Exploiting Direct Links for Physical Layer Security in Multi-User Multi-Relay Networks


Published in:
IEEE Transactions on Wireless Communications

Document Version:
Peer reviewed version

Queen's University Belfast - Research Portal:
Link to publication record in Queen's University Belfast Research Portal

Publisher rights
©2016 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other users, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works for resale or redistribution to servers or lists, or reuse of any copyrighted components of this work in other works

General rights
Copyright for the publications made accessible via the Queen's University Belfast Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The Research Portal is Queen's institutional repository that provides access to Queen's research output. Every effort has been made to ensure that content in the Research Portal does not infringe any person's rights, or applicable UK laws. If you discover content in the Research Portal that you believe breaches copyright or violates any law, please contact openaccess@qub.ac.uk.
Exploiting Direct Links for Physical Layer Security in Multi-User Multi-Relay Networks

Lisheng Fan, Nan Yang, Member, IEEE, Trung Q. Duong, Senior Member, IEEE, Maged Elkashlan, Member, IEEE, and George K. Karagiannidis, Fellow, IEEE

Abstract—We present two physical layer secure transmission schemes for multi-user multi-relay networks, where the communication from $M$ users to the base station is assisted by direct links and by $N$ decode-and-forward relays. In this network, we consider that a passive eavesdropper exists to overhear the transmitted information, which entails exploiting the advantages of both direct and relay links for physical layer security enhancement. To fulfill this requirement, we investigate two criteria for user and relay selection and examine the achievable secrecy performance. Criterion I performs a joint user and relay selection, while Criterion II performs separate user and relay selections, with a lower implementation complexity. We derive a tight lower bound on the secrecy outage probability for Criterion I and an accurate analytical expression for the secrecy outage probability for Criterion II. We further derive the asymptotic secrecy outage probabilities at high transmit signal-to-noise ratios and high main-to-eavesdropper ratios for both criteria. We demonstrate that the secrecy diversity order is $\min(M, N + M)$ for Criterion I, and $N$ for Criterion II. Finally, we present numerical and simulation results to validate the proposed analysis, and show the occurrence condition of the secrecy outage probability floor.

Index Terms—Physical layer security, multi-user multi-relay networks, direct links, secrecy outage probability, secrecy diversity order.

I. INTRODUCTION

Over the past few years, the world of wireless communications has experienced unprecedented growth, driven by the vast increase in the number of intelligent devices, the amount of base stations (BSs), and the demand of multimedia content. Surpassed by the ubiquitousness and necessity of wireless connections in the near future, an enormous volume of private and sensitive information, e.g., financial data, medical records, and customer files, will be wirelessly transmitted. It is widely accepted that wireless communications are inherently insecure, due to the broadcast nature of the medium. As such, providing an unrivalled security service is one of the top priorities in the design and implementation of the current and future wireless networks.

Differing from the traditional key-based cryptographic techniques, physical (PHY) layer security enhances the secrecy of wireless communications by exploiting the characteristics of wireless channels, without using secret keys and complex encryption/decryption algorithms [1]. As the seminal work that laid down the fundamentals of PHY layer security, the authors in [2] introduced the wiretap channel as the basic model and defined the secrecy capacity as the maximum rate at which messages are reliably transmitted to the legitimate receiver, without being intercepted by unintended parties. Inspired by early studies, PHY layer security over fading channel has been studied from both information-theoretic and practical perspectives. For example, [3], [4] considered a single-input single-output (SISO) wiretap channel over Rayleigh fading and analyzed the secrecy capacity. Built upon these studies, PHY layer security in multi-input multi-output (MIMO) communication systems has been intensively addressed, due to the benefits of multi-antenna techniques, such as high data rate and high link reliability. For instance, several MIMO secure techniques have been investigated, such as beamforming (e.g., [5]–[7]), precoding (e.g., [8]), artificial noise (e.g., [9]), and antenna selection (e.g., [10]–[12]).

Recently, PHY layer security in relay networks has attracted considerable attention, due to the fact that cooperative relaying is envisioned as a very promising technique to enhance the performance of the next-generation wireless communication networks [13]–[19]. In secure communications, researchers have investigated traditional relaying protocols [20]–[28], such as amplify-and-forward (AF) and decode-and-forward (DF), where DF can be further specified as fixed DF and selective DF [29]. For example, [21] employed relay selection to enhance secrecy in a multi-AF-relay network and adopted the intercept probability as the secrecy performance metric. In [22]–[24], a selective-DF based multi-relay network was considered and one relay out of multiple relays was selected for secrecy improvement. Note that a common feature of [21]–[24] is

1Compared with selective-DF relaying, fixed-DF relaying does not need additional feedback caused by notification, and hence is easier to implement in practice [29]. In the following, we use DF to denote fixed-DF if not specified.
that the direct link between the source and the destination (or the eavesdropper) is unavailable. To investigate the impact of the direct link on the secrecy performance, [25] studied the performance of relay selection in a fixed-DF based multi-relay network with maximal ratio combining (MRC) receiver, where the available direct link between the source and receiver is not involved in the system relay selection. Considering multiple relays used to facilitate the downlink of multi-user networks, [26] and [27] analyzed the secrecy performance for AF-relay and selective-DF-relay selection, respectively. Besides these works, the secure communications of full-duplex relay and large systems were also investigated in the literature [30]–[33].

This paper lays the groundwork for understanding the role of the direct link on the PHY layer security in the uplink of multi-user multi-relay networks, which stands as a major advancement over [26] and [27] which focused on the downlink. We investigate secure user and relay selection schemes and analyze the achievable secrecy performance of the uplink where $N$ fixed-DF relays assist the communication from $M$ users to the BS. The BS adopts MRC to process the received signals through both the direct link and the relay link. We assume that a passive eavesdropper exists in this network to overhear the transmitted information. We note that although selective-DF based multiuser multi-relay networks have been extensively investigated, e.g., [27], [34], [35], fixed-DF based multiuser multi-relay networks with an MRC receiver have not been analyzed in the literature, regardless of secure or non-secure communications. The key contributions of this paper are summarized as follows:

- We propose two user and relay selection criteria that select the best user and relay pair, to exploit the advantages of both direct and relay links for PHY layer security enhancement. In Criterion I, a joint user and relay selection is performed to maximize the data rate of the main links, from the selected user to the BS. In Criterion II, separate user and relay selections are performed, based on direct and relay links, respectively, which reduces the implementation complexity.

- We derive novel expressions for the secrecy outage probability, in order to investigate the secrecy performance achieved by the proposed criteria. For Criterion I, we derive a tight lower bound on the secrecy outage probability, whereas for Criterion II, we present an accurate analytical expression.

- We present new results for the asymptotic secrecy outage probability for both criteria. These asymptotic expressions enable us to determine the main factors that regulate the secrecy performance in the transmit high signal-to-noise ratio (SNR) and the high main-to-eavesdropper ratio (MER) regimes.

- Based on the asymptotic results, we demonstrate that Criterion I achieves the secrecy diversity order of $\min(MN, M+N)$, while Criterion II achieves the secrecy diversity order of $N$. Notably, the number of users does not affect the secrecy diversity order for Criterion II. With the help of simulations, we verify our analysis and investigate the impact of the network parameters on the secrecy performance.

- Finally, we show that the secrecy outage probability floor occurs when the transmit power increases and the MER of either direct link or relay link is fixed.

The organization of this paper is as follows. After the introduction, Section II describes the model of a two-phase uplink multi-user multi-relay network and details the proposed criteria for user and relay selection. Section III presents the secrecy outage probabilities for the two criteria, including the derivations for both the exact and asymptotic results. Numerical results are provided in Section IV to offer valuable insights into the secrecy performance. Conclusions are drawn in Section V.

**Notation:** $X \sim \mathcal{CN}(0, \sigma^2)$ denotes a circularly symmetric complex Gaussian random variable $X$ with zero mean and variance $\sigma^2$; $\Pr\{\cdot\}$ is the probability; $f_X(\cdot)$ and $F_X(\cdot)$ represent the probability density function (PDF) and cumulative distribution function (CDF) of the random variable $X$, respectively.

## II. USER AND RELAY SELECTION IN MULTI-USER MULTI-RELAY NETWORK

### A. The Multi-user Multi-relay Network Model

Let us consider a secure multi-user multi-relay network, as depicted in Fig. 1, where the communication between $M$ users $S_m$, $m \in \{1, \cdots, M\}$, and the BS $D$ is assisted by $N$ DF relays $R_n$, $n \in \{1, \cdots, N\}$. In practice, this model represents the uplink of a multi-user cellular system with multiple relays, which assist the user–BS transmission. We assume that an eavesdropper $E$ exists in this network and overhears the transmitted messages, bringing out the important issue of information wiretap. We further assume that all nodes in the network are equipped with a single antenna, due to the size limitation, and operate in a half-duplex time-division mode.

To enhance the transmission security, both user selection and relay selection will be performed in this work to select one best user $S_m$, among $M$ users to communicate with $D$, with the help of a selected $R_n$ out of $N$ relays. In practice, user selection can be applied in a multiuser LTE-Advanced cellular system to improve the system throughput.

3We assume that the $M$ users are relatively close together and in the same cluster, which have the same distance to the other nodes in the network. This assumption also holds for the $N$ relays.

4If multiple eavesdroppers exist in the network, the secrecy performance will be degraded. This is caused by an increase in the success probability of eavesdropping, i.e., either by the best eavesdropper with the most favorable channel condition or by the collaboration of multiple eavesdroppers.

5The residual users and relays are assumed to keep silent in this work. In some communication systems [24], [25], [28], [36], the residual users and relays can send jamming signals to confuse the eavesdropper, at the cost of an increased implementation complexity. The transmission of jamming signals will be addressed in future work.
whereas relay selection is feasible in IEEE 802.12j vehicular networks to improve the system capacity [34], [39]. We further assume that the direct link between the source and the destination is available. The adoption of this assumption is not to complicate the system model, but to address a practical scenario in wireless cellular networks. In practice, the direct link is available if the source and the destination are not placed remotely, or the destination does not fall within heavily shadowed areas. Motivated by this practicality, the impact of the direct link on the performance of relay-aided wireless systems has been examined in [34], [35] and [40]–[42]. Since the direct links can affect both the legitimate transmission and the illegitimate wiretap, the impact of both direct and relay links on the user and relay selection has to be considered for the secure transmission. To present the relay and user selection criteria, we first detail the two-phase transmission process, as follow:

Suppose that the user \( S_m \) and the relay \( R_n \) have been selected for data transmission. In the first phase, \( S_m \) sends the encoded signal of unit-variance, \( x_s \), with transmit power \( P \). The received signal at \( R_n \), \( D \), and \( E \) in the first phase are given by

\[
y_{R_n} = h_{S_m,R_n}\sqrt{P}x_s + n_{R_n},
\]

\[
y^{(1)}_D = h_{S_m,D}\sqrt{P}x_s + n^{(1)}_D,
\]

\[
y^{(1)}_E = h_{S_m,E}\sqrt{P}x_s + n^{(1)}_E,
\]

respectively, where \( h_{S_m,R_n} \sim \mathcal{CN}(0, \alpha) \), \( h_{S_m,D} \sim \mathcal{CN}(0, \varepsilon_1) \), and \( h_{S_m,E} \sim \mathcal{CN}(0, \varepsilon_2) \) denote the channel coefficients of the \( S_m-R_n \) link, \( S_m-D \) link, and \( S_m-E \) link, respectively. We also denote \( n_R \sim \mathcal{CN}(0, \sigma^2) \), \( n^{(1)}_D \sim \mathcal{CN}(0, \sigma^2) \), and \( n^{(1)}_E \sim \mathcal{CN}(0, \sigma^2) \) as the additive white Gaussian noise (AWGN) at \( R_n \), \( D \), and \( E \) in the first phase. If \( R_n \) correctly decodes the message received in the first phase, it then re-encodes the signal with the same code book at \( S_m \) and forwards it to \( D \) in the second phase. Accordingly, the received signal at \( D \) and \( E \) in the second phase are given by

\[
y^{(2)}_D = h_{R_n,D}\sqrt{P}x_s + n^{(2)}_D,
\]

\[
y^{(2)}_E = h_{R_n,E}\sqrt{P}x_s + n^{(2)}_E,
\]

respectively, where \( h_{R_n,D} \sim \mathcal{CN}(0, \beta_1) \) and \( h_{R_n,E} \sim \mathcal{CN}(0, \beta_2) \) denote the channel coefficients of the \( R_n-D \) link and \( R_n-E \) link, respectively. We also denote \( n^{(2)}_D \sim \mathcal{CN}(0, \sigma^2) \) and \( n^{(2)}_E \sim \mathcal{CN}(0, \sigma^2) \) as the AWGN at \( D \) and \( E \), respectively, in the second phase. Here, although we assume that the selected relay has the same transmit power as the selected user, we highlight that this assumption does not lose generality. We denote \( u_{mn} = |h_{S_m,R_n}|^2 \), \( v_{1n} = |h_{R_n,D}|^2 \), \( v_{2n} = |h_{R_n,E}|^2 \), \( w_{1m} = |h_{S_m,D}|^2 \), and \( w_{2m} = |h_{S_m,E}|^2 \) as the channel gains of the \( S_m-R_n \) link, \( R_n-D \) link, \( R_n-E \) link, \( S_m-D \) link, and \( S_m-E \) link, respectively. The end-to-end SNR at \( D \) for the repetition-coded fixed DF relaying can be written as [29, Eq. (15)]

\[
\text{SNR}_D = \frac{1}{2} \log_2 \left( 1 + \frac{\gamma}{P/\sigma^2} (u_{mn}v_{1n} + w_{1m}) \right) - \frac{1}{2} \log_2 \left( 1 + \frac{\gamma}{P/\sigma^2} (v_{2n} + w_{2m}) \right) < R_s.
\]

After some mathematical manipulations, we re-express (7) as

\[
\frac{1}{1 + \frac{\gamma}{P/\sigma^2} (v_{2n} + w_{2m})} < \frac{1 + \gamma}{1 + \frac{\gamma}{P/\sigma^2} (u_{mn}v_{1n} + w_{1m})} < \gamma_s,
\]

where \( \gamma_s = 2R_s \) is the secrecy SNR threshold.

### B. User and Relay Selection Criteria

We consider a practical passive eavesdropping scenario, where only the statistical information of the eavesdropper’s channel is known, while the instantaneous information of the eavesdropper’s channel is unknown. This indicates that the eavesdropper’s channel coefficients, i.e., \( h_{S_m,E} \) and \( h_{R_n,E} \), are not available at the users, relays, and BS. Accordingly, the values of \( v_{2n} \) and \( w_{2m} \) are not known and thus cannot be involved in the selection criterion. We highlight that the passive eavesdropping scenario is a practical consideration since in practice the eavesdropper is generally not cooperative and not willing to feedback its instantaneous channel coefficients to the legitimate nodes. Moreover, the assumption of known statistical information of the eavesdropper’s channel applies to the scenario where the eavesdropper is part of a multiuser system which in alternate time slots it becomes an active legitimate participant in the system. As such, the eavesdropper feeds back its channel state information to the transmitter for the time slot where it is being served. From this information, and assuming that the eavesdropper is static (or moving slowly), the statistical knowledge of the eavesdropper’s channel in the time slots where it is not being served can be derived. Under this consideration, we propose two user and relay selection criteria that select the best user and relay pair to carry out the secure transmission in the network. These criteria are described as follow:
1) **Criterion I:** In this criterion, the joint user and relay selection is performed by maximizing the achievable rate of the main links. Mathematically, the indices of the selected user and the relay are expressed as

\[
(m^*, n^*) = \arg \max_{1 \leq m \leq M} \max_{1 \leq n \leq N} (u_{mn}, v_{1n} + w_{1m}). \tag{9}
\]

This criterion achieves the optimal secrecy performance in the passive eavesdropping scenario. We clarify that an assumption adopted in (9) is that the eavesdropper has the same average channel gain to the users and the relays. Hence, the mathematical derivation in this scenario cannot be performed by maximizing the data rate of main link, but can be performed by maximizing

\[
\min \left( \frac{1 + \gamma}{1 + \gamma E[v_{2n} + E[w_{2m}]]} \right),
\]

where \(E[\cdot]\) denotes the statistical expectation.

In Criterion I, the term \(w_{1m}\) from the direct link is incorporated into the term \(\min (u_{mn}, v_{1n})\) from the relay links. As such, the two terms cannot be separated from each other. It follows that Criterion I is a joint selection scheme where the user selection interacts with the relay selection.

2) **Criterion II:** Differing from Criterion I, Criterion II involves separate user and relay selections. Specifically, the best user is firstly selected based on the direct links [44], and then the best relay is selected based on the two-hop relay links [45]. The indices of the selected user and the relay can be expressed as

\[
m^* = \arg \max_{1 \leq m \leq M} w_{1m}, \quad \tag{10}
\]

and

\[
n^* = \arg \max_{1 \leq n \leq N} \min (u_{mn}, v_{1n}). \tag{11}
\]

It is evident from (10) and (11) that user selection and relay selection are performed separately in Criterion II. Compared with Criterion I which needs an adder and a comparator to perform joint selection, Criterion II only requires a simple comparator to perform separate selections, bringing about a lower implementation complexity. Hence, our work provides a flexible choice for system design as follows: If the system has a powerful computational capability, Criterion I is preferred to achieve the best secrecy performance; otherwise Criterion II can be used to reduce the implementation complexity.

We next detail the channel estimation procedure for both criteria. At the beginning of each transmission block, the network needs to determine which pair of user and relay is selected for data transmission. To this end, we assume that \(D\) estimates the required channel coefficients of main links with the help of pilot signals from users and relays. Then \(D\) performs user selection and relay selection according to either Criterion I or Criterion II, and notifies the indices of the selected user and relay through dedicated feedback channels. After selection, the two-phase data transmission commences at the selected user \(S_{m^*}\) and relay \(R_{n^*}\).

Based on (8), the secrecy outage probability with the selected user \(S_{m^*}\) and relay \(R_{n^*}\) is given by

\[
P_{\text{out}} = \Pr \left[ \frac{1 + \gamma \min (u_{mn}, v_{1n} + w_{1m})}{1 + \gamma (v_{2n} + w_{2m})} < \gamma_s \right],
\]

\[
= \Pr \left[ Z < \gamma_s (v_{2n} + w_{2m}) + \gamma_s \right], \tag{12}
\]

where \(\gamma_s = (\gamma_s - 1)/\gamma\) and \(Z \triangleq \min (u_{mn}, v_{1n} + w_{1m})\). Evidently, the statistical characterization of \(Z\) is the key for the evaluation of \(P_{\text{out}}\).

### III. ANALYSIS OF SECRECY OUTAGE PROBABILITY

In this section, we derive new exact and asymptotic expressions for the secrecy outage probability, where both criteria are considered.

#### A. A Tight Lower Bound for Criterion I

For Criterion I, we first rewrite \(Z\) as

\[
Z = \max_{1 \leq m \leq M} \max_{1 \leq n \leq N} (u_{mn}, v_{1n} + w_{1m}). \tag{13}
\]

From (13), we can conclude that \(Z\) is the maximum of \(M \times N\) non-independent variables, \(\{\min (u_{mn}, v_{1n} + w_{1m})\}\). This is due to the fact that \(M\) users share the common variable \(v_{1n}\), while \(N\) relays share the common variable \(w_{1m}\). Moreover, we see that the variable \(w_{1m}\) from the direct link affects both relay selection and user selection. This makes the mathematical derivation for the fixed-DF based multi-user multi-relay networks much more complicated than that for AF or selective-DF based multi-user multi-relay networks. Therefore, it is mathematical difficult, if not impossible, to obtain an exact analytical expression for the secrecy outage probability for Criterion I. Motivated by this, we turn to derive two upper bounds on \(Z\) by exchanging the sequence of max and min operations. The first upper bound is given by

\[
Z_1 = \max_{1 \leq m \leq M} \min_{1 \leq n \leq N} \max_{1 \leq n \leq N} (u_{mn}, v_{1n} + w_{1m})
\]

\[
= \max_{1 \leq m \leq M} \min_{1 \leq n \leq N} (u_{mn}, (\max_{1 \leq n \leq N} v_{1n}) + w_{1m}), \tag{14}
\]

and the second upper bound by

\[
Z_2 = \max_{1 \leq n \leq N} \min_{1 \leq m \leq M} (u_{mn}, v_{1n} + w_{1m})
\]

\[
= \max_{1 \leq n \leq N} \min_{1 \leq m \leq M} (u_{mn}, (\max_{1 \leq m \leq M} w_{1m})). \tag{15}
\]

Built upon \(Z_1\) in (14) and \(Z_2\) in (15), we next derive the lower bounds on the secrecy outage probability, i.e., \(P_{\text{out}}^{LB}\) and \(P_{\text{out}}^{UB}\). We note that \(Z_1\) is effective only when the relay selection does not dominate the joint user and relay selection, while \(Z_2\) is effective only when the user selection does not dominate the joint user and relay selection.

\footnote{For AF [26] or selective-DF based multi-user multi-relay networks with direct links [27], [35], [42], [46], the system relay selection is based on the two-hop relay links only with a given user \(S_m\). This indicates that the direct links have no impact on the relay selection. Hence, the mathematical derivation in these studies cannot be applied to the proposed work.}
dominate the joint selection. Hence, the maximal value of $P_{1,\text{out}}^{L_B}$ and $P_{2,\text{out}}^{L_B}$ provides a very tight lower bound on the secrecy outage probability, which will be demonstrated by the numerical and simulation results in Section IV.

We now begin to derive $P_{1,\text{out}}^{L_B}$ associated with $Z_1$. Let
\begin{align*}
v_1 &= \max_{1 \leq n \leq N} v_{1n}, \quad (16) \\
u_m &= \max_{1 \leq n \leq N} u_{mn}, \quad (17)
\end{align*}
and then we rewrite $Z_1$ as
\begin{equation}
Z_1 = \max_{1 \leq m \leq M} \min \left( (uv_m, v_1 + w_{1m}) \right). \quad (18)
\end{equation}

From (18), $Z_{1m}$ is correlated with each other, because of the common variable $v_1$. To deal with this, we first derive the conditional CDF of $Z_{1m}$ with respect to $v_1$, i.e., $F_{Z_{1m}}(z|v_1)$. By statistically averaging $F_{Z_{1m}}^M(z|v_1)$ with respect to $v_1$, we then obtain the analytical CDF of $Z_1$, i.e., $F_{Z_1}(z)$. We further statistically average $F_{Z_1}(z)_{\gamma_\text{s}(v_{2n}^*, w_{2m}^*) + \gamma_\text{s}^*}$ with respect to both $v_{2n}^*$ and $w_{2m}^*$ to obtain $P_{1,\text{out}}^{L_B}$. The CDF of $Z_1$ is derived and presented in the following theorem.

*Theorem 1:* The CDF of $Z_1$ can be expressed as
\begin{align*}
F_{Z_1}(z) &= \sum_{n_1=1}^{N} \sum_{n_2=0}^{M} b_{1,n_1,n_2} e^{-c_{1,n_1,n_2}z} \\
&\quad + \sum_{m=0}^{M} \sum_{n=1}^{N} \sum_{i} q_{1i} b_{2,m,n} \left( e^{-q_{2i}z} - e^{-(q_{2i}+c_{2,m,n})z} \right), \quad (19)
\end{align*}
where
\begin{align*}
b_{1,n_1,n_2} &= (-1)^{n_1+n_2+1} \binom{N}{n_1} \binom{MN}{n_2}, \\
c_{1,n_1,n_2} &= \frac{n_1}{\beta_1} + \frac{n_2}{\alpha}, \\
q_{1i} &= \binom{m}{i_1} \binom{i_1}{i_2} \cdots \binom{i_{N-2}}{i_{N-1}} b_{3,1}^{m-i_1} b_{3,2}^{i_1-i_2} \cdots b_{3,N}^{i_{N-2}-i_{N-1}} b_{3,N}^{i_{N-1}}, \\
b_{3,n} &= \binom{N}{n} (-1)^{-n-1}, \\
b_{2,m,n} &= (-1)^{n+m-n-1} \binom{N}{n} \binom{M}{m} \frac{n \xi_1}{n \xi_1 - m \beta_1}, \\
q_{2i} &= c_{3,1}(m-i_1) + c_{3,2}(i_1-i_2) + \cdots + c_{3,N-1}(i_{N-2}-i_{N-1}) + c_{3,N}i_{N-1}, \\
c_{3,n} &= \frac{n}{\alpha} + \frac{1}{\xi_1},
\end{align*}
and
\begin{equation}
c_{2,m,n} = \frac{n}{\beta_1} - \frac{m}{\xi_1}. \quad (20)
\end{equation}

*Proof 1:* See Appendix A.

From Theorem 1 and eq. (12), we can derive the first lower bound of $P_{\text{out}}$ as
\begin{equation}
P_{1,\text{out}}^{L_B} = \int_{0}^{\infty} \int_{0}^{\infty} F_{Z_1}(z)_{\gamma_\text{s}(v_{2n}^* + w_{2m}^*) + \gamma_\text{s}^*} \times f_{v_{2n}^*}(v_{2n}^*) f_{w_{2m}^*}(w_{2m}^*) dv_{2n}^* dw_{2m}^*. \quad (21)
\end{equation}

By using the PDF of $v_{2n}^*$, given by $f_{v_{2n}^*}(x) = \frac{1}{\sigma_2} e^{-\frac{x^2}{2\sigma_2^2}}$, and the PDF of $w_{2m}^*$, given by $f_{w_{2m}^*}(x) = \frac{1}{\sigma_2} e^{-\frac{x^2}{2\sigma_2^2}}$, and solving the integral in (20), we derive $P_{1,\text{out}}^{L_B}$ as
\begin{equation}
P_{1,\text{out}}^{L_B} = \sum_{n_1=1}^{N} \sum_{n_2=0}^{M} b_{1,n_1,n_2} \mathcal{L}(c_{1,n_1,n_2}) \\
+ \sum_{m=0}^{M} \sum_{n=1}^{N} \sum_{i} q_{1i} b_{2,m,n} \left( \mathcal{L}(q_{2i}) - \mathcal{L}(q_{2i} + c_{2,m,n}) \right), \quad (22)
\end{equation}
where $\mathcal{L}(x)$ is defined as
\begin{equation}
\mathcal{L}(x) = \frac{e^{-\gamma_\text{s} x}}{(1 + \beta_2 \gamma_\text{s}) (1 + \epsilon_2 \gamma_\text{s} x)}.
\end{equation}

The second lower bound of $P_{\text{out}}$, $P_{2,\text{out}}^{L_B}$, has the same form as $P_{1,\text{out}}^{L_B}$ in (21) after replacing $M$ with $N$ and $\beta_1$ with $\epsilon_1$. This is because of the symmetry existed in (14) and (15). Finally, the tight lower bound on the secrecy outage probability for Criterion I can be obtained as
\begin{equation}
P_{\text{out}}^{L_B} = \max \left( P_{1,\text{out}}^{L_B}, P_{2,\text{out}}^{L_B} \right). \quad (23)
\end{equation}

We highlight that (23) consists of elementary functions only, and as such, it can be easily evaluated.

**B. Exact Formula for Criterion II**

To derive the secrecy outage probability for Criterion II, we first derive the CDFs of $w_{1m}^*$, $u_{mn}^*$, and $v_{1n}^*$, as per the selection criterion characterized by eqs. (10) and (11), and then we obtain the CDF of $Z_1$, $F_Z(z)$. Furthermore, by averaging $F_Z(z)$ with respect to $w_{2m}^*$ and $v_{2n}^*$, we derive an exact expression for $P_{\text{out}}$.

*Theorem 2:* The CDF of $Z$ can be expressed by
\begin{equation}
F_Z(z) = 1 - \sum_{m=1}^{M} \sum_{n_1=0}^{N-1} \sum_{n_2=0}^{N-1} \left( t_{1,n_1}, t_{3,m,n_2} e^{-2z} + t_{2,n_1} t_{3,m,n_2} \right. \\
\times e^{-\left( \frac{m+1}{\alpha} + \frac{1}{\beta_1} \right) z} + t_{1,n_1} t_{4,m,n_2} e^{-\left( \frac{m+1}{\alpha} + \frac{1}{\beta_1} \right) z} \\
+ t_{1,n_1} t_{5,m,n_2} e^{-\left( \frac{m+1}{\alpha} + \frac{2\xi_1}{\alpha} \right) z} + t_{2,n_1} t_{4,m,n_2} e^{-\left( \frac{m+1}{\alpha} + \frac{2\xi_1}{\alpha} \right) z} \\
\left. + t_{2,n_1} t_{5,m,n_2} e^{-\left( \frac{m+1}{\alpha} + \frac{2\xi_1}{\alpha} \right) z} \right), \quad (24)
\end{equation}
where
\begin{equation}
\zeta = \frac{\alpha \beta_1}{\alpha + \beta_1},
\end{equation}
\[ t_{1,n} = \frac{b_{4,n} \zeta}{\zeta + n \beta_1}, \]
\[ t_{2,n} = b_{4,n} \left( \frac{1}{n + 1} - \frac{\zeta}{\zeta + n \beta_1} \right), \]
\[ t_{3,m,n} = (-1)^{m-1} \left( \frac{M}{m} \right) \frac{b_{4,n} \zeta m \beta_1}{(\zeta + n \alpha) (m \beta_1 - \varepsilon_1)}, \]
\[ t_{4,m,n} = (-1)^{m-1} \left( \frac{M}{m} \right) \left[ \frac{1}{N} - \frac{b_{4,n} \zeta m \beta_1}{(\zeta + n \alpha) (m \beta_1 - \varepsilon_1)} \right] - b_{4,n} \left( \frac{1}{n + 1} - \frac{\zeta}{\zeta + n \alpha} \right) \frac{m \zeta}{m \zeta - (n + 1) \varepsilon_1}, \]
\[ t_{5,m,n} = (-1)^{m-1} \left( \frac{M}{m} \right) \left( \frac{1}{n + 1} - \frac{\zeta}{\zeta + n \alpha} \right) \frac{b_{4,n} m \zeta}{m \zeta - (n + 1) \varepsilon_1}, \]
\[ \text{and} \]
\[ b_{4,n} = N (-1)^n \left( \frac{N-1}{n} \right). \]

**Proof 2:** See Appendix B.

From Theorem 2 and (12), we can now derive an exact expression for \( P_{\text{out}} \) as
\[ P_{\text{out}} = \int_0^\infty \int_0^\infty F_Z (\gamma_s (v_{2n^*} + w_{2m^*}) + \gamma_s') \times f_{v_{2n^*}} (v_{2n^*}) f_{w_{2m^*}} (w_{2m^*}) dv_{2n^*} dw_{2m^*}. \]

**Proof 3:** See Appendix C.

From the asymptotic expression for \( F_{Z_1} (z) \), we can compute the asymptotic secrecy outage probability associated with \( Z_1 \) as
\[ P_{\text{out}} \approx \int_0^\infty \int_0^\infty F_{Z_1} (\gamma_s (v_{2n^*} + w_{2m^*}) + \gamma_s') f_{v_{2n^*}} (v_{2n^*}) \times f_{w_{2m^*}} (w_{2m^*}) dv_{2n^*} dw_{2m^*} \]
\[ \approx \int_0^\infty \int_0^\infty F_{Z_1} (\gamma_s (v_{2n^*} + w_{2m^*}) + \gamma_s') f_{v_{2n^*}} (v_{2n^*}) \times f_{w_{2m^*}} (w_{2m^*}) dv_{2n^*} dw_{2m^*} \]
\[ \approx \gamma_s^{M+N} (M+N)! \rho_{M,N} \sum_{k=0}^{M+N} \left( \frac{\beta_2}{\alpha} \right)^{M-k} \left( \frac{\beta_1}{\alpha} \right)^{M+N-k}, \]

where
\[ \rho_{M,N} = \sum_{m=0}^{M} \left( \frac{M}{m} \right) \frac{1}{m + 1} \left( \frac{z}{\alpha} \right)^{M-m}, \quad \text{if} \ N = 1, \]
\[ \sum_{m=0}^{M+N} \left( \frac{M+N}{m} \right) \frac{1}{m + 1} \left( \frac{z}{\alpha} \right)^{M+m}, \quad \text{if} \ N \geq 2. \]

**Remark 1:** For a single user or single relay communication system, the secrecy diversity order is \( M/N \). In particular, the secrecy diversity order is \( M \) for a single relay system with \( N = 1 \). This is due to the fact that only multi-user diversity can be exploited. On the other hand, the secrecy diversity order is \( N \) for a single user system with \( M = 1 \), since only the multi-relay diversity can be exploited.

**Remark 2:** For a multi-user and multi-relay communication system with \( M \geq 2 \) and \( N \geq 2 \), the secrecy diversity order is equivalent to \( M + N \). This indicates that both multi-user diversity and multi-relay diversity can be fully exploited for secure communication.

**D. Asymptotic \( P_{\text{out}} \) for Criterion II**

Using the Taylor’s series approximation of \( e^{-x} \) given by
\[ e^{-x} \approx 1 - x + \frac{x^2}{2} + \cdots + \frac{(-x)^N}{N!}, \]
the asymptotic CDF of \( Z \) can be written as,
Theorem 4: The asymptotic CDF of $Z$ can be expressed by

$$F_Z(z) \simeq \left( \frac{\beta_1}{\alpha + \beta_1} \right)^N z^N \xi^N,$$

(31)

Proof 4: See Appendix D.

From this asymptotic CDF, we compute the asymptotic secrecy outage probability for Criterion II as

$$P_{\text{out}} \simeq \int_0^\infty \int_0^\infty F_Z(\gamma_s(v_{2n^*} + w_{2m^*}) + \gamma'_{s}) f_{v_{2n^*}}(v_{2n^*})$$
$$\times f_{w_{2m^*}}(w_{2m^*}) dv_{2n^*} dw_{2m^*}$$
$$\simeq \int_0^\infty \int_0^\infty F_Z(\gamma_s(v_{2n^*} + w_{2m^*}) + \gamma'_{s}) f_{v_{2n^*}}(v_{2n^*})$$
$$\times f_{w_{2m^*}}(w_{2m^*}) dv_{2n^*} dw_{2m^*}$$
$$\simeq \gamma_s^N N! \left(1 + \frac{\alpha}{\beta_1} \right)^{N-1} \sum_{n=0}^N \frac{\xi_2^n}{\beta_2^n}.$$

(32)

From the asymptotic secrecy outage probability in (32), we provide some valuable insights in the following two remarks:

Remark 1: Criterion II achieves the secrecy diversity order of $N$, which comes from the multi-relay diversity. This indicates that the multi-user diversity is not efficiently exploited in Criterion II. In particular, increasing the number of users does not affect the secrecy diversity order nor the secrecy coding gain of Criterion II. This can be explained by the fact that the asymptotic secrecy outage probability is irrespective of $M$.

Remark 2: The secrecy performance of the network can be significantly enhanced by increasing the number of relays. This can be explained by the fact that the relay links are the bottleneck of the secure transmission in Criterion II.

Observing the analytical and asymptotic results presented in (23), (26), (29) and (32), it is easy to find that our analysis is developed based on the statistical information of eavesdropping channels. This indicates that the statistical information of the eavesdropping channels is utilized to evaluate the secrecy outage probabilities for Criterion I and II.

IV. NUMERICAL AND SIMULATION RESULTS

In this section, we provide numerical and simulation results to verify the presented analysis of the proposed selection criteria and to examine the impact of the network parameters on the secrecy outage probability. Throughout this section, we assume that all links in the network experience Rayleigh flat fading. Without loss of generality, the distance between the users and the BS is set to unity, and the relays are placed between in them. Let $d$ denote the distance from the users to relay. Accordingly, the average channel gains of the main links are set to $\alpha = d^{-4}$, $\beta_1 = (1 - d)^{-4}$ and $\varepsilon_1 = 1$, where the path-loss model with a loss factor of 4 is used. The secrecy data rate $R_s$ is set to 0.2 bps/Hz and thus, the secrecy SNR threshold $\gamma_s$ is equal to 1.32.

Figs. 2(a) and 2(b) plot the secrecy outage probabilities for Criterion I and II versus the transmit SNR $\gamma$ for $d = 0.5$ and $\lambda_1 = \lambda_2 = 20$ dB. As observed from both figures, the analytical result for each criterion perfectly matches the corresponding simulation over the entire SNR regime for various values of $M$ and $N$. This demonstrates the tightness of the lower bound derived for Criterion I and the correctness of the exact result proposed for Criterion II. Moreover, it is seen that the secrecy outage probability improves with the transmit SNR in the low SNR regime, but this improvement becomes saturated in the medium and high SNR regime. This is due to the fact that the MER is the bottleneck of the secrecy performance of the network. Furthermore, an increase in the number of relays brings a profound improvement in the secrecy outage probabilities for both criteria, which is due to the fact that the multi-relay diversity indeed helps the secure transmission for both of them. In addition, we can conclude that an increase in the number of users brings a profound improvement in the secrecy outage probability for Criterion I, but a minor improvement for Criterion II. This phenomenon can be explained by the fact that in Criterion II, the first hop of
the relay link $u_{m^*n^*}$ is the bottleneck of the received SNR at the destination, $\tilde{\gamma} \min(u_{m^*n^*}, v_{1n^*} + w_{1m^*})$. This bottleneck will not be improved profoundly by increasing the number of users, since the best user selected based on direct links is treated as a random user in the first hop of relay link.

Figs. 3(a) and 3(b) plot the secrecy outage probabilities for Criterion I and II versus the MER $\lambda_1$ for $d = 0.5$, $\tilde{\gamma} = 30$ dB, and $\lambda_1 = \lambda_2$. To obtain the simulation results as low as $10^{-8}$ with $M = 2$ and $N = 3$ for Criterion I, we perform $10^{11}$ Monte Carlo runs. From both figures, the asymptotic result for each criterion accurately approximates the corresponding simulation result in the high MER regime for various values of $M$ and $N$. This validates our asymptotic results derived for Criteria I and II. Moreover, the secrecy diversity order increases with $N$ for both criteria. This implies that increasing the number of relays significantly improves the secrecy outage probability, especially in the medium and high MER regime. In contrast, the secrecy diversity order increases with $M$ for Criterion I, but remains unchanged for Criterion II, as indicated by our asymptotic results. This implies that increasing the number of users leads to a prominent reduction in the secrecy outage probability for Criterion I, but a minor reduction in the secrecy outage probability for Criterion II.

Figs. 4(a) and 4(b) plot the secrecy outage probabilities for Criterion I and II versus the MER $\lambda_1$ for $d = 0.5$, $\tilde{\gamma} = 30$ dB, and $\lambda_2 = 30$ dB. Again, here the accuracy of our asymptotic results in the high MER regime for various values of $M$ and $N$. Moreover, we see that the network secrecy performance profoundly improves with $\lambda_1$ in the low and medium MER regime. Furthermore, we see that the network exhibits a secrecy performance floor in the high MER regime for both criteria. This is caused because that the relay links are the bottleneck of the secure transmission, when the MER of relay links is fixed.

Fig. 5 compares Criterion I and II with the selection schemes in [23] and [24] by plotting the secrecy outage probability versus the MER $\lambda_1$ for $d = 0.2$, $\tilde{\gamma} = 30$ dB, $\lambda_1 = \lambda_2$, and $M = N = 2$. Recall that in [23] and [24], user and relay selection is performed by maximizing $\min(u_{m^*n^*}, v_{1n^*})$ and $(w_{1m^*} + v_{11n^*})$, respectively. From Fig. 5 we find that the secrecy outage probabilities of Criterion I and II are lower than the secrecy outage probabilities of the schemes in [23]
Fig. 5. Performance comparison of selection schemes versus MER for $d = 0.2$, $\gamma = 30$ dB, $\lambda_1 = \lambda_2$, and $M = N = 2$.

and [24]. This is due to the fact that the system model and the relay protocol considered in [23] and [24] are different from those in our paper, leading to the fact that the selection criteria in [23] and [24] cannot efficiently optimize the system performance. Hence, our proposed selection schemes outperform those in [23] and [24].

From Figs. 2–5 we find that the derived lower bound on the secrecy outage probability in Criterion I perfectly matches the simulation result over the entire regime of transmit SNR and MER. We also find that the matching is valid for various numbers of users and relays. This matching demonstrates the accuracy of the derived lower bound for Criterion I.

V. CONCLUSIONS

In this work we addressed the problem of secure communication in the multi-user and multi-relay network, where direct links from the users to the BS and from the users to the eavesdropper affect both information transmission and information wiretap. Taking into account the effect of both direct and relay links, we proposed two user and relay selection criteria that select one best user and relay pair to improve secure communication. For each criterion, we derived new analytical expressions for the secrecy outage probability. We confirmed from the asymptotic expressions that Criterion I achieves the secrecy diversity order of $M + N$ for $M \geq 2$ and $N \geq 2$, while Criterion II achieves the secrecy diversity order of $N$ with a low implementation cost. Simulation results were also provided to validate the proposed analysis and to examine the impact of the network parameters on the secrecy performance.

APPENDIX A

PROOF OF THEOREM 1

To derive the CDF of $Z_1$, we first derive the conditional CDF of $Z_{1m}$ with respect to $v_1$ as

$$F_{Z_{1m}}(z|v_1) = \Pr \{\min (u_m, v_1 + w_{1m}) < z\} = 1 - \Pr [u_m \geq z] \cdot \Pr [v_1 + w_{1m} \geq z].$$

Due to the fact that $u_m = \max_{1 \leq n \leq N} u_{mn}$, the CDF of $u_m$ is given by

$$F_{u_m}(x) = (1 - e^{-\frac{x}{\xi}})^N.$$  \hfill (34)

Accordingly, we obtain $\Pr [u_m \geq z]$ as

$$\Pr [u_m \geq z] = 1 - (1 - e^{-\frac{z}{\xi}})^N.$$  \hfill (35)

To derive $F_{Z_{1m}}(z|v_1)$, we consider $\Pr [v_1 + w_{1m} \geq z]$ for two cases, namely, $z < v_1$ and $z \geq v_1$. When $z < v_1$, $v_1 + w_{1m}$ is always larger than $z$. As such, we obtain

$$F_{Z_{1m}}(z|v_1) = (1 - e^{-\frac{z}{\xi}})^N.$$  \hfill (36)

On the other hand, when $z \geq v_1$, we have

$$\Pr [v_1 + w_{1m} \geq z] = \Pr [w_{1m} \geq z - v_1] = e^{-\frac{z-v_1}{\xi}}.$$  \hfill (37)

Accordingly, we obtain

$$F_{Z_{1m}}(z|v_1) = 1 - (1 - e^{-\frac{z}{\xi}})^N e^{-\frac{z-v_1}{\xi}}.$$  \hfill (38)

$$= 1 - e^{-\frac{z}{\xi}} + \sum_{n=0}^{N} \binom{N}{n} (-1)^{n-1} e^{-\frac{n(z-v_1)}{\xi}}.$$  \hfill (39)

From (36) and (39), the CDF of $Z_1$ can be written as

$$F_{Z_1}(z) = \int_{0}^{z} F_{Z_{1m}}(z|v_1) f_{v_1}(v_1) dv_1$$

$$= \int_{0}^{z} F_{Z_{1m}}(z|v_1) f_{v_1}(v_1) dv_1 + \int_{z}^{\infty} F_{Z_{1m}}(z|v_1) f_{v_1}(v_1) dv_1.$$  \hfill (40)

By using the PDF of $v_1$, given by $f_{v_1}(x) = \sum_{m=1}^{N} (-1)^{m-1} \binom{M}{m} \frac{m}{\xi} e^{-\frac{mx}{\xi}}$, and the binomial expansion into (40), we obtain the desired CDF of $Z_1$ as shown in (19) of Theorem 1, which completes the proof.

APPENDIX B

PROOF OF THEOREM 2

Since $w_{1m^*}$ is the maximum of $M$ variables $\{w_{1m}\}_{1 \leq m \leq M}$, as per the selection criterion characterized by (10), it holds that its distribution is given by

$$f_{w_{1m^*}}(x) = \sum_{m=1}^{M} (-1)^{m-1} \frac{M}{m} \frac{m}{\xi} e^{-\frac{mx}{\xi}}.$$  \hfill (41)

We next derive the CDF of $u_{m^*n^*}$ and $v_{1m^*}$, as per the selection criterion characterized by (11). We first write the CDF of $u_{m^*n^*}$ as

$$F_{u_{m^*n^*}}(x) = \Pr [u_{m^*n^*} < x]$$

$$= \sum_{n=1}^{N} \Pr [u_{m^*n^*} < x, \min (u_{m^*n^*, v_{1n}}) > \theta_n],$$  \hfill (42)

where $\theta_n$ is defined as

$$\theta_n = \max_{n_1=1, \ldots, N, n_1 \neq n} \min (u_{m^*n_1}, v_{1n_1}).$$  \hfill (43)
Due to the symmetry among $N$ end-to-end paths, $F_{u_{m^*},n^*}(x)$ in (42) is written as

$$F_{u_{m^*},n^*}(x) = N \Pr[u_{m^*1} < x, u_{m^*1} > \theta_1, v_{11} > \theta_1]$$

$$= N \int_0^x \int_{\theta_1}^\infty f_{\theta_1}(\theta_1) f_{u_{m^*1}}(u_{m^*1})$$

$$\times f_{v_{11}}(v_{11}) dv_{11} du_{m^*1} d\theta_1. \quad (44)$$

We first note that $u_{m^*1}$ and $v_{11}$ follow exponential distribution with mean $\alpha$ and $\beta_1$, respectively. We also note that the CDF of $\theta_1$ is given by

$$F_{\theta_1}(x) = \Pr[\theta_1 < x]$$

$$= (\Pr[\min(u_{m^*2}, v_{12}) < x])^{N-1}$$

$$= \sum_{n=1}^{N-1} (-1)^{n} \left( \frac{N-1}{n} \right)e^{-\frac{c_1}{n}}, \quad (45)$$

where $\zeta = \alpha \beta_1/(\alpha + \beta_1)$. By applying these results and solving the integral in (44), we obtain $F_{u_{m^*},n^*}(x)$ as

$$F_{u_{m^*},n^*}(x) = 1 - \sum_{n=0}^{N-1} b_{4,n} \left[ \frac{\zeta}{\zeta + n\beta_1} e^{-\frac{x}{\zeta}} \right.$$

$$\left. + \left( \frac{1}{n+1} - \frac{\zeta}{\zeta + n\beta_1} \right) e^{-\frac{(n+1)x}{\zeta}} \right], \quad (46)$$

where $b_{4,n} = N(-1)^n \frac{N!}{(N-n)!}$. Similarly, we derive the CDF of $v_{1n^*}$ as

$$F_{v_{1n^*}}(x) = 1 - \sum_{n=0}^{N-1} b_{4,n} \left[ \frac{\zeta}{\zeta + n\alpha} e^{-\frac{x}{\zeta}} \right.$$

$$\left. + \left( \frac{1}{n+1} - \frac{\zeta}{\zeta + n\alpha} \right) e^{-\frac{(n+1)x}{\zeta}} \right], \quad (47)$$

Using (46), (46), and (47) the CDF of $Z$ is given by

$$F_Z(z) = \Pr[\min(u_{m^*n^*}, v_{1n^*} + w_{1m^*}) < z]$$

$$= 1 - \Pr[u_{m^*n^*} \geq z] \cdot \Pr[v_{1n^*} + w_{1m^*} \geq z]. \quad (48)$$

Note that $\Pr[u_{m^*n^*} \geq z] \neq 1 - F_{u_{m^*},n^*}(z)$ can be easily obtained using (46). Therefore, $\Pr[v_{1n^*} + w_{1m^*} \geq z]$ is calculated as

$$\Pr[v_{1n^*} + w_{1m^*} \geq z] = 1 - \Pr[v_{1n^*} + w_{1m^*} < z]$$

$$= 1 - \int_0^z F_{v_{1n^*}}(z - w) f_{w_{1m^*}}(w) dw. \quad (49)$$

Applying (41) and (47) into (49) we are able to obtain $\Pr[v_{1n^*} + w_{1m^*} \geq z]$. This leads to the analytical CDF of $Z$, as shown in (24) in Theorem 2. This completes the proof.

**APPENDIX C**

**PROOF OF THEOREM 3**

By applying the approximation of $e^{-x} \simeq 1 - x$ for small value of $|x|$ into (36) and (39), we obtain the asymptotic $F_{Z_{1m}}(z)$ as

$$F_{Z_{1m}}(z) \simeq \left( \frac{z}{\alpha} \right)^N, \quad (50)$$

for $z < v_1$ and

$$F_{Z_{1m}}(z) \simeq \left( \frac{z}{\alpha} \right)^N + \frac{z - v_1}{\epsilon_1}, \quad (51)$$

for $z \geq v_1$. Then the asymptotic CDF of $Z_1$ is derived as

$$F_{Z_1}(z) \simeq \int_0^z \left( \frac{z}{\alpha} \right)^N + \frac{z - v_1}{\epsilon_1} f_{v_1}(v_1) dv_1$$

$$\quad + \int_z^{\infty} \left( \frac{z}{\alpha} \right)^N f_{v_1}(v_1) dv_1$$

$$\simeq \int_0^{v_1} \left( \frac{z}{\alpha} \right)^N + \frac{z - v_1}{\epsilon_1} f_{v_1}(v_1) dv_1 + \frac{z}{\alpha} MN. \quad (52)$$

By applying the asymptotic $f_{v_1}(x) \simeq \frac{N(x)^{N-1}}{\beta_1^N}$ into (52) and then solving the resultant integral, we obtain the asymptotic CDF of $Z_1$ as shown in (27) of Theorem 3.

**APPENDIX D**

**PROOF OF THEOREM 4**

By using Taylor’s series approximation of $e^{-x} \simeq \sum_{n=0}^{\infty} \frac{(-x)^n}{n!}$ into (46) and (47), we obtain the asymptotic CDFs of $u_{m^*n^*}$ and $v_{1n^*}$ as

$$F_{u_{m^*},n^*}(x) \simeq \left( \frac{x}{\alpha} \right)^N \frac{\beta_1}{\alpha + \beta_1}, \quad (53)$$

and

$$F_{v_{1n^*}}(x) \simeq \left( \frac{x}{\alpha} \right)^N \frac{\alpha}{\alpha + \beta_1}, \quad (54)$$

respectively, with the aid of [47, Eq. (0.154.3), (0.154.4)]. From (48), we then derive the asymptotic CDF of $Z$ as

$$F_Z(z) \simeq 1 - \left( \frac{z}{\alpha} \right)^N \frac{\beta_1}{\alpha + \beta_1} \Pr[v_{1n^*} + w_{1m^*} \geq z]. \quad (55)$$

We note that the asymptotic $\Pr[v_{1n^*} + w_{1m^*} \geq z]$ in (55) is computed as

$$\Pr[v_{1n^*} + w_{1m^*} \geq z] = 1 - \int_0^z F_{v_{1n^*}}(z - w) f_{w_{1m^*}}(w) dw$$

$$\simeq 1 - \frac{\alpha}{\alpha + \beta_1} \int_0^z \left( \frac{z - w}{\alpha} \right)^N f_{w_{1m^*}}(w) dw$$

$$= 1 - \frac{z^{M+N}}{\alpha \beta_1} \sum_{n=0}^{N} (-1)^n \left( \frac{N}{n} \right) \frac{1}{M + n}. \quad (56)$$

where the asymptotic PDF $f_{w_{1m^*}}(x) \simeq \frac{M}{\alpha^{M-1}} x^{M-1}$ is applied to obtain the last equality. Combining the results in (55) and (56), we obtain the asymptotic CDF of $Z$ as shown in (31) of Theorem 4.


**Lisheng Fan** received the bachelor and master degrees from Fudan University and Tsinghua University, China, in 2002 and 2005, respectively, both from Department of Electronic Engineering. He received the Ph.D. degree from Department of Communications and Integrated Systems of Tokyo Institute of Technology, Japan, in 2008. From 2014, he has been an Professor. His research interests span in the areas of wireless cooperative communications, physical-layer secure communications, interference modeling, and system performance evaluation. Lisheng Fan has published many papers in international journals such as IEEE Transaction on Wireless Communications, IEEE Transaction on Vehicular Technology, IEEE Communications Letters and IEEE Wireless Communications Letters, as well as papers in conferences such as IEEE ICC, IEEE Globecon, and IEEE WCNC. He is a guest editor of EURASIP Journal on Vehicular Technology, IEEE Communications Letters and EURASIP Journal on Advances in Signal Processing. He was awarded the Best Paper Award at the IEEE Vehicular Technology Conference (VTC-Spring) in 2013, IEEE International Conference on Communications (ICC) 2014. He is the recipient of prestigious Royal Academy of Engineering Research Fellowship (2015-2020).

**Nan Yang** (S’09–M’11) received the B.Sc. degree in electronics from China Agricultural University in 2005, and the M.Sc. and Ph.D. degrees in electronic engineering from the Beijing Institute of Technology in 2007 and 2011, respectively. He is currently a Future Engineering Research Leadership Fellow and a Lecturer in the Research School of Engineering at the Australian National University. Prior to this he was a Postdoctoral Research Fellow at the University of New South Wales (UNSW) from 2012 to 2014; a Postdoctoral Research Fellow at the Commonwealth Scientific and Industrial Research Organization from 2010 to 2012; and a visiting Ph.D. student at UNSW from 2008 to 2010. He received the Top Reviewer Award of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY in 2015, the IEEE Communications Society Asia-Pacific Outstanding Young Researcher Award in 2014, the Exemplary Reviewer Certificate of the IEEE WIRELESS COMMUNICATIONS LETTERS in 2014, the Exemplary Reviewer Certificate of the IEEE COMMUNICATIONS LETTERS in 2012 and 2013, and the Best Paper Award at the IEEE 77th Vehicular Technology Conference in 2013. He is currently serving on the Editorial Board of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY and the TRANSACTIONS ON EMERGING TELECOMMUNICATIONS TECHNOLOGIES. His general research interests lie in the areas of communications theory and signal processing, with specific interests in cyber-physical security, massive multi-antenna systems, heterogeneous networks, millimeter-wave communications, collaborative networking, and molecular communications.

**Trung Q. Duong** (S’05, M’12, SM’13) received his Ph.D. degree in Telecommunications Systems from Blekinge Institute of Technology (BTH), Sweden in 2012. Since 2013, he has joined Queen’s University Belfast, UK as a Lecturer (Assistant Professor). His current research interests include cooperative communications, cognitive radio networks, physical layer security, massive MIMO, cross-layer design, mm-waves communications, and localization for radios and networks. He is the author or co-author of 170 technical papers published in scientific journals and presented at international conferences.

Dr. Duong currently serves as an Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE COMMUNICATIONS LETTERS, IET COMMUNICATIONS, WILEY TRANSACTIONS ON EMERGING TELECOMMUNICATIONS TECHNOLOGIES, and ELECTRONICS LETTERS. He has also served as the Guest Editor of the special issue on some major journals including IEEE JOURNAL IN SELECTED AREAS ON COMMUNICATIONS, IET COMMUNICATIONS, IEEE WIRELESS COMMUNICATIONS MAGAZINE, IEEE COMMUNICATIONS LETTERS, EURASIP JOURNAL ON WIRELESS COMMUNICATIONS AND NETWORKING, EURASIP JOURNAL ON ADVANCES IN SIGNAL PROCESSING. He was awarded the Best Paper Award at the IEEE Vehicular Technology Conference (VTC-Spring) in 2013, IEEE International Conference on Communications (ICC) 2014. He is the recipient of prestigious Royal Academy of Engineering Research Fellowship (2015-2020).

**Maged Elkashlan** (M’06) received the Ph.D. degree in Electrical Engineering from the University of British Columbia, Canada, 2006. From 2006 to 2007, he was with the Laboratory for Advanced Networking at University of British Columbia. From 2007 to 2011, he was with the Wireless and Networking Technologies Laboratory at Commonwealth Scientific and Industrial Research Organization (CSIRO), Australia. During this time, he held an adjunct appointment at University of Technology Sydney, Australia. In 2011, he joined the School of Electronic Engineering and Computer Science at Queen Mary University of London, UK, as an Assistant Professor. He also holds visiting faculty appointments at the University of New South Wales, Australia, and Beijing University of Posts and Telecommunications, China. His research interests fall into the broad areas of communication theory, wireless communications, and statistical signal processing for distributed data processing, millimeter wave communications, cognitive radio, and wireless security.

Dr. Elkashlan currently serves as an Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and the IEEE COMMUNICATIONS LETTERS. He also serves as the Lead Guest Editor for the special issue on “Green Media: The Future of Wireless Multimedia Networks” of the IEEE WIRELESS COMMUNICATIONS MAGAZINE, Lead Guest Editor for the special issue on “Millimeter Wave Communications for 5G” of the IEEE COMMUNICATIONS MAGAZINE, Guest Editor for the special issue on “Energy Harvesting Communications” of the IEEE COMMUNICATIONS LETTERS, and Guest Editor for the special issue on “Location Awareness for Radios and Networks” of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. He received the Best Paper Award at the IEEE Vehicular Technology Conference (VTC-Spring) in 2013. He received the Exemplary Reviewer Certificate of the IEEE Communications Letters in 2012.
George K. Karagiannidis (M’96–SM’03–F’14) was born in Pithagorion, Samos Island, Greece. He received the University Diploma (5 years) and PhD degree, both in electrical and computer engineering from the University of Patras, in 1987 and 1999, respectively. From 2000 to 2004, he was a Senior Researcher at the Institute for Space Applications and Remote Sensing, National Observatory of Athens, Greece. In June 2004, he joined the faculty of Aristotle University of Thessaloniki, Greece where he is currently Professor in the Electrical Computer Engineering Dept. and Director of Digital Telecommunications Systems and Networks Laboratory. His research interests are in the broad area of digital communications systems with emphasis on communications theory, energy efficient MIMO and cooperative communications, satellite communications, cognitive radio, localization, smart grid and optical wireless communications. He is the author or co-author of more than 300 technical papers published in scientific journals and presented at international conferences. He is also author of the Greek edition of a book on "Telecommunications Systems" and co-author of the book "Advanced Optical Wireless Communications Systems", Cambridge Publications, 2012. Dr. Karagiannidis has been a member of Technical Program Committees for several IEEE conferences such as ICC, GLOBECOM, VTC, etc. In the past he was Editor in IEEE Transactions on Communications, Senior Editor of IEEE Communications Letters and Editor of the EURASIP Journal of Wireless Communications Networks. He was Lead Guest Editor of the special issue on "Optical Wireless Communications" of the IEEE Journal on Selected Areas in Communications and Guest Editor of the special issue on "Large-scale multiple antenna wireless systems". Dr. Karagiannidis has been selected as a 2015 Thomson Reuters Highly Cited Researcher and since January 2012 he is the Editor-in Chief of IEEE Communications Letters.