On the Physical-Layer Security of a Dual-Hop UAV-Based Network in the Presence of Per-Hop Eavesdropping and Imperfect CSI

Elmehdi Illi, Member, IEEE, Marwa Qaraqe, Senior Member, IEEE, Faissal El Bouanani, Senior Member, IEEE, and Saif Al-Kuwari, Senior Member, IEEE

Abstract—In this article, the physical-layer security of a dual-hop unmanned aerial vehicle-based wireless network, subject to imperfect channel state information (CSI) and mobility effects, is analyzed. Specifically, a source node (S) communicates with a destination node (D) through a decode-and-forward relay (R), in the presence of two wiretappers (E₁ and E₂) independently trying to compromise the two hops. Furthermore, the transmit nodes (S, R) have a single transmit antenna, while the receivers (R, D, E₁, E₂) are equipped with multiple receive antennas. Based on the per-hop signal-to-noise ratios (SNRs) and correlated secrecy capacities’ statistics, a closed-form expression for the secrecy intercept probability (IP) metric is derived, in terms of key system parameters. Additionally, asymptotic expressions are revealed for two scenarios, namely: 1) mobile nodes with imperfect CSI and 2) static nodes with perfect CSI. The results show that a zero secrecy diversity order is manifested for the first scenario, due to the presence of a ceiling value of the average SNR, while the IP drops linearly at high average SNR in the second one, where the achievable diversity order depends on the fading parameters and number of antennas of the legitimate links/nodes. Furthermore, for static nodes, the system can be castigated by a 15-dB secrecy loss at IP = 3 × 10⁻³, when the CSI imperfection power raises from 0 to 10⁻³. Finally, the higher the legitimate nodes’ speed, carrier frequency, delay, and/or relay’s decoding threshold SNR, the worse is the system’s secrecy. Monte Carlo simulations endorse the derived analytical results.

Index Terms—Decode-and-forward (DF), imperfect channel state information (CSI), independent eavesdroppers, intercept probability (IP), physical-layer (PHY) security.

I. INTRODUCTION

With the rapid growth of wireless communication technologies throughout the last few years, the Internet of Things (IoT) paradigm strongly emerged as a leading actor of the fifth generation (5G) wireless network standard and beyond [1]. Practically, IoT architectures and protocols can be implemented in numerous promising services and applications, such as traffic control, smart home, smart grids, factories, and healthcare facilities [2], [3]. Recent studies forecast around 500 billion connected IoT devices over the globe by 2030 [4]. Nonetheless, despite the aforesaid features and applications, guaranteeing a fair functioning of such IoT networks is challenging in underserved areas (e.g., deserts and mountains), or in disaster zones noncovered by wireless cellular infrastructure [2], [5].

Unmanned aerial vehicles (UAVs) have been attracting remarkable interest on the wireless community as an alternative means of real-time communication and extended network coverage [6]. UAVs can be conveniently implemented in disaster regions with limited cellular coverage to act as flying base stations (BSs), where they can provide enhancements in both radio access and backhaul connectivity with clearly improved coverage [7]. Additionally, due to the high probability of the presence of line-of-sight links, UAVs can be involved in other use cases, such as media production, real-time surveillance, and automatic target detection [8], [9].

Small UAVs (i.e., below 5 kg) generally operate in swarms [8], [10]. In such a scenario, multihop relaying is implemented to reliably convey information signals between a distant source and destination nodes via routing techniques [11]. At the physical layer (PHY), two main relaying protocols are usually deployed, namely: 1) amplify-and-forward (AF), also known as the nonregenerative relaying scheme and 2) decode-and-forward (DF), also known as the regenerative relaying one. The former, although less complex, can provide acceptable performance in noise-limited scenarios. However, the higher the noise power, the worse its performance becomes due to noise amplification [12]. On the other hand, DF generally provides better performance but requires complex digital signal processing and computing circuits onboard compared to the AF scheme [13].

PHY security (PLS) has gained attention in the wireless communication community from both academia and industry [14]. The open broadcast nature of radio links exposes legitimate communication to permanent threats from malign users [15]. Therefore, information security has been regarded as a fundamental requirement, particularly on the 5 GB and especially for IoT. Upper layers look at ensuring confidentiality and authentication through key-based cryptographic
schemes [16]. Nonetheless, such schemes are often faced by several challenges and limitations in IoT networks, such as 1) the complexity of key generation and distribution in large-scale decentralized networks and 2) the operational complexity of advanced cryptographic schemes, which poses stringent burdens on low-power devices [17]. To this end, PLS\(^1\) has been a popular candidate for effective low-complexity security solutions. Its core advantage lies in establishing key-less information-theoretically secure communications by exploiting the random nature of the propagation channel along with PHY parameters, to provide high security levels with low overhead. Despite these advantages, PLS can exhibit several challenges in UAV/vehicular networks, especially when the communication is under the joint effect of imperfect channel estimation and nodes mobility, leading to outdated channel state information (CSI) with estimation errors [19].

A. Related Work

Throughout the literature, extensive research work has inspected the PLS of dual-hop or multihop communication systems [16], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31]. Fan et al. [20] proposed relay selection schemes in a multiuser network, considering AF relays to improve the secrecy level of the system. In [21] and [22], the secrecy performance was investigated under the joint use of maximal-ratio combining (MRC) and zero-forcing beamforming in a cognitive-radio network (CRN) and a noncognitive one, respectively. The work in [23] inspected secrecy metrics for a dual-hop DF-based multiuser network, under the presence of various eavesdroppers overhearing the second hop. Importantly, Illi et al. [14], [16], Yang et al. [25], Liao et al. [27], Lei et al. [28], Pattanayak et al. [30], and Bouabdellah and Bouanami [32] analyzed the end-to-end PLS of mixed radio-frequency (RF)-optical wireless communication (OWC) systems, where the optical link operates either indoor (i.e., visible light communications), outdoor (i.e., free-space optics), or in the marine medium (i.e., underwater OWC).

Nonetheless, the above-mentioned work was restricted to 1) assuming the presence of eavesdroppers in only one of the two hops and 2) the fact that all nodes are static with perfect CSI. In fact, due to the nodes’ mobility, the channel between each pair of transceivers within the network undergoes time selectivity, where the fading realizations decorrelate in time according to the well-known Jakes’ model [33], [34]. To this end, the estimated CSI at the packet preamble will be outdated compared to the actual one when processing the received signal. Furthermore, due to the imperfections in the receivers’ tracking loops, the CSI estimation suffers from estimation noise in addition to the time selectivity [35].

A number of other works from the literature tackled the secrecy performance of dual-hop networks by encompassing the joint distortions due to the CSI time selectivity and/or estimation errors. For instance, Zhao et al. [24] investigated the secrecy performance of a dual-hop network with multiantenna nodes employing transmit antenna selection along with MRC, under the presence of a single eavesdropper, and considering Nakagami-m fading channels. A similar setup was analyzed in [36] by assuming single-antenna nodes and a Rayleigh fading model. The work in [31] dealt with the performance of an AF-based dual-hop scheme with single-antenna mobile nodes and a single eavesdropper, where the two hops are subject to Rayleigh and double Rayleigh fading models. The latter work was extended in [37] by considering the generalized Nakagami-m and double Nakagami-m fading models. Moreover, Lei et al. [38] investigated the secrecy outage probability performance of a dual-hop mixed RF-FSO system, where the CSI is subject to time selectivity and estimation errors. Al-Qahtani et al. [39] analyzed the system’s secrecy in a multirelay dual-hop scheme subject to the presence of one malicious node and assuming single-antenna transceivers. In addition, Pandey et al. [40] tackled the secrecy analysis of a dual-hop AF-based CRN, subject to Rayleigh and double-Rayleigh fading and assuming single-antenna devices. In [41], the secrecy performance of a dual-hop CRN is carried out under mobility constraints and assuming a single eavesdropper and single-antenna devices. The performance of a relay-based device-to-device network with full-duplex consideration and multiple-antenna nodes was investigated in [42] by considering yet again a single eavesdropper. Le and Tsiftsis [43] investigated the secrecy level of a dual-hop network operating with various opportunistic relays and a single eavesdropper by considering a correlation between the legitimate and wiretap channels. Similarly, the authors carried out a secrecy performance analysis in [44] for a two-way dual-hop communication system by assuming a multiantenna source and destination nodes, along with a single malign one. Moreover, the work in [45] and [46] evaluated the security gains of employing artificial noise/jamming techniques in cooperative dual-hop networks.

B. Motivation

Although all the above-mentioned works have inspected the secrecy of cooperative dual-hop networks with the joint effect of imperfect CSI and node mobility, all of these works assume either the presence of 1) a single or multiple collaborative eavesdroppers within one hop; 2) single-antenna nodes; or 3) the use of the basic Rayleigh fading model. In fact, few works in the literature were reported to deal with independent eavesdroppers attacking each hop. For instance, Pattanayak et al. [30] treated a dual-hop FSO-RF scheme with two parallel paths, with the presence of multiple eavesdroppers looking to compromise the RF hop. Likewise, Singh et al. [47] investigated the impact of fading and turbulence on the secrecy performance of a dual-hop FSO-RF system with two eavesdroppers attempting to independently intercept the FSO and RF hops. A parallel analysis of a similar setup was conducted in [48] by adding the residual hardware impairments constraint along with energy harvesting into the analysis.

---

\(^1\)PLS generally refers to the use of PHY parameters to ensure either data confidentiality and/or authentication. PLS can be broadly categorized as PHY authentication (PLA) [15], PHY key generation (PLKG) [18], or conventional Wyner-inspired PLS. In this article, we adopt the latter, aiming at ensuring data confidentiality based on the system secrecy capacity.
Ill et al. [49] analyzed the secrecy performance of a dual-hop hybrid terrestrial–satellite (HTS) system with an optical feeder, subject to the presence of an eavesdropper per each hop. Finally, a similar setup was analyzed in [32] by considering an RF-FSO HTS system. Nevertheless, the analysis in all these above-mentioned work [30], [32], [47], [48], [49] was restricted to a single-antenna assumption in some of or all the nodes along with assuming static nodes with perfect CSI estimation. At the same time, the presence of UAVs and vehicular networks has been emphatically emerging in contemporary and futuristic networks. In particular, flying BSs (e.g., UAVs, high-altitude platforms, etc.) are strongly advocated to be a key actor in space-to-ground integrated communications, whereby the wireless communication community aims at providing connectivity solutions to underserved or unconnected zones [50]. Such mobile networks, often organized in swarms [8], are prone to numerous threats and security challenges, in which potential malign users attempt to independently compromise each hop of the communication network. Therefore, it is crucial to conduct a secrecy analysis of such mobile networks, by assuming CSI imperfections, mobility effects, and the presence of independent per-hop eavesdroppers.

C. Contributions

Capitalizing on the above motivations, we aim in this article to analyze the PLS of a dual-hop UAV-assisted wireless communication system (WCS) under the impact of node mobility and imperfect channel estimation. In particular, a source node (S) communicates with a destination node (D) through a DF-based relay (R). At the same time, two eavesdroppers (E₁ and E₂) are attempting to independently intercept the S–R and R–D communications, respectively. It is assumed that all transmitters (S, R) have single transmit antennas, while receivers (R, D, E₁, E₂) employ the MRC technique leveraging the multiple receive antennas onboard. Moreover, all the channels are assumed to follow a Nakagami-m fading model. Hence, this work differs from [24], [31], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45], and [46] by considering independent eavesdroppers per each of the two hops, and from [30], [32], [47], [48], and [49] by taking into account the distortions due to mobility and CSI imperfect estimation. To the best of our knowledge, our work is the first that takes into consideration the joint effect of transceivers mobility and CSI imperfect estimation. To analyze the PLS of a dual-hop UA V-assisted wireless communication system (WCS) under the impact of node mobility and imperfect channel estimation. At the same time, the presence of UAVs and vehicular networks has been emphatically emerging in contemporary and futuristic networks. In particular, flying BSs (e.g., UAVs, high-altitude platforms, etc.) are strongly advocated to be a key actor in space-to-ground integrated communications, whereby the wireless communication community aims at providing connectivity solutions to underserved or unconnected zones [50]. Such mobile networks, often organized in swarms [8], are prone to numerous threats and security challenges, in which potential malign users attempt to independently compromise each hop of the communication network. Therefore, it is crucial to conduct a secrecy analysis of such mobile networks, by assuming CSI imperfections, mobility effects, and the presence of independent per-hop eavesdroppers.

D. Organization

The remainder of this article is organized as follows. Section II describes the adopted system and channel models, and Section III provides useful statistical properties for the per-hop SNRs. In Section IV, exact closed-form and asymptotic expressions for the IP metric are provided with several insights on the impact of key system parameters on the derived results. Section V presents numerical results and discussions. Finally, Section VI concludes this article.

E. Notations

Vectors are denoted by bold letters, \( \mathcal{CN}(\mu, \sigma^2) \) refers to complex Gaussian distribution with mean \( \mu \) and variance \( \sigma^2 \), \(|.|\) is the absolute value, \( \mathbb{E} [.|...] \) refers to the expected value of a random variable, and \( \hat{h} \) and \( \hat{h} \) refer to the outdated version and estimate of \( h \), respectively. Furthermore, \( J_\mu(.) \) is the noise powers, CSI estimation error variance, and the number of receive antennas.

2) Capitalizing on the statistical properties of the per-hop SNR, we derive an exact closed-form expression for the system’s intercept probability (IP) metric in terms of key system and channel parameters; namely, the average per-branch SNR (function of the mobility-dependent correlation coefficient, depending on the carrier frequency, relative speed, and delay), the number of antennas onboard the legitimate and wiretap nodes, per-hop fading severity parameter, and the relay decoding threshold SNR.

3) The impact of the main system parameters on the setup’s security level is broadly discussed based on the derived analytical expressions. In particular, the IP behavior is inspected for particular setup parameters’ values, e.g., low and high values of decoding threshold SNR, various values of fading severity parameters, and average fading powers.

4) Numerical and simulation results are conducted to validate all the derived analytical results. We show that the system’s secrecy is significantly influenced by nodes’ relative speed, CSI estimation noise level, threshold SNR fading severity parameters, and the number of antennas onboard.

5) To obtain more insights and observations from the above results, asymptotic expressions in the high SNR regime are provided for two scenarios, namely: a) a generalized scenario of mobile nodes and imperfect CSI and b) an ideal scenario for static UAVs and perfect CSI estimation. Based on these expressions, the respective secrecy diversity order is retrieved for these two scenarios. We show that the secrecy performance of the first scenario exhibits a zero diversity order at high SNR, regardless of the number of antennas, fading parameters’ values, and threshold SNR. Nevertheless, a secrecy diversity order of \( \min(m_{SR}N_R, m_{RD}N_D) \) is reached for the second scenario, with \( m_{SR} \) and \( m_{RD} \) denote the fading severity of the S–R and R–D hops, respectively, while \( N_R \) and \( N_D \) refer to the number of antennas onboard \( R \) and \( D \), respectively.
there are no direct links from $S$ to $D$.

**II. SYSTEM MODEL**

We consider a dual-hop UAV-based WCS consisting of a source node ($S$) connected to a destination ($D$) via a relay ($R$) employing DF protocol. Two eavesdroppers, $E_1$ and $E_2$, try to intercept the legitimate messages broadcasted by $S$ and $R$, in the first and second time slots, respectively. We assume that the transmit nodes ($S, R$) are equipped with a single transmit antenna while all receiving nodes ($R_1, D, E_1$, and $E_2$) are equipped with $N_R, N_D, N_{E_1}$, and $N_{E_2}$ receiving antennas, respectively. Finally, due to the limited UAV transmit power and the significant distance between $S$ and $D$, we assume that there are no direct links from $S$ to $D$ and $E_2$. Without loss of generality, the received signals at $R, D, E_1$, and $E_2$ are expressed as

$$y_U = \sqrt{P_S} s_U h_{SU} + n_U, \quad U \in \{R, E_1\}$$

$$y_V = \sqrt{P_R} x y_{VX} + n_V, \quad V \in \{D, E_2\}$$

where $P_S$ and $P_R$ are $S$ and $R$'s transmit power, respectively.

Let $L_{XZ} = G_X^{(0)} G_Z^{(p)} \left( \frac{c}{4\pi f_c d_0} \right)^2 \left( \frac{d_0}{d_{XZ}} \right)^{\kappa}$

where $XZ \in \{SR, SE_1, RD, RE_2\}$ is the free-space path-loss (FSPL) term of the $X$–$Z$ link, where $G_X^{(0)}$ and $G_Z^{(p)}$ are the gains of $X$'s transmit antenna and Z's receive one, respectively, $c$ is the speed of light, $f_c$ is the carrier frequency, $d_0$ is a reference distance, $d_{XZ}$ is the distance between nodes $X$ and $Z$, and $\kappa$ is the environment-dependent FSPL exponent [51]. Furthermore, $x$ is the transmit signal, $y'$ is the coded and regenerated one by $R$, with $E[x] = E[y'] = 1$, $n_U$ and $n_V$ are the additive white Gaussian noise (AWGN) realizations at either $R, D, E_1$, or $E_2$'s antennas, which are independent and identically distributed (i.i.d.) zero-mean complex Gaussian random variables (ZMCGRVs) with distribution $\mathcal{CN}(0, \sigma_{h_{XZ}}^2)$, with $Z \in \{U, V\}$. Additionally

$$h_{SU} = \begin{bmatrix} h_{SU}^{(0)} \\ \vdots \\ h_{SU}^{(N_{SU})} \end{bmatrix}^T$$

and

$$h_{RV} = \begin{bmatrix} h_{RV}^{(0)} \\ \vdots \\ h_{RV}^{(N_{RV})} \end{bmatrix}^T$$

are the $S$–$U$ and $R$–$V$ channel fading vector between $S$/$R$'s transmit antenna and $U$/$V$’s receive ones, whose elements are complex-valued i.i.d. random variables with a fading envelope assumed to follow Nakagami-$m$ distribution with fading parameter $m_{XZ}$ and average fading power $\Omega_{XZ} = E[h_{XZ}^2]$.

Due to the UAV nodes’ mobility, the actual channel fading coefficients ($h_{SU}$ and $h_{RV}$) are different from the estimated one. Such a relationship can be expressed through the widely known first-order autoregressive process, $AR(1)$, as follows [19], [35]:

$$h_{XZ} = \rho_{XZ} h_{XZ} + \sqrt{1 - \rho_{XZ}^2} w_{XZ}$$

where $\rho_{XZ}$ is the underlying correlation coefficient, with $XZ \in \{SR, SE_1, RD, RE_2\}$, $\tilde{h}_{XZ}$ is the exact outdated CSI vector, and $w_{XZ}$ is the mobility noise vector whose entries are i.i.d. ZMCGRVs with distribution $\mathcal{CN}(0, \sigma_{h_{XZ}}^2)$. On the other hand, the correlation coefficient $\rho_{XZ}$ is defined, according to Jakes’ model, as [33], [35]

$$\rho_{XZ} = J_0 \left( \frac{2\pi v_{XZ} f_c \tau}{c} \right)$$

which is a function of the two nodes’ relative speed $v_{XZ}$ along with the delay time $\tau$ between the CSI estimation and signal reception, and the carrier frequency $f_c$. Such a relative speed between two nodes (i.e., $v_{XZ}$) can illustrate two nodes moving in the same direction; i.e., $v_{XZ} = |v_X - v_Z|$ or in opposite ones; i.e., $v_{XZ} = v_X + v_Z$. Moreover, in addition to the channel decorrelation over time, its estimation is also subject to the inherent noise in the receiver’s tracking loop. The final expression of the channel fading coefficient can be expressed as [35]

$$\tilde{h}_{XZ} = \rho_{XZ} \left( \hat{h}_{XZ} + \varepsilon_{XZ} \right) + \sqrt{1 - \rho_{XZ}^2} w_{XZ}$$

where $\hat{h}_{XZ}$ is the estimated channel vector, and $\varepsilon_{XZ}$ is the estimation noise vector with i.i.d. ZMCGRVs entries with distribution $\mathcal{CN}(0, \sigma_{h_{XZ}}^2)$.

**Remark 1:** The channel’s mobility-dependent correlation coefficient (i.e., $\rho_{XZ}$), given in (7), manifests the impact of nodes’ mobility on the time-varying statistical behavior of the channel. Such a coefficient is expressed in terms of the nodes’ relative speed, carrier frequency, delay, and speed of light. A static scenario, i.e., $v_{XZ} = 0$, corresponds to $\rho_{XZ} = 1$, which refers to a perfect correlation case. Likewise, at very high $v_{XZ}$ and/or $f_c$ and/or $\tau$, $\rho_{XZ}$ tends to 0, yielding severe channel time variations, in which the estimated CSI is completely uncorrelated with the actual one. Also, it worth mentioning that $J_0(x)$ in (7), with $x = (2\pi v_{XZ} f_c \tau)/c$, is a decreasing function of $v_{XZ}$ and/or $f_c$ and/or $\tau$ over $x \in [0, x_0]$, with $x_0 = 3.8317$ being the function’s minima that can be found numerically by retrieving the first zero of $J_0(x)$.

At the legitimate and wiretap nodes (i.e., $R, D, E_1$, or $E_2$), the MRC receiver is used to combine the received signals copies on its various diversity branches. To this end, the combined signal at the output of the MRC receiver at such nodes
can be formulated as
\[
\gamma^\text{(MRC)}_Z = \sqrt{P_X L_X} \left( \rho_{XZ} \phi_{XZ} \hat{h}_{XZ} u + \rho_{XZ} \phi_{XZ} \varphi_{XZ} u \right.
\]
\[
+ \phi_{XZ} \sqrt{1 - \rho_{XZ}^2} \mathbf{w}_{XZ} u \left. + \phi_{XZ} n_Z \right)
\tag{9}
\]
for \( XZ \in \{ SR, \ RD, \ SE_1, \ RE_2 \} \), where
\[
u = \begin{cases} x, & \text{if } Z \in \{ R, \ E_1 \} \\ x', & \text{if } Z \in \{ D, \ E_2 \} \end{cases}
\tag{10}
\]
and \( \phi_{XZ} = \left(||\hat{h}_{XZ}||^H/||\hat{h}_{XZ}||_2 \right) \) denotes the MRC combining vector. As a result, the corresponding instantaneous SNRs at the output of the receiving nodes’ combiners can be written using the following generalized form:
\[
\gamma_{XZ} = \frac{\rho_{XZ}^2 P_X L_X ||\hat{h}_{XZ}||^2}{P_X L_X (\rho_{XZ}^2 \sigma_{\epsilon_{XZ}}^2 + (1 - \rho_{XZ}^2) \sigma_{\phi_{XZ}}^2) + \sigma_{n_Z}^2}
\]
\[
= \sum_{i=1}^{N_Z} \gamma_{XZ}^{(i)} \tag{11}
\]
where
\[
\gamma_{XZ}^{(i)} = \frac{\rho_{XZ}^2 P_X L_X ||\hat{h}_{XZ}^{(i)}||^2}{P_X L_X (\rho_{XZ}^2 \sigma_{\epsilon_{XZ}}^2 + (1 - \rho_{XZ}^2) \sigma_{\phi_{XZ}}^2) + \sigma_{n_Z}^2}
\tag{12}
\]
denotes the instantaneous SNR at the \( i \)th branch, with an average value given as
\[
\gamma_{XZ} = \frac{\rho_{XZ}^2 \delta_{XZ}}{\Omega_{\delta_{XZ}} \left( \rho_{XZ}^2 \sigma_{\epsilon_{XZ}}^2 + (1 - \rho_{XZ}^2) \sigma_{\phi_{XZ}}^2 \right) + 1}
\tag{13}
\]
with
\[
\delta_{XZ} = \frac{P_X \Omega_{\gamma_{XZ}} L_X}{\sigma_{n_{XZ}}^2} \tag{14}
\]
Remark 2: 1) By differentiating the average SNR per branch in (13) with respect to \( \rho_{XZ} \), it yields
\[
\frac{\partial \gamma_{XZ}}{\partial \rho_{XZ}} = \frac{2 \rho_{XZ} \delta_{XZ} \left[ 1 + \frac{\delta_{XZ} \sigma_{\epsilon_{XZ}}^2}{\Omega_{\delta_{XZ}}} \right]}{\left( \frac{\delta_{XZ}}{\Omega_{\delta_{XZ}}} \left( \rho_{XZ}^2 \sigma_{\epsilon_{XZ}}^2 + (1 - \rho_{XZ}^2) \sigma_{\phi_{XZ}}^2 \right) + 1 \right)^2}
\tag{15}
\]
which is strictly positive. Henceforth, we can conclude that the effective per-branch average SNR is an increasing function of the correlation coefficient \( \rho_{XZ} \).

2) On the other hand, one can note from (13) that at higher average SNR values (i.e., \( \delta_{XZ} \rightarrow \infty \)), the effective average SNR per branch (i.e., \( \gamma_{XZ} \)) converges to the following ceiling value:
\[
\gamma_{XZ}^{(\infty)} = \frac{\rho_{XZ}^2 \Omega_{\gamma_{XZ}}}{(\rho_{XZ}^2 \sigma_{\epsilon_{XZ}}^2 + (1 - \rho_{XZ}^2) \sigma_{\phi_{XZ}}^2)} \tag{16}
\]
The above upper bound of \( \gamma_{XZ} \) leads to saturation floors in the system’s IP at high \( \delta_{XZ} \) values, within which the IP will be depending essentially on \( \rho_{XZ}^2, \sigma_{\epsilon_{XZ}}^2, \) and \( \sigma_{\phi_{XZ}}^2 \) values. As a consequence, we can conclude that the impact of nodes mobility jointly with estimation imperfections can lead to remarkable secrecy performance limitations which need to be considered in the design of such systems.

III. STATISTICAL PROPERTIES

In this section, statistical properties, such as the probability density function (PDF) and the cumulative distribution function (CDF) of the per-hop SNR, are presented.

From (11), one can infer that the instantaneous SNRs are proportional to the sum of Gamma-distributed squared fading envelopes at each branch of the receiver. To this end, the respective PDF and CDF of such instantaneous SNRs can be written as [16]
\[
f_{\gamma_{XZ}}(y) = \frac{\left( \frac{m_{XZ}}{\Gamma(m_{XZ})} \right)^{m_{XZ} - 1} \exp \left( -\frac{m_{XZ}}{\Gamma(m_{XZ})} y \right)}{\Gamma(m_{XZ})}
\tag{17}
\]
and
\[
F_{\gamma_{XZ}}(y) = \frac{\gamma_{inc}(m_{XZ} N_Z, \frac{m_{XZ}}{\Gamma(m_{XZ})})}{\Gamma(m_{XZ} N_Z)}
\tag{18}
\]
respectively.

IV. SECRECY ANALYSIS

In this section, exact closed-form and asymptotic expressions of the IP are derived, in terms of the main setup parameters.

The IP metric is defined as the probability that the secrecy capacity, which is the difference between the capacity of the legitimate channels and that of the eavesdropping ones, is less than or equal to zero. Mathematically, it is defined as [49]
\[
P_{\text{int}} = \Pr(C_s \leq 0) = 1 - \Pr(C_s > 0)
\tag{19}
\]
where
\[
C_s = \min\left( C_s^{(1)}, C_s^{(2)} \right)
\tag{20}
\]
\[
C_s^{(1)} = \log_2 \left( \frac{1 + \gamma_{SR}}{1 + \gamma_{SE_1}} \right)
\tag{21}
\]
and
\[
C_s^{(2)} = \log_2 \left( \frac{1 + \min(\gamma_{SR}, \gamma_{RD})}{1 + \gamma_{RE_2}} \right) = \min\left( C_s^{(1,2)}, C_s^{(2)} \right)
\tag{22}
\]
refer to the end-to-end, first hop, and second hops’ secrecy capacities, respectively, by assuming DF relaying protocol, with
\[
C_s^{(1,2)} = \log_2 \left( \frac{1 + \gamma_{SR}}{1 + \gamma_{RE_2}} \right)
\tag{23}
\]
\[
C_s^{(2)} = \log_2 \left( \frac{1 + \gamma_{RD}}{1 + \gamma_{RE_2}} \right)
\tag{24}
\]
To this end, the total secrecy capacity in (20) can be formulated as follows:
\[
C_s = \min\left( C_s^{(1)}, C_s^{(2)}, C_s^{(1,2)} \right)
\tag{25}
\]
Leveraging the probability theory, (19) becomes
\[
P_{\text{int}} = 1 - \Pr(C_s > 0, \gamma_{SR} > \gamma_{th})
\]
\[
- \Pr(C_s > 0, \gamma_{SR} < \gamma_{th})
\tag{26}
\]
where $\gamma_{th}$ is a decoding threshold SNR, below which the decoding process cannot be performed at the relay.

When $\gamma_{SR} < \gamma_{th}$, the relay fails at decoding the information message. Therefore, no signal will be transmitted to $D$, and consequently, it yields from (20) that $C_s < 0$. As a result, the overall IP expression in (26) reduces to

$$P_{int} = 1 - \Pr(C_s > 0, \gamma_{SR} > \gamma_{th}).$$

(27)

Remark 3:

1) From (25), it can be noticed that the system's secrecy capacity is the minimum of three elementary secrecy capacities, namely, the first hop’s one; i.e., $C_s^{(1)}$; the second’s; i.e., $C_s^{(2)}$; and a cross-term one; i.e., $C_s^{(1,2)}$; which involves the first hop’s legitimate SNR along with the second hop’s wiretap one. Indeed, the higher these three terms, the greater the overall system’s secrecy capacity. Notably, one can note from (21), (23), and (24) that such elementary secrecy capacities, and consequently the overall one in (25), increase with the rise of the legitimate instantaneous per-hop SNRs, i.e., $\gamma_{SR}$ and $\gamma_{RD}$ (better system secrecy), and decrease versus the wiretap ones, i.e., $\gamma_{SE_1}$ and $\gamma_{RE_2}$ (worse system secrecy). Thus, the IP, given by (19), is a decreasing function of $\gamma_{SR}$ and $\gamma_{RD}$, and increasing with respect to $\gamma_{SE_1}$ and $\gamma_{RE_2}$.

2) It can be noted from (3) and (11)–(14) that the higher the internodes distance, the lower the average SNRs; i.e., $\delta_{XZ} \to 0$, $XZ \in \{SR, SE_1, RD, RE_2\}$, and consequently, the lower the corresponding instantaneous ones, i.e., $\gamma_{XZ}$ in (11). Therefore, in such a case, and leveraging (21), (23), (25), the end-to-end secrecy capacity $C_s$ tends to 0. Thus, the events $C_s > 0$ and $\gamma_{SR} > \gamma_{th}$ are very unlikely to happen, leading to having $\Pr(C_s > 0, \gamma_{SR} > \gamma_{th}) \to 0$. As a result, based on (27), the IP converges to 1, indicating a certain intercept event.

3) The secrecy capacities in (21), (23), and (24) can be written in a generalized form as

$$C_s^{(\xi)} = \log_2 \left( \frac{1 + \varrho \gamma_{th}}{1 + \varrho_{F} \gamma_{th}} \right).$$

(28)

with $\varrho_{F} = (\gamma_{X,s}/\Omega_1)$, $\varrho_{F} \in \{l, w\}$

$$(\xi, l, w) \in \left\{ \begin{array}{l} \{SR, SE_1\} \\ \{RD, RD, RE_2\} \end{array} \right\}$$

and

$$\varrho_{F} = \sum_{i=1}^{N(i)} \left| h_{x}^{(i)} \right|^2$$

Thus, as mentioned in Remark 3-1), a secure system from the PLS perspective corresponds to a higher secrecy capacity. To this end, it can be intuitively noticed from (28) and (30) that the higher $\varrho_{F}$ and/or the number of legitimate nodes’ antennas (i.e., $N_R$ and $N_D$), the greater is $C_s^{(\xi)}$. Likewise, this latter drops by increasing $\varrho_{F}$ and/or $N_{E_1}, N_{E_2}$. Therefore, to gain more insights, we inspect the behavior of $C_s^{(\xi)}$, for equal average SNRs, i.e., $\gamma_{SR} = \gamma_{RD}$, and the number of antennas, i.e., $N(l) = N(w)$, by differentiating $C_s^{(\xi)}$ with respect to $\varrho_{F}$ as

$$\frac{\partial C_s^{(\xi)}}{\partial \varrho_{F}} = \frac{g_l - \gamma_{SR}}{(1 + \varrho g_l)(1 + \varrho_{F} g_w)}.$$  

(31)

One can note from (31) that $C_s^{(\xi)}$ is an increasing function of $\varrho_{F}$ if $g_l - \gamma_{SR} > 0$. Notably, as this last-mentioned quantity is random, we are interested then in analyzing the probability: $\Pr[g_l - \gamma_{SR} > 0]$. Hence, it yields

$$\gamma = \Pr[g_l - \gamma_{SR} > 0] = \int_{0}^{\infty} F_{g_w}(y)f_{g_l}(y)dy$$

(32)

where $F_{g_{w}}(.)$ and $f_{g_{l}}(.)$ are given, respectively, as follows:

$$F_{g_w}(y) = \frac{\gamma_{inc}(m_{w}N_{inc}^{(w)}, m_{w}N_{inc}^{(w)}/\Omega_{1,w})}{\Gamma(m_{w}N_{inc}^{(w)})},$$

(33)

$$f_{g_l}(y) = \frac{(m_{l}/\Omega_{1,l})^{m_{l}N(l)} \gamma_{inc}(m_{w}N_{inc}^{(w)}, m_{w}N_{inc}^{(w)}/\Omega_{1,w})}{\Gamma(m_{l}N(l))\Gamma(m_{w}N_{inc}^{(w)})} \int_{0}^{\infty} \gamma_{inc}(m_{w}N_{inc}^{(w)}, m_{w}N_{inc}^{(w)}/\Omega_{1,w}) \times y^{m_{l}N(l)-1} \exp \left( -\frac{m_{l}}{\Omega_{1,l}} y \right) dy.$$  

(34)

Thus, it produces

$$\gamma = \frac{(m_{l}/\Omega_{1,l})^{m_{l}N(l)} \gamma_{inc}(m_{w}N_{inc}^{(w)}, m_{w}N_{inc}^{(w)}/\Omega_{1,w})}{\Gamma(m_{l}N(l))\Gamma(m_{w}N_{inc}^{(w)})} \int_{0}^{\infty} \gamma_{inc}(m_{w}N_{inc}^{(w)}, m_{w}N_{inc}^{(w)}/\Omega_{1,w}) \times y^{m_{l}N(l)-1} \exp \left( -\frac{m_{l}}{\Omega_{1,l}} y \right) dy.$$  

(35)

Through the use of [53, eq. (6.455.1)], one obtains (36), shown at the bottom of the page. Figs. 2 and 3 present the plot of (36) versus $m_l$ and $m_w$ (Fig. 2), and $\Omega_l$ and $\Omega_w$ (Fig. 3), with $N(l) = N(w) = 3$. It can be noted from Fig. 2 that $\gamma$ slightly increases versus $m_l$ and decreases versus $m_w$. Essentially, for an equal number of antennas, this probability does not exceed 56% for $m_w \leq 10$. Nevertheless, as seen from Fig. 3, $\gamma$ (i.e., the probability that $C_s^{(\xi)}$ is increasing versus $\varrho_{F}$) surpasses 99% for $\Omega_l \geq 4\Omega_w$. 

[36]

$$\gamma = \frac{(m_{l}/\Omega_{1,l})^{m_{l}N(l)} \gamma_{inc}(m_{w}N_{inc}^{(w)}, m_{w}N_{inc}^{(w)}/\Omega_{1,w})}{\Gamma(m_{l}N(l))\Gamma(m_{w}N_{inc}^{(w)})} \times \frac{\gamma_{inc}(m_{w}N_{inc}^{(w)}, m_{w}N_{inc}^{(w)}/\Omega_{1,w})}{\Gamma(m_{l}N(l))\Gamma(m_{w}N_{inc}^{(w)})} \int_{0}^{\infty} \gamma_{inc}(m_{w}N_{inc}^{(w)}, m_{w}N_{inc}^{(w)}/\Omega_{1,w}) \times y^{m_{l}N(l)-1} \exp \left( -\frac{m_{l}}{\Omega_{1,l}} y \right) dy.$$  

(36)
**A. Exact Analysis**

**Proposition 1:** The IP of the considered dual-hop UAV-based WCS is given in the closed-form expression as

\[
P_{\text{int}} = 1 - \frac{(m_{SR}N_{E2} - 1)!}{(m_{SR}N_{E2} - 1)!}\times \sum_{l=0}^{m_{SR}N_{E2}-1} \binom{m_{SE}+l-1}{l} \sum_{i=1}^{4} T^{(i)}
\]

where

\[
T^{(1)} = \frac{\Gamma_{\text{inc}}(m_{SR}N_{R}, \frac{m_{SE}}{m_{SR}N_{R}})}{\frac{m_{SR}}{m_{SR}N_{R}}} \gamma_{th}
\]

\[
T^{(2)} = -\sum_{n=0}^{m_{SR}N_{E2}+l-1} \frac{\left(\frac{m_{SE}}{m_{SR}N_{R}}\right)^n}{\frac{m_{SR}}{m_{SR}N_{R}} + \frac{m_{SE}}{m_{SE}N_{E1}}} \rho_{\text{inc}}(m_{SR}N_{R} + n) \times \Gamma_{\text{inc}}(m_{SR}N_{R} + n, \frac{m_{SR}}{m_{SR}N_{R}} + \frac{m_{SE}}{m_{SE}N_{E1}}, \gamma_{th})
\]

and

\[
T^{(3)} = -\sum_{p=0}^{m_{SE}N_{E1}+l-1} \left(\frac{m_{SE}}{m_{SE}N_{E1}} + \frac{m_{SR}N_{E2}}{m_{SR}N_{R} + n} \right)^p \times \frac{\Gamma_{\text{inc}}(m_{SR}N_{R} + n, \frac{m_{SE}}{m_{SE}N_{E1}} \gamma_{th})}{\frac{m_{SR}N_{R} + n}{n!}}
\]

\[
T^{(4)} = -\sum_{n=0}^{m_{SE}N_{E1}+l-1} \sum_{p=0}^{m_{SR}N_{E2}+l-1} \left(\frac{m_{SE}}{m_{SE}N_{E1}} + \frac{m_{SR}N_{R} + n}{m_{SR}N_{R} + p} \right)^p \times \frac{\Gamma_{\text{inc}}(m_{SR}N_{R} + n + p, \frac{m_{SE}}{m_{SE}N_{E1}} \gamma_{th})}{\frac{m_{SR}N_{R} + n + p}{n!}}
\]

\[
\Delta = (\frac{m_{SR}N_{R} + n}{m_{SR}N_{R} + n + p}) \times \frac{\Gamma_{\text{inc}}(m_{SR}N_{R} + n, \frac{m_{SE}}{m_{SE}N_{E1}} \gamma_{th})}{\frac{m_{SR}N_{R} + n}{n!}}
\]

**Proof:** The proof is provided in Appendix A.

**Remark 4:**

1. The IP closed-form expression, given by (37)–(41), is formulated in terms of finite summations, upper incomplete and complete Gamma functions, and exponential terms. All the system and channel parameters are involved in such functions, such as Nakagami-m fading parameter \((m_{XZ})\), the threshold SNR \(\gamma_{th}\), and effective average SNRs \((\Upsilon_{XZ})\). These latter are essentially expressed, as shown in (13), in terms of the respective mobility-dependent correlation coefficients \((\rho_{XZ})\), computed based on UAVs’ relative speed, carrier frequency, and delay, average fading power \((\Omega_{XZ})\), and noise powers due to the CSI estimation errors and mobility \((\sigma_{XZ}^2, \sigma_{wXZ}^2)\). Of note, the aforementioned functions are already implemented in almost all computational software (e.g., MATLAB and MATHEMATICA), which can provide insightful observations on the impact of the system parameters on the overall secrecy performance.

2. One can obviously note that at lower threshold SNR values; i.e., \(\gamma_{th} \to 0\); the terms (38)–(41), leveraging \(\Gamma_{\text{inc}}(a, 0) = \Gamma(a)\), reduce to

\[
\gamma^{(1)}(a) = \frac{(m_{SR}N_{R} - 1)!}{(m_{SR}N_{R})^a}
\]

\[
\gamma^{(2)}(a) = -\sum_{n=0}^{m_{SR}N_{E2}} \frac{(m_{SE}N_{E2} + l - 1)!}{(m_{SE}N_{E2} + l - 1)^{\frac{m_{SE}N_{E2}}{m_{SR}N_{R}}}} \times \frac{(m_{SR}N_{R} + n - 1)!}{n!}
\]

\[
\gamma^{(3)}(a) = -\sum_{p=0}^{m_{SR}N_{E2} + l - 1} \frac{(m_{SR}N_{R} + p - 1)!}{p!} \times \frac{(m_{SE}N_{E2} + l - 1)!}{(m_{SR}N_{R} + p - 1)!}
\]

\[
\gamma^{(4)}(a) = -\sum_{n=0}^{m_{SR}N_{E2} + l - 1} \sum_{p=0}^{m_{SR}N_{E2} + l - 1} \frac{(m_{SR}N_{R} + n + p - 1)!}{\Psi^{m_{SR}N_{R} + n + p}} \times \frac{(m_{SE}N_{E2} + l - 1)!}{(m_{SR}N_{R} + n + p - 1)!}
\]
which are independent of $\gamma_b$. Henceforth, in this regime, the system’s IP is not improved regardless of the decrease in $\gamma_b$ (i.e., increasing the decoding probability at the relay), as the IP depends exclusively on the per-node number of antennas, links’ fading parameters, and average SNRs.

3) On the other hand, by making use of [53, eq. (8.350.4)], i.e., $\Gamma_{\text{inc}}(a, \infty) = 0 \forall a > 0$, the terms (38)–(41) vanish for high $\gamma_b$ values (i.e., $\gamma_b \to \infty$). Henceforth, the IP, given by (37), reaches one. In fact, the greater $\gamma_b$, the lower is the probability of successful decoding at the relay. As such, the relay fails at relaying the information signal to $D$, which results in zero capacity/SNR of the second hop.

### B. Asymptotic Analysis

In this section, asymptotic expressions for the system’s IP are derived at high legitimate links’ average SNR values. Two scenarios are investigated, namely: 1) moving nodes with imperfect channel estimation and 2) static nodes with perfect CSI at the receiver.

1) **Scenario I (Moving UAVs With Imperfect CSI):** In this scenario, when the average SNRs $\delta_{SR}$ and $\delta_{RD}$ become high (i.e., $\delta_{SR}, \delta_{RD} \to \infty$), their corresponding effective ones, given by (13), reduce to

$$
\Xi_{XZ} \sim \frac{\rho_{XZ}^2 \Omega_{XZ}}{\rho_{XZ}^2 \Omega_{XZ}^2 + (1 - \rho_{XZ}^2) \sigma_{xZ}^2}, \quad XZ \in \{SR, RD\}. \tag{46}
$$

As a consequence, by substituting $\Upsilon_{XZ} (XZ \in \{SR, RD\})$ in (37)–(41) by $\Xi_{XZ}$, given by the above equation, the system’s IP in such a particular case can be expressed as

$$
P^{(\infty, 1)}_{\text{int}} \sim 1 - \frac{(m_{SR} N_{E^1}^{\text{mSR}} N_R)}{(m_{SR} N_{E^1}^{\text{mSR}} N_R - 1)! (m_{RE} N_{E^2}^{\text{mRE}} N_Z - 1)!} \times \sum_{l=0}^{m_{RD} N_{E^2} - 1} \frac{\Gamma_{\text{inc}} (m_{SR} N_{E^1}^{\text{mSR}} N_R + l)}{\Gamma_{\text{inc}} (m_{RE} N_{E^2}^{\text{mRE}} N_Z + l)} \prod_{i=1}^{4} \mathcal{H}^{(i)} \tag{47}
$$

where

$$
\mathcal{H}^{(1)} = \frac{\Gamma_{\text{inc}} (m_{SR} N_{E^1}^{\text{mSR}} N_R)}{(m_{SR} N_{E^1}^{\text{mSR}} N_R - 1)!}
$$

$$
\mathcal{H}^{(2)} = - \sum_{n=0}^{m_{SR} N_{E^1} - 1} \frac{\Gamma_{\text{inc}} (m_{SR} N_{E^1}^{\text{mSR}} N_R)}{(m_{SR} N_{E^1}^{\text{mSR}} N_R - 1)!} \times \frac{\Gamma_{\text{inc}} (m_{SR} N_{E^1}^{\text{mSR}} N_R + n)}{(m_{SR} N_{E^1}^{\text{mSR}} N_R + n)!} \times \frac{\Gamma_{\text{inc}} (m_{SR} N_{E^1}^{\text{mSR}} N_R + n)}{(m_{SR} N_{E^1}^{\text{mSR}} N_R + n)!}
$$

$$
\mathcal{H}^{(3)} = - \sum_{p=0}^{m_{RE} N_{E^2} - 1} \frac{\Gamma_{\text{inc}} (m_{SR} N_{E^1}^{\text{mSR}} N_R + p)}{(m_{SR} N_{E^1}^{\text{mSR}} N_R + p)!} \times \frac{\Gamma_{\text{inc}} (m_{SR} N_{E^1}^{\text{mSR}} N_R + p)}{(m_{SR} N_{E^1}^{\text{mSR}} N_R + p)!}
$$

Proposition 2: At high average SNRs (i.e., $\delta_{SR} = \delta_{RD} = \delta \to \infty$), the IP of the considered dual-hop UAV-based WSCS can be asymptotically expanded, for Scenario II, as

$$
P^{(\infty, 2)}_{\text{int}} \sim C_{\delta} \delta^{-p} \tag{52}
$$

where

$$
C_{\delta} = \begin{cases} \mathcal{R}, & m_{SR} N_{E^1} > m_{RD} N_D \\ \frac{\mathcal{R}}{\mathcal{T}_1 + \mathcal{T}_2 - \mathcal{T}_3}, & m_{SR} N_{E^1} < m_{RD} N_D \end{cases}
$$

with

$$
\mathcal{R} = \bigg( \frac{m_{RD}^{\delta_{RE}}}{m_{RE}} \bigg) m_{SR} N_{E^1}^{\delta_{RE}} m_{SR} N_{E^1}^{\delta_{RE}} (m_{RE} N_{E^2}^{\delta_{RE}} + m_{RD} N_{E^2}^{\delta_{RE}} - 1)! \bigg( m_{RD} N_{E^2}^{\delta_{RE}} + m_{RD} N_{E^2}^{\delta_{RE}} - 1)! \bigg) (m_{RD} N_{E^2}^{\delta_{RE}} + m_{RD} N_{E^2}^{\delta_{RE}} - 1)! \bigg) \tag{54}
$$

$$
\mathcal{T}_1 = \bigg( \frac{m_{SR} N_{E^1}^{\delta_{SR}}}{m_{SR} N_{E^1}^{\delta_{SR}}} \bigg) \bigg( \frac{m_{SR} N_{E^1}^{\delta_{SR}}}{m_{SR} N_{E^1}^{\delta_{SR}} + m_{SR} N_{E^1}^{\delta_{SR}}} \bigg) \frac{m_{SR} N_{E^1}^{\delta_{SR}}}{m_{SR} N_{E^1}^{\delta_{SR}} + m_{SR} N_{E^1}^{\delta_{SR}}} \bigg) \tag{55}
$$

$$
\mathcal{F}_{X,Y} = \bigg( \frac{\mathcal{F}_{SE_1} \mathcal{F}_{SE_2}}{m_{SR} N_{E^1}^{\delta_{SR}} \mathcal{F}_{SE_1} \mathcal{F}_{SE_2}} \bigg) \frac{m_{SR} N_{E^1}^{\delta_{SR}}}{m_{SR} N_{E^1}^{\delta_{SR}} + m_{SR} N_{E^1}^{\delta_{SR}}} \bigg) \frac{m_{SR} N_{E^1}^{\delta_{SR}}}{m_{SR} N_{E^1}^{\delta_{SR}} + m_{SR} N_{E^1}^{\delta_{SR}}} \bigg) \tag{58}
$$

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
\[ G_{x,y,z,t} = \left( \frac{m_{x,y} m_{x,y} \delta_{x,y}}{y_{x,y} N_{y}} - 1 \right) \sum_{n=0}^{m_{x,y} N_{y} - 1} \left( \frac{m_{x,y}}{y_{x,y}} \right)^n n! \times \Gamma_{\text{inc}} \left( m_{x,y} N_{y} + m_{SR} N_{R} + n, \left( \frac{m_{x,y} + m_{x,y} \delta_{x,y}}{y_{x,y}} \right) n \right) \]  

\[ \times \left( \frac{m_{x,y} \delta_{x,y}}{y_{x,y}} + \frac{m_{x,y}}{y_{x,y}} \right)^n + m_{x,y} N_{y} + m_{SR} N_{R} \]  

(59)

and

\[ G_d = \min(m_{SR} N_R, m_{RD} N_D) \]  

(60)

are the respective secrecy coding gain and diversity order, respectively.

**Proof:** The proof is provided in Appendix B.

**Remark 6:** Equations (52)–(60) provide an asymptotic expression of the IP in the high SNR regime for Scenario II, written in terms of finite summations, Gamma and lower/upper incomplete Gamma functions, and exponential terms. Such expression can give insightful observations of the impact of the setup parameters on the security level in the high SNR regime. Interestingly, the achievable secrecy diversity order for this scenario depends exclusively on the legitimate links’ fading parameters and the number of antennas; i.e., \( G_d = \min(m_{SR} N_R, m_{RD} N_D) \).

### V. Numerical Results

In this section, numerical results for the secrecy performance of the considered dual-hop UAV-based WCS are presented. The IP metric is evaluated for several configurations of system and channel parameters. Unless otherwise stated, the default values of the system parameters are listed in Table I. Moreover, without loss of generality, the mobility-dependent noise power can be computed as follows: \( \sigma^2_{wXZ} = \Omega_{XZ} + \sigma^2_{wZ} \) [19]. It is worth recalling that throughout the numerical results, the relative speed between two nodes X and Z can refer to two UAVs moving either in the same direction, i.e., \( \nu_{XZ} = |\nu_Z - \nu_X| \), or in opposite ones, i.e., \( \nu_{XZ} = \nu_X + \nu_Z \). Also, we use the notation \( \delta = \delta_{SR} = \delta_{RD} \), when the IP is plotted against \( \delta_{SR} \) with \( \delta_{RD} = \delta_{SR} \), where the power-to-noise ratio (PNR) \( \varrho_{XZ} = \left[ \frac{P_X \Omega_{XZ} / \sigma^2_{wZ}}{\sigma^2_{wZ}} \right]_{XZ \in \{SR, RD\}} \) is set as follows:

\[ \varrho_{XZ} = \frac{x}{L_{XZ}}, XZ \in \{SR, RD\} \]  

(61)

to obtain a given average SNR value \( \delta = x \), where \( L_{XZ} \) can be computed leveraging (3) and the corresponding parameters’ values in Table I. Finally, Monte Carlo simulations were performed by generating \( 9 \times 10^6 \) Gamma-distributed RVs, referring to the per-hop SNRs, with PDF and CDF given by (17) and (18), respectively.

#### A. Effect of the Fading Severity Parameters and Number of Antennas

Figs. 4 and 5 present the system’s IP versus the average legitimate SNR, i.e., \( \delta_{SR} = \delta_{RD} = \delta \), for several values of the number of antennas and fading severity parameter, respectively. One can note from this figure that the analytical curves, plotted using (37), match their simulations counterpart, which corroborates the accuracy of the derived IP expression. Furthermore, at high SNR, the IP justifies with the asymptotic floors, plotted using (47)–(51), where the secrecy diversity order equals zero as pointed out in Remark 2-2) and Remark 5. On the other hand, one can note that the system’s secrecy improves by increasing the legitimate link’s fading.

![Fig. 4](image1.png)

**Fig. 4.** IP versus \( \delta \) for various (\( N_Z \)) values with \( m_{SR} = m_{RD} = 2, m_{SE_1} = m_{RE_2} = 4 \).

![Fig. 5](image2.png)

**Fig. 5.** IP versus \( \delta \) for various (\( m_{XZ} \)) values with \( N_R = N_D = 4, N_{E_1} = N_{E_2} = 2 \).
severity parameters (i.e., higher $m_{SR}$, $m_{RD}$), as was shown in Remark 3-3), and/or increasing the number of received antennas at $R$ and $D$ (i.e., $N_R$ and $N_D$). It is important to note that when the eavesdropping links are enhanced, either in terms of the number of antennas onboard and/or the fading severity parameter, the system’s secrecy deteriorates, where the IP can reach 56.5% for $m_{SR} = m_{RD} = 2$, $m_{SE_1} = m_{RE_2} = 4$ ($XZ \in \{SR, RD, RE_1, RE_2\}$) and $N_Z = 3$, as shown in Fig. 4.

B. Effect of the CSI Imperfection Level

In Fig. 6, the IP is depicted versus $\delta_{SR} = \delta_{RD} = \delta$ for numerous combinations of CSI estimation noise power ($\sigma_{E_{xx}}^2$) and nodes relative speed values. We can notice that CSI estimation noise power (i.e., $\sigma_{E_{xx}}^2$) impacts negatively the system’s IP. Specifically, three cases are considered in this figure: 1) Case 1: $(\sigma_{E_{SR}}^2 = \sigma_{E_{RD}}^2 = 0.02, \sigma_{E_{SE_1}}^2 = \sigma_{E_{RE_2}}^2 = 0.09)$; i.e., both legitimate links’ have less estimation error noise compared to their wiretap counterpart; 2) Case 2: $(\sigma_{E_{SR}}^2 = 0.02, \sigma_{E_{RD}}^2 = \sigma_{E_{SE_1}}^2 = \sigma_{E_{RE_2}}^2 = 0.09)$; i.e., estimation error at the $R$-$D$ link increases; and 3) Case 3: $(\sigma_{E_{RD}}^2 = 0.02, \sigma_{E_{SR}}^2 = \sigma_{E_{SE_1}}^2 = \sigma_{E_{RE_2}}^2 = 0.09)$; i.e., estimation error at the $S$-$R$ link increases. It is obvious that case 1 exhibits the best secrecy performance when both legitimate links experience less CSI estimation noise compared to their malign counterpart. However, we can note that case 2 manifests a slightly improved performance compared to case 3. That is, increasing CSI imperfection power on the first legitimate hop has a more negative impact on the system’s secrecy compared to the case when the CSI imperfection at the second hop is magnified. Finally, it can be ascertained as well that, for fixed $\sigma_{E_{xx}}^2$, (i.e., $\sigma_{E_{SR}}^2 = 0.02; \sigma_{E_{RD}}^2 = \sigma_{E_{SE_1}}^2 = \sigma_{E_{RE_2}}^2 = 0.09$), the system’s secrecy degrades when the nodes’ relative speed increases, where it can reach 17.24% at $v_{XZ} = 70$ km/h.

To emphasize Fig. 6 results, Fig. 7 represents the IP behavior versus $\delta$ for equal $\sigma_{E_{xx}}^2$ on all links, and various speed values. Notably, for perfect CSI (solid lines), the IP exhibits a remarkable increase by a factor of $10^4$ when the relative speed of nodes increases from 10 to 30 km/h. The degradation, however, is less significant with respect to the speed, for the remaining two levels of CSI imperfection. Moreover, at 50 km/h, there is almost no noticeable impact of the CSI estimation noise level on the performance.

From another front, Fig. 8 shows the IP performance for static nodes, with $\delta_{SE_1} = \delta_{RE_2} = 30$ dB, and considering various levels of CSI imperfections ($\sigma_{E_{xx}}^2$). The results emphatically highlight the IP linear drop for the ideal case (i.e., $v_{XZ} = \sigma_{E_{xx}}^2 = 0$), where the analytical IP curve matches its asymptotic counterpart, plotted from (52), at high $\delta$ values. In such a case, $\delta \rightarrow \infty \iff \Upsilon_{SR}, \Upsilon_{RD} \rightarrow \infty$. Thus, the achievable diversity order for this case equals $\min(m_{SR}N_R, m_{RD}N_D)$ as discussed in Remark 6; i.e., the achievable diversity order equals 8 for this ideal setup ($m_{SR} = m_{RD} = 2, N_R = N_D = 4$). On the other hand, one can note in parallel that even slight increases in $\sigma_{E_{xx}}^2$ can drastically impact the performance, where the IP exhibits a 15-dB loss at $IP \approx 3 \times 10^{-3}$ when going from the ideal case to $\sigma_{E_{xx}}^2 = 10^{-3}$. Also, one can observe that the IP for the imperfect CSI case reaches asymptotic floors at higher $\delta$ values, where the corresponding legitimate average SNR, given by (13), reaches a ceiling value,
as detailed in Remark 2-2). Thus, the secrecy diversity order in such a scenario equals zero, as pointed out in Remark 5.

C. Effect of the Legitimate/Wiretap Average SNRs

Fig. 9 provides the IP plot in three dimensions versus the average SNR of the wiretap links, i.e., δ_{SE₁} and δ_{RE₂}, with δ_{SR} = δ_{RD} = 40 dB. Expectedly, the IP is an increasing function of both malign channels’ SNRs. Notably, at low SNR values, we notice that the IP does not exhibit symmetric behavior for both eavesdropper’s SNRs. Importantly, at low- and mid-SNR values, and β > α (α, β ∈ ℝ⁺), the IP evaluated at δ_{SE₁} = α and δ_{RE₂} = β exceeds the one evaluated at δ_{SE₁} = β and δ_{RE₂} = α; e.g., IP = 16.77% for (δ_{SE₁}, δ_{RE₂}) = (0, 20) dB, while IP = 10.24% for (δ_{SE₁}, δ_{RE₂}) = (20, 0) dB. Therefore, deteriorating the link quality of the second malign user can provide a better secrecy performance than worsening the first one’s channel. Finally, the IP manifests a saturation regime at high (δ_{SE₁}, δ_{RE₂}) values, where the IP reaches 26%. As detailed in Remark 2-2), for fixed γ_{SR, i} and γ_{RD, i} values, the average wiretap SNRs (i.e., γ_{SE₁} and γ_{RE₂}) exhibit a ceiling value at higher δ_{SE₁} and δ_{RE₂}. Therefore, the IP in this regime depends on the remainder of the system parameters (i.e., legitimate SRNRs values, the number of antennas, fading parameters, correlation coefficients, and CSI imperfection level).

Fig. 10 depicts the secrecy performance in three dimensions versus the average SNR of both hops, i.e., δ_{SR} and δ_{RD}. Expectedly, the IP is a decreasing function of both δ_{SR} and δ_{RD}, where it reaches a ceiling value as pointed out in Remark 2-2) and Remark 5. Also, in a similar fashion to Fig. 9, the IP does not exhibit symmetric behavior versus δ_{SR} and δ_{RD}, particularly at low SNR values. For instance, P_{int} = 0.1661 for (δ_{SR}, δ_{RD}) = (35, 10) dB, while P_{int} = 0.2138 for (δ_{SR}, δ_{RD}) = (10, 35) dB. Thus, the IP can be improved by strengthening the first hop’s channel quality.

D. Effect of the Decoding Threshold SNR

In Fig. 11, the system secrecy performance is shown versus γ_{th}, with v_{XZ} = 20 km/h (XZ ∈ {SR, SE₁, RD, RE₂}). It can be ascertained that the IP reaches error floors at low γ_{th} values, while at higher γ_{th}, it reaches unit. Indeed, as discussed in Remark 4-2), the terms T^{(i)} of (37), given by (38)–(41), reduce to (42)–(45), which are independent of γ_{th}. Furthermore, as highlighted in Remark 4-3), the IP was shown to converge to one at high γ_{th}, i.e., the higher γ_{th}, the lower the decoding success probability at R. Henceforth, this results in a zero capacity of the second hop, leading to a second hop’s secrecy capacity equal to zero, according to (24). Thus, relying on the IP definition in (19)–(25), the IP will be evidently equal to 1.

E. Effect of the Carrier Frequency and Delay

Fig. 12 presents the system’s IP with respect to the CSI estimation time delay τ, for three main carrier frequency values, i.e., f_c = 2.4, 5, and 6 GHz, with δ_{SR} = δ_{RD} = 40 dB. It is obvious from the figure that the higher the delay and/or the carrier frequency, the worse the IP performance. Indeed, as discussed in Remark 1, ρ_{XZ}, given by (7), is decreasing over

3The considered carrier frequencies in these figures are chosen according to the Wi-Fi 802.11a, 802.11ac, and 802.11ax standards, with a dynamic range of channel estimation delay values; i.e., τ. Nevertheless, the evaluation can be easily extended to other frequency bands (e.g., LTE and mmWave) and arbitrary delay values.
the interval \([0, (2\pi v_{XZ} f_c t_0/c) = 3.8317]\), where \(t_0\) equals 5.5, 2.6, and 2.2 ms for \(f_c = 2.4, 5,\) and 6 GHz, respectively. Notably, the IP reaches one at \(\tau = 2.1, 1.1,\) and 0.9 ms, for \(f_c = 2.4, 5,\) and 6 GHz, respectively. Indeed, as mentioned above, the correlation coefficient decreases over the intervals \([0, 5.5], [0, 2.6],\) and \([0, 2.2]\) ms for the three considered frequencies in ascending order. Thus, capitalizing on Remark 2-1), it yields a decrease as well in the per-hop average SNR, given by (13), over these aforementioned intervals, leading to an increase in the system’s IP. Importantly, we can observe that the IP remains constant at one, although the correlation coefficient reincreases (i.e., reincrease of \(\Upsilon_{SR}\) and \(\Upsilon_{RD}\)) when \(t_0 > 2.6\) ms and \(t_0 > 2.2\) ms, for \(f_c = 5\) and 6 GHz, respectively.

**F. Effect of Nodes’ Speed**

Fig. 13 presents the IP behavior versus \(\delta\), for various nodes’ mobility scenarios. We assume that \(v_{XZ} = v_S + v_M\) (\(XZ \in \{SR, RD, SE_1, RE_2\}\)), which corresponds to the case of two moving UAVs in opposite directions. It can be noted that the worst performance corresponds to the case of moving legitimate nodes and static wiretap ones. The lesser the number of moving benign nodes, the better the performance. Indeed, as emphasized in Remark 1, and for \(v_{XZ} \in [0, (3.8317c/2\pi f_c t_0)]\), the greater the relative speed \(v_{XZ}\), the lower the correlation coefficient. Thus, the respective average SNR decreases, as shown in Remark 2-1). We can note as well that the best performance corresponds to the case of moving wiretappers and static legitimate nodes.

Fig. 14 shows the IP evolution in three dimensions, versus \(v_R\) and \(v_E_1\). We set \(v_S = 0, v_D = v_R,\) and \(v_E_2 = v_E_1\). It can be noted that, for fixed legitimate nodes’ speed, the IP manifests a decreasing behavior versus the wiretappers’ speed. In fact, as discussed in Remark 1, the greater the speed, the lower the correlation coefficient, leading to a decrease in the average SNR. Likewise, the IP deteriorates for fixed malign nodes speed and increasing velocity of the benign ones.

**G. Effect of Internodes Distance**

In Fig. 15, the secrecy performance is illustrated for a range of the internodes distance \(d_{XZ} = d, (XZ \in \{SR, SE_1, RD, RE_2\})\), and \(\varrho = \varrho_{SR} = \varrho_{RD}\) with \(\varrho_{XZ} = (|P_X\Omega_{XZ}|/|\sigma_n^2|)\). We notice that the IP deteriorates significantly by increasing the internodes’ distance due to the FSPL. Importantly, the system’s IP can reach 52% for \(\varrho = 70\) dB and \(d = 40\) m of distance. Notably, the system’s IP can
be maintained at $1.5 \times 10^{-3}$ with a PNR value $\varphi = 100$ dB and $d = 40$ m. Finally, for higher distances and low $\varphi$ values (i.e., low SNR values), the IP converges to 1, corroborating Remark 3-2).

VI. CONCLUSION

In this article, the secrecy performance of a dual-hop UAV-based WCS system was analyzed. Particularly, a DF relay handles the information signal from a source to a destination, under the presence of two malicious nodes attempting independently to overhear the $S$–$R$ and $R$–$D$ hops. Transmitters $(S, R)$ are assumed to be equipped with a single transmit antenna, while receivers $(R, D, E_1$, and $E_2)$ perform MRC using their multiple receive antennas. Due to nodes’ mobility and channel estimation imprecisions at the receivers, the CSI is subject to time selectivity and estimation errors. The per-hop instantaneous SNRs were expressed in terms of the mobility-dependent correlation coefficient and CSI estimation errors, by using the AR(1) model along with Gaussian estimation errors. Using per-hop SNR statistics, exact closed-form and asymptotic expressions for the IP metric were derived. In particular, asymptotic expressions were retrieved for two scenarios: 1) mobile nodes with imperfect CSI (general case) and 2) static nodes with perfect CSI estimation (ideal case). It was shown that the security level is enhanced by increasing the legitimate links’ fading parameters and/or number of antennas onboard legal receivers, while it deteriorates by increasing their eavesdropping links’ counterparts. Also, the IP admits a zero diversity order for the first scenario, due to the presence of a ceiling value of the average SNR per branch. However, the IP decreases linearly versus the average SNR in the second one, with an achievable diversity order dependent on the fading parameters and number of antennas of the legitimate links/nodes. Furthermore, the increase in legitimate nodes’ speed and CSI imperfection level has a detrimental effect on the secrecy, where for static nodes, the system can be castigated by a 15-dB secrecy loss at $IP = 3 \times 10^{-3}$, when the CSI imperfection power raises from 0 to $10^{-3}$. Finally, we showed that the higher the carrier frequency and/or delay time and/or relay’s decoding threshold SNR, the worse the system’s secrecy. As future work, the PLS analysis of dual/multihop UAV-based WCS with the presence of several cooperating eavesdroppers in a single hop can be investigated, especially when the eavesdroppers overhear $R$ (i.e., second hop).

APPENDIX A

PROOF OF PROPOSITION 1

The IP of a dual-hop DF-based WCS, subject to the presence of an eavesdropper per hop is given as [49, eq. (33)]

$$P_{\text{int}} = 1 - \int_{y=y_{\text{th}}}^{\infty} f_{y_{SR}}(y) F_{y_{SE_1}}(y) \mathcal{J}(y) dy$$

where

$$\mathcal{J}(y) = \int_{z=0}^{y} f_{\gamma_{RE_2}}(z) F_{\gamma_{RD}}(z) dz$$

and $F_{\gamma}(\cdot) = 1 - F_{\gamma}(\cdot)$ accounts for the complementary CDF. By plugging the PDF and CDF from (17) and (18), with $XZ = RE_2$ and $XZ = RD$, respectively, into (63), it yields (64)–(66), shown at the bottom of the page, where step (a) holds by involving the expressions (17) and (18) into (63), while step (b) is reached by using the finite-sum representation of $\Gamma_{\text{inc}}(\cdot, \cdot)$ [53, eq. (8.352.2)] along with [53, eq. (8.339.1)], assuming $m_{XZ} \in \mathbb{N}^*$. Finally, using [53, eq. (3.381.1)], step (c) is attained.

By involving (17) and (18) with $XZ = SR$ and $XZ = SE_1$, respectively, along with (66) into (62), using [53, eq. (8.339.1)]

$$\mathcal{J}(y) = \frac{\left(\frac{m_{RE_2}}{\Gamma_{RE_2}}\right)^{m_{RE_2}N_{E_2}}}{\Gamma(m_{RE_2}N_{E_2}) \Gamma(m_{RD}N_{D})} \int_{z=0}^{y} \exp\left(-\frac{m_{RE_2}}{\Gamma_{RE_2}} z\right) \Gamma_{\text{inc}}\left(m_{RD}N_{D}, \frac{m_{RD}}{\Gamma_{RD}} z\right) dz$$

\begin{align}
(a) & = \frac{\left(\frac{m_{RE_2}}{\Gamma_{RE_2}}\right)^{m_{RE_2}N_{E_2}}}{\Gamma(m_{RE_2}N_{E_2}) \Gamma(m_{RD}N_{D})} \int_{z=0}^{y} \exp\left(-\frac{m_{RE_2}}{\Gamma_{RE_2}} z\right) \Gamma_{\text{inc}}\left(m_{RD}N_{D}, \frac{m_{RD}}{\Gamma_{RD}} z\right) dz \\
(b) & = \sum_{l=0}^{m_{RD}N_{D}-1} \frac{\left(\frac{m_{RE_2}}{\Gamma_{RE_2}}\right)^{m_{RE_2}N_{E_2}}}{\left(\frac{m_{RE_2}}{\Gamma_{RE_2}}\right)^{m_{RE_2}N_{E_2}-1}} \frac{\left(\frac{m_{RD}}{\Gamma_{RD}}\right)^{m_{RD}N_{D}}}{\left(\frac{m_{RD}}{\Gamma_{RD}}\right)^{m_{RD}N_{D}-1}} \frac{1}{l!} \int_{z=0}^{y} \exp\left(-\frac{m_{RE_2}}{\Gamma_{RE_2}} z\right) \Gamma_{\text{inc}}\left(m_{RE_2}N_{E_2}+l, \frac{m_{RD}}{\Gamma_{RD}} z\right) dz \\
(c) & = \sum_{l=0}^{m_{RD}N_{D}-1} \frac{\left(\frac{m_{RE_2}}{\Gamma_{RE_2}}\right)^{m_{RE_2}N_{E_2}}}{\left(\frac{m_{RE_2}}{\Gamma_{RE_2}}\right)^{m_{RE_2}N_{E_2}-1}} \frac{\left(\frac{m_{RD}}{\Gamma_{RD}}\right)^{m_{RD}N_{D}}}{\left(\frac{m_{RD}}{\Gamma_{RD}}\right)^{m_{RD}N_{D}-1}} \frac{1}{l!} \int_{z=0}^{y} \exp\left(-\frac{m_{RE_2}}{\Gamma_{RE_2}} z\right) \Gamma_{\text{inc}}\left(m_{RE_2}N_{E_2}+l, \frac{m_{RD}}{\Gamma_{RD}} z\right) dz
\end{align}

$$P_{\text{int}} = 1 - \frac{m_{SR}}{m_{SR}N_{R}-1} \frac{m_{SR}}{m_{SR}N_{R}-1-1} \prod_{l=0}^{m_{RD}N_{D}-1} \frac{m_{RE_2}N_{E_2} + l}{m_{RE_2}N_{E_2} + l-1} \Gamma_{\text{inc}}\left(m_{SR}N_{R}, \frac{m_{SR}}{\Gamma_{SR}} y\right) \int_{y=y_{\text{th}}}^{\infty} \exp\left(-\frac{m_{SR}}{\Gamma_{SR}} y\right) \Gamma_{\text{inc}}\left(m_{SE_1}N_{E_1}+l, \frac{m_{SE_1}}{\Gamma_{SE_1}} y\right) dy$$

**Remark -**

$$\int_{y=y_{\text{th}}}^{\infty} \exp\left(-\frac{m_{SR}}{\Gamma_{SR}} y\right) \Gamma_{\text{inc}}\left(m_{SE_1}N_{E_1}+l, \frac{m_{SE_1}}{\Gamma_{SE_1}} y\right) dy$$

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
for $m_{XZ} \in \mathbb{N}^*$, and performing some algebraic manipulations, one obtains (67), shown at the bottom of the previous page, with $T$ and $(T^{(i)})_{1 \leq i \leq 4}$, given in (68), shown at the bottom of the previous page, (69)-(74), shown at the bottom of the page, where $\Delta$ and $\Psi$ are defined in the proposition. Step (a) is $T$'s definition, step (b) yields from using the finite-sum representation of $\gamma_{inc}(\cdot , \cdot )$ [53, eq. (8.352.1)], while step (c) and (71)-(74) are obtained by expanding step (b). Finally, armed by [53, eq. (3.381.3)] to solve (71)-(74), (38)-(41) of Proposition 1 are obtained. This concludes the proposition's proof.

APPENDIX B

PROOF OF PROPOSITION 2

In Scenario II, as mentioned before Proposition 2, the effective average SNRs $\gamma_{xz}$ in (13) reduce to $\delta_{xz}$ (i.e., $\gamma_{xz} = \delta_{xz}$). At the high SNR regime (i.e., $\delta_{SR} = \delta_{RD} = \delta \rightarrow \infty$), and relying on the IP definition in (62), we can asymptotically expand it as follows:

$$ P_{int}^{(\infty,2)} = 1 - \int_{y=y_{th}}^{\infty} f_{yz}^{(\infty)}(y) F_{ySE_1}(y) J^{(\infty)}(y) dy $$

with

$$ J^{(\infty)}(y) = \int_{z=0}^{y} f_{yRE_2}(z) F_{yc}^{(\infty)}(z) dz $$

and

$$ f_{yz}^{(\infty)}(y) = \frac{m_{XZ}}{m_{XZ} N_{Z}} \frac{m_{XZ} N_{Z} - 1}{y^{m_{XZ} N_{Z} - 1}} $$

and

$$ F_{yz}^{(\infty)}(y) = \frac{m_{XZ}}{m_{XZ} N_{Z}} \frac{m_{XZ} N_{Z} - 1}{y^{m_{XZ} N_{Z} + 1}} $$

respectively. Given that $F_{yz}^{(\infty)}(y) = 1 - F_{yz}^{(\infty)}(y)$, by plugging (17) with $(XZ = RE_2, \gamma_{RE_2} = \delta_{RE_2})$ and (78) with $(XZ = RD, \delta_{RD} = \delta)$ into (76), respectively, and using [53, eq. (8.339.1)] for $m_{XZ} \in \mathbb{N}^*$, one obtains (79) and (80), shown at the bottom of the next page, where step (a) is the definition of $J^{(\infty)}(y)$, while step (b) is attained using [53, eq. (3.381.1)]. By involving (18) with $(XZ = SE_1, \gamma_{SE_1} = \delta_{SE_1})$, (77) with $(XZ = SR, \delta_{SR} = \delta)$, and (80) into (75), it yields the asymptotic expansion of the IP at the high SNR as

$$ P_{int}^{(\infty,2)} (a) \sim 1 - \int_{y=y_{th}}^{\infty} f_{yz}^{(\infty)}(y) F_{ySE_1}(y) J^{(\infty)}(y) dy $$

$$ + \int_{y=y_{th}}^{\infty} F_{yz}^{(\infty)}(y) \left[ F_{ySE_1}(y) J^{(\infty)}(y) ight] dy $$

(c) $\bar{U}_3 + \bar{U}_2 + \bar{U}_3 + \bar{U}_4$

where step (a) is the definition of IP at high SNR, step (b) holds by using integration by parts with $u = f_{yz}^{(\infty)}(y)$ and $v = F_{ySE_1}(y), J^{(\infty)}(y)$, and step (c) is reached after using [53, eq. (8.339.1)] for $m_{XZ} \in \mathbb{N}^*$ alongside some algebraic manipulations and simplifications, where $(\bar{U}_i)_{1 \leq i \leq 4}$ are given by (84)-(89), shown at the bottom of the next page. Step (b) of $\bar{U}_3$ in (87) yields from involving (78) and (17), with $XZ = SR$ and $XZ = SE_1$, respectively, along with (63) into the corresponding prior step. On the other hand, step (b) of $\bar{U}_4$ in (89)
is produced by plugging into its initial step (78) and (18), with (XZ = SR, δSR = δ) and (XZ = SE1, γSE1 = δSE1), respectively, jointly with the first derivative of \( \mathcal{J}(\infty)(y) \) with respect to \( y \), computed using the derivative of the incomplete Gamma function [54, eq. (06.06.20.0003.01)].

Thus, one can note from (83) that the IP’s asymptotic expression is the sum of four terms, given by (84)–(89), where each term has either one or two subterms with two different coding gain and diversity order (i.e., power of \( \delta \)) pairs, where this latter equals \( m_{SR}N_{R} \), or \( m_{RD}N_{D} \), or \( m_{SR}N_{R} + m_{RD}N_{D} \) in these terms/subterms. As a result, only the terms with the lowest diversity order are summed up together. Hence, we distinguish three cases.

### A. Case I: \( m_{SR}N_{R} > m_{RD}N_{D} \)

In such a case, only the terms/subterms from (84)–(89), for which the diversity order equals \( m_{RD}N_{D} \) are considered. As a result, this yields taking into account only (84), which corresponds to the first case of (53).

### B. Case II: \( m_{SR}N_{R} < m_{RD}N_{D} \)

In this scenario, we take into account only the terms/subterms from (84)–(89) that exhibit a diversity order of \( m_{SR}N_{R} \). Hence, it yields (90) and (91), shown at the top of the next page, where step (b) is reached by using the finite
sum representation of the lower incomplete Gamma function \[ \text{IG}(a, b) \] in step (a). Finally, by making use of \[ \text{IG}(a, b) \] along with some algebraic manipulations, the second case of \[ (53) \], is attained.

\[ \text{C. Case III: } m_{SR}N = m_{RD}N_D \]

In this case, the terms considered in the two previous cases will be summed up, producing the third case of \[ (53) \]. This concludes the proof of Proposition 2.

**REFERENCES**

[1] J. Navarro-Ortiz, S. Sendra, P. Ameigeiras, and J. M. Lopez-Soler, “Integration of LoRaWAN and 4G/5G for the Industrial Internet of Things,” *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 60–67, Feb. 2018.

[2] H. Dai, H. Zhang, C. Li, and B. Wang, “Efficient deployment of multiple UAVs for IoT communication in dynamic environment,” *China Commun.*, vol. 17, no. 1, pp. 89–103, Jan. 2020.

[3] B. P. Sahoo, C.-C. Chou, C.-W. Weng, and H.-Y. Wei, “Enabling millimeter-wave 5G networks for massive IoT applications: A closer look at the issues impacting millimeter-waves in consumer devices under the 5G framework,” *IEEE Consum. Electron. Mag.*, vol. 8, no. 1, pp. 49–54, Jan. 2019.

[4] R. Han, L. Bai, J. Liu, J. Choi, and Y.-C. Liang, “A secure structure for UAV-aided IoT networks: Space-time key,” *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 96–101, Oct. 2021.

[5] W. Feng et al., “NOMA-based UAV-aided networks for emergency communications,” *China Commun.*, vol. 17, no. 11, pp. 54–66, Nov. 2020.

[6] D. Xu, Y. Sun, D. W. K. Ng, and R. Schober, “Multiuser MISO UAV communications in uncertain environments with no-fly zones: Robust trajectory and resource allocation design,” *IEEE Trans. Commun.*, vol. 68, no. 5, pp. 3153–3172, May 2020.

[7] N. Saeed, H. Almorad, H. Dahrouj, T. Y. Al-Naffouri, J. S. Shamma, and M. Alouini, “Point-to-point communication in integrated satellite-aerial 6G networks: State-of-the-art and future challenges,” *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1505–1525, 2021.

[8] S. Sabino, N. Horta, and A. Grilo, “Centralized unmanned aerial vehicle mesh network placement scheme: A multi-objective evolutionary algorithm approach,” *Sensors*, vol. 18, no. 12, pp. 1–18, Dec. 2018. [Online]. Available: https://www.mdpi.com/1424-8220/18/12/4387

[9] M. Mozaffari, X. Lin, and S. Hayes, “Toward 6G with connected sky: UAVs and beyond,” *IEEE Commun. Mag.*, vol. 59, no. 12, pp. 74–80, Dec. 2022.

[10] L. Hong, H. Guo, J. Liu, and Y. Zhang, “Toward swarm coordination: Topology-aware inter-UAV routing optimization,” *IEEE Trans. Veh. Technol.*, vol. 69, no. 9, pp. 10177–10187, Sep. 2020.

[11] M. Y. Afrat and S. Moh, “Routing protocols for unmanned aerial vehicle networks: A survey,” *IEEE Access*, vol. 7, pp. 99694–99720, 2019.

[12] J. He et al., “A tutorial on lossy forwarding cooperative relaying,” *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 66–87, 1st Quart., 2019.

[13] X. Chen, L. Lei, H. Zhang, and C. Yuen, “Large-scale MIMO relaying techniques for physical layer security: AF or DF?” *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 5135–5146, Sep. 2015.

[14] E. Illi et al., “Physical layer security of a dual-hop regenerative mixed RF/UOW system,” *IEEE Trans. Sustain. Comput.*, vol. 6, no. 1, pp. 90–104, Jan./Mar. 2021.

[15] X. N. Li, S. Zhang, and H. Tan, “An adaptive PHY-MAC scheme for physical-layer security,” *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 282–310, 1st Quart., 2021.

[16] E. Illi, F. El Bouanani, D. B. da Costa, E. Ayoub, and U. S. Dias, “Dual-hop mixed RF/UOW communication system: A PHY security analysis,” *IEEE Access*, vol. 6, pp. 55345–55360, 2018.

[17] J. M. Hamamreh, H. M. Furqan, and H. Arslan, “Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey,” *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, 2nd Quart., 2019.

[18] J. Zhang, G. Li, A. Marshall, A. Hu, and L. Hanzo, “A new frontier for IoT security emerging from three decades of key generation relying on wireless channels,” *IEEE Access*, vol. 8, pp. 138406–138446, 2020.

[19] A. Pandey and S. Yadav, “Joint impact of nodes mobility and imperfect channel estimates on the secrecy performance of cognitive radio vehicular networks over Nakagami-m fading channels,” *IEEE Open J. Veh. Technol.*, vol. 2, pp. 289–309, 2021.

[20] L. Fan, X. Lei, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, “Secure multiuser communications in multiple amplify-and-forward relay networks,” *IEEE Trans. Commun.*, vol. 62, no. 9, pp. 3299–3310, Sep. 2014.
Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
Marwa Qaraqe (Senior Member, IEEE) received the bachelor’s degree in electrical engineering from Texas A&M University at Qatar, Doha, Qatar, in 2010, and the M.Sc. and Ph.D. degrees in electrical engineering from Texas A&M University at College Station, College Station, TX, USA, in August 2012 and May 2016, respectively.

She is an Associate Professor with the Division of Information and Communication Technology, College of Science and Engineering, Hamad Bin Khalifa University, Doha. Her research interests cover the following areas: wireless communication, signal processing and machine learning, and their application in multidisciplinary fields, including but not limited to security, IoT, and health. Particular interests are in physical-layer security, federated learning over wireless networks, and machine learning for wireless communication, security, and health.

Dr. Qaraqe serves as a reviewer for several IEEE and technical international journals and conferences, including IEEE Wireless Communication and Networking Conference and IEEE Wireless Communication Magazine and serves on the IEEE Wireless Technical Committee on Wireless Communications.

Faissal El Bouanani (Senior Member, IEEE) was born in Nador, Morocco, in 1974. He received the M.S. and Ph.D. degrees in network and communication engineering from Mohammed V University-Souissi, Rabat, Morocco, in 2004 and 2009, respectively.

He was a Faculty Member with the University of Moulay Ismail, Meknes, Morocco, from 1997 to 2009. In 2009, he joined the National High School, IT/ENSIAS College of Engineering, Mohammed V University, Rabat, in 2009, where he is currently an Associate Professor. He advised many Ph.D. and master’s students with Mohammed V University and the University of Moulay Ismail. So far, his research efforts have culminated in more than 90 papers in a wide variety of IEEE/ACM international conferences and journals. His current research interests include performance analysis and design of wireless communication systems.

Dr. El Bouanani was awarded the best one by Mohammed V University-Souissi in 2010 for his Ph.D. thesis. He served as the TPC Chair for the ICSDE conferences and the General Co-Chair for ACOSIS 2016 and CommNet 2018 conferences. He served as the TPC Chair for the ICSDE conferences, the General Co-Chair for ACOSIS-16, and the General Chair for the 2019/2020/2021 CommNet conferences. He is an Associate Editor of IEEE Access and Frontiers in Communications and Networks. He is also serving as a Lead Guest Editor for the Physical Layer Security Special Issue: Frontiers in Communications and Networks. He has been involved as a TPC member in various conferences and IEEE journals.

Saif Al-Kuwari (Senior Member, IEEE) received the Bachelor of Engineering degree in computers and networks from the University of Essex, Essex, U.K., in 2006, and two Ph.D. degrees in Computer Science from the University of Bath, Bath, U.K., and Royal Holloway, University of London, Egham, U.K., in 2012.

He is currently an Assistant Professor with the College of Science and Engineering, Hamad Bin Khalifa University, Doha, Qatar. His research interests include applied cryptography, quantum computing, computational forensics, and their connections with machine learning.

Dr. Al-Kuwari is a Fellow of IET and BCS, and a Senior Member of ACM.