# Force-Based Self-Organizing MANET/FANET with a UAV Swarm

Saffre, Fabrice; Hildmann, Hanno; Anttonen, Antti

*Published in:*
Future Internet

*DOI:*
10.3390/fi15090315

Published: 01/09/2023

*Document Version*
Publisher's final version

*Please cite the original version:*
Saffre, F., Hildmann, H., & Anttonen, A. (2023). Force-Based Self-Organizing MANET/FANET with a UAV Swarm. *Future Internet*, *15*(9), Article 315. https://doi.org/10.3390/fi15090315

*future internet*

*Article*

# Force-Based Self-Organizing MANET/FANET with a UAV Swarm

**Fabrice Saffre [1,*], Hanno Hildmann [2,3] and Antti Anttonen [1]**

[1] VTT Technical Research Centre of Finland Ltd., Tekniikantie 21, Otaniemi, 02150 Espoo, Finland; antti.anttonen@vtt.fi
[2] Intelligent Autonomous Systems Group, TNO Netherlands Organisation for Applied Scientific Research, Oude Waalsdorperweg 63, 2597 AK The Hague, The Netherlands; hanno.hildmann@tno.nl
[3] Smart Sensor Systems Research Group, Department of Mechatronics, The Hague University of Applied Sciences, Rotterdamseweg 137, 2628 AL Delft, The Netherlands
* Correspondence: fabrice.saffre@vtt.fi

**Abstract:** This paper introduces a novel distributed algorithm designed to optimize the deployment of access points within Mobile Ad Hoc Networks (MANETs) for better service quality in infrastructure-less environments. The algorithm operates based on local, independent execution by each network node, thus ensuring a high degree of scalability and adaptability to changing network conditions. The primary focus is to match the spatial distribution of access points with the distribution of client devices while maintaining strong connectivity to the network root. Using autonomous decision-making and choreographed path-planning, this algorithm bridges the gap between demand-responsive network service provision and the maintenance of crucial network connectivity links. The assessment of the performance of this approach is motivated by using numerical results generated by simulations.

**Keywords:** MANET; swarm intelligence; self-organization; UAVs; drones; swarms; swarming

**Citation:** Saffre, F.; Hildmann, H.; Anttonen, A. Force-Based Self-Organizing MANET/FANET with a UAV Swarm. *Future Internet* **2023**, *15*, 315. https://doi.org/10.3390/fi15090315

Academic Editors: Nouman Ashraf and Sachin Sharma

Received: 30 June 2023
Revised: 11 September 2023
Accepted: 15 September 2023
Published: 19 September 2023

## 1. Introduction

With ever-improving and advancing technology, we are amid a communication revolution, a period of fundamental paradigm shift that arguably started decades ago, either with the invention of the Internet or the personal computer. From the ability to communicate electronically across a network of computers connected by cabled Internet, we moved to using wireless connections; and, with that, came the opportunity to create network connections relatively *ad hoc*. Customers in a coffee shop, for example, can establish a connection with the local router and access the Internet that way.

The next step was the use of mobile resources, such as routers placed on other hardware, that, through the movement of their platform, moved into and out of positions that made them suitable nodes in Mobile Ad Hoc Networks (MANETs). Although such networks were originally comprised of nodes placed on other devices and systems, and thus subject to the connections created accidentally or as a byproduct of the operation of these devices and systems, the use of dedicated mobile platforms tasked primarily with the movement of nodes is finding increased attention in the literature.

### 1.1. Mobile Ad Hoc Networks (MANETs), Flying Ad Hoc Networks (FANETs)

The principle underlying MANETs is related to wireless connectivity, and that any device that also has access to a cabled connection to the broader infrastructure can relay traffic from other wireless-only devices if they are within the coverage area of the device. This has the potential to make wireless networks flexible and more resilient to failures [1]. Due to this potential, MANETs are currently deployed in commercial [2,3], as well as in military [2,4,5], and in civil [6,7] security [8] applications and have spawned specialized sub-fields such as Vehicular Ad Hoc Networks (VANETs) [2,9–11].

The dynamic and continuously evolving nature of wireless ad hoc networks that make use of mobile routers or relays is a driving factor in their usability and success. It is, however, also posing challenges as the dynamic topology of the network requires continuous re-evaluation of the routing within the network [3,5]. The less the nodes are acting predictably, the more robust a network will have to be if it is to ensure connectivity at all times [12,13]. Research into adaptive routing algorithms for dynamic topologies has received a lot of attention in the literature [14–17]. In a more recent development, drone technology comes into play: Unmanned Aerial Vehicles (UAVs) are increasingly considered to be platforms for the routers of a Flying Ad Hoc Network (FANET) [1–3,6,18]. The potential benefits of deploying drones actively ensuring MANET or FANET connectivity and cooperating as a swarm to optimize coverage are significant [6].

### *1.2. Using Drones to Deploy MANETs*

With advancements in technology, drones are increasingly being recognized for their potential in supporting MANETs [1]. They present a viable solution for enhancing connectivity, particularly in hard-to-reach or infrastructure-less environments, such as wilderness areas or in the aftermath of a disaster [19] (see Figure 1).

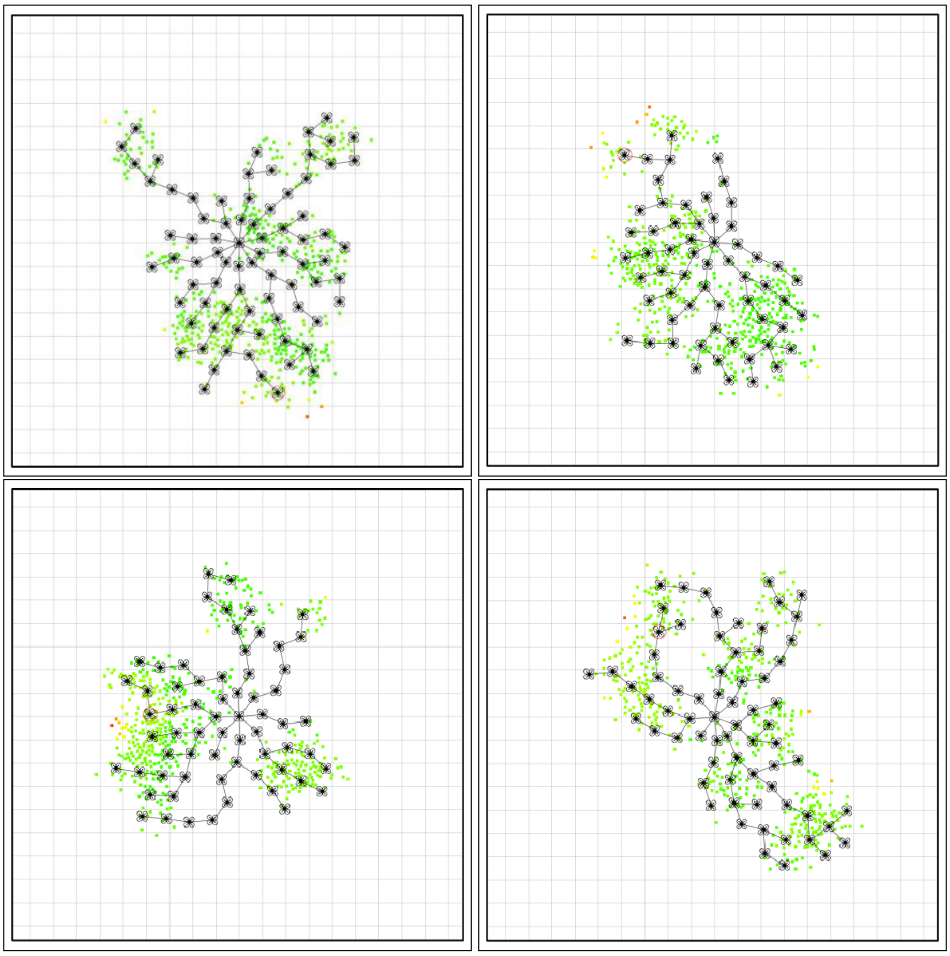

**Figure 1.** Four screenshots showing a deployed MANET servicing all the clients (the stress is indicated by color, with the continuous spectrum ranging from bright green (where the Link Quality Metric (LQM)→1), over yellow (for a LQM value of ≈0.5) to red (when LQM→0)). This sequence of screenshots shows the response of a single swarm to successive relocations of the clients.

Given their airborne nature and inherent mobility [20], drones are not hindered by ground obstacles. In addition, they can be equipped with wireless communication devices and employed as mobile nodes or access points within a MANET. This allows them to adapt and reconfigure the network's topology dynamically, and intentionally and to do so in direct response to changes in user demand or in environmental conditions. The use of drones in MANETs offers several key operational advantages:

- Flexibility of resource sourcing and maintenance: since the collective of drones (the swarm) is comprised of physically distinct and independently operating devices, the deployment of such a swarm (including the addition and removal of drones during operation) can be very flexible. The operations are the sum of the actions of independent units, which allows for different stakeholders and operators to pool their resources while each maintaining separate responsibility and ownership for the resources they contributed. Especially in cases where large-scale infrastructure, beyond the financial or operational resources of any one party, has been rendered inoperable, this enables smaller parties to come together and collectively solve a problem/provide a service.
- Adaptive network topology [7,16]: when drones are launched with the express goal of becoming members in a MANET, their movement can be designed to contribute to this goal. Due to this, drones that have no other objective can collaborate with those that do by optimizing their position to improve the overall performance of the MANET. This strengthens the ability of the MANET to respond to changing demand profiles and to client terminal movement.
- Exploiting advantages of aerial positions: purely through their ability to move in 3D space, drones can assume positions that offer advantages due to (a) not being restricted by obstacles on the ground (regarding signal transmission), (b) not being affected by conditions on the ground (with regard to the safety of the device). This does come at the price of increased operational cost (as the flight operations require continuous investment of resources) but a sufficiently large number of drones can offset this at least regarding node availability (by retiring drones that are low on battery and sending them home to re-charge).
- Reactivity and resilience: not only can drones position themselves to optimize the topology, but they can dynamically amend their positioning to ensure desired levels of redundancy. This allows them to establish a topology not only suitable for the current state of affairs but also for potential future conditions.

It is not all sunshine and rainbows, though. As already hinted at above, there are operational challenges and drawbacks to the use of drones as node-carrying platforms.

### *1.3. Real-World Challenges to Drone-Based MANETs*

As well as remaining airborne (which draws on the limited battery power), drones must (a) carry the payload (which also incurs operational cost in the form of increased energy demand for flight operations) as well as (b) operate said payload (further adding to the power demand of the drone). And while the power issue (i.e., the aspect of physically moving, operating, and keeping a drone airborne) has at least potential solutions (such as, e.g., powering/recharging drones with High Energy Lasers (HELs) from the ground [21]) there are additional functional aspects to consider. For example, maintaining a fully connected network with the desired redundancy requires cooperation between the nodes. Depending on the scenario (see Section 2.3) this may have to happen under sub-optimal or even adversarial conditions. There is furthermore the practical issue of allocating bandwidth to clients who may, depending on the application, generate a significant demand (in the case of, e.g., real-time high-definition video transmissions). Finally, there is the matter of regulation and legal frameworks [22]. It stands to reason that a larger drone-based MANET would rely on autonomously operating drones, which is currently a problematic setup due to the lack of clarity or permissions (countries are currently scrambling to put the necessary laws and oversight institutions in place [23–26]). The next section discusses some of the most prominent challenges and provides a context and scope for the focus and the modeling choices of our work.

### 1.4. Contributions of the Paper

We present a decentralized decision-making framework (in the form of a model for virtual forces) for a self-organizing drone swarm. This framework tackles two challenges simultaneously: without a central control element in the MANET, the swarm (1) dynamically creates a network that connects (potentially mobile) terminals and (2) maintains a topology that ensures all drones are connected to the base station through an unambiguous multi-hop path. We found and chose to report in this paper that the collective movement pattern of individual units (an emergent property of the pseudo-forces model) results in the access points forming a topology that reflects the heterogeneous distribution of clients (and subsequent modification thereof) while also preserving unambiguous multi-hop connectivity to a central Internet gateway. The performance of the distributed algorithm is investigated from a systemic point of view (collective behavior) using a simple LQM to study variability across multiple simulation runs, featuring different client movement patterns.

## 2. Mobile Ad Hoc Networks (MANETs)

### 2.1. Mobile Ad Hoc Networks (MANETs): Applications and Challenges

As advances in wireless technologies continue, the application range for MANETs grows [20,27,28]. The three use-case scenarios provided in Section 2.3 are just some examples of the possibilities where a drone-based MANET can offer significant value by providing, e.g., vital communication links between relief teams, survivors, and external command centers. In the approach presented in this article, we focus primarily on realizing and maintaining a connection between all clients in the field and a central data sink/command center/network root. As well as offering a communication infrastructure for personnel in the field to connect to their command center/dispatch, MANETs can also be used to provide point-to-point connectivity, e.g., Internet of Things (IoT) applications [29,30] where smart devices communicate with one another [31] to, e.g., collectively manage their demand profile. IoT devices, whether in a home automation setting or an industrial environment, often need to communicate and collaborate dynamically [29,31]. Especially when some of the IoT devices are mobile [30] or only sporadically active, MANETs can dynamically adapt to the applications' needs effectively [5,29]. This can be achieved by, e.g., allowing devices to form and manage their own networks as they come into and move out of each other's communication range. In this context, Vehicular Ad Hoc Networks (VANETs) [2,9–11] deserve special attention: with increasing vehicular autonomy, interconnecting the individual vehicles enables them to share information [22,32], to allocate available resources [5,28] and to collaborate when navigating in close proximity. VANETs [9–11] rely on the principles of MANETs to communicate among themselves and with other elements of the transport infrastructure. Among the known benefits of this are enhancing safety, increasing efficiency, and speeding up adaptability.

However, the broad and growing applicability of MANETs comes with its own set of challenges. At the forefront of these is the issue of maintaining network performance in the face of dynamic topologies [3,7,11]. As nodes in a MANET are inherently (potentially) mobile, the network topology can change rapidly and unpredictably. This presents challenges that, e.g., require novel routing protocols [12,17,30,33] capable of addressing this new complexity to ensure reliable and efficient communication between nodes.

Additionally, as the scale and complexity of MANETs increase—for instance, in a large IoT deployment—so too do the challenges associated with network management and security [29]. Protecting against threats and maintaining privacy in such a distributed, decentralized environment is inherently complex [8,29]. Furthermore, network management protocols [33] need to be capable of dealing with the potential for node failures, traffic congestion, and other disruptions [12]. Energy management is another key challenge [18,29,30], particularly for MANETs composed of battery-powered nodes, such as drones or IoT devices [29,31]. Ensuring network connectivity while optimizing their energy usage is a non-trivial task requiring careful balance.

Despite these challenges, the potential of MANETs remains vast. Their flexible, adaptable nature, coupled with their broad applicability, renders them a key contributor to our increasingly connected world. As research progresses, the development of innovative solutions to these challenges will continue to drive the evolution and adoption of MANETs across various domains. At this point, MANETs are a thriving area of research [5,12,13,17,29,30,33] and have become a fundamental contribution to modern wireless communications technologies [12,13,33]. As increased users carry mobile devices with them, the need for network flexibility grows. Since MANETs can self-organize and operate relatively independently from fixed/static infrastructure, their application areas are broad. However, while they are quite adaptable and versatile, they also come with various serious (and sometimes unique) challenges.

### *2.2. Scope of the Paper*

MANETs have the potential to transform wireless communication due to their flexibility and self-organizing capabilities [34–36]. Despite this potential, they face significant challenges [4,5,7,12,14–16,29] that can hinder their optimal operation. Understanding these challenges is crucial to improving their robustness, security, and efficiency.

One of the most prominent challenges in MANETs is the dynamic nature of the network topology [14,15]. Given the mobility of nodes, the network topology can change over time. This can cause path breakages and result in intermittent connectivity, complicating the process of routing data between nodes. Designing adaptive routing protocols [17,30] that can quickly react to such changes is a non-trivial task, requiring advanced algorithms and efficient network management strategies [12].

As the number of nodes in the network increases, the overhead involved in managing the network, maintaining routing tables, and ensuring seamless communication can become increasingly complex. Scalability issues [15] can result in decreased network performance, increased latency, and reduced reliability.

We propose the use of drone-borne access points to form MANETs. Our investigations are kept generic and within the broad range of MANETs designed to enable client-to-root connectivity, see Section 2.3. We focus on the management of the dynamic network topology (i.e., the self-organizing [37] movement of the nodes) and do so in a scalable manner. We are restricting ourselves to MANETs which are primarily concerned with connecting clients through a network with a root or data sink [13].

Topology management, i.e., the positioning and connecting of nodes in a MANET, is understood to be one of the most important challenges. Several types/classes of approaches have been proposed by the community in the literature. We distinguish by the way they control the swarm: centralized [38–40], decentralized [38,41] or hybrid, and the mechanism used to determine the individual node movement: location- [42], virtual force- [43] or machine learning-based [44–46]. The approach presented in Section 4 is decentralized: the drones in the MANET base their movement and connectivity decisions entirely on local information. However, since the base station (the root in the network topology) can trigger the release of additional drones into the swarm, there is a central component in the system, and one could argue that our approach therefore constitutes a hybrid mechanism.

The presented approach is force-based (with the three forces discussed in Sections 4.1.1–4.1.3). The nodes are assumed to be fully aware of their position (see Section 3.3) but this is merely a simplification that allows each drone to compute the exact distance to, and the direction of, another drone. These values could also be inferred through signal analysis. In general, relative position is used in the calculation of all virtual forces (e.g., repulsive between nearby drones) which does imply the reciprocal knowledge of neighboring drones' locations. However, we do not concern ourselves with how this information is procured (e.g., using visual signals).

### *2.3. Target MANET-Applications and -Scenarios*

We briefly discuss three applications. In all of these, the drone-based MANET is connected to the ground at its entry (base) and exit points (terminals). For the remainder of this article, we consider only flat landscapes and treat the problem as a 2D problem.

We argue that this approximation is valid if the vertical separation between drones is orders of magnitudes smaller than the target distance between them in the horizontal plane (e.g., tens of meters vs. kilometers) and the environment is not obstructed by tall structures (e.g., maritime or coastal region, flat plain, river delta, etc.).

#### 2.3.1. Disaster Response

Our first scenario class focuses on the case where existing infrastructure is unavailable [19], be it temporarily (as in the case of, e.g., a power outage) or permanently (such as, for example, when a hurricane has wiped out the cell tower network of a Caribbean Island). In this application, we assume some ongoing coordinated effort that includes many field units operating in uncertain terrain that need to be connected through a gateway to the global IT infrastructure or some operational headquarters [31]. This also covers the case where a MANET is deployed to serve as temporary infrastructure.

In such a setting, the demand is likely to move as rescue efforts sweep across the deployment area or as parts of the local infrastructure successively come back online. The MANET must respond to this shifting demand by dynamic node re-allocation.

#### 2.3.2. Wilderness Exploration

The second scenario class considers the temporary deployment of a MANET during, e.g., some exploration effort where the MANET is needed for a limited time. This could be, for example, a rescue effort in a remote area or the mapping of previously unexplored terrain [3]. In both cases node movement may be unpredictable.

Drone-based MANETs are especially useful when infrastructure is only needed briefly, as the MANET will automatically reduce its presence in an area where there is low or no demand to deliver high connectivity in areas with many field units.

#### 2.3.3. Contested Environments

The previous two scenarios covered the case where infrastructure was wiped out or never existed. In both cases, information can be very patchy, but what is available is considered trustworthy. For the third scenario, we want to consider the case where the available infrastructure or information cannot always be trusted [47]. In the simplest case this could be due to wide-spread sensor malfunctions due to some natural phenomenon (e.g., a solar storm). However, the literature increasingly considers the case of intentional and malevolent interference. This can come, e.g., in the form of a directed attack on the Global Positioning System (GPS) infrastructure or as GPS-spoofing.

Regarding drone-based MANETs, this is of high relevance given the massive deployment of drones in, e.g., the conflict in Ukraine where countermeasures are known to massively impair localization and remote control of drones.

## 3. Modeling MANETs

The objective of the proposed framework is to establish and maintain a multi-hop access network that would allow a population of clients to send and receive information to/from a central location (root) and by extension to/from each other if required. A subsidiary goal is to create a tree topology to ensure unambiguous routing. The challenge is to do so exclusively through autonomous local decision-making by individual mobile nodes, in the face of an arbitrary and heterogenous distribution of clients.

As discussed in Section 2.2, our approach is focused on self-organizing topology management. Although the routing is defined by the resulting tree structure, we make no claim regarding dynamic routing within the network.

### 3.1. Nodes and Clients

We model a MANET as a dynamic network topology consisting of three types of entities: clients (mobile terminals), nodes (mobile access points for the terminals) and a root or data sink (a static point of contact to the global infrastructure).

Nodes in the network are drone-mounted routers that can either serve as the entry point into the MANET (this service is provided to the mobile clients) or as a connection within the MANET, in which case the node simply connects two other nodes. In this case, the node is referred to as the child of its access point node and as the parent for all the nodes to which it provides access.

Nodes have a limited range within which they can provide connectivity and the quality of the service provided deteriorates quadratically with increasing distance to the node (see Section 3.2). They further have an upper bounded bandwidth, simplified in our model as the number of connections they can serve/the number of connections they can relay. Nodes move under their own power and control, meaning that they can determine their movements themselves. They do so using the local information available to them (see Section 4.1) so their movement is a product of their internal state and their sensed environment. We assume that nodes always know their position.

Clients are simplified as entities creating a demand for the network. We adopt the Full Buffer Model [48] which means that the number of clients in an individual cell does not change and that all clients always create a demand. Clients also can move, but their movement is determined by an outside function and is therefore not affected by the internal state of the client. Clients are also assumed to know their exact position and to communicate this to their parent node. This assumption is required to enable the drones to determine the quality of service they provide to the clients (as it is based on the distance between the two); in a real-world implementation, this signal strength received by the client could simply be communicated to the drone to achieve the same effect.

### 3.2. Link Quality Metric (LQM)

We define a metric to capture the quality of the overall connection in a multi-hop route. This metric is meant to capture the minimum signal strength when considering the entire sequence of hops between the root and the client (known as the “weakest-link” hypothesis) relative to the achievable maximum value. The signal strength plateaus at 1 for a distance $r$ equal or lower than one space unit, i.e., its value is $\min(1, \frac{1}{r^2})$.

We do this for two reasons: (1) we want to assess the performance of our approach regarding the link quality experienced by the clients (see Equation (2)) in the MANET (cf. Figure 2), and (2) we use this indicator in all nodes that are parent to more than one child, be it because they are a branch in the topology tree or because they serve as an access point for clients. Such nodes will consider the link quality between themselves and all their children to calculate a *stress* value (cf. Equation (3)) used to decide whether an additional node should be deployed into the MANET (see Section 3.3).

The normalized LQM for an individual link is defined between any two nodes $i$ and $j$ in a path (from the root/data sink to a mobile client) using the distance between them $r_{i,j}$ (see Equation (4)), with $i$ and $j$ being *parent* node/root and *child* node/client, respectively:

$$LQM_j = \frac{1}{\max(1, r_{i,j})^2} \tag{1}$$

This assigns each node a value indicating the connection strength to its parent node. Please note that the max(_,_) in the divisor is simply to ensure that the LQM cannot grow larger than 1, meaning that being closer to the parent does not offer a better LQM value.

Using these individual link values we can calculate the overall LQM for any route $LQM_{\mathrm{root},c}$ between the root and a mobile client $c$ as the worst individual link strength:

$$LQM_{\mathrm{root},c} = \min(1, LQM_j) \forall j \in \text{path to } c \tag{2}$$

The results shown in Figure 2 on page 8 make use of this metric.

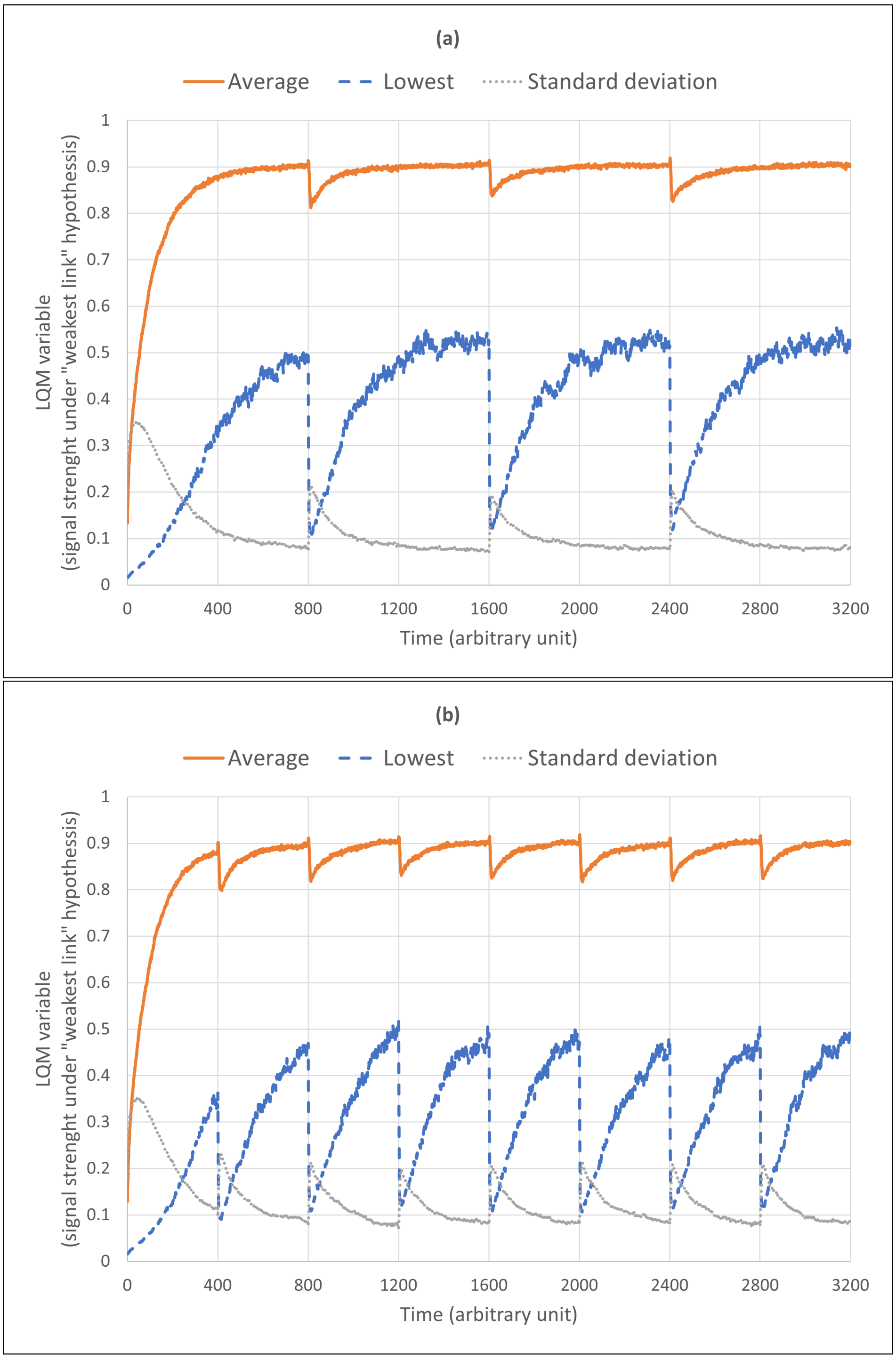

**Figure 2.** Evolution of the $LQM_{\text{root},c}$ variable for all clients $c$ (cf. Equation (2)). A total of 100 independent simulation runs (500 clients, divided into eight dynamic clusters). (**a**) Clients relocate every 800 time units. (**b**) Clients relocate every 400. The average is an "average of averages". The standard deviation is the average of the 100 SD values (1 data-point per simulation run and per time unit). The lowest is the average of the 100 worst LQM values experienced by any client $c$ (idem).

### 3.3. Stress Level

We model a node-specific performance value which we refer to as *stress*. This value represents the overall quality of service experienced by the clients connected to the node.

$$stress_i = \frac{n}{\sum_{j=1}^{n} LQM_j} \tag{3}$$

The stress level, an internal value derived from locally available information only, is used as a trigger (see Section 4, specifically Section 4.2.1 for the mechanism to deploy additional drones). The threshold for this trigger is set by default to 1.5, which, for a node serving as an access point (and therefore with only a single other node as a client), would be reached when the client's LQM drops below $\frac{2}{3}$. For nodes connected to clients, this trigger is reached when the average LQM of all associated clients drops below $\frac{2}{3}$.

### 3.4. Miscellaneous Modeling Choices

#### 3.4.1. Position, Navigation and Timing (PNT)

As mentioned in Section 3.1, we assume that all nodes are at all times able to determine their exact position using, e.g., conventional GPS signals. We understand that this is a reasonable assumption for two of target scenarios (namely disaster response, cf. Section 2.3.1 and wilderness exploration, cf. Section 2.3.2) but that this is a questionable assumption for the third scenario (contested or hostile environments, cf. Section 2.3.3).

The military domain is indeed a major application area for PNT precisely because (a) the importance of knowing one's exact location and (b) the ease with which the standard GPS signals can be denied or spoofed. However, several approaches do not need GPS reception to deliver good or even GPS-like positioning information (for example, research into stand-alone systems such as TOPS or positioning approaches using a mega-constellation such as Starlink [49,50]). In addition, nodes in the MANET could use the strength of the received signal to infer the distance to the sender and simply base their assessment on this. We argue that the presented approach would work under these settings as well. This assumption (that the location is always known) reduces the complexity of this manuscript without significantly impacting the applicability of the approach in the suggested target application areas.

#### 3.4.2. Central Dispatch

All drones can communicate with the central hub. They need to do so when, e.g., transiting from the hub to a deployment, a process during which they remain unavailable as an access point but during which time no other drone can be deployed. They further need to be able to communicate whenever their stress level exceeds the threshold as this triggers the deployment of an additional drone. Both could be realized using the intended functionality of the system: in the former case, the newly deployed drone simply does not operate as an access point until it has connected to its dedicated *point of contact* further down in the network tree. For the latter, any node's stress levels can be included in the messages sent through the network to the route.

## 4. A Novel Self-Organizing Approach to Drone-Based MANETs

We propose a self-organizing approach to enable a swarm of drones to dynamically and adaptively deploy a MANET and manage its topology to optimize LQM.

In this section, we first discuss the mechanism that allows drones to determine their direction of movement (see Section 4.1). We then discuss how the overall system uses information about the individual nodes' stress levels to iteratively deploy additional drones into the swarm (Section 4.2.1) and, conversely, how under utilized nodes can be reassigned within the swarm (Section 4.3) or retired entirely and recalled to the base (Section 4.2.2).

### *4.1. Drone Movement*

Drone movement is determined by a force $f$ seemingly *pushing* (or *pulling*) the drone in a specific direction ($f$ is given by the separate forces acting in the $x$ and $y$ direction, respectively). In our case, the force $f$ is the weighted sum (see Section 4.1.4) of three separate forces (see Sections 4.1.1–4.1.3). These three forces are (a) the *attraction* a node experiences towards its clients, (b) the *repulsion* it experiences from other nodes (other than its parent) and (c) the node's *desire* to converge towards a given (as a parameter) optimal distance to its parent node (i.e., either *attractive* or *repulsive*), respectively.

The calculation of these contributing forces uses (a) $r_{i,j}$ the distance between the entities $i$ and $j$ (calculated as Euclidean distance, cf. Equation (4)) as well as $dx_{i,j}, dy_{i,j}$, the delta between their $x$ and $y$ position. The *direction* of this delta (i.e., its sign) will determine the direction of the resulting force (see the use of $r$ and $dx, dy$ in Equations (5)–(7)).

$r_{i,j}$, the Euclidean distance between the entities $i$ and $j$, is calculated as usual:

$$r_{i,j} = \sqrt{dx_{i,j}^2 + dy_{i,j}^2} \text{with} \begin{array}{l} dx_{i,j} = x_i - x_j \\ dy_{i,j} = y_i - y_j \end{array} \tag{4}$$

Please note that while $r_{i,j} = r_{j,i}$, this symmetry does not hold for $dx$ or $dy$ (meaning that $dx_{i,j} \neq dx_{i,j}$) as either of these is directional, i.e., will always differ in their sign when reversed ($dx_{i,j} = -dx_{i,j}$). This comes back in Equations (5)–(7) where it determines the resulting direction of the force, i.e., whether the force is *attractive* or *repulsive*.

#### 4.1.1. Moving Towards Clients

We model the individual $x$- or $y$-axis attraction exerted by any client $j \in \{1, \ldots, n\}$ on its node as a virtual force that decreases as the square of the Euclidean distance between them. This effectively means that closer clients have a stronger impact than those that are further away.

Mathematical Modeling of the Attraction of Affiliated Clients

$$\begin{aligned} f'_{x_i} &= \sum_{j=1}^{n} \frac{dx_{j,i}}{r_{j,i}^3} \\ f'_{y_i} &= \sum_{j=1}^{n} \frac{dy_{j,i}}{r_{j,i}^3} \end{aligned} \tag{5}$$

#### 4.1.2. Moving Away from Other Drones

Similar to the impact of clients on a node's movement, all the surrounding nodes $j \in \{1, \ldots, n\}$ (other than the parent node) also impact the node's direction of movement, but this time (a) in the opposite direction (the dividend is $dx_{j,i}$ in Equation (5) and $dx_{i,j}$ in Equation (6)) and (b) the exponent of the divisor means that it increases slower in Equation (6) than in Equation (5).

Mathematical Modeling of the Repulsion from Other Drones

$$\begin{aligned} f''_{x_i} &= \sum_{j=1}^{n} \frac{dx_{i,j}}{r_{i,j}^2} \\ f''_{y_i} &= \sum_{j=1}^{n} \frac{dy_{i,j}}{r_{i,j}^2} \end{aligned} \tag{6}$$

#### 4.1.3. Maintaining Connectivity and Routing

Finally, we consider the impact of the one node that serves as a parent node (in the path to the root node) to our node (recall that the parent node was explicitly excluded in

Equation (6)). Please note that we (a) reverse the direction again ($dx_{j,i}$ as opposed to $dx_{i,j}$) and that the second term (in brackets) causes the resulting force to switch signs around $r_{j,i} = 1$, with it being zero at that specific point. This enables $f'''$ to be either, *attractive* or *repulsive*.

Mathematical Modeling of the Force Ensuring Connectivity

$$\begin{aligned} f'''_{x_i} &= \frac{dx_{j,i}}{r^2_{j,i}} \times \left( r_{j,i} - \frac{1}{r^2_{j,i}} \right) \\ f'''_{y_i} &= \frac{dy_{j,i}}{r^2_{j,i}} \times \left( r_{j,i} - \frac{1}{r^2_{j,i}} \right) \end{aligned} \quad (7)$$

#### 4.1.4. Overall Movement

The overall force acting on a node is then the weighted sum of the three contributing forces, as defined above. In addition, we normalize $fx$ and $fy$ for each force.

Mathematical Modeling of the Overall Force Governing a Node's Movement

$$\begin{aligned} fx_i &= w' \frac{f'_{x_i}}{\sqrt{(f'_{x_i})^2 + (f'_{y_i})^2}} + w'' \frac{f''_{x_i}}{\sqrt{(f''_{x_i})^2 + (f''_{y_i})^2}} + w''' \frac{f'''_{x_i}}{\sqrt{(f'''_{x_i})^2 + (f'''_{y_i})^2}} \\ fy_i &= w' \frac{f'_{y_i}}{\sqrt{(f'_{x_i})^2 + (f'_{y_i})^2}} + w'' \frac{f''_{y_i}}{\sqrt{(f''_{x_i})^2 + (f''_{y_i})^2}} + w''' \frac{f'''_{y_i}}{\sqrt{(f'''_{x_i})^2 + (f'''_{y_i})^2}} \end{aligned} \quad (8)$$

We found values of 0.25, 0.5 and 1 for $w'$, $w''$ and $w'''$, respectively, to work best in our numerical experiment. These values prioritize the influence of the parent node on the resulting virtual force, which is only modulated by the two other forces (attraction by the clients, and repulsion by other nodes). This tends to ensure network cohesion (e.g., by preventing a group of clients from pulling a node so far from its parent that it would result in mediocre link quality between them). NB: these values have not been the subject of a systematic optimum search and are still open for fine-tuning.

### *4.2. Dynamic Drone Deployment and Recall*

#### 4.2.1. Dynamic Deployment

After the last drone to be dispatched has reached its destination and turned on its wireless access point, if the stress value (cf. Section 3.2, Equation (3)) of any node in the MANET exceeds a given threshold value (which, in our case, was set to 1.5 by default), then the release of an additional drone is triggered, which will head to a location in the vicinity of the unit experiencing the highest stress level. Once a drone is deployed, it will travel to its designated coordinates before turning itself into a network node and becoming an active member of the MANET.

#### 4.2.2. Dynamic Recall

As Section 4.3 will discuss, nodes in the MANET are expected to adapt their connections towards the root under certain conditions. This *rewiring* amounts to the optimization of the network and manages the MANET topology. However, we first define the mechanism to shrink the swarm when its overall utilization becomes sub-optimal.

Recall that clients automatically connect to the closest node. This implies that a drone serving as a leaf-node in the MANET can lose all its clients to other, more optimally located nodes. Similarly, if a node was serving as a relay in a multi-hop route, it may see all its child nodes re-connect to other parent nodes (as described in Section 4.3; this is carried out to optimize the overall LQM of the MANET). In both cases, a node will find itself without any dependents (and therefore without any *stress* value (see Section 3.3)). After this situation has persisted for 10 or more time units, a node will start considering retirement on every subsequent time-step, with a fixed probability (currently 1 %).

The decision to retire is made autonomously by every individual node and is subject to a stochastic choice. Because the random test is performed on every time-step against a fixed probability, the longer a drone remains without clients or children in the MANET, the more likely it is to have returned to base (the probability of it remaining idle, waiting for children or clients to connect, follows an exponential decay). If any client or node connects to the drone before a decision to retire is made, it simply stops repeating the test and resumes normal operations. Once the decision to retire is taken, however, a drone will not accept new connection requests but instead return to the base.

### 4.3. Dynamic Adaptive Topology Management

The MANET created by the drones has a *tree* structure: all connections start at the base (root) and, as explained in Section 3.2, any node in the network will ultimately connect to a single root parent node (namely the one with the highest LQM). This allows for multiple children from a single parent while (a) ensuring full connectivity (consider: connections *grow* from the root and nodes only have a LQM when connected to the root in the first place) and (b) preventing loops.

Nodes assess, at regular intervals, their connections based on distance and the number of hops required to reach the root. To do so, nodes consider all potential parents within their reach and assess their suitability based on (1) the distance between them and (2) their height in the tree (number of hops to the root). Node $i$ will trigger a change from its current parent $p$ to a new parent $j$ when the following condition is met (Equation (9)):

$$r_{i,j} \times \sqrt{1+l_j} < 0.75 \times r_{i,p} \times \sqrt{l_i} \tag{9}$$

This starts at 1.06 and rapidly increases as (a) both nodes $i$ and $j$ are further from the root and (b) the hop difference between the two nodes increases, cf Table 1.

**Table 1.** Shown are, for any node $i$, The ratio that the distance from $i$ to the new drone $j$ must be better (shorter) than the distance to the current parent node $p$ before $i$ will consider re-connecting from $p$ to $j$. The ratios, shown here for different *levels* of the nodes $i$ and $j$, increase rapidly for increasing level disparity. See Equation (9).

| $l_j \backslash l_i$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | — | 1.06 | 1.3 | 1.5 |
| 2 | 1.06 | 1.3 | 1.5 | 1.68 |
| 3 | 1.3 | 1.5 | 1.68 | 1.84 |
| 4 | 1.5 | 1.68 | 1.84 | 1.98 |
| | | … | | |
| 9 | 2.25 | 2.37 | 2.49 | 2.6 |

This is meant to prevent excessive rewiring for marginal benefits. As mentioned before, the equation can be tuned and tailored by changing the value 0.75.

## 5. Performance Evaluation

The objective of the proposed framework is to establish and maintain a multi-hop access network that would allow a population of clients to send and receive information to/from a central location (root) and by extension to/from each other if required. A subsidiary goal is to create a tree topology to ensure unambiguous routing.

The challenge is to do so exclusively through local decision-making by individual mobile nodes, in the face of an arbitrary and heterogeneous distribution of clients.

We measure the swarm performance by plotting the LQM values and the swarm size over time. We are using the LQM as a first-order approximation of performance/QoS (used only to determine the parent node); we are not evaluating the QoS from a communication point of view, nor are we including the operational costs for the network (or consider different traffic volumes). Emphasis is placed on demonstrating the ability of the swarm to realize a MANET covering most (and ideally: all) mobile clients without a central command module i.e., through self-organization. Other potential performance indicators for the algorithm, such as, e.g., energy efficiency, delay, or throughput, are not considered in this article and were not the focus of our work.

### 5.1. Numerical Experiment Setup

Every client was randomly assigned four separate stations (geographical coordinates) through which it cycles over time (relocating at fixed time intervals). To ensure the heterogeneous distribution of clients, these stations were grouped into an arbitrary number of clusters of random size and position, so that at the end of every relocation phase, all clients would produce a new "patchy" distribution (featuring areas of high density separated by empty or near-empty spaces in which no coverage is needed).

N.B.: clients belonging to the same cluster at one point of the cycle may and often move on to then belong to different clusters after their movement is completed. The change in the nodes' locations can be seen in the screenshots shown in Figure 1 where we present four screenshots corresponding to a time series, each showing the swarm's self-reorganization after the clients have relocated, cf. Figure 2 for more details on the temporary negative impact of relocation on LQM.

This is not intended to mimic the real movement of mobile clients in any of the suggested scenarios. Instead, the clients' heterogeneous distribution and periodic relocation behavior described above were designed to force the swarm to first adapt its structure to reflect the variable coverage needs, then reconfigure when the demand (proportional to local client population density) changes dramatically and near instantaneously.

The use of an unrealistic deterministic cycle was deemed inconsequential since the drones have no memory and so every configuration is treated as an entirely new problem to solve (even if it is a repeat of a previous one).

The aim was to demonstrate that the swarm cannot only "grow" the network towards demand hotspots at the time of first deployment, but subsequently adapt the topology when conditions change (by letting the swarm search out the new areas of demand, seemingly "following" the clients without knowledge of their final destination).

Different intervals between relocations (800 or 400 time units) were used to evaluate the effect of higher perturbation frequency over performance (average and minimum LQM before, during, and after topology adaptation).

Summary: the number of terminals was kept constant. The upper size of the swarm is bounded. Data collection was conducted over 3200 time units with the relocation of terminals happening after either 400 or 800 time units. Monte Carlo simulation is used to model the execution of the decentralized algorithm. Simple link quality metrics (LQM) are used as a first-order approximation for performance measurements. The simulation was implemented in native JAVA without specific libraries, on a Windows 10 laptop.

### 5.2. Results

Simulation results confirm the distributed algorithm's ability to grow a multi-hop access network capable of adapting its topography (localization of nodes) and topology (connections between them) to service a population of clients featuring an arbitrary and heterogeneous distribution, see Figure 2.

Furthermore, they also indicate that the parallel execution of the decision function (which governs individual placement) by all swarm members produces a stable or near stable network configuration while clients' distribution remains static (i.e., successful self-organization). Most participating drones end up "oscillating" around a fixed location and keeping the same role/level in the tree topology for long periods.

Because the algorithm can produce a suitable fixed distribution of access points while the clients remain immobile, it can be left to run in the background even when the network is fully grown and LQM is satisfactory across the entire target population. Consequently, when the clients do relocate (see Section 5.1 for details on how this was implemented), no specific procedure needs to be invoked for the swarm to reconfigure. Through a combination of individual movement, the retirement of units made idle by the change in the demand profile, reorganization of the topology (*parent–child* relationships), and dispatching of new drones toward points of heightened stress (all procedures used to grow the initial network), the swarm can spontaneously adapt to any new situation.

Selected results are presented to illustrate system behavior. Figure 2 show the evolution of the chosen LQM approximation over time. This variable is defined as the minimum signal strength when considering the entire sequence of hops between the root and the client ("weakest-link" hypothesis) relative to the maximum achievable (signal strength plateaus at 1 for a distance $r$ equal or lower than one space unit, i.e., $\min(1, \frac{1}{r^2})$.

As expected, at relocation time, both average and lowest LQM drop sharply, whereas variability (sdev) rises in proportion. After a few steps though, the system recovers as the swarm reorganizes itself to accommodate the new client distribution.

Figure 3 shows the evolution of the number of drones involved in providing the service over time. Unsurprisingly, it follows the same pattern as LQM during the network growth phase ($t = 0 \rightarrow t = 400$ or $t = 0 \rightarrow t = 800$) and after subsequent clients' relocation.

Two aspects may be worth emphasizing:

1. Swarm size appears to saturate at around 80 for the used values (coverage area, number of clients/clusters), which is lower than the total number of drones available (100), indicating the system's ability to commit only the necessary resources.
2. After relocation, the total number of drones in the air does not drop below about 60, so the adaptation process is not equivalent to a "reboot". Only about 25% of the swarm ($\approx$20 units) is being "retired" (then progressively replaced), whereas the remaining 75% just "follow the clients" in their migration.

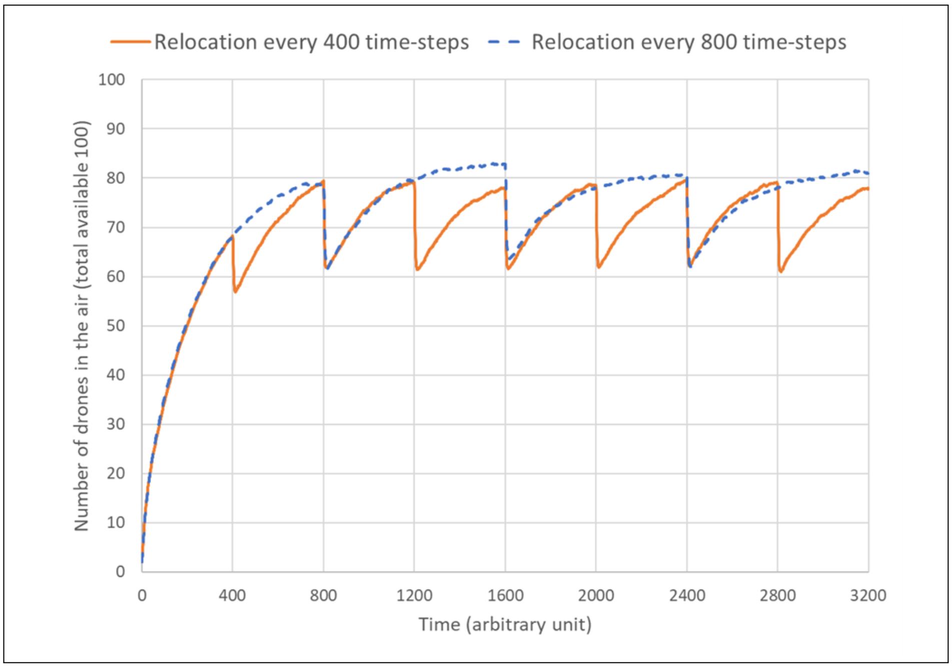

**Figure 3.** Evolution of swarm size (simultaneously airborne drones). Reported are the averages over 100 independent simulation runs. NB: all parameters, including the total number of clients and drone fleet size, are identical in both scenarios. Only the frequency of relocation (the interval between the mobile clients moving to another location) varies (800 vs. 400 time units interval).

## 6. Conclusions and Future Work

### *6.1. Summary*

We presented an approach to move nodes in a network in a distributed and self-organizing fashion. Among the advantages offered by the presented approach is the ability of the network to adapt to changes in the clients' locations (movement) without the loss of multi-hop connectivity to the central gateway (which is also the base of the drones). However, the fact that there is no guarantee that an optimal allocation/distribution is/will be found may be considered a disadvantage.

Furthermore, we wish to emphasize that we are making no claims of having developed a mature technical solution, which is why we used a simple and abstract *"link quality metric"* LQM to quantify the fluctuations in coverage.

Our findings are algorithmic and theoretical in nature: we present a decentralized decision-making framework capable of governing the suitable deployment and subsequent reorganization of mobile access points in a multi-hop ad hoc network, in an environment featuring a heterogeneous and dynamic distribution of clients.

### *6.2. Conclusions*

We conclude that the force-based approach is suitable to deploy and maintain a MANET comprised of individual nodes making autonomous decisions based on locally available information only, without the need for explicit planning or coordination, which has clear advantages for flexibility and scalability. In the proposed method, the only aspect that is centrally managed regards the decision of dispatching an additional unit to a certain region of the network, based on the stress level reported by the already deployed nodes. The choice of three distinct forces reflects the constraints that apply, namely the necessity to target regions of higher demand ("pull" exerted by the clients), to avoid bunching ("push" exerted by nodes on each other), and to balance overall reach against the risk of degraded link quality ("push-pull" exerted by the parent node on its children). The proposed and used values for the weighting parameter applying to these three forces are based on trial-and-error and are unlikely to be optimal, even though they were shown to perform well in the chosen region of the other parameters' space.

Our work realizes a MANET through a self-organizing drone swarm. Without a central control element, the swarm (1) dynamically creates a network that connects (potentially mobile) terminals and (2) maintains a topology that ensures all drones are connected to the base station through an unambiguous multi-hop path.

### *6.3. Future Work*

The work presented is based on some significant simplifications and constitutes a theoretical investigation. Regarding the continuation of our work, we are already considering several directions:

- We have not explored extreme outlier scenarios, such as the case where there are no clients present or where all clients have aggregated at the extreme ends of the map.
- The introduction mentions resilience as a benefit for MANET's (see Section 1.2). The MANET approach we developed does not provide any redundancy. However, we expect that this can be designed into the swarm and are hoping to proceed with work focusing on this (and the formal verification thereof) in the near future.
- We argue that the parameters needed to control energy efficiency are already included in the force-based control of the nodes in the network: in Section 4.1.3, Equation (7), we set the inter-drone distance for which the value of this force becomes infinitesimally small to 1. As distance affects energy efficiency later work can use this part of the model to modulate the power required for inter-drone communication.
  Similarly, the LQM (Section 3.2) is set to plateau for the distance value of 1. Despite this connection to the energy cost incurred when transmitting data over the resulting MANET, our current investigations do not assess this cost.

Future work, especially work directed at specific applications, will include considerations for this network performance indicator.

- During performance evaluation we noted that small changes in the setup as well as in Equations (5)–(7) led to peculiar emergent *behaviors* of the swarm (such as, e.g., a long *arm* of connected drones swaying from left to right until they connect with a client). Future work will investigate the design and use of such behaviors and the environmental conditions necessary to achieve them.
- In Equation (2) we defined the LQM value as simply the weakest link in the route from root to client. We can define this value in a more complex manner to reflect additional properties of the connection, the resulting LQM will be subject to the signal deterioration in the entire route to the root. The recursive definition for $LQM_i$ for any node $i$ connected to the best available access point $j$ is thus:

$$LQM_i = \frac{LQM_j}{\max(1, r_{i,j})^2}$$

  Under this revised definition, *any* sub-optimal link anywhere in the connection to the router will further degrade the overall LQM value (the presented work only considers the last link). This affects the deployment of additional nodes in at least two ways. Firstly, since sub-optimal links closer to the router may further lower the LQM value this directly impacts the deployment of additional nodes, which may now be deployed earlier (thereby potentially improving the individual link quality and thus the overall connectivity). Secondly, the LQM values now reflect the actual connection quality better and are thus more likely to result in new nodes being dispatched to the locations where they are needed most. To motivate the latter claim, consider two routes of LQM value 0.6, one where all links are perfect except one and another where all links have the sub-optimal value of 0.6. The second route would (correctly) receive a much lower overall LQM value and thus be allocated an additional drone first. Exploring the impact of this revised performance measure is future work.
- In Section 2.3 we have specifically restricted our scenario to the 2D domain. With a large number of projects in our labs being rooted in the maritime sector, the presented work currently meets our needs. That being said, while we do not foresee any issues with extending the theory to 3D in general, working on an amended approach for obstacle-rich environments or challenging landscapes (such as, e.g., urban canyons or indoor search-and-rescue) is considered future work.

**Author Contributions:** Conceptualization, F.S.; methodology, F.S.; software, F.S.; validation, F.S. and H.H.; formal analysis, F.S., H.H. and A.A.; investigation, F.S., H.H. and A.A.; resources, F.S. and A.A.; data curation, F.S.; writing–original draft preparation, F.S., H.H. and A.A.; writing–review and editing, F.S., H.H. and A.A.; visualization, F.S.; supervision, F.S. and A.A.; project administration, F.S. and A.A.; funding acquisition, F.S. and A.A. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work was supported by VTT's Government Grant (GG_SecureSoc2022, Project #132273).

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Li, X.; Chen, J.; Li, J. FATES: A Framework with Adaptive Track-Explore Strategy for Moving Targets Search by a FANET. In Proceedings of the 2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom), Melbourne, VIC, Australia, 11–13 December 2018; pp. 856–861. [CrossRef]
2. Shumeye Lakew, D.; Sa'ad, U.; Dao, N.N.; Na, W.; Cho, S. Routing in Flying Ad Hoc Networks: A Comprehensive Survey. *IEEE Commun. Surv. Tutorials* **2020**, *22*, 1071–1120. [CrossRef]
3. Singh, H.; Verma, S.; Adhya, A. A Brief Review on Position-based Routing Protocols in Flying Ad-hoc Networks. In Proceedings of the 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 14–16 December 2022; pp. 1423–1428. [CrossRef]

4. El-Zoghby, A.M.; Mosharafa, A.; Azer, M.A. Anonymous Routing Protocols in MANETs, a Security Comparative Analysis. In Proceedings of the 2018 14th International Computer Engineering Conference (ICENCO), Cairo, Egypt, 29–30 December 2018; pp. 254–259. [CrossRef]
5. Sathyaraj, P.; Devi, S.; Swethareddy, A.; Manimegalai, L.; Kannan, K.; Babu, M. A Dynamic Resource Allocation Protocol: Device to Device Communication For MANETs. In Proceedings of the 2022 International Conference on Advanced Computing Technologies and Applications (ICACTA), Coimbatore, India, 4–5 March 2022; pp. 1–6. [CrossRef]
6. Singal, G.; Laxmi, V.; Gaur, M.; Rao, D.V.; Kushwaha, R. UAVs Reliable Transmission for Multicast Protocols in FANETs. In Proceedings of the 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), Granada, Spain, 22–25 October 2019; pp. 130–135. [CrossRef]
7. Kadivar, M. An Adaptive Yao-based topology control algorithm for wireless ad-hoc networks. In Proceedings of the 2020 10th International Conference on Computer and Knowledge Engineering (ICCKE), Mashhad, Iran, 29–30 October 2020; pp. 457–462. [CrossRef]
8. Jasim, K.S.; Ali Alheeti, K.M.; Najem Alaloosy, A.K.A. A Review Paper on Secure Communications in FANET. In Proceedings of the 2021 International Conference of Modern Trends in Information and Communication Technology Industry (MTICTI), Sana'a, Yemen, 4–6 December 2021; pp. 1–7. [CrossRef]
9. Hamdi, M.M.; Yussen, Y.A.; Mustafa, A.S. Integrity and Authentications for service security in vehicular ad hoc networks (VANETs): A Review. In Proceedings of the 2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 11–13 June 2021; pp. 1–7. [CrossRef]
10. Al-shareeda, M.A.; Alazzawi, M.A.; Anbar, M.; Manickam, S.; Al-Ani, A.K. A Comprehensive Survey on Vehicular Ad Hoc Networks (VANETs). In Proceedings of the 2021 International Conference on Advanced Computer Applications (ACA), Maysan, Iraq, 25–26 July 2021; pp. 156–160. [CrossRef]
11. Hameed, A.G.; Mahmoud, M.S. Vehicular Ad-hoc Network (VANET) – A Review. In Proceedings of the 2022 Iraqi International Conference on Communication and Information Technologies (IICCIT), Basrah, Iraq, 7–8 September 2022; pp. 367–372. [CrossRef]
12. Ramphull, D.; Mungur, A.; Armoogum, S.; Pudaruth, S. A Review of Mobile Ad hoc NETwork (MANET) Protocols and their Applications. In Proceedings of the 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 6–8 May 2021; pp. 204–211. [CrossRef]
13. Hui, Z.; Lingli, Z.; Yonghang, Y.; Linlin, C. A Review of Gateway Load Balancing Methods in Connecting MANET into Internet. In Proceedings of the 2022 24th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Republic of Korea, 13–16 February 2022; pp. 330–335. [CrossRef]
14. Shah, N.; El-Ocla, H.; Shah, P. Adaptive Routing Protocol in Mobile Ad-Hoc Networks Using Genetic Algorithm. *IEEE Access* **2022**, *10*, 132949–132964. [CrossRef]
15. Dash, Y. Nature Inspired Routing in Mobile Ad Hoc Network. In Proceedings of the 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Greater Noida, India, 17–18 December 2021; pp. 1299–1303. [CrossRef]
16. Pandey, P.; Singh, R. An Intelligent and Adaptive Multipath Routing Scheme for Mobile Ad Hoc Network. In Proceedings of the 2023 6th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 3–4 March 2023; pp. 1–5. [CrossRef]
17. Margaryan, R.A.; Muratchaev, S.S.; Volkov, A.S.; Afonin, I.L.; Zhuravlev, I.A. Development of an Adaptive Routing Algorithm in MANET. In Proceedings of the 2022 Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), Saint Petersburg, Russia, 25–28 January 2022; pp. 57–63. [CrossRef]
18. Lansky, J.; Rahmani, A.M.; Zandavi, S.M.; Chung, V.; Yousefpoor, E.; Yousefpoor, M.S.; Khan, F.; Hosseinzadeh, M. A Q-learning-based routing scheme for smart air quality monitoring system using flying ad hoc networks. *Sci. Rep.* **2022**, *12*, 20184. [CrossRef] [PubMed]
19. Erim, O.; Wright, C. Optimized mobility models for disaster recovery using UAVs. In Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 8–13 October 2017; pp. 1–5. [CrossRef]
20. Anttonen, A.; Mämmelä, A.; Höyhtyä, M.; Saffre, F.; Karvonen, H. Self-Organizing UAV Swarm Placement via Layered Loose Coupling and User Prioritization. In Proceedings of the 2023 IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Toronto, ON, Canada, *to be published*.
21. Mason, R. *Feasibility of Laser Power Transmission to a High-Altitude Unmanned Aerial Vehicle*; RAND Corporation: Santa Monica, CA, USA, 2011.
22. Hildmann, H.; Eledlebi, K.; Saffre, F.; Isakovic, A.F., The Swarm Is More Than the Sum of Its Drones. In *Development and Future of Internet of Drones (IoD): Insights, Trends and Road Ahead*; Krishnamurthi, R., Nayyar, A., Hassanien, A.E., Eds.; Springer International Publishing: Cham, Switzerland, 2021; pp. 1–55. [CrossRef]
23. *IEEE P1939.1/D5.0*; IEEE Draft Standard for a Framework for Structuring Low Altitude Airspace for Unmanned Aerial Vehicle (UAV) Operations. IEEE: Piscataway, NJ, USA, 2021; pp. 1–90.
24. *IEEE P1939.1/D6.0*; IEEE Approved Draft Standard for a Framework for Structuring Low Altitude Airspace for Unmanned Aerial Vehicle (UAV) Operations. IEEE: Piscataway, NJ, USA, 2021; pp. 1–92.

25. Mikula, B.; Košuda, M. Aviation Regulations for Drone Operations in the Slovak Republic and the EU. In Proceedings of the 2022 New Trends in Aviation Development (NTAD), Novy Smokovec, Slovakia, 24–25 November 2022; pp. 145–150. [CrossRef]
26. Kandeel, M.E.; Salameh, H.B.; Elrefae, G.A.; Qasim, A. Regulations for UAV Operation in Social Applications and Services: A General Perspective. In Proceedings of the 2022 Ninth International Conference on Social Networks Analysis, Management and Security (SNAMS), Milan, Italy, 29 November–1 December 2022; pp. 1–6. [CrossRef]
27. Saffre, F.; Hildmann, H.; Karvonen, H.; Lind, T. Self-Swarming for Multi-Robot Systems Deployed for Situational Awareness. In New Developments and Environmental Applications of Drones: Proceedings of FinDrones; Lipping, T., Linna, P., Narra, N., Eds.; Springer: Berlin/Heidelberg, Germany, 2022; pp. 51–72.
28. Husain, Z.; Al Zaabi, A.; Hildmann, H.; Saffre, F.; Ruta, D.; Isakovic, A.F. Search and Rescue in a Maze-like Environment with Ant and Dijkstra Algorithms. *Drones* **2022**, *6*, 273. [CrossRef]
29. Gripsy, J.V.; Jayanthiladevi, A. Energy Optimization and Dynamic Adaptive Secure Routing for MANET and Sensor Network in IoT. In Proceedings of the 2023 7th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 23–25 February 2023; pp. 1283–1290. [CrossRef]
30. Satyanarayana, P.; Bhoomika, K.; Mukesh, D.; Srujana, P.; Bai, R.M.; Sriramam, Y.S.S. Implementation of Improved Energy Balanced Routing Protocol to Enlarge Energy Efficiency in MANET for IoT Applications. In Proceedings of the 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 17–18 March 2023; Volume 1, pp. 380–385. [CrossRef]
31. Lohokare, J.; Dani, R. An Intelligent cloud ecosystem for disaster response and management leveraging opportunistic IoT mesh networks. In Proceedings of the 2021 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM), Hangzhou, China, 3–5 December 2021; pp. 125–133. [CrossRef]
32. Arputha Babu John, A.; Dutta, R. Cooperative trajectory planning in an intercommunicating group of UAVs for convex plume wrapping. In Proceedings of the 2017 IEEE 38th Sarnoff Symposium, Newark, NJ, USA, 18–20 September 2017; pp. 1–6. [CrossRef]
33. Kurode, E.; Vora, N.; Patil, S.; Attar, V. MANET Routing Protocols with Emphasis on Zone Routing Protocol—An Overview. In Proceedings of the 2021 IEEE Region 10 Symposium (TENSYMP), Jeju, Republic of Korea, 23–25 August 2021; pp. 1–6. [CrossRef]
34. Yang, T.; Foh, C.H.; Heliot, F.; Leow, C.Y.; Chatzimisios, P. Self-Organization Drone-Based Unmanned Aerial Vehicles (UAV) Networks. In Proceedings of the ICC 2019—2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–6. [CrossRef]
35. Du, Z.; Wang, X.; Wang, S.; Chen, J.; Xu, K. Toward UAV Communication Network Self-Organization: A Game-Theoretic Distributed Control Approach. In Proceedings of the 2022 IEEE International Conference on Unmanned Systems (ICUS), Guangzhou, China, 28–30 October 2022; pp. 121–127. [CrossRef]
36. Horváth, D.; Gazda, J.; Šlapak, E.; Maksymyuk, T.; Dohler, M. Evolutionary Coverage Optimization for a Self-Organizing UAV-Based Wireless Communication System. *IEEE Access* **2021**, *9*, 145066–145082. [CrossRef]
37. Mämmelä, A.; Riekki, J.; Kiviranta, M. Loose Coupling: An Invisible Thread in the History of Technology. *IEEE Access* **2023**, *11*, 59456–59482. [CrossRef]
38. Yan, Z.; Jouandeau, N.; Cherif, A.A. A Survey and Analysis of Multi-Robot Coordination. *Int. J. Adv. Robot. Syst.* **2013**, *10*, 399. [CrossRef]
39. Kang, H.; Kim, H.; Kwon, Y.M. RECEN:Resilient MANET Based Centralized Multi Robot System Using Mobile Agent System. In Proceedings of the 2019 IEEE Symposium Series on Computational Intelligence (SSCI), Xiamen, China, 6–9 December 2019; pp. 1952–1958. [CrossRef]
40. Ahn, S.; Lim, Y. A modified centralized DNS approach for the dynamic MANET environment. In Proceedings of the 2009 9th International Symposium on Communications and Information Technology, Icheon, Republic of Korea, 28–30 September 2009; pp. 1506–1510. [CrossRef]
41. Sun, W.; Zhang, Z.; Chen, W.; Peng, B.; Xu, Y. Decentralized Execution of Composite Service in MANETs. In Proceedings of the 2008 IEEE Asia-Pacific Services Computing Conference, Yilan, Taiwan, 9–12 December 2008; pp. 355–360. [CrossRef]
42. Tharani, S.; Arutchelvan, G.; Arulanandam, G. Location based clustering implemented for multicast backbone MANET. In Proceedings of the 2017 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 6–8 April 2017; pp. 0728–0732. [CrossRef]
43. Liang, C.K.; Chung, C.Y.; Li, C.F. A Virtual Force Based Movement Scheme for Area Coverage in Directional Sensor Networks. In Proceedings of the 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Kitakyushu, Japan, 27–29 August 2014; pp. 718–722. [CrossRef]
44. Eledlebi, K.; Ruta, D.; Hildmann, H.; Saffre, F.; Al Hammadi, Y.; Isakovic, A.F. Coverage and Energy Analysis of Mobile Sensor Nodes in Obstructed Noisy Indoor Environment: A Voronoi-Approach. *IEEE Trans. Mob. Comput.* **2022**, *21*, 2745–2760. [CrossRef]
45. Moole, S.R. Comparison of Effectiveness of Machine Learning Algorithms for Vehicle Path Prediction. In Proceedings of the 2021 IEEE Integrated STEM Education Conference (ISEC), Princeton, NJ, USA, 13 March 2021; p. 210. [CrossRef]
46. Majd, A.; Ashraf, A.; Troubitsyna, E.; Daneshtalab, M. Integrating Learning, Optimization, and Prediction for Efficient Navigation of Swarms of Drones. In Proceedings of the 2018 26th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), Cambridge, UK, 21–23 March 2018; pp. 101–108. [CrossRef]
47. Hamilton, T.; Ochmanek, D.A. *Operating Low-Cost, Reusable Unmanned Aerial Vehicles in Contested Environments: Preliminary Evaluation of Operational Concepts*; RAND Corporation: Santa Monica, CA, USA, 2020. [CrossRef]

48. Ameigeiras, P.; Wang, Y.; Navarro-Ortiz, J.; Mogensen, P.E.; Lopez-Soler, J.M. Traffic models impact on OFDMA scheduling design. *EURASIP J. Wirel. Commun. Netw.* **2012**, *2012*, 61. [CrossRef]
49. Pinell, C.; Prol, F.S.; Bhuiyan, M.Z.H.; Praks, J. Receiver architectures for positioning with low earth orbit satellite signals: A survey. *EURASIP J. Adv. Signal Process.* **2023**, *2023*, 60. [CrossRef]
50. Kassas, Z.M.; Kozhaya, S.; Kanj, H.; Saroufim, J.; Hayek, S.W.; Neinavaie, M.; Khairallah, N.; Khalife, J. Navigation with Multi-Constellation LEO Satellite Signals of Opportunity: Starlink, OneWeb, Orbcomm, and Iridium. In Proceedings of the 2023 IEEE/ION Position, Location and Navigation Symposium (PLANS), Monterey, CA, USA, 24–27 April 2023; pp. 338–343. [CrossRef]