This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2016.2611979, IEEE Journal on Selected Areas in Communications

Secrecy-based Energy-Efficient Data Offloading via Dual-Connectivity over Unlicensed Spectrums

Yuan Wu *Senior Member IEEE*, Kuanyang Guo,
Jianwei Huang *Fellow IEEE*, Xuemin (Sherman) Shen *Fellow IEEE*

***Abstract*—Offloading cellular mobile users' (MUs') data traffic to small-cell networks is a cost-effective approach to relieve congestion in macrocell cellular networks. However, as many small-cell networks operate in the unlicensed bands, the data offloading might suffer from a security issue, i.e., some eavesdropper could overhear the offloaded data over unlicensed spectrums. This motivates us to investigate a secrecy-based energy-efficient uplink data offloading scheme. Specifically, we consider the recent paradigm of traffic offloading via dual-connectivity, which enables an MU to simultaneously deliver traffic to a macro base station (mBS) over the licensed channel and a small-cell access point (sAP) over the unlicensed channel. We formulate an MU's joint optimization of traffic scheduling and power allocation problem, with the objective of minimizing the total power consumption while meeting both the MU's traffic demand and secrecy-requirement. Despite the non-convex nature of the joint optimization problem, we propose an efficient algorithm to compute the optimal offloading solution. By evaluating the impact of the MU's secrecy-requirement and the eavesdropper's channel condition, we quantify the conditions under which the optimal offloading solution corresponds to the full-offloading and zero-offloading, respectively. Numerical results validate the optimal performance of our proposed algorithm, and show that the optimal offloading can significantly reduce the total power consumption compared to some fixed offloading schemes. Based on the optimal offloading solution for each MU, we further analyze the scenario of multiple MUs and sAPs, and investigate how to optimally exploit the sAPs' total offloading capacity to serve the MUs while accounting for the MUs' corresponding power consumptions for offloading data. To this end, we formulate a total network-benefit maximization problem that accounts for the reward for serving the MUs successfully, the mBS's bandwidth usage, and the MUs' power consumptions. Numerical results show that the optimal solution can improve the total network-benefit by more than 30%, compared to some heuristic sAP-selection scheme.**

I. Introduction

With a rapid growing popularity of smart wireless devices and mobile Internet services, cellular networks nowadays are facing an increasingly heavier pressure due to the explosive traffic growth. Offloading mobile users' (MUs') traffic from macrocell cellular networks to small-cell networks has been considered as a cost-effective approach for cellular operators to tackle such a pressure [1]. From the MUs' perspectives, offloading data helps them reduce power consumptions (because of the relatively short distance to small-cell access points (sAPs)) as well as mobile data cost (because of low access-fee charged by the sAPs). Most mobile devices nowadays have multiple radio-interfaces, including a long-range transceiver (such as 3G/4G radio-interface) and a short-range transceiver (such as WiFi radio-interface), which greatly facilitate dynamic traffic offloading.

Very recently, a new paradigm of *small-cell dual-connectivity*, which enables an MU to simultaneously communicate with a macro base station (mBS) and an sAP, is gaining momentums in both the 3GPP LTE-A standardizing activities [2] [3] and industrial practices [4]. With the dual-connectivity, an MU can flexibly schedule its traffic demand between the mBS and sAP to reduce its radio resource consumptions. For instance, an MU can send its delay-sensitive small-volume traffic to an mBS to satisfy the stringent QoS requirement, and offload its delay-tolerant large-volume traffic to a nearby sAP to reduce its transmit-power consumption and data cost. The key feature of dual-connectivity is that it simultaneously activates two radio-interfaces for traffic delivery, which requires a careful design of resource allocations [22]–[26].

Despite its advantages, traffic offloading to small-cell networks (via dual-connectivity) might suffer from a security issue. Specifically, small-cell networks (e.g., WiFi networks and LTE-U networks) usually operate on the unlicensed bands. Due to the open access of unlicensed spectrum, when an MU offloads traffic to an sAP, some eavesdropper (e.g., by pretending to be another sAP) can overhear the offloaded traffic for malicious purposes. Such a security threat is becoming increasingly significant, since there is a growing demand from operators to exploit unlicensed spectrums directly (such as in the context of LTE-U) [5]. Therefore, it is important to design an appropriate MU traffic offloading scheme that can fully exploit the benefits of traffic offloading while guaranteeing the MU's secrecy-requirement. To the best of our knowledge, there does not exist a comprehensive study on this issue yet.

In this paper, we propose a secrecy-based energy-efficient scheme for MUs' uplink data offloading via the dual-connectivity over unlicensed spectrum. We focus on the uplink scenario due to the following reasons. (i) For the uplink case, the network performance is often limited by the heterogeneous

This work is supported in part by the National Natural Science Foundation of China (61572440 and 61303235), and the General Research Funds (Project Numbers CUHK 412713 and 14202814) established under the University Grant Committee of the Hong Kong Special Administrative Region, China, and the Natural Sciences and Engineering Research Council (NSERC), Canada.

Y. Wu and K. Guo are with College of Information Engineering, Zhejiang University of Technology, Hangzhou, China, (email: iewuy@zjut.edu.cn).

J. Huang is with the Network Communications and Economics Lab, Department of Information Engineering, The Chinese University of Hong Kong, Hong Kong (e-mail: jwhuang@ie.cuhk.edu.hk).

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

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2016.2611979, IEEE Journal on Selected Areas in Communications

local resource constraints of different MUs (such as the battery energy levels). This often leads to a more complicated optimization problem comparing with the study of the downlink case, in which case the resource constraints are related to a centralized base station. (ii) The rapid growth of user-generated contents (such as user-generated videos on social networks) leads to a significant increase in the MUs' uplink traffic, which makes the study of data offloading in uplink transmission more important (see [10], [23], [27], [28]).

Our main contributions are summarized as follows.

- *Novel Modeling and Problem Formulation Accounting for the MU's Secrecy-Requirement*: We propose a modeling that accounts for the MU's secrecy-requirement when offloading data via dual-connectivity over unlicensed spectrum. Building upon the concept of physical-layer security throughput [29]–[31], we derive the secrecy-outage probability (as a function of the MU's offloaded data rate and transmit-power to sAP) for traffic offloading. We then propose a novel problem formulation that aims at minimizing the MU's total power consumption while guaranteeing both the MU's traffic demand and secrecy-outage requirement. The problem formulation reflects the important tradeoff between the benefit of traffic offloading via dual-connectivity and the additional cost of providing the secrecy-outage guarantee.
- *Efficient Algorithm for Solving the Non-convex Optimization Problem* : The optimization problem involves a joint optimization of the MU's traffic scheduling and transmit-powers to the sAP and mBS, and is a nonconvex optimization problem which is difficult to solve. To tackle this technical difficulty, we exploit the hidden convexity of the problem by performing a series of equivalent transformations, and then propose an efficient algorithm to compute the optimal offloading solution. By evaluating the impact of the MU's secrecy-requirement and the eavesdropper's channel condition on the optimal offloading solution, we further derive the sufficient conditions such that the optimal offloading solution leads to the full-offloading (i.e., the MU's traffic demand is completely offloaded to the sAP) and the zero-offloading (i.e., no data is offloaded to the sAP). Numerical results validate the performance of our proposed algorithm and show that the optimal offloading can significantly reduce the MU's total power consumption in comparison with some fixed offloading schemes (e.g., up to 90% of power consumption saving).
- *Extension to the Scenario of Multiple MUs and sAPs*: Based on the optimal offloading solution for each MU, we further consider the scenario of multiple MUs and sAPs, and investigate how to optimally exploit the sAPs' offloading capacity to serve the MUs while accounting for the MUs' power consumptions for offloading traffic. To this end, we formulate a total network-benefit maximization problem, which takes into account the reward for serving the MUs successfully, the MUs' power consumptions, and the mBS's bandwidth usage. Numerical results show that the optimal solution improves the total network-benefit by more than 30% compared to some heuristic sAP-selection offloading scheme, thus validating the importance of optimally offloading the MUs' data to the properly selected sAPs.

A. Related Literature Review

We first provide a literature review about the resource allocations for traffic offloading via dual-connectivity, which is closest to our study in this paper. We then provide a broad review of related literature about data offloading (but without invoking dual-connectivity). Finally, we provide a brief review on the studies of physical-layer security.

1) Related literature on dual-connectivity: Jha *et al.* in [22] provided a brief survey on the technical challenges regarding dual-connectivity, and demonstrated the potential enhancement of users' throughput. Liu *et al.* in [23] proposed a power control scheme to split the MU's transmit-power capacity into two radio-interfaces for dual-connectivity. Mukherjee in [24] took into account the impact of the backhaul delay and proposed a scheduling scheme for the MU's downlink traffic delivery via dual-connectivity. Furthermore, Mukherjee in [25] investigated the pairing between macro-cell eNodeBs and small-cell eNodeBs for providing dual-connectivity to the MUs. In [26], we proposed an efficient scheme to minimize the total mobile data cost of the MUs which offload data to a same sAP via dual-connectivity. However, the security issue has not been considered in these studies.

2) Related literature on data offloading: There have been many studies focusing on traffic offloading for different network scenarios (but without considering dual-connectivity), which can be categorized into two streams as follows. The first stream of studies focused on designing the traffic offloading schemes from the MUs' perspectives. For instance, different admission schemes have been proposed in [6] and [7] for MUs to offload data to small-cell networks. The authors of [8] and [9] proposed different schemes for the MUs' traffic scheduling to heterogeneous small networks. Yu *et al.* in [10] proposed a joint uplink bandwidth and power allocations scheme for multi-RAT heterogeneous network. In [11] and [12], different schemes have been proposed for the MUs' adaptive traffic offloading by exploiting some information (such as delay and congestion). The authors of [13] and [14] investigated the benefits of offloading the MUs' traffic to WiFi networks. The incentive mechanisms for motivating the MUs' data offloading have been investigated in [15] [16]. Data offloading via mobile users' device-to-device cooperation has been studied in [17], [18]. The second stream of studies focused on traffic offloading from the network operator's perspective [19]–[21]. Ho *et al.* in [19] considered the load-coupling effect among different cells, and investigated the corresponding traffic allocation scheme between cellular and small-cell networks for maximizing a social utility. Chen *et al.* in [20] considered the time-varying traffic in cellular networks, and proposed an MDP model to compute the optimal strategy for offloading traffic from mBSs to small-cell networks. Rao *et al.* in [21] also proposed a stochastic geometric model for analyzing the tradeoff between energy-efficiency and spectrum efficiency when offloading traffic from mBSs to small cells.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2016.2611979, IEEE Journal on Selected Areas in Communications

3) Related literature on physical layer security: The growing need for securing wireless services leads to the growing interests of understanding the physical-layer security capacity (e.g., [29]–[32]). Different from the existing protocol-oriented security-enhancing schemes (e.g., the secure socket layer (SSL) in the transport layer), the physical-layer security capacity provides a fundamental measure about how secure a wireless link transmission is from the perspective of information-theoretic analysis. In other words, the physical-layer security capacity quantifies the maximum throughput which is impossible for an eavesdropper to overhear from the received signal, no matter whether any other specific security-enhancing protocol is used or not. Furthermore, the secrecy-outage probability was developed in [33] as an effective approach to evaluate the physical-layer security capacity under uncertain system information (such as the eavesdropper's unknown locations and stochastic channels). Recent studies [34]–[37] used the measure of secrecy-outage probability to study the security issue in device-to-device communications, multi-users cellular networks, and multi-cell MIMO systems. To the best of our knowledge, the security issue in traffic offloading has not been investigated from the perspective of physical layer security.

II. System Model and Problem Formulation

We first consider an illustrative network model as shown in Figure 1, where MU i delivers its uplink traffic to an mBS via cellular radio-interface. By exploiting dual-connectivity, MU i also offloads part of its traffic to an sAP via another short-range radio-interface. In the rest of this paper, we use x_{iB} and p_{iB} to denote MU i's traffic rate and the transmit-power to the mBS, respectively (here the letter "B" represents "base station"). Meanwhile, we use x_{iA} and p_{iA} to denote MU i's offloaded traffic rate and the transmit-power to the sAP, respectively (here the letter "A" represents "access point").

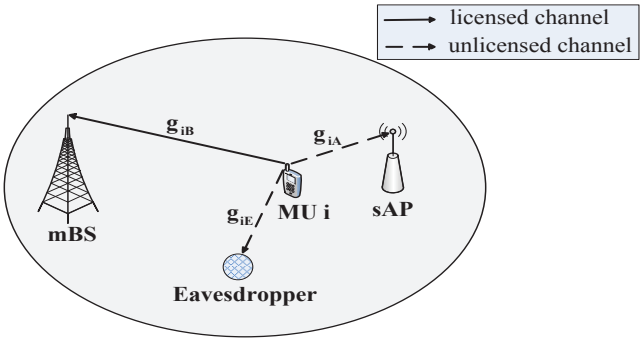


Fig. 1: System model. MU i sends the uplink data to the mBS and sAP with dual-connectivity. Due to the open access of unlicensed spectrum, an eavesdropper overhears MU i's offloaded traffic to sAP.

We assume that the mBS and sAP use different channels. Specifically, the mBS allocates a licensed channel (with a bandwidth of W_B) to accommodate MU i's uplink traffic. The sAP, in the context of LTE-U [5], uses an unlicensed channel (with a bandwidth of W_A) to accommodate MU i's offloaded uplink traffic. Due to the open access of unlicensed channel, MU i's communications over the unlicensed channel suffer from a security issue. Figure 1 illustrates an example, where an eavesdropper intentionally overhears MU i's offloaded data to the sAP for a malicious purpose.

Since the mBS uses a licensed spectrum channel for accommodating MU i's uplink traffic, we consider the transmission between MU i and the mBS to be perfectly secure[1]. Specifically, the data rate x_{iB} from MU i to the mBS, according to the Shannon-capacity formula, is given by

$$x_{iB} = W_B \log_2 \left(1 + \frac{p_{iB} g_{iB}}{n_B}\right), \tag{1}$$

where g_{iB} is the channel power gain from MU i to the mBS, and n_B is the background noise power at the mBS.

The sAP uses an unlicensed spectrum channel to accommodate MU i's offloaded traffic, which means that the eavesdropper can overhear MU i's offloaded traffic. Hence, according to [29]–[31], the achievable secrecy-rate r_{iA}^{sec} from MU i to the sAP is given by

$$r_{iA}^{\text{sec}} = \max\left\{W_A \log_2 \left(1 + \frac{p_{iA} g_{iA}}{n_A}\right) - W_A \log_2 \left(1 + \frac{p_{iA} g_{iE}}{n_E}\right), 0\right\}, \tag{2}$$

where g_{iA} denotes the channel power gain from MU i to the sAP, and g_{iE} denotes the channel power gain from MU i to the eavesdropper. Here, n_A denotes the background noise power at the sAP, and n_E denotes the background noise power at the eavesdropper. Notice that n_A and n_E can be different with each other, and with a slight modification, n_A and n_E can also account for the interference power at the sAP and the eavesdropper, respectively. As shown in (2), to ensure the secrecy of its offloaded data, MU i needs to transmit with a larger transmit-power p_{iA} than the case without considering the eavesdropper, which decreases the benefit of traffic offloading. Such a consideration will be reflected in our following problem formulation (i.e., constraint (7)).

Thanks to the advances in wireless transceiver designs, MU i can usually obtain accurate information about the channel power gains g_{iA} to the sAP and g_{iB} to the mBS through proper feedback, when the channel conditions change relatively slowly. This is in fact our target application scenario, as it will be difficult to perform effective traffic offloading for fast moving MU due to the limited coverage of small cells. However, accurate information about the eavesdropper's channel power gain is usually difficult to obtain, since the eavesdropper might intentionally conceal such information. Hence, we adopt a similar assumption as in [33]–[35], namely, only the statistics information about the eavesdropper's channel is available; more specifically, the channel power gain g_{iE} follows an exponential distribution with a mean α_i. Due to the randomness of g_{iE}, MU i's secrecy-outage probability, as

[1]The mBS usually controls a set of licensed channels, one of which is assigned to an MU i based on some resource allocation mechanism. Hence, the eavesdropper may not be able to know the specific licensed channel currently assigned to MU i. Furthermore, according to the LTE-A standards, an mBS will use encryption schemes to protect the MUs' data [38]. Therefore, it is reasonable to assume that the MU's data to the mBS is secure. In comparison, small-cell networks (in particular, WiFi networks) usually provide a considerably weaker security guarantee than mBSs [39], which results in that they are very vulnerable to security attack.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2016.2611979, IEEE Journal on Selected Areas in Communications

a function of its offloaded data rate x_{iA} and transmit-power p_{iA} to the sAP, is given by:

$$P_{\text{out}}\left(p_{iA}, x_{iA}\right) = 1 - \mathbf{Pr}\Bigg\{ r_{iA}^{\text{sec}} \geq x_{iA} | \\ W_A \log_2\left(1 + \frac{p_{iA} g_{iA}}{n_A}\right) - W_A \log_2\left(1 + \frac{p_{iA} g_{iE}}{n_E}\right) \geq 0 \Bigg\}. \quad (3)$$

The conditional probability takes into account the fact that MU i chooses to offload its traffic to sAP only when it expects to achieve a nonnegative secrecy-rate to the sAP.

Using (2), we can further express $P_{\text{out}}\left(p_{iA}, x_{iA}\right)$ in (3) as

$$P_{\text{out}}\left(p_{iA}, x_{iA}\right) = 1 - \mathbf{Pr}\Bigg\{ \\ g_{iE} \leq 2^{-\frac{x_{iA}}{W_A}} \frac{n_E}{n_A} g_{iA} - \left(1 - 2^{-\frac{x_{iA}}{W_A}}\right) \frac{n_E}{p_{iA}} | g_{iE} \leq \frac{n_E}{n_A} g_{iA} \Bigg\}. \quad (4)$$

In the rest of this paper, we define $\hat{g}_{iA}$ as MU i's effective channel power gain to the sAP as follows:

$$\hat{g}_{iA} = \frac{n_E}{n_A} g_{iA}. \quad (5)$$

Notice that $g_{iE} \leq 2^{-\frac{x_{iA}}{W_A}} \hat{g}_{iA} - \left(1 - 2^{-\frac{x_{iA}}{W_A}}\right) \frac{n_E}{p_{iA}}$ is a sufficient condition to guarantee $g_{iE} \leq \hat{g}_{iA}$, assuming that $x_{iA} \geq 0$. Therefore, after some manipulations, we can further derive MU i's secrecy-outage probability $P_{\text{out}}\left(p_{iA}, x_{iA}\right)$ as follows:

$$P_{\text{out}}\left(p_{iA}, x_{iA}\right) = \\ \frac{1}{1 - e^{-\frac{\hat{g}_{iA}}{\alpha_i}}} \left(e^{-\frac{2^{-\frac{x_{iA}}{W_A}} \hat{g}_{iA} - \left(1 - 2^{-\frac{x_{iA}}{W_A}}\right) \frac{n_E}{p_{iA}}}{\alpha_i}} - e^{-\frac{\hat{g}_{iA}}{\alpha_i}} \right). \quad (6)$$

The secrecy-outage probability can be interpreted as follows: given the MU's offloading-rate and transmit-power to the sAP, how likely the MU fails to protect its offloaded traffic from being overheard by the eavesdropper. Hence, the smaller the secrecy-outage probability, the better the secrecy-level achieved. In this sense, the secrecy-outage probability provides a meaningful measure of the secrecy-level when the MU offloads traffic. Notice that (6) leads to $P_{\text{out}}\left(p_{iA}, 0\right) = 0$, i.e., the secrecy outage probability is zero when MU i does not offload any traffic to sAP, which is consistent with the intuition. In particular, we consider that MU i, when offloading traffic, requires its secrecy-outage to be no larger than a given limit $\epsilon_i \in (0, 1]$, i.e., $P_{\text{out}}\left(p_{iA}, x_{iA}\right) \leq \epsilon_i$.

Based on the above modelings of the MU's data offloading and the derived MU's secrecy-outage probability, we formulate the following optimization problem to minimize the MU's total power consumption:

$$\begin{aligned}
&\underline{\text{(P1)}}\text{: } \min \quad p_{iA} + p_{iB} \\
&\text{Subject to:} \quad P_{\text{out}}\left(p_{iA}, x_{iA}\right) \leq \epsilon_i, && (7) \\
&\qquad x_{iB} + (1 - \epsilon_i) x_{iA} = R_i^{\text{req}}, && (8) \\
&\qquad 0 \leq p_{iA} \leq p_{iA}^{\max}, && (9) \\
&\qquad 0 \leq p_{iB} \leq p_{iB}^{\max}, && (10) \\
&\qquad x_{iA} \geq 0, x_{iB} \geq 0, \text{ and constraint } (1), \\
&\text{Variables:} \quad (x_{iA}, p_{iA}) \text{ and } (x_{iB}, p_{iB}).
\end{aligned}$$

In Problem (P1), we jointly optimize: i) MU i's data rate x_{iB} and the transmit-power p_{iB} to the mBS, and ii) MU i's offloaded data rate x_{iA} and the transmit-power p_{iA} to the sAP. The objective is to minimize MU i's total transmit-power consumption. Constraint (7) ensures that MU i, when offloading data to the sAP, experiences a secrecy-outage probability no larger than ϵ_i. As reflected in (2), such a secrecy-protection makes the MU use a larger transmit-power than that without any secrecy-protection. Constraint (8) represents that MU i receives a total data rate (which the eavesdropper cannot overhear) equal to its traffic requirement R_i^{req}. Notice that due to the secrecy-outage, only the effective (i.e., secrecy) offloading rate $x_{iA}(1 - \epsilon_i)$ is achieved under the MU i's offloading rate x_{iA}. Constraints (9) and (10) ensure that MU i's transmit-power p_{iA} to the sAP and p_{iB} to the mBS cannot exceed their respective upper bounds $p_{iA}^{\max}$ and $p_{iB}^{\max}$.

Problem (P1) captures two costs due to taking into account the secrecy issue when the MU offloads traffic to the sAP, namely, i) a larger transmit-power to the sAP to achieve a guaranteed secrecy-outage, and ii) a reduced effective offloading-rate due to nonzero secrecy-outage. These two downsides lead to an important implication: if the MU blindly offloads its traffic to the sAP without proper optimization, it might end up consuming a significant amount of transmit-power which impairs the benefit of traffic offloading. Thus, Problem (P1) aims at tackling with this issue. Specifically, by using the optimal offloading solution of Problem (P1), the MU can minimize the total transmit-power consumption while meeting both its required secrecy-level and traffic demand.

However, Problem (P1) is difficult to solve, due to i) the nonconvexity in constraint (7) which couples x_{iA} and p_{iA}, and ii) the hidden complicated coupling between p_{iA} and p_{iB} due to (1) and (8). We focus on solving Problem (P1) optimally and deriving the MU's optimal offloading solution in the next two sections, through a series of proper transformations. Before leaving this section, we make the following remark.

Remark 1: **(Another choice of constraint (8))**: In Problem (P1), we can also use the following constraint (11) to replace constraint (8), i.e.,

$$x_{iB} + x_{iA}\big(1 - P_{\text{out}}\left(p_{iA}, x_{iA}\right)\big) = R_i^{\text{req}}, \quad (11)$$

to guarantee MU i's secrecy traffic requirement. However, since $P_{\text{out}}\left(p_{iA}, x_{iA}\right)$ in (6) is already a complicated function of x_{iA}, using (11) will make Problem (P1) intractable. Hence, to simplify our following analysis and design an efficient algorithm to optimally solve Problem (P1), we choose to use (8) to ensure the MU's traffic requirement. Notice that i) because of (7), constraint (8) is a sufficient condition to guarantee that $x_{iB} + x_{iA}\big(1 - P_{\text{out}}\left(p_{iA}, x_{iA}\right)\big) \geq R_i^{\text{req}}$, and ii) the MU's secrecy-outage limit ϵ_i is usually very small. ■

III. Equivalent Transformations of Problem (P1) as a Power Allocation Problem

The key idea of solving Problem (P1) is to transform it into an equivalent single-variable optimization problem that is tractable to solve. The details are as follows.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2016.2611979, IEEE Journal on Selected Areas in Communications

By putting (6) into (7) and performing some transformations, we obtain the following constraint for (7):

$$2^{-\frac{x_{iA}}{W_A}}\hat{g}_{iA} - \left(1 - 2^{-\frac{x_{iA}}{W_A}}\right)\frac{n_E}{p_{iA}} \geq \theta_{iA}, \quad (12)$$

where the new parameter θ_{iA} is defined as follows:

$$\theta_{iA} = -\alpha_i \ln\left(1 - (1 - e^{-\frac{\hat{g}_{iA}}{\alpha_i}})(1 - \epsilon_i)\right). \quad (13)$$

Parameter θ_{iA}, which quantifies the impact of security-requirement, depends on the MU's effective channel power gain $\hat{g}_{iA}$ in (5), the eavesdropper's average channel strength α_i, and MU i's secrecy-outage limit ϵ_i. Since θ_{iA} plays a key role in the following analysis, we provide three important properties for it as follows.

Lemma *1:* **(Important Properties of Parameter θ_{iA})** The following three properties always hold: (i) θ_{iA} is decreasing in ϵ_i; (ii) θ_{iA} is increasing in α_i; (iii) $\theta_{iA} \leq \hat{g}_{iA}$ always holds.

Proof: Please refer to Appendix I for the details. ■

Lemma 1 matches with the intuition. Since θ_{iA} captures the strength of security requirement, it is reasonable that: i) θ_{iA} decreases with a larger ϵ_i (i.e., a less stringent limit on the secrecy-outage), and ii) θ_{iA} increases with a larger α_i (i.e., a stronger capability of eavesdropper to overhear data).

A further transformation on (12) gives us the following constraint, which is essentially equivalent to (7):

$$x_{iA} \leq W_A \log_2\left(\frac{p_{iA}\hat{g}_{iA} + n_E}{p_{iA}\theta_{iA} + n_E}\right). \quad (14)$$

Notice that constraint (14) is reasonable: to meet the required secrecy-outage limit ϵ_i, MU i's offloading-rate x_{iA} to the sAP should be subject to an upper bound (i.e., the right hand side of (14)), which is decreasing in θ_{iA} (recall that θ_{iA} represents the strength of security-requirement as we described before).

Moreover, to make a further transformation on Problem (P1), we identify the following result.

Lemma *2:* **(Condition on the Optimal Offloading-Rate)** At the optimal solution of Problem (P1), constraint (14) is strictly binding, i.e., MU i's offloading rate should satisfy

$$x_{iA} = W_A \log_2\left(\frac{p_{iA}\hat{g}_{iA} + n_E}{p_{iA}\theta_{iA} + n_E}\right). \quad (15)$$

Proof: The key of the proof is to show that the right hand side of (15) is increasing in p_{iA}, based on the property that $\theta_{iA} \leq \hat{g}_{iA}$ always holds (i.e., Property (iii) in Lemma 1). Please refer to Appendix II for the details. ■

Using Lemma 2 and (8), we can derive the following result:

$$x_{iB} = R_i^{\text{req}} - (1 - \epsilon_i)W_A \log_2\left(\frac{p_{iA}\hat{g}_{iA} + n_E}{p_{iA}\theta_{iA} + n_E}\right). \quad (16)$$

Then, by substituting (1) into (16), we can further obtain

$$p_{iB} = \frac{n_B}{g_{iB}}\left(2^{\frac{R_i^{\text{req}}}{W_B}}\left(\frac{p_{iA}\hat{g}_{iA} + n_E}{p_{iA}\theta_{iA} + n_E}\right)^{-\frac{(1-\epsilon_i)W_A}{W_B}} - 1\right). \quad (17)$$

Substituting (15) and (17) into Problem (P1), we can obtain the following optimization Problem (P2):

$$\underline{\text{(P2)}}: \min\ p_{iA} + \frac{n_B}{g_{iB}}\left(2^{\frac{R_i^{\text{req}}}{W_B}}\left(\frac{p_{iA}\hat{g}_{iA} + n_E}{p_{iA}\theta_{iA} + n_E}\right)^{-\frac{(1-\epsilon_i)W_A}{W_B}} - 1\right)$$

Subject to:

$$\frac{n_B}{g_{iB}}\left(2^{\frac{R_i^{\text{req}}}{W_B}}\left(\frac{p_{iA}\hat{g}_{iA} + n_E}{p_{iA}\theta_{iA} + n_E}\right)^{-\frac{(1-\epsilon_i)W_A}{W_B}} - 1\right) \leq p_{iB}^{\max}, \quad (18)$$

$$(1 - \epsilon_i)W_A \log_2\left(\frac{p_{iA}\hat{g}_{iA} + n_E}{p_{iA}\theta_{iA} + n_E}\right) \leq R_i^{\text{req}}, \quad (19)$$

and constraint (9),

Variable: p_{iA}.

Because of the above series of equivalent transformations, Problem (P2), which only involves p_{iA} as the decision variable, is equivalent to Problem (P1). Constraint $x_{iA} \geq 0$ in the original Problem (P1) is always satisfied because of $p_{iA} \geq 0$ in (9) and Lemma 2 (together with Property (iii) in Lemma 1), and constraint $x_{iB} \geq 0$ in Problem (P1) is also always satisfied because of (16) and constraint (19).

In particular, constraint (18) in Problem (P2) indicates that the MU needs to at least offload part of its traffic demand to the sAP, if MU i's $p_{iB}^{\max}$ is not large enough. This consequently leads to a lower-bound for MU i's transmit-power p_{iA} to the sAP. Meanwhile, constraint (19) indicates that the MU's secrecy throughput when offloading traffic to the sAP cannot exceed R_i^{req} (such that $x_{iB} \geq 0$). This consequently leads to a possible upper-bound for p_{iA}. The details about the lower-bound and upper-bound will be given in the next section, in which we solve Problem (P2). Before that, we use Table I to list the important notations used in this paper.

IV. Optimal Solution of Problem (P2-E) and Optimal Offloading Solution

A. Equivalent Form of Problem (P2)

We focus on solving Problem (P2) optimally in this section. To this end, we make some further equivalent transformations on (18) and obtain the following constraint:

$$p_{iA}\left(\theta_{iA} - 2^{-\frac{R_i^{\text{req}}}{(1-\epsilon_i)W_A}}\left(\frac{p_{iB}^{\max} g_{iB}}{n_B} + 1\right)^{\frac{W_B}{(1-\epsilon_i)W_A}}\hat{g}_{iA}\right) \leq n_E\left(2^{-\frac{R_i^{\text{req}}}{(1-\epsilon_i)W_A}}\left(\frac{p_{iB}^{\max} g_{iB}}{n_B} + 1\right)^{\frac{W_B}{(1-\epsilon_i)W_A}} - 1\right). \quad (20)$$

Moreover, by making some further equivalent transformations on (19), we can obtain the following constraint:

$$p_{iA}\left(\theta_{iA} - 2^{-\frac{R_i^{\text{req}}}{(1-\epsilon_i)W_A}}\hat{g}_{iA}\right) \geq n_E(2^{-\frac{R_i^{\text{req}}}{(1-\epsilon_i)W_A}} - 1). \quad (21)$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2016.2611979, IEEE Journal on Selected Areas in Communications

TABLE I: Important Notations

W_B	mBS's channel bandwidth	g_{iA}	channel power gain from MU i to the sAP
W_A	sAP's channel bandwidth	$\hat{g}_{iA}$	$n_E g_{iA}/n_A$ defined in (5)
p_{iB}	MU i's transmit-power to mBS	g_{iE}	channel power gain from MU i to the Eavesdropper
$p_{iB}^{\max}$	upper-bound of MU i's transmit-power to mBS	α_i	average of g_{iE}
p_{iA}	MU i's transmit-power to sAP	x_{iB}	MU i' data rate to mBS
$p_{iA}^{\max}$	upper-bound of MU i's transmit-power to sAP	r_{iA}^{sec}	MU i's achievable secrecy throughput to sAP
n_B	background noise power at mBS	x_{iA}	MU i's offloading-rate to sAP
n_A	background noise power at sAP	R_i^{req}	MU i's total data requirement
n_E	background noise power at eavesdropper	ϵ_i	MU i's secrecy-outage limit
g_{iB}	channel power gain from MU i to mBS	θ_{iA}	$-\alpha_i \ln\left(1-(1-e^{-\frac{g_{iA}}{\alpha_i}})(1-\epsilon_i)\right)$ defined in (13)

By using constraints (20) and (21), we can re-express Problem (P2) as follows

(P2-E):

$$\min\ p_{iA} + \frac{n_B}{g_{iB}}\left(2^{\frac{R_i^{\text{req}}}{W_B}}\left(\frac{p_{iA}\hat{g}_{iA}+n_E}{p_{iA}\theta_{iA}+n_E}\right)^{-\frac{(1-\epsilon_i)W_A}{W_B}} - 1\right)$$

Subject to: constraints $(9), (20),$ and (21),

Variable: p_{iA}.

Compared to Problem (P2), a keen observation of Problem (P2-E) is that constraints (20) and (21) are both linear in p_{iA}. Therefore, we have the following favorable property: given the parameter setting, constraints (9), (20), and (21) together yield a unique feasible interval for p_{iA} in form of $p_{iA} \in [p_{iA}^{\text{low}}, p_{iA}^{\text{upp}}]$. Such a clear feasible interval facilitates us to solve Problem (P2-E) in the next two subsections. Specifically, we first solve Problem (P2-E) in Subsection IV-B by supposing that the interval $[p_{iA}^{\text{low}}, p_{iA}^{\text{upp}}]$ is known. We then analytically derive p_{iA}^{low} and p_{iA}^{upp} in Subsection IV-C. With the derived p_{iA}^{low} and p_{iA}^{upp}, we can also determine the feasibility of Problem (P2-E) (as well as Problem (P1)) (the details are given in Proposition 4).

B. Convexity of Problem (P2-E) and the Optimal Solution

We first focus on solving Problem (P2-E), supposing that the feasible interval $p_{iA} \in [p_{iA}^{\text{low}}, p_{iA}^{\text{upp}}]$ is known. We first give the following important property regarding Problem (P2-E).

Proposition 1: (Convexity of Problem (P2-E)) Problem (P2-E) is a strictly convex optimization problem.

Proof: We use $\varphi(p_{iA})$ to denote the first order derivative of the objective function of Problem (P2-E). Specifically, after some manipulations, $\varphi(p_{iA})$ can be given by:

$$\varphi(p_{iA}) = 1 - (\hat{g}_{iA}-\theta_{iA})\frac{n_E n_B(1-\epsilon_i)W_A}{g_{iB}W_B}2^{\frac{R_i^{\text{req}}}{W_B}} \cdot \frac{1}{(p_{iA}\theta_{iA}+n_E)^2}\left(\frac{p_{iA}\theta_{iA}+n_E}{p_{iA}\hat{g}_{iA}+n_E}\right)^{\frac{(1-\epsilon_i)W_A}{W_B}+1}. \quad (22)$$

Since $\hat{g}_{iA} \geq \theta_{iA}$, then $\frac{1}{(p_{iA}\theta_{iA}+n_E)^2}\left(\frac{p_{iA}\theta_{iA}+n_E}{p_{iA}\hat{g}_{iA}+n_E}\right)^{\frac{(1-\epsilon_i)W_A}{W_B}+1}$ decreases in p_{iA}. Hence, $\varphi(p_{iA})$ decreases in p_{iA}, i.e., the objective function of Problem (P2-E) is strictly convex in p_{iA} [42]. In addition, all constraints in Problem (P2-E) are linear. Hence, Problem (P2-E) is a convex optimization problem. ■

The convexity of Problem (P2-E) enables us to use the sufficient condition $\varphi(p_{iA}) = 0$ to derive the optimal solution for Problem (P2-E), where the decision variable p_{iA} falls within a feasible interval $[p_{iA}^{\text{low}}, p_{iA}^{\text{upp}}]$ (as described at the end of Subsection IV-A, p_{iA}^{low} and p_{iA}^{upp} are uniquely specified by constraints (9), (20), and (21) together). On the other hand, if there does not exist any $p_{iA} \in [p_{iA}^{\text{low}}, p_{iA}^{\text{upp}}]$ such that $\varphi(p_{iA}) = 0$, then the optimal solution of Problem (P2-E) is one of the two boundary points, i.e., either p_{iA}^{low} or p_{iA}^{upp}.

We use p_{iA}^* to denote the optimal solution of Problem (P2-E). To derive p_{iA}^*, we propose the following Algorithm (SolP2E). In Algorithm (SolP2E), *first*, we exploit the property that $\varphi(p_{iA})$ is increasing in p_{iA} (according to the proof of Proposition 1) and make the following two checks. Check (i) if $\varphi\left(p_{iA}^{\text{low}}\right) \geq 0$, which indicates that the objective function is always increasing for $p_{iA} \in [p_{iA}^{\text{low}}, p_{iA}^{\text{upp}}]$, then we directly set $p_{iA}^* = p_{iA}^{\text{low}}$ (i.e., Step 3), and check (ii) if $\varphi\left(p_{iA}^{\text{upp}}\right) \leq 0$, which indicates that the objective function is always decreasing for $p_{iA} \in [p_{iA}^{\text{low}}, p_{iA}^{\text{upp}}]$, then we directly set $p_{iA}^* = p_{iA}^{\text{upp}}$ (i.e., Step 5). *Second*, if neither of the above two checks holds (i.e., there exists a unique $p_{iA}^* \in [p_{iA}^{\text{low}}, p_{iA}^{\text{upp}}]$ such that $\varphi(p_{iA}^*) = 0$), we then again exploit the property that $\varphi(p_{iA})$ is increasing, and use the approach of *bisection search* to find p_{iA}^* (i.e., the While-Loop from Step 8 to Step 19). The convergence of Algorithm (SolP2E) is given by the following Proposition 2.

Algorithm (SolP2E): to solve Problem (P2-E) under given p_{iA}^{low} and p_{iA}^{upp}

1: **Initialization:** Set a tolerance for computational error γ. Set $flag = 1$.
2: **if** $\varphi\left(p_{iA}^{\text{low}}\right) \geq 0$ **then**
3: Set $p_{iA}^* = p_{iA}^{\text{low}}$.
4: **else if** $\varphi\left(p_{iA}^{\text{upp}}\right) \leq 0$ **then**
5: Set $p_{iA}^* = p_{iA}^{\text{upp}}$.
6: **else**
7: $\underline{p_{iA}} = p_{iA}^{\text{low}}$, $\overline{p_{iA}} = p_{iA}^{\text{upp}}$.
8: **while** $flag = 1$ **do**
9: $p_{iA}^{\text{cur}} = \frac{\overline{p_{iA}}+\underline{p_{iA}}}{2}$.
10: **if** $\left(\overline{p_{iA}} - \underline{p_{iA}}\right) \leq \gamma$ **then**
11: $p_{iA}^* = p_{iA}^{\text{cur}}$, and set $flag = 0$.
12: **else**
13: **if** $\varphi\left(p_{iA}^{\text{cur}}\right) > 0$ **then**
14: $\overline{p_{iA}} = p_{iA}^{\text{cur}}$.
15: **else**
16: $\underline{p_{iA}} = p_{iA}^{\text{cur}}$.
17: **end if**
18: **end if**
19: **end while**
20: **end if**
21: **Output**: p_{iA}^* as the optimal solution for Problem(P2-E).

Proposition 2: (Convergence of Algorithm (SolP2E)) Given p_{iA}^{low} and p_{iA}^{upp}, Algorithm (SolP2E) is guaranteed to converge to the optimal solution p_{iA}^* for Problem (P2-E) within $\log_2\left(\left(p_{iA}^{\text{upp}} - p_{iA}^{\text{low}}\right)/\gamma\right)$ rounds of iterations, with γ representing the tolerance for computational error.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2016.2611979, IEEE Journal on Selected Areas in Communications

Proof: The proof is essentially based on the property that $\varphi(p_{iA})$ is increasing in p_{iA}. Hence, given p_{iA}^{low} and p_{iA}^{upp}, the bisection search is guaranteed to converge within $\log_2\left(\left(p_{iA}^{\text{upp}}-p_{iA}^{\text{low}}\right)/\gamma\right)$ rounds of iterations, if there exists a $p_{iA}^{*}\in[p_{iA}^{\text{low}},p_{iA}^{\text{upp}}]$ such that $\varphi(p_{iA}^{*})=0$. ■

Notice that in Algorithm (SolP2E), we still need to know the interval $[p_{iA}^{\text{low}},p_{iA}^{\text{upp}}]$ (which is specified by constraints (9), (20), and (21)). We will analytically derive p_{iA}^{low} and p_{iA}^{upp} in the next subsection. We emphasize that the tuple of $(p_{iA}^{\text{low}},p_{iA}^{\text{upp}})$, i.e., the input of Algorithm (SolP2E), will be analytically given by Propositions 3 and 4, both of which do not require any iterative computation. Hence, thanks to the nature of bisection search, Algorithm (SolP2E) is very efficient, since its total complexity is no more than $\log_2\left(\left(p_{iA}^{\text{upp}}-p_{iA}^{\text{low}}\right)/\gamma\right)$ iterations.

C. Deriving the lower-bound p_{iA}^{low} and the upper-bound p_{iA}^{upp}

In this section, we focus on deriving p_{iA}^{low} and p_{iA}^{upp} used in Algorithm (SolP2E). To derive p_{iA}^{low} and p_{iA}^{upp}, we need to consider different possible cases. For the sake of easy presentation in the rest of this paper, we define two new parameters K and L as follows:

$$K = 2^{-\frac{R_i^{\text{req}}}{(1-\epsilon_i)W_A}}, \tag{23}$$

$$L = \left(\frac{p_{iB}^{\max}g_{iB}}{n_B}+1\right)^{\frac{W_B}{(1-\epsilon_i)W_A}}. \tag{24}$$

Using parameters K and L, constraints (20) and (21) can be compactly expressed by:

$$p_{iA}\left(\theta_{iA}-KL\hat{g}_{iA}\right)\le n_E\left(KL-1\right), \tag{25}$$

$$p_{iA}\left(\theta_{iA}-K\hat{g}_{iA}\right)\ge n_E(K-1). \tag{26}$$

To derive p_{iA}^{low} and p_{iA}^{upp} based on (25) and (26), we need to consider different cases of K and L. By observing (25), we first introduce two different cases, namely, **Case I of** $KL\ge 1$ and **Case II of** $KL<1$, with their difference given as follows. Problem (P2-E) is always feasible in Case I, while it might be infeasible in Case II. The detailed explanations are given in the following remark.

Remark 2: **(Key difference between Case I and Case II):** Based on the definitions of K and L, Case I (i.e., $KL\ge 1$) means that $W_B\log_2(1+\frac{p_{iB}^{\max}g_{iB}}{n_B})\ge R_i^{\text{req}}$, namely, $p_{iB}^{\max}$ can meet MU i's entire traffic demand without offloading any traffic to the sAP. This means that Problem (P2-E) is always feasible under Case I. In comparison, Case II (i.e., $KL<1$) means that $p_{iB}^{\max}$ cannot meet MU i's entire traffic demand. Thus, Problem (P2-E) might be infeasible under Case II. ■

1) Values of p_{iA}^{low} and p_{iA}^{upp} under Case I: We first derive the values of p_{iA}^{low} and p_{iA}^{upp} under Case I.

Proposition 3: (Values of p_{iA}^{low} and p_{iA}^{upp} under Case I) Assume $KL\ge 1$. There exists two different subcases, namely, Case I.1 and Case I.2, as follows:

$$\textbf{Case I.1:}\quad \text{If } K\le\frac{\theta_{iA}}{\hat{g}_{iA}}\le 1\le KL, \text{then } p_{iA}^{\text{low}}=0 \text{ and } p_{iA}^{\text{upp}}=p_{iA}^{\max}, \tag{27}$$

$$\textbf{Case I.2:}\quad \text{If } \frac{\theta_{iA}}{\hat{g}_{iA}}<K\le 1\le KL, \text{then } p_{iA}^{\text{low}}=0 \text{ and } p_{iA}^{\text{upp}}=\min\left\{p_{iA}^{\max},\frac{n_E(1-K)}{K\hat{g}_{iA}-\theta_{iA}}\right\}. \tag{28}$$

Proof: Please refer to Appendix III for the details. ■

According to Remark 2, Case I means that $p_{iB}^{\max}$ alone can afford MU i's entire traffic demand without using any data offloading to the sAP. Hence, both Case I.1 and Case I.2 lead to $p_{iA}^{\text{low}}=0$ (according to (9)). We emphasize that the difference between Case I.1 and Case I.2 lies in the value of p_{iA}^{upp}, and the difference is due to the relationship between K and $\frac{\theta_{iA}}{\hat{g}_{iA}}$. The details are explained in the following remark.

Remark 3: **(Difference between Case I.1 and Case I.2)** In Case I.1, because of $K\le\frac{\theta_{iA}}{\hat{g}_{iA}}\Leftrightarrow\frac{\hat{g}_{iA}}{\theta_{iA}}\le 2^{\frac{R_i^{\text{req}}}{(1-\epsilon_i)W_A}}$, we have the following result:

$$\lim_{p_{iA}\to+\infty}(1-\epsilon_i)W_A\log_2\left(\frac{p_{iA}\hat{g}_{iA}+n_E}{p_{iA}\theta_{iA}+n_E}\right)=(1-\epsilon_i)W_A\log_2\left(\frac{\hat{g}_{iA}}{\theta_{iA}}\right)\le R_i^{\text{req}}. \tag{29}$$

Inequality (29) means that if θ_{iA} is strong enough (or $\hat{g}_{iA}$ is small enough), then no matter how large MU i's p_{iA} is, its effective offloaded-rate to the sAP cannot exceed R_i^{req}. Notice that (29) guarantees (19), which is equivalent to (21). Thus, constraint (26), which is equivalent to (21) via using K and L, is always satisfied.

In Case I.2, because of $\frac{\theta_{iA}}{\hat{g}_{iA}}<K\Leftrightarrow\frac{\hat{g}_{iA}}{\theta_{iA}}>2^{\frac{R_i^{\text{req}}}{(1-\epsilon_i)W_A}}$, we have the following result:

$$\lim_{p_{iA}\to+\infty}(1-\epsilon_i)W_A\log_2\left(\frac{p_{iA}\hat{g}_{iA}+n_E}{p_{iA}\theta_{iA}+n_E}\right)=(1-\epsilon_i)W_A\log_2\left(\frac{\hat{g}_{iA}}{\theta_{iA}}\right)>R_i^{\text{req}}. \tag{30}$$

Inequality (30) means that if θ_{iA} is small enough (or $\hat{g}_{iA}$ is large enough), then MU i's effective offloaded data to the sAP could exceed R_i^{req}. That is why we account for $\frac{n_E(1-K)}{K\hat{g}_{iA}-\theta_{iA}}$ (according to (26)) in p_{iA}^{upp}. ■

2) Values of p_{iA}^{low} and p_{iA}^{upp} under Case II: We next derive p_{iA}^{low} and p_{iA}^{upp} for Case II (i.e., when $KL<1$). In Case II, $p_{iB}^{\max}$ alone cannot afford MU i's R_i^{req}, and thus MU i has to offload part of its data to the sAP. As a result, the lower-bound p_{iA}^{low} is non-zero, and Problem (P2-E) might be infeasible.

Proposition 4: (Values of p_{iA}^{low} and p_{iA}^{upp} under Case II (i.e., $KL<1$)) There exists five different subcases under Case II (i.e., $KL<1$), namely, Case II.1, Case II.2 (including Case II.2a and Case II.2b), and Case II.3 (including Case II.3a and Case II.3b). The details are shown on the top of Page 8.

Proof: Please refer to Appendix IV for the details. ■

Case II.2b is similar to Case II.2a, but with the derived p_{iA}^{low} and $p_{iA}^{\max}$ in Case II.2a leading to $p_{iA}^{\text{low}}>p_{iA}^{\max}$, which consequently results in that Problem (P2-E) is infeasible under Case II.2b (that's why we use "2a" and "2b" to differ these two subcases). The similar relationship holds for Case II.3a and Case II.3b.

Proposition 4 also determines the feasibility of Problem (P2-E) (as well as Problem (P1)), i.e., if none of Case II.1, Case II.2b, and Case II.3b happens, then Problem (P2-E) (as well as Problem (P1)) is feasible.

We explain why Problem (P2-E) is always infeasible under Case II.1 in the following remark.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2016.2611979, IEEE Journal on Selected Areas in Communications

Case II.1: If $K \leq KL < \dfrac{\theta_{iA}}{\hat{g}_{iA}} \leq 1$, then Problem (P2-E) is infeasible.

Case II.2a: If $K \leq \dfrac{\theta_{iA}}{\hat{g}_{iA}} \leq KL \leq 1$ and $\dfrac{n_E(1-KL)}{KL\hat{g}_{iA}-\theta_{iA}} \leq p_{iA}^{\max}$, then $p_{iA}^{\text{low}} = \dfrac{n_E(1-KL)}{KL\hat{g}_{iA}-\theta_{iA}}$ and $p_{iA}^{\text{upp}} = p_{iA}^{\max}$.

Case II.2b: If $K \leq \dfrac{\theta_{iA}}{\hat{g}_{iA}} \leq KL \leq 1$ and $\dfrac{n_E(1-KL)}{KL\hat{g}_{iA}-\theta_{iA}} > p_{iA}^{\max}$, then Problem (P2-E) is infeasible.

Case II.3a: If $\dfrac{\theta_{iA}}{\hat{g}_{iA}} < K \leq KL \leq 1$ and $\dfrac{n_E(1-KL)}{KL\hat{g}_{iA}-\theta_{iA}} \leq \min\left\{p_{iA}^{\max}, \dfrac{n_E(1-K)}{K\hat{g}_{iA}-\theta_{iA}}\right\}$, then

$$p_{iA}^{\text{low}} = \frac{n_E(1-KL)}{KL\hat{g}_{iA}-\theta_{iA}} \text{ and } p_{iA}^{\text{upp}} = \min\left\{p_{iA}^{\max}, \frac{n_E(1-K)}{K\hat{g}_{iA}-\theta_{iA}}\right\}.$$

Case II.3b: If $\dfrac{\theta_{iA}}{\hat{g}_{iA}} < K \leq KL \leq 1$ and $\dfrac{n_E(1-KL)}{KL\hat{g}_{iA}-\theta_{iA}} > \min\left\{p_{iA}^{\max}, \dfrac{n_E(1-K)}{K\hat{g}_{iA}-\theta_{iA}}\right\}$, then Problem (P2-E) is infeasible.

Remark 4: **(Rationale behind the Infeasibility of Problem (P2-E) under Case II.1)** In Case II.1, i.e., when θ_{iA} is so large (or $\hat{g}_{iA}$ is so small) such that $KL < \frac{\theta_{iA}}{\hat{g}_{iA}}$, then we have the following result

$$\begin{aligned}\lim_{p_{iA}\to+\infty} \frac{n_B}{g_{iB}}\left(2^{\frac{R_i^{\text{req}}}{W_B}}\left(\frac{p_{iA}\hat{g}_{iA}+n_E}{p_{iA}\theta_{iA}+n_E}\right)^{-\frac{(1-\epsilon_i)W_A}{W_B}}-1\right) &= \frac{n_B}{g_{iB}}\left(2^{\frac{R_i^{\text{req}}}{W_B}}\left(\frac{\hat{g}_{iA}}{\theta_{iA}}\right)^{-\frac{(1-\epsilon_i)W_A}{W_B}}-1\right)\\ &> \frac{n_B}{g_{iB}}\left(2^{\frac{R_i^{\text{req}}}{W_B}}(KL)^{\frac{(1-\epsilon_i)W_A}{W_B}}-1\right) = p_{iB}^{\max},\end{aligned}$$

with the last equality holding due to the definitions of K and L. The above inequality means that no matter how large MU i's p_{iA} to the sAP is, the correspondingly required p_{iB} always exceeds $p_{iB}^{\max}$. Hence, Problem (P2-E) is always infeasible. ■

As stated in Remark 2, under Case II, $p_{iB}^{\max}$ alone cannot afford MU i's entire demand R_i^{req}, and MU i has to offload part of its data to the sAP. This leads to the nonzero lower-bound $p_{iA}^{\text{low}} = \frac{n_E(1-KL)}{KL\hat{g}_{iA}-\theta_{iA}}$ under Case II.2a and Case II.3a, which is the key difference from Case I.1 and Case I.2.

Until now, we have finished deriving p_{iA}^{low} and p_{iA}^{upp} in all possible cases. Figure 2 shows a summary of the above discussions about all the cases.

D. Summary of Optimal Solution for Problem (P2-E) and Optimal Offloading for Problem (P1)

In summary, we can compute p_{iA}^{low} and p_{iA}^{upp} according to Propositions 3 and 4, base on which we can derive the optimal solution p_{iA}^* for Problem (P2-E) based on Proposition 2. We have completely solved Problem (P2-E). After obtaining p_{iA}^*, we can further derive the other three optimal solutions (namely,x_{iA}^*, p_{iB}^*, and x_{iB}^*) for the original Problem (P1). The details are as follows.

Proposition 5: (Optimal Solution of Problem (P1)) Given the optimal solution p_{iA}^* for Problem (P2-E), the other three optimal solutions (namely, x_{iA}^*, p_{iB}^*, and x_{iB}^*) for the original Problem (P1) can be derived as follows. The optimal offloaded rate x_{iA}^* to the sAP for Problem (P1) is given by

$$x_{iA}^* = W_A \log_2\left(\frac{p_{iA}^*\hat{g}_{iA}+n_E}{p_{iA}^*\theta_{iA}+n_E}\right). \tag{31}$$

Meanwhile, the optimal transmit-power p_{iB}^* and the rate x_{iB}^* to the mBS are respectively given by

$$p_{iB}^* = \frac{n_B}{g_{iB}}\left(2^{\frac{R_i^{\text{req}}}{W_B}}\left(\frac{p_{iA}^*\hat{g}_{iA}+n_E}{p_{iA}^*\theta_{iA}+n_E}\right)^{-\frac{(1-\epsilon_i)W_A}{W_B}}-1\right), \text{ and}$$

$$x_{iB}^* = R_i^{\text{req}} - (1-\epsilon_i)W_A \log_2\left(\frac{p_{iA}^*\hat{g}_{iA}+n_E}{p_{iA}^*\theta_{iA}+n_E}\right). \tag{32}$$

Proof: x_{iA}^* in (31) is obtained based on Lemma 2. Meanwhile, x_{iB}^* and p_{iB}^* in (32) are obtained by equations (16) and (17), respectively. We thus finish the proof. ■

We thus finish solving the original Problem (P1) completely. As the optimal solution of Problem (P1), the MU's traffic scheduling and transmit-powers to the sAP and mBS depend on the system parameters, especially the MU's channel power gains to the sAP and mBS. In this paper, we focus on a relatively static scenario in which the MU does not move or moves slowly, e.g., when the MU is in an indoor environment. As a result, the channel statistics will not significantly change, although the actual channel realization can change over different channel coherence times. Fortunately, as long as the time period of interest is much larger than the channel coherence time, we can use proper channel coding techniques to achieve the data rates that are determined by the average channel conditions.[2]

[2]On the other hand, if the MU moves very fast, the channel statistics will change within the time period of interest. In this case, we can no longer treat the channel as fixed in the average sense, and our proposed method will not apply to this case. Nevertheless, we notice that traffic offloading is often not a good choice for fast moving MU, due to the need of fast and frequent handoff among multiple small access points.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2016.2611979, IEEE Journal on Selected Areas in Communications

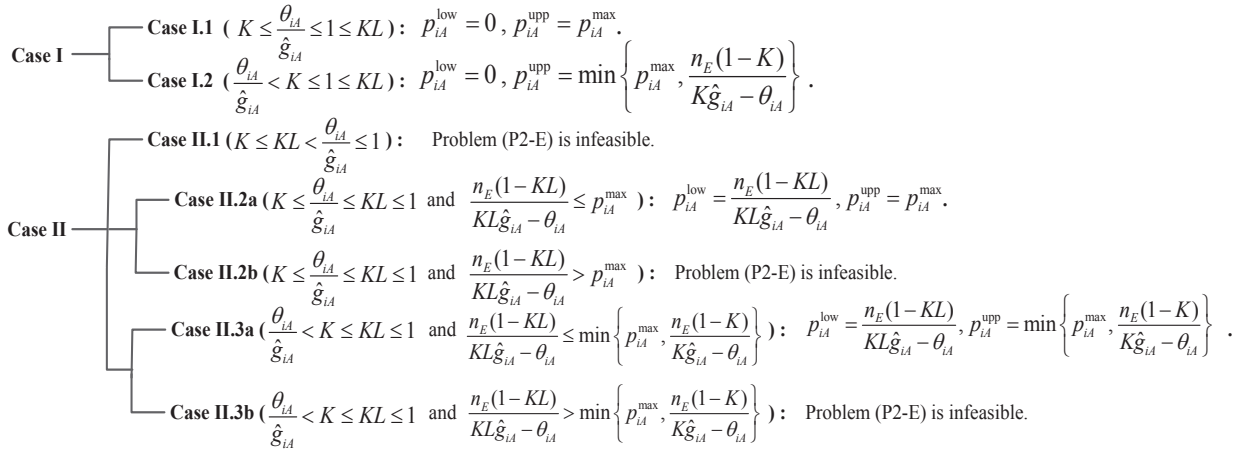


Fig. 2: Summary of all possible subcases about p_{iA}^{low} and p_{iA}^{upp}.

V. Analysis of the Full-offloading Solution and the Zero-offloading Solution

In this section, we focus on characterizing two special cases of the optimal offloading solution, namely, *the full-offloading solution* and *the zero-offloading solution*.

A. Results of the Full-Offloading Solution

Under some system parameter settings, the optimal solution of Problem (P1) is $x_{iA}^* = R_i^{\text{req}}/(1-\epsilon_i)$ and $x_{iB}^* = 0$, meaning that it is optimal for MU i to offload its entire traffic demand to the sAP. We refer to this solution as the full-offloading solution. By using the optimal offloading solution derived in the previous section, we have the following sufficient condition that leads to the full-offloading solution.

Proposition 6: (Threshold of θ_{iA} for the full-offloading solution) There exists a threshold $\theta_{iA}^{\text{thre,F}}$ given in (33) (where the superscript "F" denotes "Full"). If θ_{iA} (defined in (13)) satisfies $\theta_{iA} \le \theta_{iA}^{\text{thre,F}}$ and $\frac{n_E(1-K)}{K\hat{g}_{iA}-\theta_{iA}} \le p_{iA}^{\max}$ holds, then the optimal offloading solution of Problem (P1) corresponds to the full-offloading solution, i.e., $x_{iA}^* = \frac{R_i^{\text{req}}}{1-\epsilon_i}$ and $x_{iB}^* = 0$.

Proof: Please refer to Appendix V for the details. ■

Recall that θ_{iA} defined in (13) quantifies the impact of the security requirement (which depends on the eavesdropper's average channel power gain and the MU's secrecy-outage limit). Hence, a smaller θ_{iA} will lead to a larger optimal offloading-rate x_{iA}^* to the sAP. Moreover, $x_{iA}^* = R_i^{\text{req}}/(1-\epsilon_i)$ if θ_{iA} is smaller than a certain threshold given by $\theta_{iA}^{\text{thre,F}}$. Followed by Proposition 6, we have the following result.

Corollary 1: (Threshold of α_i for the full-offloading solution) There exists a critical threshold $\alpha_i^{\text{thre,F}}$, such that when $\alpha_i \le \alpha_i^{\text{thre,F}}$, the optimal offloading solution of Problem (P1) corresponds to the full-offloading solution (namely, $x_{iA}^* = R_i^{\text{req}}/(1-\epsilon_i)$ and $x_{iB}^* = 0$).

Proof: A keen observation of (33) is that the value of $\theta_{iA}^{\text{thre,F}}$ is independent of α_i. Moreover, according to Property (ii) in Lemma 1, θ_{iA} defined in (13) is increasing in α_i. Therefore, there exists a unique value of α_i (which is denoted by $\alpha_i^{\text{thre,F}}$) that leads to $\theta_{iA} = \theta_{iA}^{\text{thre,F}}$. Hence, $\alpha_i \le \alpha_i^{\text{thre,F}}$ leads to $\theta_{iA} \le \theta_{iA}^{\text{thre,F}}$, which consequently leads to the full-offloading solution according to Proposition 6. ■

Corollary 1 shows that the full-offloading is optimal, if the eavesdropper's average channel power gain is weak enough (i.e., weaker than $\alpha_i^{\text{thre,F}}$). Although it is difficult to derive $\alpha_i^{\text{thre,F}}$ analytically, we propose an efficient algorithm (referred as Algorithm (Thre-α_i)) to compute $\alpha_i^{\text{thre,F}}$, by using the value of $\theta_{iA}^{\text{thre,F}}$ given by (33) in Step 7. Algorithm (Thre-α_i) performs a bisection search on α_i (i.e., the while-loop from Steps 2 to 13) until $\theta_{iA}^{\text{thre,F}} + \alpha_i \ln\left(1 - (1 - e^{\frac{-\hat{g}_{iA}}{\alpha_i}})(1-\epsilon_i)\right) = 0$ holds (according to the definition of θ_{iA} in (13)).

Algorithm (Thre-α_i): to compute $\alpha_i^{\text{thre,F}}$ under given $\theta_{iA}^{\text{thre,F}}$

1: **Initialization:** Set a tolerant error parameter γ. Set $\underline{\alpha_i} = 10^{-15}$ and $\overline{\alpha_i} = 1$. Set $flag = 1$.
2: **while** $flag = 1$ **do**
3: $\quad \alpha_i^{\text{cur}} = (\overline{\alpha_i} + \underline{\alpha_i})/2$.
4: $\quad$ **if** $\overline{\alpha_i} - \underline{\alpha_i} \le \gamma$ **then**
5: $\quad\quad \alpha_i^{\text{thre,F}} = \alpha_i^{\text{cur}}$, and set $flag = 0$.
6: $\quad$ **else**
7: $\quad\quad$ **if** $\theta_{iA}^{\text{thre,F}} + \alpha_i^{\text{cur}} \ln\left(1 - (1 - e^{\frac{-\hat{g}_{iA}}{\alpha_i^{\text{cur}}}})(1-\epsilon_i)\right) > 0$ **then**
8: $\quad\quad\quad \underline{\alpha_i} = \alpha_i^{\text{cur}}$.
9: $\quad\quad$ **else**
10: $\quad\quad\quad \overline{\alpha_i} = \alpha_i^{\text{cur}}$.
11: $\quad\quad$ **end if**
12: $\quad$ **end if**
13: **end while**
14: **Output**: The value of $\alpha_i^{\text{thre,F}}$.

B. Results of the Zero-Offloading Solution

Under certain system parameters, it is also possible to have the optimal offloading solution of $x_{iA}^* = 0$ and $x_{iB}^* = R_i^{\text{req}}$, i.e., no traffic is offloaded to the sAP at all. We refer to this solution as the zero-offloading solution. We next present the sufficient conditions under which the optimal solution of Problem (P1) corresponds to the zero-offloading solution.

Proposition 7: (Threshold of θ_{iA} for the zero-offloading solution) There exists a threshold $\theta_{iA}^{\text{thre,Z}}$ given as follows (the capital letter "Z" denotes "zero"):

$$\theta_{iA}^{\text{thre,Z}} = \hat{g}_{iA} - \frac{n_E W_B g_{iB}}{n_B W_A (1-\epsilon_i) 2^{\frac{R_i^{\text{req}}}{W_B}}}. \tag{34}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2016.2611979, IEEE Journal on Selected Areas in Communications

$$\theta_{iA}^{\text{thre,F}} = K\hat{g}_{iA} - \frac{n_E g_{iB} W_B + \sqrt{(n_E g_{iB} W_B)^2 + 4(1-\epsilon_i) n_B n_E \hat{g}_{iA} g_{iB} W_A W_B 2^{\frac{R_i^{\text{req}}}{(1-\epsilon_i)W_A}} (1-K)}}{2(1-\epsilon_i) n_B W_A 2^{\frac{R_i^{\text{req}}}{(1-\epsilon_i)W_A}}}. \quad (33)$$

If θ_{iA} (defined in (13)) satisfies $\theta_{iA} \geq \theta_{iA}^{\text{thre,Z}}$ and $KL \geq 1$ holds, then the optimal offloading solution of Problem (P1) corresponds to the zero-offloading solution, namely, $x_{iA}^* = 0$ and $x_{iB}^* = R_i^{\text{req}}$.

Proof: Please refer to Appendix VI for the details. ■

Notice that θ_{iA} defined in (13) represents the strength of the security requirement. Hence, it is reasonable that a larger θ_{iA} leads to a smaller optimal offloading-rate x_{iA}^* to the sAP. Moreover, $x_{iA}^* = 0$ if θ_{iA} is larger than a certain threshold given by $\theta_{iA}^{\text{thre,Z}}$. Moreover, we have the following corollary based on Proposition 7.

Corollary 2: (Threshold of α_i for the zero-offloading solution) There exists a threshold $\alpha_i^{\text{thre,Z}}$, such that when $\alpha_i \geq \alpha_i^{\text{thre,Z}}$, the optimal solution of Problem (P1) corresponds to the zero-offloading solution, namely, $x_{iA}^* = 0$ and $x_{iB}^* = R_i^{\text{req}}$.

Proof: Notice that the right hand side of (34) is independent on α_i. Meanwhile, according to Property (ii) in Lemma 1, θ_{iA} (defined in (13)) is increasing in α_i. Thus, there exists a unique α_i (denoted by $\alpha_i^{\text{thre,Z}}$) that leads to $\theta_{iA} = \theta_{iA}^{\text{thre,Z}}$. Thus, $\alpha_i \geq \alpha_i^{\text{thre,Z}}$ leads to $\theta_{iA} \geq \theta_{iA}^{\text{thre,Z}}$, which leads to the zero-offloading solution based on Proposition 7. ■

Corollary 2 shows that the zero-offloading is optimal, if the eavesdropper's average channel power gain is large enough (i.e., larger than $\alpha_i^{\text{thre,Z}}$). Although the value of $\alpha_i^{\text{thre,Z}}$ cannot be derived analytically, we can use the proposed Algorithm (Thre-α_i) to compute $\alpha_i^{\text{thre,Z}}$ with a slight modification. Specifically, we use $\theta_{iA}^{\text{thre,Z}}$ (given in (34)) to replace $\theta_{iA}^{\text{thre,F}}$ in Step 7 of Algorithm (Thre-α_i), which thus output the value of $\alpha_i^{\text{thre,Z}}$.

VI. Numerical Results for Single MU Scenario

We validate our analytical results and the proposed algorithms for the single-MU case (notice that we will show the numerical results for the multiple-MUs case in Section VII). We set the parameters mainly according to the existing industrial data sheets, standards, and related studies. Specifically, we consider a scenario that the mBS is located at the origin $(0\text{m}, 0\text{m})$, the sAP is located at $(250\text{m}, 0\text{m})$, and MU i is located at $(220\text{m}, 0\text{m})$. Under this setting, the MU is much closer to the sAP than to the mBS, hence offloading traffic to the sAP is expected to be beneficial. We use the same channel model as in related studies [6] [7], which includes both the path-loss effect and small-scale fading effect. Specifically, we set the channel power gain g_{iB} from MU i to the mBS as $g_{iB} = \lambda d_{iB}^{-\kappa}$, where parameter d_{iB} denotes the distance between MU i and the mBS, parameter κ denotes the scaling-parameter (we use $\kappa = 2.5$), and parameter λ follows an exponential distribution with a unit mean for capturing the impact of channel fading. The channel power gain g_{iA} from MU i to the sAP is generated in a similar manner. With this scheme, the randomly generated channel power gains which are used in Figures 3 to 7 are $g_{iB} = 3.45 \times 10^{-6}$ and $g_{iA} = 1.62 \times 10^{-4}$. In addition, we set $p_{iB}^{\max} = 0.3$W and $p_{iA}^{\max} = 0.25$W [40], and set the bandwidths $W_B = 2$MHz and $W_A = 20$MHz [41]. We set $n_B = 2 \times 10^{-9}$W, $n_A = 2 \times 10^{-8}$W, and $n_E = 3 \times 10^{-8}$W.

A. Influence of the MU's offloading decisions on the secrecy-outage and total power consumption

In Figure 3, we use contour-plots to show how the MU's traffic offloading decision influences the secrecy-outage probability in Figure 3(a) and the MU's total transmit-power consumption in Figure 3(b). We compute these two quantities under different combinations of p_{iA} and x_{iA} (we enumerate p_{iA} and x_{iA} with a small step-size, and use (1) and (8) to compute x_{iB} and p_{iB} for each enumerated pair of (p_{iA}, x_{iA})).

Figure 3(a) shows that the MU's secrecy-outage probability increases in the MU's offloading-rate x_{iA}, and decreases in the MU's transmit-power p_{iA} to the sAP. Such trends are consistent with the intuitions, i.e., a larger offloading-rate leads to a larger risk of being overheard by the eavesdropper, while a larger transmit-power helps protect the offloaded data from being overheard. The result also indicates that without a proper choice of (p_{iA}, x_{iA}) (e.g., the combination of a small p_{iA} and a large x_{iA}), the MU's secrecy-outage probability could be very large. This motivates us to impose constraint (7) to ensure the MU's secrecy-outage probability no larger than a given limit ϵ_i. Figure 3(b) shows how the MU's traffic offloading decision influences the MU's consequent total transmit-power. Specifically, the combination of a large p_{iA} and a small x_{iA} yields a large total transmit-power due to the large p_{iA}. Meanwhile, the combination of a small p_{iA} and a small x_{iA} also yields a large total transmit-power consumption. This is because that a large portion of the MU's traffic demand needs to be delivered to the mBS, which consequently consumes a large p_{iB} due to the long distance between the MU and the mBS. Figure 3(a) and Figure 3(b) together demonstrate the importance of solving our formulated Problem (P1), namely, we need to properly determine the MU's traffic scheduling and transmit-powers, such that the MU's secrecy-requirement is satisfied and its total transmit-power consumption is minimized.

To further demonstrate the above point, we set the MU's secrecy-outage probability limit $\epsilon_i = 0.05$, and compute the corresponding optimal (p_{iA}^*, x_{iA}^*) by using our proposed Algorithm (SolP2E). In Figure 3(b), we mark the corresponding MU's optimal traffic offloading solution, i.e., (p_{iA}^*, x_{iA}^*) and the corresponding $P_{\text{out}}(p_{iA}^*, x_{iA}^*)$. The value of (p_{iB}^*, x_{iB}^*) can be uniquely determined by eq. (32) based on (p_{iA}^*, x_{iA}^*), and thus is not shown here. In Figure 3(b), we also plot the boundary curve for $P_{\text{out}}(p_{iA}, x_{iA}) \leq \epsilon_i = 0.05$, namely, the combinations of (p_{iA}, x_{iA}) on or below the curve lead to $P_{\text{out}}(p_{iA}, x_{iA}) \leq 0.05$, while all those above this curve lead to $P_{\text{out}}(p_{iA}, x_{iA}) > 0.05$, Therefore, only the combinations of (p_{iA}, x_{iA}) on or below this boundary curve satisfy constraint

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2016.2611979, IEEE Journal on Selected Areas in Communications

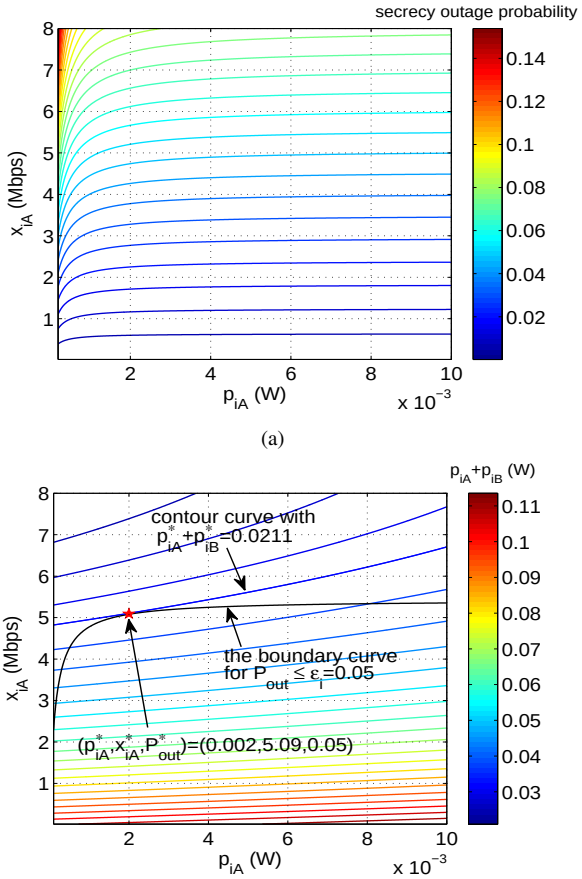


Fig. 3: Influences of the MU's traffic offloading decision on the secrecy-outage probability and total transmit-power consumption in contour plots. Subplot (a): influence on the secrecy-outage probability. Subplot (b): influence on the MU's total transmit-power consumption. We set $\alpha_i = 10^{-4}$ and $R_i^{\text{req}} = 15$Mbps.

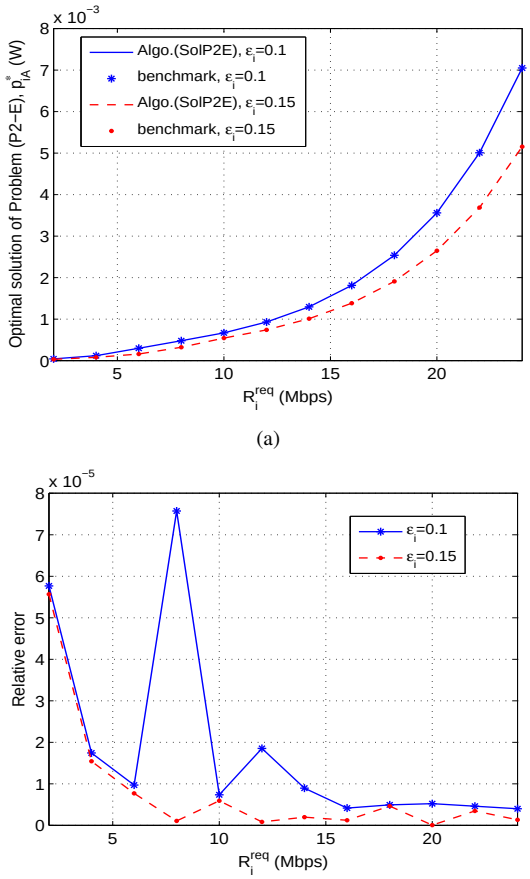


Fig. 4: Optimality (or accuracy) of p_{iA}^* obtained by Algorithm (SolP2E). Subplot (a): optimal solution p_{iA}^* of Problem (P2-E) obtained by Algorithm (SolP2E) in comparison with the benchmark solution; Subplot (b): relative error against the benchmark solution.

(7) in Problem (P1). Figure 3(b) shows that the combination of (p_{iA}^*, x_{iA}^*) is the unique intersection point between the boundary curve for $P_{\text{out}}(p_{iA}, x_{iA}) \leq 0.05$ and the contour curve with $p_{iA}^* + p_{iB}^* = 0.0211$. Such a property verifies that (p_{iA}^*, x_{iA}^*) yields the minimum MU's total transmit-power consumption among all combinations of (p_{iA}, x_{iA}) satisfying the MU's secrecy-requirement and traffic demand.

B. Verification of Algorithm (SolP2E)

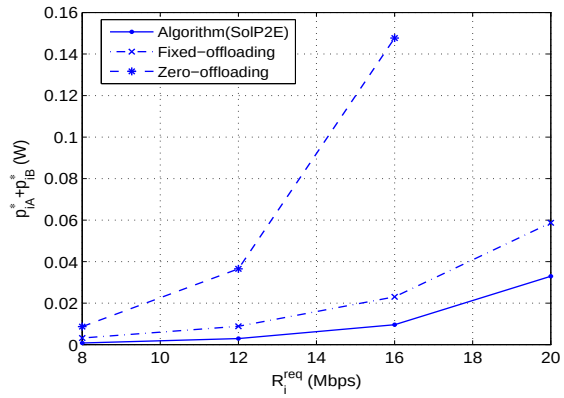
Figure 4 validates the accuracy of the proposed Algorithm (SolP2E) that optimally solves Problem (P2-E). For each tested case, we use Algorithm (SolP2E) to obtain p_{iA}^* for Problem (P2-E). We also simulate a benchmark algorithm, where we directly enumerate all possible values of p_{iA} with a very small step-size to find the best solution for Problem (P2-E). Figure 4(a) shows that p_{iA}^* obtained by Algorithm (SolP2E) (for both cases of $\epsilon_i = 0.1$ and $\epsilon_i = 0.15$) matches with the benchmark-result very well, and Figure 4(b) shows that the resulting relative error is almost negligible.

C. Performance Gain of the Optimal Offloading Solution

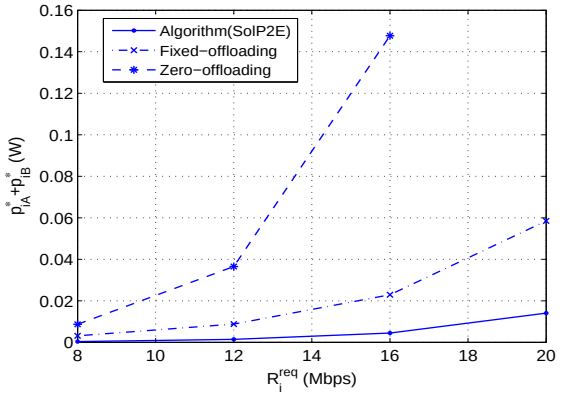
Figure 5 shows the power saving gain of the proposed optimal offloading solution computed by Algorithm (SolP2E) against two other heuristic schemes, i.e., a fixed-offloading scheme and a zero-offloading scheme. In the fixed-offloading scheme, each MU offloads a fixed portion (e.g., one thirds as we have assumed in Figure 5) of its total traffic demand to the sAP; while in the zero-offloading scheme, each MU is not allowed to offload its traffic demand at all. We can see that the optimal offloading solution always consumes the smallest total power consumption, and achieves significant power savings compared to the two other schemes. Such a gain comes from both proper traffic schedule and power optimization in Algorithm (SolP2E).

To make the comparison in Figure 5 more clear, Table II shows the the relative saving-ratio of the total power consumption by comparing the optimal offloading solution with the zero-offloading (in the second row) and the fixed-offloading (in the third row). The relative saving-ratio is thus defined as $\left(v^{\text{fix}} - v^*\right)/v^{\text{fix}}$, where $v^* = p_{iA}^* + p_{iB}^*$ denotes the total power consumption of the optimal solution, and v^{fix} denotes total power consumption of the respective heuristic scheme ("Infe" in Table II means that the zero-offloading is infeasible). The comparison between two sub-tables also shows that a larger ϵ_i (i.e., a less stringent security-outage limit) yields a greater gain, since MU i has a larger freedom

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2016.2611979, IEEE Journal on Selected Areas in Communications



(a) $\epsilon_i = 0.1$ and $\alpha_i = 10^{-4}$



(b) $\epsilon_i = 0.15$ and $\alpha_i = 10^{-4}$

Fig. 5: Power saving gain of the optimal offloading solution obtained by Algorithm (SolP2E).

in optimizing its offloading decisions.

TABLE II: Relative saving-ratio by using the optimal offloading solution obtained by Algorithm (SolP2E)

(a) $W_A = 20$MHz, $W_B = 2$MHz, $\epsilon_i = 0.1$

R_i^{req}(Mbps)	8	12	16	20
zero-offloading(%)	91.3	92.1	93.5	Infe.
fixed-offloading(%)	76.0	67.3	58.3	43.9

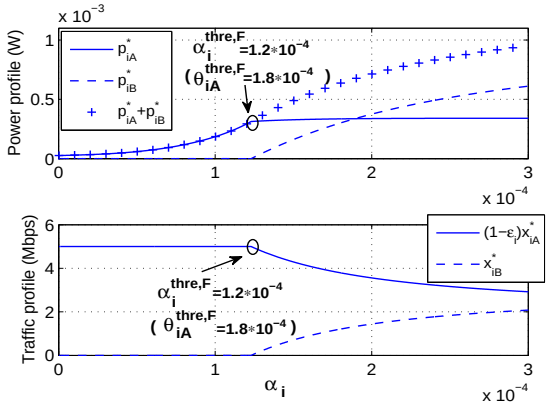
(b) $W_A = 20$MHz, $W_B = 2$MHz, $\epsilon_i = 0.15$

R_i^{req}(Mbps)	8	12	16	20
zero-offloading(%)	96.3	96.2	97.0	Infe.
fixed-offloading(%)	89.8	84.1	80.7	76.0

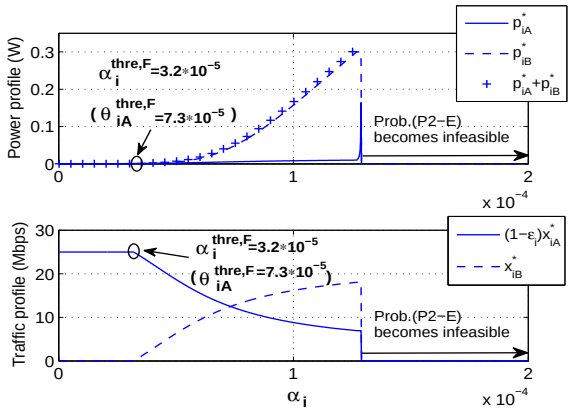
D. Influence of Eavesdroppers' Average Channel Power Gain α_i on the Optimal Offloading

Figure 6 evaluates the influence of the eavesdropper's average channel power gain α_i on the optimal offloading solution, under a given outage-limit $\epsilon_i = 0.1$. To make a clear presentation, we show two scenarios, namely, Figure 6(a) with $R_i^{\text{req}} = 5$MHz which leads to $K = 0.82$ and $KL = 1.64$ (i.e., of Case I), and Figure 6(b) with $R_i^{\text{req}} = 25$MHz which leads to $K = 0.38$ and $KL = 0.76$ (i.e., of Case II). As stated in Remark 2, the key difference between Case I and Case II is that Problem (P2-E) is always feasible under Case I, while it could be infeasible under Case II, which is reflected in Figure 6(b) when α_i is large.

Figure 6 shows that a larger α_i (i.e., a larger eavesdropper's capability to eavesdrop the MU's offloaded data) discourages the MU to offload data and consequently leads to a larger total power consumption. As shown in the top-plot of Figure 6(a), when the eavesdropper's average channel power gain α_i is smaller than $\alpha_i^{\text{thre,F}}$ (given by Proposition 6), the optimal offloading solution is always the full-offloading solution (i.e., $p^*_{iB} = 0$), and p^*_{iA} increases quickly as α_i increases. Accordingly, as shown in the bottom-plot of Figure 6(a), $x^*_{iB} = 0$ and $x^*_{iA} = R_i^{\text{req}}/(1-\epsilon_i)$ always hold when $\alpha_i \le \alpha_i^{\text{thre,F}}$. These results are consistent with Proposition 6 and Corollary 1 about the full-offloading solution. When the eavesdropper's average channel power gain $\alpha_i > \alpha_i^{\text{thre,F}}$, then both p^*_{iB} and p^*_{iA} are positive (i.e., the full-offloading solution does not hold). In this situation, p^*_{iB} increases quickly as α_i increases, while p^*_{iA} changes slightly, which leads to a quick increase in the total power consumption. Accordingly, as shown in the bottom-plot of Figure 6(a), x^*_{iB} increases as α_i increases, while x^*_{iA} gradually decreases as α_i increases. Figure 6(b) shows the similar trends as Figure 6(a) but with $KL < 1$.



(a) $R_i^{\text{req}} = 5$MHz ($K = 0.82$ and $KL = 1.64$)



(b) $R_i^{\text{req}} = 25$MHz ($K = 0.38$ and $KL = 0.76$)

Fig. 6: Influence of α_i on the optimal offloading solution. Subplot (a): $R_i^{\text{req}} = 5$MHz; Subplot (b): $R_i^{\text{req}} = 25$MHz.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2016.2611979, IEEE Journal on Selected Areas in Communications

E. Validation of Proposition 6 and Algorithm (Thre-α_i)

Table III validates Proposition 6 (to derive $\theta_{iA}^{\text{thre,F}}$) and the accuracy of Algorithm (Thre-α_i) (to find $\alpha_i^{\text{thre,F}}$), under different values of R_i^{req}. Table III(a) shows the case of $KL \geq 1$, and Table III(b) shows the case of $KL < 1$. As shown in Table III(a), for each tested R_i^{req}, the derived $\theta_{iA}^{\text{thre,F}}$ (in the second column) according to Proposition 6 matches well with $\theta_{iA,\text{enum}}^{\text{thre,F}}$ (in the third column) obtained by enumeration[3]. Meanwhile, the threshold $\alpha_i^{\text{thre,F}}$ obtained by Algorithm (Thre-α_i) (in the fourth column) also matches with $\alpha_{i,\text{enum}}^{\text{thre,F}}$ (in the fifth column) obtained by enumeration. Table III(a) also shows that the thresholds $\alpha_i^{\text{thre,F}}$ and $\theta_{iA}^{\text{thre,F}}$ decrease as R_i^{req} increases, which is consistent with the intuition. Table III(b) shows the similar results for the case of $KL < 1$ as Table III(a).

TABLE III: Validation of Proposition 6 and Algorithm (Thre-α_i)

(a) $KL \geq 1$ (R_i^{req} is in the unit of Mbps)

R_i^{req}	$\theta_{iA}^{\text{thre,F}}$	$\theta_{iA,\text{enum}}^{\text{thre,F}}$	$\alpha_i^{\text{thre,F}}$	$\alpha_{i,\text{enum}}^{\text{thre,F}}$	KL
3	$2.0*10^{-4}$	$2.0*10^{-4}$	$2.1*10^{-4}$	$2.1*10^{-4}$	1.78
4	$1.9*10^{-4}$	$1.9*10^{-4}$	$1.5*10^{-4}$	$1.5*10^{-4}$	1.72
5	$1.8*10^{-4}$	$1.8*10^{-4}$	$1.2*10^{-4}$	$1.2*10^{-4}$	1.64
6	$1.7*10^{-4}$	$1.7*10^{-4}$	$1.1*10^{-4}$	$1.1*10^{-4}$	1.58
7	$1.6*10^{-4}$	$1.6*10^{-4}$	$9.3*10^{-5}$	$9.3*10^{-5}$	1.52

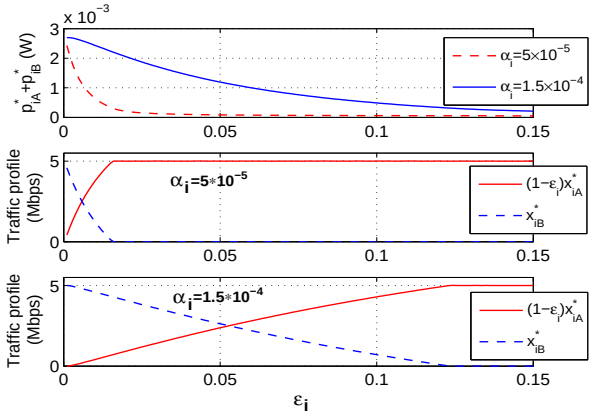
(b) $KL < 1$ (R_i^{req} is in the unit of Mbps)

R_i^{req}	$\theta_{iA}^{\text{thre,F}}$	$\theta_{iA,\text{enum}}^{\text{thre,F}}$	$\alpha_i^{\text{thre,F}}$	$\alpha_{i,\text{enum}}^{\text{thre,F}}$	KL
25	$7.3*10^{-5}$	$7.3*10^{-5}$	$3.2*10^{-5}$	$3.2*10^{-5}$	0.76
26	$7.0*10^{-5}$	$7.0*10^{-5}$	$3.1*10^{-5}$	$3.1*10^{-5}$	0.74
27	$6.7*10^{-5}$	$6.7*10^{-5}$	$2.9*10^{-5}$	$2.9*10^{-5}$	0.70
28	$6.4*10^{-5}$	$6.4*10^{-5}$	$2.8*10^{-5}$	$2.8*10^{-5}$	0.68
29	$6.1*10^{-5}$	$6.1*10^{-5}$	$2.6*10^{-5}$	$2.6*10^{-5}$	0.66

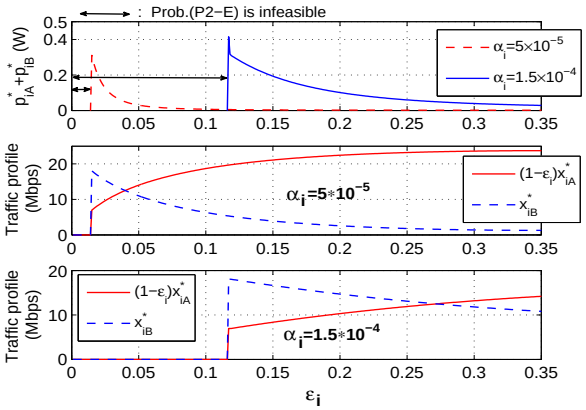
F. Influences of the MU's Secrecy-Outage Limit ϵ_i on the Optimal Offloading Solution

Figure 7 evaluates the influence of the MU's secrecy-outage limit ϵ_i on the optimal offloading solution, with two fixed values of α_i (i.e., $\alpha_i = 5 \times 10^{-5}$ and 1.5×10^{-4}). To make a clear presentation, we show two scenarios, namely, Figure 7(a) with $R_i^{\text{req}} = 5$MHz which leads to that $KL \geq 1$ always holds (i.e., of Case I)[4], and Figure 7(b) with $R_i^{\text{req}} = 25$MHz which leads to $KL < 1$ always holds (i.e., of Case II). As stated in Remark 2, the key difference between Case I and Case II is that Problem (P2-E) is always feasible under Case I, while it could be infeasible under Case II, which is reflected in Figure 7(b) when ϵ_i is very small.

Figure 7 shows that a larger ϵ_i (i.e., a less stringent limit on MU's secrecy-outage) encourages the MU to offload data, which consequently leads to a smaller total power consumption. As shown in Figure 7(a), the minimum total power consumption decreases when ϵ_i increases (in the top subplot), which is due to the fact that MU i offloads more traffic to the sAP with a less stringent security-requirement (in the middle and bottom subplots). Figure 7(b) shows the similar results as Figure 7(a), but for the case of $KL < 1$.



(a) $R_i^{\text{req}} = 5$Mbps with $KL \geq 1$ always holding.



(b) $R_i^{\text{req}} = 25$Mbps with $KL < 1$ always holding.

Fig. 7: Influence of ϵ_i on the optimal offloading solution. Subplot (a): $R_i^{\text{req}} = 5$Mbps; Subplot (b): $R_i^{\text{req}} = 25$Mbps.

VII. Multiple-MUs and Multiple-sAPs Scenario

In practice, there might exist many MUs seeking for the offloading services provided by several sAPs. Hence, it is interesting to investigate how to optimally exploit the offloading capacity provided by the sAPs via dual-connectivity. The offloading solution derived in Section IV for a single MU serves as a good starting point for analyzing this general case.

Specifically, we consider the scenario as shown in Figure 8, where a set $\mathcal{I} = \{1, ..., I\}$ of MUs and a set $\mathcal{J} = \{1, ..., J\}$ of sAPs coexist. Each MU i can form a dual-connectivity with the mBS and a selected sAP. We assume that different sAPs use different channels to accommodate the MUs' offloaded traffic. Meanwhile, there exists an eavesdropper who overhears the unlicensed channels used by the sAPs for malicious purposes.

We use $a_{ij} = 1$ to denote that MU i selects sAP j to offload data (i.e., forming a dual-connectivity with the mBS and sAP j), and $a_{ij} = 0$ otherwise. As in practice each MU has one short-range radio-interface, each MU i thus can select at most

[3]We enumerate α_i from 2×10^{-7} to 10^{-3} with a small step-size of 2×10^{-7}. We thus can find $\alpha_{i,\text{enum}}^{\text{thre,F}}$ (as shown in the fifth column in Table III(a)) which leads to the full-offloading solution when $\alpha_i \leq \alpha_{i,\text{enum}}^{\text{thre,F}}$. By using $\alpha_{i,\text{enum}}^{\text{thre,F}}$, we can derive $\theta_{iA,\text{enum}}^{\text{thre,F}}$ according to the definition of θ_{iA} in (46), since Property (ii) of Lemma 1 tells us θ_{iA} increases in α_i.

[4]Different from Figure 6, in Figure 7, the values of K and L vary with ϵ_i according to (23) and (24), respectively. Nevertheless, the parameter setting guarantees that we have $KL \geq 1$ in Figure 7(a) and $KL < 1$ in Figure 7(b).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2016.2611979, IEEE Journal on Selected Areas in Communications

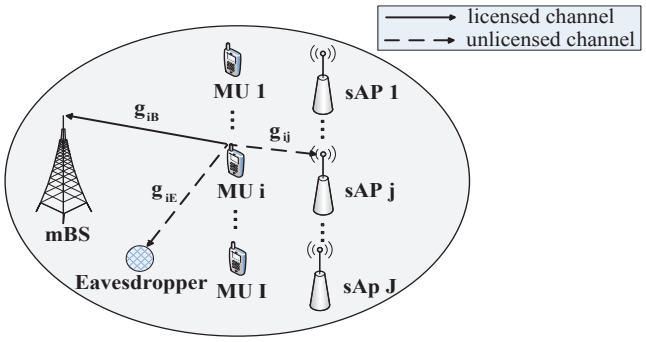


Fig. 8: Scenario of multiple-MUs and multiple-sAPs. Each MU can form dual-connectivity with the mBS and a selected sAP. An eavesdropper can overhear the MUs' offloaded data to the sAPs.

one sAP for data offloading at any given time. This leads to to the following constraint:

$$\sum_{j\in\mathcal{J}} a_{ij} \leq 1, \forall i \in \mathcal{I}. \tag{35}$$

We further assume that an sAP will only accommodate one MU's offloaded traffic at any given time, to avoid the MUs' mutual interference (e.g., IEEE 802.11 standard adopts CSMA/CA in medium access control sublayer to avoid two MUs accessing the same channel of an sAP simultaneously). This leads to the following constraint:

$$\sum_{i\in\mathcal{I}} a_{ij} \leq 1, \forall j \in \mathcal{J}. \tag{36}$$

Assuming that MU i selects sAP j to offload data, we then can use Algorithm (SolP2E) in Section IV-B to compute the optimal offloading solution. We denote the MU i's minimum total power consumption as

$$v_{ij}^* = p_{ij}^* + p_{iB}^*, \forall i \in \mathcal{I}, j \in \mathcal{J}, \tag{37}$$

where p_{ij}^* and p_{iB}^* denote MU i's optimal transmit-powers to sAP j and the mBS, respectively, for Problem (P1). By changing the subscript "A" (which denotes the sAP) to the subscript "j" (which denotes sAP j) in the notations of sections from Section II to Section V, all our prior discussions are applicable to the case of MU i choosing sAP j to offload data via dual-connectivity.

We consider the following two aspects when determining the pairing between MUs and sAPs.

- *No use of the sAP under zero-offloading solution*: According to Proposition 7, if $\theta_{ij} \geq \theta_{ij}^{\text{thre,Z}}$ (given in (34))[5], then the optimal offloading solution leads to the zero-offloading solution, i.e., $p_{ij}^* = 0$. In this case, we will set $a_{ij} = 0$ such that sAP j can serve another MU. In other words, we impose the following constraint:

$$a_{ij} = 0, \text{ if } \theta_{ij} \geq \theta_{ij}^{\text{thre,Z}}, \forall i \in \mathcal{I}, j \in \mathcal{J}. \tag{38}$$

- *No use of the mBS's channel under full-offloading solution*: According to Proposition 6, if $\theta_{ij} \leq \theta_{ij}^{\text{thre,F}}$, then the optimal offloading solution leads to the full-offloading solution, i.e., $p_{iB}^* = 0$, meaning that there is no need to use the mBS' channel. Therefore, from the mBS's channel-usage point of view, we only need to account for the mBS's channel-usage when $\theta_{ij} > \theta_{ij}^{\text{thre,F}}$.

[5]Notice that θ_{ij} can be obtained according to (13) by changing the subscript "A" to subscript "j" in the notations.

A. Modeling and Problem Formulation

We denote the reward of serving MU i successfully (i.e., meeting MU i's traffic demand and security-requirement) as π_i. Hence, as a function of $\{a_{ij}\}_{i\in\mathcal{I},j\in\mathcal{J}}$, the network-benefit of the operator and all MUs by offloading data via dual-connectivity can be given by

$$R_{\text{Dual}}(\boldsymbol{a}) = \sum_{i\in\mathcal{I}}\sum_{j\in\mathcal{J}} \big(\pi_i - \beta_i v_{ij}^* - \rho_{\text{BS}}\mathbb{I}(\theta_{ij} \geq \theta_{ij}^{\text{thre,F}})\big)a_{ij}, \tag{39}$$

where vector $\boldsymbol{a} = (\boldsymbol{a}_i, \forall i \in \mathcal{I})$ with each element $\boldsymbol{a}_i = (\{a_{ij}\}_{j\in\mathcal{J}})$. In (39), parameter β_i denotes the unit cost for MU i's transmit-power consumption, and parameter ρ_{BS} denotes the unit cost due to the mBS's channel usage. As described earlier, the indication function[6] $\mathbb{I}(\theta_{ij} \geq \theta_{ij}^{\text{thre,F}})$ captures the fact that the mBS's channel is used only when $\theta_{ij} \geq \theta_{ij}^{\text{thre,F}}$. The objective function $R_{\text{Dual}}(\boldsymbol{a})$ accounts for: i) the total reward for serving the MUs successfully, ii) the cost due to the MUs' total power consumption, and iii) the cost due to using the mBS's channels under dual-connectivity.

If MU i does not choose to offload data to any sAP (i.e., $a_{ij} = 0, \forall j \in \mathcal{J}$), it can still be served by the mBS. We use $b_{iB} = 1$ to represent that MU i is served by the mBS alone (without invoking any data offloading), and $b_{iB} = 0$ otherwise. We emphasize that constraint (38) imposes $a_{ij} = 0$ if offloading data to sAP j leads to a zero-offloading solution in dual-connectivity. Thus, if MU is served by the mBS alone, we have $b_{iB} = 1$ and $a_{ij} = 0, \forall j \in \mathcal{J}$. Hence, as a function $\{b_{iB}\}_{i\in\mathcal{I}}$, the network-benefit of the operator and all MUs via directly serving the MUs by the mBS alone can be given by

$$R_{\text{BSalone}}(\boldsymbol{b}) = \sum_{i\in\mathcal{I}} \big(\pi_i - \beta_i \frac{n_B}{g_{iB}}(2^{\frac{R_i^{\text{req}}}{W_B}} - 1) - \rho_{\text{BS}}\big)b_{iB}, \tag{40}$$

with vector $\boldsymbol{b} = (\{b_{iB}\}_{i\in\mathcal{I}})$. In (40), due to sending its entire traffic demand to the mBS, MU i's power consumption can be directly given by $\frac{n_B}{g_{iB}}(2^{\frac{R_i^{\text{req}}}{W_B}} - 1)$.

We would like to emphasize that the two sets of decision variables, i.e., $\boldsymbol{a}$ and $\boldsymbol{b}$, are coupled as follows:

- Each MU cannot simultaneously choose to be served by the mBS alone and to offload data to the sAP via dual-connectivity (i.e., sending data to both the mBS and sAP simultaneously), which leads to

$$a_{ij} + b_{iB} \leq 1, \forall i \in \mathcal{I}, j \in \mathcal{J}. \tag{41}$$

- The mBS has a limited number of channels to serve the MUs, which leads to the following constraint:

$$\sum_{i\in\mathcal{I}}\sum_{j\in\mathcal{J}} a_{ij}\mathbb{I}(\theta_{ij} \geq \theta_{ij}^{\text{thre,F}}) + \sum_{i\in\mathcal{I}} b_{iB} \leq N_{\text{BS}}^{\max}, \tag{42}$$

[6]Function $\mathbb{I}(\theta_{ij} \geq \theta_{ij}^{\text{thre,F}}) = 1$ if condition $\theta_{ij} \geq \theta_{ij}^{\text{thre,F}}$ is satisfied, and $\mathbb{I}(\theta_{ij} \geq \theta_{ij}^{\text{thre,F}}) = 0$ otherwise.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2016.2611979, IEEE Journal on Selected Areas in Communications

where $N_{\text{BS}}^{\max}$ denotes the total number of channels available at the mBS.

Taking into account the network-benefit functions $R_{\text{Dual}}(\boldsymbol{a})$ in (39) and $R_{\text{BSalone}}(\boldsymbol{b})$ in (40), and the constraints (35), (36), (38), (41), and (42), we investigate how to optimally exploit the sAPs to provide offloading services to the MUs, with the objective of maximizing the total network-benefit function $R_{\text{Dual}}(\boldsymbol{a})+R_{\text{BSalone}}(\boldsymbol{b})$. Mathematically, we formulate the following optimization problem:

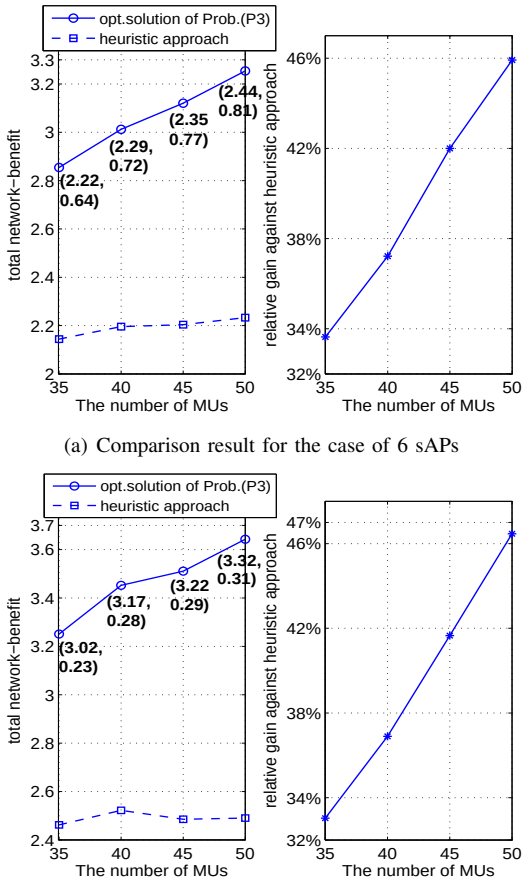
$$\begin{aligned}
\underline{\text{(P3)}}: \quad & \max \ R_{\text{Dual}}(\boldsymbol{a}) + R_{\text{BSalone}}(\boldsymbol{b}) \\
\text{Subject to:} \ & \sum_{j\in\mathcal{J}} a_{ij} + b_{iB} \le 1, \forall i \in \mathcal{I}, \qquad (43) \\
& \sum_{i\in\mathcal{I}}\sum_{j\in\mathcal{J}} a_{ij}\mathbb{I}(\theta_{ij} \ge \theta_{ij}^{\text{thre,F}}) + \sum_{i\in\mathcal{I}} b_{iB} \le N_{\text{BS}}^{\max}, \\
& \sum_{i\in\mathcal{I}} a_{ij} \le 1, \forall j \in \mathcal{J}, \\
& a_{ij} = 0, \ \text{if } \theta_{ij} \ge \theta_{ij}^{\text{thre,Z}}, \forall i \in \mathcal{I}, j \in \mathcal{J}, \\
\text{Variables:} \ & a_{ij} = \{0,1\}, \ \text{and } b_{iB} = \{0,1\}, \forall i \in \mathcal{I}, j \in \mathcal{J}.
\end{aligned}$$

Notice that in Problem (P3), because of the binary nature of $\boldsymbol{a}$ and $\boldsymbol{b}$, constraint (43) includes both constraints (35) and (41).

In Problem (P3), only $\boldsymbol{a}$ and $\boldsymbol{b}$ are variables, and all the other parameters are known. Specifically, in (39), to obtain v_{ij}^*, we can use Algorithm (SolP2E) (in Section IV-B) together with Propositions 3 and 4 to obtain the MU i's optimal transmit-power p_{ij}^* when MU i chooses sAP j to offload data. Further with Proposition 5, we can derive the corresponding p_{iB}^*, based on which we obtain $v_{ij}^* = p_{ij}^* + p_{iB}^*$ defined in (37). Moreover, we can compute θ_{ij} and $\theta_{ij}^{\text{thre,F}}$ according to (13) and (33), respectively. Hence, $\boldsymbol{a}$ and $\boldsymbol{b}$ are the variables to be optimized. Moreover, we observe that functions $R_{\text{Dual}}(\boldsymbol{a})$ and $R_{\text{BSalone}}(\boldsymbol{b})$ and all the constraints are linear with respect to $\boldsymbol{a}$ and $\boldsymbol{b}$. Therefore, Problem (P3) is a standard binary linear programming problem, which can be solved by many standard optimization solvers (such as LINGO [43]). Due to limited space, we leave the design of an efficient and distributed algorithm to solve Problem (P3) as our future works.

B. Numerical Results

We evaluate the performance of the optimal solution of Problem (P3) through several numerical studies. We assume that the mBS is located at (0m,0m), and the group of MUs in set $\mathcal{I}$ are randomly and uniformly located within a disk with the center of (220m, 0m) and a radius of 30m. Meanwhile, the sAPs in set $\mathcal{J}$ are evenly placed on a circle with the center of (220m, 0m) and a radius of 60m. For each sAP $j \in \mathcal{J}$, we set $W_j = 20$MHz and $n_j = 2\times10^{-8}$W. For each MU $i \in \mathcal{I}$, we set R_i^{req} uniformly random within $[10, 30]$Mbps, its security-outage limit $\epsilon_i = 0.1$, and the maximum transmit-power to sAP j as $p_{ij}^{\max} = 0.25$W and that to the mBS as $p_{iB}^{\max} = 0.3$W. To account for the uncertainty in the eavesdropper's information (e.g., location) with respect to different MUs, we set the average channel power gain α_i from MU i to the eavesdropper uniformly random within $[10^{-6}, 5\times10^{-4}]$. Finally, we set $W_B = 2$MHz, $n_B = 2\times10^{-9}$W, and $n_E = 3\times10^{-8}$W.



(a) Comparison result for the case of 6 sAPs

(b) Comparison result for the case of 8 sAPs

Fig. 9: Advantage of using optimal solution of Problem (P3). We use $\pi_i = 1, \beta_i = 2, \forall i \in \mathcal{I}$, and $\rho_{\text{BS}} = 0.4$. Each point in both figures represents the average result of 500 randomly generated scenarios.

Figure 9 shows the performance advantage of using the optimal solution of Problem (P3) that optimally exploits the sAPs' offloading capacity, in comparison with a heuristic sAP-selection approach. In the heuristic approach, each MU (based on its index in $\mathcal{I}$) sequently chooses the nearest available sAP to offload data; if all sAPs are used, the rest MUs choose to use the BSs' remaining channels. As shown in the left-subplot of Figure 9(a), the optimal solution of Problem (P3) always yields a larger total network-benefit than the heuristic approach. The right-subplot of Figure 9(a) shows the relative gain, which is given by $\big(R_{\text{Dual}}(\boldsymbol{a}^*) + R_{\text{BSalone}}(\boldsymbol{b}^*) - R_{\text{heu}}\big)/R_{\text{heu}}$ with R_{heu} denoting the network-benefit obtained by the heuristic approach. The results show that more than 30% of gain can be achieved by using the optimal solution.

To further validate the importance of optimal offloading solution, we provide the values of $\big(R_{\text{Dual}}(\boldsymbol{a}^*), R_{\text{BSalone}}(\boldsymbol{b}^*)\big)$ for each optimal solution of Problem (P3) in the respective left-subplots of Figures 9(a) and 9(b). The results show that $R_{\text{Dual}}(\boldsymbol{a}^*)$ is much larger than $R_{\text{BSalone}}(\boldsymbol{b}^*)$ (in fact, 60% more on average), thus validating the importance of optimally offloading MUs' data to the properly selected sAPs.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2016.2611979, IEEE Journal on Selected Areas in Communications

VIII. Conclusion

We proposed a secrecy-driven energy-efficient MU's data offloading scheme via dual-connectivity. We derived the secrecy-outage probability when the MU offloads data to sAP over unlicensed spectrum, and formulated a joint optimization of the MU's traffic scheduling and power allocations to the mBS and sAP in order to minimize the MU's total power consumption, while satisfying the secrecy-outage requirement. Despite the nonconvexity of the joint optimization problem, we proposed an efficient algorithm to compute the optimal offloading solution. By evaluating the impact of the MU's secrecy-requirement and the eavesdropper's channel condition, we further quantified the sufficient conditions under which the optimal offloading solution corresponds to the full-offloading and the zero-offloading, respectively. Numerical results validated the optimal performance of our proposed algorithm, and showed that the optimal offloading can significantly reduce the MU's total power consumption. With the proposed algorithm to compute the single MU's optimal offloading solution, we further considered the scenario of multiple MUs and sAPs, and investigated the optimal exploitation of sAPs' offloading capacity to serve the MUs while accounting for the MUs' power consumptions for offloading data. Specifically, we formulated a total network-benefit maximization problem that takes into account the reward for serving the MUs successfully, the mBS's bandwidth usage, and the MUs' power consumptions. Numerical results showed that the optimal solution can improve the total network-benefit by more than 30% compared to a heuristic sAP-selection scheme.

In this study, we mainly investigated the secrecy-driven energy-efficient data offloading in the MUs' uplink transmissions. We thus will further investigate the security issue of traffic offloading in the downlink transmission, and in particular take into account the impact of the limited backhaul capacity. An another interesting direction to extend this paper is as follows. In this paper, we did not consider the incumbent users and congestion issue in traffic offloading, since we assumed the case that the unlicensed channel used by the sAP is less congested and hence offers a larger data rate than the licensed channel used by the mBS. An interesting future direction is to investigate the congestion-aware data offloading when the sAP's unlicensed channel is congested. In this case, we need to take into account how an MU's traffic offloading influences other incumbent users and vice verse.

Appendix I: Proof of Lemma 1

Property (i) is straightforward according to the definition of θ_{iA} in (13).

We next prove Property (ii). The first order derivative of θ_{iA} with respective to α_i is given by

$$\frac{d\ \theta_{iA}}{d\ \alpha_i} = -\ln\left(1-(1-e^{-\frac{\hat{g}_{iA}}{\alpha_i}})(1-\epsilon_i)\right) - \frac{e^{-\frac{\hat{g}_{iA}}{\alpha_i}}\hat{g}_{iA}(1-\epsilon_i)}{\alpha_i\left(1-(1-e^{-\frac{\hat{g}_{iA}}{\alpha_i}})(1-\epsilon_i)\right)}. \quad (44)$$

Using (44) and after performing some manipulations, we can obtain the second order derivative as follows

$$\frac{d^2\ \theta_{iA}}{d\ \alpha_i^2} = -\frac{e^{-\frac{\hat{g}_{iA}}{\alpha_i}}\hat{g}_{iA}(1-\epsilon_i)}{\alpha_i^2\left(1-(1-e^{-\frac{\hat{g}_{iA}}{\alpha_i}})(1-\epsilon_i)\right)^2}\cdot\frac{\hat{g}_{iA}\epsilon_i}{\alpha_i} < 0, \quad (45)$$

which implies that $\frac{d\ \theta_{iA}}{d\ \alpha_i}$ (given in (44)) is decreasing. By letting α_i go to $+\infty$, we thus obtain $\lim_{\alpha_i\to+\infty}\frac{d\ \theta_{iA}}{d\ \alpha_i}=0$. Hence, we can conclude that $\frac{d\ \theta_{iA}}{d\ \alpha_i}$ is always positive, meaning that θ_{iA} is increasing in α_i.

We next prove Property (iii). Based on (13), we can derive

$$\begin{aligned}\theta_{iA} &= -\alpha_i\ln\left(1-(1-e^{-\frac{\hat{g}_{iA}}{\alpha_i}})(1-\epsilon_i)\right)\\ &\le -\alpha_i\ln\left(1-(1-e^{-\frac{\hat{g}_{iA}}{\alpha_i}})\right)=\hat{g}_{iA}. \quad (46)\end{aligned}$$

This completes the proof.

Appendix II: Proof of Lemma 2

Since $\theta_{iA}\le\hat{g}_{iA}$ always holds (i.e., Property (iii) in Lemma 1), we always have

$$\begin{aligned}&\frac{d}{dp_{iA}}W_A\log_2\left(\frac{p_{iA}\hat{g}_{iA}+n_E}{p_{iA}\theta_{iA}+n_E}\right)\\ &= W_A\frac{1}{\ln 2}\frac{p_{iA}\theta_{iA}+n_E}{p_{iA}\hat{g}_{iA}+n_E}\frac{(\hat{g}_{iA}-\theta_{iA})n_E}{(p_{iA}\theta_{iA}+n_E)^2}\ge 0,\end{aligned}$$

i.e., the right hand side of (14) is increasing in p_{iA}. Suppose that (14) is slack at the optimum of Problem (P1), we then can always reduce p_{iA} slightly (such that (14) becomes strictly binding), which reduces the objective function of Problem (P1) without violating any constraint. This completes the proof.

Appendix III: Proof of Proposition 3

We first prove Case I.1. When $LK\ge 1$, (25) is always satisfied (recall that $\hat{g}_{iA}\ge\theta_{iA}$ always holds according to Property (iii) in Lemma 1). Moreover, when $\theta_{iA}-K\hat{g}_{iA}\ge 0$, (26) is also always satisfied (recall that $K<1$ always holds according to (23)). Hence, according to (9), we obtain $p_{iA}^{\text{low}}=0$ and $p_{iA}^{\text{upp}}=p_{iA}^{\max}$.

We next prove Case I.2. For the similar reason stated before, (25) is always satisfied when $LK\ge 1$. When $\theta_{iA}-K\hat{g}_{iA}<0$ (which is opposite to Case I.1), (26) is satisfied only when $p_{iA}\le\frac{n_E(1-K)}{K\hat{g}_{iA}-\theta_{iA}}$. Hence, by further taking into account (9), we obtain $p_{iA}^{\text{low}}=0$ and $p_{iA}^{\text{upp}}=\min\left\{p_{iA}^{\max},\frac{n_E(1-K)}{K\hat{g}_{iA}-\theta_{iA}}\right\}$ in (28).

Appendix IV: Proof of Proposition 4

We first prove Case II.1. Because of $KL<\frac{\theta_{iA}}{\hat{g}_{iA}}\Leftrightarrow\theta_{iA}-KL\hat{g}_{iA}>0$ and $KL<1$ (under Case II), (25) cannot be satisfied (recall that $p_{iA}\ge 0$). Thus, Problem (P2-E) is infeasible under Case II.1.

We then prove Case II.2a and Case II.2b. Because of $\frac{\theta_{iA}}{\hat{g}_{iA}}\le KL<1$, constraint (25) leads to $p_{iA}\ge\frac{n_E(1-KL)}{KL\hat{g}_{iA}-\theta_{iA}}$. Meanwhile, because of $K\le\frac{\theta_{iA}}{\hat{g}_{iA}}$ and $K<1$, constraint (26) is always met. By further taking into account (9), we obtain $p_{iA}^{\text{low}}=\frac{n_E(1-KL)}{KL\hat{g}_{iA}-\theta_{iA}}$ and $p_{iA}^{\text{upp}}=p_{iA}^{\max}$. If the derived

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2016.2611979, IEEE Journal on Selected Areas in Communications

$p_{iA}^{\text{low}} \le p_{iA}^{\text{upp}}$, then we obtain the result of Case II.2a. Otherwise, we obtain the result of Case II.2b, under which Problem (P2-E) is infeasible.

We next prove Case II.3a and Case II.3b. Because of $\frac{\theta_{iA}}{\hat{g}_{iA}} < K \le KL < 1$, constraint (25) leads to $p_{iA} \ge \frac{n_E(1-KL)}{KL\hat{g}_{iA}-\theta_{iA}}$, and constraint (26) leads to $p_{iA} \le \frac{n_E(1-K)}{K\hat{g}_{iA}-\theta_{iA}}$. By further taking into account (9), we obtain $p_{iA}^{\text{low}} = \frac{n_E(1-KL)}{KL\hat{g}_{iA}-\theta_{iA}}$ and $p_{iA}^{\text{upp}} = \min\left\{p_{iA}^{\max}, \frac{n_E(1-K)}{K\hat{g}_{iA}-\theta_{iA}}\right\}$. If the derived $p_{iA}^{\text{low}} \le p_{iA}^{\text{upp}}$, then we obtain the result of Case II.3a. Otherwise, we obtain the result of Case II.3b, under which Problem (P2-E) is infeasible.

Appendix V: Proof of Proposition 6

The value of θ_{iA} quantifies the impact of the security requirement (which depends on the eavesdropper's average channel power gain and the MU's secrecy-outage limit). Hence, it is consistent with the intuition that a smaller θ_{iA} leads to a greater p_{iA}^* (as well as x_{iA}^*), which yields a full-offloading solution. We next prove this result. Specifically, the full-offloading solution $x_{iA}^* = R_i^{\text{req}}/(1-\epsilon_i)$ means that constraint (26) is strictly binding, which yields $p_{iA}^* = \frac{n_E(1-K)}{K\hat{g}_{iA}-\theta_{iA}}$. Thus, condition $\frac{n_E(1-K)}{K\hat{g}_{iA}-\theta_{iA}} \le p_{iA}^{\max}$ is needed in Proposition 6.

Meanwhile, according to Proposition 1, the first-order derivative of the objective function $\varphi(p_{iA})$ (in (22)) is increasing in p_{iA}. Hence, we know that $\varphi(\frac{n_E(1-K)}{K\hat{g}_{iA}-\theta_{iA}}) \le 0$ is a sufficient condition to guarantee that $p_{iA} = \frac{n_E(1-K)}{K\hat{g}_{iA}-\theta_{iA}}$ is an optimal solution for Problem (P1) (as well as Problem (P2-E)). By substituting $p_{iA} = \frac{n_E(1-K)}{K\hat{g}_{iA}-\theta_{iA}}$ into (22) and performing some further manipulations, we obtain

$$\varphi\left(\frac{n_E(1-K)}{K\hat{g}_{iA}-\theta_{iA}}\right) = 1 - \frac{n_B(1-\epsilon_i)W_A}{n_E g_{iB} W_B} 2^{\frac{R_i^{\text{req}}}{W_B}} \cdot \frac{(K\hat{g}_{iA}-\theta_{iA})^2}{(\hat{g}_{iA}-\theta_{iA})} K^{\frac{(1-\epsilon_i)W_A}{W_B}-1}. \quad (47)$$

By using (47) and making some further transformations, we can derive condition (48), which is equivalent to $\varphi\left(\frac{n_E(1-K)}{K\hat{g}_{iA}-\theta_{iA}}\right) \le 0$, as follows:

$$(1-\epsilon_i)n_B W_A 2^{\frac{R_i^{\text{req}}}{W_B}} K^{\frac{(1-\epsilon_i)W_A}{W_B}-1}\left(K\hat{g}_{iA}-\theta_{iA}\right)^2 - n_E g_{iB} W_B\left(K\hat{g}_{iA}-\theta_{iA}\right) - n_E \hat{g}_{iA} g_{iB} W_B(1-K) \ge 0. \quad (48)$$

We introduce an auxiliary variable $t = K\hat{g}_{iA} - \theta_{iA}$, which helps us represent the left hand side of (48) as:

$$\phi(t) = (1-\epsilon_i)n_B W_A 2^{\frac{R_i^{\text{req}}}{(1-\epsilon_i)W_A}} t^2 - n_E g_{iB} W_B t - n_E \hat{g}_{iA} g_{iB} W_B (1-K),$$

which is a quadratic function in t. Specifically, it can be verified that equation $\phi(t) = 0$ is guaranteed to have two roots, with one root being positive and the other being negative. Notice that according to (30) in Remark 3, the full-offloading solution can only occur when $K\hat{g}_{iA} - \theta_{iA} > 0$, i.e., $t > 0$. Using this property, we focus on deriving the positive root of $\phi(t) = 0$. We denote this positive root as t_{root}^+, which is given in eq. (49). By setting $K\hat{g}_{iA} - \theta_{iA} \ge t_{\text{root}}^+$, we obtain (50) to guarantee the full-offloading solution as the optimal solution.

Appendix VI: Proof of Proposition 7

First, to ensure $x_{iB}^* = R_i^{\text{req}}$ as an feasible solution, we require $W_B \log_2(1 + \frac{p_{iB}^{\max} g_{iB}}{n_B}) \ge R_i^{\text{req}}$, which corresponds to $KL \ge 1$ based on the definitions of K in (23) and L in (24) (please also refer to Remark 2).

Second, $x_{iB}^* = R_i^{\text{req}}$ implies $x_{iA}^* = 0$, which implies that $p_{iA}^* = 0$ is the optimal solution of Problem (P2-E). According to Proposition 1, the convexity of Problem (P2-E) indicates that the first derivative of the objective function $\varphi(p_{iA})$ (in (22)) is increasing in p_{iA}. Therefore, we know that $\varphi(0) \ge 0$ is a sufficient condition to guarantee that $p_{iA}^* = 0$ is an optimal solution for Problem (P2-E). $\varphi(0) \ge 0$ is equivalent to

$$\varphi(0) = 1 - (\hat{g}_{iA} - \theta_{iA})\frac{n_B W_A(1-\epsilon_i)}{n_E W_B g_{iB}} 2^{\frac{R_i^{\text{req}}}{W_B}} \ge 0,$$

which, after some further manipulations, can be transformed to $\theta_{iA} \ge \theta_{iA}^{\text{thre,Z}} = \hat{g}_{iA} - \frac{n_E W_B g_{iB}}{n_B W_A(1-\epsilon_i)2^{\frac{R_i^{\text{req}}}{W_B}}}$. We finish the proof.

References

[1] A. Aijaz, H. Aghvami, and M. Amani, "A Survey on Mobile Data Offloading: Technical and Business Perspectives," *IEEE Wireless Communications*, vol. 20, no. 2, pp. 104-112, April 2013.

[2] N. Ali, A. Taha, and H. Hassanein, "Quality of Service in 3GPP R12 LTE-Advanced," *IEEE Communications Magazine*, vol. 51, no. 8, pp. 103-109, 2013.

[3] C. Sankaran, "Data Offloading Techniques in 3GPP Rel-10 Networks: A Tutorial," *IEEE Communication Magazine*, vol. 50, no. 6, pp. 46-53, June 2012.

[4] Qualcomm, "LET-Advanced - Evolving and Expanding into New Frontiers," White Paper, Aug. 2014.

[5] Huawei, "U-LTE: Unlicensed Spectrum Utilization of LTE," White Paper, 2014.

[6] Y. Yang, T. Quek, and L. Duan, "Backhaul-Constrained Small Cell Networks: Refunding and QoS Provisioning," *IEEE Transactions on Wireless Communications*, vol. 13, no. 9, pp. 5148-5161, Sept. 2014.

[7] X. Kang, Y. Chia, S. Sun, and H. Chong, "Mobile Data Offloading Through A Thrid-Party WiFi Access Point: An Operator's Perspective," *IEEE Transactions on Wireless Communications*, vol. 13, no. 10, pp. 5340-5351, Oct. 2014.

[8] Q. Ye, B. Rong, Y. Chen, M. Al-Shalash, C. Caramanis, and J. Andrews, "User Association for Load Balancing in Heterogeneous Cellular Networks," *IEEE Transactions on Wireless Communications*, vol. 12, no. 6, pp. 2706-2716, June 2013.

[9] Q. Ye, O. Bursalioglu, H. Papadopoulo, C. Caramanis, and J. Andrews, "User Association and Interference Management in Massive MIMO HetNets," avaiable online at http://arxiv.org/abs/1509.07594.

[10] G. Yu, Y. Jiang, L. Xu, and G. Li, "Multi-Objective Energy-Efficient Resource Allocation for Multi-RAT Heterogenous Networks," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 10, pp. 2118-2127, Oct. 2015.

[11] M. Cheung, J. Huang, "DAWN: Delay-Aware Wi-Fi Offloading and Network Selection," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 6, pp. 1214-1223, June 2015.

[12] H. Yu, M. Cheung, L. Huang, and J. Huang, "Power-Delay Tradeoff with Predictive Scheduling in Integrated Cellular and Wi-Fi Networks, *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 4, pp. 735-742, April 2016

[13] K. Lee, I. Rhee, J. Lee, S. Chong, and Y. Yi, "Mobile Data Offloading: How Much Can WiFi Deilver," in *Proc. of ACM CoNEXT'2010*.

[14] S. Dimatteo, P. Hui, B. Han, and V. Li, "Cellular Traffic Offloading through WiFi Networks," in *Proc. of IEEE MASS'2011*.

[15] X. Zhuo, W. Gao, G. Cao, and S. Hua, "An Incentive Framework for Cellular Traffic Offloading," *IEEE Transactions on Mobile Computing*, vol. 13, no. 3, pp. 541-555, March 2014.

[16] L. Gao, G. Iosifidis, J. Huang, L. Tassiulas, and D. Li, "Bargaining-based Mobile Data Offloading," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, pp. 1114-1125, June 2014.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2016.2611979, IEEE Journal on Selected Areas in Communications

$$t_{\text{root}}^{+}=\frac{n_E g_{iB} W_B+\sqrt{(n_E g_{iB} W_B)^2+4(1-\epsilon_i) n_B n_E \hat{g}_{iA} g_{iB} W_A W_B 2^{\frac{R_i^{\text{req}}}{(1-\epsilon_i)W_A}}(1-K)}}{2(1-\epsilon_i) n_B W_A 2^{\frac{R_i^{\text{req}}}{(1-\epsilon_i)W_A}}}. \tag{49}$$

$$\theta_{iA}\leq\theta_{iA}^{\text{thre,F}}=K\hat{g}_{iA}-\frac{n_E g_{iB} W_B+\sqrt{(n_E g_{iB} W_B)^2+4(1-\epsilon_i) n_B n_E \hat{g}_{iA} g_{iB} W_A W_B 2^{\frac{R_i^{\text{req}}}{(1-\epsilon_i)W_A}}(1-K)}}{2(1-\epsilon_i) n_B W_A 2^{\frac{R_i^{\text{req}}}{(1-\epsilon_i)W_A}}}. \tag{50}$$

[17] L. Al-Kanj, V. Poor, and Z. Dawy, "Optimal cellular offloading via device-to-device communication networks with fairness constraints," *IEEE Transactions on Wireless Communications*, vol. 13, no. 8, pp. 4628-4643, Aug. 2014.

[18] Y. Wu, J. Chen, L. Qian, J. Huang, and X. Shen, "Energy-Aware Cooperative Traffic Offloading via Device-to-Device Cooperations: An Analytical Approach," *IEEE Transactions on Mobile Computing*, available at http://dx.doi.org/10.1109/TMC.2016.2539950.

[19] C. Ho, D. Yuan, and S. Sun, "Data Offloading in Load Coupled Networks: A Utility Maximization Framework," *IEEE Transactions on Wireless Communications*, vol. 13, no. 4, pp. 1912-1931, April 2014.

[20] X. Chen, J. Wu, Y. Cai, H. Zhang, T. Chan, "Energy-Efficiency Oriented Traffic Offloading in Wireless Networks: A Brief Survey and A Learning Approach for Heterogeneous Cellular Networks," *IEEE Journal on Selected Areas in Communs.*, vol. 33, no. 4, April 2015.

[21] J. Rao, A. Fapojuwo, "Analysis of Spectrum Efficiency and Energy Efficiency of Heterogeneous Wireless Networks With Intra-Inter-RAT Offloading," *IEEE Transactions on Vehicluar Technology*, vol. 64, no. 7, pp. 3120-3139, July 15.

[22] S. Jha, K. Sivanesan, R. Vannithamby, and A. Koc, "Dual Connectivity in LTE Small Cell Networks," in *Proc. of IEEE GLOBECOM'2014*.

[23] J. Liu. J. Liu, and H. Sun, "An Enhanced Power Control Scheme for Dual Connectivity," in *Proc. of VTC-Fall 2014*.

[24] A. Mukherjee, "Optimal Flow Bifurcation in Networks with Dual Base Station Connectivity and Non-ideal Backhaul," in *Proc. of Asilomar Conference on Signals, Systems and Computers, pp. 521-524, Nov. 2014*.

[25] A. Mukherjee, "Macro-Small Cell Grouping in Dual Connectivity LTE-B Networks with Non-ideal Backhaul," in *Proc. of ICC'2014*.

[26] Y. Wu, Y. He, L. Qian, and X. Shen, "Traffic Scheduling and Power Allocations for Mobile Data Offloading via Dual-Connectivity," in *Proc. of ICC'2016*.

[27] 3GPP R1-140455, "Physical Layer Aspects for Dual Connectivity", Qualcomm, RAN1#76, Prague, Czech Republic, 2014.

[28] O. Delgado, F. Labeau, "Uplink Load Balancing over Multipath Heterogeneous Wireless Networks," in *Proc. of VTC'2015*.

[29] Y. Zou, X. Wang, and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances and Future Trends," online available at http://arxiv.org/abs/1505.07919.

[30] A. Mukherjee, S. Fakoorian, J. Huang, and A.L. Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550-1573, 2014.

[31] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Renzo, "Safeguarding 5G Wireless Communication Networks Using Physical Layer Security," *IEEE Communications Magazine,* vol. 53, no. 4, pp. 20-27, April 2015.

[32] N. Zhang, N. Cheng, N. Lu, X. Zhang, J.W. Mark, and X. Shen, "Partner Selection and Incentive Mechanism for Physical Layer Security", *IEEE Transactions on Wireless Communications*, vol.14, no.8, pp. 4265-4276, 2015.

[33] X. Zhou, M. Makay, B. Maham, and A. Hjorungnes, "Rethinking the Secrecy Outage Formulation: A Secrue Transmission Design Perspective," *IEEE Communications Letters*, vol. 15, no. 3, pp. 302-304, March 2011.

[34] J. Yue, C. Ma, H. Yu, and W. Zhou, "Secrecy-based Access Control for Device-to-Device Communication Underlaying Cellular Networks," *IEEE Communications Letters*, vol. 17, no. 11, pp. 2068-2071, Nov. 2013.

[35] X. Zhou, R. Ganti, J. Andrew, and A. Hjorungnes, "On the Throughput Cost of Physical Layer Security in Decentralized Wireless Networks," *IEEE Transactions on Wireless Communications*, vol. 10, no. 8, pp. 2764-2775, Aug. 2011.

[36] Y. Jing, J. Zhu, and Y. Zou, "Secrecy Outage Analysis of Multi-User Cellular Networks in the Face of Cochannel Interference," in *Proc. of IEEE International Conference on Cognitive Informatics & Cognitive Computing, 2015*.

[37] J. Zhu, R. Schober, and V. Bhargava, "Secure Transmission in Multicell Massive MIMO Systems," *IEEE Transactions on Wireless Communications*, vol. 13, no. 9, pp. 4766-4781, Sept. 2014.

[38] C. Lai, R. Lu, D. Zheng, H. Li, and X. Shen, "Towards Secure Large-scale Machine-to-Machine Communications in 3GPP Networks: Challenges and Solutions", *IEEE Communications Magazine*, vol.53, no.12, pp.12-19, 2015.

[39] J. Xiong, K. Jamieson, "SecureArray: Improving Wifi Security with Fine-grained Physical-layer Information," in *Proc. of Mobicom'2013*.

[40] National Instruments, "Introduction to UMTS Device Testing Transmitter and Receiver Measurements for WCDMA Devices," available online at http://download.ni.com/evaluation/rf/Introduction_to_UMTS_Device_Testing.pdf.

[41] O. Bejarano, E. Knightly, "IEEE 802.11ac: From Channelization to Multi-User MIMO," *IEEE Communs. Magazine*, vol. 51, no. 10, pp. 84-90, Oct. 2013.

[42] S. Boyd and L. Vandenberghe, "Convex Optimization," Cambridge University Press, 2004.

[43] L. Schrage, "Optimization Modeling with LINGO," LINDO Systems, Inc, 2015.

Yuan Wu (S'08-M'10-SM'16) received the Ph.D degree in Electronic and Computer Engineering from the Hong Kong University of Science and Technology, Hong Kong, in 2010. He is currently an Associate Professor in the College of Information Engineering, Zhejiang University of Technology, Hangzhou, China. During 2010-2011, he was the Postdoctoral Research Associate at the Hong Kong University of Science and Technology. During 2016-2017, he is the visiting scholar at the Broadband Communications Research (BBCR) group, Department of Electrical and Computer Engineering, University of Waterloo, Canada. His research interests focus on radio resource allocations for wireless communications and networks, and smart grid. He is the recipient of the Best Paper Award in IEEE International Conference on Communications (ICC) in 2016.

Kuanyang Guo is currently pursuing his M.S. degree in College of Information Engineering, Zhejiang University of Technology, Hangzhou, China. His research interest focuses on radio resource allocations for wireless communications and networks, and secrecy-based communications.

Jianwei Huang (S'01-M'06-SM'11-F'16) is an Associate Professor and Director of the Network Communications and Economics Lab (ncel.ie.cuhk.edu.hk), in the Department of Information Engineering at the Chinese University of Hong Kong. He is the co-recipient of 8 international Best Paper Awards, including IEEE Marconi Prize Paper Award in Wireless Communications in 2011. He has co-authored five books and six ESI highly cited papers. He has served as an Associate Editor of IEEE Transactions on Cognitive Communications and Networking, IEEE Transactions on Wireless Communications, and IEEE Journal on Selected Areas in Communications - Cognitive Radio Series. He is the Vice Chair of IEEE ComSoc Cognitive Network Technical Committee and the Past Chair of IEEE ComSoc Multimedia Communications Technical Committee. He is a Fellow of the IEEE and a Distinguished Lecturer of IEEE Communications Society.

Xuemin (Sherman) Shen (M'97-SM'02-F'09) is a Professor and University Research Chair, Department of Electrical and Computer Engineering, University of Waterloo, Canada. His research focuses on resource management, wireless network security, social networks, smart grid, and vehicular ad hoc networks. He is an elected member of IEEE ComSoc Board of Governor, and the Chair of Distinguished Lecturers Selection Committee. Dr. Shen served as the Technical Program Committee Chair/Co-Chair for IEEE Globecom16, Infocom14, IEEE VTC10 Fall, and Globecom07, the Symposia Chair for IEEE ICC10, the Tutorial Chair for IEEE VTC'11 Spring and IEEE ICC08, the General Co-Chair for ACM Mobihoc15, the Chair for IEEE Communications Society Technical Committee on Wireless Communications. He also served/serves as the Editor-in-Chief for IEEE Network, Peer-to-Peer Networking and Application, and IET Communications; a Founding Area Editor for IEEE Transactions on Wireless Communications. Dr. Shen received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award from the University of Waterloo, and the Premiers Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada. Dr. Shen is a registered Professional Engineer of Ontario, Canada, a Fellow of IEEE, Engineering Institute of Canada, Canadian Academy of Engineering, and Royal Society of Canada, and a Distinguished Lecturer of IEEE Vehicular Technology Society and Communications Society.