Comm&Optics Connect
ISSN: 3006-4813
2025, Article ID. 2025.0004, Cite as: https://doi.org/10.69709/COConnect.2024.003818

SCIFINITI

Research Article

OPEN ACCESS

Physical Layer Security in Lossy Untrusted Relay Networks with Finite Blocklength

Shen Qian[✉,1,*] **Meng Cheng**[✉,2]

[1] Department of Science and Technology, Faculty of Science and Technology, Seikei University, Tokyo 180-8633, Japan
[2] College of Information, Mechanical and Electrical Engineering, Shanghai Normal University, Shanghai 200234, China

Article History
Submitted: October 27, 2024 Accepted: December 02, 2024 Published: March 18, 2025

Abstract
In this paper, we examine the physical layer security (PLS) in lossy untrusted relay networks, focusing on finite blocklength transmissions. In such networks, ensuring secure communication is particularly challenging due to the presence of untrusted relay nodes and the inherent limitations of short-packet transmissions. We propose the reliable-and-secure probability (RSP) as a performance metric to evaluate the likelihood that the destination node successfully recovers the transmitted message while untrusted relays experience an outage. Two basic network topologies are taken into consideration, which are the three-node one way network and the single-source multi-untrusted-relay network without direct source-to-destination link. By optimizing power allocation and relay positioning, the RSP can be significantly improved, even when decoding errors occur at the relays. The study demonstrates that lossy decode-and-forward relaying complicates secure communication but also presents opportunities for performance enhancement through careful resource management. Numerical simulations validate the effectiveness of the proposed optimization strategies in enhancing security, especially for applications in ultra-reliable low-latency communication and massive machine-type communication in 5G/6G networks. Future research will focus on deriving more precise closed-form expressions for RSP in finite blocklength settings and investigating machine learning-based approaches for real-time optimization of secure communications in dynamic wireless environments. This study contributes to the growing body of knowledge on PLS in modern wireless systems, offering insights for future advancements.

Keywords:
physical layer security (PLS); untrusted relay networks; finite blocklength; reliable-and-secure probability

1. Introduction

The increasing reliance on wireless networks for secure communication has introduced new vulnerabilities where traditional cryptographic measures may be insufficient. Physical layer security (PLS) has emerged as a promising alternative, offering a way to secure communications by exploiting the inherent properties of wireless channels, for example, noise, fading, and interference [1,2]. This is particularly critical in networks with untrusted relay nodes, where data confidentiality is at risk due to the presence of intermediary nodes that may not be fully reliable, as shown in Figure 1.

Untrusted relay networks introduce a unique set of challenges. These networks often involve relay nodes that assist in forwarding messages, but may attempt to intercept or modify the transmitted data [3,4]. The use of lossy channels further complicates the secure transmission of data, as these channels are prone to signal degradation and higher bit error rates (BER). Such environments require innovative solutions to ensure both the reliability and security of communication, even when relays are untrusted and channels are imperfect [5,6].

Short-packet communication is regarded a key technology for supporting emerging 5G and beyond application scenarios [7]. For instance, in intelligent sensing, short packets are commonly used by IoT devices and sensors in ultra-reliable low-latency communications (uRLLC) and massive machine-type communications (mMTC) [8]. The traditional consideration of wireless

* **Corresponding Author:**
Shen Qian, Department of Science and Technology, Faculty of Science and Technology, Seikei University, Tokyo 180-8633, Japan; shen-qian@st.seikei.ac.jp

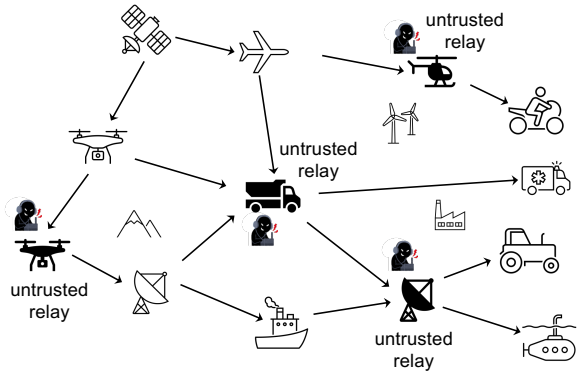

Figure 1: Application scenarios of untrusted relay networks.

transmission with Shannon's information theory is inadequate for designing infinite-block-length communications or evaluating their performance. With short-packet transmissions, the header length of the package cannot be ignored compared to the payload [9], and (2) limited block-length introduces unavoidable decoding errors and potential information leakage due to backoff from capacity [10]. As a result, short-packet transmissions experience reduced channel capacity, making it more difficult to achieve reliable communication.

This paper focuses on the evaluation of PLS in lossy untrusted relay networks, particularly under finite block-length regimes. In these scenarios, where direct source-to-destination communication is infeasible, relay nodes are essential. However, the trustworthiness of the relays and the lossy nature of the channels present significant security risks. We explore how PLS techniques can be applied to improve the security of these networks, ensuring that confidential messages remain protected even in the presence of untrusted relays.

In addition, we examine the role of finite block-length communication in these systems. Short packet transmissions, a key requirement for uRLLC, introduce challenges in achieving high secrecy rates due to the limited number of channel uses. We investigate the trade-offs between security and efficiency in such networks and propose strategies to optimize performance under these constraints [11].

The following of this paper is organized as follows: Section 2 discusses the fundamental concepts of physical layer security in the context of lossy channels and untrusted relay networks. Section 3 delves into PLS in three-node untrusted lossy one-way relaying. Section 4 focuses on the performance analysis in diamond short-packet communication systems. Section 5 lists some challenges and future research directions for PLS in relay networks. Section 6 concludes the paper.

2. Lossy Channels in Untrusted Relay Networks

2.1. Security Threats in Untrusted Relays

In wireless communication systems, untrusted relay nodes present several security challenges that can compromise the confidentiality of the data being transmitted. The presence of these relay nodes, which might act as potential eavesdroppers, complicating secure transmission. These challenges arise from the following key factors:

- Risk of Eavesdropping: Untrusted relays, although intended to assist in signal forwarding, can intercept and decode confidential information. As described in various studies, including, untrusted relays can act as eavesdroppers while forwarding information between two parties. The relay may opportunistically exploit its position to decode and intercept sensitive information without the authorization of the legitimate users [12,13].
- Relaying Vulnerabilities: In the relay node amplifies the received signal, amplify-and-forward (AF), which includes both the legitimate data and any noise, or decode the received signal DF and forwards it to the destination. However, if the relay is untrusted, it can potentially decode the signal before forwarding it. This issue is compounded in multi-input multi-output (MIMO) systems, where the untrusted relay could have access to multiple data streams, increasing the chances of successful interception [14,15].
- PLS Limitations: while PLS is employed to protect transmissions by exploiting the characteristics of the wireless channel, its effectiveness is reduced when the relay itself is untrusted. The relay may still capture the signal, especially if it is equipped with multiple antennas or operates in full-duplex mode, allowing for simultaneous transmission and reception. This setup enhances its eavesdropping capabilities [16,17].

Mitigating these challenges requires advanced techniques, such as adaptive precoding and cooperative jamming, where the legitimate parties deliberately introduce interference to confuse the untrusted relay, thereby preventing it from extracting useful information.

2025, Vol. 1, Article ID. 2025.0004
https://doi.org/10.69709/COConnect.2024.003818

2.2. Challenges and Opportunities of Lossy Channels on Secure Communication

Lossy channels present significant challenges for information transmission, particularly when implementing PLS. The inherent degradation in signal quality due to noise, fading, and interference increases the bit error rate (BER) and complicates the secure transmission of confidential data. One primary issue is that lower signal-to-noise ratios (SNR) result in higher BER, which makes it easier for legitimate receivers or relays to misinterpret the transmitted message. This potentially leads to compromising the integrity of sensitive information. Traditional PLS approaches, such as artificial noise and cooperative jamming injection, often face challenges in these conditions due to their reliance on the stability and quality of the channel. As the channel fluctuates, these methods become less reliable [18].

In systems that use decode-and-forward (DF) relays, lossy channels can introduce errors in the relayed signals, which untrusted relays could exploit to intercept and decode part of the confidential message [19]. AF relays, on the other hand, amplify both the signal and the noise, complicating the implementation of security measures such as cooperative jamming. Moreover, the randomness and unpredictability of fading conditions could sometimes allow the eavesdropper's channel to outperform that of the legitimate receiver, eventually reducing the secrecy capacity and compromising the system's security.

Despite these challenges, lossy channels can also be leveraged to enhance PLS. The natural noise and interference in these channels make it harder for eavesdroppers to reconstruct the original message accurately. Typically, the eavesdropper has imperfect channel knowledge, and as a result, receives a more distorted version of the signal compared to the legitimate receiver. This gives the legitimate user, supported by error correction mechanisms, a greater chance of successfully recovering the message while the eavesdropper struggles to do so [20].

Moreover, lossy channels create opportunities to implement controlled interference techniques such as cooperative jamming and artificial noise injection. By introducing targeted noise that selectively degrades the signal quality at the eavesdropper's receiver without significantly affecting the legitimate receiver, these methods can obscure the eavesdropper's ability to decode the transmission. In DF relay systems, lossy channels can be used to introduce controlled errors, making it more difficult for eavesdroppers to extract useful information. While this may introduce additional challenges for legitimate receivers, effective error correction techniques can still allow them to recover the message accurately.

3. Materials and Methods

3.1. Physical Layer Security in Untrusted Lossy One-Way Relay Networks

In this work, the main focus is on a short-packet transmission system involving three nodes, as illustrated in Figure 2. In this system, a legitimate sender, the source (Alice), communicates confidential data to another legitimate recipient, the destination (Bob), with assistance from an intermediary node (Eve). However, Eve is considered an untrusted relay with low trust level. We consider a single antenna setup due to limitations in power and size.

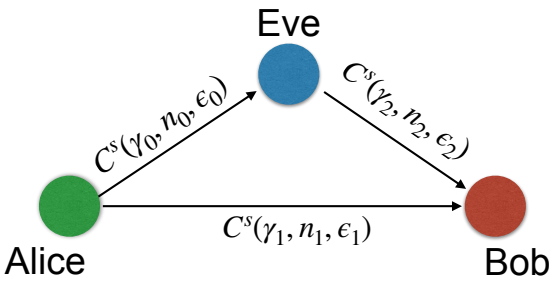

Figure 2: Three-node one-way cooperative relay network with one untrusted relay.

We consider a Time Division Multiple access (TDMA) scheme, where transmission is divided into two distinct time phases. In the 1st time phase, Alice broadcasts the independent and identically distributed (i.i.d.) message $\mathbf{b}_A$. During the 2nd time phase, the relay node, Eve, attempts to decode $\mathbf{b}_A$ and forward it to Bob, utilizing orthogonal transmission. Due to the lossy decode-and-forward (DF) relay setup, Eve's decoding result, denoted as $\mathbf{b}$E, may contain errors. Nevertheless, Eve interleaves $\mathbf{b}_E$, encodes the received message, re-transmits it to the destination Bob. Alice remains inactive in the 2nd time phase.

After receiving signals from both, Alice and Eve, Bob performs joint decoding to recover the original sequence $\mathbf{b}_A$. An iterative decoding process with two decoders is used to retrieve Alice's original messages. The two decoders exchange the decoded bits' log-likelihood ratios through an interleaver and de-interleaver.

2025, Vol. 1, Article ID. 2025.0004
https://doi.org/10.69709/COConnect.2024.003818

3.2. Channel Type

The received signals in Bob and Eva are presented by

$$y'_{\mathrm{B}} = \sqrt{P_{\mathrm{E}}^{t} G_2} h_2 x_{\mathrm{E}} + n'_{\mathrm{B}}, \tag{1}$$

$$y_{\mathrm{E}} = \sqrt{P_{\mathrm{A}}^{t} G_0} h_0 x_{\mathrm{A}} + n_{\mathrm{E}}, \tag{2}$$

$$y_{\mathrm{B}} = \sqrt{P_{\mathrm{E}}^{t} G_1} h_1 x_{\mathrm{A}} + n_{\mathrm{B}}. \tag{3}$$

P_i^t is the transmit power, n_i $(i \in \mathrm{A}, \mathrm{E}, \mathrm{B})$ and x_i represent the zero-mean additive white Gaussian noise (AWGN) and modulated symbols for the encoded information sequences. $n'\mathrm{B}$ and $y'\mathrm{B}$ refer to the noise and received signals during the 2nd time phase.

We assume $\mathbb{E}[|h_j|^2] = 1$ and that h_j remains constant during one block ubder the assumption of block-fading. For clarity, symbol indices have been omitted in Equations (20)–(22).

Each of the communication links is assumed to undergo Rayleigh fading. The PDF for the instantaneous SNR γ_j following Rayleigh distribution is expressed as

$$f(\gamma_j) = \frac{1}{\Gamma_j} \exp(-\frac{\gamma_j}{\Gamma_j}). \tag{4}$$

3.3. Reliable-and-Secure Probability (RSP) Definition

The RSP refers to the likelihood that Bob decodes the information sent by Alice successfully, while the untrusted relay Eva experiences an outage. This probability can be formulated as

$$\begin{aligned} P_{\mathrm{RSP}} &= P_{\mathrm{out}}^{\mathrm{E}} - P_{\mathrm{out}}^{\mathrm{B}}, \\ &= \underbrace{\Pr\{\text{Eva outage}\}}_{P_{\mathrm{out}}^{\mathrm{E}}} - \underbrace{\Pr\{\text{Eva outage} \cap \text{Bob outage}\}}_{P_{\mathrm{out}}^{\mathrm{B}}}. \end{aligned} \tag{5}$$

Here, P^{E}out denotes the probability that outage happens at the untrusted relay, while P^{B}out represents the outage probability occurs at both the untrusted relay and the destination simultaneously.

To provide a clearer understanding of the proposed RSP metric, a comparative analysis has been included in the Table 1 with other commonly used metrics in physical layer security. This comparison highlights the unique advantages of RSP in addressing finite blocklength constraints, which are critical for short-packet communications in 5G/6G networks.

3.4. Bob and Eva's Admissible Rate Region

As destination, Bob's objective is to decode $\mathbf{b}_{\mathrm{A}}$, the signal $\mathbf{b}_{\mathrm{E}}$ sent from Eva is regarded as supplementary information for $\mathbf{b}_{\mathrm{A}}$. Let $\mathbf{b}_{\mathrm{A}}$ and $\mathbf{b}_{\mathrm{E}}$ have transmission rates of R_1^s and R_2^s, respectively. Based on the source coding with helper theorem ([21], Section 10.4), Bob is able to successfully retrieve $\mathbf{b}_{\mathrm{A}}$ when R_1^s and R_2^s meet the following conditions

$$\begin{cases} R_1^s & \geq H(\mathbf{b}_{\mathrm{A}}|\hat{\mathbf{b}}_{\mathrm{E}}), \\ R_2^s & \geq I(\mathbf{b}_{\mathrm{E}}; \hat{\mathbf{b}}_{\mathrm{E}}). \end{cases} \tag{6}$$

In this context, $H(\cdot|\cdot)$ represents the conditional entropy, while $I(\cdot;\cdot)$ refers to the mutual information between the respective variables. The term $\hat{\mathbf{b}}\mathrm{E}$ denotes Bob's estimate of $\mathbf{b}\mathrm{E}$, with an associated error probability of ϵ_2. The rate region defined by Equation (6) is illustrated in Figure 3.

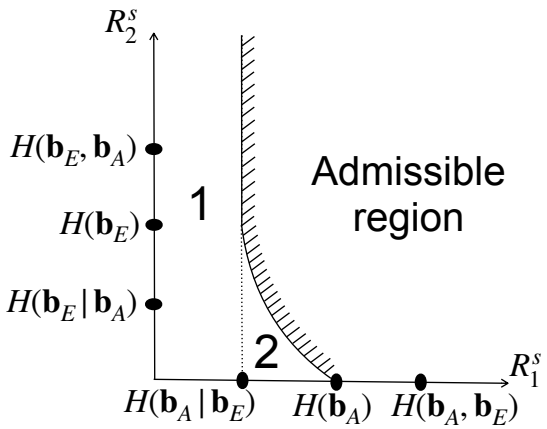

Figure 3: Achievable rate regions: $\mathbf{b}_{\mathrm{A}}$ and $\mathbf{b}_{\mathrm{E}}$ is derived from the source coding with a helper theorem.

In this paper, we focus on a source that is independently and i.i.d., and thus Equation (6) can be reformulated as

$$\begin{cases} R_1^s & \geq H(\mathcal{D} * \epsilon_0 * \epsilon_2), \\ R_2^s & \geq H(\hat{\mathbf{b}}_{\mathrm{E}}) - H(\hat{\mathbf{b}}_{\mathrm{E}}|\mathbf{b}_{\mathrm{E}}). \end{cases} \tag{7}$$

$A * B = (1-A)B + (1-B)A$ is the binary convolution. With binary source, $H(\hat{\mathbf{b}}_{\mathrm{E}}) - H(\hat{\mathbf{b}}_{\mathrm{E}}|\mathbf{b}_{\mathrm{E}}) = 1 - H(\epsilon_2) = 1 - [-\epsilon_2 \log_2 \epsilon_2 - (1-\epsilon_2)\log_2(1-\epsilon_2)]$. For Gaussian source, $H(\hat{\mathbf{b}}_{\mathrm{E}}) - H(\hat{\mathbf{b}}_{\mathrm{E}}|\mathbf{b}_{\mathrm{E}}) = \frac{1}{2}\log(2\pi\sigma_E^2) - \frac{1}{2}\log\left(2\pi\sigma_{\epsilon_2}^2\right)$, where σ_E^2 and $\sigma_{\epsilon_2}^2$ are the variances of $\hat{\mathbf{b}}_{\mathrm{E}}$ and ϵ_2, respectively.

2025, Vol. 1, Article ID. 2025.0004
https://doi.org/10.69709/COConnect.2024.003818

Table 1: Comparative analysis of RSP with the other metrics.

Metric	Definition	Feature
Reliable-and-secure Probability (RSP)	Probability that the legitimate receiver successfully decodes a message while untrusted relays experience an outage	Captures decoding errors and packet length constraints; highly applicable to finite blocklength scenarios
Secrecy Outage Probability	Probability that the eavesdropper's channel capacity exceeds the legitimate user's channel capacity	Focuses on channel secrecy without considering finite blocklength constraints
Secure Connectivity Probability	Probability that a secure link is established between source and destination	Measures network-level security but lacks granularity in packet-level reliability
Secure Capacity	Maximum achievable data rate ensuring security against eavesdroppers	Based on Shannon's infinite blocklength assumptions; not suitable for short-packet transmissions

In accordance with source-channel separation theorem, if

$$\begin{cases} R_1^s \acute{R}_1 & \leq C_1^s(\gamma_1, n_1, \epsilon_1), \\ R_2^s \acute{R}_2 & \leq C_1^s(\gamma_2, n_2, \epsilon_2). \end{cases} \tag{8}$$

The error probability can be reduced to an arbitrarily small value. $\acute{R}1$ and $\acute{R}2$ denote the overall source-channel joint coding rates for the source-destination and relay-destination channels, respectively. The terms $C_1^s(\gamma_1, n_1, \epsilon_1)$ and $C_2^s(\gamma_2, n_2, \epsilon_2)$ refer to secrecy capacities of the respective links when considering a finite blocklength.

3.5. Bob's Outage Probability

Since we assume block fading, for a given γ_0, n_0, and ϵ_0, an outage occurs during a transmission if (R_1^s, R_2^s) lies in the inadmissible rate region shown in Figure 3. Under the assumption, the fading variation varies block by block, the values of $\mathcal{D}$, γ_j, n_i, and ϵ_i $(j \in 0, 1, 2)$ vary from block to block. As a result, the Berger-Tung bound, which requires a fixed distortion level, is not applied to calculate the outage probability for the Eva-Bob transmission.

As defined in Equation (24), the probability $P_{\text{out}}^{\text{B}}$ can be expressed as

$$P_{\text{out}}^{\text{B}} = P_1 + P_2 \tag{9}$$

where

$$P_1 = \Pr[0 \leq R_1^s < H(\epsilon_1), R_2^s \geq 0, 0 < \mathcal{D} \leq 0.5] \tag{10}$$

and

$$\begin{aligned} P_2 = \Pr[&H(\epsilon_1) \leq R_1^s < H(\mathbf{b}_{\text{A}}), \\ &0 \leq R_2^s < H(\mathcal{D} * \epsilon_0 * \epsilon_2), 0 < \mathcal{D} \leq 0.5] \end{aligned} \tag{11}$$

These probabilities represent the likelihood that (R_1^s, R_2^s) fall outside the admissible rate area can be separated into two distinct regions, 1 and 2, as illustrated in Figure 3.

Note that Equations (10) and (11) do not include the case when $\epsilon_0 = 0$, which indicates the perfect decoding at Eva (no outage). When $\epsilon_0 = 0$, the inadmissible rate region becomes a triangle area as presented in Figure 2 in [22].

The error probabilities $\epsilon_0, \epsilon_1, \epsilon_2$ and the rates R_0^s, R_1^s, R_2^s are related to the corresponding link's instantaneous SNRs, as shown in Equations (8), (28) and (29). Consequently, P_1 and P_2 can be written as

$$\begin{aligned} P_1 = \Pr[0 < H^{-1}&\left(1 - \frac{C^s(\gamma_0, n_0, \epsilon_0)}{\acute{R}_0}\right) \leq 0.5, \\ &0 \leq \frac{C^s(\gamma_1, n_1, \epsilon_1)}{\acute{R}_1} < H(\epsilon_1), \\ &\frac{C^s(\gamma_2, n_2, \epsilon_2)}{\acute{R}_2} \geq 0] \end{aligned} \tag{12}$$

and

$$\begin{aligned} P_2 = \Pr[0 < H^{-1}&\left(1 - \frac{C^s(\gamma_0, n_0, \epsilon_0)}{\acute{R}_0}\right) \leq 0.5, \\ &H(\epsilon_1) \leq \frac{C^s(\gamma_1, n_1, \epsilon_1)}{\acute{R}_1} < H(\mathbf{b}_{\text{A}}), \\ &0 \leq \frac{C^s(\gamma_2, n_2, \epsilon_2)}{\acute{R}_2} < H(\mathcal{D} * \epsilon_0 * \epsilon_2)]. \end{aligned} \tag{13}$$

$H^{-1}(\cdot)$ is the inverse function of $H(\cdot)$ for binary source.

With Gaussian source,

$$P_1 = \Pr[0 < \sigma^2 2^{-\frac{2C^s(\gamma_0,n_0,\epsilon_0)}{\acute{R}_0}} \leq 0.5, \\ 0 \leq \frac{C^s(\gamma_1,n_1,\epsilon_1)}{\acute{R}_1} < H(\epsilon_1), \\ \frac{C^s(\gamma_2,n_2,\epsilon_2)}{\acute{R}_2} \geq 0] \tag{14}$$

and

$$P_2 = \Pr[0 < \sigma^2 2^{-\frac{2C^s(\gamma_0,n_0,\epsilon_0)}{\acute{R}_0}} \leq 0.5, \\ H(\epsilon_1) \leq \frac{C^s(\gamma_1,n_1,\epsilon_1)}{\acute{R}_1} < H(\mathbf{b}_{\mathrm{A}}), \\ 0 \leq \frac{C^s(\gamma_2,n_2,\epsilon_2)}{\acute{R}_2} < H(\mathcal{D} * \epsilon_0 * \epsilon_2)]. \tag{15}$$

The derivation of explicit expressions for Equations (12)–(15) can become highly complicated due to the intricacy of $C_1^s(\gamma_1,n_1,\epsilon_1)$ and $C_2^s(\gamma_2,n_2,\epsilon_2)$. As a result, a Monte Carlo simulation is employed to compute P^{E}out and P^{B}out numerically.

3.6. Optimal Power Allocation

Under the total power constraint E_T, the optimal power allocation corresponds to the point where the maximum RSP is achieved. By normalizing the noise variance for each channel to unity, the average SNR, which corresponds to the transmit power, allocated to Alice and Eva is represented by kE_T and $(1-k)E_T$, respectively, where k $(0 \leq k \leq 1)$ represent the ratio for allocated power. Given that $\Gamma 0 = kE_T$ and $\Gamma 0 = (1-k)E_T$, the expression for P^{E}out becomes $P^{\mathrm{E}}\mathrm{out} = F(kE_T,;2^{R_0(\mathcal{D}_0)\acute{R}_0} - 1)$ and $P_{\mathrm{out}}^{\mathrm{B}}$ can be written as

$$P_{\mathrm{out}}^{\mathrm{B}} = \int_0^{2^{1-\frac{C_0(\gamma_0,n_0,\epsilon_0)}{\acute{R}_0}}-1} f(\gamma_1,\ kE_T)d\gamma_1 \\ \int_0^{2^{\acute{R}_0}-1} f(\gamma_0,\ kE_T)d\gamma_0 \int_0^{\infty} f(\gamma_2,\ (1-k)E_T)d\gamma_2 \\ + \int_0^{2^{\acute{R}_0}-1} f(\gamma_0,\ kE_T)d\gamma_0 \\ \int_{2^{1-\frac{C_0(\gamma_0)}{\acute{R}_0}}-1}^{1} f(\gamma_1,\ kE_T)d\gamma_1 \\ \int_0^{\xi(\gamma_1,\gamma_2)} f(\gamma_2,\ (1-k)E_T)d\gamma_2. \tag{16}$$

The main difficulty is determining the optimal k that maximizes the system's RSP. This involves improving Bob's capability to correctly decode Alice's message while simultaneously reducing Eva's likelihood of intercepting and decoding the original information. The goal is to strike a balance between these two factors, therefore, optimizing the system's security. This challenge can be formally represented through maximizing the RSP, and the optimization can be formulated as:

$$k^* = \begin{array}{ll} \arg\max\limits_{k} & P_{\mathrm{RSP}}(k) \\ \text{subject to:} & -k \leq 0, \quad k-1 \leq 0, \quad -E_{\mathrm{T}} < 0. \end{array} \tag{17}$$

In theory, by calculating the second-order partial derivative of P_{RSP} with respect to k, the extreme point can be identified, and the convexity can be verified by determining whether the integral results are positive or negative within the range $k \in (0,1)$. Given the complexity in deriving the explicit expression for $P_{\mathrm{out}}^{\mathrm{B}}$, a numerical approach is employed to find the optimal power ratio.

3.7. Key Insights for RSP Analysis

The derived expressions for RSP reveal a fundamental trade-off between ensuring reliable communication at the destination and preventing information leakage at untrusted relays. This highlights the importance of balancing these factors through power allocation. The finite blocklength constraint introduces decoding errors at the relays, which can inadvertently improve security by increasing the likelihood of an outage at the untrusted relay nodes. However, it also necessitates the precise power optimization to maintain reliability. The RSP's dependence on multiple variables, such as blocklength, SNR, and decoding error probabilities, underscores the need for computationally efficient optimization techniques, especially in dynamic networks. These insights offer valuable guidelines for designing secure wireless systems where short-packet communication is essential, such as in uRLLC and mMTC scenarios.

4. Untrusted Diamond Relay Networks

In this section, the focus is on a relay network depicted in Figure 4. A legitimate source, Alice, sends information to another legitimate destination, Bob, with the assistance of two untrusted relays, Eva_1 (E_1) and Eva_2 (E_2). Due to obstacles or significant shadowing, direct link is not available between Alice and Bob.

The two intermediate nodes, Eva_1 and Eva_2, receive and forward the confidential information. However, both Eva_1 and Eva_2 are treated as untrusted relays due to their low security clearance. Each node is equipped with a single antenna, constrained by power constrains and facility size.

We consider the Alice-to-Bob transmission is split into two time slots. In the 1st time slot, Alice encodes, modulates, and broadcasts the confidential i.i.d. binary information sequences. These sequences follow a Bernoulli(p) $(0 \leq p \leq 1)$ distribution. During the

2025, Vol. 1, Article ID. 2025.0004
https://doi.org/10.69709/COConnect.2024.003818

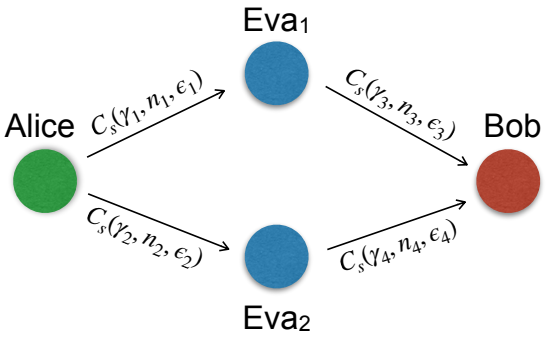

Figure 4: Diamond network with two untrusted relay.

2nd time slot, Eva_1 and Eva_2 recover the received information sequences and encode the messages before forwarding them to the destination through the designated phases, i.e., in orthogonal pattern. Alice remains inactive in the 2nd phase. It is to be noted that utilizing separate time slots for transmission could degrade spectral efficiency. However, NOMA transmission could improve the reduced spectral efficiency [23,24]. Optimization for the two time slots will be considered in future work.

In the system, Lossy DF is employed at Eva_1 and Eva_2 to enhance transmission's reliability, while maintaining message confidentiality. The sequences received by Eva_1 and Eva_2 may contain errors due to the inaccuracies in decoding, which have relation to the received SNRs. Under the lossy DF relaying scheme, both Eva_1 and Eva_2 always re-encode the received messages, forwarding them to destination, even when errors are present in the decoding process.

Once Bob receives the signals from Eva_1 and Eva_2, a joint decoding is carried out to recover the information transmitted by Alice. An iterative decoding process is applied [22] with two decoders responsible for decoding the original information forwarded by Eva_1 and Eva_2.

4.1. Short Package Transmission

Channel capacity is often regarded as a fundamental performance metric in traditional wireless communication systems. Typically, performance analyses assume an infinite block-length, which leads to the derived performance limits serving as upper bounds. However, in practical scenarios such as uRLLC and mMTC, the infinite packet-length assumption is no longer appropriate to evaluate the performance of secrecy. Additionally, short-block communications offer a solution for reducing delays, making them ideal for applications which is time-sensitive, by minimizing transmission latency [25].

The maximum rate for finite packet-length (short-block) communications, corresponding to C_s (channel capacity with short-block), is provided by [26]

$$C_s(\gamma, n, \epsilon) = -\sqrt{\frac{V}{n}} Q^{-1}(\epsilon) + C(\gamma). \tag{18}$$

$C(\gamma) = \log_2(1+\gamma)$ is the conventional Shannon's Gaussian channel capacity. n, ϵ and V represent the block-length, the decoding error probability, and the fluctuations is express as

$$V = \frac{\gamma(\gamma+2)\log^2 e}{(\gamma+1)^2 2}. \tag{19}$$

e and $Q^{-1}(x)$ are Euler's number and inverse Q-function $Q(x)$ [27], respectively.

4.2. Channel Model

Let P_i^t $(i \in \text{A}, \text{E}_1, \text{E2})$ represent the transmission power of the respective node, and let G_k denote the geometric gains, where $k \in \{1,2,3,4\}$ corresponds to AE_1, AE_2, E_1B, and E_2B links, respectively. The signals received by Eva_1, Eva_2, and Bob are

$$y_{\text{E}_1}[n] = \sqrt{P_{\text{A}}^t G_1} h_1 x_{\text{A}}[n_1] + n_{\text{E}_1}[n_1], \tag{20}$$

$$y_{\text{E}_2}[n] = \sqrt{P_{\text{A}}^t G_2} h_2 x_{\text{A}}[n_2] + n_{\text{E}_2}[n_2], \tag{21}$$

$$y_{\text{B}}[n] = \sqrt{P_{\text{E}_1}^t G_3} h_3 x_{\text{E}_1}[n_3] + n_{\text{B}}[n_3], \tag{22}$$

$$y'_{\text{B}}[n] = \sqrt{P_{\text{E}_2}^t G_4} h_4 x_{\text{E}_2}[n_4] + n'_{\text{B}}[n_3]. \tag{23}$$

where

- n represent the symbols' timing index, under an orthogonal transmission assumption. We omit the symbol indices in the subsequent sections for brevity.
- x_j denotes the coded transmit symbol.
- n_k $(k \in \text{E1}, \text{E2}, \text{B})$ is AWGN with zero-mean and variance of $\frac{N_0}{2}$ in each dimension.
- h_j refers to the gain of the corresponding channels. h_j remains constant over the duration of one block under a block-fading assumption, with $\mathbb{E}[|h_j|^2] = 1$.
- y'_{B} represent received signal.
- n'_{B} indicate AWGN.

Let $\gamma_j = |h_j|^2 \Gamma_j$ and $\Gamma j = P_k^r \frac{E_s}{N_0}$ $(j \in 1,2,3,4, k \in \text{E}_1, \text{E}_2, \text{B})$ be the instantaneous and average SNRs at Eva1, Eva2, and Bob, respectively, where E_s represents the transmission power for each symbol. It is assumed that all links are subject to i.i.d. Rayleigh fading.

4.3. Definition for Reliable-and-Secure Probability

The objective is to transmit messages to Bob, while ensuring that untrusted relays cannot access the confidential information. A common way is to transmit the information sequences at a rate lower than the secrecy rate [28] from Alice to Bob. However, if there is no direct link between Alice and Bob, it is not possible to achieve the secrecy rate [13].

With lossy DF employed at the relays, decoding errors are permissible at Eva. The decoded message at the Eva are then re-transmit to Bob after re-encoding. Same as the previous section, we define the RSP with the probability that Bob successfully decodes the message sent by Alice, while an outage occurs at Eva_1 and Eva_2, as

$$\begin{aligned} P_{\text{RSP}} &= P_{\text{out}}^{\text{E}} - P_{\text{out}}^{\text{B}}, \\ &= \underbrace{\Pr\{\text{outage at Eva}_1 \cap \text{outage at Eva}_2\}}_{P_{\text{out}}^{\text{E}}} \\ &\quad - \underbrace{\Pr\{\text{outage at Eva}_1 \cap \text{outage at Eva}_2 \cap \text{outage at Bob}\}}_{P_{\text{out}}^{\text{B}}}. \end{aligned} \tag{24}$$

Here, $P_{\text{out}}^{\text{E}}$ represents the outage probability at both untrusted relays. Meanwhile, P^{B}out denotes the outage probability at the Bob and at the, Eva_1 and Eva_2, simultaneously.

4.4. Analyses for Relay-Destination Links' Error Probability

Due to the lossy DF setup, errors are permitted in the untrusted relay-destination links (Alice-Eva_1 and Alice-Eva_2), the rates for the Alice-Eva_1 and Alice-Eva_2 links can be achieved when

$$\begin{cases} C_s(\gamma_1, n_1, \epsilon_1) \geq R_1^s(\mathcal{D}_1)\acute{R}_1, \\ C_s(\gamma_2, n_2, \epsilon_2) \geq R_2^s(\mathcal{D}_2)\acute{R}_2 \end{cases} \tag{25}$$

based on the theorem of source-channel separation coding with distortion ([21], Theorem 3.7), with distortions $\mathcal{D}_1$ and $\mathcal{D}_2$. $R_1^s(\mathcal{D}1)$ and $R2^s(\mathcal{D}_2)$ are the rate-distortion functions for the Alice-Eva_1 and Alice-Eva_2 links, respectively, with distortion $\mathcal{D}1$ and $\mathcal{D}2$. The terms $\acute{R}1$ and $\acute{R}2$ denote the source-channel coding total rates.

With binary source following Bernoulli(p) distribution,

$$R^s(\mathcal{D}) = \begin{cases} 0, & \mathcal{D} > \min(p, 1-p) \\ 1 - H(\mathcal{D}), & 0 \leq \mathcal{D} \leq \min(p, 1-p). \end{cases} \tag{26}$$

Here, $H(X) = -X\log_2(X) - (1-X)\log_2(1-X)$ represents the entropy function.

For Gaussian source,

$$R^s(\mathcal{D}) = \begin{cases} R^s(\mathcal{D}) = \frac{1}{2}\log_2\frac{\sigma^2}{\mathcal{D}}, & 0 \leq \mathcal{D} \leq \sigma^2 \\ 0, & \mathcal{D} > \sigma^2. \end{cases} \tag{27}$$

with distribution $N(0, \sigma^2)$.

It should be noted that the minimum distortions $\min \mathcal{D}_1$ and $\min \mathcal{D}_2$ correspond to the transmission error probabilities in Alice-Eva_1 and Alice-Eva_2 channels, respectively, with the Hamming distortion measure.

Based on Equations (18) and (25), the contact between $R^s(\mathcal{D})$ and γ can be established with

$$\begin{aligned} R^s(\mathcal{D})\acute{R} &\leq C(\gamma) - \sqrt{\tfrac{V}{n}}Q^{-1}(\epsilon), \\ &= \log_2(1+\gamma) - \sqrt{\tfrac{1-(1+\gamma)^{-2}}{n}}Q^{-1}(\epsilon) \end{aligned} \tag{28}$$

for Bernoulli($\frac{1}{2}$) sources. Whereas for Gaussian sources

$$\begin{aligned} R^s(\mathcal{D})\acute{R} &= \tfrac{1}{2}\log_2\tfrac{\sigma^2}{\mathcal{D}}\acute{R} \leq C(\gamma_0) - \sqrt{\tfrac{V}{n}}Q^{-1}(\epsilon), \\ &= \log_2(1+\gamma) - \sqrt{\tfrac{1-(1+\gamma)^{-2}}{n}}Q^{-1}(\epsilon). \end{aligned} \tag{29}$$

4.5. Outage Probabilities at Eva_1 and Eva_2

In short-packet communications, $P_{\text{out}}^{\text{E}}$ in Equation (24) is defined as the scenario where the transmission rates $\acute{R}_1$ and $\acute{R}_2$, with block-lengths n_1 and n_2, respectively, exceed the tolerable distortion levels $\mathcal{D}_1$ and $\mathcal{D}_2$, as

$$\begin{aligned} P_{\text{out}}^{\text{E}} =& \Pr\left\{\acute{R}_1 R_1^s(\mathcal{D}_1) \leq C_s(\gamma_1, n_1, \epsilon_1)\right\} \\ &\cdot\Pr\left\{\acute{R}_2 R_2^s(\mathcal{D}_2) \leq C_s(\gamma_2, n_2, \epsilon_2)\right\} \\ =& \Pr\left\{0 \leq \gamma_1 \leq C_s^{-1}\left(\acute{R}_1 R_1^s(\mathcal{D}_1), n_1, \epsilon_1\right)\right\} \\ &\cdot\Pr\left\{0 \leq \gamma_2 \leq C_s^{-1}\left(\acute{R}_2 R_2^s(\mathcal{D}_2), n_2, \epsilon_2\right)\right\} \\ =& \int_0^{C_s^{-1}\left(\acute{R}_1 R_1^s(\mathcal{D}_1), n_1, \epsilon_1\right)} f(\gamma_1)d\gamma_1 \\ &\cdot \int_0^{C_s^{-1}\left(\acute{R}_2 R_2^s(\mathcal{D}_2), n_2, \epsilon_2\right)} f(\gamma_2)d\gamma_2. \end{aligned} \tag{30}$$

$C_s^{-1}(\cdot,\cdot,\cdot)$ represents $C_s(\cdot,\cdot,\cdot)$' inverse function. Equation (30) establishes based on theorem of Shannon's source-channel separation and independent fading assumption.

During each fading phase, quasi-static fading channel behaves equivalently to an AWGN channel. The gain of channel remains constant within each phase but varies from phase to phase, based on channel fading distributions. As a result, the outage probability $P_{\text{out}}^{\text{E}}$ is computed with integrals of the probability density function (PDF) of the instantaneous SNRs within the rate region of inadmissibility.

2025, Vol. 1, Article ID. 2025.0004
https://doi.org/10.69709/COConnect.2024.003818

4.6. Analyses for Inadmissible Rate Region for Chief Executive Officer (CEO) Problem with Slepian-Wolf Coding

Let U represent the messages transmitted by Alice, and U_3 and U_4 denote the messages output by Eva_1 and Eva_2, corresponding to rates R_3^s and R_4^s, respectively. The sequences received by Eva_1 and Eva_2 have errors with a certain probability, meaning ($U \neq U_3$ $U \neq U_4$), according to concept of lossy DF. Despite these errors, Eva_1 and Eva_2 re-transmit the erroneous messages to Bob. Consequently, the analyses of the Eva_1-Bob and Eva_2-Bob transmissions belongs to the CEO problem category in network information theory [21]. The structure of the CEO encoding is shown in Figure 5. U_1 and U_2 are omitted in this paper, in order to maintain notation consistency. Under the assumption of block fading, the error probabilities in the Alice-Eva_1 and Alice-Eva_2 links remain constant throughout a transmission block.

Since U_3 and U_4 both originate from Alice, U_3 and U_4 are correlated. We use the bit-flipping model to represent the correlation with: $U_3 = U_4 \oplus \varepsilon_0$, where a random variable ε_0 is defined $\Pr(\varepsilon_0 = 1) = 1 - \Pr(\varepsilon_0 = 0) = \rho_0$. Here, ρ_0 represents the occurrence probability for flipped bit of U_3 and U_4.

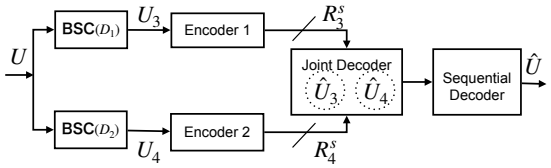

Figure 5: Binary CEO source coding schematic diagram.

According to the Slepian-Wolf theorem, since U_3 and U_4 have correlation, successful decoding of U_3 and U_4 can be achieved if the source rates of U_3 and U_4, (R_3^s, R_4^s), satisfy

$$\begin{cases} R_3^s & \geq H(U_3|\hat{U}_4), \\ R_4^s & \geq H(U_4|\hat{U}_3), \\ R_3^s + R_4^s & \geq H(U_3, U_4). \end{cases} \tag{31}$$

In this context, $\hat{U}_3$ and $\hat{U}_4$ are the estimates of U_3 and U_4, respectively, based on the decoding output at Bob. The terms $H(U_3|\hat{U}_4)$ and $H(U_4|\hat{U}_3)$ represent conditional entropy. The relationships between U_3 and $\hat{U}_3$, as well as between U_4 and $\hat{U}_4$, are represent by a bit-flipping pattern. The erroneous probabilities in the Eva_1-Bob and Eva_2-Bob links remain steady during one transmission phase, under the assumption of block fading. Thus, ε_3 and ε_4 are treated as constant parameters in each block. We consider i.i.d. source, $H(U_3|\hat{U}_4) = H(\varepsilon_0 * \varepsilon_3)$ and $H(U_4|\hat{U}_3) = H(\varepsilon_0 * \varepsilon_4)$, where $\alpha * \beta = (1-\beta)\alpha + (1-\alpha)\beta$.

In the case when both U_3 and U_4 can be completely decoded by Bob, meaning $U_3 = \hat{U}_3$ and $U_4 = \hat{U}_4$, with $\varepsilon_3 = 0$ and $\varepsilon_4 = 0$. This scenario corresponds to (R_3^s, R_4^s) falling into regions 1 and 2 in Figure 6. In the second situation, U_3 (or U_4) is decoded with an arbitrarily low error probability, whereas, U_4 (or U_3) is fully erroneous. In this situation, $\hat{U}_4$ (or $\hat{U}_3$) does not provide any meaningful information of U_4 (or U_3). The criteria then changes to $[R_k^s \geq H(U_3), R_k^s \geq 0]$ ($k \in \{3, 4\}$), which corresponds to region 3 and 4, as shown in Figure 6.

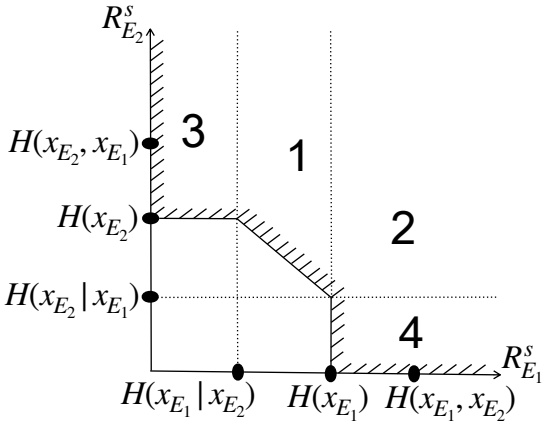

Figure 6: Admission rate region for U_1 and U_2 determined by Slepian-Wolf coding.

4.7. Formulation of CEO Problem

For a binary source, $H(U_3) = H(U_4) = 1$, $H(U_3|U_4) = H(U_4|U_3) = H(\rho_0)$, 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. It is important to note that ρ_0 is related to $\mathcal{D}_1$ and $\mathcal{D}_2$. When distortion does not exist in the Alice-Eva_1 (Alice-Eva_2) transmissions, i.e., $\mathcal{D}_1 = 0$ and $\mathcal{D}_2 = 0$, U_3 and U_4 become identical, meaning $\rho_0 = 0$.

For a Gaussian source $N \sim (0, \sigma^2)$, we have $h(U_3) = h(U_4) = \frac{1}{2}\log_2 2\pi e\sigma^2$, $h(U_4|U_3) = h(U_4, U_3) - h(U_3)$ ($h(U_3|U_4) = h(U_3, U_4) - h(U_4)$). Here, $h(\cdot)$, $h(\cdot, \cdot)$, and $h(\cdot|\cdot)$ represent differential entropy, differential entropy, and conditional entropy.

Let $\mathcal{D}_3$ and $\mathcal{D}_4$ denote the distortion levels for $\Pr(U_3 \neq \hat{U}_3)$ and $\Pr(U_4 \neq \hat{U}_4)$, respectively. Since the lowest distortion $\min\{\mathcal{D}_3\}$ and $\min\{\mathcal{D}_4\}$ are the same as p_3 and p_4, the Hamming distortion of L symbols is represented as

$$E\left[\frac{1}{l}\sum_{l=1}^{L} d\left(U_k, \hat{U}_k\right)\right] \leq \mathcal{D}_k + \delta, \quad k \in (3, 4), \tag{32}$$

to assess the probability of error propagation using

$$d(U_k,\hat{U}_k)=\begin{cases}1, & \text{if } U_k\neq\hat{U}_k,\\ 0, & \text{if } U_k=\hat{U}_k,\end{cases}\qquad k\in(3,4). \tag{33}$$

δ represents a positive number that is arbitrarily smaller, and $E[\cdot]$ denotes the expectation. Eventually, Bob estimates the message from Alice, by utilizing either majority decoding ([29], Section 4.1) or the optimal decision method [30].

4.8. Outage Probability at Bob

$P_{\text{out}}^{\text{B}}$ in Equation (24) is represented as

$$P_{\text{out}}^{\text{B}}=\Pr(\tilde{\mathcal{D}}>\min_{\mathcal{D}_3,\mathcal{D}_4}\{\mathcal{D}_3,\mathcal{D}_4\}), \tag{34}$$
$$\text{s.t.}\begin{cases}R_3^s(\mathcal{D}_3)\acute{R}_3 & \leq C_s(\gamma_3,n_3,\epsilon_3)\\ R_4^s(\mathcal{D}_4)\acute{R}_4 & \leq C_s(\gamma_4.n_4,\epsilon_4)\end{cases}$$

$\tilde{\mathcal{D}}=f(\cdot,\cdot)$ represents a function for sequential decoding associated with the decoding scheme. For a detailed explanation of the function $f(\cdot,\cdot)$, readers may refer to ([30], IV-A).

5. Results and Discussion

5.1. Reliable-and-Secure Probability Calculation

Since Alice-Eva transmission error is allowed, the Eva_1-Bob (Eva_2-Bob) transmission is equal to a CEO problem. With P_k $(k\in 1,2,3,4)$ defining the probability that the rate (R_3^s,R_4^s) falls into region k in Figure 6 for a certain value of γ, n, and ϵ. Then, $P_{\text{out}}^{\text{B}}$ is defined as

$$P_{\text{out}}^{\text{B}}=1-P_1-P_2-P_3-P_4. \tag{35}$$

Please note that, the outage happens when the distortion $\tilde{\mathcal{D}}$ outstrips $\min\{\mathcal{D}_1,\mathcal{D}_2\}$ as denoted in Equation (34). Hence, we can also treat regions 3 and 4 in Figure 6 as admissible regions if $R_3^s\geq H(U_3)$ and $R_4^s\geq H(U_3)$. Distortion level can satisfy $D_1\leq p_1$ and $D_2\leq p_2$, respectively.

When connect the rates R_3^s and R_4^s with the instantaneous channel SNRs γ_3 and γ_4, block-lengths n_3 and n_4, and error probabilities ϵ_3 and ϵ_4, P_k $(k\in 1,2,3,4)$ can be defined by averaging over the transmissions in Eva_1-Bob and Eva_2-Bob channels,

$$\begin{aligned}P_1=\ &\Pr\Big\{R_1^s(\mathcal{D}_1)>\tfrac{C_s(\gamma_1,n_1,\epsilon_1)}{\acute{R}_1},\\ &R_2^s(\mathcal{D}_2)>\tfrac{C_s(\gamma_2,n_2,\epsilon_2)}{\acute{R}_2},\\ &H(U_3|U_4)<R_3^s<H(U_3),R_3^s+R_4^s>H(U_3,U_4)\}\\ =\ &\Pr\Big\{\gamma_1>C_s^{-1}\big(\acute{R}_1R_1^s(\mathcal{D}_1),n_1,\epsilon_1\big),\\ &\gamma_2>C_s^{-1}\big(\acute{R}_2R_2^s(\mathcal{D}_2),n_2,\epsilon_2\big),\\ &H(\rho)<\tfrac{C_s(\gamma_3,n_3,\epsilon_3)}{\acute{R}_3}<H(U_1),\\ &\tfrac{C_s(\gamma_3,n_3,\epsilon_3))}{\acute{R}_3}+\tfrac{C_s(\gamma_4,n_4,\epsilon_4))}{\acute{R}_4}>H(U_3,U_4)\Big\},\end{aligned} \tag{36}$$

$$\begin{aligned}P_2=\ &\Pr\Big\{R_1^s(\mathcal{D}_1)>\tfrac{C_s(\gamma_1,n_1,\epsilon_1)}{\acute{R}_1},\\ &R_2^s(\mathcal{D}_2)>\tfrac{C_s(\gamma_2,n_2,\epsilon_2)}{\acute{R}_2},\\ &R_3^s>H(U_3),R_4^s>H(U_4|U_3)\}\\ =\ &\Pr\Big\{\gamma_1>C_s^{-1}\big(\acute{R}_1R_1^s(\mathcal{D}_1),n_1,\epsilon_1\big),\\ &\gamma_2>C_s^{-1}\big(\acute{R}_2R_2^s(\mathcal{D}_2),n_2,\epsilon_2\big),\\ &\tfrac{C_s(\gamma_3,n_3,\epsilon_3)}{\acute{R}_3}>H(U_3),\\ &\tfrac{C_s(\gamma_4,n_4,\epsilon_4)}{\acute{R}_4}>H(U_4|U_3)\Big\},\end{aligned} \tag{37}$$

$$\begin{aligned}P_3=\ &\Pr\Big\{R_1^s(\mathcal{D}_1)>\tfrac{C_s(\gamma_1,n_1,\epsilon_1)}{\acute{R}_1},\\ &R_2^s(\mathcal{D}_2)>\tfrac{C_s(\gamma_2,n_2,\epsilon_2)}{\acute{R}_2},\\ &0<R_3^s<H(U_3|U_4),R_4^s>H(U_4)\}\\ =\ &\Pr\Big\{\gamma_1>C_s^{-1}\big(\acute{R}_1R_1^s(\mathcal{D}_1),n_1,\epsilon_1\big),\\ &\gamma_2>C_s^{-1}\big(\acute{R}_2R_2^s(\mathcal{D}_2),n_2,\epsilon_2\big),\\ &0<\tfrac{C_s(\gamma_3,n_3,\epsilon_3)}{\acute{R}_3}<H(U_3|U_4),\\ &\tfrac{C_s(\gamma_4,n_4,\epsilon_4)}{\acute{R}_4}>H(U_4)\Big\},\end{aligned} \tag{38}$$

and

$$\begin{aligned}P_4=\ &\Pr\Big\{R_1^s(\mathcal{D}_1)>\tfrac{C_s(\gamma_1,n_1,\epsilon_1)}{\acute{R}_1},\\ &R_2^s(\mathcal{D}_2)>\tfrac{C_s(\gamma_2,n_2,\epsilon_2)}{\acute{R}_2},\\ &0<R_4^s<H(U_4|U_3),R_3^s>H(U_3)\}\\ =\ &\Pr\Big\{\gamma_1>C_s^{-1}\big(\acute{R}_1R_1^s(\mathcal{D}_1),n_1,\epsilon_1\big),\\ &\gamma_2>C_s^{-1}\big(\acute{R}_2R_2^s(\mathcal{D}_2),n_2,\epsilon_2\big),\\ &0<\tfrac{C_s(\gamma_4,n_4,\epsilon_4)}{\acute{R}_4}<H(U_4|U_3),\\ &\tfrac{C_s(\gamma_3,n_3,\epsilon_3)}{\acute{R}_3}>1\Big\},\end{aligned} \tag{39}$$

The derivation of the explicit expressions for Equations (36)–(39) may prove to be extremely challenging, due to the computational complexity of $C_s(\gamma,n,\epsilon)$. However, we introduce Monte Carlo simulations to compute $P^{\text{E}}\text{out}$ and $P^{\text{B}}\text{out}$ numerically.

$P_{\text{out}}^{\text{B}}$ is also influenced by the levels of $\mathcal{D}_1$ and $\mathcal{D}_2$, which vary with changes in γ_1 and γ_2, respectively, from phase to phase according to the assumption of block fading.

Figure 7 illustrates the relationship between the RSP and the average SNR, with varying values of error probability ϵ as a key parameter. Additionally, reliable-and-secure probabilities are shown for the infinite block length scenario as a comparative reference. The infinite block length performance curves are also influenced by ϵ (error probability) due to the utilization of rate-distortion function. When $\epsilon=0.5$, the RSP remains identical for both short packets and infinite block length, reflecting the same

2025, Vol. 1, Article ID. 2025.0004
https://doi.org/10.69709/COConnect.2024.003818

performance. Here, ϵ is specified as the BSC's crossover probability; thus, for $\epsilon = 0.5$, the transmitted message sent from Alice and that received at Eva are entirely uncorrelated. The capacities of the short packet and Gaussian channels converge as ϵ approaches 0.5. When $\epsilon \neq 0.5$, the RSP for short packets is lower than that achieved RSP with infinite block length. Whereas, for a fixed n, the secrecy capacity increases consistently with rising values of ϵ from 0 to 0.5. Consequently, by allowing for a degree of decoding inaccuracy, a higher RSP can be attained in short packet transmissions.

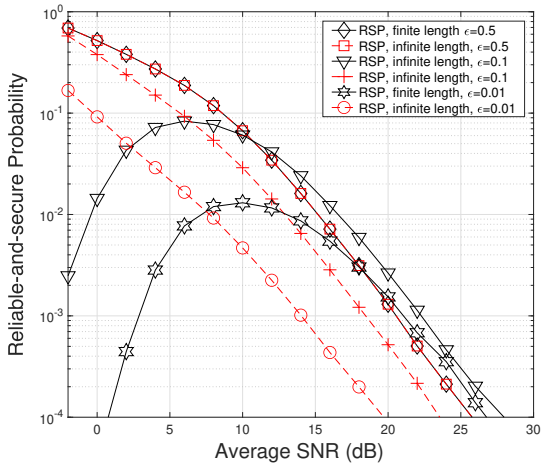

Figure 7: RSP versus average SNR (dB). Each link has the same average SNR. $n_0 = n_1 = n_2 = 1000$. $\epsilon = \epsilon_0 = \epsilon_1 = \epsilon_2$.

As observed in Figure 7, the RSP with short packets initially increases and subsequently declines as the average SNR increases. This trend reveals that enhancing the SNR does not always lead to a higher RSP. With increasing SNR, both the first and second terms $C^s(\gamma, n, \epsilon)$ in Equation (18) increase simultaneously. Furthermore, an increase in the SNR of the Alice-Eva(s) links leads to higher probabilities of correct decoding at the relays, ultimately decreasing the total RSP. However, the RSP attains the peak value when the Alice-Eva and Eva-Bob link contributions are balanced.

5.2. Relays Location with RSP

We focus on the relationship between the untrusted relay locations and the RSP. We reformulate the RSP equation as functions of the relay positions by incorporating the geometric gain. With d_k $(k \in 1, 2, 3, 4)$ representing the length of the each channel, the SNR is proportional to the channel length inversely, as

$$\Gamma_j \propto \frac{1}{d_j^{\rho}}, \tag{40}$$

ρ represents the path loss exponent Suppose, the distance between Alice and Bob is d_0 and an average SNR of Γ_0. We have each link's average SNRs as

$$\Gamma_j = \Gamma_0 \left(\frac{d_0}{d_j}\right)^{\rho}. \tag{41}$$

By substituting Equation (41) into Equations (36)–(39), we obtain the RSP expressions as functions of the untrusted relay positions. Comprehensive optimization has been formulated with respect to d_j as:

$$\begin{aligned} d_j^* = \arg\max_{d_k} \quad & P_{\text{RSP}}(d_j) \\ \text{subject to:} \quad & 0 \leq d_k,\ 0 \leq d_0. \end{aligned} \tag{42}$$

5.3. Optimization Strategy with Cooperative Jamming

Here, we demonstrate an approach to improve the RSP with allocating transmission power between Alice, Eva_1 optimally, Eva_2, and Bob, under an overall transmission power restriction En condition. Firstly, the variance of noise in each link to a unity has been normalized. Hence, the transmit power is equal to the average SNR for S, UR_1, UR_2, and D is denoted as αEn, $(1-\alpha\beta)E_T$, and $(1-\alpha)(1-\beta)En$, respectively. Here, α $(0 < \alpha \leq 1)$ and β $(0 \leq \alpha \leq 1)$ are the ratios for power allocation. Since the two untrusted relays are symmetric, Eva_1 and Eva_2 are treated as a single entity in the power allocation analysis.

The main challenge is determining the optimal values for α and β that maximize the system's RSP. This involves improving the ability of Bob to recover the message transmitted by the source in a reliable way, whereas, reducing the potential for untrusted relays to intercept and decode the information sequences, simultaneously. The goal is to optimize the security of the transmission by effectively settling these two respects, as represented in the RSP maximization metric formally.

Then, we formulate the optimization issue to:

$$\begin{aligned} \alpha^*, \beta^* = \quad & \arg\max_{\alpha,\beta} \quad P_{\text{RSP}}(\alpha, \beta) \\ & \text{subject to:} \quad \alpha - 1 \leq 0, \quad -\alpha \leq 0 \\ & \qquad\qquad\ \ \beta - 1 \leq 0, \quad -\beta \leq 0 \\ & \qquad\qquad\ \ -En < 0. \end{aligned} \tag{43}$$

Notionally, by computing the partial derivatives to α and β, we can identify the apices of P_{RSP}, and determine the eigenvalues and determinant with respect to Hessian matrix. However, due to the complexity in deriving an explicit expression for P_{RSP}, a numerical approach is employed for searching the optimal allocated power ratio.

6. Challenges and Future Research Directions

6.1. Implementation Considerations and Challenges

The optimization of RSP involves solving non-linear equations with multiple constraints, which may require significant computational resources. Real-time deployment demands efficient algorithms capable of rapid convergence. Variations in channel conditions, such as fading and mobility, require the optimization process to adapt dynamically. Traditional methods may not respond effectively to such rapid changes, necessitating adaptive approaches. Deploying these strategies on resource-constrained devices (e.g., IoT sensors) may pose challenges due to limited processing power and energy availability. Lightweight approximations or machine learning models could mitigate these issues.

To validate the proposed RSP metric under practical conditions, future work will leverage software-defined radios (SDRs) to simulate real-world environments. SDRs will allow testing of dynamic network scenarios, including varying relay positions, finite blocklength constraints, and power allocation strategies, while accounting for hardware-induced noise and interference. A testbed using platforms like GNU Radio and USRP will emulate the roles of source, untrusted relay, and destination to measure RSP and optimize performance. Insights from these experiments will guide the design of full-scale field tests, ensuring the robustness and practicality of RSP-based strategies for 5G/6G applications.

6.2. Open Issues in Secure Relay Networks

There are several unsolved challenges in secure relay networks, particularly when it comes to achieving efficient and secure communication in the presence of untrusted relays. One major issue is the development of efficient relay selection algorithms. Current methods often do not account for the complexity of the environment, such as varying channel conditions and the dynamic behavior of untrusted nodes. Additionally, the optimal relay selection under power and security constraints remains computationally intensive, especially when the network grows in scale.

Another critical open issue is the implementation of PLS in complex environments, such as those characterized by block fading, short-packet communications, or high mobility (e.g., vehicular networks). These scenarios introduce new challenges for maintaining high secrecy performance due to rapid channel variations and limited transmission opportunities. Addressing these issues requires more adaptive and efficient approaches that can dynamically optimize security and reliability in real-time.

6.3. Future Directions in PLS

The future of PLS lies in expanding its applicability and robustness in more demanding and dynamic environments. One key direction is the development of adaptive power allocation strategies for secure communication. As outlined in the optimization problems discussed earlier, balancing transmit power between trusted and untrusted nodes while maximizing RSP is non-trivial. Future research should focus on efficient numerical methods or approximate closed-form solutions for real-time optimization, especially in the presence of finite block-length constraints.

Machine learning (ML) and AI-based approaches are likely to play a significant role in advancing PLS. These techniques could be leveraged to predict channel conditions and optimize secure communication strategies dynamically. The integration of reinforcement learning to adaptively select relay nodes and power allocations based on real-time network conditions is another direction worth exploring.

Reinforcement learning algorithms could dynamically optimize power allocation and relay selection by continuously learning from real-time network conditions. These methods can significantly reduce computational overhead while adapting to channel variations, making them suitable for high-mobility scenarios [31,32].

Non-orthogonal multiple access (NOMA) is another key area for future research, particularly in improving spectral efficiency and security for short-packet communications. The integration of PLS with NOMA schemes could further enhance secure communications in highly dense IoT environments, which are expected to proliferate with the advent of 6G. Combining PLS with NOMA could improve spectral efficiency and security in densely connected environments like IoT networks.

As the adoption of emerging technologies like 5G/6G and edge computing accelerates, physical layer security must evolve to keep pace with the increasing complexity and demands of these systems. One key research direction is integrating PLS with edge computing to offload security-sensitive computations and leverage distributed resources for enhanced secrecy. This could involve designing secure offloading mechanisms that ensure confidentiality even when processing data near untrusted nodes or networks.

2025, Vol. 1, Article ID. 2025.0004
https://doi.org/10.69709/COConnect.2024.003818

7. Conclusions

This paper investigates the performance and security challenges associated with PLS in lossy untrusted relay networks, particularly under the constraints of finite block-length. The main contributions is the development of a RSP metric, which quantifies the likelihood of successful message recovery at the destination while ensuring the confidentiality of the message from untrusted relays. A key challenge addressed is the impact of decoding errors at the relays, which are allowed under the lossy DF setup. The paper further explores optimal power allocation and relay location strategies to enhance RSP performance. The numerical analyses demonstrates that even in the presence of imperfect decoding and lossy channels, optimal resource allocation can significantly improve the reliability and security. Practical implications of these findings are highly relevant for the design of secure communication systems in emerging 5G/6G networks, particularly in the contexts of uRLLC and mMTC.

Abbreviations

AF	Amplify-and-Forward
AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
CEO	Chief Executive Officer
DF	Decode-and-Forward
i.i.d.	Independent and Identically Distributed
IoT	Internet of Things
MIMO	Multi-Input Multi-Output
ML	Machine Learning
mMTC	Massive Machine-Type Communications
NOMA	Non-Orthogonal Multiple Access
PLS	Physical Layer Security
RSP	Reliable-and-Secure Probability
SDR	Software-Defined Radio
SNR	Signal-to-Noise Ratio
TDMA	Time Division Multiple Access
uRLLC	Ultra-Reliable Low-Latency Communications

Author Contributions

S.Q.: Conceptualized and designed the research study, developed the methodology, wrote the software, and conducted formal analysis and investigations. Managed the data curation and performed the visualization of the results. Authored the original draft and actively participated in reviewing and editing the manuscript. M.C.: Supervised the research project and was responsible for project administration and securing funding. Provided significant intellectual contributions and participated in reviewing and editing the manuscript. Collaborated in conceptualizing the research study and played a critical role in validating the results.

Availability of Data and Materials

Data supporting the results of this study are available upon request from the corresponding author.

Consent for Publication

Not applicable.

Conflicts of Interest

The authors declare no conflicts of interest regarding this manuscript.

Funding

No external funding was received for this research.

Acknowledgments

Declared None.

References

[1] Poor, H.V.; Schaefer, R.F. Wireless Physical Layer Security. *Proc. Natl. Acad. Sci. USA* **2017**, *114*, 19–26. [CrossRef]

[2] Xie, N.; Li, Z.; Tan, H. A Survey of Physical-Layer Authentication in Wireless Communications. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 282–310. [CrossRef]

[3] Wang, W.; Teh, K.C.; Li, K.H. Relay Selection for Secure Successive AF Relaying Networks with Untrusted Nodes. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 2466–2476. [CrossRef]

[4] Hu, H.; Gao, Z.; Liao, X.; Leung, V.C.M. Secure Communications in CIoT Networks with a Wireless Energy Harvesting Untrusted Relay. *Sensors* **2017**, *17*, 2023. [CrossRef]

[5] Sun, L.; Ren, P.; Du, Q.; Wang, Y.; Gao, Z. Security-Aware Relaying Scheme for Cooperative Networks with Untrusted Relay Nodes. *IEEE Commun. Lett.* **2015**, *19*, 463–466. [CrossRef]

[6] Zamir, N.; Ali, B.; Butt, M.F.U.; Javed, M.A.; Lee, B.M.; Ng, S.X. Cooperative Jamming-Assisted Untrusted Relaying Based on Game Theory for Next-Generation Communication Systems. *Appl. Sci.* **2023**, *13*, 7863. [CrossRef]

[7] Feng, C.; Wang, H.-M. Secure Short-Packet Communications at the Physical Layer for 5G and Beyond. *IEEE Commun. Stand. Mag.* **2021**, *5*, 96–102. [CrossRef]

[8] Feng, C.; Wang, H.-M.; Poor, H.V. Reliable and Secure Short-Packet Communications. *IEEE Trans. Wirel. Commun.* **2022**, *21*, 1913–1926. [CrossRef]

[9] Durisi, G.; Koch, T.; Popovski, P. Toward Massive, Ultrareliable, and Low-Latency Wireless Communication with Short Packets. *Proc. IEEE* **2016**, *104*, 1711–1726. [CrossRef]

[10] Yang, W.; Schaefer, R.F.; Poor, H.V. Wiretap Channels: Nonasymptotic Fundamental Limits. *IEEE Trans. Inf. Theory* **2019**, *65*, 4069–4093. [CrossRef]

[11] Tang, L.; Chen, H.; Li, Q. Social Tie Based Cooperative Jamming for Physical Layer Security. *IEEE Commun. Lett.* **2015**, *19*, 1790–1793. [CrossRef]

[12] Vo, V.N.; Tran, D.-D.; So-In, C.; Tran, H. Secrecy Performance Analysis for Fixed-Gain Energy Harvesting in an Internet of Things with Untrusted Relays. *IEEE Access* **2018**, *6*, 48247–48258. [CrossRef]

[13] Xiong, J.; Cheng, L.; Ma, D.; Wei, J. Destination-Aided Cooperative Jamming for Dual-Hop Amplify-and-Forward MIMO Untrusted Relay Systems. *IEEE Trans. Veh. Technol.* **2016**, *65*, 7274–7284. [CrossRef]

[14] Salem, A.; Musavian, L. NOMA in Cooperative Communication Systems with Energy-Harvesting Nodes and Wireless Secure Transmission. *IEEE Trans. Wirel. Commun.* **2021**, *20*, 1023–1037. [CrossRef]

[15] Zhao, S.; Liu, J.; Shen, Y.; Jiang, X.; Shiratori, N. Secure and Energy-Efficient Precoding for MIMO Two-Way Untrusted Relay Systems. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 3371–3386. [CrossRef]

[16] Kuhestani, A.; Mohammadi, A.; Yeoh, P.L. Optimal Power Allocation and Secrecy Sum Rate in Two-Way Untrusted Relaying Networks with an External Jammer. *IEEE Trans. Commun.* **2018**, *66*, 2671–2684. [CrossRef]

[17] Lv, L.; Zhou, F.; Chen, J.; Al-Dhahir, N. Secure Cooperative Communications with an Untrusted Relay: A NOMA-Inspired Jamming and Relaying Approach. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 3191–3205. [CrossRef]

[18] Qian, S. Reliable and Secure Short-Packet Communications in Untrusted Diamond Relay Networks. *IEEE Access* **2023**, *11*, 24686–24695. [CrossRef]

[19] Qian, S. Optimal power allocation for secure transmission in untrusted relay networks with Alamouti space-time block coding. *IEICE Commun. Express* **2024**, *13*, 496–499. [CrossRef]

[20] Qian, S.; Cheng, M. An Optimization Strategy for Security and Reliability in a Diamond Untrusted Relay Network with Cooperative Jamming. *Network* **2024** *4*, 405–425. [CrossRef]

[21] Gamal, A.E.; Kim, Y.-H. *Network Information Theory*; Cambridge University Press: Cambridge, UK, 2011. [CrossRef]

[22] Qian, S.; Zhou, X.; He, X.; He, J.; Juntti, M.; Matsumoto, T. Performance Analysis for Lossy-Forward Relaying Over Nakagami-m Fading Channels. *IEEE Trans. Veh. Technol.* **2017**, *66*, 10035–10043. [CrossRef]

[23] Wan, D.; Wen, M.; Ji, F.; Yu, H.; Chen, F. On the Achievable Sum-Rate of NOMA-Based Diamond Relay Networks. *IEEE Trans. Veh. Technol.* **2019**, *68*, 1472–1486. [CrossRef]

[24] Kara, F.; Kaya, H. Error Probability Analysis of NOMA-Based Diamond Relaying Network. *IEEE Trans. Veh. Technol.* **2020**, *69*, 2280–2285. [CrossRef]

[25] Xiang, Z.; Yang, W.; Cai, Y.; Ding, Z.; Song, Y.; Zou, Y. NOMA-Assisted Secure Short-Packet Communications in IoT. *IEEE Wirel. Commun.* **2020**, *27*, 8–15. [CrossRef]

[26] Polyanskiy, Y.; Poor, H.V.; Verdu, S. Channel Coding Rate in the Finite Blocklength Regime. *IEEE Trans. Inf. Theory* **2010**, *56*, 2307–2359. [CrossRef]

[27] Gradshteyn, I.S.; Ryzhik, I.M. *Table of Integrals, Series, and Products*, 8th ed.; Academic Press: New York, NY, USA, 2014. [CrossRef]

[28] Dong, L.; Han, Z.; Petropulu, A.P.; Poor, H.V. Improving Wireless Physical Layer Security via Cooperating Relays. *IEEE Trans. Signal Process.* **2010**, *58*, 1875–1888. [CrossRef]

[29] Zhou, X.; Yi, N.; He, X.; Hou, J.; Matsumoto, T.; Szott, S.; Gonzales, D.; Wolf, A.; Matthe, M.; Kuhlmorgen, S.; Adigun, O. ICT-619555 RESCUE Deliverable D1.2.1—Assessment on Feasibility, Achievability, and Limits. *Tech. Rep.* **2015**. Available online: https://cordis.europa.eu/docs/projects/cnect/5/619555/080/deliverables/001-D55final.pdf (accessed on 13 November 2024).

[30] He, X.; Zhou, X.; Komulainen, P.; Juntti, M.; Matsumoto, T. A Lower Bound Analysis of Hamming Distortion for a Binary CEO Problem with Joint Source-Channel Coding. *IEEE Trans. Commun.* **2016**, *64*, 343–353. [CrossRef]

[31] Ara, I.; Kelley, B. Physical Layer Security for 6G: Toward Achieving Intelligent Native Security at Layer-1. *IEEE Access* **2024**, *12*, 82800–82824. [CrossRef]

[32] Hoang, T.M.; Vahid, A.; Tuan, H.D.; Hanzo, L. Physical Layer Authentication and Security Design in the Machine Learning Era. *IEEE Commun. Surv. Tutor.* **2024**, *26*, 1830–1860. [CrossRef]