A survey on position-based routing protocols for Flying Ad hoc Networks (FANETs)

Omar Sami Oubbati a, * , Abderrahmane Lakas b, Fen Zhou c, Mesut Güneş d, Mohamed Bachir Yagoubi a

a Computer Science and Mathematics Laboratory, University of Laghouat, BP 37G, Chordaia Road, 03000 Laghouat, Algeria
b College of Information Technology, United Arab Emirates University, Al Ain, United Arab Emirates
c CERI-LIA, University of Avignon, France
d Institute for Intelligent Cooperating Systems, Faculty of Computer Science Ottovon-Gaericke-University, Germany

ABSTRACT

The last decade has seen a growing interest in the use of Unmanned Aerial Vehicles (UAVs) for various applications and services. UAVs, or drones as referred to, have shown to be efficient in completing complex tasks when organized as ad hoc connected groups, thus forming a Flying Ad hoc Network (FANET). Although similar to Mobile Ad hoc Network (MANET) and Vehicular Ad hoc Network (VANET), FANETs have their own characteristics. One of the main difference is the fact that UAVs in general, but particularly when organized are FANETs, are mission-based, and their mobility models are often dictated by the purpose of their mission and the nature of the task they plan to accomplish. Therefore, routing protocols for FANETs should take into consideration the nature of the applications and services that the UAVs are deployed for, and factor in the mobility models. However, designing routing protocols for FANETs is not an easy task given the highly dynamic topology of FANETs and the flying constraints they are subjected to. Compared to topology-based routing, position-based routing demonstrated high efficiency and resilience to handle the high mobility of FANET nodes. To this end, in this paper, we propose a comprehensive survey of position-based routing protocols for FANETs with their various categories. We propose a classification and a taxonomy of these protocols, including a detailed description of the routing schemes used in each category. We propose a comparative study based on various criteria, and discuss the advantages and weaknesses of each protocol. Furthermore, new challenges for future research are presented, which introduce a new kind of coordination between UAVs and existing VANETs on the ground. The originality of this survey is that it complements the existing surveys on the same theme by providing more details on some aspects that have been addressed only ostensibly by other surveys in the literature.

© 2017 Elsevier Inc. All rights reserved.

1. Introduction

The recent progress of wireless technology has been witnessed in our daily life, particularly because of the vast availability of low-cost Wi-Fi radio interfaces and other devices like GPS, sensors, micro-embedded computers, etc. All these innovative devices have paved the path for the development of small intelligent flying vehicles, e.g., Unmanned Aerial Vehicles (UAVs), leading to the creation of a new kind of network called Flying Ad hoc Network (FANET) [1]. Since the introduction of FANET, different kinds of civilian and military applications have emerged, such as the coordination of rescue teams on the ground [2–4], border supervising [5,6], and autonomous tracking [7–9]. In addition, there are also many civilian applications such as agricultural and yards monitoring, discovering oil fields, and film-making [10–14]. These types of applications need a serious support from several research areas, which require attracting the attention and interest of scientists.

Two kinds of applications of aerial nodes exist [15] (see Fig. 1). First, single-aerial-node applications in which the aerial node (AN) is at the center of a set of base stations localized on the ground. The AN can be used by the base stations as a router (relay) to communicate with other base stations, which are not within their communication ranges. However, several issues can be found such as the short transmission range of AN and the problem of interference. To overcome these challenges, the second application is...
the use of a team of aerial nodes (ANs), which provides many possibilities to solve these problems and supplies a variety of applications called multi-aerial-nodes applications. The advantages of multi-aerial-nodes over a single-aerial-node can be summarized as follows:

- The fault tolerance in multi-aerial nodes is increased when a node fails.
- In the cooperative missions, the tasks can be parallelized decreasing considerably the duration of the missions.
- The capabilities of calculations and storage can be distributed among aerial nodes.

All FANET applications have common necessities that can only be supported using multi-hop communications among aerial-nodes such as UAVs, Aircraft, Helicopters, etc. In the rest of the survey, we are interested especially in UAVs, which have been received a strong interest from both industry and academia. UAVs are driverless aerial-nodes, their movements are controlled using algorithms without any human interactions and can be deployed easily in the network. UAVs are composed of sensors, computing devices, and are recently commercialized. Consequently, UAVs are the most suitable for missions that need a cooperation and fairer distribution of tasks using multi-hop wireless communications.

The design of routing schemes becomes essential and mandatory to better assist the transmission of packets between aerial nodes. However, several challenging networking problems have made the conception of routing protocols dedicated exclusively for FANETs quite difficult. This is because many characteristics should be considered such as the high degree of mobility, uneven aerial node distributions, and the quickly changing of the network topology [16]. Among these constraints, the impact of the high dynamic movements of aerial nodes can cause several communication failures. As a result, developing a routing scheme, ensuring a great reliability toward all these constraints becomes more and more complex [17,18]. In addition, when the sky is poorly dense with aerial nodes, it can cause the loss of connectivity between the nodes.

The routing constitutes an important support for FANETs to keep their applications and services stable and active. Recently, several works were exclusively devoted to the combination of FANETs and other existing networks on the ground such as VANETs [19–23]. Indeed, due to their flexible and controlled mobility, FANET nodes can be the suitable choice to assist such highly mobile networks on the ground like VANETs. The different nodes constituting the FANETs such as UAVs are easy to be deployed and can be dispatched in different environments, which allows them to be a substitution network in the case when the networks on the ground fail to deliver data packets between the communicating nodes. Consequently, it is worth noting that the knowledge of the different routing methods applied among UAVs is important to define which method has to be applied in a given situation.

During the last few years, an important number of approaches and contributions are proposed, particularly those based on the geographical positions. This category of protocols has been designed to address the problem of the frequent disconnections between the nodes caused by their high mobility and their unpredictable movements. Some solutions [24–29] are just those proposed for Mobile Ad hoc Networks (MANETs), which are improved by including additional functionalities to adapt to the unique characteristics of FANETs. We do not ignore some topology-based routing protocols proposed for FANETs deployed only in certain cases, in which the nodes move more slowly and their numbers are limited. However, topology-based routing protocols are not suitable for scenarios characterized by highly dynamic movements and important number of nodes, since this kind of protocols is based on link information existing between the nodes, which can be quickly broken due to the high mobility. In addition, their main drawback is the consumption of more resources and energy caused by the extensive use of both memory (e.g., storage of the routing tables) and bandwidth (e.g., flooding process).

Furthermore, there are some comprehensive surveys [15,16,30], which address general issues in different lines of research in FANETs. However, they do not provide details about routing protocols, and especially those based on geographical positions. Table 1 provides a brief comparison, according to several crucial points about routing between related survey articles available in the literature and our survey. The main contributions of our survey compared with the surveys proposed in [15,16,30] can be summarized as follows:

- Description of the different routing techniques employed by the most popular routing protocols in FANETs.
- Presentation of the main mobility models used by the proposed FANET routing protocols.
- Classification of the most useful applications in FANETs.
- Proposition of a new taxonomy of existing FANET routing protocols.
- Depiction of some popular position-based routing protocols and recapitulation of all handled points using a comprehensive comparative study of all referenced routing protocols.
- Summarization of all weak points distinguished in each discussed routing protocol.

The primary reason behind this paper is to classify the proposed routing protocols for FANETs in their right category, according to the strategy used in the data delivery. Also, we mainly focus on position-based routing protocols, in which we also describe their functionalities and weaknesses. In addition, a new taxonomy is presented to distinguish the real category of each proposed
The remainder of this paper is organized as follows. In Section 2, we describe the different design features of FANET. The most used routing techniques are described in Section 3. Section 4 presents the most cited FANET position-based routing protocols. In Section 5, we propose a global comparative study of the presented FANET routing protocols. Finally, Section 6 and 7 discuss some future research challenges and conclude this paper, respectively. Table 2 provides a list of the abbreviations used in this survey.

2. FANET design

The unique characteristics of FANET have defined several crucial points of design. In the next subsections, the main important design features of a typical FANET such as architecture, applications, characteristics, and mobility models are detailed and discussed.

2.1. FANET architecture

FANETs have a similar standard as MANETs in which the nodes are flying, creating different characteristics. Fig. 2 shows two different kinds of communication which can be established between the nodes forming a classical FANET:

1. **Air-to-air wireless communications**: UAVs can communicate with each other using a pure ad hoc architecture in order to avoid the restrictions on the transmission ranges imposed by the communication between UAVs and the ground base stations [31]. In addition, this kind of wireless communication can be used to support different applications and multi-hop communications when the node wants to establish a transmission of the data packet to another node outside of the range.

2. **Air-to-ground wireless communications**: in FANET, not all UAVs can communicate with existing infrastructures such as ground stations and satellites [15]. However, only selected UAVs can establish a communication with infrastructures in order to both improve and increase the connectivity and to provide additional services.

FANET can be seen as a special case of MANET in which we distinguish certain differences like the very high degree of mobility of FANET nodes and the long distances between them. These may require wider communication ranges and different techniques to overcome these constraints. The wireless communication between FANET nodes is considered as a challenging task, which needs rules of communication in a form of routing protocols supporting the effectiveness of such transmissions.

2.2. FANET applications

Many factors make the FANET nodes easy to be deployed in different environments. Their ease of organization in an ad hoc network, allows us to not wait too long to create FANET in which its nodes can communicate and exchange data between each other. Flying nodes can also communicate with different infrastructures localized on the ground such as base stations or ground bases. It has, however, been observed that different obstructions can affect the communication between flying nodes and base stations such as mountains, walls, and buildings, which may block the radio signals of both infrastructures and flying nodes [16]. Three kinds of applications can be distinguished in FANET as follows: Multi-UAV cooperation, UAV-to-Ground tasks, and UAV-to-VANET collaborations.

2.2.1. Multi-UAV cooperation

Certain particular tasks require a cooperation between several UAVs to be carried out according to a certain time limit. The more number of UAVs in each task is, the more accurate the obtained results will be and the less the reduced time of the task. This decentralized mechanism offers more robustness since it is not related to any fixed infrastructure on the ground. Many kinds of applications are based on Multi-UAV cooperation such as target
As multi-UAV applications [33–41], all of them try to provide an appropriate and optimal solution using a given number of UAVs cooperating toward a particular task.

### 2.2.2. UAV-to-ground tasks

Important information has to be communicated between UAVs and the human operator located on the ground so that to take the right decisions in different scenarios such as search and rescue missions, military monitoring, and other civilian applications.

We can cite as UAV-to-ground applications [42–50], in which the wireless communication can be established between UAVs and both mobile or fixed nodes on the ground.

### 2.2.3. UAV-to-VANET collaborations

Recently, a new kind of wireless communication has emerged between UAVs and vehicles on the ground cooperating in ad hoc mode with each other in order to accomplish certain tasks. This creates a new possibility of potential research issues in UAV-to-VANET communications, and consequently, can be beneficial to design more applications in the near future.

Until now, the UAV-to-VANET cooperation can be used in different applications such as road traffic exploration, routing improvement, data packet delivery, traffic monitoring, route guidance, etc. The main applications proposed for this kind of cooperation are [20,21,23,51].

Based on the analysis done above, Table 3 produces a comparative study between the characteristics of the different types of FANET applications.

### 2.3. FANET characteristics

As a special class of MANET, FANET is differentiated by its unique properties that characterize the nodes and the surrounding environment. Various main characteristics can be employed to characterize FANET: UAV density [52], propagation model, topology [16], scalability [53], and localization [54,55]. Other characteristics are also distinguished in this kind of networks, which are described and discussed as follows:

#### Table 3

Comparison of potential scenarios for FANET.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Multi-UAV cooperation</th>
<th>UAV-to-ground tasks</th>
<th>UAV-to-VANET collaborations</th>
</tr>
</thead>
<tbody>
<tr>
<td>UAVs density</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>Ground environment</td>
<td>Not aware</td>
<td>Aware</td>
<td>Aware</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>No</td>
<td>Yes</td>
<td>Maybe</td>
</tr>
<tr>
<td>Obstacles effect</td>
<td>Low</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Task duration</td>
<td>Limited</td>
<td>Not limited</td>
<td>Not limited</td>
</tr>
<tr>
<td>Human operator</td>
<td>No</td>
<td>Yes</td>
<td>Maybe</td>
</tr>
</tbody>
</table>

#### 2.3.1. Unmanned Aerial Vehicles (UAVs)

In a general case, the nodes in FANET fly in the sky and move very quickly compared with default MANET nodes. These nodes are in the form of small mobile drones, or UAVs as referred to, and can fly autonomously without human interaction. The significant characteristics of UAVs is that their movements can be controlled using algorithms. Their speeds can exceed 400 km/h [56]. The density of nodes in FANET is generally low because of the great distances separating the nodes which can reach kilometers [52], resulting in the use of wider transmission ranges. Consequently, this means that the topologies of FANETs are not constant and change recurrently causing frequent link failures between the nodes [31, 57].

#### 2.3.2. Network connectivity

Due to the low density and the very high mobility of nodes, FANET can be considered to be sparsely connected. This results in the fluctuation of the link quality which may cause loss of connectivity and performance degradation. To address this problem, a proposed solution is to create an ad hoc network between the nodes in order to extend the communication coverage [58]. Even if the nodes cannot establish a connection with existing infrastructures on the ground, they can still communicate through other nodes.

#### 2.3.3. Energy autonomy

According to [59], the power and the movements of FANET nodes are powered and supplied using the energy resources of the nodes. Indeed, there is no energy restriction since each node is equipped with rechargeable batteries, which are continuously
recharged as UAVs moving. Also, batteries may be powered by the nodes resources such as solar energy, gasoline, electrical energy, etc. In addition, the amount of energy required to move a UAV is much greater than the energy required for computing data. Consequently, we can say that FANET nodes do not have energy power restrictions compared with MANET nodes, where developers have to make more attention to the energy consumption by the communication protocols to extend the lifetime of the network. However, in the case of mini UAVs, the constraint of energy consumption constitutes one of the major drawbacks in which the payload capacity of mini UAVs is considerably limited. In addition, several different characteristics are observed between ordinary UAVs and mini UAVs such as speeds, altitude, and weight, all of which make the difference in the case of energy autonomy [16,60].

2.3.4. Quality of Service (QoS) requirements

Certain FANET applications need efficient real-time services like the application dedicated for the transmission of aerial photography and video for a real-time monitoring [59]. In this case, several metrics have to be taken into consideration in order to ensure the reliability of these real-time applications such as latency, available bandwidth, packet losses, jitter, etc. For instance, in the case of video transmission, the main requirement of the QoS is to reduce the latency between the UAVs and the receivers which are exchanging the video with each other. In addition, a sufficient bandwidth has to be available to transmit the video efficiently to the target destination. These QoS requirements are crucial, especially when important decisions have to be taken by the entity receiving the video [61]. Consequently, a minimum of QoS requirements has to be guaranteed by the real-time applications while taking into consideration the highly dynamic nature of FANETs.

2.3.5. Mobility models

The movements of nodes in FANET are generally defined beforehand. However, due to external factors (e.g., weather, mission, etc.) the movements can be updated which can affect directly the mobility model of the nodes. In addition, mobility models proposed for MANET are not suitable for FANET, in which their use results in the establishment of inadequate path plans [16].

To be more accurate, different kinds of UAVs are distinguished in FANET in which certain properties cannot remain the same for each kind of UAVs. Overall, three kinds of UAVs can be distinguished in FANET such as large UAVs, small UAVs, and mini UAVs [15]. A brief comparison between these three kinds of UAVs is presented in the Table 4 as follows:

We can say that a FANET protocol has a satisfying performance level outcomes, if it covers all FANET specific characteristics mentioned above. As a result, there is a clear need to develop robust protocols for FANETS, which have to be tested and validated in real scenarios. However, the protocols proposed for VANETs and MANETS cannot be deployed directly to support the unique requirements of FANETs. Following (see Table 5) is the main differences between MANETS, VANETS, and FANETS.

2.4. Mobility models

To be adequate for the unique characteristics of FANETs, several mobility models are proposed:

- **Random way point mobility model (RWP) [62]:** this model is used in the most simulation scenarios to generate different movements based on straight trajectories in which each node selects a random destination, moves with a random speed, and a pause time at the destination. When the pause time is expired, nodes choose another random destination with a random speed and a similar pause time based on fixed probabilities.
- **Random movements [62]:** different kinds of movements are selected randomly without limitations, i.e., the speed, destination location, and direction are all selected randomly and independently of other mobile nodes.
- **Gauss–Markov [63]:** the movement can be determined based on the memory of the model through different states. Each state can determine a specific movement, according to the previous one.
- **Pheromone repel [63]:** this model is based on a pheromone map and the pheromones affect node mobility by scanning the map and sharing the pheromone map through broadcasting.
- **Semi-Random Circular Movement (SRCM) [64]:** this model is created for a circular movement around a fixed zone. It can be used in search and rescue applications where a lost victim should serve as the circling zone.
- **Paparazzi mobility model (PPRZM) [65]:** this model is considered as a stochastic mobility model which has five possible movements for nodes such as, stay-at (node hovers over a fixed position), Eight (trajectory of the node has the 8 form around two fixed zones), etc.

Overall, the success of the requirements and characteristics mentioned in Section 2.3 relies on the selection of the adequate mobility model. Path plans mobility models such as PPRZM [65], SRCM [64], and pheromone repel [63], are considered as the most preferred for FANETs because of the mission nature of this kind of networks. For instance, the power consumption and the localization can be easily estimated at each time during the mission. In the case of random mobility models, despite their simplicity, they

<table>
<thead>
<tr>
<th>Table 4</th>
<th>Comparative study between each kind of UAVs.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Properties</td>
<td>mini UAVs</td>
</tr>
<tr>
<td>Transmission range</td>
<td>Small</td>
</tr>
<tr>
<td>Altitude</td>
<td>≈300 m</td>
</tr>
<tr>
<td>Energy autonomy</td>
<td>Restricted</td>
</tr>
<tr>
<td>Speed</td>
<td>Medium</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 5</th>
<th>Difference between FANETS, VANETS, MANETS.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Characteristics</td>
<td>MANETs</td>
</tr>
<tr>
<td>Density</td>
<td>High</td>
</tr>
<tr>
<td>Network connectivity</td>
<td>High</td>
</tr>
<tr>
<td>Energy autonomy</td>
<td>Low</td>
</tr>
<tr>
<td>Topology variation</td>
<td>Occasionally</td>
</tr>
<tr>
<td>Scalability</td>
<td>Medium</td>
</tr>
<tr>
<td>QoS</td>
<td>Low</td>
</tr>
<tr>
<td>Mobility models</td>
<td>Random</td>
</tr>
<tr>
<td>Node speed</td>
<td>Medium</td>
</tr>
</tbody>
</table>
can distort the accomplishment of the missions defined beforehand. Furthermore, all the requirements cannot be satisfied during the whole scenario or the experiment.

3. FANETs routing techniques

Since FANETs have specific characteristics and operate in a special environment, they have also their own routing techniques. In fact, FANETs are considered as a subclass from MANETs and VANETs (see Fig. 3). Therefore, common techniques are shared for the data delivery [16]. However, for the right functionality of the forwarding process, these techniques have to be adapted to both mobility models and operating environment, which are specific to FANETs. Also, these requirements are quite different from those of MANETs and VANETs. The selection of the relays to forward data packets is crucial since it has to be efficient to avoid the packet losses. Although each adopted kind of technique has its own drawback, it always remains the most suitable in a given kind of situation. Fig. 4 summarizes the most popular technique used for the data delivery in FANETs.

3.1. Store-carry and forward

At a certain moment, when the network is intermittently connected, the forwarder nodes do not have any solution to find a relay node. Consequently, it is not possible to forward any data packet to a predefined node which does not exist in the transmission range. Only in this case, the current node tends to carry the packet until meeting another node or the target destination itself. This kind of routing is known as the store-carry-and-forward paradigm. Its cost is not negligible in terms of delay, which is caused by the physical movement of the node. This kind of technique is often used in FANET since it is poorly dense (see Fig. 4(A)).

3.2. Greedy forwarding

This technique is used when a conventional FANET is densely deployed. The purpose of Greedy Forwarding is to minimize the number of hops in which a data packet can make during its transition to the target destination. The principle is to select the geographically closest node to the target destination as a relay node and so on until the packet reaches its destination. Some drawbacks are to be deplored, such as the local optimum problem, in which the process is blocked at a node which is considered as the closest to the destination and cannot find any relay nodes to reach it. In this case, a combination of other techniques should be used to ensure the reliability of this technique. Fig. 4(B) illustrates this type of routing technique.

3.3. Path discovery

As shown in Fig. 4(C), the discovery process is deployed when the geographical position of the target destination is not known by the source node. The discovery is based on the RREQ dissemination to find all possible paths to the target destination. When all possible paths are received by the target destination, a suitable path is selected according to specific criteria. Then, this path is used for the data packet transition. The discovery process is among the most used methods in existing FANETs routing protocols due to its simplicity. Furthermore, the advantage of this technique is that the message will arrive at its destination, but the cost for this is significant and may unnecessarily cause excessive consumption of bandwidth.

3.4. Single path

As indicated by its name, this technique consists of establishing a single routing path between two communicating nodes. This may simplify the handling of the routing tables in each node constituting the path. However, the major disadvantage of this technique is that when a fault occurs in the network and there is no alternative path to forward data packets, it may result in crucial packet losses (see Fig. 4(D)).

3.5. Multi path

Unlike single path technique, in multi path technique, there are several paths between two communicating nodes. It is more complex to maintain the routing tables of the nodes since a node can be a central point of two different paths or more. When a fault occurs, the multi-path routing can easily detect the fault and find an alternative solution as fast as possible. As a drawback, it is very complex to configure such technique, because the slightest error, it results in routing loops blocking the network. This technique is illustrated in Fig. 4(E).

3.6. Prediction

There are several forms of prediction techniques for the data delivery used in FANETs. The most popular one is the prediction based on the geographical location, direction, and speed, to predict the future position of a given node. All these parameters can give an accurate information about the next relay node location which decreases considerably the packet losses, and sometimes reducing the end-to-end delay between two communicating nodes. Fig. 4(F) represents a prediction technique based on the future geographical location of a next relay node.

Like any routing technique, a recovery strategy is employed to avoid a critical functioning of the routing protocol and to continue working normally using different methods according to the employed technique for data delivery. For instance, under severe fragmentations of the network, the Store-Carry and Forward technique is often used to avoid the packet losses. In another case of routing protocols such as the reactive protocols using the path discovery technique, a recovery strategy can be based on the reinitialization of the discovery process, and it becomes unavoidable to find other active paths between communicating nodes.

4. Routing protocols for FANETs

There is a wide range of routing protocols proposed for FANETs in [20,21,24–29,66–101]. All these protocols are intended to im-
prove the packet delivery ratio and to provide low delays and packet losses. In addition, all FANET characteristics, and especially the high mobility of nodes have to be taken into consideration.

As shown in Fig. 5, FANET routing protocols can be classified into three main categories according to the followed technique and the idea behind each protocol: (i) Topology-based routing protocols, (ii) Swarm-based routing protocols, and (iii) Position-based routing protocols. The subsections below investigate the most relevant routing protocols. We note that the topology-based routing protocols are partially investigated since this survey is dedicated to study the most important position-based routing protocols, which are the most suitable for this kind of networks.

4.1. Topology-based routing protocols

This category of routing protocols exploits IP addresses to define the nodes and uses the existing link information in the network to forward packets through the appropriate path. The proto-
cols are classified as Proactive routing, Reactive routing, and Hybrid routing.

4.1.1. Proactive routing protocols

In this kind of routing protocols, the routing tables are updated and shared periodically among the nodes resulting in the availability of routing paths between every pair of nodes in the network. However, the proactive routing is not adequate for FANETs because of its low reaction to the frequent change of the topology resulting in many connection failures. The most popular proactive routing protocols proposed or adapted to FANET in the literature are OLSR [102–104], D-OLSR [87], M-OLSR [93], CE-OLSR [83], and DSDV [102].

4.1.2. Reactive routing protocols

In order to limit the abuse of the bandwidth consumption in the proactive routing, the reactive routing uses a discovery process on-demand when there is no route between two communicating nodes. This kind of routing can be the suitable solution for highly dynamic networks such as FANET [16]. Nevertheless, a high latency can be distinguished due to the important time taken by the discovery process and the lack of security in this kind of routing. Several reactive routing protocols have been proposed during the last decade: AODV [102,104], AODV-SEC [82], Time-slotted AODV [96], M-AODV [100], APAR [67], and DSR [25].

4.1.3. Hybrid routing protocols

To overcome the overhead problem of proactive protocols and the high latency of reactive protocols, the hybrid routing is introduced. Indeed, the network is divided into zones and inside each zone, a proactive routing is adopted and the communication between zones is based on a reactive routing [15]. As hybrid routing protocols which are adapted to FANETs, we can cite HWMP [104,105], ZRP [26], SHARP [106], HRPO [107], and TORA [27].

4.2. Swarm-based routing protocols

The swarm intelligence (SI) is a self-organized system and was first used for the cellular robotic system [108]. The SI can be considered as an optimization algorithm in intelligence theory. The implementation of such system is based on swarm algorithms. To realize this kind of algorithms, the social behaviors of birds or fishes in flocks or insects on swarm are modeled. These can be the suitable solution for complex optimization problems. These algorithms aim to find a near-optimal solution for the target mission. As swarm-based routing protocols, which are dedicated for FANETs, we distinguish BeeAdhoc [70] and APAR [67].

4.3. Position-based routing protocols

This class of routing protocols is based on the knowledge of the geographical positions, which each node is able to define using the GPS. We note that for calculating the position of the destination, the node can use a location service such as the Reactive Location Fig. 5. Taxonomy of FANET routing protocols.
Service (RLS) [109], the Grid Location Service (GLS) [110], or the Hierarchical Location Service (HLS) [102–104]. This kind of routing is the most suitable for highly dynamic networks such as FANETs. Below we investigate in details the most relevant routing protocols belonging to this category. The protocols can be classified into three categories: (i) Non-DTN routing protocols, (ii) DTN routing protocols, and (iii) Heterogeneous routing protocols.

4.3.1. Non-delay tolerant network (non-DTN) routing protocols

This kind of protocols works more effectively on well-connected networks where the density of nodes is relatively high because it does not consider the dis-connectivity issue. The main goal of these protocols is to transmit data packets to the receiver as quickly as possible using the multi hop technique through the nodes in the case when the receiver is not within the transmission range of the sender. Two categories are distinguished: (i) Reactive-based routing and (ii) Greedy-based routing. The first category needs to have the full path to the target destination based on routing paths established on-demand beforehand. However, the data delivery might be unsuccessful in the case of disconnection if the network becomes sparsely connected. Therefore, the reactive protocols have to apply their recovery strategies to tackle such failures.

In the second category, the senders transmit data packets to the closest neighbors to the target destination, but in the case when there is only the forwarder itself and no neighbor exists, the data delivery will be failed and a recovery strategy have to take place. Consequently, many proposed routing protocols in FANETs tend to handle these failures by different methods which will be shown in the following subsections.

4.3.1.1. Reactive-based routing protocols

The reactive technique is the most used technique in FANET routing protocols. Indeed, when there is no route to the target destination, the source node needs to establish an on-demand path in order to start a communication with the target destination. Many reactive routing protocols are proposed for FANETs.

1. Reactive–Greedy–Reactive protocol (RGR) [81]

Shirani et al. proposed Reactive–Greedy–Reactive protocol (RGR) [81], which is a reactive routing protocol based on the combination of a topology-based routing protocol to create on-demand paths using the well-known reactive protocol AODV (Ad hoc On-demand Distance Vector) [24], and a classic delivery technique based essentially on the Greedy Geographic Forwarding (GGF) [81]. Despite the topological nature of RGR protocol that has been observed, the geographical positions are always exploited both in the data delivery to get the destination’s location and in the case of disconnections between the nodes to select the next forwarders. Consequently, RGR can be considered as a reactive routing protocol, which must use the geographical positions during the recovery strategy.

In the example of Fig. 6(a), when a source UAV S has a data packet to send to a destination UAV D, it initiates a path discovery process (same as AODV) in order to find a connected path to reach the target destination by flooding Route Request (RREQ) over the network. As soon as the Route Reply (RREP) is received by the source from the destination UAV, it starts the data delivery.

The novelty in RGR is that the geographic position of the destination UAV D is cached in the routing table (maintained periodically based on Hello packets) of each intermediate UAV traversed by the RREP packet when it is sent back to the source. As a recovery strategy, an intermediate node may detect a disconnection with the next forwarding node due to high mobility (see Fig. 6(b)), which signifies the failure of the discovered path. In this case, RGR switches to GGF mode and forwards the packets to the closest neighbor UAV to UAV D until reaching it. If GGF fails to find the next forwarding UAV, the packet will be dropped. In parallel, a Route Error (RERR) will be sent to the previous node until reaching the source node. If the source node has more data packets to transmit, it initiates a new path discovery so as to create a new reactive path to the target destination.

- **Advantages of RGR:** The combination of the reactive and GGF techniques allows to surpass the use of the local repairs of the reactive technique in case of disconnections. In fact, the GGF component uses the RREQ/RREP architecture of AODV as its location service mechanism in order to complement each other and to enhance the delivery ratio and end-to-end delay of the network.
- **Weaknesses of RGR:** The geographical locations of the next hops are not updated regularly and in short periodicity. Indeed, due to the very high mobility of UAVs, data packets
2. **Multipath Doppler Routing (MUDOR)** [95,99]

Sakhaee et al. proposed Multipath Doppler Routing (MUDOR) [95,99], which is a reactive routing protocol inspired from Dynamic Source Routing (DSR) [25] and designed for highly mobile ad hoc networks like FANETs. MUDOR is based on the selection of the most stable path with the longest lifetime. To find the best path, MUDOR measures the frequency shift due to the Doppler effect of the received packets. This determines the relative velocity between the source and the destination aerial vehicle. Then, we can estimate the lifetime of the link. Before starting the data delivery, MUDOR uses the flooding of RREQ to discover routes toward the target destination. The first time when a node receives the RREQ packet, it rebroadcasts this packet after adding its identifier and the Doppler value from the previous node. At the end, the destination will reply by a RREP packet through the path with the longest lifetime by considering all the calculated Doppler values.

Fig. 7(a) shows the discovery phase to get the most stable path based on the Doppler values estimated for each discovered path. The target destination replies with a RREP packet through the succession of nodes, where their velocity vectors are in the direction toward the destination and their speeds are relatively the same.

Fig. 7(b) shows a scenario where MUDOR defines the best path as the most stable one according to the speed and direction of the nodes, which are very similar to each other. Indeed, the source node S selects the same sequence of nodes (i.e., C, G, F, and N) transited by the RREP packet depending on their velocities and speeds resulting in long lifetime links between them. Consequently, the selected path (S, C, G, F, N, D) has a long duration of life and MUDOR made time to initiate a new path discovery.

- **Future improvements of RGR:** The GGF and the reactive techniques need to be improved by including trajectory information (i.e., velocity). This can provide accurate positions of the next hops in GGF and make the prediction method more efficient. In addition, it allows to decrease the intensity of the paths’ discovery of the reactive technique. The geographical positions need to be updated periodically to make more accurate the selection of the next forwarders.

- **Potential applications of RGR:** RGR is initially adapted to tracking and searching missions by supporting the exchange of crucial information between the UAVs about the victims or targets. However, RGR can also be useful in emergency situations and multi-tasks cooperation since it is a delay-sensitive protocol.

3. **Ad hoc Routing Protocol for Aeronautical MANETS (ARPAM)** [98]

Could be lost if they are forwarded to an outdated geographical position. In addition, the overhead is still relatively high due to the excessive use of control packets during the discovery process.

- **Future improvements of RGR:** The GGF and the reactive techniques need to be improved by including trajectory information (i.e., velocity). This can provide accurate positions of the next hops in GGF and make the prediction method more efficient. In addition, it allows to decrease the intensity of the paths’ discovery of the reactive technique. The geographical positions need to be updated periodically to make more accurate the selection of the next forwarders.

- **Potential applications of RGR:** RGR is initially adapted to tracking and searching missions by supporting the exchange of crucial information between the UAVs about the victims or targets. However, RGR can also be useful in emergency situations and multi-tasks cooperation since it is a delay-sensitive protocol.

![Fig. 7. MUDOR functionality.](image)
Iordanakis et al. proposed Ad hoc Routing Protocol for Aeronautical Mobile ad hoc networks (ARPAM) [98], which is a routing protocol based on the geographical positions. ARPAM has the same principle as in AODV [24], and consequently, is partly reactive. ARPAM uses geographic positions of UAVs in the network to select the shortest path between the source UAV and destination UAV. Similarly to AODV protocol, when a source UAV wants to send data packets and there is no path to the destination UAV, a RREQ packet is flooded over the network. The RREQ contains the velocity vector and the position of the source. This information is used by intermediate UAVs to estimate the current position of the source UAV, which is changing rapidly due to the high speed of the UAVs. Also, the geographical position and velocity vector information can be used to provide the distance that the packet has transited, which can be used as a metric during the routing path decision. When the destination receives the RREQ packet, it responds with a RREP packet which is sent unicastly to the source node. ARPAM is also based on an on-demand path maintenance mechanism, which aims to maintain routing tables when necessary, and especially, for certain applications such as voice over IP (VoIP) or video on demand (VoD), which requires low response times from the network. Consequently, ARPAM is a reactive routing protocol which can be proactive on-demand.

As an illustration, we take the example shown in Fig. 8(a). When the source node UAV S wants to send a data packet to the destination UAV D, it broadcasts a RREQ packet in the network, which includes the geographic position and velocity vector of the source. Once UAV D receives the RREQ packet, it selects the closest path to the source based on the information included in the RREQ. When a path is selected, UAV D sends unicastly a RREP packet back to UAV S through the selected path. Once the source UAV S receives the RREP packet, it starts the data delivery to the target destination through the same path transited by the RREP packet (cf., Fig. 8(b)).

- **Advantages of ARPAM**: The selected routing paths are characterized by their shortest length and their fullness to the target destinations. This decreases significantly the delay of delivering, which is preferred for certain real-time applications requiring low response times from requests. In addition, to tackle the problem of the high mobility, the geographical positions of the nodes are taken into consideration to estimate their future positions in the case of a topology change.

- **Weaknesses of ARPAM**: In the case when the nodes of the network move at a very high speed (e.g., fast aircraft), ARPAM is not suitable and cannot be adapted in such scenario because it is characterized by its slow reaction to frequent changes of the topology. When packet losses occur, ARPAM loses completely the control of the routing process and cannot find alternative solutions to continue the data delivery. As a result, the establishment of a recovery strategy based on the same technique employed during the data delivery process becomes a mandatory condition.

- **Future improvements of ARPAM**: ARPAM needs deep improvements, and especially, in its internal routing mechanism. Indeed, the discovered routing paths need more stability and reliability to avoid the re-initialization of the discovery process each time when the network becomes sparsely connected. This can be done by exploiting and updating periodically the routing tables of the nodes. In addition, an efficient maintenance mechanism needs to be conceived, which consists of finding alternative solutions (i.e., alternative path to the target destination) at the disconnection point.

- **Potential applications of ARPAM**: ARPAM can be deployed to support time critical applications such as video on demand (VoD) and voice over IP (VoIP), which require low response times from the network since ARPAM is a delay-sensitive protocol.

### 4.3.1.2. Greedy-based routing protocols

As a forwarding strategy in a classical FANET position-based routing protocol, the technique of greedy forwarding is frequently employed for the data packet delivery. This technique aims to minimize the number of hops to the target destination, and consequently, the delay of delivery and the transited distance. Some of the well-known approaches proposed for FANETs are presented in this section.

1. **Geographic Position Mobility Oriented Routing (GPMOR)** [111]

   Lin et al. proposed Geographic Position Mobility Oriented Routing (GPMOR) [111], which is a routing scheme dedicated for FANET. GPMOR uses the mobility prediction of UAVs moving based on Gauss–Markov mobility model [112]. Indeed, each UAV has the knowledge of its own geographical location with the help of the GPS. Each UAV periodically exchanges its position with its direct neighbors trying to predict the
movement of its neighboring nodes and to define their new positions during a time interval. Consequently, it is possible to select the optimal forwarder towards the destination UAV which can itself change position occasionally. As depicted in Fig. 9(a), GPMOR can carry out the best forwarder selection based on the adopted prediction method. For instance, the UAV $S$ selects the UAV $F$ as a forwarder of the data packet because it is the most appropriate UAV according to its future movement, which is towards the destination UAV $D$. However, the UAV $B$ cannot be selected as a next hop since can move away from the transmission range of UAV $S$ which may result in the loss of data packets due to the high mobility of the nodes. Once the destination $D$ is within the communication range of the UAV $F$, the data packet is delivered to its corresponding destination (cf. Fig. 9(b)).

- **Advantages of GPMOR**: The selection of next hops is based on the geographical positions of UAVs. Indeed, GPMOR predicts the movements of UAVs with the help of the Gaussian–Markov mobility model used by this routing protocol. A result, this method increases significantly the chances to select the optimal relay to the destination node, and consequently, a high delivery ratio and low delay of delivering can be deducted.

- **Weaknesses of GPMOR**: GPMOR can be considered as the most adequate for highly dense networks. However, in the case when the network suffers from severe fragmentation, the mechanism employed by GPMOR cannot continue to function normally resulting in important packet losses. Moreover, the technique employed by GPMOR only works during a predefined interval of time and not during the entire scenario.

- **Future improvements of GPMOR**: The store-carry and forward technique can be adopted in the case of disconnections working along with the prediction technique based on the Gaussian–Markov mobility model. Even if this new adopted technique results in high delays of delivering, it allows to minimize significantly the packet losses and to improve the delivery ratio.

- **Potential applications of GPMOR**: GPMOR is preferred for collaborative applications, which aims to finish tasks regardless the duration of the missions (e.g., reconnaissance missions).

2. **Mobility Prediction based Geographic Routing (MPGR)** [80]

Lin et al. proposed Mobility Prediction based GeographicRouting (MPGR) [80], which is a routing protocol based on the geographic positions for inter-UAV communications. The same principle in GPSR (Greedy Perimeter Stateless Routing) [28] is used in MPGR. Furthermore, MPGR uses a mobility prediction method based on the Gaussian distribution function so as to reduce the impact of the high mobility of UAVs with an acceptable communication overhead.

The novelty in MPGR is when a source UAV wants to send a data packet, firstly, it must broadcast a Neighbor Discovery packet (ND) to know the available next forwarding UAVs and to select the appropriate one based on the information included in the Reply Packet (RP). However, the selected next forwarding node can move out of the source transmission range causing the loss of the data packet due to the link interruption. In this case, MPGR uses the mobility prediction to predict the accurate geographic location of UAVs at time $t_n$ based on the mobility feature and position at $t_{n-1}$. The estimated position allows the analysis of the persistent connection of the neighboring nodes. Thus, we can perform the selection of the next forwarding node more accurately.

The example of Fig. 10(a) represents the selection process of the next forwarding node based on a metric called Reliable Next Hop (RNH). This metric combines the estimated position and speed of the current node and its neighbors, and also the distance and time of persistence between each pair of nodes. The smaller is the value of RNH, the better is the next hop. RNH is calculated based on the following formula:

$$RNH_A(D) = \begin{cases} d_A + \frac{\eta}{\Delta T}, & (d_A < d_B) \land (\Delta T \geq 1) \\ \text{Max}\_\text{value}, & \text{otherwise} \end{cases}$$

(1)

where $d_A$ and $d_B$ are the distances between $A$ and destination $D$, and between $B$ and $D$, respectively. $RNH_A$ is the calculated metric of the neighbor $A$ for the destination $D$. The $\Delta T$ is the maximum persistence time of the forwarding neighbor $A$. $\eta$ is a factor used to adjust the neighbor connection persistence which is set within the range $(1, R)$, where $R$ is the transmission range. $\text{Max}\_\text{value}$ is the maximum value which has to take RNH metric.

As shown in Fig. 10(b), if an intermediate UAV detects a routing void (i.e., it is the closest to the destination UAV $D$), the greedy forwarding mode will fail and MPGR has to switch on
perimeter forwarding. The UAV $H$ calculates the distance between each two-hop neighbor and UAV $D$. In this case, UAV $M$ will be selected as a forwarding node because it has a neighbor node which is the closest to UAV $D$.

- **Advantages of MPGR:** The stability of UAV networks was significantly improved by adding the link state information into MPGR. In addition, to define the future positions of the next hops and to avoid the packet losses, each node estimates the geographical positions of its neighbors based on the Gaussian distribution function. Moreover, the routing decision process considers the distance between UAVs and the target destination, and the difference of time prediction to select next hops, which reduce considerably the delay of delivering and the packet losses.

- **Weaknesses of MPGR:** MPGR ignores the use of the link expiration time and does not consider the planned trajectory of the UAVs to find the future position of a next hop. This can provide more accurate estimation of the future position of a next hop than prediction-based methods. Furthermore, MPGR does not take into account the case when a local optimum occurs and the two hop perimeter mode cannot be applied.

- **Future improvements of MPGR:** The maintenance process can be improved by considering the link expiration time of the wireless links in order to find other alternative hops instead of re-initiating the data delivery again. Furthermore, the planned trajectory is a promising technique to efficiently select next hops and to avoid the link breakage.

- **Potential applications of MPGR:** MPGR is ideally suited for the applications requiring real-time and accurate data routing among UAVs for prosecuting tasks cooperatively such as the scenario of a battlefield or search/tracking missions.

3. **Geographic Load Share Routing (GLSR)** [79, 84, 88, 89]

Medina et al. proposed Geographic Load Share Routing (GLSR) [79, 84, 88, 89], which is a geographical routing protocol for FANET. GLSR is an extension of the protocol GPSR [28], which exploits the multiple paths between source and destination. The key idea behind GLSR is to simultaneously use multiple paths between source and destination. The key principle of GLSR is to send data packets to the nodes, which allow approaching to the destination. To this end, GLSR defines the distance advancement ($a^M_K$) that permits the neighbor UAV $K$ to reach to the destination $M$ (cf. Fig. 11(a)).

$$a^M_K = d_{1M} - \delta_{KM}$$

If $a^M_K$ is positive, the neighbor UAV $K$ allows to reduce the distance toward the destination UAV $M$. Then, GLSR determines the best path among the different available paths. For this, each node has multiple queues for packets to send. Furthermore, there is a queue for each neighbor. GLSR takes into account the degree of filling of these queues to determine the best path. The metric used to select the best neighbor is called the speed of advancement $v^M_K$ of a neighbor UAV $K$ toward the destination UAV $M$ as follows:

$$v^M_K = \frac{a^M_K}{Q_{1K, size} + 1}$$

where $Q_{1K}$ is the neighbor UAV $K$ queue size using Self-organized time-division multiple access (STDMA) link scheduling. This favors the nodes that have the highest speed advance and the lowest queuing delay to be selected to deliver data packets toward the destination UAV $M$. Similar to GPMOR, the forwarder UAV $K$ checks periodically in its neighboring to find, if possible, another suitable node to the target destination with the previously mentioned characteristics by using the same equations (2) and (3) to determine the next hop. Finally, when the destination is within the communication range of the UAV $K$, the data packet is delivered directly to its corresponding destination (cf. Fig. 11(b)).

- **Advantages of GLSR:** To select the appropriate next hop, the current UAV performs load balancing among neighboring candidates. This enhances to make the routing paths more efficient and reliable, and therefore reducing the average end-to-end packet delay and increasing the network throughput.

- **Weaknesses of GLSR:** GLSR does not take into consideration other factors during the selection of next hops such as the distances between the nodes constituting the routing path.
Moreover, in the case when there is no node approaching the target destination, GPMOR loses the packets.

- **Future improvements of GLSR**: GLSR requires to exploit the distances between the nodes and to include a prediction method to make the routing paths more efficient and stable. This allows to take into account the high mobility of the UAVs and to reduce the packet losses significantly.

- **Potential applications of GLSR**: GLSR can be the suitable candidate for delay-sensitive applications such as VoIP, VoD, video monitoring, etc., requiring a certain level of QoS.

**4.3.2. Delay tolerant network (DTN) routing protocols**

These approaches are destined to handle the technical issues of networks suffering from recurrent disconnections such as FANETs due to the high degree of nodes’ mobility. This results in distorting the end-to-end routing paths built gradually to the target destination. In most cases, this category of protocols uses the technique of store-carry-and-forward when they lose connectivity with other nodes in order to transmit data packets to the target destination. This well-known technique allows the nodes to store data packets for a certain distance until they meet other nodes, and to forward the packets based on certain metrics to the neighboring nodes. This technique decreases significantly the overhead since it does not use any additional control packets. However, it increases the delay of transmission since data packets are transited based on the movements of nodes. Some protocols are presented in this section.

1. **Location Aware Routing for Opportunistic Delay Tolerant (LAROD)** [94]

Kuiper et al. proposed Location Aware Routing for Opportunistic Delay Tolerant (LAROD) [94], which is a delay tolerant geographical routing protocol based on the combination of the store-carry-and-forward and greedy forwarding techniques according to the network situation. In addition, a beacon-less strategy is used which reduces considerably the overhead with the help of the network management.

As illustrated in Fig. 12, when a source UAV $S$ wants to send a data packet to a destination UAV $D$, it broadcasts it to the neighboring nodes. When it is received by each one, intermediate nodes start a timer. The best forwarding node, which is the first one having the timer expired, forwards the data packet in the same manner. The source UAV $S$ will overhear this transmission and deduce that the forwarder has successfully received the data packet and broadcasted it. If no transmission is heard, UAV $S$ periodically broadcasts the data packet until a node becomes available. However, if the network is sparsely connected, the current UAV (i.e., the custodian) uses the store-carry-and-forward technique by holding the data packet until it meets other UAVs nearby. In this case, it uses the greedy forwarding to resume the data packet delivery until it reaches the destination UAV $D$. When the data packet is successfully received by UAV $D$, an acknowledgment (ACK) is broadcasted back to the source.

- **Advantages of LAROD**: The store-carry and forward technique used by LAROD provides a high delivery ratio, but at a substantially lower overhead. In the case of mini UAVs, which have a limited energy consumption, this technique is not greedy in terms of energy consumption, which makes it a suitable for each kind of unmanned aerial nodes.

- **Weaknesses of LAROD**: A high delay of delivering is distinguished by using the store-carry and forward technique. Moreover, the routing overhearing cannot be applied in urban areas where there are obstructions, which can be seen as a distorting factor. This does not allow the broadcaster...
to know if the next hop has successfully received the data packet and broadcasted it, even if the latter has already carried out the broadcast. Furthermore, the high degree of mobility is not suitable for the right functionality of such mechanism. All these disadvantageous factors force the current UAV to make the broadcast of the data packet several times resulting in high overhead.

- **Future improvements of LAROD:** To avoid the reinitialization of the broadcast when no broadcast is overheard, a prediction technique needs to be employed to find the most appropriate forwarder and to be sure that data packets can reach their target without overhearing the broadcast from the neighboring nodes. This can reduce significantly the overhead and the bandwidth consumption.

- **Potential applications of LAROD:** This kind of routing protocols is not adequate for delay-sensitive applications. However, they can be the best candidate for the applications such as reconnaissance area, mapping, video, etc.

2. **Aeronautical Routing Protocol (AeroRP) [85,90]**

Jabar and Peters et al. proposed Aeronautical Routing Protocol (AeroRP) [85,90], which is a geographical delay tolerant routing protocol designed for aeronautical networks which consist of fast aerial vehicles (Aircraft). The first phase of the functionality of AeroRP is to detect the neighboring nodes by intercepting their positions and velocities. This information is updated through the periodical exchange of Hello packets. Based on the neighbors’ table, each node calculates for its neighbors a metric called Time to Intercept (TTI) which is used to select the next forwarding node. TTI indicates when a potential neighbor will be within the communication range of the current node. TTI is calculated based on the following formula:

$$TTI = \frac{\Delta d - R}{S_d}$$  \hspace{1cm} (4)

where $R$ is the transmission range of each neighbor. $\Delta d$ is the distance between the specific neighbor and the target destination. $S_d$ is the velocity of the specific neighbor in which it moves toward the target destination.

The keystone of AeroRP is that when a source airborne vehicle $S$ has a data packet to send to the destination $D$ (see Fig. 13), it has to select the fastest next forwarder or custodian among its neighboring nodes $(C-G-F)$ moving towards $D$. $S$ calculates its own TTI (i.e., if its velocity is towards $D$) and those of $(C-G-F)$. The neighbor that obtained the lowest TTI is selected to hold the data packet. However, if $S$ obtains the lowest TTI from $D$ or all nodes are moving away, $S$ continues to keep the data packet. In Fig. 13, $G$ obtains the lowest TTI and it will be selected to hold the data packet.

- **Advantages of AeroRP:** According to simulations, the employed store-carry and forward technique can provide the best PDR, accuracy, and overhead. In addition, the next hops are efficiently selected to hold the data packets to the target destination based on TTI metric.

- **Weaknesses of AeroRP:** The major drawback in AeroRP is the higher delay caused by the ferrying modes (i.e., buffering packets) applied when the network is poorly dense. According to the performance analysis, the AeroRP protocol is highly influenced by the degree of node mobility. Moreover, the mobility of the target destination is not taken into consideration when it moves out of its original position.

- **Future improvements of AeroRP:** AeroRP can be improved on the selection method of the next hops by including additional criteria such as the greedy forwarding and the exploitation of the future movements. This allows to resume the data delivery as soon as possible and to avoid the buffering of data packets for a long time. In addition, the location service has to provide the position of the target destination in real-time since it can move out of its original position when the data packet is carried during a long time by the forwarder.

- **Potential applications of AeroRP:** AeroRP can be the best support for different civilian applications such as sensors collecting information around a specified area and transferring them to a predefined node. However, it is not recommended to use AeroRP in delay-sensitive applications since it suffers from important delays.

3. **Geographic Routing protocol for Aircraft Ad hoc Network (GRAA) [86]**

Hyeon et al. proposed Geographic Routing protocol for Aircraft Ad hoc Network (GRAA) [86], which is a geographic routing protocol based on GPSR. The routing decision is taken locally at each intermediate node. To determine the next hop, each node takes into account the position and the velocity of its neighbors and the destination. Initially, the current node calculates the estimated position of the destination after a time period $t$ based on its current position and speed. Then, it calculates the estimated position of all its neighbors, according to the same time $t$. The node with the closest estimated position to that of the destination after the time $t$ is selected for the next hop.

Fig. 14 shows a scenario when the source node UAV $S$ selects the next hop according to the predicted position of its neighbors (UAV $J$ and UAV $K$) and the destination node UAV $D$ estimated after a time $\Delta t$. We clearly see that the predicted position of the neighbor node $J$ will be closer than neighbor $K$ to the destination UAV $D$ after time $\Delta t$. Therefore, the node UAV $J$ will be selected as the next hop to deliver the data packet to the destination UAV $D$. However, when the network is sparsely connected and there are no neighboring nodes, UAV $S$ continues to keep the packet until the target destination $D$.

- **Advantages of GRAA:** The routing process employed by GRAA exploits a time-based movement prediction of the nodes in order to enhance the performance of the position-based routing. In addition, GRAA provides the possibility to carry the data packets when the network is partially connected increasing the delivery ratio.

- **Weaknesses of GRAA:** In reality, the random mobility model adopted by GRAA cannot be respected all the time due to various factors in the environment where the nodes are deployed. For instance, the weather conditions, obstructions,
or mission updates, can modify the predefined route information of the nodes resulting in severe packet losses.

- **Future improvements of GRAA**: GRAA needs to be improved by adding a maintenance mechanism, which can find alternative solutions when the nodes change direction and modify the planned route. Furthermore, prediction methods can be used to define the future positions of the nodes in real-time according to the conditions of the network. A path plan mobility model can also be the suitable solution to completely exploit the adopted prediction method. Also, the greedy forwarding can be added to reduce the use of the store-carry and forward technique, and therefore, reduce the delay of delivery.

- **Potential applications of GRAA**: Among the applications where the GRAA protocol is most suitable are the mission-based applications. Indeed, the nodes move along predefined routes and the selection of next hops used by GRAA is done automatically facilitating the transmission of crucial information.

4.3.3. Heterogeneous routing

As indicated by their names, these FANET protocols maintain the interaction between UAVs and different kinds of nodes on the ground regardless of whether the nodes are fixed or are mobile. Many benefits are provided by the use of this architecture. At a first step, it can extend the coverage of the sub-network located on the ground. In addition, the fixed nodes on the ground can provide a reliable backbone network and a higher bandwidth to enable the maintenance and to better control these nodes. Various applications can be distinguished according to whether the information is shared between the nodes and the goal of the data exchange. For instance, in VANETs, nodes on the ground can be assisted by UAVs to improve the robustness and reliability of the data delivery. In addition, UAVs can be used as one team to accomplish certain tasks (as mentioned before) or to be used as sensors for different applications. Some protocols are presented here.

1. **Connectivity-based Traffic Density Aware Routing using UAVs for VANETs (CRUV)** [21]

Oubbati et al. proposed Connectivity-based Traffic Density Aware Routing using UAVs for VANETs (CRUV) [21], which is the improved version of [113,114] and is initially inspired from [115]. It is a delay tolerant protocol based on the periodic exchange of Hello packets between vehicles. This exchange allows vehicle on the ground to calculate the most connected segment among their neighboring segments. Then, the connectivity information about their neighboring segments will be shared with the existing UAVs, in order to have a global vision of all the segments around. UAVs exchange this information with all vehicles located at each intersection allowing them to take an efficient routing decision when there are data packets to deliver. In addition, UAVs can be selected as forwarding nodes in the case where the network is sparsely connected.

Fig. 15 shows a scenario when a source vehicle wants to send a data packet to the destination vehicle based on the UAVs in the sky. The source vehicle selects UAV to deliver the data packet where there is a connected segment. The UAV checks if there is a connected segment around, if yes, this segment will be selected to deliver the data packet. Otherwise, the data packet will be sent directly to the target destination if it is within the transmission range of the UAV.

If the current node is not located on an intersection, CRUV first tries to get the closest intersection in order to start calculating scores for different segments around. If there is at least one connected segment, it will be selected to forward the data packet. Otherwise, the closest UAV in range will be selected to transmit the data packet to the target destination. In the case when no forwarder is found, the current node will carry the packet until a possible neighbor is found in order to submit the carried data packet to it.

- **Advantages of CRUV**: The UAVs assist the routing process by finding connected segments when the current vehicle does not find any connected segment at the current intersection. Moreover, UAVs can be used as relays when the network is poorly dense on the ground.

- **Weaknesses of CRUV**: As a drawback, CRUV does not take into account the real distribution of vehicles on the selected segments which is very crucial to measure connectivity factor. Furthermore, when there is a disconnection, CRUV will use the store-carry-and-forward technique as a recovery strategy resulting in an important delay of delivering.

- **Future improvements of CRUV**: UAVs in CRUV can only act as relays or having a global knowledge about the connectivity of the segments around. Nevertheless, in the case when a disconnection occurs, the existing UAV can act at a relay only if it is in the range of the current vehicle on the ground. Consequently, the protocol needs to be improved in such a way that the UAVs place themselves in order to allow relaying data when a disconnection is detected on the ground.

- **Potential applications of CRUV**: Since the UAVs can increase the chances to find at each moment a connected segment to ensure a continuous connectivity to the target destination, it is preferable to use CRUV as a support for Internet access application.

2. **Load Carry and Deliver Routing (LCAD)** [97]

Le et al. proposed Load Carry and Deliver Routing (LCAD) [97], which uses a new mechanism in flying ad hoc networks using UAVs to enhance the connectivity. In this protocol, the technique of store-carry-and-forward is used uniquely by the UAVs in order to efficiently improve the connectivity and packet delivery between two different routing protocols: Disruption Tolerant Network (DTN) in the sky and Ad hoc On Demand Distance Vector (AODV) [24] on the ground.

Fig. 16 shows the main functionalities of the protocol LCAD. When a source node (base station) has a data packet to send, it starts a discovery process on the ground until it gets at least one path to the target destination. If there is no path to the target destination, it means that the destination is located in
another area. In this case, LCAD will rely on the existing UAVs in the sky to deliver the data packet to the area where the destination is located using the store-carry-and-forward technique.

- **Advantages of LCAD**: LCAD provides network connectivity in sparsely connected networks by a routing technique based on UAVs. Indeed, the UAVs are used as carriers through the technique store-carry and forward in the case when there is no connectivity on the ground, in order to maximize the throughput while increasing security. Based on the controlled movements of UAVs, the data packets can be delivered anywhere the destination is located.

Oubbati et al. proposed UAV-Assisted VANET Routing Protocol (UVAR), which tries to address part of the CRUV's drawbacks. Indeed, the routing paths are progressively built by selecting road segments gradually at each intersection by calculating a score based on four parameters: (i) the connectivity, (ii) the traffic density, (iii) the distance between a pair of nodes (Current/Destination), and (iv) the real distribution of vehicles. All these parameters are calculated based on the exchanged Hello Packets between vehicles and the deployed UAVs over each road segment. By using UVAR, this technique is beneficial to overcome existing obstacles and to provide more alternative solutions when the ground network is sparsely connected. Furthermore, the real distribution of vehicles is taken into consideration, allowing to know the most regulated road segments to be selected as a routing path.

As shown in Fig. 17, the UAV deployed over the area of four road segments can have a global knowledge about all surrounding road segments (i.e., traffic density, real distribution of vehicles, and connectivity). The real distribution and connectivity degree of vehicles are calculated by UVAR more accurately based on the intercepted Hello packets exchanged by vehicles while overcoming the present obstacles. The Dijkstra algorithm is applied by the UAVs using the current vehicles' (i.e., source and destination) geographic locations, which are collected through the Hello messages sent out by these vehicles and intercepted by the UAVs, or directly calculated by the UAVs using location services. This distance represents the shortest distance between a source and destination vehicle along the road segments and through the road intersections. The score is recalculated at each intersection until data packets reach their target destination.

- **Weaknesses of LCAD**: The major disadvantage of this protocol is that UAVs do not use GPS information and trajectory calculation during route discovery and data forwarding. This can decrease the performance of the protocol in the case when the destination is not a fixed node.
- **Future improvements of LCAD**: As improvements which can be feasible in the future is the integration of geographical positions and trajectories of UAVs during the data delivery and the discovery process. This can be done using a reliable geo-information exchange scheme in order to support the latency and mobility.
- **Potential applications of LCAD**: LCAD can be easily adapted to insensitive-delay applications such as information collection, sensors, tracking mission, and reconnaissance.

4. **Predictive-Optimized Link-State Routing (P-OLSR)** [78]

Rosati et al. developed a new variant of OLSR protocol for the prediction of the link quality based on GPS information for FANETs called P-OLSR [78]. Indeed, the original version of OLSR is modified to share the geographical positions through the Hello packets. As a result, each node knows the position of its neighbors, which allows to calculate the expected transmission count (ETX) metric by a factor that takes into consideration the relative speed between the UAVs. ETX can be computed as follows:

$$ETX^{i,j} = \frac{\beta}{\frac{v_{i,j}^{\beta}}{r_i} + \frac{v_{j}^{\beta}}{r_j}}$$

where $\beta$ is a non-negative parameter and $v_{i,j}^{\beta}$ is the relative speed between node $i$ and $j$. $v_{i,j}^{\beta}$ becomes negative when...
the UAV $i$ and $j$ move closer to each other, and therefore, the ETX will be weighted by a factor smaller than 1. However, if the UAV $i$ and $j$ move far from each other, the relative speed is positive, thus the ETX will be weighted by a factor greater than 1. As a result, a link between two nodes that move closer is more adequate to a link between two UAVs that move far from each other, even if they have the same values of $F^j$ and $r^j$. The best value of $\beta$ depends on the cruise speed of the UAVs of the link coverage extension.

The ETX and link-quality sensing are important metrics to establish a stable and reliable link-quality by using the positions of the nodes to predict how the links evolve during the routing process. The combination of these two metrics is based on Hello packets in order to analyze the link quality and to flood it to the whole network. To do so, the Hello packet format is modified by adding several fields such as the GPS position of the node and the link quality of the neighbors.

- **Advantages of P-OLSR**: The OLSR routing protocol is extended to Predictive-OLSR, which exploits GPS information of the UAVs. This can be beneficial to be adapted to highly dynamic networks such as FANETs and to provide accurate information about the future state of the wireless links between the nodes during the routing process.

- **Weaknesses of P-OLSR**: There are still many issues worth studying such as the sudden disconnection and how to deal with this situation, and the recovery technique to apply in order to resume the normal function of the network.

- **Future improvements of P-OLSR**: As future work, a maintenance mechanism needs to be conceived to deal with disconnections when they occur.

- **Potential applications of P-OLSR**: According to the simulation and the adopted mobility model by P-OLSR, it can be ideally suited for reconnaissance mission or film-making applications, moreover, it can also be an ideal support for real-time applications since it does not suffer from important delays.

5. **Position-Aware, Secure, and Efficient mesh Routing (PASER)**

Sbeiti et al. proposed a novel secure routing protocol for FANETs in order to achieve a good compromise between security and performance. PASER looks for keeping and maintaining accurate routing paths between valid nodes. In addition, PASER can quickly exclude malicious nodes which do not belong to the network and try to manipulate the routing process or to join the network. In the case of key compromise, the keys should be dynamically refreshed. The detection of malicious behaviors is based on a centralized approach implemented at the ground station. To be more clear, malicious behaviors are detected based on the modification of a UAV from its expected behavior and on the anomaly in its key performance indicators.

As illustrated in Fig. 18, from the routing side, the requesting node broadcasts a RREQ packet in the whole network. Then, intermediate nodes, which received the RREQ packet, are already registered, know the routing path to the target destination, and forward the RREQ unicastly to the destination. At the reception of the RREQ, the target destination sends a RREP unicast to the requesting node, and the routing path will be established. However, from a security side, non-trusted one-hop neighbors (e.g., Links between S-A and S-B) use the PASER asymmetric scheme to secure the exchanged messages in order to establish a trust relationship (i.e., untrusted messages secured with asymmetric-key-based cryptographic algorithms), while trusted one-hop neighbors (e.g., all other nodes but S) mainly use the PASER symmetric scheme (i.e., trusted messages secured with symmetric-key-based cryptographic algorithms).

- **Advantages of PASER**: The efficiency of PASER is demonstrated in a simulation-based and in the theoretical analysis of its route discovery process, and its scalability according to network size. Furthermore, its security side has proven its efficiency in highly dynamic networks such as FANETs.

- **Weaknesses of PASER**: A high overhead and delay are distinguished in the experimental side due to the control packets used during the discovery process.

- **Future improvements of PASER**: The performance of PASER may be further enhanced using a robust routing technique minimizing the routing overhead and the flooding process while ensuring a high level of security. This can optimize the routing performance and network security.

- **Potential applications of PASER**: UAV-assisted applications can be deployed in various scenarios, and especially the applications which need an interconnection between the UAVs and their ground control stations and Internet. This combination is beneficial to put on the field in a realistic way such routing protocol.

6. **Secure UAV Ad hoc routing Protocol (SUAP)**

Maxa et al. proposed a secured routing protocol for FANETs, which is a security extension of the AODV protocol. It is based on digital signatures for static fields such as the IP addresses of the source and destination and hash chains for dynamic fields such as hop count. When a generated routing packet has to be sent, it must be signed and checked by the nodes receiving the packet using the sender’s public key. Nevertheless, the
hop count cannot be signed during transmission, because it has to be incremented at each hop. Consequently, a technique based on hash chains is applied. This leads us to say, that the SUAP protocol is vulnerable to wormhole attacks. As a result, geographical leashes are used to calculate the correlation between the transited distance and the hop count value. In order to do so, each node has to maintain a local connectivity with its direct neighbors. When transmitting packets, each node includes its current geographical location. To protect from malicious modifications, message fields are signed (including the geographical location).

To exemplify the functionality of the SUAP protocol, we consider the scenario in Fig. 19. There are two attackers A1 and A2 while the GCS (Ground Control Station) plays the role of the victim. The GCS initiates the discovery process by flooding a RREQ packet, and then, each node sends the RREQ unicastly to its direct neighbors. The two attackers carry out a colluding attack. The first attacker records packets at a certain geographical position and replays the packets at the second attacker using a high-speed private network existing between the attackers. This private network linking the attackers can be considered as a wormhole. Due to the broadcast nature of SUAP, attackers are able to intercept the broadcasted data packets. To address this issue, a set of verifications based on the SUAP protocol is carried out in order to detect the wormhole link by comparing the hop count value present in the packet and the hop count value computed based on the traveled distance. If there is a difference the packet will be immediately dropped.

- **Advantages of SUAP**: SUAP protocol has proven its efficiency to protect the route discovery process, providing authentication, non-repudiation security services, integrity, and additional security features against wormhole attacks based on the geographical leashes method.

- **Weaknesses of SUAP**: As a routing protocol, SUAP does not provide any efficient method to deal with the high mobility of the network and to recover against the frequent disconnections while ensuring a secure exchange of data packets.

- **Future improvements of SUAP**: Different methods can be included to focus on the routing side and their different issues such as connectivity, packet losses, and the frequent change of the topology. Geographical localization along with predic-

7. **Cross-layer Link quality and Geographical-aware beaconless opportunistic routing protocol (XLinGo)** [76]

Resario et al. proposed A Cross-layer Link quality and Geographical-aware beaconless opportunistic routing protocol (XLinGo), which improves the transmission of simultaneous multiple videos flows over FANETs by creating and keeping reliable persistent multi-hop routes. In order to deal with the frequent link failures and the node’s mobility, XLinGo combines a set of human-related and cross-layer parameters for routing decisions, such as residual energy, queue length, geographical locations, link quality, and packet delivery ratio. The concept of Dynamic Forwarding Delay (DFD) is adopted by XLinGo to select the next forwarder. Indeed, when the source node broadcasts a data packet, the next relays within the forwarding area compute a DFD value based only on the location information of the current node. Therefore, the closest node to the target destination generates the shortest DFD and forwards the packet first.

As an illustration, we take the example of Fig. 20. When a source UAV S wants to transmit a video flow to a mobile or a fixed node D where its location is known, it includes its own location and that of the destination in the packet header and broadcasts it to all its neighbors (i.e., A, B, C, and E). Once the packet will be received by the S’s neighbors, XLinGo has to select only one UAV to forward the received packet. This is accomplished in a distributed manner by the neighbors by calculating different parameters such as DFD, the required energy to move and transmit packets, and also by limiting the zone (called forwarding area) in which UAVs are allowed to forward the packet.

According to the geographical positions included in the packet header, two forwarding areas can be established: (i) **PPA** (Pos-
itive Progress Area) and (ii) NPA (Negative Progress Area), which define the closest neighbors and those far from the destination $D$, respectively. Each neighbor within the NPA has to drop the received packet since nodes within the PPA are considered as the most adequate to be the relays. In our case, the UAV $E$ obtains the smallest DFD value and updates the location information of UAV $S$ included in the packet header with its own location and the algorithm continues until the packet reaches UAV $D$. An acknowledgment is sent back to $S$ by $E$ in order to send unicastly the subsequent packets.

- **Advantages of XLinGo**: A routing path is created when a node wants to send a video to another node. The video is broadcasted in the form of frames, then the neighboring nodes establish a random wait time in order to retransmit the frame to the next hop. This can avoid the problem of congestion and reduces the bandwidth overhead. Once a routing path is established, it is then used with unicast packets minimizing considerably the overhead.

- **Weaknesses of XLinGo**: In the series of tests carried out during the simulation, there is only one agent producing a video. Consequently, the impact of interference from multiple sources is not taken into consideration and it is not studied.

- **Future improvements of XLinGo**: XLinGo can be improved in a different way for both the routing and multimedia sides. For instance, general rules of routing have to be defined to minimize the broadcast and therefore the overhead. Moreover, the interference from multiple sources of video needs to be taken into account during the experiments.

- **Potential applications of XLinGo**: In general, multimedia applications which need a minimum of QoS requirements can be better supported by XLinGo.

5. Comparison of FANET protocols

The routing protocols differ from each other by taking into consideration specific parameters. As shown in Table 6, the FANET routing protocols are categorized according to the used delivery strategies. In addition, all the reviewed routing protocols assume the use of the GPS to define the geographic positions of the nodes. A location service is supposed to be used by the majority of the routing protocols to calculate the position of each node in the network, and especially destination nodes. For the knowledge of the neighboring nodes (i.e., position, speed, trajectory, etc.), neighbors’ tables are maintained and updated periodically particularly by the protocols using a prediction technique. It is known, in certain cases, FANET nodes can communicate with infrastructure on the ground in order to get or to transmit certain information, which is applied by the heterogeneous protocols. Certain protocols assume that they have a global vision about the region, which allows routing protocols to avoid certain constraints like obstructions which prevent direct communications between the nodes.

As for the evaluation features, each proposed protocol has to be tested, validated, and classified according to its drawbacks, kind of nodes, and the obtained results from the simulation. Different simulation tools are used, which may vary from a protocol to another, depending on the used techniques which require certain packages or functionalities. These tools can generate the movements of each node in the simulation scenario based on different criteria such as scenarios, environments, and applications. Different metrics are calculated in each simulation scenario for each routing protocol to study its behavior and to compare them with other protocols using the same calculated metrics. These metrics differ from a protocol to another according to the used techniques and strategies. According to the simulation outcomes, several limitations can be found or deducted in each routing protocol concerning its functioning. For instance, the limitations can be the problems of disconnection, congestion, and overhead, which are caused by different factors such as the used data delivery strategies, the control packets, and their broadcasting frequency. Finally, the environment and kind of nodes where the routing protocol is deployed to support their communications or their data exchanges. In certain cases, the network can be heterogeneous (i.e., many types of nodes can exchange data packets between each other).

As for the performance metrics, generally, six major metrics are used to evaluate the performances of the FANET routing protocols [19]:

1. **Packet Delivery Ratio (PDR)**: defined as the ratio of packets successfully delivered, i.e., the percentage of all data packets received by the receiver to all data packets generated from the senders. The bigger is $PDR$, the better is the performance of the protocol.

2. **Average End-to-End Delay (EED)**: the average time for data packets to reach the target destinations. It also includes the time taken by the discovery process in the case of reactive protocols, and the tail of data packets delivering. Only the data packets successfully received and generated are counted. The smaller is $EED$, the better is the performance of the protocol.

3. **Average number of Hops (H)**: defined as the number of data packets delivered divided by the number of hops performed by all packets. As a general idea, consumption of resources increases as the number of hops increase. The smaller, the better.

4. **Overhead (O)**: the ratio of control routing packets to the successfully delivered packets at receivers. This metric shows the degree of saturation of the network. The lower, the better.

5. **Throughput (T)**: the number of data packets successfully delivered to the target destination during a given amount of time (generally 1 (s)). The bigger is $T$, the better is the performance of the routing protocol.

6. **Latency (L)**: the measure of time taken by a data packet to transit between a pair of nodes in a given network. The lower, the better.

Table 7 gives the method of calculation of each one.
Table 6  
FANET position-based routing protocols (comparative study).

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Reactive-based</th>
<th>Greedy-based</th>
<th>Delay tolerant (DTN)</th>
<th>Heterogeneous</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ARPAHM [81]</td>
<td>RGR Ref. [98]</td>
<td>LAROD Ref. [94]</td>
<td>LCAC Ref. [97]</td>
</tr>
<tr>
<td></td>
<td>GMDOR Ref. [111]</td>
<td>GMDR Ref. [80]</td>
<td>CRAA Ref. [80]</td>
<td>P-QLSR Ref. [78]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>PASER Ref. [68]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SIAP Ref. [69]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>XLinGo Ref. [76]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>UVAR Ref. [20]</td>
</tr>
<tr>
<td>Store-carry-and-forward Greedy forwarding</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Path discovery</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Single path</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Multi-path</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Predictive Recovery strategy</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Location service</td>
<td>√</td>
<td>×</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>GPS</td>
<td>√</td>
<td>×</td>
<td>√</td>
<td>×</td>
</tr>
<tr>
<td>Neighbors Table</td>
<td>√</td>
<td>×</td>
<td>√</td>
<td>×</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>×</td>
<td>×</td>
<td>√</td>
<td>×</td>
</tr>
<tr>
<td>Environment awareness</td>
<td>×</td>
<td>×</td>
<td>√</td>
<td>×</td>
</tr>
<tr>
<td>Mobility model 1</td>
<td>Modified RWP</td>
<td>RM</td>
<td>Gauss–Markov RM</td>
<td>PR</td>
</tr>
<tr>
<td>Mobility generator</td>
<td>OPNET</td>
<td>JAVA</td>
<td>NS-2</td>
<td>RWP</td>
</tr>
<tr>
<td>Simulation tool</td>
<td>OPNET</td>
<td>Aero-MANET</td>
<td>INET</td>
<td>NS-2</td>
</tr>
<tr>
<td>Evaluation metrics 1</td>
<td>P, D, O</td>
<td>P, T, L</td>
<td>P</td>
<td>P, D, D, D, D</td>
</tr>
<tr>
<td>Latency</td>
<td>Low</td>
<td>Unknown</td>
<td>NEL, C</td>
<td>D, C</td>
</tr>
<tr>
<td>Follow-backs 1</td>
<td>FANET</td>
<td>FANET</td>
<td>FANET</td>
<td>D, C, O</td>
</tr>
<tr>
<td>Type of network</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 Evaluations metrics (P: Packet Delivery Ratio, D: End-to-End Delay, O: Overhead and H: Average number of hops).</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 Follow-backs (GFL: Greedy failure, O: Overhead, C: Congestion, D: Delay, NEL: No expiration links and IFL: Infrastructure failure).</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 7
The major evaluation metrics for routing in FANETs.

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Methods of calculation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet delivery ratio (PDR)</td>
<td>( PDR = \frac{</td>
</tr>
<tr>
<td>Average end-to-end delay (EED)</td>
<td>( EED = \frac{T_{p_i} - T_{p_i}}{P_i} ), where ( T_{p_i} ) is the time of reception of the packet ( p_i ) and ( T_{p_i} ) is the sending time of the packet ( p_i ).</td>
</tr>
<tr>
<td>Average number of hops (H)</td>
<td>( H = \frac{\sum_{i=1}^{P} H_{p_i}}{P} ), where ( H_{p_i} ) is hops made by packet ( p_i ) before reaching its receiver.</td>
</tr>
<tr>
<td>Overhead (O)</td>
<td>( O = \frac{M}{P} ), where ( M \subset P ) and (</td>
</tr>
<tr>
<td>Throughput (T)</td>
<td>( T = \frac{P_i}{Time} ), where Time is the given time of period where the data packets are successfully received by the same destination.</td>
</tr>
<tr>
<td>Latency (L)</td>
<td>( L = Time_{p_i} - Time_{p_i} ), where ( Time_{p_i} ) is the sending time of the data packet, and ( Time_{p_i} ) is the time of reception of the original packet that was sent at ( Time_{p_i} ).</td>
</tr>
</tbody>
</table>

6. Challenges and future research direction

FANET architecture is under a continuous development, since the research over this kind of highly dynamic networks is not complete on several levels, and the routing is an exception. Communications between UAVs always remain the most challenging task, because the existing routing protocols proposed for MANETs as well as VANETs cannot satisfy the unique requirements of FANETs, and consequently, they cannot be the suitable solutions for the data delivery in FANETs. Finding a single routing scheme able to adapt to all the unique characteristics of FANET, and at the same time, provides perfect outcomes is very hard and quasi-impossible. Although there is a wide range of proposed routing solutions, there still exist several issues that have not been resolved. For instance, in terms of FANET nature and communication environments, most of the routing protocols were not proposed by considering these crucial details. Moreover, other routing protocols have not functioned perfectly under a network severely partitioned and cannot cope with the security requirements, where the nodes are exposed to any kind of attack. To overcome such issues, different details should be considered further in designing FANET routing protocols. In each next subsection, we first outline the lessons learned from this research work. Then, we identify several open challenges that need a deep study. And finally, we propose future directions to overcome the highlighted challenges and to help scientists exploring novel solutions in making the routing process in FANETs efficient, reliable, and secure.

6.1. The network’s frequent disconnections

Practically, FANETs are characterized by a low density of their nodes, which are moving at a high degree of mobility. Consequently, the topology of the network changes frequently and the communications links between the nodes cannot remain stable during all the time. These can result in severe fragmentations, and therefore the network can be considered as partially connected. Consequently, it can negatively impact the routing efficiency and performance since the data exchange between the communicating nodes needs to be done using the availability of relays and the wireless links connecting them all along the routing path.

The intermittent connectivity of the network makes the routing challenge in FANETs more complex and difficult to be implemented. Indeed, the dynamic change of the topology raises several issues such as packet losses and high delay of delivery impacting seriously the routing performance. Another challenge is the fact that the overhead of discovering a routing path must be paid at each disconnection, which can also dramatically decrease the performance of the network.

Future routing solutions have to take into account this challenge by adopting the appropriate techniques or using, for instance, another kind of fixed or mobile nodes located on the ground. Since the movements of UAVs are controlled, their adequate placement can also play a key role in order to remedy this problem of partition [116–119]. Therefore, developing new methods of communications should consider the coverage of the entire network. Despite the recent propositions made in FANET routing, additional research studies are still required in order to find suitable techniques to avoid the network partitions and increase the delivery ratio of data packets.

6.2. Security requirements

Like any networks, FANETs are not free from dishonest nodes which make the security of such networks a critical issue. Indeed, if the UAVs are hijacked, they can be used as a weapon or as something more dangerous. In addition, when certain applications are targeted by an attack, it may have disastrous consequences. The network layer is considered as a building block to support the majority of FANET applications, and therefore, it is not reasonable to let future routing protocols ignore this critical issue when so many serious attacks are targeting this layer. Moreover, the characteristics of FANETs make secure routing a more important challenge than in the case of other highly dynamic networks.

Crucial information is exchanged between FANET nodes, and compromising them has catastrophic outcomes. Various FANET security challenges still need to be addressed, especially in the areas of authenticity. Indeed, scalable authentication methods are needed to protect the FANET nodes from inside or outside malicious nodes infiltrating the network using a false identity. Furthermore, all kinds of attacks should be identified, and particularly those which introduce misinformation into the network.

Further studies need to be carried out to design security methods to make the proposed routing protocols more secure. The majority of the proposed routing protocols focuses essentially on the performance improvements, and do not provide any defense against attacks or malicious attackers. Only a few secure routing protocols are proposed in the literature [68,69,120,121], hence the necessity to propose new routing solutions including security components. Future studies should, for instance, consider other issues like ensuring the security at the network layer and prevent other popular attacks like spoofing attacks or denial of service. Novel encryption techniques, operating at high speeds are more suited than traditional public key-based solutions which penalize the network with overheads and additional delays during the encryption of exchanging messages.

6.3. Simulation and experiments

More and more simulation tools and testbeds are used to evaluate existing solutions about UAVs and FANET in general [122–124]. Nevertheless, the majority of them do not provide reasonable and realistic outcomes, due to their negligence of many known characteristics of this kind of network. For instance, in most of the cases,
OPNET, NS-2, and OMNeT++ are used to evaluate the performances of protocols dedicated for FANETs. All these tools do not provide a specified channel of communications between UAVs and do not support 3D communications which are crucial parameters for UAV design. Consequently, a set of modifications is always required for these tools to model all these requirements. Moreover, most of the simulation tools also generate non-path plan mobility models of UAVs (i.e., random mobility models), which does not allow to better control the movement of UAVs.

The implementation of FANET routing protocols needs to be more credible and realistic and uses reasonable assumptions. In this review, we have observed that most of the simulations take into consideration only the important behaviors of the proposed techniques while neglecting certain details which can really change the outcomes. Based on the reviewed papers, we have identified that 12 works out of 33 used their personalized simulator. The use of such simulators does not allow either to reuse the code or to compare with different proposals. Consequently, the selection of a simulator tool does not impact the outcomes of simulation experiments, but it suggests the use of a certain set of default values and models, which are included in the widely known simulators.

A unique simulation tool or package should be designed in order to unify the parameters so that to apply verification methods for all the FANET proposed solutions to determine their proof of correctness and complexity. In addition, more realistic mobility models need to be designed for predefined situations in order to get more realistic results both in the data exchange and evaluation criteria. Therefore, the mobility of UAVs, as well as the simulation tools, still remain open issues for future research works in order to evaluate accurately the routing protocol performances and to be fairly compared with other routing proposals. Recently, the researchers encourage to do the simulation in real environments based on testbeds to study more situations not available in the simulation tools.

6.4. Routing techniques

The data exchange between UAVs faces serious issues, which are quite different from those distinguished in MANET or VANET. The UAVs should be able to have a real-time global knowledge of the dynamic topology of a network like FANET. This is why the proposed routing solutions for FANETs or even the techniques of the data delivery taken from MANET and VANET have to deal with these challenging constraints. Moreover, in the majority of cases, only a single routing technique is adopted by a given routing protocol, which is not sufficient regarding the dynamic nature of FANETs. Consequently, it is preferable that the routing protocols could deploy the suited technique in a given kind of the network situation. Nevertheless, it is observed that each technique provides favorable results in certain scenarios, but it has its own drawbacks in other ones.

Among the most drawbacks distinguished in the simulation results of the reviewed protocols is the additional delay under the constraints of the high speeds of UAVs, their unreliable connectivity, and the dynamic topology of the network. The design of routing protocols while respecting a restricted delay threshold is considered a challenging issue. In addition, the extra overhead noticed in most position-based reactive protocols is due to the flooding process employing additional control packets. Minimizing or making the overhead and the congestion at a constant level is also considered a challenging issue, especially for the reactive-based and beacon-based protocols. Finally, the packet losses are due to various causes, which may be technical (e.g., routing techniques, prediction methods, etc.) or environmental (e.g., obstacles, mountains). Therefore, the challenge is to minimize the packet losses, while satisfying a set of predetermined performance constraints such as bandwidth, delay, and overhead.

To remedy to the challenge of delay, a further study should be focused on the estimation of the delay of each path before a routing decision is made and to provide alternative solutions in the case of a path failure. Furthermore, most of the studied prediction techniques are exclusively based on the future positions and speeds of the nodes, but an effective way is to add more criteria to maximize the number of alternative solutions. Another future study should be concentrated on the minimizing of the flooding process and to make it intelligent in order to reduce the overhead. This can be done, for instance, by updating routing tables dynamically according to the topology changes of the network. Consequently, there is a crucial need to develop efficient routing techniques which provide at least a flexible behavior with the topology of FANET. Furthermore, a minimum level of performances has to be defined to guarantee the efficiency of the proposed routing schemes.

6.5. UAV coordination

Certain applications require the coordination of several UAVs to be done efficiently, and in most cases, in a timely manner (e.g., search and rescue missions). However, this requirement is not always an easy task, due to the unique characteristics of FANETs such as the high mobility and the network partitions. Also, this kind of cooperation needs a minimal of constant connectivity between the nodes in order to exchange crucial information to accomplish a given mission with an accurate way. Moreover, a certain level of QoS is required to support their right functionality and to provide a certain satisfaction to a set of requirements imposed by some performance constraints of services such as bandwidth, packet losses, delay restriction, jitter, etc. All these requirements along with a robust routing protocol constitute a keystone to support and make efficient the UAV coordination.

Two kinds of architectures can put on the field several cooperating UAVs in order to accomplish a specific mission. Firstly, the distributed architecture which is based on several UAVs exchanging messages between each other with the unique aim to be achieved. However, several limitations have been observed such as the adoption of inappropriate mobility models, which can distort the expected results, and in certain cases, make them impossible to be accomplished. Another problem with this architecture is that it assumes that a permanent connectivity exists between the nodes, which is not always true. Secondly, the centralized architecture which is based on human-centered in ground stations in order to organize and distribute the tasks among UAVs and to take the decisions. But, in spite of these additional features, this architecture is not immune to human errors and the possible incidents that may occur at the ground station.

Many improvements could be explored and brought to the paradigm of UAV coordination such as efficient path plan mobility models, strategies of communication, and the flexibility to the environment. These future studies would have to be covered by a robust routing protocol able to ensure a minimum level of the data exchange accuracy necessary for the UAV coordination [38,125].

6.6. UAV-to-VANET communication

UAVs are composed of a variety of essential devices providing various functionalities such as wireless communications, controlled movements based on algorithms, and a global knowledge on the ground activities. This kind of intelligent nodes can be the suitable choice to improve the connectivity and to serve terrestrial mobile nodes [126]. Hence, air-to-ground communications allow to exchange information with nodes located on the ground, to direct
and coordinate its actions from the air, and guaranteeing a high level of radio coverage, which is not always ensured by terrestrial mobile nodes. Therefore, this kind of communications is beneficial to develop more intelligent connected nodes in the future using UAVs.

The last three years (i.e., since 2014), scientists opened a new avenue of research on the possibility to use UAVs to assist VANETs on the ground and to coordinate specific actions. It is expected that UAV-to-VANET communications will make it possible to surpass the constraints detected in a conventional VANET. However, there are still many challenges in the implementation and deployment of such architecture. Currently, the ideal number of UAVs deployed over VANETs area is considered as an important issue. Indeed, according to the existing case of disconnections on the ground, a specific number of UAVs should be defined to bridge the communication gap whenever it is possible. Therefore, the regulation of UAV number has to be investigated by considering different situations of VANET sparseness. Based on different experiments and simulations carried out in [19–23,51], the mobility of UAVs in the sky seems to be completely uncontrolled, which can be considered as a crucial issue to get the expected results. Moreover, the wireless communications between UAVs and vehicles on the ground should be standardized in order to reduce the problem of frequency congestion and to unify the way of communications between the nodes [15].

This recently adopted architecture may be further investigated and enhanced in different sides in order to provide efficient outcomes. Indeed, further studies are required to be done in order to regulate the necessary number of UAVs able to carry out certain tasks in an optimal way. For instance, in the case of fragmentations in VANET, only one or two UAVs can be deployed to explore and estimate the number of disconnections on the ground and to define the sufficient number of UAVs to overlay the area. Furthermore, the movements of UAVs need to be organized using the different path plan mobility models or to customize novel mobility models according to the missions which are deployed for. The communications between UAVs and vehicles are also a challenging issue to be further studied. A new standard of communication needs to be established for this new kind of wireless links by defining a unified communication band since UAVs can be considered as full members belonging to the same network as vehicles. Finally, we can say that UAV-to-VANET communications are also among the worthwhile research issues to take into account since there is a reduced number of research works conducted on this topic.

7. Conclusion

In this survey, we have identified the characteristics of a large number of routing protocols for FANETs. In addition, their functionalities have been detailed based on descriptive figures. A comprehensive taxonomy of these surveyed protocols is provided, in which the routing protocols are classified into three main categories: (i) Topology-based routing protocols (ii) Swarm-based routing protocols, and (iii) Position-based routing protocols. A fully detailed comparative study is proposed to make the differentiation between the proposed routing protocols.

At the beginning of this survey, a presentation of a brief comparison between our work and some survey articles for FANETs proposed in the literature. After that, this work studies the architecture of FANETs by detailing their characteristics and their most popular applications, and then is concluded by presenting a short comparative study about FANETs applications. Also, we review the existing FANET routing protocols according to their techniques, features, routing evaluation metrics, and drawbacks, which allow us to decide which routing strategy is the most suitable to be adopted in a given situation. Finally, we discussed the main future challenges for scientists who would like to investigate in this research area. At the end of this survey, based on the global comparative study, we conclude that all the proposed protocols must deal with the high mobility and the low density of nodes, which are taken into account as important challenges. As a future work, which we are currently investigating is to conceive an efficient position-based delay tolerant routing protocol in order to overcome the intermittent connectivity of FANETs and to exploit the node mobility to resolve the problem of frequent packet losses.

Acknowledgements

This research was partially supported by grant # 31R012 from the UAEU Roadway, Transportation and Traffic Safety Research Center, and Campus France together with the Algerian Ministry of Higher Education and Scientific Research, PROFAS B+ scholarship 2016/2017. It has been partially conducted at LIA lab, University of Avignon.

References


