

Joint Accuracy and Confidentiality in Semantic-Aware Secure Remote Reconstruction

Bowen Li, and Nikolaos Pappas, *Senior Member, IEEE*

Abstract—In this paper, we consider remote reconstruction over wireless networks when simultaneous accuracy at the legitimate receiver and confidentiality against eavesdropping are required. These two objectives are often treated separately, even though they arise from the same update process and are marginals of a joint reconstruction event. This paper introduces confidential reconstruction accuracy (CRA), a metric to capture the joint event in which the legitimate receiver reconstructs correctly while the eavesdropper fails. Under randomized stationary policies, we develop a three-dimensional stationary analysis and derive closed-form expressions for the long-term average CRA and the optimal transmission probability. The results show that conventional marginal analysis can misidentify the optimal policy and misestimate the achievable simultaneous accuracy-confidentiality performance. They also reveal nontrivial behaviors: more frequent transmissions or better legitimate channels do not necessarily improve joint accurate and confidential reconstruction, and when the eavesdropping channel is strong, improving the legitimate channel alone may be insufficient. Finally, the framework induces the spatial safety boundary in a geofencing setting for secure remote reconstruction.

Index Terms—Confidential reconstruction accuracy, secure remote systems, stationary analysis, geofencing.

I. INTRODUCTION

Remote reconstruction over wireless networks is fundamental to cyber-physical systems and internet of things (IoT) applications [1], [2]. Owing to the broadcast nature of wireless propagation, transmitted updates are inherently vulnerable to eavesdropping [3]. In adversarial environments, each update jointly shapes the legitimate receiver’s reconstruction and the eavesdropper’s reconstruction [4], [5], so the value of update cannot be assessed from the legitimate side alone. Hence, the fundamental objective is not accuracy alone, nor confidentiality alone, but the joint event that the legitimate receiver reconstructs the source correctly while the eavesdropper fails.

Classical secure communication prioritizes bit-level protection against eavesdropping, with representative metrics such as secrecy capacity and equivocation characterizing achievable confidential rates and the eavesdropper’s uncertainty about the message [6], [7]. However, these metrics do not account for the task-specific importance of information. In remote reconstruction, this limitation is critical [8]; transmitting redundant or predictable updates provides negligible accuracy gains while unnecessarily increasing information leakage. Recent semantic-aware research addresses this issue by optimizing updates based on the significance of information [9], yet these

frameworks typically focus on the legitimate side, leaving confidentiality unaddressed at the semantic level.

Some existing frameworks consider both accuracy and confidentiality, for example, through threshold-based constraints, Pareto formulations, or weighted combinations of separate metrics [10]–[12]. However, they characterize the legitimate and adversarial sides separately and combine them afterward. In secure remote reconstruction, such formulations do not directly capture the event of interest, because the same transmission policy jointly governs legitimate reconstruction and adversarial exposure through a common update process. Accordingly, accuracy and confidentiality are not simply two separately optimized objectives, but different marginals of a joint reconstruction process. The relevant target is therefore the joint event that the legitimate receiver reconstructs correctly while the eavesdropper fails.

This work addresses two fundamental questions: (i) *how to characterize joint accuracy and confidentiality in secure remote reconstruction*, and (ii) *how this joint characterization affects transmission policy design*. To this end, we investigate the semantically aware confidential remote reconstruction under randomized stationary (RS) policies, making three main contributions. First, we introduce the confidential reconstruction accuracy (CRA) metric for joint accurate-and-confidential reconstruction and derive closed-form expressions for its long-term average and the optimal transmission probability via three-dimensional Markov chain stationary analysis. Second, we show that conventional marginal analysis fails to capture the intrinsic coupling between legitimate reconstruction and adversarial exposure, which can lead to suboptimal transmission policies and misestimated simultaneous accuracy-confidentiality performance; The joint characterization further reveals nontrivial structural behaviors, including that more frequent transmissions or better legitimate channels do not necessarily improve simultaneous accurate-and-confidential reconstruction, and that improving the legitimate channel alone may be insufficient when the eavesdropping channel is strong. Finally, we demonstrate the system-level implications of the proposed framework through a geofencing application, where the analytical results induce the spatial safety boundary that restricts eavesdropper proximity to ensure confidential remote reconstruction.

II. SYSTEM MODEL

We consider a remote estimation system over a wiretap channel as in Fig. 1, comprising a source, a transmitter (Alice), a legitimate receiver (Bob), and an eavesdropper (Eve).

The authors are with the Department of Computer and Information Science, Linköping University, Linköping 58183, Sweden (e-mail: bowen.li@liu.se; nikolaos.pappas@liu.se). This work has been supported by ELLIT, the European Union (6G-LEADER, 101192080).

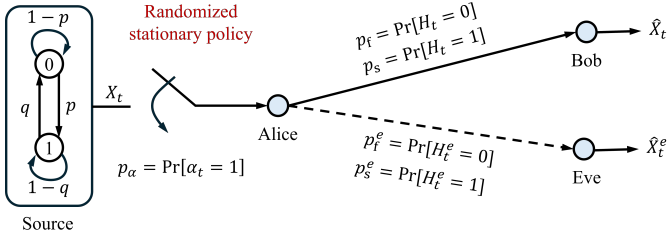


Fig. 1. Remote estimation system over a wiretap channel with a transmitter (Alice), a legitimate receiver (Bob), and an eavesdropper (Eve).

1) *Source*: The source process is modeled as a time-homogeneous binary Markov chain $\{X_t\}_{t \geq 1}$, where $X_t \in \{0, 1\}$ denotes the system state at slot $t \in \{0, 1, \dots\}$.¹ The state transition matrix is given by

$$Q = \begin{bmatrix} 1-p & p \\ q & 1-q \end{bmatrix},$$

where $p = \Pr[X_{t+1} = 1 | X_t = 0]$ and $q = \Pr[X_{t+1} = 0 | X_t = 1]$.

We assume $0 < p, q < 1$, so that the chain is irreducible and aperiodic (ergodic), and hence admits a unique stationary distribution $\mathbf{v} = [v_0, v_1]^T$ with $v_0 = \frac{q}{p+q}$, $v_1 = \frac{p}{p+q}$. The parameters p and q further characterize the temporal correlation of the source: $p+q < 1$ corresponds to a persistent (positively correlated) process, $p+q = 1$ corresponds to a memoryless (independent and identically distributed (*i.i.d.*)) process, and $p+q > 1$ corresponds to an alternating (negatively correlated) process [13].

2) *Transmission policy (Alice)*: At each slot t , Alice makes a transmission decision $\alpha_t \in \{0, 1\}$, where $\alpha_t = 1$ denotes sampling and transmitting a perfect observation of the source state X_t , and $\alpha_t = 0$ denotes idleness. We focus on RS policies, under which $\{\alpha_t\}$ is an *i.i.d.* Bernoulli process independent of the source evolution, with

$$\Pr[\alpha_t = 1] = p_\alpha, \quad \Pr[\alpha_t = 0] = 1 - p_\alpha,$$

for all $t \geq 1$, where $p_\alpha \in (0, 1]$ is the transmission probability.

3) *Wiretap Channel*: We consider a wiretap channel from Alice to Bob and Eve, where each transmission may be successfully received or erased. The main channel to Bob and the eavesdropping channel to Eve are modeled by two independent *i.i.d.* Bernoulli processes, denoted by $\{H_t\}_{t \geq 1}$ and $\{H_t^e\}_{t \geq 1}$, respectively, with

$$\Pr[H_t = 1] = p_s, \quad \Pr[H_t^e = 1] = p_s^e,$$

for all $t \geq 1$, where $p_s, p_s^e \in (0, 1)$. $H_t = 1$ means that the update transmitted at slot t is successfully received by Bob, and $H_t^e = 1$ means that the same update is successfully intercepted by Eve. The corresponding erasure probabilities are $1 - p_s$ and $1 - p_s^e$, respectively.

¹The analytical framework in this paper, including the system-dynamics characterization and stationary-distribution analysis, is applicable to general time-homogeneous finite-state Markov sources. We focus on the binary case only to keep the presentation concise.

4) *Receiver Observation and Estimation (Bob and Eve)*: The observations at Bob and Eve are jointly determined by Alice's transmission decision and the corresponding channel realizations. Specifically, Bob receives

$$Y_t = \begin{cases} X_t, & \text{if } \alpha_t = 1 \text{ and } H_t = 1, \\ \varepsilon, & \text{otherwise,} \end{cases} \quad (1)$$

where ε denotes an erasure symbol. Similarly, Eve observes

$$Y_t^e = \begin{cases} X_t, & \text{if } \alpha_t = 1 \text{ and } H_t^e = 1, \\ \varepsilon, & \text{otherwise.} \end{cases} \quad (2)$$

We assume that the receivers have no information about the source dynamics. Accordingly, both receivers employ a model-free estimator that uses the most recently received update. Let Θ_t and Θ_t^e denote the age of information (AoI) at Bob and Eve, respectively, *i.e.*

$$\Theta_t = t - \max\{\tau \leq t : Y_\tau \neq \varepsilon\}, \quad (3)$$

and Θ_t^e is defined analogously using Y_τ^e . The corresponding estimates are

$$\hat{X}_t = X_{t-\Theta_t}, \quad \hat{X}_t^e = X_{t-\Theta_t^e}. \quad (4)$$

5) *Confidential Reconstruction Accuracy*: In secure remote reconstruction, the relevant target is the joint event that the legitimate receiver is correct while the eavesdropper is not, rather than a post hoc combination of separate accuracy and confidentiality marginals, *e.g.*, [14]. To characterize this event directly, we introduce CRA.

Definition 1: The instantaneous CRA at time t is defined as

$$A_{\text{CRA}}[t] := \mathbb{I}\{\hat{X}_t = X_t, \hat{X}_t^e \neq X_t\}, \quad (5)$$

where $\mathbb{I}\{\cdot\}$ denotes the indicator function. $A_{\text{CRA}}[t] = 1$ if and only if the legitimate receiver correctly reconstructs the source state while the eavesdropper fails.

The long-term average CRA is defined as

$$\bar{A}_{\text{CRA}} := \liminf_{T \rightarrow \infty} \frac{1}{T} \sum_{t=1}^T \mathbb{E}[A_{\text{CRA}}[t]]. \quad (6)$$

III. ANALYTICAL RESULTS

This section characterizes the joint source–reconstruction dynamics. By deriving the stationary distribution of the joint state, we obtain a closed-form expression for the long-term average CRA. This expression further enables the derivation of the optimal RS policy.

A. System Dynamics

The joint evolution of the source and estimators is captured by the composite state $\mathbf{S}_t := (X_t, \hat{X}_t, \hat{X}_t^e) \in \{0, 1\}^3$. Given that the source $\{X_t\}$ is Markovian and the transmission decisions $\{\alpha_t\}$ and channel processes $\{H_t, H_t^e\}$ are mutually independent *i.i.d.* sequences, $\{\mathbf{S}_t\}_{t \geq 1}$ constitutes a finite-state time-homogeneous ergodic Markov chain, as proved below.

Since $\{X_t\}$ is Markovian, while the transmission decisions $\{\alpha_t\}$ and the channel processes $\{H_t\}$ and $\{H_t^e\}$ are *i.i.d.*, mutually independent. The updates of \hat{X}_t and \hat{X}_t^e depend only

on the current state $(X_t, \hat{X}_t, \hat{X}_t^e)$ and the current realization of (α_t, H_t, H_t^e) . Hence,

$$\Pr(\mathbf{S}_{t+1} | \mathbf{S}_1, \dots, \mathbf{S}_t) = \Pr(\mathbf{S}_{t+1} | \mathbf{S}_t).$$

For $\mathbf{s} = (x, a, b)$ and $\mathbf{s}' = (x', a', b')$, define the one-step transition probability as

$$\begin{aligned} \Pr(\mathbf{s}, \mathbf{s}') &:= \Pr(\mathbf{S}_{t+1} = \mathbf{s}' | \mathbf{S}_t = \mathbf{s}) \\ &= \Pr(X_{t+1} = x', \hat{X}_{t+1} = a', \hat{X}_{t+1}^e = b' | \\ &\quad X_t = x, \hat{X}_t = a, \hat{X}_t^e = b). \end{aligned}$$

By the chain rule, $\Pr(\mathbf{s}, \mathbf{s}')$ becomes

$$\begin{aligned} \Pr(X_{t+1} = x' | X_t = x, \hat{X}_t = a, \hat{X}_t^e = b) \cdot \Pr(\hat{X}_{t+1} = a', \\ \hat{X}_{t+1}^e = b' | X_t = x, \hat{X}_t = a, \hat{X}_t^e = b, X_{t+1} = x'), \end{aligned} \quad (7)$$

Since the source is independent of transmission decisions and channel processes, the first term in (7) becomes $\Pr(X_{t+1} = x' | X_t = x)$.

The second term is determined by the joint reception outcome. Define

$$\begin{aligned} \lambda_{11} &:= p_\alpha p_s p_s^e, && \text{(Both reconstruct)} \\ \lambda_{10} &:= p_\alpha p_s (1 - p_s^e), && \text{(Only Bob reconstructs)} \\ \lambda_{01} &:= p_\alpha (1 - p_s) p_s^e, && \text{(Only Eve reconstructs)} \\ \lambda_{00} &:= p_\alpha (1 - p_s) (1 - p_s^e) + \bar{p}_\alpha. && \text{(Neither reconstructs)} \end{aligned}$$

Then the second term of (7), denoted as \mathcal{P}_s , becomes

$$\begin{aligned} \mathcal{P}_s &= \lambda_{11} \mathbb{I}(a' = x', b' = x') + \lambda_{10} \mathbb{I}(a' = x', b' = b) \\ &\quad + \lambda_{01} \mathbb{I}(a' = a, b' = x') + \lambda_{00} \mathbb{I}(a' = a, b' = b). \end{aligned}$$

Combining the above, the transition kernel is given by

$$\Pr(\mathbf{s}, \mathbf{s}') = \Pr(X_{t+1} = x' | X_t = x) \cdot \mathcal{P}_s. \quad (8)$$

Since the source process is time-homogeneous and \mathcal{P}_s is independent of t , the Markov chain $\{\mathbf{S}_t\}$ is time-homogeneous.

Since $p_\alpha \in (0, 1]$, $p_s \in (0, 1)$, and $p_s^e \in (0, 1)$, all λ -parameters are strictly positive. Together with the irreducibility of Q , this ensures that all states of $\{\mathbf{S}_t\}$ communicate, so the chain is irreducible. Furthermore, because $\lambda_{00} > 0$ and $Q(x, x) > 0$ for some source state x , the chain has a self-loop and is aperiodic. Therefore, the finite-state chain $\{\mathbf{S}_t\}$ is ergodic. As a result, it admits a unique stationary distribution, and the long-term average exists.

B. Stationary Distribution

This subsection derives the joint stationary distribution of \mathbf{S}_t . Specifically, for any $(x, a, b) \in \{0, 1\}^3$, define

$$\pi(x, a, b) := \lim_{t \rightarrow \infty} \Pr(X_t = x, \hat{X}_t = a, \hat{X}_t^e = b).$$

The following theorem gives its closed-form expression.

Theorem 1: The joint stationary distribution $\pi(x, a, b)$ is

$$\pi(x, a, b) = T_1(x, a, b) + T_2(x, a, b) + T_3(x, a, b), \quad (9)$$

where

$$T_1(x, a, b) = \delta(a, b) v_a \lambda_{11} [(I - \lambda_{00} Q)^{-1}]_{a,x}, \quad (10)$$

$$\begin{aligned} T_2(x, a, b) &= v_b \lambda_{10} P_B \left[Q (I - (1 - P_B) Q)^{-1} \right]_{b,a} \\ &\quad \times [(I - \lambda_{00} Q)^{-1}]_{a,x}, \end{aligned} \quad (11)$$

$$\begin{aligned} T_3(x, a, b) &= v_a \lambda_{01} P_A \left[Q (I - (1 - P_A) Q)^{-1} \right]_{a,b} \\ &\quad \times [(I - \lambda_{00} Q)^{-1}]_{b,x}. \end{aligned} \quad (12)$$

Here, $[M]_{i,j}$ denotes the entry of matrix M with row index i and column index j , $\delta(a, b)$ is the Kronecker delta, and $P_A := \lambda_{11} + \lambda_{10}$ and $P_B := \lambda_{11} + \lambda_{01}$ denote the marginal success probabilities at Bob and Eve, respectively.

Proof: See Appendix A. ■

It follows from Theorem 1 that $\pi(x, a, b)$ is rational in the policy parameter p_α , which makes the joint-event metric analytically tractable under randomized stationary policies. Indeed, $\lambda_{00}, \lambda_{10}, \lambda_{01}, \lambda_{11}$, and hence P_A and P_B , are affine in p_α . Moreover, for $c \in \{\lambda_{00}, 1 - P_A, 1 - P_B\}$, the resolvent matrix $(I - cQ)^{-1}$ is rational in c , so these resolvent matrices are rational in p_α since each c is affine in p_α . As a result, $T_1(x, a, b)$, $T_2(x, a, b)$, $T_3(x, a, b)$, and hence $\pi(x, a, b)$ are rational in p_α . This rational structure will be exploited to derive closed-form expressions for the long-term average CRA and the corresponding optimal randomized stationary policy.

C. Average CRA

By the definition of $A_{\text{CRA}}[t]$ in (5), the event of successful confidential reconstruction occurs if and only if $(X_t, \hat{X}_t, \hat{X}_t^e) = (0, 0, 1)$ or $(1, 1, 0)$. Since the process $\{\mathbf{S}_t\}$ is ergodic as analyzed in Section III-A, we have

$$\bar{A}_{\text{CRA}} = \pi(0, 0, 1) + \pi(1, 1, 0).$$

By Theorem 1, each stationary probability $\pi(x, a, b)$ is rational in p_α . Therefore, $\bar{A}_{\text{CRA}}(p_\alpha)$ is also rational in p_α , which yields the following corollary.

Corollary 1: The long-term average CRA is given by

$$\bar{A}_{\text{CRA}}(p_\alpha) = \frac{A p_\alpha + B}{C p_\alpha^2 + D p_\alpha + E},$$

where

$$\begin{aligned} A &= pq [p_s^2 (1 - p_s^e) (p + q - 2) + (p_s^e)^2 (1 - p_s) (p + q)], \\ B &= pq (p + q) (2p_s p_s^e - p_s - p_s^e), \\ C &= (p_s p_s^e - p_s - p_s^e) p_s p_s^e (p + q - 1)^2 (p + q), \\ D &= (p_s p_s^e - p_s - p_s^e) (p_s + p_s^e) (1 - p - q) (p + q)^2, \\ E &= (p_s p_s^e - p_s - p_s^e) (p + q)^3. \end{aligned}$$

Remark 1: Corollary 1 is stated for the general case $p_s \neq p_s^e$. The symmetric case $p_s = p_s^e$ is degenerate, since the numerator and denominator share a common factor. In that case, the expression should be simplified before substitution to avoid an artificial zero denominator.

D. Optimal RS Policy

We consider the problem of maximizing the long-term average CRA over the transmission probability p_α

$$\mathcal{P}1: \max_{0 < p_\alpha \leq 1} \bar{A}_{\text{CRA}}. \quad (13)$$

Corollary 1 shows that $\bar{A}_{\text{CRA}}(p_\alpha)$ admits a closed-form rational form, which makes $\mathcal{P}1$ analytically tractable. The resulting optimal transmission probability is given next.

Theorem 2: The optimal solution to Problem $\mathcal{P}1$ is

$$p_\alpha^* = \left[\frac{-BC + \sqrt{\Delta}}{AC} \right]_0^1,$$

where $[x]_0^1 := \min\{1, \max\{x, 0\}\}$ denotes the Euclidean projection of x onto the feasible interval $[0, 1]$ and $\Delta := B^2C^2 + AC(AE - BD)$, where Δ is proven to be nonnegative.

Proof: See Appendix B. \blacksquare

Remark 2: The result of Theorem 2 extends directly to any interval constraint $p_\alpha \in [p_\ell, p_u]$ with $0 < p_\ell \leq p_u \leq 1$. In that case, the optimal solution is obtained by projecting the same closed-form candidate onto $[p_\ell, p_u]$, namely

$$p_\alpha^* = \left[\frac{-BC + \sqrt{\Delta}}{AC} \right]_{p_\ell}^{p_u},$$

with $[x]_{p_\ell}^{p_u} := \min\{p_u, \max\{x, p_\ell\}\}$.

Remark 3: The expression in Theorem 2 corresponds to the general case. In the special case $p_s = p_s^e$, $\bar{A}_{\text{CRA}}(p_\alpha)$ is monotonic over $p_\alpha \in [0, 1]$: it is increasing when $p + q > 1$ and decreasing when $p + q < 1$, and constant when $p + q = 1$. Accordingly, $p_\alpha^* = 1$ if $p + q > 1$, $p_\alpha^* = 0$ if $p + q < 1$, and p_α^* can be any value in $(0, 1]$ if $p + q = 1$.

Thus, in the symmetric-channel case, *the optimal transmission policy is determined entirely by the source temporal correlation*: persistent sources favor silence, alternating sources favor full transmission, and the *i.i.d.* case is indifferent to the transmission probability.

IV. NUMERICAL AND SIMULATION RESULTS

In this section, we first validate the analytical results using Monte Carlo simulations with horizon $T = 50,000$, averaged over 400 independent realizations. We then show how the proposed joint-event metric differs from conventional separate-marginal formulations, and reveal structural behaviors that are invisible under marginal analysis. Finally, we demonstrate a system-level implication of the framework through a geofencing example, where the CRA metric is used to construct the corresponding secure region and boundary.

For comparison, we consider a marginal-analysis baseline, which approximates the joint confidentiality-accuracy objective by separately evaluating the marginal accuracy and confidentiality probabilities and then combining them through a weighted sum. Specifically, define

$$\bar{A}_\omega = (1 - \omega)(\pi_{\{X_t, \hat{X}_t\}}(0, 0) + \pi_{\{X_t, \hat{X}_t\}}(1, 1)) \\ + \omega(\pi_{\{X_t, \hat{X}_t\}}(0, 1) + \pi_{\{X_t, \hat{X}_t\}}(1, 0)),$$

where $\omega \in [0, 1]$. Here, $\pi_{\{X_t, \hat{X}_t\}}(0, 0) + \pi_{\{X_t, \hat{X}_t\}}(1, 1)$ is the marginal reconstruction accuracy at Bob, while $\pi_{\{X_t, \hat{X}_t\}}(0, 1) + \pi_{\{X_t, \hat{X}_t\}}(1, 0)$ is the marginal confidentiality term at Eve. By Theorem 1 or equivalently from [14], these terms are given by

$$\pi_{\{X_t, \hat{X}_t\}}(0, 0) = \frac{q(q + p_\alpha p_s(1 - q))}{(p + q)(p + q + p_\alpha p_s(1 - p - q))},$$

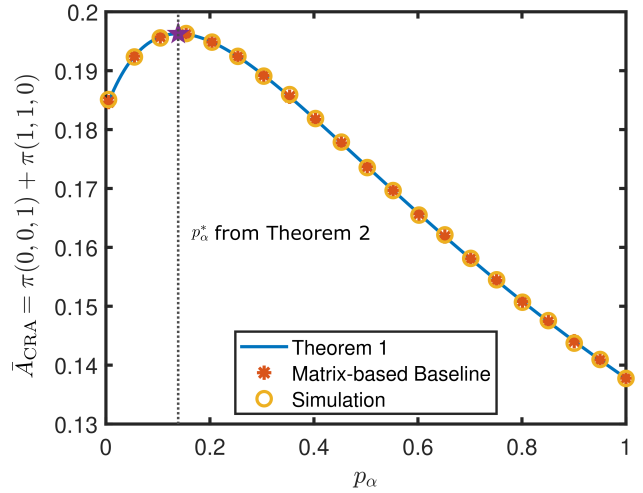


Fig. 2. Average simultaneous confidentiality and accuracy \bar{A}_{CRA} versus sampling and transmission probability p_α .

$$\pi_{\{X_t, \hat{X}_t\}}(1, 1) = \frac{p(p + p_\alpha p_s(1 - p))}{(p + q)(p + q + p_\alpha p_s(1 - p - q))}, \\ \pi_{\{X_t, \hat{X}_t\}}(0, 1) = \frac{pq(1 - p_\alpha p_s^e)}{(p + q)(p + q + p_\alpha p_s^e(1 - p - q))}, \\ \pi_{\{X_t, \hat{X}_t\}}(1, 0) = \frac{pq(1 - p_\alpha p_s^e)}{(p + q)(p + q + p_\alpha p_s^e(1 - p - q))}.$$

In particular, \bar{A}_0 reduces to the pure accuracy metric, while \bar{A}_1 reduces to the pure confidentiality metric.

1) *Analytical Validation:* Fig. 2 shows the average simultaneous confidentiality and accuracy \bar{A}_{CRA} versus the sampling probability p_α . The closed-form expression from Theorem 1, the numerical stationary solution obtained from the normalized eigenvector associated with the unit eigenvalue of the transition matrix, and the Monte Carlo results are in near-perfect agreement, thereby validating the joint system-dynamics analysis and stationary characterization. In addition, the optimizer and optimal value predicted by Theorem 2 coincide with the peak of the curve, confirming the policy characterization.

2) *CRA-Induced Insights:* Fig. 3 shows that the optimal transmission probability for maximizing \bar{A}_{CRA} is environment-dependent, unlike the marginal metrics \bar{A}_0 and \bar{A}_1 , whose optima are always attained at $p_\alpha = 1$ and $p_\alpha = 0$, respectively. In Fig. 3a, although the legitimate channel is better than the eavesdropping channel, transmitting more frequently is not always beneficial: a larger p_α improves accuracy but degrades confidentiality, and excessive transmissions eventually reduce the probability of being simultaneously confidential and accurate. In Fig. 3d, by contrast, even when the eavesdropping channel is better than the legitimate channel, increasing p_α to a proper level can still improve \bar{A}_{CRA} , because the accuracy gain outweighs the confidentiality loss.

Fig. 3 also shows that adversarially robust estimation cannot be reduced to a weighted combination of two separate marginal metrics. In Fig. 3a, the balance metric $\bar{A}_{0.5}$ both misidentifies the optimal transmission probability and overestimates the achievable performance: it suggests an apparent

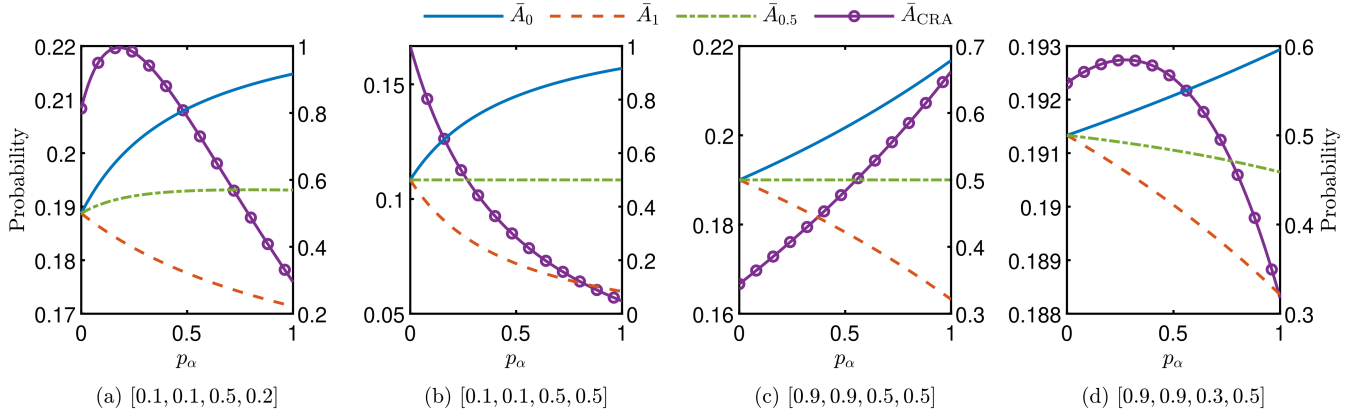


Fig. 3. Probabilities of simultaneous confidentiality and accuracy \bar{A}_{CRA} , confidentiality only \bar{A}_1 , accuracy only \bar{A}_0 , and the balance metric $\bar{A}_{0.5}$ versus the transmission probability under different settings. The metric \bar{A}_{CRA} is plotted against the left y-axis, whereas all the other metrics share the right y-axis. The title of each subfigure indicates the corresponding parameter setting $[p, q, p_s, p_s^e]$.

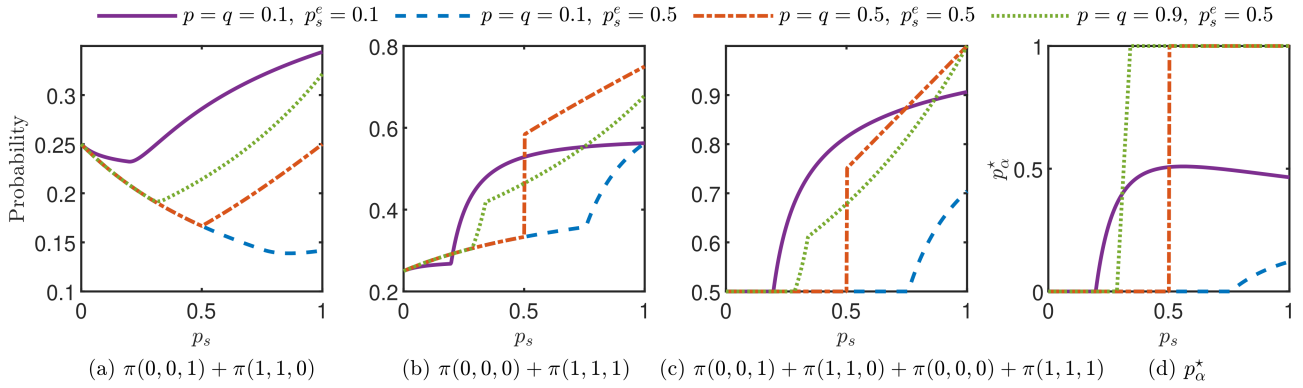


Fig. 4. (a) Probability of simultaneous confidentiality and accuracy $\bar{A}_{CRA} = \pi(0, 0, 1) + \pi(1, 1, 0)$, (b) probability of simultaneous non-confidentiality and accuracy $\pi(0, 0, 0) + \pi(1, 1, 1)$, (c) probability of accuracy $\bar{A}_1 = \pi(0, 0, 1) + \pi(1, 1, 0) + \pi(0, 0, 0) + \pi(1, 1, 1)$ under the optimal transmission policy p_α^* , and (d) the corresponding optimal transmission probability p_α^* .

optimum of about 0.57 with $p_\alpha = 0.8$, whereas the actual probability of being simultaneously confidential and accurate under the corresponding policy is only about 0.189, below the true optimum of approximately 0.22 with less transmission probability $p_\alpha = 0.18$. Figs. 3b and 3c further illustrate an extreme case with $p_s = p_s^e$, where $\bar{A}_{0.5}$ is insensitive to p_α , yet the optimal p_α for \bar{A}_{CRA} still varies significantly with the source dynamics, similar the extreme analysis in Remark 3: when the source evolves slowly, a small p_α is preferred since the state can often be inferred from temporal correlation, whereas when the source evolves rapidly, a large p_α becomes preferable because guessing is no longer reliable.

Fig. 4 reveals three key observations. First, improving the legitimate channel quality p_s does not necessarily increase the simultaneous confidential-and-accurate probability $\pi(0, 0, 1) + \pi(1, 1, 0)$ monotonically. As shown in Figs. 4a–4c, although the overall probability of accurate estimation always increases with p_s , the increment may initially be dominated by the non-confidential component $\pi(0, 0, 0) + \pi(1, 1, 1)$, which causes the confidential-and-accurate probability to decrease before increasing. Second, when the eavesdropping channel is strong, improving p_s alone may be insufficient to deliver meaningful confidentiality gain. In this case, increasing the

source dynamics ($p = q = 0.1$ to $p = q = 0.9$) or weakening the eavesdropping channel ($p_s^e = 0.5$ to $p_s^e = 0.1$) is substantially more effective. Third, the optimal transmission probability p_α^* is highly environment-dependent and can even be non-monotonic in p_s , as shown in Fig. 4d. When the source evolves slowly, and the eavesdropping channel is strong, conservative transmission is preferred; when the source evolves faster, aggressive transmission becomes optimal; and when the legitimate channel is already sufficiently reliable, further increasing the transmission frequency may be undesirable due to the additional leakage it incurs.

3) *CRA-Induced Geofencing*: To further evaluate the proposed framework in a representative practical scenario, we consider the urban layout shown in Fig. 5a, where the transmitter (Alice) is located at the center and the legitimate receiver (Bob) is placed at a fixed location, while the eavesdropper (Eve) is assumed to be able to appear anywhere in the area. The large-scale propagation is modeled by the 3GPP Urban Micro (UMi) path-loss model in [15], where the line of sight (LOS) and non-line of sight (NLOS) links are given by

$$PL_j = \begin{cases} 22.0 + 28.0 \log_{10}(d_j) + 20 \log_{10}(f_c), & \text{LOS,} \\ 22.7 + 36.7 \log_{10}(d_j) + 26 \log_{10}(f_c), & \text{NLOS,} \end{cases}$$

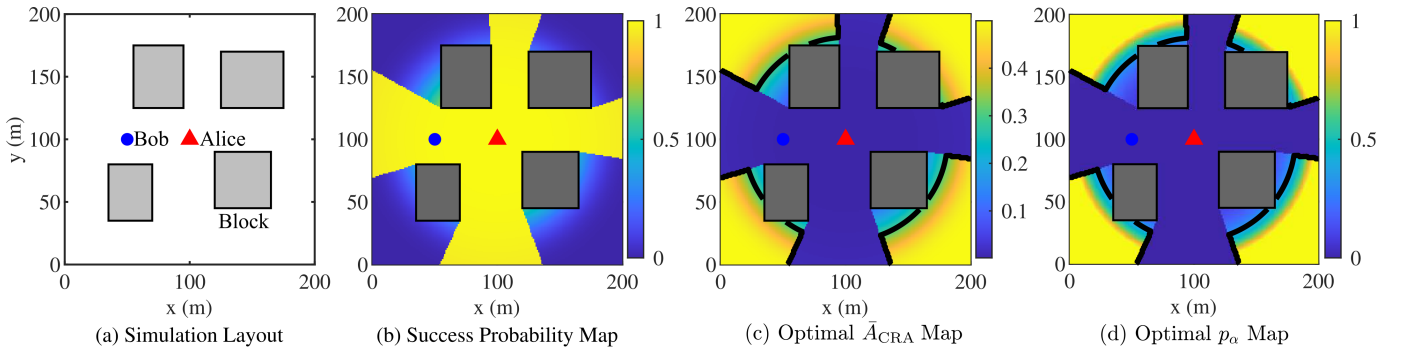


Fig. 5. Simulation layout and spatial maps under arbitrary eavesdropper locations. (a) shows the simulation layout; (b) shows Eve’s channel success-probability map; (c) shows the corresponding optimal \bar{A}_{CRA} map; and (d) shows the corresponding optimal transmission-probability p_α map. The black contour in (c) and (d) represents the geofencing boundary induced by the threshold $\bar{A}_{CRA} = 0.3$.

and the small-scale fading is modeled as Rayleigh fading. Based on this channel model, the channel success probability is defined as the probability that the instantaneous channel quality exceeds a prescribed threshold, *i.e.*, $\Pr(\gamma > \gamma_{th})$, which yields the spatial success-probability map shown in Fig. 5b. Then, by applying Theorem 2 pointwise over space, we obtain the corresponding optimal transmission probability p_α^* and the optimal simultaneous confidentiality-and-accuracy metric \bar{A}_{CRA}^* , as shown in Figs. 5c and 5d, respectively.

Based on the resulting \bar{A}_{CRA}^* map, we further define a geofencing region by imposing the constraint $\bar{A}_{CRA}^* < \tau$, where τ is a prescribed confidentiality and accuracy threshold. The resulting geofencing boundary is shown by the black contour in Figs. 5c and 5d. This contour identifies the set of Eve locations that would make the system insufficiently confidential, in the sense that once Eve enters this region, the achievable simultaneous confidentiality-and-accuracy performance falls below the required threshold. It is also observed that the geofencing region becomes relatively large in the left and right directions, where the lack of blockage leads to more favorable propagation for Eve. This observation motivates further study on how to shrink the geofencing region, for example by introducing additional blockages or by designing proactive interference or jamming strategies.

V. CONCLUSION

This paper studied the characterization and optimization of joint accuracy and confidentiality in semantic-aware secure remote reconstruction. By introducing confidential reconstruction accuracy (CRA) and developing a three-dimensional Markov-chain analysis, we derived closed-form expressions for the long-term average CRA and the optimal transmission probability. fails to capture the intrinsic coupling between legitimate reconstruction and adversarial exposure, and can therefore misidentify the optimal policy and misestimate the achievable simultaneous accuracy-confidentiality performance. We further revealed nontrivial structural behaviors: more frequent transmissions or better legitimate channels do not necessarily improve joint accurate and confidential reconstruction, and under strong eavesdropping channels, improving the legitimate channel alone may be insufficient, necessitating adjustments to source dynamics or adversary suppression.

Finally, we demonstrated the system-level implications of the proposed framework through a geofencing application that establishes spatial safety boundaries for secure remote reconstruction.

REFERENCES

- [1] M. Kountouris and N. Pappas, “Semantics-empowered communication for networked intelligent systems,” *IEEE Commun. Mag.*, vol. 59, no. 6, pp. 96–102, 2021.
- [2] S. Gil, M. Yemini, A. Chorti, A. Nedić, H. V. Poor, and A. J. Goldsmith, “How physicality enables cy-trust: A new era of trust-centered cyber-physical systems,” *Proc. IEEE*, vol. 113, no. 10, pp. 1121–1154, 2025.
- [3] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, “Cyber security and privacy issues in smart grids,” *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 981–997, 2012.
- [4] P. K. Gopala, L. Lai, and H. El Gamal, “On the secrecy capacity of fading channels,” *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.
- [5] A. Tsiamis, K. Gatsis, and G. J. Pappas, “State-secrecy codes for networked linear systems,” *IEEE Trans. Autom. Control*, vol. 65, no. 5, pp. 2001–2015, 2020.
- [6] F. Oggier and B. Hassibi, “The secrecy capacity of the MIMO wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, 2011.
- [7] S. Leung-Yan-Cheong and M. Hellman, “The gaussian wire-tap channel,” *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, 1978.
- [8] Y. Sun, E. Uysal-Biyikoglu, R. D. Yates, C. E. Koksal, and N. B. Shroff, “Update or wait: How to keep your data fresh,” *IEEE Trans. Inf. Theory*, vol. 63, no. 11, pp. 7492–7508, 2017.
- [9] J. Luo, E. Delfani, M. Salimnejad, and N. Pappas, “From information freshness to semantics of information and goal-oriented communications,” *arXiv preprint arXiv:2512.12758*, 2025.
- [10] Q. Zhang, Z. Xu, X. Lan, J. Chen, J. He, W. Ma, and Q. Chen, “Optimal age of information and throughput scheduling in heterogeneous traffic wireless physical-layer security communications,” *IEEE Internet Things J.*, vol. 11, no. 13, pp. 23 644–23 660, 2024.
- [11] J. Li, J. Li, L. Lv, Z. Ju, and F. Gong, “Multiobjective optimization of AoI and rate for secure dual-functional RIS-assisted networks: A cross-layer design,” *IEEE Internet Things J.*, vol. 12, no. 8, pp. 10 349–10 363, 2025.
- [12] J. Wang, S. Guo, J. Wang, and L. Bai, “Age-of-information-oriented security transmission scheme for UAV-aided iot networks,” *IEEE Internet Things J.*, vol. 12, no. 8, pp. 9570–9582, 2025.
- [13] E. Seabrook and L. Wiskott, “A tutorial on the spectral theory of markov chains,” *Neural Comput.*, vol. 35, no. 11, pp. 1713–1796, 10 2023.
- [14] M. Salimnejad, M. Kountouris, and N. Pappas, “Real-time reconstruction of markov sources and remote actuation over wireless channels,” *IEEE Trans. Commun.*, vol. 72, no. 5, pp. 2701–2715, 2024.
- [15] “Evolved universal terrestrial radio access (E-UTRA); further advancements for E-UTRA physical layer aspects,” 3GPP, Tech. Rep. TR 36.814 (Release 9), Mar. 2017.

APPENDIX A
PROOF OF THEOREM 1

We start by conditioning on the joint age process (Θ_t, Θ_t^e) . By the law of total probability, we have

$$\begin{aligned} \pi(x, a, b) &= \lim_{t \rightarrow \infty} \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} \Pr(X_t = x, \hat{X}_t = a, \hat{X}_t^e = b \mid \Theta_t = i, \Theta_t^e = j) \\ &\quad \times \Pr(\Theta_t = i, \Theta_t^e = j). \end{aligned} \quad (14)$$

Under the receiver estimator model induced by the age variables, as defined in (4), the first term in (14) becomes

$$\begin{aligned} \Pr(X_t = x, \hat{X}_t = a, \hat{X}_t^e = b \mid \Theta_t = i, \Theta_t^e = j) &= \Pr(X_t = x, X_{t-i} = a, X_{t-j} = b \mid \Theta_t = i, \Theta_t^e = j) \\ &= \Pr(X_t = x, X_{t-i} = a, X_{t-j} = b), \end{aligned}$$

where the last equality holds because the age process is fully determined by (α_t, H_t) , as defined in (3), and is independent of the source process $\{X_t\}$ under the RS policy.

Since $\{X_t\}$ is a finite-state ergodic Markov chain, and the joint age process $\{(\Theta_t, \Theta_t^e)\}$ is a positive-recurrent Markov chain whose states communicate and state $(0, 0)$ has finite expected return time due to $\lambda_{11} > 0$, the following limits exist.

$$\begin{aligned} \phi(x, a, b, i, j) &:= \lim_{t \rightarrow \infty} \Pr(X_t = x, X_{t-i} = a, X_{t-j} = b), \\ \rho(i, j) &:= \lim_{t \rightarrow \infty} \Pr(\Theta_t = i, \Theta_t^e = j), \end{aligned}$$

Thus, the joint stationary probability becomes

$$\pi(x, a, b) = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} \phi(x, a, b, i, j) \rho(i, j). \quad (15)$$

Next, we first derive the limiting distributions $\phi(x, a, b, i, j)$ and $\rho(i, j)$ separately, and then combine them to obtain the joint stationary distribution $\pi(x, a, b)$.

A. Stationary Distribution of Joint Age Process

The stationary distribution of joint age process $\rho(i, j)$ is characterized by three cases.

Case 1: $i = j$ (Synchronized updates). This case corresponds to the event that the most recent successful update is received simultaneously by both Bob and Eve. The age pair is reset to $(0, 0)$ with probability λ_{11} , and then increases synchronously only if neither receiver successfully receives a new update in the subsequent slots. Since a joint failure occurs with probability, λ_{00} in each slot, we obtain

$$\rho(i, i) = \lambda_{11} (\lambda_{00})^i, \quad i \geq 0. \quad (16)$$

Case 2: $i < j$ (Bob is fresher). Let $\Delta = j - i > 0$. Then, at time $t - i$, the system must be in a boundary state $(0, \Delta)$, meaning that Bob has just received a successful update while Eve's age exceeds Bob's by Δ . From that time to time t , the age pair can evolve from $(0, \Delta)$ to (i, j) only if i consecutive joint failures occur. Therefore,

$$\rho(i, j) = \rho(0, \Delta) (\lambda_{00})^i. \quad (17)$$

It remains to determine the boundary term $\rho(0, \Delta)$. The event $(\Theta_{t-i}, \Theta_{t-i}^e) = (0, \Delta)$ occurs when Bob successfully receives an update while Eve does not, and Eve's age in the previous slot equals $\Delta - 1$. The former occurs with probability λ_{10} . Moreover, Eve successfully receives an update in each slot with marginal probability $P_B := \lambda_{11} + \lambda_{01}$, so its marginal age distribution is geometric

$$\Pr(\Theta^e = k) = P_B (1 - P_B)^k, \quad k \geq 0$$

Hence,

$$\rho(0, \Delta) = \lambda_{10} P_B (1 - P_B)^{\Delta-1}.$$

Substituting $\rho(0, \Delta)$ into (17), we have

$$\rho(i, j) = \lambda_{10} P_B (1 - P_B)^{j-i-1} (\lambda_{00})^i. \quad (18)$$

Case 3: $i > j$ (Eve is fresher). This case is symmetric to Case 2, with Bob and Eve interchanged. Hence,

$$\rho(i, j) = \lambda_{01} P_A (1 - P_A)^{i-j-1} (\lambda_{00})^j, \quad (19)$$

where $P_A := \lambda_{11} + \lambda_{10}$ denotes the marginal success probability at Bob.

B. Stationary Three-Time Joint Distribution:

The stationary three-time joint distribution $\phi(x, a, b, i, j)$ is also characterized by three cases.

Case 1: $i = j$ (Synchronized updates). In this case, the time instants $t - i$ and $t - j$ coincide. Hence, the event has nonzero probability only if $a = b$. Under stationarity, the source is in state a with probability v_a , and then evolves from a to x over i steps according to Q^i . Therefore,

$$\phi(x, a, b, i, i) = \delta(a, b) v_a [Q^i]_{a,x}. \quad (20)$$

Case 2: $i < j$ (Bob is fresher). Here, $t - j < t - i < t$. The process follows the path $\xrightarrow{\infty} b \xrightarrow{j-i} a \xrightarrow{i} x$. By the Markov property and stationarity, we have

$$\phi(x, a, b, i, j) = v_b [Q^{j-i}]_{b,a} [Q^i]_{a,x}. \quad (21)$$

Case 3: $i > j$ (Eve is fresher). Here, $t - i < t - j < t$. The process follows the path $\xrightarrow{\infty} a \xrightarrow{i-j} b \xrightarrow{j} x$. Similarly, we have

$$\phi(x, a, b, i, j) = v_a [Q^{i-j}]_{a,b} [Q^j]_{b,x}. \quad (22)$$

C. Stationary Distribution of Confidentiality Reconstruction Process

Having characterized the stationary age distribution $\rho(i, j)$ and the stationary three-time joint distribution, we now derive the stationary distribution $\pi(x, a, b)$. As above, the derivation is carried out by distinguishing three cases.

Case 1: $i = j$ (Synchronized updates). In this case, the two receivers share the same freshest update, and therefore $a = b$. Substituting (16) and (20) into (15), we have

$$\begin{aligned} T_1(x, a, b) &:= \sum_{i=0}^{\infty} \delta(a, b) v_a [Q^i]_{a,x} \lambda_{11} (\lambda_{00})^i \\ &= \delta(a, b) \lambda_{11} v_a \left[\sum_{i=0}^{\infty} (\lambda_{00} Q)^i \right]_{a,x} \end{aligned}$$

$$= \delta(a, b) \lambda_{11} v_a [(I - \lambda_{00} Q)^{-1}]_{a,x}. \quad (23)$$

Case 2: $i < j$ (Bob is fresher). Let $\Delta = j - i \geq 1$. Substituting (18) and (21) into (15), we have

$$\begin{aligned} T_2(x, a, b) &:= \sum_{i=0}^{\infty} \sum_{\Delta=1}^{\infty} v_b [Q^\Delta]_{b,a} [Q^i]_{a,x} \lambda_{10} P_B (1 - P_B)^{\Delta-1} (\lambda_{00})^i \\ &= v_b \lambda_{10} P_B \left[\sum_{\Delta=1}^{\infty} (1 - P_B)^{\Delta-1} Q^\Delta \right]_{b,a} \left[\sum_{i=0}^{\infty} (\lambda_{00} Q)^i \right]_{a,x} \\ &= v_b \lambda_{10} P_B [Q(I - (1 - P_B)Q)^{-1}]_{b,a} [(I - \lambda_{00}Q)^{-1}]_{a,x}. \end{aligned} \quad (24)$$

Case 3: $i > j$ (Eve is fresher). By symmetry, let $\Delta = i - j \geq 1$. Substituting (19) and (22) into (15), we have

$$\begin{aligned} T_3(x, a, b) &= v_a \lambda_{01} P_A [Q(I - (1 - P_A)Q)^{-1}]_{a,b} \\ &\quad \times [(I - \lambda_{00}Q)^{-1}]_{b,x}. \end{aligned} \quad (25)$$

Combining the above three cases, we obtain

$$\pi(x, a, b) = T_1(x, a, b) + T_2(x, a, b) + T_3(x, a, b). \quad (26)$$

APPENDIX B PROOF OF THEOREM 2

Before proving Theorem 2, we first characterize the signs of the coefficients. It is straightforward to verify that $B \leq 0$, $C \leq 0$, and $E \leq 0$ for all $p, q, p_s, p_s^e \in [0, 1]$. In contrast, the signs of A and D are parameter-dependent and cannot be determined a priori. Next, to determine the optimal p_α , we analyze the shape of $\bar{A}_{\text{CRA}}(p_\alpha)$ via its first- and second-order derivatives.

From Corollary 1, the first derivative of $\bar{A}_{\text{CRA}}(p_\alpha)$ is

$$\frac{d\bar{A}_{\text{CRA}}}{dp_\alpha} = \frac{-AC p_\alpha^2 - 2BC p_\alpha + (AE - BD)}{(Cp_\alpha^2 + Dp_\alpha + E)^2}.$$

Define

$$M(p_\alpha) := -AC p_\alpha^2 - 2BC p_\alpha + (AE - BD).$$

Since $(Cp_\alpha^2 + Dp_\alpha + E)^2 > 0$ over the feasible interval, the sign of $\bar{A}'_{\text{CRA}}(p_\alpha)$ is completely determined by $M(p_\alpha)$.

To determine the sign of $M(p_\alpha)$, we first analyze the zero points and the vertex of $M(p_\alpha)$.

The zero points $M(p_\alpha) = 0$ are given by

$$r_\pm = \frac{-BC \pm \sqrt{\Delta}}{AC}, \quad \Delta := B^2 C^2 + AC(AE - BD).$$

Substituting the explicit expressions of A, B, C, D , and E into Δ , we obtain

$$\begin{aligned} \Delta &= p^2 q^2 p_s p_s^e (p+q)^4 (p+q-1)^2 (p_s - p_s^e)^2 (p_s + p_s^e - p_s p_s^e)^2 \\ &\quad \times \left[p_s + (p+q)p_s^e(1-p_s) \right] \left[p_s^e + p_s(2-p-q)(1-p_s^e) \right]. \end{aligned}$$

Since $p, q, p_s, p_s^e \in [0, 1]$ and $p+q \in [0, 2]$, every factor in the above expression is nonnegative. Hence, $\Delta \geq 0$.

Next, differentiating $M(p_\alpha)$ yields

$$\frac{dM}{dp_\alpha} = -2AC p_\alpha - 2BC = -2C(Ap_\alpha + B),$$

and thus the only vertex of M is located at

$$p_\alpha^v = -\frac{B}{A}.$$

We next distinguish two cases based on the sign of p_α^v .

Case 1: $A < 0$. Since $B \leq 0$, the vertex of $M(p_\alpha)$, $p_\alpha^v = -B/A \leq 0$. Moreover, $C \leq 0$ and $A < 0$ imply $-AC < 0$. Hence, $M(p_\alpha)$ is concave and therefore decreasing on $[0, 1]$.

Since $AC \geq 0$, the two roots satisfy

$$r_s = \frac{-BC - \sqrt{\Delta}}{AC} < \frac{-BC + \sqrt{\Delta}}{AC} = r_1.$$

Because the vertex lies to the left of $[0, 1]$, the smaller root satisfies $r_s < 0$ and only the larger root r_1 may lie in $[0, 1]$. Accordingly, $\bar{A}_{\text{CRA}}(p_\alpha)$ is increasing, decreasing, or increasing-then-decreasing on $[0, 1]$ depending on whether $r_1 \geq 1$, $r_1 \leq 0$, or $r_1 \in (0, 1)$, respectively. Therefore, the optimal solution is obtained by projecting r_1 onto $[0, 1]$, namely,

$$p_\alpha^* = [r_1]_0^1 = \left[\frac{-BC + \sqrt{\Delta}}{AC} \right]_0^1.$$

Case 2: $A > 0$. Using the explicit expressions of A and B , we obtain

$$A + B = -pq(1 - p_s^e) \left[(p+q)(1 - p_s)(p_s + p_s^e) + 2p_s^2 \right] \leq 0.$$

Hence, $B \leq -A$. Since $A > 0$, it follows that the vertex of $M(p_\alpha)$, $p_\alpha^v = -B/A \geq 1$. Moreover, $C \leq 0$ and $A > 0$ imply $-AC > 0$. Hence, $M(p_\alpha)$ is convex and therefore decreasing on $[0, 1]$.

Since $AC < 0$, the roots satisfy

$$r_s = \frac{-BC + \sqrt{\Delta}}{AC} < \frac{-BC - \sqrt{\Delta}}{AC} = r_1.$$

Because the vertex lies to the right of $[0, 1]$, the larger root satisfies $r_1 > 1$ and only the smaller root r_s may lie in $[0, 1]$. Accordingly, $\bar{A}_{\text{CRA}}(p_\alpha)$ is increasing, decreasing, or increasing-then-decreasing on $[0, 1]$, depending on whether $r_s \geq 1$, $r_s \leq 0$, or $r_s \in (0, 1)$, respectively. Therefore,

$$p_\alpha^* = [r_s]_0^1 = \left[\frac{-BC + \sqrt{\Delta}}{AC} \right]_0^1.$$

The stated result then follows by combining the two cases.