On Achieving High PHY-Layer Security of D2D-Enabled Heterogeneous Networks

Chun-Hung Liu*, Di-Chun Liang† and Rung-Hung Gau†
Department of Electrical and Computer Engineering, Mississippi State University, USA*
Institute of Communications Engineering, National Chiao Tung University, Hsinchu, Taiwan†
E-mail: chliu@ece.msstate.edu, ldc.cm02g@nctu.edu.tw and runghunggau@g2.nctu.edu.tw

Abstract—This paper aims to study how to achieve high transmission security in the physical (PHY) layer of a multi-tier heterogeneous network (HetNet) through a simple device-to-device (D2D) enabling scheme. For the HetNet, we propose a simple D2D-enabling scheme with low complexity for users to opportunistically enable their D2D mode and become either D2D or cellular users by exploiting the diversity of all user association signals from all base stations (BSs). To evaluate whether the proposed D2D enabling scheme improves the PHY-layer security of the HetNet, the secrecy outage probability of the HetNet is defined and analyzed from two different perspectives of BSs and users. We define the BS-centric and user-centric security outage events and derive the explicit lower bound on their probability when the proposed D2D enabling scheme is adopted. Our analytical and numerical results not only show that the proposed D2D-enabling scheme can achieve high PHY-layer security but also reveal how densely the BSs should be deployed in the HetNet in order to achieve the high PHY-layer security from the perspectives of BSs and users.

I. INTRODUCTION

In a cellular network, using (in-band) device-to-device (D2D) communication as an underlay has a few advantages. One typical advantage, for example, is to reduce the traffic load of base stations (BSs) and improve the efficiency of radio resource use at BSs since D2D communication can take care of the traffic in the vicinity of BSs [1]. Another typical advantage is to increase the spectral efficiency and thus improve physical (PHY) layer security in the cellular network by properly reusing the limited radio resources and managing interferences. However, users who arbitrarily enable their D2D mode for directly transmitting to their nearby intended receivers may seriously interfere their nearby unintended receivers, such as cellular users and BSs. Hence, a sound and efficient D2D management in a cellular network, including D2D-enabling control and device discovery, is needed because it is the key to thoroughly exploiting the advantages of D2D communication in cellular networks [2]. For a heterogeneous cellular network (HetNet) consisting of different types of BSs, the D2D management in such a HetNet is usually fairly complicate in that different types of BSs have distinct hardware capabilities and they thus need different D2D management plans to help their users enable their D2D mode appropriately.

An efficient method to reduce the complexity of the D2D management in a HetNet is to let users in the cell coverage of a BS autonomously decide when to enable their D2D mode for direct transmission, which means each user is suggested to first do device discovery and then evaluate whether enabling D2D communication benefits its own transmission in terms of data rate, energy consumption, or security risk, etc., according to its device discovery result. Such a method is able to let the users with the capability of enabling D2D transmission not join the HetNet to compete cellular resources with other non-D2D users so that BSs can reduce their system operating complexity and load in D2D management. To make users enable their D2D mode autonomously and properly, they must adopt a good D2D-enabling scheme that is able to accurately evaluate whether performing direct transmission to their desired receivers is possible with their own capability. In the prior works on D2D communication underlaid in a HetNet, how to enable the D2D mode of users so as to maximize the transmission security performances in a HetNet is not addressed much. Whereas this is an important problem because improperly activating D2D transmission significantly impacts the capacities of all wireless links and it could thus jeopardize the PHY-layer security of users and BSs from the information-theoretic point of view [3] [4]. To the best of our knowledge, the fundamental interplay between D2D enabling and PHY-layer security in a HetNet has not been studied in the literature.

Prior works on PHY-layer security and D2D communication in a cellular network mainly focused on how to improve the PHY-layer security in the network by adopting interference management means, such as power control, media access control, artificial noise, and scheduling, etc. (typically see [5]–[8]). Reference [7], for instance, investigated how to generate artificial noise so as to enhance the PHY-layer security in multi-antenna small-cell networks without D2D-enabled communications. In [6], the authors studied how to utilize the interferences generated by D2D communication as artificial noise that only affects eavesdroppers and how to schedule D2D links to achieve this effect. How to maximize the secrecy rate by jointly doing power control and access control in D2D-underlaid cellular networks was studied in [5]. None of these prior works look into when is a good opportunity for users to enable D2D communication in order to achieve high PHY-layer security in cellular networks even though they claim to improve the security based on their proposed approaches that may be complex and/or difficult to be implemented in practice.

In this paper, our focus is on how to improve the PHY-layer security of BSs and D2D users through a simple and opportunistic D2D enabling scheme. We propose a D2D-
enabling scheme of a user that compares all biased signal powers from its desired D2D transmitter and all BSs in a HetNet with \( M \) tiers, and its D2D mode enables when the strongest biased signal power is from its desired D2D transmitter. The users who do not enable their D2D mode are called cellular users and they adopt a generalized user association scheme to select their serving BS. To evaluate the security performance of the proposed D2D-enable scheme, we propose two security performance metrics: one is the BS-centric secrecy outage probability and the other is the user-centric secrecy outage probability. The BS-centric secrecy outage probability characterizes how securely a BS in each tier transmits to the best user it selects among all users in the entire network, whereas the user-centric secrecy outage probability reveals how securely a cellular user is receiving data from its tagged BS. The lower bounds on the BS-centric and user-centric secrecy outage probabilities are found and analyzed, respectively. Their analytical and numerical results demonstrate that the proposed D2D-enabling scheme is able to significantly improve the proposed two security performance metrics by optimally designing the parameters in the D2D-enabling scheme.

II. SYSTEM MODEL AND PRELIMINARIES

In this paper, we consider a large-scale and interference-limited HetNet on the \( \mathbb{R}^2 \) plane where there are \( M \) different types of base stations (BSs) (e.g., macrocells, microcells, picocells, etc.) and each type of BSs is referred as a tier in the HetNet. Specifically, all the BSs in the \( m \)-th tier form an independent homogeneous Poisson point process (PPP) of intensity \( \lambda_m \), and they can be explicitly written as a set \( \Phi_m \) given by

\[
\Phi_m \doteq \{ X_{m,i} \in \mathbb{R}^2 : i \in \mathbb{N}_+ \}, \tag{1}
\]

where \( m \in \mathcal{M} \doteq \{ 1, 2, \ldots, M \} \) and \( X_{m,i} \) denotes BS \( i \) in the \( m \)-th tier and its location. Also, all (receiving) users in the HetNet form an independent and marked homogeneous PPP \( \mathcal{U} \) of intensity \( \mu \) given by

\[
\mathcal{U} \doteq \{ (U_j \in \mathbb{R}^2, D_j \in \{ 0, 1 \}) : j \in \mathbb{N}_+ \}, \tag{2}
\]

where \( U_j \) denotes user \( j \) and its location, \( D_j \) is a Bernoulli random variable (RV) which is unity if \( U_j \) is a device-to-device (D2D) receiver and zero if \( U_j \) is a cellular user. All \( D_j \)'s are assumed to be i.i.d. throughout this paper. In this HetNet, we consider the downlink scenario and assume that each user has a sole associated D2D transmitter and it can directly receive the information from its associated transmitter if its D2D mode enables. For the users enabling their D2D mode, they are called D2D receivers whereas others are called the cellular users\(^1\). Each user in \( \mathcal{U} \) independently decides to enable its D2D mode so that the D2D receivers form a thinning independent PPP from \( \mathcal{U} \) and they can be denoted by set \( \mathcal{U}^d \subseteq \mathcal{U} \) defined as

\[
\mathcal{U}^d \doteq \{ U_j^d \in \mathcal{U} : D_j = 1, j \in \mathbb{N}_+ \} \tag{3}
\]

and the intensity of \( \mathcal{U}^d \) is \( \mu_d = \mu \mathbb{P}[D_j = 1] \) for all \( j \in \mathbb{N}_+ \). In other words, the cellular users are also a thinning PPP from \( \mathcal{U} \), and they are denoted by set \( \mathcal{U}^c \subseteq \mathcal{U} \) given by

\[
\mathcal{U}^c \doteq \{ U_j^c \in \mathcal{U} : D_j = 0, j \in \mathbb{N}_+ \} \tag{4}
\]

whose intensity is \( \mu_c = \mu \mathbb{P}[D_j = 0] \). Hence, \( \mathcal{U}^d \cap \mathcal{U}^c = \emptyset \) and \( \mathcal{U}^d \cup \mathcal{U}^c = \mathcal{U} \). Moreover, we consider that the locations of all eavesdroppers in the HetNet also can be described by an independent homogeneous PPP \( \mathcal{U}^e \) of intensity \( \mu_e \) and the eavesdroppers intend to wiretap a BS of interest. All BSs in the \( m \)-th tier are equipped with \( N_m \) antenna, whereas all users and eavesdroppers are equipped with a single antenna.

A. D2D-Mode Enabling and User Association

We consider in-band D2D communication as an underlay to this HetNet \([1]\) and user \( U_j \in \mathcal{U} \) adopts the following scheme to enable its D2D mode:

\[
D_j = \mathbb{I} \left( \sup_{m,i \in \Phi_m} \frac{\omega_m}{\|X_{m,i} - U_j\|^\alpha} < \theta_d \right), \tag{5}
\]

where \( \mathbb{I}(\mathcal{A}) \) is an indicator function that is unity if the event \( \mathcal{A} \) is true and zero otherwise, \( \Phi \doteq \bigcup_{m=1}^M \Phi_m \) denotes the entire set of all BSs in the HetNet, \( \omega_m \in \mathbb{R}_+ \) is called the user association bias of the tier-\( m \) BSs, \( \|Y_i - Y_j\| \) denotes the Euclidean distance between nodes \( Y_i \) and \( Y_j \) for \( i \neq j \), \( \alpha > 2 \) is the path-loss exponent, and \( \theta_d \geq 0 \) is the threshold of enabling the D2D mode of users. Note that \( \omega_m \|X_{m,i} - U_j\|^{-\alpha} \) pertains to the user association signal power from BS \( X_{m,i} \).
and thus a user will enable its D2D transmission mode if all user association signal powers received by it are smaller than $\theta_d$. The D2D enabling scheme in (5) is able to thoroughly exploit the channel gain diversity among all transmitters (all BSs as well as a D2D transmitter) in the HetNet. In other words, it helps users determine when to enable their D2D mode. To the best of our knowledge, such a D2D-enabling scheme in (5) that benefits the quality of the desired signal of all users has never been proposed and studied in the literature. An illustrative example of a single-tier cellular network using the scheme in (5) is shown in Fig. 1.

For the D2D-enabling scheme in (5), the probability that a user becomes a D2D receiver is shown in the following lemma.

**Lemma 1.** According to (5) with constant threshold $\theta_d$, the probability that a user enables its D2D mode is $p_d = P[D_j = 1]$ for all $j \in \mathbb{N}_+$, which can be explicitly found as

$$p_d = \exp \left(-\pi \theta_d^{-\eta} \sum_{m=1}^{M} \omega_m^{\eta} \lambda_m \right),$$

where $\eta = \frac{2}{\alpha}$ and $\eta \in (0,1)$ due to $\alpha > 2$.

**Proof:** Using Theorem 1 in [9] with the user association function defined in (7), the probability in (6) can be found readily.

This lemma indicates that the intensity of all the D2D receivers is $\mu_d \triangleq \mu p_d$ whereas the intensity of all the cellular users is $\mu_c \triangleq \mu (1 - p_d)$ so that controlling all $\omega_m$’s and adjusting $\theta_d$ give rise to traffic loading/offloading between cellular and D2D networks. Specifically, cellular user $U_c$ adopts the following user association scheme to select its BS:

$$X_j^* \triangleq \arg \sup_{m,i: X_m,i \in \Phi} \frac{\omega_m}{\|X_m,i - U_c^j\|^{\alpha}},$$

where $X_j^*$ represents the BS associated with user $U_c^j$. This scheme covers a few user association schemes by varying the bias $\omega_m$, such as nearest BS association (NBA) if $\omega_m = 1$ for all $m \in M$ and maximum (mean) received power association (MRPA) if $\omega_m = P_m$ for all $m \in M$. The scheme in (7) could lead to void BSs that are not associated with any users, as shown in Fig. 1.

**B. Laplace Transform, Interference Model and Their Related Statistical Properties**

In this subsection, the Laplace transform result of the received signal power at any point in the HetNet will be first studied, which plays a pivotal role in deriving some performance metrics in the following. For any point $O_k$ in the HetNet, the total signal power received by a receiver located at $O_k$ is given by

$$I_k = \sum_{m,i: X_m,i \in \Phi} \frac{V_{m,i}}{\|X_{m,i} - O_k\|^{\alpha}} + I_{d,k}^{\prime} + \sum_{j \in \mathbb{N}_+} \frac{T_{d,j}^{\prime} Q}{\|U_j^{\prime} - O_k\|^{\alpha}},$$

where $I_{d,j}^{\prime}$ is the signal power from all non-void (active) BSs which are associated by at least one cellular user, $P_m$ is the transmit power of the tier-$m$ BSs, $I_{d,j}^{\prime}$ is the signal power from all D2D transmitters, and $Q$ denotes the transmit power of each D2D transmitter. Also, $V_{m,i} \in \{0,1\}$ is a Bernoulli RV that is unity if BS $X_{m,i}$ is not void and zero otherwise, $h_{m,j}$ denotes the fading channel gain between nodes $X_{m,i}$ and $O_j$, and $T_{d,j}^{\prime} \in \{0,1\}$ is also a Bernoulli RV that is unity if $U_j^{\prime}$ is transmitting and zero otherwise. Note that the superscript $r \in \{c,d\}$ of $I_j$ is used to indicate which type of the receiver (such eavesdropper, cellular user or D2D receiver) located at point $O_j$. For example, if an eavesdropper is located at $O_j$, then its total received power is denoted by $I_j^e$. According to Lemma 1 in our previous work [10] and the intensity of the cellular users, the tier-$m$ non-void probability that a tier-$m$ BS is associated with at least one cellular user, i.e., $\rho_m \triangleq 1 - P[V_{m,i} = 0]$, is

$$\rho_m = 1 - \left(1 + \frac{\mu_c}{\mu_{d,m}}\right)^{-\zeta_m},$$

where $\lambda_m \triangleq \sum_{k=1}^{M} \lambda_k \omega_k^{\eta} / \omega_m^{\eta}$ and $\zeta_m \triangleq \frac{2}{\alpha}$. The distribution of $T_{d,j}^{\prime}$ depends on the transmission scheduling policy of the D2D transmitter associated with receiver $U_j^{\prime}$. We define the transmission probability of the D2D transmitters is $p_d \triangleq P[T_{d,j}^{\prime} = 1]$ for all $j \in \mathbb{N}_+$.

Let $L_Z(s) \triangleq \mathbb{E}[\exp(-s Z)]$ denote the Laplace transform of a positive RV $Z$ for $s > 0$. Some useful statistical properties of $I_j$ pertaining to $L_I(s)$ are summarized in the following theorem.

**Theorem 1.** The Laplace transform of $I_j$ can be found as

$$L_I(s) = \exp \left(-\lambda_{\Sigma} \sinh(\eta s) / \sin(\eta s) \right),$$

where $\lambda_{\Sigma} \triangleq \sum_{m=1}^{M} \rho_m \lambda_m P_m + \rho_d \mu_d Q$ and $\sin(\eta) \triangleq \pi \lambda_{\Sigma} / \sinh(\eta s)$. This leads to the CDF of $I_j$ for all $j \in \mathbb{N}_+$ found, as shown in the following:

$$F_{I,j}(x) = L_{-1}\left\{1 - \exp \left(-\lambda_{\Sigma}s \sin(\eta s) \right) / \sin(\eta s) \right\}(x),$$

where $L_{-1}\{\cdot\}(\cdot)$ denotes the operator of the inverse Laplace transform.

**Proof:** See Appendix A.

As can be seen in the sequel, Theorem 1 is very useful in deriving the statistical properties of the SIRs of eavesdroppers, D2D and cellular users.

**III. SECRECY OUTAGE ANALYSIS**

In this section, our focus is on the study of the secrecy outage probability in the scenario that all D2D transmitters always have data to transmit in every time slot and they do not adopt any scheduling policy, i.e., $T_{d,j}^{\prime} \equiv 1$ in (8) for all $j \in \mathbb{N}_+$. First, the SIR models of the eavesdroppers and cellular users are introduced, and we then study their distributions. The SIR models proposed in this section are different from those in many prior works (typically see [11], [12]) because they consider the coupled impacts of D2D transmission and
user association. Afterwards, we will define the secrecy outage event of a tier-m BS in accordance with the proposed SIR models and investigate the tier-m secrecy outage probability and the user-centric secrecy outage probability.

A. The SIR Analysis of Eavesdroppers and Cellular Users

In this subsection, first we introduce the SIR model from a BS to an eavesdropper and then study the distribution of the largest SIR among eavesdroppers. Consider the channel from BS $X_{m,i}$ to eavesdropper $U_j^e$ and the SIR received by $U_j^e$ can be written as

$$
\gamma_{m,i,j}^e \triangleq \frac{S_{m,i,j}^e}{I_j^e - S_{m,i,j}^e},
$$

(12)

where $S_{m,i,j}^e \triangleq P_{m} h_{m,i,j}^e \|X_{m,i} - U_j^e\|^{-\alpha}$ denotes the signal power from BS $X_{m,i}$, and $I_j^e - S_{m,i,j}^e$ is the interference received by $U_j^e$ where $I_j^e$ is equal to (8) evaluated at point $U_j^e$. Let $F_j^e(\xi) \triangleq \mathbb{P}[Z \geq \xi]$ denote the complementary cumulative density function (CCDF) of RV $Z$ and we can have the following theorem.

**Theorem 2.** According to $\gamma_{m,i,j}^e$ in (12), its supreme value is defined by $\gamma_{m,i,j}^e \triangleq \sup_{U_j^e \in \Phi_{m}} \gamma_{m,i,j}$; If all fading channel gains in (12) are i.i.d. exponential RVs with unit mean, a lower bound on $F_{m,i,j}^e(\xi)$ can be explicitly found as

$$
F_{m,i,j}^e(\xi) \geq 1 - \exp\left(-\frac{C_{m,i}^e}{\lambda_{m}} \left(\frac{P_{m}}{\xi}\right)^{\eta} \sin(\eta)\right).
$$

(13)

**Proof:** See Appendix B.

According to (13), we realize that the distribution of $\gamma_{m,i,j}^e$ is dominated by the term $\mu_{e} P_{m}/\xi^{\alpha} \lambda_{m}$ and we can show that $F_{m,i,j}^e(\xi) = \Theta(\mu_{e} P_{m}/\xi^{\alpha} \lambda_{m})$ as $\xi \to \infty$, which means that for a large $\xi$ we need to reduce transmit power and/or deploy more BSs in order to reduce $F_{m,i,j}^e(\xi)$ whereas decreasing $\mu_{e}/\lambda_{m}$ is more efficient than decreasing $P_{m}$ in reducing $F_{m,i,j}^e(\xi)$.

Next, we study the distribution of the SIR from a BS to its cellular user. Suppose cellular user $U_j^c$ adopts the user association scheme in (7) to associate with BS $X_{m,i}^c$. The SIR of user $U_j^c$ can be expressed as

$$
\gamma_{j}^c \triangleq \frac{S_{j}^c}{I_j^c - S_{j}^c}, \quad j \in \mathbb{N}_+
$$

(14)

where $S_{j}^c \triangleq \sum_{m=1}^{M} P_{m} H_{m,j} \|X_{j}^c - U_j^c\|^{-\alpha} 1(X_{j}^c \in \Phi_{m})$ stands for the desired signal power from BS $X_{j}^c$ and $I_j^c$ is equal to (8) evaluated at $U_j^c$. The CCDF of $\gamma_{j}^c$ in (14) can be found in the following theorem.

**Theorem 3.** Suppose each BS can do transmit beamforming to their cellular users so that the channel gain $H_{m,i}$ in (14) is a Chi-squared RV with $2N_{m} \lambda_{m}$ degrees of freedom. If all nonvoid tier-\(m\) BSs are viewed as a homogeneous PPP of intensity $\rho_{m} \lambda_{m}$ for all $m \in \Lambda$, the CCDF of $\gamma_{j}^c$ in (14) has an explicit result for all $j \in \mathbb{N}_+$ given by

$$
F_{j}^c(\xi) = \sum_{m=1}^{M} \theta_{m} \left(\sum_{n=0}^{\infty} \frac{(-\xi)^n}{n!} \lambda_{m}^{(n)} \gamma_{j}^c(\xi)\right),
$$

(15)

where $\lambda_{m}^{(n)} \triangleq \frac{d^n}{d\xi^n} \left. L_{m,\theta_{m}}(\xi) \right|_{\theta_{m}}$ and $L_{m,\theta_{m}}(\xi)$ is shown in (16).

$$
L_{m,\theta_{m}}(\xi) = 1 - \exp\left(-\pi \lambda_{m} \theta_{m}^{-\alpha} A_m(\xi)\right),
$$

(16)

where $\lambda = \sum_{k=1}^{M} \mu_{m,k}^{\eta} \lambda_{m,k}$, $A_m(\xi) = 1 + \sum_{k=1}^{M} \mu_{m,k} \theta_{m,k} e^{x_{m,k}(\xi) + \xi_{m,k}(\xi) - \alpha}$, and $\xi_{m,k}(\xi) \triangleq \frac{\alpha}{\alpha - 1} \left(\frac{\xi_{m,k}}{\alpha_{m,k}}\right)^{\alpha - 1}$.

**Proof:** See Appendix C.

The physical meaning of $F_{j}^c(\xi)$ in (15) can be interpreted as the user-centric coverage probability of a cellular user in the D2D-enabled HetNet with the SIR threshold $\xi$ and the D2D-enabled threshold $\theta_{m}$. The salient feature of $F_{j}^c(\xi)$ in (15) is that it captures the effects from user association as well as D2D-enabled transmission so that we are able to clarify which parameters of the D2D-enabled scheme in (5) and the user association scheme in (7) could significantly affect $F_{j}^c(\xi)$ for the various values of $\xi$. The results in Theorems 2 and 3 will assist us to analyze the secrecy outage probabilities of a tier-\(m\) BS and a cellular user in the following two subsections.

B. Secrecy Outage Analysis of the Tier-\(m\) BSs

In this subsection, we would like to investigate the secrecy outage probability of a BS from an information-theoretic point of view that is characterized by the channel capacities from a BS to an eavesdropper and a cellular user, as suggested in the works of Wyner’s wiretap channel in [3] and the Gaussian wiretap channel in [4]. Let the capacity of a wiretap channel from BS $X_{m,i}$ to an eavesdropper $U_j^e$ be defined as

$$
C_{m,i,j}^e \triangleq \log(1 + \gamma_{m,i,j}^e),
$$

(17)

where $\gamma_{m,i,j}^e$ is defined in (12), and the capacity of a legitimate link from BS $X_{m,i}$ to user $U_j^c$ be defined as

$$
C_{m,i,j}^c \triangleq \log(1 + \gamma_{m,i,j}^c),
$$

(18)

where $\gamma_{m,i,j}^c$ is defined similar to (14) by replacing $X_{j}^c$ with $X_{m,i}$. Then the secrecy capacity of the channel from BS $X_{m,i}$ to user $U_j^c$ can be defined as

$$
C_{m,i,j}^s \triangleq \left[C_{m,i,j}^c - C_{m,i,j}^e\right]^+,
$$

(19)

where $C_{m,i,j}^e \triangleq \sup_{U_j^e \in \Phi_{m}} \{C_{m,i,j}^e\} = \log(1 + \gamma_{m,i,j}^e)$ with $\gamma_{m,i,j}^e$ given in (13) and $[x]^+ \triangleq \max(x, 0)$. The way of defining $C_{m,i,j}^s$ in (19) is to characterize the secrecy capacity of the link between $X_{m,i}$ and $U_j^c$ in the worse case, and the event of $C_{m,i,j}^s > 0$ corresponds to the “perfect secrecy” event in which no eavesdropper can successfully wiretap the legitimate link from $X_{m,i}$ to $U_j^c$. By the same reasoning, we define the secrecy outage probability of a tier-\(m\) BS as follows

$$
\varepsilon_{m} \triangleq \mathbb{P}\left[\inf_{U_j^e \in \Phi_{m}} C_{m,i,j}^s = 0\right],
$$

(20)

where event $\inf_{U_j^e \in \Phi_{m}} C_{m,i,j}^s = 0$ represents the situation whereby all downlink channels of $X_{m,i}$ are not perfectly
secure because there exists at least one channel of $X_{m,i}$, which is successfully wiretapped by eavesdroppers. To the best of our knowledge, $\varepsilon_m$ was never proposed in the literature and it is called the tier-$m$ secrecy outage probability in the following. For the case that a BS transmits to its cellular user with a constant data rate, the tier-$m$ secrecy outage probability in (20) reduces to

$$\varepsilon_m = 1 - P\left[R_m > C_{m,*}^e\right] = F_{m,*}^\dagger\left(e^{R_m - 1}\right),$$  \hspace{1cm} (21)

where $R_m$ is the constant transmission rate of a tier-$m$ BS. $\varepsilon_m$ in (21) can be explicitly found by using the CCDF of $\gamma_{m,*}$ in Theorem 2 for $\xi = e^{R_m - 1}$, i.e.,

$$\varepsilon_m \geq 1 - \exp\left[-\frac{\mu_e}{\lambda_\Sigma} \left(\frac{P_m}{e^{R_m - 1}}\right)^\eta \text{sinc}(\eta)\right],$$  \hspace{1cm} (22)

which clearly indicates that the term $\mu_e/\lambda_\Sigma \left(P_m/e^{R_m - 1}\right)^\eta$ has to be small in order to achieve high PHY-layer security. Accordingly, we can further study how to optimize the parameters in $\omega_m$ and $\theta_d$ so as to maximize $\lambda_\Sigma$ for given $\mu_e$, $P_m$, and $R_m$ which cannot be changed in general.

C. Secrecy Outage Analysis of Cellular Users

The tier-$m$ secrecy outage probability found in the previous subsection can be viewed as a security metric that evaluates how secure a tier-$m$ BS is transmitting, but it may not realistically indicates how secure a cellular user is receiving no matter it associates with a BS in which tier. As a result, we need to study the user-centric secrecy outage probability that is a security metric of evaluating how likely a cellular user encounters a wiretapping threat in a HetNet. To do so, we first need to define the secrecy capacity of the channel from BS $X_j^*$ to a cellular user $U_j^e$ as $C_j^{se} = [C_j^s - C_j^{se}]^+$, $\forall j \in \mathbb{N}_+$ in which $C_j^s \triangleq \log\left(1 + \gamma_j^s\right)$ and $C_j^{se} \triangleq \sum_{m=1}^M 1(X_j^m \in \Phi_m) \log\left(1 + \gamma_j^{m,*}\right)$ are the capacity of the link from $X_j^m$ to $U_j$ and the capacity of the link from $X_j^m$ to $U_j^e$, respectively. By using $C_j^{se}$ and following the same way to defining the tier-$m$ outage secrecy probability in the previous subsection, the secrecy outage probability of a cellular user can be defined as

$$\varepsilon \triangleq P\left[C_j^{se} = 0\right] = 1 - P\left[C_j^s > C_j^{se}\right], \quad \forall j \in \mathbb{N}_+. \hspace{1cm} (23)$$

In the following, we call $\varepsilon$ the user-centric secrecy outage probability and its explicit lower bound is shown in the following theorem.

**Theorem 4.** If all cellular users adopt the user association scheme in (7) to associate with their BS and all non-void BSs are assumed to be independently distributed, the user-centric secrecy outage probability in (23) can be found as

$$\varepsilon \geq 1 - \sum_{m=1}^M \partial_m \int_0^{\infty} F_{m,*}^\dagger\left(\frac{\psi_m^e}{P_m}\right)^{1/\eta} \exp\left(\frac{x}{\exp(x)}\right) dx \hspace{1cm} (24)$$

where $\psi_m^e \triangleq \frac{\mu_e}{\lambda_\Sigma} \text{sinc}(\eta)P_m^\dagger$ and $F_{m,*}^\dagger(\cdot)$ is given in (15) and $\partial_m \triangleq \omega_m^\phi \lambda_m / \sum_{k=1}^M \omega_k \lambda_k$ is the probability that a cellular user associates with a tier-$m$ BS.

**Proof:** The user-centric secrecy outage probability in (23) can be explicitly rewritten as follows

$$\varepsilon = 1 - \sum_{m=1}^M \partial_m \int_0^{\infty} F_{m,*}^\dagger\left(\frac{\psi_m^e}{P_m}\right) f_{\gamma_m,*}^e(\xi) \xi d\xi .$$

According to the bounds in (13), we can find the bounds on the CDF of $\psi_m^e$ and deduce the following bound:

$$f_{\gamma_m,*}^e(\xi) \leq \frac{\eta\psi_m^e P_m^\dagger(\xi)}{\xi^{1+\eta} \exp(\psi_m^e \xi^- \eta)}.$$ 

Using the bound on $f_{\gamma_m,*}^e(\xi)$, we can have

$$\varepsilon \geq 1 - \sum_{m=1}^M \partial_m \int_0^{\infty} \frac{\eta\psi_m^e P_m^\dagger(\xi)}{\xi^{1+\eta} \exp(\psi_m^e \xi^- \eta)} d\xi ,$$

which is exactly the result in (24) after doing the variable change of $x = \psi_m^e \xi^{-\eta}$ in the integral.

The result in (24) reveals that the user-centric secrecy outage probability is fundamentally dominated by $\left(\psi_m^e\right)^{1/\eta} = \left[\frac{\mu_e}{\lambda_\Sigma} \text{sinc}(\eta)\right]^{1/\eta} P_m^\dagger$. To achieve high PHY-layer security for a cellular user, we thus have to reduce $\mu_e/\lambda_\Sigma$, which can be achieved by designing the parameters (such as $\omega_m$ and $\theta_d$) in $\lambda_\Sigma$ to maximize $\lambda_\Sigma$ assuming $P_m$ and $\mu_e$ cannot be changed, which is similar to the case of achieving high PHY-layer security for a tier-$m$ BS. We will provide some numerical results to support our observation for achieving high PHY-layer security here.

IV. NUMERICAL RESULTS

In this section, some numerical results are provided to validate the analyses of the tier-$m$ BS and user-centric secrecy outage in the previous section. We consider a two-tier HetNet composed of one tier of macrocell BSs and one tier of picocell BSs. In this HetNet, all cellular users adopt the MRPA scheme to associate with their BS, i.e., $\omega_m = P_m$. The network parameters for the simulation are listed in Table I. The simulation results for the tier-$m$ secrecy outage probability with SIR threshold $\xi = e^{R_m - 1}$ are shown in Fig. 2. As can be seen in the figure, $\varepsilon_m$ reduces as more and more picocell BSs are deployed and this is because deploying more BSs induces more interferences that make eavesdroppers have a lower SIR. Moreover, the lower bounds on the tier-1 and tier-2 secrecy outage probabilities (i.e., the result in (22)) are fairly close to their corresponding simulated results. Thus, we can say that the bound found in (22) is in general very accurate and tight. Obviously, we can see that the D2D-enabling scheme in (5) indeed can improve the PHY-layer security of BSs in the both tiers in the region when $\lambda_2/\mu$ is not too high. For the regime of high values of $\lambda_2/\mu$, the D2D-enabling scheme does not perform well and this is because deploying more picocell BSs makes more users become cellular users so that cellular users are getting closer to the picocells and the downlink SIR from a picocell BS is getting stronger. This indicates that it is better for users to adaptively enable their D2D mode based on the BS intensity in the HetNet in order to help BSs achieve high PHY-layer security. Note that the security performance of the picocell BSs is much higher than that of the macro BSs and this is due to the high transmit power of the macro BSs.
we need to deploy more BSs to improve the security of users.

probability is larger than the tier-

associate with it. Hence, when the user-centric secrecy outage

the best user for a BS transmitting in the downlink may not

security evaluated in Fig. 2 in general cannot be achieved since

by user-centric D2D enabling and BS association whereas the

the security evaluated in Fig. 3 can be realistically achieved

that the numerical results in Fig. 3 are all much smaller than

realize that the D2D-enabling scheme always benefits the

users as well. By comparing Fig. 2 with Fig. 3, we can

enabling scheme can largely improve the PHY-layer security

ences generated by more and more picocell BSs deployed.

this, as mentioned above, is due to more and more interfer-

user-centric outage probability reduces as

and thus the macro BSs should offload their security-sensitive

traffic to the picocell BSs and/or the D2D network.

The simulation results of the user-centric secrecy outage

probability are presented in Fig. 3. Likewise, we can see the

user-centric outage probability reduces as $\lambda_m / \mu$ increases and this, as mentioned above, is due to more and more interfer-

ences generated by more and more picocell BSs deployed. Most importantly, Fig. 3 validates that the proposed D2D-

enabling scheme can largely improve the PHY-layer security

of users as well. By comparing Fig. 2 with Fig. 3, we can realize that the D2D-enabling scheme always benefits the

PHY-layer security of users, which is not surprised, because it is designed from the user perspective. Also, we can observe that the numerical results in Fig. 3 are all much smaller than those in Fig 2. Fig. 3, which is a good phenomenon in that the security evaluated in Fig. 3 can be realistically achieved by user-centric D2D enabling and BS association whereas the security evaluated in Fig. 2 in general cannot be achieved since the best user for a BS transmitting in the downlink may not associate with it. Hence, when the user-centric secrecy outage probability is larger than the tier-$m$ secrecy outage probability, we need to deploy more BSs to improve the security of users.

<table>
<thead>
<tr>
<th>Parameter \ BS Type</th>
<th>Macro (Tier-1)</th>
<th>Pico (Tier-2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmit Power $P_m$ (W)</td>
<td>40</td>
<td>1</td>
</tr>
<tr>
<td>Number of Antennas $N_{m;i}$</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>User Association Bias $\omega_{m;i}$</td>
<td>40</td>
<td>1</td>
</tr>
<tr>
<td>Intensity $\lambda_m$ (BSs/m$^2$)</td>
<td>$1.0 \times 10^{-6}$</td>
<td>$[0.5, 1.5] \times \mu$</td>
</tr>
<tr>
<td>User Intensity $\mu$ (users/m$^2$)</td>
<td>$1 \times 10^4$</td>
<td></td>
</tr>
<tr>
<td>Eavesdropper Intensity $\mu_e$ (Eves/m$^2$)</td>
<td>$\mu_e \times 0.05$</td>
<td></td>
</tr>
<tr>
<td>Transmission Rate $R_{m;i}$</td>
<td>$\ln(2)$</td>
<td></td>
</tr>
<tr>
<td>Path-loss Exponent $\alpha$</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>D2D Transmit Power $Q$ (W)</td>
<td>0.2</td>
<td></td>
</tr>
<tr>
<td>D2D Transmit Distance $d$ (m)</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>D2D-enabling Threshold $\theta_d$</td>
<td>$Qd^{-\alpha}$</td>
<td></td>
</tr>
</tbody>
</table>

Fig. 2. Simulation results of the tier-$m$ secrecy outage probability

Fig. 3. Simulation results of the user-centric secrecy outage probability

V. CONCLUSION

In a HetNet, analyzing the PHY-layer security is not an easy task because its performance is affected by many factors, such as user association scheme, BS deploying model and eavesdropper distribution model. This leads to the consequence in which the fundamental performance limit of the PHY-layer security in the HetNet is still not clear at all based on the current results in the literature. To delve the how securely a transmission occurring in a HetNet can attain, we propose a D2D-enabling scheme which helps users opportunistically adopt D2D transmission in the HetNet so as to improve their transmission security. We look at the secrecy outage events from the perspectives of BSs and users and then derive the lower bounds on the tier-$m$ secrecy outage probability and the user-centric secrecy outage probability. These two probabilities reveal some key clues about how to optimize the network parameters in order to achieve high transmission security, which is further verified by some numerical results.

APPENDIX

A. Proof of Theorem 1

According to Slivnyak’s theorem [13], the distribution of $I'_j$ is the same as that of $I'$ which is the total signal power received by a receiver of type $r$ located at the origin. Let $I'_j$ be written as

$$I'_j \triangleq I' = \sum_{m,i; X_{m,i} \in \Phi} \frac{V_{m,i}^n P_m h_{m,i}}{||X_{m,i}||^\alpha} + \sum_{j: U_j \in D} Qh_j^\alpha ||U_j||^\alpha,$$

where $\triangleq$ represents the equivalence in distribution. Also, according to the conservation property in Theorem 1 [12] and considering all $V_{m,i}$’s are independent, Since we can show that $I'$ can be equivalently viewed as the interference generated by a homogeneous PPP of intensity $\lambda_S$, the Laplace transform of $I'$ can be found as shown in (10) based on the results in [14].
In addition, we can obtain the result in (11) since we know \( F_Z(z) = L^{-1}\left( \frac{1}{z} L_Z(s) \right) (x) \) for a real-valued RV \( Z \).

**B. Proof of Theorem 2**

The CCDF of \( \gamma_{m,i}^t \) can be explicitly written as

\[
F_{H_{m,i}}^t(\xi) = \mathbb{P}\left[ \sum_{j;U_0 \in U^t} \frac{S^c_{m,i,j}}{I_j - S_{m,i,j}} \geq \xi \right] = 1 - \mathbb{E}[\exp(\xi U^t)] \left( \prod_{U_0 \in U^t} \mathbb{P}\left[ \frac{S^c_{m,i,j}}{I_j - S_{m,i,j}} \leq \xi U^t \right] \right)^n \]

\[
= \left[ 1 - \mathbb{E}[\exp(\xi U^t)] \right] \left( \prod_{U_0 \in U^t} \mathbb{P}\left[ \frac{S^c_{m,i,j}}{I_j - S_{m,i,j}} \leq \xi U^t \right] \right)^n \]

which (a) is obtained by the probabilistic generation functional (PGFL) of the PPP process \( U^t \). \( \Phi \) represents the interference evaluated at any eavesdropper. Moreover, by applying Jensen’s inequality to the result in (a) yields the following bound on \( F_{H_{m,i}}^t(\xi) \)

\[
F_{H_{m,i}}^t(\xi) \geq 1 - \exp\left[-\pi \mu_e \int^\infty_0 \mathcal{L}_t \left( - \frac{\xi t^2}{P_m} \right) dt \right] .
\]

With the help of theorem 1, the result is achieved in (13) by carrying out the integral with respect to \( t \).

**C. Proof of Theorem 3**

Since \( U_j^t \)'s mark \( D_j \) is equal to zero, the CCDF of \( \gamma_j^t \) for all \( j \in \mathbb{N}_+ \) can be written as

\[
F_{\gamma_j^t}(\xi) = \mathbb{P}\left[ \sum_{i;X_j \in X_j^t} H_{m,i}^t \geq \xi I_j^t \big| D_j = 0 \right] = \sum_{m=1}^{M} \theta_m \mathbb{P}\left[ \sum_{i;X_j \in X_j^t} \|X_j^t - U_j^t\|^{\alpha} \geq \xi I_j^t \right] \]

where \( I_j^t \equiv \int_{U_j^t} - S_j^t = \sum_{m,i;X_j \in \Phi_i X_j^t; P_m h_{m,i}; \|X_j^t - U_j^t\|^{-\alpha} = \sum_{m,i;X_j \in \Phi_i X_j^t; P_m h_{m,i}} \left\| \sum_{k=1}^{M} \omega_k^{\gamma} X_{k,i} \right\|^{\alpha} \)

Now define \( \tilde{X}_{k,i} \equiv \omega_k^{\gamma} X_{k,i} \), and \( \Phi \equiv \{ \tilde{X}_{k,i} : \tilde{X}_{k,i} \in \mathbb{R}^2 \} \). Since \( \tilde{X}_{k,i} \) is the nearest point from the origin to \( \Phi \) so that we readily evaluate \( \| \tilde{X}_{k,i} \|^{\alpha} \) where \( \tilde{X}_{k,i}^* \) is the nearest point from the origin to set \( \Phi \), for given \( \| \tilde{X}_{k,i}^* \|^{\alpha} \) we can have \( \mathbb{E}[\tilde{X}_{k,i}^*] \left( - \frac{\xi \omega_k^m}{P_m} \right) \)

The CCDF of \( \gamma_j^t \) is equal to zero, the CCDF of \( \gamma_j^t \) and we will get the result with \( \mathbb{P}\left[ \| \tilde{X}_{k,i}^* \|^{\alpha} \right] = 1 - \exp(\pi \omega_k^m \omega_k^m \tilde{X}_{k,i}^* \| \tilde{X}_{k,i}^* \|^{\gamma}) \), which leads to (16). Finally, (15) will be achieved by substituting the above results into (25).

**REFERENCES**


