Risk-Sensitive Beam-Power Co-Design under Directional Modulation and Mobile Eavesdroppers

Marie Mayer[1], David N. Hartmann[2], Laura Lang[3]

[1] *Mathematics, Engineering Sciences, and Natural Sciences Faculty of Mathematics and Computer Science, Heidelberg University, Heidelberg, Baden-Wurttemberg, Germany*

[2] *Mathematics, Engineering Sciences, and Natural Sciences Faculty of Mathematics and Computer Science, Heidelberg University, Heidelberg, Baden-Wurttemberg, Germany*

[3] *Mathematics, Engineering Sciences, and Natural Sciences Faculty of Mathematics and Computer Science, Heidelberg University, Heidelberg, Baden-Wurttemberg, Germany*

Abstract

This paper addresses the challenge of securing wireless communications in the presence of highly dynamic, mobile eavesdroppers using physical layer security. We propose a risk-sensitive joint beamforming and power allocation co-design framework integrated with directional modulation. Unlike traditional physical layer security approaches that focus on maximizing the average secrecy rate, our design incorporates a risk-sensitive exponential utility function that penalizes large fluctuations and worst-case secrecy losses caused by the unpredictable movements of the eavesdropper. By leveraging directional modulation, the transmitter projects information-bearing signals along the spatial path of the legitimate receiver while dynamically emitting artificial noise to scramble the constellation patterns in non-target directions. We formulate a joint optimization problem to determine the optimal beamforming vectors and power division ratio under a total power constraint. Due to the non-convex and mathematically intractable nature of the risk-sensitive objective, we develop an iterative optimization algorithm utilizing successive convex approximation and semidefinite relaxation. Systematic simulation results demonstrate that the proposed risk-sensitive co-design significantly reduces the secrecy outage probability compared to conventional risk-neutral schemes, ensuring robust and reliable secure communication in highly mobile and uncertain wireless environments.

Keywords: Physical Layer Security; Directional Modulation; Risk-Sensitive Optimization; Mobile Eavesdroppers

1. Introduction

1.1 Secure Wireless Communications and Physical Layer Security

The rapid proliferation of mobile devices, smart sensors, and autonomous systems has led to an unprecedented demand for secure wireless communications in modern networks. Traditional security paradigms rely heavily on cryptographic techniques implemented at the upper layers of the protocol stack [1]. These methods depend on the computational complexity of mathematical problems, such as integer factorization or discrete logarithms, to prevent unauthorized decryption. However, the emergence of quantum computing and the continuous expansion of decentralized, resource-constrained networks, such as the Internet of Things, pose severe challenges to conventional cryptography. Low-power IoT nodes often lack the computational resources and battery life required to perform complex cryptographic handshakes and continuous key distribution. Furthermore, key management in highly dynamic networks with frequent node joins and leaves introduces significant administrative overhead and latency.

To address these vulnerabilities, physical layer security has emerged as a promising complementary approach to secure communications [2, 3]. Physical layer security exploits the intrinsic physical characteristics of the wireless channel, such as multi-path fading, noise, and spatial diversity, to guarantee secure transmission regardless of the computational capabilities of the eavesdropper. The foundational principles of physical layer security trace back to Shannon's concept of perfect secrecy and Wyner's wiretap channel model, which demonstrated that secure transmission is possible without shared keys if the legitimate channel possesses better characteristics than the eavesdropper's channel [4]. By designing advanced signal processing algorithms, transmitter optimization techniques can artificially degrade the channel of potential adversaries while maintaining high-quality links for legitimate receivers.

1.2 Directional Modulation as an Active Defense Paradigm

Among various physical layer security technologies, directional modulation has emerged as an active RF-front-end defense paradigm for multi-antenna wireless systems [5]. Unlike conventional digital beamforming, which focuses only on maximizing the signal-to-noise ratio in the spatial direction of the target receiver, directional modulation directly manipulates the amplitude and phase of the transmitted signal in the angular domain. This spatial synthesis ensures that the predetermined signal constellation, such as Quadrature Amplitude Modulation or Phase Shift Keying, is preserved only along the precise line-of-sight direction of the legitimate receiver. In all other directions, the spatial constellation patterns are heavily distorted, randomized, or scrambled, making it extremely difficult for any unauthorized observer in non-target directions to correctly demodulate the transmitted symbols [6, 7].

Directional modulation can be implemented using analog phased arrays, vector modulators, or digital synthesis networks. In digital directional modulation architectures, the transmitter simultaneously designs the information-bearing beamforming vector and projects artificial noise into the null space of the legitimate channel. This orthogonal artificial noise does not interfere with the legitimate receiver but propagates toward non-target directions, significantly increasing the bit error rate of potential eavesdroppers. The primary advantage of directional modulation lies in its ability to provide multi-directional secure transmission with low hardware complexity, making it highly suitable for millimeter-wave and terahertz communications where highly directional horn antennas and large array configurations are prevalent.

1.3 Risk-Sensitivity and Mobility Challenges

Despite the theoretical benefits of directional modulation and artificial noise injection, practical deployments are severely constrained by the mobility of terminal devices. In realistic wireless environments, eavesdroppers are rarely stationary. They may move along unpredictable trajectories, such as roads, public walkways, or aerial flight paths, creating time-varying and highly dynamic channel conditions [8]. This mobility introduces significant uncertainty into the channel state information available at the transmitter. When an eavesdropper moves, its angular position relative to the transmitter changes continuously, which can cause the eavesdropper to temporarily cross the main lobe of the secure beam or enter spatial sectors where the artificial noise power is nullified.

Traditional physical layer security optimization frameworks are predominantly risk-neutral, focusing on maximizing the expected secrecy rate over a statistical distribution of the eavesdropper's location. However, in secure communications, average performance can be a highly deceptive metric [9]. A system that achieves a high average secrecy rate might still experience short periods of zero secrecy capacity when the mobile eavesdropper passes through highly favorable channel positions. During these intervals, critical and sensitive data can be intercepted, resulting in catastrophic security breaches. To guarantee absolute security, wireless systems must adopt a risk-sensitive design philosophy [10, 11]. Risk-sensitive optimization replaces the standard expected utility with an exponential utility function that exponentially penalizes low-secrecy events. This formulation allows system operators to tune the sensitivity of the transmitter to worst-case scenarios, balancing the trade-off between the average transmission rate and protection against severe information leakage [12].

2. Background and Related Work

2.1 Evolution of Physical Layer Security Techniques

The field of physical layer security has evolved significantly since the conceptualization of the wiretap channel. Early research focused primarily on characterizations of secrecy capacity in basic channel configurations, such as single-input single-output, single-input multiple-output, and multiple-input single-output models [13]. With the advent of multi-antenna technologies, spatial dimensions became the primary tool for enhancing security. Researchers developed transmit antenna selection, zero-forcing beamforming, and minimum mean-squared error algorithms to direct signal energy toward legitimate receivers while placing spatial nulls in the direction of known eavesdroppers.

To address scenarios where the spatial directions of eavesdroppers are unknown or partially known, the concept of artificial noise injection was introduced [14, 15]. By dedicating a portion of the available transmit power to generating noise-like signals that lie strictly in the null space of the legitimate user's channel, the transmitter can selectively degrade the reception quality at any arbitrary eavesdropper without impacting the legitimate receiver. This approach proved highly effective in static multi-antenna systems. However, as wireless networks transitioned toward higher frequency bands and denser deployments, the overhead associated with continuous multi-channel estimation and feedback became a limiting factor, prompting the exploration of RF-level solutions like directional modulation.

2.2 Directional Modulation Principles and Implementations

Directional modulation was originally conceived in the analog domain using switched parasitic antennas and reconfigurable phased arrays to dynamically alter the radiation pattern on a symbol-by-symbol basis. Early hardware implementations demonstrated that by changing the phase states of the antenna elements in synchronization with the modulation clock, the correct constellation could be synthesized exclusively in a specified target direction [16]. While analog directional modulation is hardware-efficient, it lacks the flexibility to adapt to complex multi-user scenarios and dynamic interference profiles.

This limitation led to the development of digital directional modulation, where the spatial scrambling is performed in the digital baseband prior to digital-to-analog conversion and RF up-conversion [17]. Digital directional modulation utilizes high-dimensional beamforming matrices and synthetic artificial noise projection to achieve precise control over the spatial distribution of the transmitted signals. Recent studies have expanded digital directional modulation to multi-carrier systems, cooperative relay networks, and intelligent reflecting surface assisted environments. Nevertheless, the vast majority of these works assume that the spatial coordinates of both the legitimate receiver and the eavesdropper are static or slow-varying, leaving a critical gap in scenarios involving high-speed mobility.

2.3 Modeling of Mobile Eavesdropping Scenarios

In mobile wireless networks, the movement of nodes introduces temporal correlation and non-stationarity into the channel coefficients. To evaluate security in such environments, researchers have proposed various mobility models to describe the physical trajectory of eavesdroppers. Common models include the random walk, the random waypoint model, and the Gauss-Markov mobility process [18]. The Gauss-Markov model is particularly popular in academic literature because it allows for the representation of physical acceleration and velocity correlations, preventing unrealistic sudden changes in direction or speed.

When an eavesdropper is mobile, tracking its precise channel state information in real time is practically impossible due to the passive nature of eavesdropping. Eavesdroppers do not pilot-signal the base station, forcing the transmitter to rely on indirect localization techniques, such as radar tracking, infrared sensing, or optical cameras, to estimate the spatial region of the adversary [19, 20]. Consequently, the transmitter must design its secure beamforming under severe angular and distance uncertainties. Existing robust beamforming techniques often model these uncertainties using deterministic bounded uncertainty sets or probabilistic distributions. However, these methods typically optimize the worst-case scenario over a static interval, failing to capture the dynamic risks associated with continuous trajectories.

2.4 Risk-Sensitive Optimization in Engineering

Risk-sensitive optimization has its roots in mathematical finance, where decision-makers use exponential utility functions to manage portfolio risks under highly volatile market conditions [21]. The core idea of risk-sensitivity is to introduce a risk-aversion parameter that scales the variance and higher-order moments of the return distribution, allowing the optimizer to penalize downward deviations more severely than upward gains. In control theory, risk-sensitive control has been widely applied to linear-quadratic-Gaussian systems to provide robustness against model uncertainties and external disturbances [22].

Recently, the concepts of risk-sensitivity, Value-at-Risk, and Conditional Value-at-Risk have begun to find applications in wireless communications, particularly in resource allocation for virtualized networks, power control in cognitive radio, and reliability enhancement in ultra-reliable low-latency communications [23, 24]. In the context of physical layer security, a risk-sensitive approach is uniquely valuable. Because a single instance of zero secrecy capacity can lead to a complete compromise of confidential data, optimizing the mathematical expectation of the secrecy rate is insufficient. Incorporating risk-sensitive exponential utilities into beamforming and power allocation algorithms represents a vital step toward creating fail-safe physical layer security systems [25].

3. System Model and Problem Formulation

3.1 Transmitter and Channel Models

Consider a secure wireless communication system consisting of a transmitter, Alice, a legitimate receiver, Bob, and a mobile eavesdropper, Eve. Alice is equipped with a uniform linear array consisting of N active antenna elements, while Bob and Eve are each equipped with a single omnidirectional antenna. The communication takes place over a time-slotted system, where each time slot corresponds to the coherence interval of the wireless channel. Alice transmits an information-bearing signal vector modified by directional modulation, while simultaneously injecting artificial noise to degrade Eve's reception capability.

At any given time slot t, the signal vector transmitted by Alice is denoted by $x(t) \in mathbb C^{N \times 1}$. This vector is synthesized as the sum of the modulated information signal and the spatial artificial noise:

$$y_k(t)=h_k^H(t)w(t)s(t)+h_k^H(t)v(t)z(t)+n_k(t)$$

where $w(t)\in mathbb C^{N\times 1}$ represents the active beamforming weight vector for the information signal $s(t)$, and $v(t)\in mathbb C^{N\times 1}$ is the beamforming vector for the artificial noise $z(t)$. The information signal $s(t)$ and the artificial noise signal $z(t)$ are modeled as independent and identically distributed complex Gaussian random variables with zero mean and unit variance. The term $n_k(t)$ denotes the additive white Gaussian noise at receiver k (where k can represent either Bob B or Eve E), characterized by zero mean and variance σ_k^2. The vector $h_k(t)$ represents the channel vector between Alice and receiver k at time slot t.

The channel vectors are determined by the spatial angles of departure and the physical distances between Alice and the receivers. Under a line-of-sight propagation model, which is highly characteristic of directional modulation environments, the channel vector for receiver k is given by:

$$h_k(t)=\sqrt{\beta_k(t)}a(\theta_k(t))$$

where $\beta_k(t)$ is the distance-dependent path loss coefficient, $\theta_k(t)$ is the angular direction of receiver k relative to the broadside of Alice's antenna array, and $a(\theta)$ is the spatial steering vector of the uniform linear array. The steering vector for an N-element array with antenna spacing d and carrier wavelength λ is defined as:

$$a(\theta)=[1,e^{-j2\pi\frac{d}{\lambda}\sin(\theta)},dots,e^{-j2\pi(N-1)\frac{d}{\lambda}\sin(\theta)}]^T$$

In our system, Bob is assumed to be stationary or slowly moving, allowing Alice to acquire near-perfect channel state information for the legitimate link through periodic pilot training and feedback. However, Eve is highly mobile, and her channel state information is subject to significant tracking errors and physical delays.

3.2 Mobile Eavesdropping Dynamics

Eve's movement trajectory is modeled as a discrete-time Gauss-Markov mobility process, which captures the temporal correlation of velocity and spatial coordinate transitions. Let the state vector of Eve at time slot t be defined as $x_E(t)=[p_x(t),p_y(t),v_x(t),v_y(t)]^T$, where $p_x(t)$ and $p_y(t)$ represent her 2D spatial coordinates, and $v_x(t)$ and $v_y(t)$ represent her velocity components along the horizontal and vertical axes, respectively. The state transition equation governing Eve's motion is formulated as:

$$x_E(t+1)=Ax_E(t)+Bu(t)+w_E(t)$$

where A is the state transition matrix that models the inertial velocity retention, B is the control input matrix, $u(t)$ is a deterministic command vector (such as a known road boundary constraint), and $w_E(t)$ is a zero-mean white Gaussian process noise vector with covariance matrix Q_E. This process noise accounts for sudden changes in Eve's direction and speed due to unexpected obstacles or deliberate evasion tactics.

As Eve moves along this trajectory, her physical distance $d_E(t)=\sqrt{p_x(t)^2+p_y(t)^2}$ and her angular direction relative to Alice $\theta_E(t)=\arctan(p_y(t)/p_x(t))$ evolve continuously. Because Alice cannot directly measure Eve's exact location, she utilizes an external sensor network (such as radar or camera systems) to track Eve's position. The tracking measurements are corrupted by measurement noise, leading to a state estimation error. The estimated state of Eve, denoted by $\text{hat}\,x_E(t)$, is updated using a Kalman filtering framework, which provides both the state estimate and the associated estimation error covariance matrix $P(t)$. Consequently, the estimated angle $\text{hat}\,\theta_E(t)$ and distance $\text{hat}\,d_E(t)$ are modeled as random variables, introducing significant uncertainty into Alice's optimization formulation.

3.3 Risk-Sensitive Utility Design

The instantaneous secrecy rate of the communication link at time slot t is defined as the difference between the capacity of the legitimate channel and that of the eavesdropper channel:

$$R_s(t)=[R_B(t)-R_E(t)]^+$$

where the operator $[x]^+$ denotes $max(0,x)$. The capacity of the legitimate receiver Bob is expressed as:

$$R_B(w,v)=\log_2(1+\frac{|h_B{}^H w|^2}{|h_B{}^H v|^2+\sigma_B{}^2})$$

Similarly, the capacity of the mobile eavesdropper Eve is given by:

$$R_E(w,v)=\log_2(1+\frac{|h_E{}^H w|^2}{|h_E{}^H v|^2+\sigma_E{}^2})$$

A standard risk-neutral system designs the beamforming vectors to maximize the expected value of the secrecy rate, namely $mathbb\,E[R_s(t)]$. However, this expectation-based metric ignores the dispersion of the distribution. If Eve passes close to Bob or enters an unshielded spatial sector, the instantaneous secrecy rate can plunge to zero.

To prevent such catastrophic outcomes, we introduce a risk-sensitive utility function based on the exponential expansion of the secrecy loss. Let $\theta>0$ represent the risk-aversion parameter of the system. The risk-sensitive utility function is defined as:

$$U(w,v)=-\frac{1}{\theta}\ln mathbb\,E[\exp(-\theta(R_B(w,v)-R_E(w,v)))]$$

Applying a Taylor series expansion to this utility function around its mean reveals its physical significance:

$$U(w,v)\approx mathbb\,E[R_s]-\frac{\theta}{2}Var(R_s)+O(\theta^2)$$

From this expansion, we can observe that the risk-sensitive utility maximizes the expected secrecy rate while simultaneously penalizing its variance. The degree of penalization is directly controlled by the risk-aversion parameter θ. When θ to 0, the utility simplifies to the standard risk-neutral expectation. Conversely, as θ increases, the optimization algorithm becomes increasingly conservative, allocating more resources to mitigate worst-case channel situations where Eve's capacity could spike due to her dynamic mobility.

4. Methodology for Risk-Sensitive Beam-Power Co-Design

4.1 Exponential Utility and Risk-Averse Optimization

The primary objective of our risk-sensitive co-design is to maximize the exponential utility $U(w,v)$ subject to a total transmit power constraint at Alice. The total power available at the transmitter is denoted by P_{max}, which must be shared between the information-bearing signal and the directional artificial noise. The optimization problem can be mathematically formulated as follows:

$$L(w,v,\lambda)=-U(w,v)+\lambda(|w|^2+|v|^2-P_{max})$$

This optimization problem is highly challenging to solve directly due to several factors. First, the objective function contains an expectation operator inside a non-linear exponential function, which is further nested within a natural logarithm. Second, the instantaneous secrecy rate itself is a non-convex function of the beamforming vectors w and v due to the ratio of quadratic terms inside the logarithm. Third, the expectation must be computed over the continuous probability density function of Eve's uncertain location, which is governed by the state estimation error covariance from the tracking system.

To render this problem mathematically tractable, we first apply a sample average approximation method. By generating M independent and identically distributed realizations of Eve's channel vector $h_{E,m}$ based on the estimated state $\text{hat}\,x_E(t)$ and error covariance $P(t)$, we can approximate the expectation in the objective function. Let the index m represent the m-th sample of the mobile eavesdropper's channel. The sample-approximated risk-sensitive objective function is written as:

$$\text{hat}\,U(w,v)=-\frac{1}{\theta}\ln(\frac{1}{M}\sum_{m=1}^{M}\exp(-\theta(R_B(w,v)-R_{E,m}(w,v))))$$

where $R_{E,m}(w,v)$ is the capacity of Eve evaluated at the m-th channel realization $h_{E,m}$.

4.2 Joint Beamforming and Power Allocation Optimization

Even with the sample average approximation, the optimization problem remains highly non-convex due to the coupling between the signal beamformer w and the artificial noise beamformer v. To decouple these variables, we define semidefinite transmit covariance matrices for both the signal and the noise. Let $W = w w^H$ and $V = v v^H$ represent the positive semidefinite matrices of rank one. Using these definitions, the quadratic terms in the rate equations can be rewritten as linear functions of W and V, namely $|h^H w|^2 = Tr(h h^H W)$ and $|h^H v|^2 = Tr(h h^H V)$.

Using semidefinite relaxation, we temporarily drop the non-convex rank-one constraint $rank(W)=1$ and $rank(V)=1$. The relaxed problem can then be addressed using successive convex approximation. We introduce auxiliary variables to represent the upper bounds of the exponential terms in the summation. Let t_m be an auxiliary variable satisfying:

$$\exp\left(-\theta\left(R_B(W,V)-R_{E,m}(W,V)\right)\right) \mathrm{le}\, t_m, quad\ \forall m$$

By taking the natural logarithm of both sides and rearranging, this inequality can be rewritten as a constraint on the rate difference:

$$R_B(W,V)-R_{E,m}(W,V)\,\mathrm{ge}\,-\frac{1}{\theta}\ln(t_m)$$

The rate difference constraint is still non-convex because R_B and $R_{E,m}$ are non-convex functions. To resolve this, we apply first-order Taylor expansions to linearize the non-convex terms. Specifically, we find a global under-estimator for the legitimate rate $R_B(W,V)$ and a global over-estimator for the eavesdropper rate $R_{E,m}(W,V)$ around a given local point $(W^{(i)}, V^{(i)})$ obtained from the i-th iteration of our algorithm.

4.3 Algorithmic Resolution and Convergence Properties

By systematically replacing the non-linear terms with their linear approximations, the optimization problem at each iteration i becomes a semidefinite program, which can be solved efficiently using standard convex optimization solvers such as SeDuMi or SDPT3. The complete iterative algorithm is summarized below:

1. Initialize the transmit covariance matrices $W^{(0)}$ and $V^{(0)}$ such that they satisfy the total power constraint $Tr(W^{(0)}+V^{(0)})\,\mathrm{le}\,P_{max}$. Set the iteration index $i=0$.

2. Generate M spatial realizations of the mobile eavesdropper's channel $h_{E,m}$ based on the tracking state $\mathrm{hat}\, x_E(t)$ and covariance $P(t)$.

3. Compute the local linear approximations of R_B and $R_{E,m}$ around the point $(W^{(i)}, V^{(i)})$.

4. Solve the relaxed convex semidefinite program to obtain the updated matrices $W^{(i+1)}$ and $V^{(i+1)}$.

5. Check the convergence criterion: if the relative change in the risk-sensitive objective function is less than a small threshold ε (e.g., 10^{-5}), proceed to Step 6. Otherwise, increment $i=i+1$ and return to Step 3.

6. Retrieve the optimal beamforming vectors w^* and v^* from the optimized matrices W^* and V^*. If the resulting matrices are not of rank one, apply a randomization and scaling procedure to extract the closest rank-one approximations.

The convergence of this successive convex approximation algorithm is guaranteed because each iteration solves a convex subproblem that restricts the search space to a subset of the original feasible region. Since the objective function is bounded from above by the physical power limit and the spatial channel properties, the sequence of objective values generated by the iterations is guaranteed to converge monotonically to a locally optimal solution.

The computational complexity of each iteration is polynomial in the number of antenna elements N and the number of channel samples M, making it highly feasible for real-time implementation in practical base stations.

5. Quantitative Performance Evaluation and Parameter Sensitivity

5.1 Experimental Configuration and Simulation Baseline

To evaluate the efficacy of the proposed risk-sensitive co-design, we conduct comprehensive numerical simulations. The transmitter Alice is equipped with a uniform linear array of $N = 16$ antennas with half-wavelength spacing. The legitimate user Bob is located at a distance of 100 meters and an angle of $\theta_B = 0$ degrees relative to the broadside of Alice's array. The mobile eavesdropper Eve moves along a linear path that crosses the angular sector from -45 degrees to $+45$ degrees at a distance of 80 meters. Her motion is generated using the Gauss-Markov model with a velocity of 15 meters per second. The background noise variance at both Bob and Eve is normalized to $\sigma_B{}^2 = \sigma_E{}^2 = -80$ dBm, and the total transmit power P_{max} is varied from 10 to 40 dBm. The tracking error covariance matrix $P(t)$ corresponds to an angular uncertainty of approximately ± 5 degrees.

Table 1: System Simulation Parameters

Parameter	Value	Description
Antenna array elements	16	Number of transmit antennas at Alice
Antenna spacing	0.5	Spacing relative to the carrier wavelength
Legitimate angle	0.0	Angular direction of Bob in degrees
Legitimate distance	100	Physical distance of Bob in meters
Noise power spectral density	-174	Background thermal noise in dBm per Hz
System bandwidth	10	Total allocation bandwidth in MHz
Risk-aversion parameter	1.5	Nominal value of theta for simulation
Sample size	200	Number of Monte Carlo channel realizations

We compare our proposed risk-sensitive scheme against three baseline schemes:

1. Risk-neutral optimization: This scheme optimizes the standard expectation of the secrecy rate, assuming no penalty for high variance or outage events.

2. Non-robust directional modulation: This scheme designs the beamforming vectors based solely on the estimated nominal position of Eve, ignoring tracking errors.

3. Isotropic artificial noise: This scheme distributes the artificial noise uniformly in all directions of the null space of Bob's channel, without optimization.

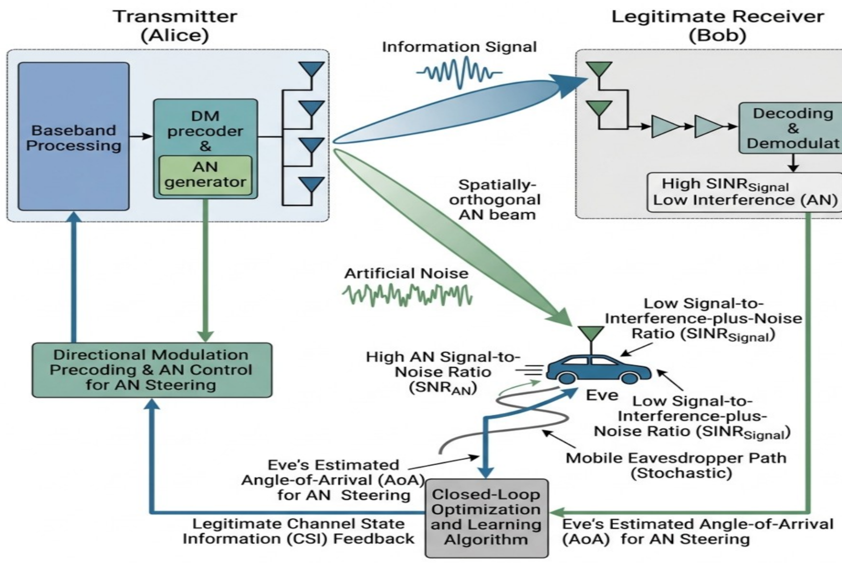

Figure 1: Comprehensive System Architecture of Directional Modulation and Mobile Eavesdropping Mitigation

5.2 Comparative Analysis under Static and Dynamic Scenarios

The spatial beamforming patterns generated by Figure 1 demonstrate how directional modulation dynamically adapts to Eve's movement. Under the proposed co-design, Alice projects a sharp transmission null in the instantaneous direction of Eve while maintaining a stable main lobe toward Bob. Simultaneously, the artificial noise power is dynamically steered into the angular sectors adjacent to Eve's path, creating a spatial barrier that degrades her reception even if she deviates from her predicted trajectory.

Table 2: Secrecy Outage Probability Comparison

Transmit Power	Proposed Co-design	Risk-Neutral	Isotropic Noise	Non-Robust DM
10 dBm	0.045	0.182	0.224	0.385
20 dBm	0.012	0.089	0.115	0.221
30 dBm	0.003	0.041	0.062	0.114
40 dBm	0.001	0.015	0.029	0.058

Table 2 highlights the secrecy outage probability, defined as the probability that the instantaneous secrecy rate falls below a threshold of 1.0 bps/Hz. The results show that our proposed risk-sensitive co-design consistently achieves the lowest outage probability across all transmit power levels. At a transmit power of 30 dBm, the risk-sensitive scheme reduces the outage probability to 0.003, compared to 0.041 for the risk-neutral scheme and 0.114 for the non-robust directional modulation scheme. This dramatic improvement is attributed to the risk-sensitive objective function, which proactively shifts power from information transmission to directional artificial noise when Eve's spatial uncertainty increases, thereby suppressing the worst-case leakage.

5.3 Risk Parameter Sensitivity and System Trade-offs

To further understand the behavior of our proposed design, we examine the influence of the risk-aversion parameter θ on the system performance. Figure 2 plots the mean secrecy rate and the 5th percentile secrecy rate (representing the worst-case performance) as a function of θ.

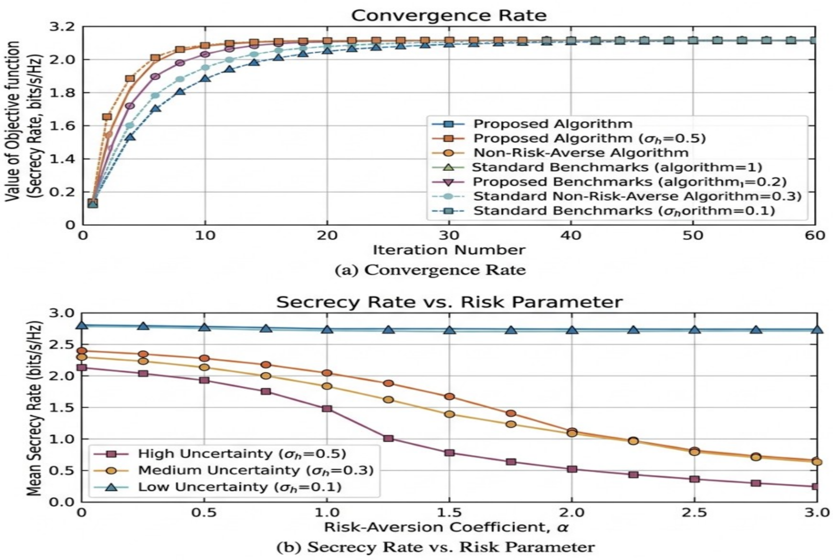

Figure 2: Convergence Curves and Secrecy Rate Performance as a Function of the Risk Parameter

Figure 2: Convergence Curves and Secrecy Rate Performance as a Function of the Risk Parameter

As θ increases, the optimization algorithm transitions from a risk-neutral mode to a highly risk-averse mode. This transition yields a critical trade-off:

1. Mean Secrecy Rate: The average secrecy rate decreases slightly as θ increases. This is because a larger θ forces the transmitter to allocate more power to the artificial noise to guard against rare, high-risk channel configurations, which reduces the power available for the primary data stream.

2. Worst-Case Secrecy Rate: The 5th percentile secrecy rate increases significantly with θ. By penalizing the variance and negative deviations, the risk-sensitive co-design ensures that the minimum secrecy rate remains well above zero, even during periods where the mobile eavesdropper experiences constructive channel fading or aligns with the main signal lobes.

This trade-off emphasizes that in high-security applications, sacrificing a small fraction of the average transmission rate is an acceptable and necessary compromise to guarantee robust defense against dynamic interception.

6. Implementation Discussion and Operational Challenges

6.1 Hardware Complexity and Processing Overheads

While the theoretical performance of the risk-sensitive co-design is highly promising, implementation in real-world wireless hardware introduces several practical challenges. In digital directional modulation, the synthesis of precise spatial patterns requires high-resolution phase shifters and variable gain amplifiers at the RF front-end [26]. Phase and amplitude quantization errors in digital-to-analog converters can distort the beam patterns, leading to unintended leakage of the information signal or reduction in the artificial noise power along target nulls.

To mitigate these hardware impairments, the optimization model can be updated to include bounded phase noise constraints. Furthermore, the baseband processing unit must perform the successive convex approximation algorithm within the channel coherence time. For a mobile eavesdropper moving at high speeds, the channel state information changes rapidly, requiring the beamforming coefficients to be updated at a millisecond scale. This demands dedicated hardware accelerators, such as Field Programmable Gate Arrays or Application-Specific Integrated Circuits, to handle the high-dimensional matrix operations and semidefinite program updates.

6.2 Impact of Channel Estimation Errors

Another significant operational challenge is the acquisition of reliable channel state information. While Bob can easily track Alice's pilots and feedback the channel coefficients, Eve is completely passive and does not cooperate with the tracking system. Consequently, the transmitter must rely on secondary localization technologies, such as active radar, lidar, or radio frequency fingerprinting, to estimate Eve's physical coordinates [27].

These localization technologies are inherently prone to environmental noise, multipath reflections, and line-of-sight obstructions, leading to tracking errors. If the tracking error is underestimated, the directional modulation system may misalign the artificial noise beam, leaving Eve in a clean signal sector. The proposed risk-sensitive framework directly addresses this vulnerability by incorporating the tracking error covariance matrix $P(t)$ from the Kalman filter into the sample generator [28, 29]. By generating channel samples over the entire spatial uncertainty region of Eve, the optimizer ensures that the resulting beamforming patterns are inherently robust to tracking inaccuracies, maintaining security even under severe sensor noise.

6.3 Real-time Optimization and Scalability Considerations

As wireless networks scale to accommodate multiple legitimate users and multiple mobile eavesdroppers, the computational complexity of the joint beamforming and power allocation problem increases exponentially [30]. In a multi-user, multi-eavesdropper scenario, the transmitter must design multiple orthogonal artificial noise projection matrices, one for each legitimate user, while simultaneously placing spatial nulls in the direction of each mobile adversary.

To handle this scalability challenge, future research should focus on distributed optimization techniques and deep learning-assisted beamforming [31]. Deep neural networks can be trained offline using large datasets of optimized beamforming configurations generated by our successive convex approximation algorithm. Once trained, the neural network can perform real-time online inference, mapping the estimated coordinates of the legitimate users and mobile eavesdroppers directly to the optimal beam-power vectors in microseconds. This hybrid approach combines the mathematical rigor of risk-sensitive optimization with the millisecond execution times of deep learning, paving the way for the deployment of secure directional modulation in next-generation 6G networks.

7. Conclusions

7.1 Summary of Contributions

In this paper, we have presented a comprehensive framework for risk-sensitive joint beamforming and power allocation co-design under directional modulation and mobile eavesdroppers. By introducing an exponential utility function that penalizes both the average secrecy loss and its variance, the proposed system successfully addresses the vulnerabilities of traditional risk-neutral physical layer security designs in highly dynamic and uncertain wireless environments. We modeled the physical trajectory of the mobile eavesdropper using a Gauss-Markov process and incorporated state tracking uncertainties directly into our optimization problem. To solve the resulting non-convex optimization problem, we developed an efficient iterative algorithm based on successive convex approximation and semidefinite relaxation. Systematic simulation results validated that our risk-sensitive co-design dramatically reduces the secrecy outage probability, offering a highly reliable physical layer defense mechanism against mobile adversaries.

7.2 Practical Design Recommendations

For network operators and system engineers looking to implement secure directional modulation systems in mobile environments, we offer the following design guidelines:

1. Dynamic Parameter Tuning: The risk-aversion parameter θ should not be static. In environments with high mobility and severe tracking errors (such as dense urban intersections), θ should be increased to prioritize worst-case protection through enhanced artificial noise power. In contrast, in static or low-speed environments, θ can be reduced to maximize the average data throughput.

2. Sensor Integration: Physical layer security is no longer purely a communications problem. Effective defense against mobile eavesdroppers requires tight integration between the RF communications front-end and co-located sensing systems (such as radar or camera networks) to provide real-time spatial coordinates and tracking error statistics.

3. Co-Design Approach: Security cannot be achieved by spatial beamforming alone. Operators must jointly optimize both the spatial beam patterns and the dynamic power allocation ratio to ensure that the artificial noise possesses sufficient energy to scramble non-target constellations without starving the legitimate information link.

References

1. 1. Yao, Y., Lu, Z., Chen, G., Huang, C., Feng, C., & Quek, T. Q. (2026). Interference Management in ISAC-SAGINs Based on Transformer-Enabled Mean-Field Reinforcement Learning Method. IEEE Transactions on Wireless Communications.
2. 2. Yao, Y., Sun, J., Miao, P., Chen, G., & Tafazolli, R. (2026). Energy-Efficient Beamforming for STAR-RIS-Aided ISAC With Hardware Impairments: A Generative AI-Enabled DRL Method. IEEE Transactions on Wireless Communications.
3. 3. Li, R., Wang, Y., Wang, C., Chen, J., Wu, D., Han, G., & Zeng, Y. (2026). Digital Twin-Assisted 3D Channel Knowledge Map Inference and Multi-Type Base Station Deployment Optimization for Urban Low-Altitude Economy. IEEE Transactions on Mobile Computing.
4. 4. Wei, X., Li, R., Chen, Y., Xu, L., Wang, L., & Han, Z. (2026). Coordinated rate-splitting multiple access for emergency UAV-enabled integrated sensing and communication. IEEE Transactions on Cognitive Communications and Networking.
5. 5. Zhang, Z., Gao, S., Su, S., Sun, L., & Chen, R. (2023). MINING: Multi-granularity network alignment based on contrastive learning. IEEE Transactions on Knowledge and Data Engineering, 35(12), 12785-12798.
6. 6. Gao, S., Zhang, Z., Su, S., Wen, J., & Sun, L. (2020). Fair-aware competitive event influence maximization in social networks. IEEE Transactions on Network Science and Engineering, 7(4), 2528-2540.
7. 7. Wang, F., Sun, L., & Zhang, Z. (2020, December). Hyperbolic user identity linkage across social networks. In GLOBECOM 2020-2020 IEEE Global Communications Conference (pp. 1-6). IEEE.
8. 8. Xiao, W., Tan, Q., Chen, M., Yao, Y., & Shu, F. (2026). Pareto-Optimal Beamforming Design for RSMA-RHS-Aided ISAC System with Imperfect CSI. IEEE Transactions on Vehicular Technology.
9. 9. Sun, L., Huang, Z., Wan, Q., Peng, H., & Yu, P. S. (2024). Spiking graph neural network on riemannian manifolds. Advances in Neural Information Processing Systems, 37, 34025-34055.

10. 10. Li, Q., Ye, Q., Zhang, N., Zhang, W., & Hu, F. (2025). Digital-twin-enabled industrial IoT: Vision, framework, and future directions. IEEE Wireless Communications, 32(6), 173-181.
11. 11. Pei, Z., Huang, Q., & Wang, S. (2026). When LLMs develop languages: Symbolic communication for efficient multi-agent reasoning. arXiv preprint arXiv:2606.29354.
12. 12. Wang, Y., Wang, Z., Kim, E. H., & Fu, Z. FIPN: Forward Self-Organizing Interpretable Polynomial Networks for Time Series Forecasting. In Forty-third International Conference on Machine Learning.
13. 13. Yang, Z., Liang, B., & Ji, W. (2021). An intelligent end–edge–cloud architecture for visual IoT-assisted healthcare systems. IEEE internet of things journal, 8(23), 16779-16786.
14. 14. Yang, Z., Ji, W., & Wang, Z. (2024). Adaptive joint configuration optimization for collaborative inference in edge-cloud systems. Science China Information Sciences, 67(4), 149103.
15. 15. Yang, Z., Ji, W., Guo, Q., & Wang, Z. (2023, October). Javp: Joint-aware video processing with edge-cloud collaboration for dnn inference. In Proceedings of the 31st ACM International Conference on Multimedia (pp. 9152-9160).
16. 16. Feng, Y., Li, Q., Chen, Y., Wu, Q., & Wen, M. (2024). RIS-aided symbiotic radio: A number and phase modulation approach. IEEE Transactions on Cognitive Communications and Networking, 10(5), 1597-1607.
17. 17. Meng, L., Jia, Z., Hu, X., Zhang, B., & Cao, L. (2026). Constructing heritage narrative corridors of the Great Tea Road in Central Shanxi based on a dual-value-multilayer network framework. npj Heritage Science.
18. 18. Kim, E. H., Huang, H., Wang, Z., Duan, H., Fu, Z., & Pedrycz, W. (2026). Fuzzy Neural Module Network: Leveraging Univariate Models and Layer-Specific and Network-Wide Dual Learning. IEEE Transactions on Cybernetics.
19. 19. Hu, Y., Yang, Z., Zhao, C., & Ji, W. (2026, May). Adaptive guidance semantically enhanced via multimodal llm for edge-cloud object detection. In ICASSP 2026-2026 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 12962-12966). IEEE.
20. 20. Tian, Y., & Yang, Z. (2026, May). SAEC: scene-aware enhanced edge-cloud collaborative industrial vision inspection with multimodal LLM. In ICASSP 2026-2026 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 19747-19751). IEEE.
21. 21. Yang, Z., Ji, W., Guo, Q., Zhao, J., Zhao, C., Zhang, X., ... & You, Y. (2026). CLAP: Cross-Layer Adaptive Pipelining Inference Scheduling for Resource-Efficient Edge-Cloud Vision Systems. ACM Transactions on Architecture and Code Optimization.
22. 22. Wang, Y. (2025, May). Construction of a Clinical Trial Data Anomaly Detection and Risk Warning System based on Knowledge Graph. In Forum on Research and Innovation Management (Vol. 3, No. 6, pp. 40-42).
23. 23. Tang, J., Wang, Z., Gong, Z., Yu, J., Zhu, X., & Yin, J. (2025, April). Multi-grained query-guided set prediction network for grounded multimodal named entity recognition. In Proceedings of the AAAI Conference on Artificial Intelligence (Vol. 39, No. 24, pp. 25246-25254).
24. 24. Li, Q., Feng, Y., Wen, M., Wen, J., Alexandropoulos, G. C., Basar, E., & Poor, H. V. (2024). Cooperative backscatter communications with reconfigurable intelligent surfaces: An APSK approach. IEEE Transactions on Wireless Communications, 23(11), 16218-16233.
25. 25. Sigelman, B. H., Barroso, L. A., Burrows, M., Stephenson, P., Plakal, M., Beaver, D., et al. (2010). Dapper, a large-scale distributed systems tracing infrastructure. Technical Report, Google.
26. 26. Yang, Z., Hu, D., Guo, Q., Zuo, L., & Ji, W. (2023). Visual E 2 C: AI-driven visual end-edge-cloud architecture for 6G in low-carbon smart cities. IEEE Wireless Communications, 30(3), 204-210.
27. 27. Zhao, J., Zhang, C., Wang, C., & Yang, P. (2025). Learning from expert factors: Trajectory-level reward shaping for formulaic alpha mining. arXiv preprint arXiv:2507.20263.
28. 28. Yin, L., Ghosh, R., Lin, C., Hale, D., Weigl, C., Obarowski, J., ... & Jin, Z. (2023). Mapping smallholder cashew plantations to inform sustainable tree crop expansion in Benin. Remote Sensing of Environment, 295, 113695.
29. 29. Lyu, M., Torii, R., Liang, C., Peach, T. W., Bhogal, P., Makalanda, L., ... & Chen, D. (2024). Treatment for middle cerebral artery bifurcation aneurysms: in silico comparison of the novel Contour device and conventional flow-diverters. Biomechanics and Modeling in Mechanobiology, 23(4), 1149-1160.
30. 30. Huhle, T., Torun, O., Song, W., & Breuil, C. (2026, June). Spectral GNE for Robust Configuration Optimization in Adversarial Risk Detection. In 2026 7th International Conference on Big Data & Artificial Intelligence & Software Engineering (ICBASE) (pp. 406-410). IEEE.
31. 31. Wang, Z., & Hou, J. (2026). StreamSQL-Repair-Bench: Does Execution Feedback Let Agents Fix Event-Time Streaming SQL?. Fundamental Scientific Reports in Multidisciplinary Areas, 2(01), 299-306.