IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 27, 2021, accepted March 10, 2021, date of publication March 17, 2021, date of current version March 30, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3066778

Survey of Security Protocols and Vulnerabilities in Unmanned Aerial Vehicles

ARSLAN SHAFIQUE[1], ABID MEHMOOD[2], (Member, IEEE), AND MOURAD ELHADEF[2]

[1]Department of Electrical Engineering, Riphah International University, Islamabad 46000, Pakistan
[2]Department of Computer Science and Information Technology, Abu Dhabi University, Abu Dhabi, United Arab Emirates

Corresponding author: Arslan Shafique (arslan.shafique@riphah.edu.pk)

This work was supported by Abu Dhabi University, UAE.

ABSTRACT With the rapid growth in technology, the use of Unmanned Aerial Vehicles (UAVs) have increased in civil and military applications including rescue operations, disaster recovery, and military operations. Despite the utility and advantages of UAVs, they may lead to major security breaches in the context of hardware, software, and communication channel, due their ease of use and availability. UAVs are vulnerable to various types of attacks such as spoofing, false data injection, jamming, fuzzing, availability, confidentiality, and integrity attacks. To overcome these security threats, researchers have been investigating strong security protocols to keep UAVs safe from the attackers. Nevertheless, there are many flaws in the developed protocols which can be exploited by hackers. Therefore, it is becomes crucial to study and analyze the existing security protocols used in UAVs to discover and address their vulnerabilities and weaknesses. The purpose of this study is to explore the vulnerabilities in the security protocols and propose guidelines to improve the security and provide future research directions.

INDEX TERMS Unmanned aerial vehicles (UAVs), security, vulnerabilities, attacks, drones, security threats.

I. INTRODUCTION

The Unmanned Aerial Vehicles (UAVs), also known as drones, have the capability of flying with and without a human pilot, and can be remotely controlled by wireless connections such as WiFi or radio. Other flying objects such as quadcopters and gliders can also be classified as UAVs. Recently, military has intensified the use of UAVs for critical operations in order to reduce the exposure of their valued human resources in high-risk environments. Apart from military uses, there are several other applications in the private sectors as well. These applications include search and rescue missions, surveillance, fire-fighting, courier services, ... [1]. UAV applications are exponentially expanding because of its rapid movement, low maintenance cost, and its ability to float and monitor real-time environments.

Figure 1 shows a sample from the various applications of UAVs. The advanced features of UAVs include the ability to carry heavy payloads, detection of mines, and scanning of unethical/unwanted activities in certain areas. All of these features are made possible thanks to the recent advancement in software and hardware technologies. In particular, Artificial Intelligence and Machine Learning have been playing a vital role in enabling UAVs to perform complex and sophisticated tasks. This has resulted in making UAVs highly susceptible to security threats.

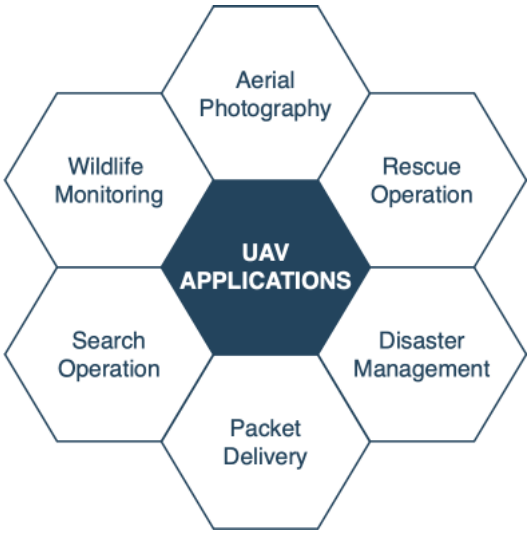

FIGURE 1. Applications of UAVs.

UAVs are prone to different security threats and can be attacked in various ways. The consequences of some attacks

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

can be devastating. Even the expensive professional ones are not secure [2], [3]. Some of the attacks focus on stealing information affecting hence its integrity, confidentiality and availability [4]. UAVs carry and transfer a lot of information using their communication channels. Such information exchange should be secured. The information can be in different forms such as images, text, audio and videos. Several encryption schemes are available in the literature by which one can encrypt the sensitive information [5], [6].

The fundamental security concern about the communication protocols is how to secure the data that is being sent over an insecure connection such as WiFi. UAVs normally send the data to the ground station over a wireless link which can be easily targeted by the attackers. To prevent the data from being intercepted by the attackers, the data should be protected. One common mechanism used to protect the data is use of encryption. For instance, the Advanced Encryption Standard (AES) is one of the secure mechanisms used nowadays. However, it cannot be used efficiently in real-time applications because of the communication overhead, especially where the data transfer rate is very high [7].

The other major concern about the security of UAVs is an attacker interfering with the UAVs in various ways to either take control of the UAVs or disabling the communication between the UAVs and the ground control station (GCS). Different attacks, which can be launched against UAVs to either take control or disable the communication, include jamming [8], spoofing [9], and false data injection [10] attacks.

In this section, we will describe the different components of a UAV system and how the information flows between these components. We will also highlight the motivations behind this study and discuss the contributions of this survey paper.

A. UAV SYSTEM

Knowing the components of UAV systems and how the information flows between them is crucial in analyzing their vulnerabilities. In addition, UAVs are highly exposed to technical system failures. The basic components of UAVs and the information flows between them are described in Figure 2.

The UAV base system is built for UAVs which is responsible for linking all the components together. It is used for inter-component communications, and for controlling the sensors and the communication/navigation systems. The UAV base system is also used for the integration of the optional components, e.g., the weapon systems. The UAV sensor system is composed of all the sensory equipment, with integrated pre-processing functionalities, such as sensors with cameras, GPS, and radars. The avionic system is responsible for executing control commands received from the controller such as engine commands, spoilers, flaps, and stabilizers. UAVs rely mainly on a wireless communication system which can either be a direct line of sight communication or indirect communication through satellites.

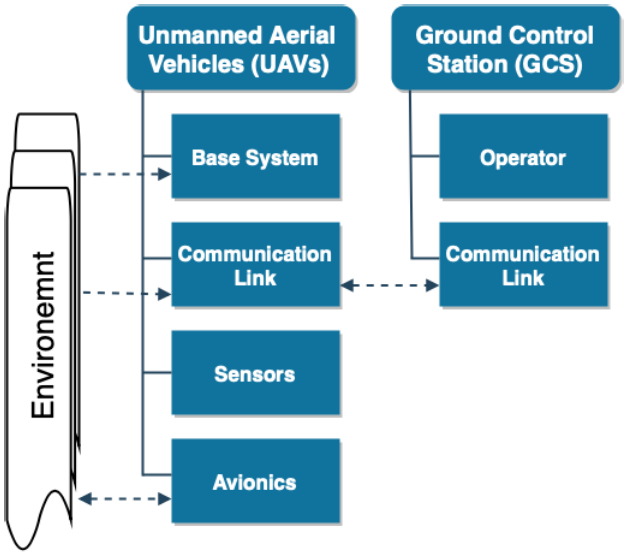

FIGURE 2. UAV components and information flows.

To attack a UAV, an attacker must influence the UAV externally unless the attacker has a physical access to its system. Due to the wireless nature of UAVs' communication system, they are highly dependent on external inputs. This provides various input channels for an attacker to attack their systems. As shown in Figure 2, information flows between the UAV and its environment through various channels. The bidirectional communication between the communication system and the GCS is the most exposed channel that can be used in an attack. The second most critical component is the information flow from the environment to the UAV sensors. These two links are very receptive to manipulations. Furthermore, the reliability of the sensors cannot be trusted. The key to control a UAV during a cyber-attack is the host's knowledge about the receptiveness of the components to the commands.

There are various cyber-attacks which could be used to exploit vulnerabilities of existing UAV systems. GPS jamming and spoofing are one of them. Jamming refers to the process of preventing the host from receiving the normal signal. While, spoofing encompasses the process of sending a malicious signal to foul the host to consider it as a legitimate one. Another form of intrusion attacks that exploits the GPS functionalities and that can be used to attack a UAV is the ''GPS spoofing attack''. I such intrusion, the attacker can overlay the GPS signal by a spoofed GPS system with a stronger signal. This leads to the false estimation of the UAV's current position. Attacks on UAVs have been continuously investigated by researchers in order to explore them in depth and to develop countermeasures that will make the future generations of UAVs more secure and less prone to attacks.

B. MOTIVATIONS

In the last decades, several review papers related to the security of UAVs were published [11]–[15]. Most of those reviews are not comprehensive and addressed only few

security concerns. In addition, the protocols discussed are not properly scrutinized for security and vulnerabilities. To the best of our knowledge, there is no exhaustive survey in the literature that overviews all possible security threats and the vulnerabilities that exist in the security protocols used in UAVs. Our survey explores two major aspects which are:

- Security protocols used to secure the UAVs.
- Vulnerabilities in the existing security protocols.

The first generations of drones were initially used mainly by the military for relief operations such as delivering of goods and rescue operations as shown in Figure 1. Nowadays, UAVs are widely used for civil applications such as capturing images and videos of different areas. Due to the ease of availability and the tremendous increase in their applications, UAVs are becoming a very attractive target for cyber criminals. As a matter of fact, it is riskier to execute sensitive operations like rescue operations via UAVs without a strong security protocol. The protocols that secure the UAVs must be strong enough to resist different types of cyber-attacks on availability, such as denial of service attacks (DoS), or confidentiality and integrity attacks. The vulnerabilities that exist in the security protocols can lead to different cyber-threats. To prevent the UAVs from cyber-threats, the security protocols used in the UAVs should be free of vulnerabilities. Several security protocols have been proposed recently and some of them offer a very good sense of security. However, it remains crucial to find out the vulnerabilities in the existing security protocols. Exploring vulnerabilities and providing solutions to the corresponding vulnerabilities is the basic motivation behind the proposed survey.

C. CONTRIBUTIONS OF THIS SURVEY

Several survey papers were published recently highlighting issues related to the security of UAVs such as, secure communication, intrusion detection, and security of the routing protocols used by UAVs [11], [16]–[19]. Most of these survey papers have discussed UAVs' security in a very sophisticated manner, However, to the best of our knowledge, only few of the existing survey papers have reflected upon the vulnerabilities of the UAVs' security protocols. In [16], security vulnerabilities of UAVs were discussed. The survey paper highlighted the vulnerabilities that can be used to attack UAVs such as attacks on the communication and control systems, spoofing, and jamming attacks. However, the paper did not discuss on how to secure UAVs from the attacks.

Zhi et. al discussed security and privacy issues of UAVs in [17]. The two major categories of attacks were covered: i) spoofing attack, and ii) WiFi attacks. However, the survey paper is not comprehensive as it lacks in-depth discussions on UAVs' vulnerabilities and attacks. In [18], secure communication protocols used in UAVs and their vulnerabilities were discussed. Nevertheless, the review paper does not discuss the techniques used to prevent cyber-attacks. A comparison of the proposed survey and the most recent review papers related to UAVs' security is given in Table 1. In our survey paper, we have covered all the important aspects such as UAV security, vulnerabilities in the existing protocols, and their countermeasures.

The contributions of this survey are as follows:

- We have done an in-depth literature review of the past research work related to the security of UAVs.
- We have analyzed the vulnerabilities that exist in the security protocols and provided possible solutions to overcome the issues of the existing security protocols.
- We have explained and analysed how different vulnerabilities such as WiFi insecurity, jamming attacks, fuzzing attacks, . . ., can be used to attack the UAVs.
- We have also highlighted the vulnerabilities in the packet forwarding and routing protocols used in UAVs and how they can be a threat to the security.
- Last, but not the least, we have highlighted the number of possible future research directions to enhance the security of the UAVs.

In this paper, we will highlight the existing security protocols for UAVs. We will also analyze the vulnerabilities in the existing protocols. This research study is organized as follows: Section II is devoted to the survey of the existing security protocols which are designed in the past few years to enhance the security of UAVs. In Section III, the vulnerabilities in the UAVs' security protocols are discussed. In Section V, we will propose potential research directions and Section VI will conclude the paper.

II. SECURITY IN UAVS

The use of drones brought several advantages that include commercial gains as well as personal benefits. However, there are several drawbacks related to security, safety, and privacy, which must be addressed before fully relying on them [20], [21].

The drones used by cyber criminals or terrorists can invade the privacy of the individuals as well as the privacy and safety of the general public. A number of drone properties are utilized in attacks that include high-level operations and unauthorized inspections. Drone utilization involves unauthorized spying on individuals, resulting in safety and privacy issues [22]. Drones must not be used to capture images of individuals and record their videos without their prior consent. The use of drones must be prohibited in residential areas and public properties that cause privacy issues, as the images captured by these drones may be used for illegal purposes that include scamming. Most of the drones nowadays are WiFi enabled so that the captured video can be broadcasted to smart devices. Some drones also use WiFi for remote control using smart mobile devices. As the WiFi connections are not strongly protected due to weak passwords, the attackers can easily access the WiFi and interfere with the communication, especially when there is no encryption protocol applied to WiFi passwords. [23].

Attackers can also use their unauthorized UAVs to destroy the authorized UAVs by performing physical collisions.

TABLE 1. Comparison of the current survey with existing review papers.

Categories discussed	Sub-categories	Krishna et al. [16]	Zhi et al. [17]	Khan et al. [18]	Sharma et al. [11]	McCoy et al. [19]	Current Survey
Secure communication	Symmetric security protocols			✓			✓
	Asymmetric security protocols			✓			✓
	Authentication protocols	✓		✓		✓	✓
Intrusion detection systems	Learning based					✓	✓
	Rules based					✓	✓
Security of Routing protocols					✓		✓
Packet forwarding							✓
Spoofing attacks	GPS spoofing	✓	✓	✓	✓	✓	✓
	False data injection		✓	✓	✓		✓
WiFi insecurity			✓	✓	✓	✓	✓
Jamming attacks		✓	✓	✓	✓		✓
Attacks on control systems		✓				✓	✓
Fuzzing attacks						✓	✓
Malicious UAVs detection			✓		✓		✓

As the unauthorized and authorized UAVs come across often, it is crucial to avoid any collision between them. Several modes were investigated by researchers to prevent UAVs from colliding [24]. The purpose was to design a UAV-Sense-and-Avoid (SAA) system to sense and elude the obstacles placed by the attackers. Another mode for SAA was also introduced by Barfield in [25]. Barfield proposed an autonomous collision avoidance system that is fully capable to protect the UAVs from any unnecessary accidents. Practical trials showed no failure during the tested the flights. The collision avoidance algorithms were designed to accomplish some important challenges that include Individual Collision Avoidance (ICA) and Group Collision Avoidance (GCA) [26]. Another method was presented by Yang *et al.* in [27] was based on a UAV 3D path planning, which consists of locating a collision-free path in a 3D cluttered environment considering geometric, physical, and temporal constraints. Different obstacle-collision avoidance methods were also presented to overcome any obstacle facing the UAVs. In [28], Ueno *et al.* presented a new algorithm that enables an UAV to accurately locate objects in its vicinity. In [29], Brandt *et al.* stated that quad-rotors are more suitable to operate indoors due to their flexible and fine-controlled operations in small and confined areas. Furthermore, an algorithm was presented by Israelsen *et al.* to manually control UAVs using automatic Obstacle Collision Avoidance (OCA) [30].

In addition to protecting the UAVs from collisions, it is very important to protect the communication between the UAVs and the GCS. For secure communication, several security protocols are proposed. The use of security protocols depends on the nature of the application which we will discuss later. The security protocols for UAVs can be broadly classified into three categories: i) secure communication, ii) physical layer security, and iii) intrusion detection system. The schematic diagram for the security protocols used in UAVs are shown in Figure 3.

A. SECURE COMMUNICATION IN UAVS

UAVs can be utilized for the surveillance of a large area without any additional help from the network infrastructure. During the flight, UAVs communicate with the GCS and continuously exchange important information. This exchange of information creates new challenges due to the dynamic topology. UAVs are frequently used for data transmission from one node to the GCS. The transmitted data can be attacked in various ways. In most of the military applications, the sensitive information is sent between two authentic

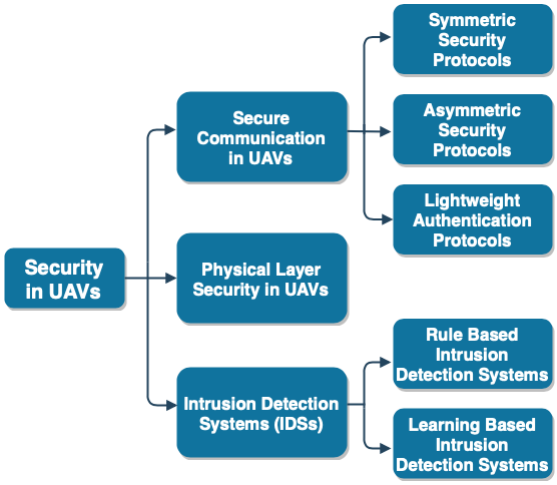

FIGURE 3. Security categories in UAVs.

users through the wireless communication channels. As the wireless channel is an insecure medium, it is quite possible to access the information by initiating cyber-attacks such as integrity, availability, and confidentiality attacks. To protect the information from the attackers, different types of security protocols are used to secure the transmission and authenticate the users. For example, symmetric and asymmetric security protocols are used to secure the communication between the UAV and the GCS. In symmetric security protocols, only one private shared key can be used for the encryption and decryption process. While in asymmetric security protocols, two different keys, one private and one public, are used. Public key is used for encryption whereas private key is used for decryption. These two types of security protocols are further discussed in sections II-A1 and II-A2. Section II-A2 also highlights the authentication protocols that are used to verify the identity the transmitter, i.e., guarantee that the received message is authentic and was not sent by an attacker. Section II-A3 presents lightweight authentication protocols which are used where less memory and low computational complexity are required.

1) CRYPTOGRAPHIC SYMMETRIC SECURITY PROTOCOLS

To ensure integrity, confidentiality, and availability, cryptographic protocols are frequently used. In particular, symmetric protocols are used to protect the sensitive data such as text, images, audio, and video. In symmetric security protocols, the same key is used to encrypt and decrypt the information, i.e., the transmitter and receiver must have identical keys to access the original information. One time pad (OTP) is an example of symmetric security protocols, which is often used to secure the transmission. To secure the data, OTP requires the same key size as the size of the data. For example, in the case of images, if an image contains M rows and N columns of pixels, the key must be equal to the length of the original image, i.e., $M \times N$. In [31], the security of the wireless communication MAV link is enhanced using OTP encryption. To secure the transmitted data, an encryption-decryption function is used. There are several commands to control the UAVs, such as start UAV, takeoff command, and autopilot enable. All these commands are in the form of bits which can be represented by 0 or 1. By combining the different bits, a long text can be created which can be secured by using an encryption scheme.

OTP-based encryption schemes have some drawbacks. For instance, the key size must be equal to the length of the data. If we want to send a large size data, we must share the key with the receiver. Hence, key distribution becomes a problem as it consumes a lot of bandwidth. Moreover, the key can be only used once, which means for each secure transmission there is a need for a new key [31]. The scheme proposed in [31] can be improved in terms of security by applying some robust transformation techniques such as discrete wavelet and discrete cosine transforms. These techniques first convert the original message into different frequency coefficients which are completely different from the original message. Moreover, transformation performed using frequency coefficients is faster as compared to transformation performed directly on the original message [32], [33].

In [34], a chaotic Lorenz system is used that encrypts and decrypts the original and transformed messages, respectively. Chaotic Lorenze systems have long-term unpredictability and can generate more randomness with minor changes in the seed values. The UAV collects the data from the sensors and camera, and passes them to the Lorenz chaotic based encoder. It does not directly encrypt the plain message. All the information is converted into bits and then undergoes encryption. The bits are continuously encrypted till the end of the original data. Following the encryption process, the UAV sends the encrypted information to the receiver which decrypts it by applying the reverse process of the chaotic Lorenze system. The proposed encryption scheme is symmetric in nature which means that the receiver uses the same key by which the original data was encrypted by the transmitter. However, the proposed protocol [34] has some weaknesses as well. For instance, there is no data scrambling process in the proposed technique. In fact, the security of any encryption scheme depends on both confusion (scrambling) and diffusion [35].

2) CRYPTOGRAPHIC ASYMMETRIC SECURITY PROTOCOLS

In asymmetric security protocols, two different keys are used. One is the public key, while the other is the private key. The user at the transmitter and receiver ends encrypts and decrypts the information using the public key and private key, respectively. The secrecy of the public key is not necessary because if anyone encrypts the information using the public key, it cannot be decrypted with that same public key. To retrieve the information, a secret (private) key must be used instead of the public key. In [36], to check whether the data received by the UAV is sent from the authentic ground station or the eavesdropper, the authors have proposed a data authentication protocol using an asymmetric key algorithm technique.

Asymmetric security protocols are used for the secure transmission of messages between the UAV and the GCS. However, because of the communication overhead, asymmetric protocols are mostly used for the symmetric key exchange between the UAV and the GCS. Asymmetric security protocols are also used to ensure the integrity of the transmitted data between different sensors or devices.

In [36], X.509 certificate with the elliptic curve cryptography (ECC) is used. By using X.509, the generated signature is shorter in length which makes the authentication process significantly faster. The scheme proposed in [37] performs signature verification after receiving the data. Once the UAV receives the data from the ground station or eavesdropper, the UAV executes the verification process to check the authenticity of the data before performing the final action. On the sender side, the 164 bits hash is generated using the SHA-1 algorithm. The hash is then encrypted using the public key before sending it to the other node. At the receiver end, the hash will be decrypted using the private key and then the hash of the original message is calculated by the receiver. In the last step, the receiver will compare both hashes, and if there is no difference between them, the received message is deemed verified and was not modified by an unauthorized person.

The asymmetric security protocols can enhance the security of the Automatic Dependent Surveillance Broadcast (ADS-B) [36]. The ADS-B is an air traffic surveillance protocol which is unacceptably insecure. The ADS-B is used to detect the other UAVs flying in the surrounding area. There are some major problems with the ADS-B which include the lack of built-in security mechanisms such as authentication codes and encryption modules that protect against the tampering of data and eavesdroppers, respectively. It is critical that the technology used in the ADS-B must meet the security requirements. In [36], Wesson *et al.* have raised a question; ''*Can an asymmetric cryptographic security protocol enhance the security of ADS-B?*''. To address this question, the existing cryptographic security protocols that are designed for the information exchange between the GCS and the UAV are evaluated on the basis of their characteristics to make the ADS-B more secure. After evaluating the cryptography in ADS-B, Wesson *et al.* declared that the asymmetric-key elliptic curve digital signature algorithm is viable. The use of asymmetric cryptography in ADS-B can be more costly and time-inefficient because in asymmetric cryptography different keys are used to encrypt and decrypt the original message which can take some time to process.

The information authentication protocols are also used to ensure the integrity of the transmitted data. To exchange the key between the nodes, Diffie and Hellman proposed a key exchange protocol that has been frequently used in the past few decades [38]. When exchanging the keys between two parties, they have no prior knowledge whether the keys which are sent over an insecure channel (e.g., Internet) by an authentic person or not. The authors in [39] have developed a public-key exchange protocol in which the sensor nodes exchange the keys and communicate with each other after authenticating their neighboring nodes. In the proposed framework, two sensor nodes are considered as two communicating parties. One sensor node sends the public key encrypted message; while the other sensor node decrypts the encrypted message with the private key and its own generated random number. Similarly, the second party sends the encrypted message with the public key. The first party decrypts the cipher message with the private key and with its own generated random number. If the decrypted message is exactly the replica of the encrypted message, the sensors will be declared as an authentic entities and will continue communicating.

In [40], Valentin *et al.* have proposed a trust-based protocol for the security of the UAVs. To check the correctness and accuracy of the data, trust values are assigned to the sensors which are determined by the UAV. The proposed methodology consists of three modules: i) a direct trust value determination phase, ii) an indirect trust value determination phase and iii) the final trust value determination phase, calculated by the UAV. In the whole environment, each sensor will determine its own trust values. The UAV will use its own trust values as well as indirect trust values generated from the sensors. The sensors in the environment can be placed by the attackers and those sensors will also generate their own trust values. The final trust value will be determined by the UAV. The trust values that will be received by the UAV are compared with the values placed in the log file of the UAV. If the final determined trust value is negative, the sensors are not trusted and the UAV will avoid taking further data from those sensors, and hence, the attacker will not be able to interfere with the UAV. In contrast, if the final determined trust value is positive, the communication between the UAV and the sensors will be enabled. Whereas, zero trust value means that the UAV requires more information to decide whether the sensors are trusted or not.

In [41], Yoon *et al.* have proposed an authentication protocol to detect whether the information received by the UAV is sent from the ground station or the attacker. In the proposed protocol, the UAV sends encrypted random stream to the GCS. After receiving the data, the GCS decrypts the random stream using the private key, then it encrypts the data a second time using its public key, and finally sends it to the UAV. The UAV will compare the received data with the data maintained in its indexes. If the authentication is successful, the UAV is ready to take off. On the other hand, if the authentication is unsuccessful during the exchange of information between the UAV and the ground station, it indicates that the attacker is trying to take control of the UAV. Therefore, it disconnects the communication channel. No further information is exchanged between the sender and the receiver after that. In this protocol, only the encryption of a random message and the comparison method are used to check whether the UAV has been hijacked or not. The proposed scheme provides information authentication. However, when large sized data is sent to the UAV for authentication purposes, it requires a high bandwidth, cost,

and processing time. To overcome these issues, we can use a small hash for authentication instead of encrypting the whole message.

In [42], to provide the authenticity and security to the data which is stored in the UAV memory chips, Steinmann *et al.* have proposed a key negotiation mechanism. In this method, the basic theme is to make an algorithm that continuously changes the random keys. For instance, the data encryption can be done by the one-time pad technique in which the key-size is equal to the original message length. Now, if the attacker explores one key, the original message can easily be revealed. So, the generation of random keys may enhance the security of the keys and the original message. In the proposed methodology, the first node sends the public key encrypted data along with the hash code to the second node. The second node decrypts the data with its private key, calculates the hash value, and then compares the calculated and received hash codes. If there is a match, it implies that the message was not changed by an external entity (attacker). This proposed methodology implements the authentication. However, it is not feasible to keep the keys secret.

3) LIGHTWEIGHT AUTHENTICATION PROTOCOLS FOR UAV

Another way to conceal confidential information from the attackers is by using lightweight encryption and authentication protocols. The use of these lightweight schemes might help in encoding the information in less time. It also does not consume heavy program memory which allows the UAV to perform actions faster. In [43], a lightweight encryption protocol was proposed that works appropriately with frequent context switching in a heavily multi-tasked environment. A lightweight blockchain-based stable routing algorithm for swarm unarmed aerial systems (UAS) networking was proposed in [44]. Wang *et al.* have used the lightweight blockchain as a bargaining chip to strengthen the routing of swarm UAS networking that uses 5G cellular network technology. The lightweight blockchain algorithm is different than traditional routing algorithms as it can easily avoid the vindictive connections from the attackers, identify malicious UAS, and reduce the intensity of the attacks from spiteful UASs. The suggested algorithms were swarm UAS pitched that strives to expand the swarm UAS deployment networking on a wide range.

The low-cost devices can be consolidated into UAVs to secure the data from the attackers by using the Internet of Things (IoT). To minimize the effects of cyber-attacks, the data should be encoded with the use of session keys familiar to the specific participating nodes. On the other hand, the embodiment of the required abilities for both generations of secure session keys and encoding/decoding of the secret information is very tough in low-cost IoT installations because of the performance limitations. In [45], Demeri *et al.* have applied a combined secure and public key data transfer system with a low-cost aerial platform that combines different cryptographic accelerators. The components are incorporated with the use of moldable and extensible application programming interference (API) in a software-hardware approached design that resulted in costless drones. With the latest enhancement in the wireless communication system and miniaturization of all the electronic devices, UAVs are offering a great relaxation to the public. Moreover, the UAV cybersecurity is getting more attention due to upcoming security issues, strategic and financial information, and the importance associated with Aerial applications.

In order to provide security and authentication to the communication parties and to ensure the privacy of the data, a lightweight authentication protocol was suggested in [46] to offer secure communication between UAVs and ground stations. The proposed scheme also mentioned a packet capture (PCAP) to ensure the secure communications between two parties. The basic idea of the PCAP is that the UAV and the ground station use the seed values of the chaotic maps that randomly shuffle the original message according to the generated chaotic sequence [46]. However, with the advancement in the remote environments and the availability of low resources, the UAVs are doubted for device capturing and dabble attacks. This increases the risk of the data stored in UAVs to be stolen by adversaries. In [47], Haque *et al.* have focused only on the secure transmission of information that UAVs send to the base station. In [47], the data security and lightweightness was discussed and a new framework was proposed to achieve the desired tasks. For the lightweightness of the system, specific encryption is performed. In the proposed scheme, apart from the cryptography, watermarking is also incorporated to increase the integrity and confidentiality of the data. The purpose of doing selective encryption is to provide the stabilization between the UAVs under limited resources. Selective encryption may also have advantages especially in real-time applications where fast processing is required.

To highlight information insecurity and authentication issues, a two-phase lightweight mutual authentication protocol was introduced in [48]. In the proposed system, a well suited software-defined networking (SDN) is supported with multi UAV network installed in the required spying areas. In addition, the security evidence of protocol was also introduced to emphasize its security features. To apply the authentication protocol more smartly in UAVs, a Smart Internet of Drone (S-IoD) supported framework for a UAV environment was proposed in [49]. The proposed scheme collects all the required information independently. For the sake of reducing the computational cost of the authentication protocol, a lightweight privacy-preserving scheme (L-PPS) was presented in [49]. The L-PPS offers robustness between the IoT devices with an appropriate authentication time.

Furthermore, due to the limited availability of the resources and risky environment around the UAV, different attacks that include wireless attack, confidentiality attack, and the man in the middle attack can be performed by the attackers. To prevent the UAVs from such attacks, authentication is quite urgent to be established before the UAVs start to communicate with each other and guaranteeing that an authentic

drone in the network is the priority of UAV network security. Whereas, the standard authentication system that contains a username/password or dynamic key is not significantly secure. RSA certification requires a long-lasting session key that is not able to fulfill the lightweight requirement in the UAV infrastructure.

In [50], a lightweight recognition authentication mode backed by ECC (Elliptic Curve Cryptography) is suggested that has three steps: i) ECC certification initiation, ii) identity authentication, and iii) key compatibility verification. Teng *et al.* have mentioned that the first two steps are fully compatible with the two-way authentication. Whereas, the last step verifies the consistency of the verification key. In contrast with the traditional authentication modes in the UAV network, the perspective suggested in [50] is based on short keys and less computing workload. Barka *et al.* suggested a capable lightweight communication plan for the aerial Named Data Networking (NDN) [51]. The proposed technique can sustain the NDN security and it predicts with 80% accuracy while reducing the end-to-end delay to less than 1 second in the worst-case scenario. The proposed scheme also reduces the average use of energy.

In [52], a novel authentication scheme for UAV is suggested. Since the UAV is supported by small-sized batteries and contains limited memory, the lightweight security methods are perfectly suited for them. In [52], Srinivas *et al.* suggested a temporal credential-based anonymous lightweight authentication scheme (TCALAS) for the Internet of Drone (IoD) networks. Contrary to the IoD surveillance framework suggested by Srinivas *et al.*, their scheme can perform only in the situation when there is only one flying zone that is not extensible. Moreover, despite their declaration of robustness, the investigation done in [53] proves that Srinivas *et al.*'s scheme does not stand with traceability and availability attacks. With the use of lightweight symmetric key primitives and temporal credentials, an upgraded scheme (uTCALAS) was suggested by Ali *et al.* in [53]. The suggested scheme offers security against several attacks that include traceability and availability attacks while keeping the lightweightness. It enhances extendibility and can perform in the area where several flying zones are available in the IoD network. Furthermore, Ali *et al.* have successfully achieved computationally fast authentication that takes 2.29ms to accomplish the authentication process.

B. PHYSICAL LAYER SECURITY IN UAVS

One extensively adopted performance metric in the physical layer security design is the so-called secrecy rate [54], at which the information can transmit securely. Traditional encryption protocols have vulnerabilities in the key distribution and high processing time. The analysis of the physical properties of cellular channels can support secure transmission. Physical layer security (PLS) is frequently used to achieve the maximum secrecy rate of transmitted data between the two different nodes. In fact, it is essential for all security controls and communication devices mounted in the UAV. Unlike the conventional cryptographic security approaches, PLS takes advantage of the characteristics of cellular channels such as fading, interference, and noise, to boost the signal reception at the legitimate receiver and reduce the received signal quality at the eavesdropper [55], [56]. PLS can be achieved by incorporating the cryptographic protocols. Several cryptographic security protocols are presented in the literature that provides a significant level of security but there is a no framework that offers an ideal security. Therefore PLS is gaining serious attention.

To enhance and maximize the secrecy rate of wireless communication in the UAVs, a variety of work have been proposed on PLS [57]–[59]. In the past few decades, static relay based communication systems were deployed to improve the existing PLS schemes. With the fascinating development in autonomous vehicles such as UAVs, a new model of relying technique known as UAV-enabled mobile relaying has become a valuable technology. In [60], the authors have proposed an improved version of a PLS scheme using UAV enabled mobile relying. To improve the security of communication system, buffer-aided mobile relay is deployed which allows data to arrive independently and more quickly which is useful for real-time applications.

C. LEARNING-BASED INTRUSION DETECTION

A digital machine can perform different tasks based on some instructions given by the user. To accomplish the automation of the tasks, machine learning (ML), deep learning, and neural networks are frequently used. ML algorithms have two phases, training and testing. In the training phase, the model learns from the data and predicts future events based on the training. The accuracy of the training model is evaluated in the testing phase and can be improved by using different strategies. The learning based techniques can be implemented in UAVs for the intrusion detection by pattern recognition. Once the UAV is trained, it is able to recognize the pattern of the intrusion.

In [61], a deep reinforcement learning and a weighted least squares algorithm [62] is incorporated to estimate the power of the jamming signal with a convolution neural network (CNN) [63]. In the first step of the proposed approach, a relay power factor is selected based on the bit error rate (BER) and the channel gain. To initialize the weights which will be equal to the anti-jamming relays, a convolutional neural network is used. These weights are updated by using a stochastic gradient descent algorithm [64]. After that, the UAV receives the BER value from the ground station. If the learning parameter is greater than the power factor of the relay power, the device chooses a random relay power. If it becomes greater than zero, the UAV sends the message with the randomly selected value of the power by using a reinforcement learning. Note that the randomly chosen relay power can increase the error rate. Although the algorithm can prevent the UAVs and communications from jamming to some extent, it can be very costly in case of a high error rate.

In [65], an attack detection technique was proposed in which two different machine learning algorithms such as Support Vector Machine (SVM) and K-mean clustering are used. These algorithms learn from the data and make decisions for the upcoming samples. There are two phases in the proposed technique. First, two parties send a signal to the UAV, and second, the UAV transmits the received signal to the third party for the detection of deviation. For this purpose, machine Learning (ML) is incorporated. After receiving the signal by the third party, it is required to build a data set by which the ML algorithms classify the output labels. The third-party will continuously receive the signal and it will find the mean and standard deviation of each received signal. As a result, the mean and the standard deviation are the two feature points of the data set. After completing the training of the model, when a third party received a new sample, it is fed into the machine learning algorithm and according to the calculated values of both the features, it gets assigned the label 1 (Attacked) or label 2 (Not attacked).

In the machine learning algorithms, there must be more features in the data set to increase the accuracy of the model in order to avoid any declassification of any event. In this mode, only two features are used, as a result, the accuracy of the model gets compromised.

D. RULES-BASED INTRUSION DETECTION

To make a device intelligent, some instructions should be given to that device. In rule-based tasks, the user must define some rules. Based on those rules, the device takes the decision and sends the command to the base station. In the case of UAVs, for each task, different rules are fed into the chip of the UAV and threshold levels of the acceptance of each rule are set. For example, if the threshold is 80%, it means that if the UAV finds the true condition of the rules equal or greater than 80 percent, the UAV performs the specific function and vice versa. In [66], a new intrusion detection system was proposed based on the specific behavior rules to minimize the false negative predictions. In the proposed detection method, seven different attacks were discussed which are related to the availability, confidentiality, and integrity attacks. When the UAV experiences anything from these seven attacks, the UAV takes measures to defend itself. First, when the UAV reaches outside to the safe space, it activates the weapons to defend itself against the attack. Second, when the sensors readings are different from the trusted node, actions are taken. Third, when bad recommendations are received regarding the trusted node and good recommendation are received regarding misbehaving UAV, appropriate actions are taken. The fourth indicator handles the situation when UAV deploys landing gear in an inappropriate area. These four attacks correspond to integrity attacks. The fifth indicator is activated when the UAV starts sending data to unauthorized parties. This attack corresponds to the confidentiality attack. The sixth attack indicator occurs when without analyzing any attack the UAV uses its countermeasures. Seventh and last attack is when the UAV uses more thrust to cross the limited altitude which is defined by the authorized person. Sixth and seventh attack correspond to the availability attack. These seven attacks are taken into account and after detecting the attack, the UAV defends initiates a defense phase to protect itself against the above-mentioned attacks.

Intrusion detection systems (IDS) are also used to detect the deviations that occur in the network. Henceforth, the IDSs remove the effect of the attack in order to prevent the systems from hazards. An IDS is a major mechanism in the UAVs network which is used to detect the malicious nodes and protect the authentic UAVs from the attacks.

In [67], intrusion detection and malicious node ejection issues are addressed. A new intrusion detection technique was proposed by using the Bayesian game model [68] to detect the intruders more accurately. The main focus was to detect the internal intruders and to eject the node which can be harmful for the UAV network. In the first step, the intrusion detection mode is activated by the different nodes. To perform this task, the IDS first computes the misbehavior rate (MR) of any other UAV which is in the UAV network. If the MR exceeds the threshold value, then the IDS starts monitoring the neighboring nodes and activates the detection system. Otherwise, the IDS does not perform any task. Similarly, the intrusion ejection system computes the MR of the node. If the MR exceeds the threshold value of the intrusion ejection mechanism, it declares the node as malicious and rejects it from the network. As far as the intrusion ejection is concerned, the ejection of a node from the network immediately is not a suitable approach. The node may misbehave for a certain period due to the environmental condition. If we eject the node immediately on the bases of the misbehavior rate, the false positive rate may increase.

Table 2 and 3 shows the comparison of security protocols used for secure communication and intrusion detection in UAVs, respectively.

We have analyzed some statistical results of machine learning based techniques for UAVs which either incorporate rule-based or learning-based techniques [65], [69]–[74]. The results analyzed are displayed in Table 4. Four important factors are used to analyze these techniques which are True Positives (TP), True Negatives (TN), False Positives (FP) and False Negatives (FP). The aforementioned factors are used to find the statistical parameters such as accuracy, precision, recall and F1-score. Accuracy tells us how many correct predictions are made by any model. The higher number of correct predictions will result in higher accuracy. The *accuracy* can be calculated as follows:

$$\text{Accuracy} = \frac{\text{No. of correct predictions}}{\text{Total number of predictions}} \tag{1}$$

OR

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{2}$$

The second parameter *Precision* is calculated by taking the ratio between the true positives and the sum of true positives and true negatives. High precision is required for a better

TABLE 2. Comparison of different protocols used for secure communication in UAVs.

Categories	Techniques	Features	Vulnerabilities/ Weaknesses
Cryptographic symmetric security protocols	OTP for securing communication links [31]	Secure technique due Large key size	More bandwidth is required for sharing the secrete key
	Data security protocols (Symmetric) [34]	More randomness due to Lorenze machine	Absence of confusion part which makes the system insecure
Cryptographic asymmetric security protocols	Data authentication using asymmetric security protocol [36]	Shorter hash length Computationally fast	Hash is in encrypted form, so, the eavesdropper may try to perform attacks to retrieve the original hash.
	Analysis of cryptography in ADS-B [37]	Declares that the elliptic curve digital signature algorithm is viable	More costly and time inefficient eavesdropper may try to perform attack
	Public-key exchange security protocols in UAVs [39]	Nodes communicate with each others after the authentication of the received commands from the ground station (GS)	Choose only one random number as a public key to encrypt the message that can easily be judge by the attacker.
	Trust-based security protocols for the UAVs and the sensors [40]	Authenticate whether the sensors placed in the UAV network are trusted or not.	Packets which are sent by the UAV to the GS are in the original form which can be fabricated or stolen by the attacker.
	Authentication scheme, whether the data received by the UAV is from the authentic or unauthentic user [41]	Protects the information even after hijacking the UAV by the attacker	When someone sends a large data to the UAV for authentication purposes, it requires a high bandwidth, high cost and the sending or processing time will also be high.
	Key negotiation mechanism for providing authenticity and security to the data stored in UAS chips [42]	Continuously changes the random keys	Not feasible to keep the keys secret
	Convex optimization [76] technique	Reduces overhearing effects, Enhances the trajectory and transmit power of the UAVs simultaneously	Takes more time to execute all the complex computations to find whether the system converges or diverges
Lightweight Authentication protocols for UAV	lightweight blockchain-based [44]	Supports 5G cellular network	Lightweight blockchain algorithm is way far different than traditional algorithms
	Authentication using public key data transfer system [45]	Components are incorporated with the use of moldable and extensible API	Slower than traditional authentication schemes because of asymmetric keys
	Authentication using packet capture (PCAP) [46]	use the challenge response pair of physical unclonable function	Less dimensional chaotic map is used
	SDN based authentication [48]	Combination of security and SDN	Computationally inefficient
	S-IoD supported framework [49]	Authentication collects all the required information independently	Low computational cost

model. The precision for the model can be calculated as follows:

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{3}$$

The third statistical parameter *Recall* refers to the sensitivity of the system, and is calculated as follows:

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{4}$$

TABLE 3. Comparison of different protocols used for intrusion detection in UAVs.

IDS type	Used techniques	Advantages	Disadvantages
Learning-based Intrusion Detection	Deep reinforcement learning technique [61]	Estimate the power of the jamming signal	High time complexity and error rate
	Attack detection technique [65]	Fast process due to the incorporation of ML algorithm	Less features selected due to which accuracy is compromised
Rule-based Intrusion Detection	Intrusion detection technique [66]	Less false-negative prediction detection, defends the UAV by the false information injected	High number of rules, due to which processing time can be high delaying the decision taken by the UAV
	Intrusion detection and malicious node ejection [67]	Use of a Bayesian game model. If we eject the node immediately on the bases of misbehavior, the false positive rate may further increase	Instead of immediately ejecting nodes, more rounds are needed. Then take the average after taking the final decision of the ejection of the malicious node.

The last parameter is called *F-Score* and it can be calculated from the recall and precision. In other words, F1-score is the weighted average of recall and precision. The range of F1-score lies between 0 and 1, whereas 1 indicates perfect precision and recall and 0 indicates either the precision or recall is 0. F1-score can be calculated as follows:

$$\text{F1-Score} = \left[\frac{(\text{Recall})^{-1} + (\text{Precision})^{-1}}{2}\right]^{-1} = 2\left(\frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}\right) \quad (5)$$

It can be seen from Table 4, the accuracy of the work proposed in [72] is higher in comparison to other schemes. This means that the percentage of TP predictions for the scheme proposed in [72] is comparatively higher. However, the accuracy for [71] is slightly less than the scheme proposed in [72].

Moreover, we have also analyzed some schemes discussed in section II in terms of applications and used technologies in Table 5 and 6. As different types of UAVs are used for different applications such as wireless coverage, remote sensing, real-time monitoring, search and rescue operations, surveillance, and delivery of goods, it is important to choose the right UAV and the suitable scheme for each specific application. For instance, in Table 5, it can be seen that the scheme which was developed in [75] is suitable for wireless coverage and surveillance. Similarly, Table 6 provides an analysis of the existing schemes in terms of used technologies. For example, the scheme presented in [75] supports secure communication. By incorporating the image processing technology, one can securely communicate by sending the encrypted digital data such as images.

III. VULNERABILITIES IN UAVS

Several methodologies have been proposed to enhance the security of UAVs. However, there are shortcomings in the proposed protocols which have made UAVs vulnerable to certain security threats. In this section, we will discuss how an attacker can breach the security of the protocols by using different attacking strategies. Vulnerabilities and their countermeasures for the security protocols are highlighted in Table 7 and the schematic diagram for the possible vulnerabilities is shown in Figure 4.

TABLE 4. Statistical results for learning and rules-based intrusion detection.

References	Accuracy (%)	Recall	Precision	F1 score
Sun et al. [69]	93.5	95.8	0.94	0.94
Hoang et al. [65]	88.8	0.98	0.91	0.94
Anwar et al. [70]	89.1	0.98	0.90	0.93
Shoufan et al. [71]	96.47	0.91	0.95	0.92
Ezuma et al. [72]	96.83	0.93	0.97	0.94
Li et al. [73]	66.87	0.81	0.76	0.78
Alipour et al. [74]	90	0.94	0.95	0.94
Han et al. [77]	74.7	0.045	0.81	0.085

A. GLOBAL POSITIONING SYSTEM (GPS) SPOOFING

GPS spoofing is categorized as a cyber-attack by which an attacker transmits a fake GPS signal with slightly higher power to mislead the reception of the UAVs. Due to the wireless connection between the GCS and the UAVs, the vulnerability factor inclines. Without the integration of complex checks, i.e., whether the signal is received from the GCS or the attacker, the UAVs may tend to perform actions from an unauthorized signal as well. To recognize the authority of a legitimate signal, a log-likelihood radio test method is adopted in [87] to fight against the signal spoofing attack. Prior information of the received signal frequency from the GCS assists the UAVs to identify the signal transmitter's information and breakdown the legitimacy of the received signal. In [87], a decision threshold methodology was designed using the Neyman-Pearson criterion [88]. To select the appropriate threshold value, the false alarm rate (FAR) value is set to be fixed. For the selection of an appropriate FAR value, a cumulative distribution function is estimated, which helps in the detection of spoofed signals.

In [89], Sedjelmaci *et al.* proposed a new methodology for the detection of spoofed signals. A rule-based detection technology, when incorporated with the protocols, helps in achieving better accuracy. In this methodology, a comparison between a specific threshold value and the transmitted signals

TABLE 5. Analysis of existing schemes in terms of applications.

Schemes	Providing Wireless Coverage	Remote Sensing	Real-Time Monitoring	Search and Rescue	Delivery of Goods	Surveillance
Faraji et al. [75]	✓					✓
Houng et al. [78]	✓			✓		✓
Challita et al. [79]	✓	✓				
Li et al. [80]	✓	✓				✓
Hudson et al. [81]	✓		✓		✓	✓
Ma et al. [33]	✓	✓		✓		
Kirichenko et al. [34]	✓					✓
Pan et al. [37]	✓	✓		✓		✓
Valentin et al. [40]	✓		✓		✓	✓
Yoon et al. [41]	✓	✓	✓			✓
Li et al. [54]	✓				✓	
Zeng et al. [57]	✓		✓			
Choi et al. [58]	✓			✓		
Li et al. [59]	✓		✓		✓	
Wang et al. [60]	✓		✓	✓	✓	
Hong et al. [65]	✓		✓	✓	✓	
Sedjelmaci et al. [67]	✓		✓	✓	✓	
Zou et al. [82]	✓	✓	✓	✓	✓	
Fotohi et al. [83]	✓	✓			✓	
Li et al. [84]	✓	✓	✓	✓	✓	
Amelin et al. [85]	✓	✓		✓		✓
Hooper et al. [86]	✓	✓			✓	✓

TABLE 6. Analysis of existing schemes in terms of used technologies.

Schemes	Collision Avoidance	Free Space Optical	Cloud Computing	Machine Learning	Image Processing
Faraji et al. [75]					✓
Houng et al. [78]				✓	✓
Challita et al. [79]		✓	✓		
Li et al. [80]		✓			✓
Hudson et al. [81]			✓		✓
Ma et al. [33]		✓		✓	
Kirichenko et al. [34]	✓		✓		✓
Pan et al. [37]	✓	✓		✓	✓
Valentin et al. [40]	✓		✓		✓
Yoon et al. [41]		✓	✓		✓
Li et al. [54]			✓		✓
Zeng et al. [57]	✓		✓		
Choi et al. [58]	✓	✓		✓	
Li et al. [59]	✓	✓	✓		
Wang et al. [60]		✓	✓	✓	
Hong et al. [65]	✓	✓	✓	✓	✓
Sedjelmaci et al. [67]	✓		✓	✓	✓
Zou et al. [82]	✓	✓		✓	✓
Fotohi et al. [83]		✓	✓		✓
Li et al. [84]	✓	✓	✓	✓	✓
Amelin et al. [85]		✓		✓	✓
Hooper et al. [86]	✓	✓	✓		✓

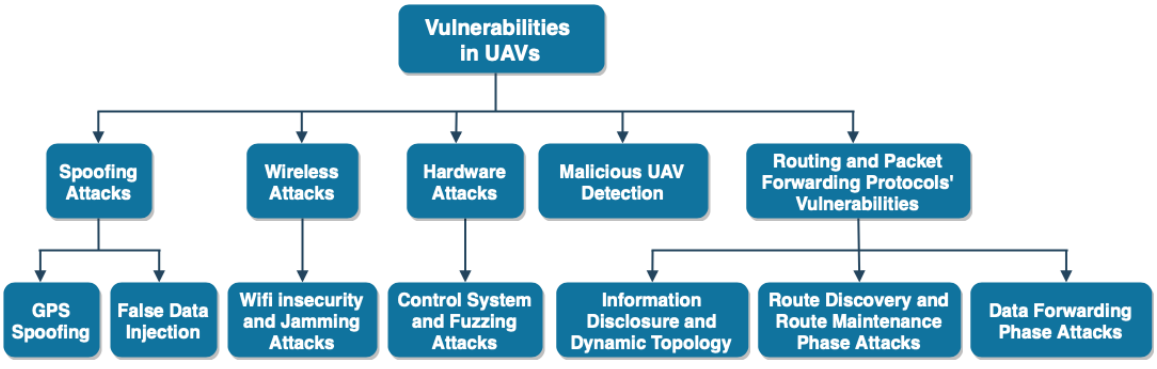

FIGURE 4. Vulnerabilities in UAVs.

is performed. If the value of the transmitted signal (transmitted by the attacker) becomes greater than the threshold value, the UAV detects that the received signal is spoofed. In [90], Qiao *et al.* proposed the use of a vision system based technique to detect the GPS spoofing for UAVs in which inertial measurement unit (IMU) sensors are used to

TABLE 7. Vulnerabilities and their countermeasures for the security protocols used in UAVs.

Categories	Techniques	Details	Countermeasures
Global Positioning System (GPS)	A log-likelihood radio test scheme [87]	False alarm rate (FAR) is set to be fixed, Gives the approximate value of FAR	FAR should be updated with time
	GPS spoofing attack detection [90]	Comparison of different values	High threshold may increase the accuracy of the attack detection
	Rule-based detection techniques are incorporated for GPS spoofing attacks [89] detection	The phenomenon of comparing the threshold values with the statistical values of the transmitter is used. Comparing the values may need high accuracy	There should be flexibility while comparing the values for the GPS spoofing attack detection purpose
	GPS spoofing attack detection [82]	Monitors the behavior of UAVs while detecting the spoofing by comparing the strengths of the signals	It can be significantly improved by placing the jammer in the UAV model
False data injection	Protection of UAVs from the sensor-spoofing attacks [10]	Based on Neural Networks with embedded Kalman filter (EKF) and only able to detect FDI, not accurate and time inefficient	Should update the Neural Network parameters continuously to make it time-efficient
WiFi Insecurity	Analysis of the vulnerability of micro-air-vehicle communication (MAVLink) protocol is performed [93]	MAVLink protocol does not encrypt the message due to the time inefficiency	—
Jamming attack	Methodology for preventing the UAVs from malicious jamming signals [94]	Artificial noise is added with the original information which can be detected and separated by the attackers	A plaintext can be added by applying the watermarking technique in order to make it a meaningful text
	Improvement of Physical layer security transmitter-receiver [106]	Artificial noise addition, height of UAVs is assumed to be fixed	By introducing the updating parameters to work on UAVs having no fixed height or position
Control system security vulnerability	Controls the performance detection of hardware failure [98]	A recursive least square (RLS) method is used to detect the divergence of the system control parameter, Not feasible to detect Spoofing attacks	Friendly jamming can be placed to overcome the non-detection problem of spoofing attacks
Fuzzing attacks	Attack detection [86]	Three different mechanisms are used due to which the overall overhead time is increased	By optimizing three mechanism and then used as a one mechanism
Malicious UAVs detection	Malicious UAV detection using machine learning [73]	Less accuracy	Use more relevant features to enhance the malicious UAV detection accuracy
	Detect the authentic UAV [104]	WiFi-based fingerprint technique is used, in which for each flow, a different fingerprint is registered which causes more processing time	Instead of registering the fingerprint, makes other feature vectors different from fingerprint

find the instantaneous acceleration and velocity of the UAV. To make the model of the proposed system, Qiao *et al.* considered three different coordinate systems which include the body frame coordinates, the ground coordinate system, and the image coordinates system. To find the GPS spoofing, it compares the two kinds of velocities which are measured by the Lucas-Kanade (LK) method [91] with root mean square error (RMSE) values. If the value of RMSE becomes greater than the threshold value then it will be declared that the UAV is spoofed else it is in a normal state. In [82], another scheme is proposed to detect GPS spoofing. It is supposed that the UAV has an inertial measurement unit (IMU) sensor which is helpful in monitoring the behavior of the UAV. The proposed GPS spoofing detection is very simple to implement because it just compares the strength of the signals and finds the error rate. Based on the error, it declares whether the UAV is spoofed or not. The concept is very much similar to the idea proposed in [90]. There is a fixed threshold value and it compares with the GPS signal strength and finds the error. If the error is smaller than the threshold value, the UAV will remain in the normal state and if the error is greater than the threshold value, it means that the UAV is hijacked. As this technique is so simple, it can be significantly improved by placing the jammers in the UAV model, i.e., those jammers will only block the signals which are greater than the threshold value. By two this, two goals can be achieved: the first is the detection of spoofing attacks which is already done in [82], and the second is the protection of the UAV from the spoofing attacks.

B. FALSE DATA INJECTION

False data injection is a technique by which an unauthorized person sends the clone data to the UAV in order to take control. UAVs are prone to vulnerable data based on the technique implemented on their security and cannot differentiate between the authentic and unauthentic data. To ensure secure operations, UAVs must be able to detect the false data injections. To address this issue, in [10], Abbaspour *et al.* proposed a protocol for the detection of cyber-attacks, known as false data injections (FDI). To perform a false data injection, intruders normally use their own sensors to inject the fake information in the UAVs sensors in order to take control of the UAVs. In Abbaspour *et al.*'s proposed system, neural networks are incorporated to increase the learning ability that will detect the FDI. Specifically, Abbaspour *et al.* have focused on IMU sensors which provide the information of angular and linear movement of the UAVs. Instead of direct application of neural network, a neural network adaptive structure (NNAS) was implemented. To improve the accuracy and time efficiency, an Embedded Kalman Filter (EKF) was used to update the neural network parameters. In [92], the ability to transmit fake information to take control on the UAV was explored. To detect the fake inserted information, a threshold based technique was adopted. The threshold values of the position and speed of the UAV are kept specific to determine whether the signal is fake or original. Information is flagged as fake when the values of the velocity and position become larger than the threshold values. Detection of fake information is not enough but it is important to equip the UAVs to take the right action against such information. Major issue with this type of techniques is that the UAV only detects the fake information when the values of the received signal raises above or decreases below the specified threshold value.

Researchers are trying to resolve the issue of insecure transmission of the data over an insecure channel using strong wireless communication security protocols [83], [84]. Although, the wireless connection (WiFi or Radio) security has now improved to some extent but more advancements are required in this area of research.

C. WIFI INSECURITY AND JAMMING ATTACK

UAVs can be connected via wireless channels such as WiFi. WiFi based UAVs are vulnerable to the wireless attacks and can be hacked by interrupting the communication between the UAV and the GCS. For the secure communication using WiFi, it can be protected via unique passwords. The analysis of the vulnerabilities of micro-air-vehicle communication (MAVLink) protocol was included in [93]. In the MAVLink protocol, two specific issues can arise. First, the MAVLink protocol does not encrypt the message which is to be sent. As a result, integrity attacks can surely happen. Secondly, if the MAVLink encrypts the message, a delay can occur due to the encryption and decryption of the messages, which can lead to availability attacks. In the proposed methodology in [93], it was supposed that the attacker has already hacked the network and gathered all the relevant information and can send this fabricated information to the host. Based on the fabricated information, the attackers can easily identify the position of the UAV. In this methodology, although a counter attack against hackers can be carried out, but the supposition can affect the overall efficiency of the technique. There should be a feasible protocol without pre-supposing any kind of attacks. Apart from the fabricated information, jamming attacks are also often performed by the eavesdropper to hack the information which is sent by the UAV to the GS.

To distract the UAVs, jamming attacks are frequently incorporated by the attackers. A jamming attack can also be planned to discontinue the communication between the authentic transmitter and the receiver. In wireless communication, jamming is a well-known research area. Many defense mechanisms are proposed by the researchers. In [94], full-duplex eavesdropping [95] is considered in which jamming and eavesdropping can occur simultaneously. To avoid the malicious jamming signals which are sent by the attackers, a new mathematical model was proposed in which the receiver values fall below the threshold. In the proposed model, it was assumed that the source and the eavesdropper have a line of sight (LoS) path [96] towards UAVs. The probability of the LoS increases with the height of the UAVs. To manage the LoS probability, path loss exponents are formulated for the UAV. In addition, for the secure transmission

of the information, an artificial noise (AN) is additionally sent with the original information for effective confusion. The eavesdropper will receive the jamming signals with the original from the UAV simultaneously. Hence, a simultaneous transmission of the original signal along with the noise can make it harder for the hacker to extract important information.

Most of the researchers are using AN frequently over the last few decades to protect the sensitive information. Protection of sensitive information from attackers has become a great challenge for the researchers. In order to sort out these issues, a new methodology was proposed in [75] for the secure transmission of sensitive information from the UAV to the GS. A protocol was proposed by Faraji *et al.* in [75] to protect the information from malicious UAVs launched by the attacker in the communication network, and the transmission of information from the UAV to the GS. The proposed technique defines rules to spot malicious UAVs, so that the information can only be sent to the authorized nodes. The purpose to spot the malicious UAV was to get rid of these UAVs in accordance to their behavior in the whole UAV network. Hence, the exchange of fake information passed on to the ground stations could be prevented. Though the presented work is fully capable of removing the malicious UAVs from the network in order to keep the information secure, it is not able to keep the information secure form the attackers due to the unencrypted nature of data. This means the information could be hijacked. Therefore, the algorithm needs to be improved and it requires the incorporation of a powerful cryptographic protocol.

In [78], a novel scheme was suggested to secure the data and to get rid of both the security and efficiency issues. While, the purpose was to uncover the security and wireless challenges that stood up in the context of a UAV-based information transfer system [79]. To expose these challenges, a solution based on ANN was suggested that enables UAVs to adaptively exploit the wireless system resources while safeguarding the operation in real-time. In [80], to prevent confidential signals and information from the cyber-attacks and hijacking, an artificial noise (AN) was incorporated. By using the AN with the original signal, the resulting signal is transmitted in a disordered form which makes it difficult for the hacker to decrypt it and extract the original information from it. To secure the information from the attackers by incorporating friendly jamming in [66]. A friendly jamming signal is a noisy signal, which is transmitted with the original signal. Noisy signal is named friendly jamming signal because it does not disturb the original signal, and its purpose is to provide the security to the original signal. For the friendly jamming signal, another reference UAV UAV_j is considered which transmits this noisy signal with the original signal. However, to maximize the secrecy rate, a block successive upper bound minimization technique (BSUBM) [97] was developed in [66]. BSUMB is used to identify the user scheduling, in which when one user is scheduled, the others are unscheduled. The UAV sends messages only to the scheduled users to protect the transmitted messages from other unknown users. Once the scheduling process is completed, the transmitted power of UAV_m (which transmits the message) and UAV_j (which transmit the friendly jamming signal) is optimized just to send the information in a more sophisticated way. The secure communication with the friendly jamming signals is guaranteed for the scheduled users. What if the jamming signal is trapped by the eavesdroppers? There should also be a protocol to secure the friendly jamming signal as well. Moreover, in the proposed algorithm, the collision of UAV_m and UAV_m is also ignored. So, another problem can be faced when UAV_m and UAV_j collide with each other.

D. CONTROL SYSTEM VULNERABILITIES AND FUZZING ATTACKS

Besides the choice of a suitable UAV type, it is also important to analyze the control system which is mounted in the UAVs. Most of the movements of UAVs are dependent on the control system. In [98], Birnbaum *et al.* focused on two major aspects. First, to develop such a system that controls the performance and detects the hardware failures of the UAVs. Secondly, to detect the different types of attacks such as attacks against the flight control, the computer and, the navigation sensors. To estimate the parameters such as the control parameters of the UAVs, a recursive least square (RLS) method [85] was adopted that takes a certain input seed value and generates the corresponding output values. The RLS method detects the divergence of the system control parameter values by continuously comparing the predicted values from the previously known values. If there is a significant divergence of the control parameters, a fail-safe protocol is executed which allows the UAVs to return on the designated spot safely. The controllers are responsible for the security of the UAVs, but it can be hacked by simple fuzzing attacks. It is another common attack that can be used to hack the controller of the UAVs.

In [86], the authors have proposed a methodology to secure the UAVs from the basic attacks such as Daniel of service (DoS) [99] and buffer overflow attacks [100] by using a fuzzy technique. WiFi-based UAVs can become easy targets of such attacks due to the wireless communication links. Moreover, it is also demonstrated in [86] that the protocols which are used to create a link between the controller and the UAVs are insecure. To solve this problem, three additional mechanisms were used which are: watchdog timer, hardline input data filtering, and anti-spoofing mechanisms [101], [102]. The watchdog timer provides security against the DoS attack and it works in the domain of operating system (OS). This ensures that the non-navigational processes are at low priority and allows access to the CPU for only a definite period of time. The second mechanism, i.e., hardline input data filtering, is able to decline the non-authenticated process. It protects the UAVs from Buffer overflow attacks that limit the data which is to be sent to the UAVs. Lastly, an anti-spoofing mechanism is incorporated

to prevent the UAVs from the Address Resolution Protocol (ARP) attack. This secures the network from unauthentic information.

In the Fuzzy logic based UAVs, landing issues require special attention. In [103], an issue of safety landing is discussed and an algorithm is proposed using Fuzzy logic. In this algorithm, a speed control mechanism is used for a safe landing. Vertical speed and altitude are the two inputs. Throttle positions are considered as an output parameter. The most important factor that is ''in ground effect'' is considered as a threshold value. Based on a threshold value, the UAV can land safely. The major advantage of this fuzzy logic-based methodology is that the processing time is less and the system can operate quickly.

E. MALICIOUS UAV DETECTION

As far as the cost is concerned for the detection of malicious UAVs, a vision-based detection system for UAVs with radar sensors and cameras can be fairly expensive. In [73], detection of malicious UAVs within a given time interval to classify the data, and a machine learning-based technique are proposed. There are two major concerns while using these algorithms: i) the selection of the right features and ii) the right identification of the event. In the data set of the detection of UAVs, eight different types of UAVs are used. In order to identify the UAV, the features such as packet size and arrival time of traffic are first extracted. After that, packet sizes for different packets and arrival times, in the data set, are defined. The different sizes of the packets will take different time to reach the destination. Based on the defined data set, UAVs are classified as secure or insecure. For the detection of malicious UAVs, the data set is used in this technique contains only two features. We can further enhance the accuracy and minimize the declassification rate by selecting more features.

In a UAV network, several UAVs exist to perform a specific task. Within the UAVs network, the possibility of an external attack is always there. In [104], a WiFi-based fingerprint technique is proposed to detect the authentication of information. In the WiFi-based channel, there are several types of traffics. In order to observe the classification of traffics, data mining algorithms were incorporated [105] which help to detect the unauthentic UAVs. In the proposed technique, fingerprint is considered as a feature vector. The technique starts by capturing the traffic flow of the packets. From each flow, one feature vector is extracted with different features, i.e., if the total number of captured flows is ten, then the total feature vectors will be ten, in which some of the feature vectors are used for training purposes while others are used for testing purposes. Different features are extracted from feature vectors and are: the average packet length, the root mean square value of the packet length, the total duration of each flow, the average inter-arrival time of the packet, the root mean square value of the packets inter-arrival times, and the transmitter and receiver addresses. After capturing the traffic flow, pre-processing is performed on the prepared data. Finally, based on the extracted features authenticity of the UAV is predicted.

F. VULNERABILITIES IN PACKET FORWARDING AND ROUTING PROTOCOLS

Flying Ad-hoc Networks (FANETs) is a type of network in which different UAVS are connected in an ad-hoc manner. UAVs are organized into teams to achieve high level goals. To establish a reliable communication between the UAVs specialized routing and packet forwarding protocols are needed.

Routing protocols are the set of defined rules used by the routers to distribute the information between different nodes. They are also used to update the routing tables so that the routing decisions can be made. Updating the routing table depends on the type of the used routing protocol and the adopted forwarding technique. For instance, in static routing protocols, an administrator manually assigns the path from the source to the destination. Moreover, other than the administrator, no one can add/update the routes. Whereas in dynamic routing protocols, a different route is chosen dynamically in case if a link goes down. As the routing protocols are also responsible for updating the routing tables efficiently, it is necessary to ensure the right route is selected to forward the packets to the destination. In addition, before forwarding the packets through any route it is important to ensure the integrity, confidentiality, repudiation, availability, and authenticity of the forwarded messages. In the absence of the aforementioned security services when using a week routing protocol, the consequences are devastating and may be in favor of the by allowing them to hack into the forwarded packets.

Apart from the security protocols such as cryptography and intrusion detection, routing protocols have their own significance in FANETs. When data is sent by the UAV to the destination, it follows a specific route. Packet forwarding and routing protocols are a major building block of modern UAVs. However, the initial design of these protocols do not consider security and vulnerability, hence, making it an attractive target for the attackers. In this section, we will analyze the vulnerabilities in the routing protocols and discuss their countermeasures. A comprehensive summary of routing protocols, vulnerabilities and their countermeasures is given in Table 8.

Securing the routing protocols has become a challenging task, due to the excessive usage of wireless connections. Typically, there are several motivations for the eavesdropper to attack the routing protocols [112]. Routing protocols in UAVs are vulnerable to different cyber-attacks because of various reasons [112]–[114]. For instance, they rely heavily on wireless connections which are highly vulnerable to attacks such as data tampering, DoS attacks, and eavesdropping [115]. Furthermore, because of the dynamic topology of FANETs, it is very hard to distinguish between a legitimate and malicious node. A legitimate node may also misbehave for a short period of time due to poor connection quality

TABLE 8. Vulnerabilities and their countermeasures for the routing protocols used in UAVs security.

Categories	Techniques	Details	Countermeasures
Packet forwarding and routing protocols	Static routing [107]	Information disclosure	Authentication precools must be incorporated
	Routing for data packets [108]	Dynamic topology	UAV must be intelligent to identify the redundant traffic
	Load-carry-and-deliver (LCAD) static routing [109]	Large latency issues	Implemented a relay function in an ad-hoc network [110]
	Static routing [110]	Does not allow to change the routing tables during the mission	can replace with it dynamic routing.
	Hybrid Packet forwarding [111]	uses delay tolerant forwarding and end-to-end routing, which is not efficient	UAV must be enough intelligent, it can be possible by incorporating ML techniques

or loss of route [116]. Moreover, the UAV launched by the attacker may behave properly for some time to gain trust, but simultaneously, it may also create inconsistencies in the routing. For example, the attacker may broadcast a non-existing link or produce a new routing message to mislead the other nodes. Such attacks are very hard to tackle as the malicious node may be a legitimate entity.

1) ANALYSIS OF SECURITY ISSUES IN ROUTING PROTOCOLS

Without proper security mechanisms, routing protocols may be subject to information disclosure. The attacker may collect information related to the network topology, the position of UAVs, the commands and controls, and the traffic payload. The confidentiality of the system is not protected if an attacker can obtain all that information by eavesdropping. Most of the routing protocols have this vulnerability [117]–[119].

Due to lack of authentication mechanisms, the attacker may also collect information related to the commands and controls, and the data traffic [107]. If the attacker can successfully attract the control packets during the discovery of a route, it can perform many attacks such as, disconnecting a specific link, rejecting the legitimate routing messages, cache poisoning, or modifying the control packets [120], [121].

The attacker can also aim to breach existing routing protocols to degrade the performance of a network or to modify its topology [108]. The performance can be degraded by perturbing the routing algorithm or by launching a DOS attack. The attacker can add redundant traffics to the system to increase the load thus decreasing the performance. The attacker can also modify the topology of a network by introducing non-existent nodes into the routing tables, forging a route link or by performing a packet modification attack.

2) ATTACKS ON ROUTING PROTOCOLS

Due to the security issues discussed in the previous section, routing protocols are exposed to different types of threats. The goal of the attacker is to control the network traffic, disrupt the routing functions, or inject malicious nodes. The threats can be classified based on the basic routing functionalities into various types of attacks such as route discovery attacks, route maintenance phase attacks, and data forwarding phase attacks [122], as described below.

- The goal of the attacker while performing a route discovery attack is to modify the network topology by adding malicious nodes or by invalidating the routes. During the route discovery process, a sender node searches for a route to a destination node. The sender broadcasts a route request and waits for a route response. The discovery process of the route is very crucial as it conditions other routing processes. A reliable route will be found if the packets are properly exchanged without any manipulation by the attacker. Otherwise, the attacker can establish a false route containing malicious node [123].
- The attacks during the route maintenance phase are conducted after route loss or when a link breaks due the node movement [124]. To reduce the excessive overhead required in discovering a new route and to achieve stability, routing maintenance is necessary. It is done by exchanging the beacon messages periodically. The objective of the attacker is to degrade the performance by adding redundant nodes, irrelevant traffic to increase the routing load and add processing delay. Normally, in a routing protocol, an error message is generated to publish the broken routes. A malicious node may exploit that functionality by broadcasting false route error messages, and hence, prevents the source node from communicating with the destination.

- During the message forwarding phase attacks, the goal of the attacker is to fail the mission by disrupting the forwarding of the payload traffic [125]. A malicious node may drop, replay, or modify the packets. In addition, the attacker can also delay/disrupt the time sensitive communication by delaying the packets to their respective next-hop destinations.

3) SECURITY SOLUTIONS FOR ROUTING PROTOCOLS

To ensure the security of the routing protocols, it is necessary to preserve the reliability, efficiency, and accuracy within the malicious attacker's environment. To preserve the integrity and confidentiality of the routing packets, traditional methods such as symmetric and asymmetric cryptography can be used as discussed in Section II-A. The hashing mechanism or a digital signature can also be incorporated to achieve the desired task. However, it adds to the computational complexity.

IV. LESSONS LEARNED

This section provides an overall picture of the proposed survey and emphasizes on the key lessons learned. The survey consists of five major sections. Sections I highlighted the issues with the security of UAVs and defined the scope of this work. Section II and Section III were devoted to addressing the security protocols used in UAVs and the vulnerabilities in these protocols, respectively. The key lessons learned from sections II and III are as follows:

1) With the exponential growth in UAVs technology and their applications, the variety of algorithms associated with the security of UAVs have been proposed. The applications of UAVs include the information transmission from UAVs to the ground station, the data capturing, and the transfer of goods. The secure transmission of information between different components of UAVs is very important. Several protocols are presented in the literature to secure the transmitted data so that attackers cannot access the sensitive information. Apart from secure transmission, it is also very important for the security protocols used in UAVs to verify the authenticity of the data. |In fact, it is common for attackers to send spoofed signals/information to trap the UAVs. The suitability of different authentication protocols was investigated and applied over the years. As UAVs have limited resources in terms of memory and processing power, it is often recommended to use lightweight authentication to make the protocols efficient.
2) Although there are several security protocols in the literature to secure the communication between the different components of UAVs, most of them can be attacked. Several weaknesses in the system can be exploited to compromise the UAV system using attacks such as GPS signal spoofing, false data injection attacks, WiFi insecurities, jamming attacks, etc. The spoofing attacks can be performed using different techniques. Commonly, the attackers use the spoofed signals with greater frequency than the actual signals sent by ground station to the UAV.
3) Routing and packet forwarding protocols are a major part of FANETs. However, most of these protocols did not consider security in the initial design. Security features in the routing protocols have not yet been explored in depth within the context of FANETs. The routing protocols used in FANETs is an attractive target for the attackers to control the network or disrupt the normal operation.

For the successful deployment of UAVs in critical missions, it is very important that all the vulnerabilities in the existing security protocols are identified and removed.

V. CHALLENGES AND FUTURE RESEARCH DIRECTIONS

With the advancement in recent UAV technology, the use and applications of UAVs are growing exponentially. There are many open research areas with elevated levels that should be tackled in an efficient way in order to produce secure and dependable future UAV generations. Furnishing new arrangements must be limited with specific necessities and limitations like low intricacy and unwavering quality. This section discusses the conceivable future directions for security correspondence frameworks.

A. CONNECTIVITY INSECURITY

There are two common ways to connect the UAVs to the ground station. The first is the connection through WiFi and the second is using the radio signals. Although wired connections are more secure than wireless connections but there are some range limitations in wired connections. So, most of the UAVs are connected through wireless connections. As the WiFi is protected with the password, the attacker can easily break the barrier and can get access to the WiFi connection. The WiFi password can either be in the form of alphabets, special characters, numeric values, or the combination of all these three. There are two ways to provide more security to the wireless connections: one is the encryption methodology [126], and the other is the watermarking technology [127]. The novelty can be produced in the existing security protocols by deploying Watermarking with cryptography. The reason is that when anyone secures the text by watermarking, the watermarked text retains its meaningful content. Hence, there is a possibility that even after hacking the password, the attacker may apply the cracked password before applying the reverse process of the watermarking.

B. DATA INSECURITY

Most of the data capture by the UAVs is in the form of images which must be protected before forwarding to the destination. Many security protocols have been presented by the researchers which are designed for the protection of the data. However, for the secure transmission of the data from the UAV to the ground station, robust secure algorithms are required which must be incorporated with different

transforms such as discrete cosine transform, discrete wavelet transform, and discrete Fourier transform. In some of the security algorithms, the key size is kept too large, due to which a large bandwidth is required. As the large key size is required to resist brute force attacks, and to significantly reduce the large bandwidth requirements, the key size should be only large enough to resist the brute force attacks.

C. AUTHENTICATION OBSTACLES IN UAVS

Authentication is a key aspect of the UAV network. In fact, most of the eavesdroppers use fake information, that comes in the form of signals such as GPS signals and WiFi signals, to hijack the UAV. Spoofing techniques are frequently used to distract the UAVs. In addition, the authentication is very important to identify the right signal received by the UAVs. Researchers are putting their efforts to tackle this research area. Although a lot of information authentication protocols have been proposed, there is still a need for improving the existing works. For instance, in some of the existing authentication protocols, a single random number is used for the authentication process. A single random number can easily be predicted by performing a brute force attack. Therefore, instead of using a single random number, chaotic maps must be used with an appropriate key for creating different random numbers [128]–[131]. Less dimensional chaos cannot work properly in order to produce more random substitution boxes and more random numbers. One can use high dimensional chaotic maps such as hyper chaotic map to solve the generation of truly random number [132].

D. INTRUSION DETECTION SYSTEMS (IDSS) IN UAVS

For intrusion detection, many machine learning algorithms have been used. Machine learning algorithms predict future events based on previously learned data. To increase the accuracy of the machine learning models, the features should be relevant. For instance, if the features that are used in the data set are irrelevant, the predicted results may be inaccurate. To improve the machine learning-based intrusion detection techniques, deep learning should be incorporated that can help in predicting the future events more accurately. Increasing the number of features used to detect the intrusions can also increase the accuracy of the model. Moreover, when utilizing a larger number of features, some attributes become useless, and hence, they will not contribute to the accuracy of the machine learning model, and they must be removed using well known methods such as correlation.

VI. CONCLUSION

In this paper, we have highlighted the issues with existing security protocols for UAVs. Firstly, we studied the existing security protocols used in the UAVs. Secondly, we identified the vulnerabilities in the existing protocols. Our survey revealed that the existing security protocols need significant improvements to make the UAVs more secure. Also, the vulnerabilities identified in the existing protocols need to be addressed in order to secure the next generations of UAVs. Furthermore, we have summarized some future research directions in the area of UAV security. We believe that the strong security in the UAVs is a fundamental concern and we expect that the researchers will show their interest to make the UAVs more secure in the forthcoming years.

REFERENCES

[1] K. Mabodi, M. Yusefi, S. Zandiyan, L. Irankhah, and R. Fotohi, "Multi-level trust-based intelligence schema for securing of Internet of Things (IoT) against security threats using cryptographic authentication," *J. Supercomput.*, vol. 76, no. 6, pp. 1–26, 2020.

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

[3] T. Fox-Brewster. Maldrone: Watch Malware That Wants to Spread its Wings Kill a Drone Mid-Flight. Forbes Magazine. Accessed: Feb. 27, 2021. [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2015/01/27/malware-takes-down-drone/?sh=65e60af44c92

[4] E. G. Abdallah, H. S. Hassanein, and M. Zulkernine, "A survey of security attacks in information-centric networking," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1441–1454, 3rd Quart., 2015.

[5] J. Li, S. Kamin, G. Zheng, F. Neubrech, S. Zhang, and N. Liu, "Addressable metasurfaces for dynamic holography and optical information encryption," *Sci. Adv.*, vol. 4, no. 6, 2018, Art. no. eaar6768.

[6] Y. Su, S. Z. F. Phua, Y. Li, X. Zhou, D. Jana, G. Liu, W. Q. Lim, W. K. Ong, C. Yang, and Y. Zhao, "Ultralong room temperature phosphorescence from amorphous organic materials toward confidential information encryption and decryption," *Sci. Adv.*, vol. 4, no. 5, 2018, Art. no. eaas9732.

[7] S. Heron, "Advanced encryption standard (AES)," *Netw. Secur.*, vol. 2009, no. 12, pp. 8–12, 2009.

[8] M. P. Arthur, "Detecting signal spoofing and jamming attacks in UAV networks using a lightweight IDS," in *Proc. Int. Conf. Comput., Inf. Telecommun. Syst. (CITS)*, Aug. 2019, pp. 1–5.

[9] M. Majidi, A. Erfanian, and H. Khaloozadeh, "Prediction-discrepancy based on innovative particle filter for estimating UAV true position in the presence of the GPS spoofing attacks," *IET Radar, Sonar Navigat.*, vol. 14, no. 6, pp. 887–897, Jun. 2020.

[10] A. Abbaspour, K. K. Yen, S. Noei, and A. Sargolzaei, "Detection of fault data injection attack on UAV using adaptive neural network," *Procedia Comput. Sci.*, vol. 95, pp. 193–200, 2016.

[11] A. Sharma, P. Vanjani, N. Paliwal, C. M. W. Basnayaka, D. N. K. Jayakody, H.-C. Wang, and P. Muthuchidambaranathan, "Communication and networking technologies for UAVs: A survey," *J. Netw. Comput. Appl.*, vol. 168, Oct. 2020, Art. no. 102739.

[12] A. Sharma *et al.*, "Communication and networking technologies or UAVs: A survey," *J. Netw. Comput. Appl.*, 2020, Art. no. 102739.

[13] 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.

[14] V. Moss, D. Jones, and S. Nwaneri, "Analysis of homeland security and economic survey using special missions unmanned aerial vehicle utilities," in *Proc. IEEE Int. Geosci. Remote Sens. Symp.*, Jul. 2012, pp. 6154–6157.

[15] 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, 2nd Quart., 2019.

[16] 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.

[17] Y. Zhi, Z. Fu, X. Sun, and J. Yu, "Security and privacy issues of UAV: A survey," *Mobile Netw. Appl.*, vol. 25, no. 1, pp. 95–101, Feb. 2020.

[18] N. A. Khan, S. N. Brohi, and N. Z. Jhanjhi, "UAV's applications, architecture, security issues and attack scenarios: A survey," in *Intelligent Computing and Innovation on Data Science*. Singapore: Springer, 2020, pp. 753–760.

[19] J. McCoy and D. B. Rawat, "Software-defined networking for unmanned aerial vehicular networking and security: A survey," *Electronics*, vol. 8, no. 12, p. 1468, Dec. 2019.

[20] A. Cavoukian, "Privacy and drones: Unmanned aerial vehicles," Inf. Privacy Commissioner Ontario, Toronto, ON, Canada, 2012, pp. 1–30.
[21] M. A. Kafi, Y. Challal, D. Djenouri, M. Doudou, A. Bouabdallah, and N. Badache, "A study of wireless sensor networks for urban traffic monitoring: Applications and architectures," *Procedia Comput. Sci.*, vol. 19, pp. 617–626, 2013.
[22] P. Peterson, "Cryptkeeper: Improving security with encrypted RAM," in *Proc. IEEE Int. Conf. Technol. Homeland Secur. (HST)*, 2010, pp. 120–126.
[23] A. Jones and G. L. Kovacich, *Global Information Warfare: The New Digital Battlefield*. Boca Raton, FL, USA: CRC Press, 2015.
[24] A. Zeitlin, A. Lacher, J. Kuchar, and A. Drumm, "Collision avoidance for unmanned aircraft: Proving the safety case," MITRE Corp., McLean, VA, USA, 2006.
[25] F. Barfield, "Autonomous collision avoidance: The technical requirements," in *Proc. IEEE Nat. Aerosp. Electron. Conf. Eng. Tomorrow (NAECON)*, Oct. 2000, pp. 808–813.
[26] R. K. Sharma and D. Ghose, "Collision avoidance between UAV clusters using swarm intelligence techniques," *Int. J. Syst. Sci.*, vol. 40, no. 5, pp. 521–538, May 2009.
[27] L. Yang, J. Qi, J. Xiao, and X. Yong, "A literature review of UAV 3D path planning," in *Proc. 11th World Congr. Intell. Control Autom.*, Jun. 2014, pp. 2376–2381.
[28] J. Awrejcewicz, *Numerical Analysis: Theory and Application*. Norderstedt, Germany: BoD-Books on Demand, 2011.
[29] A. M. Brandt and M. B. Colton, "Haptic collision avoidance for a remotely operated quadrotor UAV in indoor environments," in *Proc. IEEE Int. Conf. Syst., Man Cybern.*, Oct. 2010, pp. 2724–2731.
[30] J. Israelsen, M. Beall, D. Bareiss, D. Stuart, E. Keeney, and J. van den Berg, "Automatic collision avoidance for manually tele-operated unmanned aerial vehicles," in *Proc. IEEE Int. Conf. Robot. Autom. (ICRA)*, May 2014, pp. 6638–6643.
[31] S. Atoev, O.-J. Kwon, C.-Y. Kim, S.-H. Lee, Y.-R. Choi, and K.-R. Kwon, "The secure UAV communication link based on OTP encryption technique," in *Proc. 11th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2019, pp. 1–3.
[32] Y. Niu, S. Xu, L. Wu, and W. Hu, "Airborne infrared and visible image fusion for target perception based on target region segmentation and discrete wavelet transform," *Math. Problems Eng.*, vol. 2012, pp. 1–10, 2012.
[33] Y. Ma, X. Wu, G. Yu, Y. Xu, and Y. Wang, "Pedestrian detection and tracking from low-resolution unmanned aerial vehicle thermal imagery," *Sensors*, vol. 16, no. 4, p. 446, Mar. 2016.
[34] V. V. Kirichenko, "Information security of communication channel with UAV," *Electron. Control Syst.*, vol. 3, no. 45, pp. 23–27, Oct. 2015.
[35] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[36] K. D. Wesson, T. E. Humphreys, and B. L. Evans, "Can cryptography secure next generation air traffic surveillance?" *IEEE Secur. Privacy Mag.*, to be published. [Online]. Available: https://rnl.ae.utexas.edu/images/stories/files/papers/adsb_for_submission.pdf
[37] W.-J. Pan, Z.-L. Feng, and Y. Wang, "ADS-B data authentication based on ECC and X. 509 certificate," *J. Electron. Sci. Technol.*, vol. 10, no. 1, pp. 51–55, Mar. 2012.
[38] E. Bresson, O. Chevassut, and D. Pointcheval, "Provably secure authenticated group Diffie–Hellman key exchange," *ACM Trans. Inf. Syst. Secur.*, vol. 10, no. 3, p. 10, Jul. 2007.
[39] O. K. Sahingoz, "Multi-level dynamic key management for scalable wireless sensor networks with UAV," in *Ubiquitous Information Technologies and Applications*. Dordrecht, The Netherlands: Springer, 2013, pp. 11–19.
[40] V. Valentin-Alexandru, B. Ion, and P. Victor-Valeriu, "Energy efficient trust-based security mechanism for wireless sensors and unmanned aerial vehicles," in *Proc. 11th Int. Conf. Electron., Comput. Artif. Intell. (ECAI)*, Jun. 2019, pp. 1–6.
[41] K. Yoon, D. Park, Y. Yim, K. Kim, S. K. Yang, and M. Robinson, "Security authentication system using encrypted channel on UAV network," in *Proc. 1st IEEE Int. Conf. Robotic Comput. (IRC)*, Apr. 2017, pp. 393–398.
[42] J. A. Steinmann, R. F. Babiceanu, and R. Seker, "UAS security: Encryption key negotiation for partitioned data," in *Proc. Integr. Commun. Navigat. Surveill. (ICNS)*, Apr. 2016, pp. 1E4-1–1E4-7.
[43] K. Driscoll, "Lightweight crypto for lightweight unmanned arial systems," in *Proc. Integr. Commun., Navigat., Surveill. Conf. (ICNS)*, Apr. 2018, pp. 1–15.
[44] J. Wang, Y. Liu, S. Niu, and H. Song, "Lightweight blockchain assisted secure routing of swarm UAS networking," *Comput. Commun.*, vol. 165, pp. 131–140, Jan. 2021.
[45] A. Demeri, W. Diehl, and A. Salman, "SADDLE: Secure aerial data delivery with lightweight encryption," in *Proc. Sci. Inf. Conf.* Cham, Switzerland: Springer, 2020.
[46] C. Pu and Y. Li, "Lightweight authentication protocol for unmanned aerial vehicles using physical unclonable function and chaotic system," in *Proc. IEEE Int. Symp. Local Metrop. Area Netw. (LANMAN)*, Jul. 2020, pp. 1–6.
[47] M. S. Haque and M. U. Chowdhury, "A new cyber security framework towards secure data communication for unmanned aerial vehicle (UAV)," in *Proc. Int. Conf. Secur. Privacy Commun. Syst.* Cham, Switzerland: Springer, 2017.
[48] T. Alladi, V. Chamola, and N. Kumar, "PARTH: A two-stage lightweight mutual authentication protocol for UAV surveillance networks," *Comput. Commun.*, vol. 160, pp. 81–90, 2020.
[49] B. D. Deebak and F. Al-Turjman, "A smart lightweight privacy preservation scheme for IoT-based UAV communication systems," *Comput. Commun.*, vol. 162, pp. 102–117, Oct. 2020.
[50] L. Teng, M. Jianfeng, F. Pengbin, M. Yue, M. Xindi, Z. Jiawei, C. Gao, and L. Di, "Lightweight security authentication mechanism towards UAV networks," in *Proc. Int. Conf. Netw. Netw. Appl. (NaNA)*, Oct. 2019, pp. 379–384.
[51] E. Barka, C. Kerrache, R. Hussain, N. Lagraa, A. Lakas, and S. Bouk, "A trusted lightweight communication strategy for flying named data networking," *Sensors*, vol. 18, no. 8, p. 2683, Aug. 2018.
[52] J. Srinivas, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "TCALAS: Temporal credential-based anonymous lightweight authentication scheme for Internet of drones environment," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6903–6916, Jul. 2019.
[53] Z. Ali, S. A. Chaudhry, M. S. Ramzan, and F. Al-Turjman, "Securing smart city surveillance: A lightweight authentication mechanism for unmanned vehicles," *IEEE Access*, vol. 8, pp. 43711–43724, 2020.
[54] Q. Li, Y. Yang, W.-K. Ma, M. Lin, J. Ge, and J. Lin, "Robust cooperative beamforming and artificial noise design for physical-layer secrecy in AF multi-antenna multi-relay networks," *IEEE Trans. Signal Process.*, vol. 63, no. 1, pp. 206–220, Jan. 2015.
[55] L. Sun and Q. Du, "Physical layer security with its applications in 5G networks: A review," *China Commun.*, vol. 14, no. 12, pp. 1–14, Dec. 2017.
[56] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.
[57] Y. Zeng, R. Zhang, and T. J. Lim, "Throughput maximization for UAV-enabled mobile relaying systems," *IEEE Trans. Commun.*, vol. 64, no. 12, pp. 4983–4996, Dec. 2016.
[58] D. H. Choi, S. H. Kim, and D. K. Sung, "Energy-efficient maneuvering and communication of a single UAV-based relay," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 50, no. 3, pp. 2320–2327, Jul. 2014.
[59] 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.
[60] Q. Wang, Z. Chen, W. Mei, and J. Fang, "Improving physical layer security using UAV-enabled mobile relaying," *IEEE Wireless Commun. Lett.*, vol. 6, no. 3, pp. 310–313, Jun. 2017.
[61] X. Lu, L. Xiao, C. Dai, and H. Dai, "UAV-aided cellular communications with deep reinforcement learning against jamming," 2018, *arXiv:1805.06628*. [Online]. Available: http://arxiv.org/abs/1805.06628
[62] W.-S. Ra, I.-H. Whang, and J. B. Park, "Robust weighted least squares range estimator for UAV applications," in *Proc. SICE Annu. Conf.*, Aug. 2008, pp. 251–255.
[63] M. Bejiga, A. Zeggada, A. Nouffidj, and F. Melgani, "A convolutional neural network approach for assisting avalanche search and rescue operations with UAV imagery," *Remote Sens.*, vol. 9, no. 2, p. 100, Jan. 2017.
[64] A. Nemes and G. Mester, "Unconstrained evolutionary and gradient descent-based tuning of fuzzy-partitions for UAV dynamic modeling," *FME Trans.*, vol. 45, no. 1, pp. 1–8, 2017.
[65] T. M. Hoang, N. M. Nguyen, and T. Q. Duong, "Detection of eavesdropping attack in UAV-aided wireless systems: Unsupervised learning with one-class SVM and K-means clustering," *IEEE Wireless Commun. Lett.*, vol. 9, no. 2, pp. 139–142, Feb. 2020.

[66] H. Lee, S. Eom, J. Park, and I. Lee, "UAV-aided secure communications with cooperative jamming," *IEEE Trans. Veh. Technol.*, vol. 67, no. 10, pp. 9385–9392, Oct. 2018.
[67] H. Sedjelmaci, S. M. Senouci, and N. Ansari, "Intrusion detection and ejection framework against lethal attacks in UAV-aided networks: A Bayesian game-theoretic methodology," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 5, pp. 1143–1153, May 2017.
[68] J. Xu, Z. Deng, Q. Song, Q. Chi, T. Wu, Y. Huang, D. Liu, and M. Gao, "Multi-UAV counter-game model based on uncertain information," *Appl. Math. Comput.*, vol. 366, Feb. 2020, Art. no. 124684.
[69] M. Z. Anwar, Z. Kaleem, and A. Jamalipour, "Machine learning inspired sound-based amateur drone detection for public safety applications," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2526–2534, Mar. 2019.
[70] A. Shoufan, H. M. Al-Angari, M. F. A. Sheikh, and E. Damiani, "Drone pilot identification by classifying radio-control signals," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 10, pp. 2439–2447, Oct. 2018.
[71] M. Ezuma, F. Erden, C. K. Anjinappa, O. Ozdemir, and I. Guvenc, "Detection and classification of UAVs using RF fingerprints in the presence of Wi-Fi and Bluetooth interference," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 60–76, 2020.
[72] F. Li, J. Xin, T. Chen, L. Xin, Z. Wei, Y. Li, Y. Zhang, H. Jin, Y. Tu, X. Zhou, and H. Liao, "An automatic detection method of bird's nest on transmission line tower based on faster_RCNN," *IEEE Access*, vol. 8, pp. 164214–164221, 2020.
[73] A. Alipour-Fanid, M. Dabaghchian, N. Wang, P. Wang, L. Zhao, and K. Zeng, "Machine learning-based delay-aware UAV detection over encrypted Wi-Fi traffic," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Jun. 2019, pp. 1–7.
[74] J. Han, Z. Yang, H. Xu, G. Hu, C. Zhang, H. Li, S. Lai, and H. Zeng, "Search like an eagle: A cascaded model for insulator missing faults detection in aerial images," *Energies*, vol. 13, no. 3, p. 713, Feb. 2020.
[75] M. Faraji-Biregani and R. Fotohi, "Secure communication between UAVs using a method based on smart agents in unmanned aerial vehicles," *J. Supercomput.*, pp. 1–28, 2020.
[76] Y. Li, R. Zhang, J. Zhang, and L. Yang, "Cooperative jamming via spectrum sharing for secure UAV communications," *IEEE Wireless Commun. Lett.*, vol. 9, no. 3, pp. 326–330, Mar. 2020.
[77] W. D. Scheller, *Detecting Drones Using Machine Learning*. Ames, IA, USA: Iowa State Univ., 2017. [Online]. Available: https://lib.dr.iastate.edu/etd/16210/
[78] W. Hong, L. Jianhua, L. Chengzhe, and W. Zhe, "A provably secure aggregate authentication scheme for unmanned aerial vehicle cluster networks," *Peer-to-Peer Netw. Appl.*, vol. 13, no. 1, pp. 53–63, Jan. 2020.
[79] U. Challita, A. Ferdowsi, M. Chen, and W. Saad, "Machine learning for wireless connectivity and security of cellular-connected UAVs," *IEEE Wireless Commun.*, vol. 26, no. 1, pp. 28–35, Feb. 2019.
[80] 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.
[81] B. Hudson, "Drone attacks are essentially terrorism by joystick," The Washington Post, 2018.
[82] 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.
[83] R. Fotohi, E. Nazemi, and F. S. Aliee, "An agent-based self-protective method to secure communication between UAVs in unmanned aerial vehicle networks," *Veh. Commun.*, vol. 26, Dec. 2020, Art. no. 100267.
[84] C. Li, Y. Xu, J. Xia, and J. Zhao, "Protecting secure communication under UAV smart attack with imperfect channel estimation," *IEEE Access*, vol. 6, pp. 76395–76401, 2018.
[85] K. Amelin, S. Tomashevich, and B. Andrievsky, "Recursive identification of motion model parameters for ultralight UAV," *IFAC-PapersOnLine*, vol. 48, no. 11, pp. 233–237, 2015.
[86] 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. MILCOM IEEE Mil. Commun. Conf.*, Nov. 2016, pp. 1213–1218.
[87] K.-W. Huang and H.-M. Wang, "Combating the control signal spoofing attack in UAV systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7769–7773, Aug. 2018.
[88] 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.
[89] H. Sedjelmaci, S. M. Senouci, and N. Ansari, "A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 48, no. 9, pp. 1594–1606, Sep. 2018.
[90] 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.
[91] S. Kamate and N. Yilmazer, "Application of object detection and tracking techniques for unmanned aerial vehicles," *Procedia Comput. Sci.*, vol. 61, pp. 436–441, Jan. 2015.
[92] D. Davidson, H. Wu, R. Jellinek, V. Singh, and T. Ristenpart, "Controlling UAVs with sensor input spoofing attacks," in *Proc. 10th USENIX Workshop Offensive Technol. (WOOT)*, 2016.
[93] 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.
[94] 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.
[95] 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.
[96] R. Rysdyk, "UAV path following for constant line-of-sight," in *Proc. 2nd AIAA 'Unmanned Unlimited' Conf. Workshop Exhibit*, Sep. 2003, p. 6626.
[97] M. Hong, T.-H. Chang, X. Wang, M. Razaviyayn, S. Ma, and Z.-Q. Luo, "A block successive upper-bound minimization method of multipliers for linearly constrained convex optimization," *Math. Oper. Res.*, vol. 45, no. 3, pp. 833–861, Aug. 2020.
[98] Z. Birnbaum, A. Dolgikh, V. Skormin, E. O'Brien, D. Muller, and C. Stracquodaine, "Unmanned aerial vehicle security using recursive parameter estimation," *J. Intell. Robotic Syst.*, vol. 84, nos. 1–4, pp. 107–120, Dec. 2016.
[99] S. Utsai and R. B. Joshi, "DOS attack reduction by using Web service filter," *Int. J. Comput. Appl.*, vol. 105, no. 14, 2014.
[100] A. Kolichtchak, "Buffer overflow attack detection and suppression," U.S. Patent 09 904 502, Jan. 16, 2003.
[101] A. Crosland, R. May, E. Flaherty, and A. Draper, "Embedded processor with watchdog timer for programmable logic," U.S. Patent 7 340 596, Mar. 4, 2008.
[102] W. Gruszczy ski, E. Puniach, P. wi kała, and W. Matwij, "Application of convolutional neural networks for low vegetation filtering from data acquired by UAVs," *ISPRS J. Photogramm. Remote Sens.*, vol. 158, pp. 1–10, Dec. 2019.
[103] M. Talha, F. Asghar, A. Rohan, M. Rabah, and S. H. Kim, "Fuzzy logic-based robust and autonomous safe landing for UAV quadcopter," *Arabian J. Sci. Eng.*, vol. 44, no. 3, pp. 2627–2639, Mar. 2019.
[104] I. Bisio, C. Garibotto, F. Lavagetto, A. Sciarrone, and S. Zappatore, "Blind detection: Advanced techniques for WiFi-based drone surveillance," *IEEE Trans. Veh. Technol.*, vol. 68, no. 1, pp. 938–946, Jan. 2019.
[105] W.-H. Au, K. C. C. Chan, and X. Yao, "A novel evolutionary data mining algorithm with applications to churn prediction," *IEEE Trans. Evol. Comput.*, vol. 7, no. 6, pp. 532–545, Dec. 2003.
[106] Y. Zhou, P. L. Yeoh, H. Chen, Y. Li, R. Schober, L. Zhuo, and B. Vucetic, "Improving physical layer security via a UAV friendly jammer for unknown eavesdropper location," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11280–11284, Nov. 2018.
[107] N. Vanitha and G. Padmavathi, "A comparative study on communication architecture of unmanned aerial vehicles and security analysis of false data dissemination attacks," in *Proc. Int. Conf. Current Trends Towards Converging Technol. (ICCTCT)*, Mar. 2018, pp. 1–8.
[108] J. A. Maxa, M. S. Mahmoud, and N. Larrieu, "Survey on UAANET routing protocols and network security challenges," *Adhoc Sensor Wireless Netw.*, vol. 37, Apr. 2017.
[109] C. Pu, "Link-quality and traffic-load aware routing for UAV ad hoc networks," in *Proc. IEEE 4th Int. Conf. Collaboration Internet Comput. (CIC)*, Oct. 2018, pp. 71–79.
[110] B.-S. Kim, K.-I. Kim, B. Roh, and H. Choi, "A new routing protocol for UAV relayed tactical mobile ad hoc networks," in *Proc. Wireless Telecommun. Symp. (WTS)*, Apr. 2018, pp. 1–4.
[111] C. Pu and L. Carpenter, "To route or to ferry: A hybrid packet forwarding algorithm in flying ad hoc networks," in *Proc. IEEE 18th Int. Symp. Netw. Comput. Appl. (NCA)*, Sep. 2019, pp. 1–8.

[112] M. Islabudeen and M. K. K. Devi, "A smart approach for intrusion detection and prevention system in mobile ad hoc networks against security attacks," *Wireless Pers. Commun.*, vol. 112, no. 1, pp. 193–224, May 2020.
[113] A. Mondal and S. Mitra, "Security issues in vehicular ad hoc networks for evolution towards Internet of Vehicles," in *Connected Vehicles in the Internet of Things*. Cham, Switzerland: Springer, 2020, pp. 253–307.
[114] A. K. Malhi, S. Batra, and H. S. Pannu, "Security of vehicular ad-hoc networks: A comprehensive survey," *Comput. Secur.*, vol. 89, Feb. 2020, Art. no. 101664.
[115] N. M. Rodday, R. D. O. Schmidt, and A. Pras, "Exploring security vulnerabilities of unmanned aerial vehicles," in *Proc. NOMS IEEE/IFIP Netw. Oper. Manage. Symp.*, Apr. 2016, pp. 993–994.
[116] M. O. Kalinin and A. Minin, "Security evaluation of a wireless ad-hoc network with dynamic topology," *Autom. Control Comput. Sci.*, vol. 51, no. 8, pp. 899–901, 2017.
[117] J.-A. Maxa, M. S. B. Mahmoud, and N. Larrieu, "Performance evaluation of a new secure routing protocol for UAV ad hoc network," in *Proc. IEEE/AIAA 38th Digit. Avionics Syst. Conf. (DASC)*, Sep. 2019, pp. 1–10.
[118] M. J. Alala, K. I. Khorzom, and W. Y. Aljuneidi, "Effects of communication channel on AODV performance within UAANETs," *Int. J. Commun.*, vol. 3, Mar. 2018.
[119] H. Nawaz and H. M. Ali, "Implementation of cross layer design for efficient power and routing in UAV communication networks," *Stud. Informat. Control*, vol. 29, no. 1, pp. 111–120, Mar. 2020.
[120] D. Sasirekha and N. Radha, "Secure and attack aware routing in mobile ad hoc networks against wormhole and sinkhole attacks," in *Proc. 2nd Int. Conf. Commun. Electron. Syst. (ICCES)*, Oct. 2017, pp. 505–510.
[121] K. Wang, C. Pan, H. Ren, W. Xu, L. Zhang, and A. Nallanathan, "Packet error probability and effective throughput for ultra-reliable and low-latency UAV communications," *IEEE Trans. Commun.*, vol. 69, no. 1, pp. 73–84, Jan. 2021.
[122] V. Desnitsky, N. Rudavin, and I. Kotenko, "Modeling and evaluation of battery depletion attacks on unmanned aerial vehicles in crisis management systems," in *Proc. Int. Symp. Intell. Distrib. Comput.* Cham, Switzerland: Springer, 2019.
[123] S. Abbas, M. Faisal, H. Ur Rahman, M. Z. Khan, M. Merabti, and A. U. R. Khan, "Masquerading attacks detection in mobile ad hoc networks," *IEEE Access*, vol. 6, pp. 55013–55025, 2018.
[124] R. H. Jhaveri, A. D. Patel, J. D. Parmar, and B. I. Shah, "Manet routing protocols and wormhole attack against AODV," *Int. J. Comput. Sci. Netw. Secur.*, vol. 10, no. 4, pp. 12–18, 2010.
[125] A. Kamble, V. S. Malemath, and D. Patil, "Security attacks and secure routing protocols in RPL-based Internet of Things: Survey," in *Proc. Int. Conf. Emerg. Trends Innov. ICT (ICEI)*, Feb. 2017, pp. 33–39.
[126] V. Kriz and P. Gabrlik, "UranusLink–communication protocol for UAV with small overhead and encryption ability," *IFAC-PapersOnLine*, vol. 48, no. 4, pp. 474–479, 2015.
[127] M. P. Marcinak and B. G. Mobasseri, "Digital video watermarking for metadata embedding in UAV video," in *Proc. MILCOM IEEE Mil. Commun. Conf.*, Oct. 2005, p. 1637.
[128] Z. Cheng, Y. X. Tang, and Y. L. Liu, "3-D path planning for UAV based on chaos particle swarm optimization," *Appl. Mech. Mater.*, vol. 232, pp. 625–630, Nov. 2012.
[129] M. Rosalie, G. Danoy, S. Chaumette, and P. Bouvry, "Chaos-enhanced mobility models for multilevel swarms of UAVs," *Swarm Evol. Comput.*, vol. 41, pp. 36–48, Aug. 2018.
[130] M. Rosalie, G. Danoy, S. Chaumette, and P. Bouvry, "From random process to chaotic behavior in swarms of UAVs," in *Proc. 6th ACM Symp. Develop. Anal. Intell. Veh. Netw. Appl.*, Nov. 2016, pp. 9–15.
[131] J. Sun, W. Wang, L. Kou, Y. Lin, L. Zhang, Q. Da, and L. Chen, "A data authentication scheme for UAV ad hoc network communication," *J. Supercomput.*, vol. 76, no. 6, pp. 4041–4056, Jun. 2020.
[132] P. S. Gohari, H. Mohammadi, and S. Taghvaei, "Using chaotic maps for 3D boundary surveillance by quadrotor robot," *Appl. Soft Comput.*, vol. 76, pp. 68–77, Mar. 2019.

ARSLAN SHAFIQUE received the B.E. and M.S. degrees in mechatronics and electrical engineering from Wah Engineering College, Heavy Industries Taxila Education City (HITEC) University, Pakistan, in 2014 and 2017, respectively. He is currently pursuing the Ph.D. degree with Riphah International University, Islamabad, Pakistan. He also serving as a Research Associate with the Faculty of Engineering and Applied Sciences, Riphah International University. He has five journal publications with accumulative impact factor of 14.54. His research interests include cryptography, secure communication, and machine learning.

ABID MEHMOOD (Member, IEEE) received the Ph.D. degree in computer science from Deakin University, Australia. He is currently an Assistant Professor with Abu Dhabi University. His research interests include information security and privacy, data mining, machine learning, and cloud computing.

MOURAD ELHADEF received the B.Sc. and M.Sc. degrees in computer science from the Institut Supérieur de Gestion de Tunis, Tunisia, and the Ph.D. degree in computer science from the University of Sherbrooke, Sherbrooke, QC, Canada. He is currently a Professor of Computer Science with the College of Engineering, Abu Dhabi University, United Arab Emirates. He has over 50 publications in refereed journals and conference proceedings. His current research interests include fault tolerance and fault diagnosis in distributed, wireless and ad-hoc networks, cloud computing, artificial intelligence, and security. He is an Active Reviewer for various international conferences and journals, such as IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS and *Journal of Parallel and Distributed Computing*.