Secrecy-Driven Resource Management for Vehicular Computation Offloading Networks

Yuan Wu, Li Ping Qian, Haowei Mao, Xiaowei Yang, Haibo Zhou, Xiaoqi Tan, and Danny H. K. Tsang

Abstract

The growing developments in vehicular networks and vehicular Internet services have yielded a variety of computation-intensive applications, resulting in great pressure on vehicles equipped with limited computation resources. The cloud/edge-based service, which enables in-motion vehicles to actively offload computation tasks to cloud/edge servers, has provided a promising approach to address the intensive computation burden. However, due to the possibility of disclosing private data, offloading computation tasks suffers from potential eavesdropping attacks. In this article, we focus on the eavesdropping attack when vehicular users (VUs) deliver computation tasks to cloud/edge servers over radio frequency channels. We take the tool of physical layer security and investigate resource management for secrecy provisioning when the VUs offload computation tasks. We then discuss three promising technologies, including non-orthogonal multiple access, multi-access assisted computation offloading, and mobility- and delay-aware offloading, which facilitate the enhancement of secrecy against the eavesdropping attack. Finally, as a detailed example of the multi-access assisted computation offloading, we present a case study on the optimal dual-connectivity-assisted computation task offloading with secrecy provisioning and show the performance of the proposed computation offloading.

Introduction

The past decades have witnessed explosive growth of vehicular networks comprising a large number of Internet-connected smart vehicles and intelligent transportation infrastructures. Along with the growing maturity of vehicular networks and mobile Internet services, a lot of data-intensive and computation-intensive services have appeared, such as virtual-reality-assisted driving safety services, which require a significant amount of computation resources to process and analyze the huge volume of sensing data in real time. However, due to the cost issue, an individual vehicle is usually equipped with limited computation resources, which limit the in-motion vehicular user's (VU's) capability to process the huge volume of data. By exploiting the advanced fourth/fifth generation (4G/5G) cellular networks comprising a large number of heterogeneous small cells, actively offloading on-vehicle computation tasks to cloud servers with vast computation resources has been envisioned as a promising paradigm to realize computation-efficient and resource-efficient vehicular services [1–4]. To further reduce the backhaul delay when delivering a computation task to the cloud, one can deploy small computation-servers directly at the edge of radio access networks (RANs), for example, by being co-located with roadside units (RSUs) in intelligent transportation infrastructures. Hence, vehicles can actively exploit the computation resources in close proximity to RSUs and improve the computation efficiency and resource efficiency when offloading computation tasks. In essence, the above paradigms of vehicular cloud/edge computing (VCEC) coordinate distributed resources (e.g., computing, communication, and sensing) in vehicles and intelligent transportation infrastructures, and thus are expected to realize vehicular Internet services with low latency and high reliability.

Despite the potential of VCEC, there are several challenging issues to address. For instance, a significant computation delay will occur if too many VUs aggressively offload their computation tasks to the same cloud/edge server. Such a phenomenon will be aggravated if we take into account the transmission delay when lots of VUs share the same frequency channel to offload their computation tasks. Thus, to reap the benefit of VCEC, joint management of computation task offloading and radio resource management (for transmitting computation tasks and receiving the results) is required. Security is another important issue for the success of VCEC, which necessitates effective strategies to tackle security threats such as denial of service (DoS) attacks and authentication attacks. In particular, since migrating a computation task to cloud/edge servers requires disclosing VUs' private data, eavesdropping attacks on the VUs' offloaded data has been considered as a critical security threat in VCEC. The risk of being eavesdropped becomes even more severe when we take into account that the VUs rely on the RF channel to transmit computation task to RSUs and receive the consequent computation result. The broadcasting nature and open access of the RF channel undoubtedly lead to the issue of secrecy outage, namely, some malicious users can overhear the computation task offloaded from the VUs and the computation result returned by the RSUs, by intentionally collecting radio signal over some targeted frequency channel. Such a secrecy outage risk has become more critical, since future 5G heterogeneous RANs rely more on the unlicensed bands to accommodate VUs [5].

This work was supported in part by the National Natural Science Foundation of China under Grant 61572440 and Grant 61379122, in part by the Zhejiang Provincial Natural Science Foundation of China under Grant LR17F010002 and Grant LR16F010003 , and in part by the Young Talent Cultivation Project of Zhejiang Association for Science and Technology under Grant 2016YCGC011.

Digital Object Identifier: 10.1109/MNET.2018.1700320

Li Ping Qian (corresponding author), Haowei Mao, and Xiaowei Yang are with Zhejiang University of Technology; Yuan Wu is with Zhejiang University of Technology and Xidian University; Haibo Zhou is with Nanjing University; Xiaoqi Tan and Danny H. K. Tsang are with Hong Kong University of Science and Technology.

In this article, we thus focus on the eavesdropping attack on VUs' computation offloading in VCEC and investigate the secrecy provisioning strategy against the eavesdropping attack from the perspective of radio resource allocation. Despite many existing studies focusing on encryption-based algorithms [6–8], we provide secrecy provisioning for the VUs' computation offloading based on the theory of physical layer security [9, 10]. In particular, the capacity of physical layer security provides a fundamental measure of how secure it is when the VUs use the RF channel to offload computation tasks without being eavesdropped by any malicious user. Specifically, we first overview the resource management of VUs' computation offloading that takes into account secrecy provisioning against the eavesdropping attack. We then discuss three promising technologies, including non-orthogonal multiple access (NOMA) [12], multi-access-assisted computation offloading [14], and mobility- and-delay-aware offloading, which facilitate the enhancement of secrecy provisioning in VCEC. As a concrete example of the multi-access-assisted computation offloading, we present a case study on the small cell dual connectivity (DC)-assisted computation task offloading with secrecy provisioning, and show the performance of the proposed computation task offloading. We finally conclude this article and discuss future directions.

Secrecy Provisioning Based on Physical Layer Security for VUs' Computation Offloading

A Brief Introduction to Physical Layer Security

We first provide a brief introduction to physical layer security, through which we quantify how secure it is when VUs offload computation tasks against potential eavesdropping attacks. Specifically, based on the information-theoretic analysis, the physical layer security stems from Shannon's channel capacity theory and provides a fundamental measure of the throughput (e.g., for offloading the VUs' computation tasks) which can be securely delivered over wireless channel without being overheard by any malicious user. Mathematically, according to the principle of physical layer security [9, 10], the secure capacity (which is also referred to as the physical layer security capacity) from VU i to RSU k can be given by

$$C_{ik}^{\text{sec}}(W_k, p_{ik}) = \max\left\{W_k \log_2\left(1+\frac{p_{ik}g_{ik}}{n_0}\right) - W_k \log_2\left(1+\frac{p_{ik}g_{iE}}{n_0}\right), 0\right\}, \quad (1)$$

where W_k denotes the channel bandwidth provided by RSU k, and p_{ik} denotes the transmit power of VU i for offloading its computation task to RSU k. Parameter g_{ik} denotes the channel power gain from VU i to RSU k, and g_{iE} denotes the channel gain from VU i to the eavesdropper (i.e., the malicious user). Parameter n_0 denotes the power of the background noise. Essentially, C_{ik}^{sec} quantifies the difference between Shannon's channel capacity from VU i to RSU k and the channel capacity from VU i to the eavesdropper. As shown in Eq. 1, the physical layer security capacity depends on radio resource allocation (e.g., the RSU's channel bandwidth and the VU's transmit power).

As a key difference compared to these encryption-based algorithms, the metric of physical layer security does not rely on any particular application-layer-oriented cryptography technique. In other words, the secrecy level provided by the physical layer security will not be compromised by the VUs' limited computation resources.

Taking into account that the eavesdropper might intentionally hide its position, the channel power gain from VU i to the malicious user is usually considered as a random parameter. As a result, by assuming an average channel power gain from VU i to the malicious user, the secrecy outage probability when VU i offloads its computation task to RSU k can be given by

$$P_{out}^{\text{sec}}(W_k, p_{ik}, r_{ik}) = \Pr\left\{r_{ik} > C_{ik}^{\text{sec}}(W_k, p_{ik})\right\}, \quad (2)$$

that is, the probability that VU i's assigned offloading rate r_{ik} to RSU k is greater than the corresponding physical layer security capacity given in Eq. 1. $P_{\text{out}}^{\text{sec}}$ measures how likely it is that VU i's offloaded computation task will be eavesdropped by the malicious node (or equivalently, the percentage of VU i's offloaded computation task that is overheard). The secrecy outage probability in Eq. 2 indicates that the secrecy-based transmission rate depends on a joint effect of the VU's transmit power allocation, the assigned offloading rate, and the RSU's radio frequency bandwidth. Specifically, assigning a large offloading rate but using small transmit power will lead to a severe offloading outage, meaning that a significant portion of the offloaded task will be overheard by the malicious user. On the other hand, assigning a small offloading rate but using a large transmit power yields a low offloading outage (meaning that strong secrecy provisioning is provided), but with the downside of wasting radio resources overly provided.

Please notice that although there have been many application-layer encryption-based algorithms proposed for protecting users' private data from being eavesdropped, the performance of these encryption-based algorithms strongly depends on the involved computational complexity [7, 8]. In general, the higher computation complexity used by the encryption algorithm, the stronger the security level that can be achieved. As a key difference compared to these encryption-based algorithms, the metric of physical layer security does not rely on any particular application-layer-oriented cryptography technique. In other words, the secrecy level provided by the physical layer security (e.g., the secrecy outage probability) will not be compromised by the VUs' limited computation resources.

Different Paradigms of Eavesdropping Attack in VCEC

The RF channel is indispensable for in-motion VUs to offload computation tasks. Thanks to the advanced heterogeneous 5G RANs, a variety of radio connections can be exploited by VUs, including the long-distance radio link based on 4G/5G cellular systems, and the short-distance radio link based on WiFi hotspots [1]. In particular, the recently advanced LTE for vehicular communi-

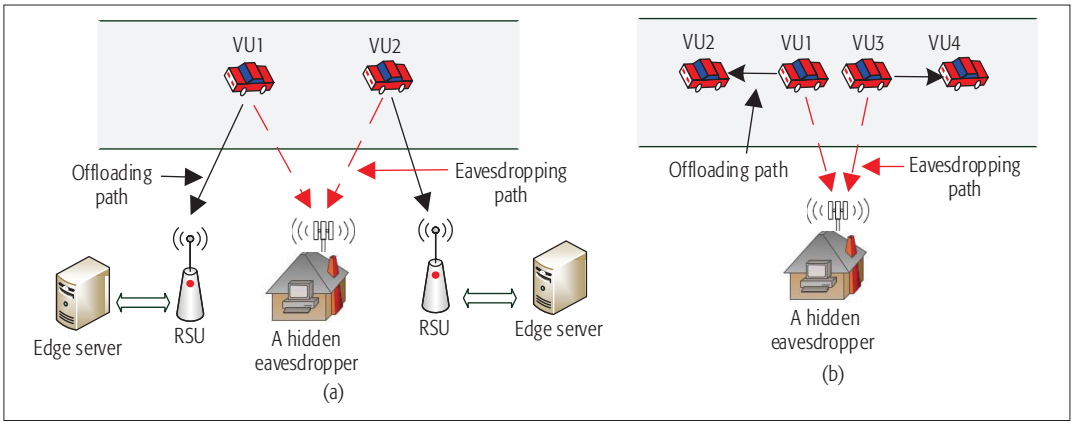

FIGURE 1. Illustration of eavesdropping attack on a) V2I links; b) V2V links.

Although the highly dynamic topology of in-motion VUs makes the eavesdropping attack on V2V offloading much more difficult, the dynamic topology also leads to the challenge to achieve distributed coordination among different VUs' resource management to reach the required secrecy provisioning.

cations (LTE-V) [11] enables both paradigms of vehicular-to-infrastructure (V2I) communications and vehicular-to-vehicular (V2V) communications, which thus facilitate the VU's computation task offloading to infrastructure (e.g., cloud/edge servers) as well as computation offloading to nearby VUs with sufficient computation resources. As shown in Fig. 1, the corresponding eavesdropping attack can be categorized as follows.

Eavesdropping attack on computation offloading over a V2I link: As shown in Fig. 1a, the paradigm of V2I communication enables the VUs to offload computation tasks to RSUs, which are either equipped with edge servers or connected to remote cloud servers. The RF channels for the RSUs to accommodate the VUs' computation task offloading are usually open to the public, and thus are apt to be eavesdropped by malicious users who can intentionally collect the radio signal over some targeted channels. In addition, the fixed location of the RSU further makes the secrecy outage issue serious, since malicious users can estimate the channel gain information to the RSUs to eavesdrop the data.

Eavesdropping attack on computation offloading over a V2V link: As shown in Fig. 1b, by exploiting the paradigm of V2V communications, a VU can also offload its computation task to nearby VUs with sufficient computation resources. In addition, with V2V communications, the VU can act as a relay to forward the computation task from some other VU to the RSU. Although the highly dynamic topology of the in-motion VUs makes the eavesdropping attack on V2V offloading much more difficult, the dynamic topology also leads to the challenge of achieving distributed coordination among different VUs' resource management to reach the required secrecy provisioning.

Resource Consumption for Secrecy Provisioning in VCEC

The VUs' computation task offloading and the associated secrecy provisioning incur a variety of different costs. We discuss some of them as follows.

Cost for computation resource: Despite reducing the computation burden at the VUs, offloading computation tasks consumes the computation resources at the cloud/edge servers, which needs to be taken into account. Moreover, when many VUs offload their computation tasks to the same cloud/edge server, cooperative sharing or allocation of the computation resources at the cloud/edge servers is necessary to avoid excessive processing delay.

Cost for delay in computation offloading: Compared to processing the computation task locally, offloading computation tasks involves additional delays, which include:

- The processing delay for the computation task at the cloud/edge servers
- The backhaul delay for delivering computation tasks among differen cloud/edge servers
- The transmission delay in RANs for delivering the computation tasks to the RSUs and receiving the computation result from the RSUs

Radio resource cost: Offloading computation tasks over the radio link requires the use of various radio resources, including frequency channel, transmit power, and time slot (in both the uplink stream from the VUs to infrastructure and the downlink stream from the infrastructure to VUs). In general, the VU can achieve a faster computation task offloading rate if more radio resources are utilized.

Secrecy outage cost: Secrecy outage can be considered as a cost in computation task offloading. For instance, a security-sensitive application may require the re-execution of the computation task (with some randomized parameter setting) if the offloaded task has been overheard by malicious users. However, re-executing a computation task consumes additional computation resources as well as radio resources for data delivery.

Trade-off among Computation Efficiency, Resource Efficiency, and Secrecy Efficiency

The physical layer security capacity in Eq. 1 and the associated metric of secrecy outage probability in Eq. 2 mean that radio resource provisioning and the VU's computation task offloading rate will together influence the experienced secrecy. In general, the more radio resources utilized (e.g., larger bandwidth allocation or larger transmit power), the less the risk of being overheard. On the other hand, the higher the VU's computation task offloading rate, the higher the risk of being overheard.

For instance, due to limited local computation resources, a group of VUs might choose to aggressively offload their computation tasks to the same RSU equipped with an edge server, which consequently leads to longer transmission delay and a degraded secrecy level according to Eq. 2. In essence, as shown in Fig. 2, careful management of the trade-off among resource utilization efficiency, computation task offloading efficiency, and secrecy provisioning efficiency is required.

Computation efficiency vs. radio resource efficiency: By exploiting the computation resources provided by the cloud/edge servers, offloading computation tasks from VUs can significantly improve the overall computation efficiency and yield a short computation time. However, offloading a computation task over a wireless link consumes radio resources (e.g., transmit power and channel bandwidth). Such consumption of radio resources might be significant when a very short transmission delay is required for offloading delay-sensitive computation tasks. Moreover, when a larger number of VUs simultaneously offload their computation tasks to the same RSU, severe congestion might occur on the wireless link, which leads to significant transmission delay and degrades the efficiency of resource utilization.

Secrecy efficiency vs. radio resource efficiency: As illustrated before, secrecy provisioning according to the physical layer security (and the associated secrecy outage probability) requires the use of a certain amount of radio resources. In general, the more radio resources utilized (e.g., transmit power and channel bandwidth), the stronger the secrecy provisioning provided, which leads to the trade-off between secrecy efficiency and radio resource utilization.

The above coupling issues yield challenges in balancing the computation efficiency, resource efficiency, and secrecy efficiency. Therefore, for secrecy provisioning, the VU's computation offloading needs to jointly take into account several issues, such as the data volume of the task, the delay requirement for executing the task, the available radio resource, as well as the secrecy requirement.

Technologies for Enhancing Secrecy in Computation Task Offloading

In this section, we discuss three promising technologies that can enhance secrecy provisioning in VCEC by proper radio resource allocation, including NOMA-assisted computation task offloading, multi-access-assisted computation offloading, and mobility- and-delay-aware offloading.

NOMA-Assisted Computation Task Offloading

As an enabling technology for future 5G cellular systems, NOMA has attracted lots of interest in recent years [12]. Different from conventional orthogonal multiple access (OMA), which uses separate radio resource blocks (RRBs) to serve different mobile users, NOMA enables a group of users to share a frequency channel simultaneously via power/code domain division and further adopts successive interference cancellation to mitigate the co-channel interference among users. Therefore, NOMA is able to realize the massive connectivity required by 5G applications

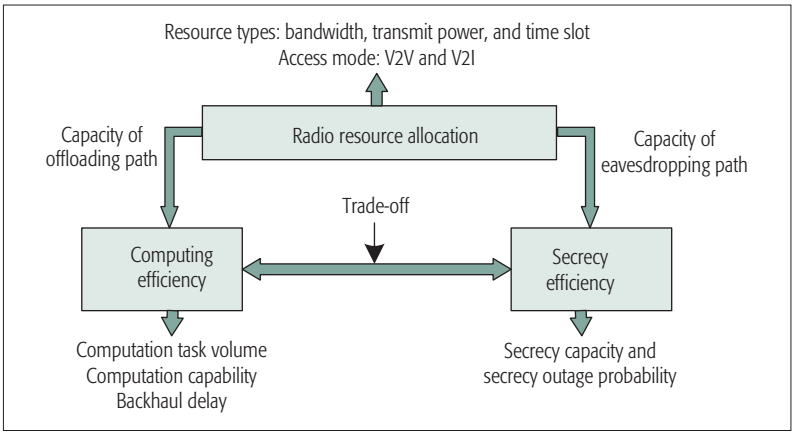

FIGURE 2. Relationships among resource utilization efficiency, computation task offloading efficiency, and secrecy efficiency.

(e.g., massive Internet of Things and vehicular networks) and significantly improve the spectrum efficiency and system throughput [13]. The potential of NOMA makes it an important technology to support VUs' computation task offloading. Specifically, by using NOMA, a group of VUs can form a NOMA cluster and simultaneously offload their computation tasks to the RSU over the same frequency channel. Similarly, to share the computation resources at a nearby VU, a group of VUs can form a NOMA cluster to simultaneously offload their computation tasks to this targeted VU. Based on different VUs' offloading requirements (e.g., data volume and delay requirement), one can significantly increase the offloading throughput by properly forming the NOMA cluster and allocating the consequent transmit power for each VU in the NOMA cluster. As a result, NOMA-assisted computation task offloading is expected to reach the ultimate goals of ultra-high throughput and low latency for VCEC.

The nature of NOMA and the in-cluster VUs' simultaneous transmissions over one frequency channel also bring the advantage of enhancing secrecy against the eavesdropping attack, namely, the allowable co-channel interference among VUs provides a helpful jamming signal to the eavesdropper. Figure 3 shows an example. Specifically, a group of five VUs form a NOMA cluster to offload their computation tasks to the RSU. There is a malicious user who intentionally overhears the offloaded computation task of VU 5. Thanks to the nature of NOMA, other in-cluster VUs' (i.e., VUs 1–4) signal provides artificial interference to the malicious user and effectively reduces the malicious user's capability of overhearing VU 5's signal. By properly allocating the channel bandwidth for serving the VUs, and allocating the VUs' transmit powers and computation task offloading rates, one can achieve the triple goals of satisfying the VUs' specified quality of service (QoS) for computation task offloading, providing sufficient jamming to the malicious user to protect the secrecy of the VUs' offloaded tasks, as well as improving the overall radio resource efficiency.[1]

Multi-Access-Assisted Computation Task Offloading

Multi-access edge computing (MAEC) is an emerging paradigm to improve the efficiency of edge computing by exploiting the multi-tier and

[1] Notice that when using NOMA, the successive interference cancellation requires decoding the vehicular users' respective messages one by one. Thus, additional decoding delay may be incurred for the VUs with strong channel power gains if there is a large number of VUs in the same NOMA cluster.

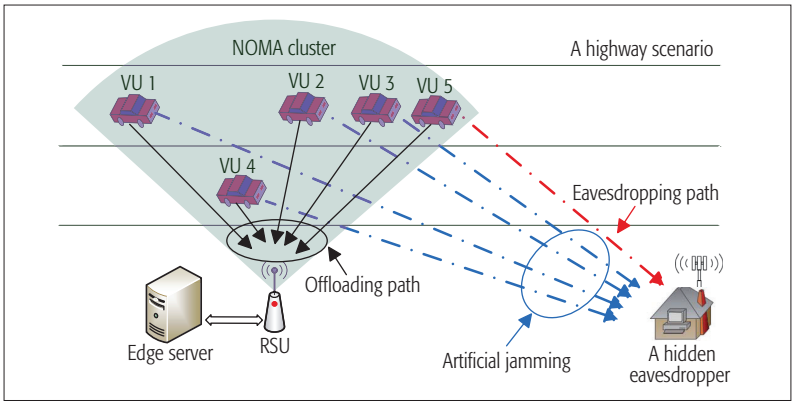

FIGURE 3. Example of NOMA-assisted computation task offloading to enhance the secrecy provisioning against eavesdropping attack.

heterogeneous structure of future RANs [14]. Specifically, driven by the heterogenous QoS and data-intensive mobile Internet service, future RANs have been evolving toward the architecture of dense small cells comprising micro/pico/femtocells, Wi-Fi hotspots, and various near-field access networks. Densely deployed small cells can significantly improve the capacity and quality of the connections between mobile terminals and cloud/edge servers. Based on MAEC, VUs, by exploiting the equipped multiple radio interfaces, can flexibly choose several RSUs to access simultaneously, which significantly improves throughput and reliability for accessing cloud/edge service. MAEC facilitates the implementation of reliable and ultra-low-latency connections and services. Specifically, exploiting MAEC and the available computation resources at different RSUs, the VU can offload its computation task to several RSUs simultaneously, which effectively reduces the transmission delay in delivering the computation task and improves the utilization efficiency of overall computation resources. In particular, as a concrete paradigm of MAEC, the recent Third Generation Partnership Project (3GPP) specification has proposed the paradigm of small cell dual connectivity (DC), which enables a mobile terminal (e.g., a VU) to communicate with the macrocell and simultaneously offload data to the small cell (e.g., the RSU in the intelligent transportation systems) [15].

The nature of heterogeneous multi-connectivity in MAEC can enhance the secrecy provisioning for the VUs' computation task offloading against the eavesdropping attack. Specifically, based on different levels of secrecy provided by different RSUs (or equivalently, the malicious user's eavesdropping strength to different RSUs), the VU can adaptively schedule the computation task to different RSUs to optimize the overall experience in offloading computation task while reaching the required secrecy level (e.g., by guaranteeing that the secrecy outage probability cannot exceed a certain threshold). Figure 4 illustrates such an example in which VU 1 exploits DC to simultaneously offload computation tasks to a macrocell base station (BS) and RSU 1. Based on the risk of being eavesdropped when delivering a computation task to RSU 1, VU 1 can adaptively schedule its computation tasks to RSU 1 and the macro BS. Specifically, VU 1 can use a large offloading rate to offload more pieces of a computation task to RSU 1 if RSU 1 experiences a low risk of being eavesdropped. In comparison, if RSU 1 experiences a high risk of being eavesdropped, VU 1 can offload more pieces of the computation task to the macro BS. Such freedom in adjusting the offloading rate and scheduling different amounts of computation tasks to the RSU and macro BS yields resource-efficient computation offloading with secrecy provisioning. Specifically, one can jointly optimize the computation task scheduling, the RSU access selection, and the associated radio resource allocation to achieve resource-efficient computation offloading while guaranteeing both QoS requirements and secrecy requirements for the VUs.

Mobility-Aware Computation Offloading

Due to physical limitations such as limited transmit power, the RSU suffers from limited coverage, meaning that the VU's offloaded computation task might not be finished within one edge server if the VU is moving quickly. Therefore, based on the predictive trajectory and the moving pattern, the VU can partition its computation task into many small pieces and adaptively offload these pieces to different RSUs. The advantage of this mobility-aware adaptive offloading lies in the VU being able to exploit the computation resources at different RSUs with different levels of secrecy provisioning. For instance, the VU can slow down the computation offloading when suffering from a high risk of being eavesdropped, and offload a computation task at a faster offloading rate to the RSU with sufficient computation resources and a lower risk of being eavesdropped.

However, as a key feature different from the MAEC-assisted computation offloading discussed in the previous subsection, the VU's mobility-aware offloading needs to take into account the delay tolerance of the targeted application. Specifically, given a stringent deadline (or delay-sensitive application), the VU will have very limited freedom in waiting to reach the RSU with a lower risk of being eavesdropped. As a result, the VU needs to either execute the computation task locally or spend more radio resources (e.g., a larger transmit power) to provide the required secrecy level against the eavesdropping attack. In comparison, with loose delay tolerance, the VU can have large freedom in waiting to reach the RSU with a lower risk of being eavesdropped and then executing the computation task offloading. Specifically, based on the delay tolerance of the computation task and the conditions of different RSUs (e.g., different risks of being eavesdropped, available computation resources, and channel gain conditions) on the moving trajectory, the VU can jointly optimize the RSU selection and the associated radio resource allocation to improve the resource utilization efficiency while satisfying both the VU's QoS requirement and secrecy requirement.

A Case Study of DC-Assisted Computation Offloading with Secrecy Provisioning

In this section, we provide a case study of DC-enabled computation offloading with secrecy provisioning [15]. As an example of MAEC, the DC enables each VU to simultaneously communi-

cate with the macrocell and an RSU, which thus facilitates flexible computation task scheduling between the macro base station (BS) and the RSU (we consider that both macro BS and RSU are connected with edge servers to provide computation resources).

Given the data volume to be processed within each scheduled period, the VU distributes its computation tasks between the macro BS and the RSU. Thanks to the close proximity to the RSU, the VU prefers to offload more computation tasks to the RSU, since it can save the total transmit-power consumption while providing a fast offloading rate (which reduces the delay in delivering the computation task). However, the RSU operates on unlicensed bands, and the offloaded data to the RSU might be overheard by some malicious eavesdroppers. Thus, aggressively offloading a computation task to the RSU, in spite of saving the VU's transmit power consumption, will lead to a large secrecy outage (i.e., a large portion of the offloaded data for executing the computation task will be eavesdropped by the malicious user), which may negatively influence the VU's experience. Therefore, a joint optimization of computation task scheduling and radio resource allocation is necessary to reap the benefit of DC-enabled computation task offloading with secrecy provisioning. Specifically, we consider the joint optimization as follows. The VU aims at minimizing its total transmit power consumption to deliver the computation task to the macro BS and the RSU. Regarding the constraints, we consider the following ones:

- *Secrecy requirement*: The VU ensures that the experienced secrecy outage probability (i.e., the percentage of the offloaded computation task that is overheard by the eavesdropper) is no greater than a given threshold.
- *QoS requirement*: The VU ensures that the total computation tasks securely delivered to the RSU and the macro BS are no smaller than the required volume, which can be equivalently translated to a constraint that the VU reaches a given secure offloading rate for delivering the computation tasks to the RSU and the macro BS.

Correspondingly, in the joint optimization problem, the control variables include i) the VU's offloading rate toward the macro BS and the RSU to deliver the respective computation tasks, and ii) the VU's transmit powers to the macro BS and the RSU. Notice that at the small cell side, in addition to accommodating the assigned offloading rate, the VU's transmit power needs to ensure that the offloading rate is sufficiently protected according to the secrecy requirement.

Figures 5a and 5b show the performance of the proposed computation task offloading when the VU moves along a line-street. We set a line-street to be of 1 km length, and the macro BS is located at (500, −300) m. There are three RSUs deployed, RSU 1 at (250, −10) m, RSU 2 at (500, −10) m, and RSU 3 at (750, −10) m. Meanwhile, we consider that there are three eavesdroppers close to the respective RSUs. To differentiate the eavesdroppers, we consider that the three eavesdroppers have different strengths to overhear the respective RSUs, with Eavesdropper 1 (overhearing RSU 1) the strongest and Eavesdropper 3 (overhearing RSU 3) the weakest. Figure 5a shows the result when one VU is moving along this line-street, and Fig. 5b shows the result of a group of 10 VUs (we set that each RSU can serve no more than 3 VUs in this case). We set that all VUs are moving at the speed of 50 km/h.

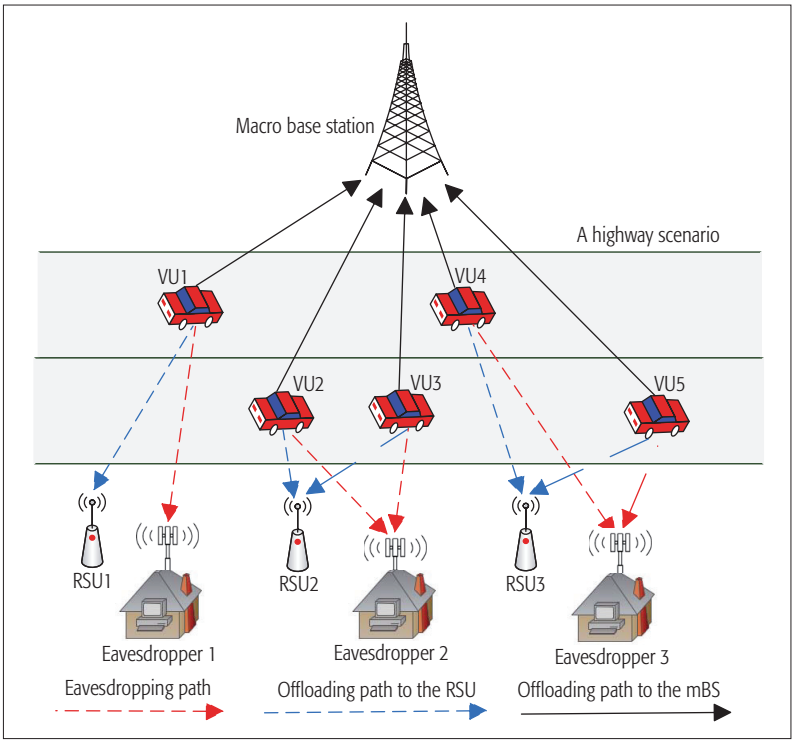

FIGURE 4. Example of MAEC-assisted (or DC-assisted) computation task offloading to enhance the secrecy provisioning against eavesdropping attack.

Figure 5a shows the performance of one VU moving along the line-street. We set two different secrecy requirements for the VU's secrecy outage probability, namely, $\varepsilon = 0.01$ (i.e., a loose secrecy requirement) and $\varepsilon = 0.005$ (i.e., a more stringent secrecy requirement). The top subplot shows the VU's total power consumption (i.e., the sum of the VU's transmit-power to the RSU and that to the macro BS) when the VU is moving at different locations along the line-street. Correspondingly, the bottom subplot shows the VU's computation offloading scheduling, namely, the ratio between the VU's secure data offloaded through the RSUs and the VU's total offloading demand. The results in the top subplot show that when the VU is close to the RSUs, the VU's total power consumption decreases, which is due to the fact that more computation tasks are offloaded to the RSUs to process (as indicated in the bottom subplot). In particular, since the eavesdropping strengths gradually decrease from RSU 1 to RSU 3, the VU adaptively increases its computation task offloading rate from RSU 1 to RSU 3, which can save more total power consumption. In addition, the results in Fig. 5a also show that a less stringent secrecy requirement will motivate the VU to offload more computation tasks to the RSUs, which consequently yields lower total power consumption due to the close proximity between the VU and the RSUs.

Figure 5b further shows the performance of the optimal computation task offloading for a group of 10 VUs moving along the line-street,

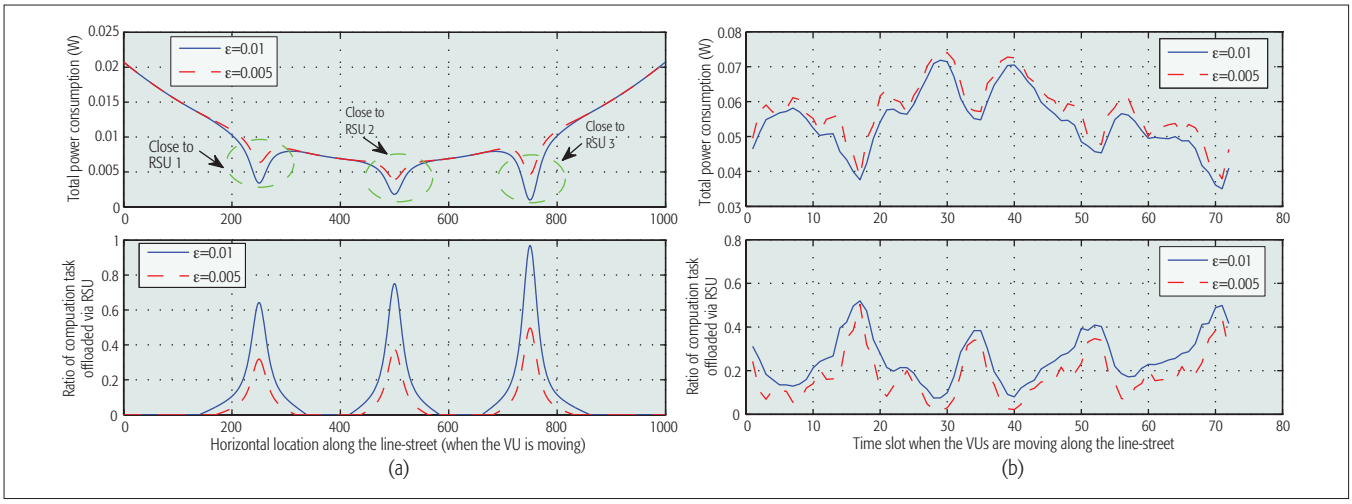

FIGURE 5. Illustration of the optimal computation -task offloading for the scenario of a line-street: a) the case of one VU moving along the line-street; b) case of 10 VUs moving along the line-street.

with the initial positions of the VUs randomly generated on the line-street. Since the VUs are located at different positions when moving, we use the time slot (each slot 1 s) as the x-axis. Correspondingly, we plot the total power consumption of all VUs in the top subplot, and plot the ratio of all VUs' computation tasks offloaded to the RSUs in the bottom subplot. The results again show that the VUs' total power consumption can be saved when more computation tasks are offloaded to the RSUs. In addition, a loose secrecy requirement motivates more computation tasks offloaded and thus yields a smaller total power consumption compared to a stringent secrecy requirement.

We next test the performance of the proposed computation task offloading when the VU moves along a circle-street. Specifically, the macro BS is located at (0,0) m, and we consider a circle-street with the radius of 300 m. Four RSUs are deployed at (−320,0) m, (0,320) m, (320,0) m, and (0, −320) m. Again, we consider that there are four eavesdroppers close to the respective RSUs. To differentiate these eavesdroppers, we consider that the four eavesdroppers have different strengths to overhear the respective RSUs, with Eavesdropper 1 (overhearing RSU 1) the strongest and Eavesdropper 4 (overhearing RSU 4) the weakest. Figure 6a shows the result when one VU is moving along the this circle-street, and Fig. 6b shows the result of a group of 10 VUs (we set that each RSU can serve no more than 3 VUs in this case). Again, we set that all VUs are moving at the speed at 50 km/h.

Figure 6a shows the performance of one VU moving along the circle-street. The top subplot shows the VU's total power consumption when the VU is moving at different locations along the circle-street (for the sake of clear presentation, we use the angle of the VU on the circle-street as the x-axis). Correspondingly, the bottom subplot shows the VU's computation offloading scheduling, namely, the ratio between the VU's secure data offloaded through the RSUs and the VU's total offloading demand. The results in the top subplot show that the VU's total power consumption decreases when the VU is close to the RSUs since more computation tasks are offloaded to the RSUs, as shown in the bottom subplot. In addition, since the eavesdropping strengths gradually decrease from RSU 1 to RSU 4, the VU adaptively increases its computation task offloading rate from RSU 1 to RSU 4, which facilitates the saving of more total power consumption.

Figure 6b shows the result of a group of 10 VUs moving along the circle-street, with the initial positions of the VUs randomly generated on the circle. Since the VUs are located at different positions on the circle-street when moving, we use the time slot (each slot 1 s) as the x-axis. Correspondingly, we plot the total power consumption of all VUs in the top subplot, and plot the ratio of all VUs' computation tasks offloaded to the RSUs in the bottom subplot. The results again show that the VUs' total power consumption can be effectively reduced when more computation tasks are offloaded to the RSUs. In addition, a loose secrecy requirement can yield a smaller total power consumption of all VUs since more computation tasks are offloaded via the RSUs.

Conclusion

In this article, targeted on the eavesdropping attack to VUs' computation offloading over RF channels, we investigate the resource management for computation task offloading with secrecy provisioning based on the measure of physical layer security. We discuss several costs for providing secrecy requirements and QoS requirements for computation offloading, and illustrate the associated trade-off among computation efficiency, resource efficiency, and secrecy efficiency. Furthermore, we discuss three promising technologies (i.e., NOMA-assisted computation offloading, multi-access-assisted computation offloading, and mobility- and-delay-aware offloading) to enhance the secrecy provisioning. As a detailed example of the multi-access-assisted computation offloading, we present a case study on the optimal dual-connectivity-enabled computation task offloading with secrecy provisioning and show its performance.

Since the vehicular network is highly dynamic, for our future work, we will investigate the distributed radio resource management for computation task offloading in VCEC with secrecy provisioning. In particular, game-theoretic-based analysis pro-

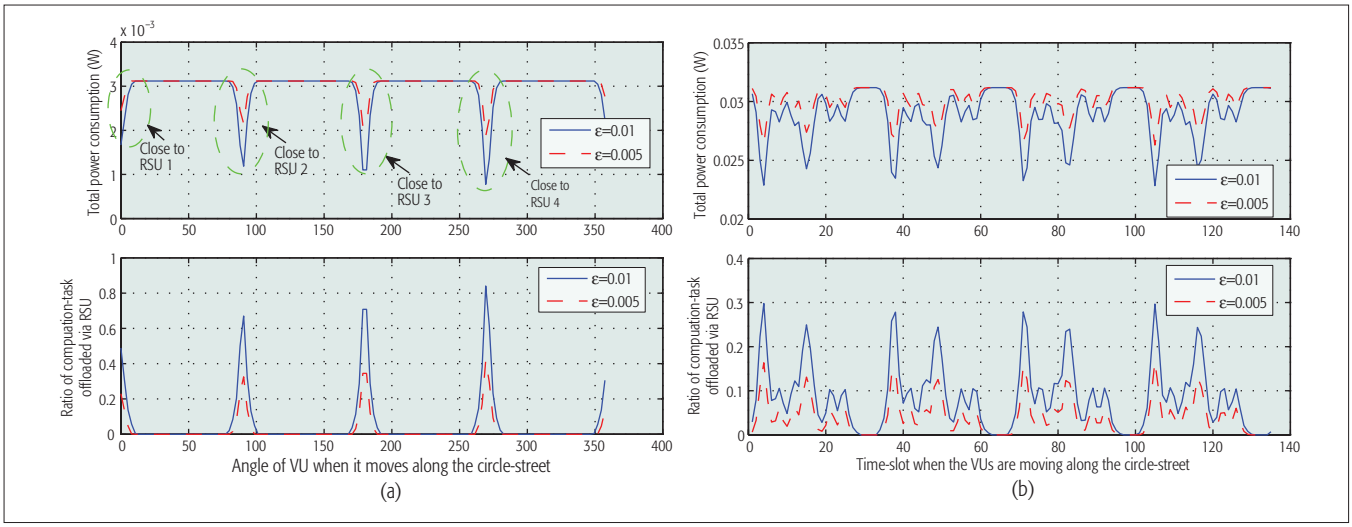

FIGURE 6. Illustration of the optimal computation-task offloading for the scenario of a circle-street: a) case of One VU Moving along the Circle-Street; b) case of Ten VUs Moving along the Circle-Street.

vides a promising tool to model the cooperative/non-cooperative computation offloading among a group of self-interested VUs.

References

[1] K. Abboud, H. A. Omar, and W. Zhuang, "Interworking of DSRC and Cellular Network Technologies for V2X Communications: A Survey," *IEEE Trans. Vehic. Tech.*, vol. 65, no. 12, Dec. 2016, pp. 9457–70.

[2] X. Chen *et al.*, "Efficient Multi-User Computation Offloading for Mobile-Edge Cloud Computing," *IEEE/ACM Trans. Net.*, vol. 24, no. 5, Oct. 2016, pp. 2795–808.

[3] K. Zheng *et al.*, "Mobile-Edge Computing for Vehicular Networks: A Promising Network Paradigm with Predictive Off-Loading," *IEEE Vehic. Tech. Mag.*, vol. 12, no. 2, Apr. 2017, pp. 36–44.

[4] M. Sookhak *et al.*, "Fog Vehicular Computing: Augmentation of Fog Computing Using Vehicular Cloud Computing," *IEEE Vehic. Tech. Mag.*, vol. 12, no. 3, Sept. 2017, pp. 55–64.

[5] H. Zhang *et al.*, "Coexistence of Wi-Fi and Heterogeneous Small Cell Networks Sharing Unlicensed Spectrum," *IEEE Commun. Mag.*, vol. 53 no. 3, Mar. 2015, pp. 158–64.

[6] C. Lai *et al.*, "Toward Secure Large-Scale Machine-to-Machine Communications in 3GPP Networks: Challenges and Solutions," *IEEE Commun. Mag.*, vol. 53, no. 12, Dec. 2015, pp. 12–19.

[7] H. Li *et al.*, "Privacy Leakage Via De-Anonymization and Aggregation in Heterogeneous Social Networks," *IEEE Trans. Dependable and Secure Computing*. DOI: 10.1109/TDSC.2017.2754249.

[8] H. Li *et al.*, "Privacy Leakage of Location Sharing in Mobile Social Networks: Attacks and Defense," *IEEE Trans. Dependable and Secure Computing*. DOI: 10.1109/TDSC.2016.2604383.

[9] N. Yang *et al.*, "Safeguarding 5G Wireless Communication Networks Using Physical Layer Security," *IEEE Commun. Mag.*, vol. 53, no. 4, Apr. 2015, pp. 20–27.

[10] A. Mukherjee *et al.*, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," *IEEE Commun. Surveys & Tutorials*, vol. 16, no. 3, 2014, pp. 1550–73.

[11] S. Chen *et al.*, "LTE-V: A TD-LTE-Based V2X Solution for Future Vehicular Network," *IEEE Internet of Things J.*, vol. 3, no. 6, Dec. 2016, pp. 997–1005.

[12] L. Dai *et al.*, "Non-Orthogonal Multiple Access for 5G: Solutions, Challenges, Opportunities, and Future Research Trends," *IEEE Commun. Mag.*, vol. 53, no. 9, Sept. 2015, pp. 74–81.

[13] L. Qian *et al.*, "Non-Orthogonal Multiple-Access Vehicular Small Cell Networks: Architecture and Solution," *IEEE Network*, vol. 31, no. 4, July/Aug. 2017, pp. 15–21.

[14] T. Taleb *et al.*, "On Multi-Access Edge Computing: A Survey of the Emerging 5G Network Edge Cloud Architecture and Orchestration," *IEEE Commun. Surveys & Tutorials*, vol. 19, no. 3, 2017, pp. 1657–81.

[15] C. Rosa *et al.*, "Dual Connectivity for LTE Small Cell Evolution: Functionality and Performance Aspects," *IEEE Commun. Mag.*, vol. 54, no. 6, June 2016, pp. 137–43.

Biographies

Yuan Wu (iewuy@zjut.edu.cn) received his Ph.D. degree in electronic and computer engineering from Hong Kong University of Science and Technology in 2010. He is currently an associate professor in the College of Information Engineering, Zhejiang University of Technology, China. His research interests focus on wireless communications and networking and smart grid. He was a recipient of the Best Paper Award at IEEE ICC 2016.

Li Ping Qian (lpqian@zjut.edu.cn) received her Ph.D. degree in information engineering from the Chinese University of Hong Kong in 2010. She is currently an associate professor with the College of Information Engineering, Zhejiang University of Technology. Her research interests lie in the areas of wireless communication and networking, cognitive networks, and smart grids, including power control and adaptive resource allocation.

Haowei Mao is currently pursuing his M.S. degree in the College of Information Engineering, Zhejiang University of Technology. His research interests focus on resource management for wireless communications and networks, mobile data offloading, and non-orthogonal multiple access.

Xiaowei Yang is currently pursuing her M.S. degree in the College of Information Engineering, Zhejiang University of Technology. Her research interests focus on resource management for wireless communications and networks, and green communications.

Haibo Zhou (haibozhou@nju.edu.cn) received his Ph.D. degree in information and communication engineering from Shanghai Jiao Tong University, China, in 2014. He is currently an associate professor with the School of Electronic Science and Engineering, Nanjing University, China. His research interests include resource management and protocol design in cognitive radio networks and vehicular networks.

Xiaoqi Tan (xtanaa@ust.hk) is now with the research group of Computing, Communications and Energy System Optimization (C2E) in the ECE Department at Hong Kong University of Science and Technology. From October 2015 to April 2016, he was a visiting research fellow in the School of Engineering and Applied Science, Harvard University. He primarily works on the mathematical aspects of energy systems and wireless networking, and is particularly interested in optimization, distributed and online algorithms, and performance evaluation.

Danny H. K. Tsang [F] (eetsang@ust.hk) received his Ph.D. degree in electrical engineering from the University of Pennsylvania in 1989. He joined Hong Kong University of Science and Technology in 1992 and is now a professor. He was a Guest Editor for the *IEEE Journal of Selected Areas in Communications*, an Associate Editor for the *Journal of Optical Networking*, and a Guest Editor for the *IEEE Systems Journal* and *IEEE Network*. His research interests include cloud computing, cognitive radio networks, and smart grids. He is currently a Technical Editor for *IEEE Communications Magazine*. He is a HKIE Fellow.