AoI Optimization in the UAV-Aided Traffic Monitoring Network Under Attack: A Stackelberg Game Viewpoint

Yaoqi Yang, Weizheng Wang, Lingjun Liu, Kapal Dev, *Senior Member, IEEE*, and Nawab Muhammad Faseeh Qureshi

***Abstract*— Intelligent Vehicle Systems (IVSs) devote to integrating the data sensing, processing, and transmission in the Vehicle to Everything (V2X) scenarios, where the Unnamed Aircraft Vehicle (UAV)-aided traffic monitoring network is one of the most significant applications. Moreover, since the central premise to support the IVS is timely and effectively sensing data processing, Age of Information (AoI) can precisely reflect the timeliness and effectiveness of the communication process in the UAV-aided traffic monitoring network. However, recent researches pay little attention to AoI minimization issue, especially when the malicious attacker attempts to deteriorate the network performance. The accurately modelling of the adversarial relationship between legitimate UAVs and attacker is not fully investigated. To make up this research gap, we start from the Stackelberg game viewpoint to investigate the AoI optimization problem in the UAV-aided traffic monitoring network under attack. Firstly, the system model and three-layer Stackelberg game-based optimization goal are established. Secondly, based on the Backward Induction (BI) analysis, the follower's data sensing rate, transmission power, and the leader's attacking power are determined by the Lagrange duality optimization technology successively. Moreover, the sub-gradient update-based optimization technology is used to achieve the Stackelberg Equilibrium (SE). Finally, simulations are performed under various parameters. The evaluation results present better performance of our proposed approach when compared with the typical baselines.**

***Index Terms*— UAV, traffic monitoring network, AoI, Stackelberg game.**

I. Introduction

With the rapid development of the digital society, Intelligent Vehicle System (IVS) has been playing an increasingly important role in vehicle communication. Although IVS brings more efficient communication protocols, establishes the cooperation framework, and enhances the performance for the Vehicle to Everything (V2X) networks, it still faces some fundamental challenges (e.g., timely data transmission, computation-oriented data sensing, and high request arrival rate), which result from the massive data integration needs, complex application scenarios, and dynamic transmission environments. At the same time, timeless and effective data processing is also critical for the IVS [1], especially in the traffic monitoring network scenarios. Moreover, the Unnamed Aircraft Vehicle (UAV) equipped with advanced sensing modules is commonly used to perform traffic monitoring tasks due to its fast development, high mobility, and ultra-reliability [2], [3]. Hence, it is of great significance to address the freshness-oriented data processing issue in the UAV-aided traffic monitoring network, whose solutions could be applied to solve the major challenges of the IVS.

As a critical indicator of data freshness, Age of Information (AoI) is defined as the elapsed time from sample generation to receive. Besides, fundamentally different from the latency conception at the protocol layers, AoI represents the performance metric in the application layer which can well capture the elapsed time after the latest successful transmission of the sensing data. Up to now, some AoI optimization efforts have been made in the traffic monitoring networks, such as data collection for the vehicle [4], self-risk assessment [5], and cooperative driving [6]. However, some security factors are not considered while the AoI value is minimized. For example, an attacker may intrude the system and degrade network performance, intercept, monitor and even steal the transmitted data content. Therefore, the unbenign relationship between legitimate UAVs and the attackers should be concisely curved to defend attackers in the considered scenario. Moreover, the relevant variables influencing AoI should be optimized simultaneously.

When it comes to the AoI optimization problem in the UAV-aided traffic monitoring network under attack, game theory is a promising solution that can form the optimal AoI optimization strategy. Currently, some game-based performance optimization strategies in the light of attacks have been made to describe the players' relationships, such as cooperative relationships in multi-machine defence optimization [7], completion relationships in false data injection defence [8]. However, the data freshness has not been fully investigated in their scenarios, i.e., AoI minimization. To solve this problem, we transform these two challenges into some game models with two goals: 1. the leader-follower relationship between the legitimate UAV and the attacker should be analyzed and modelled correctly; 2. the AoI-related variables should be considered for the data freshness optimization.

Manuscript received 13 September 2021; revised 12 December 2021 and 7 February 2022; accepted 3 March 2022. Date of publication 22 March 2022; date of current version 26 January 2023. The Associate Editor for this article was A. Jolfaei. *(Corresponding authors: Weizheng Wang; Nawab Muhammad Faseeh Qureshi.)*

Yaoqi Yang is with the Graduate School, Army Engineering University of PLA, Nanjing 210000, China (e-mail: yaoqi_yang@yeah.net).

Weizheng Wang is with the Department of Computer Science, City University of Hong Kong, Hong Kong (e-mail: weizheng.wang@ieee.org).

Lingjun Liu is with the Designing Institute of Communication and Information Engineering, Shenyang 110000, China (e-mail: chaconne2013@foxmail.com).

Kapal Dev is with the Institute of Intelligent Systems, University of Johannesburg, Johannesburg 2092, South Africa (e-mail: kapal.dev@ieee.org).

Nawab Muhammad Faseeh Qureshi is with the Department of Computer Education, Sungkyunkwan University, Seoul 03005, South Korea (e-mail: faseeh@skku.edu).

Digital Object Identifier 10.1109/TITS.2022.3157394

To solve the above-mentioned challenges, we formulate the AoI optimization problem from the Stackelberg game viewpoint in the UAV-aided traffic monitoring network encountering attack. Then, based on the Lagrange duality optimization technology, the Stackelberg Equilibrium (SE) solution is derived. The main contributions for this paper can be summarized as follows:

1) Given the existence of attacker in the UAV-aided traffic monitoring networks, the adversarial relationship-based Stackelberg game model and the observation model with incomplete information are established.
2) In order to reach the SE status of the formulated Stackelberg game, the Lagrange duality optimization technology is used to derive the optimal solution. Besides, the property analysis of the Stackelberg game is also presented in detail.
3) To verify the feasibility and performance of the proposed approach, we conduct simulations experiments under various parameters. The experiment results show that our proposal could obtain better AoI performance under different parameters settings.

The rest of the paper is organized as follows. The related work is introduced in Section II, which contains two respects, i.e., AoI optimization in the traffic networks and game-based performance optimization under attack. In Section III, after the system model establishment, a three layer optimization goal is formulated. Besides, the Stackelberg game-based AoI optimization strategy is determined in Section IV. Subsequently, Section V sets the simulation parameters and evaluates the effectiveness of the proposed algorithm. Finally, Section VI briefly concludes this paper.

II. Related Works

A. AoI Optimization in the Traffic Networks

With the emergence of the ITS, rapid and efficient data processing is becoming more and more important. Simultaneously, AoI can play a vital role in traffic networks to describe the data freshness. Therefore, the AoI optimization issue in traffic networks is of great interest and far-reaching significance. Up to now, some efforts have been paid to optimize AoI in the traffic networks. For example, to overcome the constrains of the sample rates and queue models, Qin *et al.* [4] minimize the AoI based on the Lyapunov optimization technique. Choudhury *et al.* [5] take the self tracking error into consideration while optimizing the trackability-aware AoI. Ploger *et al.* [6] use the Markov modulated process model to minimize the AoI after modeling the cooperative driving relationships. Wang *et al.* [14] aim at optimizing the long term average AoI with Hybrid Automatic Repeat Request (HARQ) scheme, where the transmission errors and encoding types are considered. Wang *et al.* [15] formulate the AoI expression in the closed form and jointly optimize the AoI and information reachability. Zhang *et al.* [16] consider the AoI and latency performance at the same time, where AoI and service time all both optimized. Alabbasi *et al.* [18] utilize the convex optimization approach to make the balance between AoI and completion time. As we can see from Table I, current efforts in this field are categorized by four aspects, i.e., optimization goal, proposed method, optimization constraints, and attack consideration. It is clear can be seen that all of the listed references omit the critical security issue, i.e., attack scenario, when optimizing the AoI and other indicators. However, AoI minimization under attack cases is indispensable, especially in the traffic networks with the coexistence of challenges and opportunities.

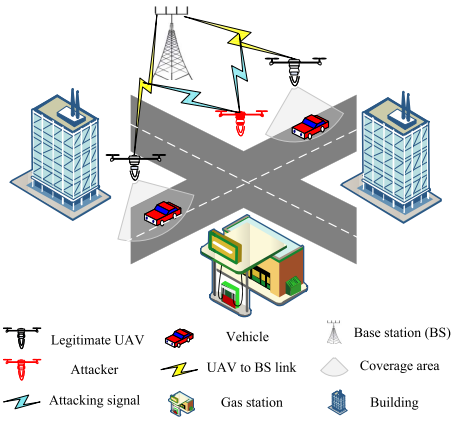


Fig. 1. UAV-aided traffic monitoring network under attack.

B. Game-Based Performance Optimization Under Attack

As an important branch of the applied mathematics, game theory can be used to model the cooperative or non-cooperative relationships among the players. Especially when mentioning the security issue in wireless networks, game theory can effectively find the performance optimization strategy. For instance, Liu *et al.* [2] enhance the secure data transmission rate with backward induction method, where the zero-sum model is established. Xu *et al.* [7] propose one cooperative and non-cooperative game-based model, which aim at jointly optimizing the attack risk and defense model. Ahmadian *et al.* [8] focus on the false data injection defense, where the GAN approach and zero-sum game mode are combined. Yang *et al.* [19] improve the failure rate and mean time performance at the same time, where the attack-defense game model is put forward. Eisenstadt Moshaiov [20] optimize the network utility, where the evolution algorithm is adopted after establishing the multi-object game. Rudenko *et al.* [21] consider the secrecy capacity after establishing the extensive model. After modeling the Stackelberg game model, Liu *et al.* [22] optimize the transmission with the DNN-based method. Wang *et al.* [23] pay attention to optimizing the selection strategy of the relay with an approximation algorithm, in which Bertrand game is used. As shown in Table II, we compare the current work in terms of four aspects such as optimization goal, proposed method, established game model, and data freshness consideration. However, few researches consider the AoI metrics for the optimization goal, while AoI is critical for network performance evaluation.

III. System Model and Problem Formulation

As shown in Fig. 1, several UAVs are hovering over the sky to perform the traffic monitoring tasks. Simultaneously, these UAVs are equipped with sensing modules to collect related data (e.g., the vehicles' speed and density) within their coverage area. On the other hand, the network can be viewed as the status updating system owing to the mobility of the vehicles, so the freshness of the sensed data is inevitable [9]. UAV should transmit the data to the Base Station (BS) immediately to maintain the timeliness and effectiveness of sensing data. However, an intelligent attacker can also disguise as a legitimate member in the UAV swarm, which is maliciously

TABLE I
AOI OPTIMIZATION IN THE TRAFFIC NETWORKS

Ref.	Optimization goal	Proposed method	Optimization constrains	Attack-mentioned
[4]	AoI minimization	The Lyapunov optimization technique	Sample rate, queue models, routing, and reward constrains	No
[5]	Trackability-aware Age of Information (TAoI) minimization	Decentralized TAoI rate control algorithm	Self tracking error (self-TE)	No
[6]	AoI minimization	The generic Markov modulated process model analysis in theory	The cooperative driving relationships	No
[14]	Long term average AoI minimization	Hybrid Automatic Repeat Request (HARQ) scheme	Transmission errors, encoding types, and codeword length	No
[15]	Joint AoI and information reachability optimization	A closed equation in theory	Multiple interference, noise and path loss factor	No
[16]	Joint average AoI and service latency optimization	The roadside unit centric (RSUC) scheme and request adaptive (ReA) scheme	AoI and latency trade-off	No
[18]	Joint AoI and completion time optimization	The convex optimization technology	AoI and completion time trade-off	No
Ours	AoI minimization	The Lagrange duality optimization technology	Attacking distance, data sensing rate, and transmission power	Yes

TABLE II
GAME-BASED PERFORMANCE OPTIMIZATION UNDER ATTACK

Ref.	Optimization goal	Proposed method	Established game model	Data freshness consideration
[2]	The secure data transmission	The backward induction method	Zero-sum game	No
[7]	The multi-machine joint attack and defense model	The optimal control optimization algorithm	Cooperative game and non-cooperative game	No
[8]	The false data injection defense	The Generative Adverserial Network (GAN)-based approach	Zero-sum game	No
[19]	The failure rate and mean time optimization	Event simulation and analysis	Attack-Defense game	No
[20]	The network functionality	The evolutionary-based algorithm	Multi-Objective game	No
[21]	The secrecy capacity	An extensive game-based algorithm	Extensive game	No
[22]	The transmission power	The deep neural network (DNN)-based approach	Stackelberg game	No
[23]	The selection of the relay	An approximation algorithm	Bertrand game	No
Ours	AoI minimization	The Lagrange duality optimization technology	Stackelberg game	Yes

manipulated [10] to deteriorate the network's performance by intervening the links between UAV and BS. In summary, the legitimate UAV and attacker could perceive the mutual position and transmission power and make strategies to maximize their utilities. Firstly, the attacker is the leader, which damages the network performance by one attacking power. Then, the legitimate UAV optimizes its data sensing rate and transmission power to restore the AoI performance. For ease of presentation, the main notations used in this paper are shown in Table III.

A. UAV Model

For the UAV model, assume the number of the UAVs is N, the UAV set is $\mathcal{U} = \{U_1, U_2, \ldots, U_N\}$, the position set is $\Theta = \left\{\left(x_1^U, y_1^U, z_1^U\right), \left(x_2^U, y_2^U, z_2^U\right), \ldots, \left(x_N^U, y_N^U, z_N^U\right)\right\}$, and the power set is $\mathcal{P} = \{P_1, P_2, \ldots, P_N\}$, where U_i is the i-th UAV, $\left(x_i^U, y_i^U, z_i^U\right)$, λ_i and P_i are the position, date sensing rate and transmitting power of the i-th UAV, respectively. Besides, the available channel set for the UAVs is $\mathcal{A} = \{A_1, A_2, \ldots, A_N\}$, and the channel gain between the i-th UAV and base station is $\eta_i^U = d_i^{-\alpha}$, where the position of BS is $\left(x^B, y^B, 0\right)$, $d_i = \sqrt{\left(x_i^U - x^B\right)^2 + \left(y_i^U - y^B\right)^2 + \left(z_i^U\right)^2}$ is the distance between the i-th UAV and base station, and α is the path loss factor.

B. Attacker Model

As for the attacker model, the attacker's position is $\left(x^J, y^J, z^J\right)$. Besides, J represents the power of the attacking signal, and the channel gain for the attacker is $\eta^J = d_J^{-\alpha}$, where $d_J = \sqrt{\left(x^J - x^B\right)^2 + \left(y^J - y^B\right)^2 + \left(z^J\right)^2}$ is the distance from the attacker to the BS. Note that it is impossible to infinitely increase the transmission power to improve the network performance, so the transmission cost of the i-th UAV and the attacker are defined as C^{Ui} and C^J, respectively.

C. AoI Model

The considered AoI model is based on the queue theory, where the queue rule is FSFS (First Come First Serve), and the queue model is M/M/1 [1]. Concretely, the data sensed by the UAV is transmitted to the BS through the wireless channels. Hence, the sensed data is the guest and the channel is the server. Besides, the data sensing rate λ subjects to the Poisson distribution, and the serving rate μ, i.e., channel capacity, obeys the negative exponential distribution. Note that the channel capacity μ_i for the i-th UAV is:

$$\begin{aligned}\mu_i &= B \times \log_2\left(1 + \Omega_i\right) \\ &= B \times \log_2\left(1 + P_i / \left(J + N_0 + \sum_{m \neq i} P_m\right)\right), \end{aligned} \quad (1)$$

where B is the bandwidth, Ω is the Signal-on-Interference-plus-Noise Ratio (SINR) [11] and related with P_i and J, N_0 is the environment noise, and $\sum_{m \neq i} P_m$ is the co-channel interference [12]. Define the utilization rate $\rho_i = \frac{\lambda_i}{\mu_i}$, following the similar analysis in [1]'s Section III, the AoI value can be determined as follows.

In Fig. 2, $t = 0$ is the observation starting time, and the initial AoI value is $AoI(0) = AoI_0$. After that, $t_1, t_2, \ldots, t_n$

TABLE III
NOTATIONS

Notation	Description
$\mathcal{U}$	The legitimate UAVs set
U_i	The i-th legitimate UAV
N	The number of the legitimate UAVs
Θ	The position set of the legitimate UAVs
$\left(x_i^U, y_i^U, z_i^U\right)$	The position of the i-th legitimate UAV
$\mathcal{P}$	The transmission power set of the legitimate UAVs
P_i	The transmission power of the i-th legitimate UAV
$\mathcal{A}$	The available channel set of the legitimate UAVs
A_i	The available channel set of the i-th legitimate UAV
$\left(x^B, y^B, 0\right)$	The position of the base station
η_i^U	The channel gain between the i-th UAV and base station
$\left(x^J, y^J, z^J\right)$	The position of the attacker
η^J	The channel gain of the attacker
J	The attacking power
C^{U_i}	The transmission cost of the i-th legitimate UAV
C^J	The transmission cost of the attacker
λ_i	The data sensing rate of the i-th legitimate UAV
B	The bandwidth of the wireless channel
Ω	The SINR of the sensed data
ρ_i	The data serving rate of the i-th legitimate UAV
AoI_i	The AoI value of sensed data for the i-th legitimate UAV
$\Re_J$	The utility of the attacker
$\Re_{U_i}$	The utility of the i-th legitimate UAV
$\varphi_i\left(\eta_k^J, C_h^{Ui}\right)$	The joint distribution of η_k^J, C_h^{Ui}
$\gamma_i\left(\eta_{is}^U, C_l^J\right)$	The joint distribution of η_{is}^U, C_l^J
t	The iteration index set
ε_{U_i}	The dual variable for the i-th legitimate UAV's power
N_0	The environment noise
λ_{max}	The maximum value of the data sensing rate
P_{max}	The maximum transmission power of the legitimate UAV
J_{max}	The maximum attacking power
λ_{opt}	The optimal data sensing rate of the legitimate UAV
P_{i_opt}	The optimal power of the i-th legitimate UAV
J_{opt}	The optimal attacking power

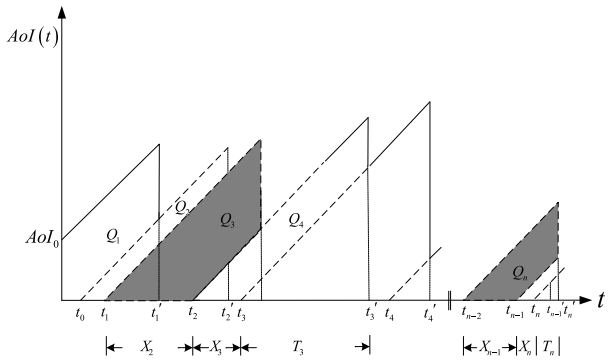


Fig. 2. The AoI model in the UAV-aided traffic monitoring network.

represents the data status update time. Besides, the AoI value increases as time climbs unless a new status is updated at $t_1', t_2', \ldots, t_n'$. To be specific, at time t_i', the AoI value $AoI(t_i')$ is denoted as the age of updating stage $T_i = t_i - t_i'$, and T_i is the system time for updating the i-th sensing data. Based on the above analysis, the AoI function can be represented by the serrated function in Fig. 2.

Considering the time interval $(0, T)$, the average AoI can be expressed as:

$$AoI = \frac{1}{T}\int_0^T AoI\,(t)\,dt. \tag{2}$$

For ease of presentation, let $T = t_n'$ be the observation time interval. Simultaneously, the integral area in Eq. (2) can be divided into three kinds of parts, i.e., polygonal area Q_1, trapezoid area Q_i $(i \geq 2)$, and the triangle with T_n side. When $N(T) = \max\{n | t_n \leq T\}$ represents the arrival time of the data to be transmitted with time T, the average AoI can be denoted as:

$$AoI = \frac{1}{T}\left(Q_1 + \frac{1}{2}T_n^2 + \sum_{i=2}^{N(T)} Q_i\right). \tag{3}$$

In addition, area Q_i can also be calculated with the difference of area between isosceles triangle with side connect point t_{i-1} and point t_i', and isosceles triangle with side connect point is t_i and point t_i'. Define $X_i = t_i - t_{i-1}$ as the i-th data state updating time, we have:

$$Q_i = \frac{1}{2}(T_i + X_i)^2 - \frac{1}{2}{T_i}^2 = T_i X_i + \frac{1}{2}{X_i}^2. \tag{4}$$

Under the M/M/1 queue model, when X_i means the i-th data's arrival time, and take Eq. (4) into Eq. (3), the average AoI can be computed as:

$$AoI = \frac{\tilde{Q}}{T} + \frac{N(T)-1}{T}\cdot\frac{1}{N(T)-1}\sum_{i=1}^{2}\left[T_i X_i + \frac{1}{2}{X_i}^2\right]. \tag{5}$$

where $\tilde{Q} = Q_1 + \frac{{T_n}^2}{2}$. Note that $\frac{\tilde{Q}}{T}$ will converge to zero when T increases. Denote $\lambda = \lim_{T\to\infty}\frac{N(T)-1}{T}$ as the steady rate for sensing data, i.e., the data generation rate of mobile sensor nodes.

Therefore, for the i-th legitimate UAV, the average AoI can be calculated as [1]:

$$AoI_i = \frac{1}{\lambda_i} + \frac{1}{\mu_i} + \frac{{\lambda_i}^2}{{\mu_i}^2(\mu_i - \lambda_i)} = \frac{1}{\mu_i}\left(1 + \frac{1}{\rho_i} + \frac{{\rho_i}^2}{1-\rho_i}\right). \tag{6}$$

D. Observation Model

In addition, due to the incomplete information from the observation of legitimate UAVs and attacker [12], the channel gains (i.e., η_i^U and η^J) and the transmission cost (i.e., C^{Ui} and C^J) are calculated with certain probability. In detail, assume there are S kinds of possible positive states for η_i^U, i.e., $\eta_{i1}^U, \ldots, \eta_{is}^U, \ldots, \eta_{iS}^U$, and η^J has K types of positive states, i.e., $\eta_1^J, \ldots, \eta_k^J, \ldots, \eta_K^J$. Besides, H and L positive states exist in C^{Ui} and C^J, which can be denoted as $C_1^{Ui}, \ldots, C_h^{Ui}, \ldots, C_H^{Ui}$ and $C_1^J, \ldots, C_l^J, \ldots C_L^J$ respectively. At this time, the joint distribution of η_k^J, C_h^{Ui} and η_{is}^U, C_l^J are defined as $\varphi_i\left(\eta_k^J, C_h^{Ui}\right)$ and $\gamma_i\left(\eta_{is}^U, C_l^J\right)$, where equations $\sum_{k=1}^{K}\sum_{h=1}^{H}\varphi_i\left(\eta_k^J, C_h^{Ui}\right) = 1$ and $\sum_{s=1}^{S}\sum_{l=1}^{L}\gamma_i\left(\eta_{is}^U, C_l^J\right) = 1$ hold.

E. Problem Formulation

According to Eq. (1) and Eq. (6), two indicators (i.e., λ_i and μ_i) can influence the AoI value, where μ_i is determined by P_i and J. To maximize the AoI, the attacker determines its power strategy J according to the perception results of the legitimate UAV, which acts as the leader. Then, the legitimate UAV aims to minimize the AoI value by changing the data sensing rate λ_i and transmission power P_i. Note that this UAV is regarded as the follower. At this time, taking the incomplete

observation information into consideration, the attacker's utility $\Re_J$ and the i-th legitimate UAV's utility $\Re_{Ui}$ are defined as follows:

$$\Re_J = \sum_{i=1}^{N}\sum_{s=1}^{S}\sum_{l=1}^{L}\gamma_i\left(\eta_{is}^U, C_l^J\right)\cdot AoI_i - \sum_{s=1}^{S}\sum_{l=1}^{L}\gamma_i\left(\eta_{is}^U, C_l^J\right)\cdot C^J\cdot J. \tag{7}$$

$$\Re_{Ui} = \sum_{k=1}^{K}\sum_{h=1}^{H}\varphi_i\left(\eta_k^J, C_h^{Ui}\right)\cdot\left(-AoI_i - C^{Ui}\cdot P_i\right). \tag{8}$$

Therefore, based on the defined utilities, when the upper bounds of λ_i, P_i and J are λ_{max}, P_{max} and J_{max} accordingly, and the optimal strategies are λ_{opt}, P_{opt} and J_{opt}, the optimization goal is described as follows:

$$\begin{cases}\max\limits_{J}\Re_J\left(\lambda_i, P_i, J\right)\\ subject\ to:\ 0\le J\le J_{\max}\quad(\Pi_1)\\ The\ optimal\ solution:\ \left(\lambda_{opt}, P_{i\_opt}, J\right)\\ \begin{cases}\max\limits_{P_i}\Re_{U_i}\left(\lambda_i, P_i, J\right)\\ subject\ to:\ 0\le P_i\le P_{\max}\quad(\Pi_2)\\ The\ optimal\ solution:\ \left(\lambda_{opt}, P_i, J\right)\\ \begin{cases}\max\limits_{\lambda_i}\Re_{U_i}\left(\lambda_i, P_i, J\right)\\ subject\ to:\ 0\le\lambda_i\le\lambda_{\max}\quad(\Pi_3).\end{cases}\end{cases}\end{cases} \tag{9}$$

IV. Stackelberg Game-Based AoI Optimization Strategy

In this section, for the UAV-aided traffic monitoring network, the attacker acts as the leader to deteriorate the AoI performance, and the legitimate UAVs are the followers that aim to minimize the AoI. As shown in Eq. (9), the optimization variables contain three parameters, i.e., the attacking power J, the transmission power P_i, and the data sensing rate λ_i. In order to determine their values, the Backward Induction (BI) [11] method is adopted. After introducing the SE and NE in the formulated Stackelberg game, the follower-sub game is firstly analyzed and solved, then the leader sub-game is determined. Next, the sub-gradient update-based optimization strategy determination algorithm is put forward to determine the SE of the formulated Stackelberg game. Finally, the properties of the formulated Stackelberg game are proofed.

A. Definition of NE and SE

When the legitimate UAVs and the attacker optimize their data sensing rate, transmission power and the attacking power independently at the same time, the AoI optimization problem could be regarded as the static game. Note that the NE could be derived by determining the optimal strategy of the static game. However, once the NE is reached, the utility of the legitimate UAVs and attacker cannot be improved by the strategy change of the legitimate UAVs and attacker unilaterally. Besides, for the formulated Stackelberg game, SE is the equilibrium point of the Stackelberg game, in other words, when the player unilaterally changes its strategies from SE to others, the utility would not be improved at this time. The SE $\left(\lambda_{opt}, P_{i\_opt}, J_{opt}\right)$ can be determined as follows:

$$\begin{cases}\Re_J\left(\lambda_{opt}, P_{i\_opt}, J_{opt}\right)\ge\Re_J\left(\lambda_i, P_{i\_opt}, J_{opt}\right),\\ \Re_{U_i}\left(\lambda_{opt}, P_{i\_opt}, J_{opt}\right)\ge\Re_{U_i}\left(\lambda_{opt}, P_i, J_{opt}\right),\\ \Re_{U_i}\left(\lambda_{opt}, P_{i\_opt}, J_{opt}\right)\ge\Re_{U_i}\left(\lambda_{opt}, P_{i\_opt}, J\right).\end{cases} \tag{10}$$

B. Follower Sub-Game

Theorem 1: For the i-th legitimate UAV, its optimal data sensing rate λ_{opt} can be determined as:

$$\lambda_{opt} = \begin{cases}\lambda^*, & \Pi_3\cap\Pi_4\\ 0, & otherwise,\end{cases} \tag{11}$$

where λ^* is determined in Eq. (15), and Π_4 is:

$$\Pi_4:\lambda_i<\mu_i. \tag{12}$$

Proof: By performing the second derivative of the utility function $\Re_{U_i}$, we have

$$\frac{\partial^2\Re_{U_i}}{\partial{\lambda_i}^2} = \sum_{k=1}^{K}\sum_{h=1}^{H}\varphi_i\left(\eta_k^J, C_h^{Ui}\right)\cdot\left(-\frac{2}{\lambda_i^3}+\frac{2}{\mu_i\left(\lambda_i-\mu_i\right)}-\frac{4\lambda_i}{\mu_i^2(\lambda_i-\mu_i)^2}+\frac{2\lambda_i^2}{\mu_i^2(\lambda_i-\mu_i)^3}\right). \tag{13}$$

Note that the serving rate μ_i is larger than the data sensing rate λ_i, so $\frac{\partial^2\Re_{U_i}}{\partial{\lambda_i}^2}<0$, and the first derivative $\frac{\partial\Re_{Ui}}{\partial\lambda_i}$ monotonically decreases. At this time, the λ_{opt} can be achieved by solving

$$\frac{\partial\Re_{Ui}}{\partial\lambda_i} = \sum_{k=1}^{K}\sum_{h=1}^{H}\varphi_i\left(\eta_k^J, C_h^{Ui}\right)\cdot\left(\frac{{\lambda_i}^2}{\mu_i^2(\lambda_i-\mu_i)^2}-\frac{2\lambda_i}{\mu_i(\lambda_i-\mu_i)^2}-\frac{1}{\lambda_i^2}\right)=0. \tag{14}$$

When taking Eq. (6) into Eq. (14), we have

$$\sum_{k=1}^{K}\sum_{h=1}^{H}\varphi_i\left(\eta_k^J, C_h^{Ui}\right)\cdot\left(\rho_i^4-2\rho_i^3+\rho_i^2-2\rho_i+1\right)=0. \tag{15}$$

Note that based on the conclusion in [1]'s Section IV, $\lambda^*\approx 0.53\mu_i$. ∎

Remark 1: Owing to $\frac{\partial^2\Re_{U_i}}{\partial{\lambda_i}^2}<0$, the problem of $\Re_{U_i}$ maximization still belongs to the convex optimization problem, and the Lagrange duality optimization approach is effective [12]. Given the value range of the λ_i, here we determine the value of λ_{opt} by letting the value of $\frac{\partial\Re_{Ui}}{\partial\lambda_i}$ be 0, where the $\Re_{Ui}$ monotonically increases within $(0, J^*)$, and monotonically decreases within $(J^*, J_{\max})$.

Theorem 2: For the i-th legitimate UAV, its optimal transmission power P_{i_opt} can be determined as:

$$P_{i\_opt} = \begin{cases}P_i^*, & \Pi_2\cap\Pi_5\\ 0, & otherwise.\end{cases} \tag{16}$$

where P_i^* is defined in Eq. (25), and Π_5 is:

$$\Pi_5:\frac{\sum_{k=1}^{K}\pi_k^J\left(\eta_k^J\right)\cdot\eta_k^J\cdot J+N_0+\sum_{m\ne i}\eta_m^U\cdot P_m}{\eta_i^U}\ge\frac{B}{\ln 2\left(\sum_{h=1}^{H}\pi_h^{Ui}\left(C_h^{Ui}\right)\cdot C_h^{Ui}+\varepsilon_{U_i}\right)}. \tag{17}$$

Proof: When the data sensing rate λ_{opt} is determined, according to the conclusion in [1], AoI minimization is equal to serving rate μ_i maximization. In other words, maximizing

$\Re_{U_i}\left(\lambda_{opt}, P_i, J\right)$ in Eq. (8) is equal to maximizing μ_i in Eq. (1) by determining P_{i_opt}, i.e.,

$$\max_{P_i} \Re_{U_i}\left(\lambda_{opt}, P_i, J\right) = \max_{P_i}\left\{\begin{array}{l}\sum_{k=1}^{K}\sum_{h=1}^{H}\varphi_i\left(\eta_k^J, C_h^{Ui}\right)\cdot \\ \left(\frac{\eta_i^U\cdot P_i}{\eta_k^J\cdot J+N_0+\sum_{m\neq i}\eta_m^U\cdot P_m}-C_h^{Ui}\cdot P_i\right)\end{array}\right\}, \tag{18}$$

Considering the incompletion information from observation, we assume that the attacker's channel gain η_k^J and the user's transmission cost C_h^{Ui} are independent [12], i.e.,

$$\varphi_i\left(\eta_k^J, C_h^{Ui}\right) = \pi_k^J\left(\eta_k^J\right)\cdot\pi_h^{Ui}\left(C_h^{Ui}\right). \tag{19}$$

where $\sum_{k=1}^{K}\pi_k^J\left(\eta_k^J\right)=1$ and $\sum_{h=1}^{H}\pi_h^{Ui}\left(C_h^{Ui}\right)=1$. At this time, Eq. (18) can be rewrote as:

$$\max_{P_i}\Re_{U_i}\left(\lambda_{opt}, P_i, J\right) = \max_{P_i}\left\{\begin{array}{l}\frac{\eta_i^U\cdot P_i}{\sum_{k=1}^{K}\pi_k^J\left(\eta_k^J\right)\cdot\eta_k^J\cdot J+N_0+\sum_{m\neq i}\eta_m^U\cdot P_m} \\ -\sum_{h=1}^{H}\pi_h^{Ui}\left(C_h^{Ui}\right)\cdot C_h^{Ui}\cdot P_i\end{array}\right\}. \tag{20}$$

For ease of presentation, define Γ_{Ui} as the new goal function for the UAV, which is equal to $\max_{P_i}\Re_{U_i}\left(\lambda_{opt}, P_i, J\right)$, i.e.,

$$\Gamma_{Ui} = B\cdot\log_2\left(1+\frac{\eta_i^U\cdot P_i}{\sum_{k=1}^{K}\pi_k^J\left(\eta_k^J\right)\cdot\eta_k^J\cdot J+N_0+\sum_{m\neq i}\eta_m^U\cdot P_m}\right) - \sum_{h=1}^{H}\pi_h^{Ui}\left(C_h^{Ui}\right)\cdot C_h^{Ui}\cdot P_i. \tag{21}$$

By performing the second derivative of Γ_{Ui}, we have:

$$\frac{\partial^2\Gamma_{Ui}}{\partial {P_i}^2} = -\frac{B\cdot\left(\frac{\eta_i^U}{\sum_{k=1}^{K}\pi_k^J\left(\eta_k^J\right)\cdot\eta_k^J\cdot J+N_0+\sum_{m\neq i}\eta_m^U\cdot P_m}\right)^2}{\ln 2\left(1+\frac{\eta_i^U\cdot P_i}{\sum_{k=1}^{K}\pi_k^J\left(\eta_k^J\right)\cdot\eta_k^J\cdot J+N_0+\sum_{m\neq i}\eta_m^U\cdot P_m}\right)^2}<0. \tag{22}$$

Hence, it is a convex optimization problem to determine the value of P_{i_opt}. Then, according to the Lagrange duality optimization theory [11] and introduced nonnegative dual variable ε_{U_i}, the Lagrange function σ_{U_i} is:

$$\sigma_{U_i} = B\cdot\log_2\left(1+\frac{\eta_i^U\cdot P_i}{\sum_{k=1}^{K}\pi_k^J\left(\eta_k^J\right)\cdot\eta_k^J\cdot J+N_0+\sum_{m\neq i}\eta_m^U\cdot P_m}\right) - \sum_{h=1}^{H}\pi_h^{Ui}\left(C_h^{Ui}\right)\cdot C_h^{Ui}\cdot P_i+\varepsilon_{U_i}\cdot\left(P_{\max}-P_i\right). \tag{23}$$

Based on the Karush-Kuhn-Tucker (KKT) conditions [11], let the first derivative of the Lagrange function σ_{U_i} be 0, such as:

$$\frac{\partial\sigma_{U_i}}{\partial P_i} = \frac{B\cdot\left(\frac{\eta_i^U}{\sum_{k=1}^{K}\pi_k^J\left(\eta_k^J\right)\cdot\eta_k^J\cdot J+N_0+\sum_{m\neq i}\eta_m^U\cdot P_m}\right)}{\ln 2\left(1+\frac{\eta_i^U\cdot P_i}{\sum_{k=1}^{K}\pi_k^J\left(\eta_k^J\right)\cdot\eta_k^J\cdot J+N_0+\sum_{m\neq i}\eta_m^U\cdot P_m}\right)} - \sum_{h=1}^{H}\pi_h^{Ui}\left(C_h^{Ui}\right)\cdot C_h^{Ui}-\varepsilon_{U_i}=0. \tag{24}$$

Hence, P_i^* is determined as:

$$P_i^* = \frac{\sum_{k=1}^{K}\pi_k^J\left(\eta_k^J\right)\cdot\eta_k^J\cdot J+N_0+\sum_{m\neq i}\eta_m^U\cdot P_m}{\eta_i^U} - \frac{B}{\ln 2\left(\sum_{h=1}^{H}\pi_h^{Ui}\left(C_h^{Ui}\right)\cdot C_h^{Ui}+\varepsilon_{U_i}\right)}. \tag{25}$$

■

C. Leader Sub-Game

Theorem 3: For the attacker, its optimal attacking power J_{opt} can be determined as:

$$J_{opt} = \begin{cases} J_{\max}, & \Pi_1\cap\Pi_7\cap\Pi_9 \\ J^*, & \Pi_1\cap\Pi_6\cap\Pi_7\cap\Pi_{10}\cap\Pi_{11} \\ J_{\max}, & \Pi_1\cap\Pi_6\cap\Pi_7\cap\Pi_{10}\cap\Pi_{12} \\ J^*, & \Pi_1\cap\Pi_6\cap\Pi_8\cap\Pi_9 \\ J^{**}, & \Pi_1\cap\Pi_8\cap\Pi_{10}. \end{cases} \tag{26}$$

where $\Im_1$ and $\Im_2$ are defined in Eq. (35) and Eq. (36), J^* and J^{**} are defined in Eq. (38) and Eq. (40), and Π_6–Π_{12} can be expressed as:

$$\begin{cases} \Pi_6: \Im_2 > \Im_1 \\ \Pi_7: J > J^{**} \\ \Pi_8: J < J^{**} \\ \Pi_9: J^* < J^{**} \\ \Pi_{10}: J^* > J^{**} \\ \Pi_{11}: J^{**} < J < J^* \\ \Pi_{12}: J^* < J < J_{\max}. \end{cases} \tag{27}$$

Proof: As a leader in the AoI optimization process, the attacker aims to maximize the AoI value. Since λ_{opt} and P_{i_opt} are determined, according to [1], the attacker's utility maximization $\Re_J$ in Eq. (7) is equal to minimizing μ_i, i.e.,

$$\max_J \Re_J\left(\lambda_{opt}, P_{i\_opt}, J\right) = \min_J \mu_i = \max_J\left\{\begin{array}{l}\frac{-\sum_{i=1}^{N}\sum_{s=1}^{S}\sum_{l=1}^{L}\gamma_i\left(\eta_{is}^U, C_l^J\right)\cdot\eta_{is}^U\cdot P_i^*}{\eta^J\cdot J+N_0+\sum_{m\neq i}\eta_m^U\cdot P_m} \\ -\sum_{s=1}^{S}\sum_{l=1}^{L}\gamma_i\left(\eta_{is}^U, C_l^J\right)\cdot C_l^J\cdot J\end{array}\right\}. \tag{28}$$

Similarly, due to the incomplete information of the attacker's observation, the legitimate UAV's channel gain η_{is}^U and the attacking cost C_l^J are also independent [12], i.e.,

$$\gamma_i\left(\eta_{is}^U, C_l^J\right) = \pi_{is}^U\left(\eta_{is}^U\right)\cdot\pi_l^J\left(C_l^J\right). \tag{29}$$

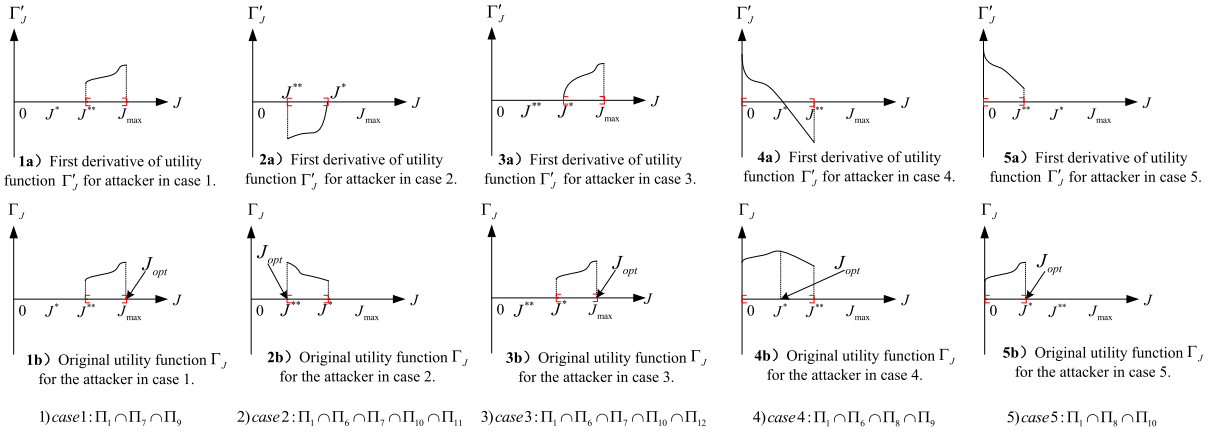


Fig. 3. The optimal attacking power J_{opt} under different cases.

where $\sum_{s=1}^{S} \pi_{is}^{U}\left(\eta_{is}^{U}\right)=1$, and $\sum_{l=1}^{L} \pi_{l}^{J}\left(C_{l}^{J}\right)=1$ hold on. Hence, Eq. (28) can be rewrote as:

$$\begin{aligned}&\max_{J} \Re_J\left(\lambda_{opt}, P_{i\_opt}, J\right)\\&=\max_{J}\left\{-\sum_{i=1}^{N} \frac{\sum_{s=1}^{S} \pi_{is}^{U}\left(\eta_{is}^{U}\right) \cdot \eta_{is}^{U} \cdot P_{i}^{*}}{\eta^{J} \cdot J+N_{0}+\sum_{m \neq i} \eta_{m}^{U} \cdot P_{m}}\right.\\&\left.-\sum_{l=1}^{L} \pi_{l}^{J}\left(C_{l}^{J}\right) \cdot C_{l}^{J} \cdot J\right\}. \end{aligned} \tag{30}$$

At this time, define Γ_J as the new goal function for the attacker, i.e.,

$$\begin{aligned}\Gamma_J=\sum_{i=1}^{N} B \cdot \log_2\left(1-\frac{\sum_{s=1}^{S} \pi_{is}^{U}\left(\eta_{is}^{U}\right) \cdot \eta_{is}^{U} \cdot P_{i}^{*}}{\eta^{J} \cdot J+N_{0}+\sum_{m \neq i} \eta_{m}^{U} \cdot P_{m}}\right)\\-\sum_{l=1}^{L} \pi_{l}^{J}\left(C_{l}^{J}\right) \cdot C_{l}^{J} \cdot J. \end{aligned} \tag{31}$$

By performing the first derivative of Γ_J, we have:

$$\begin{aligned}\frac{\partial \Gamma_J}{\partial J}=\sum_{i=1}^{N} \frac{B}{\ln 2} \cdot \frac{\partial\left(\frac{\sum_{s=1}^{S} \pi_{is}^{U}\left(\eta_{is}^{U}\right) \cdot \eta_{is}^{U} \cdot P_{i}^{*}}{\eta^{J} \cdot J+N_{0}+\sum_{m \neq i} \eta_{m}^{U} \cdot P_{m}}\right)}{\partial J}}{\frac{\sum_{s=1}^{S} \pi_{is}^{U}\left(\eta_{is}^{U}\right) \cdot \eta_{is}^{U} \cdot P_{i}^{*}}{\eta^{J} \cdot J+N_{0}+\sum_{m \neq i} \eta_{m}^{U} \cdot P_{m}}}\\-\sum_{l=1}^{L} \pi_{l}^{J}\left(C_{l}^{J}\right) \cdot C_{l}^{J}. \end{aligned} \tag{32}$$

Denote $\frac{\sum_{s=1}^{S} \pi_{is}^{U}\left(\eta_{is}^{U}\right) \cdot \eta_{is}^{U} \cdot P_{i}^{*}}{\eta^{J} \cdot J+N_{0}+\sum_{m \neq i} \eta_{m}^{U} \cdot P_{m}}$ as Δ, then,

$$\begin{aligned}\frac{\partial \Delta}{\partial J}=\frac{\sum_{k=1}^{K} \pi_{k}^{J}\left(\eta_{k}^{J}\right) \cdot \eta_{k}^{J} \cdot\left(\eta^{J} \cdot J+N_{0}+\sum_{m \neq i} \eta_{m}^{U} \cdot P_{m}\right)}{\left(\eta^{J} \cdot J+N_{0}+\sum_{m \neq i} \eta_{m}^{U} \cdot P_{m}\right)^{2}}\\-\frac{\sum_{s=1}^{S} \pi_{is}^{U}\left(\eta_{is}^{U}\right) \cdot \eta_{is}^{U} \cdot P_{i}^{*} \cdot \eta^{J}}{\left(\eta^{J} \cdot J+N_{0}+\sum_{m \neq i} \eta_{m}^{U} \cdot P_{m}\right)^{2}}. \end{aligned} \tag{33}$$

At this time, take Eq. (33) into Eq. (32) and let $\frac{\partial \Gamma_J}{\partial J}=0$, the following equations hold:

$$\begin{aligned}&\left(\ln 2 \cdot \sum_{l=1}^{L} \pi_{l}^{J}\left(C_{l}^{J}\right) \cdot C_{l}^{J} \cdot \sum_{k=1}^{K} \pi_{k}^{J}\left(\eta_{k}^{J}\right) \cdot \eta_{k}^{J}\right) \cdot J+\Im_1\\&=B \cdot \sum_{k=1}^{K} \pi_{k}^{J}\left(\eta_{k}^{J}\right) \cdot \eta_{k}^{J} \cdot \eta^{J} \cdot J+\Im_2. \end{aligned} \tag{34}$$

$$\begin{aligned}\Im_1=\ln 2 \cdot \sum_{l=1}^{L} \pi_{l}^{J}\left(C_{l}^{J}\right) \cdot C_{l}^{J}\\ \cdot\left(N_{0}+\sum_{m \neq i} \eta_{m}^{U} \cdot P_{m}\right.\\\left.-\frac{B \cdot \sum_{s=1}^{S} \pi_{is}^{U}\left(\eta_{is}^{U}\right) \cdot \eta_{is}^{U}}{\ln 2\left(\sum_{h=1}^{H} \pi_{h}^{Ui}\left(C_{h}^{Ui}\right) \cdot C_{h}^{Ui}+\varepsilon_{U_i}\right)}\right). \end{aligned} \tag{35}$$

$$\begin{aligned}\Im_2=B \cdot\left[\sum_{k=1}^{K} \pi_{k}^{J}\left(\eta_{k}^{J}\right) \cdot \eta_{k}^{J} \cdot\left(N_{0}+\sum_{m \neq i} \eta_{m}^{U} \cdot P_{m}\right)\right]\\-B \cdot \eta^{J} \cdot \sum_{k=1}^{K} \pi_{k}^{J}\left(\eta_{k}^{J}\right) \cdot \eta_{k}^{J}. \end{aligned} \tag{36}$$

$$\Im_3=\left(\begin{array}{l}\ln 2 \cdot \sum_{l=1}^{L} \pi_{l}^{J}\left(C_{l}^{J}\right) \cdot C_{l}^{J} \cdot \sum_{k=1}^{K} \pi_{k}^{J}\left(\eta_{k}^{J}\right) \cdot \eta_{k}^{J} \\ -B \cdot \sum_{k=1}^{K} \pi_{k}^{J}\left(\eta_{k}^{J}\right) \cdot \eta_{k}^{J} \cdot \eta^{J}\end{array}\right). \tag{37}$$

Therefore, J^* can be determined as:

$$J^{*}=\frac{\Im_2-\Im_1}{\Im_3}. \tag{38}$$

Then, we perform the second derivative of Γ_J, i.e.,

$$\frac{\partial^2 \Gamma_J}{\partial J^2}=\sum_{i=1}^{N} \frac{B}{\ln 2} \cdot \frac{\left(\frac{\partial^2 \Delta}{\partial J^2}\right) \cdot(\Delta)-\left(\frac{\partial \Delta}{\partial J}\right)^2}{\Delta^2}. \tag{39}$$

by $\frac{\partial^2 \Gamma_J}{\partial J^2}=0$, we could get J^{**} by solving the following equation, i.e.,

$$\Delta=\varpi_1 \cdot e^{\varpi_2 \cdot J^{**}}. \tag{40}$$

where ϖ_1 and ϖ_2 are the constants determined by the following conditions (41) and (42), shown at the bottom of the next page.

Simultaneously, as shown in Fig. 3, under the considered five following cases, we firstly determine the value range of the variable J. Then, by transforming the sign of the second derivative Γ''_J, we could obtain the monotonicity curve of the first derivative Γ'_J. Finally, according to the sign of the first derivative within different range values of J, the optimal value for the attacker's power J_{opt} can be derived through reaching the maximum value of Γ_J.

Case 1: $\Pi_1 \cap \Pi_7 \cap \Pi_9$. As shown in Fig. 3-1), at first, the value range of J is $J^{**} < J < J_{\max}$. Then, since

the second derivative is greater than 0, the first derivative increases monotonically. This phenomenon guarantees that Γ_J also increases monotonically within $J^{**} < J < J_{\max}$, so the optimal value of Γ_J can be obtained at $J = J_{\max}$.

Case 2: $\Pi_1 \cap \Pi_6 \cap \Pi_7 \cap \Pi_{10} \cap \Pi_{11}$. As shown in Fig. 3-2), the value range of J is determined as $J^{**} < J < J^*$. Subsequently, since the second derivative is greater than 0 and the first derivative increases monotonically, the Γ_J decreases monotonically within $J^{**} < J < J^*$. In the end, the optimal value of Γ_J can be obtained at $J = J^{**}$.

Case 3: $\Pi_1 \cap \Pi_6 \cap \Pi_7 \cap \Pi_{10} \cap \Pi_{12}$. As shown in Fig. 3-3), $J^* < J < J_{\max}$ is the value range of J. At the same time, the second derivative is greater than 0, so the first derivative increases monotonically. Finally, since Γ_J also increases monotonically within $J^* < J < J_{\max}$, the optimal value of Γ_J can be obtained at $J = J_{\max}$.

Case 4: $\Pi_1 \cap \Pi_6 \cap \Pi_8 \cap \Pi_9$. As shown in Fig. 3-4), we can get the value range of J is $0 < J < J^* < J^{**}$, and the second derivative is smaller than 0. Hence, the first derivative decreases monotonically, which guarantees that Γ_J increases monotonically within $0 < J < J^*$, and decreases monotonically within $J^* < J < J^{**}$. Finally, based on the above analysis, the optimal value of Γ_J can be obtained at $J = J^*$.

Case 5: $\Pi_1 \cap \Pi_8 \cap \Pi_{10}$. As shown in Fig. 3-5), the value range of J is $0 < J < J^{**}$. Given the second derivative is smaller than 0 and the first derivative decreases monotonically, Γ_J increases monotonically within $0 < J < J^{**}$. At last, the optimal value of Γ_J can be obtained at $J = J^{**}$. ■

Remark 2: In case 4 and case 5, i.e., $\Pi_1 \cap \Pi_6 \cap \Pi_8 \cap \Pi_9$ and $\Pi_1 \cap \Pi_8 \cap \Pi_{10}$, the second derivative of $\frac{\partial^2 \Gamma_J}{\partial J^2}$ is smaller than 0, so it is a convex optimization problem to determine the value of attacking power J_{opt}. Note that the Lagrange duality optimization approach works out. However, as for other non-convex cases, such as case 1)–case 3), we can also determine their optimal values by analyzing the monotonicity of Γ_J, which is shown in Fig. 3. In summary, by using the Lagrange duality optimization approach and the monotonicity analysis, the optimal value of J can be solved under the convex and non-convex situations.

D. Sub-Gradient Update-Based Optimization Strategy Determination

Based on the sub-gradient update technology [12], the AoI optimization strategy can be determined by the Algorithm 1. To be specific, in step 1, the iteration index variable t is updated for looping, then the variable $\lambda_i(t+1)$, $P_i(t+1)$ and $J(t+1)$ are calculated by Eq. (11), Eq. (16) and Eq. (26) in step 2–step 4, respectively. Next, the dual variable ε_{U_i} is updated with the iteration step $\delta_{U_i}^t$ in step 5. Finally, the looping is ended under the condition $t \geq t_{\max}$. In addition, the symbol "+" in Eq. (43) means the gradient decreasing direction is from the maximum value to the optimized value [11]. It is worth noting that our proposed scheme can derive the AoI optimization solution quickly, when the limited iterations are made, the data sensing rate, transmission power and the attacking power strategies are all determined. Our proposed method is cost-effective and can be easily adopted.

Algorithm 1 Sub-Gradient Update-Based Optimization Strategy Determination

Input: $t = \{0, 1, \ldots, t_{\max}\}$, N_0, B, λ_{max}, P_{max}, J_{max}, η_i^U, η^J, C^{U_i}, C^J, and ε_{U_i}.

Output: λ_{opt}, P_{i_opt}, and J_{opt}.

Step 1) Update $t = t + 1$.

Step 2) Determine $\lambda_i(t+1)$ based on Eq. (11).

Step 3) Determine $P_i(t+1)$ based on Eq. (16).

Step 4) Determine $J(t+1)$ based on Eq. (26).

Step 5) Determine ε_{U_i} based on

$$\varepsilon_{U_i}(t+1) = \left[\varepsilon_{U_i}(t) - \delta_{U_i}^t \cdot (P_{\max} - P_i(t+1))\right]^+. \quad (43)$$

Step 6) When $t \geq t_{\max}$, end iterations and return the value of λ_{opt}, P_{i_opt} and J_{opt}.

TABLE IV
COMPLEXITY ANALYSIS OF THE PROPOSED ALGORITHM

Variable	Calculation expression	Sum complexity
λ	Eq. (11)	$o(N\tau_1)$
P	Eq. (16)	$o(N\tau_2)$
J_{opt}	Eq. (26)	$o(\tau_3)$
δ_U^t	Eq. (43)	$o(N\tau_4)$

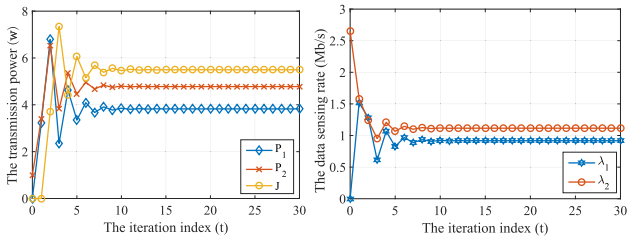
Inspired by the algorithm's complexity analysis in [12], the complexity for the proposed algorithm is detailed in Table IV. To be specific, we denote the total looping times as t_{max}, and the number of the legitimate UAVs arrives as N at first. Then, the calculation complexity for the data sensing rate λ determination is $o(N\tau_1)$, where τ_1 is the small constant for calculating Eq. (11). For the transmission power of legitimate UAV P, its complexity is $o(N\tau_2)$, and τ_2 is the small constant for Eq. (16). Besides, τ_3 and τ_4 are the constants for the calculation complexities in Eq. (26) and Eq. (43), so their complexity are $o(\tau_3)$ and $o(N\tau_4)$. Finally, the total complexity for Algorithm 1 is $o(t_{\max} \cdot (o(N\tau_1) + o(N\tau_2) + o(\tau_3) + o(N\tau_4)))$.

E. Property of the SE in the Formulated Stackelberg Game

Theorem 4: In the formulated Stackelberg game, the SE $(\lambda_{opt}, P_{i\_opt}, J_{opt})$ always exists.

$$\Delta|_{J=0} = \varpi_1 = \frac{N_0 + \sum_{m \neq i} \eta_m^U \cdot P_m - \frac{B \cdot \sum_{s=1}^{S} \pi_{is}^U(\eta_{is}^U) \cdot \eta_{is}^U}{\ln 2\left(\sum_{h=1}^{H} \pi_h^{Ui}(C_h^{Ui}) \cdot C_h^{Ui} + \varepsilon_{U_i}\right)}}{N_0 + \sum_{m \neq i} \eta_m^U \cdot P_m} \quad (41)$$

$$\frac{\partial \Delta}{\partial J}|_{J=0} = \varpi_1 \cdot \varpi_2 = \frac{\sum_{k=1}^{K} \pi_k^J(\eta_k^J) \cdot \eta_k^J \cdot \left(N_0 + \sum_{m \neq i} \eta_m^U \cdot P_m\right)}{\left(N_0 + \sum_{m \neq i} \eta_m^U \cdot P_m\right)^2} - \frac{\eta^J \cdot \left[N_0 + \sum_{m \neq i} \eta_m^U \cdot P_m - \frac{B \cdot \sum_{s=1}^{S} \pi_{is}^U(\eta_{is}^U) \cdot \eta_{is}^U}{\ln 2\left(\sum_{h=1}^{H} \pi_h^{Ui}(C_h^{Ui}) \cdot C_h^{Ui} + \varepsilon_{U_i}\right)}\right]}{\left(N_0 + \sum_{m \neq i} \eta_m^U \cdot P_m\right)^2} \quad (42)$$



(a) (b)

Fig. 4. The convergence behavior evaluation. (a) The convergence behavior of the transmission power. (b) The convergence behavior of the data sensing rate.

Proof: According to definition of SE in Eq. (10), the SE means the optimal strategy when we fix two variables to optimize the third variable for λ, P, and J. Besides, based on the proofs of Theorem 1–Theorem 3, where the optimization problems of the utility function $\max_{J} \Re_J(\lambda_i, P_i, J)$, $\max_{P_i} \Re_{U_i}(\lambda_i, P_i, J)$, and $\max_{\lambda_i} \Re_{U_i}(\lambda_i, P_i, J)$ can be (or partially) transformed into the convex optimization issues, the optimal values of λ, P, and J are solved with λ_{opt}, P_{i_opt}, J_{opt} respectively, so the condition of being the SE is satisfied at this time, and the SE $(\lambda_{opt}, P_{i\_opt}, J_{opt})$ always exists as discussed in [13]'s Section 2. ■

Theorem 5: In the formulated Stackelberg game, the existing SE $(\lambda_{opt}, P_{i\_opt}, J_{opt})$ is unique.

Proof: Based on the proof of Theorem 4, the existing SE refers to the optimal strategies in Eq. (9). The unique values of SE $(\lambda_{opt}, P_{i\_opt}, J_{opt})$ are determined by the Lagrange duality optimization technology, which are shown in Eq. (11), Eq. (16), and Eq. (26). Hence, according to the conclusion in [13]'s Section 3, the existing SE $(\lambda_{opt}, P_{i\_opt}, J_{opt})$ is unique. ■

Theorem 6: With the proposed sub-gradient update-based algorithm, the SE $(\lambda_{opt}, P_{i\_opt}, J_{opt})$ can be reached.

Proof: Based on the conclusions of Theorem 4 and Theorem 5, the existence and the uniqueness of the SE are guaranteed. Under such condition, according to the conclusion in [12], only if the iteration step size of dual variables are determined properly, the sub-gradient update-based algorithm can finally converge to the SE $(\lambda_{opt}, P_{i\_opt}, J_{opt})$. Therefore, by finding one suitable value of dual variable δ_U^t, the SE $(\lambda_{opt}, P_{i\_opt}, J_{opt})$ can be reached. ■

V. Simulation Results and Analysis

A. Parameters Settings

The parameters settings of the simulation are shown in Table V. As can be seen from Table V, there are main three parts in the parameters settings, i.e., legitimate UAV settings, attacker settings, and the environment settings. In addition, the initial value of the dual variable ε_{U_1} and ε_{U_2} all are set as 0.15, and more details about the UAV are consistent with [11].

B. Convergence Behavior

Figure 4(a) is the convergence behavior of the legitimate UAVs' transmission and the attacker's power. At the beginning of the iteration process, the attacker launches the attack with the initial attacking power, then the legitimate UAVs increase the transmission power to minimize the AoI value. Next, in order to damage the AoI performance, the attacker also increases the power. However, owing to the transmission cost limitation, their powers are all deteriorated. After several iterations, finally the power strategies of the legitimate UAVs and the attacker all are determined, which also means that the SE is existent and unique.

Fig. 4(b) is the convergence behavior of the legitimate UAVs' data sensing rate. The legitimate UAVs perform the data sensing tasks with the initial sensing rate value, when the attacker increases the attacking power to deteriorate the network performance, the UAVs also decrease the sensing rate to restore the AoI performance. After several iterations of confrontation, their data generation rates are steady and converged, where the existences and uniqueness of the SE are verified.

TABLE V
Notations

UAV settings			
Symbol	**Value**	**Symbol**	**Value**
(x_1^U, y_1^U, z_1^U)	$(6km, 6km, 150m)$	(x_2^U, y_2^U, z_2^U)	$(8km, 8km, 180m)$
$\lambda_1(0)$	0 Mb/s	$\lambda_2(0)$	2.7 Mb/s
$P_1(0)$	0w	$P_2(0)$	1w
λ_{max}	3 Mb/s	P_{max}	8w
Attacker settings			
Symbol	**Value**	**Symbol**	**Value**
(x^J, y^J, z^J)	$(7km, 7km, 200m)$	$J(0)$	0w
J_{max}	10w		
Environment settings			
Symbol	**Value**	**Symbol**	**Value**
η_1^U	0.5	η_2^U	0.8
C^{U_1}	0.05	C^{U_2}	0.1
η^J	0.4	C^J	0.1
N_0	-50dBm	B	50MHz
$(x^B, y^B, 0)$	$(2km, 2km, 0km)$	α	2
$\delta_{U_1}^t$	1	$\delta_{U_2}^t$	1

C. Effectiveness Performance Evaluation

Fig. 5(a) presents the utility performance under different attacker's costs. When the attacker's transmission cost increases, the utilities of legitimate UAVs' and the attacker's utility climb simultaneously. If the transmission cost of the attacker increases, the attacker would correspondingly enlarge the attacking power to maintain the utility defined in Eq. (7). This situation leads to the decrease of attacker's utility. At this time, the legitimate UAVs could use the lower power to maintain the AoI performance. Hence the legitimate UAV's utility defined in Eq. (8) is improved.

Fig. 5(b) shows the utility performance under different attacking distances. When the distance between the legitimate UAVs and the attacker increases, the channel gain of the legitimate UAVs will keep, but the attacker's channel gain will go down. Note that the channel gain is negatively related with the distance between the legitimate UAV or attacker and the BS. To maximize their respective utilities, the legitimate UAV could reduce its transmission power, while the attacker needs to increase the attacking power. Finally, based on Eq. (7) and Eq. (8), the legitimate UAV's utilities increase, while the attacker's utility decrease.

Fig. 5(c) illustrates the utility performance under different equilibriums. The utilities under SE are better than those under NE [11]. Since the SE solution takes the coupling relationship between the attacker and the legitimate UAVs into consideration, where the power and data sensing rate are not determined independently, so the legitimate UAVs can adjust their strategy timely to maintain the AoI performance.

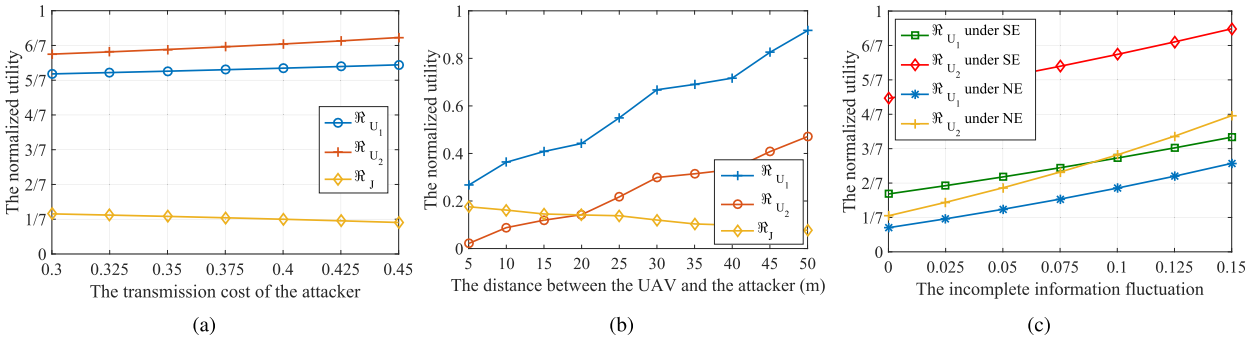


Fig. 5. The effectiveness performance verification. (a) The utility performance under different attacker's costs. (b) The utility performance under different attacking distances. (c) The utility performance under different equilibriums.

While for the NE situation, all the variables are optimized independently, so the data sensing rate λ, transmission power P, and the attacking power J are not optimized in the leading-follower order. Unavailable real-time update can decrease the utility performance. Hence, given the hierarchical adversarial conditions in Eq. (9), the utility performance under SE is better than the one under NE.

VI. Conclusion

From the Stackelberg game viewpoint, this paper investigates the AoI optimization problem in the UAV-aided traffic monitoring network under attack. Compared with the existing related works, we consider the security issue to curve an adversarial relationship between the legitimate UAVs and the attacker for AoI-related parameters optimization. At first, the system model and the optimization goal are formulated with the Stackelberg game perspective. Then, to reach the SE status of the formulated Stackelberg game, we use the Lagrange duality optimization technology to derive the optimal solution, where the legitimate UAVs' data sensing rate, transmission power and the attacker's power are determined by the sub-gradient update-based optimization approach. Finally, under different parameters settings, simulations are performed to evaluate the performances of the proposed approach.

References

[1] S. Kaul, R. Yates, and M. Gruteser, "Real-time status: How often should one update?" in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 2731–2735.

[2] B. Liu, Z. Su, and Q. Xu, "Game theoretical secure wireless communication for UAV-assisted vehicular Internet of Things," *China Commun.*, vol. 18, no. 7, pp. 147–157, Jul. 2021.

[3] S. Kouroshnezhad, A. Peiravi, M. S. Haghighi, and A. Jolfaei, "Energy-efficient drone trajectory planning for the localization of 6G-enabled IoT devices," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5202–5210, Apr. 2021.

[4] X. Qin, Y. Xia, H. Li, Z. Feng, and P. Zhang, "Distributed data collection in age-aware vehicular participatory sensing networks," *IEEE Internet Things J.*, vol. 8, no. 19, pp. 14501–14513, Oct. 2021.

[5] B. Choudhury, V. K. Shah, A. Dayal, and J. H. Reed, "Joint age of information and self risk assessment for safer 802.11p based V2V networks," in *Proc. IEEE INFOCOM*, Vancouver, BC, Canada, May 2021, pp. 1–10.

[6] D. Ploger, M. Segata, R. L. Cigno, and A. Timm-Giel, "Markov-modulated models to estimate the age of information in cooperative driving," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Los Angeles, CA, USA, Dec. 2019, pp. 1–4.

[7] G. Xu, Q. Liu, and H. Zhang, "Multi-machine joint attack and defense game based on Pareto optimality," in *Proc. Chin. Control Decis. Conf. (CCDC)*, Nanchang, China, Jun. 2019, pp. 842–847.

[8] S. Ahmadian, H. Malki, and Z. Han, "Cyber attacks on smart energy grids using generative adverserial networks," in *Proc. IEEE Global Conf. Signal Inf. Process. (GlobalSIP)*, Anaheim, CA, USA, Nov. 2018, pp. 942–946.

[9] M. Amadeo, "A literature review on caching transient contents in vehicular named data networking," *Telecom*, vol. 2, no. 1, pp. 75–92, Feb. 2021.

[10] S. Feng and S. Haykin, "Anti-jamming V2V communication in an integrated UAV-CAV network with hybrid attackers," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Shanghai, China, May 2019, pp. 1–6.

[11] Z. Feng *et al.*, "Power control in relay-assisted anti-jamming systems: A Bayesian three-layer Stackelberg game approach," *IEEE Access*, vol. 7, pp. 14623–14636, 2019.

[12] Y. Xu *et al.*, "A one-leader multi-follower Bayesian-Stackelberg game for anti-jamming transmission in UAV communication networks," *IEEE Access*, vol. 6, pp. 21697–21709, 2018.

[13] J. B. Rosen, "Existence and uniqueness of equilibrium points for concave N-person games," *Econometrica*, vol. 33, no. 3, pp. 520–534, Jul. 1965.

[14] Y. Wang, S. Wu, J. Jiao, W. Wu, Y. Wang, and Q. Zhang, "Age-optimal transmission policy with HARQ for freshness-critical vehicular status updates in space-air-ground integrated networks," *IEEE Internet Things J.*, early access, Dec. 28, 2020, doi: 10.1109/JIOT.2020.3047665.

[15] X. Wang and R. A. Berry, "MAC trade-offs between age and reachability of information in vehicular safety applications," in *Proc. IEEE INFOCOM*, Toronto, ON, Canada, Jul. 2020, pp. 689–695.

[16] S. Zhang, J. Li, H. Luo, J. Gao, L. Zhao, and X. S. Shen, "Low-latency and fresh content provision in information-centric vehicular networks," *IEEE Trans. Mobile Comput.*, early access, Sep. 18, 2020, doi: 10.1109/TMC.2020.3025201.

[17] L. Baldesi, L. Maccari, and R. Lo Cigno, "Keep it fresh: Reducing the age of information in V2X networks," in *Proc. 1st ACM MobiHoc Workshop Technol., Models, Protocols Cooper. Connected Cars*, 2019, pp. 7–12.

[18] A. Alabbasi and V. Aggarwal, "Joint information freshness and completion time optimization for vehicular networks," *IEEE Trans. Services Comput.*, early access, Mar. 3, 2020, doi: 10.1109/TSC.2020.2978063.

[19] S. Yang and X. Wei, "Research on optimization model of network attack-defense game," in *Proc. 8th IEEE Int. Conf. Softw. Eng. Service Sci. (ICSESS)*, Beijing, China, Nov. 2017, pp. 426–429.

[20] E. Eisenstadt and A. Moshaiov, "Novel solution approach for multi-objective attack-defense cyber games with unknown utilities of the opponent," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 1, no. 1, pp. 16–26, Feb. 2017.

[21] O. Rudenko, Y. Liu, C. Wang, and S. Rahardja, "An extensive game-based resource allocation for securing D2D underlay communications," *IEEE Access*, vol. 7, pp. 43052–43062, 2019.

[22] J. Liu *et al.*, "Intelligent jamming defense using DNN Stackelberg game in sensor edge cloud," *IEEE Internet Things J.*, vol. 9, no. 6, pp. 4356–4370, Mar. 2022.

[23] K. Wang, L. Yuan, T. Miyazaki, D. Zeng, S. Guo, and Y. Sun, "Strategic antieavesdropping game for physical layer security in wireless cooperative networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 9448–9457, Oct. 2017.