Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.053587

ARTICLE

Physical Layer Security of 6G Vehicular Networks with UAV Systems: First Order Secrecy Metrics, Optimization, and Bounds

Sagar Kavaiya[1], Hiren Mewada[2,*], Sagarkumar Patel[3], Dharmendra Chauhan[3], Faris A. Almalki[4] and Hana Mohammed Mujlid[4]

[1]Smt. Chandaben Mohanbhai Patel Institute of Computer Applications, Charotar University of Science and Technology, Changa, Anand, 388421, India

[2]Electrical Engineering Department, Prince Mohammad Bin Fahad University, P.O. Box 1664, Al Khobar, 31952, Kingdom of Saudi Arabia

[3]Department of Electronics and Communication Engineering, Chandubhai S. Patel Institute of Technology, Charotar University of Science and Technology, Changa, Anand, 388421, India

[4]Department of Computer Engineering, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif, 21944, Kingdom of Saudi Arabia

*Corresponding Author: Hiren Mewada. Email: hmewada@pmu.edu.sa

Received: 05 May 2024 Accepted: 29 July 2024 Published: 12 September 2024

ABSTRACT

The mobility and connective capabilities of unmanned aerial vehicles (UAVs) are becoming more and more important in defense, commercial, and research domains. However, their open communication makes UAVs susceptible to undesirable passive attacks such as eavesdropping or jamming. Recently, the inefficiency of traditional cryptography-based techniques has led to the addition of Physical Layer Security (PLS). This study focuses on the advanced PLS method for passive eavesdropping in UAV-aided vehicular environments, proposing a solution to complement the conventional cryptography approach. Initially, we present a performance analysis of first-order secrecy metrics in 6G-enabled UAV systems, namely hybrid outage probability (HOP) and secrecy outage probability (SOP) over 2×2 Nakagami-m channels. Later, we propose a novel technique for mitigating passive eavesdropping, which considers first-order secrecy metrics as an optimization problem and determines their lower and upper bounds. Finally, we conduct an analysis of bounded HOP and SOP using the interactive Nakagami-m channel, considering the multiple-input-multiple-output configuration of the UAV system. The findings indicate that 2×2 Nakagami-m is a suitable fading model under constant velocity for trustworthy receivers and eavesdroppers. The results indicate that UAV mobility has some influence on an eavesdropper's intrusion during line-of-sight-enabled communication and can play an important role in improving security against passive eavesdroppers.

KEYWORDS

Physical layer security; 3D positioning; 6G communications; UAV systems

1 Introduction

1.1 Background

A continuous 1000× increase in network capacity has driven the evolution of wireless networks to date. Despite this growing demand for wireless capacity, the Internet of Everything (IoE) system requires ultra-reliable, low-latency communications. To meet the demands of this new breed of services, we must address unusual challenges, such as characterizing the fundamental rate-reliability-latency tradeoffs that govern their performance, unlocking frequencies beyond sub-6 GHz, and transforming wireless systems into intelligent, self-sustaining networks. The forthcoming sixth-generation (6G) wireless system, with an architecture naturally adapted to the needs of IoE applications and related technological advancements, can potentially address these issues [1]. In recent years, there has been a focus on research on UAVs, also called drones, due to their numerous application fields, autonomy, and adaptability. A wide range of industries, including the military, telecommunications, medical supply delivery, surveillance, monitoring, and rescue missions, have utilized UAVs. When deployed and operated appropriately, UAVs can address various real-world problems [2]. Unauthorized receivers have the potential to intercept information signals sent across wireless Line of Sight (LoS) channels, increasing the risk of information leakage. Wireless UAV transceivers, however, are susceptible to malevolent jamming attempts. For this reason, security in UAV wireless communications is crucial. Regretfully, conventional encryption methods are energy-intensive and require a high level of computer complexity. Physical layer security (PLS) effectively and efficiently protects wireless communication networks by taking advantage of the inherent unpredictability of wireless channels [3]. Table 1 summarises the abbreviations used in the paper and their meanings.

Table 1: Summary of the abbreviations

Sr. No.	Abbreviation	Meaning
1	6G	Sixth-Generation
2	A2G	Air-to-Ground
3	B5G	Beyong 5G Networks
4	DSM	Diffrential Spatial Modulation
5	FL	Federated Learning
6	IoT	Internet of Things
7	NN	Neural Network
8	PLS	Physical Layer Security
9	SM	Spatial Modulation
10	UAVs	Unmanned Aerial Vehicles
11	SNR	Signal-to-Noise Ratio
12	HOP	Hybrid Outage Probability
13	SOP	Secrecy Outage Probability
14	CDF	Cumulative Distribution Function
15	MIMO	Multiple-Input-Multiple-Output
16	PDF	Probability Distribution Function
17	OP	Outage Probability
18	BER	Bit Error Rate
19	ECC	Elliptic Curve Cryptography

(Continued)

Table 1 (continued)

Sr. No.	Abbreviation	Meaning
20	CNN	Convolutional Neural Network
21	AI	Artificial Intelligence
22	SHA	Secure Hash Algorithm
23	LoS	Line of Sight
24	NLoS	Non Line of Sight
25	MATLAB	Matrix Laboratory
26	CVX	Convex Optimization
27	RAM	Random Access Memory
28	CPU	Central Processing Unit

1.2 Related Works

Smart cities utilize advanced technologies like drones, robotics, artificial intelligence (AI), and IoT to enhance life quality, reduce waste, and act as sustainable resource ecosystems. These technologies enhance service quality, energy efficiency, and connection, supporting applications in the fields of healthcare, e-waste reduction, transportation, agriculture, defense, disaster prevention, environmental protection, service delivery, energy conservation, and communication. To improve smart city applications, the reference [4] examined possible methods and uses of collaborative drones and IoT, with an emphasis on data collection, security, privacy, safety for people, disaster prevention, consumption of energy, and quality of life.

Furthermore, Edge Intelligence employs AI to support B5G requirements, with drones serving as relay stations for data collection. Federated learning (FL) improves global model accuracy in smart environments. However, its use is limited by security and decentralization management challenges. Blockchain offers privacy-preserving data sharing but still faces challenges like scalability and energy efficiency. This survey explores the synergy of FL and blockchain for green, sustainable environments, discussing challenges, opportunities, and future trends [5]. Using an AI framework, the reference [6] created a smart cellular architecture for UAV wireless communication. The framework includes self-organizing maps and an NN fitting tool. Validated in a proof-of-concept scenario, it demonstrates high levels of adaptive wireless communication forecasting and achieves efficient and optimized automatic design without human intervention. The reference [7] investigated blockchain technology, which can support smart farming with the goals of increasing productivity, lessening environmental effects, and automating farmer tasks. It suggests a safe blockchain-based system for secure communication between drones and sensors that makes use of the Secure Hash Algorithm (SHA)-256 hash function encryption and the ECC authentication algorithm. A proof-of-concept deployment on the Ethereum blockchain demonstrated the framework's viability and its potential to address data availability and integrity challenges in smart farming.

The reference [8] presented a national research project that aims to use a digital elevation model and a 3D structure change detection model to enable the autonomous operation of UAVs. The UAVs receive training from a Convolutional Neural Network (CNN) for autonomous flight and terrain identification. The UAVs can detect water flows with 99.6% accuracy in areas with limited satellite images. The study also looks at how channel correlation affects spatial modulation (SM)

and differential spatial modulation (DSM) [9], keeping baseband technologies in mind. It emphasizes how crucial channel correlation is to greater spectral efficiency in DSM and SM. In Rayleigh fading channels, the analysis takes into account three send and two receive antennas. The results demonstrate that DSM-BER improves with higher modulation schemes, with the receiving antenna side more affected by spatial correlation or antenna spacing.

In reference [10], researchers examined opportunities for enhanced physical layer security in UAV communication, taking into account PLS technology. A PLS-based UAV communication solution for 5G and beyond networks has been investigated in [11], illustrating the static and mobile deployment of UAVs. In reference [11], researchers proposed a PLS-based study of UAV-powered communication networks. They presented an evaluation of various ground-to-air channel links in a UAV-based communication network, providing a basic concept of the ground-to-air channel. The references [12,13] focused on UAV-aided vehicular communications, deriving insights into architecture, intelligence, and research challenges.

Over the past few years, UAV applications in military, civil, and commercial areas have also made significant progress. However, challenges in high-speed communication links, flexibility in control strategies, and collaborative decision-making algorithms swirl around autonomy, robustness, and reliability. The resulting enhanced Swarm focus on more collaborative communication allows groups of swarming UAVs to self-organize and collaborate, which leads to higher fault tolerance and efficiency [14,15]. Additionally, in [16] a K-means online learning routing protocol (KMORP) was presented for UAV ad hoc networks. This protocol gets around the problems that traditional routing algorithms have with fixed nodes and predetermined network topologies. The KMORP includes a 3D Gauss Markov mobility model for accurately predicting where a UAV is, as well as a K-means online learning method for dynamic clustering and load balancing. It can swiftly adapt to network fluctuations, simultaneously broadcasting fewer messages and sending or receiving more packets, thereby enhancing network performance through packet resending. However, this rapid expansion of consumer UAVs also creates new business opportunities for cellular operators. When integrated into the cellular network as user equipment (UE), UEs like UAVs can generate significant revenue and enhance coverage, spectral efficiency, network quality, and user experience. Although standardization bodies are still exploring ways to service commercial UAVs with cellular networks [17], industries have already begun pilot trials of such prototype models.

Reference [18] examined the current state of UAV-PLS and its implementation in both military and civil applications. A new air-to-ground channel and aerial distributions of the node model are part of this. So are UAV roles in PLS and performing secrecy system secrecy, as well as improving static deployment-based UAV systems through secrecy analysis. It also discusses the methodologies employed in the field of UAV-PLS, as well as the relevant literature, research directions, and challenges. Furthermore, this letter examines the use of relay nodes for secure communications in wireless communication and investigates transmit optimization in a four-node channel model. The authors solved the nonconvex secrecy rate maximization problem by introducing the difference-of-concave program and proposing an iterative algorithm. It is a computationally efficient algorithm with a closed-form solution that improves secrecy via relay, which outperforms static relaying.

1.3 Motivations, Novelties and Contributions

From the common limitations presented in the literature, it has been noticed that future 6G services will significantly focus on surveillance, monitoring, and even UAVs as base stations for various multimedia and infotainment applications. However, due to the broadcast nature of wireless links, the

transmission path remains vulnerable to malicious attacks. Furthermore, it is crucial to implement an analytical framework for the 6G channel model, as it enhances the impact of mobility. Therefore, this work presents a novel analytical framework for 6G UAV-aided vehicular communications to restrict passive attacks done by malicious users. We consider the static deployment of the UAVs in the air, which is similar to the deployment of roadside units for vehicular communications. Specifically, we aim to evaluate and secure the vehicle-to-infrastructure link. With the given air-to-ground (A2G) link under the coverage area, we obtained closed-form formulas for the SNR received while accounting for mobility. The derived expressions are helpful in computing the hybrid outage probability (HOP) and secrecy outage probability (SOP). The expressions also provide information on the vehicle's maximum transmission power and the impact of its distance from UAVs.

1.4 Objectives of This Research

- **Analyze the Performance of First-Order Secrecy Metrics:** Preliminarily, we analyzed the HOP and SOP over 6G-assisted UAV systems and studied the effect of air-to-ground channel properties for both LoS and NLoS (Non-Line of Sight) communication scenarios.
- **Introduce an Optimization Technique for Eavesdropping Mitigation:** We propose a new approach to tackle passive eavesdropping in UAV-assisted vehicular environments and calculate the first-order secrecy metrics and lower and upper bounds to improve security.
- **Analyze the Role of Mobility in Security:** We present a Closed-Form Expression of HOP and SOP in the Nakagami-*m* Channel, analyzing the role of mobility in security with a single legitimate receiver and an eavesdropper with MIMO Nakagami-*m* channel. Later, we investigated the impact of UAV mobility on an eavesdropper's ability to intercept legitimate communications on LoS links.

2 System Model

2.1 Network Structure

The network structure describes a scenario where a UAV serves as a communication node for a legitimate broadcaster and receiver. Fig. 1 illustrates the scenario in which a UAV functions as a communication node for vehicles. Usually, the automobile (R) starts the trip from point A to point C as a valid receiver. When the passive eavesdropper (E) is present in the network, P keeps R connected without interruption.

2.2 Channel Model

The dynamic fading condition is assumed. To determine the practical applicability, the wiretap channel model for the eavesdropping scenario has been taken into consideration [19]. The dynamic 2 $\times$ 2 Nakagami-*m* channel between the authorized transmitter, authorized receiver, and eavesdropper is taken into account to represent the fading.

The channel status data is thought to be accurate. According to the joint eigenvalues of 2 $\times$ 2 Nakagami-*m*, reference [20] provided the distribution of received SNR in Eq. (23).

$$p(L) = \frac{K_{22}8\pi^{5/2}}{2^{2m-1}} \times \frac{m\mathrm{tr}(LL')}{\Omega} \times l_{11}^{4m-1} \sum_{i_1=0}^{m-1} \sum_{k_1=0}^{i_1} \sum_{i_2=0}^{m-1} \sum_{k_2=0}^{i_2} \binom{m-1}{i_1} \binom{i_1}{k_1} \binom{m-1}{i_2} \binom{i_2}{k_2} \times s_1 \times s_2 \tag{1}$$

where, the terms

$$s_1 = (-1)^{m-1-i_2}(l_{21I}^2 + l_{21R}^2)^{k_1+k_2+\frac{1}{2(2m-i_1-i_2-2)}} \cdot l_{22}^{i_2-2k_2+i_1-2k_1+2m-1}\Gamma(1/2(2-i_1)) \tag{2}$$

$$s_2 = \frac{2^{4m-4-i_1-i_2}\Gamma(1/2(4m+2k_1+i_2-2k_2-2-i_1))}{\Gamma(4(m-1))} \cdot \frac{\Gamma(1/2(i_1-2k_1+2k_2+4m))}{\Gamma(1/2(2m-i_1-i_2))} \tag{3}$$

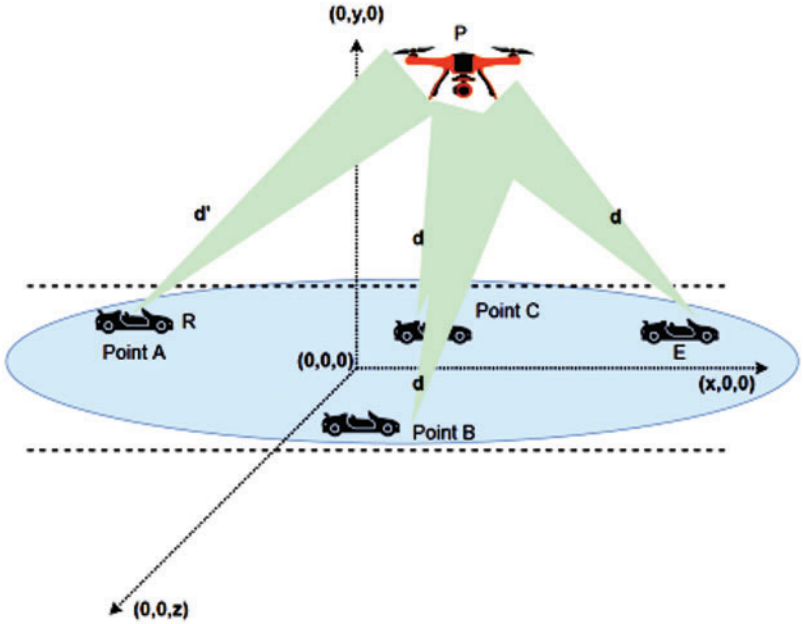

Figure 1: Network model with UAVs and passive mobile eavesdropper

m is the fading parameter. $\Gamma(\cdot)$ is the Gamma function. It can be observed that P(L) dropped to a uniform distribution throughout the Ω-radius circle at $m = 1$. This is represented by the $K_{ij} = (m^m \pi \Omega^m \Gamma(m))^{ij}$. Additionally, it is possible to think of $f(i_1, i_2, k_1, k_2)$ as Eq. (14) of [20], where l represents the multi-path component connecting the transmitter and reception antenna, and L denotes the number of branches. The term $s_1 = (-1)^{m-1-i_2}(l_{21I}^2 + l_{21R}^2)^{k_1+k_2+\frac{1}{2(2m-i_1-i_2-2)}} \cdot l_{22}^{i_2-2k_2+i_1-2k_1+2m-1}$, $s_2 = \frac{2^{4m-4-i_1-i_2}\Gamma(1/2(4m+2k_1+i_2-2k_2-2-i_1))}{\Gamma(4(m-1))} \cdot \frac{\Gamma(1/2(i_1-2k_1+2k_2+4m))}{\Gamma(1/2(2m-i_1-i_2))}$ within the larger context of CDF for Nakagami-m fading channels captures a specific part of the integrand that contributes to the overall calculation of the secrecy outage probability. It includes several components that reflect different aspects of the wireless channel's behavior under Nakagami-m fading conditions. The term starts with an alternating sign factor $(-1)^{m-1-i_2}$ which introduces a positive or negative sign based on the values of (m) and (i_2). This is followed by a power term $(l_{21I}^2 + l_{21R}^2)^{k_1+k_2+\frac{1}{2(2m-i_1-i_2-2)}}$ which involves $(l_{\{21\}})$ a parameter related to the channel fading or path loss.

2.3 Signal Model

The mathematical structure of the signals received on both the legitimate receiver side and the eavesdropper side is represented by the signal model. The ideal transmit antenna index is ascertained as:

$$p^* = \left\{ \sum_{l_R=1}^{L_R} \left| h_{p,(l_R)} \right|^2 \right\} \tag{4}$$

where, an average power limitation is applied to the codeword, i.e., $\frac{1}{L}\sum_{l=1}^{L}\mathbb{E}[|x(l)|^2]$. The number of branches at the valid receiver side is l_R. The channel gain is h_p. The secret message block W is encoded into a codeword $\mathbf{x} = (x(1), \cdots, x(l), \cdots, x(L))$, where L denotes $\mathbf{x}$'s length, in order to achieve secure transmission. The received signal vector in the main channel at time slot l is provided by:

$$y_R(l) = h(l) * x(l) + \boldsymbol{n}_R(l) \tag{5}$$

where, $\boldsymbol{h} = [h_{p^*,1}, h_{p^*,2}, \cdots, h_{p^*,N_R{}^T \in C^{N_R \times 1}}]$ represents channel vector between the antenna of transmitter and receiver. $*$ denotes the convolutional operator. By integrating the subset of receive antennas at legitimate receivers with the highest SNRs provides instantaneous SNR in the main channel as expressed in Eq. (6).

$$\gamma_R = \sum_{l_R=1}^{L_R} \gamma_{(l_R)}^{R} \tag{6}$$

The signal received at the authorized receiver side is implied by the above equation. Additionally, the received signal vector in the eavesdropper's channel during time slot $\boldsymbol{l}$ is provided by:

$$y_E(l) = h * x(l) + n_E(l) \tag{7}$$

The following is an additional expression of the $\boldsymbol{h}$ as a function of the distance between the authorized transmitter and the eavesdropper [21]:

$$h_{(t)} = \frac{g_x}{\sqrt{1 + d_X^{\alpha}(t)}}, \tag{8}$$

where, g_x is the channel gain over MIMO Nakagami-m distribution and α is the route loss exponent. The distribution of distance is d_X.

3 Examination of First-Order Secrecy Measures for the 6G-UAVs System

This section focuses on the performance analysis of a hypothetical UAV vehicular network. In contrast with [13–16], the current work considers the updated, generic but tractable vehicular scenario in terms of the vehicle mobility and path loss exponent. The earlier work [13] did not demonstrate the effect of path loss on the effectiveness of secrecy metrics. However, in the UAV-enable scenario, the proposed work focuses on the multiple positions of the legitimate receiver, starting from point A to point C (Fig. 1). The car, which has two antennas, starts its journey from point A to point C. The legitimate transmitter also has a dual antenna, thus resulting in a MIMO scenario. In the presence of small-scale fading and vehicle mobility, it is advantageous to consider the dynamic fading channels for better modeling of the performance metrics. Therefore, this work involves the 2×2 Nakagami-m fading channel.

The proposed workflow is shown in Fig. 2, in addition, the paper is structured as follows: Section 3.1 first generates the analytical closed-form expression for the received SNR. Subsequently, Section 3.2 carries out the analysis of SOP, while Section 3.3 proceeds with the HOP analysis. Section 4 focuses on knowing outage probability (OP) and SOP limits, while Section 5 focuses on the optimization method of restricting eavesdropping, followed by numerical results in Section 6.

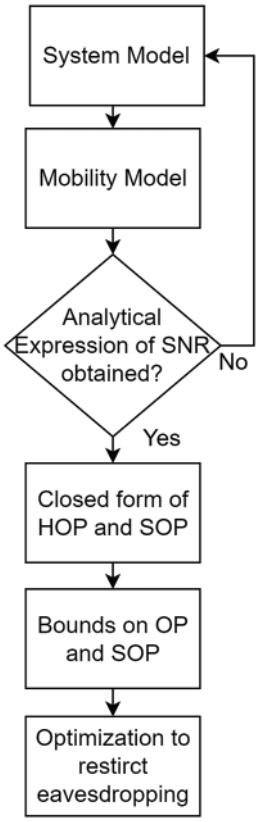

Figure 2: Flowchart of workflow

3.1 Analytical Closed-Form of Received SNR for 6G UAVs MIMO System

Vehicle mobility's PDF is given by [22]:

$$f_Y(y) = \frac{d}{4ab}\left[\pi + 2\,arcsin\left(\frac{2(y^2 - (d'')^2)}{y^2}\right) - 1\right], \tag{9}$$

where, the parameters of the road structure are a and b. The joint cumulative distribution function (CDF) which encounters the impact of vehicle mobility for the received SNR can be calculated as follows:

$$F_Z(z) = \int_0^{\infty} \int_{-\infty}^{yz} f_{XY}(x, y)dxdy. \tag{10}$$

For above, Eq. (10) has been re-denoted as $f_X(x)$. Additionally, the CDF can be expressed as:

$$F_Z(z) = \int_0^{\infty} \int_{-\infty}^{yz} \frac{d}{4ab} \left[\pi + 2\, arcsin\left(\frac{2(y^2 - (d'')^2)}{y^2} \right) \right] \frac{K_{22} 8\pi^{5/2}}{2^{2m-1}}$$

$$\times \frac{mtr\,(xx')}{\Omega} l_{11}^{4m-1} \sum_{i_1=0}^{m-1} \sum_{k_1=0}^{i_1} \sum_{i_2=0}^{m-1} \sum_{k_2=0}^{i_2} \binom{m-1}{i_1} \binom{i_1}{k_1} \binom{m-1}{i_2} \binom{i_2}{k_2}$$

$$\times (-1)^{m-1-i_2} (l_{21I}^2 + l_{21R}^2)^{k_1+k_2+} \frac{1}{2\,(2m - i_1 - i_2 - 2)} l_{22}^{i_2-2k_2+i_1-2k_1+2m-1} \Gamma(1/2(2m - i_1))$$

$$\times B_j \sum_{n=1}^{T_j} \lambda_j^n k x^k \frac{e^{\frac{hq\gamma}{cd}} \left(\frac{1}{cd} \right)}{d^2} \frac{2^{4k-4-i_1-i_2} \Gamma\left(\frac{1}{2\,(4k + 2j_1 + i_2 - 2j_2 - 2 - i_1)} \right)}{\Gamma\,(4\,(k-1))}$$

$$\times \frac{\Gamma(1/2(i_1 - 2j_1 + 2j_2 + 4k))}{\Gamma(1/2(2k - i_1 - i_2))} dxdy \tag{11}$$

The given Eq. (11) represents the CDF $\left(F_{Z(z)}\right)$ for a random variable (Z) in the context of Nakagami-m fading channels, a common model in wireless communications. This equation involves a double integral over variables (x) and (y), with integration limits from 0 to ∞ and ∞ to (yz), respectively. The integrand contains multiple components, starting with a term involving the arcsine function, which is influenced by the fading channel's parameters. It includes a constant $\left(\frac{K_{22} 8\pi^{5/2}}{2^{2m-1}} \right)$ and a combination of several exponential and Gamma functions, which account for the statistical distribution of the channel's fading coefficients. Within the integrand, a set of nested summations involves binomial coefficients and powers of channel parameters $(-1)^{m-1-i_2}(l_{21I}^2 + l_{21R}^2)^{k_1+k_2+1/2(2m-i_1-i_2-2)}$. These summations capture the combinatorial aspects of the fading environment, considering the contributions from multiple paths and their interactions. The term $\Gamma(1/2(2m-i_1))$ denotes the Gamma function, which generalizes factorials and is crucial in probability distributions.

$$f_X(x) = A_j \times B_j \sum_{n=1}^{T_j} \lambda_j^n k x^k \frac{e^{\frac{hq\gamma}{cd}} \left(\frac{1}{cd} \right)}{d^2} + \frac{2^{4k-4-i_1-i_2} \Gamma\left(\frac{1}{2\,(4k + 2j_1 + i_2 - 2j_2 - 2 - i_1)} \right)}{\Gamma\,(4\,(k-1))}$$

$$\times \frac{\Gamma\,(1/2\,(i_1 - 2j_1 + 2j_2 + 4k))}{\Gamma\,(1/2\,(2k - i_1 - i_2))} \tag{12}$$

where, $A_J = \left(\frac{L}{\Gamma(m)} \right)$, $B_J = \left(\frac{\Gamma(m+d+r)L}{\Gamma(m)} \right)$, m is the Nakagami-m parameter, $T_k = m_k\, L$ and $\lambda_k = e^{T_k}$.

3.2 Analysis of the Probability of Secrecy Outage

This section looks at the likelihood of a secrecy outage on the legitimate receiver side. However, since the legitimate transmitter lacks the channel state information for the eavesdropper's channel,

it is forced to encode data at a constant code rate R_s. Reference [21] provided instantaneous secrecy capability as:

$$C_t(\alpha_R, \alpha_E) = max\left\{ln(1+\alpha_R) - ln(1+\alpha_E), 0\right\}. \tag{13}$$

The eavesdropper and legitimate receiver have received SNRs of α_E and α_R, respectively. The another definition of the SOP:

$$Pr\left\{C_t(\alpha_R, \alpha_E) \leq R_t\right\}. \tag{14}$$

The transmitter power at S in the hybrid network of the 6G-UAVs system can be expressed as shown in [22–24].

$$P_s = min\left(P_{max}, \frac{I_p}{X}\right), \tag{15}$$

Given a maximum broadcast power of P_{max}, an interference power of I_P, and a channel gain of X between the transmitter S and the receiver P. Moreover, this channel is considered optimal since it makes it possible to determine the average outage. Lastly, the SOP can be presented with (15) as follows:

$$P_{sop} = \underbrace{Pr\left\{C_t(\alpha_R, \alpha_E) \leq R_t, P_t = P_{max}\right\}}_{I_1} + \underbrace{Pr\left\{C_t(\alpha_R, \alpha_E) \leq R_t, P_t = \frac{I_p}{X}\right\}}_{I_2}, \tag{16}$$

3.2.1 First Integral Term Derivation

The outer part of the I_{11} is given as per reference [18]:

$$Pr(x \leq \frac{I_P}{P_{max}}) = 1/\Gamma(m) \times t_1 \times t_2 \tag{17}$$

The I_{11} is further expanded as under:

$$I_{11} = \sum_{i_1=0}^{k-1} \sum_{j_1=0}^{i_1} \sum_{i_2=0}^{k-1} \sum_{j_2=0}^{i_2} \binom{k-1}{i_1} \binom{i_1}{j_1} \binom{k-1}{i_2} \binom{i_2}{j_2} \times A_j \times B_j \sum_{n=1}^{\tau_j} \lambda_j^n j x^j \frac{e^{hq\alpha/cd}(1/cd)}{d^2} \tag{18}$$

The SOP is defined as follows after additional solution with the help of [11, Section IV]:

$$P_{SOP} = \frac{y^{2LnB_j}}{Ln} \times F_1(p, q; r; s) \times \frac{1}{\Gamma(n)} \left(\frac{n}{\Omega}\right)^{Ln} \times \frac{A_j}{L}^n \times \frac{\Gamma(1/2(i_1 - 2j_1 + 2j_2 + 4n))}{\Gamma(1/2(2n - i_1 - i_2))} \tag{19}$$

The function $\Gamma(\cdot)$ refers to the Gamma function. The function F_1 is a monotonically declining generalized Gaussian hypergeometric function with four components, as described in Section IV of the reference [11]. The variable p is defined as $p = \frac{z}{2abLm}$. The expression q is equal to $\frac{1 - det(\Lambda)}{4d}$, where $det(\Lambda)$ represents the determinant of Λ and d is a constant. The value of r is equal to $\frac{2z}{2d^2 + 1}$. The expression for s is given by $\frac{1 - det(\Lambda)}{Lm}$, where $det(\Lambda)$ represents the determinant of Λ and Lm

represents a constant. The symbol m represents the Nakagami-m parameter, while Λ represents the antenna correlation parameter.

3.3 Derivations of Hybrid Outage Probability

This section computes the likelihood of a power failure based on the starting locations of a sanctioned transmitter node. An outage is a likelihood that the received instantaneous SNR, denoted as x, is lower than a specified threshold x_{th}. The formula used to calculate the chance of an outage is as follows:

$$P_{out} = Pr(0 \leq x \leq x_{th}), \tag{20}$$

$$P_{out} = \int_0^{x_{th}} f_X(x)dx \tag{21}$$

The fading envelope caused by the mobility is equal to the resultant channel gain, as demonstrated in (8). Additionally, Jake's correlation function is not a random variable with a specific coding rate. The system's ability to tolerate more information than a particular rate R_s is determined by the outage probability. Therefore, using (21), the following is the outage probability:

$$P_{out} = \int_0^{x_{\text{th}}} \frac{K_{22}8\pi^{5/2}}{2^{2m-1}} \times \frac{m\text{tr}\,(xx')}{\Omega} l_{11}^{4m-1} \sum_{i_1=0}^{m-1} \sum_{k_1=0}^{i_1} \sum_{i_2=0}^{m-1}$$
$$\sum_{k_2=0}^{i_2} \binom{m-1}{i_1} \binom{i_1}{k_1} \binom{m-1}{i_2} \binom{i_2}{k_2} A_j \times B_j \sum_{n=1}^{T_j} \lambda_j^n k x^k \frac{e^{hq\gamma/cd}\,(1/cd)}{d^2}$$
$$+ \frac{2^{4k-4-i_1-i_2}\Gamma(1/2(4k+2j_1+i_2-2j_2-2-i_1))}{\Gamma(4(k-1))} \times \frac{\Gamma(1/2(i_1-2j_1+2j_2+4k))}{\Gamma(1/2(2k-i_1-i_2))} dx \tag{22}$$

Using [11, Section IV] to solve the preceding expression, the outage probability is as follows:

$$P_{out} = \frac{Lr^{\pi\frac{\mu_x+\mu_y}{2}} \sum_{k=0}^{\infty} \frac{k!\, m_k L_k^{\frac{\mu_x+\mu_y}{2}} \left(\left(\frac{2}{\mu_x+\mu_y}+1\right)2r^{\alpha}\right)}{\left(\frac{\mu_x+\mu_y}{2}+1\right)_k}}{2^{\frac{\mu_x+\mu_y}{2}+1}\Gamma\left(\frac{\mu_x+\mu_y}{2}+1\right)\exp\left(\frac{r^{\pi}}{2}\right)}$$

$$A_j \times B_j \sum_{n=1}^{T_j} \lambda_j^n k x^k \frac{e^{hq\gamma/cd}\,(1/cd)}{d^2} + \frac{2^{4k-4-i_1-i_2}\Gamma\left(1/2\left(4k+2j_1+i_2-2j_2-2-i_1\right)\right)}{\Gamma\left(4\left(k-1\right)\right)}$$
$$\times \frac{\Gamma(1/2(i_1-2j_1+2j_2+4k))}{\Gamma(1/2(2k-i_1-i_2))} \tag{23}$$

It is evident from (23) that wireless fading parameters and mobility parameters determine the OP. It implies how the speed of the authorized receiver may affect the likelihood of being overheard.

4 The Importance of Knowing the Limits of Secrecy Metrics

In this section, we derive the upper and lower bounds of PLS metrics. These metrics are crucial for gauging the potential for eavesdropping. In essence, they assist us in assessing the security of our communication and detecting any unauthorized access.

4.1 Outage Probability

The outage probability measures the likelihood of a communication security breakdown. We require a secrecy capacity that is higher than the target secrecy rate. This capacity is the difference between the legitimate communication link's capacity and the eavesdropper's link. This stops the transfer of information between the eavesdropper's channel and the main channel. We express this mathematically as follows:

$$P_{out} = 0|R_s \tag{24}$$

Although this expression is well articulated, it is important to consider the impact of noisy fading channels on the range of secrecy rates (R_s). In such scenarios, the outage probability (P_{out}) can reach its maximum or minimum values. The lower bound for a given scenario, like vehicular communication, depends on the fading characteristics. We can formulate the lower bound condition using maximum likelihood as follows:

$$P_{out} = min_{L\subseteq\{1,2,\cdots,L_t\}} \frac{L_t}{|L|} logdet(\boldsymbol{I}_{L_R} + \boldsymbol{H}_L \boldsymbol{H}_L^H) \tag{25}$$

To handle this expression more effectively, we convert it into an inequality, as shown in [25], to explore its integral variations for convex optimization.

$$min\Bigg(\Bigg[\frac{d}{ds} \frac{z^{2LmB_k}}{Lm} F_1(p,q;r;s) \frac{1}{\Gamma(m)} \left(\frac{m}{\Omega}\right)^{Lm} \frac{A_k}{L}^m \frac{\Gamma\left(\frac{1}{2(i_1 - 2k_1 + 2k_2 + 4m)}\right)^{+(t+1)}}{\Gamma\left(\frac{1}{2(2m - i_1 - i_2)}\right)} - \frac{d}{ds} P_{sop}^{+}(t) \Bigg)$$
$$- \Bigg(\frac{d}{ds} \frac{z^{2LmB_k}}{Lm} \times F_1(p,q;r;s) \times \frac{1}{\Gamma(m)} \left(\frac{m}{\Omega}\right)^{Lm}$$
$$\times \frac{A_k}{L}^m \times \frac{\Gamma(1/2(i_1 - 2k_1 + 2k_2 + 4m))^{-(t+1)}}{\Gamma(1/2(2m - i_1 - i_2))} - \frac{d}{ds} P_{sop}^{-}(t) \Bigg) \Bigg) \tag{26}$$

4.1.1 Lower Bound of Outage for 6G UAV System

Denote P_{LB} as the series terms of Eq. (21) using techniques from [25]. Ensuring the absence of any roots is essential to achieve the lower bound of P_{LB}. When we apply the integral bound technique, we obtained $P_{\text{LB}} = \ln(m+1) \leq P_{\text{out}} \leq 1 + \ln(m)$.

In the system, m represents a fading parameter. If the fading parameter m is satisfied, then a closed-form integral is present. Therefore, the lower bound integral is defined as:

$$P_{LB} = \int_1^{m+1} \frac{1}{P_{out}} dm \tag{27}$$

We may reduce the given equation even more by substituting P_{out} and then we can establish the lower bound over the area ranging from 1 to $\mu+1$ according to the given equation. The methods given in [25] of Section VI and [26] can be used to solve the upper integral and yield the lower bound. The nonlinearity medium parameter is the main determinant of the calculated bound.

$$P_{out} = \frac{2^{L\frac{m_x+m_y}{2}}}{2^{\frac{m_x+m_y}{2}+1}\Gamma\left(\frac{m_x+m_y}{2}+1\right)\exp\left(\frac{m^L}{2}\right)} \tag{28}$$

The above expression of OP reveals that the non-linear medium parameter affects the lower bounds.

4.1.2 Upper Bound of Outage for 6G UAVs System

Let's denote P_{UB} as the series terms of Eq. (21). Achieving the upper bound of P_{UB} means having infinite roots available. This is expressed as: $P_{UB} = \ln(m+1) \geq P_{\text{out}} \geq 1 + \ln(m)$

Like the lower limit, the condition states that there must be an unlimited number of coefficients for a closed-form integral on each side of P_{out}. Therefore, the upper limit integral can be described as:

$$P_{UB} = \int_1^{m+1} \frac{p_{out}}{m} dm \tag{29}$$

Substituting P_{out} from the provided equation and further simplifying, we establish the maximum limit for the range between 1 and $m+1$.

$$P_{out} = \frac{\sum_{k=0}^{\infty} \frac{k!\, m_k L_k^{\frac{m_x+m_y}{2}} \left(\left(\frac{2}{m_x+m_y}+1\right)2m^L\right)}{\left(\frac{m_x+m_y}{2}+1\right)_k}}{2^{\frac{m_x+m_y}{2}+1}\Gamma\left(\frac{m_x+m_y}{2}+1\right)\exp\left(\frac{d^L}{2}\right)} \tag{30}$$

This expression demonstrates that the maximum limit is influenced by the quantity of antennas and the fluctuating distance from the authorized transmitter.

4.2 Comprehending the Probability of a Secrecy Outage

This section delves into the concept of SOP and its bounds, as represented by Eq. (19).

4.2.1 Lower Bound of Secrecy Outage for 6G UAVS System

Denote S_{LB} as the series terms of Eq. (19). At the point where a specific constraint parameter approaches infinity, The minimum limit of the SOP has been achieved. As the value of m increases without bounds, this phenomenon occurs. Here is the definition of S_{LB}:

$$SOP \leq \int_1^m \frac{1}{SOP} dm \tag{31}$$

Now, using this phrase, we can represent the minimum value of SOP as (24). By replacing Eq. (19) with the previous expression and simplifying it, we can establish the minimum value for the range from

1 to m as 24.

$$SOP \leq \frac{L_E L_R}{2^{m_{R''}+m_R+2\theta}\Gamma(m_R)\Gamma(m_{R''})} \tag{32}$$

4.2.2 Upper Bound of Outage for 6G UAV System

The upper limit of SOP is achieved when a certain constraint parameter tends toward zero. This occurs when m approaches zero. We define S_{LB} as:

$$SOP \geq \int_1^m \frac{SOP}{m} dm \tag{33}$$

Now, based on this expression, we can express the upper bound of SOP as (25). After substituting (23) into the given expression and simplifying, The maximum limit for the area ranging from 1 to m can be determined as follows:

$$SOP = \frac{L_E L_R}{2^{m_R+2\theta}} \sum_{k=0}^{\infty} \sum_{l=0}^{\infty} \frac{l!\, c_{l,R}}{(m_R)_l} \tag{34}$$

The above expression demonstrates that as k approaches infinity [27], Chebyshev's inequality is satisfied and simplifies to an exponential term. Additionally, it's notable that by substituting $m = 1$ in (31), the expression reduces to Eq. (19) of [19], hence proving backward compatibility. Moreover, when mobility is not considered, the expression reduces to its non-linear form given as Eq. (8) of [28].

5 Restricting Eavesdropping for 6G-UAVs System through an Optimisation Problem

This study aims to develop a solution that reduces passive eavesdropping in connected vehicular scenarios. In this context, the term SNR pertains to users engaging in secure transmissions. Because the scenario is clandestine, pinpointing the eavesdropper is inherently challenging.

The proposed solution aims to reduce passive eavesdropping in connected vehicular scenarios. Fig. 3 illustrates the possible conditions under which eavesdropping can occur with respect to the performance of SOP against SNR. Typically, when the secrecy rate (R_s) is in the range of kbps, a transmission is considered maximally compromised when the SOP is one, whereas a SOP of zero indicates that the transmission is secure and private. The convex optimization problem is depicted in Fig. 3 showcasing the impact of SNR on SOP. The left panel depicts a scenario where the SOP is falling (from 1 to 0), while the SNR is increasing, as indicated by the middle vertical line. A decrease in SNR is associated with an increase in SNR on the right side of the vertical line, from 0 to 1. Under conditions of poor fading ($m = 1$, or close to 1), it becomes especially challenging to improve SOP performance. Consequently, it is imperative to enhance the SNR to decrease the SNR. The convex optimization strategy aims to prevent the value of SOP from decreasing below a predetermined or desirable threshold.

The optimization approaches are created to prevent eavesdropping in unfavorable settings. The convexity of the problem is demonstrated by Theorem 1, while Theorem 2 offers a way to limit eavesdropping.

Theorem 1: There is a domain ($dom[H]$) such that the output power $P_{out}(R_S)$ is maximized for any given value of R_s.

Proof: SOP cannot be defined as a minimum or maximum at any moment. On the other hand, limitations can be created for a certain domain of fading coefficients. Consequently, the issue is

classified as convex optimization. The following is the proof:

$$\frac{\mathrm{d}}{\mathrm{d}s}(P_{sop}) \neq 0 | \gamma = \gamma_i \,\&\, R_s = min(R_s) \tag{35}$$

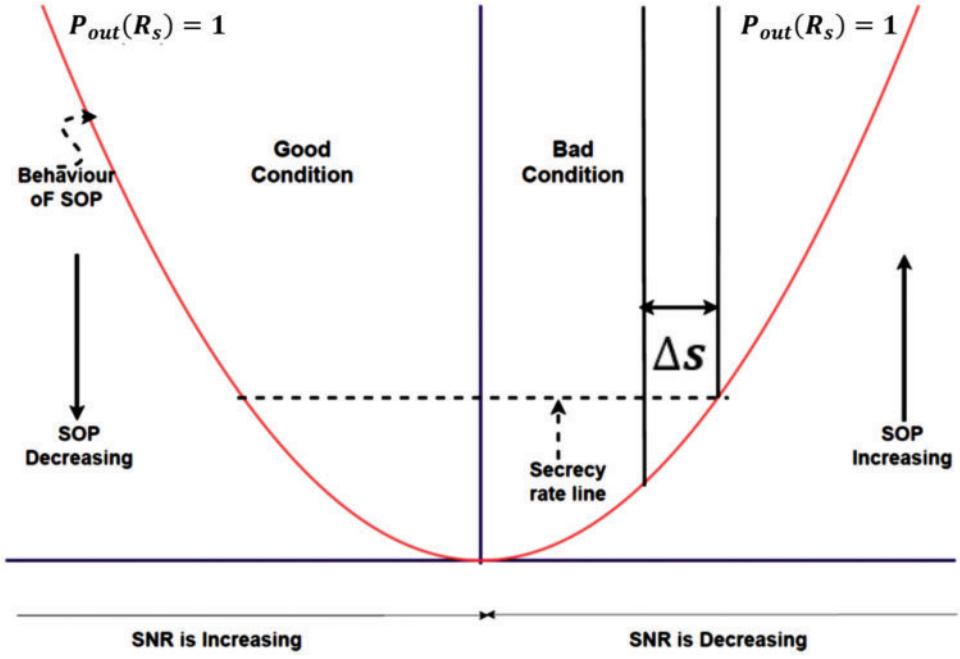

Figure 3: Convex optimisation scenario for restricting eavesdropping

Specify a period P^{+}_{sop} in which the SOP values rise, given the values of γ_i and R_s. Conversely, the range in which the SOP values decrease under the given restrictions is denoted as P^{-}_{sop}. The smallest value of the sum of products is defined according to Newton's method for nonlinear optimization.

$$min\left[\frac{\mathrm{d}}{\mathrm{d}s}P^{+}_{sop} - \frac{\mathrm{d}}{\mathrm{d}s}P^{-}_{sop}\right] = 0 \tag{36}$$

The concept mentioned above can be further defined as follows:

$$min\left(\left[\frac{\mathrm{d}}{\mathrm{d}s}P^{+(t+1)}_{sop} - \frac{\mathrm{d}}{\mathrm{d}s}P^{+}_{sop}(t)\right] - \left[\frac{\mathrm{d}}{\mathrm{d}s}P^{-(t+1)}_{sop} - \frac{\mathrm{d}}{\mathrm{d}s}P^{-}_{sop}(t)\right]\right) = 0 \tag{37}$$

Using the SOP expression from 19, the additional term in the equality above can be expressed as 26. There is no evidence to support the aforesaid equality. Thus, convex optimization can be used to solve Theorem 1.

Theorem 2: The falsification factor (f') for a given range (Δs) of SNR is defined such that $f' \in (dom[H])$, but $f' \neq (max\, dom[H])$, if $P_{out}(R_S) = \max(P_{out}(R_S))$, for all $(dom[H])$.

Proof: Depending on the orientation of the intervals, there are three subclasses for the convex optimization problem.

1. Subclass 1: If $\rightarrow \max(P_{out}(R_S))$ then $P_{out}(R_S)$
2. Subclass 2: If $\leftarrow \max(P_{out}(R_S)) = P_{out}(R_S)$

3. Subclass 3: If $P_{out}(R_S) = \max(P_{out}(R_S))$

The difference between the intended value $P_{out}(R_s)^d$ and the actual value $P_{out}(R_s)^a$ of $P_{out}(R_s)$, together with the function of direction factor (D'), is known as the falsification factor (f'). Hence, f' has the following mathematical definition:

$$f' = (P_{out}(R_s)^d - P_{out}(R_s)^a) \pm D' \tag{38}$$

From (38), it is evident that the expression yields an optimal root given the specified restrictions. There is availability of the optimal root when

$$\frac{\mathrm{d}}{\mathrm{d}\Delta s} f' = 0 | R_s \tag{39}$$

The following is how D' values can be attained:

1. If $P_{out}(R_S) \rightarrow \max(P_{out}(R_S))$, $D' = 1$
2. If $P_{out}(R_S) \leftarrow \max(P_{out}(R_S))$, $D' = -1$
3. If $P_{out}(R_S) = \max(P_{out}(R_S))$ $D' = 0$

The direction factor indicates whether OP is going in a tractable direction—that is, rising or decreasing. As a result, the falsification factor can be zero, positive, or negative. Furthermore, the direction factor is manageable, indicating that command over the falsification element may be assumed, consistently creating an atmosphere that is resistant to eavesdropping. Controlling the eavesdropping can be achieved by adding a negative D' if f' is positive, and vice versa.

6 Simulation Results

This section contains simulation details to validate SOP's analytical expression. We performed these simulations using the optimization and mathematical toolbox of MATLAB (Matrix Laboratory) R2022b. More precisely, the convex optimization (CVX) tool was used to formalize SOP coefficients so that the tasks could be optimized. This required a mix of nonlinear, analytical, and convex methods to validate the problem. We used Monte-Carlo simulations with about 10^8 generations. Both analytical and non-linear methods are used to draw inferences from the results.

The former is the analytical expression's ultimate form, incorporating the direct reliance on single or multiple variables on metrics such as SOP and OP performance. The performance metric incorporates the wireless medium parameter in its non-linear form; however, the final formulation does not account for this factor. We review the methodology, emphasizing how the vehicle's motion, the wireless medium parameter, and the corresponding mathematical parameters affect the effectiveness of SOP and OP. In all numerical results, $L = 2$ and $m = 4$ values are taken into account. The analytical behavior of OP and SOP is revealed by the simulations. Secrecy outage probability is displayed against SNR in Fig. 4, which also illustrates how OP varies for different SNR values at different velocities. It is evident that the vehicle's high speed increases the likelihood of being overheard.

Fig. 5 displays the maximum limit integral of the outage probability *vs.* series convergence terms. The upper bound is achieved by equating the range between the authorized emitter and the eavesdropper to 100 meters. It represents that as the outage performance quickly approaches unity for higher series terms of more than six, raising the secrecy rate is required. Fig. 6 displays the secrecy outage probability performance against SNR at various velocities. The fact that the secrecy

outage is only 0.4 indicates that more secure information transfer is taking place between authorized transmitters and authentic receivers, thanks to appropriate modeling of the fading environment.

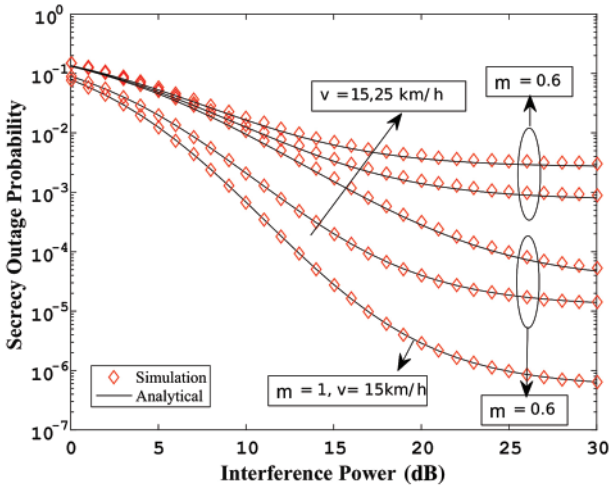

Figure 4: ($c = 2$ km, $b = 30$ m and $d' = 100$ m) as SOP *vs*. SNR

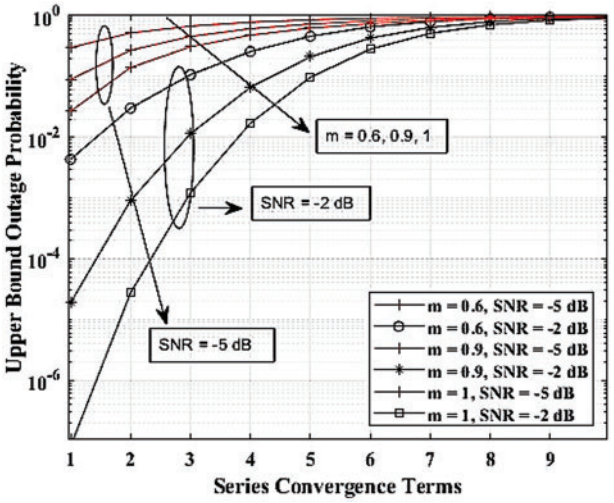

Figure 5: OP's maximum limit integral *vs.* the convergence terms, where $m = 4$, $d' = 100$ m, $c = 2$ km, and $b = 30$ m

As demonstrated in Fig. 7, however, the wireless medium is quite unpredictable, necessitating the determination of the lower and upper bounds. Additionally, it shows how well the SOP performs in comparison to the bound index. The analytical form of the SOP allows for the identification of the hyper-geometric special function. This function assists in finding the infinite series using closed-form methods. The bound index determines the number of iterations after which we can treat the expression as closed form. Fig. 8 illustrates the SOP's performance in relation to the bound index of the hypergeometric function. It is evident that when the index rises, the SOP expresses itself more accurately, reducing the likelihood of being overheard when mobility is at its peak.

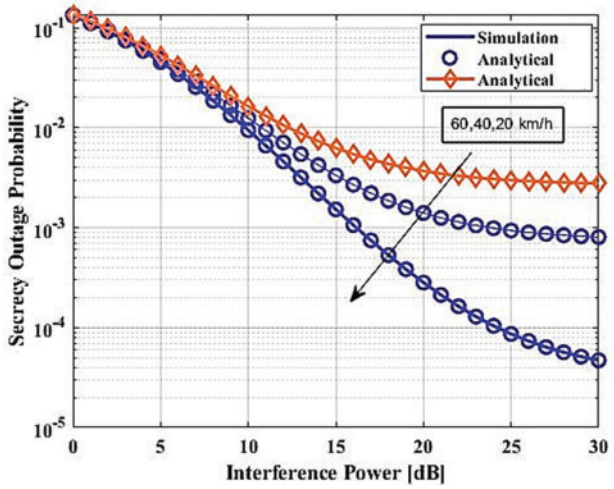

Figure 6: The SOP is compared to the SNR with $m = 4$, $d' = 100\,\text{m}$, $c = 2\,\text{km}$, and $b = 30\,\text{m}$ [14]

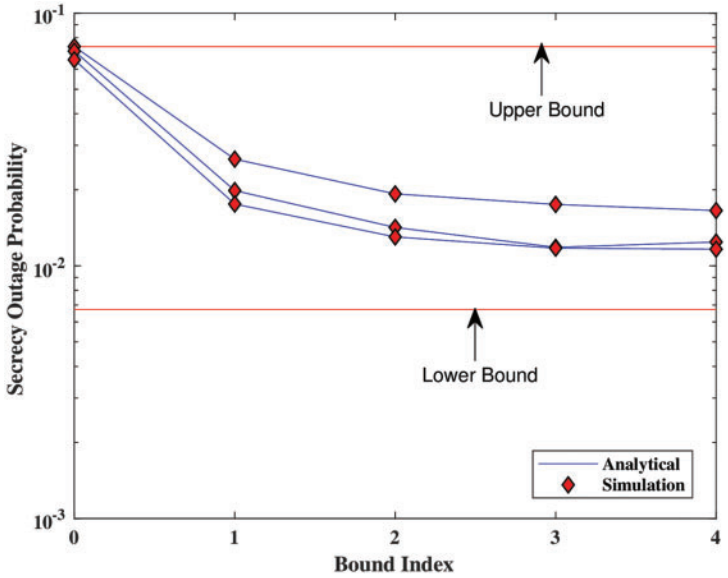

Figure 7: Using the bound index to guide decision-making ($m = 4$, $\text{d}' = 100$ m, $c = 2\,\text{km}$ and $\text{b} = 30$ m)

Fig. 8 displays the counting of the roots of the SOP closed-form expression. The nonlinear technique does not provide the exact number, and it may vary up to infinity. We have observed that root identification is dependent on the sign of the falsification factor. This suggests that the procedure is cognizant of SOP's increasing and lowering values. Fig. 9 shows the ability of Theorem 2 to find the optimization roots over Eigenvalues provided by the characteristic expression of SOP. The behavior demonstrates that the convex technique performs better when applied to closed-form expressions because it converges quickly toward zero at very low Eigenvalues. In that scenario, however, the direction factor's value should be known. In practice, we can use it to ensure that the SOP increases in value whenever the eavesdropper initiates the process of breaking into the communication link.

Applying the predefined negative direction factor reduces the effectiveness of eavesdropping in that situation. In practice, the Reed-Muller codes can be used to enforce them on the system.

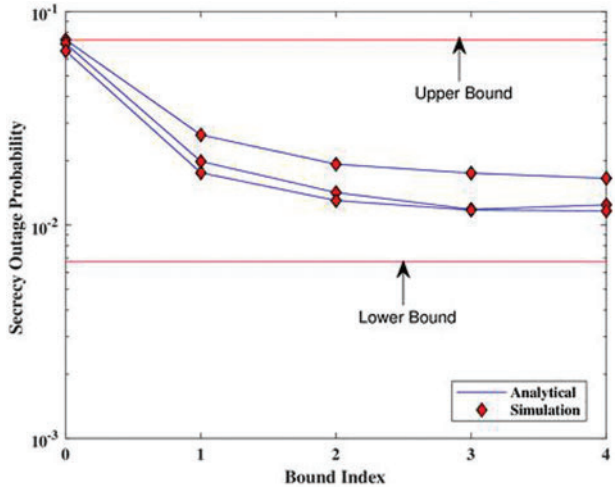

Figure 8: Coefficient of optimization roots ($L = 2$, $m = 4$, $d' = 100\,\text{m}$, $c = 4\,\text{km}$ and $b = 30\,\text{m}$) compared to SOP roots

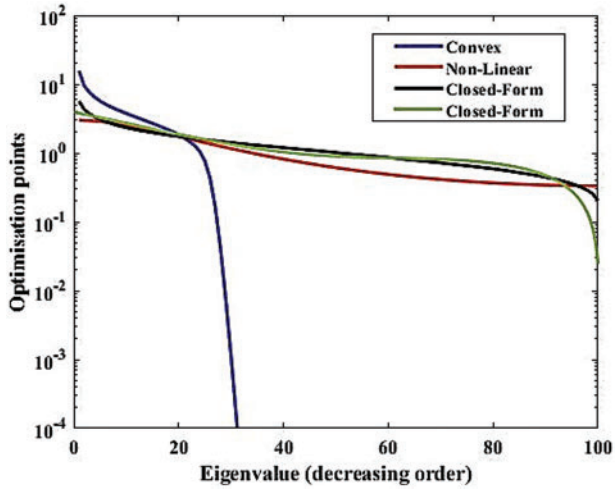

Figure 9: Optimization roots for anti-eigenvalues ($m = 4$, $d' = 100\,\text{m}$, $c = 4\,\text{km}$, $b = 30\,\text{m}$ and $L = 2$) [25]

Accordingly, Fig. 10 demonstrates that the convex approach is appropriate for the optimization. The convex approach optimizes the falsification factor more effectively than the non-linear and closed-form approaches. Fig. 11 presents the insights into exact roots obtained from the closed form, convex, and non-linear approaches. Unlike Fig. 6, we show the asymptotic behavior of SOP for $m = 0.5$. Fig. 12 shows the velocity-induced asymptotic behavior of SOP. Even with two antennas operating at a high speed of 50 km/h, SOP is restricted to a value of less than 0.5. However, moving slowly reduces the likelihood of overhearing.

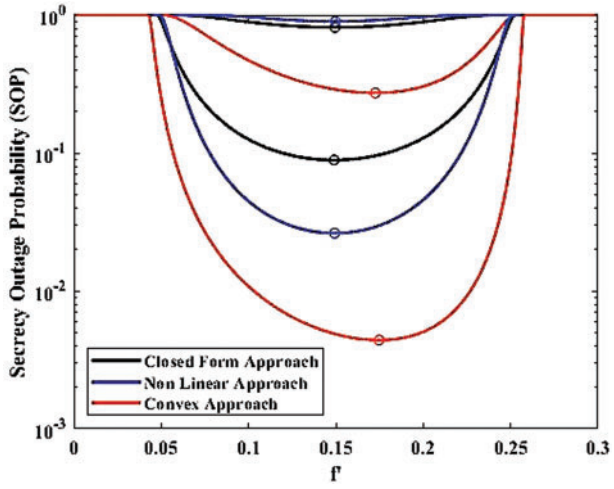

Figure 10: SOP for preventing falsification ($m = 4$, $d' = 100$ m, $c = 4$ km, $b = 30$ m and $L = 2$)

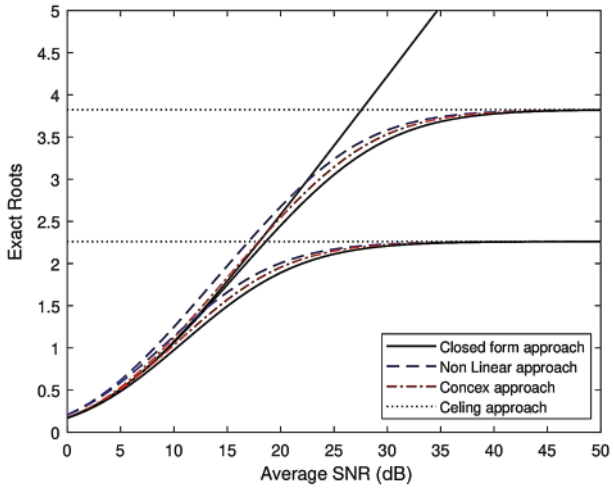

Figure 11: Exact roots for $m = 4$, $d' = 100$ m, $c = 2$ km, $b = 30$ m, and $L = 2$ in relation to average SNR

Figs. 13 to 15 show the outcomes of a closed-form method and its non-linear version. The first one pertains to the final form of the analytical statement and includes the measurement of the direct relationship between one or more variables and metrics like SOP and HOP. However, the final expression of the non-linear performance metric does not include the wireless medium parameter. This study looks at how wireless medium variables, vehicle mobility, and the mathematical parameters that go along with them affect how effective SOP and OP are. L and m have default values of 2 and 4, respectively, for all numerical outcomes. Analytical behavior is shown in both OP and SOP simulations. As shown in Fig. 13, the variance in OP with respect to SNR for varying vehicle velocities can be found by plotting OP *vs*. SNR. Because of its rapid speed, the car makes it more likely that someone will be listening in on them. Fig. 14 illustrates the probability of a hybrid outage under the influence of mobility. The findings show that size had an impact on the level of intrusion. Fig. 15 illustrates

the network's reaction to several eavesdroppers. The potential for eavesdropping increases with the number of eavesdroppers, which raises the possibility of a secrecy outage.

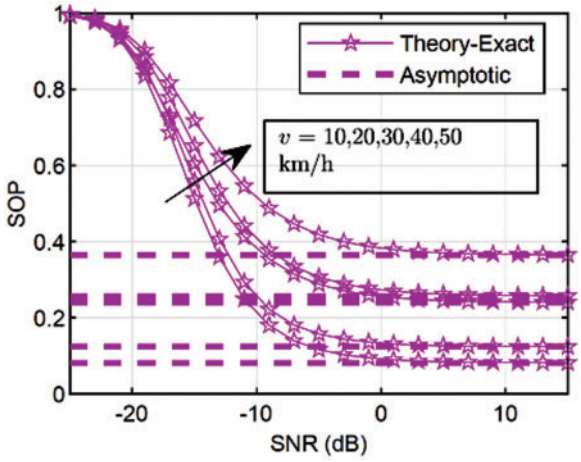

Figure 12: Asymptotic behavior of SOP ($m = 0.5$, $d' = 100$ m, $c = 2$ km and $b = 30$ m)

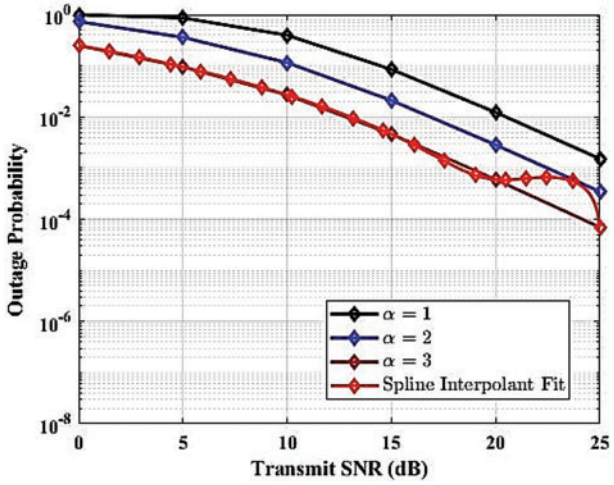

Figure 13: Outage probability against transmit SNR for various path loss

SOP *vs.* SNR function for Nakagami-*m* fading channels is plotted in Fig. 16, focusing on different fading parameters (m) of the legitimate and eavesdropping channels. The output is the SOP *vs.* the SNR (dB) with three different Nakagami-*m* parameters (m = 1), (m = 2), and (m = 3) using a logarithmic scale for the SOP. The m values distinguish between a legal channel and an eavesdropper channel, represented by the curves on the plot. Curves in blue, yellow, and green color represent legitimate channels regarding m = 1, m = 2, and m = 3, respectively (Fig. 6). In contrast to the eavesdropper channels for both m and values, the SOP experiences a decrease across all scenarios as the SNR rises, due to the plot's clear display of strong secrecy performance at elevated SNR levels. Still, the secrecy outage probability is never zero, i.e., the SOP is zero for all block lengths. Higher m values correspond to curves lying lower on the graph, indicating that better secrecy performance is present in channels with higher m values. Higher m values correspond to less severe fading conditions. Also, it

is evident from the valid and eavesdropper channels. For all m, the eavesdropper channels have higher SOP than the corresponding legitimate channels which means that the eavesdropper experiences worse secrecy performance than the legitimate user. In general, Fig. 16 well reveals that the secrecy outage performance of wireless communication systems can be significantly influenced by the parameter of Nakagami-*m* fading and also SNR and that the Ser can be greatly improved by increasing SNR and by adopting the large m value.

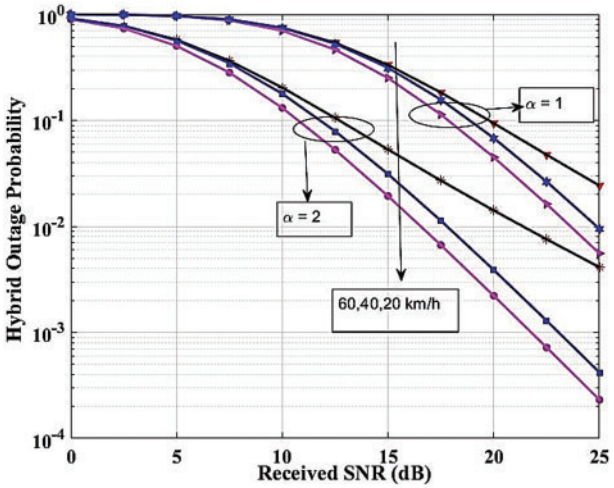

Figure 14: Hybrid outage probability against transmit SNR for various velocity

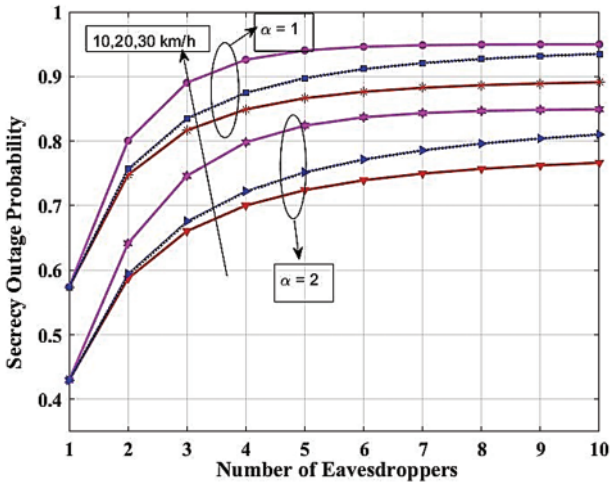

Figure 15: Secrecy outage probability against the number of eavesdroppers

Fig. 17 illustrates the SOP as a function of eavesdropper velocity for Nakagami-*m* fading channels with a fading parameter (m = 2). The SOP, plotted on a logarithmic scale, measures the likelihood that the secrecy capacity falls below a threshold of 0.1. The *x*-axis represents the eavesdropper's velocity in meters per second (m/s), ranging from 0 to 30 m/s. As the eavesdropper's velocity increases, the SOP exhibits significant fluctuations, indicating variability in secrecy performance due to the Doppler effect, which alters the channel conditions for the eavesdropper. These fluctuations highlight the SOP's

sensitivity to changes in the eavesdropper's velocity. The lack of a clear trend may be due to the complicated interaction between the Doppler shift and Nakagami-*m* fading, which changes the quality of the received signal and, in turn, the SOP. This underscores the importance of considering mobility in secure communication analysis, as varying eavesdropper velocities can substantially affect the system's secrecy performance.

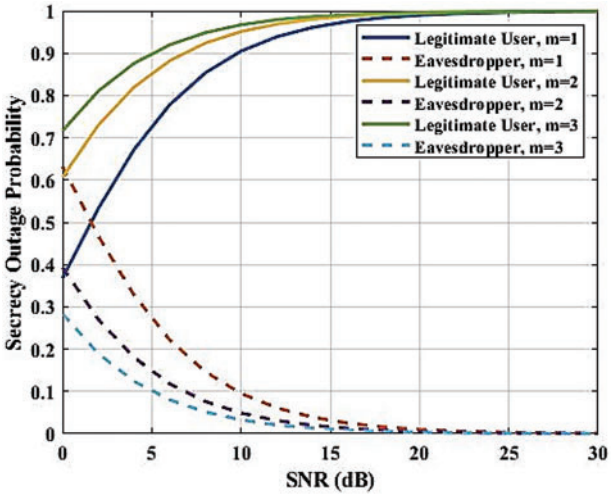

Figure 16: SOP against SNR with various channel parameters

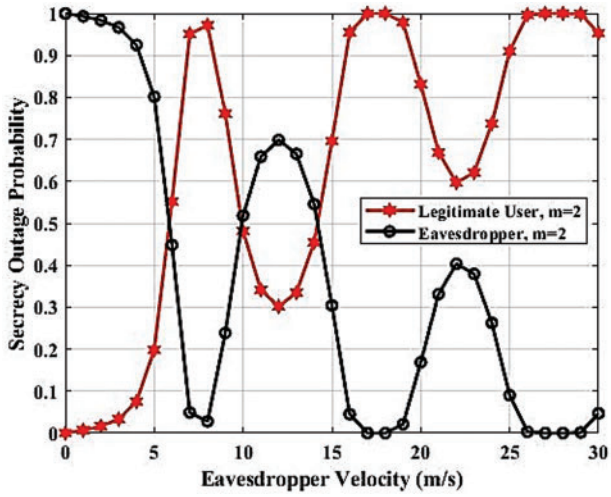

Figure 17: SOP against velocity

6.1 The Influence of Parameters on Outcomes

The influence of each parameter on the performance of secrecy is explicated in the following manner:

1. The effect on high fading parameters: The fading parameter frequently switches to dynamic fading, which is a more realistic depiction for a vehicular scenario, when it is given a significant value (m = 4). When fading parameters are substantial (Fig. 3), SOP's velocity behavior changes

significantly. Consequently, it is anticipated that an increase in velocity will lead to a decline in secrecy performance. However, the consequences of this degradation are controllable and can be effectively mitigated by taking into account the value of $m \geq 4$.

2. The findings indicate that in the context of analytical representations (Eq. (17)) of SOP, the utilization of several antennas yields significantly superior performance compared to a single antenna. In the extremely variable fading situation ($m > 4$ and higher), the secrecy outage can be further strengthened by maintaining a constant velocity and SNR. Consequently, better secrecy performance is achieved with a greater number of antennas.

3. The influence of the convex approach: Fig. 1 illustrates how the requirement for limitation increases as the SNR decreases. For instance, when the SNR is set at 0.2, the required value of SOP is observed to grow to 0.7. As stated in reference [15], the falsification factor should be designed to maintain the optimal value of SOP. Therefore, in accordance with Theorem 2, the direction factor value of 1 is included into the system, thereby restricting the occurrence of eavesdropping. Various numerical methods, both fast and slow, have been examined as potential measures to mitigate eavesdropping activities. The convex technique has been seen to rapidly identify outlier roots. Consequently, the falsification factor is designed in a manner that prevents the standard deviation from exceeding a specific desired value.

4. The precise modeling of dynamic fading factors is crucial when dealing with extreme fading circumstances. Hence, a high dynamic fading parameter frequently signifies precise modeling, thereby enhancing the performance of secrecy. The outage probability exhibits fast variation in response to changes in velocity when the fading parameter is high. The issue can be addressed and resolved by taking into account an appropriate fading model.

5. Velocity has an effect in that large variations in SNR may result from increasing receiver-side velocity. The receiver's signal reconstruction will yield imprecise approximations of the original transmitted signal. As a result, considering the higher velocity during processing will directly affect the signal reconstruction. Thus, the fading scenario gets better as node velocity increases, which raises the probability of incursion.

6. The process of obtaining information from outside sources: The functions defined by the non-linear coefficient of the wireless communication medium are referred to as the computed bounds. The constraints exhibit a static yet conditional nature, indicating that it is not advisable to consistently raise the signal power in the event of the most severe fading scenario. This is supported by the findings presented in Fig. 6, which indicate that the SOP is largely constrained after reaching an indexing value of 3.

6.2 Analysis of Computation Time

The computation time for each result was the main emphasis of this section. 8 GB of RAM (Random Access Memory)) and an Intel(R) Core(TM) i7-4790 CPU (Central Processing Unit) operating at 3.60 GHz were used to run the Monte-Carlo simulations.

Table 2 illustrates the computational time required for plotting analytical expressions of OP and SOP (referred to as analysis time) and the Monte Carlo simulations (referred to as simulation time). It is noted that the hyper-geometric functions involved in the simulations for Figs. 4, 6, and 8 can significantly reduce the computation time in comparison with the rest of the results.

Table 2: Analysis of computational time for OP and SOP

	Figure 4	Figure 5	Figure 6	Figure 7	Figure 8	Figure 9	Figure 10
Simulation time (sec)	2245	1279	4655	1344	3453	1322	3722
Analysis time (sec)	32	41	14	16	21	45	88

7 Conclusions

This paper focuses on the problem of eavesdropping in the context of 6G-enabled UAV communications. Expressions of physical layer security metrics were obtained across a dynamic Nakagami-*m* fading model with a time complexity of $2\times$ the number of layers. The generated closed-form equations are validated by Monte Carlo simulations. Since there are fewer changes in the SOP, the findings indicate that 2×2 Nakagami-*m* is a suitable fading model under constant velocity for trustworthy receivers and eavesdroppers. The impact of mobility on mobile performance indicators has been demonstrated. Poor fading situations elevate the level of OP, posing a potential threat to the integrity of valid transmissions. Consequently, the suggested approach can be valuable in creating safe systems with minimal complexity for cognitive vehicular networks. Furthermore, studies have demonstrated that a LoS link's mobility may affect its eavesdropping capability, resulting in a reduced capacity for eavesdropping.

Acknowledgement: We extend our sincere gratitude to Taif University, Saudi Arabia, for their invaluable support and collaboration in this research endeavor. Our deepest appreciation also goes to Smt. Chandaben Mohanbhai Patel Institute of Computer Applications and Chandubhai S. Patel Institute of Technology for their significant contributions and unwavering assistance throughout this study. The collective efforts and resources provided by these esteemed institutions have been instrumental in the successful completion of this research.

Funding Statement: This research was funded by Taif University, Taif, Saudi Arabia, Project No. (TU-DSPP-2024-139).

Author Contributions: Study Conception: Sagar Kavaiya and Sagarkumar Patel; Methodology: Sagar Kavaiya and Dharmendra Chauhan; Mathematical Formulation: Sagarkumar Patel; Software: Hiren Mewada and Sagarkumar Patel; Validation and Formal Analysis: Hiren Mewada and Faris A. Almalki; Writing—Original Draft, Visualization: Sagar Kavaiya, Dharmendra Chauhan and Hana Mohammed Mujlid; Writing—Review & Editing: Sagarkumar Patel, Hiren Mewada and Faris A. Almalki; Project Administration and Funding: Faris A. Almalki and Hana Mohammed Mujlid. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Netw.*, vol. 34, no. 3, pp. 134–142, 2020. doi: 10.1109/MNET.001.1900287.

[2] M. Mozaffari, W. Saad, M. Bennis, Y. H. Nam, and M. Debbah, "A tutorial on UAVs for wireless networks: Applications, challenges, and open problems," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 3, pp. 2334–2360, 2019. doi: 10.1109/COMST.2019.2902862.

[3] X. Sun, D. W. K. Ng, Z. Ding, Y. Xu, and Z. Zhong, "Physical layer security in UAV systems: Challenges and opportunities," *IEEE Wirel. Commun.*, vol. 26, no. 5, pp. 40–47, 2019. doi: 10.1109/MWC.001.1900028.

[4] S. H. Alsamhi, O. Ma, M. S. Ansari, and F. A. Almalki, "Survey on collaborative smart drones and internet of things for improving smartness of smart cities," *IEEE Access*, vol. 7, pp. 128125–128152, 2019. doi: 10.1109/ACCESS.2019.2934998.

[5] S. H. Alsamhi *et al.*, "Drones' edge intelligence over smart environments in B5G: Blockchain and federated learning synergy," *IEEE Trans. Green Commun. Netw.*, vol. 6, no. 1, pp. 295–312, 2022. doi: 10.1109/TGCN.2021.3132561.

[6] E. S. Alkhalifah and F. A. Almalki, "Developing an intelligent cellular structure design for a UAV wireless communication topology," *Axioms*, vol. 12, no. 2, 2023, Art. no. 129. doi: 10.3390/axioms12020129.

[7] K. S. Alqarni, F. A. Almalki, B. O. Soufiene, O. Ali, and F. Albalwy, "Authenticated wireless links between a drone and sensors using a blockchain: Case of smart farming," *Wirel. Commun. Mob. Comput.*, vol. 2022, no. 1, 2022, Art. no. 4389729. doi: 10.1155/2022/4389729.

[8] F. A. Almalki and M. C. Angelides, "Autonomous flying IoT: A synergy of machine learning, digital elevation, and 3D structure change detection," *Comput. Commun.*, vol. 190, no. 1, pp. 154–165, 2022. doi: 10.1016/j.comcom.2022.03.022.

[9] S. Patel *et al.*, "Impact of antenna spacing on differential spatial modulation and spatial modulation for 5G-based compact wireless devices," in *2021 4th International Symposium on Advanced Electrical and Communication Technologies (ISAECT)*, Alkhobar, Saudi Arabia, Dec. 6–8, 2021, pp. 1–6. doi: 10.1109/ISAECT53699.2021.9668400.

[10] W. U. Khan *et al.*, "Opportunities for physical layer security in UAV communication enhanced with intelligent reflective surfaces," *IEEE Wirel. Commun.*, vol. 29, no. 6, pp. 22–28, 2022. doi: 10.1109/MWC.001.2200125.

[11] A. Omri and M. O. Hasna, "Physical layer security analysis of UAV based communication networks," in *IEEE Veh. Technol. Conf.*, Chicago, IL, USA, Aug. 27–30, 2018, pp. 1–6. doi: 10.1109/VTC-Fall.2018.8690950.

[12] J. Hu, C. Chen, L. Cai, M. R. Khosravi, Q. Pei and S. Wan, "UAV-assisted vehicular edge computing for the 6G internet of vehicles: Architecture, intelligence, and challenges," *IEEE Commun. Standards Mag.*, vol. 5, no. 2, pp. 12–18, 2021. doi: 10.1109/MCOMSTD.001.2000017.

[13] Z. Yin *et al.*, "UAV-assisted physical layer security in multi-beam satellite-enabled vehicle communications," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 3, pp. 2739–2751, 2022. doi: 10.1109/TITS.2021.3090017.

[14] S. Javaid *et al.*, "Communication and control in collaborative UAVs: Recent advances and future trends," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 6, pp. 5719–5739, 2023. doi: 10.1109/TITS.2023.3248841.

[15] A. Vashisth and R. S. Batth, "An overview, survey and challenges in UAVs communication network," in *2020 International Conference on Intelligent Engineering and Management (ICIEM)*, London, UK, 2020, pp. 342–347. doi: 10.1109/ICIEM48762.2020.9160197.

[16] Saifullah, Z. Ren, K. Hussain, and M. Faheem, "K-means online-learning routing protocol (K-MORP) for unmanned aerial vehicles (UAV) adhoc networks," *Ad Hoc. Netw.*, vol. 154, no. 2, 2024, Art. no. 103354. doi: 10.1016/j.adhoc.2023.103354.

[17] A. Fotouhi *et al.*, "Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 4, pp. 3417–3442, 2019. doi: 10.1109/COMST.2019.2906228.

[18] J. Wang *et al.*, "Physical layer security for UAV communications: A comprehensive survey," *China Commun.*, vol. 19, no. 9, pp. 77–115, 2022. doi: 10.23919/JCC.2022.09.007.

[19] S. K. Leung-Yan-Cheong and M. E. Hellman, "The gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978. doi: 10.1109/TIT.1978.1055917.
[20] G. Fraidenraich, O. Lévêque, and J. M. Cioffi, "On the MIMO channel capacity for the Nakagami-m channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3752–3757, 2008. doi: 10.1109/TIT.2008.926467.
[21] S. Kavaiya, D. K. Patel, Z. Ding, Y. L. Guan, and S. Sun, "Physical layer security in cognitive vehicular networks," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3752–3757, Aug. 2008. doi: 10.1109/TIT.2008.926467.
[22] S. Zhu, C. Guo, C. Feng, and X. Liu, "Performance analysis of cooperative spectrum sensing in cognitive vehicular networks with dense traffic," in *2016 IEEE 83rd Vehicular Technology Conference (VTC Spring)*, Nanjing, China, 2016, pp. 1–6. doi: 10.1109/VTCSpring.2016.7504402.
[23] S. Kavaiya and D. K. Patel, "Restricting passive attacks in 6G vehicular networks: A physical layer security perspective," *Wirel. Netw.*, vol. 29, no. 3, pp. 1355–1365, 2022. doi: 10.1007/s11276-022-03189-1.
[24] H. Lei *et al.*, "Secrecy outage performance for SIMO underlay cognitive radio systems with generalized selection combining over Nakagami-m channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10126–10132, 2016. doi: 10.1109/TVT.2016.2536801.
[25] I. S. Gradshteyn, I. M. Ryzhik, A. Jeffrey, Y. V. Geronimus, M. Y. Tseytlin and Y. C. Fung, "Table of integrals, series, and products," *J. Biomech. Eng.*, vol. 103, no. 1, p. 58, 1981. doi: 10.1115/1.3138251.
[26] D. E. Barton, M. Abramovitz, and I. A. Stegun, "Handbook of mathematical functions with formulas graphs and mathematical tables," *J. R. Stat. Soc. Ser. A*, vol. 128, no. 4, pp. 593–594, 1965. doi: 10.2307/2343473.
[27] M. Bloch and J. Barros, "Secrecy limits of Gaussian Wiretap Channel," in *Physical–Layer Security: From Information Theory to Security Engineering*, 1st ed. New York, NY, USA: Cambridge University Press, 2011, pp. 177–190.
[28] Y. Ai, M. Cheffena, A. Mathur, and H. Lei, "On physical layer security of double Rayleigh fading channels for vehicular communications," *IEEE Wirel. Commun. Lett.*, vol. 7, no. 6, pp. 1038–1041, 2018. doi: 10.1109/LWC.2018.2852765.