IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 18 September 2022, accepted 1 October 2022, date of publication 19 October 2022, date of current version 1 November 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3215975

SURVEY

Security Threats and Mitigation Techniques in UAV Communications: A Comprehensive Survey

GAURAV KUMAR PANDEY[1], (Graduate Student Member, IEEE), DEVENDRA SINGH GURJAR[1], (Senior Member, IEEE), HA H. NGUYEN[2], (Senior Member, IEEE), AND SUNEEL YADAV[3], (Senior Member, IEEE)

[1]Department of Electronics and Communication Engineering, National Institute of Technology Silchar, Cachar, Silchar, Assam 788010, India
[2]Department of Electrical and Computer Engineering, University of Saskatchewan, Saskatoon, SK S7N 5C5, Canada
[3]IoT Security Laboratory, Department of Electronics and Communications Engineering, Indian Institute of Information Technology Allahabad, Allahabad, Uttar Pradesh 211015, India

Corresponding authors: Suneel Yadav (suneel@iiita.ac.in) and Devendra Singh Gurjar (dsgurjar@ece.nits.ac.in)

This work is part of the 'IoT Security' Project supported by the C3iHub, Indian Institute of Technology, Kanpur with funding from the Department of Science and Technology, Government of India.

ABSTRACT Unmanned aerial vehicles (UAVs) have been instrumental in enabling many new applications and services, including military and rescue operations, aerial surveillance, civilian applications, precision farming, as well as providing extensive wireless network access in remote areas. They have also been used in other areas such as transmission line and oil rig monitoring, disaster recovery, etc. With their increasing payload ability and flight duration, using UAVs is a preferred choice for a multitude of upcoming wireless communication systems. However, because of their open operational nature, UAVs are highly vulnerable to severe security breaches via cyber attacks, eavesdropping on navigational and communication links, etc. Given their widespread applications, the requirement of secured UAV communications has become more and more critical since security failures can lead to detrimental consequences. Several works have examined the extent of privacy and security issues in UAV-assisted networks and introduced various mitigation techniques to address different security challenges. In this paper, a comprehensive survey is conducted that centers on the security issues related to UAV-aided networks. A descriptive taxonomy of various security intrusions on the UAV networks and commonly-used secrecy performance metrics are thoroughly reviewed. An in-depth discussion is provided on alleviating threats with proactive security techniques blended with key wireless communication technologies such as mmWave, non-orthogonal multiple access (NOMA), massive multiple-input multiple-output (MIMO), and cognitive radio. Moreover, several emerging topics like machine learning, software-defined networks, fog and edge computing, blockchain, are discussed in the context of UAV-aided secure communications.

INDEX TERMS Physical layer security, unmanned aerial vehicles (UAVs), proactive mitigation techniques, secrecy metrics, emerging wireless technologies.

I. INTRODUCTION

Unmanned aerial vehicles (UAVs), also commonly known as drones, are remotely-controlled aircrafts or computer program-aided aerial vehicles devoid of a boarded pilot. UAVs have traditionally been used in defense applications, e.g., being deployed in hostile regions for remote monitoring and intelligence without risking pilots' lives. In most scenarios, they are adaptable, agile, relatively inexpensive, and easy to deploy. In the beginning, UAVs were envisioned as an essential component of futuristic warfare in military battlegrounds [1]. However in recent years, the use of UAVs has flourished thanks to skyrocketed demands of civilian applications, such as agronomic preservation [2], search and rescue operations [3], [4], environmental-based predictions, natural calamity monitoring [5], [6], remote commodity deliveries [7], wireless communication relay nodes [8], [9], airborne ground stations [10], [11], infrastructure [12], and

The associate editor coordinating the review of this manuscript and approving it for publication was Mehdi Sookhak.

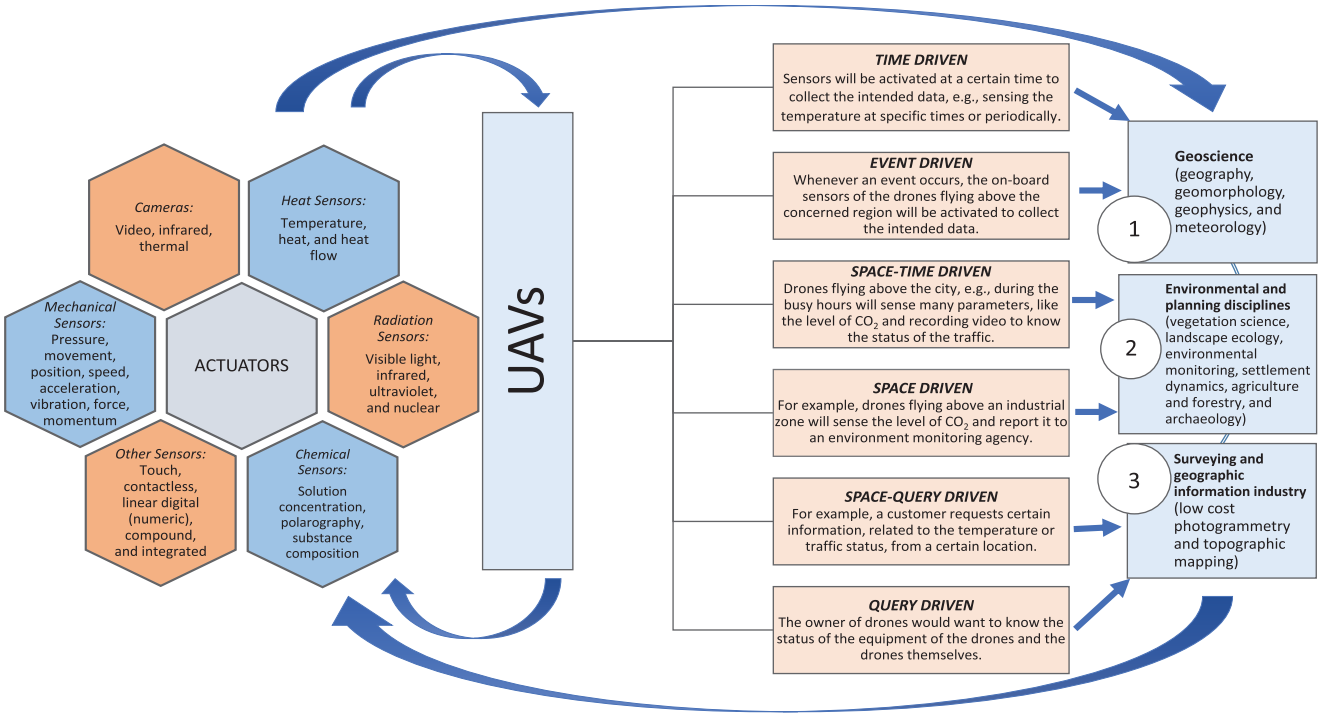

FIGURE 1. Deployment of UAVs in practical scenarios.

traffic monitoring [13]. In the COVID-19 pandemic, the use of UAVs has been an efficient and most promising method to reduce transportation costs and time for applications like aerial spraying, delivery of medical supplies, and monitoring of infection-affected space without being exposed to infection [14].

Although the IMT-2020 standard lays out many important advantages of the 5G wireless communications networks, including low latency, high mobility, ultra reliability, and ample bandwidth [15], the use of airborne base stations (BSs) and UAVs has gained a phenomenal popularity in recent years [16], [17] because of their unique ability to meet the high data rate and reliability requirements. In particular, UAVs can have the upper hand over the terrestrial BSs for serving flash populated locations, e.g., carnivals, festivals, sport, and musical events. They can also help strengthening the communication networking backbone by collaborating with ground BSs [18]. In such scenarios, the use of UAV relay nodes can be a better option and much cheaper than building a new terrestrial BS. In addition, accessibility to hazardous locations and hard-to-reach destinations is also much more feasible with UAV-enabled networks.

UAVs are assorted based on various criteria, including weight and payload, wing configuration, shape, size, flying trajectory, and altitude. Further, they can also be classified based on endurance, control mechanism, maximum and hovering speeds, cruise range, and energy feeding methods. For instance, UAVs can be categorized as rotary or fixed-wing UAVs based on the wing configuration. Fixed-wing UAVs not only have a considerably higher flight speed but can also haul heavier payloads for long ranges than rotary-wing UAVs. Nevertheless, the main limitations of fixed-wing UAVs include the need for a take-off/landing launcher or runway, and the inability to hover at a fixed location. Rotary-wing UAVs, on the contrary, can take off and land steeply and can also stably hover over a particular site. In addition, different applications that require specific attributes, like, deployment environment, endurance, payload, cost constraint, etc., naturally give rise to many variations in design and modeling of UAVs.

UAVs can also be sub-categorized as LAPs and HAPs on the basis of the height of operation. LAPs have low capacity and power with respect to autonomy, endurance, and payload, whereas HAPs have higher endurance and wider radial coverage [12]. The likelihood of getting a LoS link for A2G communication improves as the height of operation of the UAV increases. However, as the height of UAV operation increases, both path-loss and turbulence become more severe. As such, a UAV's operation altitude needs to be optimized, and there is a trade-off between the radial coverage and link reliability [19].

A. DEPLOYMENT OF UAVs IN PRACTICAL SCENARIOS

The use of UAVs has emerged as an attractive solution for many commercial and civilian applications, thanks to their unique attributes and desirable features like augmentation capability and accessibility to society. Fig. 1 depicts diverse deployment scenarios of UAVs in different disciplines and applications [20].

TABLE 1. List of acronyms.

List of Acronyms			
2D	Two-dimensional	JTAG	Joint test action group
3D	Three-dimensional	KKT	Karush-Kuhn-Tucker
3GPP	Third generation partnership project	LAPs	Lower altitude platforms
5G	Fifth-generation	LEO	Low earth orbital
A2G	Air-to-ground	LoS	Line-of-sight
A2A	Air-to-air	LPI/LPD	Low probability of intercept/detection
ADMM	Alternate direction method multipliers	LR	Logistic regression
AI	Artificial intelligence	LSTM	Long short term memory
AN	Artificial noise	M2M	Machine-to-machine
ANN	Artificial neural network	MAC	Media access control
ASC	Average secrecy capacity	MA-DDPG	Multi-agent deep deterministic policy gradient
ASR	Achievable secrecy rate	MEC	Mobile edge computing
ASSR	Average system secrecy rate	MHCPP	Matern hardcore point process
AWGN	Additive white Gaussian noise	ML	Machine learning
B5G	Beyond 5G	m-MIMO	Massive multiple-input multiple-output
BATS	Blockchain and AI-assisted telesurgery system	mmWave	Milli-meter wave
BCD	Block coordinate descent	MSGC	Mobile secrecy guarded cone
BER	Bit error rate	MSCs	Mobile switching centres
BSs	Base stations	mURLLC	Massive ultra-reliable low-latency communication
CCC	Control and command center	NAVSTAR	Navigation satellite timing and ranging
CC	Covert communications	NCC	Navigational command and control
CNN	Convolutional neural network	NFV	Network function virtualization
CNPC	Control and non-payload communication	NLoS	Non line-of-sight
CR	Cognitive radio	NOMA	Non-orthogonal multiple access
CSI	Channel state information	OFDM	Orthogonal frequency division multiplexing
D2D	Device-to-device	ORB	Oriented fast and rotated brief
DAG	Directed acyclic graph	OTFS	Orthogonal time frequency space
DC	Difference-of-concave	PCP	Poisson cluster process
DDOS	Distributed-denial of service	PoS	Proof of stake
DDPG	Deep deterministic policy gradient	PoW	Proof of work
DL	Deep learning	PRs	Passive receivers
DoS	Denial of service	PS	Power-splitting
DRL	Deep reinforcement learning	QoS	Quality of service
DSSS	Direct sequence spread spectrum	RF	Radio-frequency
DT	Decision tree	RNN	Recurrent neural network
EH	Energy harvesting	SAR	Search and rescue
ESC	Ergodic secrecy capacity	Sat-Com	Satellite communications
FANET	Flying ad-hoc networks	SCA	Successive convex approximation
FCSD	Fog computation-assisted swarm of drones	SDN	Software-defined network
FD	Full-duplex	SEE	Secrecy energy efficiency
FHSS	Frequency hopping spread spectrum	SINR	Signal-to-interference-and-noise ratio
FL	Federated learning	SNR	Signal-to-noise ratio
G2A	Ground-to-air	SOP	Secrecy outage probability
GCSs	Ground control stations	SR	Secrecy rate
GNs	Ground nodes	SSID	Service set identifier
GNSS	Global navigational satellite system	SWAP	Size, weight and power
GPS	Global positioning system	SWIPT	Simultaneous wireless information and power transfer
GV	Ground vehicle	TDMA	Time-division multiple access
HAPs	Higher altitude platforms	TS	Time-switching
HD	Half-duplex	UAVs	Unmanned aerial vehicles
HKS	Han-Kobayashi signaling	UEDs	UAV eavesdroppers
HMI	Human-machine interface	vFirewalls	Virtual-Firewalls
HSTNs	Hybrid satellite- terrestrial networks	vIDS	Virtual-intrusion detection system
IDS	Intrusion detection system	VSF	Virtual-network security function
IMT	International Mobile Telecommunications	WCNs	Wireless communication networks
IoD	Internet of Devices	Wi-Fi	Wireless fidelity
IoT	Internet of Things	Wi-MAX	Worldwide interoperability for microwave access
IoV	Internet of Vehicles	WMNs	Wireless mesh networks
IRNSS	Indian regional navigation satellite system	WPA2	Wi-Fi protected access 2
IRS	Intelligent reflecting surface	WSNs	Wireless sensor networks

- *Time Driven*: In a time driven scenario, the applications demand primarily for the UAV's capabilities to provide low latency and high fidelity performance.
- *Event Driven*: Event driven scenario consists of specific event-based applications that are required for a particular time duration. For example, the use of UAVs can offer early disaster predictions and expedite rescue and recovery missions in SAR operations. Furthermore, they can transport medical essentials to unreachable locations.
- *Space Driven*: Space driven scenario usually refers to applications over a fixed location that are repetitive in nature. For example, UAVs can be used in agriculture practices to assist in various mapping activities like crop

maturity, soil texture, field-tile, residue covering, crop yields, and tillage, and help in irrigation scheduling and detecting plant diseases.
- *Space-Time Driven*: Space-time driven scenario deals with applications over a fixed location and their operation demands for low latency and high reliability. This scenario covers many application domains, such as, military, remote sensing, natural disaster, etc.
- *Query Driven*: Query driven scenario requires continuous reporting of the status of any particular event or inspection of risky areas. For example, using UAVs can help to find faults in the gas pipeline, power line, power stations, etc.
- *Space-Query Driven*: In space-query driven scenario, continuous feedback of any events in particular locations is supported. Some examples of using UAVs in this scenario are delivery portals, e-transportation, and e-health [21].

Data sensing abilities of UAVs rely on embedded actuators or sensors, like heat, mechanical, radiation, and chemical. These sensors assist UAVs in interacting with environmental, geoscience, surveying, and geographic information disciplines. High definition cameras are another essential component of UAVs required for applications such as monitoring and SAR [22]. UAVs-assisted relay nodes and swarm networks utilize LoS connectivity and low path loss of the transmission channel to serve terrestrial users. Specifically, several vital attributes make UAVs a desirable contender to eliminate or supplement ground-based cellular networks [23]. They are as follows:
- *Adaptive Deployment*: Unlike the fixed terrestrial infrastructure, UAVs can be flexibly deployed in response to applications of real-time scenario that demand more resistance against environmental variations. Moreover, the inexpensive aerial BS-aided UAVs can reduce the requirement for large-size terrestrial antennas and multiple BSs.
- *Uninterrupted LoS Availability*: UAV's variable trajectory and operating altitude provide more reliable LoS communication links across large areas and remote locations, and hence a better way in serving terrestrial consumers.
- *UAV Swarm Networks*: UAV swarms can form an extensible multi-UAV networking platform that can offer pervasive interconnection to global coverage. A UAV swarm network is a viable alternative for quickly restoring and extending the cellular coverage area, thanks to its flexible design and rapid scaling features.

B. CHALLENGES IN ADOPTING UAVs

As discussed, the adoption of UAVs in different domains has enhanced performance and reliability of various systems and services. Nevertheless, the deployment of UAVs has raised a number of challenges which need to be addressed to realize their full potential [24]. These challenges are summarized below.

- *Airspace Regulations*: Airspace access is organized and enforced to assure the safety of manned aerial vehicles and boarded people. The deployment of mobile UAVs presents a crucial challenge in airspace regulations [12]. UAVs' spectrum regulation and maximum altitude should not affect air traffic. Thus, aviation regulatory bodies should provide a general agreement for UAV communications.
- *UAV-Core Inter-Network Link*: The next concern is how to support UAV's communication using existing terrestrial wireless networks, given that they are designed to serve ground users and devices rather than onboard mobile UAVs. The UAV's mobility and dynamic air-to-ground channel require rigorous investigation for UAV's connectivity setup.
- *UAV-Application Link*: Another issue is selecting appropriate wireless communication infrastructure like cellular or Wi-MAX for connecting UAVs to external networks. This is primarily influenced by the number of UAVs employed in the task, the mobile or static nature of UAVs, and application scenarios [13], [15].
- *Intra UAV-Network Link*: Although the UAV's flexible mobility offers enormous benefits, designing a flying ad-hoc network (FANET) to connect multiple UAVs is challenging due to the frequently varying channels and UAVs' mobility [25]. In particular, the frequent disruptions of neighboring UAVs need to be modeled dynamically, especially in mission-critical applications [26].
- *Network Congestion*: With multiple UAVs attempting to connect to a single BS, network congestion becomes inevitable unless the UAV access links are efficiently scheduled [27]. Moreover, the UAV networks can also be affected by intentional jamming and false injection attacks that may cause network failure due to UAV's inability to provide security measures against these threats.
- *Multi UAV Collisions*: In multi-UAV communications, the UAVs are generally piloted through predetermined routes that require physical collision avoidance and mission planning information [27]. The C&CC need to frequently update the geographical coordinates to efficiently control the remote UAVs.
- *Interference Management*: Interference and additive noise due to hardware impairments, cooperative UAV links, and malicious eavesdroppers need to be addressed for required reliability. Indeed, higher LoS availability to multiple BSs and transmitting antennas can create significant co-channel interferences in both uplink and downlink transmissions.
- *Security Threats*: Despite many benefits offered by high LoS availability and A2G wireless access, the transmissions to and from UAVs can suffer from serious security threats, leading to compromise on confidentiality and reliability of the information. Specifically, malicious receivers can intercept the UAV's A2G and A2A wireless channels to tap the transmitted signals, causing

information leakage. On the other hand, UAV-BSs communication links are vulnerable to jamming false injection attacks.

C. NEED FOR PHY SECURITY

Many IoT applications rely on 5G communication technologies, including mmWave, NOMA, and m-MIMO [2], [28]. UAVs have also emerged as an integral part of the communication links between IoT devices and cellular clusters. Owing to the dominant LoS links and mobility, UAVs are extensively used in diverse fields for different applications and objectives. However, the higher availability of LoS links makes UAV-assisted communications more vulnerable to various security threats as compared to terrestrial communications. Moreover, due to the strong LoS links between UAVs and ground/aerial intruders, data security and privacy become critical issues.

Compared to the wireless channels in the terrestrial infrastructure that predominantly suffer from severe path loss and heavy shadowing, the UAV-terrestrial communications experience better channel conditions owing to their dominant LoS transmissions. However, airframe shadowing can occur when the UAV itself obstructs the LoS signal while performing specific maneuvers following its predetermined trajectory. For characterizing the significant causes of airframe shadowing, such as aerodynamics due to UAV's structural design, sharp transitions in flight dynamics, and placement of on–board antenna and circuitry, an accurate and empirical model must be considered [29].

Furthermore, even a remote malicious UAV can intercept the strong A2G link to overhear the information transmitted from UAV-BS to the user equipment. The hostile UAVs can use their strong LoS links and flexible mobility to impose more severe jamming signals to legitimate users compared to terrestrial jammers with the same jamming signal power. In some cases, a terrestrial jammer can exploit the strong G2A link of the UAV to launch more severe jamming attacks by interfering with the UAV's control signals, thus detaching the UAV from its dedicated C&CC [30]. Also, a malicious node can utilize the dominant LoS link from the UAV to tap the confidential information of ground users/sensors. These attacks may degrade the confidentiality of the data or even cause a complete failure of the UAV-enabled communication system. This may degrade the confidentiality of the data or even cause a complete failure of the UAV system due to failure in retrieving the control data. Thus, both the aerial links (A2G and G2A) are much more susceptible to eavesdropping and jamming as compared to terrestrial-based infrastructures.

Recent studies have demonstrated that PHY security can be a feasible wireless security approach for UAVs and IoT interconnections [3], [4]. In a nutshell, PHY security can secure information by exploiting intrinsic characteristics of communication channels and ensuring that the legitimate link is less noisy than the wiretap link.

PHY security can support UAV-enabled wireless communication technologies in reducing authentication latency, particularly in roaming situations. For instance, the vehicles and UAVs in the UAV-assisted Internet of Vehicles networks are highly random in their positions [5]. In such networks, migrating through multiple access points or BSs causes repeated authenticating handoffs that may pile up to a huge handover validation overhead and thereby slow down the communication. In such scenarios, PHY security can offer a practical and immediate identification process by examining the radio frequency signals, simplifying the handoff procedure, and reducing authentication delays [6]. Moreover, PHY security techniques may be utilized as an additional security means, collaborating with existing security procedures to protect UAV-enabled cellular devices effectively.

Many innovative types of equipment from Industry 4.0 (a new phase in the industrial revolution) and IoT are spanning towards heterogeneous connections. It is not easy to accomplish effective key allocation and administration under such vast and diverse UAV-aided networks. With PHY security methods, key generation depends upon the stochastic nature of wireless channels that could ease this task [7]. Also, designing secure communication channels with the help of information theory can lead to the secure wireless transmission without encrypting and decrypting the data. However, integrating PHY security with new 5G wireless technologies faces several challenges to UAV-aided cellular communications. Massive MIMO, for example, requires accurate CSI to implement appropriate beamforming techniques. An intruder can undermine the channel prediction during the training phase and replicate and transmit the legitimate signals by imitating an authorized user. Consequently, the adversary may acquire a non-legitimate advantage over the subsequent communication phases [8].

The recently-emerged NOMA approach can provide extensive network connections and high spectral efficiency for UAV-enabled wireless cellular communications [9]. However, it is also prone to authorized user contamination-based threats, as in the case of massive MIMO. Because NOMA transponders may simultaneously interact with several legitimate users in identical channels, they are at high risk of being intruded and corrupted via pilot contamination threats. The superimposed and complex transmitting signals in NOMA [10] make it even more challenging for detecting and resisting these attacks. Moreover, enabling FD capabilities grants an active intruder extra freedom when executing jamming and eavesdropping attacks in wireless networks [10]. Nevertheless, the unique properties of 5G and B5G wireless technologies also assist PHY security with new potential to combat physical-layer vulnerabilities in UAV-enabled cellular systems. In some scenarios, large propagation losses and high directionality with mmWave communication systems can be exploited to prevent eavesdropping and spoofing intrusions [11]. Further, the different characteristics of mmWave and MIMO systems can be utilized to recognize legitimate user contamination threats in a UAV network [31], [32]. In addition, jamming attacks can

be circumvented using UAV-aided cellular devices embedded with in-band FD capabilities [19].

D. PRIOR SURVEY PAPERS

In recent years, many research studies have been conducted in the field of PHY security in cellular communication systems. On the other hand, key challenges concerning the use of UAVs for wireless communications are still a vast area to be pondered. Several survey studies have been carried out separately, focusing on each of these areas, to examine critical issues in UAV communications, like, trajectory optimization, scheduling the flight path, relaying, etc. Other works have focused on security threats, classifications, performance metrics, and mitigation techniques. The recent and relevant surveys are summarized in Table 2, which have constituted survey studies concerning security in cellular communications [3], [33], [34], [38], and key UAV technologies [21], [35], [36].

In [33], the authors have presented a survey on PHY security for the 5G communication technologies focusing on paradigms like MIMO, mmWave, NOMA techniques, etc. Nevertheless, the authors have not exclusively covered IoT applications and various upcoming 5G and B5G technologies, such as UAV-aided relaying and energy harvesting. Further, the authors in [3] have surveyed key technologies for PHY security in cellular networks and their classification along with mitigation methods. Likewise, the authors in [34] have highlighted the categories of threats in 5G communications and examined critical technologies, like NOMA, massive MIMO, and others. However, practical scenarios and applications are missing from this survey. A comprehensive study of the PHY security perspective of Sat-Com has been discussed in [38] by focusing on various challenges related to satellite-based IoT networks. Moreover, they have categorized state-of-the-art research works as integrated terrestrial networks, hybrid satellite to terrestrial relay networks, and terrestrial mobile to Sat-Com networks. However, UAV-assisted communication scenarios are not included in that study.

The authors in [35] have comprehensively covered a vast categorization of UAVs based on SWAP, along with their applications and potential challenges. They have also detailed the characterization of channel models, performance metrics, altitude and trajectory design of UAVs, etc. However, the security issues related to UAV networks have not been covered. By focusing on 5G and B5G communications, reference [36] has highlighted the requirements of UAV-aided mmWave communication systems. It has also covered UAVs' path and altitude designing aspects for performance improvement. A tutorial on UAV-assisted 5G and B5G wireless communication systems has been provided in [21] that discusses desirable network needs, channel models, and practical constraints. On the other hand, the authors in [37] have analyzed and reported the involvement of drones in mischievous deeds in both commercial and military applications. They have also presented a detailed scenario-based classification of UAVs.

It is pointed out that all these earlier works [3], [21], [33], [34], [35], [36], [37], [38] either covered the security aspects of terrestrial communication networks or highlighted the need and significance of UAV-enabled communications for emerging practical scenarios. These survey articles are summarized and compared with this work in Table 2 based on technological themes.

There are several survey studies on the security of UAV-aided communication systems [30], [39], [40], [41], [42], [43], [44], [45], [46]. In particular, the survey paper [39] has considered various cyber vulnerabilities on drones along with their mitigation techniques and defensive strategies. It has covered works on classifying the application scenarios based on channel encryption, providing secure and reliable firmware via monitoring, and overhauling corrupted components of the communication system hardware. Further, PHY security concerns in UAV communications related to active and passive eavesdropping attacks are discussed in [40]. Herein, the authors have pointed out various emerging techniques to secure UAV networks.

The authors in [41] have emphasized works on UAV-aided wireless networks and specific problems like aerial BS prototypes, cyber-security threats on cellular UAV systems, required third generation partnership project (3GPP) enhancements, and economics of UAV adoption in cellular networks. Yet, the paper has not covered mitigation techniques for threats in UAV-enabled communication systems. They have discussed the emerging vulnerabilities in exploiting the UAVs for malicious purposes in both military and civilian applications. They have also described a realistic scenario of a simulated attack performed on the drone.

The recent survey papers [30], [42], [43], [44], [45], [46] provide key insights into several emerging techniques for enhancing the secrecy performance of UAV communications. A survey report on the vulnerabilities and intrusions on the Internet of devices has been provided in [42]. Herein, the authors have presented a detailed taxonomy of intrusions on communication networks. However, recent technologies for mitigating the threats have not been included in their studies. In [43], the authors have discussed various security protocols utilized for securing UAV-enabled communications. They also discussed different vulnerabilities of existing security protocols. However, PHY security concerns and their mitigation techniques using UAVs are left unexplored. Also, emerging techniques like blockchain, fog-computing, and UAV-enabled PHY security methods are missing.

Similarly, [44] has extensively surveyed the active and passive security issues of UAVs at hardware, software, communication, and sensor levels and also presented possible mitigation techniques to protect UAVs from such vulnerabilities. Nevertheless, a detailed classification of security threats is not given. The authors in [30] have reviewed the security-critical applications of drones and security challenges such as man in the middle attacks, DoS attacks, de-authentication attacks, etc. They underlined SDN, ML, blockchain, and edge computing as solutions to security

TABLE 2. Surveys on PHY security/UAV communications.

Technological Theme	[33] (2018)	[3] (2019)	[34] (2019)	[35] (2019)	[36] (2019)	[21] (2019)	[37] (2020)	[38] (2020)	This survey
Threat taxonomy	✓	✓	✓					✓	✓
Satellite link	✓		✓	✓	✓	✓		✓	✓
UAV trajectory optimization				✓	✓	✓		✓	✓
Throughput evaluation	✓	✓	✓	✓	✓	✓	✓	✓	✓
Resource allocation							✓	✓	✓
3D scheduling				✓	✓	✓	✓		✓
UAV's application scenarios					✓				✓
Relaying schemes					✓	✓	✓		✓
Quality of service	✓	✓	✓	✓		✓		✓	✓
Energy harvesting	✓			✓					✓
Cooperative jamming schemes							✓	✓	✓
5G paradigms	✓	✓	✓	✓	✓	✓		✓	✓
Cyber protection schemes								✓	✓
Security and privacy aspects	✓	✓	✓					✓	✓
Mitigation taxonomy							✓	✓	✓
Blockchain technique		✓			✓			✓	✓
Covert communication									✓
Fog computing									✓
Software defined network								✓	✓
Machine learning	✓	✓	✓	✓	✓	✓	✓	✓	✓

TABLE 3. Surveys on security of UAV communications.

UAV-enabled key technologies	[39] (2018)	[40] (2019)	[41] (2019)	[37] (2020)	[42] (2021)	[43] (2021)	[44] (2021)	[30] (2021)	[45] (2021)	[46] (2021)	This survey
Threat taxonomy	✓		✓		✓	✓		✓		✓	✓
Satellite communications	✓				✓					✓	✓
UAV trajectory optimization		✓	✓	✓			✓				✓
Throughput evaluation and optimization	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Resource allocation and optimization		✓	✓	✓	✓		✓	✓	✓		✓
3D scheduling	✓	✓		✓	✓		✓	✓		✓	✓
Cooperative UAV strategies		✓		✓			✓			✓	✓
Proactive eavesdropping		✓					✓		✓	✓	✓
Relaying Schemes		✓		✓			✓			✓	✓
UAV's application and scenarios			✓				✓	✓			✓
Quality of Service	✓	✓	✓		✓	✓	✓	✓		✓	✓
Energy harvesting		✓						✓	✓		✓
Cooperative jamming schemes							✓		✓		✓
5G communication technologies	✓	✓	✓	✓			✓				✓
Cyber protection schemes			✓		✓	✓	✓	✓		✓	✓
Security and privacy aspects	✓	✓	✓	✓	✓	✓			✓	✓	✓
Mitigation classification					✓			✓		✓	✓
Blockchain technique		✓		✓			✓	✓	✓		✓
Covert communication								✓	✓		✓
Fog computing								✓	✓		✓
Software defined network		✓		✓			✓	✓	✓		✓
Machine learning	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

issues of drones. But, UAV-enabled PHY security methods like trajectory design, resource allocation, and multi-UAV relaying have not been discussed.

The authors in [45] have surveyed techniques such as ML, blockchain, and watermarking for securing UAV-assisted application scenarios. Likewise, [46] has highlighted works on the UAVs' current developments and PHY security of UAV-aided communications. They have summarized the widely-utilized secrecy performance metrics for secure UAV communications and commonly-adopted methods to enhance security. However, the study has not covered emerging techniques like ML, NOMA, beamforming, etc.

The above survey articles on UAV-based secure communications are summarized in Table 3, which gives the reader a quick glance to find the technical focuses of these surveys, along with the featured contributions of this survey work.

E. OUR SURVEY CONTRIBUTIONS

Motivated by the existing works discussed above, this comprehensive survey focuses on the PHY security concerns related to UAV-aided wireless communication systems. With special attention to state-of-the-art technologies, the paper presents an in-depth literature survey on mitigating threats with proactive security techniques merged with emerging cellular communication technologies like mmWave, NOMA, massive MIMO, cognitive radio, etc. Moreover, a descriptive taxonomy of the most critical security threats on UAV networks is also laid out. We believe that this comprehensive survey can be a handful resource for researchers who have

a keen interest in state-of-the-art threat mitigation techniques in UAV communications. The main contributions of our work are as follows:

- We provide a detailed background of different security attacks like navigational, data injecting, software installation, etc., along with secrecy performance metrics adopted in recent research works.
- An in-depth classification of existing and anticipated threats in the UAV networks is provided.
- We perform an up-to-date exhaustive review of realistic and effective mitigation solutions for secure UAV communications in different domains, like defense, maritime and satellite communications, IoT applications, etc.
- Different from existing surveys, the mitigation techniques are comprehensively and clearly discussed by sub-categorizing them into UAV-assisted counter methods and B5G paradigms, cooperative networks using UAV swarms, and various emerging techniques. Moreover, critical insights into each category are provided.
- In the later part of the survey, based on the advantages, drawbacks, and crucial challenges in existing and emerging technologies for security enhancement, we elaborate on several future research directions in this domain.

The survey is organized as follows. After a brief introduction to the UAV's intervention and requirement of PHY security, Section II introduces definitions of vulnerabilities in wireless networks and common secrecy performance metrics. Section III provides a detailed categorization of security threats on UAV-aided communications. Sections IV, V, VI, and VII are devoted to surveys on the most recent research done on intrusion mitigation methods based on proactive measures, multi UAV-aided co-operative methods, NOMA and beamforming methods, and several emerging techniques, respectively. In Section VIII, future research directions related to UAV-enabled communications are highlighted, along with a figure summarizing the future directions and aspects. Section IX summarizes and concludes the paper.

The table of contents showing the organization of this survey is depicted in Fig. 2. The list of acronyms used in the paper are summarized in Table 1.

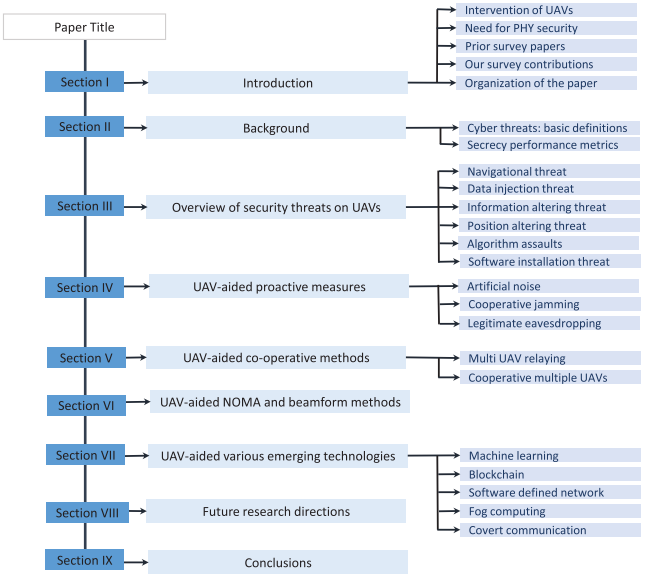

FIGURE 2. Organization of the survey.

II. BACKGROUND

UAV-aided wireless networks can be designed to serve a massive number of ground users and augment existing communication frameworks. Specifically, UAVs can operate as aerial BSs, relay nodes, and form swarm networks to serve various application scenarios, such as vehicular communications, naval communications, cellular communications, and hybrid satellite communications. In addition to these scenarios, they can form the backbone for upcoming generations of cellular networks, smart cities, military and agricultural activities, remote monitoring, and e-health applications.

A cellular wireless communication system can extend its coverage area with the aid of UAV-based mobile aerial BSs and swarms relay nodes. In order to enhance the system performance, multiple UAVs are employed instead of a single UAV. With the help of FANETs, UAVs can perform far-off missions like emergency SAR, surveillance, and providing backup to interrupted cellular infrastructure. In Fig. 3, UAVs swarm-assisted naval communication is depicted. Unlike the UAV-terrestrial user link, the UAV-maritime communication channel is affected by signal attenuation due to climatic change in the sea, seawater fluctuations, irregular sea surface, and waveguide impacts due to temperature, pressure, and humidity of the troposphere over the sea. Thus, accurate UAV-ship channel, UAV's trajectory, topology, and task-scheduling need to be jointly optimized to acquire reliable UAV-naval communications [27].

However, due to the unmanned nature of UAVs and the requirement for remote wireless communications, security becomes one of the most critical issues. A UAV-based BS is more prone to network failure than a terrestrial BS when a suspicious object intrudes on it. As such, it is critical to safeguard the UAV-based connections from both cyber and physical-layer prospects.

A. CYBER THREATS: BASIC DEFINITIONS

In recent years, cyber attacks have substantially raised on the UAVs as their use in various applications gained popularity [47]. The dominant LoS UAV radio access links are more prone to radar intrusions. They contain access commands and valuable information like navigating locations, CNPC signals, routing and networking details, etc. For example, an intruder can steal the transmitted data or hack the UAVs by accessing the command signals and manipulating them, thus affecting the reliability, secrecy, and QoS of UAV-assisted communication infrastructure. Besides, the A2G channel between UAVs and terrestrial users has low path loss that increases the probability of intrusion. Therefore, a large

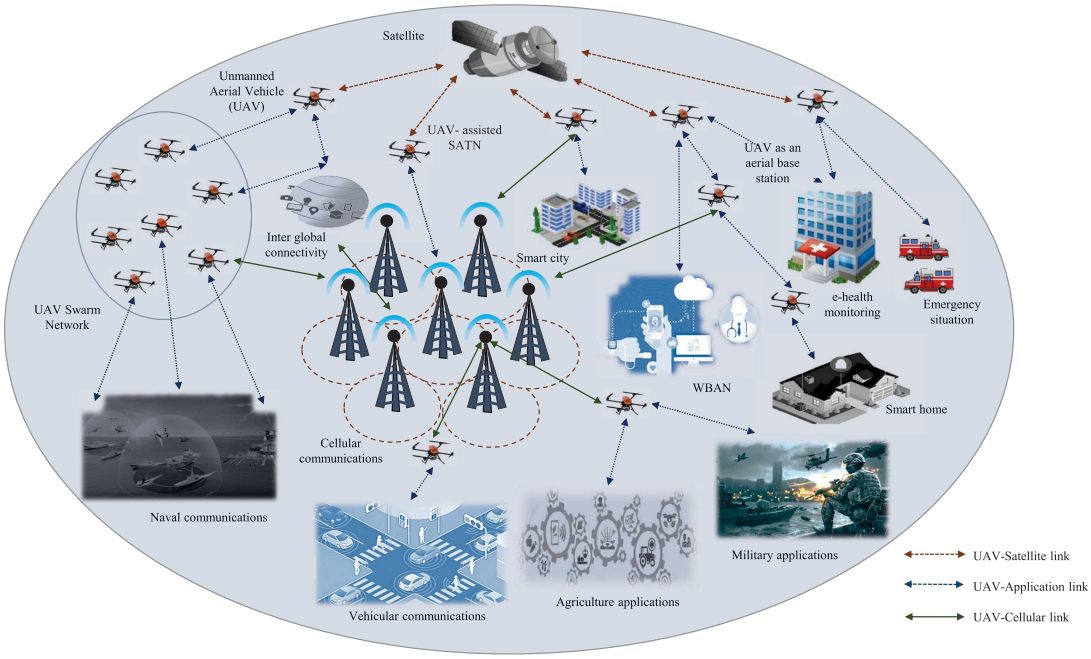

FIGURE 3. Potential application scenarios of UAV-enabled communication networks.

portion of research has been carried out in the last decade to secure radio links and reduce the risk of communication link failure. Threats associated with these networks are elaborated below to highlight the overall risk level of radio links in practical scenarios.

1) EAVESDROPPING

Eavesdropping is a typical security threat in which the aerial or terrestrial intruders secretly intercept the confidential information exchange between two legitimate nodes. This type of security threat impacts the secrecy leakage and gains access to the source and destination nodes, personal data like access codes, control commands, navigational details, etc. For example, FANETS and cellular communications can be attacked by nearby intruders, which may be difficult to identify as they do not transmit any signal and hence cause an adverse effect on the security of the communication network [34]. More sophisticated PHY security schemes can be a general solution, and further encryption can shield against eavesdropping.

2) JAMMING

The jamming attack blocks legitimate communication links and disrupts the information exchange between legitimate nodes by transmitting interference or jamming signals [48]. In jamming, the attacker generates interference signals and transmits them in the same frequency band, which degrades the SINR at the legitimate destination node. This affects the reception of the original data and causes a delay for the responder to acknowledge the response. UAV's easily accessible A2G link and high radial coverage can be exploited by either malicious aerial or terrestrial intruders to jam the communication link. A report based on GPS jamming has been presented in [49], which examines the crashing of a small drone in 2012. The legitimate user was perceived to be responsible, but later on, the suspect was identified. Several algorithms have been developed that estimate the probability of intrusions and their impact on the received data. Increasing the SNR is a robust first line of defense against jamming. However, the energy constraint of UAVs limits the transmitted signal power and practical receiver algorithms to reduce noise at the receiver.

Considering the UAV's energy constraints, the authors in [50] examined the performance of jammer nulling transmit-adaptive energy-constrained waveforms for UAVs to suppress the jamming signals generated by the sweep jammers and base jammers. Broadly, jamming attacks can be classified as pilot jamming, proactive jamming, and reactive jamming. Pilot jamming is the most common jamming attack in which the channel training phase of the legitimate link is corrupted by introducing the jamming of the pilot signals. In proactive jamming, the intruder continuously transmits the interfering signals over the same communication channel without knowing the legitimate nodes. However, the jammers sporadically spread either standard data or random bits into the networks to toggle between the jamming and sleep phase in order to save their energy. Proactive jamming is the most sophisticated among the others in which reactive jammers closely monitor legitimate nodes' activity and then adversely transmit the jamming signals.

3) DENIAL OF SERVICE (DoS) ASSAULT

In this type of threat, the adversaries transmit the copies of a large number of service interrupts to the wireless access point

of the legitimate network to increase the network congestion. These interrupts can be in the form of service requests, acknowledgments, unknown source advertisements, or sometimes spoofing copies of signals [51]. This can cause the terrestrial BS to delay in providing the service or control and command replies to UAVs. The attacker can launch a security attack on the legitimate UAV nodes, resulting in losing the service from the legitimate service provider. DoS can be performed by either malicious UAVs through enhanced radial coverage (operating at high altitudes) or by the terrestrial attackers exploiting a strong LoS link. DDoS attack is a class of DoS attack that is initiated from synchronized multiple systems to attack a single target.

An experiment was carried out in [52] to show how a software, Telnet, can be utilized for clogging the UAV to controller network link of the ARDiscovery process (i.e., linking the UAV with its legitimate controller) with multiple copies of requests to gain the controlling of the UAV. DoS or DDoS attack can be followed by de-authentication attack, that try to gain access to the authentication process that a legitimate user uses to verify its identity, service, or application.

4) HIJACKING

The term hijacking means ''to attain the full control ove''. When the wireless link is hijacked, the intruder gets full access to the link. For instance, the access and communication links between UAV nodes and GCS are Wi-Fi connections. Adversaries could first use de-authentication management frames to dissociate a drone from its associated GCS to initiate a hijacking attack. Further, it can remotely control the drone via IEEE 802.11 protocols. Numerous security techniques exist to protect against de-authentication attacks. Practical detection algorithms and encryption of transmitted frames are possible. The authors in [53] have recommended that with an appropriate key length, WPA2 encryption (802.11i 2004) can work as a countermeasure to hijacking. On the other hand, the work in [54] has demonstrated that encryption with dynamic secret key shields an additional layer of defense against attackers. Furthermore, the Wi-Fi-connected UAV can be protected by restricting the MAC address that conceals the Wi-Fi access points, whereas the Wi-Fi links can be shielded from intruders by not allowing SSID broadcast.

5) SPOOFING

Spoofing attackers inject the forged identity information into the legitimate communication link to corrupt or gain access to the data. It uses an incorrect deceiving signal with high power to get control over the source nodes [55]. Common spoofing attacks include access to emails, phone calls, IP addresses, cache poisoning of the address resolution protocol, etc. At the same time, GPS spoofing is common in UAVs, which is carried out by transmitting high-power unauthorized signals in the frequency band of operation. Thus, with GPS spoofing, an intruder can access personal information, change GPS locations, or spread a virus in the system. Identity spoofing and Sybil attacks are the two common spoofing attacks. In identity spoofing, the intruder can claim itself as a legitimate user by using the fake MAC or IP address of the legitimate user in the network [5]. With this, the intruder can launch more sophisticated attacks like man-at-the-center and DOS attacks after gaining illegal access. Whereas in Sybil attacks, a single malicious device can impersonate arbitrary false identities claiming as additional nodes [56]. The authors in [52] have demonstrated a spoofing attack by ARP acknowledges, which they continuously transmitted from a genuine MAC address.

B. SECRECY PERFORMANCE METRICS

The secured UAV-assisted communication is required for many applications such as mission-critical communication, healthcare monitoring, defense applications, and so on. Most research works in this domain focus on evaluating the secrecy metrics and optimizing them to achieve reliable communication. The secrecy performance metrics that are most commonly used are summarized in this section.

1) **Secrecy Rate** (R_s)**:** This metric is defined as the difference between the achievable data rate of the legitimate channel and that of the eavesdrop channel. It is expressed as [38]

$$R_s = [R_b - R_w]^+, \tag{1}$$

where $[x]^+ = \max[x, 0]$, $R_b = \log_2(1 + \gamma_b)$, and $R_w = \log_2(1 + \gamma_w)$. Here R_b is the achievable rate of the UAV's legitimate link and R_w is the rate of the wiretap link. Further, γ_b and γ_w are the instantaneous SINRs of the signals received over the legitimate and wiretap channels, respectively.

2) **Secrecy Outage Probability (SOP):** This metric is utilized for quantifying the likelihood of the condition in which secured transmission is not guaranteed in the UAV-aided system design. Secrecy outage occurs when the instantaneous secrecy rate R_s is less than the target rate R_t (in bps/Hz). The SOP is evaluated as

$$\mathcal{P}_{out}(R_t) = \Pr[R_s < R_t]. \tag{2}$$

3) **Secrecy Capacity** ($\mathcal{C}_s$)**:** It is defined as an upper bound for the transmission data rate up to which the secrecy of the information exchange between legitimate users can be guaranteed in the presence of an eavesdropper link. For AWGN channels, secrecy capacity is the difference between the legitimate channel capacity and the wiretap channel capacity:

$$\mathcal{C}_s = \max[I(X, Y_d) - I(X, Y_e)]^+, \tag{3}$$

where X is the channel input at the source node, $I(X, Y)$ denotes the mutual information, while Y_d and Y_e are the channel outputs at destination and eavesdropper nodes, respectively.

4) **Ergodic Secrecy Capacity (ESC):** The ESC can be defined as the rate below which any average secure

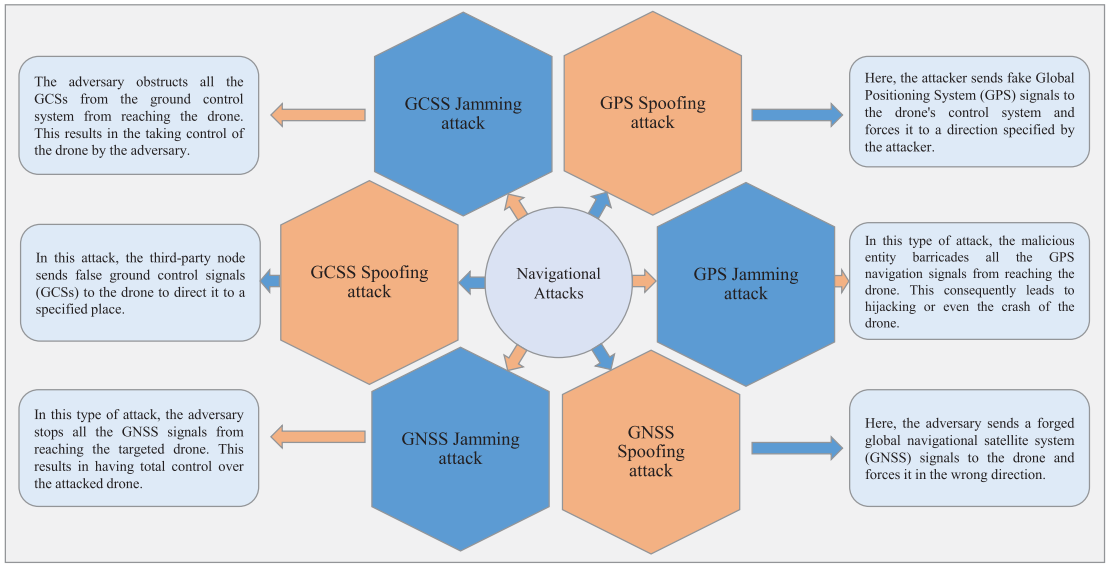

FIGURE 4. Description of different navigational attacks.

communication rate is achievable. Mathematically, it can be expressed as

$$\mathcal{E}_s = \mathbb{E}\{[\mathcal{C}_b - \mathcal{C}_w]^+\}, \tag{4}$$

where $\mathbb{E}\{\cdot\}$ is the expectation operator, $\mathcal{C}_b$ and $\mathcal{C}_w$ are the Shannon capacities of legitimate and wiretap channels, respectively.

5) **Intercept Probability** ($\mathcal{P}_{\text{IP}}$)**:** Intercept probability denotes the probability of the occurrence of an intercept event. In other words, it estimates the probability that the eavesdropper is able to intercept the information. This occurs when wiretap channel conditions are more reliable than the main channel conditions. Thus, it can be mathematically expressed as

$$\mathcal{P}_{\text{IP}} = \Pr[\mathcal{C}_b - \mathcal{C}_w < 0]. \tag{5}$$

6) **Secrecy Energy Efficiency (SEE):** The secured communication from the energy-constrained UAVs requires energy-efficient strategies to solve security-related threats jointly. SEE is a crucial metric for such energy-constrained systems. It is defined as the ratio of the transmitted secrecy bits and the energy consumed, expressed as

$$\eta_{\text{SEE}} = \frac{R_b}{E_{\text{tot}}}, \tag{6}$$

where E_{tot} is total energy consumption of the system.

7) **Achievable Secrecy Diversity Order** ($\mathbb{D}$)**:** The SOP and ASR are related by the expression, $P_{\text{out}}(\text{SNR}, R_t) = \Pr[R_s(\text{SNR}) < R_t]$ [57], where R_t is the threshold secrecy rate. The ASR provides a lower bound of the transmission rate of information, which can also be utilized to obtain the achievable secrecy diversity order as

$$\mathbb{D} \triangleq \lim_{\text{SNR}\to\infty} \frac{-\log P_{out}(\text{SNR}, R_t)}{\log \text{SNR}}. \tag{7}$$

III. OVERVIEW OF SECURITY THREATS ON UAVs

The risk levels at the cellular, satellite, and Wi-Fi communication links can be classified as low, medium, and high based on different transmitting bit frames and encryption methods employed for these links. The authors in [58] analyzed a multi-tier network that employs UAVs as relays to bridge cellular connectivity between satellites and terrestrial BSs and found that UAVs are more prone to Wi-Fi controlled threats. There are two scenarios in that data can be under threat: (i) when two different frequency bands are utilized for CNPC and information transmission, and (ii) CNPC broadcasting and data access are done via the same radio links. Apart from cyber attacks, adversaries can also physically target the UAVs, adding another security concern for UAV systems. To launch the physical attacks, initially, the intruders are required to obtain access to UAVs, which they can acquire by ensuing any of the following two steps. The first is finding the damaged UAV on the ground due to any possible means such as the drained battery, colloidal damage, physical attack, or loss of trajectory. Another method of accessing the UAVs is by launching different cyber-attacks, which are more likely to be used by the intruders. Based on the two categories of attacks introduced by the intruders for having illegal control over the UAVs, the authors in [59] have summarized the attacker's capability levels for launching the data theft.

1) *Low Complexity Level:* With the deployment of UAVs at remote locations or some restricted places for undercover surveillance, the attacker can locate the UAVs and gain access to their internal data by using physical attacks like caging or assaulting. After accessing

the UAV, easily available interfaces like USB, pen drives, etc., can be used to access the information. To protect confidential data, these UAVs must be equipped with self-destruction mechanisms that can be activated under predefined circumstances. However, self-destruction should be used sparingly due to its severe consequences, which include a potential threat to public safety and the loss of both data and drones [60].

2) *Medium Complexity Level:* After accessing the UAV through a physical attack, intruders can acquire the data from the UAVs using highly standard interfaces, such as the JTAG, and through embedded system decryption. However, the UAV's data can be encrypted to secure it in such circumstances. Although encryption may only prolong the time for data loss, it can provide an extra level of defense and can get activated through the acknowledged command by the MSCs [61].
3) *High Complexity Level:* When the aerial or terrestrial intruders launch sophisticated cyber attacks, such as side-channel attacks, fault injection attacks, software attacks, etc., into the legitimate UAV's link, UAVs should be equipped with advanced cryptographic mechanisms and secure key management to combat such attacks [62]. These attacks are complex to execute as they are supposed to surpass the security levels of the legitimate link to overhear the transmitted information.

PHY security adds an extra guard to UAVs against the eavesdroppers who aim to attain unofficial control over them. The integrity, confidentiality, privacy access, and navigation threats can be categorized by grouping basic cyber attacks. These grouped threats are essential to be identified and mitigated. A lot of research work has been done in this area. This section shall briefly review some of the studies done on the classification and mitigation of these threats.

A. NAVIGATIONAL THREATS

The navigational signals from GNSS play a vital role in determining the locations of the UAVs, thus allowing the C&CC to monitor their trajectories, altitudes, and the presence of any suspicious object approaching them [63]. GNSS is a broad term comprising several satellite-based positioning, navigation, and timing systems such as USA's GPS, European Galileo, Chinese BeiDou, and India's IRNSS. A summary of different types of navigational threats is provided in Fig. 4, as also highlighted in [42]. Details of different forms of navigational attacks on GPS [64], [65], [66], [67], [68], [69], [70], [71], [72], [73], [74], [75], [76] and GNSS [63], [77], [78] along with their countermeasures are summarized in Table 4, constituting a survey of recent research works on both the analysis of the threats and mitigation techniques.

B. DATA INJECTING ATTACKS

These are the localization threats related to injecting wrong data into the legitimate command or information signals transmitted from C&CC to the UAVs. Under this attack, the UAVs become unable to differentiate between original or unauthentic data transmitted by the intruder present in their coverage area [43]. Examples of data injecting attacks are cross-site scripting, Structured Query Language injections, operating system command injection, code injection, host header injection, etc. Data injecting attacks can be categorized into false data injection and generic false data injection attacks, which are discussed as follows.

1) FALSE DATA INJECTION ATTACK

The unauthorized attacker aims to manipulate the predefined UAV's trajectory measurements by transmitting the false copies of direction estimated signals communicated by C&CC to the UAVs. Due to the tampered direction state estimation, the UAVs follow deviated trajectories that make them untraceable for the C&CC.

2) GENERIC FALSE DATA INJECTION ATTACK

These attacks are just a subpart of a false data injection attack in which an intruder can tamper with the UAV's location and trajectory estimation data in a particular range [80]. The trajectory and altitude of the UAV are primarily targeted in this type of attack, thus affecting the performance and QoS.

C. DATA ALTERING ATTACKS

The intruders launch this attack to acquire control over the UAVs by altering the control signals transmitted through the legitimate link and stealing or tampering with the information signals. These attacks can be categorized as follows.

1) MAN IN THE MIDDLE ATTACK

In this attack, an unauthorized node starts operating between C&CC and the UAV to access the control signal, acknowledgment messages, and information signals transmitted from the control center through the legitimate link [81]. Then, it secretly transmits the tampered information to the UAVs and replies to the C&CC with the false acknowledgment message received from the UAVs. Thus, compromising the control of the legitimate command center over the UAVs and also results in the loss of confidentiality of the information.

2) ACTIVE EAVESDROPPING ATTACK

The active eavesdropper intercepts the information exchange between C&CC and the UAV through a wiretap link. Although an active eavesdropping attack is similar to the man in the middle attack, it is limited to only accessing the information rather than tampering with the data [82]. The attacker can eavesdrop on confidential information after accessing the link. Additionally, to mislead the controller that is communicating with UAVs, the attacker sends the false acknowledgment replies to the C&CC [83].

3) WORMHOLE ATTACK

This attack creates two or more malicious nodes near the terminals of the legitimate communication link. With a

TABLE 4. Research studies on mitigation techniques for navigational spoofing threats.

WORK	OVERVIEW	OBJECTIVE AND MITIGATION TECHNIQUE					
		Devised system	Maximizing SINR	Maximizing tracking performance	Energy constraints in system model	Maximizing accuracy and probability of detection	Optimizing UAV trajectory and altitude
[78]	Reviewed the GNSS employed in UAV systems and proposed spoofing detection for multiple-UAV systems	Flat form blockchain	✓	✓	✓		✓
[64]	Developed a UAV model for detecting GPS spoofing	Decision rule scheme	✓	✓	✓		✓
[65]	Analyzed One Class SVM applied to navigation data for UAV	Fusion algorithm			✓	✓	✓
[66]	Analyzed effects of GPS spoofing attacks on a UAV	Software in the Loop (SITL) simulator and Extended Kalman Filter (EKF)	✓	✓	✓		✓
[67]	Proposed a neural network based method to detect GPS spoofing	Neural network based algorithm	✓		✓	✓	✓
[68]	Collaborative approach to assist UAV control systems in detecting GPS spoofing attacks as observed	Hidden Markov model		✓	✓		✓
[79]	Described a portable system capable of diverting unauthorized UAVs using GPS spoofing techniques	Software Defined Radio (SDR)	✓	✓	✓		✓
[69]	Covert spoofing algorithm of UAV based on GPS/INS (Integrated Navigation System) was studied	GPS/INS integrated navigation			✓	✓	
[70]	Proposed a model to mitigate GPS spoofing that targets UAVs	Stackelberg game problem	✓	✓	✓		✓
[71]	Proposed a vision-based method to detect GPS spoofing in UAVs	Root mean square error (RMSE) model of comparison			✓	✓	✓
[72]	Analyzed security and safety measures in the HAMSTER architecture to detect GPS spoofing in UAVs	HAMSTER architecture		✓	✓		✓
[73]	Threat detection method was modelled, analyzed and evaluated for spoofing	Detection matrix modelling		✓	✓		✓
[74]	Proposed an index system of UAV navigation spoofing effectiveness evaluation from three aspects of system devices	Fuzzy evaluation, Hierarchy analysis	✓	✓	✓		✓
[75]	Presented a device to detect and localize GPS spoofing attacks targeted at aircraft and UAVs	Crowd-GPS-Sec model			✓	✓	✓
[76]	Devised a model that provides effective navigation functionalities by exploiting jamming signal to the drone	JAM-ME navigation system		✓	✓	✓	

low-latency tunnel, these nodes are more likely to be selected as the intermediate nodes for the optimal path by the C&CC for data transmission. Upon considering them for the channel's preferred and shortest route, the attackers can overhear the data transmitted to the intended UAV from the C&CC or vice versa. Moreover, the attacker can falsify it and sends the manipulated data to the UAVs [84]. These threats are more severe in VANETS, FANETS, and other ad-hoc networks, as they can conduct a DOS attack that can cause disrupting the network's routing.

D. POSITION ALTERING THREAT

These are other types of localization error attacks intended to alter the remotely located UAVs' path and trajectory predicted information. The falsified data can affect the UAVs' service performance, hinder the reception of command and control signals from the controlling base, and in the worst case, lead to losing control over the UAVs [84].

1) EXTENSION ATTACK

The attacker alters the UAV's original path by making it appear longer than what is accurately estimated by the associated C&CC. This results in delivering the information or command signals to the targeted UAV earlier than the predetermined time, thus causing a loss of synchronization between UAVs and C&CC.

2) CONSTRICTION ATTACK

Opposite to the extension attack, the intruder alters the actual path or trajectory of the UAV by making it appear shorter than

what is initially estimated by the C&CC, which transmits the control or information signals to the intended UAV.

E. SOFTWARE ASSAULTS

The malicious algorithms are developed to attack the generic algorithms of the UAV's operation, thus intruding on the confidential data transmitted by the UAV in the communication network.

1) AUTOPILOT ASSAULT

The intruder exploits flaws in the UAV's state estimation model to drive a remotely deployed automated UAV to a deceptive flight trajectory. The attacker disrupts and attempts to access navigational control of the targeted UAV with the aid of false state insertion [85].

2) ACOUSTIC ASSAULT

With the motive of redirecting the targeted UAV from its original trajectory, the attacker utilizes a mischief drone integrated with speakers capable of generating a noise signal distinct from the gyro's resonating frequency of the legitimate UAV. As the gyroscope is incapable of filtering out the noise component, the audio command-based trajectory controlling algorithm of the intended UAV gets spoiled. Thus the UAV deviates from its legitimate path [42]. The UAV's state estimation is solely responsible for its functionality and controlling these types of threats. There have been various research works to develop an advanced UAV gyroscope capable of isolating large bands of noise frequencies.

F. SOFTWARE INSTALLATION THREATS

Software attacks have emerged as the most prominent security concerns that have severe effects, extended duration, and high adaptability. Cyber security is often overlooked in the design and implementation of UAV-aided communication systems, making them prone to cyber threats or software-based attacks. The control and command signals delivered from the controlling center are responsible for operating UAVs, and they are a common target of software attacks [42]. The malicious software is installed in the UAV's authentic algorithms and deploys viruses in the UAV-BS network. These viruses control and disintegrate the UAV from the command base station, thus affecting the confidentiality and reliability of the information. The software-based attacks are classified as Snoopy, Sky jet, Skyjack, and Maldrone attacks, which are summarized in Fig. 5.

Numerous algorithms and analytical models explored in the literature can mitigate these software attacks, but their performance varies depending upon the system models and the types of threats. Table 5 summarizes recent research works [86], [87], [88], [89], [90], [91], [92], [93] carried in the field of secrecy improvement and cyber attack analysis.

IV. UAV-AIDED PROACTIVE MEASURES

This section summarizes recent research works that focus on enhancing the secrecy of information using different

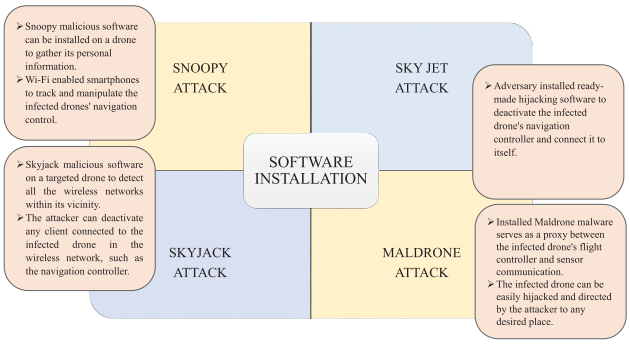

FIGURE 5. Different software-based attacks on UAVs.

physical-layer techniques for various application scenarios. Several proactive methods like friendly AN transmission, cooperative jamming, and legitimate eavesdropping have been utilized to improve system security. These methods have been exploited in different system models in conjunction with various communication technologies such as m-MIMO, mmWave, MEC, etc. Further, UAV's flexible mobility, dynamic routing, and dominant LoS link play important roles in trespassing the eavesdropper's link.

A. ARTIFICIAL NOISE-AIDED PHY SECURITY

This section discusses one of the most popular PHY security techniques that utilize AN. In this method, the eavesdropper's channel is intentionally deteriorated by transmitting artificial noise along with information signals, as illustrated in Fig 6.

Several research works [94], [95], [96], [97], [98], [99], [100], [101], [102], [103], [104], [105], [106], [107], [108], [109], [110], summarized in Table 6, have emphasized the need to employ AN to secure communication at the physical layer. Specifically, the authors in [94] have investigated a wiretap channel where a reliable network was established between the multi-antenna transmitters and a single-antenna UE relay node. The unauthorized active eavesdropper interrupts the communication in the FD mode. The source transmitter utilizes AN to confuse the suspected attacker. Further, the power allocation factor and the UAV's operating altitude are optimized simultaneously to obtain the minimum outage probability. As a continuation of [94], the authors in [95] have considered a similar network model and analyzed the asymptotic hybrid outage probability and secrecy rate with multiple transmitting antennas. They inferred that the secrecy performance could be enhanced by selecting the number of transmitter's antennas and adjusting the UAV's height against the eavesdroppers. They also concluded that for the low power signal transmission, jamming could be more hazardous than eavesdropping.

The authors in [96] have explored a swarm of UAVs enabled with coordinated aerial multi-points and assisted with AN for secure communication against the eavesdroppers. The power allocation and trajectory of the transmitting UAV are analyzed. Both large-scale and small-scale fading effects are modeled in a composite channel. But due to the

TABLE 5. Summary of recent research studies for mitigation of cyber threats.

WORK	OVERVIEW	OBJECTIVE	MITIGATION TECHNIQUE	KEY METRICS
[86]	Analyzed MAVLink (micro-air-vehicle) communication protocols for GCS-based control of UAVs	To analyze the vulnerability of the MAVLink protocol	Disable attack methodology for protecting an ongoing mission	Security parameters
[87]	Closed-loop cognitive control cycle was studied for a UAV network and a management cloud	To evaluate abnormal power emission posed to UAVs	Cloud based surveillance model Ternary hypothesis test Neyman-Pearson test criterion	Abnormal power emission; False alarm and missed detection; Local decision regions; Global decision threshold
[88]	Data packet transfer between the UAV and sensor nodes was investigated	To improve the reliability of collecting data packets and reducing the data redundancy	Trust-Based Active Detection (TBAD)	Reliability of data packets; Trajectory and path; Trust of sensor nodes
[89]	Blockchain based data acquisition process for UAV relays	To show the feasibility of a blockchain based data acquisition process	Blockchain at MEC server	Secrecy parameters; Server validations
[90]	Designed UAV security network intruder game for a random UAV operator and a random interdictor	To model and analyze the cyber-physical security of time-critical UAV applications	Cumulative prospect theory Classical game theory optimal path selection policy	Locations and trajectory; Mission duration time
[91]	Advanced persistent threat (APT) malware on UAVs-based communication with C&C	To detect and mitigate APT malware	String matching based periodicity detection; Fourier transformation based periodicity detection	Domain Name System (DNS) attack; Payload command and control server
[92]	Considered autonomous UAVs, whose behaviors are regularly monitored by a set of distributed observers (DOs)	To detect UAVs' abnormal behavior in a real-time manner. To distinguish abnormal activities due to real attacks	UAV trust chain based on blockchain time-stamped series	UAVs trust scores; UAVs trajectory
[93]	The UAV-GS and UAV-UAV authentication model was designed	To analyze various security features such as mutual authentication, user anonymity etc	Physical Unclonable Functions (PUFs) for UAV-GS authentication	Masquerade, replay, node tampering and cloning attacks

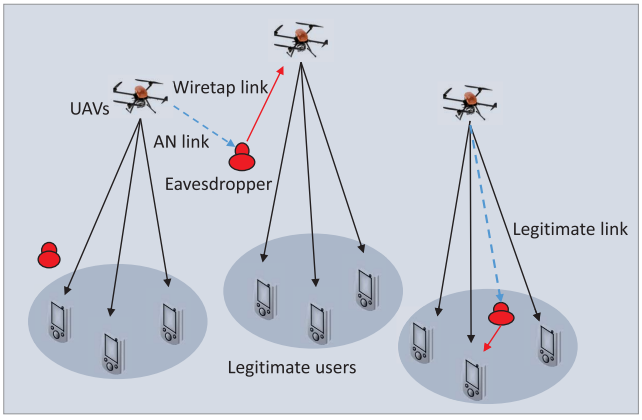

FIGURE 6. System model for UAV employing AN for secure communication.

difficulty in obtaining the perfect CSI of the attacker and legitimate receivers, large-scale fading is taken into account for secrecy throughput maximization. They further developed a non-convex problem formulation in which the signal transmission power and the AN power are considered. Further, [97] considered the random jitter caused by the UAV's vibration and wind turbulence that occurred in an energy-constraint air-to-ground downlink secure communication system. Specifically, they analyzed power allocation and minimization of signal transmission power for the USB nodes handling secured communication between legitimate users. Additionally, the effects of key parameters such as UAV's trajectory, attacker's location, minimum data rates, and UAV's azimuthal angle of departure were mathematically quantified. It has been shown that the optimal height and power allocation provide secured communication against eavesdroppers and other threats. The effects of variations in the model attributes on the total transmission and information signal power are summarized in Table 7.

In [98], the authors have considered HKS for the PHY security in a UAV-enabled multiuser communication system, which outperforms NOMA as well as orthogonal multiplexing techniques in terms of system throughput. In this model, the difficult task of adding the AN in the user's null space channel is performed, and a secure model is procured for single-antenna UAVs. A convex problem is formulated to maximize the minimum secrecy throughput by joint optimization of bandwidth, power, and time. The path-following algorithm is efficiently utilized to solve the optimization problem along with an inner approximation algorithm. Although the model shows impressive results, designs of the UAV's path and altitude were not considered.

Furthermore, the authors in [99] have jointly optimized the power splitting factor and UAV's trajectory to maximize the minimum ASR with the consideration of AN. The formulated problem was non-convex, which was tackled by an iterative method that uses alternating optimizing procedures and SCA algorithms. While considering both UAV's energy

TABLE 6. Summary of recent research studies for mitigation techniques using artificial noise.

WORK	SYSTEM MODEL	NATURE OF OPTIMIZATION TECHNIQUE AND OBJECTIVE					
		Problem formation and solution category	Minimizing the hybrid outage probability	Maximizing the secrecy throughput	Optimizing the power splitting factor	Maximizing the minimum secrecy rate	Optimizing the UAV trajectory and altitude
[94]	Multi-antenna source transmits to a single-antenna UAV	Convex (Derived compact expression)	✓		✓	✓	✓
[95]	Multi-antenna source transmits to a single-antenna UAV	Convex (Derived compact expression)	✓		✓		✓
[96]	Composite channel rotary wing swarm enabled UAV	Non-convex (Iterative algorithm)		✓	✓		
[97]	Multiuser downlink A2G communication	Non-convex (Linear approximation and linear matrix inequality alternation)	✓	✓		✓	
[98]	UAV-enabled multi-user communication	Non-convex (Efficient path-following algorithm)		✓	✓	✓	✓
[99]	Single UAV-enabled secure data dissemination system	Non convex (Alternating optimization and SCA)			✓	✓	✓
[100]	UAV aided remote MIMO wireless communication system	Convex (Power division and distributed interference alignment algorithm)	✓		✓		✓
[101]	FD MIMO-enabled UAV to combat aerial eavesdroppers	Convex (TD-based RL algorithms)		✓		✓	✓
[102]	UAVs adopt ZF precoding to serve multiple users	Non-convex (Iterative algorithm)		✓	✓	✓	✓
[103]	UAV to transmit confidential information and AN to BSs simultaneously	Non-convex (Iterative algorithm)	✓		✓	✓	✓
[104]	Two-phase transmission protocol via AN-assisted UAV communications	ASR optimization problem (Computational algorithm)	✓	✓		✓	✓
[105]	UAV-assisted overlay cognitive radio network	Convex (Derived compact expression)			✓		✓
[106]	Satellite-enabled vehicular communications	Inner-stage and Bi-convex problem (SDR and Charnes Cooper transformation)	✓		✓	✓	
[107]	OFDM system for mmWave and FD-UAVs with ground cellular networks	Non-convex (Walsh-Hadamard transform cholesky decomposition, QR decomposition, block diagonalization precoding)		✓	✓		✓
[108]	Energy constrained UAV-assisted secure communication system	Non-convex (BCD, integer relaxation, S-procedure, and SCA)		✓	✓		✓
[109]	EH-based FD UAV-aided MEC system.	Non-Convex (Analytical derivations)	✓		✓	✓	
[110]	PHY security of networks comprising cellular-connected UAVs served by m-MIMO links security	Convex (Derived compact expression)			✓	✓	✓
[111]	Non-orthogonal UAV-assisted secure downlink communications security	Non-convex (SCA and BCD methods)	✓	✓	✓		✓

efficiency and PHY security of the relay network, the authors in [100] have proposed a power splitting distribution and interference alignment method. Their research considered a remotely operated UAV MIMO relay node assisting wireless cellular communication and utilizing the power splitting method for energy harvesting to extend the battery lifetime. The noise added to the network interferes with the eavesdropper's signal, which is filtered along with the interference at the receiver side by using an interference alignment algorithm.

In [101], an FD UAV relay node assists the multiple ground nodes in a secure communication system where aerial eavesdroppers are randomly present in the 3D space. Herein, MIMO-based beamforming methods with AN and interference aided relaying scheme have been considered at the BS and UAV to combat eavesdroppers. The optimization problem was formulated to maximize the ASSR and minimize the instantaneous secrecy rate without prior CSI for reliable and secure information transfer in the network. The developed algorithm proved to be a better candidate for evaluating

TABLE 7. Variations of power allocation with respect to several system parameters [97].

Parameters	Total Transmission Power		Information Signal Power	
	High	Low	High	Low
Increase in the number of antennas at the BS		✓	✓	
Increased gap between the minimum data rate	✓		✓	
Maximum eavesdropping data rate	✓		✓	
Link suffers more jittering	✓			✓
EVE is located in the legitimate path	✓			✓

UAV's optimal trajectory to avoid collision with obstacles during flight duration and reduce flight time. Similarly, the authors in [102] have considered terrestrial eavesdroppers and proposed a PS-based AN and information transmission for secured UAV-to-ground communication. In addition, the ASSR is jointly optimized with respect to the power splitting factors and transmission power levels by exploiting the controlled trajectory of aerial vehicles. Although simulation results show better performance than that of the existing algorithms, several practical issues like noise and interference reduction at the receiver and outage probability were not explored.

The authors in [103] studied secrecy performance and network coverage of a UAV network and modeled the UAV node as an MHCPP and ground user as a PCP. Further, UAVs employ zero-forcing precoding to provide services to multiple user nodes and transmit AN to safeguard against eavesdroppers. Mathematical expressions for coverage probability, secrecy throughput, and secrecy outage probability are formulated. In [104], the UAV utilizes a PS approach to ensure secured communication by dividing the total transmitted power into message transmit power and AN power. The research aims to maximize the ASSR via joint optimization of total transmit power, UAV's path and operation height, and power splitting factors for different flight durations. The optimization considers constraints on the total transmission energy, mobility energy, UAV's maximum velocity, and others. The developed iterative algorithm has favorable attributes like having significantly less complexity and closed-form formulation in each step, and it can further be extended to 3D UAV trajectory.

By considering the CR network for spectrum sensing, the authors in [105] have proposed a UAV-enabled CR-based secured communication system which also utilizes AN. The objective was to jointly optimize the UAV's trajectory, spectrum sensing time, and PS factor.

Later, the authors in [106] have examined multi-beam satellite facilitated secured UAV communication in which it serves legitimate terrestrial users and further utilizes AN to tackle eavesdroppers. They considered joint optimization of satellite beamforming and UAV power allocation to enhance the legitimate users' secrecy rate. The desired user is guaranteed to be within the satellite's transmitted signal beam to improve the QoS. Further, zero-padded OFDM system-aided multi-antenna transceivers for mmWave are considered in [107] by integrating FD UAVs with ground cellular networks in the presence of a passive eavesdropper. An intertwining logistic map-cosine transform-assisted algorithm and AN are utilized to enhance PHY security.

The authors in [108] have investigated a dual-energy constrained UAV-assisted secure communication system, wherein one UAV transmits information to mobile UE. The other one sends AN to confuse eavesdroppers. They formulated the worst-case secrecy rate maximization problem by jointly optimizing UAVs' 3D trajectory, maximum speed, collision avoidance, positioning error, time allocation, and EH. To address the limited computational capability and energy constraint of the UAVs, the authors in [109] have proposed an EH-based FD UAV-aided MEC system to simultaneously transmit and receive the information and broadcast the artificial interference to confuse the eavesdroppers. They aimed to enhance the offloading energy efficiency by optimizing UAVs' energy consumption and the harvested energy.

The authors in [110] have utilized AN to improve the PHY security of networks comprising cellular-connected UAVs served by m-MIMO links. They have obtained the compact expression of the ergodic secrecy rate and the optimal power allocations for transmission and AN. Further, the authors in [111] have considered the AN transmitting non-orthogonal UAV-assisted secure downlink communications in which the single antenna UAV served multiple terrestrial users in the presence of multiple eavesdroppers. They have formulated a non-convex optimization problem for maximizing the minimum average secrecy rate by jointly optimizing the UAV's trajectory, power allocation, and PS ratio, which they tackled using SCA and BCD methods.

1) KEY INSIGHTS OF THIS SECTION

1) The main objectives of research works discussed in this section are to minimize SOP, maximize the system throughput, and maximize the ergodic secrecy capacity to obtain better secrecy performance.
2) Optimizing the UAV's trajectory and operating altitude helps to enhance the PHY security.
3) There exists a trade-off between the power splitting factor for signal and AN transmission to enjoy the optimum system performance and security.

4) Many research works employed AN in different UAV-assisted B5G techniques such as massive MIMO, mmWave, OFDM, and MEC based system models to obtain higher secrecy.

B. COOPERATIVE JAMMING-AIDED PHY SECURITY

The security concern with the UAV communication hampers the reliability and confidentiality of the information. There have been various research studies conducted in the domain of employing cooperative jamming to prevent foreign intrusion. In this approach, the UAV initially transmits a jamming signal to the eavesdropper while the source transmits information. The intended receiver then filters the jamming noise via the self-interference cancellation method. Various research works [108], [112], [113], [114], [115], [116], [117], [118], [119], [120], [121], [122], listed in Table 8, have employed cooperative jamming for different system models. Fig. 7 represents a general model of cooperative jamming aided UAV communication, where a UAV BS is engaged in assisting data transmission between the terrestrial source and legitimate receiver. At the same time, a UAV jammer is overcrowding the suspicious ground receiver with the jamming signal who tries to eavesdrop on the legitimate link. Further, Fig. 8 illustrates a model of the switching jammer technique that is employed in UAV communications. In this technique, a UAV BS assists the data transmission between the terrestrial source and legitimate receiver. When the eavesdropper tries to attack the legitimate link and penetrates under the link coverage, the UAV BS switches to a UAV jammer to tackle the suspected attacker.

The authors in [112] have investigated a new approach to handle the eavesdroppers in UAV-to-ground node communications by employing cooperating jamming. In the considered model, a UAV delivers legitimate information to the ground nodes, and another nearby UAV jammer transmits AN to the eavesdropper. With the aid of jamming signals, secured and confidential information transfer is achieved. The trajectories of both the UAVs are versatile so that completely-controlled mobility can be exploited. The exact locations of ground nodes and partial locations of the eavesdroppers are assumed to be known to the UAV's navigational control. The objective was to maximize the minimum secrecy rate from the UAV transmitter by jointly optimizing its path and power allocation for information and jamming signal transfer.

Further, the research work in [113] has proposed a novel UAV-aided secure information transmission network in which a UAV transmits confidential legitimate signals to a terrestrial destination node. The UAV employs AF relaying under energy constraints and is interrupted by a ground eavesdropper. The expressions for various secrecy metrics, like average secrecy rate, secrecy outage probability, and connection success probability, are obtained for the UAV operating at low altitudes. The Rician fading channel model has been considered, whose parameters depend on the elevation angle. It is challenging to cope with UAVs' integrated wireless network vulnerabilities because of the A2G LoS communication links.

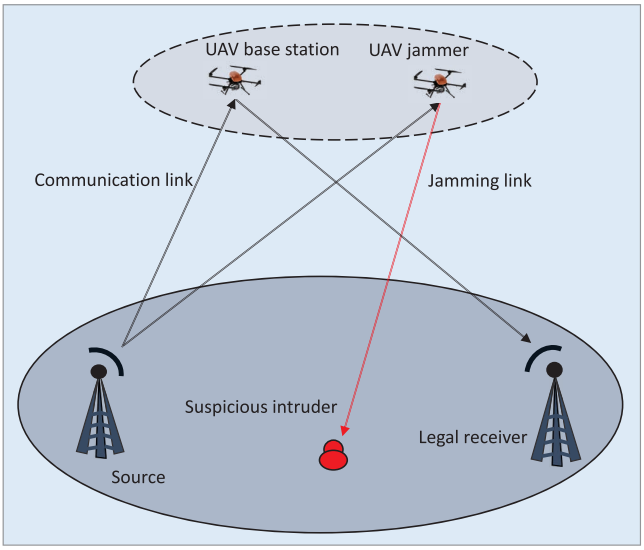

FIGURE 7. System model for cooperative jamming via assisting jammer UAV.

To resolve potential problems, the authors in [114] have introduced a unique cooperative communication strategy from a PHY security perspective. Herein, a cooperative UAV jammer is deployed to strengthen the system's privacy by transmitting interference signals to confuse the eavesdropper. The UAVs were constrained with both power and mobility, whereas the relaying UAV was constrained with information causality.

The authors in [115] have examined an energy-constrained UAV-enabled relay network assisting legitimate communication between the source and destination nodes in the presence of multiple eavesdroppers. The UAV employs PS and TS techniques for energy harvesting and relaying of information, respectively. In addition, they also examined an FD destination node that acquires legitimate information from the UAV while also collaborating to transmit AN signals to deceive hostile intruders. They have formulated a worst scenario secrecy rate maximization problem that optimizes the UAV's trajectory, AN power, and the TS and PS ratios to improve the system's dependability and security. The formulated non-convex problem has been solved by separating it into three subproblems. The iterative algorithm facilitates a numerical approach and multi-dimension search to find solutions.

UAV-enabled communication has been an efficient strategy for improving transmission reliability in defense and commercial sectors. Still, owing to its broadcast nature, it is also exposed to passive eavesdropping. In this regard, the research work in [116] has investigated multi UAV-enabled relays and jammer-aided secured mmWave communications, where randomly dispersed terrestrial eavesdroppers are present. Compact expressions of the SOP based on the opportunistic relay selection scheme involving the characteristics of the air-to-ground channel are derived. Considering the A2G channel's three-dimensional antenna gain and random behavior, a closed-form expression for the SOP is obtained. The authors in [108] have studied a dual UAV-enabled

TABLE 8. Summary of recent research studies for mitigation techniques using cooperative jamming.

WORK	OVERVIEW	OBJECTIVE AND MITIGATION TECHNIQUE					
		Problem formation and solution category	Minimizing the hybrid outage probability	Relay selection scheme	Optimizing PS and TS factors	Maximizing the minimum secrecy rate	Optimizing UAV's trajectory and altitude
[108]	Considered dual-UAV enabled secure communication system	Non-convex (Iterative algorithm and SCA)	✓	✓			✓
[112]	Proposed dual UAV model, where one UAV transmits information to GN and the other acts as a jammer	Convex (Derived compact expression)		✓	✓	✓	✓
[113]	Analyzed a source transmitting confidential information to a destination via an energy-constrained AF-based UAV relay	Convex (Derived compact expression)	✓			✓	✓
[114]	Proposed a DF-based UAV relay model to forward confidential information between two ground users	Non-convex (Update rate assisted, BCD and SCA)		✓	✓	✓	✓
[115]	Modelled a UAV-enabled FD mobile relay assisted secure communication system	Non-convex (Sub-optimal iterative algorithm)			✓	✓	✓
[116]	Analyzed mmWave communications assisted by multiple UAV-enabled relays and jammers	Convex (Derived closed-form expressions)	✓	✓		✓	✓
[117]	Proposed UAV-based monitoring and jamming system	Non-Convex (Judicious reformulation and SCA approach)		✓	✓	✓	✓
[118]	Proposed cooperative jamming scheme for UAV-employed DF relaying scheme	Non-Convex (Gauss-Chebyshev quadrature method)	✓	✓	✓	✓	
[119]	Proposed OTFS technique for UAV-satellite communication system	Convex (Derived closed-form expressions)	✓	✓		✓	✓
[120]	Proposed a UAV-MEC-based secured communication model	Non-Convex (SCA and BCD methods)			✓	✓	
[121]	Considered joint UAVs' trajectory and resource allocation optimization scheme	Non-Convex (Alternate optimization algorithm)	✓		✓		✓
[122]	Studied a UAV-assisted cognitive relaying system	Non-Convex (SCA and alternate optimization methods)	✓		✓	✓	

secure communication system, where a mobile UAV sends legitimate signals to a mobile user, and a nearby UAV acts as a cooperative jammer by transmitting the jamming signal to confuse eavesdroppers. The 3D UAV's trajectory and time allocation for EH and transmitting signals or jamming are jointly optimized to maximize the minimum secrecy rate. The formulated non-convex problem is divided into three subproblems, solved by iterative methods employing the BCD technique, SCA, and integer relaxation algorithm.

The authors in [117] have exploited UAV's flexibility for monitoring and transmitting the jamming signal to suspicious eavesdroppers in the legitimate terrestrial link. They focussed on jointly minimizing the overall jamming energy and propulsion energy consumption by applying the SCA approach to find a feasible solution fulfilling the KKT conditions. Similarly, a cooperative jamming scheme has been proposed in [118] that helps the destination and an external UAV to improve the secrecy performance in the UAV-aided DF relaying system to disrupt eavesdroppers. By considering the Nakagami-*m* fading model, compact expressions for both schemes, with and without jamming, were obtained using the Gauss-Chebyshev quadrature method. On the other hand, the authors in [119] have investigated the secrecy performance of the OTFS technique employed in the uplink transmission of a LEO satellite communication system, in which the

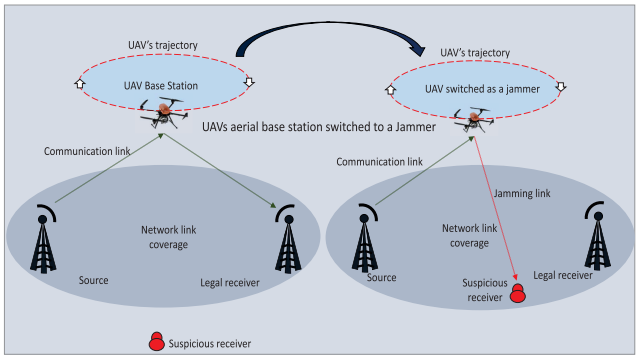

FIGURE 8. System model for cooperative jamming via switching UAV.

cooperative UAV transmits jamming signals to a reconnaissance satellite. Intending to maximize the minimum secured capacity of the user, [120] has proposed a UAV-MEC-based communication model, in which the UAV assists in calculating the offloading tasks and transmits jamming signals to terrestrial eavesdroppers. Likewise, the authors in [121] have formulated the joint UAV's trajectory and resource allocation optimization problem for a cognitive UAV-assisted jamming scheme.

Considering a UAV-assisted cognitive relaying system, the authors in [122] have proposed a system model in which secondary-UAV relay assists in the information transfer from multiple secondary IoDs to secondary users by sharing the spectrum of the primary user. A friendly UAV jammer is leveraged for transmitting the jamming signals to enhance the PHY security against the secondary eavesdropper. Further, in [111], the authors have considered the FD UAV-assisted covert communication model to confuse the warden. They have obtained the compact expression of SOP from the acquired threshold for optimal detection and minimum detection error probability. Then, they formulated an optimization problem for maximizing the effective covert throughput by optimizing the covertness power constraint.

1) KEY INSIGHTS OF THIS SECTION

1) In order to make a UAV-enabled communication system more secure, most of the works discussed in this section focused on minimizing the SOP or maximizing the system throughput and ergodic secrecy capacity.
2) The UAV's high altitude and dominant LoS link can be leveraged to cooperatively jam the far-located malicious attackers.
3) The cooperative jamming technique employs multiple UAVs, and therefore their trajectories and routes require stringent planning to avoid collisions.
4) Softarization of the UAV network integrating with different B5G techniques such as massive MIMO, mmWave, OFDM, OTFS, and MEC can obtain higher reliability and better secrecy performance.

C. LEGITIMATE EAVESDROPPING AIDED PHY-SECURITY

Legitimate eavesdropping is another emerging research topic in PHY security. This approach can enhance public safety by monitoring the communication between suspicious users, such as terrorists and criminals. In a UAV communication network, the UAV may act as a legitimate attacker and transmits the jamming signal to the suspicious users. The UAV utilizes the null space of the receiver to inflict interference into the eavesdropper's link to enhance the security of legitimate transmissions. On the other hand, the legitimate receiver applies self-interference cancellation to filter out noise and interference signals. Table 9 summarizes research works on the legitimate eavesdropping approach [123], [124], [125], [126], [127], [128], [129], [130], [131], [132].

The authors in [123] have considered wireless surveillance in a UAV-assisted information transmission network, in which a proactive UAV legitimately intervenes the suspicious UAVs. They have explored a power-efficient legitimate eavesdropping scheme to jam the suspicious link by maximizing the legitimate eavesdrop packets and maintaining the SINR at the suspect node. For protection against cyber attacks, the authors in [124] have adopted a proactive UAV legitimate tracking and jamming model for suspicious eavesdroppers. Key system parameters, like eavesdropping packets, receiver's signal strength, and angle of eavesdropper's signal arrival, were estimated using the developed algorithm. Further, the authors in [125] have explored a practical power-constrained UAV in a UAV communication system, where the legitimate eavesdropper UAV can eavesdrop on the communication between two suspicious UAVs. An optimization problem is formulated to increase the overall eavesdropping efficiency during the flight period. To simplify the proposed optimization problem, the authors exploit (i) integer linear programming algorithm as an optimal scheme and (ii) power sorting algorithm as a suboptimal scheme with reduced complexity.

In [126], the authors have presented a UAV-based monitoring system for suspicious UAVs. To acquire the data about suspected UAVs, a legitimate UAV jams the suspected receiver purposefully to influence the suspicious UAV to reduce its transmission rate and enhance the chances of successful eavesdropping. The developed framework was realized by integrating the mobility tracking system and MATLAB optimizing toolbox. The work in [127] analyzed security parameters for a UAV-assisted terrestrial network in the presence of legitimate jammer and UEDs. Further, assuming that the terrestrial links suffer from long-distance path-loss and Rayleigh fading, and both A2G and A2A links experience free space path-loss, the authors have derived expressions of the secure connection probability for the legitimate terrestrial link in the presence of non-colluding UEDs. In [128], the authors have investigated the performance of a novel covert communication system, where a friendly UAV-jammer is used to protect the covert transmission between two users against the eavesdropper. They have exploited the spatial diversity technique, where the UAV can

TABLE 9. Summary of recent research studies on mitigation techniques using legitimate eavesdropping.

WORK	OVERVIEW	NATURE OF OPTIMIZATION TECHNIQUE AND OBJECTIVE					
		Problem formation and solution category	Maximizing the throughput	Maximizing the SINR and transmit power	Optimizing the PS and TS factors	Maximizing the minimum secrecy rate	Optimizing the UAV trajectory and altitude
[123]	Analyzed a legitimate UAV that eavesdrops two suspicious UAVs	Convex (Derived a compact expression)	✓	✓			
[124]	Studied a legitimate UAV that tracks suspicious UAVs' flight for preventing intended crimes and terror attacks	Convex (Derived a compact expression)	✓	✓		✓	✓
[125]	Considered a power limited UAV to eavesdrop suspicious communications of two UAVs	Convex (Integer linear programming algorithm)	✓			✓	
[126]	Studied a legitimate UAV which is employed to track flight of suspicious UAVs for preventing safety and security threats	Convex (Optimization toolbox)		✓	✓	✓	✓
[127]	Considered a legitimate ground link aided with friendly jamming UAVs in a finite space	Convex (Derived a compact expression)	✓	✓	✓	✓	✓
[128]	Investigated a friendly UAV-jammer to protect the transmission from Alice to Bob against the eavesdrop	Convex (Derived a compact expression)	✓	✓		✓	
[129]	Analyzed SWIPT based UAV communication with two cooperative UAVs and wireless powered ground destination node	Non-convex (SCA and BCD)	✓	✓	✓	✓	✓
[130]	Monitoring system with three UAVs performing spoofing relaying and proactive eavesdropping was considered	Non-convex (Iterative algorithm)		✓	✓	✓	
[131]	Proposed the MA-DDPG algorithm-based legitimate eavesdropping technique	Convex (Derived a compact expression)		✓			✓
[132]	Legitimate monitoring system for information transfer between two suspicious nodes	Convex (Derived a compact expression)		✓	✓		✓

emit AN to complicate the eavesdropper. An approximate expression of the ergodic privacy rate using the Taylor series expansion under Nakagami-*m* fading was also deduced.

The authors in [129] have investigated collaborative UAVs-assisted communications, where SWIPT was utilized in the terrestrial source-terminal link with consideration of the presence of a passive eavesdropper. In particular, one UAV transmits information to the destination, and another UAV jams the eavesdropper link and exploits the EH technique to fulfill the energy requirement at the destination. By considering friendly UAV jamming and Gaussian jamming transmission schemes for the jammers under the assumption of limited availability of eavesdropper's information at the UAVs, the authors have formulated the problem of maximizing the minimum secrecy rate by jointly optimizing the signal transmitting power, destination power allocation, and UAV's trajectory. Likewise, the authors in [130] have presented an approach to maximize the effective eavesdropping rate for the legitimate eavesdropper UAV by jointly optimizing its power allocation and flight duration. They have proposed an optimal scheme for legitimate eavesdropper UAVs to switch between jammer and relaying nodes based on the power availability.

In [131], the authors have proposed the MA-DDPG-based legitimate eavesdropping technique to address the dual-hop malicious link. They have considered the DF-based relaying method to assist information transfer cooperatively and transmit jamming to a suspicious attacker. Considering the proactive eavesdropping scenario, the authors in [132] have introduced a legitimate monitoring system for supervising the information transfer between two suspicious nodes by adopting two strategies, namely, passive eavesdropping first and jamming first. They have considered the problem of maximizing the sum eavesdropping rate and utilized the SIC to enhance the eavesdropping rate.

1) KEY INSIGHTS OF THIS SECTION

1) The A2G or A2A channel consideration is crucial for stringent planning of UAV's route or optimizing the trajectory and altitude for enforcing PHY security.
2) Legitimate eavesdropping by a UAV jammer can also affect the legitimate link, so it should be employed

only for intruders at a distance far from the receiver of interest.
3) CSI should be accurately estimated so that the legitimate nodes can effectively cancel the jamming signal transmitted by UAVs to malicious nodes.
4) UAVs can be utilized to improve the covertness in confidential data transmission by employing jamming and eavesdropping strategies collaboratively.

V. MULTI UAV-AIDED COOPERATIVE METHODS

In several mission-critical applications such as emergency healthcare services, defense, surveillance and imaging, and remote accessing for backing cellular services, employing a single UAV may not be adequate to provide the required performance [11]. In these application scenarios, the swarm of UAVs is utilized for mission completion, and the mission performance critically depends on the number of UAVs. The connectivity within the UAV swarm is generally provided through the FANET, which is more prone to security threats. Additionally, designing the proper routing protocol for FANETs is very challenging due to the mobility of the UAV nodes in 3D space, the UAV swarm's dynamic topology, and UAV's energy limitations [26]. The UAV swarm's dynamic topology routing decision can be made more reliable by using a Q-learning-based topology-aware routing protocol that considers two-hop neighbor nodes [133]. As such, there is a trade-off between the numbers of UAVs used as network relay nodes and as mission-assigned ones [25]. Various research works have focused on multi-UAV relaying and UAV swarm's trajectory optimization to address security threats using cooperative UAV strategies.

A. PHY SECURITY IN MULTI UAV RELAYING

The deployment of UAVs as relays for assisting communication between source and destination nodes is of paramount importance. The UAV-assisted relay nodes may effectively extend communication for disaster-affected people (e.g., partial or complete infrastructure is damaged due to natural disasters) by quickly enabling a communication link. To this end, several research works [118], [134], [135], [136], [137], [138], [139], [140], [141], [142], [143], [144], [145], [146], [147], [148], [149] have exploited the multi-UAV relaying concept in various communication scenarios, as summarized in Table 10. Specifically, the authors in [134] have evaluated the SOP for A2G wireless communication by considering multiple UAV transmitters, UAV-relay nodes, and cooperative eavesdroppers. Here, the information is transmitted through the selected UAV-transmitter and UAV-receiver pair to the destination user via the legitimate channel. By considering various practical constraints, such as interfered LoS transmission, network synchronization, and network congestion, the optimization problem was simplified to a convex problem by employing the SCA technique.

With the growing need to monitor suspicious eavesdroppers, the authors in [135] have proposed an FD-based eavesdropping technique. This technique can proactively monitor the non-legitimate communication while transmitting the gathered data to the UAV. In particular, the authors have adopted a semi-analytical method to determine the UAV's height and transmission power for the single-antenna scenario and a semi-definite relaxation method for jointly optimizing the transmit beamforming, UAV's height of operation, and transmission power efficiency for the multiple antennas case. In [136], the authors have investigated the PHY-security performance of a UAV communication system, in which a four-node wiretap channel with a UAV-enabled relay is considered, and the eavesdroppers' location information is partially known. For optimizing the source/relay transmission power, a secrecy rate maximization problem is formulated and tackled using the difference-of-concave programming.

The authors in [137] have discussed a blockchain-assisted secure information gathering system with the aid of a UAV swarm, wherein the IoDs collect the information and then transmit it to a nearby server. Here, secure communication can be achieved by exchanging the common key among the UAV swarm and IoDs for initiating data collection. At the same time, IoDs employ data encryption techniques before forwarding signals to the UAV swarm. In addition, the authors have proposed a two-phase device validation mechanism to corroborate the security analysis by utilizing a π-hash bloom filter and a digital signature algorithm.

In addition to strategic, agricultural, and healthcare applications, IoT has influenced industrial accessibility by enabling M2M and HMI. The data's secrecy and reliability are crucial issues for establishing a diverse IoT network. In [138], the authors have introduced a wireless security strategy that utilizes UAV-based secured data transmissions. They have modeled an IoT-link wiretapping system in the presence of a multi-UAV relay network considering AN in the wiretap link. Furthermore, the integration of UAVs and terrestrial cellular networks has been analyzed in [139], in which the authors have examined anti-eavesdropping methods by employing two UAVs as a guardian and an intruder. In particular, two UAV scenarios, namely authenticated UAV and eavesdropping UAV, were considered. For the authenticated UAV scenario, the impact of using UAV relays with a focus on the UAV's flight parameters, such as the height of the UAV and the elevation angle between the relay node and the ground transmitter, to maximize the secrecy rate of ground users was studied. For the case where UAV performs eavesdropping attack, the performance of multi-hop aerial relaying for securing terrestrial links against aerial eavesdropping was also analyzed.

In [140], the authors have considered a 3D mobility model for UAV relays employing DF protocol in the HSTNs under the presence of an aerial intruder in the coverage of the UAV relay. They have proposed a random mixed modeling approach for UAV relays to enhance security, which follows 3D-trajectory to serve the terrestrial UEs. They have further examined different eavesdropper locations by considering two scenarios of interest; (i) when the attacker was uniformly positioned at a random distance near the relay, and (ii) when

TABLE 10. Summary of recent research studies on mitigation using multi UAV relaying and eavesdropping.

WORK	SYSTEM MODEL	OBJECTIVE AND MITIGATION TECHNIQUE					
		Problem formation and solution category	Minimizing the hybrid outage probability	Relay selection scheme	Maximizing the SINR	Maximizing the minimum secrecy rate	Optimizing the UAVs' trajectory and height
[118]	Proposed a DF-based UAV mmWave relaying network	Convex (Gauss-Chebyshev quadrature)	✓		✓		✓
[121]	Enhanced the PHY security with UAV-friendly jammer	Non-convex (BCD and SCA)	✓	✓			✓
[134]	Analyzed selective relaying networks with M UAV-transmitters, N UAV-relays, and K collaborative UAV-eavesdroppers	Convex (SCA)	✓	✓		✓	
[135]	Proposed a model for FD-based UAV communication	Convex (Semi-definite relaxation approach)			✓		
[136]	Considered UAV-to-ground communication system with spatially random eavesdroppers	Convex (Derived closed-form expression)	✓		✓		✓
[137]	Blockchain enabled UAV swarm network and IoT devices	Convex (FI-hash bloom filter)	✓	✓	✓	✓	
[138]	Analyzed UAVs to terrestrial IoT devices being served by cellular networks	Convex (Derived closed-form expression)		✓	✓	✓	
[139]	Described the security implications of integrating UAVs into cellular networks	Convex (SCA)	✓			✓	✓
[140]	Proposed a DF-based 3D mobile UAV relaying for HSTNs in a circular plane	Convex (Derived closed-form expression)	✓	✓	✓	✓	✓
[141]	Analyzed the 3D random trajectory for UAV mobility	Convex (Derived closed-form expression)	✓			✓	✓
[142]	UAV swarm assisted multi-hop mobile relay system was investigated	Non-convex (BCD, SCA, and Dinkelbach method)			✓	✓	✓
[143]	Proposed UAV as an aerial relay between the cluster and terrestrial BS against eavesdroppers	Non-Convex (Iterative algorithm)	✓	✓			✓
[144]	Studied IRS-assisted UAV relay communication system under terrestrial eavesdroppers	Convex (Derived closed-form expression)			✓	✓	✓
[145]	Proposed cache memory-aided UAV-relaying method for D2D communications	Non-Convex (SCA and BCD methods)		✓	✓	✓	✓
[146]	Proposed UAV relay-based transmission model with terrestrial nodes and malicious eavesdropper	Non-Convex (SCA method)	✓	✓	✓		✓
[147]	Proposed secured transmission in UAVs relay-assisted vehicular ad-hoc networks	Non-Convex (Newton method and SCA method)	✓	✓			✓
[148]	Proposed caching-based UAV-relayed WCN to broadcast files to users and eavesdropper	Non-Convex (SCA technique)	✓		✓	✓	
[149]	Proposed two cooperative dual UAV-enabled secure data transfer	Non-convex (BCD and SCA)	✓		✓	✓	✓
[150]	Focussed on UAV's energy and IoD's latency constraints	Non-convex (Inner approximation, iterative algorithm)		✓	✓		✓
[151]	PHY security in an UAV relay-assisted communication system	Convex (Derived closed-form expression)			✓	✓	
[152]	UAV-based relaying from terrestrial BS to IoT terminals	Convex (Derived closed-form expression)		✓		✓	✓

the attacker was placed at a fixed position near the engaged UAV relay. The authors have evaluated the secrecy performance metrics, such as the probability of non-zero secrecy capacity and SOP. Moreover, the authors in [141] have evaluated the ergodic secrecy rate and SOP of a ground-based RF network with the aid of multiple coordinated UAV spies. The

approximated expressions of the stochastic trajectories and secrecy metrics were derived for fading channels. To cope with the malicious eavesdropper threats and energy constraints in the LoS A2G communication link, the authors in [142] have developed a UAV swarm aided multi-hop mobile relay method that can boost the secrecy performance in severe blockage scenarios or remote communication. In the proposed method, some UAVs operate as multi-hop relay nodes to advance information between ground users, whereas other UAVs operate as cooperative jammers to mislead the terrestrial eavesdroppers.

In [143], the authors have focused on securing data transmissions against eavesdroppers among multiple UEs by using a UAV as an aerial relay between the UE cluster and a terrestrial BS. The joint secrecy energy efficiency maximization non-convex problem was divided into two subproblems and solved using an iterative algorithm. Further, the authors in [144] have studied the secrecy performance of an IRS-assisted UAV relay communication system under multiple distributed terrestrial eavesdroppers. Focusing on the cache applications, the authors in [145] have proposed a cache memory-aided UAV-relaying method for D2D communications to address the security issues in the presence of eavesdroppers. They formulated a non-convex problem for maximizing the minimum secrecy rate of users by optimizing the UAV's transmission power, trajectory, and scheduling, along with the distribution of users. The joint mixed-integer programming problem was solved using an iterative algorithm based on SCA and block alternating descent methods.

The authors in [146] have focused on maximizing the end-to-end secured throughput in a UAV relay-based transmission model having terrestrial nodes and a malicious eavesdropper. The formulated non-convex optimization problem is divided into power allocation and trajectory designing subproblems and solved with the help of the SCA method. Considering vehicular communication networks, the authors in [147] have studied the information delay minimization problem in a UAV relay-assisted VANET by assuring a secure transmission. The formulated joint optimization problem of the UAV relay's trajectory and channel allocation is simplified by Newton and SCA methods. Further, the authors in [148] have proposed the caching-based UAV-relaying WCNs to broadcast the required files to users. They have formulated a non-convex problem for maximizing the minimum average secrecy rate by joint optimization of UAV's time scheduling and trajectory.

Deploying UAVs in millimeter-wave networks has emerged as a promising alternative for assisting distant or obstructed communication. In [118], the authors have performed secrecy analysis by adopting two different jamming scenarios for a UAV-based mmWave relaying network. In the first scenario, the authors have utilized the DF relaying method for information transfer in the presence of an eavesdropper. Under the second scenario, a dual-stage relaying method was designed for both destination and UAV node that uses cooperative jamming to interfere with the eavesdropper's link. The authors in [149] have considered the UAV's propulsion energy as a constraint and investigated a cooperative UAV aided secured information transmission model. The minimum secrecy rate maximization problem is handled by jointly optimizing propulsion energy, time scheduling of data transfer and jamming, and the speeds of both UAVs.

The authors in [150] have focussed on UAV's energy and IoD's latency constraints and compared the performance of HD and FD UAV relay-assisted IoD networks. Considering a secured communication framework for a dual-UAV relaying-based MEC system, the authors in [120] have proposed a system model wherein a UAV-friendly jammer transmits the jamming signals to the UAV eavesdropper to degrade its offloading information. They have utilized SCA and BCD techniques to tackle the optimization problem of maximizing the minimum secure calculation capacity of the user by considering the UAV server's trajectory and resources.

In [151], a UAV relay-assisted communication system has been considered in which a terrestrial BS transmits confidential information to a legitimate user via UAV relay in the presence of multiple terrestrial and aerial eavesdroppers. They have utilized an optimal beamforming technique to minimize the SOP of the considered system. To study the PHY security of UAV relaying-assisted multi-terminal IoT systems, [152] has considered a UAV that relays confidential information from terrestrial BS to a cluster of IoT terminals in the presence of an eavesdropper. Recently, the authors in [146] have analyzed a UAV relay that assists in confidential information transmission between the unconnected terrestrial nodes in the presence of an eavesdropper. The non-convex optimization problem to maximize the throughput has been tackled by leveraging the SCA-based iterative algorithm.

1) KEY INSIGHTS OF THIS SECTION

1) Practical constraints like network congestion, self-interference, and hardware impairments should be considered in modeling the UAV's mobility and trajectory, relay selection, and task scheduling for multi-relays scenarios.
2) The relay selection technique, number of hops, and transmission power of each node should be jointly optimized while maintaining the necessary trade-offs to counter the security threats efficiently.
3) Compared to terrestrial channels having less availability of LoS links, the dominant LoS links made possible by the UAVs can benefit more from beamforming techniques to enhance PHY-security.
4) Exchange of security keys in blockchain technology can prevent malicious eavesdropping and ensure secure information transfer between UAV relays.

B. PHY SECURITY WITH COOPERATIVE UAV SWARMS AND MULTIPLE UAVs

The UAV swarm can enhance the network capability by offering various benefits such as higher reliability,

more comprehensive coverage, improved throughput, etc. Recently, numerous strategies, such as beamforming, UAV node selection, and multiple antennas, have been exploited in the UAV swarm-based threat mitigating systems. With the help of jamming techniques, an information security-enabled UAV swarm network can establish the communication link with the UE transmitter as depicted in Fig. 9. Here, the UAV swarm network assists the cellular communication between the terrestrial-based UE transmitter and receiver. Further, a UAV jammer within the UAV swarm handles the malicious UAV that tries to intrude the legitimate link.

The following research works [142], [153], [154], [155], [156], [157], [158], [159], [160], [161], summarized in Table 11, have been carried out for the cooperative UAV swarms under PHY security. In [153], the authors have examined the transmission security of an A2A communication link with multiple UAV relays, wherein the source transmits the information to an authorized UAV receiver in the presence of several malicious UAVs that seek to eavesdrop the information. Assuming that both the legitimate receiver and the snooping UAVs are randomly scattered in the coverage area of the source, the authors have derived a compact SOP expression. Furthermore, a UAV swarm-aided secured network was investigated in [154], where both large-scale and small-scale fading channels were considered for the A2G link. A trajectory optimization approach was suggested to maximize the system throughput by focusing on the transmitting power limits, transmission intervals, and UAV's energy during its flight period. The formulated non-convex problem was solved by obtaining a high-order compact expression of the secrecy throughput and then by applying the SCA-aided iterative method. To enhance the PHY security of a UAV-aided system, the trajectory planning of UAVs is an important task. The authors in [155] have explored a UAV-to-ground base station link to support terrestrial users in the presence of an intruder. The adaptive optimization technique has been utilized for the UAV's 3D trajectory to maximize the secrecy capacity under the altitude and obstacle restrictions. In addition, they have exploited random sampling and eigenvector approximation to obtain the solution for the SDR problem. From the standpoint of strategic and defense applications of wireless communication, the authors in [156] have obtained the expressions of recognition probability for the host's GV and opponent's G2A link. To obtain secured transmission, they first defined the statistical parameters of the SNRs for the G2A and G2V links and then evaluated the average detection capacity and the detection outage probability.

The authors in [157] have studied a model where the transmitter and the receiver are located very far and in the presence of the eavesdroppers. They have utilized multi-UAVs as relay nodes to gain better flexibility in allocating resources for trajectory, mobility, and coverage compared to a single UAV model. They have introduced a strategy based on S-procedure and SCA methods to tackle the joint optimization of power splitting and UAV's trajectory to enhance the throughput. Similarly, the authors in [158] have

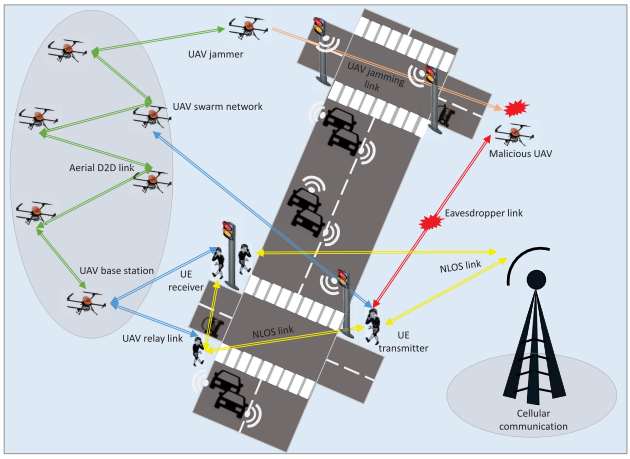

FIGURE 9. UAV swarm network assisting cellular communication and jamming the intruder.

proposed a secured UAV-assisted model wherein a centralized controller forms a WMN of multiple UAVs. It utilizes cryptographic methods like Blowfish, advanced encryption standards, and the A-search method to mitigate security threats, offering higher throughput and assured transmission of information with the least encryption-decryption time. Further, in [159], the authors have presented the learning-based task offloading algorithm for UAV-aided WSN to enhance the rate of service satisfaction by considering the assigned tasks and intermediate threats. It predicts queuing delays of the UAVs to reduce the communication networks' overhead due to some external malicious attack.

Considering the RIS-based multi UAVs secured communication, the research work in [160] has considered TDMA protocol-based RIS-aided UAV and terrestrial users for data transmission, in which an eavesdropper wiretaps their links. The authors in [142] have developed a cooperative transmission technique to address PHY-security in a UAV swarm-assisted multi-hop mobile relay system, wherein a UAV acts as a relay between terrestrial users, and other UAVs act as jammers for eavesdroppers. Further, the research work in [161] has analyzed the secrecy performance of a UAV-assisted vehicular communication system, wherein the data is transmitted between the UAV base station and a moving vehicle in the presence of an eavesdropping vehicle.

The authors in [162] have proposed a cooperative jamming-assisted two-phase transmission model for the untrusted UAV-mounted relay operating in the THz frequency band for data acquisition from multiple terrestrial user equipment. They have formulated the non-convex problem for maximizing the minimum secrecy energy efficiency by optimizing the transmission power allocation, UAV's trajectory and velocity, and communication scheduling. Considering a secured bidirectional communication model for dual UAV–based relaying for terrestrial devices, the authors in [163] have proposed to use a UAV-friendly jammer that transmits the jamming signals to confuse the eavesdropper. They have jointly optimized the peak transmit power,

TABLE 11. Summary of recent research studies on mitigation using cooperative UAV swarms.

WORK	SYSTEM MODEL	NATURE OF OPTIMIZATION TECHNIQUE AND OBJECTIVE					
		Problem formation and solution category	Minimizing the hybrid outage probability	Maximizing the SINR and throughput	Energy constraint modelling of UAV	Maximizing the minimum secrecy rate	Optimizing the UAV trajectory and altitude
[142]	Developed a cooperative transmission technique for UAV swarm- assisted multi-hop mobile relay system	Non-convex (BCD method, SCA techniques, and Dinkelbach method)		✓	✓	✓	
[153]	Investigated the secrecy performance of an UAV-UAV system	Convex (Derived a closed form expression)	✓	✓	✓	✓	
[154]	Considered power allocation for UAV swarm enabled A2G link	Non-convex (Iterative algorithm and SCA)		✓	✓	✓	✓
[155]	Studied 3D ultra low-altitude UAV enabled cellular communication system	Convex (Semi-definite relaxation method)			✓	✓	✓
[156]	Studied the home country's GV to enemy's ground station GS-to-UAV transmission system	Convex (Derived a closed form expression)	✓	✓	✓		
[157]	Considered the deploying of multi-UAVs as relays to secure wireless communication	Non-convex (SCA and S-procedure)		✓	✓	✓	✓
[158]	Proposed a secured Wireless mesh network of multiple UAVs	Convex (Derived a closed form expression)		✓	✓	✓	
[159]	Proposed the learning-based task offloading algorithm for UAV-aided WSN	Convex (Derived a closed form expression)	✓		✓	✓	✓
[160]	Investigated RIS-aided secured UAVs communication	Non-convex (SCA, S-Procedure, and SDR methods)	✓	✓	✓		
[161]	Analyzed secrecy performance of UAV to vehicle communication system	Convex (Derived a closed form expression)		✓		✓	✓
[162]	Cooperative jamming-assisted untrusted UAV-mounted relay system	Non-Convex (Greedy block SCA, non-linear fractional programming)	✓	✓	✓		✓
[163]	UAV-friendly jammer to confuse the eavesdropper	Non-convex (DDPG-based algorithm)		✓	✓	✓	✓
[164]	Investigated the covertness of UAV jammer-assisted CR network	Convex (Derived a closed form expression)	✓	✓		✓	✓
[165]	UAV acquired the information in uplink and transmits jamming signals in downlink	Non-convex (BCD)	✓	✓			✓

UAV's flight space and speed, and energy capacity to maximize the minimum average secrecy rate, which they tackled by using a DDPG-based algorithm to solve the constrained Markov decision process.

Further, the authors in [164] have investigated the covertness of a secondary user in a UAV jammer-assisted CR network against an eavesdropper whose CSI is partially known. They have proposed a joint optimization model for maximizing the probability of error detection and covert rate by optimizing the UAV's power and trajectory tackled by a generative adversarial network. Aiming to maximize the secrecy energy efficiency of the FD UAV-enabled WSN, [165] has studied the system model in which a UAV acquires the information in the uplink and transmits jamming signals to confuse the terrestrial eavesdropper.

1) KEY INSIGHTS OF THIS SECTION

1) Planning of UAV swarms trajectory should stringently consider crucial factors such as jamming noise and interference, 3D mobility and placement, and power

allocation for security and data transmission based on the application scenario.
2) There is a trade-off between secrecy performance and data transmission based on the number of UAVs in the swarm network engaged in the communication link.
3) Adaptive optimization of UAV's 3D trajectory, resource allocation, and path planning can provide flexible swarm topology that effectively avoids collision in the distributed UAV swarm network.
4) UAVs in the swarm network can act as a relay node and jammer to counter the eavesdropper that tries to intrude on the legitimate link.
5) In the UAV swarm, a centralized UAV controller can employ cryptographic methods to secure the control signal transmitted by C&CC about adding or removing a new UAV-relay node in the existing link.

VI. UAV-AIDED NOMA AND BEAMFORMING METHODS

The use of the UAV-assisted NOMA technique to ensure secured communication is illustrated in Fig. 10. Here, the UAV is equipped with m antennas to communicate with n legitimate receivers by exploiting the NOMA principle and enables data security from a foreign intruder via jamming technique. Furthermore, employing transmit beamforming can improve the throughput of the legitimate user while managing the throughput of the wiretapped signal at the eavesdroppers, hence enhancing PHY security.

Numerous research works [97], [106], [166], [167], [168], [169], [170], [171], [172], [173], [174], [175], [176], [177], [183] have considered NOMA/beamforming techniques in UAV networks in order to enhance the network security. A brief overview of these works is presented in Table 12. The PHY-security challenges in the UAV-aided mmWave downlink communication systems were addressed in [166]. Herein, one UAV interacts with terrestrial sensors, whereas another UAV eavesdrops the communications between them. Furthermore, the authors in [167] have examined the security of airborne-assisted downlink data transmission networks, in which a UAV operates as an aerial platform that enables secured transmission for MUs in the existence of IoT nodes. They proposed an eavesdropper-free zone surrounded by the UAV shield to enhance the secrecy rates for MUs. The NOMA technique was utilized to optimize the MU's allocated power to maximize the least secrecy rate in the protected regions.

The effect of UAV's jitter on reduction of energy consumption as well as on secure transmission for a downlink A2G wiretap system was investigated in [97]. A combined beamforming optimization of information signal and AN signal was proposed with the constraints on worst-case secrecy performance so as to reduce the overall transmit power for a UAV-aided base station. To analyze the secrecy performance, the formulated non-convex was reformed using linear matrix inequality and linear approximation for system constraints and variations in the channel, respectively, and then simplified with the help of the SDR algorithm. The authors in [168] have analyzed a UAV-assisted NOMA technique for enabling SWIPT and ensuring security of data transfer for passive terrestrial receivers. Time splitting and power splitting approaches were utilized simultaneously with two time frames, and non-linear EH was performed in the first frame. Specifically, the maximum throughput was obtained by canceling the maximum jamming power received at each passive receiver using the SIC technique. The proposed non-convex optimization problems were first converted into convex ones and then solved by iterative algorithms. In [169], the authors have examined the influence of UAV jitters on the beamforming technique in a downlink A2G network. The objective was to maximize the least secrecy rate via a joint optimization of the secret signal and AN signal beamforming. The formulated non-convex problem was tackled by applying the Taylor series expansion to linearize the introduced auxiliary variables. Further, an iterative algorithm was designed using linear matrix inequality and linear approximation methods aided with the Cauchy-Schwarz inequality and S-procedure to characterize the constraints and channel imperfections.

A new PHY-security key generation technique for A2G UAV-aided MIMO communications was suggested in [170]. The LoS propagation in UAV-assisted communication, a key property enabled by the use of UAVs, can drastically degrade the efficiency of CSI-dependent keys. As a result, a unique channel element, called 3D spatial angle, was used to counter an eavesdropping approach, called an environment reconstruction-oriented attack on secret keys. Compared to the existing plane angle aided technique, the design better uses spatially oriented inputs and produces more keys at a high rate. Moreover, a UAV-aided communication strategy has been presented in [171] to raise the QoS of edge users, where the UAV supports the primary BS as well as the coordinating BS simultaneously. Since the UAV only feedbacks the CSI to the main base station, the CSI retrieved at the synchronized station becomes obsolete. In particular, the authors have studied the ML-aided channel estimation algorithm at the coordinated BS for implementing the combined beamforming to counteract performance losses incurred due to CSI feedback lag. Additionally, a max-SINR-oriented compensation technique for beamforming was adopted for the UAV and the main BS to reduce inter-BS interference.

The authors in [172] have proposed a novel framework of the cell wall for hybrid 5G-empowered UAVs swarm architecture to increase the throughput and flexibility. They have formulated and simplified the optimization problem to obtain the maximum and minimum throughput, which help in designing the cell wall with maximum capacity. Further, they have utilized the optimal edged coloring algorithm, which allows selecting upper and lower bounded colors for scheduling the active communication links.

Considering the mmWave technology in UAV-aided WPCN, the authors in [173] have proposed a NOMA-based transmission strategy in the vulnerable sub-region to improve the secrecy-rate performance by the protected-zone method. They evaluated the effects of UAV's altitude, protected-zone

TABLE 12. Summary of recent research studies on mitigation using NOMA and beamforming techniques.

WORK	SYSTEM MODEL	NATURE OF OPTIMIZATION TECHNIQUE AND OBJECTIVE						
		NOMA or Beamforming	Problem formation and solution category	Maximizing the throughput	Energy constraints	Optimizing the PS and TS factors	Maximizing the minimum secrecy rate	Optimizing the UAV trajectory and altitude
[106]	Investigated UAV relay-aided PHY security in a satellite-assisted vehicular communications	Beamforming	Non-Convex (1D-search, SDR, SDP, Charnes-Cooper and Dinkelbach method)	✓	✓	✓		✓
[166]	UAV enabled mmWave downlink transmission was considered	Beamforming	Non-convex (BCD and SCA)	✓	✓			✓
[167]	Studied downlink transmission where the UAV provides secure transmission to the MUs	NOMA	Convex (Dichotomy based algorithm)	✓	✓	✓	✓	
[168]	Analyzed a network in which UAV achieves SWIPT and EH for ground PRs	NOMA	Non-convex (Iterative algorithms)	✓	✓		✓	
[169]	A downlink A2G wiretap network UAV was studied	Beamforming	Non-convex (S-procedure and Cauchy-Schwarz inequality)		✓		✓	
[170]	Analyzed an A2G MIMO and FDD based UAV systems	Beamforming	Convex (Derived a closed form expression)	✓	✓	✓		✓
[171]	Investigated a UAV that aids primary base station and a coordinated base station simultaneously	Beamforming	Convex (Derived a closed form expression)		✓		✓	✓
[172]	Heterogeneous 5G-enabled UAV swarm network was considered	NOMA	Non-Convex (Optimal edge coloring solution)	✓	✓	✓		✓
[173]	Considered mmWave technology in UAV-aided NOMA-based WPCN	NOMA	Convex (Derived a closed form expression)			✓	✓	✓
[174]	Proposed NOMA and TDMA in dual UAV-assisted MEC systems	NOMA	Non-Convex (BCD and penalized BCD algorithm)	✓		✓		✓
[175]	Proposed beamforming method in UAV-BS and IRS-assisted mmWave networks	Beamforming	Non-Convex (Semi-definite relaxation and alternating method)			✓	✓	✓
[176]	Proposed beamformer in UAV-aided cellular networks with two-user MISO system	Beamforming	Non-Convex (Sequential parametric approximation and bespoke initialization algorithm)		✓		✓	✓
[177]	Developed 3D robust beamforming technique for the UAV communications	Beamforming	Convex (Derived a closed form expression)			✓		✓
[179]	Considered ultra-dense heterogeneous network of cache-aided UAVs with power domain NOMA	NOMA	Non-Convex (Iterative algorithm)	✓	✓		✓	
[180]	Virtual antenna array in UAV swarm that employs collaborative beamforming	Beamforming	Convex (Derived a closed form expression)	✓	✓		✓	
[181]	Collaborative beamforming in UAV-virtual antenna array communications	Beamforming	Convex (Derived a closed form expression)	✓	✓		✓	
[182]	Demonstrated the NOMA-integrated UAV communication networks	NOMA	Non-Convex (Iterative algorithm)	✓	✓		✓	

size, and transmitted power on the secrecy rate and optimized the protected zone's shape to improve the secrecy rate. In [174], the authors have formulated a non-convex problem for maximizing the minimum secrecy computing capacity for NOMA and TDMA techniques in dual UAV-assisted MEC systems. The UAV is used to assist terrestrial devices in evaluating offloading tasks and jam eavesdroppers. Further, the authors in [175] have jointly analyzed the positions and beamforming of UAV-BS and IRS-assisted mmWave networks. They have also exploited AN against eavesdroppers to maximize the secrecy rate. The formulated non-convex problem was divided into subproblems, namely, planning UAV-BS and IRS positions and UAV-BS and IRS beamforming. A suboptimal solution was obtained by utilizing semi-definite

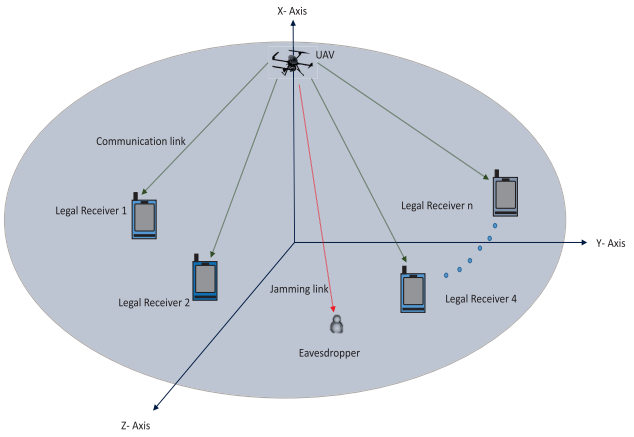

FIGURE 10. NOMA-enabled UAV secured communications.

relaxation and alternating optimization. Further, the authors in [176] have evaluated the maximum-minimum secrecy fairness of a UAV-aided cellular network with a two-user MISO system.

Based on learning strategies, the authors in [177] have developed a 3D robust beamforming technique for UAV communications to obtain a better secrecy rate and dynamic beam steering. They have proposed a DL-trained neural network to maximize the system's average secrecy rate and optimize beamformer for information signal and AN. Focusing on SATN, the authors in [106] have investigated UAV relay-aided PHY-security in satellite-assisted vehicular communications, wherein a UAV relay assists the satellite-vehicular link and also transmits AN to confuse eavesdroppers. They have formulated a joint optimization problem of UAV's power allocation and satellite beamforming for maximizing the legitimate users' secrecy rate. Furthermore, RF-EH models have been considered in [168] to provide onboard energy supply. The authors have proposed a non-linear EH model for UAV communications that harvest energy in the first phase and utilizes the NOMA-based SWIPT technique to transmit data to terrestrial PRs and artificial jamming signals to malicious attacks in the second phase.

A dynamic power allocation and an aerial jamming technique for UAV-assisted NOMA communication networks have been studied by the authors in [178] to enhance the reliability and security in the presence of a terrestrial eavesdropper. Whereas the authors in [179] have considered an ultra-dense heterogeneous network of cache-aided UAVs employing power domain NOMA protocol and IoT-mobile devices. They have aimed to maximize the secured cache throughput by optimizing the UAV's 3-D positions, number of UAVs and mobile devices, and UAV's cache placement probability by employing fast global K-means and iterative algorithms.

Then, focussing on extending the secured network's range from the constrained transmit power, the authors in [180] have considered a virtual antenna array in the UAV swarm that employs collaborative beamforming. They have examined the SEE of an analog collaborative beamforming-assisted PHY security technique using a UAV. Similarly, the authors in [181] have also studied collaborative beamforming to obtain energy-efficient and secured UAV-enabled virtual antenna array communications for remote terrestrial users. They have solved a non-deterministic polynomial-time hard problem to minimize the UAV's propulsion energy consumption by optimizing the UAV's hovering position, weight, and scheduling using evolutionary computation. The authors in [182] have recently demonstrated that NOMA integrated with UAV communication networks can achieve higher spectrum efficiency and massive connectivity. They proposed to employ AN in a UAV-assisted NOMA downlink transmission scheme to counter security threats from a passive eavesdropper.

2) KEY INSIGHTS OF THIS SECTION

1) UAV's dominant LoS link makes the NOMA and beamforming techniques more effective by improving the SINR of the legitimate link or degrading the SINR of the eavesdropper's link.
2) These spectral-efficient techniques can enhance the system's throughput with a higher secrecy rate by transmitting AN or jamming signals to the terrestrial eavesdroppers.
3) By jointly employing NOMA and 3D beamforming techniques, UAVs can counter the malicious nodes present even at the cell edges.
4) Outdated or corrupted CSI-dependent keys can increase the probability of attack. However, 3D spatial angle-based key generation can improve the secrecy-rate performance in vulnerable regions.
5) Optimization of beamforming weight, power allocation, and UAV's position and trajectory can improve secrecy performance even in the worst-case scenario.

VII. PHY-SECURITY VIA UAV-AIDED EMERGING TECHNOLOGIES

In this section, we discuss several emerging technologies widely utilized to enhance the security and reliability of UAV-integrated networks.

A. SECURED UAV COMMUNICATIONS USING MACHINE-LEARNING

ML techniques assist the system to automatically learn and ameliorate by utilizing pre-knowledge experience without any human intervention and programmed algorithms. They can be sub-categorized as supervised, unsupervised, and reinforcement ML algorithms. ML algorithms can be employed to identify various spoofing, man-in-the-middle attacks, and software attacks, both originating through malicious UAV nodes or terrestrial UEs. Algorithms like SVM, CNN, RNN,

LSTM, and DRL, are utilized in [188], [189], [190], [191], and [192] for UAV-enabled communications to detect security threats in the network and enhance UAVs' recovery from failure. Emerging applications of ML-based secured UAV communications are depicted in Fig. 11.

Focusing on UAVs' data collection ability, the authors in [184] have studied energy-efficient and secured video streaming in a rotary-wing UAV-aided WCN by considering a scalable video coding method. A constrained Markov decision process problem was formed by jointly considering the secrecy timeout probability and required time delays. The formulated problem was solved by dynamically adjusting the Lyapunov function and inducing a safe deep Q-learning network. A UAV-aided privacy-preserving system has been developed in [185] for anonymous masking people's faces in videos captured by UAVs without losing the semantic information.

Several research studies have examined reinforcement learning-based UAV-aided secure communications. For instance, the work in [186] investigated DDPG and twin-DDPG deep reinforcement learning algorithm-based secure transmission in UAV-assisted mmWave communications by utilizing RIS under imperfect CSI. The UAV's active beamforming, RIS elements' coefficients, and UAV's trajectory were jointly optimized to maximize the sum secrecy rate of the legitimate users in the presence of multiple attackers. The work in [187] has introduced a multi-agent DRL-based management scheme to minimize the UAVs' overlap and shadowed regions for reliable and flexible UAVs-assisted surveillance services over a large area. The authors in [188] have investigated a distributed RL-based energy-constrained UAV relay network under a jamming attack in which the locations of both UAV and jammer are unknown.

1) KEY INSIGHTS OF THIS SECTION

1) ML strategies can be employed in rule-based, signature-based and anomaly-based intrusion detection in UAV-enabled communications.
2) Learning techniques like ANN, CNN, SVM, and CRNN can be utilized to enhance security in different UAV-based paradigms to provide precise predictions about non-deterministic events based on past experiences.
3) ML-based PHY security either deals with detecting any unauthorized UAVs in the region of interest or preventing legitimate UAVs from entering an unauthorized zone.

B. SECURED UAV COMMUNICATIONS USING BLOCKCHAIN

Blockchain-assisted networks enable an additional security layer to UAVs that hinders data tampering and retrieval by malicious objects. The scalable chains of blocks use a cryptographic hash function to record an immutable transaction that a key can access. The data transmission steps from a source to a destination UAV via blockchain hash and chain are

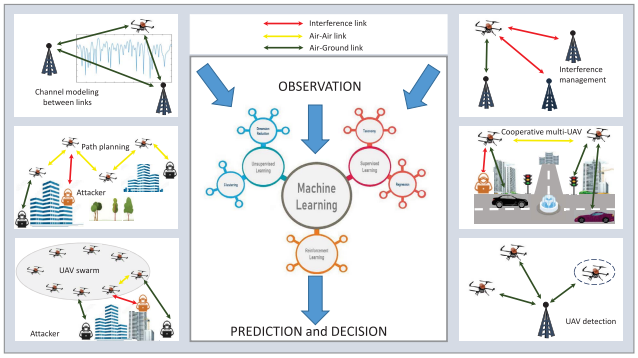

FIGURE 11. ML-based secured UAV communications.

described in Fig. 12. The blockchain networks can be private, public, hybrid, or consortium that allow the use of UAVs in highly confidential as well as in real-time applications. Besides, several consensus algorithms, such as PoS, DAG, PoW, etc., have been utilized in mission-critical applications. Data in the blockchain is distributed by using hashes. Thus, decentralized data controlling is more resilient to any adversary as compared to the single C&C system. There are several research works [189], [190], [191], [192], [193], [194] that have focused on integrating blockchain techniques with UAVs for addressing security threats.

Motivated by the benefits of FL and blockchain, the authors in [189] have surveyed mobile drone-edge intelligence for decentralization management and security in green smart environments. They have discussed fundamental technological aspects, frameworks, and challenges like transaction capacity, energy efficiency, and scalability in blockchain-assisted applications. Blockchain offers less probable traceability and decentralized nature of transactions, which was discussed in [190].

Concentrating on the heterogeneous FANET, the authors in [191] have presented a blockchain-aided distributed scheme for secure key management in UAV-assisted applications. The scheme enables UAVs to autonomously move between clusters, distribute cluster keys, and update key pairs while countering external and internal malicious UAVs. To address challenges such as reliability, security, and transparency in robotic surgery or telesurgery, the work in [192] proposed a blockchain and AI-assisted telesurgery system. It utilizes ultra-reliable low-latency communications and eXtreme gradient boosting-AI algorithm-aided UAVs to provide healthcare facilities in emergency situations.

In [193], the authors have proposed a blockchain-based strategy for the forger node that utilizes the Merkle hash tree and PoS algorithm for secure data dissemination in IoD-aided communications. They used blockchain technology for the forger node to perform key management, verification, and secured transaction from the user layer to the IoD layer. However, the work in [193] has not considered false injection attacks on the UAV's localization algorithm, which was addressed in [194] using a blockchain-aided localization algorithm that has three key features; decentralization, drone

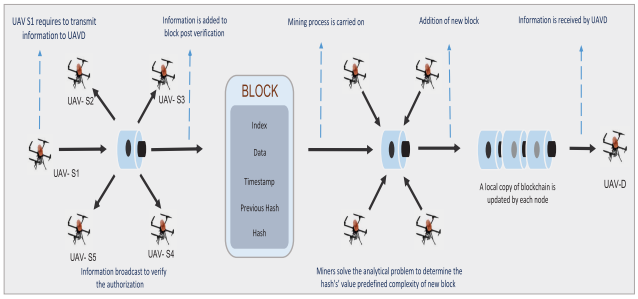

FIGURE 12. Data transmission process in blockchain-based UAV communications.

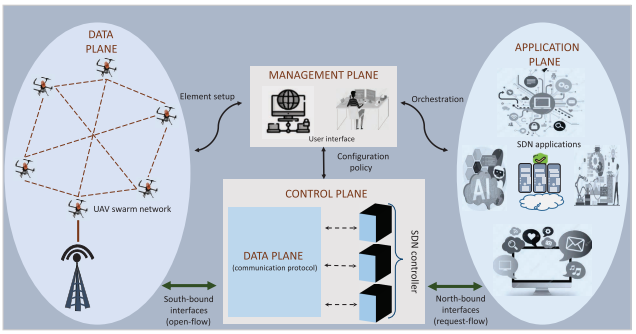

FIGURE 13. SDN operation in UAVs network.

to drone peer communication, and omitting the central trust node.

1) KEY INSIGHTS OF THIS SECTION

1) Blockchain's key features like incentive model and smart contract can provide an extra security layer to UAV communications.
2) Cryptographically connected blocks in the consensus blockchain method can counter non-legitimate interactions, like false data injection attacks.
3) By accessing the onboard blockchain copy of a pre-planned route, a UAV can change its trajectory without C&CC controls, which reduces network congestion.

C. SECURED UAV COMMUNICATIONS USING SDN

Centrally programmed software-based networking architecture provides consistent network management through real-time monitoring and reconfiguring the switching functionality of the network layer. The SDN framework initially decouples the single plane of the network into data, control, and application planes to make it programmable, which provides an extra degree of freedom in designing the networking protocols [195]. In general, an SDN controller operates as the network's brain that configures the topology and handles traffic management. Vulnerabilities like jamming, spoofing, and software attacks are persistent to resource-constrained networks that SDN-assisted UAV communications can counter. Fig. 13 depicts SDN operations in a UAV network that decouples the network into planes and enables each UAV to act as an individual switch. The control plane of the SDN controller handles data traffic by controlling the flow of data between UAVs. In contrast, UAVs themselves act as the data plane that acknowledges the controller's commands [195], whereas the application plane performs all decision-making and high-level operations like setting up network function virtualization. Several research works [196], [197], [198] have focused on switching and routing of UAV nodes for addressing security threats.

The authors in [196] have proposed an SDN-assisted system model for providing robust relaying and data security against intentional jamming by utilizing centralized SDN-controlled UAV switches. They have leveraged 3D coverage metrics to evaluate multiple diverse paths for UAVs to minimize the effects of malicious jamming. The authors in [197] have introduced an SDN-based architecture for secure communication with swarms of UAVs. The authors in [198] have proposed an NFV/SDN-aided security management model for deployment, configuration, and orchestration of VSFs like vProxies, vFirewalls, and vIDS in on-boarded MEC-UAVs.

1) KEY INSIGHTS OF THIS SECTION

1) The decoupling of a single plane into control, network, and data planes makes task scheduling and node fragmentation easy to alter.
2) There are benefits in scalability and flexibility in UAV networks by decoupling the data plane from the control plane, but the link between these planes is susceptible to threats like DDoS and DoS.
3) SDN along with NFV and ML-based strategies can be integrated to form efficient security management and intrusion detection model for UAV networks.

D. SECURED UAV COMMUNICATIONS USING FOG COMPUTING

SWAP constraints of UAVs limit the onboard computing capability, making it inefficient to perform computation-intensive tasks. Therefore, cloud-assisted computational offloading has been primarily utilized in UAV applications. But, the security threats to the computational offloads are severe concerns for the UAV-assisted offloading applications. In particular, the authors in [199] focused on securing the offloaded information against the eavesdropper in an EH and FD relaying protocol employed by UAV-assisted MEC. The expressions of the offloading time, data size, and transmit power were obtained, and additionally, they analyzed the full, partial, and non-offloading conditions. Finally, they optimized the PS ratio to enhance the computational resource and offload energy efficiency. In another work, [109] proposed the NOMA-based UAV-MEC system against the flying eavesdropper in which they have maximized the average security-computational capacity by ensuring minimum security computation required at each ground unit.

However, excessive delay and the requirement of cloud-UAVs connecting infrastructures restrict the

deployment of UAVs in various low latency and remote application scenarios, respectively. Additionally, cloud-based servers are difficult and costly to deploy. Thus, to overcome these limitations and extend the capabilities of cloud applications, fog computing is used [23]. When the user queries for fetching or uploading data requests, the nearest stratum of the fog layer connects between cloud and edge devices with the assistance of mobile networks. Fog does not consist of any single entity for handling the data. In contrast, multiple fog layers are used to store the data that secures confidential information from any vulnerabilities compared to storing it in a single place. Several works [200], [201], [202] have considered the security issues in fog-assisted UAV communication to counter the security threats.

With the aim of meeting low latency and high-reliability requirements, the authors in [200] have considered using a UAV as a fog node that operates as an aerial fog computing system and addresses the UAV's flight security. They have proposed a GPS spoofing detection technique for UAV's IMU sensor and monocular camera and have also utilized oriented fast and rotated brief-based error reduction to localize autonomous UAVs. The authors in [201] have considered the delay in the cloud-aided computation of UAV's deployment in harsh conditions and proposed an FCSD framework. They have formulated the task allocation minimization problem for energy consumption of FCSD architecture and adopted a proximal-Jacobi ADMM-assisted distributed algorithm to solve it. Massive data aggregation in fog-aided UAV communications may lead to network traffic and privacy leakage, which can be countered using FL techniques. Thus, the authors in [202] have introduced an FL-based security system for preserving the UAV's data privacy and training parameters in the fog node. Using a low-complexity FL-based algorithm, they have optimally solved the security rate maximization non-linear programming problem.

1) KEY INSIGHTS OF THIS SECTION

1) Fog computing, along with MEC, provides a high computational capacity to UAVs so that they can impart computation offloading to terrestrial users.
2) Fog computing mainly focuses on reducing the latency of the system. However, it can also be leveraged along with several ML algorithms to counter threats like man-in-the-center, GPS spoofing, and eavesdropping.
3) Distributed data handling with fog computing makes the UAV's data difficult to overhear.

E. SECURED UAV COMMUNICATIONS USING COVERT COMMUNICATION

In any secured communication, the radiation source of the signal can be identified and physically attacked by advanced encryption and analysis of the source-to-destination side channel. Recently, researchers have focused on covert communication that takes the security of UAV networks to an advanced level by hiding not only confidential information but also its origin and existence [203]. Covert communication utilizes a low probability of intercept/detection technique that provides better performance than traditional spread spectrum techniques to realize covertness. A UAV can act as a warden for detecting the suspicious transmission, and also, its mobility and LoS link are exploited to weaken the malicious warden's signal strength by inferring AN. Several works [128], [204], [205], [206] have performed optimization of the UAV's trajectory and altitude to increase the covertness nature of transmission.

The authors in [204] have analyzed crucial challenges in cooperative jamming and mode selection for covert communication in UAV-assisted D2D communications. They aim to enhance the covert capacity performance by integrating the mode selection method to adopt HD and FD communication modes dynamically. Meanwhile, idle device links can employ cooperative jamming to confuse the adversaries. The work in [205] has considered FD UAV-based covert communication network for gathering data from scheduled ground users and simultaneously transmitting AN to restrict unscheduled users from detecting the data. They have jointly optimized the 3D deployment and transmission power of UAVs to maximize the covertness subject to communication quality constraints. They have derived compact expressions for the UAV's optimal transmission power and 3D location by considering finite blocklength coding.

The authors in [128] have analyzed a novel covert communication system by exploiting novel spatial diversity for AN interfering UAV jammer-aided technique. Further, UAV-based covert A2G communication has been discussed in [206] for hiding the wireless data transmission based upon the overall detection error probability of the warden. Herein, the UAV's trajectory and resource allocation are optimized to maximize the average covert rate by considering the warden's location uncertainty. Further, the authors in [203] have also focused on improving the covert rate by confusing the warden via a jamming approach to enhance the covertness of a UAV-aided secured network.

1) KEY INSIGHTS OF THIS SECTION

1) Covert communication complements UAV-assisted military or other dissipative-prone applications by hiding the monitoring UAV's locations and the information transmitted to its C&CC.
2) UAV's dominant LoS link makes it prominent for covert communication. Additionally, the UAV's trajectory and operating height can be optimized to enhance covertness.

VIII. LESSONS LEARNED AND FUTURE RESEARCH DIRECTIONS

Security threats in UAV-assisted wireless communication are extensively investigated and classified in the previous sections. The paper also explores many approaches and techniques implemented for mitigating assaults on UAV-assisted communication networks. Nevertheless, several unresolved challenges need to be addressed to fully facilitate the

successful implementation of aerial networks, and they are elaborated in this section.

A. SECURITY AND PRIVACY STRATEGIES WITH ARTIFICIAL INTELLIGENCE

AI-based measures are required for UAV networks, which are prone to several sophisticated cyber-based threats. Utilizing AI methods can significantly enhance security and privacy in UAV-assisted communication systems. These learning techniques can be utilized to predict the non-deterministic behavior of the channels and an attacker's presence through prior experiences. In addition to immense challenges regarding selecting appropriate algorithms like RL, DRL, CNN, DDPG, for practical imperfect and stochastic cases, the real-time implementation of these algorithms requires further exploration.

B. LIGHTWEIGHT INTRUSION DETECTION SYSTEM

The majority of existing security and privacy protection methods for UAV networks either retain security breaches, or their deployment might not be feasible due to their hardware complexity. It is crucial and necessary to maintain a trade-off between these two facts. Real-time analysis of network traffic and anomaly monitoring and detecting malicious activities can be done by adopting honeypot and honeynets and IDS. However, the trade-off between performance and security puts a constraint on developing such frameworks. Consequently, designing compact and verified security approaches for UAV deployment remains an important field of research.

C. MOBILE EDGE COMPUTING

MEC devices can be incorporated with UAVs to extend their performance. Being mobile, they can assist the UAVs in moving along their trajectory freely and accurately. Due to reliable computations, MEC simultaneously predetermines the navigational coordinates and presence of malicious objects. Furthermore, they have greater computational processing and storage capacity than UAVs, allowing faster and more effective communication. Consequently, the communicated messages are offloaded to the nearest authenticated MEC device to reduce the computational complexity. However, they require higher storage capacity and advanced infrastructure, making them expensive. Additionally, handling a large amount of data also imposes security constraints.

D. REINFORCEMENT LEARNING FOR UAV's SAR APPLICATIONS

High-fidelity cameras with higher resolutions are preferred in the public domain as well as in civilian and military applications. Similarly, UAVs' flexible trajectory is responsible for their higher accessibility. By exploiting image processing and RL techniques, UAVs can be configured to select the optimum hovering site or aerial trajectory for data transmission between both the UAVs and the target terrestrial base station (when the UAV is functioning as a piece of aerial user equipment) or between the UAV and terrestrial user equipment (when the UAV is operating as an aerial base station). RL benefits from environment-based learning that can be exploited to estimate unpredictable trajectories and routes with low latency and accurately detect unpredictable targets in SAR applications. Joint optimization of operating altitude, 3D positioning, and effective trajectory planning of the UAVs requires efficient learning-based algorithms for the B5G communication scenarios. Additionally, learning techniques are more prone to software attacks due to the diverse environment.

E. SECURE UAV-CORE NETWORK

There is a requirement to develop secure and reliable UAV communication protocols that can enhance confidential data exchange secrecy between multiple UAVs or UAVs to different interfaces. Authentication and authorization schemes can leverage false data injecting, replay, and impersonation attacks. However, these are still serious concerns for researchers. Specific network models like FANET have been investigated, considering multi-UAV nodes and UAV swarm networks. Nevertheless, these are vulnerable to eavesdropping and several attacks due to networks' open access and strong LoS availability of UAVs that either terrestrial or aerial intruders can attack. Several routing algorithms are proposed to address these issues, but they are insufficient to provide satisfactory performance and security. Blockchain-enabled and software-based security algorithms and network design for dynamic UAV topology can offer promising solutions.

F. BLOCKCHAIN RESOURCE CONSTRAINTS

Cryptographic keys and hash-based blockchain techniques can assist in effectively managing tasks and provide security in multi-UAV and UAV swarms applications against GPS spoofing, wormhole attacks, jamming, DoS, and eavesdropping. Several consensus algorithms are constrained in providing high throughput in the distributed network. In addition to drawbacks in the current architecture, blockchain's security algorithms also impose a high computational delay to the UAV swarm network, making it unsuitable in critical and low latency applications. Blockchain technologies are still in their infancy and require further research to fit as a security solution to resource-constrained UAVs. Future developments in consensus algorithms and software-based cryptographic key impairments can lead to useful solutions for UAV security.

G. FOG ARCHITECTURE DESIGN

The use of fog nodes can provide higher scalability, QoS and flexible adoption, least platform dependency, low latency, and enhanced network security against GPS spoofing, hijacking, DoS attacks, and eavesdropping. Although these benefits make fog nodes suitable for UAV applications requiring extensive data handling, high computation, and low latency, the existing architecture lacks task-sharing and inter-fog layer resourcing. By fixing these shortcomings, fog nodes can interact among themselves to share the loaded tasks and reduce UAV's energy consumption by distributing the

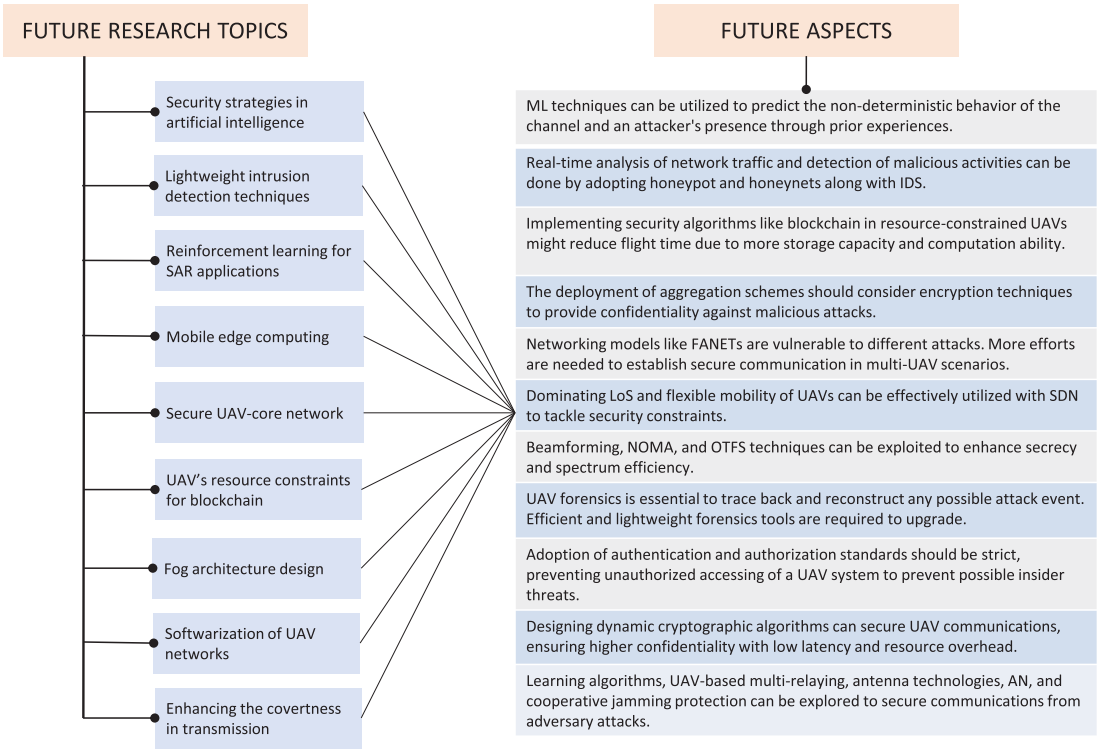

FIGURE 14. Summary of future research topics and different aspects.

computational tasks equitably. The inter-layer resourcing can form the aerial fog platform to serve terrestrial users seeking offloading tasks. The independence of the task handling from the cloud will reduce the latency and enhance security thanks to the reduced data transfer from fog to cloud.

H. CONTROL PLANE FAILURE IN SDN AND NFV

Automation of the network makes it more flexible, scalable, and agile. As a sequence, it can adjust to dynamic variations of the channel, UAV's trajectory, and task scheduling. It can secure the UAV communication against jamming, DoS black holes, and GPS spoofing. SDN generally separates a single application plane into control and data planes, increasing the delay and making it unsuitable for low latency applications. Moreover, a single control plane is responsible for the decision-making, so failure to it can affect the complete architecture. Distributed and multi controllers can overcome this issue. NFV can be integrated with SDN to minimize the complexity and improve the latency issue of SDN-based UAV communications. Further research can ensure secure near-time communication among SDN controllers to make UAV networks more flexible and secure.

I. ENHANCING COVERTNESS IN UAV COMMUNICATION

Covert communication provides three important benefits by using the LPD technique to mask the authentic wireless transmission from the malicious adversary. First, apart from other PHY security techniques, it prevents the intruder from identifying any transmission in the network, thus avoiding the launch of an attack. Second, it is cost-effective as compared to encryption techniques. Third, it can be complemented with AI-based learning algorithms. However, enhancements of covertness in the transmission model can be achieved at the cost of increasing the latency and reducing the transmission rate. Thus, several learning algorithms like federated learning, DL, and DRL techniques can be a key solution to reduce this time-lapse. Additionally, channel estimation and modeling and prediction of malicious nodes or devices can be accurately made by DRL techniques based on past experiences. However, more research is required to acquire the benefits of learning algorithms such as UAV-based multi-relaying, massive antenna technologies, AN, and cooperative jamming to protect the learning models from adversary attacks.

IX. CONCLUSION

UAVs have been employed in many practical applications, including civilian and defense applications, due to their adaptability, agility, relatively low cost, and ease of deployment. In recent years, UAVs have flourished with skyrocketed needs for civilian applications such as agronomic preservation, search and rescue operations, weather forecast and natural calamity monitoring, healthcare, etc. Moreover, UAVs have also emerged as an integral part of communication links between IoT infrastructures and cellular clusters. Within the domain of wireless communication systems, UAVs can

serve as relay nodes, airborne ground stations, and form infrastructure in remote areas. But security and privacy of UAV-assisted wireless networks are serious aspects concerning their performance and reliability. Our comprehensive survey have focused on security issues and mitigation techniques in UAV-assisted wireless communications systems, considering security as the top priority.

- First, we have provided a detailed background of different security attacks like navigational, data injecting, software installation, etc., along with secrecy performance metrics commonly adopted in the literature.
- Then, a detailed classification of various existing and emerging security threats in UAV networks has been provided.
- Later, we have performed an up-to-date exhaustive review of realistic and effective mitigation solutions for UAV communications in multiple domains like defense, maritime and satellite communication, IoT applications, etc.
- In our work, the mitigation techniques have been comprehensively discussed by sub-categorizing them into UAV-assisted counter methods and B5G paradigms, cooperative networks using UAV swarms, and various emerging techniques.
- Based on the survey, we have provided key findings on existing and emerging technologies, and several promising areas for future research.

As UAV cellular communication is still at an early development stage, we firmly believe that research related to security issues is a pressing need and a worthwhile research domain. In particular, new research directions concerning secured wireless communications integrating satellite and terrestrial bases with UAV relay nodes will flourish in the coming years.

REFERENCES

[1] S. Li, L. D. Xu, and S. Zhao, "5G Internet of Things: A survey," *J. Ind. Inf. Integr.*, vol. 10, pp. 1–9, Jun. 2018.
[2] D. Wang, B. Bai, W. Zhao, and Z. Han, "A survey of optimization approaches for wireless physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1878–1911, 2nd Quart., 2019.
[3] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, Feb. 2019.
[4] K. M. Alam, M. Saini, and A. E. Saddik, "Toward social Internet of Vehicles: Concept, architecture, and applications," *IEEE Access*, vol. 3, pp. 343–357, 2015.
[5] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks security and privacy in emerging wireless networks," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 56–62, Oct. 2010.
[6] K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33–39, Jun. 2015.
[7] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.
[8] Z. Ding, M. Xu, Y. Chen, M. G. Peng, and H. V. Poor, "Embracing non-orthogonal multiple access in future wireless networks," *Frontiers Inf. Technol. Electron. Eng.*, vol. 19, no. 3, pp. 322–339, 2018.
[9] N. Wang, L. Jiao, A. Alipour-Fanid, M. Dabaghchian, and K. Zeng, "Pilot contamination attack detection for NOMA in 5G mm-wave massive MIMO networks," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1363–1378, 2020.
[10] X. Tang, P. Ren, Y. Wang, and Z. Han, "Combating full-duplex active eavesdropper: A hierarchical game perspective," *IEEE Trans. Commun.*, vol. 65, no. 3, pp. 1379–1395, Mar. 2017.
[11] C. Wang and H.-M. Wang, "Physical layer security in millimeter wave cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5569–5585, Aug. 2016.
[12] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.
[13] T. A. Ahanger and A. Aljumah, "Internet of Things: A comprehensive study of security issues and defense mechanisms," *IEEE Access*, vol. 7, pp. 11020–11028, 2019.
[14] M. Y. Arafat and S. Moh, "JRCS: Joint routing and charging strategy for logistics drones," *IEEE Internet Things J.*, early access, Jun. 14, 2022, doi: 10.1109/JIOT.2022.3182750.
[15] E. Dahlman, G. Mildh, S. Parkvall, J. Peisa, J. Sachs, Y. Selén, and J. Sköld, "5G wireless access: Requirements and realization," *IEEE Commun. Mag.*, vol. 52, no. 12, pp. 42–47, Dec. 2014.
[16] S. A. R. Naqvi, S. A. Hassan, H. Pervaiz, and Q. Ni, "Drone-aided communication as a key enabler for 5G and resilient public safety networks," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 36–42, Jan. 2018.
[17] V. Sharma, M. Bennis, and R. Kumar, "UAV-assisted heterogeneous networks for capacity enhancement," *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1207–1210, Jun. 2016.
[18] P. Yang, X. Cao, C. Yin, Z. Xiao, X. Xi, and D. Wu, "Proactive drone-cell deployment: Overload relief for a cellular network under flash crowd traffic," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 10, pp. 2877–2892, Oct. 2017.
[19] T.-X. Zheng, H.-M. Wang, Q. Yang, and M. H. Lee, "Safeguarding decentralized wireless networks using full-duplex jamming receivers," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 278–292, Jan. 2017.
[20] Z. Ullah, F. Al-Turjman, and L. Mostarda, "Cognition in UAV-aided 5G and beyond communications: A survey," *IEEE Trans. Cognit. Commun. Netw.*, vol. 6, no. 3, pp. 872–891, Sep. 2020.
[21] H. Shakhatreh, A. H. Sawalmeh, A. Al-Fuqaha, Z. Dou, E. Almaita, I. Khalil, N. S. Othman, A. Khreishah, and M. Guizani, "Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges," *IEEE Access*, vol. 7, pp. 48572–48634, 2019.
[22] N. H. Motlagh, T. Taleb, and O. Arouk, "Low-altitude unmanned aerial vehicles-based Internet of Things services: Comprehensive survey and future perspectives," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 899–922, Dec. 2016.
[23] B. Alzahrani, O. S. Oubbati, A. Barnawi, M. Atiquzzaman, and D. Alghazzawi, "UAV assistance paradigm: State-of-the-art in applications and challenges," *J. Netw. Comput. Appl.*, vol. 166, Sep. 2020, Art. no. 102706.
[24] Q. Wu, W. Mei, and R. Zhang, "Safeguarding wireless network with UAVs: A physical layer security perspective," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 12–18, Oct. 2019.
[25] D.-Y. Kim and J.-W. Lee, "Joint mission assignment and topology management in the mission-critical FANET," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 2368–2385, Mar. 2020.
[26] M. Y. Arafat, S. Poudel, and S. Moh, "Medium access control protocols for flying ad hoc networks: A review," *IEEE Sensors J.*, vol. 21, no. 4, pp. 4097–4121, Feb. 2021.
[27] Y. Liu, C.-X. Wang, H. Chang, Y. He, and J. Bian, "A novel non-stationary 6G UAV channel model for maritime communications," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 10, pp. 2992–3005, Oct. 2021.
[28] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A survey on 5G networks for the Internet of Things: Communication technologies and challenges," *IEEE Access*, vol. 6, pp. 3619–3647, 2017.
[29] A. A. Khuwaja, Y. Chen, N. Zhao, M.-S. Alouini, and P. Dobbins, "A survey of channel modeling for UAV communications," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2804–2821, 4th Quart., 2018.
[30] V. Hassija, V. Chamola, A. Agrawal, A. Goyal, N. C. Luong, D. Niyato, F. R. Yu, and M. Guizani, "Fast, reliable, and secure drone communication: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2802–2832, 2021.

[31] N. Wang, L. Jiao, and K. Zeng, "Pilot contamination attack detection for NOMA in mm-wave and massive MIMO 5G communication," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, May 2018, pp. 1–9.

[32] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.

[33] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[34] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8169–8181, Oct. 2019.

[35] Y. Zeng, Q. Wu, and R. Zhang, "Accessing from the sky: A tutorial on UAV communications for 5G and beyond," *Proc. IEEE*, vol. 107, no. 12, pp. 2327–2375, Dec. 2019.

[36] C. Zhang, W. Zhang, W. Wang, L. Yang, and W. Zhang, "Research challenges and opportunities of UAV millimeter-wave communications," *IEEE Wireless Commun.*, vol. 26, no. 1, pp. 58–62, Feb. 2019.

[37] J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, "Security analysis of drones systems: Attacks, limitations, and recommendations," *Internet Things*, vol. 11, Sep. 2020, Art. no. 100218.

[38] B. Li, Z. Fei, C. Zhou, and Y. Zhang, "Physical-layer security in space information networks: A survey," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 33–52, Jan. 2020.

[39] M. Leccadito, T. Bakker, R. Klenke, and C. Elks, "A survey on securing UAS cyber physical systems," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 33, no. 10, pp. 22–32, Oct. 2018.

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

[41] A. Fotouhi, H. Qiang, M. Ding, M. Hassan, L. G. Giordano, A. G. Rodriguez, and J. Yuan, "Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3417–3442, 4th Quart., 2019.

[42] M. Yahuza, M. Y. I. Idris, I. B. Ahmedy, A. W. A. Wahab, T. Nandy, N. M. Noor, and A. Bala, "Internet of Drones security and privacy issues: Taxonomy and open challenges," *IEEE Access*, vol. 9, pp. 57243–57270, 2021.

[43] A. Shafique, A. Mehmood, and M. Elhadef, "Survey of security protocols and vulnerabilities in unmanned aerial vehicles," *IEEE Access*, vol. 9, pp. 46927–46948, 2021.

[44] Y. Mekdad, A. Aris, L. Babun, A. E. Fergougui, M. Conti, R. Lazzeretti, and A. S. Uluagac, "A survey on security and privacy issues of UAVs," 2021, *arXiv:2109.14442*.

[45] F. Syed, D. S. Gupta, S. Alsamhi, M. Rashid, and X. Liu, "A survey on recent optimal techniques for securing unmanned aerial vehicles applications," *Trans. Emerg. Telecommun. Tech.*, vol. 32, p. e4133, Jul. 2021.

[46] J. Wang, X. Wang, R. Gao, C. Lei, W. Feng, N. Ge, S. Jin, and T. Q. S. Quek, "Physical layer security for UAV communications in 5G and beyond networks," 2021, *arXiv:2105.11332*.

[47] A. Y. Javaid, W. Sun, V. K. Devabhaktuni, and M. Alam, "Cyber security threat analysis and modeling of an unmanned aerial vehicle system," in *Proc. IEEE Conf. Technol. Homeland Secur. (HST)*, Nov. 2012, pp. 585–590.

[48] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 4, pp. 42–56, 4th Quart., 2009.

[49] C. G. L. Krishna and R. R. Murphy, "A review on cybersecurity vulnerabilities for unmanned aerial vehicles," in *Proc. IEEE Int. Symp. Saf., Secur. Rescue Robot. (SSRR)*, Oct. 2017, pp. 194–199.

[50] Q. J. O. Tan and R. A. Romero, "Jammer nulling adaptive waveforms with cognitive radar for aircraft RCS recognition in presence of frequency sweep and base jammers," in *Proc. 52nd Asilomar Conf. Signals, Syst., Comput.*, Oct. 2018, pp. 1339–1343.

[51] S. Dong, K. Abbas, and R. Jain, "A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments," *IEEE Access*, vol. 7, pp. 80813–80828, 2019.

[52] M. Hooper, Y. Tian, R. Zhou, B. Cao, A. P. Lauf, L. Watkins, W. H. Robinson, and W. Alexis, "Securing commercial WiFi-based UAVs from common security attacks," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Nov. 2016, pp. 1213–1218.

[53] D. He, S. Chan, and M. Guizani, "Communication security of unmanned aerial vehicles," *IEEE Wireless Commun.*, vol. 24, no. 4, pp. 134–139, Aug. 2017.

[54] C. Javali, G. Revadigar, M. Ding, and S. Jha, "Secret key generation by virtual link estimation," in *Proc. 10th EAI Int. Conf. Body Area Netw.*, 2015, pp. 301–307.

[55] M. H. Yilmaz and H. Arslan, "A survey: Spoofing attacks in physical layer security," in *Proc. IEEE 40th Local Comput. Netw. Conf. Workshops (LCN Workshops)*, Oct. 2015, pp. 812–817.

[56] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based detection of Sybil attacks in wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 3, pp. 492–503, Sep. 2009.

[57] M. Chraiti, A. Ghrayeb, C. Assi, and M. O. Hasna, "On the achievable secrecy diversity of cooperative networks with untrusted relays," *IEEE Trans. Commun.*, vol. 66, no. 1, pp. 39–53, Jan. 2018.

[58] I. Jawhar, N. Mohamed, J. Al-Jaroodi, D. P. Agrawal, and S. Zhang, "Communication and networking of UAV-based systems: Classification and associated architectures," *J. Netw. Comput. Appl.*, vol. 84, pp. 93–108, Apr. 2017.

[59] K. Namuduri, S. Chaumette, K. Jae, and S. James, *UAV Networks and Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2017.

[60] D. He, S. Chan, and M. Guizani, "Drone-assisted public safety networks: The security aspect," *IEEE Commun. Mag.*, vol. 55, no. 8, pp. 218–223, Aug. 2017.

[61] S. P. Arteaga, L. A. M. Hernandez, G. S. Perez, A. L. S. Orozco, and L. J. G. Villalba, "Analysis of the GPS spoofing vulnerability in the drone 3DR solo," *IEEE Access*, vol. 7, pp. 51782–51789, 2019.

[62] M. Karimibiuki, M. Aibin, Y. Lai, R. Khan, R. Norfield, and A. Hunter, "Drones face off: Authentication by machine learning in autonomous IoT systems," in *Proc. IEEE 10th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, Oct. 2019, pp. 0329–0333.

[63] P. Zimmer, R. Weinreich, C. T. Zenger, A. Sezgin, and C. Paar, "Keys from the sky: A first exploration of physical-layer security using satellite links," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2021, pp. 1–7.

[64] P. Tedeschi, G. Oligeri, and R. Di Pietro, "Leveraging jamming to help drones complete their mission," *IEEE Access*, vol. 8, pp. 5049–5064, 2020.

[65] G. Panice, S. Luongo, G. Gigante, D. Pascarella, C. D. Benedetto, A. Vozella, and A. Pescape, "A SVM-based detection approach for GPS spoofing attacks to UAV," in *Proc. 23rd Int. Conf. Autom. Comput. (ICAC)*, Sep. 2017, pp. 1–11.

[66] D. Mendes, N. Ivaki, and H. Madeira, "Effects of GPS spoofing on unmanned aerial vehicles," in *Proc. IEEE 23rd Pacific Rim Int. Symp. Dependable Comput. (PRDC)*, Dec. 2018, pp. 155–160.

[67] M. R. Manesh, J. Kenney, W. C. Hu, V. K. Devabhaktuni, and N. Kaabouch, "Detection of GPS spoofing attacks on unmanned aerial systems," in *Proc. 16th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2019, pp. 1–6.

[68] H. Zhu, M. L. Cummings, M. Elfar, Z. Wang, and M. Pajic, "Operator strategy model development in UAV hacking detection," *IEEE Trans. Hum.-Mach. Syst.*, vol. 49, no. 6, pp. 540–549, Dec. 2019.

[69] Y. Guo, M. Wu, K. Tang, J. Tie, and X. Li, "Covert spoofing algorithm of UAV based on GPS/INS-integrated navigation," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6557–6564, Jul. 2019.

[70] A. Eldosouky, A. Ferdowsi, and W. Saad, "Drones in distress: A game-theoretic countermeasure for protecting UAVs against GPS spoofing," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2840–2854, Apr. 2020.

[71] Y. Qiao, Y. Zhang, and X. Du, "A vision-based GPS-spoofing detection method for small UAVs," in *Proc. 13th Int. Conf. Comput. Intell. Secur. (CIS)*, Dec. 2017, pp. 312–316.

[72] I. G. Ferrao, S. A. Da Silva, D. F. Pigatto, and K. R. Branco, "GPS spoofing: Detecting GPS fraud in unmanned aerial vehicles," in *Proc. Latin Amer. Robot. Symp. (LARS), Brazilian Symp. Robot. (SBR) Workshop Robot. Educ. (WRE)*, Nov. 2020, pp. 1–6.

[73] C. Jiang, S. Chen, B. Zhang, Y. Chen, Y. Bo, and Z. Feng, "Effectiveness analysis of the covariance matrix for spoofing detection application," in *Proc. Ubiquitous Positioning, Indoor Navigat. Location-Based Services (UPINLBS)*, 2018, pp. 1–5.

[74] H. Mei, H. Changyi, and W. Guangming, "Novel method to evaluate the effectiveness of UAV navigation spoofing," in *Proc. 14th IEEE Int. Conf. Electron. Meas. Instrum. (ICEMI)*, Nov. 2019, pp. 1388–1395.

[75] K. Jansen, M. Schafer, D. Moser, V. Lenders, C. Popper, and J. Schmitt, "Crowd-GPS-sec: Leveraging crowdsourcing to detect and localize GPS spoofing attacks," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2018, pp. 1018–1031.

[76] Q. Zou, S. Huang, F. Lin, and M. Cong, "Detection of GPS spoofing based on UAV model estimation," in *Proc. IECON 42nd Annu. Conf. IEEE Ind. Electron. Soc.*, Oct. 2016, pp. 6097–6102.
[77] Q.-Y. Fu, Y.-H. Feng, H.-M. Wang, and P. Liu, "Initial satellite access authentication based on Doppler frequency shift," *IEEE Wireless Commun. Lett.*, vol. 10, no. 3, pp. 498–502, Mar. 2021.
[78] R. Han, L. Bai, J. Liu, and P. Chen, "Blockchain-based GNSS spoofing detection for multiple UAV systems," *J. Commun. Inf. Netw.*, vol. 4, no. 2, pp. 81–88, Jun. 2019.
[79] J. Gaspar, R. Ferreira, P. Sebastiao, and N. Souto, "Capture of UAVs through GPS spoofing," in *Proc. Global Wireless Summit (GWS)*, Nov. 2018, pp. 21–26.
[80] W. Chen, Y. Dong, and Z. Duan, "Manipulating drone position control," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Jun. 2019, pp. 1–9.
[81] A. Koubaa, B. Qureshi, M.-F. Sriti, A. Allouch, Y. Javed, M. Alajlan, O. Cheikhrouhou, M. Khalgui, and E. Tovar, "Dronemap Planner: A service-oriented cloud-based management system for the Internet-of-Drones," *Ad Hoc Netw. J.*, vol. 86, pp. 46–62, Apr. 2019.
[82] S. Sciancalepore, O. A. Ibrahim, G. Oligeri, and R. Di Pietro, "PiNcH: An effective, efficient, and robust solution to drone detection via network traffic analysis," *Comput. Netw.*, vol. 168, Feb. 2020, Art. no. 107044.
[83] T. Alladi, V. Chamola, B. Sikdar, and K. R. Choo, "Consumer IoT: Security vulnerability case studies and solutions," *IEEE Consum. Electron. Mag.*, vol. 9, no. 2, pp. 17–25, Mar. 2020.
[84] P. Perazzo, K. Ariyapala, M. Conti, and G. Dini, "The verifier bee: A path planner for drone-based secure location verification," in *Proc. IEEE 16th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2015, pp. 1–9.
[85] W. Chen, Y. Dong, and Z. Duan, "Compromising flight paths of autopiloted drones," in *Proc. Int. Conf. Unmanned Aircr. Syst. (ICUAS)*, Jun. 2019, pp. 1316–1325.
[86] Y.-M. Kwon, J. Yu, B.-M. Cho, Y. Eun, and K.-J. Park, "Empirical analysis of MAVLink protocol vulnerability for attacking unmanned aerial vehicles," *IEEE Access*, vol. 6, pp. 43203–43212, 2018.
[87] L. Zhang, G. Ding, Q. Wu, and P. Liu, "Detection of abnormal power emission in UAV communication networks," *IEEE Wireless Commun. Lett.*, vol. 8, no. 4, pp. 1179–1182, Aug. 2019.
[88] Y. Liu, A. Liu, X. Liu, and M. Ma, "A trust-based active detection for cyber-physical security in industrial environments," *IEEE Trans. Ind. Informat.*, vol. 15, no. 12, pp. 6593–6603, Dec. 2019.
[89] A. Islam and S. Y. Shin, "BUAV: A blockchain based secure UAV-assisted data acquisition scheme in Internet of Things," *J. Commun. Netw.*, vol. 21, no. 5, pp. 491–502, Oct. 2019.
[90] A. Sanjab, W. Saad, and T. Basar, "A game of drones: Cyber-physical security of time-critical UAV applications with cumulative prospect theory perceptions and valuations," *IEEE Trans. Commun.*, vol. 68, no. 11, pp. 6990–7006, Nov. 2020.
[91] W. Niu, J. Xiao, X. Zhang, X. Zhang, X. Du, X. Huang, and M. Guizani, "Malware on internet of UAVs detection combining string matching and Fourier transformation," *IEEE Internet Things J.*, vol. 8, no. 12, pp. 9905–9919, Jun. 2021.
[92] M. Keshavarz, M. Gharib, F. Afghah, and J. D. Ashdown, "UAS-TrustChain: A decentralized blockchain-based trust monitoring framework for autonomous unmanned aerial systems," *IEEE Access*, vol. 8, pp. 226074–226088, 2020.
[93] T. Alladi, N. Naren, G. Bansal, V. Chamola, and M. Guizani, "SecAuthUAV: A novel authentication scheme for UAV-ground station and UAV-UAV communication," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 15068–15077, Dec. 2020.
[94] C. Liu, T. Q. S. Quek, and J. Lee, "Secure UAV communication in the presence of active eavesdropper (invited paper)," in *Proc. 9th Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Oct. 2017, pp. 1–6.
[95] C. Liu, J. Lee, and T. Q. S. Quek, "Safeguarding UAV communications against full-duplex active eavesdropper," *IEEE Trans. Wireless Commun.*, vol. 18, no. 6, pp. 2919–2931, Jun. 2019.
[96] X. Wang, W. Feng, Y. Chen, and N. Ge, "UAV swarm-enabled aerial CoMP: A physical layer security perspective," *IEEE Access*, vol. 7, pp. 120901–120916, 2019.
[97] H. Wu, Y. Wen, J. Zhang, Z. Wei, N. Zhang, and X. Tao, "Energy-efficient and secure air-to-ground communication with jittering UAV," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 3954–3967, Apr. 2020.
[98] Z. Sheng, H. D. Tuan, A. A. Nasir, T. Q. Duong, and H. V. Poor, "Secure UAV-enabled communication using Han–Kobayashi signaling," *IEEE Trans. Wireless Commun.*, vol. 19, no. 5, pp. 2905–2919, May 2020.
[99] A. Li, W. Zhang, and S. Dou, "UAV-enabled secure data dissemination via artificial noise: Joint trajectory and communication optimization," *IEEE Access*, vol. 8, pp. 102348–102356, 2020.
[100] Q. Ning, T. Yang, B. Chen, X. Zhou, C. Zhao, and X. Yang, "Cooperative transmission of wireless information and energy in anti-eavesdropping UAV relay network," *IEEE Trans. Green Commun. Netw.*, vol. 5, no. 3, pp. 1283–1292, Sep. 2021.
[101] M. T. Mamaghani and Y. Hong, "Intelligent trajectory design for secure full-duplex MIMO-UAV relaying against active eavesdroppers: A model-free reinforcement learning approach," *IEEE Access*, vol. 9, pp. 4447–4465, 2021.
[102] M. T. Mamaghani and Y. Hong, "Joint trajectory and power allocation design for secure artificial noise aided UAV communications," *IEEE Trans. Veh. Technol.*, vol. 70, no. 3, pp. 2850–2855, Mar. 2021.
[103] J. Lyu and H.-M. Wang, "Secure UAV random networks with minimum safety distance," *IEEE Trans. Veh. Technol.*, vol. 70, no. 3, pp. 2856–2861, Mar. 2021.
[104] K. Xu, M.-M. Zhao, Y. Cai, and L. Hanzo, "Low-complexity joint power allocation and trajectory design for UAV-enabled secure communications with power splitting," *IEEE Trans. Commun.*, vol. 69, no. 3, pp. 1896–1911, Mar. 2021.
[105] X. He, X. Li, H. Ji, and H. Zhang, "Resource allocation for secrecy rate optimization in UAV-assisted cognitive radio network," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2021, pp. 1–6.
[106] Z. Yin, M. Jia, N. Cheng, W. Wang, F. Lyu, Q. Guo, and X. Shen, "UAV-assisted physical layer security in multi-beam satellite-enabled vehicle communications," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 3, pp. 2739–2751, Mar. 2022.
[107] J. J. Sadique, S. E. Ullah, M. R. Islam, R. Raad, A. Z. Kouzani, and M. A. P. Mahmud, "Transceiver design for full-duplex UAV based zero-padded OFDM system with physical layer security," *IEEE Access*, vol. 9, pp. 59432–59445, 2021.
[108] W. Wang, X. Li, R. Wang, K. Cumanan, W. Feng, Z. Ding, and O. A. Dobre, "Robust 3D-trajectory and time switching optimization for Dual-UAV-enabled secure communications," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 11, pp. 3334–3347, Nov. 2021.
[109] X. Gu, G. Zhang, M. Wang, W. Duan, M. Wen, and P.-H. Ho, "UAV-aided energy-efficient edge computing networks: Security offloading optimization," *IEEE Internet Things J.*, vol. 9, no. 6, pp. 4245–4258, Mar. 2022.
[110] S. J. Maeng, Y. Yapc, I. Guvenc, A. Bhuyan, and H. Dai, "Precoder design for physical-layer security and authentication in massive MIMO UAV communications," *IEEE Trans. Veh. Technol.*, vol. 71, no. 3, pp. 2949–2964, Mar. 2022.
[111] H. Fu, Z. Sheng, A. A. Nasir, A. H. Muqaibel, and L. Hanzo, "Securing the UAV-aided non-orthogonal downlink in the face of colluding eavesdroppers," *IEEE Trans. Veh. Technol.*, vol. 71, no. 6, pp. 6837–6842, Jun. 2022.
[112] C. Zhong, J. Yao, and J. Xu, "Secure UAV communication with cooperative jamming and trajectory control," *IEEE Commun. Lett.*, vol. 23, no. 2, pp. 286–289, Feb. 2019.
[113] M. Tatar Mamaghani and Y. Hong, "On the performance of low-altitude UAV-enabled secure AF relaying with cooperative jamming and SWIPT," *IEEE Access*, vol. 7, pp. 153060–153073, 2019.
[114] J. Miao and Z. Zheng, "Cooperative jamming for secure UAV-enabled mobile relay system," *IEEE Access*, vol. 8, pp. 48943–48957, 2020.
[115] W. Wang, X. Li, M. Zhang, K. Cumanan, D. W. K. Ng, G. Zhang, J. Tang, and O. A. Dobre, "Energy-constrained UAV-assisted secure communications with position optimization and cooperative jamming," *IEEE Trans. Commun.*, vol. 68, no. 7, pp. 4476–4489, Jul. 2020.
[116] R. Ma, W. Yang, Y. Zhang, J. Liu, and H. Shi, "Secure mmWave communication using UAV-enabled relay and cooperative jammer," *IEEE Access*, vol. 7, pp. 119729–119741, 2019.
[117] S. Hu, Q. Wu, and X. Wang, "Energy management and trajectory optimization for UAV-enabled legitimate monitoring systems," *IEEE Trans. Wireless Commun.*, vol. 20, no. 1, pp. 142–155, Jan. 2021.
[118] X. Pang, M. Liu, N. Zhao, Y. Chen, Y. Li, and F. R. Yu, "Secrecy analysis of UAV-based mmWave relaying networks," *IEEE Trans. Wireless Commun.*, vol. 20, no. 8, pp. 4990–5002, Aug. 2021.
[119] J. Hu, J. Shi, S. Ma, and Z. Li, "Secrecy analysis for orthogonal time frequency space scheme based uplink LEO satellite communication," *IEEE Wireless Commun. Lett.*, vol. 10, no. 8, pp. 1623–1627, Aug. 2021.

[120] W. Lu, Y. Ding, Y. Gao, S. Hu, Y. Wu, N. Zhao, and Y. Gong, "Resource and trajectory optimization for secure communications in dual unmanned aerial vehicle mobile edge computing systems," *IEEE Trans. Ind. Informat.*, vol. 18, no. 4, pp. 2704–2713, Apr. 2022.
[121] Z. Tao, F. Zhou, Y. Wang, X. Liu, and Q. Wu, "Resource allocation and trajectories design for UAV-assisted jamming cognitive UAV networks," *China Commun.*, vol. 9, pp. 206–217, May 2022.
[122] R. Zhang, X. Chen, M. Liu, N. Zhao, X. Wang, and A. Nallanathan, "UAV relay assisted cooperative jamming for covert communications over rician fading," *IEEE Trans. Veh. Technol.*, vol. 71, no. 7, pp. 7936–7941, Jul. 2022.
[123] X. Wang, K. Li, S. S. Kanhere, D. Li, X. Zhang, and E. Tovar, "PELE: Power efficient legitimate eavesdropping via jamming in UAV communications," in *Proc. 13th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2017, pp. 402–408.
[124] K. Li, S. S. Kanhere, W. Ni, E. Tovar, and M. Guizani, "Proactive eavesdropping via jamming for trajectory tracking of UAVs," in *Proc. 15th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2019, pp. 477–482.
[125] M. Zhang, H. Yi, Y. Chen, and X. Tao, "Proactive eavesdropping via jamming for power-limited UAV communications," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2019, pp. 1–5.
[126] K. Li, R. C. Voicu, S. S. Kanhere, W. Ni, and E. Tovar, "Energy efficient legitimate wireless surveillance of UAV communications," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2283–2293, Mar. 2019.
[127] J. Tang, G. Chen, and J. P. Coon, "Secrecy performance analysis of wireless communications in the presence of UAV jammer and randomly located UAV eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 11, pp. 3026–3041, Nov. 2019.
[128] W. Liang, J. Shi, Z. Tie, and F. Yang, "Performance analysis for UAV-jammer aided covert communication," *IEEE Access*, vol. 8, pp. 111394–111400, 2020.
[129] M. T. Mamaghani and Y. Hong, "Improving PHY-security of UAV-enabled transmission with wireless energy harvesting: Robust trajectory design and communications resource allocation," *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 8586–8600, Aug. 2020.
[130] M. Zhang, Y. Chen, X. Tao, and I. Darwazeh, "Power allocation for proactive eavesdropping with spoofing relay in UAV systems," in *Proc. 26th Int. Conf. Telecommun. (ICT)*, Apr. 2019, pp. 102–107.
[131] Y. Yang, B. Li, S. Zhang, W. Zhao, and L. Jiao, "Cooperative proactive eavesdropping over two-hop suspicious communication based on reinforcement learning," *J. Commun. Inf. Netw.*, vol. 6, no. 2, pp. 166–174, Jun. 2021.
[132] G. Hu, J. Ouyang, Y. Cai, and Y. Cai, "Proactive eavesdropping in two-way Amplify-and-forward relay networks," *IEEE Syst. J.*, vol. 15, no. 3, pp. 3415–3426, Sep. 2021.
[133] M. Y. Arafat and S. Moh, "A Q-learning-based topology-aware routing protocol for flying ad hoc networks," *IEEE Internet Things J.*, vol. 9, no. 3, pp. 1985–2000, Feb. 2022.
[134] H. Liu and K. S. Kwak, "Secrecy outage probability of UAV-aided selective relaying networks," in *Proc. 9th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2017, pp. 24–29.
[135] Z. Mobini, B. K. Chalise, M. Mohammadi, H. A. Suraweera, and Z. Ding, "Proactive eavesdropping using UAV systems with full-duplex ground terminals," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2018, pp. 1–6.
[136] A. Islam and S. Y. Shin, "BUS: A blockchain-enabled data acquisition scheme with the assistance of UAV swarm in Internet of Things," *IEEE Access*, vol. 7, pp. 103231–103249, 2019.
[137] G. Sun, N. Li, X. Tao, and H. Wu, "Power allocation in UAV-enabled relaying systems for secure communications," *IEEE Access*, vol. 7, pp. 119009–119017, 2019.
[138] A. S. Abdalla, B. Shang, V. Marojevic, and L. Liu, "Securing mobile IoT with unmanned aerial systems," in *Proc. IEEE 6th World Forum Internet Things (WF-IoT)*, Jun. 2020, pp. 1–6.
[139] A. S. Abdalla, B. Shang, V. Marojevic, and L. Liu, "Performance evaluation of aerial relaying systems for improving secrecy in cellular networks," in *Proc. IEEE 92nd Veh. Technol. Conf. (VTC-Fall)*, Nov. 2020, pp. 1–5.
[140] P. K. Sharma and D. I. Kim, "Secure 3D mobile UAV relaying for hybrid satellite-terrestrial networks," *IEEE Trans. Wireless Commun.*, vol. 19, no. 4, pp. 2770–2784, Apr. 2020.
[141] X. Yuan, Z. Feng, W. Ni, R. P. Liu, J. A. Zhang, and W. Xu, "Secrecy performance of terrestrial radio links under collaborative aerial eavesdropping," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 604–619, 2020.
[142] J. Miao, H. Li, Z. Zheng, and C. Wang, "Secrecy energy efficiency maximization for UAV swarm assisted multi-hop relay system: Joint trajectory design and power control," *IEEE Access*, vol. 9, pp. 37784–37799, 2021.
[143] A. S. Abdalla and V. Marojevic, "Securing mobile multiuser transmissions with UAVs in the presence of multiple eavesdroppers," *IEEE Trans. Veh. Technol.*, vol. 70, no. 10, pp. 11011–11016, Oct. 2021.
[144] W. Wang, H. Tian, and W. Ni, "Secrecy performance analysis of IRS-aided UAV relay system," *IEEE Wireless Commun. Lett.*, vol. 10, no. 12, pp. 2693–2697, Dec. 2021.
[145] J. Ji, K. Zhu, D. Niyato, and R. Wang, "Joint trajectory design and resource allocation for secure transmission in cache-enabled UAV-relaying networks with D2D communications," *IEEE Internet Things J.*, vol. 8, no. 3, pp. 1557–1571, Feb. 2021.
[146] Y. Ning and R. Chen, "Secure UAV relay communication via power allocation and trajectory planning," *IEEE Syst. J.*, early access, Jan. 20, 2022, doi: 10.1109/JSYST.2021.3134305.
[147] Y. He, D. Wang, F. Huang, R. Zhang, and J. Pan, "Trajectory optimization and channel allocation for delay sensitive secure transmission in UAV-relayed VANETs," *IEEE Trans. Veh. Technol.*, vol. 71, no. 4, pp. 4512–4517, Apr. 2022.
[148] F. Cheng, G. Gui, N. Zhao, Y. Chen, J. Tang, and H. Sari, "UAV-relaying-assisted secure transmission with caching," *IEEE Trans. Commun.*, vol. 67, no. 5, pp. 3140–3153, May 2019.
[149] R. Zhang, X. Pang, W. Lu, N. Zhao, Y. Chen, and D. Niyato, "Dual-UAV enabled secure data collection with propulsion limitation," *IEEE Trans. Wireless Commun.*, vol. 20, no. 11, pp. 7445–7459, Nov. 2021.
[150] D.-H. Tran, V.-D. Nguyen, S. Chatzinotas, T. X. Vu, and B. Ottersten, "UAV relay-assisted emergency communications in IoT networks: Resource allocation and trajectory optimization," *IEEE Trans. Wireless Commun.*, vol. 21, no. 3, pp. 1621–1637, Mar. 2022.
[151] T. Bao, H. Wang, W.-J. Wang, H.-C. Yang, and M. Hasna, "Secrecy outage performance analysis of UAV-assisted relay communication systems with multiple aerial and ground eavesdroppers," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 58, no. 3, pp. 2592–2600, Jun. 2022.
[152] Z. Na, C. Ji, B. Lin, and N. Zhang, "Joint optimization of trajectory and resource allocation in secure UAV relaying communications for Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 17, pp. 16284–16296, Sep. 2022.
[153] J. Ye, C. Zhang, H. Lei, G. Pan, and Z. Ding, "Secure UAV-to-UAV systems with spatially random UAVs," *IEEE Wireless Commun. Lett.*, vol. 8, no. 2, pp. 564–567, Apr. 2019.
[154] X. Wang, W. Feng, Y. Chen, and N. Ge, "Power allocation for UAV swarm-enabled secure networks using large-scale CSI," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6.
[155] D. Wang and Y. Yang, "Joint obstacle avoidance and 3D deployment for securing UAV-enabled cellular communications," *IEEE Access*, vol. 8, pp. 67813–67821, 2020.
[156] K. Wang, H. Lei, G. Pan, C. Pan, and Y. Cao, "Detection performance to spatially random UAV using the ground vehicle," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 16320–16324, Dec. 2020.
[157] S. Gao, Y. Ma, and B. Duo, "Safeguarding multi-UAVs relaying communications via joint trajectory design and power control," in *Proc. Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Oct. 2020, pp. 1182–1187.
[158] G. Raja, S. Anbalagan, A. Ganapathisubramaniyan, M. S. Selvakumar, A. K. Bashir, and S. Mumtaz, "Efficient and secured swarm pattern multi-UAV communication," *IEEE Trans. Veh. Technol.*, vol. 70, no. 7, pp. 7050–7058, Jul. 2021.
[159] R. Al-Share, M. Shurman, and A. Alma'aitah, "A collaborative learning-based algorithm for task offloading in UAV-aided wireless sensor networks," *Comput. J.*, vol. 64, no. 10, pp. 1575–1583, Oct. 2021.
[160] S. Li, B. Duo, M. D. Renzo, M. Tao, and X. Yuan, "Robust secure UAV communications with the aid of reconfigurable intelligent surfaces," *IEEE Trans. Wireless Commun.*, vol. 20, no. 10, pp. 6402–6417, Apr. 2021.
[161] T. Li, J. Ye, J. Dai, H. Lei, W. Yang, G. Pan, and Y. Chen, "Secure UAV-to-vehicle communications," *IEEE Trans. Commun.*, vol. 69, no. 8, pp. 5381–5393, Aug. 2021.
[162] M. T. Mamaghani and Y. Hong, "Terahertz meets untrusted UAV-relaying: Minimum secrecy energy efficiency maximization via trajectory and communication co-design," *IEEE Trans. Veh. Technol.*, vol. 71, no. 5, pp. 4991–5006, May 2022.
[163] H. Kang, X. Chang, J. Mixi, V. B. Mixi, J. Fan, and J. Bai, "Improving dual-UAV aided ground-UAV bi-directional communication security: Joint UAV trajectory and transmit power optimization," *IEEE Trans. Veh. Tech.*, pp. 1–14, 2022.

[164] M. Li, X. Tao, N. Li, H. Wu, and J. Xu, "Secrecy energy efficiency maximization in UAV-enabled wireless sensor networks without eavesdropper's CSI," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3346–3358, Mar. 2022.

[165] Z. Li, X. Liao, J. Shi, L. Li, and P. Xiao, "MD-GAN-based UAV trajectory and power optimization for cognitive covert communications," *IEEE Internet Things J.*, vol. 9, no. 12, pp. 10187–10199, Jun. 2022.

[166] Y. Wu, W. Yang, and X. Sun, "Securing UAV-enabled millimeter wave communication via trajectory and power optimization," in *Proc. IEEE 4th Int. Conf. Comput. Commun. (ICCC)*, Dec. 2018, pp. 970–975.

[167] Z. Yin, M. Jia, W. Wang, N. Cheng, F. Lyu, and X. Shen, "Max-min secrecy rate for NOMA-based UAV-assisted communications with protected zone," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6.

[168] W. Wang, J. Tang, N. Zhao, X. Liu, X. Y. Zhang, Y. Chen, and Y. Qian, "Joint precoding optimization for secure SWIPT in UAV-aided NOMA networks," *IEEE Trans. Commun.*, vol. 68, no. 8, pp. 5028–5040, Aug. 2020.

[169] Y. Wen, H. Wu, H. Li, and X. Tao, "Robust AN-aided secure beamforming design for A2G communication networks with UAV jitter," in *Proc. IEEE Wireless Commun. Netw. Conf. Workshops (WCNCW)*, Apr. 2020, pp. 1–6.

[170] K. Lin, Z. Ji, Y. Zhang, G. Chen, P. L. Yeoh, and Z. He, "Secret key generation based on 3D spatial angles for UAV communications," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2021, pp. 1–6.

[171] J. Wang, R. Han, L. Bai, T. Zhang, J. Liu, and J. Choi, "Coordinated beamforming for UAV-aided millimeter-wave communications using GPML-based channel estimation," *IEEE Trans. Cognit. Commun. Netw.*, vol. 7, no. 1, pp. 100–109, Mar. 2021.

[172] J. Wang, Y. Liu, S. Niu, and H. Song, "Extensive throughput enhancement for 5G-enabled UAV swarm networking," *IEEE J. Miniaturization Air Space Syst.*, vol. 2, no. 4, pp. 199–208, Dec. 2021.

[173] Y. Yapici, N. Rupasinghe, I. Guvenc, H. Dai, and A. Bhuyan, "Physical layer security for NOMA transmission in mmWave drone networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 4, pp. 3568–3582, Apr. 2021.

[174] Y. Xu, T. Zhang, D. Yang, Y. Liu, and M. Tao, "Joint resource and trajectory optimization for security in UAV-assisted MEC systems," *IEEE Trans. Commun.*, vol. 69, no. 1, pp. 573–588, Jan. 2021.

[175] G. Sun, X. Tao, N. Li, and J. Xu, "Intelligent reflecting surface and UAV assisted secrecy communication in millimeter-wave networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 11, pp. 11949–11961, Nov. 2021.

[176] H. Bastami, M. Letafati, M. Moradikia, A. Abdelhadi, H. Behroozi, and L. Hanzo, "On the physical layer security of the cooperative rate-splitting-aided downlink in UAV networks," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 5018–5033, 2021.

[177] R. Dong, B. Wang, and K. Cao, "Deep learning driven 3D robust beamforming for secure communication of UAV systems," *IEEE Wireless Commun. Lett.*, vol. 10, no. 8, pp. 1643–1647, Aug. 2021.

[178] D. Diao, B. Wang, K. Cao, R. Dong, and T. Cheng, "Enhancing reliability and security of UAV-enabled NOMA communications with power allocation and aerial jamming," *IEEE Trans. Veh. Technol.*, vol. 71, no. 8, pp. 8662–8674, Aug. 2022.

[179] F. Fazel, J. Abouei, M. Jaseemuddin, A. Anpalagan, and K. N. Plataniotis, "Secure throughput optimization for cache-enabled multi-UAVs networks," *IEEE Internet Things J.*, vol. 9, no. 10, pp. 7783–7801, May 2022.

[180] H. Jung, I.-H. Lee, and J. Joung, "Security energy efficiency analysis of analog collaborative beamforming with stochastic virtual antenna array of UAV swarm," *IEEE Trans. Veh. Technol.*, vol. 71, no. 8, pp. 8381–8397, Aug. 2022.

[181] G. Sun, J. Li, A. Wang, Q. Wu, Z. Sun, and Y. Liu, "Secure and energy-efficient UAV relay communications exploiting collaborative beamforming," *IEEE Trans. Commun.*, vol. 70, no. 8, pp. 5401–5416, Aug. 2022.

[182] Y. Li, W. Wang, M. Liu, N. Zhao, X. Jiang, Y. Chen, and X. Wang, "Joint trajectory and power optimization for jamming-aided NOMA-UAV secure networks," *IEEE Syst. J.*, early access, Mar. 15, 2022, doi: 10.1109/JSYST.2022.3155786.

[183] N. Zhao, Y. Li, S. Zhang, Y. Chen, W. Lu, J. Wang, and X. Wang, "Security enhancement for NOMA-UAV networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 3994–4005, Apr. 2020.

[184] Q. Zhang, J. Miao, Z. Zhang, F. R. Yu, F. Fu, and T. Wu, "Energy-efficient video streaming in UAV-enabled wireless networks: A safe-DQN approach," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2020, pp. 1–7.

[185] H. Lee, M. U. Kim, Y. Kim, H. Lyu, and H. J. Yang, "Development of a privacy-preserving UAV system with deep learning-based face anonymization," *IEEE Access*, vol. 9, pp. 132652–132662, 2021.

[186] X. Guo, Y. Chen, and Y. Wang, "Learning-based robust and secure transmission for reconfigurable intelligent surface aided millimeter wave UAV communications," *IEEE Wireless Commun. Lett.*, vol. 10, no. 8, pp. 1795–1799, Aug. 2021.

[187] W. J. Yun, S. Park, J. Kim, M. Shin, S. Jung, A. Mohaisen, and J.-H. Kim, "Cooperative multi-agent deep reinforcement learning for reliable surveillance via autonomous multi-UAV control," *IEEE Trans. Ind. Informat.*, vol. 18, no. 10, pp. 7086–7096, Oct. 2022.

[188] W. Wang, Z. Lv, X. Lu, Y. Zhang, and L. Xiao, "Distributed reinforcement learning based framework for energy-efficient UAV relay against jamming," *Intell. Converged Netw.*, vol. 2, no. 2, pp. 150–162, Jun. 2021.

[189] S. H. Alsamhi, F. A. Almalki, F. Afghah, A. Hawbani, A. V. Shvetsov, B. Lee, and H. Song, "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, Mar. 2022.

[190] B. Bera, S. Saha, A. K. Das, N. Kumar, P. Lorenz, and M. Alazab, "Blockchain-envisioned secure data delivery and collection scheme for 5G-based IoT-enabled Internet of Drones environment," *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 9097–9111, Aug. 2020.

[191] Y. Tan, J. Liu, and N. Kato, "Blockchain-based key management for heterogeneous flying ad hoc network," *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7629–7638, Nov. 2021.

[192] R. Gupta, A. Shukla, and S. Tanwar, "BATS: A blockchain and AI-empowered drone-assisted telesurgery system towards 6G," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 4, pp. 2958–2967, Oct. 2021.

[193] S. Aggarwal, M. Shojafar, N. Kumar, and M. Conti, "A new secure data dissemination model in Internet of Drones," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6.

[194] O. Cheikhrouhou and A. Koubaa, "BlockLoc: Secure localization in the Internet of Things using blockchain," in *Proc. 15th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2019, pp. 629–634.

[195] O. S. Oubbati, M. Atiquzzaman, T. A. Ahanger, and A. Ibrahim, "Softwarization of UAV networks: A survey of applications and future trends," *IEEE Access*, vol. 8, pp. 98073–98125, 2020.

[196] G. Secinti, P. B. Darian, B. Canberk, and K. R. Chowdhury, "SDNs in the sky: Robust end-to-end connectivity for aerial vehicular networks," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 16–21, Jan. 2018.

[197] C. Guerber, N. Larrieu, and M. Royer, "Software defined network based architecture to improve security in a swarm of drones," in *Proc. Int. Conf. Unmanned Aircr. Syst. (ICUAS)*, Jun. 2019, pp. 51–60.

[198] A. Hermosilla, A. M. Zarca, J. B. Bernabe, J. Ortiz, and A. Skarmeta, "Security orchestration and enforcement in NFV/SDN-aware UAV deployments," *IEEE Access*, vol. 8, pp. 131779–131795, 2020.

[199] W. Lu, Y. Ding, Y. Gao, Y. Chen, N. Zhao, Z. Ding, and A. Nallanathan, "Secure NOMA-based UAV-MEC network towards a flying eavesdropper," *IEEE Trans. Commun.*, vol. 70, no. 5, pp. 3364–3376, May 2022.

[200] D. He, Y. Qiao, S. Chan, and N. Guizani, "Flight security and safety of drones in airborne fog computing systems," *IEEE Commun. Mag.*, vol. 56, no. 5, pp. 66–71, May 2018.

[201] X. Hou, Z. Ren, J. Wang, S. Zheng, W. Cheng, and H. Zhang, "Distributed fog computing for latency and reliability guaranteed swarm of drones," *IEEE Access*, vol. 8, pp. 7117–7130, 2020.

[202] J. Yao and N. Ansari, "Secure federated learning by power control for Internet of Drones," *IEEE Trans. Cognit. Commun. Netw.*, vol. 7, no. 4, pp. 1021–1031, Dec. 2021.

[203] X. Jiang, X. Chen, J. Tang, N. Zhao, X. Y. Zhang, D. Niyato, and K.-K. Wong, "Covert communication in UAV-assisted air-ground networks," *IEEE Wireless Commun.*, vol. 28, no. 4, pp. 190–197, Aug. 2021.

[204] X. Zhou, S. Yan, F. Shu, R. Chen, and J. Li, "UAV-enabled covert wireless data collection," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 11, pp. 3348–3362, Nov. 2021.

[205] X. Zhou, S. Yan, D. W. K. Ng, and R. Schober, "Three-dimensional placement and transmit power design for UAV covert communications," *IEEE Trans. Veh. Technol.*, vol. 70, no. 12, pp. 13424–13429, Dec. 2021.

[206] X. Jiang, Z. Yang, N. Zhao, Y. Chen, Z. Ding, and X. Wang, "Resource allocation and trajectory optimization for UAV-enabled multi-user covert communications," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1989–1994, Feb. 2021.

GAURAV KUMAR PANDEY (Graduate Student Member, IEEE) received the B.Tech. degree in electrical and electronics engineering from the Krishna Institute of Engineering and Technology, Ghaziabad, India, in 2015, and the M.Tech. degree in communication engineering from the National Institute of Technology Nagaland, India, in 2018. He is currently pursuing the Ph.D. degree with the Department of Electronics and Communication Engineering, National Institute of Technology Silchar, India. He has cleared both GATE and NET exams. His research interests include simultaneous wireless information and power transfer, UAV communications, and physical layer security.

DEVENDRA SINGH GURJAR (Senior Member, IEEE) received the B.Tech. degree in electronics and communications engineering from Uttar Pradesh Technical University, Lucknow, India, in 2011, the M.Tech. degree in wireless communications and computing from the Indian Institute of Information Technology Allahabad, India, in 2013, and the Ph.D. degree in electrical engineering from the Indian Institute of Technology Indore, India, in 2017. He was with the Department of Electrical and Computer Engineering, University of Saskatchewan, Canada, as a Postdoctoral Research Fellow. Currently, he is working as an Assistant Professor with the Department of Electronics and Communication Engineering, National Institute of Technology Silchar, Assam, India. He has numerous publications in peer-reviewed journals and conferences. His research interests include MIMO communication systems, cooperative relaying, device-to-device communications, smart grid communications, physical layer security, and simultaneous wireless information and power transfer. He is a member of the IEEE Communications Society and the IEEE Vehicular Technology Society. He was a recipient of the Alain Bensoussan Fellowship from the European Research Consortium for Informatics and Mathematics (ERCIM), in 2019.

HA H. NGUYEN (Senior Member, IEEE) received the bachelor's degree from the Hanoi University of Technology (HUT), Hanoi, Vietnam, in 1995, the master's degree from the Asian Institute of Technology (AIT), Bangkok, Thailand, in 1997, and the Ph.D. degree from the University of Manitoba, Winnipeg, MB, Canada, in 2001, all in electrical engineering. He joined the Department of Electrical and Computer Engineering, University of Saskatchewan, Saskatoon, SK, Canada, in 2001, and became a Full Professor, in 2007. He currently holds the position of the NSERC/Cisco Industrial Research Chair in low-power wireless access for sensor networks. He is the coauthor (with Ed Shwedyk) of the textbook *A First Course in Digital Communications* (Cambridge University Press). His research interests include communication theory, wireless communications, and statistical signal processing. He is a fellow of the Engineering Institute of Canada (EIC) and a Registered Member of the Association of Professional Engineers and Geoscientists of Saskatchewan (APEGS). He served as the Technical Program Chair for numerous IEEE events and was the General Chair for the 30th Biennial Symposium on Communications, in 2021. He was an Associate Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and IEEE WIRELESS COMMUNICATIONS LETTERS, from 2007 to 2011 and from 2011 to 2016, respectively. He is currently serving as an Associate Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY and IEEE TRANSACTIONS ON COMMUNICATIONS.

SUNEEL YADAV (Senior Member, IEEE) received the B.Tech. degree in electronics and communication engineering from the Meerut Institute of Engineering and Technology, Meerut, India, in 2008, the M.Tech. degree in digital communications from the ABV-Indian Institute of Information Technology and Management, Gwalior, India, in 2012, and the Ph.D. degree in discipline of electrical engineering from the Indian Institute of Technology Indore, Indore, India, in 2016. He is currently working with the Department of Electronics and Communication Engineering, Indian Institute of Information and Technology Allahabad, Prayagraj, India, as an Assistant Professor. He is serving as a Faculty-in-Charge of the Mobile and Wireless Networking Laboratory (MoWiNeT), Indian Institute of Information and Technology Allahabad, Prayagraj. He has numerous publications in peer-reviewed journals and conferences. His current research interests include wireless relaying techniques, cooperative communications, cognitive relaying networks, device-to-device communications, reconfigurable intelligent surfaces, signal processing, physical layer security, and MIMO systems. He also served as a TPC member, the session chair, the program co-chair, and a reviewer for various national and international conferences. He is serving as a Reviewer for the number of international journals including the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the IEEE COMMUNICATIONS LETTERS, the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, the IEEE SYSTEMS JOURNAL, IEEE ACCESS, the IEEE INTERNET OF THINGS JOURNAL, the IEEE TRANSACTIONS ON SIGNAL AND INFORMATION PROCESSING OVER NETWORKS, and *Physical Communication*.