IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 15 February 2023, accepted 6 March 2023, date of publication 10 March 2023, date of current version 15 March 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3255881

RESEARCH ARTICLE

Reliable and Secure Short-Packet Communications in Untrusted Diamond Relay Networks

SHEN QIAN, (Member, IEEE)
Department of Information Systems Creation, Faculty of Engineering, Kanagawa University, Kanagawa 221-8686, Japan
e-mail: shenqian@kanagawa-u.ac.jp

This work was supported by the Japan Society for the Promotion of Science, KAKENHI, under Grant 21K17738.

ABSTRACT This paper investigates short-packet communications over a diamond relay network with two untrusted relays (potential eavesdroppers) with the purpose of guaranteeing reliability and security simultaneously. As the performance metric, reliable-and-secure probability (RSP), considering both reliability and secrecy, is defined from the perspective of physical layer security. An analytical approach is proposed to investigate reliability and security by taking into account the characteristics of the short-packet transmission. RSPs are numerically obtained via the analytical framework by utilizing the source-channel separation theorem for the source-to-relay transmission and chief executive officer (CEO) problem analyses for the relay-to-destination transmission. It is found that the optimal RSP is achieved when the contributions from the source-relay transmission and the relay-destination transmission are balanced, even without support from a friendly jamming signal or artificial noise.

INDEX TERMS Physical layer security, untrusted relay, short package, reliable-and-secure probability, diamond network.

I. INTRODUCTION

Network security is basically considered a high-layer issue and can be addressed with cryptographic schemes. However, due to the infrastructure dependency, low spectral efficiency, excessive resource consumption, or signal processing complexity, the typical upper-layer encryption mechanism cannot fully address the security challenges of potential applications, such as autonomous driving, Internet of Vehicles, and industrial Internet of Things (IoT) [1]. Physical layer security (PLS) is based on the information theory by exploiting the physical features of the transmission medium, such as fading, shadowing, and interference [2]. The low-complexity security solution in the physical layer is guaranteed regardless of the computational capability of terminals. Moreover, it is flexible in the implementation of deployment compared with bit-level cryptographic schemes [3]. Therefore PLS is regarded as a promising security solution as an alternative or as an additional level of protection to traditional cryptography techniques in the beyond 5G communications [4].

In 5G and beyond, many IoT applications, such as sensor networks collecting traffic information or intelligent logistics, are going to confront more serious secrecy challenges. Especially in heterogeneous networks, where network nodes have different security clearance, a misbehaving node may also be a potential eavesdropper making the relay untrustworthy [5]. The untrusted relays are not malicious, maybe just because of their low level of trust or insufficient security permissions [6].

In the pioneering study of untrusted relay networks, Oohama derived the positive secrecy capacity for which messages are reliably transmitted with the security of confidential messages being larger than a prescribed level. The security of the confidential messages to relay was measured by conditional entropy by studying the coding problem of the relay channel [7]. Reference [8] measured the level of secrecy of private information confidential to the relay with the entropy rate of private information conditioned on channel outputs at the relay. In [9] and [10], it was shown that

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Feng.

in single untrusted relay transmission with no direct source-destination link, introducing jamming signals could result in a positive secrecy rate. In [11], it was illustrated that an increased ergodic secrecy sum rate could be obtained in a two-way untrusted relay network with increasing relays even without jamming signal support. Furthermore, [11] proposed a relay selection criterion for multiple two-way untrusted relays to maximize the instantaneous secrecy sum rate. However, the selection criterion is given by the relay with the maximum channel gain in the relay-to-destination link without considering the security level of the untrusted relays.

In [12], the authors demonstrated that even if suffers an ergodic secrecy sum-rate reduction, compared with the case when the direct link between source and destination is fully exploited, a positive ergodic secrecy sum rate can be guaranteed without a direct link between source and destination due to the deep fading and/or heavy shadowing. To prevent the untrusted relay from intercepting confidential information, Zhao et al. investigated the secure and energy-efficient precoding design in a multiple-input and multiple-output (MIMO) two-way untrusted relay system without a direct link between source and destination, by jointly optimizing the source and relay precoders to maximize the secrecy energy efficiency [5]. Sun et al. investigated the covertness and secrecy of wireless communications in an untrusted relay-assisted device-to-device up-link network to prevent the untrusted relay from eavesdropping on the user equipment message [13]. It is worth noting that the direct link from the user equipment to the base station is assumed to be unavailable in [5] and [13]. Although PLS security for untrusted relaying has received widespread attention, the discussions mentioned above are based on an infinite block-length assumption. Qian et al. proposed a short package transmission scheme with a single untrusted relay [14]. There still is a lack of research focused on the multiple untrusted relays network with diversity gain being exploit. To the best of the author's knowledge, the PLS issue for multiple untrusted relaying with finite block-length has not been addressed in literature yet.

Short-packet communication is considered a critical technology to support the emerging application scenarios in 5G and beyond [1]. Taking intelligent sensing as an example, short packets are the most common form of information collected by sensors and other devices involved in massive machine-type communication (mMTC) and ultra-reliable low-latency communication (uRLLC) [15]. The assumption of infinite block-length within the Shannon information theoretic framework is unsuitable for designing short-packet transmissions and for performance evaluation. This is because in short package transmissions, (1) the size of the package header may no longer be negligible compared with the payload part in one package [16]; (2) limited block-length leads to an inevitable decoding error probability and information leakage caused by the backoff from capacity [17]. Therefore, transmission with a short-packet is significantly different due to the reduction in channel capacity, making it challenging to ensure communication reliability.

In this work, the author considers the security issue on the IoT sensor networks with multiple untrusted relays. In an IoT sensor network, the sensors and relays do not have the same security clearance since they may be in a heterogeneous network [9]. Therefore, the relays can also be considered potential eavesdroppers. Confidential information sensed in the IoT terminal can be wiretapped due to the misbehaving of untrusted relays. Information-theory-based PLS has been recognized as a promising approach to mitigate the security issue due to its low complexity and effective characteristic regardless of the computational capability of terminals [18]. Moreover, in IoT sensor networks, the terminals and relays are usually under strict power constraints limited by the device size. Therefore, this work focuses on the physical layer security issue in a two-untrusted relay network under the single antenna consideration.

It should be noted that this work differs from previous works in the following aspects.

- This paper highlights the reliable and secure performance of a diamond short package communication system with two untrusted relays, from the perspective of the physical layer. Lossy decode-and-forward (DF) is considered at the untrusted relays to improve transmission reliability while keeping the message confidential. Since lossy DF allows decoding errors in the source-relay links, it is conducive to preventing the untrusted relay from overhearing the original message sent from the source.
- A general analytical framework is proposed by utilizing lossy source-channel separation in the source-relay transmission (intro-link), which can be applied to establish the relationship between the error probability and the instantaneous signal-to-noise ratio (SNR). In addition, the transmission from the two untrusted relays to the destination is evaluated by solving a chief executive officer (CEO) problem.
- To evaluate the reliable and secure performance, this paper calculate the reliable-and-secure probability (RSP), representing the probability that the destination can decode the original message of the source, whereas the relays cannot. It is revealed from the numerical results that to achieve the optimal reliable and secure performance in terms of RSP, the balance between the transmit power of the source and the relays needs to be considered.

The paper is organized as follows. In section II, we present the diamond relay network model for short-packet transmission. The RSP definition and the analytical framework for calculating the RSP are given in III. The corresponding simulation results are provided in Section IV. V summarizes this paper.

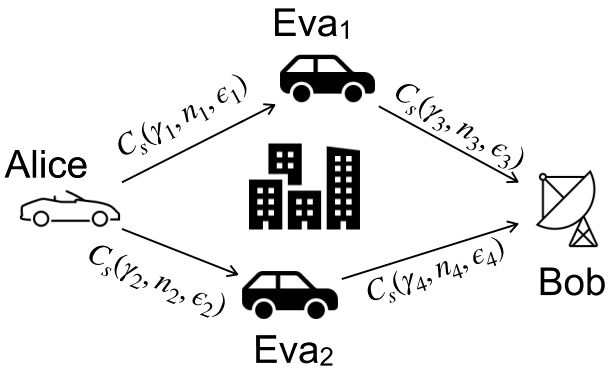


FIGURE 1. The block diagram of the diamond network with two untrusted relay.

II. SYSTEM MODEL

A. DIAMOND RELAY NETWORK WITH LOSSY DF

We consider a diamond relay network consisting of four nodes, as shown in Fig. 1. A legitimate user, Alice (source), transmits confidential information to another legitimate user, Bob (destination), with the help of two users, Eva_1 (E_1) and Eva_2 (E_2). There is no direct link between Alice (A) and Bob (B) due to obstacles or heavy shadows. The two intermediate nodes, i.e., Eva_1 and Eva_2, receive and forward confidential messages. However, Eva_1 and Eva_2 are considered untrusted relays due to their low security clearance. All the nodes are assumed to equip with a single antenna due to the facility size and power constraint.

The overall transmission from Alice to Bob is divided into two phases. In the first phase, the original independent and identically distributed (i.i.d.) binary information sequences are encoded, modulated, and broadcast from Alice. The original binary information sequences follow Bernoulli(p) distribution with parameter p ($0 \leq p \leq 1$). The relay Eva_1 and Eva_2 decode the received messages and forward the re-encoded information sequences to Bob in the second phase over different channels at their dedicated time slots, i.e., in orthogonal transmission.[1] Alice does not transmit during the second phase.

Lossy DF is considered at the untrusted relay to improve the transmission reliability while keeping the message confidential. The sequences received by Eva_1 and Eva_2 may contain errors due to the inaccuracy of the decoding related to the received SNR. With the lossy DF relaying implementation, Eva_1 and Eva_2 always interleave and re-encode the received information sequences and forward them to Bob despite the decoding errors.

After receiving the signals from Eva_1 and Eva_2, joint decoding is performed at Bob to retrieve the original information sent from Alice. An iterative decoding process [21] is utilized between two decoders for decoding the messages sent from Eva_1 and Eva_2, respectively.

[1]Transmitting through different time slots may cause a decrease in spectral efficiency, which can be alleviated by non-orthogonal multiple access (NOMA) [19], [20]. Discussion on the optimization issue for the two time slots in the second phase is left as a future study.

B. SHORT PACKAGE TRANSMISSION

According to Shannon's definition, the channel capacity is the maximum mutual information between the channel input and output alphabets, representing the biggest transmit rate at which a message can be sent with the error being as infinitely small as possible. Therefore, capacity is usually considered a critical performance metric in conventional wireless communication systems. In general, infinite block-length is assumed for performance analyses, resulting in the derived performance limits being the upper bounds. However, in practice, e.g., in uRLLC and mMTC scenarios, channel capacity based on infinite block-length is no longer suitable for analyzing secrecy performances. Moreover, short-packet communications can provide anti-delay solution, which is suitable for time-sensitive IoT applications and helps reduce communication delays [22]. Therefore, there is considerable interest in investigating the penalty in secrecy capacity and the backoff of system performances for a given block-length.

The maximal transmission rate with a short package (finite block-length), which is equivalent to the capacity C_s is given by [23]

$$C_s(\gamma, n, \epsilon) = C(\gamma) - \sqrt{\frac{V}{n}} Q^{-1}(\epsilon) \tag{1}$$

for a block-length n, a decoding error probability ϵ and an instantaneous SNR γ, where $C(\gamma) = \log_2(1+\gamma)$ is Shannon's Gaussian-codebook based channel capacity with infinite block-length. Channel dispersion V, which characterizes the stochastic variability in the finite block-length regime relative to a deterministic channel, is defined as

$$V = \frac{\gamma(\gamma+2)}{2(\gamma+1)^2} \log^2 e \tag{2}$$

where e is the Euler's number. $Q^{-1}(x)$ is the inverse Q-function $Q(x)$ with

$$Q(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} e^{-t^2/2} \mathrm{d}t. \tag{3}$$

The performance analysis of the capacity with short package is provided ed in Appendix A.

C. CHANNEL MODEL

Let P_i^t ($i \in \{\text{A}, \text{E}_1, \text{E}_2\}$) denote the transmit power of the corresponding node, and G_j represent the geometric gain, where $j \in \{1, 2, 3, 4\}$ indicates the AE_1, AE_2, E_1B, and E_1B, links, respectively. The signal received at Eva_1, Eva_2, and Bob are expressed as

$$y_{\text{E}_1}[n] = \sqrt{P_{\text{A}}^t G_1} h_1 x_{\text{A}}[n] + n_{\text{E}_1}[n], \tag{4}$$

$$y_{\text{E}_2}[n] = \sqrt{P_{\text{A}}^t G_2} h_2 x_{\text{A}}[n] + n_{\text{E}_2}[n], \tag{5}$$

$$y_{\text{B}}[n] = \sqrt{P_{\text{E}_1}^t G_3} h_3 x_{\text{E}_1}[n] + n_{\text{B}}[n], \tag{6}$$

$$y'_{\text{B}}[n] = \sqrt{P_{\text{E}_2}^t G_4} h_4 x_{\text{E}_2}[n] + n'_{\text{B}}[n], \tag{7}$$

under the assumption that an orthogonal transmission is considered in the second phase. n indicates the timing index

of the symbols. x_j is the modulated symbol corresponding to the coded information sequences. n_k ($k \in \{\mathrm{E}_1, \mathrm{E}_2, \mathrm{B}\}$) represents the zero-mean additive white Gaussian noise with the variance of $\frac{N_0}{2}$ per dimension. h_j denotes the complex channel gain of the corresponding links. y'_{B} and n'_{B} indicate the received signal and noise in the second time slot of the second phase. Due to the block-fading assumption, h_j stays constant over a one-block duration, and $\mathbb{E}[|h_j|^2] = 1$. The symbol indexes are omitted in the following discussion for conciseness.

We use the two-ray model [24, Section 2.4.1] to describe the geometric gain G_j of link j. The received power P_k^r ($k \in \{\mathrm{E}_1, \mathrm{E}_2, \mathrm{B}\}$) is defined as

$$P_k^r = \left(\frac{\sqrt{M_j} l_i l_k}{d_j^2}\right)^2 P_i^t, \tag{8}$$

$i \in \{\mathrm{A}, \mathrm{E}_1, \mathrm{E}_2\}, j \in \{1, 2, 3, 4\}, k \in \{\mathrm{E}_1, \mathrm{E}_2, \mathrm{B}\}$, where M_j and d_j are the radiation pattern and distance of the corresponding link. l_i and l_k represent the height of the transmitter and receiver of the corresponding node, respectively.

The average and instantaneous received SNRs at Eva_1, Eva_2, and Bob are expressed as $\Gamma_j = P_k^r \frac{E_s}{N_0}$ and $\gamma_j = |h_j|^2 \Gamma_j$ ($j \in \{1, 2, 3, 4\}, k \in \{\mathrm{E}_1, \mathrm{E}_2, \mathrm{B}\}$), respectively, where E_s is the transmit power of each symbol. All the links are assumed to experience independent and identically distributed (i.i.d) Rayleigh fading. The probability density function of instantaneous SNR γ of the Rayleigh fading is given by

$$f(\gamma) = \frac{1}{\Gamma} \exp(-\frac{\gamma}{\Gamma}). \tag{9}$$

III. RELIABLE-AND-SECURE ANALYSES

A. RELIABLE-AND-SECURE PROBABILITY DEFINITION

In untrusted relay networks, the messages are transmitted to the destination while remaining confidential to the untrusted relays. An intuitive approach is to convey the message under an achievable secrecy rate [25] from the source to the destination. However, if there is no direct link exists between the source and the destination, in general, a positive secrecy rate can not be achieved [6].

However, since lossy DF is considered at the relays, error is allowed during the decoding process at the untrusted relay. The decoded information sequences at the untrusted relay are re-encoded, and forwarded to the destination. The RSP is defined as the probability that the destination (Bob) can recover the message sent from the source (Alice) and the outage happening at the untrusted relays (Eva_1 and Eva_2), as

$$\begin{aligned} &P_{\mathrm{RSP}} \\ &= P_{\mathrm{out}}^{\mathrm{E}} - P_{\mathrm{out}}^{\mathrm{B}}, \\ &= \underbrace{\Pr\{\text{outage at } \mathrm{Eva}_1 \cap \text{outage at } \mathrm{Eva}_2\}}_{P_{\mathrm{out}}^{\mathrm{E}}} \\ &\quad - \underbrace{\Pr\{\text{outage at } \mathrm{Eva}_1 \cap \text{outage at } \mathrm{Eva}_2 \cap \text{outage at Bob}\}}_{P_{\mathrm{out}}^{\mathrm{B}}}, \end{aligned} \tag{10}$$

with $P_{\mathrm{out}}^{\mathrm{E}}$ representing the outage probability at both untrusted relays Eva_1 and Eva_2. $P_{\mathrm{out}}^{\mathrm{B}}$ is the probability that an outage happening at the destination (Bob) and the untrusted relays (Eva_1 and Eva_2) at the same time.

B. INTRO LINKS ERROR PROBABILITY ANALYSIS

Since decoding error is allowed in the intro links (Alice-Eva_1 and Alice-Eva_2 links), according to the source-channel separation theorem with distortion [26, Theorem 3.7], the rates with distortions $\mathscr{D}_1$ and $\mathscr{D}_2$ in the Alice-Eva_1 and Alice-Eva_2 links are achievable if and only if

$$R_1^s(\mathscr{D}_1)\acute{R}_1 \le C_s(\gamma_1, n_1, \epsilon_1), \tag{11}$$

$$R_2^s(\mathscr{D}_2)\acute{R}_2 \le C_s(\gamma_2, n_2, \epsilon_2), \tag{12}$$

where $R_1^s(\mathscr{D}_1)$ and $R_2^s(\mathscr{D}_2)$ represent the rate-distortion functions in Alice-Eva_1 and Alice-Eva_2 links, respectively, with distortion levels $\mathscr{D}_1$ and $\mathscr{D}_2$. $\acute{R}_1$ and $\acute{R}_2$ are the total joint source-channel coding rate of the corresponding link. The detailed introduction of $\acute{R}$ can be referred to in Appendix B.

For binary source following Bernoulli(p) distribution,

$$R^s(\mathscr{D}) = \begin{cases} 1 - H(\mathscr{D}), & 0 \le \mathscr{D} \le \min(p, 1-p) \\ 0, & \mathscr{D} > \min(p, 1-p), \end{cases} \tag{13}$$

where $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function.

For Gaussian source, following $N(0, \sigma^2)$ distribution,

$$R^s(\mathscr{D}) = \begin{cases} R^s(\mathscr{D}) = \frac{1}{2}\log_2\frac{\sigma^2}{\mathscr{D}}, & 0 \le \mathscr{D} \le \sigma^2 \\ 0, & \mathscr{D} > \sigma^2. \end{cases} \tag{14}$$

Note that with the Hamming distortion measure and for a given instantaneous SNR γ, the minimum distortion $\min\{\mathscr{D}_1\}$ and $\min\{\mathscr{D}_2\}$ are equivalent to the Alice-Eva_1 and Alice-Eva_2 transmission error probabilities, respectively.

According to (1), (11), and (12), the relationship between the instantaneous channel SNR γ and $R^s(\mathscr{D})$ is given by

$$\begin{aligned} R^s(\mathscr{D})\acute{R} &= (1 - H(\mathscr{D}))\acute{R} \le C(\gamma) - \sqrt{\frac{V}{n}}Q^{-1}(\epsilon), \\ &= \log_2(1+\gamma) - \sqrt{\frac{1-(1+\gamma)^{-2}}{n}}Q^{-1}(\epsilon) \end{aligned} \tag{15}$$

with a Bernoulli($\frac{1}{2}$) source. With a Gaussian source

$$\begin{aligned} R^s(\mathscr{D})\acute{R} &= \frac{1}{2}\log_2\frac{\sigma^2}{\mathscr{D}}\acute{R} \le C(\gamma_0) - \sqrt{\frac{V}{n}}Q^{-1}(\epsilon), \\ &= \log_2(1+\gamma) - \sqrt{\frac{1-(1+\gamma)^{-2}}{n}}Q^{-1}(\epsilon). \end{aligned} \tag{16}$$

C. OUTAGE PROBABILITIES AT Eva_1 AND Eva_2

In the short package communications, $P_{\mathrm{out}}^{\mathrm{E}}$ in (10) is defined as the case that the transmission with rate $\acute{R}_1$ and $\acute{R}_2$ with block-length n_1 and n_2, respectively, violate the tolerable distortion level $\mathscr{D}_1$ and $\mathscr{D}_2$, as

$$P_{\mathrm{out}}^{\mathrm{E}} = \Pr\left\{\acute{R}_1 R_1^s(\mathscr{D}_1) > C_s(\gamma_1, n_1, \epsilon_1)\right\}$$

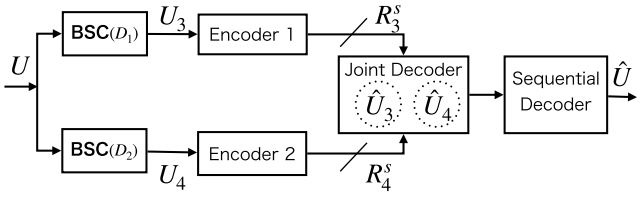


FIGURE 2. Abstract model of a binary CEO problem.

$$\begin{aligned}
&\cdot \Pr\left\{\acute{R}_2 R_2^s(\mathscr{D}_2) > C_s(\gamma_2, n_2, \epsilon_2)\right\} \\
&= \Pr\left\{0 \le \gamma_1 < C_s^{-1}\left(\acute{R}_1 R_1^s(\mathscr{D}_1), n_1, \epsilon_1\right)\right\} \\
&\quad \cdot \Pr\left\{0 \le \gamma_2 < C_s^{-1}\left(\acute{R}_2 R_2^s(\mathscr{D}_2), n_2, \epsilon_2\right)\right\} \\
&= \int_0^{C_s^{-1}\left(\acute{R}_1 R_1^s(\mathscr{D}_1), n_1, \epsilon_1\right)} f(\gamma_1)\, d\gamma_1 \\
&\quad \cdot \int_0^{C_s^{-1}\left(\acute{R}_2 R_2^s(\mathscr{D}_2), n_2, \epsilon_2\right)} f(\gamma_2)\, d\gamma_2, \qquad (17)
\end{aligned}$$

where $C_s^{-1}(\cdot)$ denotes the inverse function of $C_s(\cdot)$. Eq.(17) holds according to Shannon's separation theorem and the independent fading assumption.

In each duration of the fading block, the quasi-static fading channel is equvenletn to additive white Gaussian noise (AWGN) channels. The channel gain fixes in each block and varies block-by-block according to the fading distribution. Therefore, the outage probability $P_{\text{out}}^{\text{E}}$ is calculated as a set of integrals over the PDF of the instantaneous SNRs over the inadmissible rate region.

D. ADMISSIBLE RATE REGION ON SLEPIAN-WOLF CODING BASED FORMULATION FOR CEO PROBLEM

Let U denote the original information sequence transmitted from Alice, and U_3 and U_4 denote the information sequences outputted of Eva_1 and Eva_2, described by R_3^s and R_4^s, respectively. Due to the lossy DF setup, even though the sequences received at Eva_1 and Eva_2 may contain errors, i.e., $U \neq U_3$ and $U \neq U_4$ with a certain probability, Eva_1 and Eva_2 still forward the erroneous sequences to Bob. Therefore, the transmission analysis of the Eva_1-Bob and Eva_2-Bob transmission falls into the category of the CEO problem in network information theory [26]. The abstract model of the CEO problem is depicted in Fig. 2.[2] Due to the block fading assumption, the errors that happen in both Alice-Eva_1 and Alice-Eva_2 links are with fixed probabilities during one transmission block.

U_3 and U_4 are correlated with each other since they originated from the same source Alice. The correlation is expressed by a bit-flipping model as $U_3 = U_4 \oplus \varepsilon_0$, where ε_0 represents a random variable with $\Pr(\varepsilon_0 = 1) = 1 - \Pr(\varepsilon_0 = 0) = \rho_0$. ρ_0 indicates the bit-flipping probability between U_3 and U_4.

[2] U_1 and U_2 are the missing numbers and are not used in this paper to keep the sign consistent.

Since U_3 and U_4 are correlated, according to the Slepian-Wolf theorem, successful recovery of U_3 and U_4 after joint decoding at Bob can be realized if the source rate pair (R_3^s, R_4^s) of U_3 and U_4 satisfy

$$\begin{cases} R_3^s \ge H(U_3|\hat{U}_4), \\ R_4^s \ge H(U_4|\hat{U}_3), \\ R_3^s + R_4^s \ge H(U_3, U_4), \end{cases} \qquad (18)$$

where $\hat{U}_3$ and $\hat{U}_4$ are the estimates of U_3 and U_4 from the final output at Bob. $H(U_3|\hat{U}_4)$ and $H(U_3|\hat{U}_4)$ are conditional entropy. The relationship between U_3 and $\hat{U}_3$ and the relationship between U_4 and $\hat{U}_4$ are also modeled by the bit-flipping model with the flipping probabilities ρ_3 and ρ_4, respectively. Due to the block fading assumption, the error probabilities in the Eva_1-Bob and Eva_2-Bob links keep constant within one transmission block. Therefore, ε_3 and ε_4 are regarded as fixed parameters in each phase. Since i.i.d. source is considered in this work, we have $H(U_3|\hat{U}_4) = H(\varepsilon_0 * \varepsilon_3)$ and $H(U_4|\hat{U}_3) = H(\varepsilon_0 * \varepsilon_4)$ where $x * y = (1-y)x + (1-x)y$.

Let's consider two extreme cases. In the case U_3 and U_4 can be fully recovered at Bob simultaneously, $U_3 = \hat{U}_3$ and $U_4 = \hat{U}_4$, $\varepsilon_3 = 0$ and $\varepsilon_4 = 0$, which corresponds to the case (R_3^s, R_4^s) falls into the areas 1 and 2 in Fig. 3. In the case U_3 (or U_4) can be recovered in arbitrarily small error probability while U_4 (or U_3) is totally wrong, $\hat{U}_4$ (or $\hat{U}_3$) does not contain any useful information on U_4 (or U_3). Therefore, the conditions become $\left[R_3^s \ge H(U_3), R_4^s \ge 0\right]$ (or $\left[R_3^s \ge 0, R_4^s \ge H(U_4)\right]$), which corresponds to the area 4 (or 3), respectively, in Fig. 3.

E. CEO PROBLEM FORMULATION

With binary source, we have $H(U_3) = H(U_4) = 1$, $H(U_3|U_4) = H(U_4|U_3) = H(\rho_0)$, and $H(U_3, U_4) = H(U_4) + H(U_3|U_4) = H(U_3) + H(U_4|U_3) = 1 + H(\rho_0)$, where $H(\rho_0) = -\rho_0 \log_2(\rho_0) - (1-\rho_0)\log_2(1-\rho_0)$ is the binary entropy function. Note that ρ_0 is related to the $\mathscr{D}_1$ and $\mathscr{D}_2$. In the case there is no distortion occurred in the Alice-Eva_1 and Alice-Eva_1 transmission, $\mathscr{D}_1 = 0$ and $\mathscr{D}_2 = 0$. U_3 and U_4 become the same, $\rho_0 = 0$.

With Gaussian source $N \sim (0, \sigma^2)$, $h(U_3) = h(U_4) = \frac{1}{2}\log_2 2\pi e\sigma^2$, $h(U_3|U_4) = h(U_3, U_4) - h(U_4)$, $h(U_4|U_3) = h(U_4, U_3) - h(U_3)$, where $h(\cdot)$, $h(\cdot|\cdot)$, and $h(\cdot, \cdot)$ are the differential entropy, conditional, and joint differential entropy, respectively.

Let $\mathscr{D}_3$ and $\mathscr{D}_4$ represent the distortion level of $\Pr(U_3 \neq \hat{U}_3)$ and $\Pr(U_4 \neq \hat{U}_4)$, respectively. The expected Hamming distortion measure over M symbols is defined as

$$E\left[\frac{1}{m}\sum_{m=1}^{M} d\left(U_v, \hat{U}_v\right)\right] \le \mathscr{D}_v + \delta, \quad v \in (3, 4), \qquad (19)$$

to evaluate the error propagation probability with

$$d(U_v, \hat{U}_v) = \begin{cases} 1, & \text{if } U_v \neq \hat{U}_v, \\ 0, & \text{if } U_v = \hat{U}_v, \end{cases} \quad v \in (3, 4), \qquad (20)$$

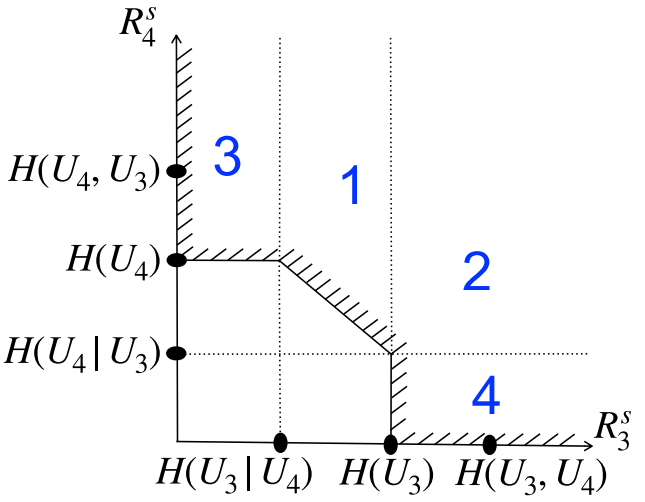


FIGURE 3. Admission rate region for U_1 and U_2 determined by Slepian-Wolf coding.

where δ is an arbitrarily small positive number. $E[\cdot]$ represents the expectation operator. Finally, the original message of the source, Alice is estimated by using the majority logic decoding [27, Section 4.1] or optimal decision [28] at Bob.

The outage probability $P_{\text{out}}^{\text{B}}$ in (10) is defined as

$$P_{\text{out}}^{\text{B}} = \Pr(\tilde{\mathscr{D}} > \min_{\mathscr{D}_3, \mathscr{D}_4} \{\mathscr{D}_3, \mathscr{D}_4\}), \tag{21}$$
$$\text{s.t.} \begin{cases} R_3^s(\mathscr{D}_3)\acute{R}_3 & \leq C_s(\gamma_3, n_3, \epsilon_3) \\ R_4^s(\mathscr{D}_4)\acute{R}_4 & \leq C_s(\gamma_4, n_4, \epsilon_4) \end{cases}$$

where $\tilde{\mathscr{D}} = f(\cdot, \cdot)$ denotes the sequential decoding function related to the decoding scheme. Readers may refer to [28, IV-A] for the detailed introduction of function $f(\cdot, \cdot)$.

F. RELIABLE-AND-SECURE PROBABILITY CALCULATION

Let P_q ($q \in \{1, 2, 3, 4\}$) represent the probability that the rate pair (R_3^s, R_4^s) fall into the area q in Fig. 3 for given γ, n, and ϵ, $P_{\text{out}}^{\text{B}}$ can be calculated as

$$P_{\text{out}}^{\text{B}} = 1 - P_1 - P_2 - P_3 - P_4, \tag{22}$$

with the block fading assumption. Note that the outage occurs if and only if the value of distortion $\tilde{\mathscr{D}}$ exceeds $\min\{\mathscr{D}_1, \mathscr{D}_2\}$ as defined in (21). Therefore, areas 3 and 4 in Fig. 3 can also be considered admissible regions when $R_3^s \geq H(U_3)$ and $R_4^s \geq H(U_3)$.

With the relationship between the rates R_3^s and R_4^s and the corresponding instantaneous channel SNR γ_3 and γ_4, the block-length n_3 and n_4, and the error probabilities ϵ_3 and ϵ_4 being taken into account, the outage probability P_q ($q \in \{1, 2, 3, 4\}$) is defined by taking the average over the transmissions in the Eva_1-Bob and Eva_2-Bob links, as

$$\begin{aligned} P_1 = \Pr\Big\{ & R_1^s(\mathscr{D}_1) > \frac{C_s(\gamma_1, n_1, \epsilon_1)}{\acute{R}_1}, \\ & R_2^s(\mathscr{D}_2) > \frac{C_s(\gamma_2, n_2, \epsilon_2)}{\acute{R}_2}, \\ & H(U_3|U_4) < R_3^s < H(U_3), R_3^s + R_4^s > H(U_3, U_4)\Big\} \\ = \Pr\Big\{ & \gamma_1 > C_s^{-1}\left(\acute{R}_1 R_1^s(\mathscr{D}_1), n_1, \epsilon_1\right), \\ & \gamma_2 > C_s^{-1}\left(\acute{R}_2 R_2^s(\mathscr{D}_2), n_2, \epsilon_2\right), \\ & H(\rho) < \frac{C_s(\gamma_3, n_3, \epsilon_3)}{\acute{R}_3} < H(U_1), \\ & \frac{C_s(\gamma_3, n_3, \epsilon_3))}{\acute{R}_3} + \frac{C_s(\gamma_4, n_4, \epsilon_4))}{\acute{R}_4} > H(U_3, U_4)\Big\}, \end{aligned} \tag{23}$$

$$\begin{aligned} P_2 = \Pr\Big\{ & R_1^s(\mathscr{D}_1) > \frac{C_s(\gamma_1, n_1, \epsilon_1)}{\acute{R}_1}, \\ & R_2^s(\mathscr{D}_2) > \frac{C_s(\gamma_2, n_2, \epsilon_2)}{\acute{R}_2}, \\ & R_3^s > H(U_3), R_4^s > H(U_4|U_3)\Big\} \\ = \Pr\Big\{ & \gamma_1 > C_s^{-1}\left(\acute{R}_1 R_1^s(\mathscr{D}_1), n_1, \epsilon_1\right), \\ & \gamma_2 > C_s^{-1}\left(\acute{R}_2 R_2^s(\mathscr{D}_2), n_2, \epsilon_2\right), \\ & \frac{C_s(\gamma_3, n_3, \epsilon_3)}{\acute{R}_3} > H(U_3), \\ & \frac{C_s(\gamma_4, n_4, \epsilon_4)}{\acute{R}_4} > H(U_4|U_3)\Big\}, \end{aligned} \tag{24}$$

$$\begin{aligned} P_3 = \Pr\Big\{ & R_1^s(\mathscr{D}_1) > \frac{C_s(\gamma_1, n_1, \epsilon_1)}{\acute{R}_1}, \\ & R_2^s(\mathscr{D}_2) > \frac{C_s(\gamma_2, n_2, \epsilon_2)}{\acute{R}_2}, \\ & 0 < R_3^s < H(U_3|U_4), R_4^s > H(U_4)\Big\} \\ = \Pr\Big\{ & \gamma_1 > C_s^{-1}\left(\acute{R}_1 R_1^s(\mathscr{D}_1), n_1, \epsilon_1\right), \\ & \gamma_2 > C_s^{-1}\left(\acute{R}_2 R_2^s(\mathscr{D}_2), n_2, \epsilon_2\right), \\ & 0 < \frac{C_s(\gamma_3, n_3, \epsilon_3)}{\acute{R}_3} < H(U_3|U_4), \\ & \frac{C_s(\gamma_4, n_4, \epsilon_4)}{\acute{R}_4} > H(U_4)\Big\}, \end{aligned} \tag{25}$$

and

$$\begin{aligned} P_4 = \Pr\Big\{ & R_1^s(\mathscr{D}_1) > \frac{C_s(\gamma_1, n_1, \epsilon_1)}{\acute{R}_1}, \\ & R_2^s(\mathscr{D}_2) > \frac{C_s(\gamma_2, n_2, \epsilon_2)}{\acute{R}_2}, \\ & 0 < R_4^s < H(U_4|U_3), R_3^s > H(U_3)\Big\} \\ = \Pr\Big\{ & \gamma_1 > C_s^{-1}\left(\acute{R}_1 R_1^s(\mathscr{D}_1), n_1, \epsilon_1\right), \\ & \gamma_2 > C_s^{-1}\left(\acute{R}_2 R_2^s(\mathscr{D}_2), n_2, \epsilon_2\right), \\ & 0 < \frac{C_s(\gamma_4, n_4, \epsilon_4)}{\acute{R}_4} < H(U_4|U_3), \\ & \frac{C_s(\gamma_3, n_3, \epsilon_3)}{\acute{R}_3} > 1\Big\}, \end{aligned} \tag{26}$$

The derivation for the explicit expression of (23), (24), (25), and (26) may be exceedingly difficult due to the

complexity of $C_s(\gamma, n, \epsilon)$. Therefore, a series of Monte Carlo simulations are used to numerically calculate $P_{\text{out}}^{\text{E}}$ and $P_{\text{out}}^{\text{B}}$.

Note that the outage probability $P_{\text{out}}^{\text{B}}$ also depends on the values of $\mathscr{D}_1$ and $\mathscr{D}_2$, which changes with the variation of γ_1 and γ_2, respectively, block by block due to the block fading assumption. Since the derivation of the Berger-Tung bound for multiple terminals with Hamming distortion measure is still an open problem, the reliable-and-secure probability analysis based on Berger-Tung bound with a specific distortion level is left as a future study.

G. IMPACT OF RELAYS LOCATION ON THE RSP

In this section, we investigate the impact of the location of the untrusted relays on RSP. The RSP expressions can be rewritten as functions of position of the untrusted relays by taking the geometric gain into consideration. With d_j ($j \in \{1, 2, 3, 4\}$ being the distance of the corresponding link as in (8), SNR is inversely proportional to the propagation distance, as

$$\Gamma_j \propto \frac{1}{d_j^{\rho}}, \tag{27}$$

where ρ is path loss exponent [29, Section 1.2.2]. Let's assume a virtual Alice-Bob link with the distance being d_0 and the average SNR being Γ_0. Then, the average SNRs of each link can be given as

$$\Gamma_j = \Gamma_0 \left(\frac{d_0}{d_j}\right)^{\rho}. \tag{28}$$

By substituting (28) into (23), (24), (25), and (26), we have the RSP expressions with respect to the position of the untrusted relays. The general optimization problem with regard to d_j can be formulated as

$$\begin{aligned} d_j^* =& \arg\max_{d_j} \; P_{\text{RSP}}(d_j) \\ & \text{subject to: } 0 \le d_j, \; 0 \le d_0. \end{aligned} \tag{29}$$

It may challenging to formulate the untrusted relay location optimization as a convex optimization problem due to the complexity of the short package capacity expression. However, the numerical results of RSP versus the untrusted relay locations are shown in Fig. 8 in the next section.

IV. NUMERICAL RESULTS

This section presents the numerical results of the reliable and secure performance of the short-packet transmission over the diamond untrusted relay network. All the numerical results are obtained by averaging over 10^6 channel realizations. The total joint coding rates of all the links are set as $\acute{R}_j = 0.5$, ($j \in \{1, 2, 3, 4\}$).

Fig. 4 plots the RSP versus the average SNR of the A-E_1 link Γ_1 and A-E_2 link Γ_2 ($\Gamma_1 = \Gamma_2$) with the average SNR of the E_1-B link Γ_3 and E_2-B link Γ_4 fixed, ($\Gamma_3 = \Gamma_4 = 5$dB). The point-to-point (P2P) outage probabilities (OP), which are defined as the probability that the total joint source-channel coding rate exceeds the channel capacity, i.e., $\acute{R} > C_s$, are also plotted as the references. It is found that the only first-order diversity (no diversity gain) is shown in the outage curves for P2P transmission. However, as shown in the figure, there is a gap between the OP curves with a short package and with infinite block-length, which comes from the capacity reduction introduced by finite block-length. It clearly identifies the second-order diversity of the RSP curves since the destination receives two information copies of the same source sent from different relays. Due to the penalty introduced by the limited block length, RSP performance is poorer in short-packet communications than in the infinite block-length counterpart. However, notable diversity gain can still be achieved even when the packet is short. Note that the RSPs in short-packet communications are decreased with increasing average SNR in both A-E_1 and A-E_2 links, simultaneously, which have the same tendency with the results when the packet length is infinite. The reason behind this is that with the average SNR at the relays increase, the probability of the received information sequences being recovered errorlessly becomes high, which results in an RSP reduction.

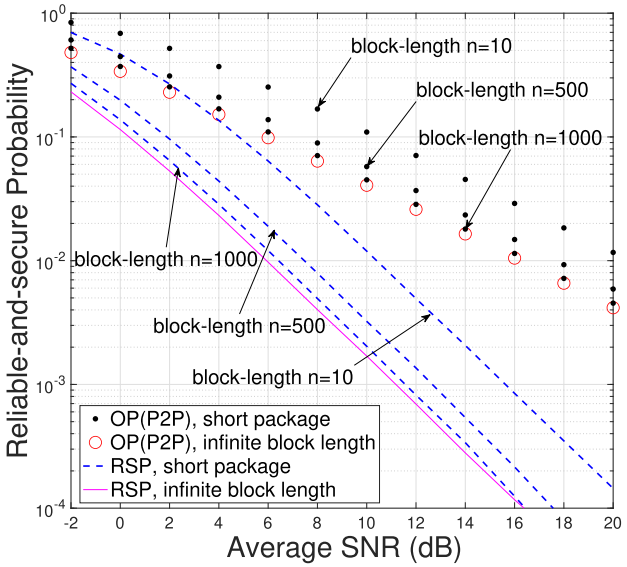


FIGURE 4. Reliable-and-secure probability versus average SNR (dB) of the A-E_1 and A-E_2, $\Gamma_1 = \Gamma_2$, with the block-length of each link as parameters. The average SNR of the E_1-B and E_2-B $\Gamma_3 = \Gamma_4$ are fixed. $\epsilon_1 = \epsilon_2 = \epsilon_3 = \epsilon_4 = 0.001$.

Fig. 5 shows the RSP versus the average SNR of the E_1-B link Γ_3 and E_2-B link Γ_4 ($\Gamma_3 = \Gamma_4$) with the average SNR of the A-E_1 link Γ_1 and A-E_2 link Γ_2 fixed ($\Gamma_1 = \Gamma_2 = 1$dB). As increasing the SNR of the E_1-B and E_2-B links, the probabilities of being correctly decoded at the destination increase, which enlarges the overall RSP according to the definition in (10). However, the performance gains are degraded when adopting short-packet communications.

Fig. 6 plots the RSP versus the average SNR with the block-length n as a parameter. The average SNR of the A-E_1, A-E_2, E_1-B, and E_2-B are assumed to be the same $\Gamma_1 = \Gamma_2 = \Gamma_3 = \Gamma_4$. It is found that the RSPs with short package increase first and then decrease as the average

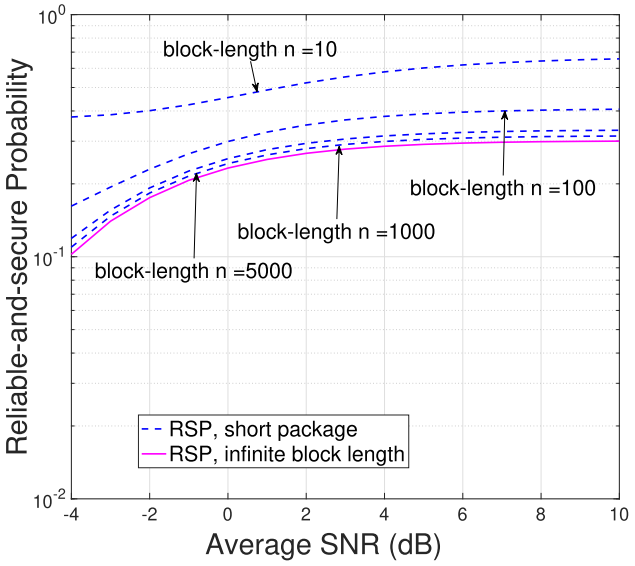


FIGURE 5. Reliable-and-secure probability versus average SNR (dB) of the E_1-B and E_2-B, $\Gamma_3 = \Gamma_4$, with the block-length of each link as parameters. The average SNR of the A-E_1 and A-E_2 $\Gamma_1 = \Gamma_2$ are fixed. $\epsilon_1 = \epsilon_1 = \epsilon_2 = \epsilon_3 = \epsilon_4 = 0.001$.

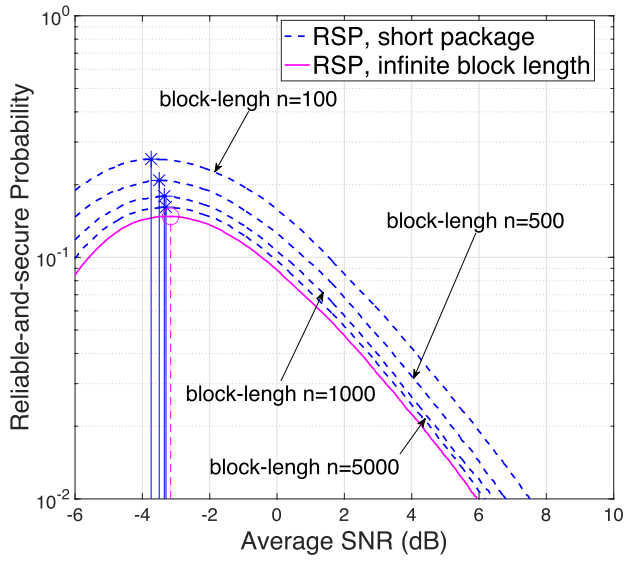


FIGURE 6. Reliable-and-secure probability versus average SNR (dB). The average SNR of the A-E_1, A-E_2, E_1-B, and E_2-B are assumed to be the same $\Gamma = \Gamma_1 = \Gamma_2 = \Gamma_3 = \Gamma_4$. $\epsilon_1 = \epsilon_2 = \epsilon_3 = \epsilon_4 = 0.001$.The vertical lines indicate the points where the RSPs are maximized.

SNR becomes large. This indicates that increasing the SNR does not constantly improve the RSP. As increasing SNR, the first term and the second term of the capacity $C_s(\gamma, n, \epsilon)$ in (1) become large simultaneously. Therefore, when the SNR increases, the probability of being correctly decoded at the destination increases, enlarging the overall RSP. However, the RSP reaches the maximum point when the contribution of the source-relay link and the relay-destination link is balanced. After that, the increasing SNR in the source-relay link dominates the RSP, which results in a decline in the RSP curves. The vertical lines in Fig. 6 indicate the point where the

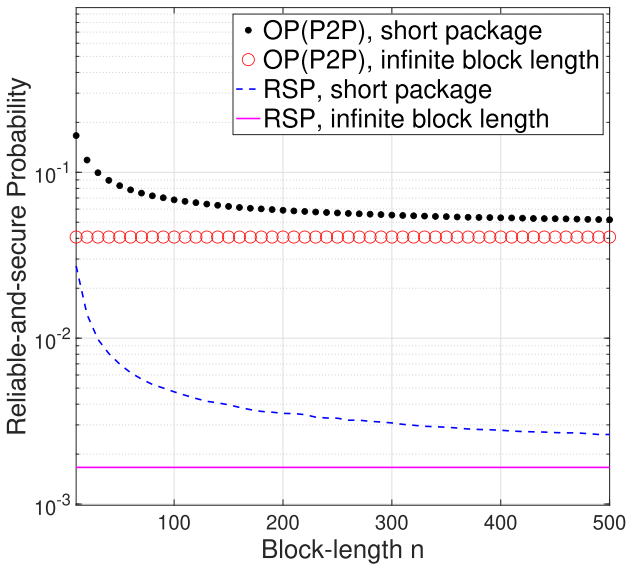


FIGURE 7. Reliable-and-secure probability versus block-length. The average SNRs of all the links are fixed at 5dB. $\epsilon_1 = \epsilon_2 = \epsilon_3 = \epsilon_4 = 0.001$.

RSP reach the maximum. It can be observed from the figure that the maximal RSP is achieved when the average SNR reach a certain point. However, as the block-length increases, the average SNR where RSP reaches the maximum point approaches the SNR where the RSP with infinite block-length reaches the maximum point.

Fig. 7 presents RSP versus the block-length n, with given ϵ and Γ in finite (short package) and infinite domains. As the curves show, compared to the infinite block-length case, utilizing of short package results in a loss related to n in terms of RSP. However, as n increases, the loss diminishes as the short package curve approaches the infinite curve when the block-length becomes longer. When $n \to \infty$, $C_s(\gamma, n, \epsilon)$ become consistent with $C(\gamma)$ asymptotically. Note that since the channel capacity in the presence of infinite block length would not change as $C(\gamma) = \log_2(1 + \gamma)$, the curves of RSP with infinite block length in Fig. 7 keep constant.

Fig. 8 shows the impact of the untrusted relay location on RSP performances of the diamond network in line-of-sight ($\rho = 2$) and non-line-of-sight ($\rho = 4$) environments. We assume that Eva_1 and Eva_2 move along the line between Alice and Bob, simultaneously, and $\Gamma_0 = 3$ (dB). It is found from Fig. 8 that the RSPs increase monotonously as Eva_1 and Eva_2 move from Alice to Bob. In both the line-of-sight ($\rho = 2$) and non-line-of-sight ($\rho = 4$) environments, the optimal untrusted relay locations that achieve the largest RSP are $\frac{d_3}{d_0} = \frac{d_4}{d_0} = 1$ or $\frac{d_1}{d_0} = \frac{d_2}{d_0} = 0$. This observation indicates that when Eva_1 and Eva_2 are close to the destination, the probability that they decode the received message decreases and the probability that Bob recovers the original information of Alice becomes large due to the proximity to the untrusted relays. It is worth noting that even though the information sequences forwarded by Eva_1 and Eva_2 may contain errors, they are from the same source, and therefore,

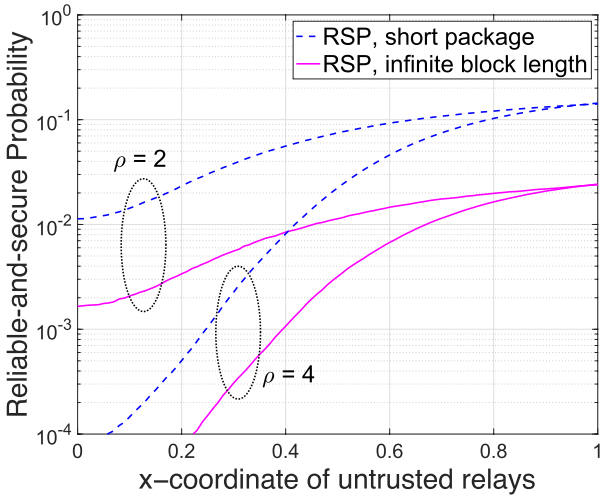


FIGURE 8. Reliable-and-secure probability versus untrusted relay locations with different path loss ρ with $\rho = 2$ for line-of-sight and $\rho = 4$ for non-line-of-sight environments, respectively. $n_1 = n_2 = n_3 = n_4 = 10$. $\epsilon_1 = \epsilon_1 = \epsilon_2 = \epsilon_3 = \epsilon_4 = 0.001$.

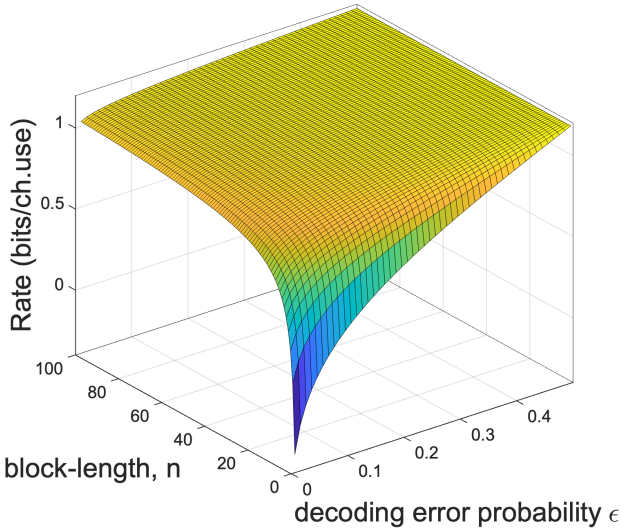


FIGURE 9. Short package capacity $C_s(\gamma, n, \epsilon)$ [bits/ch.use].

they are correlated. An iterative joint decoding process at Bob can retrieve the original message of Alice by utilizing the correlation between the information sequences transmitted from Eva_1 and Eva_2. Moreover, the performance difference between RSP with short package and RSP with infinite block length gradually vanishes when Eva_1 and Eva_2 get close to Bob.

V. CONCLUSION

In this paper, the reliable and secure performances of short-package transmission over a diamond relay system have been analyzed. Two untrusted relays utilize lossy DF relaying, which allows decoding errors in the source-relay links. The RSP of the proposed system has been calculated numerically, which distinguishes between reliability and security. The numerical results have shown that the maximum RSP is achieved when the contributions of source-relay transmission and the relay-destination transmission are balanced, which makes the investigations of the optimal power allocation are of great interest. The calculation framework proposed in this paper sheds light on analyzing the performance of multiple (more than three) untrusted relays scenarios by utilizing the multiple-terminal CEO problem analysis and multiple-source Slepian-Wolf theorem. Verification for the theoretical results via soft-defined radio and field test are planned as future work, along with the comparison with other physical layer security schemes, including directional modulation, covert communication, and emerging intelligent reflecting surface.

APPENDIX A
PERFORMANCE ANALYSIS OF $C_s(\gamma, n, \epsilon)$

The capacity (maximum rate) with short package $C_s(\gamma, n, \epsilon)$ in (1) is plotted in Fig. 9 versus the error probability ϵ and the block-length n. As ϵ $(0 \leq \epsilon \leq 0.5)$ is defined as a crossover probability of a binary symmetric channel (BSC), $C_s(\gamma, n, \epsilon)$ increases when the value of ϵ becomes larger. Since the inverse Q-function $Q^{-1}(\epsilon)$ is a monotone decreasing function on the domain of ϵ and $Q^{-1}(\epsilon = 0.5) = 0$, the second term of the polynomial in (1) becomes 0, and the capacity with short package $C_s(\gamma, n, \epsilon)$ turns into Gaussian capacity $C(\gamma)$. Therefore, the value of $C_s(\gamma, n, \epsilon)$ keeps constant when $\epsilon = 0.5$ regardless of the block-length n. As n increases, the value of $C_s(\gamma, n, \epsilon)$ also approaches the value $C(\gamma)$. This is because, with a non-0.5 ϵ value, the second term of the polynomial in (1) approaches an infinitely small value as n increases. However, n becomes less influential on the $C_s(\gamma, n, \epsilon)$ with larger ϵ. Similarly, ϵ becomes less influential on the $C_s(\gamma, n, \epsilon)$ with a longer block-length.

APPENDIX B
EXPLANATION OF TOTAL JOINT SOURCE-CHANNEL CODING RATE $\acute{R}$

A point-to-point signaling chain is shown in Fig. 10, where U is i.i.d binary information sequences with the length of L_u, V is L_v-bit information sequence outputted from the source encoder, and W represents the L_w-bit symbol sequences sent to the decoder over a channel. The joint encoder E_n, which can be regarded as a combination of source and channel encoders, assigns a codeword with length L_w to each sequence U, as $W = E_n(U)$. Modulation is ignored in Fig. 10 for the sake of simplicity.

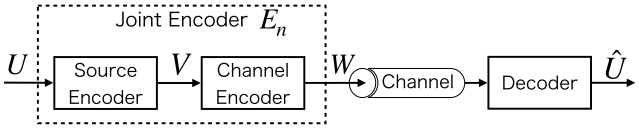


FIGURE 10. Abstract model for joint source-channel coding with source-channel separation.

According to the source-channel separation theorem [26, Theorem 3.7], the total joint source-channel coding rate is defined as

$$\acute{R} = \frac{L_v/L_w}{L_v/L_u} = \frac{L_u}{L_w}, \tag{30}$$

where L_v/L_u is the source coding rate, and L_v/L_w can be regarded as spectrum efficiency, including both channel coding rate and modulation multiplicity.

REFERENCES

[1] C. Feng and H.-M. Wang, "Secure short-packet communications at the physical layer for 5G and beyond," *IEEE Commun. Standards Mag.*, vol. 5, no. 3, pp. 96–102, Sep. 2021.

[2] H. V. Poor, M. Goldenbaum, and W. Yang, "Fundamentals for IoT networks: Secure and low-latency communications," in *Proc. 20th Int. Conf. Distrib. Comput. Netw.* New York, NY, USA: Association for Computing Machinery, Jan. 2019, pp. 362–364.

[3] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[4] B. Van Nguyen, H. Jung, and K. Kim, "Physical layer security schemes for full-duplex cooperative systems: State of the art and beyond," *IEEE Commun. Mag.*, vol. 56, no. 11, pp. 131–137, Nov. 2018.

[5] S. Zhao, J. Liu, Y. Shen, X. Jiang, and N. Shiratori, "Secure and energy-efficient precoding for MIMO two-way untrusted relay systems," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3371–3386, 2021.

[6] J. Xiong, L. Cheng, D. Ma, and J. Wei, "Destination-aided cooperative jamming for dual-hop amplify-and-forward MIMO untrusted relay systems," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7274–7284, Sep. 2016.

[7] Y. Oohama, "Coding for relay channels with confidential messages," in *Proc. IEEE Inf. Theory Workshop*, Sep. 2001, pp. 87–89.

[8] Y. Oohama, "Capacity theorems for relay channels with confidential messages," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 926–930.

[9] X. He and A. Yener, "Two-hop secure communication using an untrusted relay: A case for cooperative jamming," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Dec. 2008, pp. 1–5.

[10] X. He and A. Yener, "Two-hop secure communication using an untrusted relay," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, no. 1, pp. 1–13, Nov. 2009.

[11] A. Kuhestani, A. Mohammadi, and P. L. Yeoh, "Optimal power allocation and secrecy sum rate in two-way untrusted relaying networks with an external jammer," *IEEE Trans. Commun.*, vol. 66, no. 6, pp. 2671–2684, Jun. 2018.

[12] L. Lv, F. Zhou, J. Chen, and N. Al-Dhahir, "Secure cooperative communications with an untrusted relay: A NOMA-inspired jamming and relaying approach," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 12, pp. 3191–3205, Dec. 2019.

[13] R. Sun, B. Yang, Y. Shen, X. Jiang, and T. Taleb, "Covertness and secrecy study in untrusted relay-assisted D2D networks," *IEEE Internet Things J.*, vol. 10, no. 1, pp. 17–30, Jan. 2023.

[14] X. Pan, S. Ge, X. Zhou, and Z. Wang, "Physical layer security in untrusted decode-and-forward relay networks allowing intra-link errors," in *Proc. 15th Int. Conf. Mobile Ad-Hoc Sensor Netw. (MSN)*, Dec. 2019, pp. 119–124.

[15] C. Feng, H.-M. Wang, and H. V. Poor, "Reliable and secure short-packet communications," *IEEE Trans. Wireless Commun.*, vol. 21, no. 3, pp. 1913–1926, Mar. 2022.

[16] G. Durisi, T. Koch, and P. Popovski, "Toward massive, ultrareliable, and low-latency wireless communication with short packets," *Proc. IEEE*, vol. 104, no. 9, pp. 1711–1726, Sep. 2016.

[17] W. Yang, R. F. Schaefer, and H. V. Poor, "Wiretap channels: Nonasymptotic fundamental limits," *IEEE Trans. Inf. Theory*, vol. 65, no. 7, pp. 4069–4093, Jul. 2019.

[18] V. N. Vo, D.-D. Tran, C. So-In, and H. Tran, "Secrecy performance analysis for fixed-gain energy harvesting in an Internet of Things with untrusted relays," *IEEE Access*, vol. 6, pp. 48247–48258, 2018.

[19] D. Wan, M. Wen, F. Ji, H. Yu, and F. Chen, "On the achievable sum-rate of NOMA-based diamond relay networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 2, pp. 1472–1486, Feb. 2019.

[20] F. Kara and H. Kaya, "Error probability analysis of NOMA-based diamond relaying network," *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 2280–2285, Feb. 2020.

[21] S. Qian, X. Zhou, X. He, J. He, M. Juntti, and T. Matsumoto, "Performance analysis for lossy-forward relaying over Nakagami-*m* fading channels," *IEEE Trans. Veh. Technol.*, vol. 66, no. 11, pp. 10035–10043, Nov. 2017.

[22] Z. Xiang, W. Yang, Y. Cai, Z. Ding, Y. Song, and Y. Zou, "NOMA-assisted secure short-packet communications in IoT," *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 8–15, Aug. 2020.

[23] Y. Polyanskiy, H. V. Poor, and S. Verdu, "Channel coding rate in the finite blocklength regime," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2307–2359, Apr. 2010.

[24] A. Goldsmith, *Wireless Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

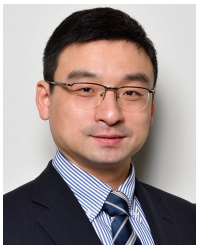
[25] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[26] A. E. Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[27] X. Zhou, N. Yi, X. He, J. Hou, T. Matsumoto, S. Szott, D. Gonzales, A. Wolf, M. Matthe, S. Kuhlmorgen, and O. Adigun, "Deliverable D1.2.1, assessment on feasibility, achievability, and limits V1.0," ICT-619555 RESCUE, Tech. Rep. D1.2.1, Apr. 2015.

[28] X. He, X. Zhou, P. Komulainen, M. Juntti, and T. Matsumoto, "A lower bound analysis of Hamming distortion for a binary CEO problem with joint source-channel coding," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 343–353, Jan. 2016.

[29] M. Dohler and Y. Li, *Cooperative Communications: Hardware, Channel and PHY*. Hoboken, NJ, USA: Wiley, 2010.



SHEN QIAN (Member, IEEE) received the degree from the School of Telecommunication Engineering, Xidian University, Xi'an, China, in 2003, the M.Sc. and Ph.D. degrees in information science from the Japan Advanced Institute of Science and Technology (JAIST), in 2014 and 2017, respectively, and the Ph.D. degree in communications engineering from the University of Oulu, Finland, in 2017.

From 2018 to 2019, he was a Postdoctoral Researcher with the Information Theory and Signal Processing Laboratory, JAIST. Since 2019, he has been an Assistant Professor with the Department of Information Systems Creation, Faculty of Engineering, Kanagawa University, Japan. His research interests include network information theory, cooperative wireless communication, and information transmission security in the IoT networks.

Dr. Qian was a recipient of the IEICE Outstanding Student Award, in 2014; the NEC C&C Grants for Non-Japanese Researchers, in 2015; the IEEE International Conference on Communications (ICC) Presentation Award, in 2016; the JAIST Outstanding Performance Award, in 2017; and the Niwa Yasujiro Memorial Paper Awards, in 2019 and 2020, consecutively.