

in which the overhead is much smaller than that of vehicular computation. Each simulation runs 10000 times.

Next, we want to show the impact of MEC server computing capacity on system latency in Fig. 4. Several observations can be made as follows. First, SCOS has a better performance than others, and the scheme of MEC server alone outperforms the scheme with initial CSIs when MEC server computing capacity is large enough. Second, latency decreases with an increasing MEC server computing capacity, but its gain is not large enough because the smallest one of a_m, R_u, and R_d decides the capability of edge computing as discussed in Remark 4. Unilateral increasing of a_m can not provide a large gain if R_u and R_d are limited. Also, if we use local computing resources only, latency keeps constant. Note that latency of simulations is approximately 50 ms with the proposed scheme. Nevertheless, the round-trip time of LTE BS caused by access and control scheduling should be added in total latency in real-world systems. The round-trip time is approximately 20 ms in 4G and will be reduced to less than 10 ms in 5G NR [52].

The effect of ICV computing capacity is shown in Fig. 5. Similar to the MEC server computing capacity, an increasing ICV computing capacity also reduces latency, and yet provides a higher gain than the MEC server computing capacity as the lines drop quickly. It shows that a better way to improve vehicle performance is to increase ICV computing capacity, rather than the MEC server, because MEC-assisted vehicular computation follows the cask principle.

The effects of transmission SNRs of SBS and ICV are examined in Figs. 6 and 7, respectively. These figures show similar trends that latency reduces with an increasing transmission SNR in SCOS, MEC server alone, and the scheme

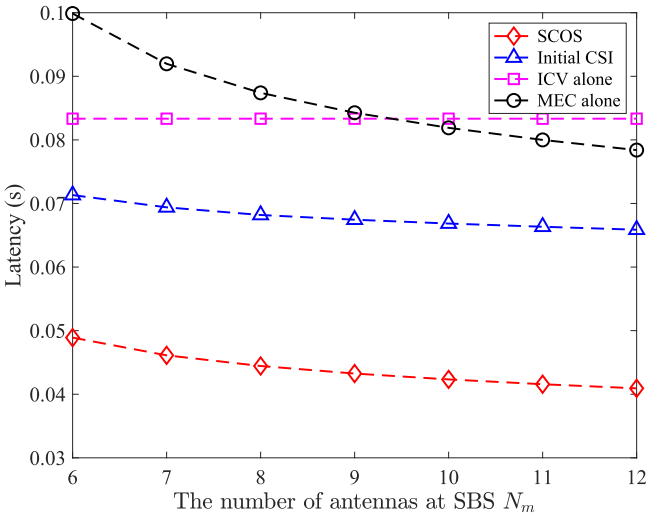


Fig. 8. Latency in terms of the number of antennas at SBS, i.e., N_m, where we set $a_m = 12 \times 10^7$ bit/s, $a_v = 6 \times 10^7$ bit/s, $N_e = 4$, and transmission SNRs of SBS and ICV are 20 dB and 10 dB, respectively.

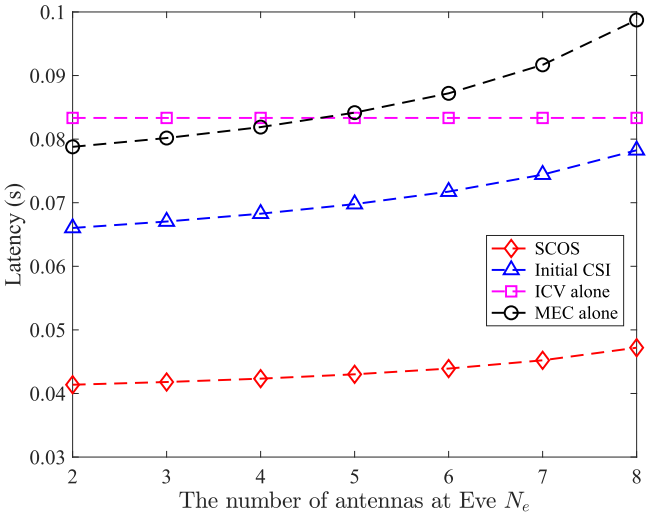


Fig. 9. Latency in terms of the number of antennas at Eve, i.e., N_e, where we set $a_m = 12 \times 10^7$ bit/s, $a_v = 6 \times 10^7$ bit/s, $N_m = 10$, and transmission SNRs of SBS and ICV are 20 dB and 10 dB, respectively.

with initial CSIs, because by increasing transmission SNR of SBS or ICV, secrecy rate between SBS and ICV increases, and latency of MEC-assisted schemes reduces. As shown in Fig. 6, we can observe that the gap between SCOS and the scheme with initial CSIs is small at the beginning, and then the gap will be enlarged with an increasing SNR of SBS. It means that the scheme with initial CSIs is very sensitive to the transmission power of SBS as SBS undertakes the tasks of secure transmissions.

Finally, Figs. 8 and 9 illustrate the impacts of the number of antennas on system latency. From Fig. 8, we can observe that an increasing number of antennas at Eve will increase latency because secrecy rates will be reduced with an increasing number of antennas at Eve. An opposite trend can be seen in Fig. 9, where secrecy rates increase with an increasing number of antennas at SBS, such that latency will be decreased. Also, the gain of N_m is small, because an increasing N_m provides a small gain on R_u that is limited by the upper bound $C_{v,u}$. Nevertheless, an increasing number of antennas at Eve will cause a large latency in the system.

VII. Conclusion and Future Works

In this paper, we proposed SCOS, in which an ICV can offload part of computation tasks to an MEC server to minimize computation delay for latency-critical vehicular communications. Specifically, we designed a computation task partition scheme, as well as a way to secure uplink and downlink transmissions between ICV and SBS. We adopted ergodic uplink and downlink secrecy rates for task partition and adaptive wiretap coding to avoid a large secrecy outage probability incurred by high mobility. Simulation results have shown that SCOS can reduce system latency significantly by almost 40% in comparison with state-of-the-art schemes. According to the computation complexity analysis, the proposed scheme can be applied to computation offloading in 5G for autonomous driving applications because it does not cause a huge burden to 5G wireless communication systems. As one of our future works, we will integrate multi-antenna technologies with ICV, in which multiple independent secrecy information streams will be transmitted between ICV and SBS, so that feedback latency of computation tasks can be reduced further. Also, we should address the problems caused by the correlation between wiretap and legitimate channels if Eve has mobility like ICV.

Appendix A
Proof of Proposition 1

Recall Eqn. (8) as

$$\bar{R}_u = \mathrm{E}_{\mathbf{h}_{vm}}[C_{v,u}] - \mathrm{E}_{\mathbf{h}_{vm},\mathbf{h}_{ve},\mathbf{H}_{me}}[C_{e,u}]. \tag{49}$$

Based on [53, Eq. (21)], we know $\mathrm{E}_{\mathbf{h}_{vm}}[C_{v,u}]$ has a closed-form expression as

$$\mathrm{E}_{\mathbf{h}_{vm}}[C_{v,d}] = \frac{B_1}{\ln(2)} \exp(\rho_1) \sum_{k=0}^{N_m-1} E_{k+1}(\rho_1), \tag{50}$$

where $\rho_1 = \frac{\sigma_{vm}^2}{P_v}$, and $E_{\tau(z)}$ is an exponential integral of order τ as defined in Eqn. (13).

Then, we can simplify $C_{e,u}$ as

$$\begin{aligned} C_{e,u} &= B_1 \log_2 \det\left(\mathbf{I}_{N_e} + \frac{P_v \mathbf{h}_{ve}\mathbf{h}_{ve}^\dagger}{\sigma_{ve}^2 \mathbf{I}_{N_e} + \frac{P_m}{N_m-1}\mathbf{H}_1\mathbf{H}_1^\dagger}\right) \\ &= B_1 \log_2 \det\left(\frac{\mathbf{I}_{N_e} + \rho_2 \mathbf{H}_1\mathbf{H}_1^\dagger + P_v/\sigma_{ve}^2 \mathbf{h}_{ve}\mathbf{h}_{ve}^\dagger}{\mathbf{I}_{N_e} + \rho_2 \mathbf{H}_1\mathbf{H}_1^\dagger}\right) \\ &= B_1 \log_2 \det\left(\frac{\mathbf{I}_{N_e} + \mathbf{H}_2\mathbf{Q}\mathbf{H}_2^\dagger}{\mathbf{I}_{N_e} + \rho_2 \mathbf{H}_1\mathbf{H}_1^\dagger}\right), \end{aligned} \tag{51}$$

where $\mathbf{Q} = \mathrm{diag}(P_v/\sigma_{ve}^2, \rho_2, \ldots, \rho_2)$, $\mathbf{H}_1 = \mathbf{H}_{me}\mathbf{G}_u \in \mathbb{C}^{N_e \times (N_m-1)}$, and $\mathbf{H}_2 = [\mathbf{h}_{ve}, \mathbf{H}_1] \in \mathbb{C}^{N_e \times N_m}$. Hence, the second part of Eqn. (49), i.e., $\mathrm{E}_{\mathbf{h}_{vm},\mathbf{h}_{ve},\mathbf{H}_{me}}[C_{e,u}]$, can

be expressed as

$$\begin{aligned}&\mathrm{E}_{\mathbf{h}_{vm},\mathbf{h}_{ve},\mathbf{H}_{me}}[C_{e,u}]\\&=\mathrm{E}\left[B_1\log_2\det\left(\frac{\mathbf{I}_{N_e}+\mathbf{H}_2\mathbf{Q}\mathbf{H}_2^{\dagger}}{\mathbf{I}_{N_e}+\rho_2\mathbf{H}_1\mathbf{H}_1^{\dagger}}\right)\right]\\&=B_1\{\Psi(\mathbf{H}_2,\rho_2,P_v)-C(\mathbf{H}_1,\rho_2)\},\end{aligned}\tag{52}$$

where

$$\Psi(\mathbf{H}_2,\rho_2,P_v)=\mathrm{E}_{\mathbf{H}_2}[\log_2\det(\mathbf{I}_{N_e}+\mathbf{H}_2\mathbf{Q}\mathbf{H}_2^{\dagger})],\tag{53a}$$

$$C(\mathbf{H}_1,\rho_2)=\mathrm{E}_{\mathbf{H}_1}[\log_2\det(\mathbf{I}_{N_e}+\rho_2\mathbf{H}_1\mathbf{H}_1^{\dagger})],\tag{53b}$$

because $\mathbf{H}_1$ and $\mathbf{H}_2$ are mutually independent complex Gaussian random matrices [35]. According to [53, Eq. (18)], we have a closed-form expression of $C(\mathbf{H}_1,\rho_2)$ as in Eqn. (12). $\Psi(\mathbf{H}_2,\rho_2,P_v)$ can be deduced by ergodic mutual information in an MIMO Rayleigh fading channel with an input covariance matrix $\mathbf{Q}$, which is written as

$$\Psi(\mathbf{H}_2,\rho_2,P_v)=C_{\mathrm{SU}}(N_m,P_v,\mathbf{Q}),\tag{54}$$

where the ergodic mutual information $C_{\mathrm{SU}}(N_m,P_v,\mathbf{Q})$ is formulated in [54, Eq. (30)].

Substituting $C(\mathbf{H}_1,\rho_2)$, (54), and (50) to Eqn. (49), we get Eqn. (9) in Proposition 1. The proof is completed. ■

Appendix B
Proof of Corollary 1

Based on [55, Eq. (80)] and the condition $N_e\le N_m-1$, we have the lower bound of $C(\mathbf{H}_1,\rho_2)$ as

$$C(\mathbf{H}_1,\rho_2)\ge N_e\log_2(\rho_2)+\sum_{i=0}^{N_e-1}\psi(N_m-1-i),\tag{55}$$

where $\psi(x)$ is defined in Eqn. (22).

Then, we can rewrite $\Psi(\mathbf{H}_2,\rho_2,P_v)$ as

$$\begin{aligned}\Psi(\mathbf{H}_2,\rho_2,P_v)&=\mathrm{E}_{\mathbf{H}_2}[\log_2\det(\mathbf{I}_{N_e}+\mathbf{H}_2\mathbf{Q}\mathbf{H}_2^{\dagger})]\\&=\mathrm{E}_{\mathbf{H}_2}[\log_2\det(\mathbf{I}_{N_e}+\rho_2\mathbf{H}_2\mathbf{Q}'\mathbf{H}_2^{\dagger})],\end{aligned}\tag{56}$$

where

$$\mathbf{Q}'=\mathrm{diag}\Big(\frac{P_v}{\sigma_{ve}^2\rho_2},1,\ldots,1\Big).\tag{57}$$

We use Jensen's inequality to get

$$\begin{aligned}&\mathrm{E}_{\mathbf{H}_2}[\log_2\det(\mathbf{I}_{N_e}+\rho_2\mathbf{H}_2\mathbf{Q}'\mathbf{H}_2^{\dagger})]\\&\qquad\le\log_2\{\det(\mathbf{I}_{N_e}+\rho_2\mathrm{E}_{\mathbf{H}_2}[\mathbf{H}_2\mathbf{Q}'\mathbf{H}_2^{\dagger}])\}.\end{aligned}\tag{58}$$

Based on [56, Eqs. (5) and (7)], in a high SNR region, we have the upper bound of $\Psi(\mathbf{H}_2,\rho_2,P_v)$ as

$$\begin{aligned}&\Psi(\mathbf{H}_2,\rho_2,P_v)\\&\le\log_2\Big\{\rho_2^{N_e}\sum_{i=0}^{N_e}[N_m-i+1]_i\mathrm{Tr}_i(\mathbf{Q}')\Big\}\\&=N_e\log_2(\rho_2)+\log_2\Big\{\sum_{i=0}^{N_e}[N_m-i+1]_i\mathrm{Tr}_i(\mathbf{Q}')\Big\},\end{aligned}\tag{59}$$

where the function $\mathrm{Tr}_i(\mathbf{W}),i=0,\ldots,K$ is the i-th elementary symmetric function of $(K\times K)$ matrix $\mathbf{W}$. $\mathrm{Tr}_i(\mathbf{W})$ depends only on the eigenvalues of $\mathbf{W}$, which are denoted by $\lambda_1,\ldots,\lambda_K$. For instance, $\mathrm{Tr}_0(\mathbf{W})=1$, $\mathrm{Tr}_1(\mathbf{W})=\mathrm{Tr}(\mathbf{W})$, and $\mathrm{Tr}_K(\mathbf{W})=\det(\mathbf{W})$. In general, $\mathrm{Tr}_i(\mathbf{W})=\sum_{i=1}^{K}\lambda_{j_1}\times\lambda_{j_2}\ldots\times\lambda_{j_i}$, where the sum is calculated over all $\binom{K}{i}$ combinations of i indices with $j_1<\ldots<j_i$. Based on the characteristics of $\mathbf{Q}'$, we have $\mathrm{Tr}_0(\mathbf{Q}')=1$, $\mathrm{Tr}_1(\mathbf{Q}')=P_v/(\sigma_{ve}^2\rho_2)+N_m-1$, $\mathrm{Tr}_{N_m}(\mathbf{Q}')=P_v/(\sigma_{ve}^2\rho_2)$, and

$$\begin{aligned}&\sum_{i=0}^{N_e}[N_m-i+1]_i\mathrm{Tr}_i(\mathbf{Q}')\\&=1+\sum_{i=1}^{N_e}[N_m-i+1]_i\binom{N_m-1}{i-1}\frac{P_v}{\sigma_{ve}^2\rho_2}\\&\quad+\sum_{i=1}^{N_e}\sum_{j=2}^{N_m}[N_m-i+1]_i\binom{N_m-j}{i-1},\end{aligned}\tag{60}$$

which reduces the complexity of the trace operations. Substituting (55), (59), and (50) to Eqn. (49), we obtain the lower bound of Eqn. (49) as shown in Eqn. (21) of Corollary 1. The proof is completed. ■

Appendix C
Proof of Corollary 2

Recall the ergodic secrecy rate in downlink phases $\bar{R}_d$ as

$$\bar{R}_d=B_2\{\Phi(\rho_3)+C(\mathbf{H}_3,\rho_4)-C(\mathbf{H}_4,\rho_4)\}.\tag{61}$$

Similar to Corollary 1, the lower bound of $C(\mathbf{H}_3,\rho_4)$ in a high SNR region can be expressed as

$$C(\mathbf{H}_3,\rho_4)\ge N_e\log_2(\rho_4)+\sum_{i=0}^{N_e-1}\psi(N_m-1-i),\tag{62}$$

where $\psi(x)$ is defined in Eqn. (22). Based on [55, Eq. (81)], we have the upper bound of $C(\mathbf{H}_4,\rho_4)$ in a high SNR region as

$$C(\mathbf{H}_4,\rho_4)\le N_e\log_2(\rho_4)+\log_2\left(\frac{N_m!}{(N_m-N_e)!}\right).\tag{63}$$

Substituting Eqns. (62), (63), and (50) to Eqn. (61), we have Eqn. (32) in Corollary 2. The proof is completed. ■

Appendix D
Proof of Proposition 3

We can adopt a reverse-proof method to show Proposition 3. Differentiating $T_v(\eta)$ and $T_{\mathrm{MEC}}(\eta)$ with respect to η, we get

$$\begin{aligned}\frac{dT_v(\eta)}{d\eta}&=\frac{M}{a_v},\\\frac{dT_{\mathrm{MEC}}(\eta)}{d\eta}&=-\Big(\frac{M}{a_m}+\frac{\beta M}{\bar{R}_u}+\frac{\alpha M}{\bar{R}_d}\Big),\end{aligned}\tag{64a}$$

which means that $T_v(\eta)$ is a monotonically increasing function of η, and $T_{\mathrm{MEC}}(\eta)$ is a monotonically decreasing function of η.

Find η_0 as

$$f_0=T_v(\eta_0)=T_{\mathrm{MEC}}(\eta_0),\tag{65}$$

and assume that $\eta_1\ne\eta_0$ minimizes $\max\{T_v(\eta),T_{\mathrm{MEC}}(\eta)\}$ as

$$f_1=\max\big(T_v(\eta_1),T_{\mathrm{MEC}}(\eta_1)\big),\tag{66}$$

such that $f_1 < f_0$. First, considering the case $T_v(\eta_1) > T_{\text{MEC}}(\eta_1)$, we have

$$T_{\text{MEC}}(\eta_0) = T_v(\eta_0) > T_v(\eta_1) > T_{\text{MEC}}(\eta_1). \tag{67}$$

Since $T_v(\eta_0) > T_v(\eta_1)$, we get $\eta_0 > \eta_1$. In this case, $T_{\text{MEC}}(\eta_0) < T_{\text{MEC}}(\eta_1)$ because $T_{\text{MEC}}(\eta)$ is a monotonically decreasing function, which is contradictory to Eqn. (67). For $T_v(\eta_1) \leq T_{\text{MEC}}(\eta_1)$, the proof is similar to the case $T_v(\eta_1) > T_{\text{MEC}}(\eta_1)$. Thus, $\eta_1 \neq \eta_0$ can not minimize $\max\{T_v(\eta), T_{\text{MEC}}(\eta)\}$, and only η_0 can minimize it.

Then, we solve the equation

$$T_{\text{MEC}}(\eta) = T_v(\eta), \tag{68}$$

and get the solution as in Eqn. (35). The proof is completed. ∎

APPENDIX E
PROOF OF PROPOSITION 4

Here, Lemma 1 is used to prove Proposition 4.

Lemma 1 (Proved in [57]): For $a \times 1$ vector $\mathbf{h}$ and $a \times (b-1)$ matrix $\mathbf{H}$ that consist of i.i.d. complex Gaussian entries obeying $\mathcal{CN}(0,1)$, the complementary cumulative distribution function (CCDF) of $Z = \mathbf{h}^\dagger (r\mathbf{I}_a + \mathbf{H}\mathbf{H}^\dagger)^{-1}\mathbf{h}$ is given by

$$\begin{aligned} F_Z(z) &= \exp(-zr) \sum_{k=0}^{a-1} \frac{A_k(z)}{k!} (zr)^k, \\ A_k(z) &= \frac{\sum_{n=0}^{a-k-1} \binom{b-1}{n} z^n}{(1+z)^{b-1}}, \end{aligned} \tag{69}$$

where r is a non-negative real number.

As channel capacity $C_{v,u}$ can be calculated by $\mathbf{h}_{vm}$ and Eqn. (6a), and $\mathbf{H}_1 = \mathbf{H}_{me}\mathbf{G}_u$ is a cyclic symmetry complex Gaussian matrix [35], we can transform $P_{\text{out}}(R_u)$ to

$$\begin{aligned} P_{\text{out}}(R_u) &= P(C_{e,u} > C_{v,u} - R_u) \\ &= P(\mathbf{h}_{ve}^\dagger (a_1 \mathbf{I}_{N_e} + \mathbf{H}_1 \mathbf{H}_1^\dagger)^{-1} \mathbf{h}_{ve} \geq \phi_1) \\ &= F_{Z_1}(\phi_1), \end{aligned} \tag{70}$$

where $Z_1 = \mathbf{h}_{ve}^\dagger (a_1 \mathbf{I}_{N_e} + \mathbf{H}_1 \mathbf{H}_1^\dagger)^{-1} \mathbf{h}_{ve}$, $\phi_1 = \frac{P_m}{P_v(N_m-1)}(2^{C_{v,u}-R_u} - 1)$, and $a_1 = \frac{\sigma_{ve}^2 (N_m-1)}{P_m}$. Substituting Eqn. (70) into Eqn. (39), we obtain the expression of effective secrecy rates as in Eqn. (47). The proof is completed. ∎

REFERENCES

[1] S. Zhang, J. Chen, F. Lyu, N. Cheng, W. Shi, and X. Shen, "Vehicular communication networks in the automated driving era," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 26–32, Sep. 2018.

[2] F. Lyu *et al.*, "Characterizing urban vehicle-to-vehicle communications for reliable safety applications," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 6, pp. 2586–2602, Jun. 2020.

[3] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: Challenges," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 26–33, Jan. 2017.

[4] D. Yang *et al.*, "Intelligent and connected vehicles: Current status and future perspectives," *Sci. China Technol. Sci.*, vol. 61, no. 10, pp. 1446–1471, Oct. 2018.

[5] J. Mei, K. Zheng, L. Zhao, Y. Teng, and X. Wang, "A latency and reliability guaranteed resource allocation scheme for LTE V2 V communication systems," *IEEE Trans. Wireless Commun.*, vol. 17, no. 6, pp. 3850–3860, Jun. 2018.

[6] *Tesla Online Store*. Accessed: Nov. 12, 2020. [Online]. Available: https://www.tesla.com/models/design#autopilot

[7] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2322–2358, 4th Quart., 2017.

[8] X. Hu, K.-K. Wong, K. Yang, and Z. Zheng, "UAV-assisted relaying and edge computing: Scheduling and trajectory optimization," *IEEE Trans. Wireless Commun.*, vol. 18, no. 10, pp. 4738–4752, Oct. 2019.

[9] X. Cheng *et al.*, "Space/aerial-assisted computing offloading for IoT applications: A learning-based approach," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 5, pp. 1117–1129, May 2019.

[10] Y. Wang, M. Sheng, X. Wang, L. Wang, and J. Li, "Mobile-edge computing: Partial computation offloading using dynamic voltage scaling," *IEEE Trans. Commun.*, vol. 64, no. 10, pp. 4268–4282, Oct. 2016.

[11] X. Chen, L. Jiao, W. Li, and X. Fu, "Efficient multi-user computation offloading for mobile-edge cloud computing," *IEEE/ACM Trans. Netw.*, vol. 24, no. 5, pp. 2795–2808, Oct. 2016.

[12] X. Yang, X. Wang, Y. Wu, L. P. Qian, W. Lu, and H. Zhou, "Small-cell assisted secure traffic offloading for narrowband Internet of Thing (NB-IoT) systems," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1516–1526, Jun. 2018.

[13] J. Xu and J. Yao, "Exploiting physical-layer security for multiuser multicarrier computation offloading," *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, pp. 9–12, Feb. 2019.

[14] T. Bai, J. Wang, Y. Ren, and L. Hanzo, "Energy-efficient computation offloading for secure UAV-edge-computing systems," *IEEE Trans. Veh. Technol.*, vol. 68, no. 6, pp. 6074–6087, Jun. 2019.

[15] Z. Yan, P. Zhang, and A. V. Vasilakos, "A security and trust framework for virtualized networks and software-defined networking," *Secur. Commun. Netw.*, vol. 9, no. 16, pp. 3059–3069, Nov. 2016.

[16] B. Brecht *et al.*, "A security credential management system for V2X communications," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 12, pp. 3850–3871, Dec. 2018.

[17] J. Zhou, X. Dong, Z. Cao, and A. V. Vasilakos, "Secure and privacy preserving protocol for cloud-based vehicular DTNs," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 6, pp. 1299–1314, Jun. 2015.

[18] J. Zhou, Z. Cao, X. Dong, X. Lin, and A. V. Vasilakos, "Securing m-healthcare social networks: Challenges, countermeasures and future directions," *IEEE Wireless Commun.*, vol. 20, no. 4, pp. 12–21, Aug. 2013.

[19] Y. Zhang, C. Xu, H. Li, K. Yang, J. Zhou, and X. Lin, "HealthDep: An efficient and secure deduplication scheme for cloud-assisted eHealth systems," *IEEE Trans. Ind. Informat.*, vol. 14, no. 9, pp. 4101–4112, Sep. 2018.

[20] M. Wazid, A. K. Das, V. Bhat, and A. V. Vasilakos, "LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment," *J. Netw. Comput. Appl.*, vol. 150, Jan. 2020, Art. no. 102496.

[21] W. Wang, K. C. Teh, S. Luo, and K. H. Li, "Physical layer security in heterogeneous networks with pilot attack: A stochastic geometry approach," *IEEE Trans. Commun.*, vol. 66, no. 12, pp. 6437–6449, Dec. 2018.

[22] X. Zhou, M. R. McKay, B. Maham, and A. Hjorungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.

[23] W. K. Harrison, T. Fernandes, M. A. C. Gomes, and J. P. Vilela, "Generating a binary symmetric channel for wiretap codes," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 8, pp. 2128–2138, Aug. 2019.

[24] F. Oggier, P. Sole, and J.-C. Belfiore, "Lattice codes for the wiretap Gaussian channel: Construction and analysis," *IEEE Trans. Inf. Theory*, vol. 62, no. 10, pp. 5690–5708, Oct. 2016.

[25] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6428–6443, Oct. 2011.

[26] S. Sardellitti, G. Scutari, and S. Barbarossa, "Joint optimization of radio and computational resources for multicell mobile-edge computing," *IEEE Trans. Signal Inf. Process. Over Netw.*, vol. 1, no. 2, pp. 89–103, Jun. 2015.

[27] J. Wang, L. Zhao, J. Liu, and N. Kato, "Smart resource allocation for mobile edge computing: A deep reinforcement learning approach," *IEEE Trans. Emerg. Topics Comput.*, early access, Mar. 4, 2019, doi: 10.1109/TETC.2019.2902661.

[28] A. P. Miettinen and J. K. Nurminen, "Energy efficiency of mobile clients in cloud computing," *HotCloud*, vol. 10, no. 4, pp. 1–7, Jun. 2010.

[29] S. E. Mahmoodi, R. N. Uma, and K. P. Subbalakshmi, "Optimal joint scheduling and cloud offloading for mobile applications," *IEEE Trans. Cloud Comput.*, vol. 7, no. 2, pp. 301–313, Apr. 2019.

[30] Y. Zhou *et al.*, "Secure communications for UAV-enabled mobile edge computing systems," *IEEE Trans. Commun.*, vol. 68, no. 1, pp. 376–388, Jan. 2020.

[31] J.-B. Wang, H. Yang, M. Cheng, J.-Y. Wang, M. Lin, and J. Wang, "Joint optimization of offloading and resources allocation in secure mobile edge computing systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 8843–8854, Aug. 2020.

[32] W. Wu, F. Zhou, R. Q. Hu, and B. Wang, "Energy-efficient resource allocation for secure NOMA-enabled mobile edge computing networks," *IEEE Trans. Commun.*, vol. 68, no. 1, pp. 493–505, Jan. 2020.

[33] X. He, R. Jin, and H. Dai, "Physical-layer assisted secure offloading in mobile-edge computing," *IEEE Trans. Wireless Commun.*, vol. 19, no. 6, pp. 4054–4066, Jun. 2020.

[34] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[35] Y. Liu, H. H. Chen, and L. Wang, "Secrecy capacity analysis of artificial noisy MIMO channels—An approach based on ordered eigenvalues of Wishart matrices," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 3, pp. 617–630, Mar. 2017.

[36] Y. Liu, H. Chen, L. Wang, and W. Meng, "Artificial noisy MIMO systems under correlated scattering Rayleigh fading—A physical layer security approach," *IEEE Syst. J.*, vol. 14, no. 2, pp. 2121–2132, Jun. 2020.

[37] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.

[38] *Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall Description; Stage 2 (V15.1.0, Release 15)*, 3GPP, document 36.300, Mar. 2018, rev. 1.

[39] Z. Yan, X. Li, M. Wang, and A. V. Vasilakos, "Flexible data access control based on trust and reputation in cloud computing," *IEEE Trans. Cloud Comput.*, vol. 5, no. 3, pp. 485–498, Jul. 2017.

[40] C. S. Patel, G. L. Stuber, and T. G. Pratt, "Simulation of Rayleigh-faded mobile-to-mobile communication channels," *IEEE Trans. Commun.*, vol. 53, no. 11, pp. 1876–1884, Nov. 2005.

[41] *3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Channels and Modulation (Release 13)*, 3GPP, document 36.211, Jun. 2016, rev. 13.2.0.

[42] B. He and X. Zhou, "Secure on-off transmission design with channel estimation errors," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 1923–1936, Dec. 2013.

[43] B. Li, Z. Fei, Z. Chu, F. Zhou, K. Wong, and P. Xiao, "Robust chance-constrained secure transmission for cognitive satellite–terrestrial networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4208–4219, May 2018.

[44] O. Munoz, A. Pascual-Iserte, and J. Vidal, "Optimization of radio and computational resources for energy efficiency in latency-constrained application offloading," *IEEE Trans. Veh. Technol.*, vol. 64, no. 10, pp. 4738–4755, Oct. 2015.

[45] D. W. K. Ng, E. S. Lo, and R. Schober, "Secure resource allocation and scheduling for OFDMA Decode-and-Forward relay networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 3528–3540, Oct. 2011.

[46] N. Sloane, "Tables of sphere packings and spherical codes," *IEEE Trans. Inf. Theory*, vol. 27, no. 3, pp. 327–338, May 1981.

[47] R. Raz, "On the complexity of matrix product," in *Proc. 34th Annu. ACM Symp. Theory Comput. (STOC)*, 2002, pp. 144–151.

[48] *3rd Generation Partnership Project; Technical Specification Group Radio Access Network; V2X Services Based on NR; User Equipment (UE) Radio Transmission and Reception; (Release 16)*, 3GPP, document 38.886, 6 2020, rev. 16.1.0.

[49] R. Molina-Masegosa and J. Gozalvez, "LTE-V for sidelink 5G V2X vehicular communications: A new 5G technology for short-range vehicle-to-everything communications," *IEEE Veh. Technol. Mag.*, vol. 12, no. 4, pp. 30–39, Dec. 2017.

[50] D. Taubman, "High performance scalable image compression with EBCOT," *IEEE Trans. Image Process.*, vol. 9, no. 7, pp. 1158–1170, Jul. 2000.

[51] Z. Shu, J. Wan, D. Li, J. Lin, A. V. Vasilakos, and M. Imran, "Security in software-defined networking: Threats and countermeasures," *Mobile Netw. Appl.*, vol. 21, no. 5, pp. 764–776, Jan. 2016.

[52] I. Parvez, A. Rahmati, I. Guvenc, A. I. Sarwat, and H. Dai, "A survey on low latency towards 5G: RAN, core network and caching solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3098–3130, 4th Quart., 2018.

[53] H. Shin and J. Hong Lee, "Capacity of multiple-antenna fading channels: Spatial fading correlation, double scattering, and keyhole," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2636–2647, Oct. 2003.

[54] M. Chiani, M. Z. Win, and H. Shin, "MIMO networks: The effects of interference," *IEEE Trans. Inf. Theory*, vol. 56, no. 1, pp. 336–349, Jan. 2010.

[55] M. R. McKay and I. B. Collings, "General capacity bounds for spatially correlated rician MIMO channels," *IEEE Trans. Inf. Theory*, vol. 51, no. 9, pp. 3121–3145, Sep. 2005.

[56] J. Salo, F. Mikas, and P. Vainikainen, "An upper bound on the ergodic mutual information in rician fading MIMO channels," *IEEE Trans. Wireless Commun.*, vol. 5, no. 6, pp. 1415–1421, Jun. 2006.

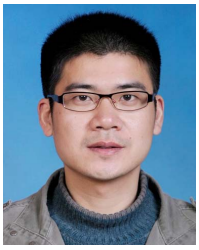
[57] H. Gao, P. J. Smith, and M. V. Clark, "Theoretical reliability of MMSE linear diversity combining in Rayleigh-fading additive interference channels," *IEEE Trans. Commun.*, vol. 46, no. 5, pp. 666–672, May 1998.

Yiliang Liu received the B.E. and M.Sc. degrees in computer science and communication engineering from Jiangsu University, Zhenjiang, China, and the Ph.D. degree from the School of Electronics and Information Engineering, Harbin Institute of Technology, Harbin, China, in 2012, 2015, and 2020, respectively. He was a Visiting Research Student with the Department of Engineering Science, National Cheng Kung University, Tainan, Taiwan, from 2014 to 2015, and the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada, from 2018 to 2019. His research interests include the security of wireless communications, physical layer security, and intelligent connected vehicles.

Wei Wang (Member, IEEE) received the B.Eng. degree in information countermeasure technology and the M.Eng. degree in signal and information processing from Xidian University, Xi'an, China, in 2011 and 2014, respectively, and the Ph.D. degree in electrical and electronic engineering from Nanyang Technological University (NTU), Singapore, in 2018. From September 2018 to August 2019, he was a Postdoctoral Fellow with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. He is currently a Professor with the Nanjing University of Aeronautics and Astronautics, Nanjing, China. His research interests include wireless communications, space-air-ground integrated networks, wireless security, and electromagnetic spectrum security. He was awarded the IEEE Student Travel Grants for the IEEE International Conference on Communications in 2017 and the Chinese Government Award for outstanding self-financed students abroad in 2018.

Hsiao-Hwa Chen (Fellow, IEEE) received the B.Sc. and M.Sc. degrees from Zhejiang University, China, and the Ph.D. degree from the University of Oulu, Finland, in 1982, 1985, and 1991, respectively. He is currently a Distinguished Professor with the Department of Engineering Science, National Cheng Kung University, Taiwan. He has authored or coauthored over 400 technical articles in major international journals and conferences, six books, and more than ten book chapters in the areas of communications. He has served as the general chair, TPC chair, and symposium chair for major international conferences. He is a fellow of the IET. He was a recipient of the Best Paper Award at the IEEE WCNC 2008 and a recipient of the IEEE 2016 Jack Neubauer Memorial Award. He has served as the Editor-in-Chief of the IEEE WIRELESS COMMUNICATIONS from 2012 to 2015. He was an elected Member-at-Large of the IEEE ComSoc from 2015 to 2016. He has served or is serving as an editor or a guest editor for numerous technical journals. He is the founding Editor-in-Chief of the *Security and Communication Networks Journal* (Wiley).

Feng Lyu (Member, IEEE) received the B.S. degree in software engineering from Central South University, Changsha, China, in 2013, and the Ph.D. degree from the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China, in 2018. During respective September 2018 to December 2019 and October 2016 to October 2017, he worked as a Postdoctoral Fellow and was a Visiting Ph.D. Student with the BBCR Group, Department of Electrical and Computer Engineering, University of Waterloo, Canada. He is currently a Professor with the School of Computer Science and Engineering, Central South University, Changsha, China. His research interests include vehicular networks, beyond 5G networks, big data measurement and application design, and could/edge computing. He was a recipient of the best paper award of IEEE ICC 2019. He currently serves as Associate Editor of the IEEE SYSTEMS JOURNAL and leading Guest Editor of *Peer-to-Peer Networking and Applications*, and served as TPC members for many international conferences. He is a member of the IEEE Computer Society, Communication Society, and Vehicular Technology Society.



Liangmin Wang (Member, IEEE) received the B.S. degree in computational mathematics from Jilin University, Changchun, China, in 1999, and the Ph.D. degree in cryptology from Xidian University, Xi'an, China, in 2007. He is currently a Full Professor with the School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang, China. He has authored or coauthored more than 60 technical papers at premium international journals and conferences, such as the IEEE/ACM TRANSACTIONS ON NETWORKING, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE Global Communications Conference, and IEEE Wireless Communications and Networking Conference. His current research interests include data security and privacy. He has served as a TPC member of many IEEE conferences, such as IEEE ICC, IEEE HPCC, and IEEE TrustCOM. He is currently an Associate Editor of *Security and Communication Networks*, a member of ACM, and a Senior Member of Chinese Computer Federation. He has been honored as a "Wan-Jiang Scholar" of Anhui Province since November 2013.

Weixiao Meng (Senior Member, IEEE) received B.Eng., M.Eng., and Ph.D. degrees from the Harbin Institute of Technology (HIT), China, in 1990, 1995, and 2000, respectively. From 1998 to 1999, he worked at NTT DoCoMo for beyond 3G. He is currently a Full Professor and the Vice Dean of the School of Electronics and Information Engineering, HIT. He has published four books and over 300 papers on journals and international conferences. He is the Chair of IEEE Communications Society Harbin Chapter, a fellow of the China Institute of Electronics, and a Senior Member of IEEE ComSoc and China Institute of Communication. He has been an editorial board member for IEEE Communications Surveys and Tutorials from 2014 to 2017, and IEEE Wireless Communications since 2015. He acted as leading TPC co-chair of ChinaCom2011 and ChinaCom2016, Awards co-chair of IEEE ICC2015, and the leading Workshop co-Chair of IEEE ICC2019 and IEEE ICNC2020. In 2005, he was selected as one of New Century Excellent Talents (NCETs) by Ministry of Education, China, in 2008, and the Distinguished Academic Leader of Harbin. Under his leadership, Harbin Chapter won IEEE ComSoc Chapter of the Year Award and Asia Pacific Region Chapter Achievement Award, and he won Member and Global Activities Contribution Award in 2018.

Xuemin (Sherman) Shen (Fellow, IEEE) received the Ph.D. degree in electrical engineering from Rutgers University, New Brunswick, NJ, USA, in 1990. He is currently a University Professor with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. His research focuses on network resource management, wireless network security, social networks, 5G and beyond, and vehicular ad hoc and sensor networks. He is a registered Professional Engineer of Ontario, Canada, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, a Royal Society of Canada Fellow, a Chinese Academy of Engineering Foreign Fellow, and a Distinguished Lecturer of the IEEE Vehicular Technology Society and Communications Society. He was a recipient of the R.A. Fessenden Award in 2019 from IEEE, Canada, James Evans Avant Garde Award in 2018 from the IEEE Vehicular Technology Society, Joseph LoCicero Award in 2015 and Education Award in 2017 from the IEEE Communications Society. He was also a recipient of the Excellent Graduate Supervision Award in 2006 and Outstanding Performance Award five times from the University of Waterloo and the Premier's Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada. He was the Technical Program Committee Chair/Co-Chair for the IEEE Globecom16, the IEEE Infocom14, the IEEE VTC10 Fall, the IEEE Globecom07, the Symposia Chair for the IEEE ICC10, the Tutorial Chair for the IEEE VTC11 Spring, and the Chair for the IEEE Communications Society Technical Committee on Wireless Communications. He is an Editor-in-Chief for the IEEE INTERNET OF THINGS JOURNAL and the Vice President on Publications of the IEEE Communications Society.