

Spectrum Sharing and Covert Jamming for Wireless D2D Link Surveillance

Sibo Wang, Bin Yang, Wenhao Zhang, Yulong Shen, Zhiqian Liu, Xiaohong Jiang, Tarik Taleb

Abstract—Device-to-device (D2D) communications in cellular systems improve spectral efficiency and reduce latency but also create security challenges, as suspicious D2D links can bypass base station monitoring and evade detection. This paper proposes a theoretical framework for covert surveillance of such links. A full-duplex Warden legitimately monitors a suspicious D2D pair via eavesdropping in the presence of a base station and a cellular user (Alice), covertly injecting artificial noise to aid eavesdropping. We derive the average minimum detection error probability at the D2D receiver and its optimal threshold for both underlay (spectrum reuse) and overlay (orthogonal spectrum) modes. To evaluate performance, we present an eavesdropping non-outage probability metric, capturing the reliability of the legitimate eavesdropping link while ensuring quality-of-service (QoS) for cellular and D2D communications. To maximize this metric, the transmit powers and the spectrum partition factor are optimized under both modes, considering a fixed-power adversary and an adaptive one that adjusts power to maintain QoS. We solve the resulting non-concave problems by a unified concave-convex procedure. Additionally, a flexible mode selection scheme is proposed to reduce selection overhead while meeting a minimum surveillance requirement. Extensive numerical results demonstrate the effectiveness of the proposed framework in enhancing covert surveillance.

Index Terms—Physical layer security, active eavesdropping,

Received 23 December 2025; revised 6 July 2026; accepted 24 August 2026. This work was supported in part by the National Natural Science Foundation of China under Grants 62372076 and 62302366, in part by the Education Department Research Foundation of Anhui Province under Grant DTR2023051, in part by the Innovation Team on Smart Home Appliance Security and Applications of Chuzhou City, in part by the Japan Society for the Promotion of Science under Grant 23K28076, in part by the China Postdoctoral Science Foundation under Grant 2023M744309, in part by the Federal Ministry of Research, Technology, and Space (BMFTR), Germany, through the Project 6GEM+ under Grant 16KIS2411, and in part by the European Union's Horizon Europe research and innovation programme through the 6G-Path project under Grant 101139172. (*Corresponding authors: Bin Yang; Wenhao Zhang.*)

S. Wang and X. Jiang are with the School of Systems Information Science, Future University Hakodate, Hakodate, Hokkaido, Japan. Email: {g3224003, jiang}@fun.ac.jp.

B. Yang is with the School of Cyber Security, Chuzhou University, Chuzhou 239000, China. Email: yang-binchi@gmail.com.

W. Zhang is with the College of Cyber Security, Tarim University, Xinjiang, 843300, China. Email: hizhangwenhao@gmail.com.

Y. Shen is with the School of Computer Science and Technology, Xidian University, Xi'an, Shaanxi 710071, China, and also with the Shaanxi Key Laboratory of Network and System Security, Xi'an, Shaanxi 710071, China. Email: ylsen@mail.xidian.edu.cn.

Z. Liu is with the College of Cyber Security, Jinan University, Guangzhou 510632, China, also with the Guangdong Key Laboratory of Data Security and Privacy Preserving, Jinan University, Guangzhou 510632, China, also with the Guangdong Hong Kong Joint Laboratory for Data Security and Privacy Protection, Jinan University, Guangzhou 510632, China, and also with the Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin 541004, China. Email: zqliu@vip.qq.com

Tarik Taleb is with the Faculty of Electrical Engineering and Information Technology, Ruhr University Bochum, Bochum 44801, Germany. Email: tarik.taleb@rub.de.

device-to-device, mode selection, covert jamming, channel uncertainty.

I. INTRODUCTION

Device-to-Device (D2D) communication has emerged as a key technology enabling direct information exchange between user devices without routing through a base station, offering high spectral efficiency, low latency, and large throughput. These advantages have led to its widespread adoption in diverse applications, including the Internet of Things (IoT) [1]–[3], vehicle-to-everything (V2X) communication [4], emergency communication [5], [6], edge computing [7], and unmanned aerial vehicle (UAV)-assisted systems [8], [9]. However, D2D links can bypass base station monitoring, making them vulnerable to misuse by malicious users for sensitive information exchange or illicit activities. Such circumvention of core network oversight renders traditional monitoring ineffective, highlighting the urgent need for active eavesdropping mechanisms that enable authorized nodes to efficiently intercept data from suspicious D2D communications.

To address emerging security challenges, active eavesdropping for suspicious link surveillance has been extensively studied in wireless systems, with research efforts primarily devoted to spoofing relay [10] and active jamming strategies [11]–[20] (See Related work of Section II for details). In the former, the monitoring node is disguised as a relay to transmit spoofed signals, thereby inducing the suspicious source to adjust its transmission rate in favor of eavesdropping. In the latter, jamming signals are injected to deliberately degrade the suspicious receiver's channel quality, with techniques such as beamforming [21], antenna selection [22], and cooperative jamming schemes [16], [17] employed to mitigate self-interference. These strategies have been further extended to scenarios involving multi-node cooperation, and recent studies have introduced deep learning methods to enable adaptive selection of surveillance modes [13]. Overall, these approaches share the common objective of enhancing eavesdropping performance through optimal system parameter design.

Although significant progress has been made in jamming-assisted active eavesdropping, existing studies have not fully addressed three issues: the covert jamming strategy, the adversary's adaptive countermeasure, and flexible mode selection under dynamic spectrum management. First, most assume the injected jamming signal is overt [13], [14], [18], overlooking that suspicious users may detect it, interrupt communication, or alter their transmission strategy, causing the surveillance to fail. Second, most assume the suspicious transmitter uses

fixed power [18]–[20], ignoring that a more capable adversary in a realistic setting may adjust its transmit power to maintain quality of service (QoS) and evade eavesdropping when jamming degrades its link quality. Third, most works consider only underlay (spectrum reuse) or overlay (orthogonal spectrum) modes [16]–[20], neglecting how dynamic spectrum partitioning and flexible mode selection can minimize management overhead while meeting a basic surveillance requirement. These gaps both compromise surveillance covertness and fail to exploit the complex spectrum environment of D2D communication systems.

To address these gaps, this paper is the first to investigate covert active eavesdropping for suspicious D2D link surveillance through a joint design of a covert jamming strategy and spectrum sharing modes. In underlay mode, spectrum reuse improves efficiency but introduces mutual interference, so we exploit the cellular signal as additional interference to strengthen surveillance while controlling transmit power to limit its impact on the eavesdropping link. In overlay mode, orthogonal spectrum reduces interference at the cost of efficiency, so we optimize spectrum allocation to balance the QoS of cellular and D2D communications while sustaining the Warden’s monitoring performance. For both modes, we further consider two types of suspicious adversaries, one with fixed transmit power and one with adaptive power that adjusts itself to maintain QoS under jamming. We jointly optimize the transmit power and spectrum resource allocation to maximize surveillance performance while preserving covertness. We also design a flexible mode selection mechanism over a long horizon of multiple blocks, which weighs the surveillance performance of the underlay and overlay modes against their selection overhead to minimize this overhead while meeting a minimum surveillance requirement. The studied problem is also grounded in practical systems. Within the Third Generation Partnership Project (3GPP) framework, D2D communication is supported through Proximity Services and sidelink operation [23]. A D2D link carries data directly between the two devices without traversing the base station, so monitoring a suspicious D2D pair is a real and valuable task for public safety and legitimate surveillance. The studied scenario thus has clear deployment relevance across a wide range of practical settings.

The main contributions of this paper are summarized as follows:

- 1) We develop a theoretical framework for covert active eavesdropping in a D2D system comprising a base station (BS), a cellular user (Alice), a suspicious D2D pair, and a full-duplex legitimate Warden. The Warden injects artificial noise (AN) to aid eavesdropping while staying undetected by the suspicious receiver D_r . Under channel uncertainty, we derive the average minimum detection error probability of D_r for the jamming signal in both underlay and overlay modes, which gives quantitative constraints for covert monitoring.
- 2) We model and optimize the eavesdropping non-outage probability under both spectrum sharing modes. In underlay mode, the model jointly captures the eavesdropping link and the QoS of cellular and D2D communica-

tions, and we maximize this probability under covertness constraints by jointly optimizing the transmit powers of the Warden and Alice. In overlay mode, the spectrum partition factor becomes an additional optimization variable. For each mode, we consider a fixed-power adversary in Case 1 and an adaptive-power one in Case 2 that adjusts power to maintain QoS under jamming. Since these problems are non-concave, we propose a unified concave-convex procedure (CCCP) that solves both modes and both cases, with a convergence guarantee and complexity analysis.

- 3) We propose a flexible mode selection scheme over a long horizon of multiple blocks. We model the mode selection overhead, a practical cost often overlooked in real systems, and minimize it while meeting a minimum surveillance requirement. Rather than staying in a single mode, the legitimate surveillance system selects between underlay and overlay modes according to the required surveillance performance, which improves adaptability.
- 4) Extensive numerical results show how power control, spectrum partition, and mode selection affect the eavesdropping non-outage probability in both modes. They reveal the dual role of channel uncertainty: excessive uncertainty on the suspicious link degrades D2D quality and causes eavesdropping failure, whereas moderate uncertainty on the jamming link can improve covertness and effectiveness depending on the suspicious transmitter’s power. Alice’s transmit power aids eavesdropping within a certain range but becomes detrimental when too high in underlay mode, while it consistently raises the non-outage probability in overlay mode. The scheme stays effective under both the fixed-power and adaptive-power cases.

The rest of this paper is organized as follows. Section II reviews related work. Section III introduces the covert eavesdropping system model. Section IV analyzes the detection performance of covert AN transmission. Sections V and VI model and optimize the eavesdropping performance for the underlay and overlay modes and present a unified CCCP-based solver. Section VII presents a flexible mode selection mechanism. Section VIII provides numerical results, and Section IX concludes the paper.

II. RELATED WORK

A. Active Eavesdropping

Active eavesdropping has been extensively studied to improve legitimate surveillance in wireless systems. The techniques like beamforming [21] and antenna selection [22] enable efficient monitoring with low system complexity, while optimization schemes for delay-sensitive and delay-tolerant scenarios further enhance reliability and accuracy [11]. In cooperative and multi-node systems, monitors can transmit interference to assist others [12] or dynamically select between surveillance and interference modes using deep learning [13], and in relay-assisted or two-hop communications, adaptive mode selection maximizes interception performance [14], [15]. To mitigate self-interference, alternating [16] and rotational

[17] interference strategies have been proposed, allowing monitors to cancel their own interference while degrading the suspicious link, and closed-form solutions for optimal interference power further improve multi-antenna monitoring [18]. Building on these approaches, covert transmission techniques have been introduced to jointly optimize monitoring effectiveness and stealth [19]. This work provides an important benchmark for covert jamming-assisted surveillance. However, it considers a basic suspicious transmitter-receiver-monitor model with fixed suspicious transmit power, and does not account for D2D-enabled cellular coexistence, cellular/D2D outage constraints, or underlay/overlay spectrum sharing. In D2D-oriented surveillance, underlay schemes leveraging uplink signals and beamforming can enable simultaneous monitoring and communication [20], but the injected interference is not modeled as covert AN detectable by the suspicious D2D receiver, and overlay spectrum allocation and overhead-aware mode selection are not considered. Therefore, the covertness-performance tradeoff of covert jamming-assisted surveillance in D2D-enabled cellular networks remains insufficiently explored, especially under adaptive suspicious transmit power and practical mode-selection overhead.

B. Covert Transmission

Covert transmission aims to enable undetectable communication by exploiting uncertainties in power [24], distance [25], phase [26], or time [27], making signals statistically difficult to distinguish from noise. Compared to noise uncertainty [28], [29], which is difficult to control, channel uncertainty [30], [31] is more designable and often arises from channel estimation errors. Channel uncertainty has been shown to significantly degrade monitor detection, can be jointly optimized with interference uncertainty [30], and may dominate noise uncertainty under high signal-to-interference-plus-noise ratio (SINR) [31]. In D2D-enabled cellular systems, spectrum sharing can follow underlay or overlay modes: underlay improves spectral efficiency but introduces interference, whereas overlay reduces inter-link interference and provides better rate guarantees; in both cases, interference can serve as cover to enhance covert performance. Covert-transmission models have been developed to jointly optimize mode selection, spectrum allocation, and transmit powers under both underlay and overlay [32], [33]. However, these approaches have rarely been integrated with active eavesdropping research, which seldom considers D2D scenarios or jointly analyzes eavesdropping strategies with underlay and overlay mode selection, leaving a significant research gap.

III. SYSTEM MODEL

A. System Model

As illustrated in Fig. 1, we design a covert surveillance system that consists of a base station (BS), a cellular user (Alice), a suspicious D2D pair (D_t, D_r), and a legitimate full-duplex monitor (Warden). The system operates in two spectrum sharing modes: underlay and overlay.

In the underlay mode, all nodes share the same spectrum. Alice transmits uplink data to the BS using a single antenna,

while D_t communicates with D_r over a single-antenna D2D link. The Warden employs two antennas¹ to simultaneously eavesdrop on D_t and covertly transmit AN to jam D_r , introducing self-interference. Spectrum sharing causes additional interference: the Warden's AN and D_t 's signal affect the BS, and Alice's uplink signal interferes with both the Warden's reception and D_r . Under this mode, there exist five link types as shown in Fig. 1(a): communication, eavesdropping, jamming, interference, and self-interference.

In the overlay mode, the spectrum is divided into two orthogonal portions: a fraction β for Alice-BS uplink and $1 - \beta$ for the D2D pair and the Warden. Within this band, D_t transmits to D_r , while the Warden simultaneously eavesdrops and covertly jams D_r . Orthogonal allocation eliminates cross-interference between the cellular and D2D transmissions. Under this mode, four link types exist as shown in Fig. 1(b): communication, eavesdropping, jamming, and self-interference.

The single cellular user and single D2D-pair model is a basic resource-block-level coexistence model. It represents one scheduled cellular uplink and one suspicious D2D link that share the same resource block in the underlay mode or split the spectrum in the overlay mode. This is an in-coverage D2D surveillance setting, where the suspicious pair uses a direct link that may bypass data-plane monitoring at the BS. Such models are widely adopted in D2D-enabled cellular networks, since they capture the core interaction among spectrum sharing, co-channel interference, and QoS requirements [32], [33], [35]. The framework extends to dense multi-user scenarios. When multiple cellular users or D2D pairs reuse the same resource block, the system must handle user scheduling, resource block assignment, per-user power control, aggregated interference, and multiple QoS constraints, which complicates the analysis and yields a high-dimensional optimization problem. This paper therefore focuses on the single cellular user and single D2D-pair model as an analytically tractable baseline. It reveals the key tradeoff among covert jamming, Warden detection, eavesdropping reliability, cellular user QoS, and D2D QoS. We leave the full multi-user extension to future work.

B. Channel Model

We consider that all wireless channels in the system undergo quasi-static Rayleigh block fading², meaning that the channel coefficients remain constant within each transmission

¹The two antennas at the Warden denote one transmit/receive pair assigned to the surveillance task, not a limit on its total physical antennas. This corresponds to the minimum separated full-duplex configuration for simultaneous eavesdropping and AN/jamming, widely adopted in proactive eavesdropping studies [19], [34]. A multi-antenna Warden then reduces to the special case of selecting one receive and one transmit antenna from the available sets. We leave the extension to multi-antenna beamforming or antenna-pair selection for future work.

²This assumption suits the considered urban/indoor D2D scenario with rich scattering and mainly non-line-of-sight propagation. Without a dominant line-of-sight component, the received baseband channel is the sum of many random-phase multipath components, so each coefficient follows a zero-mean complex Gaussian distribution $g_{i,j} \sim \mathcal{CN}(0, \lambda_{i,j})$, where $\lambda_{i,j} = \mathbb{E}\{|g_{i,j}|^2\}$ is the average channel power gain. This Rayleigh fading model is a widely adopted baseline in D2D-enabled cellular networks [32], [36]–[38].

TABLE I
SUMMARY OF NOTATIONS

$g_{i,j}$	The channel coefficient between i and j , where $i \in \{A, D_t, W\}$, $j \in \{B, D_r, W\}$
$\hat{g}_{i,j}$	The perfectly known part of $g_{i,j}$
$\tilde{g}_{i,j}$	The uncertain part of $g_{i,j}$
$\rho_{i,j}$	The channel state information (CSI) uncertainty coefficient of channel $g_{i,j}$
$\lambda_{i,j}$	The mean of the channel gain $ g_{i,j} ^2$
σ_j^2	The noise variance at node j
Ψ^u, Ψ^o	The detection threshold at D_r
Ψ^{u*}, Ψ^{o*}	The optimal detection threshold at D_r
P_E	The detection error probability at D_r
P_E^*	The minimum detection error probability at D_r
$\bar{P}_E^*$	The average minimum detection error probability at D_r
P_{D_t}	The transmission power of D_t
$P_{D_t}^{\max}, P_{D_t}^{\min}$	The maximum and minimum transmission power of D_t
$P_{D_t}^{\text{fix}}$	The prescribed fixed transmission power of D_t in Case I
Q_d	The target QoS reliability of the suspicious D2D link
P_A	The transmission power of Alice
P_J	The transmission power of the Warden
P_J^{covert}	The transmission power at the Warden satisfying covertness constraint
Ω	The maximum transmission power of Alice
η	The maximum transmission power of the Warden
ϕ	The normalized residual self-interference coefficient at the Warden
$\text{SINR}_{D_r}^u, \text{SINR}_{D_r}^o$	The instantaneous signal-to-interference-plus-noise ratio at D_r
$\text{SINR}_W^u, \text{SINR}_W^o$	The instantaneous signal-to-interference-plus-noise ratio at the Warden
$\text{SINR}_B^u, \text{SINR}_B^o$	The instantaneous signal-to-interference-plus-noise ratio at the BS
$C_{D_r}^u, C_{D_r}^o$	The instantaneous channel capacity at D_r
C_W^u, C_W^o	The instantaneous channel capacity at the Warden
C_B^u, C_B^o	The instantaneous channel capacity at the BS
R_B, R_D	The minimum required transmission rates of the cellular and D2D links
X	The indicator function for the event of successful eavesdropping at the Warden
$\mathbb{S}[X]^u, \mathbb{S}[X]^o$	The eavesdropping non-outage probability of the Warden at D_t
$\mathbb{S}[X]_{\text{all}}^u, \mathbb{S}[X]_{\text{all}}^o$	The system eavesdropping non-outage probability for the network
$P_{c,\text{out}}^u, P_{c,\text{out}}^o$	The transmission outage probability of the cellular link
$P_{d,\text{out}}^u, P_{d,\text{out}}^o$	The transmission outage probability of the D2D link
ε	The predetermined threshold for the covertness requirement
β	The spectrum allocation ratio of cellular user Alice under the overlay mode
ϖ^u, ϖ^o	The normalized management overhead coefficient under two modes
$\mathbb{U}^u, \mathbb{U}^o$	The surveillance utility under the underlay and overlay modes
$U_{\min}$	The required minimum long-term average surveillance utility
P_{eff}	The long-term time-sharing fraction of the underlay mode
N_b	The total number of transmission blocks

block but vary independently across blocks³. Let $g_{i,j}$ denote the channel coefficient from transmitter $i \in \{A, D_t, W\}$ to receiver $j \in \{B, D_r, W\}$, where A, B, and W represent Alice, the BS, and the Warden, respectively. Under this model, the channel gain $|g_{i,j}|^2$ follows an exponential distribution with mean $\lambda_{i,j}$, whose probability density function (PDF) is given by $f_{|g_{i,j}|^2}(x) = \frac{1}{\lambda_{i,j}} \exp\left(-\frac{x}{\lambda_{i,j}}\right)$. The channel coefficients are denoted as follows: the communication links by $g_{A,B}$ and g_{D_t,D_r} , the eavesdropping link by $g_{D_t,W}$, the jamming link by g_{W,D_r} , the interference links by g_{A,D_r} , $g_{A,W}$, $g_{D_t,B}$, and $g_{W,B}$, and the self-interference at the Warden by $g_{W,W}$.

The suspicious transmitter D_t transmits with power P_{D_t} , where $0 \leq P_{D_t} \leq P_{D_t}^{\max}$. Alice transmits with power P_A ,

³The adopted quasi-static block-fading model captures block-level variations rather than continuous intra-block aging. Each coefficient $g_{i,j}$ remains fixed within a transmission block and varies independently across blocks, so over a long horizon the channel changes from block to block and the statistical analysis averages over these fading realizations. This differs from the time-varying channel-aging model in [39], where the channel matrix evolves across successive time indices within one sounding round under a first-order autoregressive process, and outdated CSI degrades the SINR and data rate. Extending the proposed covert surveillance framework to temporally correlated intra-block aging remains future work.

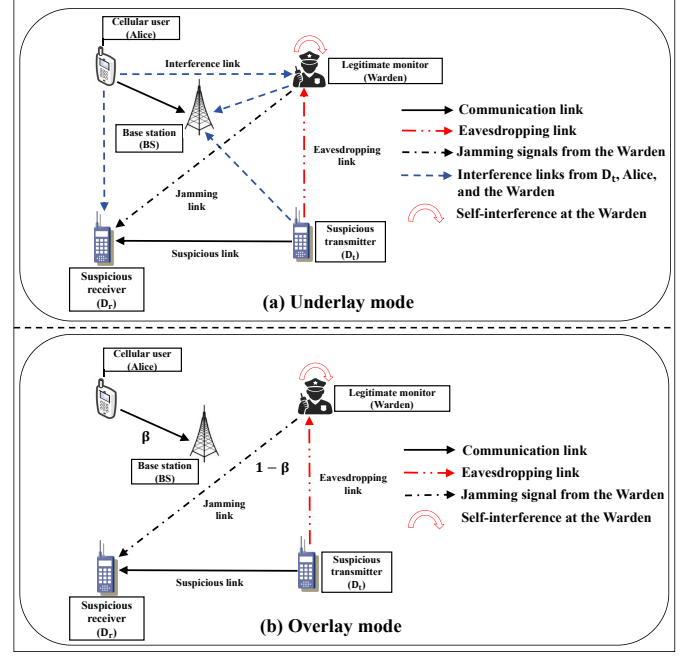


Fig. 1: A covert surveillance system model under two modes.

where $0 \leq P_A \leq \Omega$, while satisfying the uplink QoS requirement at the BS. The Warden simultaneously injects AN with power P_J , where $0 \leq P_J \leq \eta$. Here $P_{D_t}^{\max}$, Ω , and η denote the respective maximum transmit powers.

Under the underlay mode, we denote the signals received at the BS, Warden, and D_r during the i -th symbol interval by $y_B^u[i]$, $y_W^u[i]$, and $y_{D_r}^u[i]$, respectively. These signals are expressed as follows:

$$y_B^u[i] = \sqrt{P_A} g_{A,B} s_A[i] + \sqrt{P_{D_t}} g_{D_t,B} s_{D_t}[i] + \sqrt{P_J} g_{W,B} j_W[i] + n_B[i], \quad (1)$$

$$y_W^u[i] = \sqrt{P_A} g_{A,W} s_A[i] + \sqrt{P_{D_t}} g_{D_t,W} s_{D_t}[i] + \sqrt{\phi P_J} g_{W,W} j_W[i] + n_W[i], \quad (2)$$

and

$$y_{D_r}^u[i] = \sqrt{P_A} g_{A,D_r} s_A[i] + \sqrt{P_{D_t}} g_{D_t,D_r} s_{D_t}[i] + \sqrt{P_J} g_{W,D_r} j_W[i] + n_{D_r}[i]. \quad (3)$$

Similarly, under the overlay mode, let $y_B^o[i]$, $y_W^o[i]$ and $y_{D_r}^o[i]$ represent the received signals at the BS, Warden and D_r , respectively. They are formulated as follows:

$$y_B^o[i] = \sqrt{P_A} g_{A,B} s_A[i] + n_B[i], \quad (4)$$

$$y_W^o[i] = \sqrt{P_{D_t}} g_{D_t,W} s_{D_t}[i] + \sqrt{\phi P_J} g_{W,W} j_W[i] + n_W[i], \quad (5)$$

and

$$y_{D_r}^o[i] = \sqrt{P_{D_t}} g_{D_t,D_r} s_{D_t}[i] + \sqrt{P_J} g_{W,D_r} j_W[i] + n_{D_r}[i]. \quad (6)$$

In this paper, we consider an infinite number of channel uses, i.e., $n \rightarrow \infty$. Let $i \in \{1, 2, \dots, n\}$ denote the index of each transmitted symbol. The random variables $s_A[i]$, $s_{D_t}[i]$, and $j_W[i]$ represent the signals transmitted by Alice, D_t , and the Warden, respectively. They satisfy the following conditions: $\mathbb{E}[|s_A[i]|^2] = 1$, $\mathbb{E}[|s_{D_t}[i]|^2] = 1$, and $\mathbb{E}[|j_W[i]|^2] = 1$. Here, $\mathbb{E}[\cdot]$ denotes the expectation operator. As n becomes arbitrarily large, the average power of each transmitted symbol converges to its expected value. The

parameter ϕ denotes the normalized residual self-interference coefficient at the Warden, with $\phi \in [0, 1]^4$. In the considered system, additive white Gaussian noise is assumed at the BS and D_r . Specifically, the noise at the BS, denoted by $n_B[i]$, is the Gaussian random variable with zero mean and variance σ_B^2 (i.e., $n_B[i] \sim \mathcal{CN}(0, \sigma_B^2)$). Similarly, the noise at the Warden, denoted by $n_W[i]$, has variance σ_W^2 (i.e., $n_W[i] \sim \mathcal{CN}(0, \sigma_W^2)$). The noise at D_r , represented by $n_{D_r}[i]$, is characterized by a variance of $\sigma_{D_r}^2$ (i.e., $n_{D_r}[i] \sim \mathcal{CN}(0, \sigma_{D_r}^2)$). The total bandwidth of the system spectrum is W_{bw} MHz. Without loss of generality, we assume $W_{bw} = 10$ throughout this paper [47].

D_t employs a minimum mean square error (MMSE) estimator to obtain the time-varying CSI [48]. Since imperfect channel estimation is common, the D2D channel between D_t and D_r inevitably suffers from estimation errors. Specifically, the actual channel coefficient g_{D_t, D_r} is modeled as

$$g_{D_t, D_r} = \hat{g}_{D_t, D_r} + \tilde{g}_{D_t, D_r}, \quad (7)$$

where $\hat{g}_{D_t, D_r}$ denotes the estimation of channel coefficient and $\tilde{g}_{D_t, D_r}$ represents the corresponding estimation error. Both $\hat{g}_{D_t, D_r}$ and $\tilde{g}_{D_t, D_r}$ are assumed to be zero-mean complex Gaussian random variables, with variances $(1 - \rho_{D_t, D_r}) \lambda_{D_t, D_r}$ and $\rho_{D_t, D_r} \lambda_{D_t, D_r}$, respectively. The parameter $\rho_{D_t, D_r} \in [0, 1]$ denotes the correlation coefficient between the actual channel gain and its estimation error [49], [50].

The interfering link varies over time because of Doppler shifts and multipath propagation, which introduces CSI uncertainty. For covert jamming and eavesdropping, the Warden can also transmit from a concealed position, so its signal to D_r undergoes richer multipath. D_r therefore struggles to obtain perfect instantaneous CSI, and its channel estimation accuracy is inherently limited. We thus model the interference channel as the sum of a known component and an uncertainty component, i.e.,

$$g_{W, D_r} = \hat{g}_{W, D_r} + \tilde{g}_{W, D_r}, \quad (8)$$

where $\hat{g}_{W, D_r}$ and $\tilde{g}_{W, D_r}$ are independent zero-mean complex Gaussian random variables with variances $(1 - \rho_{W, D_r}) \lambda_{W, D_r}$ and $\rho_{W, D_r} \lambda_{W, D_r}$, respectively. The parameter $\rho_{W, D_r} \in [0, 1]$ denotes the correlation coefficient between g_{W, D_r} and $\tilde{g}_{W, D_r}$.

C. Hypothesis Testing

D_r must decide whether the Warden transmits AN to jam it based on the received signal. This can be formulated as a binary hypothesis test: $\mathcal{H}_0$ denotes no AN transmission, and $\mathcal{H}_1$ denotes AN transmission. We first consider the underlay mode.

⁴Here, ϕ is an effective normalized residual self-interference coefficient. In practical full-duplex transceivers, self-interference arises from transmit-to-receive leakage due to antenna coupling, circulator leakage, and power amplifier nonlinearity. It is suppressed in stages, combining antenna-domain passive isolation, radio-frequency analog cancellation, and digital baseband cancellation [40]–[43]. In our model, $g_{W, W}$ captures the residual loop channel after passive suppression, and $\phi \in [0, 1]$ abstracts the remaining normalized residual power ratio after analog and digital cancellation. This scalar model follows common practice in full-duplex covert communication and proactive eavesdropping studies and keeps the closed-form detection error probability and outage probability derivations tractable [18], [32], [44]–[46].

1) Underlay Mode: Under the two hypotheses, the signal received at D_r can be expressed as:

$$y_{D_r}^u[i] = \begin{cases} \sqrt{P_A} g_{A, D_r} s_A[i] + \sqrt{P_{D_t}} g_{D_t, D_r} s_{D_t}[i] + n_{D_r}[i], & \mathcal{H}_0, \\ \sqrt{P_A} g_{A, D_r} s_A[i] + \sqrt{P_{D_t}} g_{D_t, D_r} s_{D_t}[i] + \sqrt{P_J} g_{W, D_r} j_W[i] + n_{D_r}[i], & \mathcal{H}_1, \end{cases} \quad (9)$$

since D_r 's received vector $\mathbf{y}_{D_r}^u = [y_{D_r}^u(1), \dots, y_{D_r}^u(n)]$ consists of independent and identically distributed (i.i.d.) components, each symbol $y_{D_r}^u[i]$ is a zero-mean complex Gaussian random variable. Consequently, the entire vector is composed of i.i.d. zero-mean complex Gaussian random variables.

Since the i.i.d. property of the received signal at D_r , each symbol follows the distribution:

$$y_{D_r}^u[i] \sim \begin{cases} \mathcal{CN}(0, P_A |g_{A, D_r}|^2 + P_{D_t} |g_{D_t, D_r}|^2 + \sigma_{D_r}^2), & \mathcal{H}_0, \\ \mathcal{CN}(0, P_A |g_{A, D_r}|^2 + P_{D_t} |g_{D_t, D_r}|^2 + P_J |g_{W, D_r}|^2 + \sigma_{D_r}^2), & \mathcal{H}_1, \end{cases} \quad (10)$$

where $\mathcal{CN}(0, \sigma^2)$ denotes a circularly symmetric complex Gaussian distribution with zero mean and variance σ^2 . The total received power $\sum_{i=1}^n |y_{D_r}^u(i)|^2$ is used as a sufficient statistic for the hypothesis test performed at D_r . In particular, we define the normalized received power as

$$Y_{D_r}^u = \frac{1}{n} \sum_{i=1}^n |y_{D_r}^u(i)|^2, \quad (11)$$

which serves as a sufficient statistic [51].

We consider an infinite number of received signals at D_r in each transmission block, i.e., $n \rightarrow \infty$, and then the average received power $Y_{D_r}^u$ at D_r under the underlay mode is given by

$$Y_{D_r}^u = \begin{cases} P_A |g_{A, D_r}|^2 + P_{D_t} |g_{D_t, D_r}|^2 + \sigma_{D_r}^2, & \mathcal{H}_0, \\ P_A |g_{A, D_r}|^2 + P_{D_t} |g_{D_t, D_r}|^2 + P_J |g_{W, D_r}|^2 + \sigma_{D_r}^2, & \mathcal{H}_1. \end{cases} \quad (12)$$

Based on the orthogonality principle of MMSE estimation, the uncertainty in the suspect and interference links implies that the mean square value of the channel gain from D_t to D_r can be decomposed as $\mathbb{E}(|g_{D_t, D_r}|^2) = \mathbb{E}(|\hat{g}_{D_t, D_r}|^2) + \mathbb{E}(|\tilde{g}_{D_t, D_r}|^2)$, and similarly, the mean square value of the channel gain from W to D_r satisfies $\mathbb{E}(|g_{W, D_r}|^2) = \mathbb{E}(|\hat{g}_{W, D_r}|^2) + \mathbb{E}(|\tilde{g}_{W, D_r}|^2)$ [49], [50]. This indicates that the mean square value of the actual channel gain is determined by both the estimated channel and the estimation error.

Therefore, the average received power at D_r under the underlay mode can be expressed as

$$Y_{D_r}^u = \begin{cases} P_A |g_{A, D_r}|^2 + P_{D_t} |\hat{g}_{D_t, D_r}|^2 + P_{D_t} |\tilde{g}_{D_t, D_r}|^2 + \sigma_{D_r}^2, & \mathcal{H}_0, \\ P_A |g_{A, D_r}|^2 + P_{D_t} |\hat{g}_{D_t, D_r}|^2 + P_{D_t} |\tilde{g}_{D_t, D_r}|^2 + P_J |\hat{g}_{W, D_r}|^2 + P_J |\tilde{g}_{W, D_r}|^2 + \sigma_{D_r}^2, & \mathcal{H}_1. \end{cases} \quad (13)$$

Based on the above discussion, D_r performs threshold test following the decision rule [52]: if $Y_{D_r}^u$ is greater than the predefined threshold Ψ^u , the decision $\mathcal{D}_1$ is made (accepting $\mathcal{H}_1$). Otherwise, if $Y_{D_r}^u$ is less than the predefined threshold Ψ^u , the decision $\mathcal{D}_0$ is made (accepting $\mathcal{H}_0$). Accordingly, based on the threshold test and the average received power $Y_{D_r}^u$, the error probabilities are defined as $P_{FA}^u = \Pr\{Y_{D_r}^u > \Psi^u \mid \mathcal{H}_0\}$ and $P_{MD}^u = \Pr\{Y_{D_r}^u < \Psi^u \mid \mathcal{H}_1\}$, where P_{FA}^u and P_{MD}^u denote the false alarm and missed detection probabilities, respectively.

Then, the detection error probability (DEP) is defined as the sum of these two error probabilities, i.e.,

$$P_E^u = P_{FA}^u + P_{MD}^u, \quad (14)$$

where P_E^u denotes the DEP under the underlay mode. $P_E^u = 0$ indicates perfect detection of AN, while $P_E^u = 1$ corresponds to complete detection failure.

The objective of D_r is to accurately detect AN by determining the optimal threshold Ψ^{u*} that minimizes the DEP P_E^{u*} , based on the CSI of the suspicious and jamming links. Since the Warden cannot know D_r 's detection threshold Ψ^u , a conservative worst-case analysis assumes that D_r adopts the optimal threshold minimizing its DEP.

2) Overlay Mode:

Under the overlay mode, D_r performs a hypothesis test using the average received power $Y_{D_r}^o$ as the test statistic to detect the presence of a jamming signal. Leveraging the orthogonality of channel uncertainties in the suspicious and jamming links, the average received power at D_r can be expressed as

$$Y_{D_r}^o = \begin{cases} P_{D_t} |\hat{g}_{D_t, D_r}|^2 + P_{D_t} |\hat{g}_{D_t, D_r}|^2 + \sigma_{D_r}^2, & \mathcal{H}_0, \\ P_{D_t} |\hat{g}_{D_t, D_r}|^2 + P_{D_t} |\hat{g}_{D_t, D_r}|^2 + P_J |\hat{g}_{W, D_r}|^2 + P_J |\hat{g}_{W, D_r}|^2 + \sigma_{D_r}^2, & \mathcal{H}_1. \end{cases} \quad (15)$$

Similar to the underlay mode, based on the threshold test and the average received power $Y_{D_r}^o$ under the overlay mode, the error probabilities are defined as $P_{FA}^o = \Pr\{Y_{D_r}^o > \Psi^o \mid \mathcal{H}_0\}$ and $P_{MD}^o = \Pr\{Y_{D_r}^o < \Psi^o \mid \mathcal{H}_1\}$, where P_{FA}^o and P_{MD}^o denote the false alarm and missed detection probabilities, respectively.

Thus, the DEP is given by

$$P_E^o = P_{FA}^o + P_{MD}^o. \quad (16)$$

This metric quantifies the detection performance of D_r and is closely related to the threshold Ψ^o . In the overlay mode, we consider a worst-case scenario in which D_r operates with optimal detection capability for AN. Under this assumption, the DEP is minimized to evaluate the covert injection performance. The analysis of hidden AN injection under both modes is presented in Section IV.

D. Channel Capacity

1) Underlay Mode:

Consider the uplink transmission from Alice to BS under the underlay mode. Let SINR_B^u , $\text{SINR}_{D_r}^u$ and SINR_W^u denote the instantaneous SINR at the BS, D_r and the Warden, respectively. Since the D2D pair shares the same spectrum with Alice and the BS, D_r experiences interference from both the Warden and Alice, while the Warden suffers from interference from Alice as well as self-interference. Following prior work [49], [50], we model the channel uncertainty as additive noise. Then, the SINRs at the BS, D_r , and the Warden are given by

$$\text{SINR}_B^u = \frac{P_A |g_{A,B}|^2}{P_{D_t} |g_{D_t,B}|^2 + P_J |g_{W,B}|^2 + \sigma_B^2}, \quad (17)$$

$$\text{SINR}_{D_r}^u = \frac{P_{D_t} |\hat{g}_{D_t, D_r}|^2}{P_{D_t} |\hat{g}_{D_t, D_r}|^2 + P_A |g_{A, D_r}|^2 + P_J |g_{W, D_r}|^2 + \sigma_{D_r}^2}, \quad (18)$$

and

$$\text{SINR}_W^u = \frac{P_{D_t} |g_{D_t, W}|^2}{P_A |g_{A, W}|^2 + \phi P_J |g_{W, W}|^2 + \sigma_W^2}. \quad (19)$$

Therefore, the instantaneous channel capacity C_B^u , $C_{D_r}^u$ and C_W^u at the BS, D_r and the Warden are given by

$$C_B^u = W_{bw} \log_2 (1 + \text{SINR}_B^u), \quad (20)$$

$$C_{D_r}^u = W_{bw} \log_2 (1 + \text{SINR}_{D_r}^u), \quad (21)$$

and

$$C_W^u = W_{bw} \log_2 (1 + \text{SINR}_W^u). \quad (22)$$

2) Overlay Mode: Let SINR_B^o , $\text{SINR}_{D_r}^o$ and SINR_W^o denote the SINR at the BS, D_r and the Warden, respectively, under the overlay mode. Then,

$$\text{SINR}_B^o = \frac{P_A |g_{A,B}|^2}{\sigma_B^2}, \quad (23)$$

$$\text{SINR}_{D_r}^o = \frac{P_{D_t} |\hat{g}_{D_t, D_r}|^2}{P_{D_t} |\hat{g}_{D_t, D_r}|^2 + P_J |g_{W, D_r}|^2 + \sigma_{D_r}^2}, \quad (24)$$

and

$$\text{SINR}_W^o = \frac{P_{D_t} |g_{D_t, W}|^2}{\phi P_J |g_{W, W}|^2 + \sigma_W^2}. \quad (25)$$

Due to spectrum allocation, the D2D link and the cellular link are orthogonal in frequency. Thus, the instantaneous channel capacities C_B^o , $C_{D_r}^o$ and C_W^o at the BS, D_r and Warden under the overlay mode can be expressed as

$$C_B^o = \beta W_{bw} \log_2 (1 + \text{SINR}_B^o), \quad (26)$$

$$C_{D_r}^o = (1 - \beta) W_{bw} \log_2 (1 + \text{SINR}_{D_r}^o), \quad (27)$$

and

$$C_W^o = (1 - \beta) W_{bw} \log_2 (1 + \text{SINR}_W^o). \quad (28)$$

IV. DETECTION PERFORMANCE

This section investigates the detection performance of the suspicious receiver under channel uncertainties, where D_t ceases transmission once D_r detects jamming from the Warden. Specifically, we characterize the false alarm and missed detection probabilities, derive the optimal detection thresholds and corresponding DEPs, and obtain the average minimum DEP for both underlay and overlay modes.

A. Probabilities of False Alarm and Missed Detection

We denote by P_{FA}^u and P_{MD}^u the false alarm and missed detection probabilities under underlay mode, and by P_{FA}^o and P_{MD}^o their counterparts under overlay mode. The corresponding detection thresholds are Ψ^u and Ψ^o . We obtain these two types of probabilities in the following theorem.

Theorem 1. *The probabilities of false alarm and missed detection under the underlay and overlay modes are given by*

$$P_{FA}^u = \begin{cases} 1, & \Psi^u \leq \Gamma_0, \\ \exp\left(-\frac{T_1}{\rho_{D_t, D_r} P_{D_t} \lambda_{D_t, D_r}}\right), & \Psi^u > \Gamma_0, \end{cases} \quad (29)$$

where $\Gamma_0 = P_{D_t} |\hat{g}_{D_t, D_r}|^2 + P_A |g_{A, D_r}|^2 + \sigma_{D_r}^2$ and $T_1 = \Psi^u - \Gamma_0$. We further determine the probability of missed detection as

$$P_{MD}^u = \begin{cases} 0, & \Psi^u \leq \Gamma_1, \\ \frac{\rho_{D_t, D_r} P_{D_t} \lambda_{D_t, D_r} \left(1 - \exp\left(-\frac{T_2}{\rho_{D_t, D_r} P_{D_t} \lambda_{D_t, D_r}}\right)\right)}{\rho_{D_t, D_r} P_{D_t} \lambda_{D_t, D_r} - \rho_{W, D_r} P_J \lambda_{W, D_r}}, & \Psi^u > \Gamma_1, \\ -\frac{\rho_{W, D_r} P_J \lambda_{W, D_r} \left(1 - \exp\left(-\frac{T_2}{\rho_{W, D_r} P_J \lambda_{W, D_r}}\right)\right)}{\rho_{D_t, D_r} P_{D_t} \lambda_{D_t, D_r} - \rho_{W, D_r} P_J \lambda_{W, D_r}}, & \Psi^u > \Gamma_1, \end{cases} \quad (30)$$

where $\Gamma_1 = P_{D_t} |\hat{g}_{D_t, D_r}|^2 + P_J |\hat{g}_{W, D_r}|^2 + P_A |g_{A, D_r}|^2 + \sigma_{D_r}^2$ and $T_2 = \Psi^u - \Gamma_1$. The expression in (30) is derived for the general non-degenerate case $\rho_{D_t, D_r} P_{D_t} \lambda_{D_t, D_r} \neq \rho_{W, D_r} P_J \lambda_{W, D_r}$. When $\rho_{D_t, D_r} P_{D_t} \lambda_{D_t, D_r} = \rho_{W, D_r} P_J \lambda_{W, D_r}$, the corresponding special case can be obtained by taking the limit of (30), which yields $P_{MD}^u = 1 - \exp(-T_2/(\rho_{D_t, D_r} P_{D_t} \lambda_{D_t, D_r}))(1 + T_2/(\rho_{D_t, D_r} P_{D_t} \lambda_{D_t, D_r}))$ for $\Psi^u > \Gamma_1$.

Proof. We provide the derivations of P_{FA}^u and P_{MD}^u in Appendix A. Similarly, under the overlay mode, the derivation of P_{FA}^o and P_{MD}^o follows the same procedure as that of P_{FA}^u and P_{MD}^u , and is therefore omitted here for brevity.

B. Optimal Detection Thresholds and Minimum Detection Error Probabilities

We denote the optimal detection thresholds at D_r under the underlay and overlay modes as Ψ^{u*} and Ψ^{o*} , respectively. The optimal thresholds and the corresponding minimum DEPs are given in the following theorem.

Theorem 2. The optimal detection thresholds at D_r under the underlay and overlay modes are expressed as

$$\Psi^{u*} = P_{D_t} |\hat{g}_{D_t, D_r}|^2 + P_J |\hat{g}_{W, D_r}|^2 + P_A |g_{A, D_r}|^2 + \theta + \sigma_{D_r}^2, \quad (31)$$

and

$$\Psi^{o*} = P_{D_t} |\hat{g}_{D_t, D_r}|^2 + P_J |\hat{g}_{W, D_r}|^2 + \theta + \sigma_{D_r}^2. \quad (32)$$

Given these optimal thresholds, the minimum DEPs under these two modes are identical and denoted by P_E^* . Then,

$$P_E^* = P_{FA}^{u*} = P_{FA}^{o*} = 1 + \exp\left(-\frac{P_J |\hat{g}_{W, D_r}|^2 + \theta}{\rho_{D_t, D_r} P_{D_t} \lambda_{D_t, D_r}}\right) - \frac{\rho_{D_t, D_r} P_{D_t} \lambda_{D_t, D_r} \exp\left(-\frac{\theta}{\rho_{D_t, D_r} P_{D_t} \lambda_{D_t, D_r}}\right) + \rho_{W, D_r} P_J \lambda_{W, D_r} \exp\left(-\frac{\theta}{\rho_{W, D_r} P_J \lambda_{W, D_r}}\right)}{\rho_{D_t, D_r} P_{D_t} \lambda_{D_t, D_r} - \rho_{W, D_r} P_J \lambda_{W, D_r}}, \quad (33)$$

$$\text{where } \theta = \frac{\rho_{D_t, D_r} P_{D_t} \lambda_{D_t, D_r} \rho_{W, D_r} P_J \lambda_{W, D_r}}{\rho_{W, D_r} P_J \lambda_{W, D_r} - \rho_{D_t, D_r} P_{D_t} \lambda_{D_t, D_r}} \times \ln\left(1 - \left(1 - \frac{\rho_{W, D_r} P_J \lambda_{W, D_r}}{\rho_{D_t, D_r} P_{D_t} \lambda_{D_t, D_r}}\right) \exp\left(-\frac{P_J |\hat{g}_{W, D_r}|^2}{\rho_{D_t, D_r} P_{D_t} \lambda_{D_t, D_r}}\right)\right).$$

Proof. The detailed proof is provided in Appendix B.

According to Theorem 2, the minimum DEP at D_r is identical for both underlay and overlay modes. This follows from the worst-case scenario for the Warden, where D_r is assumed to have optimal detection capability.

We assume D_r knows the instantaneous channel gain $|g_{A, D_r}|^2$ exactly, so Alice's signal does not affect D_r 's detection of P_J . Unlike the suspicious D2D pair and the concealed Warden, Alice is a legitimate cellular user scheduled by the

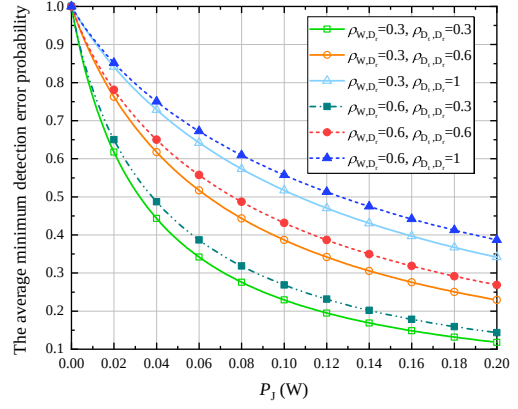


Fig. 2: The average minimum DEP $\overline{P_E^*}$ versus P_J under various ρ_{D_t, D_r} and ρ_{W, D_r} .

BS, so its channel is accurately estimated from uplink pilots. This gives D_r the strongest detection capability and thus the worst case for the Warden. If P_J stays covert under this optimal detection, it stays covert under weaker conditions. When the Alice- D_r link is also imperfect, the extra uncertainty weakens D_r 's detection and eases covert injection, as Section IV-C verifies. Covert communication studies commonly adopt this worst-case setting [19], [28], [32], [44], [50], which serves as a stress test for the proposed scheme.

Theorem 3. The average minimum DEP $\overline{P_E^*}$ at D_r is expressed as

$$\overline{P_E^*} = \int_0^\infty \left(1 + \exp\left(-\frac{x + \theta(x)}{\rho_{D_t, D_r} P_{D_t} \lambda_{D_t, D_r}}\right) - \frac{\rho_{D_t, D_r} P_{D_t} \lambda_{D_t, D_r} \exp\left(-\frac{\theta(x)}{\rho_{D_t, D_r} P_{D_t} \lambda_{D_t, D_r}}\right) + \rho_{W, D_r} P_J \lambda_{W, D_r} \exp\left(-\frac{\theta(x)}{\rho_{W, D_r} P_J \lambda_{W, D_r}}\right)}{\rho_{D_t, D_r} P_{D_t} \lambda_{D_t, D_r} - \rho_{W, D_r} P_J \lambda_{W, D_r}}\right) \times \frac{1}{(1 - \rho_{W, D_r}) P_J \lambda_{W, D_r}} \exp\left(-\frac{x}{(1 - \rho_{W, D_r}) P_J \lambda_{W, D_r}}\right) dx. \quad (34)$$

Proof. In (33), the minimum DEP P_E^* is a function of the random variable $P_J |\hat{g}_{W, D_r}|^2$ and denoted by $f_{P_J |\hat{g}_{W, D_r}|^2}(x)$. Then,

$$f_{P_J |\hat{g}_{W, D_r}|^2}(x) = \frac{1}{(1 - \rho_{W, D_r}) P_J \lambda_{W, D_r}} \exp\left(-\frac{x}{(1 - \rho_{W, D_r}) P_J \lambda_{W, D_r}}\right). \quad (35)$$

The average minimum DEP, denoted by $\overline{P_E^*}$. Therefore, the average minimum DEP is calculated as

$$\overline{P_E^*} = \int_0^\infty P_E^*(x) f_{P_J |\hat{g}_{W, D_r}|^2}(x) dx. \quad (36)$$

By substituting (33) and (35) into (36), we obtain (34).

To ensure covert AN transmission, the Warden must satisfy the covertness constraint $\overline{P_E^*} \geq 1 - \varepsilon$ for a given $\varepsilon \geq 0$.

Fig. 2 shows that the average minimum DEP $\overline{P_E^*}$ decreases with increasing jamming power P_J , as higher P_J improves D_r 's detection of the jamming signal, reducing the chance of successful covert transmission. The figure also illustrates the effects of the CSI uncertainty coefficients. Over the considered range of P_J , $\overline{P_E^*}$ rises with both ρ_{D_t, D_r} and ρ_{W, D_r} , so larger uncertainty on either link makes the jamming harder to detect at D_r and promotes covert transmission.

Under the same jamming power P_J , a larger ρ_{D_t, D_r} yields a higher $\overline{P_E^*}$. When $\rho_{D_t, D_r} = 1$ (fully uncertain suspicious

link), $\overline{P_E^*}$ is much higher than those for $\rho_{D_t, D_r} = 0.3$ or 0.6 , showing that the suspicious link uncertainty weakens D_r 's detection. A larger ρ_{W, D_r} raises $\overline{P_E^*}$ in the same direction and also enhances covert transmission, but its effect is weaker than that of ρ_{D_t, D_r} .

Analysis of the average minimum DEPs shows that uncertainty in the suspicious link affects D_r 's detection more than that in the jamming link. As channel uncertainty impacts D_r 's ability to detect P_J , which in turn shapes the Warden's transmit strategy, covert surveillance performance can be controlled by adjusting P_J .

C. Robustness Discussion on Imperfectly Known Alice- D_r CSI

We now test the robustness of the proposed scheme when D_r knows the Alice- D_r channel imperfectly. All quantities in this case carry the superscript $\dagger$. We model the coefficient as $g_{A, D_r} = \hat{g}_{A, D_r} + \tilde{g}_{A, D_r}$, with estimate $\hat{g}_{A, D_r}$ and error $\tilde{g}_{A, D_r}$. Both are independent zero-mean complex Gaussian random variables with variances $(1 - \rho_{A, D_r})\lambda_{A, D_r}$ and $\rho_{A, D_r}\lambda_{A, D_r}$, where $\rho_{A, D_r} \in [0, 1]$ is the CSI uncertainty coefficient. Setting $\rho_{A, D_r} = 0$ recovers the perfect-CSI case above.

Following $U_D = P_{D_t}|\hat{g}_{D_t, D_r}|^2$ and $U_W = P_J|\hat{g}_{W, D_r}|^2$, we define $U_A = P_A|\hat{g}_{A, D_r}|^2$. It is independent of U_D and U_W and follows an exponential distribution with mean $\rho_{A, D_r}P_A\lambda_{A, D_r}$. Thus U_A appears under both hypotheses and acts as background uncertainty, not useful detection information. Appendix C gives the received statistic with the false alarm and missed detection probabilities.

Let $\Psi^{\dagger}$ be the detection threshold, and define $\Gamma_0^{\dagger} = P_A|\hat{g}_{A, D_r}|^2 + P_{D_t}|\hat{g}_{D_t, D_r}|^2 + \sigma_{D_r}^2$ and $\Gamma_1^{\dagger} = \Gamma_0^{\dagger} + P_J|\hat{g}_{W, D_r}|^2$. The DEP equals one for $\Psi^{\dagger} \leq \Gamma_0^{\dagger}$ and decreases beyond it, so the minimum lies in $\Psi^{\dagger} > \Gamma_1^{\dagger}$. With $x = P_J|\hat{g}_{W, D_r}|^2$ and $\theta^{\dagger} = \Psi^{\dagger} - \Gamma_1^{\dagger} \geq 0$, the DEP in this region is $P_E^{\dagger}(\theta^{\dagger}; x) = 1 - F_{U_A+U_D}(\theta^{\dagger} + x) + F_{U_A+U_D+U_W}(\theta^{\dagger})$, where $F_{U_A+U_D}(\cdot)$ and $F_{U_A+U_D+U_W}(\cdot)$ are the cumulative distribution functions of $U_A + U_D$ and $U_A + U_D + U_W$ derived in Appendix C.

The optimal threshold is $\Psi^{u\dagger*} = \Gamma_1^{\dagger} + \theta^{\dagger*}$, where $\theta^{\dagger*}$ minimizes the DEP. An interior optimum satisfies $f_{U_A+U_D+U_W}(\theta^{\dagger*}) = f_{U_A+U_D}(\theta^{\dagger*} + x)$. Unlike the perfect-CSI case, this optimum is implicit and admits no closed form. The minimum DEP is

$$P_E^{u\dagger*}(x) = 1 - F_{U_A+U_D}(\theta^{\dagger*} + x) + F_{U_A+U_D+U_W}(\theta^{\dagger*}). \quad (37)$$

Since x is random, the average minimum DEP is $\overline{P_E^{u\dagger*}} = \int_0^\infty P_E^{u\dagger*}(x) f_{P_J|\hat{g}_{W, D_r}|^2}(x) dx$. For $\rho_{A, D_r} = 0$, $U_A = 0$ and the model reduces to the perfect-CSI case. For $\rho_{A, D_r} > 0$, U_A adds background uncertainty that weakens D_r 's detection of P_J .

Fig. 3 shows this effect on the average minimum DEP. In Fig. 3(a), $\overline{P_E^{u\dagger*}}$ grows with ρ_{A, D_r} , since a larger uncertainty strengthens $U_A = P_A|\tilde{g}_{A, D_r}|^2$ and makes the Warden's AN harder to detect. Fig. 3(b) shows that the perfectly known case yields the lowest $\overline{P_E^{u\dagger*}}$, whereas imperfect CSI raises it. This confirms that perfect Alice- D_r CSI is a conservative worst-case benchmark for the covertness of the proposed scheme.

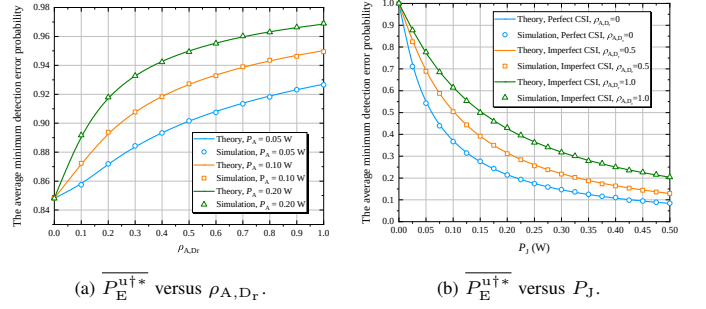


Fig. 3: Impact of imperfect Alice- D_r CSI on the average minimum detection error probability.

Remark 1. This interpretation extends to a multi-cellular-user underlay scenario with K co-channel cellular users $\mathcal{A} = \{A_1, \dots, A_K\}$. With perfect A_k - D_r CSI, D_r knows the aggregate cellular user power $\sum_{k=1}^K P_{A_k} |g_{A_k, D_r}|^2$ and adapts its detection threshold to $\Psi^{u, K*} = P_{D_t} |\hat{g}_{D_t, D_r}|^2 + P_J |\hat{g}_{W, D_r}|^2 + \sum_{k=1}^K P_{A_k} |g_{A_k, D_r}|^2 + \theta + \sigma_{D_r}^2$. Under imperfect CSI, the unknown terms form an aggregate uncertainty $U_A^K = \sum_{k=1}^K P_{A_k} |\tilde{g}_{A_k, D_r}|^2$, which appears under both hypotheses and adds only background uncertainty at D_r , weakening its AN detection.

V. SURVEILLANCE PERFORMANCE UNDER THE UNDERLAY MODE

In this section, we develop a theoretical model for Warden's surveillance performance based on the system eavesdropping non-outage probability, which accounts for Warden's eavesdropping and the communication non-outage probabilities of both the cellular and D2D links. We then formulate an optimization problem to maximize this metric by optimizing the transmit powers of Warden and Alice.

A. System Eavesdropping Non-Outage Probability Modeling

To evaluate system security, we define the system eavesdropping non-outage probability $\mathbb{S}[X]_{\text{all}}^u$, as the product of Warden's eavesdropping non-outage probability and the non-outage probabilities of the cellular and suspicious D2D links. This metric can be expressed as

$$\mathbb{S}[X]_{\text{all}}^u = \mathbb{S}[X]^u (1 - P_{c, \text{out}}^u) (1 - P_{d, \text{out}}^u), \quad (38)$$

where $\mathbb{S}[X]^u$ denotes the eavesdropping non-outage probability of Warden at D_t , with X representing the event that Warden successfully performs eavesdropping, which can be expressed as

$$X = \begin{cases} 1, & \text{if } C_W \geq C_{D_r}, \\ 0, & \text{otherwise,} \end{cases} \quad (39)$$

where $X = 1$ denotes the eavesdropping non-outage event in which Warden successfully decodes the message, whereas $X = 0$ corresponds to the outage event where decoding fails [11]. Then, $\mathbb{S}[X]^u$ can be expressed as

$$\mathbb{S}[X]^u = \Pr\{C_W^u \geq C_{D_r}^u\} = \Pr\{\text{SINR}_W^u \geq \text{SINR}_{D_r}^u\}. \quad (40)$$

The outage probability is the probability that the instantaneous channel capacity falls below a threshold of transmission

rate, resulting in a decoding failure. We use $C_{D_r}^u$ and C_B^u to represent the instantaneous channel capacities of D2D link and cellular links, respectively. R_D and R_B are the corresponding thresholds of transmission rates for these two links. Thus, the outage probabilities of cellular and D2D links under the underlay mode are $P_{c,out}^u = \Pr\{C_B^u < R_B\}$ and $P_{d,out}^u = \Pr\{C_{D_r}^u < R_D\}$, with non-outage probabilities $(1 - P_{c,out}^u)$ and $(1 - P_{d,out}^u)$, respectively. We further obtain their expressions of $\mathbb{S}[X]^u$, $P_{c,out}^u$, and $P_{d,out}^u$ in Theorem 4.

Theorem 4. *Under the underlay mode, the eavesdropping non-outage probability $\mathbb{S}[X]^u$, the transmission outage probability $P_{c,out}^u$ of the cellular link and $P_{d,out}^u$ of the D2D link are given by*

$$\begin{aligned} \mathbb{S}[X]^u &= \int_0^\infty \left(1 - \exp\left(-\frac{\sigma_{D_r}^2 x}{(1 - \rho_{D_t,D_r})P_{D_t}\lambda_{D_t,D_r}}\right) \right. \\ &\quad \times \frac{(1 - \rho_{D_t,D_r})P_{D_t}\lambda_{D_t,D_r}}{(1 - \rho_{D_t,D_r})P_{D_t}\lambda_{D_t,D_r} + \rho_{D_t,D_r}P_{D_t}\lambda_{D_t,D_r}x} \\ &\quad \times \frac{(1 - \rho_{D_t,D_r})P_{D_t}\lambda_{D_t,D_r}}{(1 - \rho_{D_t,D_r})P_{D_t}\lambda_{D_t,D_r} + P_A\lambda_{A,D_r}x} \\ &\quad \times \frac{(1 - \rho_{D_t,D_r})P_{D_t}\lambda_{D_t,D_r}}{(1 - \rho_{D_t,D_r})P_{D_t}\lambda_{D_t,D_r} + P_J\lambda_{W,D_r}x} \Bigg) \\ &\quad \times \left(\frac{\phi P_J \lambda_{W,W} \exp\left(-\frac{\sigma_W^2}{P_{D_t}\lambda_{D_t,W}}x\right)}{P_{D_t}\lambda_{D_t,W} \left(1 + \frac{P_A\lambda_{A,W}x}{P_{D_t}\lambda_{D_t,W}}\right) \left(1 + \frac{\phi P_J \lambda_{W,W}x}{P_{D_t}\lambda_{D_t,W}}\right)^2} \right. \\ &\quad + \frac{P_A\lambda_{A,W} \exp\left(-\frac{\sigma_W^2}{P_{D_t}\lambda_{D_t,W}}x\right)}{P_{D_t}\lambda_{D_t,W} \left(1 + \frac{P_A\lambda_{A,W}x}{P_{D_t}\lambda_{D_t,W}}\right)^2 \left(1 + \frac{\phi P_J \lambda_{W,W}x}{P_{D_t}\lambda_{D_t,W}}\right)} \\ &\quad \left. + \frac{\exp\left(-\frac{\sigma_W^2}{P_{D_t}\lambda_{D_t,W}}x\right) \sigma_W^2}{P_{D_t}\lambda_{D_t,W} \left(1 + \frac{P_A\lambda_{A,W}x}{P_{D_t}\lambda_{D_t,W}}\right) \left(1 + \frac{\phi P_J \lambda_{W,W}x}{P_{D_t}\lambda_{D_t,W}}\right)} \right) dx, \\ P_{c,out}^u &= 1 - \frac{\lambda_{A,B}^2 \exp\left(-\frac{\gamma \sigma_B^2}{\lambda_{A,B}}\right)}{(\lambda_{A,B} + \gamma P_J \lambda_{W,B})(\lambda_{A,B} + \gamma P_{D_t} \lambda_{D_t,B})}, \end{aligned} \quad (41)$$

and

$$\begin{aligned} P_{d,out}^u &= 1 - \frac{(1 - \rho_{D_t,D_r})\lambda_{D_t,D_r}}{(1 - \rho_{D_t,D_r})\lambda_{D_t,D_r} + \mu P_{D_t}\rho_{D_t,D_r}\lambda_{D_t,D_r}} \\ &\quad \times \frac{(1 - \rho_{D_t,D_r})\lambda_{D_t,D_r}}{(1 - \rho_{D_t,D_r})\lambda_{D_t,D_r} + \mu P_A\lambda_{A,D_r}} \\ &\quad \times \frac{(1 - \rho_{D_t,D_r})\lambda_{D_t,D_r}}{(1 - \rho_{D_t,D_r})\lambda_{D_t,D_r} + \mu P_J\lambda_{W,D_r}} \\ &\quad \times \exp\left(-\frac{\mu \sigma_{D_r}^2}{(1 - \rho_{D_t,D_r})\lambda_{D_t,D_r}}\right), \end{aligned} \quad (43)$$

$$\text{where } \gamma = \frac{2R_B/W_{bw} - 1}{P_A} \text{ and } \mu = \frac{2R_D/W_{bw} - 1}{P_{D_t}}.$$

Proof. The main derivations of $\mathbb{S}[X]^u$, $P_{c,out}^u$, and $P_{d,out}^u$ are provided in Appendix D.

Remark 2. The underlay eavesdropping non-outage formulation extends to multiple cellular users by replacing the single-user interference with the aggregate terms $I_{A,W}^K = \sum_{k=1}^K P_{A_k}|g_{A_k,W}|^2$ and $I_{A,D_r}^K = \sum_{k=1}^K P_{A_k}|g_{A_k,D_r}|^2$ in the SINR expressions, which gives the eavesdropping non-outage probability $\mathbb{S}[X]^{u,K} = \Pr\{\text{SINR}_W^{u,K} \geq \text{SINR}_{D_r}^{u,K}\}$. Since the aggregate interference affects both the Warden and D_r , its impact is not monotonic and depends on the relative strengths of the A_k -W and A_k - D_r links. Under the D2D and K cellular QoS constraints, the system-level probability becomes $\mathbb{S}[X]_{\text{all}}^{u,K} = \mathbb{S}[X]^{u,K}(1 - P_{d,out}^{u,K}) \prod_{k=1}^K (1 - P_{c,out,k}^{u,K})$.

The full extension thus requires joint power control, aggregate interference management, and multiple QoS constraints, which raises the optimization dimension.

B. System Eavesdropping Non-Outage Probability Maximization

Under the underlay mode, we maximize the system eavesdropping non-outage probability $\mathbb{S}[X]_{\text{all}}^u$ over the Warden's covert jamming power P_J and Alice's transmit power P_A , subject to the covertness requirement. The power of the suspicious transmitter D_t defines two cases: fixed (Case 1) and adaptive (Case 2).

Case 1 (fixed P_{D_t}).

$$\max_{P_A, P_J} \mathbb{S}[X]_{\text{all}}^u, \quad (44a)$$

$$\text{s.t. } \overline{P}_E^* \geq 1 - \varepsilon, \quad (44b)$$

$$0 \leq P_A \leq \Omega, \quad (44c)$$

$$0 \leq P_J \leq \eta, \quad (44d)$$

where (44a) follows (38). Constraint (44b) keeps the average minimum DEP $\overline{P}_E^*$ no less than $1 - \varepsilon$ for the covertness requirement ε . Constraints (44c) and (44d) bound P_A and P_J by Ω and η .

We first analyze the optimal structure, starting with P_J . Let $P_J^{\text{covert}} = f(\varepsilon)$ denote the covert jamming power that solves $\overline{P}_E^* = 1 - \varepsilon$. When $f(\varepsilon) \leq \eta$, any $P_J > f(\varepsilon)$ violates the covertness constraint (44b) and forces D_t to suspend transmission, giving $\mathbb{S}[X]_{\text{all}}^u = 0$. When $f(\varepsilon) > \eta$, every $P_J \in [0, \eta]$ stays covert and only the budget η binds. The feasible range is thus $0 \leq P_J \leq \min(\eta, P_J^{\text{covert}})$.

Case 2 (adaptive P_{D_t}). Here D_t drops the fixed power. It presets a target reliability Q_d and transmits at the minimum power $P_{D_t}^{\min}$ that meets Q_d under the current interference. Although D_r cannot separate the covert jamming from the background noise, the D2D pair senses the raised interference and adapts P_{D_t} accordingly. Stronger interference forces D_t to raise power to hold the target, whereas a smaller Q_d lowers both the required power and the surveillance exposure at the cost of D2D reliability. In practice Q_d stays above a minimum service reliability, typically no less than 0.9 [53]. The Warden and the BS do not set Q_d but anticipate and exploit this behavior when designing P_J and P_A . Case 2 thus captures the surveillance performance under dynamic power control. With P_{D_t} adaptive, the fixed P_{D_t} in both the objective and the average minimum DEP $\overline{P}_E^*$ becomes $P_{D_t}^{\min}$, while the P_A and P_J constraints stay unchanged.

$$\begin{aligned} \max_{P_A, P_J} \mathbb{S}[X]_{\text{all}}^u(P_A, P_{D_t}^{\min}, P_J), \\ \text{s.t. } \overline{P}_E^*(P_J, P_{D_t}^{\min}) \geq 1 - \varepsilon, \end{aligned} \quad (45)$$

(44c), (44d),

where

$$P_{D_t}^{\min}(P_A, P_J) \triangleq \min_{0 < P_{D_t} \leq P_{D_t}^{\max}} P_{D_t}, \quad (46)$$

$$\text{s.t. } 1 - P_{d,out}^u(P_A, P_{D_t}, P_J) \geq Q_d.$$

In (46), Q_d is the target QoS reliability, that is, the minimum D2D non-outage probability $1 - P_{d,out}^u$, and $P_{D_t}^{\max}$ is the

maximum transmit power of D_t . Since $P_{D_t}^{\min}$ is the smallest power meeting Q_d , P_{D_t} becomes a function of P_A and P_J . If even $P_{D_t}^{\max}$ fails to meet Q_d , the link is infeasible and $\mathbb{S}[X]_{\text{all}}^u = 0$.

From (18), (19), and (40), the objective is highly non-concave in P_J and P_A . Self-interference makes $\mathbb{S}[X]^u$ non-monotonic in P_J , while $P_{c,\text{out}}^u$ and $P_{d,\text{out}}^u$ both rise with P_J . This trades eavesdropping gain against system outage and rules out jamming at full power. A larger P_A lowers $P_{c,\text{out}}^u$ but raises $P_{d,\text{out}}^u$, a further trade-off. Case 2 shares this structure, with $P_{D_t}^{\min}$ replacing the fixed P_{D_t} , so the objective stays non-concave. Closed-form optima P_J^* and P_A^* are thus intractable in both cases, and we develop a unified low-complexity solver based on the CCCP in Section VI-C.

VI. SURVEILLANCE PERFORMANCE UNDER THE OVERLAY MODE

In this section, we formulate an optimization problem to maximize the system eavesdropping non-outage probability $\mathbb{S}[X]_{\text{all}}^o$, by optimizing the transmit powers of Warden and Alice and the spectrum partition factor.

A. System Eavesdropping Non-Outage Probability Modeling

We denote the system eavesdropping non-outage probability by $\mathbb{S}[X]_{\text{all}}^o$, which is defined as

$$\mathbb{S}[X]_{\text{all}}^o = \mathbb{S}[X]^o (1 - P_{c,\text{out}}^o) (1 - P_{d,\text{out}}^o), \quad (47)$$

where $\mathbb{S}[X]^o$ denotes the eavesdropping non-outage probability of Warden at D_t , and $P_{c,\text{out}}^o$ and $P_{d,\text{out}}^o$ are the transmission outage probabilities of the cellular link and the D2D link, respectively, under the overlay mode. From (39),

$$\mathbb{S}[X]^o = \Pr\{C_W^o \geq C_{D_r}^o\} = \Pr\{\text{SINR}_W^o \geq \text{SINR}_{D_r}^o\}. \quad (48)$$

Under the overlay mode, the cellular and D2D outage probabilities are given by $P_{c,\text{out}}^o = \Pr\{\beta W_{\text{bw}} \log_2(1 + \text{SINR}_B^o) < R_B\}$ and $P_{d,\text{out}}^o = \Pr\{(1 - \beta) W_{\text{bw}} \log_2(1 + \text{SINR}_{D_r}^o) < R_D\}$, with non-outage probabilities $(1 - P_{c,\text{out}}^o)$ and $(1 - P_{d,\text{out}}^o)$, respectively. The expressions of $\mathbb{S}[X]^o$, $P_{c,\text{out}}^o$, and $P_{d,\text{out}}^o$ are provided in Theorem 5.

Theorem 5. *Under the overlay mode, the eavesdropping non-outage probability $\mathbb{S}[X]^o$, the transmission outage probability $P_{c,\text{out}}^o$ of the cellular link and $P_{d,\text{out}}^o$ of the D2D link are given by*

$$\begin{aligned} \mathbb{S}[X]^o = & \int_0^\infty \left(1 - \exp\left(-\frac{\sigma_{D_t}^2 x}{(1 - \rho_{D_t,D_r}) P_{D_t} \lambda_{D_t,D_r}}\right) \right. \\ & \times \frac{(1 - \rho_{D_t,D_r}) P_{D_t} \lambda_{D_t,D_r}}{(1 - \rho_{D_t,D_r}) P_{D_t} \lambda_{D_t,D_r} + \rho_{D_t,D_r} P_{D_t} \lambda_{D_t,D_r} x} \\ & \times \frac{(1 - \rho_{D_t,D_r}) P_{D_t} \lambda_{D_t,D_r}}{(1 - \rho_{D_t,D_r}) P_{D_t} \lambda_{D_t,D_r} + P_J \lambda_{W,D_r} x} \Big) \\ & \times \frac{\exp\left(-\frac{\sigma_W^2 x}{P_{D_t} \lambda_{D_t,W}}\right) (\phi P_J \lambda_{W,W} P_{D_t} \lambda_{D_t,W} + \sigma_W^2 (P_{D_t} \lambda_{D_t,W} + \phi P_J \lambda_{W,W} x))}{(P_{D_t} \lambda_{D_t,W} + \phi P_J \lambda_{W,W} x)^2} dx, \end{aligned} \quad (49)$$

$$P_{c,\text{out}}^o = 1 - \exp\left(-\frac{\zeta \sigma_B^2}{\lambda_{A,B}}\right), \quad (50)$$

and

$$\begin{aligned} P_{d,\text{out}}^o = & 1 - \frac{(1 - \rho_{D_t,D_r}) \lambda_{D_t,D_r}}{(1 - \rho_{D_t,D_r}) \lambda_{D_t,D_r} + \tau P_{D_t} \rho_{D_t,D_r} \lambda_{D_t,D_r}} \\ & \times \frac{(1 - \rho_{D_t,D_r}) \lambda_{D_t,D_r}}{(1 - \rho_{D_t,D_r}) \lambda_{D_t,D_r} + \tau P_J \lambda_{W,D_r}} \\ & \times \exp\left(-\frac{\tau \sigma_{D_r}^2}{(1 - \rho_{D_t,D_r}) \lambda_{D_t,D_r}}\right), \end{aligned} \quad (51)$$

where $\zeta = \frac{2^{\frac{R_B}{\beta W_{\text{bw}}}} - 1}{P_A}$ and $\tau = \frac{2^{\frac{R_D}{(1-\beta)W_{\text{bw}}}} - 1}{P_{D_t}}$, with R_B and R_D denoting the desired rates of the cellular and D2D links, respectively.

Proof. The proof of Theorem 5 is similar to that of Theorem 4. Thus, we omit the proof process here.

B. System Eavesdropping Non-Outage Probability Maximization

In the overlay mode, we jointly optimize the spectrum partition factor β and the transmit powers P_A and P_J to maximize the system eavesdropping non-outage probability, while accounting for the outage probabilities of the D2D and cellular links. As in the underlay mode, the power of D_t defines a fixed case (Case 1) and an adaptive case (Case 2), now with the extra variable β .

Case 1 (fixed P_{D_t}).

$$\max_{\beta, P_A, P_J} \mathbb{S}[X]_{\text{all}}^o \quad (52a)$$

$$\text{s.t. } 0 \leq \beta \leq 1, \quad (52b)$$

$$(44b), (44c), (44d), \quad (52c)$$

where $\mathbb{S}[X]_{\text{all}}^o$ follows (47), (52b) bounds β , and the remaining constraints repeat those of the underlay mode.

Case 2 (adaptive P_{D_t}). Case 2 follows the same design as underlay mode. D_t transmits at the minimum power $P_{D_t}^{\min}$ meeting its preset Q_d , and the Warden and the BS exploit this when optimizing β , P_A , and P_J . The difference is that the overlay D2D outage probability $P_{d,\text{out}}^o$ depends on β rather than P_A , so the adaptive power becomes $P_{D_t}^{\min}(\beta, P_J)$. It replaces the fixed P_{D_t} in the objective and in the average minimum DEP $\bar{P}_E^*$, leaving the constraints unchanged.

$$\begin{aligned} \max_{\beta, P_A, P_J} \mathbb{S}[X]_{\text{all}}^o(\beta, P_A, P_{D_t}^{\min}, P_J), \\ \text{s.t. } \bar{P}_E^*(P_J, P_{D_t}^{\min}) \geq 1 - \varepsilon, \end{aligned} \quad (53)$$

$$(52b), (44c), (44d),$$

where

$$P_{D_t}^{\min}(\beta, P_J) \triangleq \min_{0 < P_{D_t} \leq P_{D_t}^{\max}} P_{D_t}, \quad (54)$$

$$\text{s.t. } 1 - P_{d,\text{out}}^o(\beta, P_{D_t}, P_J) \geq Q_d.$$

Here Q_d , $P_{D_t}^{\max}$, and $P_{D_t}^{\min}$ keep their underlay definitions. If even $P_{D_t}^{\max}$ fails to meet Q_d , the link is infeasible and $\mathbb{S}[X]_{\text{all}}^o = 0$. The objective stays non-concave in β , P_A , and P_J , so no closed-form optimum exists and both cases use the CCCP of Section VI-C.

C. CCCP-Based Solution for the Underlay and Overlay Modes

Both problem (44a) and problem (52a) are non-concave, and a direct grid search over their feasible boxes scales poorly with the variable dimension. We therefore solve them with a unified CCCP [54], which maximizes a sequence of concave surrogates and treats the underlay and overlay modes together with Case 1 and Case 2 under one procedure. CCCP is an effective solver for non-convex resource allocation in wireless

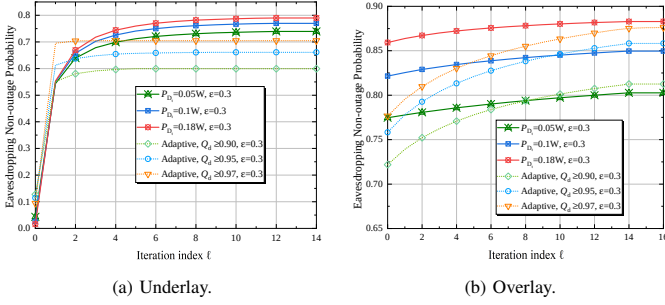


Fig. 4: Convergence analysis of the unified CCCP under the underlay and overlay modes.

networks, such as energy-efficient D2D mode switching [55] and joint communication-caching-computing allocation in mobile edge networks [56].

We let $m \in \{u, o\}$ index the underlay and overlay modes and stack each mode's variables into $\mathbf{v}_m$, with $\mathbf{v}_u = [P_A, P_J]^T$ and $\mathbf{v}_o = [\beta, P_A, P_J]^T$, giving dimensions $d_u = 2$ and $d_o = 3$. The feasible box $\mathcal{V}_m$ follows each problem's constraints. The two cases differ only in how P_{D_t} enters the objective. Case 1 fixes it at $P_{D_t}^{\text{fix}}$. Case 2 replaces it by the minimum feasible power $P_{D_t}^{\min}(\mathbf{v}_m)$, recovered at each objective evaluation by a one-dimensional bisection of tolerance ξ_P that meets the D2D QoS target. Since $P_{D_t}^{\min}$ decreases monotonically with P_{D_t} , this power is uniquely determined whenever the target Q_d is reachable. On the positive feasible interior, where the solution stays off the power boundary, it can be treated as an induced response of $\mathbf{v}_m$ in the objective evaluation.

Because $\log(\cdot)$ is increasing, maximizing $\mathbb{S}[X]_{\text{all}}^m$ is equivalent to maximizing the log-smoothed objective $\Lambda_m(\mathbf{v}_m) = \log(\mathbb{S}[X]_{\text{all}}^m(\mathbf{v}_m) + \alpha)$, where $\alpha > 0$ keeps Λ_m bounded. On the feasible interior, Λ_m is non-concave but twice continuously differentiable with bounded Hessian. Following the difference-of-convex (D.C.) principle [54], we split $-\Lambda_m(\mathbf{v}_m) = G_m(\mathbf{v}_m) - H_m(\mathbf{v}_m)$, with $G_m(\mathbf{v}_m) = -\Lambda_m(\mathbf{v}_m) + \frac{\chi_m}{2} \|\mathbf{v}_m\|^2$ and $H_m(\mathbf{v}_m) = \frac{\chi_m}{2} \|\mathbf{v}_m\|^2$. Choosing the regularization $\chi_m \geq \chi_{\min}^m$, where $\chi_{\min}^m$ upper-bounds the spectral norm of $\nabla^2 \Lambda_m$ over the explored region, makes G_m convex and the split a valid D.C. form. In practice we set χ_m from a conservative finite-difference estimate of this bound.

At iteration ℓ , we linearize H_m at $\mathbf{v}_m^{(\ell)}$ and maximize the resulting concave surrogate,

$$\mathbf{v}_m^{(\ell+1)} = \arg \max_{\mathbf{v} \in \mathcal{V}_m} \left[\Lambda_m(\mathbf{v}) - \frac{\chi_m}{2} \|\mathbf{v} - \mathbf{v}_m^{(\ell)}\|^2 \right], \quad (55)$$

solved by an interior-point routine over the low-dimensional box $\mathcal{V}_m$.

Because $\chi_m \geq \chi_{\min}^m$, the surrogate in (55) is concave and is a lower bound of Λ_m that is tight at $\mathbf{v}_m^{(\ell)}$. The objective $\mathbb{S}[X]_{\text{all}}^m$ is therefore non-decreasing across the accepted feasible iterates, which converge to a stationary point under the standard CCCP conditions [54], [55]. This claim is restricted to the positive feasible interior, where Λ_m is smooth; infeasible points return a zero objective from EVALOBJ and are excluded from this interior, so they do not affect the convergence on it.

Convergence. Fig. 4(a) and 4(b) plot $\mathbb{S}[X]_{\text{all}}^m(\mathbf{v}_m^{(\ell)})$ against the outer-iteration index ℓ at $\varepsilon = 0.3$ for the three fixed-power

Algorithm 1 Unified CCCP for Underlay and Overlay Mode Optimization

- 1: **Input:** mode m , case index, feasible box $\mathcal{V}_m$, case-specific parameters ($P_{D_t}^{\text{fix}}$ for Case 1, or Q_d and $P_{D_t}^{\max}$ for Case 2), regularization $\chi_m \geq \chi_{\min}^m$, smoothing constant $\alpha > 0$, and tolerances $\xi, \xi_P > 0$.
- 2: **Initialize:** $\mathbf{v}_m^{(0)} \in \mathcal{V}_m$ and $\ell \leftarrow 0$.
- 3: **repeat**
- 4: Obtain $\mathbf{v}_m^{(\ell+1)}$ from (55) by interior-point, with $\Lambda_m(\mathbf{v}) = \log(\text{EVALOBJ}(\mathbf{v}) + \alpha)$.
- 5: $\ell \leftarrow \ell + 1$.
- 6: **until** $|\mathbb{S}[X]_{\text{all}}^m(\mathbf{v}_m^{(\ell)}) - \mathbb{S}[X]_{\text{all}}^m(\mathbf{v}_m^{(\ell-1)})| < \xi$
- 7: **Output:** $\mathbf{v}_m^* = \mathbf{v}_m^{(\ell)}$ and $\mathbb{S}[X]_{\text{all}}^{m,*} = \mathbb{S}[X]_{\text{all}}^m(\mathbf{v}_m^*)$.
- 8: **function** EVALOBJ($\mathbf{v}$)
- 9: **if** Case 1 **then**
- 10: Set $P_{D_t} = P_{D_t}^{\text{fix}}$.
- 11: **else**
- 12: Solve (46) or (54) for $P_{D_t}^{\min}(\mathbf{v})$ by bisection on $(0, P_{D_t}^{\max}]$.
- 13: **return** 0 if the target Q_d is unreachable.
- 14: Set $P_{D_t} = P_{D_t}^{\min}(\mathbf{v})$.
- 15: **end if**
- 16: **return** 0 if $\overline{P}_E(P_J, P_{D_t}) < 1 - \varepsilon$.
- 17: **return** $\mathbb{S}[X]_{\text{all}}^m(\mathbf{v})$ evaluated at this P_{D_t} .
- 18: **end function**

settings of Case 1 and the three QoS targets of Case 2. Across all settings the objective rises monotonically and saturates within about 15 iterations, where the per-iteration change drops below $\xi = 10^{-4}$. Carrying one extra variable, the overlay mode makes each iteration slightly costlier, while its outer-iteration count stays close to the underlay mode.

Complexity. The cost of Algorithm 1 comes from its two nested loops, that is, the total number of objective evaluations times the per-evaluation cost. For mode m , the outer loop runs L_m CCCP iterations, and each iteration solves one concave surrogate over $\mathcal{V}_m$ with $\tilde{N}_{\text{eval}}^m$ objective evaluations on average, so the total evaluation count is $L_m \tilde{N}_{\text{eval}}^m$. Let Φ_m denote the per-evaluation cost under the considered mode and adversary case, dominated by the single one-dimensional integration in the eavesdropping factor $\mathbb{S}[X]^m$, since the cellular and D2D outage factors are closed form. The CCCP cost is then $\mathcal{O}(L_m \tilde{N}_{\text{eval}}^m \Phi_m)$. In Case 1, Φ_m covers this integration and the closed-form feasibility check. In Case 2, each evaluation further recovers $P_{D_t}^{\min}$ by a monotone bisection with tolerance ξ_P , which adds $\mathcal{O}(\log(1/\xi_P))$ closed-form evaluations and makes Φ_m larger than in Case 1. A grid search instead samples M_g points along each of the d_m axes of $\mathcal{V}_m$, giving $M_g^{d_m}$ evaluations each with cost Φ_m , and hence the complexity $\mathcal{O}(M_g^{d_m} \Phi_m)$. Thus grid search grows exponentially in d_m , whereas CCCP skips exhaustive enumeration and needs far fewer evaluations for comparable accuracy in both modes and both cases.

VII. SURVEILLANCE UTILITY UNDER FLEXIBLE MODE SELECTION

We develop an overhead-aware surveillance utility model under flexible mode selection. The aim is to minimize the long-term average normalized management overhead while guaranteeing a minimum long-term average surveillance utility. Over a horizon of N_b blocks, the channel is time-varying across blocks. The per-mode statistics derived earlier, such as $\mathbb{S}[X]_{\text{all}}^m$ and the related outage probabilities, are already averaged over the block fading, so they serve directly as the per-block performance in this long-term model.

A. Overhead-Aware Utility Modeling

Operating each mode incurs a management overhead [57], [58] from the control signaling, power control, and resource configuration that the BS computes and delivers at each block. Let $\varpi^m \in (0, 1)$ denote the fraction of system resources consumed by the management of mode $m \in \{u, o\}$. The overlay mode additionally computes and broadcasts the partition factor β and coordinates the orthogonal scheduling, so we model it with a larger overhead than the underlay mode, $\varpi^u < \varpi^o < 1$.

The surveillance utility of mode m scales the per-mode performance by the residual resource fraction,

$$\mathbb{U}^m = (1 - \varpi^m) \mathbb{S}[X]_{\text{all}}^m, \quad m \in \{u, o\}. \quad (56)$$

This multiplicative discounting follows the resource-overhead tradeoff convention [59]. Let $p_{\text{eff}} \in [0, 1]$ be the long-term time-sharing fraction of the underlay mode, with $1 - p_{\text{eff}}$ for the overlay mode. The long-term average utility and average normalized overhead are

$$\bar{\mathbb{U}}(p_{\text{eff}}) = p_{\text{eff}} \mathbb{U}^u + (1 - p_{\text{eff}}) \mathbb{U}^o, \quad (57)$$

$$\bar{\varpi}(p_{\text{eff}}) = p_{\text{eff}} \varpi^u + (1 - p_{\text{eff}}) \varpi^o. \quad (58)$$

B. Overhead-Aware Mode Selection Optimization

Given the optimized per-mode values of $\mathbb{S}[X]_{\text{all}}^m$ obtained in Sections V and VI, the remaining decision variable is the long-term underlay fraction p_{eff} . The mode-selection problem minimizes the average overhead subject to a utility floor,

$$\min_{p_{\text{eff}}} \bar{\varpi}(p_{\text{eff}}) \quad (59a)$$

$$\text{s.t. } \bar{\mathbb{U}}(p_{\text{eff}}) \geq \mathbb{U}_{\min}, \quad (59b)$$

$$0 \leq p_{\text{eff}} \leq 1, \quad (59c)$$

where $\mathbb{U}_{\min}$ is the required minimum average utility.

Because $\bar{\varpi}(p_{\text{eff}})$ decreases in p_{eff} , the optimum takes the largest p_{eff} that meets the utility floor. When $\mathbb{U}^o > \mathbb{U}^u$, the optimal fraction is

$$p_{\text{eff}}^* = \begin{cases} 1, & \mathbb{U}_{\min} \leq \mathbb{U}^u, \\ \frac{\mathbb{U}^o - \mathbb{U}_{\min}}{\mathbb{U}^o - \mathbb{U}^u}, & \mathbb{U}^u < \mathbb{U}_{\min} < \mathbb{U}^o, \\ 0, & \mathbb{U}_{\min} = \mathbb{U}^o, \end{cases} \quad (60)$$

and the problem is infeasible for $\mathbb{U}_{\min} > \mathbb{U}^o$. When $\mathbb{U}^o \leq \mathbb{U}^u$, the underlay mode gives no smaller utility at a lower overhead,

so $p_{\text{eff}}^* = 1$ for $\mathbb{U}_{\min} \leq \mathbb{U}^u$ and the problem is infeasible otherwise.

The interior regime $\mathbb{U}^u < \mathbb{U}_{\min} < \mathbb{U}^o$ gives $p_{\text{eff}}^* \in (0, 1)$, where the system runs the underlay mode in part of the blocks and the overlay mode in the rest. The achieved overhead is $\bar{\varpi}(p_{\text{eff}}^*) = \varpi^o - p_{\text{eff}}^*(\varpi^o - \varpi^u) < \varpi^o$, so flexible mode selection meets the utility requirement at a lower overhead than running the single mode with the higher utility, so it is more efficient.

VIII. NUMERICAL RESULTS

In this section, numerical simulations examine how key parameters such as ρ_{D_t, D_r} , β , Ω , and ε affect the system covert eavesdropping performance under the underlay mode, the overlay mode, and the mode selection mechanism. Unless otherwise specified, the main parameters are as follows. The suspicious transmitter power satisfies $0 \leq P_{D_t} \leq P_{D_t}^{\max}$ with $P_{D_t}^{\max} = 0.2$ W, $\lambda_{i,j} = 1$, $\rho_{D_t, D_r} = 0.5$, $\rho_{W, D_r} = 0.5$, $\sigma_j^2 = 0.02$ W, $R_B = 0.1$ Mbit/s, $R_D = 0.1$ Mbit/s, $\varepsilon = 0.3$, $\Omega = 0.2$ W, $\eta = 0.2$ W, and $\phi = 0.1$. The transmit power bounds follow 3GPP specifications, where 0.2 W corresponds to 23 dBm, the power class 3 limit for user equipment in 3GPP TS 38.101-1 [47]. The thresholds R_B and R_D are low-rate QoS requirements for the cellular and suspicious D2D links. The channel means $\lambda_{i,j}$ and the noise power σ_j^2 are normalized baseline values that reveal the fundamental tradeoffs. The value $\phi = 0.1$ is a representative operating point under imperfect self-interference cancellation, not a hardware-specific constant. Fig. 5 further evaluates the full range $\phi \in [0, 1]$, from ideal cancellation at $\phi = 0$ to no active cancellation at $\phi = 1$, so the main conclusions do not depend on this single default value.

We consider both a fixed suspicious transmitter and an adaptive one. In the fixed case, P_{D_t} is a constant. In the adaptive case, D_t transmits at the minimum power that meets a target reliability Q_d . We propose a jointly optimized active eavesdropping scheme (JAS) and compare it with two benchmarks [11], [18], [19]. The passive eavesdropping scheme (PES) sets $P_J^* = 0$. The constant-power active eavesdropping scheme (CAS) sets $P_J^* = \min(\eta, P_J^{\text{covert}})$, that is, the largest jamming power meeting the covertness constraint within the budget. JAS jointly optimizes all the remaining variables to maximize the system eavesdropping non-outage probability.

A. Surveillance Performance under the Underlay Mode

Fig. 5 shows the effect of the normalized residual self-interference coefficient ϕ on $\mathbb{S}[X]_{\text{all}}^u$ for $P_{D_t} = 0.1$ W, $\varepsilon = 0.3$, $\Omega = 0.2$ W, and $\eta = 0.2$ W. PES stays constant because $P_J = 0$ removes any self-interference. CAS decreases monotonically with ϕ and eventually falls below PES, since its fixed jamming power leaves residual self-interference at the Warden. JAS matches CAS at small ϕ , where active jamming still helps the Warden. As ϕ grows, JAS first decreases and then saturates. The joint optimization of P_J and P_A trades self-interference at the Warden against interference at D_r . At large ϕ , the optimum stops jamming, so JAS reduces to PES.

We examine how the suspicious transmit power P_{D_t} affects $\mathbb{S}[X]_{\text{all}}^u$ for $\rho_{W,D_r} \in \{0,1\}$, setting $\lambda_{D_t,D_r} = 1.5$, $\lambda_{D_t,W} = 1.25$, $\lambda_{W,W} = 3.2$, and the other gains to 1. Fig. 6 shows that $\mathbb{S}[X]_{\text{all}}^u$ grows with P_{D_t} , since a larger P_{D_t} strengthens the eavesdropping link SINR_W^u and raises the covert jamming power P_J^{covert} . At small P_{D_t} , P_J^{covert} stays limited, so JAS and CAS coincide and sit slightly above passive eavesdropping. As P_{D_t} grows, P_J^{covert} rises and JAS keeps the best performance. CAS degrades in the mid-to-high range and drops below passive eavesdropping, because jamming at the maximum covert power injects excessive interference into the BS and D_r and raises both $P_{c,\text{out}}^u$ and $P_{d,\text{out}}^u$.

Fig. 6 also shows that at small P_{D_t} , the unknown jamming link case $\rho_{W,D_r} = 1$ outperforms the known case $\rho_{W,D_r} = 0$ and passive eavesdropping. Although $\mathbb{S}[X]_{\text{all}}^u$ has no explicit dependence on ρ_{W,D_r} , this parameter affects the detection level at D_r and thus P_J^{covert} . At small P_{D_t} , the larger P_J^{covert} under $\rho_{W,D_r} = 1$ strengthens surveillance. As P_{D_t} increases, the eavesdropping link becomes strong, so JAS lowers P_J or turns passive, and its two ρ_{W,D_r} curves merge. CAS still jams at P_J^{covert} , where the larger value under $\rho_{W,D_r} = 1$ causes excessive jamming and makes CAS the worst at large P_{D_t} . Increasing the jamming link uncertainty thus enhances covert surveillance only at small P_{D_t} , and it should be coordinated with the transmit power for optimal eavesdropping performance.

Fig. 7 shows how Alice's transmit power P_A affects $\mathbb{S}[X]_{\text{all}}^u$. The fixed case sets $P_{D_t} = 0.1$ W with $\varepsilon \in \{0.1, 0.2, 0.3\}$. The adaptive case uses $Q_d \geq 0.90, 0.95$, and 0.97 . In the fixed case, $\mathbb{S}[X]_{\text{all}}^u$ rises sharply and then decreases gradually as P_A grows, so an interior optimum P_A^* exists. A moderate P_A aids eavesdropping, while an excessive P_A causes strong interference to the Warden and D_r and degrades performance. For a given P_A , a looser covertness constraint, e.g., $\varepsilon = 0.3$ rather than 0.1 , lets the Warden transmit at higher power and eavesdrop more effectively. In the adaptive case, $\mathbb{S}[X]_{\text{all}}^u$ rises sharply and then stays flat. As P_A grows, D_t raises P_{D_t} to hold $1 - P_{d,\text{out}}^u$ at Q_d . The D2D non-outage thus stays fixed, and the higher P_{D_t} offsets the interference from P_A , so the curve saturates rather than falling. A higher Q_d gives a higher saturation level.

We study the effect of the Warden AN power P_J on $\mathbb{S}[X]_{\text{all}}^u$ for fixed $P_{D_t} \in \{0.05, 0.10, 0.18\}$ W and the adaptive $Q_d \geq 0.90, 0.95$, and 0.97 . In Fig. 8, each curve holds nearly constant as P_J grows and then falls sharply to zero. This drop marks the covert feasibility boundary P_J^{covert} . Beyond it, the covertness constraint $\bar{P}_E^* \geq 1 - \varepsilon$ fails, D_r detects the jamming, and D_t stops transmitting, giving $\mathbb{S}[X]_{\text{all}}^u = 0$. The boundary shifts right as P_{D_t} grows or Q_d tightens. A stricter Q_d raises the D_t transmit power needed for its QoS, and a larger P_{D_t} lifts $\bar{P}_E^*$, both widening the feasible P_J range under the same ε .

Next, we examine the effect of ρ_{D_t,D_r} on $\mathbb{S}[X]_{\text{all}}^u$, with fixed JAS, CAS, and PES at $P_{D_t} = 0.1$ W and adaptive JAS at $Q_d \geq 0.90, 0.95$, and 0.97 . As shown in Fig. 9, the fixed case first rises and then falls with ρ_{D_t,D_r} . At small ρ_{D_t,D_r} , $\mathbb{S}[X]_{\text{all}}^u$ grows faster than $\text{SINR}_{D_r}^u$ declines, so the

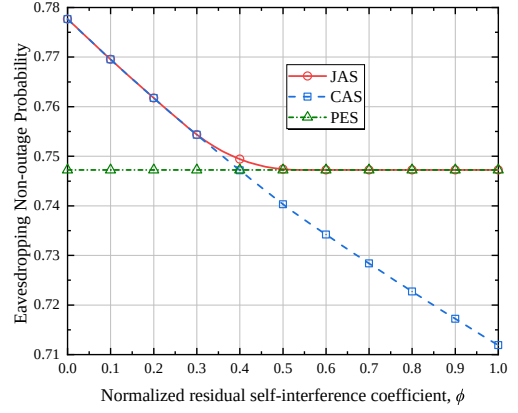


Fig. 5: The effect of the normalized residual self-interference coefficient ϕ on $\mathbb{S}[X]_{\text{all}}^u$ under the underlay mode.

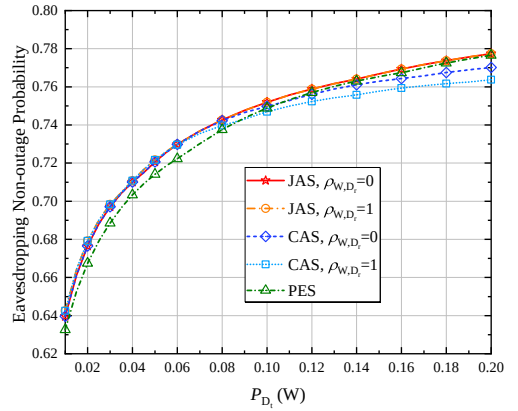


Fig. 6: The effect of P_{D_t} on $\mathbb{S}[X]_{\text{all}}^u$ under the underlay mode.

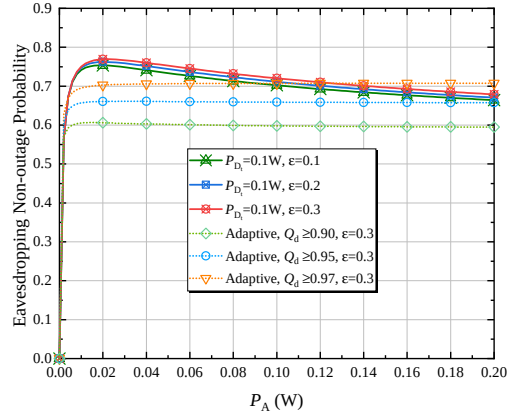


Fig. 7: The effect of P_A on $\mathbb{S}[X]_{\text{all}}^u$ under the underlay mode.

performance improves. As ρ_{D_t,D_r} grows further, the $\text{SINR}_{D_r}^u$ decline dominates and raises $P_{d,\text{out}}^u$, lowering $\mathbb{S}[X]_{\text{all}}^u$. At $\rho_{D_t,D_r} = 1$, the D2D link fails with $\text{SINR}_{D_r}^u = 0$ and $P_{d,\text{out}}^u = 1$, and the three fixed schemes drop to zero. At small ρ_{D_t,D_r} , the optimal jamming power equals P_J^{covert} . At large ρ_{D_t,D_r} , the Warden stays silent and JAS reduces to PES, since the jamming gain on $\mathbb{S}[X]_{\text{all}}^u$ no longer offsets the rise it causes in $P_{c,\text{out}}^u$ and $P_{d,\text{out}}^u$. CAS still jams at P_J^{covert} , and the excessive jamming makes it fall slightly below PES.

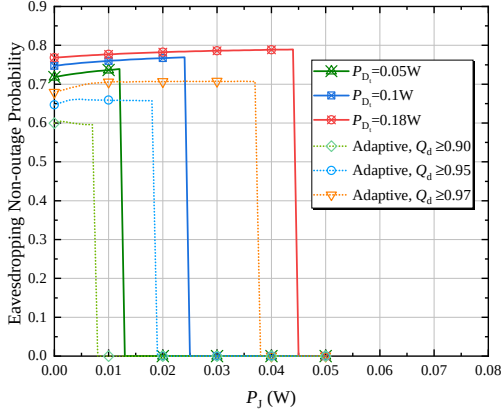


Fig. 8: The effect of P_J on $\mathbb{S}[X]_{\text{all}}^u$ under the underlay mode.

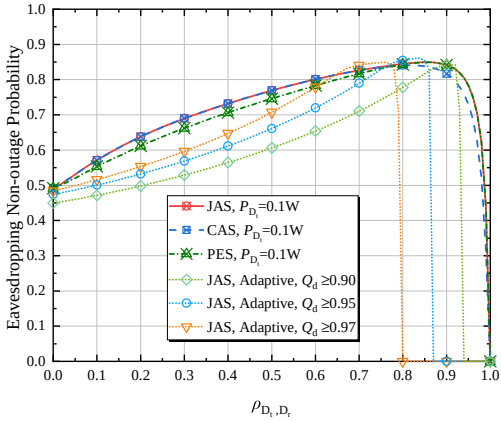


Fig. 9: The effect of ρ_{D_t, D_r} on $\mathbb{S}[X]_{\text{all}}^u$ under the underlay mode.

In the adaptive case, $\mathbb{S}[X]_{\text{all}}^u$ rises with ρ_{D_t, D_r} and then drops abruptly to zero once ρ_{D_t, D_r} exceeds a critical level. As the channel degrades, D_t raises P_{D_t} to hold $1 - P_{d, \text{out}}^u$ at the target Q_d . Beyond the critical level, even the maximum power cannot meet Q_d . A looser QoS tolerates more degradation, so a smaller Q_d shifts the drop to a larger ρ_{D_t, D_r} . The channel uncertainty thus plays a dual role. Moderate uncertainty aids the covert surveillance, while excessive uncertainty breaks the D2D link, forces D_t to stop transmission, and fails the surveillance. We compare this with [19], where the suspicious link uncertainty generally improves the covert surveillance. Our eavesdropping non-outage probability also accounts for the cellular and D2D outage probabilities, so the channel uncertainty plays a dual role under both the fixed and the adaptive cases. This confirms the necessity of the QoS constraints in covert surveillance.

Finally, we examine the effect of the QoS target Q_d on $\mathbb{S}[X]_{\text{all}}^u$ under the adaptive adversary, where the D2D link requires $1 - P_{d, \text{out}}^u \geq Q_d$. We compare JAS, CAS, and PES with $\varepsilon \in \{0.1, 0.2, 0.3\}$. As shown in Fig. 10, $\mathbb{S}[X]_{\text{all}}^u$ increases with Q_d for all schemes. JAS and CAS coincide because the covert-boundary power P_J^{covert} is optimal for both, and both stay above PES. For a given Q_d , a larger ε relaxes the covertness constraint and allows a larger feasible P_J , which raises $\mathbb{S}[X]_{\text{all}}^u$. The trend follows from the adaptive behavior of D_t . A stricter Q_d forces D_t to raise its transmit power to

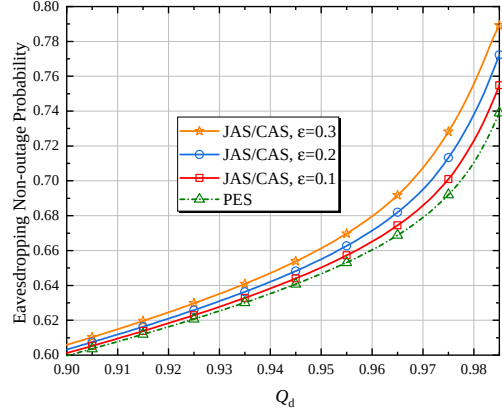


Fig. 10: The effect of Q_d on $\mathbb{S}[X]_{\text{all}}^u$ under the underlay mode.

maintain reliability, and the higher P_{D_t} strengthens the eavesdropping link. A looser target such as 0.90 lets D_t transmit at lower power, so $\mathbb{S}[X]_{\text{all}}^u$ reaches its lowest value. Unlike the fixed-power suspicious transmitter assumed in most studies [15]–[20], Case 2 models a more challenging adversary that adjusts P_{D_t} to meet its own D2D QoS. The proposed power-control design stays effective across Q_d targets, confirming its robustness against the adaptive adversary.

B. Surveillance Performance under the Overlay Mode

Since the effect of some parameters (e.g., ϕ , P_{D_t} , and ρ_{D_t, D_r}) on the eavesdropping performance under the overlay mode is similar to that under the underlay mode, we omit their analysis here for brevity. We focus on Alice's transmit power P_A , the spectrum allocation factor β , and the QoS target Q_d . Unless otherwise stated, $\rho_{D_t, D_r} = 0.5$, $\rho_{W, D_r} = 0.5$, $\Omega = 0.2$ W, $\eta = 0.2$ W, and $\phi = 0.1$.

Fig. 11 shows how the spectrum partition factor β affects $\mathbb{S}[X]_{\text{all}}^o$. The fixed JAS, CAS, and PES use $P_{D_t} = 0.1$ W, and the adaptive JAS uses $Q_d \geq 0.90, 0.95$, and 0.97 . In the fixed case, $\mathbb{S}[X]_{\text{all}}^o$ vanishes at $\beta = 0$ and $\beta = 1$. At $\beta = 0$, Alice gets too little spectrum to meet the cellular QoS, so $P_{c, \text{out}}^o = 1$. At $\beta = 1$, the D2D pair gets too little to meet the D2D QoS, so $P_{d, \text{out}}^o = 1$. A larger β lowers $P_{c, \text{out}}^o$ but raises $P_{d, \text{out}}^o$. An interior optimum β^* thus maximizes $(1 - P_{c, \text{out}}^o)(1 - P_{d, \text{out}}^o)$ and $\mathbb{S}[X]_{\text{all}}^o$. JAS and CAS nearly coincide and stay above PES.

In the adaptive case, $\mathbb{S}[X]_{\text{all}}^o$ rises with β and then drops abruptly to zero at a critical β . As β grows, the D2D pair gets less spectrum, so D_t raises P_{D_t} to hold Q_d . The stronger P_{D_t} strengthens the eavesdropping link and keeps $\mathbb{S}[X]_{\text{all}}^o$ rising. At the critical β , P_{D_t} hits its maximum $P_{D_t}^{\text{max}}$ and can no longer meet Q_d , so the D2D link drops and the surveillance fails. A looser QoS tolerates more D2D outage, so a smaller Q_d pushes the critical β higher.

Fig. 12 shows the joint impact of P_A and β on $\mathbb{S}[X]_{\text{all}}^o$. Subfigure (a) fixes $P_{D_t} = 0.10$ W and subfigure (b) uses the adaptive $Q_d = 0.95$, with $\varepsilon = 0.3$. $\mathbb{S}[X]_{\text{all}}^o$ rises monotonically with P_A , since P_A enters only $1 - P_{c, \text{out}}^o$, so the maximum occurs at $P_A = 0.20$ W. An interior optimum β^* exists in both cases. In (a), the surface is smooth and peaks at $\beta^* \approx 0.19$,

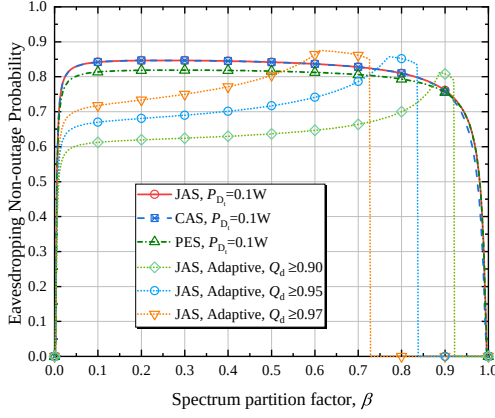


Fig. 11: The effect of β on $\mathbb{S}[X]_{\text{all}}^o$ under the overlay mode.

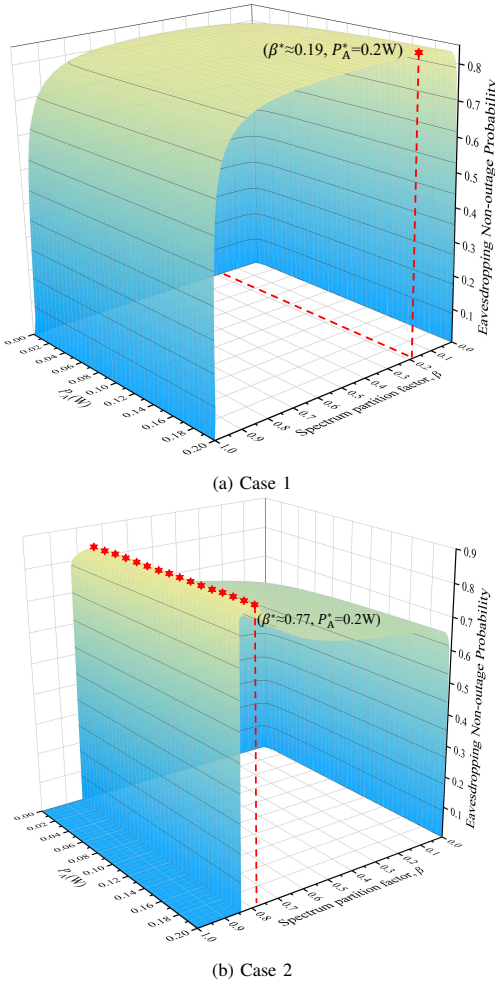


Fig. 12: The effect of P_A and β on $\mathbb{S}[X]_{\text{all}}^o$ under the overlay mode.

agreeing with the fixed result in Fig. 11. In (b), $\mathbb{S}[X]_{\text{all}}^o$ first increases with β and then drops abruptly to zero. As β grows, the D2D spectrum shrinks and D_t raises P_{D_t} to maintain Q_d , strengthening the eavesdropping link. Beyond a critical β , P_{D_t} can no longer meet Q_d , so the D2D link drops and surveillance fails. The peak is at $\beta^* \approx 0.77$. The two surfaces contrast the smooth fixed case with the adaptive case that collapses at the critical β .

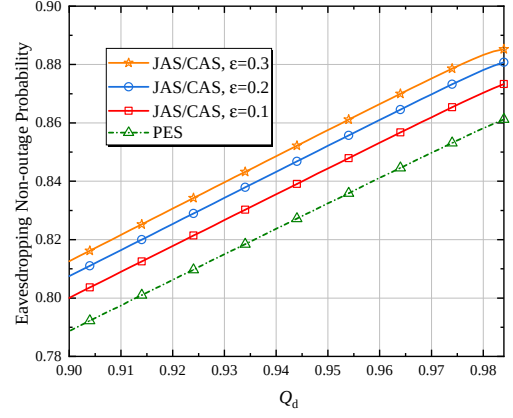


Fig. 13: The effect of Q_d on $\mathbb{S}[X]_{\text{all}}^o$ under the overlay mode.

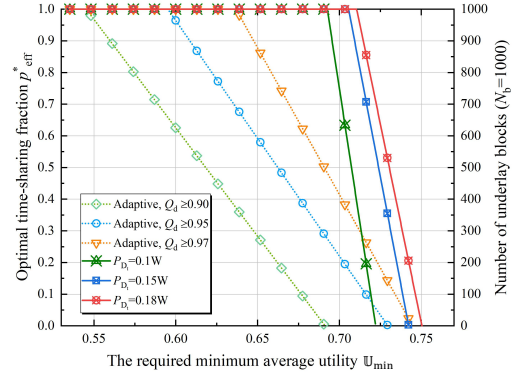


Fig. 14: The effect of $\mathbb{U}_{\min}$ on the optimal time-sharing fraction p_{eff}^* under flexible mode selection.

Finally, Fig. 13 shows the effect of the QoS target Q_d on $\mathbb{S}[X]_{\text{all}}^o$ under the adaptive adversary for JAS, CAS, and PES at $\varepsilon \in \{0.1, 0.2, 0.3\}$. As in the underlay mode, $\mathbb{S}[X]_{\text{all}}^o$ increases with Q_d for all schemes, and a larger ε raises it further. JAS and CAS coincide throughout. Even when D_t adapts its power to evade surveillance, both stay above PES.

C. Surveillance Utility under Flexible Mode Selection

Fig. 14 plots the optimal time-sharing fraction p_{eff}^* against the minimum utility requirement $\mathbb{U}_{\min}$. The fixed case uses $P_{D_t} \in \{0.10, 0.15, 0.18\}$ W and the adaptive case uses $Q_d \geq 0.90, 0.95$, and 0.97 . When $\mathbb{U}_{\min} \leq \mathbb{U}^u$, the underlay mode alone meets the requirement and $p_{\text{eff}}^* = 1$. When $\mathbb{U}^u < \mathbb{U}_{\min} < \mathbb{U}^o$, p_{eff}^* lies strictly within $(0, 1)$, and the scheme runs both modes in proportion. The right axis reports the corresponding number of underlay blocks for $N_b = 1000$. As $\mathbb{U}_{\min}$ approaches $\mathbb{U}^o$, p_{eff}^* drops to zero. Beyond $\mathbb{U}^o$, even overlay-only fails to meet the requirement and the problem becomes infeasible. A larger fixed P_{D_t} or a higher Q_d raises the achievable utility and shifts each curve to the right. This trend holds under both adversary types, which confirms that the proposed mode selection meets the minimum average utility at the lowest overhead.

Fig. 15 shows, on the long-term average overhead and long-term average effective utility plane, the operating points from underlay-only to overlay-only under the fixed-power and

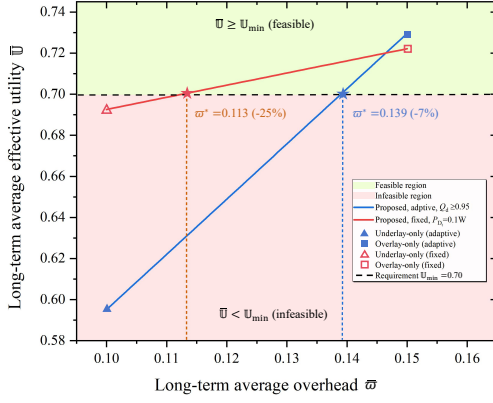


Fig. 15: The overhead and effective utility tradeoff under flexible mode selection.

the adaptive case. The fixed case uses $P_{D_t} = 0.10$ W, the adaptive case uses $Q_d \geq 0.95$, and $U_{\min} = 0.70$. The two endpoints of each line are underlay-only and overlay-only. Underlay-only has the lowest overhead ϖ^u but also the lowest utility. Overlay-only has the highest utility but also the highest overhead ϖ^o . The green area is the feasible region $\bar{U} \geq U_{\min}$, and the red area is infeasible. Overlay-only is feasible but the most costly. The proposed scheme time-shares the two modes over N_b blocks and places the operating point at the intersection of the requirement line $U_{\min}$ and the line, meeting the requirement at the minimum average overhead $\bar{\varpi}^*$. Here $\bar{\varpi}^* = \varpi^o - p_{\text{eff}}^*(\varpi^o - \varpi^u) < \varpi^o$, and the overhead saving over overlay-only is $(\varpi^o - \bar{\varpi}^*)/\varpi^o$. The saving is about 25% in the fixed case and 7% in the adaptive case, which shows the proposed scheme is more efficient while meeting the same utility requirement.

Table II reports the overhead saving for the fixed-power and adaptive adversaries. The fixed case sets $P_{D_t} \in \{0.08, 0.10, 0.12\}$ W with $U_{\min} = 0.70$, and the adaptive case sets $Q_d \geq 0.93, 0.95$, and 0.97 with $U_{\min} = 0.68$. Since the two adversaries occupy different utility ranges, each uses a representative requirement. Here U^u and U^o are the underlay-only and overlay-only utilities from (56), p_{eff}^* and $\bar{\varpi}^*$ follow (60) and (58), and the overhead saving is $(\varpi^o - \bar{\varpi}^*)/\varpi^o$. Underlay-only has the lowest overhead ϖ^u but falls below $U_{\min}$. Overlay-only meets the requirement at the highest utility U^o but the highest overhead ϖ^o . The proposed scheme meets the same $U_{\min}$ at the minimum average overhead $\bar{\varpi}^*$, with $p_{\text{eff}}^* \in (0, 1)$ showing a flexible choice between the two modes. The overhead saving ranges from 7.6% to 32.3% across the two cases, so the proposed selection saves overhead while meeting the utility requirement under different adversaries and parameters.

IX. CONCLUSION

This paper studies active eavesdropping for wireless D2D link surveillance under the overlay, underlay, and mode selection schemes, considering spectrum sharing, covertness, and channel uncertainty. We model the uncertain suspicious and jamming links, derive closed-form expressions for the DEP, outage, and covert non-outage probabilities, and formulate an

TABLE II
OVERHEAD SAVING OF FLEXIBLE MODE SELECTION

Case	$U_{\min}$	U^u	U^o	p_{eff}^*	$\bar{\varpi}^*$	Saving
<i>Fixed-power adversary</i>						
$P_{D_t} = 0.08$ W	0.70	0.685	0.710	0.400	0.130	13.3%
$P_{D_t} = 0.10$ W	0.70	0.693	0.722	0.759	0.112	25.3%
$P_{D_t} = 0.12$ W	0.70	0.699	0.730	0.968	0.102	32.3%
<i>Adaptive-QoS adversary</i>						
$Q_d = 0.93$	0.68	0.572	0.712	0.229	0.139	7.6%
$Q_d = 0.95$	0.68	0.595	0.730	0.370	0.131	12.3%
$Q_d = 0.97$	0.68	0.637	0.745	0.602	0.120	20.1%

optimization problem that maximizes eavesdropping performance. A unified CCCP solves it for both modes and both adversary cases. Numerical results reveal a dual effect of channel uncertainty. Excessive uncertainty on the suspicious link degrades communication quality and causes eavesdropping failure, while moderate uncertainty on the jamming link can improve performance, depending on the D_t transmit power. Alice's signal power aids eavesdropping within limits under the underlay mode but always helps under the overlay mode. Optimizing the jamming power and relaxing the covertness constraints further improve surveillance, and with proper parameters, the overlay mode with optimized spectrum allocation outperforms the underlay mode. The scheme stays effective against both the fixed-power and adaptive-power adversaries. Flexible mode selection also reduces the selection overhead while meeting a minimum surveillance requirement. In future work, we will study more general scenarios, such as networks with multiple cellular users, multi-antenna Warden beamforming and antenna-pair selection, and time-varying channels with intra-block channel aging.

REFERENCES

- [1] Y. Sun, J. Cao, M. Ma, Y. Zhang, H. Li, and B. Niu, "EAP-DDBA: Efficient anonymity proximity device discovery and batch authentication mechanism for massive D2D communication devices in 3GPP 5G HetNet," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 1, pp. 370–387, 2022.
- [2] V. N. Sathi, M. Srinivasan, P. K. Thiruvassagam, and C. S. R. Murthy, "Novel protocols to mitigate network slice topology learning attacks and protect privacy of users' service access behavior in software-defined 5G networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 6, pp. 2888–2906, 2020.
- [3] R. Sun and B. Yang, "Covert communication with truncated channel inversion power control in D2D underlaid cellular networks," *Journal of Networking and Network Applications*, vol. 1, no. 4, pp. 179–186, 2022.
- [4] H. Xiao, D. Zhu, and A. T. Chronopoulos, "Power allocation with energy efficiency optimization in cellular D2D-based V2X communication network," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 12, pp. 4947–4957, 2020.
- [5] K. Ali, H. X. Nguyen, P. Shah, Q.-T. Vien, and E. Ever, "D2D multi-hop relaying services towards disaster communication system," in *2017 24th International Conference on Telecommunications (ICT)*. IEEE, 2017, pp. 1–5.
- [6] X. Ren, J. Cao, B. Niu, L. Gan, Y. Zhang, L. Xiong, Y. Luo, and H. Li, "A formal analysis of 5G prose aka protocols for U2N relay communication," *IEEE Transactions on Dependable and Secure Computing*, 2024.
- [7] Z. Hu, J. Niu, T. Ren, X. Liu, and M. Guizani, "SITOff: Enabling size-insensitive task offloading in D2D-assisted mobile edge computing," *IEEE Transactions on Mobile Computing*, vol. 24, no. 3, pp. 1567–1584, 2025.

- [8] T. Zhang, Y. Wang, W. Yi, Y. Liu, and A. Nallanathan, "Joint optimization of caching placement and trajectory for UAV-D2D networks," *IEEE Transactions on Communications*, vol. 70, no. 8, pp. 5514–5527, 2022.
- [9] J. Ji, K. Zhu, D. Niyato, and R. Wang, "Joint trajectory design and resource allocation for secure transmission in cache-enabled UAV-relaying networks with D2D communications," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1557–1571, 2021.
- [10] Y. Zeng and R. Zhang, "Wireless information surveillance via proactive eavesdropping with spoofing relay," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1449–1461, 2016.
- [11] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via cognitive jamming in fading channels," *IEEE Transactions on Wireless Communications*, vol. 16, no. 5, pp. 2790–2806, 2017.
- [12] D. Xu, H. Zhu, and Q. Li, "Jammer-assisted legitimate eavesdropping in wireless powered suspicious communication networks," *IEEE Access*, vol. 7, pp. 20363–20380, 2019.
- [13] J. Moon, S. H. Lee, H. Lee, S. Baek, and I. Lee, "Deep learning-based proactive eavesdropping for wireless surveillance," in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, 2019, pp. 1–6.
- [14] Y. Zhang, X. Jiang, C. Zhong, and Z. Zhang, "Performance of proactive eavesdropping in dual-hop relaying systems," in *2017 IEEE GLOBE-COM Workshops (GC Wkshps)*, 2017, pp. 1–6.
- [15] G. Ma, J. Xu, L. Duan, and R. Zhang, "Wireless surveillance of two-hop communications: (invited paper)," in *2017 IEEE 18th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2017, pp. 1–5.
- [16] L. Sun, Y. Zhang, and A. L. Swindlehurst, "Wireless physical-layer surveillance via proactive eavesdropping and alternate jamming," in *2021 IEEE Wireless Communications and Networking Conference (WCNC)*, 2021, pp. 1–7.
- [17] H. Xu and L. Sun, "Wireless surveillance via proactive eavesdropping and rotated jamming," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 11, pp. 10713–10727, 2019.
- [18] C. Zhong, X. Jiang, F. Qu, and Z. Zhang, "Multi-antenna wireless legitimate surveillance systems: Design and performance analysis," *IEEE Transactions on Wireless Communications*, vol. 16, no. 7, pp. 4585–4599, 2017.
- [19] Z. Cheng, J. Si, Z. Li, L. Guan, Y. Zhao, D. Wang, J. Cheng, and N. Al-Dhahir, "Covert surveillance via proactive eavesdropping under channel uncertainty," *IEEE Transactions on Communications*, vol. 69, no. 6, pp. 4024–4037, 2021.
- [20] Y. Hu, S. Zhang, J. Wang, Y. Li, and L. Guo, "Wireless surveillance with interference exploitation in unauthorized underlaid D2D networks," *IEEE Access*, vol. 8, pp. 123 151–123 164, 2020.
- [21] Q. Li, H. Zhang, J. Qiao, and D. Yuan, "Cooperative relay-assisted proactive eavesdropping for wireless information surveillance systems," in *2018 IEEE Global Communications Conference (GLOBECOM)*, 2018, pp. 1–6.
- [22] F. Feizi, M. Mohammadi, Z. Mobini, and C. Tellambura, "Proactive eavesdropping via jamming in full-duplex multi-antenna systems: beamforming design and antenna selection," *IEEE Transactions on Communications*, vol. 68, no. 12, pp. 7563–7577, 2020.
- [23] X. Lin, J. G. Andrews, A. Ghosh, and R. Ratasuk, "An overview of 3GPP device-to-device proximity services," *IEEE Communications Magazine*, vol. 52, no. 4, pp. 40–48, 2014.
- [24] C. Wan, D. Wu, M. Wang, X. Shi, and X. Guan, "Covert communication with power uncertainty for D2D content sharing," in *2019 11th International Conference on Wireless Communications and Signal Processing (WCSP)*, 2019, pp. 1–6.
- [25] Y. Han, R. Chen, Z. Chen, X. Liu, S. Peng, L. Fan, and D. Yu, "Distance uncertainty aided covert transmission in Internet of vehicle networks," in *2024 IEEE 24th International Conference on Communication Technology (ICCT)*, 2024, pp. 611–616.
- [26] X. Chen, Z. Chang, M. Liu, N. Zhao, T. Hämäläinen, and D. Niyato, "UAV-IRS assisted covert communication: introducing uncertainty via phase shifting," *IEEE Wireless Communications Letters*, vol. 13, no. 1, pp. 103–107, 2024.
- [27] X. Lu, S. Yan, W. Yang, M. Li, and D. W. K. Ng, "Covert communication with time uncertainty in time-critical wireless networks," *IEEE Transactions on Wireless Communications*, vol. 22, no. 2, pp. 1116–1129, 2023.
- [28] B. He, S. Yan, X. Zhou, and V. K. N. Lau, "On covert communication with noise uncertainty," *IEEE Communications Letters*, vol. 21, no. 4, pp. 941–944, 2017.
- [29] D. Wang, P. Qi, Y. Zhao, C. Li, W. Wu, and Z. Li, "Covert wireless communication with noise uncertainty in space-air-ground integrated vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 3, pp. 2784–2797, 2022.
- [30] Z. Du, W. Chen, J. Luo, H. Ding, S. Wang, and Z. Sun, "Covert communications in D2D underlaying cellular networks with dual uncertainties at the warden," *IEEE Internet of Things Journal*, vol. 12, no. 12, pp. 21 195–21 209, 2025.
- [31] H. Q. Ta and S. W. Kim, "Covert communication under channel uncertainty and noise uncertainty," in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, 2019, pp. 1–6.
- [32] R. Sun, H. Wu, B. Yang, Y. Shen, W. Yang, X. Jiang, and T. Taleb, "On covert rate in full-duplex D2D-enabled cellular networks with spectrum sharing and power control," *IEEE Transactions on Mobile Computing*, vol. 23, no. 10, pp. 9931–9945, 2024.
- [33] R. Sun, B. Yang, Y. Shen, X. Jiang, and T. Taleb, "On joint covert and secure communications in D2D-enabled cellular systems," *IEEE Transactions on Mobile Computing*, 2025.
- [34] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via jamming for rate maximization over rayleigh fading channels," *IEEE Wireless Communications Letters*, vol. 5, no. 1, pp. 80–83, 2015.
- [35] Y. Yang, B. Yang, S. Shen, Y. She, X. Jiang, and T. Taleb, "Covert communications for intelligent reflecting surface-enabled D2D networks," *IEEE Transactions on Mobile Computing*, 2025.
- [36] J. Liu, H. Nishiyama, N. Kato, and J. Guo, "On the outage probability of device-to-device-communication-enabled multichannel cellular networks: An rss-threshold-based perspective," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 1, pp. 163–175, 2015.
- [37] L. Wang, H. Tang, H. Wu, and G. L. Stüber, "Resource allocation for D2D communications underlay in rayleigh fading channels," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 2, pp. 1159–1170, 2016.
- [38] Y. Zhang, Y. Shen, X. Jiang, and S. Kasahara, "Mode selection and spectrum partition for D2D inband communications: A physical layer security perspective," *IEEE Transactions on Communications*, vol. 67, no. 1, pp. 623–638, 2018.
- [39] L. Zhang, L. Cao, D. Wei, M. Chen, Z. Chen, and S. Cui, "Cross-layer channel sounding optimization toward next-gen Wi-Fi: From model driven to data driven," *IEEE Transactions on Wireless Communications*, vol. 25, pp. 3319–3332, 2026.
- [40] T. Riihonen, S. Werner, and R. Wichman, "Mitigation of loopback self-interference in full-duplex MIMO relays," *IEEE transactions on signal processing*, vol. 59, no. 12, pp. 5983–5993, 2011.
- [41] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: Challenges and opportunities," *IEEE Journal on selected areas in communications*, vol. 32, no. 9, pp. 1637–1652, 2014.
- [42] D. Bharadia, E. McMillin, and S. Katti, "Full duplex radios," in *Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM*, 2013, pp. 375–386.
- [43] E. Ahmed and A. M. Eltawil, "All-digital self-interference cancellation technique for full-duplex systems," *IEEE Transactions on Wireless Communications*, vol. 14, no. 7, pp. 3519–3532, 2015.
- [44] K. Shahzad, X. Zhou, S. Yan, J. Hu, F. Shu, and J. Li, "Achieving covert wireless communications using a full-duplex receiver," *IEEE Transactions on Wireless Communications*, vol. 17, no. 12, pp. 8517–8530, 2018.
- [45] M. Zheng, A. Hamilton, and C. Ling, "Covert communications with a full-duplex receiver in non-coherent Rayleigh fading," *IEEE Transactions on Communications*, vol. 69, no. 3, pp. 1882–1895, 2021.
- [46] Y. Wang, S. Yan, W. Yang, C. Zhong, and D. W. K. Ng, "Probabilistic accumulate-then-transmit in wireless-powered covert communications," *IEEE Transactions on Wireless Communications*, vol. 21, no. 12, pp. 10 393–10 406, 2022.
- [47] 3GPP, "NR; User Equipment (UE) radio transmission and reception; Part 1: Range 1 Standalone," 3GPP, TS 38.101-1, V18.12.0, Rel. 18, Jan. 2026.
- [48] S. M. Kay, *Fundamentals of statistical signal processing: estimation theory*. Prentice-Hall, Inc., 1993.
- [49] B. He and X. Zhou, "Secure on-off transmission design with channel estimation errors," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 1923–1936, 2013.
- [50] K. Shahzad and X. Zhou, "Covert wireless communications under quasi-static fading with channel uncertainty," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1104–1116, 2021.
- [51] Y. Jiang, L. Wang, and H.-H. Chen, "Covert communications with randomly distributed adversaries in wireless energy harvesting enabled D2D underlaying cellular networks," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 5401–5415, 2023.

- [52] X. Chen, J. An, Z. Xiong, C. Xing, N. Zhao, F. R. Yu, and A. Nalanthan, "Covert communications: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 2, pp. 1173–1198, 2023.
- [53] 3GPP, "Service requirements for enhanced V2X scenarios," 3GPP, TS 22.186, V18.0.1, Rel. 18, May 2024.
- [54] A. L. Yuille and A. Rangarajan, "The concave-convex procedure (CCCP)," *Advances in neural information processing systems*, vol. 14, 2001.
- [55] D. Feng, G. Yu, C. Xiong, Y. Yuan-Wu, G. Y. Li, G. Feng, and S. Li, "Mode switching for energy-efficient device-to-device communications in cellular networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 12, pp. 6993–7003, 2015.
- [56] L. Zhang, Y. Sun, Z. Chen, and S. Roy, "Communications-caching-computing resource allocation for bidirectional data computation in mobile edge networks," *IEEE Transactions on Communications*, vol. 69, no. 3, pp. 1496–1509, 2021.
- [57] A. Asadi, Q. Wang, and V. Mancuso, "A survey on device-to-device communication in cellular networks," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1801–1819, 2014.
- [58] P. Mach, Z. Becvar, and T. Vanek, "In-band device-to-device communication in OFDMA cellular networks: A survey and challenges," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 1885–1922, 2015.
- [59] Y.-C. Liang, Y. Zeng, E. C. Peh, and A. T. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," *IEEE transactions on Wireless Communications*, vol. 7, no. 4, pp. 1326–1337, 2008.



Sibowang Wang received the B.E. and M.S. degrees from Jiangsu University, Zhenjiang, China, in 2017 and 2021, respectively. He is currently pursuing the Ph.D. degree at the School of Systems Information Science, Future University Hakodate, Hakodate, Japan. His research interests include physical layer security and covert wireless communication.



Bin Yang received his Ph.D. degree in systems information science from Future University Hakodate, Japan in 2015. He was a research fellow with the School of Electrical Engineering, Aalto University, Finland, from 2019 to 2021. He is currently a professor with the School of Cyber Security, Chuzhou University, China. His research focuses on cybersecurity, authentication, performance optimization, and AI driven technologies for unmanned aerial vehicle networks, satellite systems, and the Internet of Things. He also serves as an editorial board member

and Technical Committee member for several journals and conferences, such as IEEE Transactions on Communications, IEEE Global Communications Conference (GLOBECOM), IEEE World Forum on Internet of Things (WF-IoT), and International Conference on Networking and Network Applications (NaNA).

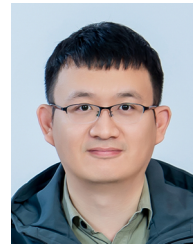


Wenhao Zhang received his B.E. degree in Computer Science from Henan University of Science and Technology, Luoyang, China, in 2015, and the M.S. and Ph.D. degrees in Systems Information Science from Future University Hakodate, Hakodate, Japan, in 2020 and 2024, respectively. He is currently a Lecturer at the College of Cyber Security, Tarim University, Xinjiang, China. His research interests include covert wireless communication in the physical layer and unmanned aerial vehicle networks.



has also served on the technical program committees of several international conferences, including ICEBE, INCoS, CIS, and SOWN.

Yulong Shen received the B.S. and M.S. degrees in computer science and the Ph.D. degree in cryptography from Xidian University, Xi'an, China, in 2002, 2005, and 2008, respectively. He is currently a Professor with the School of Computer Science and Technology, Xidian University, where he is also an Associate Director of the Shaanxi Key Laboratory of Network and System Security and a member of the State Key Laboratory of Integrated Services Networks. His research interests include wireless network security and cloud computing security. He



Information Fusion, Computer Networks, Journal of Systems Architecture, Ad Hoc Networks, etc. His homepage is <https://www.zqliu.com>.

Zhiquan Liu received the B.S. degree from the School of Science, Xidian University, Xi'an, China, in 2012, and the Ph.D. degree from the School of Computer Science and Technology, Xidian University in 2017. He is currently a full professor with the College of Cyber Security, Jinan University, Guangzhou, China. His current research focuses on security, trust, privacy, and intelligence in vehicular networks. He currently serves as the area editor or associate editor of multiple SCI-index journals, such as IEEE TIFS, IEEE TDSC, IEEE TII, IEEE IOTJ,



Communications, IEEE Transactions on Parallel and Distributed Systems, and IEEE INFOCOM. His research interests include computer communications networks, mainly wireless networks and optical networks, network security, and router/switch design.

Xiaohong Jiang received the B.S., M.S., and Ph.D. degrees from Xidian University, China, in 1989, 1992, and 1999, respectively. He was an associate professor with Tohoku University from 2005 to 2010. He is currently a full professor with Future University Hakodate, Japan. He has authored or coauthored more than 300 technical papers in premier international journals and conferences, including over 70 papers published in top IEEE journals and conferences, such as IEEE/ACM Transactions on Networking, IEEE Journal on Selected Areas in



reer, he served as a Senior Researcher and 3GPP Standards Expert at NEC Europe Ltd., Heidelberg, Germany, where he contributed to the evolution of mobile network architectures and standardization activities. Before joining NEC, he was an Assistant Professor at the Graduate School of Information Sciences, Tohoku University, Japan, working in a research laboratory fully funded by KDDI. He also held a Research Fellowship at the Intelligent Cosmos Research Institute, Japan, from 2005 to 2006. Prof. Taleb is widely recognized for his pioneering contributions to mobile network softwareization, network slicing, cloud-edge continuum management, and autonomous networking. His current research interests include autonomous network and service management, edge-cloud continuum systems, network softwareization and slicing, software-defined security, and AI-native communication networks.

Tarik Taleb received the B.E. degree with distinction in Information Engineering and the M.Sc. and Ph.D. degrees in Information Sciences from Tohoku University, Sendai, Japan, in 2001, 2003, and 2005, respectively. He is currently a Full Professor at Ruhr University Bochum (RUB), Germany, where he leads research activities on next-generation mobile and distributed systems. Prior to joining RUB, he was a Professor at the University of Oulu, Finland (2018–2023), and an Associate Professor at Aalto University, Finland (2014–2021). Earlier in his