Self-adaptive Intrusion Detection System for UAV-to-UAV Communications in UAV Networks

Reza Fotohi (✉ fotohi.reza@gmail.com)

Shahid Beheshti University <https://orcid.org/0000-0002-1848-0220>

Masoud Abdan

Ferdowsi University of Mashhad

Research Article

Keywords: Attacker UAVs, Multi-module methods, Human Immune System (HIS), Self-adaptive Intrusion Detection System

Posted Date: April 26th, 2021

DOI: <https://doi.org/10.21203/rs.3.rs-179732/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Self-adaptive Intrusion Detection System for UAV-to-UAV Communications in UAV Networks

Reza Fotohi¹ . Masoud Abdan²

Abstract Unmanned aerial vehicles (UAVs) have recently attracted many researchers' attention because of their extensive applications. Security issues, in particular, are a serious concern in such networks since the top-secret information exchanged between UAVs is susceptible to various attacks such as Sybil, blackhole, and Flooding attacks. To identify such malicious UAVs that threaten the connections between normal UAVs, we introduce an impermeability method called SID-UAV that works at the level of UAV-to-UAV. The SID-UAV method, by employing a self-adaptive system, discovers the most reliable route from origin to destination. This approach deals with finding the malicious UAV and selecting the most reliable routes in several phases, including the route discovery phase, the decision-making phase, the attacker counter phase, and the knowledge database phase by using multi-module methods and applying Human Immune System (HIS). In the SID-UAV method, three main modules are intended: route analysis module, decision module, and defense module. Each of these modules has sub-modules and is distributed in different parts in UAV networks. Each module and its sub-modules have tasks, and all of these modules are connected to the knowledge base to record information in it and use the stored information quickly. The NS-3 simulator tool is exploited to simulate the proposed method. The results gained from simulation indicated that the SID-UAV method in criteria of Average Detection Ratio (ADR), Average Packet Delivery Ratio (APDR), Average Packet Lost Ratio (APLR), Average False Positive (AFP), Average False Negative (AFN) have acceptable performance relative to BRUIDS, SFA, and SUAS-HIS methods.

Keywords Attacker UAVs . Multi-module methods . Human Immune System (HIS). Self-adaptive Intrusion Detection System

✉ Reza Fotohi*
R_fotohi@sbu.ac.ir; Fotohi.reza@gmail.com

✉ Masoud Abdan
Abdan@mail.um.ac.ir

¹ Faculty of Computer Science and Engineering, Shahid Beheshti University, G. C. Evin, Tehran 1983969411, Iran

² Faculty of Engineering, Ferdowsi University of Mashhad, Mashhad, Iran

1 Introduction

In recent years, UAV networks have great progress in the field of wireless big data such as search and rescue operations, military duties, and delivery services, and establishing a secure communication link. Considering that these UAVs can be controlled remotely automatically or using an operator, and also the communication link between UAVs and the ground control station is a wireless communication link that allows attackers to control a UAV with their operations and cause it to crash, numerous security methods have been proposed [1-3].

A typical scenario is shown in Figure 1, which shows the connections between UAVs. This scenario includes multiple UAVs, satellite links, and links between UAVs. Each link in this type of communication is responsible for exchanging information between UAVs. In such usages, the UAVs are normally responsible for patrolling an intermediary land stretched within the site, in which the ballistic missile is launched and its considered target. Considering that the ballistic missiles are able to cruise at severely high speeds, they dictate using the fast-detecting techniques to eliminate and to track. In specific, for increasing the opportunity to intercept a ballistic missile successfully, having a swift tracking and detection system is essential to detect and track the missile immediately after launching. The designers who work on ballistic missile defense networks make the system able to intercept the missiles over their preliminary 2 to 5 min of flight known as the boost phase. Over the boost phase, if the missile's trajectory is straightly away from the UAV's trajectory, it will simply decrease from the sensors range over the UAV. Therefore, the information

routing utilized in the network of the ballistic missile's sensors needs to be stated utilizing hybrid wireless sensors' networks able to comply with high availability and necessities instructed owing to security.

In this paper, the proposed SID-UAV deals with finding the malicious UAV and selecting the most reliable routes in several phases, including the route discovery phase, the decision-making phase, the attacker counter phase, and the knowledge database phase by using multi-module methods and applying artificial immune system. To achieve this, the proposed scheme employs a self-protective method with multiple modules and sub-modules as well as a knowledge base, which is continuously updated. Each of the modules has sub-modules and is distributed in different sections of the UAV networks. All of these modules connect to a knowledge base to quickly record information and use the stored information to identify malicious UAVs accurately.

The main contribution of this article is as follows:

- Using an HIS to detect and discover attacker UAVs
- Using a self-adapting system to eliminate human resources
- Using multiple modules to accurately detect malicious UAVs

Table 1 shows all the abbreviations used, the symbol and the descriptions of some of them in this article.

Fig. 1 Typical UAV communication scenario.

Table 1 Symbol and descriptions of some of them.

Symbol	Description	Symbol	Description
UAVs	Unmanned aerial vehicles	SINR	Signal-to-interference-plus-noise ratio
SID-UAV	Self-adaptive Intrusion Detection System for UAV-to-UAV Communications in UAV Networks	$P_{DR}(r)$	Possibility of destructive route
APDR	Average Packet Delivery Ratio	Th	Threshold
APLR	Average Packet Lost Ratio	α	Smoothing factor
AFP	Average False Positive	X_t	Test packets submitted over a period of time
AFN	Average False Negative	P_t	Average transfer of Test packages in each time period
ADR	Average Detection Ratio	ATN	Average True Negative
NS-3	Network Simulator 3	AFN	Average False Negative
BRUIDS	Behavior rule-based UAV IDS	κ	Intruder rate
SFA	Security framework to protect an aircraft	N	Experiments
Ab	Anti-body	CBR	Constant bitrate
U2U	UAV-to-UAV	Ag	Anti gent
GPS	Global Positioning System	D	Distance
UASs	Unmanned Aerial Systems	AN	Artificial Noise
DoS	Denial of Service	SHA	Secure Hash Algorithms
DDoS	Distributed Denial of Service	MA	Mutual authentication
RREQ	Route Request	MITM	Man-in-the-middle attack
RREP	Route Reply	HMT	Hello Packet Table
HIS	Human Immune System	N	Time period

The organization of the different sections of this article is as follows: Section 2 describes in detail the Preliminaries, which include two subsections, Cyber Security Threats and HIS. Section 3 describes the latest Related work related to the topic of this article and compares them all. The proposed SID-UAV approach with all its details and subsections is given in Section 4. Section 5 of this paper presents the performance evaluation in which the simulation results of the proposed method and the other two methods were compared and discussed. Conclusion and future work This article is presented in the final section.

2 Preliminaries

This section provides a detailed description of both Cyber Security Threats and HIS subsections in detail.

2.1 Cyber Security Threats

In the world of communication between UAVs, there are various attacks that jeopardize the normal communication between UAVs and as a result packets are not exchanged successfully between UAVs. This article discusses three types of Attacker UAVs, which are described as follows:

2.1.1 Sybil Attack

Sybil attack is one of these attacks that the attacker UAV attempts to use network resources unfairly by impersonating other UAVs and tries to disrupt the security of the network with the identity of other UAVs so that they seem to be the cause of those UAVs whose identity has been stolen [5].

2.1.2 Blackhole Attack

Blackhole attack is a type of Denial-of-Service attack in which the routing, the UAV that is

supposed to send the packets, discards them and does not deliver them to the target UAV (neighbor or destination). Since packets are usually removed in UAV networks, the detection and prevention of this type of attack are very difficult [6].

2.1.3 Flooding Attack

Flooding attack falls into the category of DDoS attacks. This attack tries to minimize the capacity of the desired UAV to respond to the request of other normal UAVs and prevent other UAVs from accessing the service by sending too many RREQ messages and keeping the desired UAV busy [7].

2.2 Human Immune System (HIS)

The HIS must be able to distinguish its own cells from foreign cells by identifying the surface proteins of the cells. Each cell has proteins on its surface membrane that are known to it, and these proteins are ignored by the immune system on the surface of the body's cells so that the immune system only reacts to the proteins on the surface of foreign cells. Any substance that can trigger an immune response in the immune system is called an antigen. In many cases, the antigen is a bacterium, fungus, virus, toxin, or foreign body. But sometimes an antigen can be one of the body's own cells that is damaged or dead. A wide range of immune system cells work together to detect an antigen [8].

The immune system responds to pathogens in two specific and non-specific ways. When the body's defense barriers, such as the skin and mucous membranes, prevent foreign agents from entering the body and identify and eliminate foreign agents, regardless of their type, it is in fact using a non-specific mechanism for the body's immunity. Deadly phagocytes and lymphocytes also use the general properties of external agents to detect

and destroy them, and these cells also defend the body in a non-specific way [8].

According to Figure 2, the cells of different parts of the immune system are made up of several organs.

Fig. 2 Location of immune system cells.

2.2.1 Affinity

Using various models in HIS, the affinity between antigens (attacking) and antibodies (defending) is calculated [8]. The affinity model is very vital since the detection ability depends on the affinity between the detector and the antigen. Suppose that the coordinates of an antibody are provided by $Ab = (Ab1, Ab2, \dots, Abn)$ and the coordinates of an antigen are represented by $Ag = (Ag1, Ag2, \dots, Agn)$; the distance between them, D shows the affinity, which can be calculated using Eq. (1).

$$\text{Let } R = \{r_0, r_1, \dots, r_m\}, \quad S = \{s_0, s_1, \dots, s_m\} \quad (1)$$

$$\text{Manhattan } D = \sum_{i=0}^m |r_i - s_i|$$

$$\text{Hamming } D = \sum_{i=0}^m \delta = 1 \text{ if } r_i \neq s_i, \text{ if otherwise}$$

$$\text{Euclidean } D = \sqrt{\sum_{i=0}^m (r_i - s_i)^2}$$

where r and s respectively represent different characteristics of columns, m is the number of data.

2.2.2 Learning

In a HIS, agents are trained to differentiate via actions like negative selection, danger theory, clonal selection, or self and non-self-human immune networks [8].

3 Related work

In this section, all articles related to securing communication between UAVs against a series of attacks such as black holes, wormholes, sink and flooding are analyzed and also, in Table 2, under the Complexity and Robustness criteria, all these articles were compared.

Due to the highly influential role of the cluster head, such as transferring data to a UAV, distributing UAV data among existing members, and collecting data from members, many attackers attempt to put their infected nodes as cluster head. Because infected nodes can easily declare themselves as cluster heads in the cluster head selection process, so an infected cluster consumes more energy than a conventional cluster since it must greedily send corrupt and destructive messages to the sink (destination) node in addition to its usual role. Accordingly, we offer an efficient energy cluster head selection method with the assistance of a UAV that collects the residual energy of the nodes and employs them to select a new cluster head. Our proposed method provides better security than the conventional cluster head selection method (with a short selection period) due to the cluster head selection period. Moreover, changing the node contamination time does not influence our framework's superiority relative to the conventional selection framework [9].

In [10], a method of data transmission based on artificial noise (AN) in a UAV-based IoT system is suggested to protect legitimate transfer (i.e., secret key distribution) with WPT integration. It involves a passive eavesdropper, a target IoD, and free K IoDs. In order for the user to be able to decode the confidential information by removing the fake noise, the UAV gate must transfer the confidential information (e.g., the secret key) to a target IoD. The reason it cannot decode confidential data is that the eavesdropper is not able to remove the artificial voice. We simplify the security rate maximization (SRM)

problem under the restriction of the likelihood of eavesdropping by the following items:

1. Simplifying the objective function to gain an analytical solution to the problem.
2. Reducing restrictions and thus simplifying the possibility of eavesdropping
3. Examining the optimal power allocation problem

To improve the security and data privacy of VC-based tools, a BlockChain Technology (BCT) solution is offered. The obtained data is then stored in an atrium-based public blockchain to provide the conditions for the integrated and continuous execution of BCT transactions. In a virtual vehicle monitoring system, the proposed scheme is evaluated by implementing an IoT-based application. Technical information on the necessary instructions for the UAV, authentication, and vehicle response is stored on a cloud platform in which pentatop-based??? and SHA-based elliptic curve cryptography (ECC) is employed to ensure data privacy in the data warehouse. Therefore, the proposed method helps to protect data against cryptographic and plain text attacks. The simulation results indicated that the proposed approach in service quality criteria has a much better performance than previous methods [11].

In [12], we considered a new scenario in which two UAVs are employed to transmit confidential information and an eavesdropper whose real position is unknown. Besides, we proposed an optimization problem for the confidentiality rate under multiple constraints to test how much wireless communications security would improve when the UAV was exploited as a wireless relay. In the proposed method, the problem is non-convex and mixed optimization, which simultaneously optimizes "route lines" and "transfer power" to maximize the confidentiality rate through the block coordinate descent (BCD) technique and the sequential convex approximation technique.

In [13], the mutual authentication (MA) of the proposed PARTH protocol is achieved among three levels of institutions in the defined software "UAV" network (SDUAVN). The main contribution of this paper:

1. The PARTH technique ensures mutual authentication, message integrity, identity protection, secrecy, and confidentiality of data. It is also shown that this mechanism is perfectly safe against drone lure attacks, replay attacks, MITM attacks even without the storage of hidden keys in the UAV.
2. We propose PARTH, a PUF-based authentication protocol for three-layer defined software UAV networks, which includes a ground station and two layers of drones.
3. This paper presents a lightweight security plan that creates two unique session keys for security applications.

In [14], the authors suggest a cyber defense solution based on a non-cooperative game to protect the UEC against network attacks, which is an Unmanned Aerial Vehicle Edge Computing (UEC) network. Investigating security issues in a UAV-edge computing network is almost difficult and mandatory because of the importance of UEC services, such as network traffic monitoring or search operations. Computational overhead and energy consumption aim to achieve an optimal protection rate of the proposed method.

In [15], the default Diffie-Hellman computational basis of the elliptic curve is developed in a random oracle model. All types of UAV data can be verified by batch verification instead of "one-to-one verification." The IBE-AggAuth scheme has also been demonstrated to be safe and resistant against attacks of adaptive selected messages and ID (EUF-CMA) attacks. The simulation assessments represented the following cases:

1. IBE - AggAuth can be applied to the decentralized and self-organizing UAVCN environment.
2. IBE - AggAuth not only ensures data security but also guarantees the verification process by reducing computing and communication costs.
3. UAVs are allowed to join the data transfer process at any time dynamically.

The main innovation of the proposed method in [16] is a new hybrid approach that can detect malicious attacks and traffic anomalies such as DDoS attacks. This malicious traffic data was generated using a hybrid UAV network simulator. The simulation results of the new IDS system from its performance test on real UAV routes, real DDoS attacks, and real UAV foreground traffic indicate its optimal efficiency. Ultimately, various types of anomalies were carefully identified by the intrusion detection process proposed in this paper.

In [17], a method for detecting malicious UAVs based on the rule of conduct relies on the use of monitor nodes. In this method, each UAV is responsible for monitoring its neighbor. Also, the sensors placed in the UAVs are able to control the same UAV, and if it removes normal packets, it is quickly detected and removed from the circuit. However, this method requires propulsion sensors to be able to detect multiple destructive drones.

In [18], the authors reviewed all the methods proposed to identify Attacker UAVs and focused on the most dangerous of all Attackers. This paper presents a security framework, called SFA, that is proposed to identify and prevent an attack that targets UAVs. The old methods had two main problems: one was low strength and the other was high complexity. To address these vulnerabilities, the authors of this article [18] provided a security framework that can be used to secure a UAV against malicious threats.

In [19], an efficient and safe method in order to secure unmanned aerial systems is proposed, which has efficiency in two ways: first, it has high detection accuracy and low false-positive and false-negative rates, and second, it quickly detects and isolates attacks. Method [19] has defended against malicious drones in two phases. In the first phase, it has initially evaluated the candidate routes using Hello packets and, in the second phase, it has

evaluated and discovered the routes containing malicious UAVs. Moreover, in the method [19], security issues such as wormhole, blackhole, gray hole attacks, and dissemination of fake information that can target the drone are prevented.

In Table 2, all the methods mentioned in the related work section in Attack type, Complexity and Robustness were compared.

Table 2 Compare Complexity and Robustness of all related tasks

References	Attack type	Complexity	Robustness
[9]	Cyber attack	Medium	Medium
[10]	Opportunistic attacker	High	High
[11]	Hybrid	High	Medium
[12]	Reply attack	High	High
[13]	Plaintext and ciphertext attacks	Low	Low
[14]	Malicious attacks	Medium	Medium
[15]	Physical tampering attacks	Medium	High
[16]	Cyber Attacks	High	Low
[17]	ID attacks	High	High
[18]	DDoS	Medium	Low
[19]	Wormhole, Blackhole, Gray hole, and Fake information dissemination	High	High

4 The proposed SID-UAV approach

In the method introduced in this section, using a self-adaptive system, the most reliable route from origin to destination is discovered. The proposed scheme deals with finding the malicious UAV and selecting the most reliable routes in several phases, including the route discovery phase, the decision-making phase, the attacker counter phase, and the knowledge database phase by using multi-module methods and applying an artificial immune system. To achieve this, the proposed scheme employs a self-protective method with multiple modules

and sub-modules as well as a knowledge base, which is continuously updated. In the SID-UAV method, three main modules are considered: route analysis module, decision module, and defense module. Each of the modules has sub-modules and is distributed in different sections of the UAVN. Each module and its sub-modules have tasks, and all of these modules are connected to the knowledge base to record information in it and use the stored information quickly. Figure 3 illustrates the relationship between the modules with each other and with the knowledge base. The proposed scheme is

introduced to detect Sybil, blackhole, and Flooding attacks.

4.1 First phase: Discovering and examining the routes

In the proposed SID-UAV design, the routes between the origin and the destination must be discovered in the first step to choose the most reliable route from them. Therefore, in the first step, the route request packet (RREQ) is sent from the origin UAV to the destination UAV to discover the routes between the origin and destination. After sending the RREQ packet, with receiving the route reply packet (RREP), the most reliable route should be selected from

the existing routes, and the attacking nodes should be detected and disconnected from the network.

4.1.1 Route Analysis Module

In order to study the routes on the basis of the artificial immune algorithm, antigens are exploited. Antigens are intended as the set of all detected routes from the source UAV to the destination UAV according to RREP messages.

Route analysis module behaves like a T-Cell in the immune system and is responsible for routing by studying abnormal behaviours of UAVs on the routes and reporting them. These modules have three sub-modules, each of which is part of the task. These sub-modules are:

1. Data collection sub-module
2. Filtering sub-module
3. Connection with decision module sub-module

Route analysis modules in SID-UAVs are modules that examine existing routes to a destination or antigen intended in order to detect the malicious behaviour of UAVs in each route and to detect malicious UAVs.

First, the data collection sub-module creates routing tables based on the RREQ messages sent and received according to the RREP messages. Then, the filtering sub-module works so that a "hello packet" is sent from the origin to the single-hop neighbouring nodes after creating the routing table. In this step, the listening algorithm is employed to check the routes. Each node must maintain a hello message table (HMT), which is a packet to detect the malicious or healthy nodes in the route.

Fig. 3 The relationship between the modules with the knowledge base and the UAV network

The listening algorithm is divided into three phases:

- When a hello packet is sent to a single-hop node, its specification is added to the HMT, and the other nodes listen to it.
- When the hello packet is received, the hello packet information is stored in HMT.
- At a specific time period, the node must calculate the listening rate of the hello packets in this period and compare it with the threshold. Here we define the listening rate in the N-th time period as Eq. (2).

$$LR(N) = \left(\frac{\text{Total number of forward packets sent}}{\text{Total number of packets listened}} \right) \quad (2)$$

To compute the listening rate, the node calculates the ratio of the number of hello packets it has received and sent forward to the number of packets it has listened to. If the packet delivery rate is below the threshold (TLR (N)), the node becomes suspicious of its neighbor node, then sends the suspicious node ID to the origin. This route is then rejected by the filtering sub-module and sends the other routes to the decision sub-module so that this sub-module sends all the route information to the decision module and the knowledge base. In this design, the filtering sub-module considers a threshold of 0.7, meaning that if more than 30% of the packets are not sent, the UAV node will

be suspicious. The pseudo-code of filtering routes is shown in Figure 4.

The decision module can combine infiltration information and make more precise infiltration decisions.

Fig. 4 Pseudo-code of filtering routes

Pseudo-code 1: Filtering routes
Input: Routes detected by the data collection module
Output: Send non-suspicious UAV routes to the sub-module of communication with the decision module
1: Start 2: Send detected routes from data collection module sub-module to filtering sub-module 3: Create a hello packet and send it to single-hop UAVs of source 4: Save the hello packet information in the <i>HMT</i> table and send it to other single-hop UAVs on the route to the destination 5: Hello packet listening 6: Calculate the listening rate $LR(N)$ by each UAV 7: If $LR(N) < (TLR(N))$ is Then 7-1 Send suspicious UAV ID to source UAV Otherwise 7-2 The route is reliable 8: Send routes without suspicious UAVs to the sub-module of communication with the decision module 9: End

4.2 Second phase: Decision-making

The second phase is to make a decision by employing a decision-making module. The decision module operates similarly to the B-Cell in the HIS algorithm. The decision module can effectively make the right decision for the existence of attacks in the network based on the information received from the module and communicate with the knowledge base. The main objective of the SID-UAV decision module, similar to the B-Cell operation in the HIS algorithm, is to discover outsider patterns in a potentially large set of insider patterns.

The module also immediately sends its detected information to the knowledge base when it detects the presence of a suspicious node in the route. Therefore, the knowledge base can communicate with the generator to

create new modules for review, decision-making, and defense against these attacks.

The decision module in the proposed scheme exploits four criteria of latency, energy, average packet loss ratio (APLR), and signal-to-noise ratio (SINR) to detect attacks based on the information received from the route analysis module. A malicious UAV produces a signal intensity higher than normal (SINR generated by a malicious UAV). The discovery process is performed so that it initially collects all the SINRs generated by the senders. It then compares them to conventional SINRs (SINRs generated by a normal UAV). This distinguishes the intensity of the suspicious and normal signals, and the SINR is much higher than normal for malicious UAVs.

Table 3. Decision module

Suspicious routes	SINR	Energy	PLR	Latency
R ₁	32	85%	15%	30ms
R ₂	73	75%	25%	15ms
R ₃	30	95%	5%	20ms
Threshold	$Th = \left(\left(\frac{Latency}{MaxLatency} \right) + \left(\frac{PLR}{MaxPLR} \right) + \left(\frac{MaxEnergy}{Energy} \right) + \left(\frac{SINR}{MaxSINR} \right) \right)$			

These criteria are chosen based on the types of attacks intended in this scheme because the malicious UAV deletes all the packets it receives in some attacks, while the attacking UAV deletes only a few packets received in others.

Hence, the decision module examines the four considered criteria based on the route monitoring phase and obtaining the information obtained in each route. The decision module calculates the threshold for suspicious routes and sends an alert to the defense module for routes with the highest threshold to detect malicious UAVs along the route. Table 3 illustrates the considered criteria and the relationship between these criteria for calculating the threshold. Calculating the threshold is so that high latency, high packet loss rate (APLR), low energy level, and low SINR in the route indicate the improper route and the presence of malicious UAVs on the route.

The decision module, based on the information received from the review module, calculates the value of Th for each of the paths using the four criteria expressed and is placed in a variable called. This module removes the path with the highest value and sends it to the defense module.

On the basis of the information received from the monitoring module, the decision module calculates the value of Th for each of the routes using the four criteria stated and is placed in a variable called $P_{DR}(r)$. This module removes the route with the highest value $P_{DR}(r)$ and sends it to the defense module.

4.3 Third phase: Attacker counter phase

In the third phase, defense modules are exploited for accurate detection of the attacker. These modules act somewhat like antibodies in the HIS algorithm. Defense modules function similar to antibodies, including proliferation and reduction. According to the information received from the decision modules, the defense modules can check the UAVs in the routes with malicious nodes sent by the decision module to take appropriate measures. In this way, by detecting an attacking UAV, neighboring UAVs are asked to refuse to resend packets received from these attacking UAVs, and these UAVs are removed from routing altogether.

To detect an attacking UAV in the desired route, the defense modules duplicate themselves around each node and start sending several test packets in the route in several consecutive periods. The test packet is similar to conventional packets in the UAVN network.

Thus, the attacking UAV node also tries to remove it by receiving this packet. The defense module for each UAV detects a malicious UAV in a suspicious route by examining Eq. (3).

$$\begin{cases} P_t = X_1 & \text{For } t=1 \\ P_t = \alpha * X_t + (1-\alpha) * P_{t-1} & \text{For } t > 1 \end{cases} \quad (3)$$

In formula (1):

- Coefficient α is actually the smoothing factor that has a constant value between zero and one.
- X_t is the number of test packets sent in a time period t is by the defense module.
- P_t is the average transfer of test packets in each time period t by the defense module.

In each period, a number of specific test packets are transmitted in the route with $P_{DR}(r)$,

which has a suspicious node specified in the previous phases. For each UAV, the defense module then calculates the number of test packets transmitted by that UAV. If the number of test packets transmitted (N_T) by a UAV is less than or equal to P_t value, it indicates that this UAV is an attacker UAV and deletes a number of packets. The coefficient α is considered a constant value between zero and one. The lower this coefficient is taken into account; the more packets are expected to be lost. Whereas if the coefficient α is selected to be a larger number close to one, the proposed scheme expects to lose a smaller number of packets. By doing this, defense modules can successfully detect attacking UAVs and disconnect them from the network (Figure 5).

The defense modules replicate themselves to remove attackers, and after a specified time period, by removing the attacker, more proliferation is prevented.

Fig. 5 Defense modules, by duplicating themselves, detect and discover malicious UAVs on suspicious routes.

The Pseudo-code of attacker counter phase is shown in Figure 6.

Fig. 6 Pseudo-code of attacker counter phase

Pseudo-code 2: Attacker counter phase
Input: The route with the highest value $P_{DR}(r)$ having a suspicious UAV received from the decision module Output: Distribution of ID of malicious UAVs detected and recording in the knowledge base
1: Start 2: Activate replication sub-module, and the replication of UAVs (lymphocytes) around the suspected UAVs 3: Send TEST packets in the network from the route with suspicious UAVs 4: Compute P_t based on the number of test packet set by defense module 5: If $N_T < P_t$ 5-1 The UAV node is malicious, send the malicious UAVs ID to the defense module 5-1-1 Send malicious UAVs ID to all UAVs 5-1-2 Activation of sub-module Reduction and reduction of lymphocytes Otherwise 5.2 The route is reliable. Send information to the defense module 5-2-1 Activation of the sub-module Reduction and Reduction of lymphocytes 6: Registration of malicious node ID and all information in the knowledge base by the defense module 7: End

The defense module can detect malicious UAVs by replicating itself, and after detecting malicious UAVs in the network, the reduction sub-module is activated and commands to reduce replicated UAVs.

All this information is recorded in the defense module, and this module asks all UAVs in the route not to send the packets they receive from this UAV and to delete them. Besides, they ask all UAVs to stop sending messages to this malicious UAV. The defense module also sends a message to identify the malicious UAV to the knowledge base so that this UAV is not utilized in routing.

4.4 Fourth phase: Recording of information in the knowledge base

In the proposed scheme, the knowledge base is associated with all modules and must be intelligently developed to defend against various

types of attacks. The knowledge base is similar to security memory in the HIS algorithm and includes the following five steps to select the most reliable route in the security memory to send data based on the information received from the modules:

4.4.1 Perform affinity

As defined in the human immune system, the greater the affinity of the antibody for the antigen, that is, the shorter the distance between the antibody and the antigen, the better the supplement to the antigen. Besides, when this information is stored in memory cells, it causes it to produce more antibodies in a shorter time when it comes in contact with the same antigen again. In the proposed method, to select the best B-Cell and perform the affinity operation, routes are selected that have low latency, low packet loss rate, SINR, and high energy; that is, at this

stage, routes are selected that have a moderate threshold and their value is moderate.

4.4.2 Adapting

At this stage, we compare and evaluate the routes that had a medium threshold (routes with a moderate value $P_{DR}(r)$) with the following two features to select the most reliable route. It should also be noted that the most important feature of an attacker detection mechanism is that they are modified over time and also defined in such a way that they can be modified and can easily have the power of learning. Details of the first and second features in the adapting section are expressed as follows:

First feature: The distance between the source and destination UAV (Distance): On the basis of the information obtained, the knowledge base calculates the distance between

the source and destination UAV for all routes received from the source UAV to the destination UAV.

Second feature: The rate of packets received by UAVs (APDR): In the proposed method, by considering several attacks, intruders destroy all or part of the packets received by receiving the packet. Therefore, the rate of receiving APDR packets is lower than these UAVs, and they destroy them by receiving the packet and do not send them to other UAVs in the network.

4.4.3 Complete the detector set

In the step of completing the detector set for all routes whose threshold value (Th) was moderate, i.e., routes that have medium $P_{DR}(r)$, algorithm 3 is used to select the most reliable route, according to Figure 7:

Fig. 7 Pseudo-code for the selection of reliable route

Pseudo-code 3: Choose a trusted route
<p>1: Initialization</p> <p>2: Variable $P_{DR}(r)$ Rate of 4 criteria for each route</p> <p>3: Variable C Indicates the number of candidate routes between the origin and destination UAVs</p> <p>4: Variable F_r represents the fitness of the route</p> <p>5: Variable $UAV_{trusted}$ represents a reliable route between UAVs</p> <p>6: Reliable route selection procedure:</p> <p>7: Do for routes from: 1 to C.</p> <p>8: Calculate the value of Th for each route.</p> <p>9: If $P_{DR}(r) \leq MAX\ Th.$, Then</p> <p>10: Delete the route and send a warning to the defense module.</p> <p>11: Otherwise</p> <p>12: Select routes with average Th ($AVG(p_{dr})$)</p> <p>13: Calculate variable F_r as follows</p> $F_r(PDR_i, Distance_i) = \left(\frac{Max\ APDR}{APDR_i} \right) + \left(\frac{Distance_i}{Max\ Distance} \right)$ <p>14: The route with the following condition is selected:</p> $UAV_{trusted} = AVG(p_{dr}) \ \& \ MAX(F_r)$ <p>15: End</p> <p>16: End</p> <p>17: End</p>

According to pseudo-code 3, after filtering the destructive routes by calculating the threshold Th and placing it in the variable $P_{DR}(r)$ for each route, the routes that have average $P_{DR}(r)$ based on the function F_r are also compared for the fitness of the routes, and the route that has a larger number F_r is selected as the most reliable route to send the packet.

4.4.4 Carrying out overshoot

Among the routes evaluated in the previous step, the routes that have almost the identical conditions (average threshold and maximum evaluation function) are sent to the overshoot stage so that the routes in this step are evaluated with another measure, which is the lowest loss rate in this criterion to select the most reliable route with the lowest loss rate for UAVs.

4.4.5 Record in immunological memory

Routes that have the conditions of a relation $UAV_{trusted}$ or besides have the lowest loss rate after the overshoot stage, that route is the most reliable route and will be recorded in immunological memory for use the next time.

The flowchart of the proposed SID-UAV method is represented in Figure 8.

4.5 SID-UAV feature analysis

In this design, a method has been proposed using an artificial immune system algorithm and intelligent multi-module technology that generates several desirable features. We will explain some of them below.

Distributivity: Because the intended modules are similar to the distribution of lymphocytes in the body, they are distributed in the entire UAV, and the knowledge base is updated periodically by all modules, which has led to increased distributivity of the work. The three modules considered are logically independent, and each has sub-modules, and also have interfaces to communicate with each other through sub-modules or independently. Route analysis modules that have three sub-modules can filter the performance of UAVs in the route by sending a hello message. The decision module can analyze the behavior of UAVs on the routes based on the intended criteria and detect routes with malicious UAVs, and the defense module can also independently detect attackers and remove them from the network.

Independence: Since the artificial immune system algorithm that is derived from the immune system does not require external management and maintenance to classify and destroy pathogens, so the knowledge base and a variety of proposed modules can independently examine, decide, and defend the attacking UAVs of the three intended attacks in cooperation with other modules. The knowledge base and modules can be updated or renewed independently in the SID-UAV in the proposed scheme.

Self-protection: The proposed scheme based on the HIS algorithm, such as the immune system, which is capable of learning to defend against new pathogens, can work with the proposed modules and use a trained knowledge base to quickly detect attacks.

Fig. 8 Flowchart of the proposed SID-UAV method

In the SID-UAV method, each step of the self-adaptive cycle was applied in accordance with Figure 9:

Figure 9 Self-adaptive steps

Managed resource: The source in the proposed scheme is the UAVN network.

Sensor: The sensor is actually a sub-module for data collection from UAVs, which performs route information collection operations by sending RREQ and receiving RREP from the UAVN network.

Monitoring: This component is done using the filtering submodule. The received RREPs examine the information of the UAVs obtained by the collection sub-module and discover the routes with suspicious nodes according to the refining step.

Analysis: The analysis component in the proposed method takes the routes between the UAVs from the monitoring component and analyzes them and then selects the reliable route. This section is done by two sub-modules of filtering and communication that are in the monitoring module and by refining the detected

routes and routes with suspicious nodes and their information to the decision module.

Planning: This component decides to choose the most reliable routes. The planning of this component in the proposed SID-UAV method is based on the decision module by considering four criteria and calculating the threshold parameter Th and the criterion $P_{DR}(r)$.

Execution: The execution department has mechanisms for performing planned operations. In the proposed SID-UAV method, it is done in two parts: one in the defense module to remove malicious UAVs and the other in the knowledge base to select the safest route by performing affinity, mutation, and adapting operations.

Knowledge: In the SID-UAV method, knowledge means the knowledge base intended in Figure (9).

Operator: The operator in the SID-UAV method is defined as sending the selected reliable route to the UAV network by the knowledge base.

Since the SID-UAV method works with all modules and sub-modules, so it is very accurate and completely impressive to detect Sybil, blackhole, and flooding attacks. In the hypothetical scenario, several modules are employed in the UAVs; however, if necessary, they can increase the duplication of the sub-modules to be reduced to the sub-modules again after the detection of malicious UAVs. Hence, in the SID-UAV method, the following two methods are taken into account to update the knowledge base:

1. Regarding the efficiency of the modules themselves and the abnormal behavior of the network, periodic surveys are collected from all the modules.
2. If an unknown attack occurs, the information of that attack will be recorded in the knowledge base by the module.

5 Performance evaluation

This section has two subsections called Performance metrics and Simulation results and analysis: The results extracted from the simulator are shown in the format of tables and graphs. It also compares the simulation results of the proposed SID-UAV method with the last three methods that worked on the detection of malicious UAVs under important criteria. The results were compared with three methods (BRUIDS [17], SFA [18], and SUAS-HIS [19]). To demonstrate a feasibility study, the performance analysis of BRUIDS, SFA, and SUAS-HIS has been divided into five parts: ADR, APDR, APLR, AFP, and AFN.

5.1 Performance metrics

In this subsection, the concept and formula of all measure are explained in detail.

APDR: Total packets that were successfully received in the destination UAV divided by the total packets that were successfully sent in the origin UAVs. Multiply the result by 100 to get the percentage [21, 22]. This measure has been analyzed using Eq (4).

$$APDR = \left(\left(\frac{1}{N} \right) * \left(\frac{\sum_{i=1}^N R_i}{\sum_{i=1}^N S_i} \right) * 100 \right) \quad (4)$$

APLR: Number of data packets sent by the source UAV; Minus the number of data packets received by the destination UAV [23-25]. The meaning of the variables used in Eq (4) and (5) is explained in Table 4. Eq (5) shows the *APLR* measure.

$$APLR = \left(\left(\frac{1}{N} \right) * \left(\frac{\sum_{i=1}^N S_i - \sum_{i=1}^N R_i}{\sum_{i=1}^N S_i} \right) * 100 \right) \quad (5)$$

Table 4 Variables and their meanings

Variables	Means
R_i	Total data packets received by UAV_i
S_i	Total data packets sent by UAV_i
N	Number of scenarios executed

ADR: The definition of this measure is as follows: the ratio of intruder UAVs to total intruder UAVs that have been correctly identified as intruder UAVs [26-28]. This measure has been analyzed using Eq (6). Also, the meaning of the variables used in Eq (6) is explained in Table 5.

$$\begin{aligned}
ADR &= \left(\frac{ATP}{ATP + AFN} \right) * 100 & (6) \quad AFP &= \left(\frac{AFP}{AFP + ATN} \right) & ATP &= \left(\frac{ATP}{ATP + AFN} \right) \\
\text{Where:} \quad All &= ATP + ATN + AFP + AFN & AFN &= \left(\frac{ATP + ATN}{All} \right) & ATN &= \left(\frac{ATN}{ATN + AFP} \right)
\end{aligned}$$

Table 5 Definition of measures.

Measure	Definition
AFP	The number of normal UAVs falsely detected as intruder UAVs [29].
AFN	The number of intruder UAVs detected as the normal UAVs divided by the total number of intruder UAVs.
ATN	The number of normal UAVs correctly detected as the normal UAVs divided by the total number of normal UAVs.
ATP	The number of normal UAVs falsely detected as the intruder UAVs divided by the total number of normal UAVs [30].

5.2 Simulation results and analysis

In this subsection, simulation results are shown for all measures. The proposed SID-UAV method has been simulated and its performance evaluated in NS-3 Simulator on Linux Ubuntu 14 LTS. Because the data extracted from the simulation is correct and logical, the most important parameters of UAVs such as MAC Layer, UAV speed, etc. are used. The rest of the parameters used in the simulator are listed in Table 6.

Details of the parameters used in the three scenarios are given in Table 7. The only difference between the three scenarios is the intruder UAV rate. The rest of the parameters are considered the same.

Table 6 Details of the parameters used in the simulation

Parameters	Value
Number of UAVs	140
UAV speed	150 m/s
Packet size	256 bytes
Transmission range	25 M
Intruder UAV	5%, 10%, 15%
Intruder UAV ratio	5, 10, and 15%
Channel type	Wireless
MAC	MAC/802.11.b
Traffic type	Constant Bit Rate
Transmission layer	UDP (User Datagram Protocol)

Table 7 Important parameters of all three scenarios

Scenario #1		Scenario #2	
Antibody	150	Antibody	150
Intruder UAV rate (%)	5	Intruder UAV rate (%)	10
Topology (m x m)	500 x 500	Topology (m x m)	1000 x 1000
Time	3000	Time	3000
Scenario #3			
Antibody	150		
Intruder UAV rate (%)	15		
Topology (m x m)	1500 x 1500		
Time	3000		

APDR: Since the proposed approach selects the safest (most reliable) route from source to destination using a self-adapting system, it has a better APDR than other methods. These results are represented in Table 8 and Figure 10. Moreover, because the proposed method employs a self-protection method that has multi-modules and sub-modules, as well as having a knowledge base that is constantly updated, UAVs exchange packets with a safe route, thus improving the APDR measure. Unfortunately,

due to the lack of an accurate and robust security system in other methods, this criterion is influenced by malicious UAVs, and their efficiency dramatically drops. Therefore, while the malicious UAV rate is 10%, the APDR of SID-UAV, SUAS-HIS, SFA, and BRUIDS methods are 90%, 78%, 75%, and 71%, respectively. This output for the second scenario is 82, 73, 71, and 69, respectively, and it is 77, 69, 65, and 62, respectively, for the third scenario.

Table 8 APDR all 4 methods against the number of UAVs

Number of UAVs	APDR (%)			
	BRUIDS	SFA	SUAS-HIS	SID-UAV
20	63.2	64.1	66.8	69
40	63.6	65.5	67.3	71
60	64.2	66.7	68	72
80	64.6	66.9	69	73
100	64.9	67.6	70	74
120	65.5	68.2	71	75
140	65.8	68.7	72	77

Fig. 10 APDR with different κ

(A) $\kappa = 10\%$

(B) $\kappa = 15\%$

(C) $\kappa = 20\%$

APLR: Because three main modules, including route analysis module, decision module, and defense module are employed in the SID-UAV method, no malicious UAV can bypass this restriction and penetrate the network. Therefore, since packet deletion will not occur in this network, the APLR criterion will be in a better position in the proposed method. These results are displayed in Table 9 and Figure 11. Unfortunately, due to the lack of a strong and

accurate security system in other methods, this criterion is affected by malicious UAVs, and their efficiency is severely reduced. Hence, in the case of malicious UAV rate equal to 10%, APLR of SID-UAV, SUAS-HIS, SFA, and BRUIDS methods are equal to 10, 16, 21, and 24%, respectively. This output for the second scenario is 15, 21, 28, and 34, respectively, and it is 17, 25, 34, and 39, respectively, for the third scenario.

Table 9 APLR all 4 methods against the number of UAVs

Number of UAVs	APLR (%)			
	BRUIDS	SFA	SUAS-HIS	SID-UAV
20	37	35	33	29
40	36	34	32	27
60	35	33	31	25
80	34	32	31	23
100	33	31	29	20
120	32	30	21	19
140	31	28	20	17

Fig. 11 APLR with different κ

(A) $\kappa = 10\%$

(B) $\kappa = 15\%$

AFP: The SID-UAV method has a lower AFP than the other approaches, as indicated in Table 10 and Figure 12. This is in a situation where the AFP of the SID-UAV method is lower than the methods compared in this paper. The reason for the superiority of the proposed method is the use of security modules, each of which has sub-modules and are distributed in different sections in the UAV network. Also, each module with its sub-modules has security tasks in identifying enemy UAVs, and all of these modules are

(C) $\kappa = 20\%$

connected to the knowledge base to quickly record information in it and use the information stored in this knowledge base to Stop the activity of enemy UAVs. The AFP of all methods is 6, 19, 26, and 35% for the SID-UAV, SUAS-HIS, SFA, and BRUIDS methods, respectively, when a malicious UAV rate is equal to 10%. The output for the second scenario is 12, 24, 31, and 39, respectively, and it is equal to 18, 29, 35, and 43, respectively, for the third scenario.

Table 10 AFP all 4 methods against the number of UAVs.

Number of UAVs	AFP (%)			
	BRUIDS	SFA	SUAS-HIS	SID-UAV
20	12.11	10.1	9.08	4.5
40	15.7	14.8	12.9	6
60	24.9	16.6	14.7	7
80	29.7	19.4	17.8	9
100	38.7	26.4	22.7	10
120	45.8	31.8	23.4	13
140	51.8	39.6	27.8	15

Fig. 12 AFP with different κ

(A) $\kappa = 10\%$

(B) $\kappa = 15\%$

(C) $\kappa = 20\%$

AFN: As you can see in Table 11 and Figure 13, the AFN method proposed in all three scenarios is better than the other three methods. When the range of enemy UAVs increases from 100 to 140, the AFN criterion has grown less in the proposed method, but in all three methods this growth has been very high, indicating that the enemy UAV has had a greater impact on these three methods. The reason for the high AFN percentage in the other two methods, SFA and BRUIDS, is that they used only classical, rule-based methods to detect the position of the UAV, which has no effect on the stronger and safer identification of enemy UAVs. Also, because the BRUIDS method uses the least

amount of stealth with joint optimization of transmission power, it can not work against malicious UAVs. But because the proposed method uses a MAPE-K-based self-protection and self-adaptation method to secure communications between UAVs, it has a better AFN than other methods. Therefore, the output obtained from the simulation shows that in the proposed method, when the percentage of enemy UAVs is 10, 15 and 20%, respectively, the AFN output is 5, 7 and 11%. However, this value for SUAS-HIS, SFA and BRUIDS methods is 15%, 32% and 38%, respectively, which indicates the poor performance of all three methods.

Table 11 AFN all 4 methods against the number of UAVs.

Number of UAVs	AFN (%)			
	BRUIDS	SFA	SUAS-HIS	SID-UAV
20	9.8	9.8	9.8	4.3
40	12.9	11.4	10.5	5.5
60	13.7	12.3	11.9	5.9
80	19.4	14.8	12.8	6.9
100	22.9	16.9	13.7	7
120	23.9	17.8	14.9	8.5

140	24.6	18.2	15.4	10.5
-----	------	------	------	------

Fig. 13 AFN with different κ

(A) $\kappa = 10\%$

(B) $\kappa = 15\%$

(C) $\kappa = 20\%$

ADR: As you can see in Table 12 and Figure 14, the ADR method proposed in all three scenarios is better than the other three methods. The reason for better ADR in the proposed method is that the routes between the origin and the destination must be discovered in the first step in order to choose the safest route among

them. Therefore, in the first step, the route request packet (RREQ) is initially sent from the origin UAV to the destination

UAV to detect the routes between the origin and destination. After sending the RREQ packet, with receiving the reply packet (RREP), the safest route should be selected from the existing

routes, and the attacking nodes should be detected and disconnected from the network. The reason for bad ADR in the three methods of SUAS-HIS, SFA, and BRUIDS is that they merely employed the classical method to detect the position of UAVs, which cannot completely stop the malicious UAV. Thus, while the

malicious UAV rate is 10%, the ADR SID-UAV, SUAS-HIS, SFA, and BRUIDS methods are 95%, 80%, 65%, and 53%, respectively. The output for the second scenario is 91, 75, 61, and 50, respectively, and it is equal to 85, 71, 58, and 45, respectively, for the third scenario.

Table 12 ADR all 4 methods against the number of UAVs.

Number of UAVs	DR (%)			
	BRUIDS	SFA	SUAS-HIS	SID-UAV
20	85	86	86	90
40	80	83	84	89
60	74	80	83	88
80	70	78	81	87
100	65	76	78	86
120	61	72	76	83
140	57	68	73	80

Fig. 14 ADR with different κ

(A) $\kappa = 10\%$

(B) $\kappa = 15\%$

(C) $\kappa = 20\%$

6 Conclusion and future work

Nowadays, UAVs' application has led to remarkable progress in the fields of trade, agriculture, environmental, military, and civilian programs. Therefore, a safe self-adaptation method on the basis of an artificial immune system was offered in this article. The proposed method is based on the MAPE-K self-adaptation loop, which acts based on three factors: analysis, decision, and defense agents to identify enemy UAVs. These agents themselves consist of several modules, and all of these modules are connected to the knowledge base to receive and send information. The proposed approach's main advantages are maintaining the security and better performance of communications between UAVs, in UAV-to-UAV communication structures against wormhole attacks, flooding attacks, and selective sending. The results obtained from the simulation in the form of charts and tables indicated that the SID-UAV method in APDR (higher than 10, 15, and 20%), APLR (less than 10, 15, and 20%), AFP (less than 10, 15, and

20%), AFN (less than 10, 15, and 20%), and ADR (higher than 10, 15, and 20%) were compared to BRUIDS, SFA, and SUAS-HIS methods, respectively.

Conflict of Interest

None

Funding

None

Informed Consent Statement

None

Credit authorship contribution statement

Reza Fotuhi: Conceptualization, Data curation, Formal analysis, Methodology, Validation, Writing- review & editing, Supervision.

Masoud Abdan: Methodology, Writing - original draft, Writing - review & editing.

References

1. Abdalla, A. S., Powell, K., Marojevic, V., & Geraci, G. (2020). UAV-assisted attack

- prevention, detection, and recovery of 5G networks. *IEEE Wireless Communications*, 27(4), 40-47.
2. Chamola, V., Kotes, P., Agarwal, A., Gupta, N., & Guizani, M. (2020). A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques. *Ad hoc Networks*, 102324.
3. Kumari, A., Gupta, R., Tanwar, S., & Kumar, N. (2020). A taxonomy of blockchain-enabled softwarization for secure UAV network. *Computer Communications*, 161, 304-323.
4. Faraji-Biregani, M., & Fotuhi, R. (2020). Secure communication between UAVs using a method based on smart agents in unmanned aerial vehicles. *The Journal of Supercomputing*, 1-28.
5. Singh, M. M., Dutta, N., Singh, T. R., & Nandi, U. (2020). A Technique to Detect Wormhole Attack in Wireless Sensor Network Using Artificial Neural Network. In *Evolutionary Computing and Mobile Sustainable Networks* (pp. 297-307). Springer, Singapore.
6. Fu, H., Liu, Y., Dong, Z., & Wu, Y. (2020). A Data Clustering Algorithm for Detecting Selective Forwarding Attack in Cluster-Based Wireless Sensor Networks. *Sensors*, 20(1), 23.
7. Tourani, R., Torres, G., & Misra, S. (2020, September). PERSIA: a Puzzle-based InterSt FloodIng Attack Countermeasure. In *Proceedings of the 7th ACM Conference on Information-Centric Networking* (pp. 117-128).
8. Schluter, J., Peled, J. U., Taylor, B. P., Markey, K. A., Smith, M., Taur, Y., ... & Amoretti, L. A. (2020). The gut microbiota is associated with immune cell dynamics in humans. *Nature*, 1-5.
9. Wang, G., Lee, B., Ahn, J., & Cho, G. (2020). A UAV-assisted CH election framework for secure data collection in wireless sensor networks. *Future Generation Computer Systems*, 102, 152-162.
10. Wang, Q., Dai, H. N., Li, X., Shukla, M. K., & Imran, M. (2020). Artificial noise aided scheme to secure UAV-assisted Internet of Things with wireless power transfer. *Computer Communications*, 164, 1-12.
11. Ch, R., Srivastava, G., Gadekallu, T. R., Maddikunta, P. K. R., & Bhattacharya, S. (2020). Security and privacy of UAV data using blockchain technology. *Journal of Information Security and Applications*, 55, 102670.
12. Xu, W., Zhang, H., Cao, X., Deng, R., Li, H., & Zhang, J. Securing wireless relaying communication for dual unmanned aerial vehicles with unknown eavesdropper. *Information Sciences*, 546, 871-882.
13. Alladi, T., Chamola, V., & Kumar, N. (2020). PARTH: A two-stage lightweight mutual authentication protocol for UAV surveillance networks. *Computer Communications*.
14. Sedjelmaci, H., Boudguiga, A., Jemaa, I. B., & Senouci, S. M. (2019). An efficient cyber defense framework for UAV-Edge computing network. *Ad Hoc Networks*, 94, 101970.
15. Hong, W., Jianhua, L., Chengzhe, L., & Zhe, W. (2020). A provably secure aggregate authentication scheme for unmanned aerial vehicle cluster networks. *Peer-to-Peer Networking and Applications*, 13(1), 53-63.
16. Condomines, J. P., Zhang, R., & Larrieu, N. (2019). Network intrusion detection system for UAV ad-hoc communication: From methodology design to real test validation. *Ad Hoc Networks*, 90, 101759.
17. Mitchell, R., & Chen, R. (2013). Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 44(5), 593-604.
18. Sedjelmaci, H., & Senouci, S. M. (2018). Cyber security methods for aerial vehicle networks: taxonomy, challenges and solution. *The Journal of Supercomputing*, 74(10), 4928-4944.
19. Fotuhi, R. (2020). Securing of Unmanned Aerial Systems (UAS) against security threats using human immune system. *Reliability Engineering & System Safety*, 193, 106675.
20. Zhang, H., He, X., & Dai, H. (2020, July). Secure UAV communication networks via friendly jamming and bandwidth allocation. In *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (pp. 894-899). IEEE.
21. Kuo, Y. T., & Wei, H. Y. (2019, August). Reliable two-hop device-to-device communications for UAVs. In *2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS)* (pp. 1-5). IEEE.
22. Vanitha, N., & Ganapathi, P. (2020). Traffic Analysis of UAV Networks Using

- Enhanced Deep Feed Forward Neural Networks (EDFFNN). In Handbook of Research on Machine and Deep Learning Applications for Cyber Security (pp. 219-244). IGI Global.
23. Zaminkar, M., Sarkohaki, F., & Fotohi, R. (2021). A method based on encryption and node rating for securing the RPL protocol communications in the IoT ecosystem. *International Journal of Communication Systems*, 34(3), e4693.
 24. Zhou, Y., Pan, C., Yeoh, P. L., Wang, K., Elakashlan, M., Vucetic, B., & Li, Y. (2019). Secure communications for UAV-enabled mobile edge computing systems. *IEEE Transactions on Communications*, 68(1), 376-388.
 25. Fotohi, R., Nazemi, E., & Aliee, F. S. (2020). An Agent-Based Self-Protective Method to Secure Communication between UAVs in Unmanned Aerial Vehicle Networks. *Vehicular Communications*, 100267.
 26. Zaminkar, M., & Fotohi, R. (2020). SoS-RPL: Securing Internet of Things Against Sinkhole Attack Using RPL Protocol-Based Node Rating and Ranking Mechanism. *WIRELESS PERSONAL COMMUNICATIONS*.
 27. Li, Y., Zhang, R., Zhang, J., & Yang, L. (2019). Cooperative jamming via spectrum sharing for secure UAV communications. *IEEE Wireless Communications Letters*, 9(3), 326-330.
 28. Jamali, S., & Fotohi, R. (2017). DAWA: Defending against wormhole attack in MANETs by using fuzzy logic and artificial immune system. *the Journal of Supercomputing*, 73(12), 5173-5196.
 29. Li, Y., Zhang, R., Zhang, J., Gao, S., & Yang, L. (2019). Cooperative jamming for secure UAV communications with partial eavesdropper information. *IEEE Access*, 7, 94593-94603.
 30. Li, B., Fei, Z., Zhang, Y., & Guizani, M. (2019). Secure UAV communication networks over 5G. *IEEE Wireless Communications*, 26(5), 114-120.

Figures

Figure 1

Typical UAV communication scenario. Note: The designations employed and the presentation of the material on this map do not imply the expression of any opinion whatsoever on the part of Research Square concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries. This map has been provided by the authors.

Figure 2

Location of immune system cells.

Figure 3

The relationship between the modules with the knowledge base and the UAV network

Pseudo-code 1: Filtering routes
Input: Routes detected by the data collection module Output: Send non-suspicious UAV routes to the sub-module of communication with the decision module
1: Start 2: Send detected routes from data collection module sub-module to filtering sub-module 3: Create a hello packet and send it to single-hop UAVs of source 4: Save the hello packet information in the <i>HMT</i> table and send it to other single-hop UAVs on the route to the destination 5: Hello packet listening 6: Calculate the listening rate $LR(N)$ by each UAV 7: If $LR(N) < (TLR(N))$ is Then 7-1 Send suspicious UAV ID to source UAV Otherwise 7-2 The route is reliable 8: Send routes without suspicious UAVs to the sub-module of communication with the decision module 9: End

Figure 4

Pseudo-code of filtering routes

Figure 5

Defense modules, by duplicating themselves, detect and discover malicious UAVs on suspicious routes.

Pseudo-code 2: Attacker counter phase

Input: The route with the highest value $P_{DR}(r)$ having a suspicious UAV received from the decision module

Output: Distribution of ID of malicious UAVs detected and recording in the knowledge base

1: Start

2: Activate replication sub-module, and the replication of UAVs (lymphocytes) around the suspected UAVs

3: Send TEST packets in the network from the route with suspicious UAVs

4: Compute Pt based on the number of test packet set by defense module

5: If $N_T < Pt$

5-1 The UAV node is malicious, send the malicious UAVs ID to the defense module

5-1-1 Send malicious UAVs ID to all UAVs

5-1-2 Activation of sub-module Reduction and reduction of lymphocytes **Otherwise**

5.2 The route is reliable. Send information to the defense module

5-2-1 Activation of the sub-module Reduction and Reduction of lymphocytes

6: Registration of malicious node ID and all information in the knowledge base by the defense module

7: End

Figure 6

Pseudo-code of attacker counter phase

Pseudo-code 3: Choose a trusted route
<p>1: Initialization</p> <p>2: Variable $P_{DR}(r)$ Rate of 4 criteria for each route</p> <p>3: Variable C Indicates the number of candidate routes between the origin and destination UAVs</p> <p>4: Variable F_r represents the fitness of the route</p> <p>5: Variable $UAV_{trusted}$ represents a reliable route between UAVs</p> <p>6: Reliable route selection procedure:</p> <p>7: Do for routes from: 1 to C.</p> <p>8: Calculate the value of Th for each route.</p> <p>9: If $P_{DR}(r) \leq \text{MAX Th.}$, Then</p> <p>10: Delete the route and send a warning to the defense module.</p> <p>11: Otherwise</p> <p>12: Select routes with average Th (AVG (p_{dr}))</p> <p>13: Calculate variable F_r as follows</p> $F_r (PDR_i, \text{Distance}_i) = \left(\frac{\text{Max APDR}}{\text{APDR}_i} \right) + \left(\frac{\text{Distance}_i}{\text{Max Distance.}} \right)$ <p>14: The route with the following condition is selected:</p> $UAV_{trusted} = \text{AVG} (p_{dr}) \ \& \ \text{MAX} (F_r)$ <p>15: End</p> <p>16: End</p> <p>17: End</p>

Figure 7

Pseudo-code for the selection of reliable route

Figure 8

Flowchart of the proposed SID-UAV method

Figure 9

Self-adaptive steps

(A) $\kappa = 10\%$

(B) $\kappa = 15\%$

(C) $\kappa = 20\%$

Figure 10

APDR with different K

(A) $\kappa = 10\%$

(B) $\kappa = 15\%$

(C) $\kappa = 20\%$

Figure 11

APLR with different K

(A) $\kappa = 10\%$

(B) $\kappa = 15\%$

(C) $\kappa = 20\%$

Figure 12

AFP with different K

(A) $\kappa = 10\%$

(B) $\kappa = 15\%$

(C) $\kappa = 20\%$

Figure 13

AFN with different K

(A) $\kappa = 10\%$

(B) $\kappa = 15\%$

(C) $\kappa = 20\%$

Figure 14

ADR with different K