*Preprints* (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 January 2020 doi:10.20944/preprints202001.0229.v1

# An Agent-Based Self-Protective Method to Secure Communication between UAVs in Unmanned Aerial Vehicle Networks

Reza Fotohi [1,*] Eslam Nazemi [1]

[1] Faculty of Computer Science and Engineering, Shahid Beheshti University, Tehran, Iran

*Corresponding author: Reza Fotohi, R_fotohi@sbu.ac.ir; Fotohi.reza@gmail.com*

**Abstract**

UAVNs (unmanned aerial vehicle networks) may become vulnerable to threats and attacks due to their characteristic features such as high mobility, highly dynamic network topology, and open-air wireless environments. Since previous work has focused on classical and metaheuristic-based approaches, none of these approaches have a self-adaptive approach. In this article, we examine the challenges of cyber detection methods to secure UAVNs and review exiting security schemes proposed in the current literature. Furthermore, we propose an agent-based self-protective method (ASP-UAVN) for UAVNs that is based on the Human Immune System (HIS). In ASP-UAS, the safest route from the source UAV to the destination UAV is chosen according to a self-protective system. In this method, a multi-agent system using an Artificial Immune System (AIS) is employed to detect the attacking UAV and choose the safest route. In the proposed ASP-UAVN, the route request packet (RREQ) is initially transmitted from the source UAV to the destination UAV to detect the existing routes. Then, once the route reply packet (RREP) is received, a self-protective method using agents and the knowledge base is employed to choose the safest route and detect the attacking UAVs. The method is evaluated here via extensive simulations carried out in the NS-3 environment. The experimental results of four scenarios demonstrated that the ASP-UAS increases the Packet Delivery Rate (PDR) by more than 17.4, 20.8, and 25.91%, and detection rate by more than 17.2, 23.1, and 29.3%, and decreases the Packet Loss Rate (PLR) by more than 14.4, 16.8, and 20.21%, the false-positive and false-negative rate by more than 16.5, 25.3, and 31.21% those of SUAS-HIS, SFA and BRUIDS methods, respectively.

**Keywords:** Unmanned aerial vehicle networks (UAVNs), Secure communication, Agent-based self-protective, HIS

## 1 Introduction

An unmanned aerial vehicle (UAV) is, in fact, an aircraft flying with no human pilot on board. Instead, an operator or the on-board computer systems control autonomously its flight either remotely. UAVs are regularly denoted to as drones as well. By developments in computing, device miniaturization and communication, other flying objects including quadcopters, gliders, and balloons could be also included in UAVs. Historically, military operations utilized in missions imposing high-risk levels to human pilots. However, more applications were recently found in civilian domains for UAVs. They involve rescue and search operations, inspection, and policing. Figure 1 represents a

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 January 2020 doi:10.20944/preprints202001.0229.v1

usual setup for communicating within the UAVs. The setup involves multiple components and numerous links to communication. The task of each link is to transmit certain kinds of information and data. Generally, based on the kind of transmitted information, 3 various types of links should exist in these networks, i.e. radio communication, Satellite link, and U2U. The radio communication links transmit telemetry data, control audio, and video information. Furthermore, the task of satellite links is to carry GPS, meteorological, and weather information, along with the data transferred by the radio communication links. one of their applications is to utilize UASs in the networks for ballistic missile defense with the greatest vitality level. 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.

Further discussion is provided in the following sections in this regard to prove the applications of UAVs with innate time sensitivity, and to indicate the insistence of offering security in communication channels [2]. Nevertheless, despite the advantages of UAVs in different applications as a result of the circumstances where the activities are monitored by no pilot, they are potentially susceptible to lethal threats. This strengthens the emergence of designing reliable and secure UASs and overcoming the challenges to prevent destruction and damage to other systems and human lives [3].

Hence, UAVs become a fascinating target of lethal attacks, theft, and manipulation. Some attacks including Sinkhole (SH), Wormhole (WH), and Selective Forwarding (SF) improperly enter the system. When an attack affects the unmanned system, it is difficult to remove the threat and bring the system back online. It is worth to mention that the usual approaches to secure information, like intrusion detection or encryption [4] are insufficient to deal with such risks. For elaborating, the stated outlines do not take into account the actuator and sensor measurements compatibility factor with the control mechanism and physical procedure of the UAV, which are considerable for the protection outline. The malevolent UAV is strong against 3 lethal attacks (SH, WH, and SF) within the ASP-UAVN proposed design, hence, the intrusive operations are rapidly recognized and eliminated from the or top-secret data surveillance spying missions. Within the suggested schema, the critical standards of service quality are improved such as PLR, PDR, detection rates, false-negative, and false-positive rates.

This study is mainly focused as follows:

- Analyzing the UAV network to discover unknown attacks launched by external or internal attackers
- Analyzing the sensitivity and robustness of the UAV autopilot system against lethal security attacks.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 January 2020 doi:10.20944/preprints202001.0229.v1

- Designing an efficient intrusion and self-protective detection system utilizing an AIS for unknown and known attacks in UAV.
- Providing a set of descriptions of the most related routing protocols in the literature accompanied by their disadvantages. Moreover, we performed a comparative investigation for examining the deficiencies between our suggested scheme and the evaluated protocols.
- Validating the proposed protocol by investigating its behavior based on QoS followed by demonstrating its loop freedom feature.
- Performing a set of simulations to investigate the realistic impacts of UAVNs environments over our suggested protocol. The efficiency of ASP-UAVN was demonstrated by the attained results.

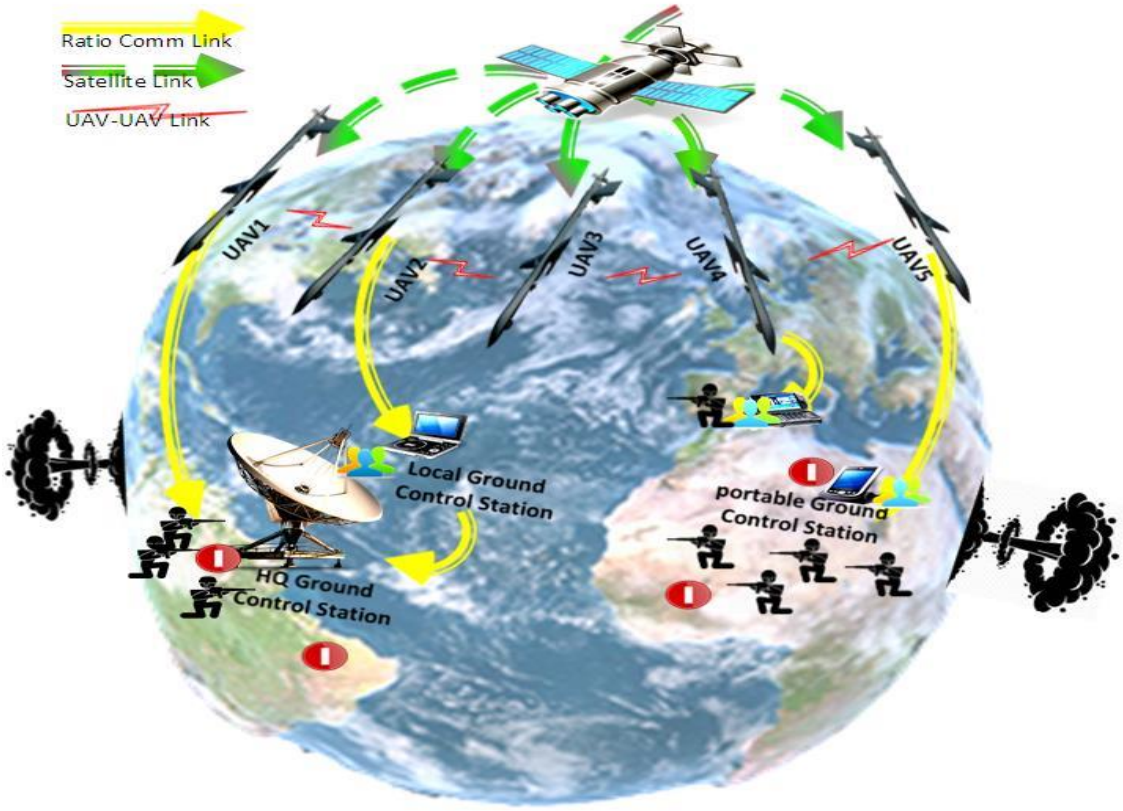


Figure 1: Typical UAV communication scenario.

The paper presented here is organized as the following. Section 2 converses lethal security threats and detection schemes for UAVNs. Section 3 presents the HIS. In Sect. 4 brings the proposed ASP-UAVNs strategy. In Section 5, the simulation results are discussed to demonstrate the efficiency of the proposed ASP-UAVN. Finally, conclusions and future works of this research are discussed in Section 6.

## 2 Lethal security threats and detection schemes

Here, the following issues will be discussed: lethal security threats targeting UAVs, detecting schemes for UAVNs protection.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 January 2020 doi:10.20944/preprints202001.0229.v1

### 2.1 Lethal Security Threats

It was prone that UAVs are function degradation and cyber-security threats as active or passive since they depend on wireless channels for communicating. Figure 2 provides a list of main lethal security targeting UAVs. The following vulnerabilities are concerned with this study:

- *Wormhole Attack:* Or WH attacks are the main attack threatening the UAVs. In WH attacks, data packets are received by a hostile node at a definite location in UAV, and the packets are tunnelled to another hostile node at a distant point to regulate the packets to its adjacent nodes. It is possible to establish this tunnel using multiple techniques including a channel established out of band, a high-powered transmission, or an encapsulated packet. In these approaches, through tunnels, the packet transmitted is received rather directly or with fewer hop counts in comparison to ordinary packets that are conveyed via a multi-hop path. This method establishes an illusion whit two close tunnel endpoints [5]. Hence, the hostile nodes are made as decoys within the destination and source nodes that can accomplish subversions like packet manipulation and droppings.

- *Selective Forwarding Attack*: In this attack, a forged RREP is transmitted by an SF node while receiving an RREQ packet, appealing an unexpired and shorter route, even for missing the destination entry from the routing table. By reaching the created RREP packet the source node, a route is established via this malevolent middle node, to remove all legitimate RREP messages conveyed from destination nodes and another intermediate. Thus, the data traffic is successfully attracted by the BH node to that destination by misleading the source. Then, all the data packets are dropped by the SF node rather than forwarding the incoming messages. By forging a transmission route, the hop count is reset by the BH node to a very low value as well as the number of destination sequence to the quite high value to increment the reception opportunity at the source node. The SF attack can also launch from the source node through making fields-source sequence numbers in hop counts and RREQ packets, leading to harming the directing tables in middle nodes and the destination nodes [6].

- *Sink hole Attack:* One of the main attacks threatening the UAVNs is the attack known as the Sinkhole (SH) attack. In these attacks, a malicious node broadcasts illusive information regarding the routings to impose itself as a route towards specific nodes for the neighbouring nodes and thus, attract data traffic. The objective of this process is to draw all the traffic in the network towards the sinkhole node and as a result, alter the packets of data or silently drop them altogether. Sinkhole attacks can increase the network overhead, increase the consumption of energy and decrease the life time of the network , and ultimately annihilate the network [7].

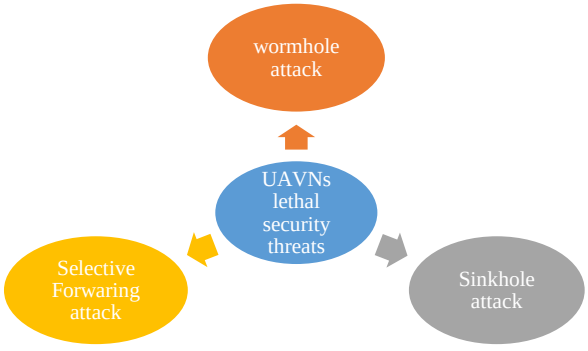


Figure 2: UAVNs lethal security threats

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 January 2020 doi:10.20944/preprints202001.0229.v1

### 2.2 Detection schemes

Through different security measurements in different ways, lethal attacks were addressed and the UAV was protected against these attacks. It is not a new subject, and numerous studies were performed to provide various methods to state these attacks.

In [9], a security framework was proposed by the authors to offer protection against malicious performance targeting SFA communication systems in aircraft. According to the numerical outcomes presented in this work, the suggested security framework leads to prediction and detection rates with high accuracy in comparison with the intrusion detection approaches in the literature.

An adaptive IDS is suggested in [10], in terms of device specifications to find suspicious UAVs in cooperative operations with substantial operation continuity. the UAVs are audited by the suggested IDS system in a distributed system for determining their state whether normally functioning or under malicious attacks. In this study, the efficiency of the suggested rule-based UAV IDS (BRUIDS) performance is investigated on random, reckless, and opportunistic intrusive performances (usual cyber-attack behavioural techniques). The suggested technique is the base for the audition on behavioural rules to quickly investigate a UAV's survivability under malevolent attacks.

An IDS (Intrusion Detection System) was provided in [11], to protect against the security problems through the human immune system (HIS). The IDSs are utilized for detecting and responding to efforts to cooperate with the target system. As the UASs act in the real world, the validation and testing these systems with various sensors are opposed to the problems. This design is stimulated by HIS. In mapping, insecure signals are equal to an antigen detected by antibody-based training designs and eliminated from the operation cycle. The fast detecting of the intrusive signals and quarantining their activity are amongst the key usages of the proposed design.

This study supports using the movement data and each UAV's residual energy level for guaranteeing high-level communication stability while forecasting a sudden link breakage before occurring. Using a strong route detection process, routing paths are explored to take into account the link breakage prediction, the balanced energy consumption, and the connectivity level of the explored pathways [12].

In [13], a data dissemination method is provided by constructing a virtual topology based on the charge of WSN nodes using software-defined networks (SDNs) via UAVs. Constantly, the topology is monitored and reconfigured if necessary. For facilitating simultaneous communication with the ground nodes, the SDN controller and the base station, the aerial nodes are armed with multiple-input multiple-output (MIMO) antennas. Within the proposed method, an efficient sleep timer and back-off counter approaches are used as well. The topology formation and preservation of a sleep timer and a back-off counter are facilitated by the SDN controller.

The problem is intensified by a sporadic network connection disrupting communication in UAVs. Therefore, a drone requires a deep learning-based, adaptive Intrusion Detection System to recognize its intruders and guarantee its safe return-to-home (RTH). In the suggested IDS, using Self-Taught Learning (STL) with a multiclass SVM, the IDS's high true positive rate is maintained, even in unknown territory. The Deep-Q Network is used by the self-healing technique in the IDS recovery phase that is a deep reinforcement learning algorithm for dynamic route learning facilitating the safe return home of the drone. Based on the simulation outcomes, the effectiveness of the proposed IDS is represented [14].

In [15], the UAV (physical layer security of an unmanned aerial vehicle) network is studied, in which the information is transmitted by a UAV-B (UAV base station) confidential to multiple information receivers (IRs) by assisting a UAV jammer (UAVJ) by existing the multiple

 doi:10.20944/preprints202001.0229.v1

eavesdroppers. Here, an optimization problem is formulated to mutually design the trajectories and convey the power of UAV-J and UAV-B for maximizing the minimum average secrecy rate overall IRs. The optimization problem is non-convex with the coupled optimization variables leading to the mathematically inflexible optimization problem. Hence, the optimization problem is decomposed into two subproblems and then solved using the succeeding convex approximation technique and an alternating iterative algorithm.

In [16], two aspects of secure communication and cooperative control are considered. The cooperative control is implemented by a clustering algorithm to increase the speed of converging the multi-UAV formation. Adjusting the flight control factor for accelerating the convergence of multi-UAV, a flock is created by the UAV group. For facilitating secure communication, the hierarchical virtual communication ring (HVCR) strategy is arranged to decrease the boundary of group communication and minimalize the insecure range.

In this paper, a method is proposed to maintain the security in UAV networks within surveillance, by verifying the data regarding events occurring from various sources. Hence, UAV networks are able to adapt peer-to-peer information stimulated by the blockchain principles and to discover the compromised UAVs in terms of trust policies. In the suggested method, secure asymmetric encryption is used with the official UAVs' pre-shared list. This method makes possible to detect the wrong information when hijacking an official UAV physically [17].

In [18], SCOTRES—a trust-oriented system is proposed for secure routing in ad-hoc networks to advance the network entities' intelligence using 5 innovative metrics. The resource consumption of each node is considered by the energy metric to impose similar quantity of collaboration and to increase the network's lifetime. The topology metric knows the positions of the nodes and improves the load balancing. The tolerance in periodic malfunctioning is provided by channel-health metric owing to bad channel circumstances and the network is protected versus jamming attacks. The collaboration of each subject for a particular network operation is evaluated by reputation metric to detect the specific attacks, however, the total compliance is estimated by trust metric, protecting against combinatorial attacks. The system's security features are validated by the Theoretic analysis.

This paper investigates the trajectory design and resource allocating for energy-efficient secure unmanned aerial vehicle (UAV) communication systems in which multiple legitimate ground users are served by a UAV base station while existing a potential eavesdropper. Our objective is to maximize the UAV's energy efficiency while optimization of its user scheduling, transmit power, velocity, and trajectory. The formulation of the design is a nonconvex optimization problem considering the minimum data rate requirement of each user, the maximum tolerable signal-to-noise ratio (SNR) leakage, and the location ambiguity of the eavesdropper. To attain an efficient suboptimal solution, an iterative algorithm is suggested [19].

This paper studies a joint optimization problem of ground terminals (GTs) association under wiretap channels, unmanned aerial vehicle (UAV) flight trajectory, and downlink transmission power. Precisely, a scenario is considered, in which a group of GTs is served by a UAV and the minimum secrecy rate is maximized to guarantee the fairness among GTs. We establish an iterative algorithm in terms of the alternating and successive convex approximation (SCA) approaches for solving the nonconvex optimization problem [20].

Through unmanned aerial vehicles (UAVs), it is possible to support surveillance even in areas with no network infrastructure. By UAV networks, the security challenges are raised as a result of its dynamic topology. In the present study, a method is proposed to maintain the security in UAV networks within the framework of surveillance, by verifying data regarding events from various

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 January 2020 doi:10.20944/preprints202001.0229.v1

sources. Thus, UAV networks are able to adapt peer-to-peer general information stimulated by the blockchain ethics in terms of the trust policies. In this technique, secure asymmetric encryption is used with a pre-shared list of official UAVs. This work states detecting the misinformation when hijacking an official UAV physically [21].

In [22], an innovative trust model is proposed for UAVNs in terms of the mobility and performance pattern of UAV nodes and the features of inter-UAV channels. The suggested trust model includes 4 parts of the indirect trust section, the direct trust section, the trust update section, and the integrated trust section. According to the trust model, the perception of a secure link in UAVNs is formulated existing only a trust link and a physical link between two UAVs. Furthermore, the connectivity of UAVNs is analyzed by adapting the metrics of the secure connectivity probability and physical connectivity probability between two UAVs. Utilizing stochastic geometry with Doppler shift or without it, we originate analytical and accurate expressions of the secure connectivity probability and the physical connectivity probability.

In [23], a security model is suggested in terms of Identity Based (IB) authentication outline for UAV-integrated HetNets. the AVISPA tool is used to screen the absolutism of such a proposed scheme and some of its results indicated that our outline is resistant to the susceptibilities of intruders like replay, and impersonation.

Table 1 highlights a taxonomy of current cyber detection schemes developed to protect the UAV against malicious threats.

Table 1: Comparison between detection schemes for UAV

| References | Attack type | Complexity | Robustness |
|---|---|---|---|
| [9] | Cyber attack | Medium | Medium |
| [10] | Opportunistic attacker | High | High |
| [11] | Cyber security threats | Low | High |
| [12] | Flooding | High | Medium |
| [13] | Hybrid | High | High |
| [14] | Jamming attacks | Low | Low |
| [15] | Physical layer security | Medium | Medium |
| [16] | Hidden terminals | Medium | High |
| [17] | Sybil, Blackhole attack | High | Low |
| [18] | Signature-based | High | High |
| [19] | Physical layer | Low | Low |
| [20] | DoS | Low | Low |
| [21] | Physical-layer security | Medium | High |
| [22] | GPS spooling attack and the Wi-Fi attack | Medium | High |
| [23] | Packet modification attacks | Medium | Medium |

## 3 HIS

HIS as the human's basic protection system supports human beings to survive diseases and environmental threats. Furthermore, by resembling the internet to humans in different ways, it is possible to develop an immune system for the internet in terms of the HIS's fundamentals. Immunity system denotes all bodily mechanisms in charge of protection of the body against detrimental agents in the situation like microorganisms and their products, pollen grains, drugs, and chemicals. The HIS includes three defensive lines operating in cooperation. Mucous, skin, secretions of skin, and membranes are included in the first layer. Phagocytic white blood cells, the

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 January 2020 doi:10.20944/preprints202001.0229.v1

inflammatory responses, and antimicrobial proteins are the subsections for the second layer. Ultimately, the third layer as the specific defensive mechanism involves antibodies and lymphocytes. Antibodies react to aberrant body cells, particular microorganisms, toxins and other materials signed by foreign molecules specifically. Two innate immunity system and acquired immunity system are included in the human immunity system [24]. The lymphoid organs and their main functions are illustrated in Figure 3.

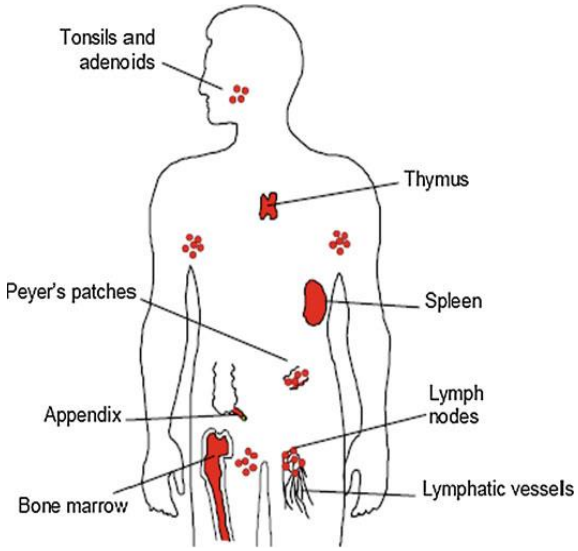


Figure 3: HIS structures [22]

### 3.1 HIS Algorithm

According to the former part, the HIS is a relatively complex mechanism able to protect the body against a tremendous group of irrelevant pathogens. It constructed mechanism of HIS is remarkably effective considerably in self and non-self-antigens distinction. The non-self-antigen is any external factor able to trigger an immune response like an attack or the bacteria. However, self-antigens are on the reverse side of non-self-antigens. The self-antigens are the cells of the living. Clonal selection, affinity, and negative selection are the main theories about HIS algorithms.

*Affinity*: using various models in HIS, the affinity between antigens (attacking) and antibodies (defending) is calculated. 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 $Ab = (Ab1, Ab2, \ldots, Abn)$ and the coordinates of an antigen are represented by $Ag = (Ag1, Ag2, \ldots, Agn)$; the distance between them, $D$, shows the affinity [24], which can be calculated using Eq. (1).

$$\text{Let} \quad R = \{r_0, r_1, \ldots, r_m\} \quad , \quad S = \{s_0, s_1, \ldots, s_m\} \tag{1}$$

$$\text{Manhattan} \quad D = \sum_{i=0}^{m} |r_0 - s_0|$$

$$\text{Hamming} \quad D = \sum_{i=0}^{m} \delta = 1 \text{ if } r_0 \neq s_0, \text{ if otherwise}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 January 2020 doi:10.20944/preprints202001.0229.v1

Euclidean $D=\sqrt{\sum_{i=o}^{m}(r_0-s_0)^2}$

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

- *Clonal Selection Algorithm*: A response is described through the immune system by the clonal selection to an antigen. The antibodies able to identify the antigens multiply are selected over ones that do not. It makes it possible for the detectors to clone their parents via a mutation mechanism with high rates although eliminating the self-reactive antibodies. This is called clonal selection. CLONALG was the algorithm made by De Castro on the basis of the clonal selection [24]. In this algorithm, all counts are considered regarding cloning the best antibodies, taking out non-stimulated antibodies, affinity maturation, and preserving diversity. The clonal selection contains a great strategy for optimizing and pattern recognizing. This contributes to progress in the immune system; hence, it is able to identify the antigens met previously.

- *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 [24].

The pseudo-code for the Negative Selection Algorithm is confirmed in Algorithm 1 [24].

**Algorithm 1:** Pseudo code for Negative Selection Algorithm

```
Procedure Negative Selection Algorithm
Input: A S ⊂ Ui ("self-set"); a set Mo ⊂ Ui ("monitor set"); an integer ni
Output: For each element mo ∈ Mo , either "normal UAV" or "malicious UAV".
    // phase I: Training
        de ← empty set
        while |De| < ni do
            de ← the random detector set
            if de does not match any element of Si then
                insert de into De
            End if
        End while
    // phase II: Classification
            For each mo ∈ mo do
                if mo matches any detector de ∈ De then
                    output " mo is non-self" (an attacker)
                else
                    output " mo is self"
                End if
            End For
End Procedure
```

## 4 The proposed ASP-UAVN approach

We provide a lethal attacks-security threats-immune schema in the following section using the self-protective algorithm. Six sections are included in the ASP-UAVN: in Sect, 4.1. The motion direction of the UAV is discussed. Sect 4.2. deals with the information exchange pattern of UAVNs. In Sect. 4.3 ASP-UAVN network model is discussed. In Sect, 4.4. the evaluation agent (to evaluate the

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 January 2020 doi:10.20944/preprints202001.0229.v1

routes) is discussed. Sect 4.5. deals with the decision-making agent, and in Sect. 4.6 defensive agent in ASP-UAVN is discussed. Table 3 represents the main notations and acronyms utilized in this study.

### 4.1 ASP-UAVN network model

We take into account a UAS network where UAVs are arranged in an infinite 3D Euclidean space based on a homogeneous Poisson Point Process (PPP). A maximum one-hop communication range is included in the UAVs. A UAV is able to convey the data to the considered destination UAV straightly, or through a relay by one or further UAVs. A multi-hop outline is decode-and-forward, where an arriving packet is decoded by the relaying UAV then transmitted to the next hop. Moreover, a safe solution is presented in the ASP-UAVN network model, to protect the UAVs that are operative on two perspectives: First, it contains low false negative and positive rates and high detection accuracy. Second, it quickly discovers and separates attacks. In the suggested technique, the security issues like SF, WH, and SH attacks able to target the UAV are prohibited. Other properties should be added to Table 2 for detecting the attacks with high accurateness.

### 4.2 Information exchange pattern of UAS

The information is exchanged through the typical process. Originally, a message is delivered by a source ground station ($G_{src}$) to a UAV ($U_1$). Then, this UAV passes through a distance ($D_1$) to satisfy and send the message to another UAV ($U_2$). The message is delivered then by this UAV to another UAV ($U_3$) continuing in the same mode until delivering the message by the final UAV ($U_N$)to the ground station in the destination ($G_{DST}$). To minimize the latency in delivering end-to-end packets, each UAV in this procedure is directed to satisfy the next UAV exactly at the selected time.

However, in real environments as a result of the different performances of UAVs owing to changes in environmental uncertainties and engines, they fly at various velocities, hence, it is impracticable to anticipate that all UAVs can follow the same pattern. For example, UAVs with greater speeds may pass longer distances in comparison to others. Furthermore, it is possible to establish a communication line within two UAVs only into the communication range. Hence, it is essential to develop an association between UAVs. By the two UAVs in the communication range, or by their similar connection area, they will be able to exchange the information packets. This process needs a huge deal of time. No data packet exchange is probably happened by a UAV traveling in a connectionless area or outside the connection area.

### 4.3 Motion Direction of the UAV

To offer motion for the UAVs, in this work, the smooth turn (ST) mobility model was employed. ST makes the UAVs contain smoother trajectories such as taking turns with a larger radius or flying in straight trajectories. Thus, ST has a wide usage in analyzing UASs. This model can capture the UAVs' acceleration correlation in both spatial and temporal domains accommodating the analysis and design. Based on [27], a uniform distribution exists for the ST model's stationary node leading to some closed-form connectivity.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 January 2020 doi:10.20944/preprints202001.0229.v1

Table 2: Lethal attacks features

| Cyber security threats | Features |
|---|---|
| Wormhole attack | Data injection rate |
| Selective forwarding attack | Data injection rate |
| Sybil attck | Data injection rate |

The major acronyms and notations used in this paper are provided Table 3.

Table 3: Major acronyms and notations used in this paper.

| Acronyms | Abbreviated acronyms | Notation | Abbreviated notations |
|---|---|---|---|
| *NS* – 3 | Network Simulator 3 | *RREQ* | Route Request |
| *NAM* | Network Animator | *RREP* | Route Reply |
| *IDS* | Intrusion Detection System | $UAV_S$ | Source *UAV* |
| *HIS* | Human Immune System | $UAV_D$ | Destination *UAV* |
| *AIS* | Artificial Immune System | ST | Smooth Turn |
| *ASP* – *UAVNs* | Agent-Based Self-Protective Unmanned Aerial Vehicle Networks | *Th* | Threshold |
| *UAV* | Unmanned Aerial Vehicles | $P_m(r)$ | Probability malicious (route) |
| *GPS* | Global Positioning System | *SSI* | Signal Strength Intensity |
| *WH* | Wormhole | $F_r$ | Fitness route |
| *SF* | Selective Forwarding | $P_{UAV_M}$ | Probability Malicious UAV |
| *SH* | Sinkhole | *MaxRTT* | Maximum RTT |
| *FP* | False positive rate | $SSI_i$ | Signal Strength Intensity i |
| *FN* | False negative rate | *MaxSSI* | Maximum SSI |
| *TP* | True positive rate | *D* | Distance |
| *TN* | True negative rate | *R* | Route |
| *DR* | Detection rate | *AS* | Antigen Self |
| *SFA* | Security Framework Aircraft | *Ab* | Anti-body |
| *DoS* | Denial of Service | UAVNs | Unmanned Aerial Vehicles Networks |
| *Ag* | Anti-gen | PLR | Packet Loss Rate |

**Employing Agents to Detect Attacking UAVs:** In our proposed method, the safest route from the starting point to the destination is chosen according to a self-matching system. In this method, a multi-agent system using an artificial immune system is employed to detect the attacking UAV and choose the safest route. In the proposed ASP-UAVN, the route request packet (RREQ) is initially transmitted from the source UAV to the destination UAV to detect the existing routes. Then, once the route response packet (RREP) is received, a self-protective method using agents and the knowledge base is employed to choose the safest route and detect the attacking UAVs. In ASP-UAVN, three types of agents are considered, including:

- Evaluation agent (to evaluate the routes)
- Decision making agent

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 January 2020 doi:10.20944/preprints202001.0229.v1

- Defensive agent

These agents have modules distributed in different segments of the UAS, and each have a distinct responsibility. All agents are connected to the knowledge base to register the data and utilize the registered information. Figure 4 demonstrates the relationship between the agents and between the agents and the knowledge base. In the proposed method, agents are considered to detect Selective Forwarding attack, Wormhole attack, and Sybil attack.

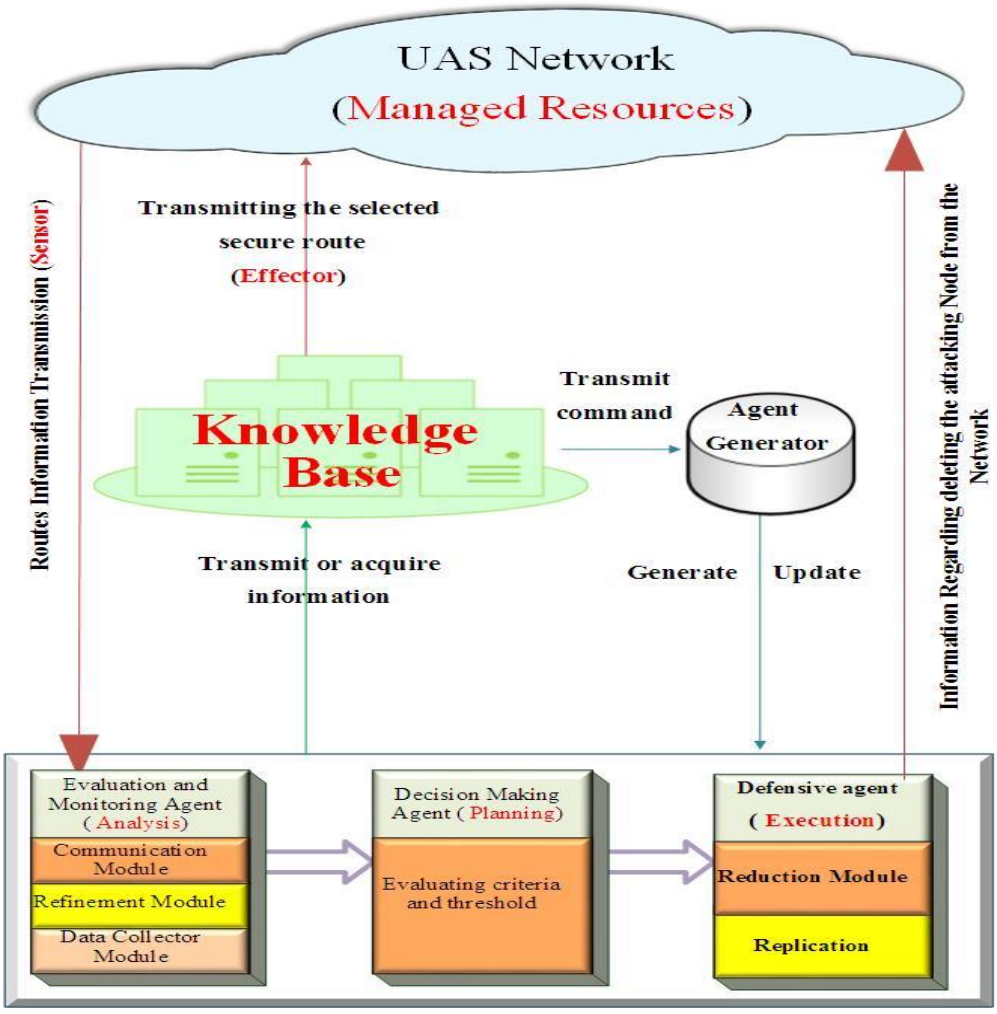


Figure 4: Relationship between agents with the knowledge base and UAV network

### 4.4 The evaluation agent

Antigens are considered as the set of all detected routes from the source UAV to the destination UAV. The considered evaluation agents are similar to the T-cells in the immune system: they are responsible for evaluating abnormal behavior of the existing UAVs in routes and reporting their behavior. These agents have three functional modules as follows:

1. Module for Data Collection
2. Module for Refinement
3. Module for Communication with the Decision-Making Agent

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 January 2020 doi:10.20944/preprints202001.0229.v1

The evaluation agents in ASP-UAVN are agents that evaluate the existing routes to the destinations (i.e. the antigens); so that destructive behavior of the UAVs on each route can be detected.

The routes evaluation agent can be in the form of a table in the source UAV that registers the existing routes to the destination. For instance, the UAV in the source S has three routes to the destination, namely $R_1$, $R_2$, and $R_3$. The route evaluation agent is demonstrated in Table 4.

In this stage, all routes with received RREP are examined in terms of security. For this aim, one "Hello Packet" is transmitted over each route, and the destination UAV is responsible for transmitting a confirmation packet on the routes containing UAVs, following the receiving of the "Hello Packet". It is evident that if a route is contaminated with a destructive UAV, the "Hello Packet" will fail to reach the destination and thus, no confirmation packet will be received in the source. In such cases, the probability for the route to be contaminated increases (i.e. the value for $P_{UAV_M}(r)$ increases for the route r). On the other hand, if the "Hello Packet" reaches the destination, the confirmation packet will be received in the source, indicating that the route does not contain a destructive UAV (i.e. the value for $P_{UAV_M}(r)$ decreases). The procedure for transmitting the "Hello Packet" is repeated 4 times.

**The initial value for $P_{UAV_M}(r)$:** if the route is confirmable according to the attacking UAV detection mechanism, the initial value for $P_{UAV_M}(r)$ will be zero, but if the route cannot be confirmed, $P_{UAV_M}(r)$ is initiated with 100. Next, to update the value for this variable, the source UAV transmits a "Hello Packet" to the destination UAV through all existing routes in its table in 4 iterations. If a confirmation packet is received from the destination UAV, 25 units is decreased from the value of $P_{UAV_M}(r)$. However, if no confirmation is received from the destination UAV, 15 units is added to the value for $P_{UAV_M}(r)$. This stage is repeated 4 times, and the value for $P_{UAV_M}(r)$ is updated for all routes. Finally, if the value for $P_{UAV_M}(r)$ is more than 50 for a route, it is rejected. The rest of the routes are sent to the decision-making agent and the knowledge base.

Table 4: Examining the attacker detection mechanism using the probability variable $P_{UAV_M}(r)$

| Response from the routes | Confirmation that packet is received | Confirmation that packet is not received | $P_{UAV_M}(r)$ |
|---|---|---|---|
| Response for Route 1 | √ | | $P_{UAV_M}(r)$ - 25 |
| Response for Route 2 | | √ | $P_{UAV_M}(r)$ + 15 |

The decision-making agent is capable of synthesizing the information on breaches to reach a precise decision regarding the breach.

### 4.5 The decision-making agent

The decision-making agent is similar to the B-Cells in the AIS, and is capable of making effective decisions regarding the distribution of the attacks. The main objective of the decision-making agent

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 January 2020 doi:10.20944/preprints202001.0229.v1

in the ASP-UAVN is detecting the existence of unfamiliar patterns in a potentially-large set of the existing familiar patterns.

Moreover, when this agent detects a suspicious route, it transmits the information regarding its set to the knowledge base instantly, so that the knowledge base can contact the agent generator to generate new agents to evaluate, make decision, and defend against these unknown attacks.

Making decision on the routes is carried out using 4 criteria, namely Delay, the Ratio for delivering healthy packets from the previous stage (PDRH), Packet Loss Ratio (PLR), and the Frequency of sending packages in each route (FSR), according to the considered attacks. For instance, in some attacks, the destructive UAV deletes all packets, while in some others, the invading UAV deletes only some of the packets.

Therefore, the decision-making agent examines these four criteria based on the information obtained during pre-acquisition and acquisition stages of every route. For suspicious routes, the decision-making agent determines the threshold and transmits a warning to the defensive agent so that it can detect the destructive UAVs. In Table 5, the considered equation for the threshold is in a way that the existence of high delay, high PLR, low ratio for receiving the Hello packet, and high number of repeats (i.e. transferring repeated packets) denotes the existence of a destructive UAV in the route.

Table 5: Decision making agent

| Suspicious routes | Delay | PLR | PDR | FSR |
|---|---|---|---|---|
| $R_1$ | 30ms | 15% | 85% | 24 |
| $R_2$ | 10ms | 25% | 75% | 3 |
| $R_3$ | 20ms | 5% | 95% | 2 |
| Threshold | $Th = \left( \frac{Delay}{MaxDelay} + \frac{PLR}{MaxPLR} + \frac{MaxPDR}{PDR} + \frac{FSR}{MaxFSR} \right)$ (2) | | | |

$P_{DR}(r)$: The value for the threshold (Th) for each route is determined according to the four criteria mentioned, and is registered in $P_{DR}(r)$. The route with the highest threshold is eliminated and is sent to the defensive agent.

### 4.6 Defensive agent

Defensive agents act similar to the antibodies exuded by the lymphocyte. Their functional modules include replication and reduction modules. Defensive agents can evaluate the existing UAVs in the defective route to perform proper actions according to the information provided by the decision-making agent. According to the procedure, when an attacker UAV is detected, the neighboring UAVs are requested not to resend the packets they received from the attacker UAVs.

To detect the attacker in the designated route, the agents replicate themselves in the vicinity of each node and send some Test packets over the route in consecutive periods. A test packet is a packet similar to the normal packets in the UAS network. Therefore, the attacking UAV receives and tries to delete it. The defensive agent detects the destructive UAV in a suspicious route using the following Eq. (3):

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 January 2020 doi:10.20944/preprints202001.0229.v1

$$\begin{cases} M_1 = X_1 & For\ t = 1 \\ M_t = \alpha * X_t + (1-\alpha) * M_{t-1} & For\ t > 1 \end{cases} \quad (3)$$

Where $\alpha$ is the regulation factor coefficient with a constant value between 0 and 1, $X_t$ is the value for the test packet in a time interval $t$, and $M_t$ is the mean transmission value for the test packets in every time interval $t$.

In every interval, a predetermined number of test packets are transmitted in the designated route. Then, for each UAV, the defensive agent determines the number of the test packets transmitted by that specific UAV. If the total number of the test packets transmitted by a UAV is fewer or equal to the value for $M_t$, it demonstrates that this UAV is a destructive UAV that removes a number of the packets. The value for the coefficient $\alpha$ is considered a constant value between 0 and 1. Considering lesser value for this coefficient indicates higher expected probability for the loss of packets. On the other hand, if the value for $\alpha$ is considered closer to 1, it indicates that we expect fewer packets to be lost.

Using this method, the defensive agents can successfully isolate the attacking UAVs, as illustrated in Figure 2. To remove the breaches, the defensive agents replicate themselves and barricade further replication of the attacker after a certain time interval by removing the attackers.


Figure 5: Defensive agents replicate themselves to evaluate and detect the destructive UAVs in suspicious routes.

When the defensive agent detects a destructive UAV, it will ask all the UAVs in the route to disregard and delete any packets received from this UAV. In addition, it sends a message regarding

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 January 2020 doi:10.20944/preprints202001.0229.v1

detection of the destructive UAV to the knowledge base, so that the destructive UAV is no longer employed for route finding.

**The Knowledge Base Layer:** The knowledge base is in connection with all agents, and they needed to be intelligently evolved to defend against a wide range of attacks. The knowledge base includes the following stages to choose the most secure route (based on the information received from the agents) for transmission of data in the immune memory:

**Affinity:** as defined in the immune system of the human body, the main objective of B-Cells is creating antibodies against antigens, and ultimately evolving into memory cells once they are activated by antigen interactions. The memory cells generate more antibodies in shorter time during further impacts with the same antigen. In our proposed method, to choose the best B-cell and to perform affinity, routes with low latency, low ratio for loss of packets, high ratio for receiving packets, and low packet re-transmission number are chosen. In other words, at this stage, routes with low threshold value are chosen.

**Matching:** in this stage, routes with low threshold are compared and evaluated using the following two attributes to choose the safest route. In addition, the most significant attribute of the attacker-detection mechanism is its capability to be corrected over time. In other words, they need to be correctable and have the capacity for easy learning.

The details for the first and second attribute of matching: the details are described in the following two attributes:

**Attribute 1, round trip time between the source UAV and the destination UAV:** the knowledge base calculates the round-trip time for all the received routes from the source UAV to the destination UAV based on the acquired information.

**Attribute 2, the signal strength index of the received signal:** the invader generates a high strength signal (the SSI that a destructive UAV has generated) to gain control over the UAV. The procedure for detection is that the knowledge base initially collects all the generated SSIs from the transmitters. It then compares these values with the value for a normal SSI (i.e. SSI generated by a normal UAV). In this manner, suspicious generated signal strengths and normal ones are distinguished.

**Finalizing the Detection Set:** for all the routes with low threshold (Th) value, the safest route is selected according to the Algorithm 1 demonstrated in Figure 6:

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 January 2020 doi:10.20944/preprints202001.0229.v1

**Algorithm 1:** Pseudo code for ASP-UAVN approach

**Initialize** the Antigen collection time to 15s;
**Initialize** the Antigen towards min to 80s;
**Initialize** the Delay buffer size max to 1400;
**Initialize** the Storing time to 10s;
**Initialize** the Max number of antigens to 1000;
**Let** $P_{DR}(r)$ as the probability for destructiveness of the route
**Let** $N$ represents the number of candidate routes between the source UAV and the destination UAV
**Let** $F_r$ represents the fitness route
**Let** $UAV_{PR}$ represents a secure and reliable route between UAVs
***Procedure*** Selecting a safe and reliable route
    *For* $r = 1$ *To* $N$ *Do*
        Calculate the value for $Th$ in every route
        *IF* $Max_{(Th)}(r) < P_m(r)$ **Then**
            Remove the route and send a warning to the defensive agent
        **Else**
            Select routes with the lowest $Th$ value $Min(Th)$
            Calculate the value for $F_r$ according to this equation:
            $$F_r(RTT_i, SSI_i) = \left(\frac{MaxRTT}{RTT_i}\right) + \left(\frac{SSI_i}{MaxSSI}\right)$$
            The route with the following criteria is selected:
            $$UAV_{PR} = Min(Th) \,\&\, Max(F_r)$$
        *EndIf*
    *EndFor*
***End Procedure***

Figure 6: The algorithm for selecting a secure and reliable route

According to Algorithm 1, once the threshold value ($Th$) for each route was determined and the destructive routes were refined, the routes with low Th value are once again compared according to the function $F_r$ for the fitness route, and the route with the highest $F_r$ is selected as the safest route.

**Hyper-mutation:** among the evaluated routes, those with approximately similar conditions (i.e. minimum threshold level and maximum evaluation function) are transferred into the hyper-mutation stage. At this stage, the routes are evaluated with another criterion (i.e. in a similar condition, the route with the highest PDR is selected), so that the safest route for the UAVs is selected.

**Registration in the Security Memory:** the routes that meet the conditions of the equation $UAV_{RR}$, or those that have the highest PDR value following the hyper-mutation stage, are the safest routes. Therefore, they will be registered in the security memory for further use.

The flowchart for the proposed ASP-UAVN is demonstrated in Figure 7.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 January 2020 doi:10.20944/preprints202001.0229.v1

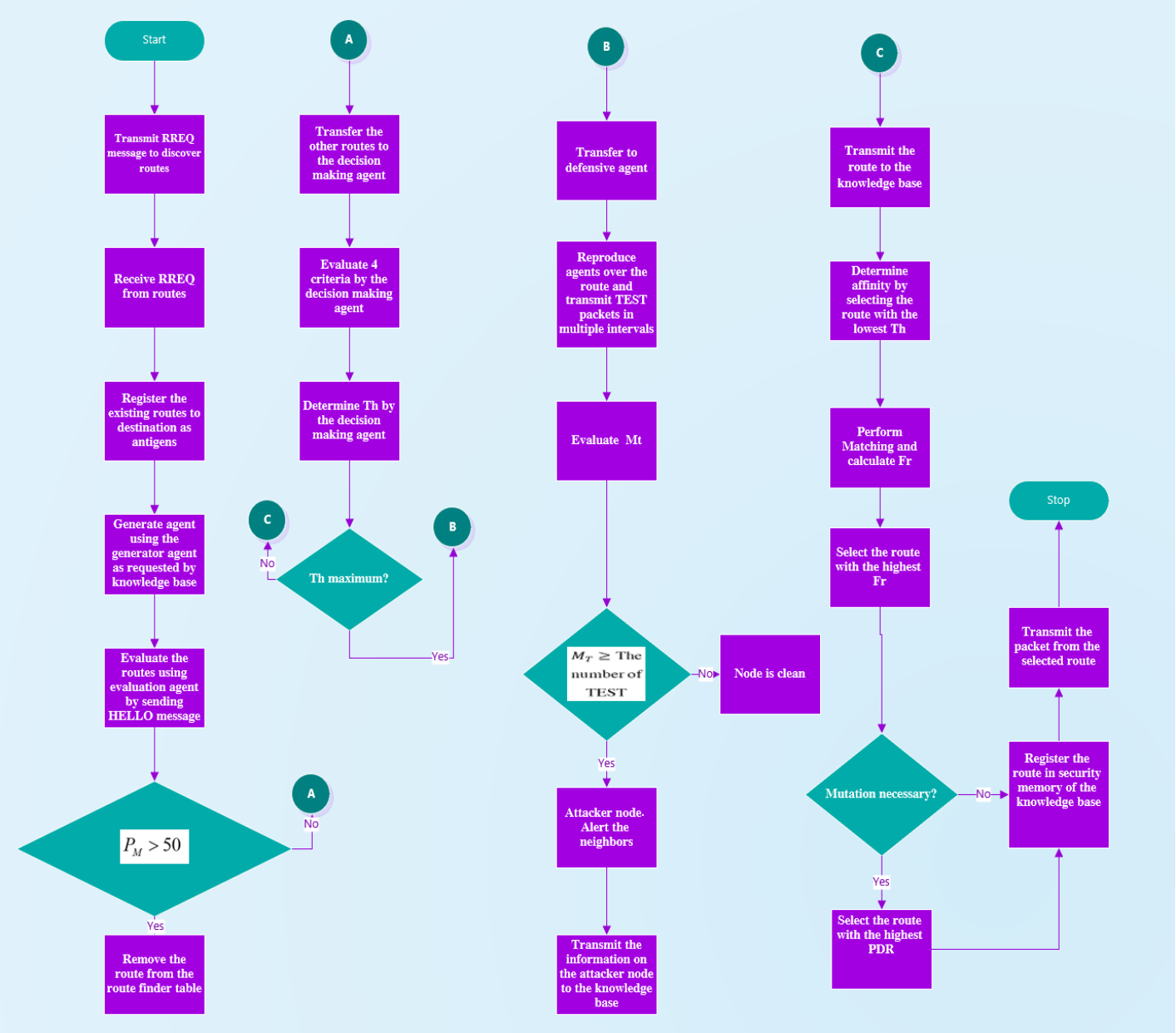


Figure 7: Flowchart of the ASP-UAVN

**Analyzing the characteristics of ASP-UAVN**: There are numerous advantageous characteristics in the proposed ASP-UAVN by employing artificial immune system and multi-agent intelligent technology. In the following, a number of these characteristics are discussed.

**Distributivity:** As our considered agents are distributed in all UAVs similar to the distribution of lymphocytes in the body, and since the knowledge base is updated periodically or when the UAV is under attack, the three considered agents are logically independent, with intermediaries to enable communication. The evaluation agents are capable of controlling the performance of the UAVs on the route via transmitting HELLO messages. Moreover, the decision-making agents analyze the performance of the UAVs over the route based on the considered criteria to detect destructive routes. Furthermore, defensive agents can detect attackers independently and remove them from the network.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 January 2020 doi:10.20944/preprints202001.0229.v1

**Independence:** Similar to the body immune system that does not require external administration and maintenance for classification and elimination of the pathogenic agents, the knowledge base and the agents can evaluate, make decision, and defend against the attacker UAVs in the three considered attacks cooperatively (with the cooperation of other UAVs) or independently. In ASP-UAVN, the knowledge base and the agents can be updated or reproduced independently.

**Self-protection:** Similar to the body immune system that is capable of learning to defend against new pathogens and detecting the known pathogenic agents through the use of immune memory, the proposed ASP-UAVN is capable of detecting these attacks via a cooperation between the considered agents and the use of the knowledge base.

The proposed ASP-UAVN is a self-matching method that all the stages of self-matching, as illustrated in Figure 5, are applied to it according to the following steps:

**Administered Source:** the source in this project is the UAS network.

**Sensor:** Collecting UAV information via transmitting RREQ and receiving RREP in the UAS network.

**Evaluation:** This component collects the UAV information by employing the received RREPs. This activity is carried out using the data collection module in the evaluation agent.

**Analysis:** This component receives the information between the UAVs from the evaluation component. It then analyzes the acquired information to determine the desired routes. Using refinement and communication modules from the evaluation agent, this stage carries out its responsibility by refining the detected routes and discarding a number of them, followed by transmitting the desired routes to the decision-making agent.

**Planning:** this component makes decision regarding the safest routes. The planning for this component in the proposed ASP-UAVN is performed according to the decision-making agent by evaluating the four considered criteria and determining the value for the threshold (Th).

**Execution:** This component provides mechanisms for the network to perform planning. In the proposed ASP-UAVN, execution is performed in two stages, namely defensive agent (to delete the destructive UAVs), and knowledge base (to select the safest route via affinity and matching).

**Knowledge:** The common knowledge in the self-matching structure is the knowledge base employed according to the Figure 1 in the proposed method.

**Effector:** This component is employed to apply the final decision to the environment. In the proposed method, it is carried out via transmitting the selected safe route to the UAS by the knowledge base.

The proposed ASP-UAVN is effective and efficient in defense against Selective Forwarding, Wormhole, and Sybil attacks. ASP-UAVN is capable of effectively detecting these attacks in cooperation with the agents. In addition, in normal conditions, only a limited number of agents exist in the UAV. However, agents can reproduce and increase swiftly when needed, and decrease once the attacker is detected. In addition, the following two methods are considered in the proposed method to keep the knowledge base up to date:

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 January 2020 doi:10.20944/preprints202001.0229.v1

- Periodic polling from all agents regarding the collection of abnormal behaviors of the network and operational performance of the agents.
- Active registration of information in the knowledge base by the agents if necessary (e.g. when an unknown attack occurs in large scale).

# 5 Evaluating the Performance

The ASP-UAVN performance is assessed in the following section to avoid the lethal attacks.

## 5.1 Performance metrics

Here, the performance and effectiveness of our suggested ASP-UAVN method are systematically assessed with complete simulations. A comparison is performed between the results and with SFA, BRUIDS, and SUAS methods proposed in [9], [10] and [11], respectively. The PDR, PLR, false negative, false positive, and detection ratio are assessed. The meaning of notations used in the equations are given in Table 6.

**Table 6** The parameters specified for *PDR and PLR*

| Notations | Means |
|---|---|
| $X_i$ | Number of packets received by node i |
| $Y_i$ | Number of packets sent by node i |
| n | Experiments |

### *5.1.1 PDR*

As defined, *PDR* results from dividing the total received packets of data at the destination UAV, to the total transmitted packets of data by the source UAV, denoted in percentage [25-28]. Eq. (4) demonstrates the average obtained PDR for $n$ experiments.

$$PDR = \left(\frac{1}{n}\right) * \left(\frac{\sum_{i=1}^{n} X_i}{\sum_{i=1}^{n} Y_i}\right) * 100 \tag{4}$$

### *5.1.2 PLR*

It is calculated by the total number of packets dropped divided by the total number of packets sent by the source *100%. The average PLR for $n$ experiments is obtained by the following equation. The PLR is calculated using Eq. (5) as follows:

$$PLR = \left(\frac{1}{n}\right) * \left(\frac{\sum_{i=1}^{n} Y_i - \sum_{i=1}^{n} X_i}{\sum_{i=1}^{n} Y_i}\right) * 100 \tag{5}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 January 2020 doi:10.20944/preprints202001.0229.v1

*5.1.3 FP*

The FP is calculated by the total number of nodes wrongly detected as the malicious nodes divided by the total number of normal nodes [29,30]. Therefore, the is defined as illustrated in Eq. (6).

$$FP = \left( \frac{FP}{FP + TN} \right) * 100 \qquad \text{Where:} \qquad TN = \left( \frac{TN}{TN + FP} \right) * 100 \tag{6}$$

*5.1.4 FN*

The rate of the malicious node to total normal nodes that were mistakenly marked as a normal node [31]. Eq. (7) demonstrates the calculation.

$$FN = \left( \frac{TP + TN}{All} \right) * 100 \qquad \text{Where:} \qquad TP = \left( \frac{TP}{TP + FN} \right) * 100 \tag{7}$$

*5.1.5 DR*

It is determined as the ratio of the number of lethal attack nodes marked to the total number of existing lethal attack nodes in the IoT. DR is calculated by Eq. (8). Table 7 lists the parameters used for DR [32].

$$DR = \left( \frac{TP}{TP + FN} \right) * 100 \qquad \text{where} \qquad All = TP + TN + FP + FN \tag{8}$$

**Table 7** The parameters specified for *DR*

| Parameters | Description |
|---|---|
| TP | The *TP* is obtained from the whole number of marked lethal attack nodes divided by the whole number of the lethal attack nodes. |
| FP | The *FP* is obtained by the total number of nodes improperly recognized as the lethal attack nodes divided by the whole number of normal nodes. |
| TN | The rate of the lethal attack nodes being properly marked as a lethal attack node. |
| *FN* | The rate of the lethal attack node to whole normal nodes being wrongly marked as a normal node. |

**5.2 Simulation setup and comparing algorithms**

Because of the difficulty in debugging and implementing UAVNs in real networks, it is necessary to view simulations as a basic design tool. The primary benefit of simulation is that analysis is simplified and protocol is verified, mostly, it is evident in systems in large scales [33-35]. The performance of the suggested method is assessed in this part by the use of NS-3 as the simulation means, and the discussion on the obtained results is presented. It should be noted that it is assumed that all ASP-UAVN, SFA, BRUIDS, and SUAS settings and parameters are equal.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 January 2020 doi:10.20944/preprints202001.0229.v1

### 5.3 Simulation results and Analysis

In this section, we analyze the security performance of ASP-UAVN under the four attack scenarios (described in Table 8). This attack is categorized into lethal attacks. There are 500 UAV nodes uniformly deployed in the network area initially. Some important parameters are listed in Table 8.

Table 8: Setting of simulation parameters.

| Parameters | Value |
|---|---|
| Channel type | Channel/Wireless channel |
| MAC Layer | MAC/802.11. b |
| Traffic type | CBR |
| UAV speed | 180 m/s |
| Transmission layer | UDP |
| Packet size | 512 Byte |
| Malicious UAV | 5%, 10%, 15% |
| Type of attacks | WH, SF, SH |
| Transmission range | 30 M |
| Selection of target UAV | Random |

The main simulation settings for four scenarios are summarized in Table 9.

**Table 9** The setting of simulation parameters for four scenarios.

| **Scenario #1** | | **Scenario #2** | |
|---|---|---|---|
| Number of Antibody | 200 | Number of Antibody | 200 |
| Malicious UAV rate | 5% | Malicious UAV rate | 10% |
| Coverage area (m x m) | 1000 x 1000 | Coverage area (m x m) | 2000 x 2000 |
| Simulation time | 1000 | Simulation time | 1500 |
| **Scenario #3** | | **Scenario #4** | |
| Number of Antibody | 200 | Number of Antibody | 50, 100, 150, 200, 250, 300,350 |
| Malicious UAV rate | 15% | Malicious UAV rate | 20% |
| Coverage area (m x m) | 3000 x 3000 | Coverage area (m x m) | 4000 x 4000 |
| Simulation time | 2000 | Simulation time | 2500 |

Table 10-14 compares the performance of ASP-UAVN with that of SFA, BRUIDS, and SUAS in terms of $PDR$, $PLR$, $FP$, $FN$, and $DR$.

Table 10: *PDR* (in %) vs number of antibodies.

| PDR (%) | | | | |
|---|---|---|---|---|
| Number of Antibody | BRUIDS | SFA | SUAS-HIS | ASP-UAVN |
| 50 | 37 | 38 | 57 | 82 |
| 100 | 38 | 40 | 61 | 83 |
| 150 | 40 | 42 | 65 | 84 |
| 200 | 44 | 46 | 59 | 87 |
| 250 | 42 | 48 | 56 | 88 |
| 300 | 40 | 51 | 64 | 90 |
| 350 | 46 | 55 | 70 | 91 |

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 January 2020 doi:10.20944/preprints202001.0229.v1

Table 11: *PLR* (in %) vs number of antibodies.

| PLR (%) | | | | |
|---|---|---|---|---|
| Number of Antibody | BRUIDS | SFA | SUAS-HIS | ASP-UAVN |
| 50 | 60 | 58 | 41 | 16 |
| 100 | 57 | 53 | 38 | 14 |
| 150 | 55 | 48 | 37 | 13 |
| 200 | 50 | 43 | 35 | 11 |
| 250 | 48 | 40 | 34 | 10 |
| 300 | 45 | 39 | 32 | 9 |
| 350 | 41 | 36 | 30 | 8.5 |

Table 12: *FP* (in %) vs number of antibodies.

| FPR (%) | | | | |
|---|---|---|---|---|
| Number of Antibody | BRUIDS | SFA | SUAS-HIS | ASP-UAVN |
| 50 | 0.083 | 0.069 | 0.059 | 0.037 |
| 100 | 0.078 | 0.061 | 0.057 | 0.032 |
| 150 | 0.064 | 0.052 | 0.048 | 0.03 |
| 200 | 0.059 | 0.052 | 0.042 | 0.028 |
| 250 | 0.045 | 0.032 | 0.029 | 0.024 |
| 300 | 0.038 | 0.03 | 0.025 | 0.02 |
| 350 | 0.021 | 0.026 | 0.018 | 0.019 |

Table 13: *FN* (in %) vs number of antibodies.

| FNR (%) | | | | |
|---|---|---|---|---|
| Number of Antibody | BRUIDS | SFA | SUAS-HIS | ASP-UAVN |
| 50 | 0.119 | 0.08 | 0.07 | 0.065 |
| 100 | 0.102 | 0.077 | 0.067 | 0.0495 |
| 150 | 0.1 | 0.071 | 0.061 | 0.055 |
| 200 | 0.09 | 0.065 | 0.055 | 0.0485 |
| 250 | 0.08 | 0.06 | 0.06 | 0.0465 |
| 300 | 0.06 | 0.044 | 0.054 | 0.0425 |
| 350 | 0.06 | 0.049 | 0.052 | 0.0385 |

Table 14: *DR* (in %) vs number of antibodies.

| DR (%) | | | | |
|---|---|---|---|---|
| Number of Antibody | BRUIDS | SFA | SUAS-HIS | ASP-UAVN |
| 50 | 71 | 68 | 75 | 81 |
| 100 | 72 | 71 | 76 | 82 |
| 150 | 73 | 74 | 77 | 84 |
| 200 | 74 | 76 | 78 | 88 |
| 250 | 75 | 77 | 79 | 90 |
| 300 | 76 | 78 | 80 | 91 |
| 350 | 77 | 79 | 81 | 92 |

*Preprints* (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 January 2020 doi:10.20944/preprints202001.0229.v1

**PDR:** Comparing the ASP-UAVN suggested method, SUAS-HIS, SFA, and BRUIDS models based on PDR in lethal attacks is represented in Figure 8 ((a) Number of UAVs (5% malicious), (b) Number of UAVs (10% malicious), (c) Number of UAVs (15% malicious), and (d) Number of Antibody in 30% malicious; respectively). We found that ASP-UAVN outperforms SUAS-HIS, SFA, and BRUIDS in terms of PDR since they have the capability to accurately prevent lethal execution and false information lethal attacks. In the worst case, i.e., when the number of attackers is equal to 20%, the PDR of SUAS-HIS, SFA, and BRUIDS when lethal and false information injection attacks occur is approximately equal, respectively, to 90, 40, 50, and 45%, as shown in Fig. 8. Hence, the excellent performance of the ASP-UAVN framework is achieved due to an efficient collaboration between the decision-making agent and the defensive agent. These modules model the current misbehavior of an intrusion and use a rule-based specification detection to detect the intrusion that executes an attack.

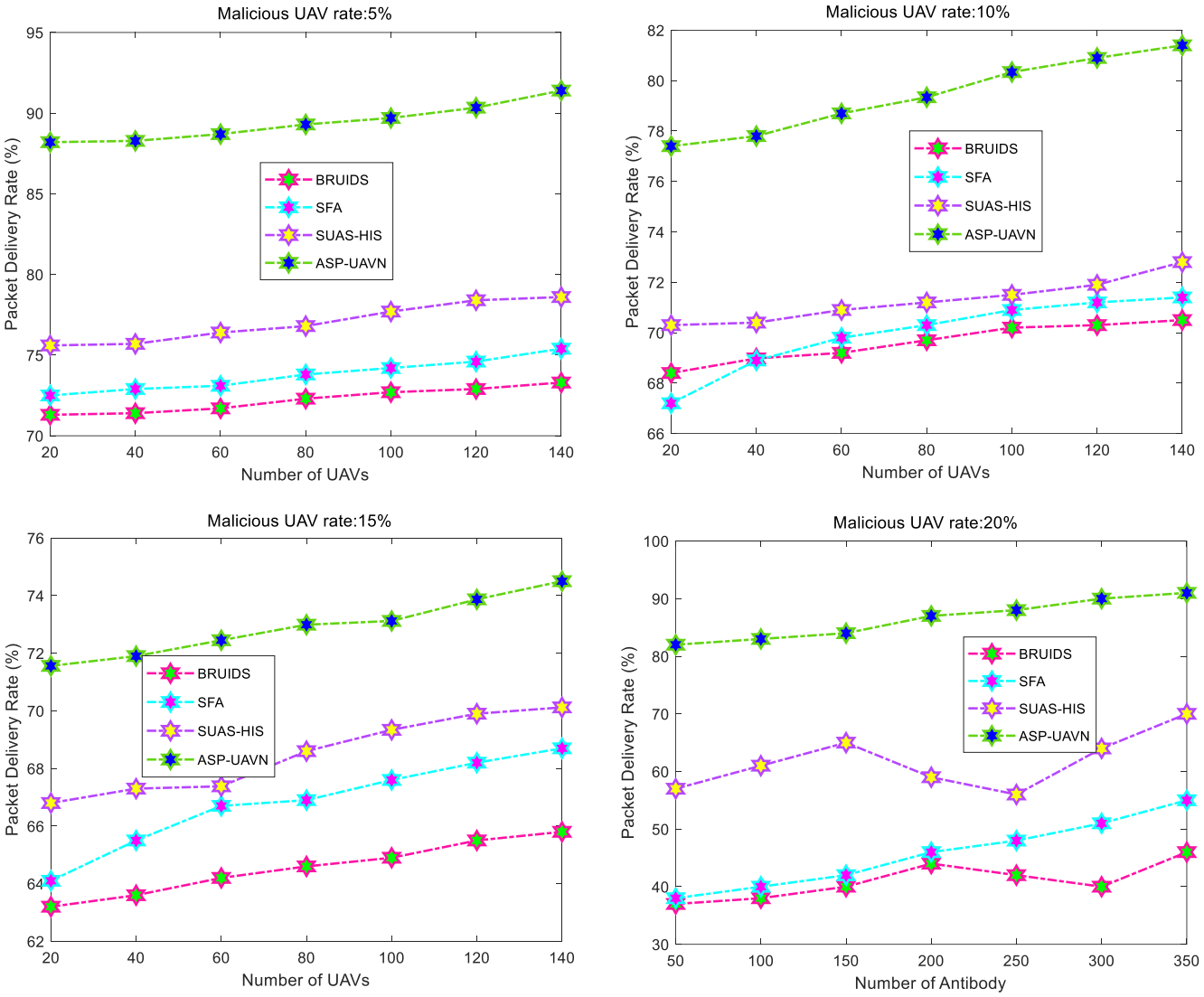


**Fig. 8** Comparison of the ASP-UAVN, SUAS-HIS, SFA and BRUIDS models in term of PDR.

*Preprints* (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 January 2020 doi:10.20944/preprints202001.0229.v1

**PLR:** Figure 9 compares the performance of ASP-UAVN with that of SUAS-HIS, SFA, and BRUIDS for detection of the lethal attacks. As shown in the figure, ASP-UAVN decreases the packet loss rate by more than 10.45, 17.54% and 27.05% those of SUAS-HIS, SFA, and BRUIDS, respectively.

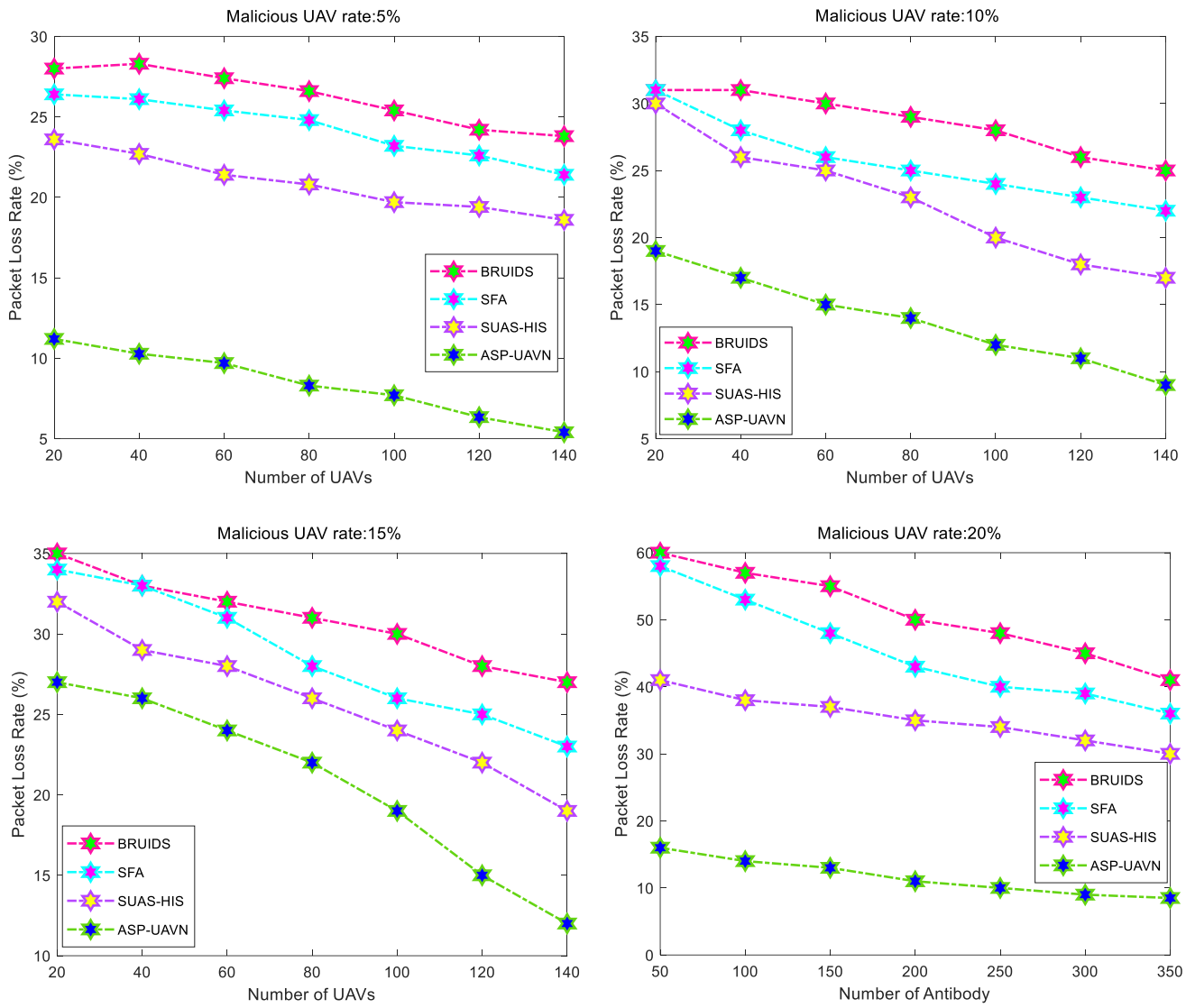


**Fig. 9** Comparison of the ASP-UAVN, SUAS-HIS, SFA and BRUIDS models in term of PLR.

**FP:** Figure 10 presents the false positive rate in four scenarios against normal UAV counts and malicious UAV rates for ASP-UAVN, SUAS-HIS, SFA, and BRUIDS in lethal conditions. As shown in the diagrams, when the number of normal UAVs increases from 20 to 140 and the malicious UAV rate increases from 5 to 20 percent, the generated false positive rate of the proposed method has shown slower and lower growth than other methods. The false positive rate of the proposed method is less than 3 percent when the number of normal UAVs and malicious UAV rate are 120 and 5 percent respectively. However, this value is 17 percent for the SUAS-HIS method, 25 percent for the SFA method, and 35 percent for the BRUIDS method. The reason for the superiority of the proposed scheme is the fast recognition of malicious UAVs and eliminating them with the

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 January 2020 doi:10.20944/preprints202001.0229.v1

cooperation of ground stations and normal UAVs using a self-protective method based on AIS. The aforementioned process is carried out using pre-trained rules saved in safety memory.

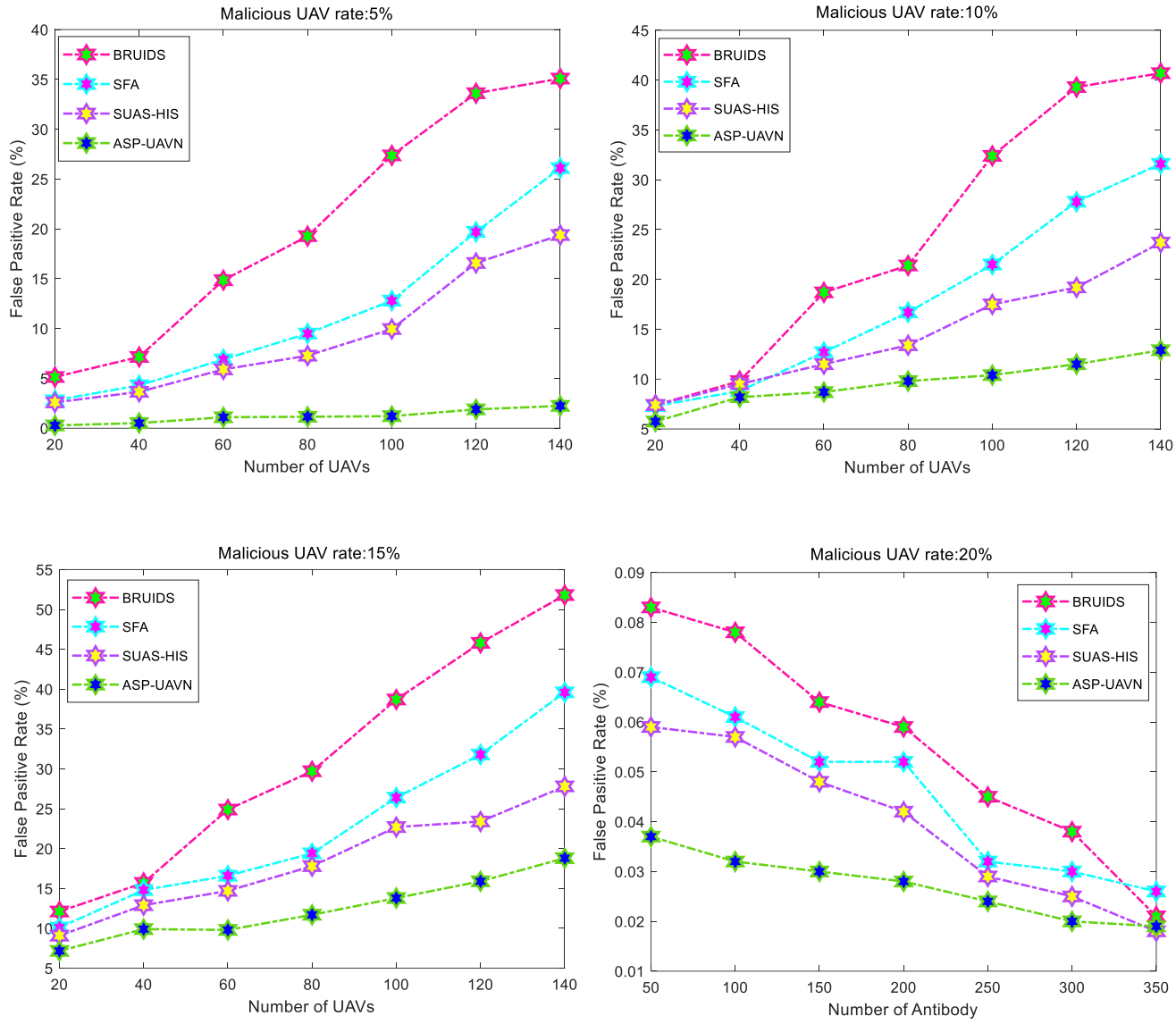


**Fig. 10** Comparison of the ASP-UAVN, SUAS-HIS, SFA and BRUIDS models in term of FPR.

**FN:** As shown in the diagrams, the false negative rate (FN) has shown little growth while this value is much higher for ASP-UAVN, SUAS-HIS, SFA, and BRUIDS. In Figure 11, the false negative rate of the proposed method is less than 1.5 percent when the number of UAVs is 120 but for the other three methods, it is 12 percent, 15 percent, and 18 percent respectively. Also, in figure 11, when the number of antibodies is 350, FN is 0.04 in the proposed scheme. However, this value for the other three methods is 0.05, 0.06, and 0.07 respectively. The reason for the FN of the proposed method being low is the utilization of three evaluation, decision-making, and defensive agents that quickly detect malicious UAVs and remove them from the packet transmission operation among UAVs.

*Preprints* (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 January 2020 doi:10.20944/preprints202001.0229.v1

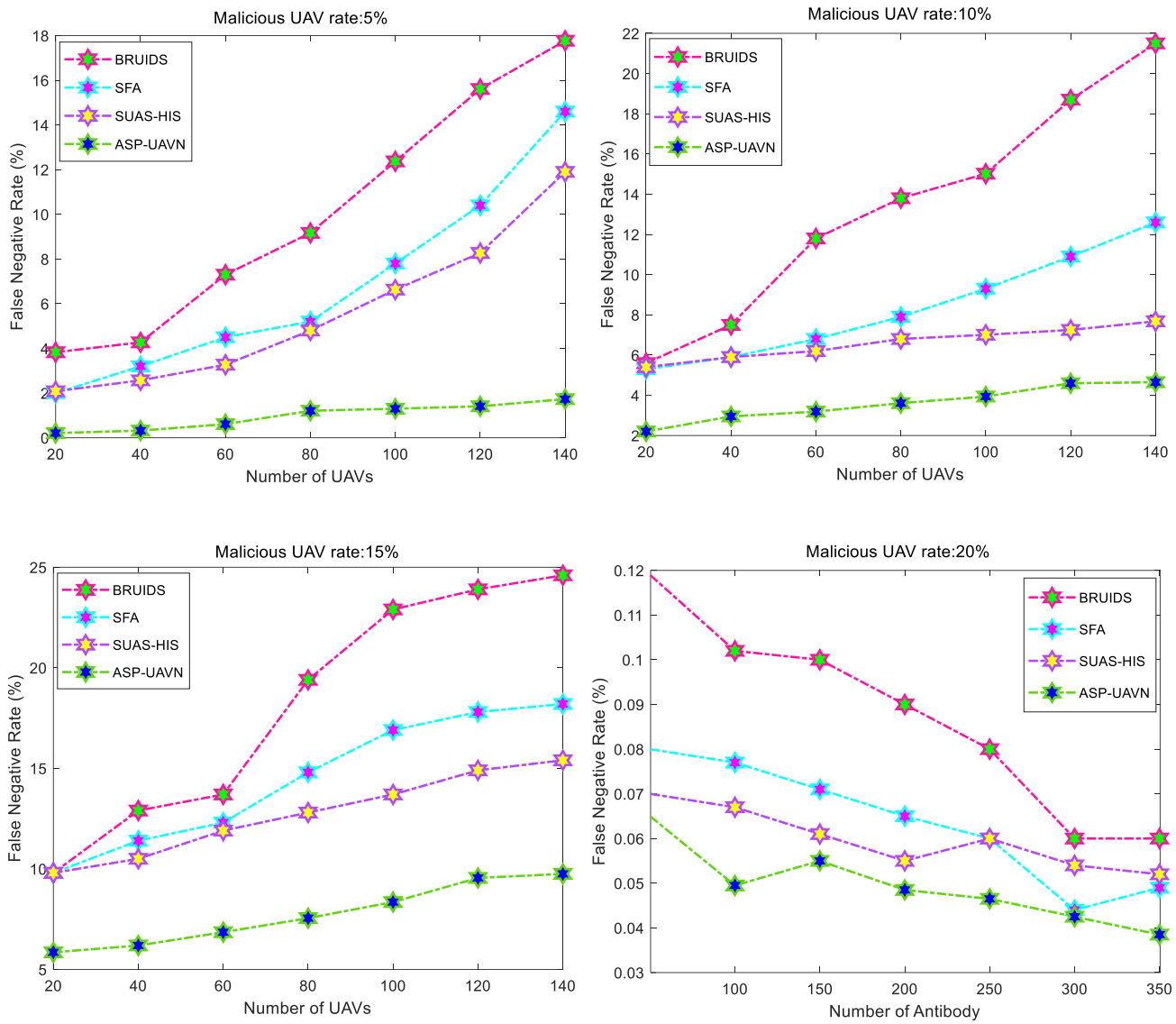


**Fig. 11** Comparison of the ASP-UAVN, SUAS-HIS, SFA and BRUIDS models in term of FNR.

**DR:** As shown in the diagrams, detection rate (DR) has decreased in all four methods according to the four scenarios, especially when the number of attackers is high. This decrease is much more for BRUIDS compared to other mechanisms. The proposed scheme can detect all the aforementioned attacks with a detection rate higher than 95 percent. This result is achieved when the number of normal UAVs and the malicious UAV rate are 120 and 5 percent respectively. The reason for the superiority of the proposed scheme is the fast identification of malicious UAVs and their elimination using the mapping performed in this scheme. This mapping is carried out between insecure routes defined as anti-genes and the pattern trained based on antibodies. This results in the identification of malicious UAVs and their elimination from the operation cycle.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 January 2020 doi:10.20944/preprints202001.0229.v1

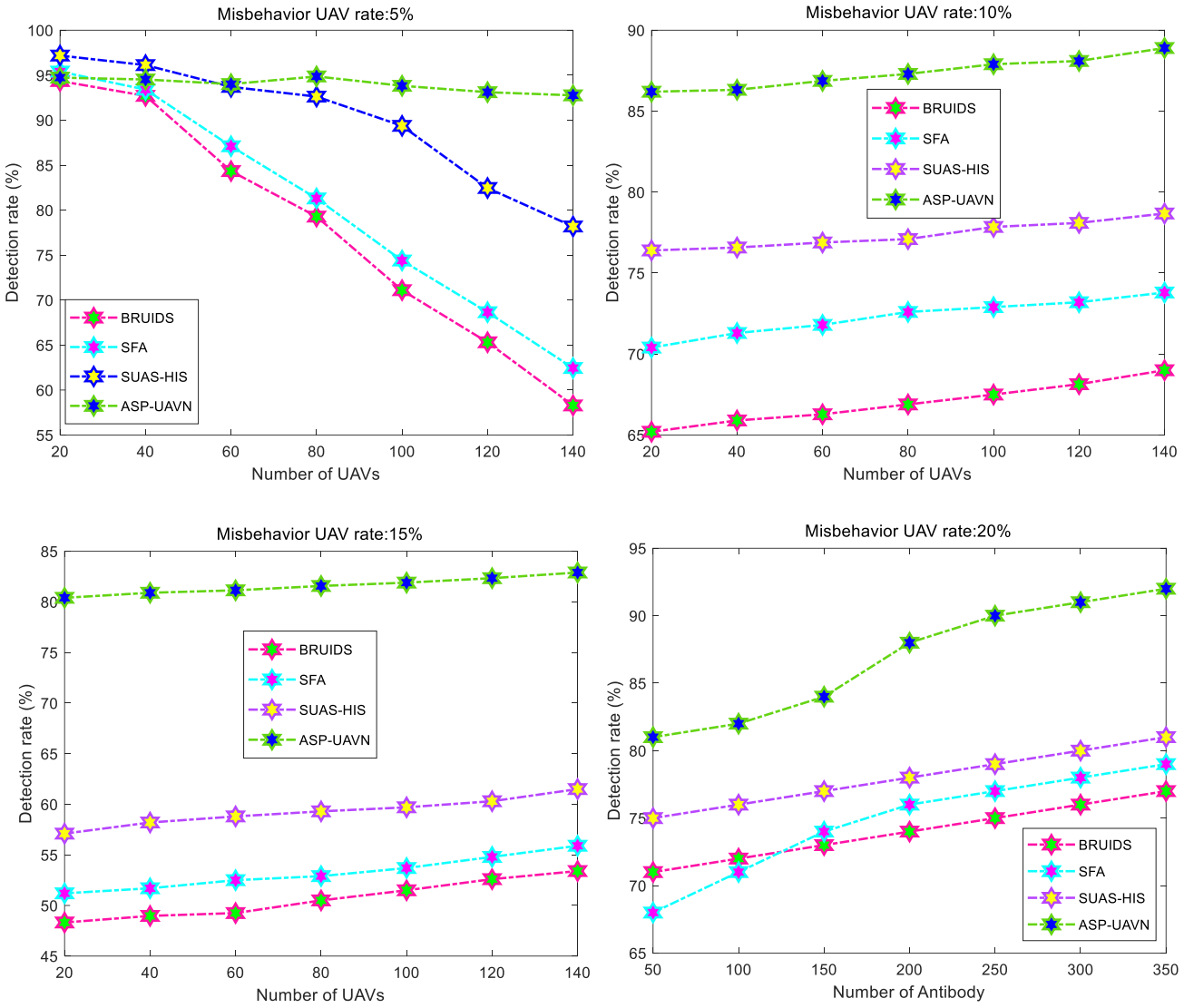


**Fig. 12** Comparison of the ASP-UAVN, SUAS-HIS, SFA and BRUIDS models in term of DR.

## 6 Conclusion and Future work

UAVs have increasing utilization in civilian and military applications recently. Communication security is one of the critical factors ensuring the appropriate UAVs' operation. Rather, UAVs can be captured by adversaries. In this study, it was confirmed that some devastating attacks can be launched simply at a low-cost including wormhole, Sybil and sinkhole attacks, which appears complicated. Hence, it is important to take into account the communication security for UAVs severely. In ASP-UAVN proposed method, the safest route from the source UAV to the destination UAV is chosen according to a self-protective system. In this method, a multi-agent system using an artificial immune system is employed to detect the attacking UAV and choose the safest route. In the proposed P-method, the route request packet (RREQ) is initially transmitted from the source UAV to the destination UAV to detect the existing routes. Then, once the route response packet (RREP) is received, a self-protective method using agents and the knowledge base is employed to choose the safest route and detect the attacking UAVs. We investigated

the ASP-UAVN scheme performance using NS-3. According to the results of the simulation, the ASP-UAVN was highly powerful against lethal attacks. It was demonstrated that it enjoys a high PDR (below 87.8%), a low PLR (below 11.8%), a low FP (below 7.104%) and a high level of security, high detection rate (above 94.50%), and low FN (below 4.95%) in comparison with present methods. In future work, the use of Firefly optimization is suggested to further reduce consumption energy and malicious attacks on the Unmanned Aerial Vehicle Networks. Firefly algorithm is proposed to cluster UAV nodes and authenticate /security in two levels to prevent from attacks.

## Conflict of Interest

None.

# Reference


1. Sun, X., Ng, D. W. K., Ding, Z., Xu, Y., & Zhong, Z. (2019). Physical layer security in UAV systems: Challenges and opportunities. IEEE Wireless Communications, 26(5), 40-47.
2. Mabodi, K., Yusefi, M., Zandiyan, S., Irankhah, L., & Fotohi, R. Multi-level trust-based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication. The Journal of Supercomputing, 1-25.
3. Fu, Z., Mao, Y., He, D., Yu, J., & Xie, G. (2019). Secure Multi-UAV Collaborative Task Allocation. IEEE Access, 7, 35579-35587.
4. Jamali, S., & Fotohi, R. (2016). Defending against wormhole attack in MANET using an artificial immune system. New Review of Information Networking, 21(2), 79-100.
5. Shang, B., Liu, L., Ma, J., & Fan, P. (2019). Unmanned Aerial Vehicle Meets Vehicle-to-Everything in Secure Communications. IEEE Communications Magazine, 57(10), 98-103.
6. Jamali, S., Fotohi, R., Analoui, M. (2018). An Artificial Immune System based Method for Defense against Wormhole Attack in Mobile Adhoc Networks. TABRIZ JOURNAL OF ELECTRICAL ENGINEERING, 47(4), 1407-1419
7. Won, J., Seo, S. H., & Bertino, E. (2019). A Secure Shuffling Mechanism for White-box Attack-resistant Unmanned Vehicles. IEEE Transactions on Mobile Computing.
8. Atoev, S., Kwon, O. J., Kim, C. Y., Lee, S. H., Choi, Y. R., & Kwon, K. R. (2019, July). The Secure UAV Communication Link Based on OTP Encryption Technique. In 2019 Eleventh International Conference on Ubiquitous and Future Networks (ICUFN) (pp. 1-3). IEEE.
9. 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.
10. 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.
11. Fotohi, R. (2020). Securing of Unmanned Aerial Systems (UAS) against security threats using human immune system. Reliability Engineering & System Safety, 193, 106675.
12. Oubbati, O. S., Mozaffari, M., Chaib, N., Lorenz, P., Atiquzzaman, M., & Jamalipour, A. (2019). ECaD: Energy-efficient routing in flying ad hoc networks. International Journal of Communication Systems.
13. Sayeed, M. A., Kumar, R., & Sharma, V. (2020). Efficient data management and control over WSNs using SDN-enabled aerial networks. International Journal of Communication Systems.
14. Arthur, M. P. (2019, August). Detecting Signal Spoofing and Jamming Attacks in UAV Networks using a Lightweight IDS. In 2019 International Conference on Computer, Information and Telecommunication Systems (CITS) (pp. 1-5). IEEE.
15. Zhou, X., Wu, Q., Yan, S., Shu, F., & Li, J. (2019). UAV-enabled secure communications: Joint trajectory and transmit power optimization. IEEE Transactions on Vehicular Technology, 68(4), 4069-4073.
16. Wu, J., Zou, L., Zhao, L., Al-Dubai, A., Mackenzie, L., & Min, G. (2019). A multi-UAV clustering strategy for reducing insecure communication range. Computer Networks, 158, 132-142.

17. García-Magariño, I., Lacuesta, R., Rajarajan, M., & Lloret, J. (2019). Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain. Ad Hoc Networks, 86, 72-82.
18. Hatzivasilis, G., Papaefstathiou, I., & Manifavas, C. (2017). SCOTRES: secure routing for IoT and CPS. IEEE Internet of Things Journal, 4(6), 2129-2141.
19. Cai, Y., Wei, Z., Li, R., Ng, D. W. K., & Yuan, J. (2019). Energy-efficient resource allocation for secure UAV communication systems. arXiv preprint arXiv:1901.09308.
20. Li, Z., Chen, M., Pan, C., Huang, N., Yang, Z., & Nallanathan, A. (2019). Joint Trajectory and Communication Design for Secure UAV Networks. IEEE Communications Letters, 23(4), 636-639.
21. García-Magariño, I., Lacuesta, R., Rajarajan, M., & Lloret, J. (2019). Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain. Ad Hoc Networks, 86, 72-82.
22. Yuan, X., Feng, Z. Y., Xu, W. J., Wei, Z. Q., & Liu, R. P. (2018). Secure connectivity analysis in unmanned aerial vehicle networks. Frontiers of Information Technology & Electronic Engineering, 19(3), 409-422.
23. Rashid, A., Sharma, D., Lone, T. A., Gupta, S., & Gupta, S. K. (2019, July). Secure communication in UAV assisted HetNets: a proposed model. In International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage (pp. 427-440). Springer, Cham.
24. Dasgupta, D. (Ed.). (2012). Artificial immune systems and their applications. Springer Science & Business Media.
25. Seyedi, B., & Fotohi, R. NIASHPT: a novel intelligent agent-based strategy using hello packet table (HPT) function for trust Internet of Things. The Journal of Supercomputing, 1-24.
26. Chen, J., Feng, Z., Wen, J. Y., Liu, B., & Sha, L. (2019, March). A Container-based DoS Attack-Resilient Control Framework for Real-Time UAV Systems. In 2019 Design, Automation & Test in Europe Conference & Exhibition (DATE) (pp. 1222-1227). IEEE.
27. Fotohi, R., & Bari, S. F. (2020). A novel countermeasure technique to protect WSN against denial-of-sleep attacks using firefly and Hopfield neural network (HNN) algorithms. The Journal of Supercomputing, 1-27.
28. Sun, X., Ng, D. W. K., Ding, Z., Xu, Y., & Zhong, Z. (2019). Physical layer security in UAV systems: Challenges and opportunities. IEEE Wireless Communications, 26(5), 40-47.
29. Fotohi, R., Bari, S. F., & Yusefi, M. (2019). Securing Wireless Sensor Networks Against Denial-of-Sleep Attacks Using RSA Cryptography Algorithm and Interlock Protocol. International Journal of Communication Systems.
30. Lei, K., Zhang, Q., Lou, J., Bai, B., & Xu, K. (2019). Securing ICN-Based UAV Ad Hoc Networks with Blockchain. IEEE Communications Magazine, 57(6), 26-32.
31. Yihunie, F. L., Singh, A. K., & Bhatia, S. (2020). Assessing and Exploiting Security Vulnerabilities of Unmanned Aerial Vehicles. In Smart Systems and IoT: Innovations in Computing (pp. 701-710). Springer, Singapore.
32. Madan, B. B., Banik, M., & Bein, D. (2019). Securing unmanned autonomous systems from cyber threats. The Journal of Defense Modeling and Simulation, 16(2), 119-136.
33. Haque, M. S., & Chowdhury, M. U. (2019, November). Ad-Hoc Framework for Efficient Network Security for Unmanned Aerial Vehicles (UAV). In International Conference on Future Network Systems and Security (pp. 23-36). Springer, Cham.
34. 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.
35. Lodeiro-Santiago, M., Caballero-Gil, P., Aguasca-Colomo, R., & Caballero-Gil, C. (2019). Secure UAV-Based System to Detect Small Boats Using Neural Networks. Complexity, 2019.