Safeguarding ISAC Performance in Low-Altitude Wireless Networks Under Channel Access Attack

Jiacheng Wang, *Member, IEEE*, Jialing He, *Member, IEEE*, Geng Sun, *Senior Member, IEEE*, Zehui Xiong, *Senior Member, IEEE*, Dusit Niyato, *Fellow, IEEE*, Shiwen Mao, *Fellow, IEEE*, Dong In Kim, *Life Fellow, IEEE*, and Tao Xiang, *Senior Member, IEEE*

***Abstract*—The increasing saturation of terrestrial resources has driven the exploration of low-altitude applications such as air taxis. Low altitude wireless networks (LAWNs) serve as the foundation for these applications, and integrated sensing and communication (ISAC) constitutes one of the core technologies within LAWNs. However, the open nature of low-altitude airspace makes LAWNs vulnerable to malicious channel access attacks, which degrade the ISAC performance. Therefore, this paper develops a game-based framework to mitigate the influence of the attacks on LAWNs. Concretely, we first derive expressions of communication data's signal-to-interference-plus-noise ratio and the age of information of sensing data under attack conditions, which serve as quality of service metrics. Then, we formulate the ISAC performance optimization problem as a Stackelberg game, where the attacker acts as the leader, and the legitimate drone and the ground ISAC base station act as second and first followers, respectively. On this basis, we design a backward induction algorithm that achieves the Stackelberg equilibrium while maximizing the utilities of all participants, thereby mitigating the attack-induced degradation of ISAC performance in LAWNs. We further prove the existence of the equilibrium. Simulation results show that the proposed algorithm outperforms existing baselines and a static Nash equilibrium benchmark, ensuring that LAWNs can provide reliable service for low-altitude applications.**

***Index Terms*—Low-altitude wireless networks (LAWNs), integrated sensing and communication (ISAC), channel access attack, Stackelberg game.**

Received 5 August 2025; revised 26 February 2026 and 11 March 2026; accepted 12 March 2026. Date of publication 18 March 2026; date of current version 25 March 2026. This work was supported in part by the Seatrium New Energy Laboratory, Singapore Ministry of Education (MOE) Tier 1, under Grant RT5/23 and Grant RG24/24; in part by the Nanyang Technological University (NTU) Centre for Computational Technologies in Finance (NTU-CCTF); in part by the Research Innovation and Enterprise (RIE) 2025 Industry Alignment Fund-Industry Collaboration Projects (IAF-ICP), administered by Agency for Science, Technology and Research (A*STAR) under Award I2301E0026; in part by the National Natural Science Foundation of China under Grant 62302071; and in part by the Institute of Information and Communications Technology Planning and Evaluation (IITP)-Information communication Technology (ICT) Creative Consilience Program funded by Korean Government Ministry of Science and ICT (MSIT) under Grant IITP-2026-RS-2020-II201821. The associate editor coordinating the review of this article and approving it for publication was Prof. Ning Xie. *(Corresponding author: Jialing He.)*

Jiacheng Wang and Dusit Niyato are with the College of Computing and Data Science, Nanyang Technological University, Singapore 639798 (e-mail: jiacheng.wang@ntu.edu.sg; dniyato@ntu.edu.sg).

Jialing He and Tao Xiang are with the College of Computer Science, Chongqing University, Chongqing 400044, China (e-mail: hejialing@cqu.edu.cn; txiang@cqu.edu.cn).

Geng Sun is with the College of Computer Science and Technology, Jilin University, Changchun 130012, China (e-mail: sungeng@jlu.edu.cn).

Zehui Xiong is with the School of Electronics, Electrical Engineering and Computer Science (EEECS), Queen's University Belfast, BT7 1NN Belfast, U.K. (e-mail: z.xiong@qub.ac.uk).

Shiwen Mao is with the Department of Electrical and Computer Engineering, Auburn University, Auburn, AL 36849 USA (e-mail: smao@ieee.org).

Dong In Kim is with the Department of Electrical and Computer Engineering, Sungkyunkwan University, Suwon 16419, South Korea (e-mail: dongin@skku.edu).

Digital Object Identifier 10.1109/TIFS.2026.3675426

I. Introduction

As GROUND resources become increasingly constrained, the focus of economic development is gradually shifting from the ground to the low-altitude airspace [1], [2]. In this domain, various applications, such as low-altitude logistics and urban air taxi, are emerging [3]. For instance, drones can expedite parcel deliveries, while autonomous electric vertical take-off and landing (eVTOL) vehicles can service as the air taxi to relieve stress of ground transportation [4]. To support these low-altitude applications, low-altitude wireless networks (LAWNs) become a crucial enabling infrastructure. LAWNs provide the communication, computing, and control capability needed to coordinate the operations of the low-altitude drones [5], [6]. In essence, LAWNs connect low-altitude vehicles to ground base stations (BSs) and with each other, thereby enabling real-time data exchange, decision making, and remote control.

One of the core technologies in LAWNs is integrated sensing and communication (ISAC), which can simultaneously provide data exchange and environmental sensing functions [7]. This indicates the transmitted signals can not only carry information, but also act as probes that detect obstacles or track time-sensitive targets. For example, by sending out the wireless signal, a ground ISAC BS can communicate with drones and scan the surroundings to collect sensing data [8], which can enable quick reactions for applications such as air traffic management. Moreover, drones equipped with reconfigurable intelligent surfaces (RIS) can even dynamically reflect and shape signals, thereby extending coverage and supporting more low-altitude applications [9].

While appealing, the openness of the low-altitude airspace exposes LAWNs to significant security threats. A particular threat is the channel access attack [10], wherein an attacker can jam the wireless channels, thereby preventing drones from receiving updates, increasing the risk of air traffic accidents. In response, researchers have developed various defense strategies. In [11], a drone recycles artificial noise for joint

1556-6021 © 2026 IEEE. All rights reserved, including rights for text and data mining, and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: Auburn University. Downloaded on March 26,2026 at 04:01:58 UTC from IEEE Xplore. Restrictions apply.

jamming and sensing, while Kalman filtering with a neural network predictor adapts its trajectory and resources to deter eavesdropping. Beyond waveform-level defenses, researchers have developed secure protocols to protect data integrity and confidentiality in adversarial settings [12], designed robust channel-access strategies that sustain reliable detection and data exchange under jamming [13], and applied blockchain-based encryption schemes to strengthen the security and privacy of drone data [14]. These studies assume a static and nonadaptive attacker. In practice, however, an attacker can dynamically vary its strategy by switching frequencies or adjusting jamming power. Ignoring this adaptability makes it difficult to analyze the hierarchical and iterative game between the attacker and LAWNs and leads to weaker defenses.

To address these challenges, this paper proposes a defense framework by modeling the interactions between the channel access attacker and LAWNs as a Stackelberg game to optimize the ISAC performance. The attacker, acting as the leader, selects its attack strategy first, while the defenders (legitimate drones and base stations) adjust their responses to mitigate the attack. This framework is particularly suitable for dynamic attack scenarios, where the attacker's actions evolve based on the defenders' responses. Similar game-theoretic models have been used in wireless networks to address jamming and interference [15], [16], [17], reinforcing the validity of using a Stackelberg game to capture the strategic interaction between attackers and defenders in LAWNs. The main contributions of this paper are summarized below.

- We propose an age of information (AoI)-based metric to describe the freshness of sensing data in LAWNs. This metric inherently captures the temporal dynamics and the freshness of the information about the state of a time-sensitive target, crucial for low-altitude applications.
- We formulate a Stackelberg game-based ISAC performance optimization problem for time-sensitive target under channel access attacks, where the attacker, legitimate drone, and ISAC BS act as the game leader, second follower, and first follower, respectively. The model can analyze the hierarchical confrontation relationship and game iteration process between the attacker and LAWNs, making LAWNs capable of handling dynamic attacks.
- We design a backward induction (BI)-based algorithm to solve the optimization problem. We further theoretically prove the existence of the Stackelberg equilibrium for the formulated game and show that the equilibrium maximizes the utilities of all players.
- Under the typical parameter settings, the proposed BI-based algorithm can realize an average sensing AoI of 2.236 and an average communication SINR of 0.576. In the RIS-element evaluation, the proposed scheme achieves utilities of 0.571 and −3.895 for the RIS and BS, respectively, while the average allocation baseline is 0.517 and −6.28, and the random allocation baseline is 0.256 and −46.718.

The paper is organized as follows. Section II reviews related work. Section III gives the system model. Section IV derives the communication signal to interference plus noise ratio (SINR) and the freshness of sensing data. Section V formulates the Stackelberg game and presents the solution. Section VI reports evaluation results. The open issues are discussed in Section VII. Section VIII concludes the paper.

II. Related Work

This section surveys recent progress on ISAC performance optimization in LAWNs and game-theoretic defense of ISAC, thereby summarizing the current research challenges and gaps.

A. ISAC Performance Optimization in LAWNs

ISAC enables both wireless sensing and communication using the shared network resources, which can improve LAWNs efficiency [18]. In [19], the authors modeled the drone as a low altitude platform and adopted an alternating optimization scheme that jointly optimizes task allocation, computing resources, and transmit and receive beamforming, reducing system energy consumption by up to 54.12%. The authors in [20] maximized the drone's achievable rate with the sensing frequency and beam pattern gain constraints. By jointly optimizing drone trajectory, user association, target sensing selection, and transmit beamforming, the system's sum rate can reach to 12 bps/Hz. Besides, the authors in [21] formulated the drone trajectory design as a weighted optimization problem and propose a multi-stage optimization algorithm to obtain the optimal while optimizing ISAC performance.

From the antenna design perspective, the authors in [22] proposed a movable-antenna array-enabled ISAC system for low-altitude applications, which adjusts the antenna array's positions via the alternation optimization to improve achievable data rate and beamforming gain. In [22], the authors design an ISAC system for low-altitude scenarios that employs a movable antenna array. By alternately optimizing the array's positions, the system raises both the achievable data rate and the beamforming gain. The authors in [23] focus on signal design and develop a low-altitude ISAC system where deep reinforcement learning (DRL) jointly optimizes BS beamforming and drone trajectories, enhancing the communication sum rate while satisfying sensing constraints. As can be seen, current studies optimize ISAC in LAWNs through resource allocation, UAV trajectory planning, and related methods [24]. However, the openness of the low altitude airspace exposes sensing and communication to wireless attacks, hence maintaining ISAC performance under attack is essential.

B. Game-Theoretic Defense of ISAC in LAWNs

Game theory models the strategic interaction between attackers and defenders, providing a foundation for designing resilient ISAC in LAWNs. For instance, in [25], the authors formulate a Bayesian Stackelberg game where the BS (leader) optimizes the transmit precoder and the jammer (follower) selects its power. Using semidefinite relaxation with Gaussian randomization, they derive closed-form strategies, and simulations show the Stackelberg equilibrium yields higher utility than baseline methods. To safeguard the ISAC BS from a mobile hostile drone, the authors in [26] constructed a non-cooperative Stackelberg game and proposed a DRL algorithm to jointly refine resource allocation and drone trajectory,

Authorized licensed use limited to: Auburn University. Downloaded on March 26,2026 at 04:01:58 UTC from IEEE Xplore. Restrictions apply.



Fig. 1. System model of the LAWNs under channel access attack. Here, the malicious UAV first launches an attack by injecting additional noise to the wireless channel. In response, the legitimate UAV with RIS and BS respectively adjust the gain and sensing data generation rate to mitigate the impact of the attack, thereby maintaining the ISAC performance.

thereby enhancing secrecy rate, radar accuracy, and energy efficiency. In [27], the authors tackle resource allocation under composite jamming and interchannel interference by embedding game theory into a DRL framework, which maximizes the communication rate and sensing power, outperforming baseline methods on both sensing and communication metrics.

For drone-aided traffic monitoring, the authors in [28] formulated a three-layer Stackelberg game that jointly determines sensing rate, transmission power, and attack power, attaining an age-of-information (AoI) minimum via subgradient updates. In multi-channel IoT networks subject to dynamic access attacks, the authors in [29] recast channel selection as two ordinary potential games, prove the existence of Nash equilibrium, and design a reinforcement-learning algorithm that converges to them, yielding lower AoI. To support personalized anti-jamming in heterogeneous drone swarms, the authors in [30] modeled the channel-and-power selection problem as an adversarial game with a unique equilibrium and propose a personalized federated soft actor-critic algorithm that markedly improves interference resilience. As can be seen, prior studies have shown that game theoretic defenses are effective across wireless networks [31]. Hence, we cast ISAC performance optimization for time-sensitive targets under channel access attack as a Stackelberg game, enabling LAWNs to provide secure and efficient services.

III. System Model

This section established the LAWN system model, signal model, wireless channel model, and attack model, serving as the basis for the ISAC performance indicators.

A. Low Altitude Wireless Network Model

Figure 1 presents the low-altitude scenario supported by LAWNs, which includes the dual-function ISAC BS, mobile users, legitimate drone equipped with RIS for communication and sensing, time-sensitive targets, and the illegitimate drone for channel access attack. Specifically, the ISAC BS is equipped with multiple antennas that support communication with multiple users and drones while transmitting sensing waveforms to detect nearby targets. Legitimate low-altitude drones equipped with RIS can communicate with the BS and relay both communication and sensing services to targets beyond the base station's reach. Moreover, we consider a malicious drone that executes a channel-access attack aimed at degrading the ISAC performance of the LAWNs. For ease of presentation, the main symbols and their meanings are presented in Table I.

TABLE I
Notation Table

Symbol	Meaning
$\mathbf{B}_r$	Sensing beamforming matrix
$\mathbf{B}_c$	Communication beamforming matrix
$\mathbf{s}$	Transmitted ISAC signal
$\mathbf{s}_r$	Sensing signal vector
$\mathbf{s}_c$	Communication symbol vector
$\mathbf{B}$	ISAC beamforming matrix
$\mathbf{R}$	Transmit-signal covariance matrix
$\mathbf{R}_i$	User-i rank-1 covariance matrix
$\mathbf{H}$	BS–RIS channel matrix
$\mathbf{h}_{1,i}$	RIS–user i channel vector
$\mathbf{h}_{2,i}$	BS–user i channel vector
$\mathbf{\Phi}$	RIS reflection coefficient matrix
g	RIS amplification gain
$g_{\max}$	Maximum RIS amplification gain
n_{att}	Attacker-added noise
σ^2_{att}	Attacker noise power density
σ^2	Environmental noise power density
σ^2_y	User noise power density
σ^2_r	BS noise power density
$SINR_i^{\text{com}}$	Communication SINR of user i
$SINR^{\text{sense}}$	Sensing SINR at the BS
η	System bandwidth
γ_{sense}	Sensing transmission (service) rate
$AoI(t)$	AoI at time t
$AAoI$	Average AoI
λ	Sensing data generation rate
ρ	Queue utilization factor
$ASINR$	Average communication SINR
ϕ_{BS}	Base-station utility
ϕ_{att}	Attacker utility

B. ISAC Signal Model at BS

Let (x_{BS}, y_{BS}, z_{BS}) be the location of the BS, M represents the number of transmitting antenna of BS, and $\mathbf{s}_r \in \mathbb{C}^{M\times 1}$ and $\mathbf{s}_c \in \mathbb{C}^{N\times 1}$ be the sensing signal and communication symbol to N users, respectively. Therefore, we denote $\mathbf{B}_{\text{r}} = [\text{b}_{\text{r},1}, \text{b}_{\text{r},2}, \ldots, \text{b}_{\text{r},M}] \in \mathbb{C}^{M\times M}$ and $\mathbf{B}_{\text{c}} = [\text{b}_{\text{c},1}, \text{b}_{\text{c},2}, \ldots, \text{b}_{\text{c},N}] \in \mathbb{C}^{M\times N}$ as the beamforming matrices for sensing and communication signals, and then the transmitted signal of BS can be expressed as

$$\mathbf{s} = \mathbf{B}_{\text{r}}\mathbf{s}_{\text{r}} + \mathbf{B}_{\text{c}}\mathbf{s}_{\text{c}} = [\mathbf{B}_{\text{r}}, \mathbf{B}_{\text{c}}][(\mathbf{s}_{\text{r}})^{\text{T}}, (\mathbf{s}_{\text{c}})^{\text{T}}]^{\text{T}} = \mathbf{B}\hat{\mathbf{s}}, \tag{1}$$

where $\mathbf{B} \in \mathbb{C}^{M\times(M+N)}$ is the ISAC transmission beamforming matrix. Without loss of generality, according to [32], the sensing signal can be generated through the pseudo-random

Authorized licensed use limited to: Auburn University. Downloaded on March 26,2026 at 04:01:58 UTC from IEEE Xplore. Restrictions apply.

coding with $\mathbb{E}[\mathbf{s}] = \mathbf{0}$ and $\mathbb{E}\left[\mathbf{s}\mathbf{s}^{\mathrm{T}}\right] = \mathbf{I}_M$. On this basis, let the transmission symbol $\mathbf{s}_{\mathrm{c}}$ satisfies $\mathcal{CN}(\mathbf{0}, \mathbf{I}_K)$, then the covariance matrix of the transmitted signal is determined as

$$\mathbf{R} = \mathbb{E}\left[\mathbf{s}\mathbf{s}^{\mathrm{H}}\right] = \mathbf{B}\mathbf{B}^{\mathrm{H}} = \mathbf{B}_{\mathrm{r}}\mathbf{B}_{\mathrm{r}}^{\mathrm{H}} + \sum_{i=1}^{N} \mathbf{R}_i, \tag{2}$$

where $\mathbf{R}_i$ is the rank-1 matrix, calculated as $\mathbf{R}_i = \mathrm{b}_{\mathrm{c},i}\mathrm{b}_{\mathrm{c},i}^{\mathrm{H}}$.

C. Wireless Channel Model

Let the RIS of legitimate drone has P reflecting elements, then the wireless channel between BS and drone, drone and the i-th user, and BS and the i-th user, can be denoted as $\mathbf{H} \in \mathbb{C}^{P\times M}$, $\mathbf{h}_{1,i} \in \mathbb{C}^{P\times 1}$, and $\mathbf{h}_{2,i} \in \mathbb{C}^{M\times 1}$, respectively. On this basis, the BS receives the wireless signals and estimates the channel state information (CSI). In the considered LAWNs, the communication link can be modeled as the large-scale fading channel, and the path loss can be calculated as

$$\begin{aligned} Loss\,[dB] = {} & 10\beta_1 \log_{10}\left(\frac{r_s}{r_0}\right) + \beta_2 \\ & + 10\beta_3 \log_{10}\left(\frac{f_s}{f_0}\right) + \beta_4, \end{aligned} \tag{3}$$

where β_1 and β_3 are the coefficients indicating the impact of path loss on distance and frequency aspects, respectively, β_2 is the optimized offset for path loss, r_s and f_s represent the distance from the transmitter to receiver and the carrier frequency, respectively, and $r_0 = 1$ m and $f_0 = 1$ GHz are the reference for distance and frequency metrics, respectively. Moreover, β_4 denotes the signal's large-scale fluctuations due to random shadowing on the mean path loss over distance.

Given that the communication users are distributed with densely surrounded scatters, the channel ($\mathbf{h}_{1,i}$) between drone and the i-th user, as well as the channel ($\mathbf{h}_{2,i}$) between BS and the i-th user can be represented by the Rayleigh fading channels. Meanwhile, as the link between the BS and the drone comprises both line-of-sight (LoS) and non-line-of-sight (NLoS) components, then the corresponding channel ($\mathbf{H}$) between BS and drone can be represented by the Rician fading channel. More concretely, for the Rician fading channel, the NLoS component $\mathbf{H}_{NLoS}$ follows the complex normal distribution with zero-mean vector and the covariance that is the Kronecker product of Σ_{BS} and Σ_{RIS}, indicating

$$\mathbf{H}_{NLoS} \sim \mathcal{CN}(\mathbf{0}, \Sigma_{RIS} \otimes \Sigma_{BS}). \tag{4}$$

Here, $\Sigma_{BS} \geq 0$ and $\Sigma_{RIS} \geq 0$ represent the spatial correlation matrices with unit diagonal elements at BS and drone, respectively. Additionally, the LoS part $\mathbf{H}_{LoS}$ in the Rician fading channel can be defined as

$$\mathbf{H}_{LoS} = \mathrm{a}_2(\theta_2)\,\mathrm{a}_1^{\mathrm{H}}(\theta_1), \tag{5}$$

where θ_1 is the the angle of departure (AoD) at the BS, θ_2 is the angle of arrival (AoA) at the drone. Besides, $\mathrm{a}_1(\theta_1)$ and $\mathrm{a}_2(\theta_2)$ represent the array response vectors of the antennas from BS and drone, which are expressed as

$$\mathrm{a}_1(\theta_1) = \left[1, e^{-j2\pi d_{BS}\frac{\sin(\theta_1)}{\omega}}, \ldots, e^{-j2\pi d_{BS}(M-1)\frac{\sin(\theta_1)}{\omega}}\right]^{\mathrm{T}} \tag{6}$$

and

$$\mathrm{a}_2(\theta_2) = \left[1, e^{-j2\pi d_{RIS}\frac{\sin(\theta_2)}{\omega}}, \ldots, e^{-j2\pi d_{RIS}(P-1)\frac{\sin(\theta_2)}{\omega}}\right]^{\mathrm{T}}, \tag{7}$$

respectively, where d_{BS} represents the antenna spacing at the BS, d_{RIS} is the element spacing distance of the RIS at drone, and ω is the wavelength of the transmitted signal. For ease of computation, as well as the AoA and AoD estimations, both d_{BS} and d_{RIS} are set to $\omega/2$.

As for the target sensing aspect, similar to (6) and (7), let θ_3 be the AoA of the RIS, then the channel response matrix between drone and the target can be obtained

$$\mathbf{T} = \beta_5 \mathrm{a}_3(\theta_3)\,\mathrm{a}_3^{\mathrm{H}}(\theta_3) \in \mathbb{C}^{P\times P}, \tag{8}$$

where the amplitude β_5 is the multiplicative fading of the drone-based target sensing channel. Based on [33], the target acts as a single scattering object and the its loss and gain factors are negligible. Hence, the energy of the sensing signal reflected from the RIS and received at the BS is calculated as

$$P_{sense} = P_{trans}G^2\omega^2 S \,/\, (4\pi)^3 R^4, \tag{9}$$

where P_{trans} and G are the transmission power and antenna gain for sending the sensing signal, respectively, S is the target's radar cross section (RCS), and R represents the distance between drone and target. By treating the drone as the monostatic multiple-input and multiple-output radar, the path loss of the drone-based sensing link (β_5) can be calculated as

$$\beta_5 = \sqrt{\omega^2 S \,/\, (4\pi)^3 R^4}. \tag{10}$$

D. Legitimate Drone Model

For the RIS deployed on the drone, its reflecting coefficient matrix can be denoted as $\mathbf{\Phi} = \mathrm{Diag}\left(\left[g_1, \ldots, g_i, \ldots, g_P\right]\right)$. Note that due to the limited energy supply of the drone, we let the power amplification gain of all the RIS's reflecting elements to be the same, indicating $|g_1|^2 = \cdots = |g_P|^2 = g^2$. In addition, the maximum power amplification gain of the reflecting element is denoted by g_{max}, and the RIS position is represented by the coordinates $(x_{RIS}, y_{RIS}, z_{RIS})$. On this basis, as presented in Fig. 1, the RIS facilitates two kinds of signal reflections. First, it redirects the signals transmitted by the BS toward both the users (for communication) and the time-sensitive target (for sensing). Then, the echo signal returning from the time-sensitive target is reflected back to the BS. According to [34], the above reflections is:

$$\mathbf{r}_1^{refle} = \mathbf{\Phi}\mathbf{H}\mathbf{s} + \mathbf{\Phi}\mathbf{n}_1, \tag{11}$$

$$\mathbf{r}_2^{refle} = \mathbf{\Phi}^{\mathrm{H}}\mathbf{T}\mathbf{\Phi}\mathbf{H}\mathbf{s} + \mathbf{\Phi}^{\mathrm{H}}\mathbf{T}\mathbf{\Phi}\mathbf{n}_1 + \mathbf{\Phi}^{\mathrm{H}}\mathbf{n}_2, \tag{12}$$

where $\mathbf{n}_1 \sim \mathcal{CN}\left(\mathbf{0}, \sigma^2\mathbf{I}_K\right)$ and $\mathbf{n}_2 \sim \mathcal{CN}\left(\mathbf{0}, \sigma^2\mathbf{I}_K\right)$ are the additive white Gaussian noise (AWGN) at the RIS end with the same distribution of the noise power σ^2.

E. Channel Access Attack Drone Model

To attack various applications supported by LAWNs, the malicious drone first launches the channel access attack [10], that is spoofing the medium access control (MAC) protocol and then invading the communication and sensing channel.

Authorized licensed use limited to: Auburn University. Downloaded on March 26,2026 at 04:01:58 UTC from IEEE Xplore. Restrictions apply.

After obtaining access, it further adds the extra noise into the channels, including the channels between BS and drone, drone and user, BS and user, and drone and target, thereby degrading the ISAC performance of LAWNs. Moreover, to lower the probability of being detected, we consider that the added noise of the attacker, denoted as $\mathbf{n}_{att}$, has the same distribution as the AWGN, whose power density is σ_{att}^2 with the maximum value of σ^2. For example, for the channel from drone to the users, after the channel access attack is launched, the attacker adds the noise with distribution of $\mathbf{n}_{att} \sim \mathcal{CN}\left(\mathbf{0}, \sigma_{att}^2 \mathbf{I}_K\right)$.

IV. ISAC Performance of Time-Sensitive Target Under Attack

This section characterizes ISAC degradation under channel access attacks by analyzing the attacked communication SINR and sensing data's freshness performances.

A. Communication SINR Analysis

With the help of an RIS on the drone, the users can receive communication signals from two propagation paths, including the direct link from the BS to users, as well as the reflected link from drone to users. Building on this, the signal received by the i-th user can be expressed as

$$\mathbf{r}_{c,i}^{com} = \mathbf{h}_{1,i}^{\mathrm{H}} \mathbf{\Phi} \mathbf{H} \mathbf{s} + \mathbf{h}_{1,i}^{\mathrm{H}} \mathbf{\Phi} \mathbf{n}_1 + \mathbf{h}_{2,i}^{\mathrm{H}} \mathbf{s} + \mathrm{y}_i, \tag{13}$$

where y_i is the AWGN at the user with the variance of σ_{y}^2. Considering the channel access attack, after defining the equivalent channel between BS and the i-th user as $\mathbf{h}_i^{\mathrm{H}} = \mathbf{h}_{1,i}^{\mathrm{H}} \mathbf{\Phi} \mathbf{H} + \mathbf{h}_{2,i}^{\mathrm{H}}$, then the SINR of the i-th user is evaluated as

$$\mathrm{SINR}_i^{\mathrm{com}} = \frac{\mathbf{h}_i^{\mathrm{H}} \mathbf{R}_i \mathbf{h}_i}{\mathbf{h}_i^{\mathrm{H}} \left(\mathbf{R} - \mathbf{R}_i\right) \mathbf{h}_i + \left(\sigma^2 + \sigma_{\mathrm{att}}^2\right) \mathbf{h}_{1,i}^{\mathrm{H}} \mathbf{\Phi} \mathbf{\Phi}^{\mathrm{H}} \mathbf{h}_{1,i} + \left(\sigma_{\mathrm{att}}^2 + \sigma_{\mathrm{y}}^2\right)}. \tag{14}$$

B. Freshness of Sensing Data

In the considered low-altitude airspace, for tracking the time-sensitive target, the SINR metric primarily reflects the instantaneous quality of the received signal for a single measurement. A higher SINR indicates a stronger and better signal at a specific moment. However, it does not inherently capture the temporal dynamics and the freshness of the information about the target's state. Such a state is crucial, especially for those applications that require fast response, such as an air taxi. To quantify information freshness, the AoI metric is required. Hence, in this section, we analyze sensing data freshness by deriving closed-form AoI expressions using queuing theory.

1) Transmission of Sensing Data: During sensing, the BS receives the echo signals reflected from RIS of drone, which contain three main components, including the thermal noise produced at both the BS and drone, the self-interference term that propagates along the BS–drone–BS path, and the desired sensing signals that travels via the BS–drone–target–drone–BS route. As the BS–drone–BS component conveys no information about the target, it is treated like interference. Hence, the aggregated signals at the BS can be expressed as

$$\begin{aligned} \tilde{\mathbf{r}}^{\mathrm{BS}} &= \mathbf{H}^{\mathrm{H}} \left(\mathbf{r}_1^{\mathrm{refle}} + \mathbf{r}_2^{\mathrm{refle}}\right) + \mathbf{w}_r \\ &= \mathbf{H}^{\mathrm{H}} \mathbf{\Phi}^{\mathrm{H}} \mathbf{T} \mathbf{\Phi} \mathbf{H} \mathbf{s} + \mathbf{H}^{\mathrm{H}} \mathbf{\Phi}^{\mathrm{H}} \mathbf{T} \mathbf{\Phi} \mathbf{n}_1 + \mathbf{H}^{\mathrm{H}} \mathbf{\Phi} \mathbf{n}_1 \\ &\quad + \mathbf{H}^{\mathrm{H}} \mathbf{\Phi}^{\mathrm{H}} \mathbf{n}_2 + \mathbf{H}^{\mathrm{H}} \mathbf{\Phi} \mathbf{H} \mathbf{s} + \mathbf{w}_r, \end{aligned} \tag{15}$$

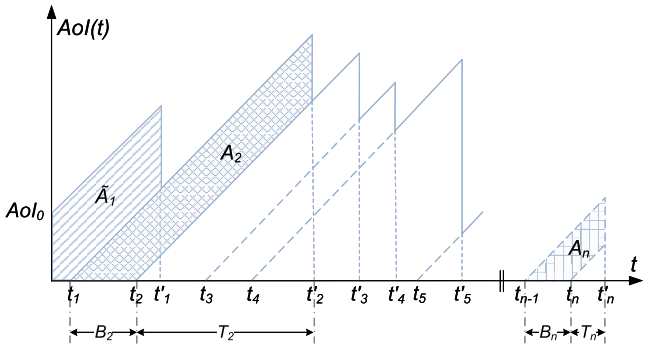


Fig. 2. The modeling of the AoI metric.

where $\mathbf{H}^{\mathrm{H}} \mathbf{\Phi} \mathbf{H} \mathbf{s}$ is the interference echo, and $\mathbf{w}_r$ is the AWGN at the BS end, σ_r^2 is the noise power density, and $\mathbf{w}_r \sim \mathcal{CN}\left(\mathbf{0}, \sigma_r^2 \mathbf{I}_M\right)$. With the aid of the self-interference (SI) cancellation, the interference echo can be alleviated. Therefore, in the presence of the channel access attack, the received sensing signal can be further expressed as

$$\begin{aligned} \mathbf{r}^{\mathrm{BS}} &= \mathbf{H}^{\mathrm{H}} \mathbf{\Phi}^{\mathrm{H}} \mathbf{T} \mathbf{\Phi} \mathbf{H} \mathbf{s} + \mathbf{H}^{\mathrm{H}} \mathbf{\Phi}^{\mathrm{H}} \mathbf{T} \mathbf{\Phi} \mathbf{n}_1' + \mathbf{H}^{\mathrm{H}} \mathbf{\Phi} \mathbf{n}_1' \\ &\quad + \mathbf{H}^{\mathrm{H}} \mathbf{\Phi}^{\mathrm{H}} \mathbf{n}_2' + \varepsilon \mathbf{H}^{\mathrm{H}} \mathbf{\Phi} \mathbf{H} \mathbf{s} + \mathbf{w}'_r, \end{aligned} \tag{16}$$

where ε represents the SI coefficient, $\mathbf{n}'_1 \sim \mathcal{CN}\left(\mathbf{0}, \left(\sigma^2 + \sigma_{att}^2\right) \mathbf{I}_K\right)$, $\mathbf{n}'_2 \sim \mathcal{CN}\left(\mathbf{0}, \left(\sigma^2 + \sigma_{att}^2\right) \mathbf{I}_K\right)$, and $\mathbf{w}'_r \sim \mathcal{CN}\left(\mathbf{0}, \left(\sigma_r^2 + \sigma_{att}^2\right) \mathbf{I}_M\right)$. On this basis, the interference-plus-noise covariance matrix is calculated as

$$\mathbf{J} = \mathbf{Z} + \mathbf{C} \mathbf{R} \mathbf{C}^{\mathrm{H}}, \tag{17}$$

where

$$\begin{aligned} \mathbf{Z} &= \left(\sigma^2 + \sigma_{att}^2\right) \left(\mathbf{H}^{\mathrm{H}} \mathbf{\Phi} \mathbf{\Phi}^{\mathrm{H}} \mathbf{T} \mathbf{\Phi} \mathbf{H} + \mathbf{H}^{\mathrm{H}} \mathbf{\Phi}^{\mathrm{H}} \mathbf{T} \mathbf{\Phi} \mathbf{\Phi}^{\mathrm{H}} \mathbf{H}\right) \\ &\quad + \left(\sigma^2 + \sigma_{att}^2\right) \mathbf{X} \mathbf{X}^{\mathrm{H}} + 2\left(\sigma^2 + \sigma_{att}^2\right) \mathbf{H}^{\mathrm{H}} \mathbf{\Phi}^{\mathrm{H}} \mathbf{\Phi} \mathbf{H} \\ &\quad + \left(\sigma_r^2 + \sigma_{att}^2\right) \mathbf{I}_M \end{aligned} \tag{18}$$

represents the equivalent noise covariance matrix, $\mathbf{X} = \mathbf{H}^{\mathrm{H}} \mathbf{\Phi}^{\mathrm{H}} \mathbf{T} \mathbf{\Phi} \in \mathbb{C}^{M \times P}$, and $\mathbf{C} = \varepsilon \mathbf{H}^{\mathrm{H}} \mathbf{\Phi} \mathbf{H}$. On this basis, by defining $\mathbf{F} = \mathbf{H}^{\mathrm{H}} \mathbf{\Phi}^{\mathrm{H}} \mathbf{T} \mathbf{\Phi} \mathbf{H} \in \mathbb{C}^{M \times M}$, the SINR of the sensing signal can be obtained

$$\mathrm{SINR}^{sense} = \mathrm{Tr}\left(\mathbf{F} \mathbf{R} \mathbf{F}^{\mathrm{H}} \mathbf{J}^{-1}\right), \tag{19}$$

where $\mathrm{Tr}(\cdot)$ is the trace calculator. Finally we let η represent the bandwidth of the BS, then the transmission rate of the sensing signal can be evaluated as

$$\gamma_{sense} = \eta \log_2\left(1 + \mathrm{SINR}^{sense}\right). \tag{20}$$

2) Average AoI of Sensing Data: As shown in Fig. 2, the AoI curve can be represented by the sawtooth function, where the sensing data AoI first increases with time increasing. When the sensing data is successfully received by the BS, the AoI value decreases immediately. Based on queuing theory, the sensing data generated by the BS can be regarded as the customer, while the wireless links (from BS to drone, drone to target, target to drone, and drone to BS) can act as the server. Let AoI_0 be the initial AoI value of sensing data at $t = 0$, t_i be

Authorized licensed use limited to: Auburn University. Downloaded on March 26,2026 at 04:01:58 UTC from IEEE Xplore. Restrictions apply.

the generation time of the i-th sensing data, and t_i' be the time that i-th sensing data is received by terminal end. Building on this, at t_i', the AoI of the sensing data can be expressed as $T_i = t'_i - t_i$. Note that T_i represents the system time of the i-th sensing data, including the time waiting for service and the time being served. Therefore, within the time interval $(0, \tau)$, the average AoI of the sensing data can be calculated as

$$AAoI_\tau = \frac{1}{\tau}\int_0^\tau AoI(t)\,dt. \tag{21}$$

For ease of presentation, the average AoI can be further calculated as the unit area of the graph enclosed by the sawtooth function and time axis, which can be denoted as [35], [36]:

$$AAoI_\tau = \frac{1}{\tau}\left(\tilde{A}_1 + \sum\nolimits_{i=2}^{\Omega(\tau)} A_i + \frac{T_n^2}{2}\right), \tag{22}$$

where $\tilde{A}_1$ is the polygon area, $A_i\,(2 \le i \le n)$ is the trapezoid areas, $T_n^2/2$ is the triangular area, and $\Omega(\tau) = \max\{n | t_n \le \tau\}$ defines the number of arrivals by time τ. Here, $A_i\,(2 \le i \le n)$ can be calculated as the difference of two isosceles triangles. Let $B_i = t_i - t_{i-1}$ denote the elapsed time between the producing of i-th and $(i-1)$-th sensing data, then we have:

$$A_i = \frac{1}{2}(T_i + B_i)^2 - \frac{T_i^2}{2} = B_i T_i + \frac{B_i^2}{2}. \tag{23}$$

By regarding the generation of the sensing data as a stochastic process, B_i can represent the inter-arrival time of the generation of the i-th sensing. Therefore, (22) can be further expressed as

$$AAoI_\tau = \frac{\tilde{A}}{\tau} + \frac{\Omega(\tau)-1}{\tau}\frac{1}{\Omega(\tau)-1}\sum\nolimits_{i=2}^{\Omega(\tau)}\left[B_i T_i + \frac{B_i^2}{2}\right], \tag{24}$$

where $\tilde{A} = \tilde{A}_1 + T_n^2/2$. Note that when $\tau \to \infty$, $\tilde{A}/\tau \to 0$. In this way, let λ denote the generation rate of sensing data, we have

$$\lambda = \lim_{\tau\to\infty}\left[\Omega(\tau)/\tau\right]. \tag{25}$$

With $\Omega(\tau) \to \infty$, the rest part of (24) can converge to its stochastic average value. At this time, (24) can be further determined as

$$AAoI = \lim_{\tau\to\infty} AAoI_\tau = \lambda\left(\mathbb{E}[BT] + \frac{1}{2}\mathbb{E}\left[B^2\right]\right). \tag{26}$$

In LAWNs, the newly generated sensing data gets preemptive wireless channel access to ensure real-time transmission. The transfer procedure can be modeled by the first-come first-serve principle. Furthermore, according to [37], the service rate of sensing data can be represented by the wireless channel's transmission rate of the sensing data. Therefore, the server (wireless channel) utilization can be defined as

$$\rho = \lambda/\gamma_{sense}. \tag{27}$$

As the low-altitude applications involve many time-sensitive targets, the generation and service processes of sensing data should be represented by appropriate queuing models, allowing the arrival and service rates to follow distinct probability distributions. Hence, three models are adopted here [38]. Specifically, we first utilize M/M/1 model to describe unpredictable low-altitude airspace with irregular sensing data generation and varying service time due to the changing target signals, clutter, and interference. Second, we use D/M/1 model to describe a time-division multiplexing sensing system with fixed time slots for target monitoring, but service time varies due to changing environmental conditions. Third, M/D/1 model is employed to describe a scenario where sensing data generation is random, but wireless channel condition is ideal enough, thereby sensing data has the deterministic service time.

Based on above analysis, we have the following theorems to derive the mathematical expressions of the AoI, thereby quantifying the freshness of the sensing data.

Theorem 1: In the case where both the generation and service time of sensing data follow exponential distribution, the AoI of the sensing data can be expressed as

$$AAoI^{M/M/1} = \frac{1}{\gamma_{sense}}\left(1 + \frac{\gamma_{sense}}{\lambda} + \frac{\lambda^2}{\gamma_{sense}^2 - \lambda\gamma_{sense}}\right). \tag{28}$$

Proof: Please refer to Appendix A for more details. ∎

Theorem 2: When the sensing data is deterministically generated, and the corresponding service time follows exponential distribution, the AoI of the sensing data can be expressed as

$$AAoI^{D/M/1} = \frac{1}{\gamma_{sense}}\left(\frac{\gamma_{sense}}{2\lambda} + \frac{1}{1-\delta}\right), \tag{29}$$

where $\delta = \mathcal{L}_B(\gamma_{sense}(1-\delta))$, and $\mathcal{L}(\cdot)$ is the Laplace transform operator.

Proof: Please refer to Appendix B for more details. ∎

Theorem 3: In the case where the sensing data arrivals follow an exponential distribution and the service time is deterministic, then the AoI can be expressed as

$$AAoI^{M/D/1} = \lambda\int_0^\infty b(\xi_1\xi_2)d\Theta_U(u) + Cons + \frac{1}{\lambda}, \tag{30}$$

where $Cons$ represents the fixed service time of sensing data, ξ_1, ξ_2, $\chi_{Cons}(b)$, and $\Theta_U(u)$ are defined as follows:

$$\xi_1 = \frac{(Cons)\rho}{2(1-\rho)} + Cons - b - \chi_{Cons}(b), \tag{31}$$

$$\xi_2 = \int_0^{b-Cons}(u + Cons - b)\,d\Theta_U(u), \tag{32}$$

$$\chi_{Cons}(b) = \begin{cases} 1, & b \ge Cons \\ 0, & \text{otherwise} \end{cases}, \tag{33}$$

$$\Theta_U(u) = (1-\rho)\sum\nolimits_{i=0}^{\lfloor u/Cons\rfloor}\rho^i\left(i - \frac{u}{Cons}\right)^i e^{\rho\left(\frac{u}{Cons} - i\right)}. \tag{34}$$

Proof: Please refer to Appendix C for more details. ∎

V. ISAC Performance Optimization for Time-Sensitive Targets Under Attacks

This section formulates the attacker–defender interaction as a Stackelberg game, and develops an equilibrium solution via a backward induction-based approach.

Authorized licensed use limited to: Auburn University. Downloaded on March 26,2026 at 04:01:58 UTC from IEEE Xplore. Restrictions apply.

A. Stackelberg Game-Based Problem Formulation

In the low-altitude airspace, a malicious drone launches the channel access attack and then adds noise to all the channels, deteriorating the ISAC performance of LAWNs. By using the channel estimation techniques, the legitimate drone and BS can detect the ISAC performance degradation. On this basis, LAWNs operators make corresponding adjustments to maintain the ISAC performance. Such a process matches the Stackelberg game with players including the malicious drone, the legitimate drone with an RIS, and the BS. Here, the malicious drone is the game leader, and the legitimate drone with RIS and BS are the second and first follower, respectively. In this way, the leader first takes actions to maximize its utility. Then, the followers make corresponding changes to maximize their own utilities. Finally, after reaching the Stackelberg equilibrium, all players' utilities can converge, arriving at their own steady states. More concretely, two performance metrics are optimized in the game, including the average AoI of the sensing data defined in (28) to (30) and the average communication SINR for all users, which is defined as follows:

$$\mathrm{ASINR} = \frac{1}{N}\sum_{i=1}^{N} \mathrm{SINR}_i^{com}. \tag{35}$$

1) First Follower Sub-Game: In the considered game, the BS acts as the first follower, it aims at minimizing the average AoI of sensing data and the cost of generating the sensing data, while maximizing the SINR of all the communication users. Therefore, the utility function of the BS can be defined as

$$\varphi_{BS} = -\zeta_1 AAoI + \zeta_2 \mathrm{ASINR} - \vartheta_{BS}\lambda, \tag{36}$$

where ζ_1 and ζ_2 are the coefficients to keep different performance metrics in the same order of magnitude, ϑ_{BS} represents the unit cost of generating sensing data with different rates. For the BS, its action is to adopt different rate strategies to produce the sensing data. Hence, the sub-game for the first follower can be expressed as

$$\begin{aligned} \mathrm{SP}_{BS}: \quad & \max_{\lambda} \varphi_{BS} \\ & \text{s.t. } 0 \le \lambda \le \gamma_{sense} \\ & \quad \mathrm{SINR}_i^{\mathrm{com}} \ge \mathrm{SINR}_{\mathrm{thre}}, \end{aligned} \tag{37}$$

where SINR_{thre} is the threshold to ensure the communication link, λ is the variable to be optimized by the BS, the constraint $0 \le \lambda$ can ensure that λ is positive, and $\lambda \le \gamma_{sense}$ indicates the data generation rate is smaller than the service rate, guaranteeing the queue converges to the steady state.

2) Second Follower Sub-Game: The legitimate drone with RIS acts as the second follower in the established game. Similar to the BS, its optimization goal is to minimize the average AoI of sensing data and the power cost of the reflecting elements for amplifying the signal, while maximizing the SINR for all communication users. Therefore, the utility is defined as

$$\varphi_{RIS} = -\zeta_1 AAoI + \zeta_2 \mathrm{ASINR} - \vartheta_{RIS} g, \tag{38}$$

where ϑ_{RIS} is the unit cost of reflecting elements' power amplification. Besides, the legitimate drone with RIS optimizes the reflecting elements' power amplification gain to maximize its utility. Thereby, the sub-game for the second follower is

$$\begin{aligned} \mathrm{SP}_{RIS}: \quad & \max_{g} \varphi_{RIS} \\ & \text{s.t. } 0 \le g \le g_{\max} \\ & \quad \mathrm{SINR}_i^{\mathrm{com}} \ge \mathrm{SINR}_{\mathrm{thre}}, \end{aligned} \tag{39}$$

where SINR_{thre} is the SINR threshold to ensure the communication link, g_{max} is the maximum power amplification gain of RIS's reflecting elements, which is constrained by the limited energy supply of the legitimate drone.

3) Leader Sub-Game: As for the malicious drone conducting attack, it serves as the leader within the Stackelberg game. In contrast to the first follower and second follower, the optimization objective of the malicious drone is to maximize the average AoI of sensing data, while minimizing the SINR of all the communication users and the cost for adding noise to all available channels. On this basis, we let φ_{att} be the utility function of the malicious drone, we have

$$\varphi_{att} = \zeta_1 AAoI - \zeta_2 \mathrm{ASINR} - \vartheta_{att}\sigma_{att}, \tag{40}$$

where ϑ_{att} represents the unit cost of adding noise to all the accessed channels. On this basis, the malicious drone can adjust the power of the added noise to maximize its utility, and therefore the leader sub-game can be formulated as

$$\begin{aligned} \mathrm{SP}_{\mathrm{att}}: \quad & \max_{\sigma_{\mathrm{att}}} \varphi_{\mathrm{att}} \\ & \text{s.t. } 0 \le \sigma_{\mathrm{att}} \le \nu\sigma \\ & \quad \mathrm{SINR}_i^{\mathrm{com}} < \mathrm{SINR'}_{\mathrm{thre}} \end{aligned} \tag{41}$$

where $\mathrm{SINR}_i^{\mathrm{com}} < \mathrm{SINR'}_{\mathrm{thre}}$ can ensure the effectiveness of the channel access attack. ν is a constant, $\sigma_{att} \le \nu\sigma$ is the constraint to ensure the attack's ability and covertness, ensuring that the added noise is similar to the environment noise to confuse the attack detection approaches.

B. Stackelberg Game Equilibrium Solution

1) Problem Reformulation: Note that there is hierarchical conflicting relationship among leader and followers. Therefore, to further highlight the actions' order of all the players, based on the backward induction (BI) method [28], the sub-problems in (37), (39), and (41) can be reformulated as a three layer programming problem, which can be expressed as

$$\begin{cases} \max\limits_{\sigma_{\mathrm{att}}} \varphi_{\mathrm{att}}(\lambda, g, \sigma_{\mathrm{att}}) \\ \text{s.t.} \quad 0 \le \sigma_{\mathrm{att}} \le \sigma \\ \mathrm{SINR}_i^{\mathrm{com}} < \mathrm{SINR'}_{\mathrm{thre}} \\ \text{Optimal solution: } (\lambda_{\mathrm{opt}}, g_{\mathrm{opt}}, \sigma_{\mathrm{att}}) \\ \begin{cases} \max\limits_{g} \varphi_{\mathrm{RIS}}(\lambda, g, \sigma_{\mathrm{att}}) \\ \text{s.t.} \quad 0 \le g \le g_{\max} \\ \mathrm{SINR}_i^{\mathrm{com}} \ge \mathrm{SINR}_{\mathrm{thre}} \\ \text{Optimal solution: } (\lambda_{\mathrm{opt}}, g, \sigma_{\mathrm{att}}) \\ \begin{cases} \max\limits_{\lambda} \varphi_{\mathrm{BS}}(\lambda, g, \sigma_{\mathrm{att}}) \\ \text{s.t.} \quad 0 \le \lambda \le \gamma_{sense} \\ \mathrm{SINR}_i^{\mathrm{com}} \ge \mathrm{SINR}_{\mathrm{thre}} \end{cases} \end{cases} \end{cases}, \tag{42}$$

Authorized licensed use limited to: Auburn University. Downloaded on March 26,2026 at 04:01:58 UTC from IEEE Xplore. Restrictions apply.

Algorithm 1 GSSPI-Based Algorithm for Sub-Problem Solving

Input: Ψ: the target function to be minimized; Λ: the variable to be optimized; $[\Lambda_{min}, \Lambda_{max}]$: the feasible domain of the variable; $Iter = 1$: the looping iteration index; $Iter_{max}$: the maximum iteration index; Λ_1: the initial variable value; ς: the error tolerance threshold.

Output: Λ_{opt}: the optimized variable value; $\Psi(\Lambda_{opt})$: the optimal value of the target function.

1: **Repeat**
2: $Iter = Iter + 1$
3: Based on the Golden section searching, determine the global optimal domain $\left[\Lambda_{opt-min}(Iter), \Lambda_{opt-max}(Iter)\right]$ for variable Λ
4: Based on the parabolic interpolation, determine the solution $\Lambda_{opt}(Iter)$ within $\left[\Lambda_{opt-min}(Iter), \Lambda_{opt-max}(Iter)\right]$
5: **Until** $\left|\Lambda_{opt}(Iter) - \Lambda_{opt}(Iter-1)\right| \le \varsigma$ or $Iter > Iter_{max}$
6: Calculate $\Psi\left(\Lambda_{opt}(Iter)\right)$ based on $\Lambda_{opt}(Iter)$

where λ_{opt} and g_{opt} represent optimized values for variable λ and g, respectively. Following the BI approach, three sub-problems are solved from bottom to top, which can provide the optimal generation rate of sensing data, optimal power of reflecting elements' amplification, as well as the optimal values of the added noise in order. In this regard, this sequential approach reflects the natural order of decision-making in such adversarial settings and allows for the computation of a Stackelberg equilibrium.

2) GSSPI-Based Sub-Problems Solution: To solve the problem in (42), the first step is to handle the three sub-problems.Due to the lack of closed-form solutions for the objective functions, Golden section search and parabolic interpolation (GSSPI) methods-based approach [39] is improved here to derive the optimized solution of each sub-problem. Generally, GSSPI is a derivative-free optimization technique that does not rely on gradient information, making it well-suited for sub-problems that are noisy or non-differentiable. GSSPI can refine the search interval using golden section search's guaranteed convergence, and accelerates the process with parabolic interpolation's quadratic convergence, effectively handling the constraints. Specifically, GSSPI first narrows the search interval through the golden section method, whose convergence is guaranteed. Then, it accelerates the optimization with parabolic interpolation, which achieves quadratic convergence while satisfying the imposed constraints.

The GSSPI is designed for minimization problems, and hence we define $\Psi = \{-\varphi_{BS}, -\varphi_{RIS}, -\varphi_{att}\}$ as the objective function to be minimized and $\Lambda = \{\lambda, g, \sigma_{att}\}$ as the variable to be optimized. Besides, let Λ_{min}, Λ_{max} and Λ_{opt} represent the lower bound, upper bound, and the optimized variable, respectively. On this basis, the GSSPI-based algorithm for sub-problem is detailed in Algorithm 1. Specifically, Step 1–Step 2 first initialize the loop settings. Then, Step 3 determines the global optimal domain, reducing the search range of the solution [40], [41]. Next, Step 4 determines the solution $\Lambda_{opt}(Iter)$, and Step 5 clarifies the loop ending conditions. At last, Step 6 determines the final value of the target function.

Algorithm 2 Stackelberg Equilibrium Calculation

Input: φ_{BS}, λ, $[0, \gamma_{sense}]$, φ_{RIS}, g, $[0, g_{\max}]$, φ_{att}, σ_{att}, $[0, \sigma]$, $Iter' = 1$, and $Iter'_{max}$.

Output: λ_{opt}, g_{opt}, σ_{att_opt}, φ_{BS_opt}, φ_{RIS_opt}, and φ_{att_opt}.

1: **//Stage 1: Parameters initialization**
2: Initialize parameters of all the players' actions: $\lambda_{opt}(1)$, $g_{opt}(1)$, and $\sigma_{att_opt}(1)$
3: Initialize parameters of all the players' utilities with (36), (38), and (40): $\varphi_{BS_opt}(1)$, $\varphi_{RIS_opt}(1)$, and $\varphi_{att_opt}(1)$
4: **//Stage 2: Repeat iterations**
5: **While** $Iter' < Iter'_{\max}$ **do**
6: $Iter' = Iter' + 1$
7: **//Stage 2-1: First follower sub-game solving**
8: Derive $\lambda_{opt}(Iter)$ with **Algorithm 1**
9: Based on (36), calculate the current utility $\varphi_{BS_opt}(Iter)$ with $\lambda_{opt}(Iter)$, $g_{opt}(Iter-1)$ and $\sigma_{att_opt}(Iter-1)$
10: **If** $\varphi_{BS_opt}(Iter) < \varphi_{BS_opt}(Iter-1)$ holds on
11: Let $\lambda_{opt}(Iter) = \lambda_{opt}(Iter-1)$
12: Let $\varphi_{BS_opt}(Iter) = \varphi_{BS_opt}(Iter-1)$
13: **End**
14: **//Stage 2-2: Second follower sub-game solving**
15: Derive $g_{opt}(Iter)$ with **Algorithm 1**
16: Based on (38), calculate the current utility $\varphi_{RIS_opt}(Iter)$ with $\lambda_{opt}(Iter)$, $g_{opt}(Iter)$ and $\sigma_{att_opt}(Iter-1)$
17: **If** $\varphi_{RIS_opt}(Iter) < \varphi_{RIS_opt}(Iter-1)$ holds on
18: Let $g_{opt}(Iter) = g_{opt}(Iter-1)$
19: Let $\varphi_{RIS_opt}(Iter) = \varphi_{RIS_opt}(Iter-1)$
20: **End**
21: **//Stage 2-3: Leader sub-game solving**
22: Derive $\sigma_{att_opt}(Iter)$ with **Algorithm 1**
23: Based on (40), calculate the current utility $\varphi_{att_opt}(Iter)$ with $\lambda_{opt}(Iter)$, $g_{opt}(Iter)$ and $\sigma_{att_opt}(Iter)$
24: **If** $\varphi_{att_opt}(Iter) < \varphi_{att_opt}(Iter-1)$ holds on
25: Let $\sigma_{att_opt}(Iter) = \sigma_{att_opt}(Iter-1)$
26: Let $\varphi_{att_opt}(Iter) = \varphi_{att_opt}(Iter-1)$
27: **End**
28: **//Stage 3: End iterations**
29: **End**
30: Determine λ_{opt}, g_{opt}, σ_{att_opt}, φ_{BS_opt}, φ_{RIS_opt}, φ_{att_opt} as the Stackerberg equilibrium solutions and utilities.

3) Backward Induction Stackelberg Equilibrium Solution: To simultaneously maximize all the players' utilities, we proposed a BI-based algorithm to calculate the Stackelberg equilibrium, as shown in Algorithm 2. Specifically, Step 1 to Step 3 first initialize the parameters of all players' actions and utilities. Step 4 to Step 6 determine the looping rule and iteration index. Next, through Step 7 to Step 13, the first follower sub-game can be solved. Similarly, the second follower sub-game and leader sub-game can also be solved through Step

Authorized licensed use limited to: Auburn University. Downloaded on March 26,2026 at 04:01:58 UTC from IEEE Xplore. Restrictions apply.

14 to Step 20, and Step 21 to Step 27, respectively. Finally, Step 28 to Step 30 end the loop, and determine the output results as the Stackelberg equilibrium solutions and utilities.

4) Complexity and Convergence Analysis: According to [40] and [41], the computational complexity of Algorithm 1 is bounded by $O(\log[(\Lambda_{\max}-\Lambda_{\min})/\varsigma])$ and $o\left((Iter_{\max})^2\right)$. Additionally, the convergence of Algorithm 1 is primarily determined by the search step and tolerance threshold. Because the search range is bounded, Algorithm 1 is guaranteed to converge in only a few iterations. At each step it reduces the bracketing interval monotonically by a factor of about 0.618 without requiring derivative information, so the optimum remains inside an interval that shrinks at a linear rate. Once this interval becomes sufficiently small, the GSSPI procedure typically attains the optimum quickly because the local behavior of many functions near a minimum is well approximated by a parabola. For the proposed BI-based Algorithm 2 for Stackelberg equilibrium calculating, according to [28], its complexity mainly depends on Stage 2-1 to Stage 2-3. Based on Section V-B-III), one can see that the complexity of calculating the player's utility is $o(\varpi)$, where ϖ is a constant. Hence, the complexity of solving a single player's sub-game one time is bounded by $o\left\{\log[(\Lambda_{\max}-\Lambda_{\min})/\varsigma]\right\}+o(\varpi)$ and $o\left\{(Iter_{\max})^2\right\}+o(\varpi)$. In this regard, the total complexity of Algorithm 2 is within $o(1)+o\left\{3Iter'_{\max}\left[o\left(\log((\Lambda_{\max}-\Lambda_{\min})/\varsigma)\right)+o(\varpi)+o(1)\right]\right\}$ and $o(1)+o\left\{3Iter'_{\max}\left[o\left((Iter_{\max})^2\right)+o(\varpi)+o(1)\right]\right\}$. In addition, the convergence of Algorithm 2 follows from that of Algorithm 1. Section V-B-III) shows that Algorithm 1 converges in a finite number of iterations. Because Algorithm 2 invokes Algorithm 1 only a finite number of times, it also reaches a stable solution within limited iterations.

C. Stackelberg Equilibrium Analysis

For the formulated Stackelberg game in (42), its Stackelberg equilibrium can be determined as follows:

$$\begin{cases}\varphi_{BS}\left(\lambda_{opt},g_{opt},\sigma_{att_opt}\right)\geq\varphi_{BS}\left(\lambda,g_{opt},\sigma_{att_opt}\right)\\ \varphi_{RIS}\left(\lambda_{opt},g_{opt},\sigma_{att_opt}\right)\geq\varphi_{BS}\left(\lambda,g,\sigma_{att_opt}\right)\\ \varphi_{att}\left(\lambda_{opt},g_{opt},\sigma_{att_opt}\right)\geq\varphi_{BS}\left(\lambda,g_{opt},\sigma_{att}\right)\end{cases}. \quad (43)$$

For the above-defined Stackelberg equilibrium, we have the following theorem to ensure its existence.

Theorem 4: For the formulated Stackelberg game in (42), its Stackelberg equilibrium always exists.

Proof: According to [42], by combining the followers' best response mapping with the leader's strategy space, a mapping from the strategy space to the leader itself can be created. If this mapping satisfies the conditions of a fixed-point theorem [42], then a fixed point exists, which corresponds to a Stackelberg equilibrium. Specifically, the followers' best response mapping can be represented as follows:

$$R_{F_RIS}(g)=\arg\max_{g\in[0,g_{\max}]}\varphi_{RIS}(g,\lambda,\sigma_{att}), \quad (44)$$

$$R_{F_BS}(\lambda)=\arg\max_{\lambda\in[0,\gamma_{sense}]}\varphi_{BS}(\lambda,g,\sigma_{att}). \quad (45)$$

On this basis, the leader can derive its strategy with:

$$\sigma*_{att}=\arg\max_{\sigma_{att}\in[0,\nu\sigma]}\varphi_{att}(\lambda,g,\sigma_{att}). \quad (46)$$

TABLE II
SIMULATION SETTINGS

Symbol	Value	Symbol	Value
M	4	σ^2	-174 dBm/Hz
N	2	P	16
(x_{BS},y_{BS},z_{BS})	$[0,0,1.5]$	$(x_{RIS},y_{RIS},z_{RIS})$	$[5,10,1.5]$
$(x_{user},y_{user},z_{user})$	$[30,10,1.5]$	$(x_{tar},y_{tar},z_{tar})$	$[0,60,1.5]$
r_{user}	10	ε	0.1
η	10^7 Hz	P_{trans}	0.9
σ_y^2	-174 dBm/Hz	σ_r^2	-174 dBm/Hz
g_{max}	1	$Iter_{max}$	25

Then, we can further construct a mapping $\Xi(\sigma_{att})$ from leader's strategy space to itself, mathematically,

$$\Xi(\sigma_{att})=\arg\max_{\sigma'_{att}\in[0,\nu\sigma]}\varphi_{att}\left(\sigma'_{att},R_{F_RIS}(\sigma_{att}),R_{F_BS}(\sigma_{att})\right). \quad (47)$$

In this regard, based on the fixed-point theorem [42], if the leader's strategy space is a non-empty, compact, and convex set in Euclidean space, and the constructed mapping is a continuous mapping, then the constructed mapping has a fixed point, corresponding to a Stackelberg equilibrium. Since the leader's strategy space $[0,\nu\sigma]$ is non-empty, compact, and convex, and the constructed mapping $\Xi(\sigma_{att})$ is a continuous single-value function, satisfying the continuous mapping needs. Finally, the fixed point exists, and Theorem 4 is proved. ■

VI. EVALUATIONS AND ANALYSIS

This section evaluates the proposed algorithm under various configurations. First, we evaluate the convergence property of the proposed algorithm from the perspectives of utility, optimized variables, and performance metrics. Next, we compare the proposed method with the three existing baselines in terms of utility. The baselines contain lightweight solutions and computationally intensive approaches. The former includes the average and random resource allocation schemes, and the latter refers to the Genetic Algorithm (GA)-based optimization scheme. Finally, we further compare the derived Stackelberg equilibrium solution with the Nash equilibrium [28] solution to demonstrate the superiority of Stackelberg equilibrium.

A. Parameter Setting

In the low-altitude air space, with the help of a legitimate drone equipped with RIS, one BS with a multi-antenna is used to simultaneously communicate with two signal-antenna users and sense one target. The simulation parameters are presented in Table II, the AoI is calculated with the M/M/1 queue model, and the communication SINR threshold is set as 5 dB. Furthermore, average allocation, random allocation, and GA-based optimization are introduced to make a comparison with the proposed method. Specifically, the average scheme allocates resources, such as the noise power of the attacker and sensing data generation rate, with the average value across the feasible domain [43]. This ensures fairness by allocating equal resources to all players regardless of channel quality or their individual needs and provides a neutral baseline for comparison. In the random allocation scheme [44], each resource value

Authorized licensed use limited to: Auburn University. Downloaded on March 26,2026 at 04:01:58 UTC from IEEE Xplore. Restrictions apply.

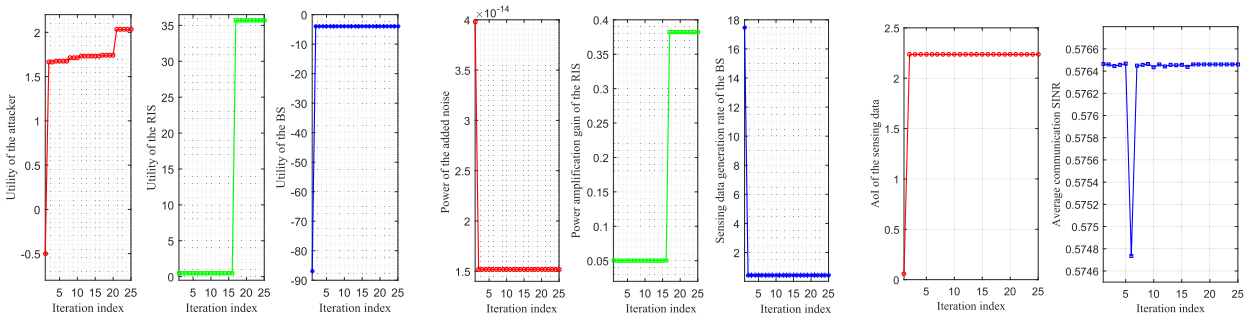


Fig. 3. Convergence behaviors evaluation of utility functions, performance metrics, and optimized variables. (a) Convergence behavior of the utility functions. (b) Convergence behavior of the optimized variables. (c) Convergence behavior of the performance metrics.

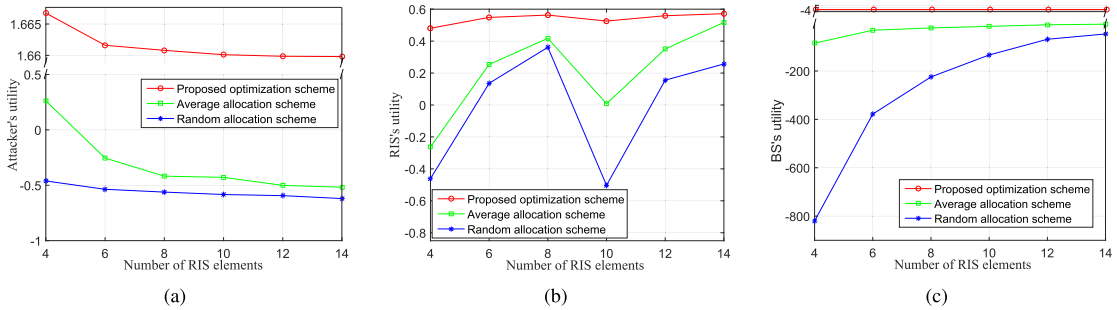


Fig. 4. Utility functions comparison of the attacker, RIS, and BS with different number of RIS elements. (a) The attacker's utility with different RIS element number. (b) The RIS's utility with different RIS element number. (c) The BS's utility with different RIS element number.

is independently sampled from a uniform distribution within its feasible range and assigned to a player. Since this process is purely random and does not consider the current system state, it serves as a baseline for unstructured and non-intelligent resource management. In the GA-based optimization scheme [45], a population of candidate solutions is iteratively evolved using selection, crossover, and mutation operations to obtain the optimal solution. This approach captures the complex relationship between resource allocation and system performance, enabling convergence toward superior solutions with a higher computational cost.

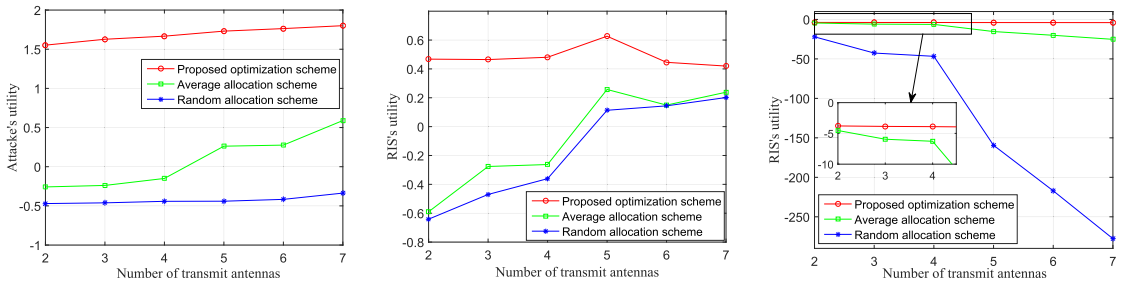
B. Convergence Analysis

Figure. 3(a) is the convergence evaluation of utility functions. As shown in Fig. 3(a), we can see that as the number of iterations grows, utilities of the attacker, legitimate drone with RIS, and BS all can reach the stable values, confirming the convergence property of the proposed scheme. Moreover, each player's utility rises throughout the iterations. This is because the established Stackelberg game is not cooperative and each participant is selfish and rational, aiming to maximize its own utility during the iterative optimization process. Fig. 3(b) evaluates the convergence of the optimized variables, including the sensing data generation rate of the BS, power amplification gain of the RIS, and the power of the added noise from attacker. Specifically, following the backward induction order, the BS, as the first follower, optimizes its sensing data generation rate and converges to 0.447. Then, the drone with RIS, acting as the second follower, optimizes the power amplification gain and reaches stability at 0.382. Finally, the attacker, as the game leader, optimizes the added noise power and reaches a stable value of 1.52×10^{-14}. Therefore, within the finite iterations, all above-mentioned variables can converge. Fig. 3(c) presents the convergence evaluation of performance metrics. As can be seen from Fig. 3(c), within the finite iteration steps, by optimizing the sensing data generation rate of the BS, power amplification gain of the RIS, and added noise power of the attacker in order, the formulated game can reach the Stackelberg equilibrium. At this time, the AoI of the sensing data and average communication SINR converge to 2.236 and 0.576, respectively.

C. Effectiveness Analysis

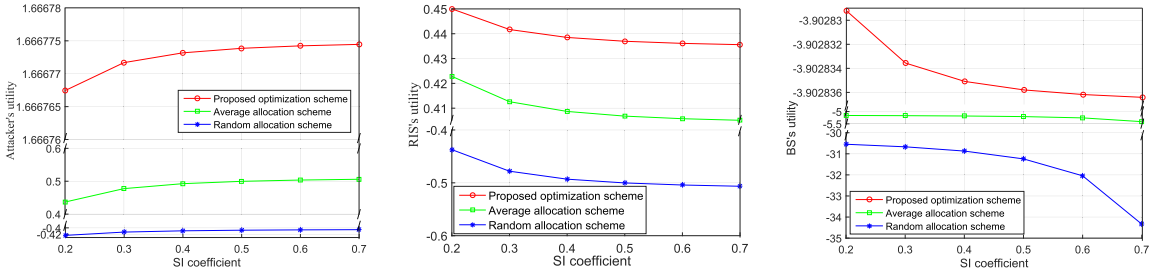
1) Performance Versus the Number of RIS Elements: Fig. 4 is the utility comparison of the attacker, RIS, and BS with different number of RIS elements. As shown in Fig. 4, the proposed scheme achieves utility of 1.659, 0.571, and −3.895 for the attacker, RIS, and BS, respectively, outperforming those of the average-allocation scheme (−0.517, 0.517, and −6.28) and the random-allocation scheme (−0.62, 0.256, and −46.718). This demonstrates the effectiveness of the proposed approach. Moreover, Fig. 4(a) shows that the attacker's utility falls as the number of RIS elements grows. The reason is that more elements improves the SINR, thereby reducing the attacker's utility. Furthermore, from Fig. 4(b), we can see that the RIS's utility first increases, then decreases, and increases again. This is because, with 8 or 14 RIS elements, the payoff is larger than the additional cost, whereas with 10 elements the payoff is lower than the cost, reducing overall utility. For the BS, Fig. 4(c) shows that its utility rises as the number of RIS elements increases. This can be interpreted by that more elements enhance signal strength, which raises the average

Authorized licensed use limited to: Auburn University. Downloaded on March 26,2026 at 04:01:58 UTC from IEEE Xplore. Restrictions apply.



(a) (b) (c)

Fig. 5. Utility functions comparison of the attacker, RIS, and BS with different number of transmit antennas. (a) The attacker's utility with different transmit antenna number. (b) The RIS's utility with different transmit antenna number. (c) The BS's utility with different transmit antenna number.



(a) (b) (c)

Fig. 6. Utility functions comparison of the attacker, RIS, and BS with different self-interference coefficient values. (a) The attacker's utility with different self-interference coefficient values. (b) The RIS's utility with different self-interference coefficient values. (c) The BS's utility with different self-interference coefficient values.

SINR. The higher SINR increases channel capacity, allowing sensing data to be transmitted without delay, thereby reducing the AoI. Hence, as reflected in (36), the BS utility grows.

2) Performance Versus the Number of Transmitting Antennas: Fig. 5 presents the utility comparison of the attacker, RIS, and BS with different number of BS's transmitting antennas. As can be seen, across all cases, all players can obtain higher utilities by using the proposed optimization scheme compared to the average and random allocation schemes. Besides, different players obtain different benefits when the number of transmit antennas increases. Specifically, Fig. 5(a) shows that the attacker's utility rises with more transmit antennas, because a multi-antenna system enlarges the signal's spatial dimension, broadening the effective range of the attack. Fig. 5(b) shows that the RIS's utility fluctuates with the increasing number of transmit antennas. With 2, 3, 6, and 7 antennas at the BS, the RIS's utility gain is smaller than that of the attacker, and hence its utility declines. In contrast, with 4 or 5 antennas, the multi-antenna benefit outweighs the attacker's advantage, thereby raising the RIS utility. Moreover, in Fig. 5(c), we can see that, unlike attacker and RIS, the BS's utility decreases as the number of transmit antennas increases. This is because the multi-antenna system can increase the BS's transmitting capacity. To maintain the AoI performance, the BS needs to increase the sensing data generation rate, which increases cost and therefore reduces the BS's overall utility.

3) Performance Versus Different Self-Interference Coefficient: Fig. 6 compares the utility the attacker, RIS, and BS with different self-interference coefficient values. Overall, across different interference levels, the proposed scheme consistently outperforms all baselines, further demonstrating its superiority. Concretely, Fig. 6(a) shows that the attacker's utility rises as the self-interference coefficient increases. The reason is that according to (17), a higher self-interference coefficient raises the interference-plus-noise level, which lowers both AoI and average SINR, thereby enhancing attacker's utility. For the same reason, Figs. 6(b) and 6(c) reveal that the utilities of the RIS and the BS move in the opposite direction.

4) Performance Comparison: Fig. 7 is the performance comparison of the proposed and GA-based optimization schemes. As shown in Fig. 7, compared with the listed baselines, the proposed optimization can realize higher utilities for all the players within the established Stackelberg game. The reason is that GSSPI is a more efficient and targeted approach, fully exploiting the specific structure of the Stackelberg game and the players' interaction. As a result, it converges faster and more reliably to a better solution than the GA (which explores the solution space more generally), average, and random allocation schemes. Moreover, as the attack intensity increases, the utilities of the attacker and the RIS both rise, while the base station's utility remains stable. The reasons are that the attacker directly benefits from increased noise, enabling it to disrupt communication more. At the same time, the RIS can strategically adjust its power amplification gain to further mitigate interference and enhance the signal strength towards the legitimate receiver, while the BS can adjust its sensing data generation strategy to counteract the increased noise and maintain its performance.

5) Comparison of Stackelberg and Nash Equilibrium: Fig. 8 compares the utilities achieved under the Nash and Stackelberg equilibria. Under the considered system model and

Authorized licensed use limited to: Auburn University. Downloaded on March 26,2026 at 04:01:58 UTC from IEEE Xplore. Restrictions apply.

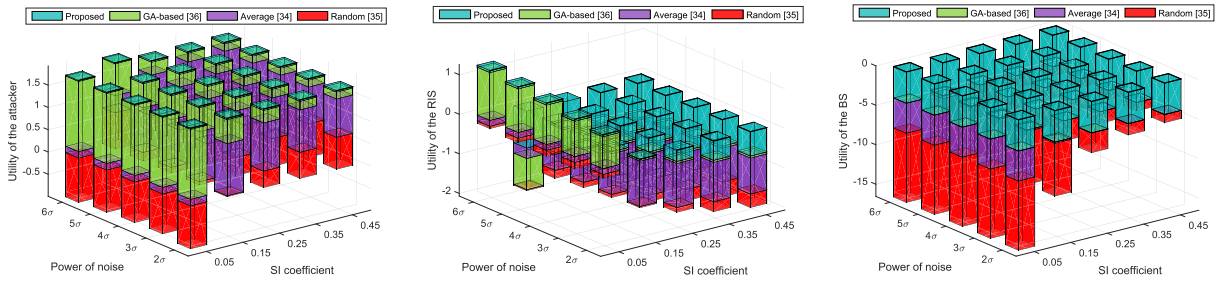


Fig. 7. Performance comparison of the proposed and GA-based optimization schemes. (a) The attacker's utility with different SI coefficients and attacking noise. (b) The RIS's utility with different SI coefficients and attacking noise. (c) The BS's utility with different SI coefficients and attacking noise.

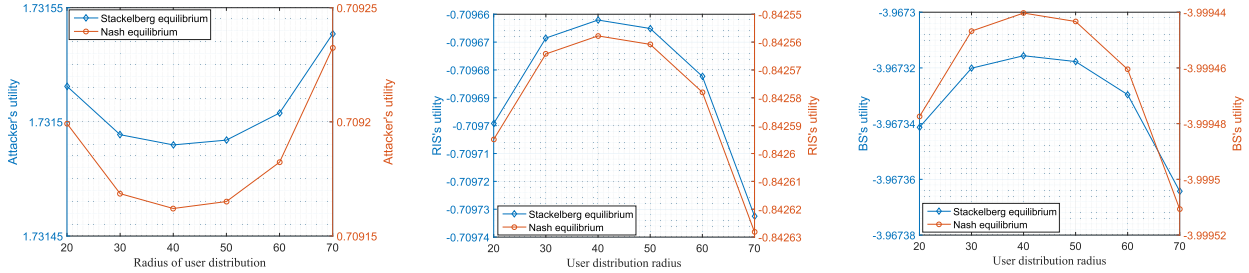


Fig. 8. Performance comparison of Stackelberg equilibrium and Nash equilibrium. (a) The attacker's utility with different equilibriums. (b) The RIS's utility with different equilibriums. (c) The BS's utility with different equilibriums.

parameter settings, the Stackelberg equilibrium yields higher utilities for all players than the Nash equilibrium. This is because the leader commits to its strategy first and explicitly anticipates the followers' best responses, which provides an implicit coordination mechanism and mitigates the inefficiency caused by simultaneous decision-making. In contrast, the Nash equilibrium considers only the static games between players [28], decreasing the utility in the focused scenario. For example, under a channel access attack, the BS and the RIS may simultaneously increase the sensing-data generation rate λ and the RIS amplification gain g to compensate for the perceived performance degradation; however, a larger g also amplifies the attacker-injected noise on the reflected link (i.e., the $(\sigma^2 + \sigma_{\text{att}}^2)\mathbf{h}_{1,i}^H \boldsymbol{\Phi}\boldsymbol{\Phi}^H \mathbf{h}_{1,i}$ term in (14)) and increases the interference-plus-noise level in sensing (in (16)–(18)), which reduces $\text{SINR}_{\text{sense}}$ and thus the sensing service rate γ_{sense} in (20). Consequently, the sensing-queue utilization $\rho = \lambda/\gamma_{\text{sense}}$ increases (in (27)), leading to a larger AoI and lower utilities. Moreover, as the user-distribution radius expands, users closest to the BS enjoy higher SINR while those farther away suffer lower SINR. When the radius increases from 20 to 40 m, the average SINR rises, which lowers the attacker's utility and raises the utilities of both the RIS and the BS. In contrast, extending the radius from 50 to 70 m reduces the average SINR, increasing the attacker's utility and decreasing the utilities of the RIS and the BS.

VII. Open Issues

A. Leader and Follower Modeling

If the attacker were the follower and the BS and legitimate UAV with RIS were the leaders, the game would shift from modeling adaptive attacks to focusing on preemptive defense strategies. While this could theoretically lead to a different set of outcomes and equilibrium, it would significantly alter the dynamics of the interaction and make the model less realistic for this specific use case. The attacker's initiative in launching the attack provides a more accurate representation of the challenges faced in low-altitude network security, where attackers often act first, leaving the defenders to adapt.

B. Multi-Attacker Scenario

In a scenario with multiple attackers, the game model could be extended to account for either cooperative or non-cooperative behavior among the attackers. When attackers collaborate, they can combine efforts to maximize their impact, for instance, through synchronized jamming. On the other hand, if the attackers act independently, each would focus on maximizing its own utility, leading to a more complex multi-agent game structure. Both types of interactions would require different approaches in terms of defense strategies, making the game more intricate and requiring the defenders to adapt to a broader set of attack strategies.

VIII. Conclusion

This paper aims to enhance the ISAC performance of LAWNs for time-sensitive targets under channel access attack. We have established the low-altitude network model under attack, deriving the communication data's SINR and sensing data's AoI expressions. Then, based on the defined utility functions and actions, we have formulated a Stackelberg game-based ISAC performance optimization problem, where the attacker acts as the leader, and legitimate drone with RIS and ISAC BS are regarded as the vice and first followers, respectively. With the proposed BI-based optimization algorithm,

Authorized licensed use limited to: Auburn University. Downloaded on March 26,2026 at 04:01:58 UTC from IEEE Xplore. Restrictions apply.

the Stackelberg equilibrium can be reached. The evaluation verifies the effectiveness and superiority of the proposed method, providing support for ensuring ISAC performance and building a reliable LAWNs. In the future, more constraints including energy consumption and control will be considered to further enhance LAWNs.

Appendix A

When both the generation and service of the sensing data follow exponential distributions, the M/M/1 queue model can be adopted to derive the AoI expression. Then, according to [35], we have $\mathbb{E}[B] = \frac{1}{\lambda}$ and $\mathbb{E}\left[B^2\right] = \frac{1}{\lambda^2}$. For the i-th generated sensing data, let U_i and O_i represent its waiting time and service time, its system time can be determined as

$$T_i = U_i + O_i. \tag{48}$$

In addition, if the $(i-1)$-th sensing data completes service before the i-th sensing data is generated, $U_i = 0$. Otherwise, if the i-th sensing data is generated while the $(i-1)$-th sensing data is still queued or being served, $U_i = T_{i-1} - B_i$. Therefore, the waiting time of i-th sensing data is:

$$U_i = (T_{i-1} - B_i)^+. \tag{49}$$

Based on [46], for the M/M/1 queue model, when the system state is stable, the system times are stochastically identical, i.e., $T \overset{st}{=} T_i \overset{st}{=} T_{i-1}$. The probability density function (PDF) of the system time is expressed as

$$f_T(t) = \gamma_{sense}(1-\rho)\, e^{-\gamma_{sense}(1-\rho)t}, \quad t \geq 0. \tag{50}$$

At this time, when $B_i = b$, the conditional expectation of the waiting time U_i can be calculated as

$$\begin{aligned}\mathbb{E}[U_i|B_i = b] &= \mathbb{E}\left[(T_{i-1} - B_i)^+|B_i = b\right] \\ &= \mathbb{E}\left[(T-b)^+\right] \\ &= \int_b^\infty (t-b) f_T(t)\, dt \\ &= \frac{e^{-\gamma_{sensing}(1-\rho)b}}{\gamma_{sensing}(1-\rho)}.\end{aligned} \tag{51}$$

Since the service time O_i is independent of B_i, we have:

$$\mathbb{E}[T_i B_i] = \mathbb{E}[(U_i + O_i) B_i] = \mathbb{E}[U_i B_i] + \mathbb{E}[O_i]\,\mathbb{E}[B_i]. \tag{52}$$

Note that $\mathbb{E}[O_i] = \frac{1}{\gamma_{sense}}$, combined with (51), we have:

$$\mathbb{E}[U_i B_i] = \int_0^\infty b\mathbb{E}[U_i|B_i = b] f_{B_i}(b)\, db = \frac{\rho}{\gamma_{sense}^2(1-\rho)}. \tag{53}$$

Finally, by integrating (52) and (53) to (26), we can obtain the average AoI of the sensing data as shown in (28). Hence, Theorem 1 is proved.

Appendix B

When the sensing data is deterministically generated, and its service time is exponentially distributed, the sensing data AoI can be calculated under the D/M/1 queue model. Let $Cons$ represents the sensing data's fixed generation rate, we have $\lambda = 1/Cons$, $\mathbb{E}\left[B^2\right]/2 = (Cons)^2/2$, and $\mathbb{E}[BT] = Cons\mathbb{E}[T]$. At this time, (26) can be further expressed as

$$AAoI = \frac{1}{Cons}\left[\frac{(Cons)^2}{2} + Cons\mathbb{E}[T]\right]. \tag{54}$$

In addition, according to [35], the expectation of system can be calculated as

$$\mathbb{E}[T] = \mathbb{E}[O] + \mathbb{E}[U] = \frac{1}{\gamma_{sense}} + \frac{\delta}{\gamma_{sense}(1-\gamma_{sense})}, \tag{55}$$

where $\delta \in [0,1]$ can be determined by solving the equation $\delta = \mathcal{L}_B(\gamma_{sense}(1-\delta))$, and $\mathcal{L}(\cdot)$ is the Laplace transform operator. Additionally, based on [47], for the deterministic sensing data generation, δ can further be expressed as

$$\delta = e^{-\gamma_{sense}(1-\delta)Cons} = -\rho\Xi\left(-\frac{e^{-\frac{1}{\rho}}}{\rho}\right), \tag{56}$$

where $\Xi(\cdot)$ represents the Lambert-W function. Therefore, combined with (54) and (55), we can get (29). Hence, Theorem 2 can be proved.

Appendix C

Let the generation rate of the sensing data follow exponential distribution and the service time is deterministic, we can use M/D/1 queue model to derive the AoI expression of the sensing data. In this way, we have $O_i = Cons$. Since $T_i = U_i + Cons$, then:

$$\mathbb{E}[T_i B_i] = \mathbb{E}[U_i B_i] + Cons\mathbb{E}[B_i]. \tag{57}$$

Furthermore, similar to the calculation process of (51), at the condition $B_i = b$, the conditional expectation of the waiting time U_i can be calculated as

$$\begin{aligned}\mathbb{E}[U_i|B_i = b] &= \mathbb{E}\left[(T_{i-1} - B_i)^+|B_i = b\right] \\ &= \mathbb{E}\left[(T-b)^+\right] \\ &= \mathbb{E}\left[(U + Cons - b)^+\right] \\ &= \mathbb{E}[U] + Cons - b - \chi_{Cons}(b)\,\xi_2.\end{aligned} \tag{58}$$

Note that, based on [37], for the M/D/1 queuing model, the expectation of waiting time U can be expressed as

$$\mathbb{E}[U] = \frac{\rho Cons}{2(1-\rho)}. \tag{59}$$

Finally, by integrating (53) and (58) into (26), we can obtain (30), and hence Theorem 3 is proved.

References

[1] W. Yuan et al., "From ground to sky: Architectures, applications, and challenges shaping low-altitude wireless networks," 2025, *arXiv:2506.12308*.

[2] Y. Yang, Y. Chen, J. Wang, G. Sun, D. Niyato, and Z. Han, "Leveraging the power of ensemble learning for secure low altitude economics," *IEEE Commun. Mag.*, vol. 64, no. 2, pp. 164–171, Feb. 2026.

[3] G. Sun et al., "Recovery of UAV swarm-enabled collaborative beamforming in low-altitude wireless networks under wind field disturbances," *IEEE Trans. Veh. Technol.*, early access, Jan. 15, 2026, doi: 10.1109/TVT.2026.3654588.

[4] K. Xiong, J. Xie, and S. Leng, "EVTOL communication and trajectory optimization in low-altitude economy," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC Workshops)*, China, Aug. 2024, pp. 845–850.

Authorized licensed use limited to: Auburn University. Downloaded on March 26,2026 at 04:01:58 UTC from IEEE Xplore. Restrictions apply.

[5] H. Jin et al., "Predictive control over LAWN: Joint trajectory design and resource allocation," 2025, *arXiv:2507.02374*.
[6] J. Zhang et al., "RIS-assisted beam tracking for low-altitude economy networking: Enabling technologies and applications," *IEEE Internet Things Mag.*, vol. 9, no. 2, pp. 117–123, Mar. 2026.
[7] J. Wang et al., "Generative AI for integrated sensing and communication: Insights from the physical layer perspective," *IEEE Wireless Commun.*, vol. 31, no. 5, pp. 246–255, May 2023.
[8] J. Mu, R. Zhang, Y. Cui, N. Gao, and X. Jing, "UAV meets integrated sensing and communication: Challenges and future directions," *IEEE Commun. Mag.*, vol. 61, no. 5, pp. 62–67, May 2023.
[9] Y. Jiang et al., "Integrated sensing and communication for low altitude economy: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 63, no. 12, pp. 72–78, Dec. 2025.
[10] X. Wei, L. Li, C. Tang, M. Doroslovacki, and S. Subramaniam, "Classification of channel access attacks in wireless networks: A deep learning approach," in *Proc. IEEE 40th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Nov. 2020, pp. 809–819.
[11] Z. Wei, F. Liu, C. Liu, Z. Yang, D. W. K. Ng, and R. Schober, "Integrated sensing, navigation, and communication for secure UAV networks with a mobile eavesdropper," *IEEE Trans. Wireless Commun.*, vol. 23, no. 7, pp. 7060–7078, Jul. 2024.
[12] N. A. Khan, N. Z. Jhanjhi, S. N. Brohi, A. A. Almazroi, and A. A. Almazroi, "A secure communication protocol for unmanned aerial vehicles," *Comput., Mater. Continua*, vol. 70, no. 1, pp. 601–618, 2022.
[13] Y. Yang, B. Zhang, D. Guo, R. Xu, C. Su, and W. Wang, "Age of information optimization for privacy-preserving mobile crowdsensing," *IEEE Trans. Emerg. Topics Comput.*, vol. 12, no. 1, pp. 281–292, Jan. 2024.
[14] R. Ch, G. Srivastava, T. Reddy Gadekallu, P. K. R. Maddikunta, and S. Bhattacharya, "Security and privacy of UAV data using blockchain technology," *J. Inf. Secur. Appl.*, vol. 55, Dec. 2020, Art. no. 102670.
[15] Y. Yang, B. Zhang, D. Guo, R. Xu, N. Kumar, and W. Wang, "Mean field game and broadcast encryption-based joint data freshness optimization and privacy preservation for mobile crowdsensing," *IEEE Trans. Veh. Technol.*, vol. 72, no. 11, pp. 14860–14874, Nov. 2023.
[16] Z. Han et al., "Smart optimization solution for channel access attack defense under UAV-aided heterogeneous network," *IEEE Internet Things J.*, vol. 10, no. 21, pp. 18890–18897, Nov. 2023.
[17] W. Wang, G. Srivastava, J. C.-W. Lin, Y. Yang, M. Alazab, and T. R. Gadekallu, "Data freshness optimization under CAA in the UAV-aided MECN: A potential game perspective," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 11, pp. 12912–12921, Nov. 2023.
[18] J. Wang et al., "Generative AI based secure wireless sensing for ISAC networks," *IEEE Trans. Inf. Forensics Security*, vol. 20, pp. 5195–5210, 2025.
[19] Y. Chen et al., "Full-duplex integrated sensing, communication, and computation over low-altitude wireless networks," 2025, *arXiv:2504.18143*.
[20] K. Meng, Q. Wu, S. Ma, W. Chen, K. Wang, and J. Li, "Throughput maximization for UAV-enabled integrated periodic sensing and communication," *IEEE Trans. Wireless Commun.*, vol. 22, no. 1, pp. 671–687, Jan. 2023.
[21] X. Jing, F. Liu, C. Masouros, and Y. Zeng, "ISAC from the sky: UAV trajectory design for joint communication and target localization," *IEEE Trans. Wireless Commun.*, vol. 23, no. 10, pp. 12857–12872, Oct. 2024.
[22] Z. Kuang et al., "Movable-antenna array empowered ISAC systems for low-altitude economy," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC Workshops)*, China, Aug. 2024, pp. 776–781.
[23] X. Ye, Y. Mao, X. Yu, S. Sun, L. Fu, and J. Xu, "Integrated sensing and communications for low-altitude economy: A deep reinforcement learning approach," 2024, *arXiv:2412.04074*.
[24] J. Tang et al., "Cooperative ISAC-empowered low-altitude economy," *IEEE Trans. Wireless Commun.*, vol. 24, no. 5, pp. 3837–3853, May 2025.
[25] Y. Liu et al., "A game theoretical anti-jamming beamforming approach for integrated sensing and communications systems," *IEEE Trans. Veh. Technol.*, vol. 73, no. 10, pp. 15780–15785, Oct. 2024.
[26] M. T. Mamaghani, X. Zhou, N. Yang, and A. Lee Swindlehurst, "Securing integrated sensing and communication against a mobile adversary: A Stackelberg game with deep reinforcement learning," *IEEE J. Sel. Areas Commun.*, vol. 44, pp. 942–958, 2026.
[27] Y. Chen, H. Yang, X. Ou, Y. Jiang, and Z. Xiong, "Anti-jamming resource allocation for integrated sensing and communications based on game-guided reinforcement learning," *IEEE Wireless Commun. Lett.*, vol. 14, no. 1, pp. 223–227, Jan. 2025.
[28] Y. Yang, W. Wang, L. Liu, K. Dev, and N. M. F. Qureshi, "AoI optimization in the UAV-aided traffic monitoring network under attack: A Stackelberg game viewpoint," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 1, pp. 932–941, Jan. 2023.
[29] Y. Yang, X. Wei, R. Xu, L. Peng, and L. Liu, "Game-based channel access for AoI-oriented data transmission under dynamic attack," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8820–8837, Jun. 2022.
[30] Y. Qin, J. Tang, F. Tang, M. Zhao, and N. Kato, "Multi-agent reinforcement learning in adversarial game environments: Personalized anti-interference strategies for heterogeneous UAV communication," *IEEE Trans. Mobile Comput.*, vol. 24, no. 9, pp. 8886–8898, Sep. 2025.
[31] S. Feng, Z. Xiong, D. Niyato, and P. Wang, "Dynamic resource management to defend against advanced persistent threats in fog computing: A game theoretic approach," *IEEE Trans. Cloud Comput.*, vol. 9, no. 3, pp. 995–1007, Jul. 2021.
[32] X. Liu, T. Huang, N. Shlezinger, Y. Liu, J. Zhou, and Y. C. Eldar, "Joint transmit beamforming for multiuser MIMO communications and MIMO radar," *IEEE Trans. Signal Process.*, vol. 68, pp. 3929–3944, 2020.
[33] Z. Yu et al., "Active RIS-aided ISAC systems: Beamforming design and performance analysis," *IEEE Trans. Commun.*, vol. 72, no. 3, pp. 1578–1595, Mar. 2024.
[34] K. Liu, Z. Zhang, L. Dai, S. Xu, and F. Yang, "Active reconfigurable intelligent surface: Fully-connected or sub-connected?" *IEEE Commun. Lett.*, vol. 26, no. 1, pp. 167–171, Jan. 2022.
[35] S. Kaul, R. Yates, and M. Gruteser, "Real-time status: How often should one update?" in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 2731–2735.
[36] Y. Yang, M. He, W. Han, X. Lu, and C. Hou, "Data freshness performance analysis and optimization in timely and secure low altitude economics," *IEEE Trans. Cognit. Commun. Netw.*, vol. 12, pp. 6016–6030, 2026.
[37] Y. Yang et al., "Stochastic geometry-based age of information performance analysis for privacy preservation-oriented mobile crowdsensing," *IEEE Trans. Veh. Technol.*, vol. 72, no. 7, pp. 9527–9541, Jul. 2023.
[38] T. Phung-Duc, K. Akutsu, K. Kawanishi, O. Salameh, and S. Wittevrongel, "Queueing models for cognitive wireless networks with sensing time of secondary users," *Ann. Operations Res.*, vol. 310, no. 2, pp. 641–660, Mar. 2022.
[39] Y. Yang, B. Zhang, D. Guo, Z. Xiong, D. Niyato, and Z. Han, "Can we realize data freshness optimization for privacy preserving-mobile crowdsensing with artificial noise?" *IEEE Trans. Mobile Comput.*, vol. 23, no. 12, pp. 11357–11374, Dec. 2024.
[40] G. E. Forsythe, M. A. Malcolm, and C. B. Moler, *Computer Methods for Mathematical Computations*. Upper Saddle River, NJ, USA: Prentice-Hall, 1977.
[41] R. P. Brent, *Algorithms for Minimization Without Derivatives*. North Chelmsford, MA, USA: Courier Corporation, 2013.
[42] J.-P. Aubin, *Mathematical Methods of Game and Economic Theory*. North Chelmsford, MA, USA: Courier Corporation, 2007.
[43] S.-L. Chang, K.-C. Lee, R.-R. Huang, and Y.-H. Liao, "Resource-allocation mechanism: Game-theory analysis," *Symmetry*, vol. 13, no. 5, p. 799, May 2021.
[44] H. M. Birhanie, S.-M. Senouc, M. A. Messous, A. Arfaoui, and A. Kies, "A stochastic theoretical game approach for resource allocation in vehicular fog computing," in *Proc. IEEE 17th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2020, pp. 1–2.
[45] S. Ma, L. L. Zhang, and X. Cai, "Optimizing joint technology selection, production planning and pricing decisions under emission tax: A Stackelberg game model and nested genetic algorithm," *Expert Syst. Appl.*, vol. 238, Mar. 2024, Art. no. 122085.
[46] I. Miller, "Probability, random variables, and stochastic processes," Arthur D. Little, Inc., Cambridge, MA, USA, Tech. Rep., 1966.
[47] R. Nelson, *Probability, Stochastic Processes, and Queueing Theory: The Mathematics of Computer Performance Modeling*. Cham, Switzerland: Springer, 2013.



Jiacheng Wang (Member, IEEE) received the Ph.D. degree from the School of Communications and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing, China. He is currently a Research Fellow with the College of Computing and Data Science, Nanyang Technological University, Singapore. His research interests include wireless sensing security, generative AI, low-altitude wireless networks, and semantic communications.

Authorized licensed use limited to: Auburn University. Downloaded on March 26,2026 at 04:01:58 UTC from IEEE Xplore. Restrictions apply.



Jialing He (Member, IEEE) received the M.S. and Ph.D. degrees from Beijing Institute of Technology, Beijing, China, in 2018 and 2022, respectively. She is currently an Associate Professor with the College of Computer Science, Chongqing University, Chongqing, China. Her current research interests include AI security, user behavior mining, and blockchain.



Geng Sun (Senior Member, IEEE) received the B.S. degree in communication engineering from Dalian Polytechnic University and the Ph.D. degree in computer science and technology from Jilin University in 2011 and 2018, respectively. He was a Visiting Researcher with the School of Electrical and Computer Engineering, Georgia Institute of Technology, USA. He is currently a Professor with the College of Computer Science and Technology, Jilin University. His research interests include wireless networks, UAV communications, mobile edge computing, and generative AI.



Zehui Xiong (Senior Member, IEEE) received the Ph.D. degree from Nanyang Technological University (NTU). He is currently a Full Professor with the School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, U.K. Prior to that, he was with Singapore University of Technology and Design and NTU. He was a Visiting Scholar with Princeton University and University of Waterloo. Recognized as a Clarivate Highly Cited Researcher, he has published over 250 peer-reviewed research papers in leading journals, with numerous best paper awards from international flagship conferences. Featured in Forbes Asia 30U30, he serves as an editor for many leading journals and the chair for numerous international conferences. His honors include the IEEE Asia–Pacific Outstanding Young Researcher Award, IEEE VTS Early Career Award, IEEE Early Career Award for Excellence in Scalable Computing, IEEE Technical Committee on Blockchain and Distributed Ledger Technologies Early Career Award, IEEE Internet Technical Committee Early Achievement Award, IEEE TCSVC Rising Star Award, IEEE TCI Rising Star Award, IEEE TCCLD Rising Star Award, IEEE ComSoc Outstanding Paper Award, IEEE Best Land Transport Paper Award, IEEE Asia–Pacific Outstanding Paper Award, IEEE CSIM Technical Committee Best Journal Paper Award, IEEE SPCC Technical Committee Best Paper Award, and IEEE Big Data Best Influential Conference Paper Award.



Dusit Niyato (Fellow, IEEE) received the B.Eng. degree from the King Mongkut's Institute of Technology Ladkrabang (KMITL), Thailand, and the Ph.D. degree in electrical and computer engineering from the University of Manitoba, Canada. He is currently a Professor with the College of Computing and Data Science, Nanyang Technological University, Singapore. His research interests are in the areas of mobile generative AI, edge general intelligence, quantum computing and networking, and incentive mechanism design.



Shiwen Mao (Fellow, IEEE) is currently a Professor and the Earle C. Williams Eminent Scholar Chair and the Director of the Wireless Engineering Research and Education Center, Auburn University, Auburn, AL, USA. His research interests include wireless networks, multimedia communications, and smart grid. He received the NSF CAREER Award in 2010, IEEE ComSoc TCCSR Distinguished Technical Achievement Award in 2019, and the IEEE ComSoc MMTC Outstanding Researcher Award in 2023. He was a co-recipient of the 2022 Best Journal Paper Award of IEEE ComSoc eHealth Technical Committee, the 2021 Best Paper Award of Elsevier/Digital Communications and Networks (KeAi), the 2021 IEEE Internet of Things Journal Best Paper Award, the 2021 IEEE Communications Society Outstanding Paper Award, the IEEE Vehicular Technology Society 2020 Jack Neubauer Memorial Award, the 2018 ComSoc MMTC Best Journal Paper Award and the 2017 Best Conference Paper Award, the 2004 IEEE Communications Society Leonard G. Abraham Prize in the Field of Communications Systems, and several ComSoc technical committee and conference best paper/demo awards. He is the Editor-in-Chief of IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING. He is a Distinguished Lecturer of IEEE Communications Society and the IEEE Council of RFID.



Dong In Kim (Life Fellow, IEEE) received the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, CA, USA, in 1990. He was a Tenured Professor with the School of Engineering Science, Simon Fraser University, Burnaby, BC, Canada. He is currently a Distinguished Chair Professor with the College of Information and Communication Engineering, Sungkyunkwan University, Suwon, South Korea. He is a fellow of Korean Academy of Science and Technology and a Life Member of the National Academy of Engineering of Korea. He was a first recipient of the NRF of Korea Engineering Research Center (ERC) in Wireless Communications for RF Energy Harvesting from 2014 to 2021. He received several research awards, including the 2023 IEEE ComSoc Best Survey Paper Award and the 2022 IEEE Best Land Transportation Paper Award. He was selected the 2019 recipient of the IEEE ComSoc Joseph LoCicero Award for Exemplary Service to Publications. He was the General Chair of the IEEE ICC 2022, Seoul. From 2001 to 2024, he served as an Editor, an Editor at Large, and an Area Editor of Wireless Communications I for IEEE TRANSACTIONS ON COMMUNICATIONS. From 2002 to 2011, he served as an Editor and a Founding Area Editor of Cross-Layer Design and Optimization for IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS. From 2008 to 2011, he served as the Co-Editor-in-Chief for the IEEE/KICS JOURNAL OF COMMUNICATIONS AND NETWORKS. He served as the Founding Editor-in-Chief for the IEEE WIRELESS COMMUNICATIONS LETTERS from 2012 to 2015. He has been listed as a 2020/2022/2025 Highly Cited Researcher (HCR) by Clarivate Analytics.



Tao Xiang (Senior Member, IEEE) received the B.Eng., M.S., and Ph.D. degrees in computer science from Chongqing University, China, in 2003, 2005, and 2008, respectively. He is currently a Professor and the Dean of the School of Computer Science, Chongqing University. His research interests include multimedia security, cloud security, data privacy, and cryptography. He has published over 200 papers on international journals and conferences. He serving as an Associate Editor for IEEE TRANSACTIONS ON CLOUD COMPUTING, IEEE TRANSACTIONS ON CYBERNETICS, and IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING.

Authorized licensed use limited to: Auburn University. Downloaded on March 26,2026 at 04:01:58 UTC from IEEE Xplore. Restrictions apply.