International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 28, No. 1, February, 2023, pp. 49-66
Journal homepage: http://iieta.org/journals/isi

An Adaptive Secure and Efficient Bio-Inspired Routing Protocol for Effective Cooperation in FANETs

Abdesselem Beghriche

Computer Science Department, Ferhat Abbas University Sétif -1, Sétif 19000, Algeria

Corresponding Author Email: abdesselem_beghriche@univ-setif.dz

https://doi.org/10.18280/isi.280106

Received: 4 November 2022
Accepted: 10 February 2023

Keywords:
Artificial Immune System, dendritic cells, flying ad hoc networks, penguin search optimization algorithm, routing protocol, security threats, unmanned aerial vehicle

ABSTRACT

The advancement of automated systems and their capabilities stimulate the formation of ad hoc networks using Unmanned Aerial Vehicles (UAVs). The network composed by these UAVs is known as Flying Ad hoc Network (FANET). The provision of security in such systems is particularly challenging because of their unique characteristics, which make it difficult to enhance their defenses against continually emerging security threats. The purpose of this paper is to create a new secure and reliable security framework by proposing an adaptive secure and efficient bio-inspired routing model based on the Artificial Immune System approach (AIS), as well as applying the meta-heuristic Penguins Search Optimization Algorithm (PeSOA) in order to improve its performance. Actually, an experimental study was carried out to evaluate the efficiency of the proposed idea regarding network interaction quality, malicious node mitigation, and system security enhancements.

1. INTRODUCTION

Recent technical advancements of embedded systems have helped to produce the Unmanned Aerial Vehicles (UAVs) with highly efficient reliability, since these aircrafts have proven to be a very flexible platform for a variety of applications [1]. These developments and heavy involvement of information technology have made it easier than ever to set up an Unmanned Aerial System (UAS) with complex topology in order to accomplish sophisticated missions that were previously impossible to accomplish without the involvement of actual humans. The use of this type of aircrafts has been intensified in the recent years, due to the various advantages offered compared to conventional aircrafts, as well as their ability to operate in harsh environments. The deployment of a swarm of collaborative UAVs with ad hoc routing fashion could be one of the possible solutions to setup a new kind of applications, named as Flying Ad hoc Networks (FANETs) [2].

FANETs are autonomous systems made up of a swarm of UAVs and one or more ground control stations (GCS) (Ground Control Station). In addition, to flying independently on pre-programmed flight plans, the UAVs may be controlled by using complicated dynamic automation systems, which are typically agile and flexible in their implementation [3]. During operation, UAVs are controlled and monitored from the ground-controlled station, based on information sent by on-board equipment via a wireless channel. FANETs offer self-organized and independent behavior of nodes (UAVs). UAVs are free to move in any direction to complete assigned tasks, due to which the network topology changes frequently. The UAVs can also join or leave the network as needed.

This network can also be considered as a subcategory of the famous MANET (Mobile Ad hoc network). However, it has certain specific features (such as UAV velocity, specific mobility model, etc.) which can have an impact on the performance of routing protocols. Furthermore, the nature of the wireless medium, as well as the lack of the fixed infrastructure, which is necessary to verify the authentication of UAVs and messages, thus creating security breaches [4]. In this setting, to accomplish the desired functionality, there is an inherent reliance on cooperation between the UAVs. The collaboration is only fruitful if all members are honest with one another [5]. In reality, it is possible that such a perfect arrangement may not always be achieved. There is a possibility that some UAVs would act maliciously, resulting in a decrease of network performance or perhaps a complete interruption of the network's functioning [6]. Therefore, developing an efficient and secure routing protocol in FANETs has attained a significant interest in the research community.

A number of studies have been undertaken on how to establish a FANET, but only a few of them have taken into account the security aspects of this endeavor. Where, FANET's unique features have made it hard to strengthen its defense against any changing security threats [1]. In order to mitigate the effects of misbehaving UAVs, several secure routing protocols [1, 7-13] have been proposed to secure the communication content and guarantee reliable delivery of the exchanged messages. Although they have proven their effectiveness, these solutions have been designed based on the assumption that all UAVs in the network are trustworthy. However, owing to resource constraints or malevolent conduct, this assumption may turn out to be incorrect. Consequently, the UAVs may not act as planned, making the network functioning inefficiently. While it is reasonable to assume that UAVs would act appropriately, this assumption might result in unforeseen consequences, such as poor network efficiency, excessive resource consumption, and increased susceptibility to attacks [14]. Hence, these protocols are limited in their coverage of potential risks and are not flexible enough to be merged with one another [6]. Nevertheless, the intrinsic question is how to find a balanced trade-off among security, efficiency, and the network requirements.

To attenuate the effects of misbehaving UAVs and to reach high levels of security and reliability in such a cooperative communication environment, an appropriate routing mechanism is crucial for the desired service provision, as well as the improvement of communication performance and security. In order to meet these requirements, biologically inspired approaches [15-17] seem promising when high level of robustness and adaptability is required. Biological approaches can usually be adopted to solve network problems at high levels due to the high similarity between both of them. In fact, when, looking carefully at nature, it is clearly observed that the dynamics of many biological systems and laws governing them are based on simple generic rules which produce collaborative and effective patterns, without the need for any external controlling entity [16], leading to intelligent global behavior.

Generally, biological systems and processes have intrinsic appealing characteristics of self-organization, adaptivity, scalability, robustness, and distribution. The combination of these traits leads to various degrees of inspiration from biological systems, which in turn leads to the development of various approaches and algorithmic designs for efficient and secure communication networks [18, 19]. So, these approaches can be correctly used to FANETs in order to resolve a variety of challenges that arise during the construction and operation of such networks.

The creation of routing protocols inspired by advanced biological behaviors has occurred as a research consequence conducted in this regard [20-22]. However, the problem of security in these protocols is still an open issue. It would not be able to achieve widespread acceptance and adoption of these protocols in FANETs unless the security implications of these protocols had been carefully considered.

The main purpose of this paper is to design and implement a new reliable security framework in FANETs by establishing an adaptive secure and efficient bio-inspired routing model based on an Artificial Immune System approach, which is referred to as "Penguin-AIS", a new trend that aims to protect and enhance the security of ad hoc networks.

Based on the many similarities that exist between the tissue environment in the human body and the ad hoc network environment, it was are convinced that the robust defense achieved by the Human Immune System (HIS) may be mimicked into an Artificial Immune System (AIS) [23] in order to protect FANETs. Thus, AIS is described as the abstraction of the structure and function of the human immune system to be used in computational systems (mathematics, engineering, and information technology) [23]. AIS security techniques are judged to be more compatible with FANETs where no central management points are present. Those techniques are also known to be less complex and more adaptable since they take up the limitations of such networks [24].

The proposed routing model describes a novel bio-inspired routing protocol that applies the meta-heuristic Penguins Search Optimization Algorithm (PeSOA) [25], which is inspired by the hunting behavior of penguins. The penguins can collaborate their efforts and synchronize their dives in order to maximize the global energy in the process of collective hunting and nourishment. The idea consists to divide the penguins into several groups, where each group is allotted to a separate region in the food space [26]. During the foraging phase, the penguins in each group attempt to hunt as many fish as possible around the allotting region. Food information is shared among elements of other groups and also between elements within the same group, enabling to reach of the optimal solution in a given time. The global solution is chosen by electing the best group of penguins that ate the maximum of fish.

The main technical contributions of this work can be summarized as follows:

(1) Designing a new reliable security framework for FANETs, the proposed scheme consists of two main phases: a. Establishing a new bio-inspired routing model based on the PeSOA meta-heuristic, this latter plays a significant role in selecting the optimal paths, allowing routing to be well optimized, resulting in improved protocol performance in terms of QoS parameters, packet delivery rate, energy efficiency metric, and end-to-end delay, amongst other measures. b. Accomplishment of a secure routing that incorporates the concepts of AIS approach, meanwhile utilizing the optimum routing discovered in the first phase of the proposed scheme, including the mechanism of anti-attack and decision-making applications.

(2) An appropriate security model for multiple routing strategies in FANETs is described, and a routing protocol is shown as an example of how the proposed model might be implemented in practice.

(3) Simulations are carried out to evaluate the performance of the proposed protocol, including its capacity to detect and isolate malicious UAVs, as well as its efficacy against a variety of various attacks.

The remainder of this paper is structured as follows: After the introduction, Section 2 describes related works and literature review dealing with security issues in FANETs, as well as various bio-inspired schemes that have been proposed in this field. The background about the AIS and the meta-heuristic PeSOA is described in Section 3. Section 4 presents the detailed design of the proposed security framework and describes the intuitive properties that any scheme should have in this context. Implementation and performance evaluation of the applied model are presented in Section 5. Finally, the conclusion is discussed in Section 6 with an outlook to future research.

2. RELATED WORKS

In FANETs, the communication is a highly important component for any application concerning cooperation between the UAVs. For this reason, problems regarding security must be considered as much as the problems related to efficiency or reliability, as there is a trade-off to establish between routing efficiency and security overheads. Many relevant research works have been conducted [7-13, 20-22, 27, 28] in the direction of designing routing protocols, these works mainly focus on the development of efficient and secure routing protocols in terms of specific metrics.

Indeed, all these works could be classified into three main categories: (i) Cryptography-based solutions [7, 8, 12, 13, 27, 28], (ii) Trust-based solutions [9-11], and (iii) Bio-inspired based solutions [20-22]. Some of the related previous works that have been carried out in order to make FANETs more trustworthy are explained in this section.

2.1 Main cryptography-based solutions

In this context, many solutions have been proposed to secure inter-UAV communications. They are primarily focusing on various security services such as authentication, access control, data integrity, availability, and privacy. These methods are the greatest defense against malicious insiders, but they are notoriously resource-intensive and computationally intensive, making them impractical for use in today's UAVs.

Haque and Chowdhury [7] suggested to investigate the feasibility of using Identity-Based Encryption (IBE) in a UAV network with limited resource availability. Where they have assessed the practicality and performance of IBE in the UAV network by measuring the energy used by key management procedures, assessing the feasibility of the technique, and presenting an efficient security framework for a resource restricted wireless UAV network.

The work featured in the study [8] describes the implementation of a blind signature method in a certificate-less environment for UAVs. There are no public-key certificates needed for the proposed scheme. It also does not have the problem of having to keep the keys safe. Nevertheless, the amount of data that is gathered from the platform that monitors the UAVs may be too large to be processed by the same UAVs that are involved in the monitoring activity. Therefore, the authors extend their model to the 5G mobile network by using Multi-access Edge Computing (MEC) in its architecture to ensure secure communication between drones and the base station (BS).

In the same context, a pairwise key establishment scheme is proposed in the study [12], in which nodes in FANETs are not susceptible to get compromised. The idea of this work is based on the phenomenon of the small-world, each node in the network establishes the initial keys with nodes that are no more than three-hops away from it. Then, a pairwise key is established when any two nodes on the path between them exchange partial keys with one another. The pairwise key is generated by adding the partial keys together at each node. During the process of obtaining partial keys, the nodes on the route make use of the initial keys to safely transfer their partial key to the other nodes on the route.

SUAP (Secure UAV Ad Hoc Routing Protocol) is a novel secure routing protocol proposed in the study [13]. The approach enables message authentication while also providing detection and prevention of wormhole attacks. SUAP is a reactive protocol that makes use of public key cryptography and hash chains to protect data. However, the size of the authentication messages and the amount of computing power needed are the main drawbacks of this work.

He et al. [27] proposed a secure communication scheme for UAVs network. The idea proposes that each node maintains and controls a region in which the authorized devices may get a broadcast key without the need for a centralized online authority, this could be achieved by using the hierarchical identity-based broadcast encryption and pseudonym method. All devices in this system are capable to anonymously broadcast encrypted communications and decrypting the lawful ciphertext.

The cryptographic approaches are deployed to transform readable information into meaningless one, so ensuring the confidentiality and integrity of this information. However, cryptographic protection is complex by the fact that UAVs have a limited energy capacity and they cannot efficiently perform cryptographic calculations. Therefore, generating different security codes has been always considered as a difficult problem.

2.2 Main trust-based solutions

The goal of these solutions is to find the misbehaving node when it forwards a packet in the network. Each node builds trust links with other nodes by giving trust values to its relations, and such systems give a way for a requesting node to evaluate the confidence he provides to the provider of a resource. Currently available solutions for FANETs that are based on trust were first presented for MANETs [6, 14], with just a few solutions being specifically designed for FANETs.

As described in the study [9], a new trust model for FANETs has been presented, in which an evolutionary algorithm is utilized to optimize the weights of different factors in order to calculate direct trust values. Direct trust is grouped together with a recommendation to calculate the final trust value of a node. Based on the evaluation of the final trust values, the nodes are either included in the recommended list or removed from the list.

A Trust Based Clustering Scheme (TBCS) for FANETs was suggested in the study [10]. This scheme employs a multi-criteria fuzzy method for classification, which is based on the behavior of the node in a fuzzier and more complicated environment. In this proposal, there is a reward and punishment mechanism that tries to turn the node's behavior into trustful state, and to separate bad and malicious nodes from the rest of the nodes in the FANETs.

Barka et al. [11] proposed a new trust-aware Monitor-based communication architecture for Flying Named Data Networking (FNDN). In this work, the selection of monitors is based on their reliability and stability, they are then tasked with the responsibility of disseminating the interest packets in order to prevent the issue of broadcast storms. Once the data producer receives the interest, the data is sent to the requester through the quickest and most trusted method possible, depending on the circumstances.

Most of these models are based on the notion of recommendation, which, however, suffer from the drawbacks of sluggish convergence and excessive complexity of trust calculations, as well as the huge overhead of network traffic, leading to an inaccurate evaluation of trust value.

2.3 Main bio-inspired based solutions

As it was have mentioned above, all of the current solutions from both pervious categories are suffering from high rates of packet loss, which is considered an intrinsic property of the FANETs. Actually, no previous work for FANETs has focused on bio-inspired routing protocols and the manner they can be used to improve network security. Nonetheless, some papers which are considered to be among the worth noting work in the field have specifically treated FANET communication architecture design challenges and issues. Among these papers, some of them could be quoted, like:

It has been suggested [20] to apply a bio-inspired clustering strategy for FANETs (BICSF), which employs a hybrid mechanism of glowworm swarm optimization (GSO) and krill herd optimization (KH). The researchers suggested an effective cluster management algorithm for the optimal position of the UAV based on the behavioral research of (KH) and genetic operators such as mutation and crossover. In order to guarantee effective communication between the UAVs, a path recognition algorithm based on the weighted residual energy, the number of neighbors, and the distance between the UAVs has been developed to aid in route selection.

With the use of a clustering strategy, the work referenced in the study [21] tries to resolve the problem of the short lifetime of the FANETs. In order to do this, two alternative clustering techniques are used: the first scheme is a mix of the k-means clustering algorithm and the firefly algorithm, while the second scheme is based on the glowworm swarm optimization (GSO) algorithm and the firefly algorithm.

Several FANET algorithms, as well as algorithms based on swarm intelligence, are discussed briefly in the study [22], including a brief summary of the current algorithms in use (ant and bee colonies). It was shown via the experimental research carried out by the authors that it is possible to use bio-inspired algorithms in a cost-effective manner.

3. CONTEXT OF THE PROPOSED APPROACH

Some essential concepts are presented in this section, as well as the frameworks being used in this paper such as Artificial immune systems (AIS) and the meta-heuristic Penguins Search Optimization (PeSOA).

3.1 Artificial immune systems (AIS)

A new field of problem-solving strategies is the bio-inspired approach. In fact, bio-inspired algorithms are bottom-up, adaptive, and flexible, allowing them to provide elegant solutions to engineering issues that are hampered by standard techniques. Many bio-inspired algorithms function as highly decentralized systems composed of several components. FANETs are also near to be completely decentralized systems, and it consists of mobile nodes as system components. So, bio-inspired techniques can be precisely applied to FANETs to solve various issues, including functioning, design, and security. In this context, an AIS incorporates many properties of HIS, including diversity, dynamic learning, distributed computation, error tolerance, adaptation, and self-monitoring. These properties are highly desirable in a security system for FANETs.

3.1.1 The human immune system (HIS)

Biological immune systems have intelligent capabilities of detecting antigens in the body, their main function is to protect the body from different types of pathogens, such as viruses, germs, bacteria, parasites and to clear it from debris. The immune system can be classified into two types, innate and adaptive as shown in Figure 1. The innate immune system is responsible for general defense, whereas the adaptive immune system is responsible for specialized defense.

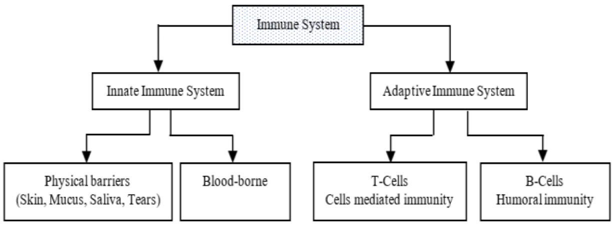

Figure 1. Classification of Immune System

When pathogens (infections) enter the system, the innate immune system acts as the body's first line of defense. All infections and foreign substances trigger an immune response. If the innate immune system fails to eliminate the pathogen, the adaptive immune system takes over the infection. Indeed, the adaptive immune response is carried out by white blood cells called lymphocytes [15], lymphocytes are of two types, namely T-Cells and B-Cells.

3.1.2 AIS algorithms

The algorithms designed for AIS mainly model the innate mechanism, that apply in solving a wide range of computational problems. The four major algorithms that form the basis of AIS research are [29]: Negative Selection Algorithm (NSA) [30], Clonal Selection Algorithm (CSA) [31], Immune Network algorithms Theory [32], and Danger Theory [33].

3.2 The meta-heuristic penguins search optimization

The development of new approaches based on meta-heuristics inspired by natural phenomena [25, 34-37] has proved its effectiveness in solving and optimizing a plethora of problems and applications, including NP-hard problems [26]. These techniques can be classified according to different research characteristics such as trajectory-based methods and population-based methods by memory usage. They are as diverse as the sources of inspiration from which they originate (physical, biological, ecological behavior, etc.).

The PeSOA is one of the latest proposed nature-inspired meta-heuristic optimization algorithms, which was first proposed in the study [25], it was inspired by the hunting behavior of penguins in nature.

3.2.1 Hunting comportment of penguins

The hunting strategy of penguins is based on the assumption admitting that eating behavior is most likely determined by economic reasoning: That is to say, having an energy benefit larger than the cost in searching for food. The Penguins, as biological entities, utilize this assumption to measure the amount of time and energy necessary to seek for food and the abundance of prey, on the one hand and determine where they should congregate.

To maximize forage opportunities, penguins must hunt in groups and coordinate their dives [38]. Penguins interact with one another using vocalizations, each penguin has its own set of vocalizations (like fingerprints in humans). As a result, each penguin may be uniquely identified and penguins can recognize one another [25]. Because of the huge size of the colonies and the penguins' striking resemblance, this issue of identification and recognition is critical.

3.2.2 The PeSOA algorithm

There are several methods to define the optimization method based on the hunting behavior of the penguins. While all approaches agree on the need of optimizing their objective functions, such as maximizing the quantity of energy retrieved from the energy invested. The following guidelines are offered to summarize the findings from penguin foraging behavior.

(1) A penguin population (colony) is made up of multiple groups. The number of penguins in each group changes according to food availability in the appropriate foraging location.

(2) In accordance with the knowledge regarding energy

acquisition and the cost of getting it, each group of penguins begins foraging at a specified depth beneath the water and randomly roam about until they discover food, when oxygen reserves are not depleted.

(3) Penguins return to the surface after a number of dives to discuss the locations and availability of food sources with their local affiliates through intra-group communication.

(4) When food supplies are inadequate for a given group of penguins, a component of the group or the whole group, migrates to another place through inter-group communication. Swimming Course, Oxygen Reserve, Intra-group Communication, and Food Availability are among the biological behaviors that are abstracted in the sections below.

Update on the Swimming Course. Let (G_1, G_2, …, G_k) denote the set of "k" disjoint penguin groups that are randomly dispersed across the solution space "φ". Each penguin "j" in "G_i" is put at a solution at time instance "t" and the penguin "j" swims to a new location at a time "t+1" in "φ" according to the following Equation [26]:

$$x_j^i(t+1) = x_j^i(t) + O_j^i(t) * \alpha * \left(x_{Local\ Best}^i - x_j^i(t)\right) \tag{1}$$

where, $x_j^i(t)$ represents the position of penguin "j" in the i^{th} group at the t^{th} occurrence, $O_j^i(t)$ represents the oxygen reserve of the j^{th} penguin of the i^{th} group, α represents a randomly distributed number drawing from [0, 1], and $x_{Local\ Best}^i$ represents the best solution found by the i^{th} group.

Update on the Oxygen Reserve. Following each dive, the penguin's oxygen reserve is updated in the following manner [26]:

$$O_j^i(t+1) = O_j^i(t) + \left[f(x_j^i(t+1)) - f(x_j^i(t))\right] * \left|x_j^i(t+1) - x_j^i(t)\right| \tag{2}$$

where, "f" is the underlying problem's objective function. The penguin's oxygen reserve is determined by both the amount of food he consumes and the amount of time he spends while swimming. If the energy gain is positive, the penguin will remain under water longer, catching more food and therefore becoming healthier. Otherwise, the longer the penguin swims, the more oxygen he uses. As a result, the oxygen reserve is updated in accordance with the improvement of the objective function.

Intra-group Communication. Penguins feed in a group and have excellent intra-group communication skills. Penguins will follow the local guide who performed the best of the previous dive (Eq. (1)). Every time a penguin dives, it may discover a better food source and become the new local guide. Team foraging is an autocatalytic process that ensures that experimental solutions are continually improved.

Update on Food Availability. In the context of penguin foraging, the Quantity of Eaten Fish (*QEF*), may be used to assess the degree of food abundance, which is computed using the following expression [26].

$$QEF^i(t+1) = QEF^i(t) + \sum_{j=1}^{d_i}(O_j^i(t+1) - O_j^i(t)) \tag{3}$$

A high QEF score indicates that the location provides adequate food for the whole group and even attracts penguins migrating from neighboring groups.

Update on the Membership of the Group. Due to the food undersupply in the original group, the penguin may move to another group. The penguin changes its group membership by referring to a function that is related to the degree of food availability in different groups of penguins. The probability of entering the group "i" is provided by the following membership function value [26]:

$$P_i(t+1) = \frac{QEF^i(t)}{\sum_j^k QEF^j(t)} \tag{4}$$

The pseudocode of the PeSOA is given in algorithm 1.

Algorithm 1 The PeSOA algorithm
Inputs: Random population of penguins in"K" groups.
Output: The fitness value for each group of penguins.

```
Generate "K" regions in the solution space;
Generate penguins (j=1, 2, ..., N/K) for each group "i" in the specified area;
Initialize each penguin's oxygen reserve;
While criterion of stop is not met do // *
    For (i=1) to number of groups generated
        For each penguin ($j \in G_i$) do
            While ($O_2 > 0$) do // oxygen reserves are not depleted
                Improve the penguin position $x_j^i$ using Eq. (1);
            End while
        End for
        Update the food abundance degree for this group using Eq. (3);
    End for
    Update the best global solution;
    Update the value of each group membership function using Eq. (4);
    Redistribute penguins by membership function to groups;
    Leave the group unless there are no members;
End while
End.
```

***** // either the number of fish has reached its limit or the number of iterations has ended.

4. THE PROPOSED MODEL

Because a hacked or disloyal node offers a significant risk to the network, the path that avoids the malicious node may be more important than the shortest route. As a matter of fact, most routing protocols used by the FANET community are designed to discover the shortest route from a source to a destination without taking into consideration the existence of any malicious nodes along the route. In order to enhance the routing protocol regarding security issues, high interest is focused on the creation of a solution that will make the routing protocol more resistant against malicious nodes actions.

This section depicts a novel reliable security framework based on AIS and PeSOA algorithms, which may be subdivided into two phases: Penguin-AIS-Routing and Penguin-AIS-Security.

4.1 A routing protocol based on PeSOA (Phase 1)

Generally, Ad hoc routing protocols, in their most basic form, follow a common procedure. When the RREQ (*Route REQuest*) procedure is initiated (step 1 in the Figure 2), the sender node waits for RREPs (*Route REPlay*) from the other nodes, after that, the routes reply (step 2) is conveyed to the source through a variety of different paths. Nodes provide information about their residual energy, routing load, and hop-count in the reply packets they send back to the sender. Once the reply packets have been received from multiple routes, the source node assesses the data and deduces the fitness value for each path (step 3).

In order to accomplish this, the source node selects the number of paths "*n*" having the best fitness value and ranks them in its routing table according to the fitness values of each path in descending order, and then it transmits data over the path with the highest fitness value that is ranked at the top of the routing table (step 4). In the event that the route fails, the data transmission is resumed using the path with the highest fitness value after failing. If all "*n*" routes fail to transmit data, the algorithm begins the process over again, searching for the best fitness multi-paths and repeating the process until the data is successfully sent.

So, the optimal route between source and destination is carried out using the characteristics of the PeSOA algorithm, by treating groups of penguins as UAVs. The area-based search may be mapped using PeSOA, the inter-group migration of UAVs based on explored routes is analogous to penguin inter-group movement based on fish presence. Each group of UAVs will be led by a drone (leader) that will transmit data to the central command, such as, position and discovered targets, and thus, data may be shared with the other groups.

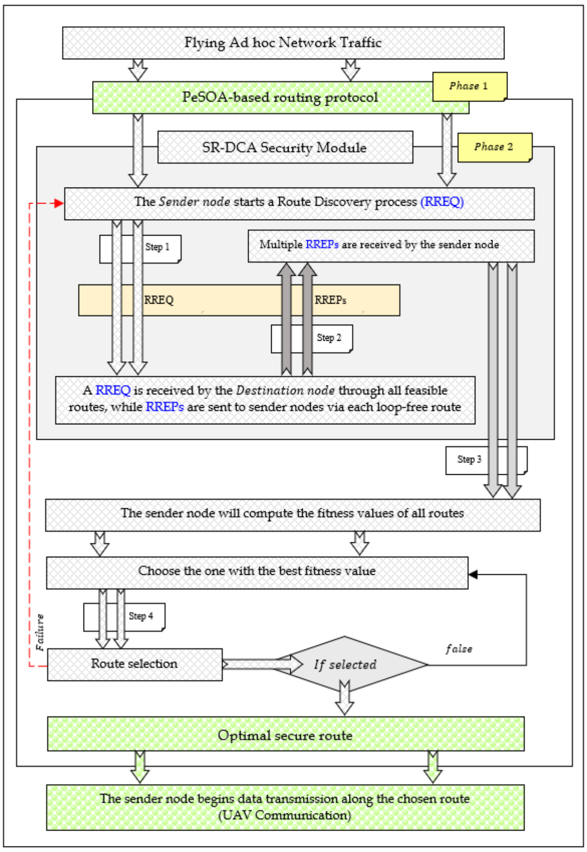
Flying Ad hoc Network Traffic
PeSOA-based routing protocol
Phase 1
SR-DCA Security Module
Phase 2
The Sender node starts a Route Discovery process (RREQ)
Step 1
Multiple RREPs are received by the sender node
RREQ
RREPs
Step 2
A RREQ is received by the Destination node through all feasible routes, while RREPs are sent to sender nodes via each loop-free route
Step 3
The sender node will compute the fitness values of all routes
Choose the one with the best fitness value
Step 4
Failure
Route selection
If selected
false
Optimal secure route
The sender node begins data transmission along the chosen route (UAV Communication)

Figure 2. Architecture of Penguin-AIS model

4.1.1 Objective function

In most cases, there are three major reasons making the route broken between sources and destinations in FANETs networks: The first one is that the UAVs will be rendered inoperative due to a shortage of energy, the second one is UAV mobility, and the third one is traffic congestion, as traffic increases, there will be greater congestion, which may result in packet droppage in certain instances. In this study, the three aspects used to verify the consistency and fidelity of a route are: The Remaining Energy level, the Link Firmness, and the Congestion level.

The best route should have a balanced UAVs energy distribution, excellent connection reliability and, a balanced congestion distribution. Alternatively, this may be stated as the integrated cost function of routing between two UAVs, as shown in the following relationship:

$$F_{ij} = \sum_{\substack{i,j \\ i\neq j}} \Big(\omega_1 * (Enr_{\,lev\,(i)} + Enr_{\,lev\,(j)}) + \omega_2 * L_{Frm\,(i,j)} + \omega_3 * 1/Cong_{\,lev\,(i,j)}\Big) \tag{5}$$

where, F_{ij} represents the objective function, ω denotes the parameter for weight adjustment, such that ($\omega_1+\omega_2+\omega_3=1$), $Enr_{lev(i)}$ and $Enr_{lev(j)}$ indicate the Remaining Energy level of the UAVs (*i*) and (*j*) respectively, $L_{Frm(i,\,j)}$ represents the Link Firmness between UAVs (*i*) and (*j*), and $Cong_{lev\,(i,\,j)}$ represents the Congestion level between UAVs (*i*) and (*j*).

The section below explains all relevant expressions in relation with the objective function:

Remaining Energy Level. It is necessary to estimate and update the remaining energy of each UAV regularly in order to improve the endurance of each UAV.

$$Enr_{Rem} = Enr_{Initial} - Enr_{Exhausted} \tag{6}$$

where, "$Energy_{Rem}$" represents the residual energy level, "$Enr_{Initial}$" shows the initial level of energy, and "$Enr_{Exhausted}$" indicates the level of energy used when conveying a message. "$Enr_{Exhausted}$" can be given as [39]:

$$Enr_{Exhausted} = Enr_{Send} + Enr_{Rec} \tag{7}$$

where, "Enr_{Send}" is the quantity of energy consumed while sending the data, and "Enr_{Rec}" is the quantity of energy consumed while receiving the data. The "Enr_{Send}" and "Enr_{Rec}" may be calculated using Eq. (8) and Eq. (9), respectively.

$$Enr_{Send} = (Enr_{Trans} * Nbr_{bits}) + (Enr_{SNR} * Nbr_{bits} * d^2) \tag{8}$$

$$Enr_{Rec} = (Enr_{Trans} * Nbr_{bits}) \tag{9}$$

where, "Enr_{Trans}" represents the quantity of energy used to convey a message in one unit, "Enr_{SNR}" stands for the quantity of energy required to achieve a certain Signal to Noise Ratio (SNR), "Nbr_{bits}" indicates the number of bits present in the message, and "*d*" describes how a UAV is far from another (See Eq. (13)).

The energy level has a value that varies in [0, 1]. If the energy level value is greater than the threshold value, a UAV could be associated with other UAVs in order to facilitate the routing process in an efficient manner, else the UAV is isolated and will not participate in the routing process.

Link Firmness. This measure is composed of three components: connection quality, safety degree and mobility prediction factor. If UAVs "*i*" and "*j*" are within communication range of one another, the link firmness between "*i*" and "*j*" may be described as a combination of link quality "$L_{Qty\ (i,j)}$", safety degree $S_{Deg\ (i,j)}$, and a mobility prediction factor "$M_{Prd\,(i,\,j)}$", that could be described as:

$$\begin{cases} L_{Frm\,(i,j)} = \lambda_1 * L_{Qty} + \lambda_2 * S_{Deg\,(i,j)} + \lambda_3 * M_{Prd\,(i,j)} \\ \quad with \quad (\lambda_1 + \lambda_2 + \lambda_3) = 1 \end{cases} \tag{10}$$

where, λ_1, λ_2 and λ_3 are the weighting factors that are determined by the considered state. It is worth noting that all three costs are standardized to a unit cost. As a result, the value of $Link_{Frm\,(i,j)}$ is restricted to the range of [0, 1]. After that, we'll go through each of the measures that are mentioned in Eq. (10).

(1) Link quality: The forward and reverse delivery ratios are used in order to determine the link quality. Its computation is referred to [40], and the function expression is provided in Eq. (11).

$$L_{Qty\,(i,j)} = \gamma^f * \gamma^r \tag{11}$$

where, "γ^f" stands for the forward delivery ratio, it is defined as the ratio of a packet being successfully sent from UAV "i" and received by UAV "j". Similarly, "γ^r" stands for the reverse delivery ratio.

(2) Safety degree: Assume that (x_i, y_i, z_i) is the coordinates of UAV "i". The degree of safety $S_{Deg\,(i,j)}$ denotes the proximity between the UAVs "i" and "j" based on their current space, as shown in the following Equation:

$$S_{Deg\,(i,j)} = \frac{R-d}{R} \tag{12}$$

where, "R" is the communication range of a UAV, and "d" denotes the distance between two UAVs, such as:

$$d = \sqrt{[x_j(t) - x_i(t)]^2 + [y_j(t) - y_i(t)]^2 + [z_j(t) - z_i(t)]^2} \tag{13}$$

(3) Mobility prediction factor: Real-world kinematic and dynamic constraints prohibit a UAV from moving in an unexpected way, which is undesirable. For the purpose of evaluating the movement trend throughout the duration of the next period of time, the relative velocity between UAVs "i" and "j" at each given point of time, the following formula should be used [40]:

$$v_{relative} = \frac{d_t - d_{(t-\Delta t)}}{\Delta t} \tag{14}$$

where, "t" and "t-Δt" are the times of the most recent and second-to-last respectively of the received “Hello” messages. "d_t" and "$d_{t-\Delta t}$" are the distances between UAVs "i" and "j" respectively. If both UAVs move apart in the opposite direction at a maximum velocity "v_{max}", then "$v_{relative}$" is up to the maximum value "$2v_{max}$". If they are near to each other while traveling at their maximum velocity, "$v_{relative}$" will approach the minimum value, to become "$-2v_{max}$". So, the mobility prediction factor is defined as follows:

$$M_{Prediction\,(i,j)} = e^{1-\frac{v_{relative}}{2*v_{max}}} \tag{15}$$

Congestion Level. The congestion level measure is calculated using the traffic mass (T_{mass}) that happens between the UAVs routes. When the volume of traffic increases, the specific data will either not be transferred or transmitted at a very low transmission rate, resulting in incomplete transmission of the data, which leads to stagnation. The data may be lost as a result of a UAV's buffer Queue being overloaded. So, T_{mass} is a metric that is used to evaluate the buffer queue degree of each UAV.

To make the routing procedure more efficient, a route with the least quantity of traffic will be picked. The initiator UAV will always keep an eye on the queue state of the neighboring UAV. Every neighboring UAV will regularly update its queue length, and send it to the source. The traffic mass and traffic mass level may be expressed as:

$$\begin{cases} T_{mass} = \dfrac{\sum_{i=1}^{n} P_i}{Overall_{Queue}} \\ T_{mass-level} = \dfrac{T_{mass}}{Queue_{max}} \end{cases} \tag{16}$$

where, P_i, is the i^{th} pattern value that reflects the size of the buffer queue at any given time, $Overall_{Queue}$ represents the total number of buffer queue, that expanses patterns for a certain time period, $Queue_{max}$ reflects the buffer queue's maximum length, and "n" represents the number of UAVs along the route. In this way, the congestion level could be given according to the following formula:

$$Congestion_{\,level} = 1 - T_{mass-level} \tag{17}$$

The $Congestion_{level}$ value must be in the [0, 1] range. If it is more than 1, indicating that there is more traffic, and hence a greater chance of packet loss, indicating also, that UAV should not be used as a forwarding UAV.

4.1.2 Design of the fitness function

The fitness model presented for the PeSOA algorithm is based on the three parameters mentioned above. The solution that offers the greatest quantity of energy remaining, the greatest amount of link firmness intensity, and the lowest degree of congestion, results in the highest fitness function value and represents the best solution. The fitness function may be expressed as follows:

$$Fit(F_{ij}) = Max\ (F_{ij}) \tag{18}$$

4.2 AIS module (Phase 2)

In order to prevent these kinds of attacks from occurring in the network, a technique that mimics the Artificial Immune System based on the AIS features is used. This objective is accomplished by inspiring the Dendritic Cell (DC) model from the HIS, allowing it to recognize and detect all kinds of malicious attacks in FANETs. Before moving into the construction of the suggested algorithm, it's important addressing the following section to demonstrate how this cell operates.

4.2.1 Dendritic cells

Dendritic Cells (DCs) are immune system antigen-presenting cells (also known as accessory cells). Their primary role is to digest antigen material and deliver it to immune system T-Cells on the cell surface. They serve as conduits for information between the innate and adaptive immune systems. DCs perform anomaly detection on newly discovered antigens and generate adaptive immunity in order to identify the antigen's precise response.

DCs have three primary functions: collecting, processing and immune response regulation. At the collection step, each DC gathers an input antigen and its associated signals. When the first antigen is collected, the processing step starts. As many antigens as possible should be gathered and processed, DCs should operate in tandem to combat the invasion of antigens with varying structural characteristics.

DCs may be classified into three distinct different states: immature, semi-mature and fully mature. In the presence of sufficient input signals, immature DCs develop into either semi-mature or mature DCs, depending on the concentration of particular kinds of these input signals. Immature DCs are exposed to four kinds of input signals: PAMP, danger, safe, and inflammatory signals.

Each signal concentration affects the terminal differentiation state of immature DC when it is subjected to these input signals (either mature or semi-mature). Immature DC processes its contents and produces the cytokine interleukin-12 (IL-12) in response to PAMP and danger signals. Interleukin-10 (IL-10) production is also triggered by safe signals. As a result, incoming input signals provide information about the behavioral context of digested antigens, which may determine whether they are benign or malicious. IL-12 and IL-10 are often used to determine if a migrating DC is semi-mature or mature. In adaptive immunity, DCs move to meet T-Cells after processing the incoming antigen and its associated signals.

To be activated, each T-Cell in the lymph node needs two impulses. The first signal is produced when T-Cell epitopes attach to peptide-MHC on the surface of DC in both danger and safe situations. The second signal will be released either from completely mature DCs like IL-12 in order to encourage naïve T-Cells (NT-Cells) to combat in the danger state, or by semi-mature DC in the form of IL-10 to inhibit NT-Cell in the safe state [41].

As soon as the NT-Cell forms a bond with a mature DC and begins to receive IL-12, the NT-Cell begins to differentiate via a series of events known as clonal expansions. Clones are then separated into memory T-Cells (MT-Cells) and suppressor T-Cells (ST-Cells). MT-Cells store the malicious pathogen identified in the body as soon as it is found, to take a rapid reaction to this pathogen. Further, complete mature DCs will migrate into the lymph node NT-Cells.

4.2.2 Secure routing using DCs algorithm “SR-DCA”

This section describes the techniques used to develop the suggested security model, dubbed (SR-DCA: Secure Routing using Dendritic Cell Algorithm). SR-DCA is a stand-alone algorithm that secures the routing protocols in each UAV in FANETs. It mostly relies on the ability of DCs to serve as abnormality detectors and immune response controllers, respectively.

The SR-DCA is designed to be a monitoring point for verifying certain routing packet types, such as RREQ, RREP or Hello packets (as shown in Figure 3), before proceeding to the packet management of the routing protocol.

This approach seeks to eliminate the attack when it reaches the nearest legitimate UAV. At first sight, A stream of fusible information represented in packets with different IP source addresses and different behaviors of each packet appears to be difficult to identify an attacker. Indeed, if a group of anomalous and normal packets arrives at the queue of the legitimate UAV at the same time of detection, an intrusion detection system may mistakenly associate the behavior of anomalous packets with that of a legitimate UAV, which leads to ignore the aggressor identity.

The SR-DCA is made up of three major units (Figure 3): Monitoring and security unit, Innate unit, and Adaptive processing unit. Each unit consists of different components that interact with one another, and have a link to other components in outer units. In addition, each unit is in charge of performing a specified task in the intrusion detection process.

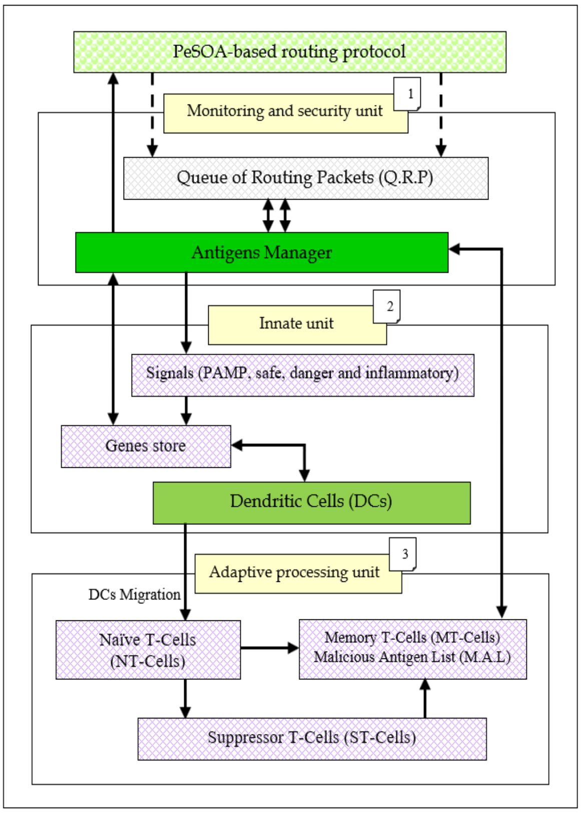
PeSOA-based routing protocol
1
Monitoring and security unit
Queue of Routing Packets (Q.R.P)
Antigens Manager
2
Innate unit
Signals (PAMP, safe, danger and inflammatory)
Genes store
Dendritic Cells (DCs)
3
Adaptive processing unit
DCs Migration
Naïve T-Cells (NT-Cells)
Memory T-Cells (MT-Cells) Malicious Antigen List (M.A.L)
Suppressor T-Cells (ST-Cells)

Figure 3. SR-DCA model

Monitoring and security unit. It is comprised of two main components: a Queue of Routing Packets (Q.R.P) and an Antigens Manager.

(1) The Q.R.P has three primary functions: collecting input packets from the routing protocol, storing the input packets in a First-In-First-Out (FIFO) queue, and delivering a packet from the front of the queue to the Antigens Manager as required.

(2) The Antigens Manager acts as the nerve center of SR-DCA's operations management. It is in charge of controlling the reception and delivery of inputs and outputs from and to the routing protocol, respectively.

Innate unit. In response to a Q.R.P entry, the Antigens Manager extracts an antigen from the packet. Each retrieved antigen reflects the packet's IP address. In the next step, the Antigens Manager determines whether or not the antigen is present in the entire gene list (Global-List).

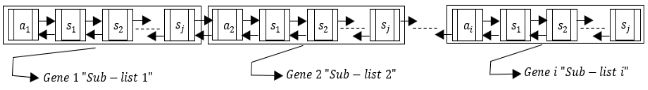

Figure 4. Genes store component

The Genes Store component (Figure 4) contains a list of various genes, which is represented by the (Global-List) variable. For each gene, a sub list from the Global-List is

defined as (Sub-List), which consists of one antigen "a_i" and many associated signals (PAMP, safe, danger, and inflammatory) that are specific to that gene "s_j".
where, "i" is the number of antigens in the Global-List and "j" is the number of signals per Sub-List. The signals in each gene, on the other hand, are calculated from a variety of effects produced by the antigen's packet in terms of both its rate and the breaks of link it caused.

The Antigens Manager examines the input antigen, if an antigen is found in the Global-List, then the index of the stored antigen is got and the input antigen needs to be checked. Otherwise, a new gene list for that antigen and its associated signals is generated. The Antigens Manager checks if the input antigen has ever been classified as malicious in the Malicious Antigen List (M.A.L).

Adaptive processing unit. In order to make use of the M.A.L, it must be placed in the MT-Cells (Memory T-Cells). M.A.L is a collection of malicious antigen profiles. A malicious antigen and its corresponding existence counter "C" are included in each profile. This counter calculates how many times the antigen is identified and classified as malicious in the SR-DCA. If the Antigens Manager discovers a counter associated with the antigen in M.A.L that is higher than a specified threshold "t", the input antigen is deemed malicious and a context of "1" is used to symbolize it. A consequence of this, is that the associated routing packet is regarded as an abnormal packet. The routing protocol subsequently loses the packet and does not reply to the source node, causing the package to be deleted.

For the input antigen, two different scenarios could happen in the abnormal detection of DCs.

(1) The first scenario occurs, when the input antigen is not detected in MT-Cells.

(2) The second scenario occurs when the input antigen is discovered, but its counter of existence is less than a particular threshold.

It should be noted in this part that the MT-List threshold "t" value is very significant and difficult to be calculated, because if "C" surpasses the tested input antigen, the antigen is regarded dangerous each time it appears in SR-DCA. Although the use of MT-Cells may expedite response times, its implementation should be done with caution.

The immature DC differentiates into a semi-mature DC, when the antigen context is "0". On the other hand, the DC differs from the mature DC, if the context is "1". Regardless of the state, by following the maturity, the DC should move directly to the adaptive processing unit, where it may regulate the immune response of the NT-Cell, which is controlled by the NT-Cells component.

In the first instance (context=0), DC causes the NT-Cell to become an ST-Cell by causing it to a process of differentiation. ST-Cells are notified to examine MT-Cells for a benign antigen and reduce "C" if such a situation occurs. Conversely, in the second instance, the NT-Cell develops into an MT-Cell inside the MT-Cells component. It is in both instances that the stimulated NT-Cell returns the antigen context to the Antigens Manager located in the Monitoring and security unit. Due to this, the Antigens manager provides results (either 1 or 0) to the routing protocol. The result of "1" should be interpreted by the routing protocol as the presence of an attack produced by the antigen packet, and the result of "0" should be interpreted as the absence of an attack.

Algorithms 2 and 3 present SR-DCA pseudo-code to describe Figure 3's model steps.

Algorithm_2 SR-DCA algorithm (the main algorithm)
Input: Inputs packets.
Output: Antigen and its context.

```
While (Q.R.P  !=Null) do
  Extract antigen ($a_i$);
    If the antigen is present in the Global-List then
      Get the index of the stored antigen;
      Check the input antigen;
        If (($a_i$ is found in M.A.L) & (C>t)) then
          Context of antigen=1;
          C++; //Increase the antigen counter for M.A.L
        Else
          Calculate the signals;
          Signals storage;
          Call Algorithm_3;
        End If
    Else
      Calculate the signals;
      Initialize the list of gene;
      Adding genes to the list;
      Call Algorithm_3;
    End If
End while
```

Algorithm_3 Anomaly detection trigger by DCs.
Input: Antigen and its associated signals.
Output: Antigen and its context.

```
Initialize DC;
If (C>t) then
    Context of antigen = 1;
    If $a_i$ is not found in M.A.L then
        Add $a_i$ to M.A.L;
        Create (C);
        C=1;
    Else
        C++;
    End If
Else
    Context of antigen = 0;
    If $a_i$ is not found in M.A.L then
        Decrease antigen counter;
    End If
End If
Destroy DC;
Return the "Context of antigen" to algorithm 2;
```

4.3 Description and functioning

4.3.1 Optimization-PeSOA procedure in FANETs

The specifics of the proposed model and its pseudocode are described in the steps below: (Figure 5 and Algorithm 4)

(1) Step 1 (Area Definition): The first step is to determine the entire region (the total area) covered by the network and split it into Sub-areas.

(2) Step 2 (Drone population): Define the population of UAVs and the area.

(3) Step 3 (Group Formation) (the first characteristic of PeSOA): Is the process of dividing the UAVs into groups that were determined in step 2. The division of the group takes place as follows:

a) Divide UAVs equally according to the number of sub-areas, for example, 6 UAVs with 2 sub-areas implies that 3 UAVs are required for each area.

b) Otherwise, create as many equally dispersed groups as possible and place the remaining UAVs in the final group, for example, 7 UAVs with 3 sub-areas equals group formations of: Group 1=2 UAVs, Group 2=2 UAVs and Group 3=3 UAVs.

(4) Step 4 (Group Head): Define the UAV-leader for each group to communicate with the central command and to communicate within intra-group.

(5) Step 5 (Boundaries for velocity and position): For each UAV group and sub-area, define the minimum and maximum limits for velocity (v_{max}, v_{min}) and position (x_{max}, x_{min}).

(6) Step 6 (Search start): Coordinates for a beacon are provided to the UAV-leaders for their particular sub-area, from which the UAV group will launch its search operation.

(7) Step 7 (Search within a group): In order to carry out its communications, each drone conducts a search inside its group to find the target drones in a sub-area. The search is carried out using the Eq. (1) from paragraph 3.2.2.

(8) Step 8 (Information sharing): At the end of each time interval "t", the UAV-leader gathers certain information (such as remaining battery capacity and recorded track coordinates) from neighboring UAVs in the group and sends it to the command center (PeSOA inter-group information sharing strategy).

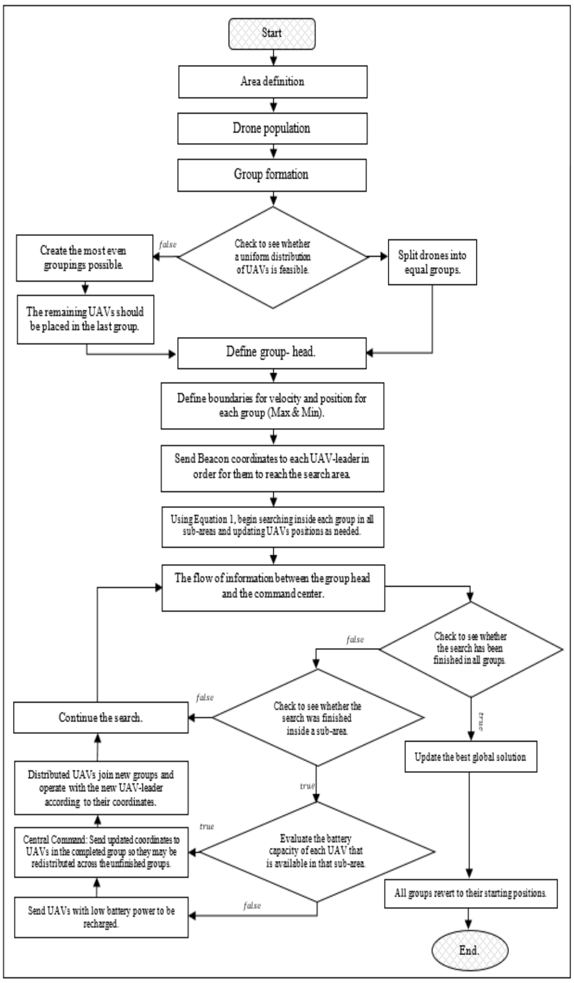
Start
Area definition
Drone population
Group formation
Check to see whether a uniform distribution of UAVs is feasible.
false
Create the most even groupings possible.
The remaining UAVs should be placed in the last group.
Split drones into equal groups.
Define group- head.
Define boundaries for velocity and position for each group (Max & Min).
Send Beacon coordinates to each UAV-leader in order for them to reach the search area.
Using Equation 1, begin searching inside each group in all sub-areas and updating UAVs positions as needed.
The flow of information between the group head and the command center.
Check to see whether the search has been finished in all groups.
false
true
Check to see whether the search was finished inside a sub-area.
false
true
Continue the search.
Update the best global solution
Distributed UAVs join new groups and operate with the new UAV-leader according to their coordinates.
Central Command: Send updated coordinates to UAVs in the completed group so they may be redistributed across the unfinished groups.
true
Evaluate the battery capacity of each UAV that is available in that sub-area.
false
Send UAVs with low battery power to be recharged.
All groups revert to their starting positions.
End.

Figure 5. Flowchart of the Penguin-AIS-Routing model

(9) Step 9 (Inter-group movement of UAVs) (the second characteristic of PeSOA): The inter-group exchange is dependent on the battery capacity and the criteria of the area search completion. The steps needed to complete this operation are as follows:

a) Following the conclusion of a search in a particular sub-area, the command center is responsible for determining whether or not the battery capacity is accessible in the UAVs belonging to that specific group.

b) Ensure that the battery is not completely exhausted (as in the case of penguin oxygen) and then verify the status of the other groups, otherwise, send the drones with low battery capacity for recharging.

c) First, determine if other groups are still doing searches, and if so, instruct the group-head to distribute all of the UAVs, including itself, to the new coordinates so that it may join the other groups still conducting searches.

d) After joining the new groups, UAVs will begin operating under the supervision of the new UAV-leader of that group.

(10) Step 10 (Finalizing research): After all of the groups have completed their particular sub-area searches, and the overall search for the whole area has been completed, all of the UAVs will return to their starting points and the search will be completed.

Algorithm_4: *Penguin-AIS-Routing*

```
Create an initialized total search area by dividing it into subareas;
Set the maximum "$v_{max}$" and minimum "$v_{min}$" velocities, as well as the maximum "$x_{max}$" and minimum "$x_{min}$" position limits, for the UAV population;
Initialize the battery capacity for each UAV;
If even distribution is feasible in the set of UAVs then
    Divide UAVs into "G" groups equally; $//G = \{g_1, g_2, \ldots, g_i\}$
Else
    Form the most equally distributed groups possible, then put the remaining UAVs in the last group;
End If
Identify the head of each group;
                // Initialize search in each sub-area
While exploration is completed in all groups do
    For each group "$g_i$" do
        For each UAV in "$g_i$" do
            Start search;
            Update the UAV position using Eq. (1);
        End for
        Update the fitness function for $g_i$ using Eqns. (2) & (3);
            // Similar to the oxygen approach, check the battery capacity
        UAV-leader updates after interval "$t$": battery capacity, finished coordinates and number of targets found using Eq. (2);
            //Check to see whether the search has been finished in all groups.
        If (G = search has not been finished) then
            If the search is finished inside a subarea "$g_i$" then
                For each UAV in "$g_i$" do
                    If (battery capacity > threshold) then
                        Send the UAV to the new search group and instruct it to resume it search as before;
                    Else
                        Send the UAV for recharging before joining the search in the new group;
                    End if
                End for
            Else
                Continue the search in the same subarea;
            End if
        Else
            End search;
        End if
    End for
    Update the best global solution;
    Update the fitness value of each group membership function using Eq. (4);
    Redistribute the UAV by membership function to groups;
    Leave the group unless there are no members;
End while
End.
```

4.4 Secure and efficient bio-inspired routing protocol

4.4.1 Integration with AODV Routing Protocol

Although Penguin-AIS can be used with a variety of FANET routing protocols, it is considerably more compatible with reactive routing systems since RREQ is only transmitted when a UAV intends to communicate with a destination UAV. As a consequence, it produces superior outcomes, particularly in terms of security, performance and routing efficiency.

Actually, the major emphasis is on network layer implementation, the protocol presented here is an extension of the Ad hoc On-Demand Distance Vector (AODV) protocol [42], a thorough description of this protocol “Penguin-AIS-AODV” is provided below.

This section focuses on the use of the SR-DCA algorithm in order to improve the security of Penguin-AIS-AODV, in particular to prevent most attacks in FANETs, such as packet-loss attacks and resource-consumption attacks. When the Penguin-AIS-AODV gets a RREQ, it must first examine the context of the RREQ in order to establish its source, that is, whether the RREQ was provided by an attacker or a legal source node, before proceeding. Therefore, the SR-DCA protects the Penguin-AIS-AODV by processing the fictitious request for response packets (RREQs), which take resources from the destination nodes and from the network itself. The SR-DCA also conducts local anomaly intrusion detection in each UAV, without requiring any information about collaboration between the UAVs in the network.

The SR-DCA puts the received RREQs in the Q.R.P and processes them in the order in which they were received, using the FIFO queuing system. When this is done successfully, the SR-DCA extracts the RREQ antigen and its input signals with the help of the Antigens Manager. Each recovered antigen has a unique IP address that corresponds to the packet's original IP address. At the same time, the Antigens Manager computes the PAMP, safe, danger, and inflammatory signals depending on the processed RREQ's rate and the link breaks it induced.

The antigen of each RREQ and its associated signals are combined in the Genes Store's gene list. The presence of a new gene causes the SR-DCA to generate a new DC in the Innate unit, which continually checks the gene list for new input genes. Each DC manipulates a single antigen but not a single gene. It is possible that the Genes Store will have genes that have the same antigen but distinct signals. However, the technique does not require that an input antigen be repeated in several genes on the gene list. Once a DC has been generated, it manipulates the newly produced gene in the list of genes.

Finally, the context of the RREQ is determined depending on "*C*" and "*t*" according to the SR-DCA algorithm, as indicated in the part 3 of section 4.2.2. If a suspect UAV is determined to be a malicious UAV, it will be added to the list of malicious UAVs and the findings are shared with all neighbors. New routes won't include the rogue node, so it can't communicate with the rest of the network.

4.4.2 Complexity analysis of the Penguin-AIS model

It is vital to note that complexity is a key criterion for evaluating the performance of algorithms. The time and space complexity of the suggested model are detailed in the following section.

Time Complexity. The following processes are the most important factors influencing the time complexity of the Penguin-AIS model:

(1) The process of initializing a population takes $O(n)$ time, where "n" is the size of the population to be initialized.

(2) Assuming that $Max_{Iteration}$ is the maximum number of evolutionary iterations required to simulate the proposed algorithm, each group's fitness needs $O(Max_{Iteration} * n * e)$ time, where "e" shows the entropy function.

(3) The method of position updating has a time complexity $O(Max_{Iteration} * n * dim)$, where "$dim$" denotes the space dimension.

(4) The Penguin-AIS-Routing algorithm is run until the termination requirements are fulfilled (stopping criterion), which takes $O(k)$ time.

(5) In the Penguin-AIS-Security algorithm, the “SR-DCA” procedure requires $O(k')$ as complexity time. It seems to be less complicated, since it just includes one “WHILE”.

Hence, the overall time complexity needs:
$O(Initialization) + O(Fitness\ function) + O(Position\ update) + O(\text{Penguin} - \text{AIS} - \text{Routing}) + O(\text{Penguin} - \text{AIS} - \text{Security})$, meaning:
$O(n) + O(Max_{Iteration} * n * e) + O(Max_{Iteration} * n * dim) + O(k) + O(k') \Rightarrow O(k * n\big(1 + Max_{Iteration}(e + dim)\big) + k')$.

Space complexity. An algorithm's space complexity is the maximum amount of space used at any moment that is taken into account during the initialization step. Thus, Penguin-AIS algorithm's overall space complexity is $O(n*dim)$.

5. SIMULATION RESULTS AND DISCUSSIONS

This study includes a series of experiments designed to test the accuracy of the proposed approach. The efficiency of the proposed protocol as well as the analyze of its security performance were assessed using the NS-3 simulator [43].

5.1 Experiment settings

Table 1. Simulation parameters

	Parameter	Value
	Simulator	*NS-3.26*
Physical & MAC	Wireless propagation model	*Free Space*
	Frequency band	5 GHz
	Transmission power	35 dbm
	Data link antenna	*Omni-directional*
	MAC layer protocol	*IEEE 802.11*
	Sending capacity	*6 Mbps*
Routing	Mobility model	*Random*
	Radio range	*300 m*
	Packet size	*512 Bytes*
	Packet type	*TCP*
	Traffic type	*CBR*
	Queue management and scheduling	*DropTail-FIFO*
	Queue capacity	*50 packets*
	Energy level at start time	*1000 Joules*
Scenario	Number of UAVs	*100 UAVs*
	Simulated area	*(2000*2000) sq.m*
	Movement	*Random Waypoint*
	UAV Velocity (Min – Max)	*(0-50) m/s*
	Simulation duration	*1000 s*
	Pause time	*10 s*
	Maximum malicious UAVs	*20%*
	Type of attack	Coordinated attack
	The specified threshold *"t"*	3 times
	$\lambda_1, w_1\ \lambda_2, w_2\ \lambda_3, w_3$	1⁄3

With the goal of evaluating the Penguin-AIS-AODV protocol's performance in light of the network's scalability and dynamic nature. Several scenarios are examined under different networking conditions by altering the settings depicted in Table 1.

5.1.1 Defining some initial parameters

Different experimental setups and test scenarios with varying performance and security settings, as well as contextual factors, are built to assess the adaptivity, efficiency, and security of the proposed routing method. The simulation results were analyzed and compared with AODV, AntHocNet, BeeHocNet, and Favorite-AODV protocols proposed in studies [6, 42, 44, 45] respectively.

The security parameter test scenarios involve injecting a varied number of malicious UAVs with various network topologies to determine the route's trustworthiness. On the other hand, test cases for contextual characteristics are developed using a variety of UAVs with different processing capability.

The performance test cases have different performance metrics that are [6]: Packet Delivery Ratio (PDR), End to End Delay (EED), Throughput, Remaining Energy, and Work Done Capacity [46]. Other tests are also done to see how well SR-DCA does at keeping information secure used by the Penguin-AIS protocol. The following performance metrics take into consideration, namely [47, 48]: False positive Rate (FP), False Negative Rate (FN), Attack Detection Rate (DR), and Accuracy.

In order to evaluate and compare the routing protocol's performance in a noisy environment where random packet losses may occur, an error model is created for the UAVs during simulation. The following is a simplified illustration of the error model.

Error model. In order to produce random noise in the simulation, The following actions are taken:

(1) It is necessary to calculate the distance "*d*" between the transmitter and receiver.

(2) The path-loss model is used to determine the Signal to Noise Ratio (SNR) based on the computed distance. Path loss may be computed mathematically as follows:

$$P_r = \frac{P_t * G_r * G_t}{[{}^{4\pi d}/_{\lambda}]^2 * L} \qquad (19)$$

where, $P_{t(r)}$ represents the transmitter (receiver) power, $G_{t(r)}$ represents the system gain of the transmitter (receiver), "*d*" is the transmitter-receiver distance, "λ" is the signal wavelength, and "*L*" is the system (transmitter-receiver) loss.

5.2.2 Experimental results and discussion

To make the findings more realistic, the suggested algorithm is presented through its paces, using the aforementioned measures. The results are broken down into two main tests, the first test is about optimizing routing (Penguin-AIS-Routing) using the PeSOA algorithm and its attributes, while the second is about making sure that the routing is secure (Penguin-AIS-Security), which improves the protocol's quality of service, packet delivery rate, and End-to End delay.

Test 1. The following PeSOA characteristics will be used during this test: Area division, UAV group search, and intergroup UAV exchange. The findings (Figures 6, 7, and 8) are obtained by dividing the area using the Voronoi diagram [36], which results in an uneven area split to create a more realistic scenario.

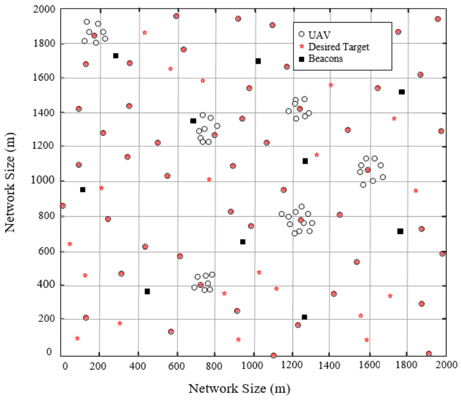

Figure 6. Results at 80 iterations for PeSOA without groups and sub-area division (2000*2000) m^2

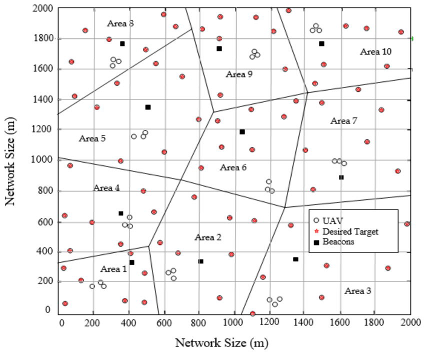

Figure 7. Results at 80 iterations for PeSOA with sub-area division (2000*2000) m^2

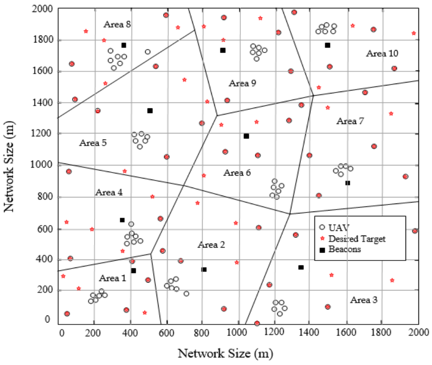

Figure 8. Results at 44 iterations for PeSOA with sub-area division (2000*2000) m^2

The connection between the number of targets discovered and the total number of iterations is shown in Figure 9. It is evident that there is a direct link between the number of iterations and the number of objectives attained, the number of iterations increases accordingly with the number of targets to be identified, and vice versa. In most cases. If there are several objectives in a multi-objective optimization problem, the number of non-inferior solutions will rise exponentially as the number of targets becomes larger.

Due to the random movement of UAVs, PeSOA simulation results may differ somewhat from one another, but the overall trend is the same. This is mostly due to the fact that with area division and UAV grouping, the search area is reduced, hence boosting the efficiency of the UAVs and estimating the target positions with greater accuracy.

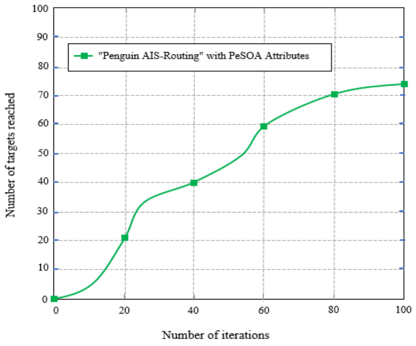

Figure 9. Number of located targets Vs. total number of iterations

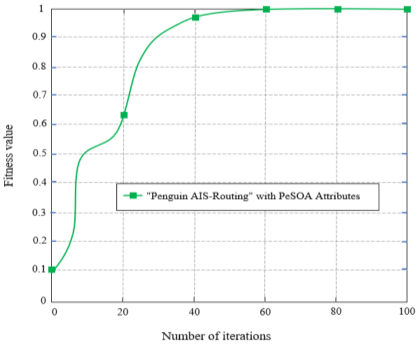

Figure 10. Convergence graph of the fitness function for Penguin-AIS-Routing using PeSOA attributes

Figure 10 depicts the relationship between the number of iterations for Penguins-AIS-Routing and the convergence of the optimal fitness value for the objective function provided by Eq. (18). Using the previously mentioned optimization technique with a number of iterations equal to 100 and a fitness function, the convergence graph is generated. By looking at the graph in Figure 11, it can be seen that the proposed model gets closer to convergence quicker and achieves a higher overall fitness value for the goal function.

Test 2. Following the implementation of the proposed protocol, the simulation is run three times respectively in terms of both malicious UAVs ratio and the maximum UAVs velocity. This simulation is assessed using the metrics listed above, in which some UAVs misbehave by deleting or changing data packets.

As shown in the Figure 11, the proposed method has a high PDR because, it can quickly detect any lethal attack while preventing UAVs from any intra-exchange, and consequently getting adapted to such situation, since this is quite unlikely, PDR rises as a result. When the proportion of attacks is equal to 20%, the suggested technique, BeeHocNet, AntHocNet and AODV have efficiencies of 87%, 80%, 72% and 53%, respectively. In this way, the Penguin-AIS technique may achieve high performance due to the efficient collaboration between the UAVs of the network.

In general, the PDR rises as the simulation velocity increases. Figure 12 shows that the PDR value of the suggested technique is almost steady even under variable velocity conditions (81% at 20 m/s, 80% at 50 m/s). As a result, the change in velocity has no influence on the PDR. Due to the fact that the attacker UAV is unable to engage in the network, communication continues as if there is no attack taking place in the network. On the other hand, the performance of AODV, drops significantly as the velocity of the network increases because the high velocity impacts the stability of the AODV topology, which is required to build the routing path.

The average EED may be used to gauge the network's efficiency, and this value should be as low as feasible. A look at the illustration in Figure 13 reveals that the proposed FANET routing scheme has an average EED that is significantly lower than that of other routing schemes. This is due to the fact that the groups-heads are responsible for maintaining their own group of UAVs, which on the one hand, results in lower overhead messages and EED. On the other hand, when intermediate UAVs pick the next hop, they will not take into account the malicious UAVs, allowing them to save valuable time in the process. However, the average delay in AODV clearly increases (Queuing delays and retransmission delays are mostly responsible for this average delay).

Further, as shown in Figure 14, the average EED with the four schemes increases usually with the increasing speed. The findings reveal that UAVs mobility has a significant influence on routing in FANETs. It is possible that route interruptions will occur on a regular basis in the case of high-speed mobility. Because of this, using optimal routing (Penguin-AIS-AODV) throughout the route discovery phase will significantly enhance the network's overall stability.

Throughput is calculated by measuring the number of packets transmitted per second, which is analyzed in Figures 15 and 16. Figure 15 clearly shows that the rising number of attacks on all the four protocols has a negative influence on throughput. As the number of malicious UAVs grows, the throughput for AODV falls, because the malicious UAVs prevent packets from reaching their destination. However, because of the efficiency of the proposed protocol, even if the number of malicious UAVs rises, the throughput does not suffer from any significant reduction in performance.

The obtained results show that there is no significant difference in terms of throughput between Penguin-AIS-AODV and that of AntHocNet and BeeHocNet, with the exception of the fact that Penguin-AIS-AODV is able to maintain a stable throughput by the end of the simulation even when the number of attacks is increasing. This stability might be attributed to the auto-adaptive nature of the intrusion detection system that has been incorporated in the system.

As seen in Figure 16, the throughput is almost steady in the proposed scheme while operating at maximum velocity, demonstrating that this technique has excellent dynamics.

As shown in Figure 17, there are some malicious UAVs that vary between 0% and 20% among the UAVs in the network, while the other UAVs in the network behave correctly. Because malicious UAVs either do not participate in the route discovery phase in the proposed protocol or cannot properly execute data packet forwarding. Experimental results show that even if individual malicious UAVs seriously affect network performance, the proposed security mechanism remains active in order to invite and encourage other UAVs to transmit data packets. According to the simulation results, the proposed routing model can generate energy savings and extend the network lifetime. It is then necessary that the security scheme adapted to malicious behavior imposes the execution of the transfer of data packets on the routing protocols in the FANETs.

It can be shown in Figure 18 that increasing the number of UAVs enhances the Work Done Capacity in all the schemes. Bit per joule is an important factor to show how long a network can last. It shows how much energy is needed to get a good amount of Work Done Capacity. Penguin-AIS-AODV has the highest value, which means it can make the network last a lot longer.

Figure 19 depicts the false positive rate (FP) in the four protocols compared to harmful UAV rates for Penguin-AIS-AODV, Favorite-AODV, and AODV. The produced false positive rate of the suggested technique has grown at a slower and lower rate than other methods, when the malicious UAV rate climbs from 5 to 20%. The reason for the superiority of the suggested technique is the rapid identification of malicious UAVs and their elimination with the assistance of regular UAVs via the use of an AIS-based self-protective mechanism. The aforementioned procedure is carried out with the help of pre-programmed rules that have been kept in the safety memory.

As seen in the plot displayed in Figure 20, the false negative rate (FN) has shown little growth while this value is much larger for Favorite-AODV and AODV, respectively. The proposed technique has a higher FN since it includes a self-protection and self-adaptation mechanism, which results in a greater level of communication security between UAVs. Using simulation results, it can be shown that when the proportion of malicious UAVs is 10%, 15%, and 20%, the FN output is 8%, 13% and 20% for each of these percentages.

As seen in Figure 21, the detection rate (DR) has reduced in all the four tested approaches, particularly when the number of attackers is large. It has been shown that the suggested technique can identify all of the aforementioned attacks with a detection rate greater than 90%. The reason the proposed scheme is better is that it can quickly identify and remove malicious UAVs using the mapping that is done. This leads to the identification of malicious UAVs and the removal of them from the operation process.

Figure 22 depicts the accuracy performance of the proposed intrusion detection and prevention model, as well as a comparison with earlier research. The accuracy of the suggested model is greater when compared to two other models, as can be seen in the graph below. According to the results of the experimental assessment, the suggested routing protocol is capable of adapting to the shifting needs and dynamic behavior of the FANET environment effectively and efficiently. As an added benefit, it constantly enhances the overall performance of the network and assures safe end-to-end transmission of packets over an optimal and secure route when compared to the standard AODV routing method.

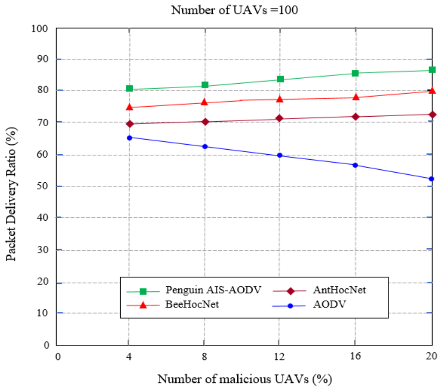

Figure 11. PDR with different number of malicious UAVs

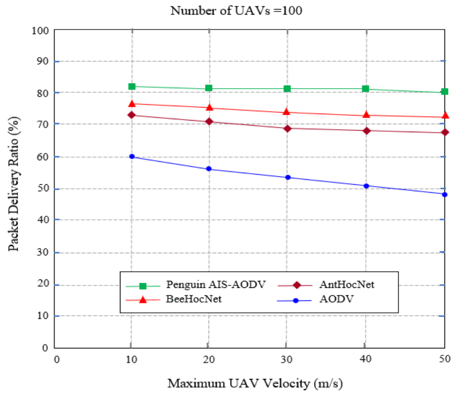

Figure 12. PDR at different velocity levels

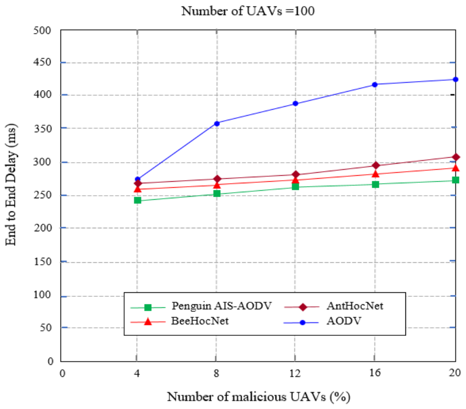

Figure 13. EED with different number of malicious UAVs

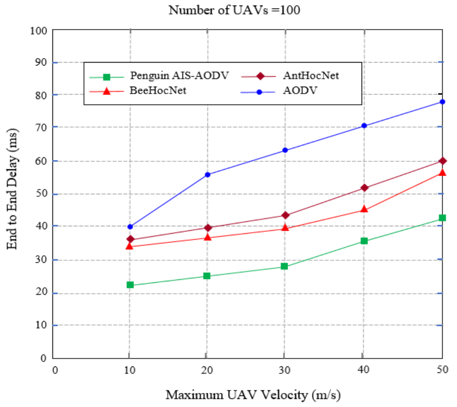

Figure 14. EED at different velocity levels

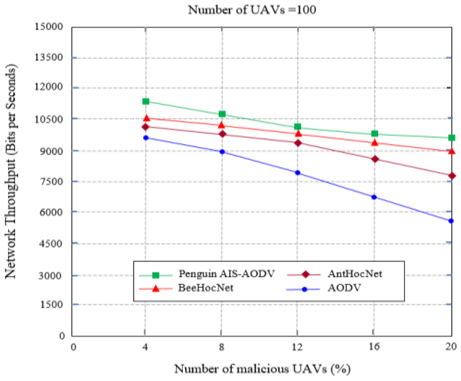

Figure 15. Network Throughput with different number of malicious UAVs

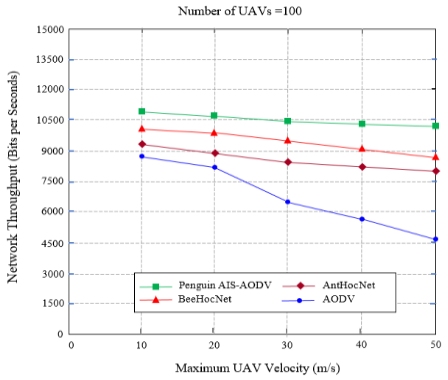

Figure 16. Network Throughput at different velocity levels

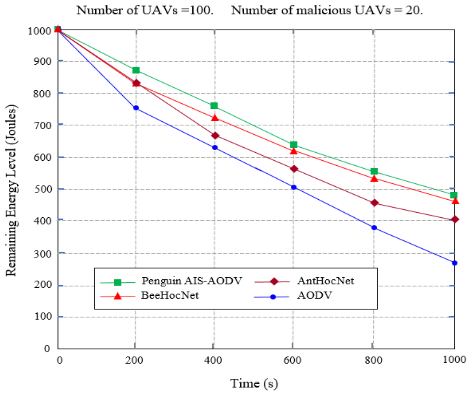

Figure 17. Remaining Energy Level vs. Time

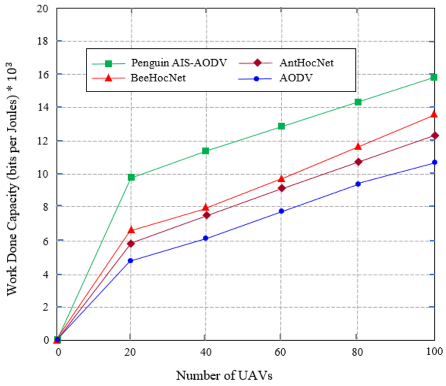

Figure 18. Work Done Capacity vs number of UAVs

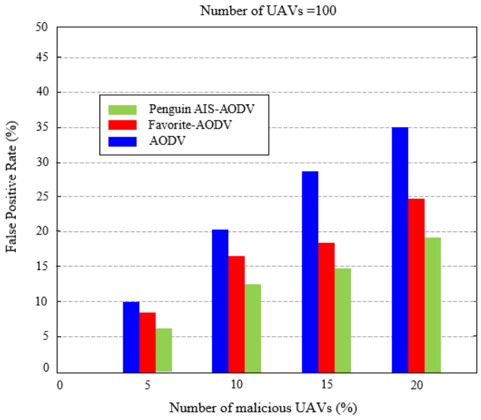

Figure 19. False Positive rate with different number of malicious UAVs

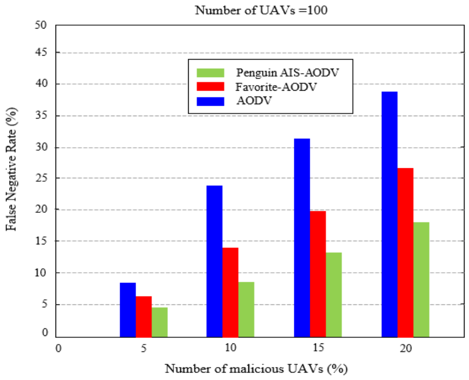

Figure 20. False Negative rate with different number of malicious UAVs

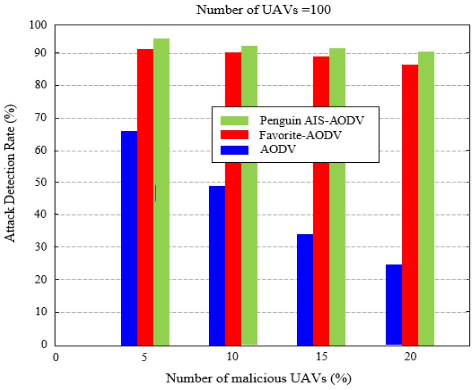

Figure 21. Detection Rate with different number of malicious UAVs

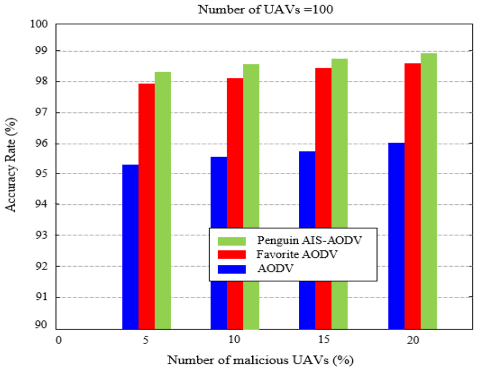

Figure 22. Accuracy Rate with different number of malicious UAVs

6. CONCLUSIONS AND FUTURE WORK

This paper came up with a bio-inspired routing model (Penguin-AIS) for FANETs that is both adaptable and secure. The suggested paradigm is divided into two phases. The model's first phase is concerned with routing (Penguin-AIS-Routing), while the second phase is concerned with protecting the transmitted data against the different attacks (Penguin-AIS-Security).

The first phase exploits the optimization technique "PeSOA" which is based on the collaborative foraging strategy utilized by penguins, while also taking into consideration some of the issues that may emerge in the FANETs. The Penguin-

AIS-Routing is likewise concerned with finding the most optimal path between the initiator and the destination. This is accomplished by exploiting the features of the PeSOA algorithm and considering groups of penguins as UAVs.

The security phase of the Penguin-AIS model is all about protecting data that are sent by developing an artificial immune algorithm. In order to achieve this goal, the dendritic cell (DC) model is used in the HIS. This allows the HIS to recognize and detect all kinds of malicious attacks in FANETs.

This model provides a flexible and feasible approach that has been validated on a well-known set of benchmark functions that have been widely used in the literature. A performance comparison with other algorithms such as AntHocNet, BeeHocNet, Favorite-AODV, and AODV is made using the NS-3 simulator. The experimental findings reveal that the proposed strategy is ranked first in most metrics such as: Packet delivery ratio, End to End latency, Throughput, False Positive rate, False Negative rate, Detection Rate, and Accuracy Rate.

As future perspective, this work could get extended to be used with various routing systems, it would be interesting to compare the obtained results with other recent works as well. It would also be a good idea to present a new framework based on the suggested routing protocol's behavior, which takes into account a variety of mobility use cases.

REFERENCES

[1] 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(2): 1-14. https://doi.org/10.1016/j.adhoc.2018.09.004

[2] Bekmezci, I., Sahingoz, O.K., Temel, Ş. (2013). Flying Ad-Hoc networks (FANETs): A survey. Ad Hoc Networks, 11(3): 1254-1270. https://doi.org/10.1016/j.adhoc.2012.12.004

[3] Sahingoz, O.K. (2014). Networking models in flying ad-hoc networks (FANETs): Concepts and challenges. Journal of Intelligent & Robotic Systems, 74(1-2): 513-527. https://doi.org/10.1007/s10846-013-9959-7

[4] Qureshi, K.N., Sandila, M.A.S., Javed, I.T., Margaria, T., Aslam, L. (2022). Authentication scheme for unmanned aerial vehicles based internet of vehicles networks. Egyptian Informatics Journal, 23(1): 83-93. https://doi.org/10.1016/j.eij.2021.07.001

[5] Zhou, S., Xia, H. (2015). Node trust assessment and prediction in mobile ad-hoc networks. International Journal of Security and Its Applications, 9(10): 361-372. https://doi.org/10.14257/IJSIA.2015.9.10.33

[6] Beghriche, A., Bilami, A. (2018). A fuzzy trust-based routing model for mitigating the misbehaving nodes in mobile Ad hoc networks. International Journal of Intelligent Computing and Cybernetics, 11(2): 309-340. https://doi.org/10.1108/IJICC-04-2017-0038

[7] Haque, M.S., Chowdhury, M.U. (2019). Ad-Hoc framework for efficient network security for unmanned aerial vehicles (UAV). In Proceedings of the 5th International Conference on Future Network Systems and Security - FNSS 2019, CCIS 1113, Springer, Cham, Switzerland, pp. 23-36. https://doi.org/10.1007/978-3-030-34353-8_2

[8] Khan, M.A., Qureshi, I.M., Ullah, I., Khan. S., Khanzada, F., Noor, F. (2020). An efficient and provably secure certificateless blind signature scheme for flying Ad-Hoc network based on multi-access edge computing. Electronics, 9(1): 30. https://doi.org/10.3390/electronics9010030

[9] Singh, K., Verma, A.K. (2018). A trust model for effective cooperation in flying ad hoc networks using genetic algorithm. In 2018 International Conference on Communication and Signal Processing (ICCSP), pp. 0491-0495. https://doi.org/10.1109/ICCSP.2018.8524558

[10] Singh, K., Verma, A.K. (2020). TBCS: A trust based clustering scheme for secure communication in flying Ad-Hoc network. Wireless Personal Communications, 114(4): 3173-3196. https://doi.org/10.1007/s11277-020-07523-8

[11] Barka, E., Kerrache, C.A., Hussain, R., Lagraa, N., Lakas, A., Bouk, S.H. (2018). A trusted lightweight communication strategy for flying named data networking. Sensors, 18(8): 2683. https://doi.org/10.3390/s18082683

[12] Wang, G., Lee, B.S., Ahn, J.Y. (2018). Secure pairwise key establishments for flying ad hoc networks. In Proceedings of the International Conference on Computational Science and Computational Intelligence (CSCI), pp. 1450-1451. https://doi.org/10.1109/CSCI46756.2018.00285

[13] Maxa, J.A., Mahmoud, M.S.B., Larrieu, N. (2016). Extended verification of secure UAANET routing protocol. In Proceedings of the IEEE/AIAA 35th DASC Digital Avionics Systems Conference (DASC'16), pp. 1-16. https://doi.org/10.1109/DASC.2016.7777970

[14] Beghriche, A., Bilami, A. (2012). RTIC: Reputation and trust evaluation based on fuzzy LogIC system for secure routing in mobile ad-hoc networks. In Proceedings of Networked Digital Technologies, Communications in Computer and Information Science Series of Springer LNCS, Springer-Verlag Berlin Heidelberg, 293: 620-634. https://doi.org/10.1007/978-3-642-30507-8_51

[15] Rathore, H. (2016). Mapping biological systems to network systems. Springer. https://doi.org/10.1007/978-3-319-29782-8

[16] Dressler, F., Akan, O.B. (2010). A survey on bio-inspired networking. Computer Networks, 54(6): 881-900. https://doi.org/10.1016/j.comnet.2009.10.024

[17] Wang, H., Zheng, R., Li, X., Liu, D. (2006). A bio-inspired multidimensional network security model. In Proceedings of First International Multi-Symposiums on Computer and Computational Sciences (IMSCCS'06), pp. 3-7. https://doi.org/10.1109/IMSCCS.2006.140

[18] Roy, S., Das, S.K. (2019). A bio-inspired approach to design robust and energy-efficient communication network topologies. In Proceedings of IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp. 449-450. https://doi.org/10.1109/PERCOMW.2019.8730691

[19] Conti, V., Militello, C., Rundo, L., Vitabile, S. (2021). A novel bio-inspired approach for high-performance management in service-oriented networks. IEEE Transactions on Emerging Topics in Computing, 9(4): 1709-1722. https://doi.org/10.1109/tetc.2020.3018312

[20] Khan, A., Aftab, F., Zhang, Z. (2019). BICSF: Bio-Inspired clustering scheme for FANETs. IEEE Access, 7:

31446-31456. https://doi.org/10.1109/ACCESS.2019.2902940

[21] Goswami, M., Arya, R., Prateek. (2020). UAV communication in FANETs with metaheuristic techniques. In proceedings of Next Generation Information Processing System, Proceedings of ICCET 2020, Springer, 2: 1-11. https://doi.org/10.1007/978-981-15-4851-2_1

[22] Leonov, A.V. (2016). Modeling of bio-inspired algorithms AntHocNet and BeeAdHoc for flying ad hoc networks (FANETS). In 2016 13th International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE), pp. 90-99. https://doi.org/10.1109/APEIE.2016.7806419

[23] De Castro, L.N., Timmis, J. (2002). Artificial immune systems: A new computational intelligence approach. Springer-Verlag, Heidelberg. https://link.springer.com/book/9781852335946

[24] Khannous, A., Elouaai, F., Rghioui, A., Bouhorma, M. (2016). MANET: Securing AODV based on a combined immune theories algorithm (CITA). International Journal of Security and its Applications, 10(9): 211-228. https://doi.org/10.14257/ijsia.2016.10.9.21

[25] Gheraibia, Y., Moussaoui, A. (2013). Penguins search optimization algorithm (PeSOA). In Proceedings of the International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems, IEA/AIE Recent Trends in Applied Artificial Intelligence, pp. 222-231. https://doi.org/10.1007/978-3-642-38577-3_23

[26] Gheraibia, Y., Moussaoui, A., Yin, P.Y., Papadopoulos, Y., Maazouzi, S. (2019). PeSOA: Penguins search optimisation algorithm for global optimisation problems. The International Arab Journal of Information Technology, 16(3): 371-379. https://doi.org/10.48550/arXiv.1809.09895

[27] He, S., Wu, Q., Liu, J., Hu, W., Qin, B.B., Li, Y.N. (2017). Secure communications in unmanned aerial vehicle network. In Proceedings of the International Conference on Information Security Practice and Experience, Springer International Publishing LNCS, pp. 601-620. https://doi.org/10.1007/978-3-319-72359-4_37

[28] He, D., Chan, S., Guizani, M. (2017). Drone-assisted public safety networks: the security aspect. IEEE Communications Magazine, 55(8): 218-224. https://doi.org/10.1109/MCOM.2017.1600799CM

[29] Fotohi, R., Ebazadeh, Y., Geshlag, M.S. (2016). A new approach for improvement security against dos attacks in vehicular Ad-Hoc network. International Journal of Advanced Computer Science and Applications, 7(7): 10-16. https://doi.org/10.14569/IJACSA.2016.070702

[30] Forrest, S., Perelson, A.S., Allen, L., Cherukuri, R. (1994). Self-nonself discrimination in a computer. In Proceedings of IEEE Symposium on Research in Security and Privacy, pp. 202-212. https://doi.org/10.1109/RISP.1994.296580

[31] Wang, X., Deshpande, A.S., Dadi, G.B., Salman, B. (2016). Application of clonal selection algorithm in construction site utilization planning optimization. In Procedia Engineering, 145: 267-273. https://doi.org/10.1016/j.proeng.2016.04.073

[32] Jerne, N.K. (1974). Towards a network theory of the immune system. Annales d'immunologie, 125c(N6): 373-389.

[33] Matzinger, P. (1998). An innate sense of danger. Seminars in Immunology, 10(5): 399-415. https://doi.org/10.1006/smim.1998.0143

[34] Mohamed, S.A., Alsaif, O.I., Saleh, I.A. (2022). Intrusion detection network attacks based on whale optimization algorithm. Ingénierie des Systèmes d'Information, 27(3): 441-446. https://doi.org/10.18280/isi.270310

[35] Krishna, K.V.S.S.R., Prakash, B.B. (2019). Intrusion detection system employing multi-level feed forward neural network along with firefly optimization (FMLF2N2). Ingénierie des Systèmes d'Information, 24(2): 139-145. https://doi.org/10.18280/isi.240202

[36] Suseela, S., Eswari, R., Savarimuthu, N. (2022). A voronoi-ant colony-based routing (VoR-Ant-R) algorithm for WMSNs. International Journal of Swarm Intelligence Research, 13(2): 1-19. https://doi.org/10.4018/IJSIR.287546

[37] Temurnikar, A., Verma, P., Dhiman, G. (2022). A PSO enable multi-hop clustering algorithm for VANET. International Journal of Swarm Intelligence Research (IJSIR), 13(2): 1-14. https://doi.org/10.4018/IJSIR.20220401.oa7

[38] Takahashi, A., Sato, K., Nishikawa, J., Watanuki, Y., Naito, Y, (2004). Synchronous diving behavior of Adelie penguins. Journal of Ethology, 22(1): 5-11. https://doi.org/10.1007/s10164-003-0111-1

[39] Thebiga, M., Pramila, S.R. (2021). Adaptable and energy efficacious routing using modified emperor penguin colony optimization multi-faceted metaheuristics algorithm for MANETS. Wireless Personal Communications, 118(2): 1245-1270. https://doi.org/10.1007/s11277-021-08070-6

[40] Hussain, A., Hussain, T., Faisal, F., Ali, I., Khalil, I., Nazir, S., Khan, H.U. (2021). DLSA: Delay and link stability aware routing protocol for flying Ad-Hoc networks (FANETs). Wireless Personal Communications, 121(4): 2609-2634. https://doi.org/10.1007/s11277-021-08839-9

[41] Motran, C.C., Ambrosio, L.F., Volpini, X., Celias, D.P., Cervi, L. (2017). Dendritic cells and parasites: From recognition and activation to immune response instruction. Seminars in Immunopathology, 39(2): 199-213. https://doi.org/10.1007/s00281-016-0588-7

[42] Perkins, C.E., Royer, E.M. (1999). Ad-hoc on-demand distance vector routing. In Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, RFC Editor, United States. https://doi.org/10.1109/MCSA.1999.749281

[43] NS-3 Network Simulator. (2016). http://www.nsnam.org, accessed on Jul. 22, 2022.

[44] Di Caro, G., Ducatelle, F., Gambardella, L.M. (2005). AntHocNet: An adaptive nature-inspired algorithm for routing in mobile ad hoc networks. European Transactions on Telecommunications, 16(5): 443-455. https://doi.org/10.1002/ett.1062

[45] Zhao, B., Ding, Q. (2019). Route discovery in flying ad-hoc network based on bee colony algorithm. In International Conference on Artificial Intelligence and Computer Applications (ICAICA), pp. 364-368. https://doi.org/10.1109/ICAICA.2019.8873436

[46] Khan, I.U., Qureshi, I.M., Aziz, M.A., Cheema, T.A., Shah, S.B.H. (2020). Smart IoT control-based nature inspired energy efficient routing protocol for flying ad

hoc network (FANET). IEEE Access, 8: 56371-56378. https://doi.org/10.1109/ACCESS.2020.2981531

[47] Abdelhaq, M., Alsaqour, R., Algarni, A., Alabdulhafith, A., Alawi, M.A., Taha, A., Sharef, B., Tariq, M. (2020). Human immune-based model for intrusion detection in mobile ad hoc networks. Peer-to-Peer Networking and Applications, 13(5): 1046-1068. https://doi.org/10.1007/s12083-019-00862-9

[48] 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, 26: 1-20. https://doi.org/10.1016/j.vehcom.2020.100267