IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON COMMUNICATION AND FOG/EDGE COMPUTING TOWARDS INTELLIGENT CONNECTED VEHICLES (ICVS)

Received December 31, 2019, accepted January 4, 2020, date of publication January 8, 2020, date of current version January 16, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2964795

Optimal Access Scheme for Security Provisioning of C-V2X Computation Offloading Network With Imperfect CSI

BIN QIU[1,2], HAILIN XIAO[2], (Member, IEEE), ANTHONY THEODORE CHRONOPOULOS[3], (Senior Member, IEEE), DI ZHOU[4], AND SHAN OUYANG[5], (Senior Member, IEEE)

[1]Key Laboratory of Cognitive Radio and Information Processing, Guilin University of Electronic Technology, Guilin 541004, China
[2]School of Computer Science and Information Engineering, Hubei University, Wuhan 430062, China
[3]Department of Computer Science, The University of Texas at San Antonio, San Antonio, TX 78249, USA
[4]Zhejiang Uniview Technologies Company, Ltd., Hangzhou 310051, China
[5]Guangxi Key Laboratory of Wireless Wideband Communication and Signal Processing, Guilin University of Electronic Technology, Guilin 541004, China

Corresponding author: Hailin Xiao (xhl_xiaohailin@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61872406 and Grant 61472094, in part by the Guangxi Natural Science Foundation under Grant 2018GXNSFBA281057, and in part by the Key Research and Development Plan Project of Zhejiang Province under Grant 2018C01059.

ABSTRACT In a cellular vehicle-to-everything (C-V2X) enabled computation-offloading network, vehicular users may deliver computation tasks to a cellular base station (BS) through vehicle-to-infrastructure (V2I) transmission links in order to accommodate computation-intensive applications, where the BS is usually equipped with a mobile edge computing (MEC) server. However, due to the broadcast nature of wireless communications and high-mobility of vehicles, the computation-offloading information may suffer from an eavesdropping threat. In practice, the interference generated by device-to-device-based V2V (D2D-V) links can be utilized for protecting the offloading information against eavesdropping. This observation motivates a security provisioning for C-V2X computation-offloading network. Specifically, a dynamic threshold-based access scheme is required to maintain the interference under control for different channel conditions. Unfortunately, the previous studies that are based on the assumption of perfect channel state information (CSI) can not be applied for the dynamic vehicular networks. In this paper, we propose a dynamic threshold-based access scheme for security provisioning of C-V2X computation-offloading network by considering an imperfect CSI. In this scheme, an optimized access threshold is set to update adaptively in terms of channel estimation error for balancing both the security and reliability of the offloading link. Furthermore, the proposed scheme can maximize the secrecy throughput under a connection outage constraint of the D2D-V links, with the total area spectral efficiency optimized under the security performance criterion for the offloading link. Numerical results are provided for validating the proposed theoretical analysis. A useful design insight is provided for attaining an optimal configuration of C-V2X computation-offloading network.

INDEX TERMS Cellular V2X communication, mobile edge computing, physical-layer security, secrecy throughput, imperfect channel state information, access threshold.

I. INTRODUCTION

Mobile edge computing (MEC) has been regarded as a promising technique for supporting the tremendous demand for various data-intensive and computation-intensive applications through offloading computation tasks to MEC servers in cellular vehicle-to-everything (C-V2X) network [1]–[4]. However, due to both the broadcast nature of wireless signals and the characteristics of high-mobility in a dynamic vehicular environment, the wireless computation offloading of vehicle-to-infrastructure (V2I) or vehicle-to-vehicle (V2V) links may introduce new information security threats, e.g., MEC-based denial of service (DoS) attacks and authentication attacks [5]. Therefore, security provisioning has become a critical issue in C-V2X computation-offloading network [6], [7].

Recently, the security provisioning of vehicular networks has been widely investigated [8]–[11]. For instance, in [8],

The associate editor coordinating the review of this manuscript and approving it for publication was Junhui Zhao.

a malicious detection module was proposed in vehicular networks, where the module was utilized to detect whether there exist malicious neighboring vehicles. The works in [9], [10] presented some possible attacks, offering possible solutions for vehicular networks. Furthermore, in [11], a MEC-based malicious vehicle detection method was proposed for defending against DoS attacks. Numerical results in [11] showed that the proposed method can detect malicious vehicles with a high accuracy. However, all the above-mentioned works mainly focused on certificate revocation and cryptographic methods for an attacker operating on upper layers to improve the communication security introducing computational and communication overheads [12], [13]. As an alternative to complex cryptographic techniques, the technique of physical-layer security (PLS) relying on exploiting the physical characteristics of wireless channels has emerged as a promising approach for ensuring secure communication against eavesdropping attacks in vehicular networks [14]. In other words, the PLS secrecy level can not be compromised by the individual vehicle' limited computation resources [6].

Cooperative jamming is of great significance in enabling PLS technique that can emit interference signals to disrupt the reception of an eavesdropper, thus degrading the received signal quality of eavesdroppers [15]–[17]. Depending on the design considerations, the cooperative jamming signals were found to come from Gaussian noise or co-channel interference [18]. In [19], the co-channel interference generated by multiple device-to-device-based V2V (D2D-V) links was utilized for both impairing the wiretap channel quality and protecting the confidential messages in the vehicular heterogeneous networks. However, the co-channel interference is also an obstacle to the improvement of throughput of primary links [20]. Therefore, how to control and manage the access of spectrum multiplex links has become a key issue in keeping a desired trade-off balance between security protection efficiency and spectrum utilization. In [21], an opportunistic jammer selection scheme was presented for limiting the transmission power of D2D links, where the interference caused by a D2D pair can be utilized for intercepting eavesdroppers. In [22], the distance among nodes was employ as an access threshold for quantifying the pairing probabilities of candidate D2D nodes, where the radio channel conditions did not change. However, for a mobile vehicle environment, a dynamic access threshold following the vehicle movement must be established.

To improve the performance of security provisioning, the channel state information (CSI) plays an important role in acting as an access threshold in the C-V2X computation-offloading network. In [23], an access selection scheme was proposed for protecting the cellular users against eavesdropping under a perfect CSI, where the achievable secrecy throughput can be maximized. However, from the spectral efficiency perspective, the performance of D2D spectrum sharing network has not been investigated well in the literature. In [24], the authors maximized the area spectral efficiency (ASE) of D2D links by setting a appropriate access threshold for each D2D link, where the ASE of cellular link was neglected. In [25], a channel access scheme was proposed for controlling the interference from D2D pairs to cellular users under the perfect CSI, where the Pareto optimal access threshold was obtained for maximizing the total ASE. However, the existed works considered only a perfect knowledge of CSI. In practice, it would be hard to obtain a perfect CSI in dynamic vehicular networks because of the limited CSI feedback, an error of estimation and outdated CSI [26]–[28]. In particular, it is yet unknown how does a channel estimation error influence both the spectrum efficiency and secrecy provisioning performances of C-V2X computation-offloading network.

The main contributions of this paper are summarized in follows:

- We propose a dynamic threshold-based access scheme for security provisioning of C-V2X computation-offloading network. Unlike the studies in [21]–[23], the proposed scheme takes into account both the vehicular speed information and the feedback delay time in dynamic vehicular networks. Furthermore, the proposed scheme is capable of implementing the interference control under variant channel conditions for C-V2X computation-offloading networks.
- For the imperfect CSI, we derive the optimized access threshold for maximizing the security throughput of an offloading link under a connection outage constraint of D2D-V links. In this case, the optimized access threshold is set to update adaptively in terms of channel estimation error, thus balancing both the security and reliability of the offloading link. Numerical results show that the proposed scheme provides significant performance gains in terms of secrecy throughput compared with the previous access schemes.
- Apart from increasing security throughput, achieving a high spectral efficiency is regarded as an important issue for designing dynamic threshold-based access schemes under the security outage constraints. Hence, we obtain an optimized access threshold with imperfect CSI that aims to maximize the total ASE while satisfying the required secrecy performance of the offloading link. Unlike the existed works [24], [25], the total ASE of the D2D-V links and the offloading link is considered in acquiring the optimal solution of the access threshold at the same time. Furthermore, the optimized access threshold keeps a desired balance in the spectral efficiency trade-off between the offloading link and the D2D-V links.

The remainder of this paper is organized as follows. Section II presents the system model and performance metrics. Section III proposes a dynamic access scheme for analyzing the outage performance. Section IV presents the optimal access solutions for maximizing both the secrecy throughput and total ASE. Finally, section V provides numerical results and discussions, followed by conclusions and future work given by Section VI.

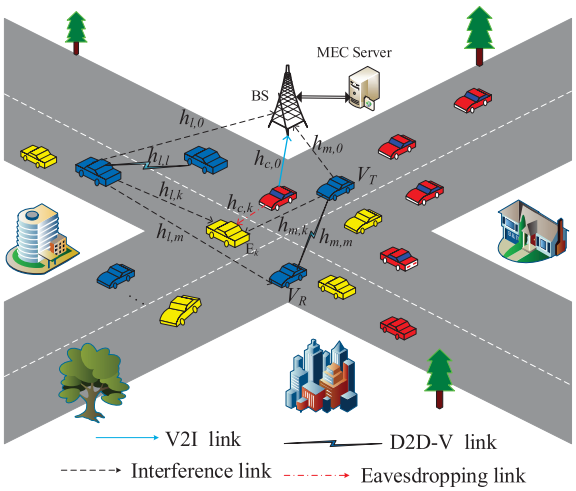


FIGURE 1. C-V2X computation-offloading network model.

Notations: $\mathcal{L}(\cdot)$ denotes the Laplace transform of a random variable, and $\mathbb{E}(\cdot)$ stands for the expectation operator. $\mathcal{CN}\left(0, \delta^2\right)$ denotes complex Gaussian distribution with mean zero and variance δ^2, and $exp(1)$ represents the exponential distribution with unit mean. Furthermore, $\Pr\{\cdot\}$ stands for a probability function. We use subscripts 0, c, m, l, and k to represent the base station (BS), the cellular vehicular user, the m-th D2D-V pair, the l-th D2D-V pair and the k-th eavesdropper, respectively. In addition, $h_{i,j}$ and $d_{i,j}$ $(i \in \{c, m, l\}, j \in \{0, m, k\})$ denote the small-scale fading and the propagation distance over the $i \to j$ link, respectively. Finally, $\Gamma(x)$ and $\Gamma(a, x)$ denote the Gamma function and incomplete Gamma function with $\Gamma(x) = \int_0^\infty t^{x-1}e^{-t}dt$, $\Gamma(a, x) = \int_x^\infty t^{a-1}e^{-t}dt$, respectively.

II. SYSTEM MODEL AND PERFORMANCE METRICS

A. SYSTEM MODEL

We consider the C-V2X computation-offloading network model in the cross roads congestion scenario, as shown in Fig. 1. A cellular vehicular user (C-VU) aims to offload its computation tasks to the BS (with a MEC server integrated) through the uplink V2I link, where the offloading transmission is captured by randomly located passive malicious eavesdropper vehicles (Eves). Without loss of generality, we assume that one and only one C-VU is allowed to offload the computation tasks to the BS. Although we limit ourselves to one C-VU for simplicity, the proposed scheme can be readily extended to the scenarios that comprise multiple C-VUs. The reason is that multiple C-VUs may offload their respective tasks by using the orthogonal frequency division multiplexing (OFDM) technique and each C-VU is pre-allocated an orthogonal channel to reduce interference between different C-VUs [29]. There also exist multiple potential D2D-V pairs that exchange data by reusing the same spectrum as C-VU [30], [31]. Furthermore, we also consider that the Eves' physical locations and CSI cannot be obtained in the realistic scenario of eavesdropping due to the vehicle mobility and Eves' intention to hide their exact position [32]. In addition, the potential D2D-V pairs sets and malicious Eves sets are denoted as S_1 and S_2, respectively. Note that, the spatial locations of S_1 and S_2 are characterized by two independent homogeneous Poisson Point Processes (PPP) Φ_v and Φ_e, with the densities λ_v and λ_e in the two-dimensional (2-D) plane, respectively [33]–[35]. The 2-D plane is simplified as a BS-centered circular area with radius R. In this paper, we only focus on the eavesdropping attack on C-VU's offloading link and investigate a dynamic threshold-based access scheme for security provisioning of C-V2X computation-offloading network from the perspective of PLS.

In this model, each communication node is equipped with a single antenna. Moreover, the V2X communication channel model includes both large-scale fading and small-scale fading. For the large-scale fading, we adopt the general path-loss fading model $d_{i,j}^{-\alpha/2}$, where α is the path-loss exponent that satisfies $\alpha > 2$ [30]. In the C-V2X computation-offloading network, it is hard to obtain perfect CSI in dynamic vehicular environment [36]. Thus, for a more realistic representation, we usually adopt a first-order Gauss-Markov process to model the small-scale fading channel variation over the vehicular feedback delay time T [26], [28]. The small-scale fading channel model of $h_{i,j}$ is given by

$$h_{i,j} = \sqrt{1-\varepsilon}\,\widehat{h}_{i,j} + \sqrt{\varepsilon}\,\widetilde{h}_{i,j}, \tag{1}$$

where the estimated value $\widehat{h}_{i,j}$, and the channel estimation error $\widetilde{h}_{i,j}$ are mutually independent with $\widehat{h}_{i,j} \sim \mathcal{CN}(0, 1)$ and $\widetilde{h}_{i,j} \sim \mathcal{CN}(0, 1)$. We may consider $\varepsilon \in [0, 1]$ as channel estimation error coefficient, with the small value of ε indicating an accurate channel estimation. Note that $\varepsilon = 0$ corresponds to a perfect channel estimation, while $\varepsilon = 1$ means "no CSI is acquired at all". For the Jakes' fading model, ε is given by $\varepsilon = 1 - (J_0(2\pi f_d T))^2$, where $J_0(\cdot)$ is the zero-order Bessel function of the first kind, $f_d = \nu f_c/c$ denotes the maximum Doppler frequency with $c = 3 \times 10^8$ m/s, ν is the vehicle speed, and f_c is the carrier frequency [28]. It is worth noting that the proposed channel model takes into account both the vehicular speed and the feedback delay time information. The C-VU is located at a deterministic distance $d_{c,0}$ from the BS. Furthermore, the change in distance is so small that it is ignored over the feedback delay time of the channel [37]. Similar assumption is in the existed works [26], [28].

In such a C-V2X computation-offloading network deployment, the received signal-to-interference-plus-noise (SINR) at BS and k-th Eve can be given by

$$\gamma_0 = \frac{(1-\varepsilon)\left|\widehat{h}_{c,0}\right|^2 d_{c,0}^{-\alpha} P_c}{\varepsilon d_{c,0}^{-\alpha} P_c + I_{m,0} + N_0}, \tag{2}$$

$$\gamma_k = \frac{(1-\varepsilon)\left|\widehat{h}_{c,k}\right|^2 d_{c,k}^{-\alpha} P_c}{\varepsilon d_{c,k}^{-\alpha} P_c + I_{m,k} + N_0}, \quad k \in \Phi_e, \tag{3}$$

where $I_{m,0} = \sum_{m\in\Phi_v}\left[(1-\varepsilon)\left|\widehat{h}_{m,0}\right|^2 + \varepsilon\right] d_{m,0}^{-\alpha} P_v$ and $I_{m,k} = \sum_{m\in\Phi_v}\left[(1-\varepsilon)\left|\widehat{h}_{m,k}\right|^2 + \varepsilon\right] d_{m,k}^{-\alpha} P_v$ denote the cumulative

cross-tier interference from co-channel D2D-V transmitters to the BS and the k-th Eve, respectively. Furthermore, P_v and P_c denote the transmission power of each D2D-V transmitter and the C-VU, respectively. Similarly, the received SINR at the m-th D2D-V receiver can be given by

$$\gamma_m = \frac{P_v(1-\varepsilon)\left|\widehat{h}_{m,m}\right|^2 d_{m,m}^{-\alpha}}{\varepsilon d_{m,m}^{-\alpha} P_v + I_{c,m} + I_{l,m} + N_0}, \tag{4}$$

where $I_{c,m} = P_c\left[(1-\varepsilon)\left|\hat{h}_{c,m}\right|^2 + \varepsilon\right] d_{c,m}^{-\alpha}$ denotes the interference from the C-VU to the m-th D2D-V receiver, and $I_{l,m} = \sum_{l\in\Phi_v\setminus\{m\}} P_v\left[(1-\varepsilon)\left|\widehat{h}_{l,m}\right|^2 + \varepsilon\right] d_{l,m}^{-\alpha}$ denotes the cumulative inter-interference from the co-channel D2D-V transmitters to the m-th D2D-V receiver. Note that all the V2X communication channels are impaired by additive Gaussian noise with variance N_0 [38]. In this paper, we are centered on the interference-limited C-V2X computation-offloading network, where the power of thermal noise N_0 would be negligible compared to the inter-tier and cross-tier aggregate interference [33], [39]. In the following, the SINR in (2), (3) and (4) will be replaced by the signal-to-interference ratio (SIR) since $N_0 \to 0$.

B. PERFORMANCE METRICS

In this part, we introduce two performance metrics, i.e., secrecy throughput and ASE. As for the security consideration, the Wyner's wiretap encoding scheme is used for protecting confidential information from eavesdropping [32]–[35]. We denote by R_t and R_s the transmitted codeword rate and secret message rate, respectively. Furthermore, $R_e = R_t - R_s$ denotes the rate of redundant information. We let the transmitters have the same R_t and R_s for reducing the complexity of the proposed system. If the capacity of a legitimate receiver is below the transmitted codeword rate, a connection outage event occurs, in which case the connection outage probability (COP) P_{cop} is given by

$$P_{cop} = \Pr\left\{\log_2(1+\gamma_b) \le R_t\right\}, \tag{5}$$

where γ_b denotes the SINR of the legitimate receiver. Accordingly, if the redundant rate is below the capacity of the equivalent wiretap channel, a secrecy outage inevitably occurs. The corresponding secrecy outage probability (SOP) P_{sop} can thus be defined:

$$P_{sop} = \Pr\left\{\max_{k\in\Phi_e} C_{E_k} > R_e\right\}, \tag{6}$$

where $C_{E_k} = \log_2(1+\gamma_k)$ denotes the channel capacity of the k-th Eve in Φ_e. In fact, the SOP can be considered as a cost in computation-offloading network. For instance, a security-sensitive application may require the re-execution of the computation task, if the offloaded task has been overheard by malicious Eves [6].

As a key performance metric of secure transmission efficiency, secrecy throughput is defined as the rate of message reliably and securely transmitted from the legitimate source node to the destination node (bps/Hz) [23], [33], [34], [40]. Therefore, the secrecy throughput T is given by

$$T = (1-P_{sop})(1-P_{cop})R_s. \tag{7}$$

As the other important performance metric of spectrum utilization efficiency, ASE is defined as the average rate of successful transmissions message per unit bandwidth per unit area (bps/Hz/m^2) [24], [25]. Therefore, the ASE η is given by

$$\eta = \lambda(1-P_{cop})R_t, \tag{8}$$

where λ denotes the effective access density.

III. DYNAMIC ACCESS SCHEME AND OUTAGE PERFORMANCE ANALYSIS

In this section, we first propose a dynamic threshold-based D2D-V access scheme, followed by deriving the general analytical expressions for both the COP and SOP as function of estimation error coefficient. Furthermore, we seek to investigate the effects of the system parameters on the outage performance.

A. DYNAMIC THRESHOLD-BASED D2D-V ACCESS SCHEME

In this subsection, we propose a dynamic threshold-based D2D-V access scheme, which is an efficient method for mitigating interference and safeguarding wireless communications. Each D2D-V transmitter has to decide whether to access the network or not, relying on the channel quality for his respective receiver. Driven by the fact that both the estimated value $\hat{h}_{m,m}$ and the estimation error coefficient ε can be obtained by sending training sequences to the receiver, the access probability can thus be calculated as the probability that the channel strength is above a certain threshold [40]–[42]. The access probability for the dynamic threshold-based D2D-V access scheme will be:

$$\begin{aligned} p_s &= \Pr\{(1-\varepsilon)\left|\hat{h}_{m,m}\right|^2 d_{m,m}^{-\alpha} \ge G\} \\ &= \exp(-\frac{G d_{m,m}^{\alpha}}{1-\varepsilon}), \end{aligned} \tag{9}$$

where G denotes an access threshold. Interference generated by D2D-V links gives both negative and positive impacts on the offloading link, since they cause degradation of the received SIR at the BS as well as the received SIR at the Eves. When G becomes larger, the system allows fewer D2D-V pairs to be activated. However, less D2D-V interference will be suffered by Eves. On the other hand, when G is small, more D2D-V pairs are activated, which increases D2D-V's interference at both C-VU and other D2D-V pairs. Hence, G plays a pivot role in determining the secrecy throughput and the ASE. The active D2D-V pairs set are equivalent to a thinning of a homogeneous PPP with an effective access density $\lambda_{v,a} = p_s\lambda_v$.

B. CONNECTION OUTAGE ANALYSIS

In the interference-limited C-V2X computation-offloading network, based on a variety of parameters, including the SIR of the offloading link in (2), the SIR of the D2D-V link in (4), and the COP defined in (5), we can derive the COP of the offloading link and D2D-V link by the following *Theorem 1* and *Theorem 2*, respectively.

Theorem 1: The COP of an offloading link for a given $d_{c,0}$ can be expressed:

$$P_{cop,c}=1-\exp(-\frac{\varepsilon\beta_{R_t}}{1-\varepsilon}-\pi\lambda_{v,a}(\frac{P_v}{P_c})^{\frac{2}{\alpha}}\Omega(\alpha,\varepsilon)\beta_{R_t}^{\frac{2}{\alpha}}d_{c,0}^2), \quad (10)$$

where $\beta_{R_t}=2^{R_t}-1$, $\Omega(\alpha,\varepsilon)=\Gamma(1+\frac{2}{\alpha},\frac{\varepsilon}{1-\varepsilon})\Gamma(1-\frac{2}{\alpha})e^{\frac{\varepsilon}{1-\varepsilon}}$. It is shown in (10) that the COP of an offloading link depends on ε, $\lambda_{v,a}$ and R_t.

Proof: The COP of an offloading link can be expressed as:

$$\begin{aligned}P_{cop,c} &= \Pr\left\{\log_2(1+\gamma_b)\le R_t\right\}\\ &= \mathbb{E}_{\Phi_v}(\Pr\{\left|\widehat{h}_{c,0}\right|^2\le\frac{\beta_{R_t}}{P_c(1-\varepsilon)d_{c,0}^{-\alpha}}(\varepsilon d_{c,0}^{-\alpha}P_c+I_{m,0})\})\\ &\overset{(a)}{=} 1-\exp(-\frac{\varepsilon\beta_{R_t}}{1-\varepsilon})\mathbb{E}_{\Phi_v}(\exp(-\frac{\beta_{R_t}d_{c,0}^{\alpha}}{P_c(1-\varepsilon)}I_{m,0}))\\ &\overset{(b)}{=} 1-\exp(-\frac{\varepsilon\beta_{R_t}}{1-\varepsilon})\mathcal{L}_{I_{m,0}}(s), \end{aligned}\quad (11)$$

where $s=\frac{\beta_{R_t}d_{c,0}^{\alpha}}{P_c(1-\varepsilon)}$, and (a) holds due to the fact that $\left|\widehat{h}_{c,0}\right|^2\sim exp(1)$. In (b), $\mathcal{L}_{I_{m,0}}(\cdot)$ represents the Laplace transform of $I_{m,0}$, as given by

$$\begin{aligned}&\mathcal{L}_{I_{m,0}}(s)\\ &=\mathbb{E}_{\Phi_v}(\exp(-s\sum_{m\in\Phi_v}H\left(\left|\widehat{h}_{m,0}\right|,\varepsilon\right)d_{m,0}^{-\alpha}P_v))\\ &\overset{(c)}{=}\mathbb{E}_{\Phi_v}\left(\prod_{m\in\Phi_v}\mathbb{E}_{d_{m,0}}\left(\exp(H(\left|\hat{h}_{m,0}\right|,\varepsilon)d_{m,0}^{-\alpha}P_v)\right)\right)\\ &\overset{(d)}{=}\exp\left(-2\pi\lambda_{v,a}\int_0^{\infty}\mathbb{E}_{\left|\hat{h}_{m,0}\right|}\left(1-e^{-sH(\left|\hat{h}_{m,0}\right|,\varepsilon)r^{-\alpha}P_v}\right)rdr\right)\\ &\overset{(e)}{=}\exp\left(-\pi\lambda_{v,a}\Gamma(1-\frac{2}{\alpha})(sP_v)^{\frac{2}{\alpha}}\mathbb{E}_{\left|\hat{h}_{m,0}\right|}\left(H(\left|\hat{h}_{m,0}\right|,\varepsilon)^{\frac{2}{\alpha}}\right)\right)\\ &\overset{(f)}{=}\exp(-\pi\lambda_{v,a}s^{\frac{2}{\alpha}}P_v^{\frac{2}{\alpha}}(1-\varepsilon)^{\frac{2}{\alpha}}\Omega(\alpha,\varepsilon)), \end{aligned}\quad (12)$$

where $H\left(\left|\widehat{h}_{m,0}\right|,\varepsilon\right)=(1-\varepsilon)\left|\widehat{h}_{m,0}\right|^2+\varepsilon$, (c) holds for the assumption of independent small scale fading, and (d) holds because of the fact that applying the probability generating functional (PGFL) of the PPP [33]: $\mathbb{E}_{\Phi}(\prod_{k\in\Phi}f(x))=\exp(-\lambda\int_{R^2}(1-f(x)))$ and $\int_{R^2}f(x)dx=2\pi\int_0^{\infty}xf(x)dx$. Furthermore, (e) holds for the use of exponential distributed random variables, and (f) holds for utilizing the appendix B in [40]. By substituting $s=\frac{\beta_{R_t}d_{c,0}^{\alpha}}{P_c(1-\varepsilon)}$ into (12), we can get:

$$\mathcal{L}_{I_{m,0}}(s)=\exp\left(-\pi\lambda_{v,a}(\frac{P_v}{P_c})^{\frac{2}{\alpha}}\Omega(\alpha,\varepsilon)\beta_{R_t}^{\frac{2}{\alpha}}d_{c,0}^2\right). \quad (13)$$

By substituting (13) into (11), we obtain a closed-form expression in (10) for the COP of the offloading link. This completes the proof.

Similarly, the closed-form expression for the COP of a typical D2D-V link can be obtained by the following *Theorem 2*.

Theorem 2: The COP of a typical D2D-V link is given by

$$P_{cop,v}=1-\frac{1}{1+K(\alpha)}\exp\left(-\frac{\varepsilon\beta_{R_t}}{1-\varepsilon}-K(\alpha)(\frac{\varepsilon}{1-\varepsilon})^{2/\alpha}-\pi\lambda_{v,a}\Omega(\alpha,\varepsilon)\beta_{R_t}^{\frac{2}{\alpha}}d_{m,m}^2\right), \quad (14)$$

where $K(\alpha)=(\frac{P_c}{P_v})^{2/\alpha}\frac{d_{m,m}^2\beta_{R_t}^{2/\alpha}}{(128R/45\pi)^2}$. It is shown that the $P_{cop,v}$ also depends on ε, $\lambda_{v,a}$ and R_t. From (10) and (14), $P_{cop,c}$ and $P_{cop,v}$ increase as the parameter $\lambda_{v,a}$ increases. Furthermore, the imperfect CSI in terms of channel estimation error has a harmful influence on the connection performance.

Proof: The COP of a typical D2D-V link can be expressed:

$$\begin{aligned}P_{cop,v} &= \Pr\left\{\log_2(1+\gamma_m)\le R_t\right\}\\ &= \mathbb{E}_{\Phi_v\setminus\{m\}}(\Pr\{\left|\widehat{h}_{m,m}\right|^2\le s(\varepsilon d_{m,m}^{-\alpha}P_v+I_{l,m}+I_{c,m})\})\\ &= 1-\exp(-\frac{\varepsilon\beta_{R_t}}{1-\varepsilon})\mathcal{L}_{I_{l,m}}(s)\cdot\mathcal{L}_{I_{c,m}}(s), \end{aligned}\quad (15)$$

where $s=\frac{\beta_{R_t}d_{m,m}^{\alpha}}{P_v(1-\varepsilon)}$, similar to the argument in (12), $\mathcal{L}_{I_{l,m}}(s)$ can be obtained following a similar procedure:

$$\mathcal{L}_{I_{l,m}}(s)=\exp\left(-\pi\lambda_{v,a}\Omega(\alpha,\varepsilon)\beta_{R_t}^{\frac{2}{\alpha}}d_{m,m}^2\right). \quad (16)$$

and $\mathcal{L}_{I_{c,m}}(s)$ is given by

$$\begin{aligned}\mathcal{L}_{I_{c,m}}(s) &= \mathbb{E}\left(\exp\left(-sP_c\left[(1-\varepsilon)\left|\widehat{h}_{c,m}\right|^2+\varepsilon\right]d_{c,m}^{-\alpha}\right)\right)\\ &= \mathcal{L}_{d_{c,m}}(\frac{1}{1+\frac{\beta_{R_t}P_c}{P_v}(\frac{d_{m,m}}{d_{c,m}})^{\alpha}})\\ &\quad\times\mathcal{L}_{d_{c,m}}(\exp(-\frac{\beta_{R_t}P_c\varepsilon}{P_v(1-\varepsilon)}(\frac{d_{m,m}}{d_{c,m}})^{\alpha}))\\ &\overset{(a)}{=}\frac{\exp\left(-K(\alpha)(\frac{\varepsilon}{1-\varepsilon})^{2/\alpha}\right)}{1+K(\alpha)}, \end{aligned}\quad (17)$$

where (a) holds for the approximate expressions by $\mathbb{E}(e^{-\frac{k}{d_{c,m}^{\alpha}}})\simeq e^{-\frac{k^{2/\alpha}}{\mathbb{E}(d_{c,m})^2}}$, $\mathbb{E}_{d_{c,m}}(1/(1+\frac{k}{d_{c,m}^{\alpha}}))\simeq 1/(1+\frac{k^{2/\alpha}}{\mathbb{E}(d_{c,m})^2})$, and $\mathbb{E}\left(d_{c,m}\right)=\frac{128R}{45\pi}$ as shown in [41]. By substituting (16) and (17) into (15), we obtain a closed-form expression in (14). This completes the proof.

C. SECRECY OUTAGE ANALYSIS

According to the SIR of the typical eavesdropping link in (3) and the SOP defined in (6), a closed-form expression for the SOP of the offloading link is derived in the interference-limited C-V2X computation-offloading network by the following theorem.

Theorem 3: The SOP of an offloading link can be expressed:

$$P_{sop,c} = 1 - \exp\left(-\frac{\lambda_e \exp(\frac{\varepsilon\beta_{R_e}}{\varepsilon-1})}{\lambda_{v,a}(\frac{P_v}{P_c})^{\frac{2}{\alpha}}\Omega(\alpha,\varepsilon)\beta_{R_e}^{\frac{2}{\alpha}}}\right), \quad (18)$$

where $\beta_{R_e} = 2^{R_t - R_s} - 1$.

Proof: Considering the non-colluding eavesdropping scenario [35], the SOP of the offloading link can be determined by the most detrimental eavesdropper, as expressed by

$$\begin{aligned}
&P_{sop,c}\\
&= \Pr\left\{\max_{k\in\Phi_e} C_{E_k} > R_e\right\}\\
&= 1 - \Pr\left\{\max_{k\in\Phi_e} \gamma_k < \beta_{R_e}\right\}\\
&= 1 - \mathbb{E}_{\Phi_e,\Phi_v}\Big(\prod_{e\in\Phi_e} \Pr\left(\gamma_k < \beta_{R_e}\right)\Big)\\
&= 1 - \mathbb{E}_{\Phi_e}\left(\prod_{e\in\Phi_e}\left(1 - \Pr\left(\left|\widehat{h}_{c,k}\right|^2 > \frac{(\varepsilon d_{c,k}^{-\alpha} P_c + I_{m,k}) d_{c,k}^{\alpha}}{P_c(1-\varepsilon)}\right)\right)\right)\\
&\overset{(a)}{=} 1 - \mathbb{E}_{\Phi_e}\left(\prod_{e\in\Phi_e}\left(1 - \exp\left(-\frac{\varepsilon\beta_{R_e}}{1-\varepsilon}\right)\mathcal{L}_{I_{m,k}}\left(\frac{r^{\alpha}}{P_c(1-\varepsilon)}\right)\right)\right)\\
&\overset{(b)}{=} 1 - \exp\left(-2\pi\lambda_e \int_0^{\infty} \exp\left(-\frac{\varepsilon\beta_{R_e}}{1-\varepsilon}\right)\mathcal{L}_{I_{m,k}}\left(\frac{r^{\alpha}}{P_c(1-\varepsilon)}\right) r dr\right),
\end{aligned} \quad (19)$$

where (a) follows the Rayleigh distribution. (b) is obtained by using the PGFL of PPP and double integral in polar coordinates, and $\mathcal{L}_{I_{m,k}}(\cdot)$ denotes the Laplace transform of $I_{m,k}$. Similar to the argument in (12), we get

$$\mathcal{L}_{I_{m,k}}(\cdot) = \exp\left(-\pi\lambda_{v,a}\left(\frac{P_v}{P_c}\right)^{\frac{2}{\alpha}}\Omega(\alpha,\varepsilon)\beta_{R_e}^{\frac{2}{\alpha}} d_{m,k}^2\right). \quad (20)$$

By substituting (20) into (19), we have

$$\begin{aligned}
P_{sop,c} &= 1 - \exp\left(-2\pi\lambda_e \int_0^{\infty} \exp\left(-\frac{\varepsilon\beta_{R_e}}{1-\varepsilon}\right.\right.\\
&\quad \left.\left. - \pi\lambda_{v,a}\left(\frac{P_v}{P_c}\right)^{\frac{2}{\alpha}}\Omega(\alpha,\varepsilon)\beta_{R_e}^{\frac{2}{\alpha}} r^2\right) r dr\right)\\
&= 1 - \exp\left(-\frac{\lambda_e \exp\left(-\frac{\varepsilon\beta_{R_e}}{1-\varepsilon}\right)}{\lambda_{v,a}\left(\frac{P_v}{P_c}\right)^{\frac{2}{\alpha}}\Omega(\alpha,\varepsilon)\beta_{R_e}^{\frac{2}{\alpha}}}\right).
\end{aligned} \quad (21)$$

This completes the proof.

Remark 1: It can be observed from (10) and (18) that the parameter $\lambda_{v,a}$ makes a tradeoff between the $P_{cop,c}$ and the $P_{sop,c}$. To ensure the reliability performance of the offloading link, the secrecy performance of the offloading link should be compromised. In other words, a moderate value of $\lambda_{v,a}$, i.e. selecting an appropriate access threshold G, is controlled in order to satisfy the reliability and secrecy in computation offloading.

Up to now, we have completed the general analytical expressions derivation of the COP and the SOP, which is essential to the formulation of the optimization problem. From the results in (10), (14) and (18), we verify that the value of access threshold G and the channel estimation error coefficient ε affect both the security and the reliability performance. Specifically, the parameter G value is a tradeoff between the security performance and the reliability performance of the offloading link. A smaller G stands for allowing more D2D-V links to access the spectrum-sharing network that achieve a higher security performance while leading to a lower reliability performance. Therefore, by selecting a moderate G, we can improve the security-reliability tradeoff. In the next section, we will discuss the optimized access threshold solution for maximizing the secrecy throughput and the total ASE, respectively.

IV. OPTIMAL ACCESS SOLUTION

Following the analytical results presented above, the parameter G is shown to play pivot roles in the security and reliability performance. In this section, we derive the optimal solutions G for schemes S1 and scheme S2. In particular, scheme S1 maximizes the secrecy throughput of the offloading link under a connection outage constraint of the D2D-V links. On the other hand, scheme S2 maximizes the total ASE of the C-V2X computation-offloading network under the security performance criterion for the offloading link.

A. SCHEME S1

According to *Theorems 1 and 2*, the active D2D-V pairs are allowed to access the sharing spectrum, implying that the interference would increase the COP $P_{cop,c}$ and the COP $P_{cop,v}$. However, the analytical results in *Theorem 3*, the SOP $P_{sop,c}$ can be reduced. Thus, the access threshold G must be appropriatly designed to ensure the performance of the offloading link as well as to enhance the performance of the D2D-V links. Using the definition given by (7), a closed-form expression for the secrecy throughput of the offloading link is obtained T_c, as shown in (22). By adjusting the access probability p_s (i.e., selecting an appropriate access threshold G), the achievable T_c can be maximized. This expression will be used for investigating the dependence of maximizing T_c on key system parameters, such as G, λ_v, λ_e and ε.

$$\begin{aligned}
T_c = R_s \exp\Big(&-\frac{\varepsilon\beta_{R_t}}{1-\varepsilon} - \pi p_s\lambda_v\left(\frac{P_v}{P_c}\right)^{\frac{2}{\alpha}}\Omega(\alpha,\varepsilon)\beta_{R_t}^{\frac{2}{\alpha}} d_{c,0}^2\\
&- \frac{\lambda_e \exp\left(-\frac{\varepsilon\beta_{R_e}}{1-\varepsilon}\right)}{p_s\lambda_v\left(\frac{P_v}{P_c}\right)^{\frac{2}{\alpha}}\Omega(\alpha,\varepsilon)\beta_{R_e}^{\frac{2}{\alpha}}}\Big).
\end{aligned} \quad (22)$$

Subject to COP of the D2D-V links, the problem of maximizing T_c in (22) can be formulated as

$$\begin{aligned}
&\underset{p_s}{maximize} \quad T_c\\
&s.t. \quad 0 \le P_{cop,v} \le \delta_v,\\
&\qquad 0 \le p_s \le 1,
\end{aligned} \quad (23)$$

where δ_v is the COP constraint of the D2D-V links. According to (14), the multi-constraints of inequality in (23) can be transformed into the feasible regions of p_s in (24) for simplifying the optimization problem.

$$\begin{cases} p_s \le \dfrac{\ln((1-\delta_v)(1+K(\alpha)))+\frac{\varepsilon\beta_{R_t}}{1-\varepsilon}+K(\alpha)(\frac{\varepsilon}{1-\varepsilon})^{2/\alpha}}{-\lambda_v\pi\,\Omega(\alpha,\varepsilon)\beta_{R_t}^{\frac{2}{\alpha}}d_{m,m}^{\alpha}} = p_{s,1} \\ 0 \le p_s \le 1. \end{cases} \tag{24}$$

From (22), it is shown that maximizing T_c is equivalent to minimizing $-\ln T_c$. To further simplify these notations, we may define

$$\begin{cases} a = \pi\lambda_v(\frac{P_v}{P_c})^{\frac{2}{\alpha}}\Omega(\alpha,\varepsilon)\beta_{R_t}^{\frac{2}{\alpha}}d_{c,0}^2 \\ b = \dfrac{\lambda_e\exp(-\frac{\varepsilon\beta_{R_e}}{1-\varepsilon})}{\lambda_v(\frac{P_v}{P_c})^{\frac{2}{\alpha}}\Omega(\alpha,\varepsilon)\beta_{R_e}^{\frac{2}{\alpha}}}, \end{cases} \tag{25}$$

Consequently, problem (23) can be rewritten as

$$\begin{aligned} &\underset{p_s}{maximize} \quad f(p_s) = ap_s + \frac{b}{p_s} \\ &s.t. \;\; 0 \le p_s \le \min(p_{s,1}, 1). \end{aligned} \tag{26}$$

The first- and second-order derivatives of $f(p_s)$ on p_s are given by

$$\begin{cases} \dfrac{\partial f(p_s)}{\partial p_s} = a - \frac{b}{p_s{}^2} \\ \dfrac{\partial^2 f(p_s)}{\partial p_s^2} = \frac{2b}{p_s^3}, \end{cases} \tag{27}$$

Clearly, when $\frac{\partial f(p_s)}{\partial p_s} = 0$, we get

$$\begin{aligned} p_{s,T}^* &= \sqrt{\frac{b}{a}} \\ &= (\frac{P_c}{P_v})^{\frac{2}{\alpha}}\frac{1}{\lambda_v\Omega(\alpha,\varepsilon)\beta_{R_t}^{\frac{1}{\alpha}}\beta_{R_e}^{\frac{1}{\alpha}}d_{c,0}}\sqrt{\exp(\frac{\varepsilon\beta_{R_e}}{\varepsilon-1})\lambda_e/\pi}, \end{aligned} \tag{28}$$

With (27),we can conclude that $\frac{\partial^2 f(p_s)}{\partial p_s{}^2} \ge 0$ always holds. Thus $f(p_s)$ is a quasi-convex function of p_s, enabling he optimal access probability $p_{s,T}^{opt}$ for maximizing the T_c to be achieved either on the critical point $p_{s,T}^*$ or the boundary point $\min(p_{s,1}, 1)$. Therefore, the optimal access probability $p_{s,T}^{opt}$ can be given by

$$p_{s,T}^{opt} = \begin{cases} p_{s,T}^*, & if \;\; 0 \le p_{s,T}^* \le \min(p_{s,1}, 1), \\ \min(p_{s,1}, 1), & otherwise. \end{cases} \tag{29}$$

Furthermore, the optimal access threshold $G_{T,opt}$ for the scheme S1 can be designed according to the optimal access probability $p_{s,T}^{opt}$, as given by

$$G_{T,opt} = (\varepsilon - 1)d_{m,m}^{-\alpha}\ln\left(p_{s,T}^{opt}\right). \tag{30}$$

From (30), the optimized access threshold is set to be updated adaptively in terms of channel estimation error for balancing both the security and reliability of the offloading link.

B. SCHEME S2

In this subsection, we will optimize the access threshold of D2D-V transmitters for maximizing the total ASE. The total ASE of the whole network is equal to the sum of the ASE of the D2D-V links and the ASE of the offloading link. We denote η_v and η_c as the ASE of the D2D-V links and the offloading link, respectively. In the following, η_v can be expressed as

$$\begin{aligned} \eta_v &= p_s\lambda_v(1-P_{cop,v})\log(1+\beta_{R_t}) \\ &= p_s\lambda_v\log(1+\beta_{R_t})\frac{1}{1+K(\alpha)\beta_{R_t}{}^{2/\alpha}}\exp(-\frac{\varepsilon\beta_{R_t}}{1-\varepsilon} \\ &\quad - K(\alpha)\beta_{R_t}{}^{2/\alpha}(\frac{\varepsilon}{1-\varepsilon})^{2/\alpha} - \pi p_s\lambda_v\Omega(\alpha,\varepsilon)\beta_{R_t}^{\frac{2}{\alpha}}d_{m,m}^2) \\ &= Ap_s\exp(-Bp_s), \end{aligned} \tag{31}$$

where

$$\begin{aligned} A &= \lambda_v\log(1+\beta_{R_t})\frac{1}{1+K(\alpha)\beta_{R_t}{}^{2/\alpha}} \\ &\quad \times \exp\left\{-\frac{\varepsilon\beta_{R_t}}{1-\varepsilon} - K(\alpha)\beta_{R_t}{}^{2/\alpha}(\frac{\varepsilon}{1-\varepsilon})^{2/\alpha}\right\}, \end{aligned} \tag{32}$$

$$B = \pi\lambda_v\Omega(\alpha,\varepsilon)\beta_{R_t}^{\frac{2}{\alpha}}d_{m,m}^2. \tag{33}$$

Similarly, the η_c can be expressed as [25]

$$\eta_c = \frac{(1-P_{cop,c})\log(1+\beta_{R_t})}{\pi R^2} = C\exp(-Dp_s), \tag{34}$$

where

$$\begin{cases} C = log(1+\beta_{R_t})\exp(-\frac{\varepsilon\beta_{R_t}}{1-\varepsilon})/\pi R^2 \\ D = \pi\lambda_v(\frac{P_v}{P_c})^{\frac{2}{\alpha}}\Omega(\alpha,\varepsilon)\beta_{R_t}^{\frac{2}{\alpha}}d_{c,0}^2, \end{cases} \tag{35}$$

According to (31) and (34), the access probability p_s for maximizing the total ASE η_{tot} under the secrecy performance criterion for the offloading link can be obtained by solving the following optimization problem:

$$\begin{aligned} &\underset{p_s}{maximize} \quad \eta_{tot} = \eta_v + \eta_c \\ &s.t. \; P_{sop,c} \le \sigma_c, \\ &\quad 0 \le p_s \le 1, \end{aligned} \tag{36}$$

where σ_c is the SOP of the offloading link. The optimal access probability can be derived:

$$\begin{aligned} &\underset{p_s}{maximize} \;\; \eta_{tot} = Ap_s\exp(-Bp_s) + C\exp(-Dp_s) \\ &s.t. \; p_{s,3} \le p_s, \\ &\quad 0 \le p_s \le 1, \end{aligned} \tag{37}$$

where

$$p_{s,3} = \frac{\lambda_e\exp(-\frac{\varepsilon\beta_{R_e}}{1-\varepsilon})}{-\lambda_v(\frac{P_v}{P_c})^{\frac{2}{\alpha}}\ln(1-\sigma_c)\Omega(\alpha,\varepsilon)\beta_{R_t}^{\frac{2}{\alpha}}}. \tag{38}$$

The derivative of η_{tot} with respect to p_s is written as

$$\frac{\partial\eta_{tot}}{\partial p_s} = Ae^{-Bp_s} - ABp_se^{-Bp_s} - CDe^{-Dp_s}. \tag{39}$$

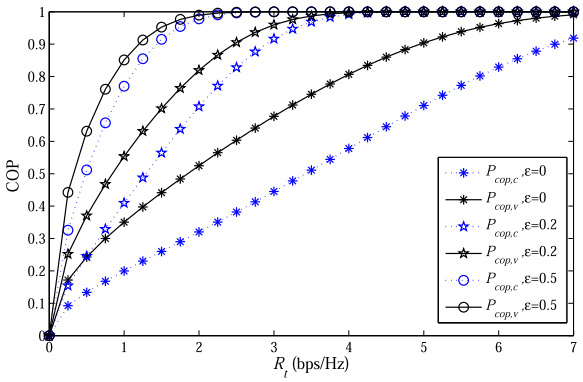


FIGURE 2. The COP versus the transmitted codeword rate R_t for different error coefficient ε.

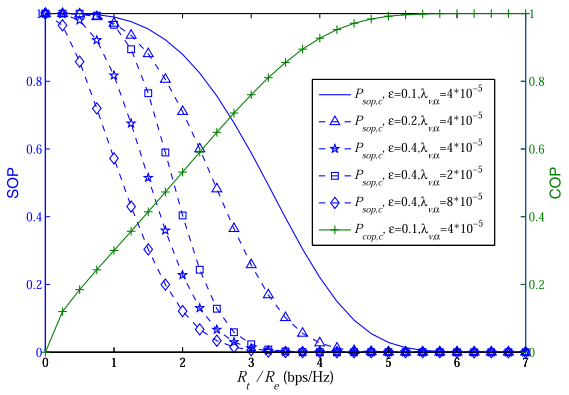


FIGURE 3. The SOP and the COP versus the transmitted codeword rate R_t and the redundant rate R_e.

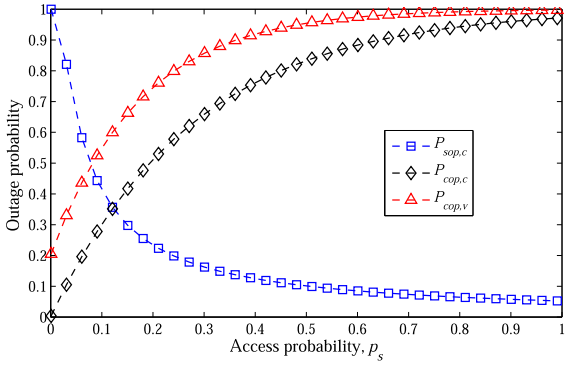


FIGURE 4. The outage probability versus the access probability p_s.

when $\frac{\partial \eta_{tot}}{\partial p_s} = 0$, we have

$$(1 - Bp_s) = \frac{CD}{A} e^{(B-D)p_s}. \tag{40}$$

A solution that satisfies the first-order optimality condition, which is given by:

$$\widehat{p_s} = \frac{1}{B} + \frac{1}{D-B} W\left(-\frac{CD(D-B)e^{-(D-B)/B}}{AB}\right), \tag{41}$$

where $W(\cdot)$ denotes the Lambert-W function [25], [33], which defined as the inverse function of $f(x) = xe^x$. Therefore, the optimal access probability $p_{s,\eta}^{opt}$ for scheme S2 is given by

$$p_{s,\eta}^{opt} = \max\{\min\{\widehat{p_s}, 1\}, p_s, 3\}. \tag{42}$$

Similarly, according to (9) and (42), the optimal access threshold $G_{\eta,opt}$ for the scheme S2 can also be obtained.

V. NUMERICAL RESULTS AND DISCUSSIONS

In this section, numerical results are given out to provide more insight into the theoretical analysis. In particular, the effects of system parameters such as: R_t, R_e, ε, $\lambda_{v,a}$, λ_e, δ_v, and σ_c on security performance are presented and the corresponding results are shown in the figures below. We adopt the following simulation parameters: $\alpha = 4$, $R = 500$ m, $d_{c,0} = 100$ m, $d_{m,m} = 40$ m, $P_c = 30$ dBm, and $P_v = 10$ dBm. Additionally, the transmission rate is $R_t = 3.5$ bps/Hz, the redundant rate is $R_e = 3$ bps/Hz, and the error coefficient is $\varepsilon = 0$ unless otherwise stated.

Fig. 2 presents the COP of offloading link $P_{cop,c}$ and the COP of D2D-V links $P_{cop,v}$ as a function of the transmitted codeword rate R_t for different error coefficient, i.e., $\varepsilon = 0, 0.2, 0.5$ when effective access density $\lambda_{v,a} = 4 \times 10^{-5}/m^2$. We observed that as the transmitted codeword rate R_t increases, the $P_{cop,c}$ and $P_{cop,v}$ are always increasing and tending toward 1 (i.e., the system will be in connection outage) for three different values of error coefficient ε. The results matched the analytical expression in (10) and (14) very well. Furthermore, by fixing R_t unchanged, the growth of the values of ε will increase the COP, because the imperfect CSI in terms of channel estimation error has a harmful influence on the connection performance.

Fig. 3 presents the SOP of offloading link $P_{sop,c}$ and the COP of offloading link $P_{cop,c}$ versus the transmitted codeword rate R_t and the redundant rate R_e for different ε and $\lambda_{v,a}$, respectively. It is shown that there is a tradeoff between the SOP and the COP. Furthermore, the secrecy performance of the offloading link can be improved significantly when $\lambda_{v,a}$ or ε increases, indicating that increasing $\lambda_{v,a}$ or ε will enhance the secrecy performance of the offloading link. However, the SOP of the offloading link $P_{sop,c}$ decreases as R_e increases, because large redundant rate can bring enhancement to secrecy performance.

Fig. 4 presents the outage probability versus the access probability p_s with $\lambda_v = 20 \times 10^{-5}/m^2$ and $\lambda_e = 0.5 \times 10^{-5}/m^2$. It is shown the COP $P_{cop,c}$ and $P_{cop,v}$ increases as the parameter p_s increases. By contrast, the $P_{sop,c}$ decreases as the parameter p_s increases. This phenomenon comes from the fact that the larger access probability brings more active access D2D-V links. As a consequence, the co-channel interference generated by D2D-V links causes a weaker connection performance of the offloading link and D2D-V links, whereas it is of great benefit to confuse the eavesdroppers. The result is consistent with Fig. 2 and Fig. 3.

Fig. 5 plots the security throughput T_c and the total ASE η_{tot} versus the access threshold G. From Fig. 5, it is observed that the security throughput and the total ASE rise at first

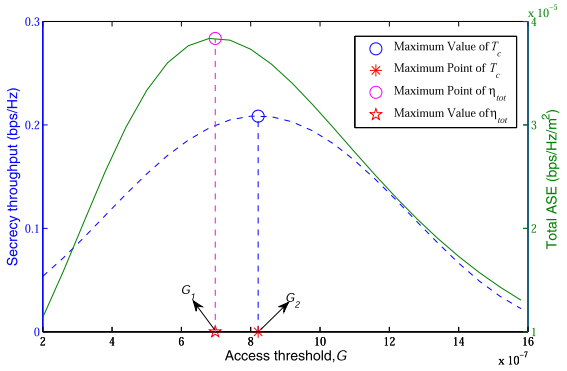


FIGURE 5. The security throughput T_c and the total ASE η_{tot} versus the access threshold G.

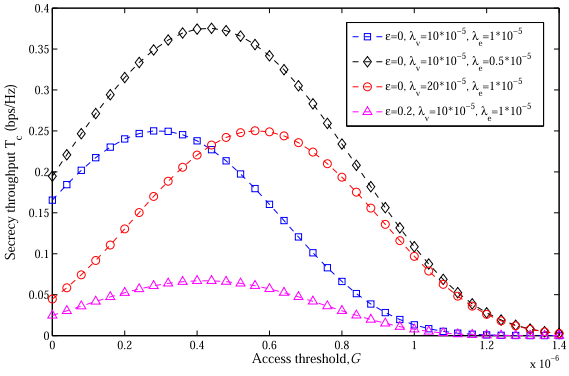


FIGURE 6. The security throughput T_c versus the access threshold G.

and then decrease as the parameter G increases, respectively. This reveals that there exist optimum access thresholds G_1 and G_2 that yield the maximum security throughput and the total ASE, respectively, because increasing the access threshold will cause the access probability of D2D-V links to decrease. When the parameter G becomes small (e.g., $G < G_1$), the total ASE and the security throughput increase simultaneously as the parameter G increases, because a large access threshold can bring enhancement to connection performance. However, when the parameter G is moderate (e.g., $G_1 < G < G_2$), the benefits of co-channel interference for confusing eavesdropping are greater than the impact on connectivity. Hence, the security throughput continuously increases while the total ASE keeps dropping. Furthermore, if this continues increasing (e.g., $G > G_2$), the co-channel interference should not be ignored and leads to a decrease of the total ASE and the security throughput. This provides a very useful design insight to find the optimal access threshold according to the different requirements of C-V2X computation-offloading network.

Fig. 6 presents the security throughput T_c versus the access threshold G for different ε, λ_v and λ_e. Comparing the four curves, under the same λ_v and ε, the optimal value of access threshold is shown to increase with the decrease of the parameter λ_e. We can explain it as follows: when the parameter λ_e decreases, this will reduce the capacity of Eves, so that less

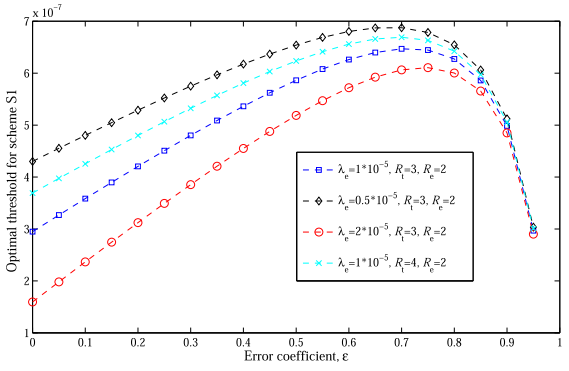


FIGURE 7. The optimum access threshold for scheme S1 versus the error coefficient ε.

interference can guarantee security. Under the same λ_e and ε, the security throughput T_c will not improve by increasing the potential D2D-V density λ_v, because an increase in λ_v leads to more serious aggregate interference at the offloading link, thus resulting in an increase the COP as well as decreasing the SOP. Furthermore, another noticeable trend shown in Fig. 6 implies that as the error coefficient ε increases, a significant decrease in the security throughput T_c can be observed. For example, there is an 86 % reduction in the maximum value of T_c from $\varepsilon = 0$ to $\varepsilon = 0.2$ at $\lambda_v = 10 \times 10^{-5}\ /m^2$ and $\lambda_e = 1 \times 10^{-5}\ /m^2$.

Fig. 7 presents the optimum access threshold for scheme S1 versus the error coefficient ε for different R_t and λ_e. For each curve in Fig. 7, the optimum access threshold is shown to increase at the beginning as the parameter ε increases, because a larger access threshold can bring an enhancement to connection performance to balance the deterioration caused by the channel estimation error. However, when the parameter ε continuously increases, the interference caused by the channel estimation error becomes more and more serious, which leads to a reduction of access threshold in order to maintain the quality of the offloading link to support the target offloading secrecy rate. Furthermore, for a given ε, the tendency that the optimum access threshold declines as the Eves density λ_e increases is also presented in Fig. 7, which can be attributed to the growing interference caused by D2D-V links. The increase in the Eves density λ_e leads to more serious security outage to the offloading link. Consequently, the optimum access threshold decreases because a higher level of interference brings potential benefits to confuse the eavesdroppers. As expected, an increased transmitted codeword rate R_t implies an improved the optimum access threshold. This is because a larger access threshold can bring about an enhancement to connection performance for balancing the deterioration caused by the increase in R_t. By an overall, comparison of the four curves, the difference of optimal access threshold is shown to decrease and then gradually tend to zero with the increases of the parameter ε, because the security throughput is very small when the channel estimation error becomes larger. As a result, optimizing access threshold does not boost the security throughput.

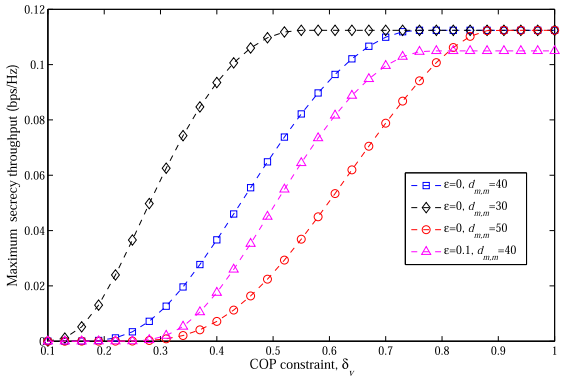


FIGURE 8. The maximum security throughput versus the COP constraint δ_v.

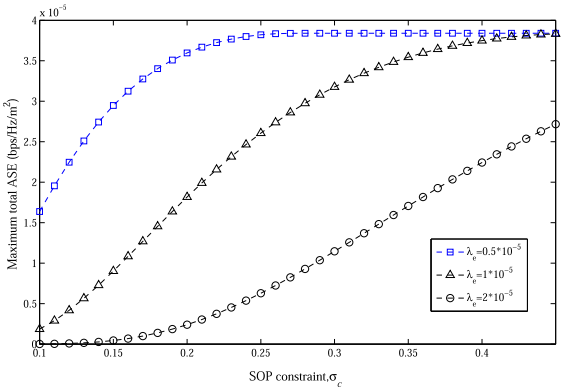


FIGURE 9. The maximum total ASE versus the SOP constraint σ_c.

Fig. 8 presents the maximum security throughput versus the COP constraint δ_v for different ε and $d_{m,m}$, where $R_t = 0.8$ bps/Hz, $R_e = 0.2$ bps/Hz, $\lambda_v = 20 \times 10^{-5}$ $/m^2$, and $\lambda_e = 1 \times 10^{-5}$ $/m^2$. It is shown that the maximum security throughput rises gradually at the beginning and then gradually tends to stabilize with increasing δ_v from all considered ε and $d_{m,m}$. The reason is that the optimal access threshold that maximizes security throughput can be achieved either on the boundary point or on the critical point. When the COP is relatively small (e.g., $\delta_v < 0.7$), the boundary point $p_{s,1}$ for guaranteeing the connection performance of D2D-V link is less than the critical point p_s^*. Therefore, the maximum security throughput increases as the COP constraint increases. Specifically, when $p_{s,1}$ is beyond p_s^*, the maximum security throughput remains unchanged, which agrees with the result in (29). At the same time, the longer the D2D-V link distance $d_{m,m}$, the faster the convergence. This phenomenon can be explained as follows: the longer $d_{m,m}$ brings more propagation loss to the connection performance of D2D-V links, and we need to reduce the access D2D-V pairs in order to maintain the same security throughput. Furthermore, the estimation error coefficient is also shown to bring about security throughput deterioration from the curve of Fig. 8.

Fig. 9 presents the maximum total ASE versus the SOP constraint σ_c for variant λ_e. With the increases in SOP constraint σ_c, the maximum total ASE η_{tot} increases substantially, implying that improving the total ASE causes a worse security performance. Given a fixed σ_c, the total ASE is shown to be lower when $\lambda_e = 1 \times 10^{-5}$ $/m^2$ than that of the case when $\lambda_e = 0.5 \times 10^{-5}$ $/m^2$, because the optimal access threshold decreases with λ_e and thus the cross-tier and the intra D2D-V interference become more serious. Hence, the maximum total ASE decreases with λ_e.

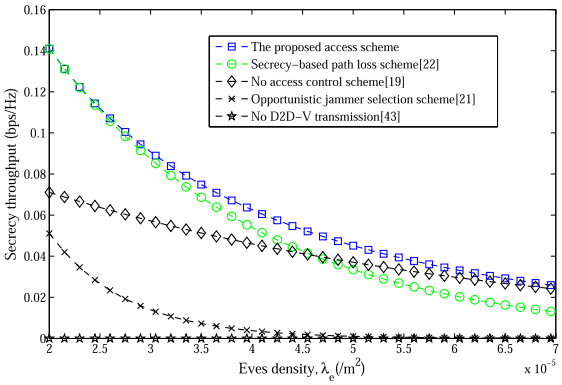


FIGURE 10. The maximum security throughput versus the Eves density λ_e for different schemes.

Fig. 10 presents a comparison of the maximum security throughput against the Eves density λ_e for the proposed scheme as well as the No access control scheme in [19], (i.e., all D2D-V links are active), the opportunistic jammer selection scheme in [21], the secrecy-based path loss access scheme in [22], and the No D2D-V links transmission scheme in [43]. It is shown that the maximum security throughput decreases gradually as λ_e increases for all considered D2D-V access schemes. Furthermore, it is also shown that the proposed access scheme can improve the security throughput and provide evident performance gain when compared with the other access schemes. As expected, as the Eves density increases, the proposed scheme always outperforms the no access control scheme, and the disparity continues to lessen. We can explain it as follows: when the parameter λ_e is small, the co-channel interference generated by all active D2D-V links severely disrupts the connection performance of the offloading link. However, this interference has a positive influence on protecting the offloading link from eavesdropping threat when the parameter λ_e is larger. Compared with the secrecy-based path loss access scheme, we can benefit by using our scheme, especially in the high Eves density regime. This means that the proposed access scheme is capable of effectively selecting and controlling the access threshold of D2D-V links under different channel conditions, thereby improving the security throughput performance.

VI. CONCLUSION AND FUTURE WORK

In this paper, the dynamic threshold-based D2D-V access scheme has been investigated for security provisioning of C-V2X computation-offloading network with imperfect CSI. The interference generated by D2D-V links spectrum multiplex has been exploited to confuse the eavesdroppers. Meanwhile, the optimized access thresholds have been designed

for maximizing the security throughput of the offloading link under a connection outage constraint of the D2D-V links, as well as maximizing the total ASE subject to a secrecy outage constraint. Furthermore, numerical results have demonstrated the performance of the proposed scheme. More importantly, the optimized access threshold can be set to update adaptively under variant channel conditions, which operation is expected to benefit future security provisioning research in this area. For our future work, we will extend the current work to investigate the secrecy provisioning issues by incorporating secrecy guard zone and computation resource management for C-V2X computation-offloading network. In addition, it is also an interesting future direction for us to investigate the PLS analysis for non-orthogonal multiple access (NOMA) scheme in C-V2X computation-offloading network, where multiple vehicular users offloaded their respective computation tasks to the BS with the uplink NOMA scheme.

REFERENCES

[1] J. Zhao, Q. Li, Y. Gong, and K. Zhang, "Computation offloading and resource allocation for cloud assisted mobile edge computing in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 8, pp. 7944-7956, Aug. 2019.

[2] P. Liu, J. L. Li, and Z. G. Sun, "Matching-based task offloading for vehicular edge computing," *IEEE Access*, vol. 7, pp. 27628-27640, Mar. 2019.

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

[4] P. Mach and Z. Becvar, "Mobile edge computing: A survey on architecture and computation offloading," *IEEE Commun. Surv. Tuts.*, vol. 19, no. 3, pp. 1628-1656, 3rd Quart., 2017.

[5] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Veh. Commun.*, vol. 1, no. 2, pp. 53-56, Apr. 2014.

[6] Y. Wu, L. P. Qian, H. W. Mao, X. X. Yang, H. B. Zhou, X. Tan, and D. H. K. Tsang, "Secrecy-driven resource management for vehicular computation offloading networks," *IEEE Netw.*, vol. 32, no. 3, pp. 84-91, May 2018.

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

[8] M. Raya, P. Papadimitratos, I. Aad, D. Jungels and J. P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 8, pp. 1557-1568, Oct. 2007.

[9] N. Kaur and S. Kad, "A review on security related aspects in vehicular ad hoc networks," *Procedia Comput. Sci.*, vol. 78, pp. 387-394, Apr. 2016.

[10] C. K. Karn and C. P. Gupta, "A survey on VANETs security attacks and sybil attack detection," *Int. J. Sensors Wireless Commun. Control.*, vol. 6, no. 1, pp. 45-62, 2016.

[11] Y. Li, R. H. Hou, K. S. Lui, and H. Li, "An MEC-based DoS attack detection mechanism for C-V2X Networks," *2018 IEEE Global Communications Conference (GLOBECOM)*, Abu Dhabi, UAE, pp. 1-6, 2018.

[12] Z. Zhang, K. Long, S. Member, and J. Wang, " On swarm intelligence inspired self-organized networking: Its bionic mechanisms, designing principles and optimization approaches," *IEEE Commun. Surv. Tuts.*, vol. 16, no. 1, pp. 513-537, 1th Quart., 2014.

[13] Y. Zou, X. Wang, W. Shen, and L. Hanzo, " Security versus reliability analysis of opportunistic relaying," *IEEE Trans. Veh. Technol.*, vol. 63, no. 6, pp. 2653-2661, Jul. 2014.

[14] D. W. Wang, P. Y. Ren, Q. H. Du, L. Sun, and Y. C. W, "Security provisioning for MISO vehicular relay networks via cooperative jamming and signal superposition," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 10732-10747, Dec. 2017.

[15] X. Hu, P. Mu, B. Wang, and Z. Li, "On the secrecy rate maximization with uncoordinated cooperative jamming by single-antenna helpers," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 4457-4462, May 2017.

[16] Y. Huo, X. Fan, L. Ma, X. Cheng, Z. Tian, and D. C. Chen, "Secure communications in tiered 5G wireless networks with cooperative jamming," *IEEE Trans. Signal Process.*, vol. 18, no. 6, pp. 3265-3280, Jun. 2019.

[17] L. Hu, H. Wen, B. Wu, J. Tang, F. Pan, and R. F. Liao, "Cooperative jamming aided secrecy enhancement in wireless networks with passive eavesdroppers," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2108-2117, Mar. 2018.

[18] F. Jameel, S. Wyne, G. Kaddoum, and Q. Duong, "A comprehensive survey on cooperative relaying and jamming strategies for physical layer security," *IEEE Commun. Surv. Tuts.*, vol. 21, no. 3, pp. 2734-2771, 3th Quart., 2019.

[19] L. M. Wang, and X. L. Liu, "Secure cooperative communication scheme for vehicular heterogeneous networks," *Veh. Commum.*, vol. 11, pp. 46-56, Jan. 2018.

[20] J. Zhao, X. Guan, Z. Ding, and X. Li, "Power allocation based on genetic simulated annealing algorithm in cognitive radio networks," *Chinese J. Electron.*, vol. 22, no. 1, pp. 177-180, Jan. 2013.

[21] J. Yue, C. Ma, H. Yu, and W. Zhou, "Secrecy-based access control for device-to-device communication underlaying cellular networks," *IEEE Commun. Lett.*, vol. 17, no. 11, pp. 2068-2071, Nov. 2013.

[22] Y. J. Tolossa, S. Vuppala, G. Kaddoum, and G. Abreu, "On the uplink secrecy capacity analysis in D2D-enabled cellular network," *IEEE Syst. J.*, vol. 12, no. 3, pp. 2297-2307, 2018.

[23] W. Wang, K. Teh, and K. Li, 'Enhanced physical layer security in D2D spectrum sharing networks," *IEEE Wireless Commun. Lett.*, vol. 6, no. 1, pp. 106-109, Feb. 2017.

[24] P. Sun, G. S. Kang, H. Zhang, and L. He, "Transmit power control for D2D underlaid cellular networks based on statistical features," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 4110-4119, May 2017.

[25] Y. Ma, L. Zhou, Z. Gu, Y. Song, and B. Wang, "Channel access and power control for mobile crowdsourcing in device-to-device underlaid cellular networks," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1-13, Jan. 2018.

[26] L. Liang, J. Kim, S. C. Jha, K. Sivanesan, and G. Y. Li, "Spectrum and power allocation for vehicular communications with delayed CSI feedback," *IEEE Wireless Commun. Letters*, vol. 6, no. 4, pp. 458-461, Aug. 2017.

[27] P. S. Bithas, G. P. Efthymoglou, and A. G Kanatas, "V2V cooperative relaying communications under interference and outdated CSI," *IEEE Trans. Veh. Technol.*, vol. 67, no. 4, pp. 3466-3480, Apr. 2018.

[28] Z. X. Liu, X. Han, Y. Liu, and Y. Wang, "D2D-based vehicular communication with delayed CSI feedback," *IEEE Access*, vol. 6, pp. 52857-52866, Oct. 2018.

[29] H. Zhang, Y. Ma, D. Yuan, and H. -H. Chen, "Quality-of-service driven power and sub-carrier allocation policy for vehicular communication networks," *IEEE Trans. Intell. Syst.*, vol. 29, no. 1, pp. 176-206, Jan. 2011.

[30] N. Cheng, H. Zhou, L. Lei, N. Zhang, Y. Zhou, X. Shen, and F. Bai, "Performance analysis of vehicular device-to-device underlay communication," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 5409-5421, Jun. 2017.

[31] W. Sun, D. Yuan, E. G. Ström, and F. Brännström, "Cluster-based radio resource management for D2D-supported safety-critical V2X communications," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2756-2769, Apr. 2016.

[32] Y. Cai, X. Xu, and W. Yang, "Secure transmission in the random cognitive radio networks with secrecy guard zone and artificial noise," *IET Commun.*, vol. 10, no. 15, pp. 1904-1913, Oct. 2016.

[33] X. Y. Liu, K. C. Zheng, X.Y. Liu, X. B. Wang, and G. J. Dai, 'Towards secure and energy-efficient CRNs via embracing interference: A stochastic geometry approach," *IEEE Access*, vol. 6, no. 1, pp. 36757-36770, Jul. 2018.

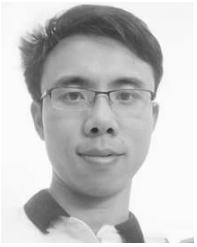
[34] L. Wang, J. M. Liu, M. K. Chen, G. Gui, and H. Sari, "Optimization-based access assignment scheme for physical-layer security in D2D communications underlaying a cellular network," *IEEE Trans. Veh. Technol.*, pp. 67, no. 7, pp. 5766-5777, Jul. 2018.

[35] T. X. Zheng and H. M. Wang, "Optimal power allocation for artificial noise under imperfect CSI against spatially random eavesdroppers," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8812-8817, Oct. 2016.

[36] B. Rong, Z. Zhang, X. Zhao, and X. Yu, "Robust superimposed training designs for MIMO relaying systems under general power constraints," *IEEE Access*, vol. 7, pp. 80404-80420, Jun. 2019.

[37] M. F. Feteiha and M. Uysal, "On the performance of MIMO cooperative transmission for broadband vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 6, pp. 2297-2305, Aug. 2015.

[38] Y. Zhang, Y. Shen, X. Jiang, and S. Kasahara, "Mode selection and spectrum partition for D2D inband communications: A physical layer security perspective," *IEEE Trans. Commun.*, vol. 67, no. 1, pp. 623-638, Jan. 2019.
[39] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjorungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764-2775, Jun. 2011.
[40] A. Menmi, Z. Rezki, and M. S. Alouini, "Power control for D2D underlay cellular networks with channel uncertainty," *IEEE Trans. Wireless Commun.*, vol. 16, no. 2, pp. 1330-1343, Apr. 2017.
[41] Z. Chen and M. Kountouris, "Decentralized opportunistic access for D2D underlaid cellular networks," *IEEE Trans. Wireless Commun.*, vol. 66, no. 10, pp. 4842-4853, Oct. 2018.
[42] N. Lee, X. Lin, J. G. Andrews, and R. W. Heath, "Power control for D2D underlaid cellular networks: Modeling, algorithms, and analysis," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 1, pp. 1-13, Jan. 2015.
[43] S. Vuppala and G. Abreu, "Unicasting on the secrecy graph," *IEEE Trans. Inf. Forens. Security*, vol. 8, no. 9, pp. 1469-1481, Sep. 2013.



BIN QIU received the B.S. and M.S. degrees from the School of Computer and Electronic Information, Guangxi University, Nanning, China, in 2010 and 2013, respectively. He is currently pursuing the Ph.D. degree with the Guilin University of Electronic Technology, Guilin, China. He is currently a Lecturer with the College of Information Science and Engineering, Guilin University of Technology, Guilin. His research interests include vehicular communication, physical layer security, and channel modeling.

HAILIN XIAO (Member, IEEE) received the B.S. degree from Wuhan University, in 1998, the M.S. degree from Guangxi Normal University, in 2004, and the Ph.D. degree from the University of Electronic Science and Technology of China (UESTC), in 2007. He was a Research Fellow with the Joint Research Institute for Signal and Image Processing, School of Engineering and Physical Sciences, Heriot-Watt University, from January 2011 to February 2012. He was also a Research Fellow with the School of Electronics and Computer Science (ECS), University of Southampton, from March 2016 to March 2017. He is currently a Professor with the School of Computer Science and Information Engineering, Hubei University, China. He has published one book chapter and over 200 articles in refereed journals and conference proceedings. His research interests include MIMO wireless communications, cooperative communications, and vehicular communication. He has received Guangxi Natural Science Foundation for Distinguished Young Scholars, the Guangxi Natural Science Award, and a Distinguished Professor of the Qianjiang Scholars, China, in 2014, 2015, and 2018, respectively. He has served as a TPC Member and the Session Chair for some international conferences.

ANTHONY THEODORE CHRONOPOULOS (Senior Member, IEEE) received the Ph.D. degree in computer science from the University of Illinois at Urbana-Champaign, in 1987. He is currently a Full Professor with the Department of Computer Science, The University of Texas at San Antonio, San Antonio, TX, USA, and a Visiting Professor with the Department of Computer Engineering and Informatics, University of Patras, Greece. He is the author of 89 journal and 73 peer-reviewed conference proceedings publications in the areas of distributed and parallel computing, grid and cloud computing, scientific computing, wireless communications, computational intelligence, and machine learning. He is also a fellow of the Institution of Engineering and Technology (FIET), and ACM Senior member.

DI ZHOU received the M.S. degree from Southeast University, China, in 2001. He is currently pursuing the Ph.D. degree with Zhejiang University, Hangzhou, China. He is currently a Senior Engineer with Zhejiang Uniview Technologies Company, Ltd., Hangzhou. His research interests include intelligent information processing and cloud computing.

SHAN OUYANG (Senior Member, IEEE) received the B.S. degree in electronic engineering from the Guilin University of Electronic Technology (GUET), China, in 1986, and the M.S. and Ph.D. degrees in electronic engineering from Xidian University, Xi'an, China, in 1992 and 2000, respectively. From June 2001 to May 2002, he was a Research Associate with the Department of Electronic Engineering, The Chinese University of Hong Kong. From January 2003 to January 2004, he was a Research Fellow with the Department of Electronic Engineering, University of California, Riverside. He is currently a Professor with the School of Information and Communications, GUET. His research interests are mainly in the areas of signal processing for communications and radar, adaptive filtering, and neural network learning theory and applications. He received the Outstanding Youth Award from the Ministry of Electronic Industry and the Guangxi Province Outstanding Teacher Award, China, in 1995 and 1997, respectively. He received the National Excellent Doctoral Dissertation of China, in 2002.