

Article

New Multipath OLSR Protocol Version for Heterogeneous Ad Hoc Networks

Chaimae Benjbara * , Ahmed Habbani and Nada Mouchfiq

Smart Systems Laboratory, Ecole Nationale Supérieure d'Informatique et d'Analyse des Systèmes-ENSIAS, Mohammed V University in Rabat, Agdal Rabat 10106, Morocco; ahmed.habbani@um5.ac.ma (A.H.); nada_mouchfiq@um5.ac.ma (N.M.)

* Correspondence: chaimae_benjbara@um5.ac.ma

Abstract: From a basic refrigerator to a self-driving car, emerging technologies are increasingly involving various facets of our daily lives. These bring together many regularly used devices, each with its own characteristics, to communicate and collaborate within the same system. Computer network experts regard this so-called structure as a heterogeneous network made up of several connected objects that do not speak the same language. Communication is therefore ensured by additional types of nodes, such as gateways or converters. In this case, we can detect an increased complexity and a decreased level of security. And thus, the need to adopt a common slang for these kinds of networks has been brought to life. In this work, we compare two different routing protocols: optimized link-state routing (OLSR) and the multipath heterogeneous ad hoc network OLSR (MHAR-OLSR). The latter is an OLSR extension with new functionalities: nodes identification, paths calculation, paths classification, and paths choice that we designed for heterogeneous ad hoc networks composed of MANET, VANET, and FANET devices; it ensures direct communication between these diverse components. We verify and explain all the elements of our solution using colored Petri nets. We also present a global evaluation of Packet Delivery Ratio (PDR), End-To-End Delay, and energy consumption as QoS measures with different numbers of nodes in a heterogeneous scenario. To do this, we use NS-3 and BonnMotion as a tool-set of simulation. Experimental results show improvement in performance when compared to the classical routing protocol.

Keywords: ad hoc; wireless communication; classification; colored Petri nets; heterogeneous; identification; multi-path; OLSR; protocol; IoT



Citation: Benjbara, C.; Habbani, A.; Mouchfiq, N. New Multipath OLSR Protocol Version for Heterogeneous Ad Hoc Networks. *J. Sens. Actuator Netw.* **2022**, *11*, 3. <https://doi.org/10.3390/jsan11010003>

Academic Editor: Lei Shu, Adnan Al-Anbuky, Stefan Fischer, Joel J. P. C. Rodrigues and Mário Alves

Received: 15 October 2021
Accepted: 20 December 2021
Published: 28 December 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The world is trending to becoming a connected space with the emerging new technologies that mainly consist of broadband and wireless systems, such as IoT, AI, smart cities, precision agriculture, etc.

The ad hoc network is an ultimate example of a special case of wireless architecture without infrastructure. It is commonly used in recent engineering ventures. It appears in multiple forms: mesh, sensor, mobile, vehicular, flying, and body wireless networks [1–4].

Generally, ad hoc networks have a wide range of routing protocols belonging to different families (proactive, reactive, hybrid, and others) [5], each of which is divided into two distinct categories: mono-path and multi-path. This latter ensures good communication performance by improving different aspects: security enhancement, bandwidth boost, load balancing, and transmission delay mitigation.

An architecture that contains two or more kinds of networks represents a new net named heterogeneous. Heterogeneity is embodied in two facets: a communication channel and a well-defined nature of the nodes. Several studies aimed at improving the efficiency of this network family by affecting several aspects: organization [6], energy [7], security [8], throughput [9], routing protocols [10–13], and others.

The main problem with heterogeneous ad hoc networks is the diversity of their components. Each node has specific characteristics related to its nature, such as range, speed, routing protocol, etc. Ad hoc signifies without infrastructure, so depending on the node position in the data exchange route, it can play the role of a simple node, router, gateway, or translator between two nodes that do not speak the same language. Thus we can have one or more gateways/translators within the same network, which increases the sending time and creates a risk of losing the link due to the mobility of the nodes. As a result, data routing becomes increasingly complex, less secure, and less efficient.

As the M3S team (Mobile Smart Security Systems team, in Smart Systems Laboratory, ENSIAS, UM5, Rabat, Morocco), we chose this novel research track by suggesting an original routing protocol which ensures reliable, secure, and optimal direct communication without intermediate nodes. It also respects the advantage of every node characteristic. As a matter of course, each member offers a new idea that affects one or more aspects of the proposed solution:

- Multipath routing based on classification paths ensuring the exchange of data between source and destination as well as benefiting from the presence of several links [14].
- Reduction of traffic broadcast based on geographic broadcasting rules (GFR), which act on bandwidth, energy consumption, and packet loss [15].
- Security based on the location and insulation of black holes [16].

In this paper, we present our multipath routing protocol that provides the same communication language to heterogeneous components of an ad hoc network by taking into account the characteristics of each of them (range, position, speed). This protocol has four main functions: node identification, path computation, path classification, and path selection. Based on several studies, we noticed that the OLSR protocol is the base protocol for the mobile ad hoc network “MANET”, the vehicular ad hoc network “VANET”, and the flying ad hoc network “FANET”. Therefore, we chose a specific heterogeneous ad hoc network composed of nodes from these three environments using a dedicated version of the OLSR protocol entitled multipath heterogeneous ad hoc network OLSR “MHAR-OLSR”. In the latter, we changed the form of the HELLO message and added the protocol’s features. Under the NS-3 simulator, we tested the performance of our protocol by comparing it with the OLSR. Additionally, we designed the first three stages of the new version with the colored Petri net to understand their functional and dysfunctional behaviors.

The rest of the paper is structured as follows: in the next section, an overview of the existing studies about routing within heterogeneous networks is undertaken. In Section 3, we present our new routing protocol concept, and we outline the developed model and sub-models of the new OLSR multi-path version. In Section 4, we propose a case study of the solution in Section 5, after we show the evaluation performances in Section 6, and finally in Section 7, we draw our conclusion and present directions for future work.

2. Related Work

This subsection brings a set of works dealing with the various studies made around the communication within the heterogeneous ad hoc networks. In [10], the authors have proposed an ad hoc Traversal Routing “ATR” solution resolving the obstacle of communication created by the lack of interoperability between the different routing protocols existing inside a heterogeneous ad hoc architecture composed by nodes belonging to networks MANET, VANET, and Mesh. The ATR is a mechanism implemented in some nodes representing gateways that convert control messages from one network to another according to the routing protocols used. Okano and his colleagues [11] have integrated this ATR solution in their work, named the autonomous clustering-based inter-domain routing protocol. It consists of three protocols: a local routing protocol for routing in each MANET, an ATR that ensures the communication among multiple MANETs, and an autonomous clustering that allows managing NwGW nodes. Their idea has been based on self-governing clustering that creates groups in each MANET. Each array has a head that selects according to the information collected on the other networks, one or more NwGws endowed by the ATR

algorithm for playing the role of gateway between the different clusters. Wang et al. [12] have undertaken studies on the heterogeneous MANET system by considering the conventional border gateway protocol as a new routing layer architecture that applies commercial concepts of virtual routers toward transparent connect heterogeneous networks even in the presence of mobility. The work achieved by Rekha and DV Ashoka [13] have devised an analytical modeling strategy where the main objective is to ensure the establishment of sustainable routes for mobile nodes in a heterogeneous mobile ad hoc network integrated into the IoT.

Analyzing all these proposals, we notice that they all use a gateway to ensure the communication between nodes of distinct networks. This concept has a limitation which is reflected in the consumption of memory space and energy at the bridge node, in addition to a high risk of data loss due to an eventually broken link between the intermediate neighbors.

On the other hand, Omar Sami Oubbati and colleagues [17] propose a new strategy for efficient routing within the heterogeneous network composed of vehicles and drones (UAVs) inside an urban area that makes data delivery reliable and guarantees robust paths in case of timeout of each discovered route. This solution is based on ad hoc cooperation between the VANET and FANET components. However, it remains limited to a well-defined type of network and architecture.

In this paper, we propose a new multipath routing protocol concept. It applies in a heterogeneous network comprising all ad hoc nodes types while respecting the characteristics of each of them. Our design presents a relevant solution that addresses both limitations of gateway-based communication and the predefined customized architectures.

3. New Protocol Concept

In this section, we present a new routing protocol named the multi-path heterogeneous ad hoc routing protocol “MHAR” that ensures sustainable connectivity within a heterogeneous network while respecting the characteristics of each component.

As shown in Figure 1, the main idea of the protocol is to exploit route discovery to choose the best path for a specific type of data exchanged between communicating nodes. Established paths are not only made up of a single category but can also be made up of two or more depending on the traffic density and the actual distribution of nodes making up the path.

When multiple paths are computed, they are then classified based on the characteristics of the nodes that compose them, and packets will be delivered through the routes destined to a specific type of data (critical, informative, or preventive).

These options give our protocol a specific structure made up of different stages linked to guarantee the transmission of data from the source to the destination:

- The identification step allows each node to assign a class identifier to its neighbors according to their range and relative speed,
- The classification of the computed paths based on the class identifiers assigned to the nodes which compose them,
- The choice of the transmission path linked to the nature of the transmitted data,
- Data analysis determines the nature of the transmitted data:
 - i. Critical data (311) is very important when it comes to sending a fast and reliable path. The pH of the earth in precision agriculture is a very important measure. If it ever reaches a critical threshold, then the action must be taken immediately.
 - ii. Preventive data (312) is shared information to warn of potential danger. It must be transmitted reliably, but not necessarily via the fastest route. In the forestry sector, a sensor sends the reached temperature in precise time to a specific location to notify the command post.
 - iii. Informative data (313) is data communicated periodically on a less important path (the longest among those calculated) that is sufficient for its transmission. For example, a taxi regularly sends its position to its transport company.

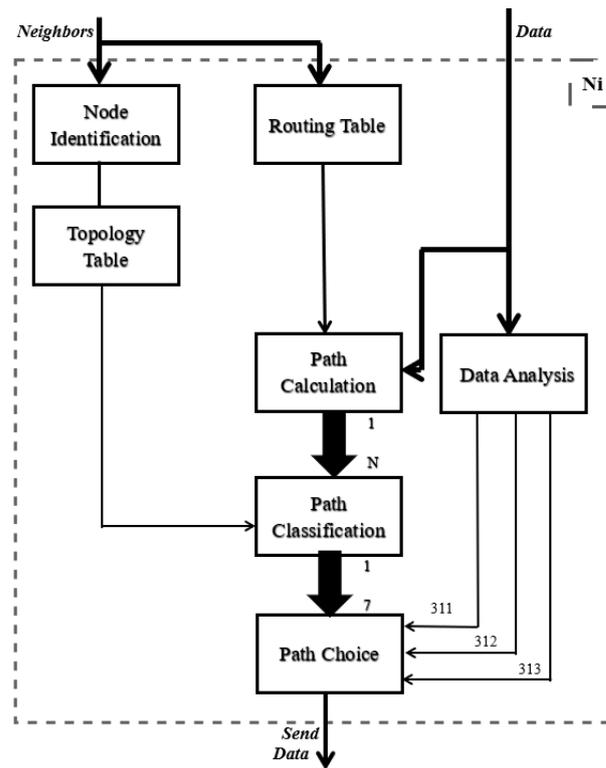


Figure 1. Node communication architecture [14].

Before bringing the MHAR protocol into the real world and defining its packet and message formats, it is important to experiment with its operational concept in a basic study environment. For this purpose, we carried out a comparative study between different types of ad hoc networks (Table 1).

Table 1. comparison table of characteristics of ad hoc network categories.

Types of Ad Hoc Network	Criteria				
	Mobility	Density	Topology Change	Power	Protocol
WMN	Low	High	Slow	Limited	AODV [18]
WSN	Low	High	Slow	Limited	AODV [19]
MANET	Low	High	Slow	Limited	OLSR [20]
VANET	Medium	Medium	Average	Average	QoS-OLSR [21,22]
FANET	High	Low	Rapid	High	P-OLSR [23–26]

According to this comparison table, we notice that the MANET, VANET, and FANET networks can constitute an example of a hybrid network regrouping mobile, vehicular, and flying components using various versions of the same protocol OLSR standard. The latter already has a multi-path version MPOLSR [27] that improves the quality of communication by affecting various aspects: security, bandwidth, load balancing, and transmission delay.

Based on this analysis, we decided to apply the concept of our MHAR protocol on OLSR, producing a new multi-path version, called MHAR-OLSR, that ensures the communication inside the MANET VANET FANET heterogeneous ad hoc network (HADN_MVF).

4. MHAR-OLSR Protocol

4.1. Overview: “CPN”

A colored Petri network “CPN” is a colorful and hierarchical high-level version of the standard Petri nets. It provides a graphical and mathematical representation of discrete

event systems in several domains (computer science, industrial ...) by modeling and verifying their static and dynamic behavior.

A CPN model contains [28]:

- Places represented in the oval forms with a type and can also have an initial marking indicating a multi-set of values (tokens) of the corresponding type. They are passive components of the system that can contain/store objects or information.
- Arcs are arrows that indicate the sense of connection between places and transitions. They contain expressions with zero or more free variables.
- Transitions have rectangular forms and depict the active components of the model, named "the bindings". An active binding is a liaison that ensures all input places contain at least the tokens prescribed by evaluating the arc expressions. It also can create new tokens on output places by removing corresponding tokens on input places.

The number of places, transitions, and tokens increase with the complexity of the modeled system. So the increased number of components makes it more delicate to monitor and verify this system's functioning.

The hierarchical feature of CPN brings modularity to the system by creating modules (sub-models or pages). That simplifies the supervision of the system. The colorful aspect gives each token a color to differentiate between them to simplify the reading of models and sub-models.

Graphically, the module has a rectangle form with a double outline (substitution transition). It has two interface (places) types that must share the same name:

- Port places inside the sub-model schema having an annotation of In, Out, or I/O. They are illustrated by an oval with a double contour.
- Socket places outside the schema connected to the substitution transition, and directly to port places using port/socket attributions.

4.2. CPN MHAR-OLSR Model

This section describes the colored Petri net modeling technique used to implement the MHAR protocol concept. In particular, the model developed in this paper is referred to as the MHAR-OLSR protocol.

The model in Figure 2 presents the main module of the hierarchical CPN model describing the generic behavior of the protocol's algorithm:

- The topology of the network is defined as a set of tokens in the place "Topology". Every token is a triplet containing a bow connecting two nodes (N1, arc, N2). The order of the nodes in this triplet tells us the direction of the flow.
- After detecting the presence of the data, the place "Found Data" ensures the activation of "Path_Calculation" and "Path_Choice" sub-models.
- The places "Found Path tree" gives the list of the calculated paths. That represents the input arc expressions with those of the "Identified Neighbor" of the sub-model "Path_Classification".

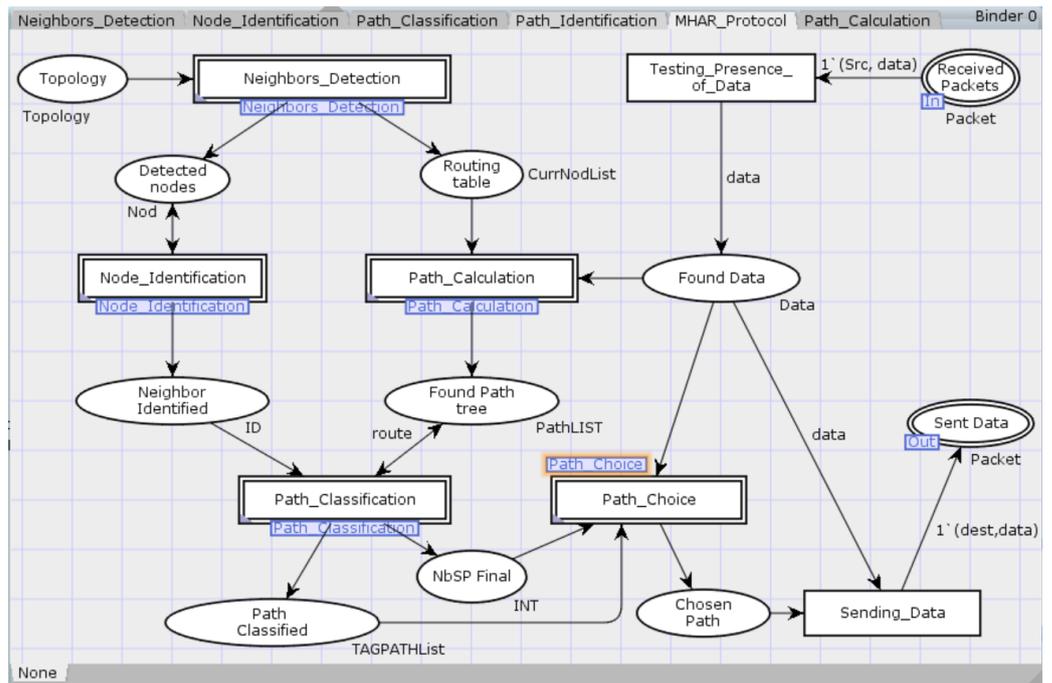


Figure 2. MHAR algorithm model.

4.2.1. Sub-Model “Node_Identification”

The figure below (Figure 3) illustrates the module of the identification step, where each node of the network must identify proportionally its first neighborhood according to two main criteria: the range and the instantaneous relative speed. These characteristics are inserted in the triplet (N1, S, r) of the “detected nodes” place tokens.

The identifier at each node indicates the network nature of its neighbors. It can take one of three values: 1, 2, or 3, respectively referred to as MANET, VANET, or FANET.

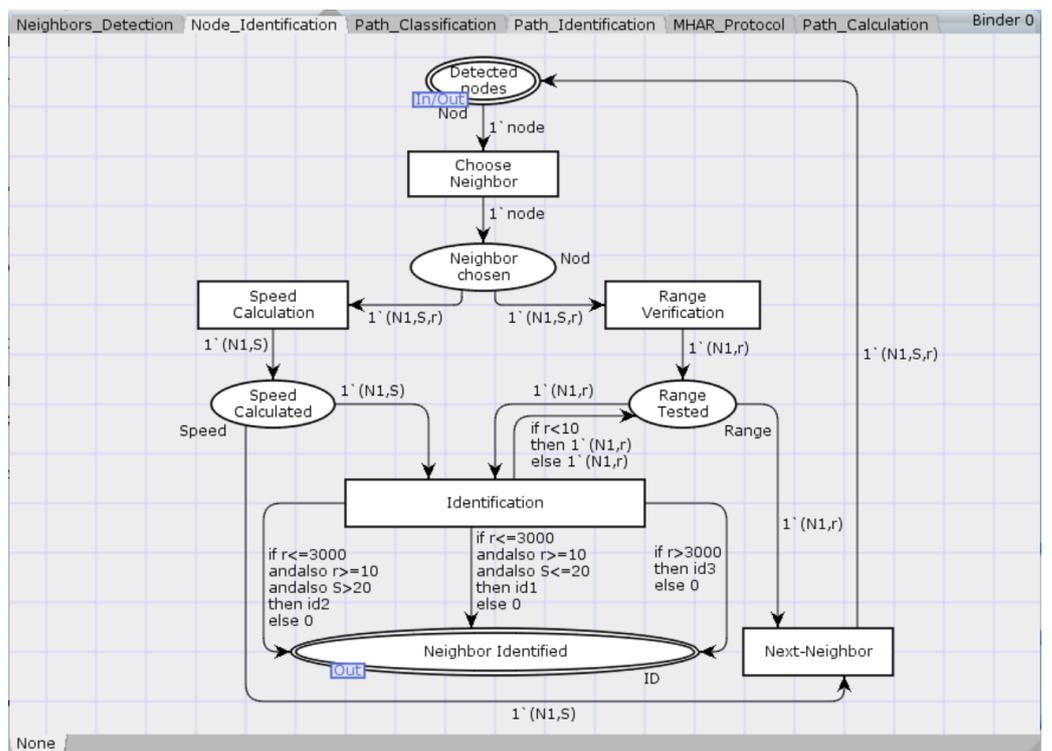


Figure 3. CPN modeling of node identification.

In Figure 4, the RANGE_FANET value depends on the type of MAC protocol used, when HUMAN_SPEED could take the maximum speed score ever achieved by men. In other terms, these limits would take values accommodated to the domain application needs.

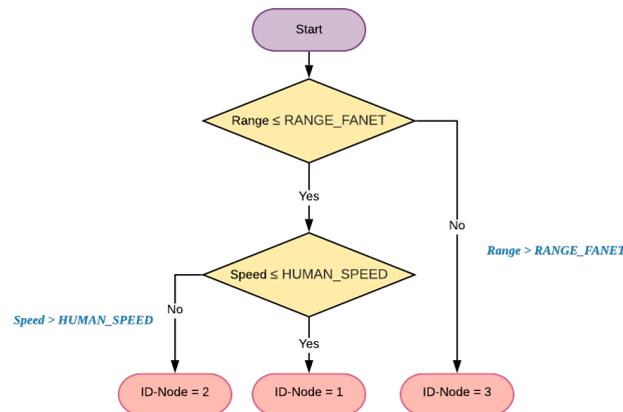


Figure 4. Identification organizational chart [14].

4.2.2. Sub-Model “Path_Calculation”

Dijkstra’s algorithm provides the shortest path calculation. The researchers created its multi-path version, which they applied in OLSRv2 [29] to obtain the MPOLSR multi-path routing protocol [30].

This new algorithm maintains QoS metrics by supporting frequent changes in the network topology using two auxiliary functions: route recovery and loop verification. It also improves the flexibility and scalability of Dijkstra’s original model [31] by adding link metrics and cost functions into its principle:

1. fp increases the costs of arcs belonging to the previous path Pi (or of opposite arches belonging to it), which gives us the possibility to have routes with disjoint links by penalizing only the links used. For this, the cost functions will be defined as follows: fp (c) = 3c and fe (c) = c,
2. fe gives paths with disjointed links and nodes. It grows costs of arcs affected to the vertices of the previous path Pi, which penalizes the links and nodes, setting this by: fp (c) = 3c and fe (c) = 2c.

The Dijkstra multi-path algorithm is only active when data is present to be sent (it can be said to be an on-demand path calculation).

Given the complexity of the Dijkstra algorithm, several researchers [32] have been able to model it in Petri net to make it more manipulatable. Kadri [33] has used multi-path Dijkstra in his study and has modeled it with High-Level Petri nets. Based on his model, I was able to design my own.

4.2.3. Sub-Model “Paths_Classification”

The existing classification methods use the number of jumps, the state of the link [34], or the energy consumption [35] to rank the calculated paths. In our study, we exploit the nature of the nodes that make up the detected routes as a classification measure.

The CPN net shown in Figure 5 illustrates the main transitions of the classification phase:

- From the “Found path tree” port place where the calculated paths are saved from the shortest to the longest according to their number of hops, one route is chosen among them.
- In the “browse_list_hops” transition, the identifiers of all selected path components will be extracted.
- The “Path identification” (Figure 6) substitution transition exploits the received information to identify this route being processed. And the “Next Path” transition is fired

enough times to recover all paths from the “Paths identified” place to the “Found path tree” place.

- Each route will have an identifier and a tag indicating its class. These represent its quality, efficiency, and availability for sending data.

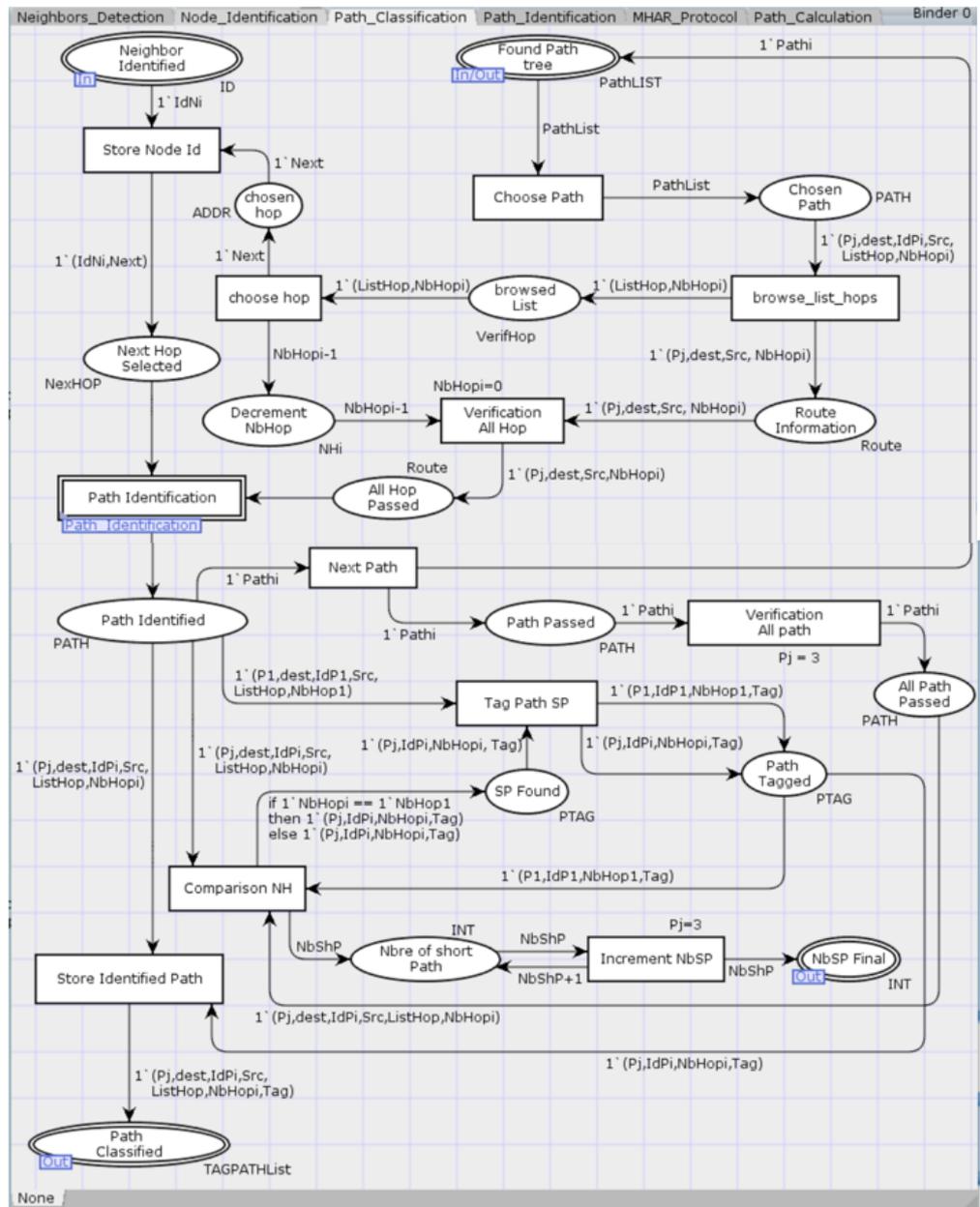


Figure 5. CPN model of path classification.

To give a clearer idea of the path identification phase, the flowchart (Figure 7) shows the label values from 1 to 7 assigned to each route based on the identifiers of its components:

- A path composed of FANET nodes (ID-Node = 3) will have an identifier 1 (Path-Id = 1),
- The presence of MANET nodes (ID-Node = 1) and at least one FANET node gives an identifier 2 for this path,
- A route having an identifier 3 will link nodes of at least all MANET, VANET (ID-Node = 2), and FANET network categories,
- ...

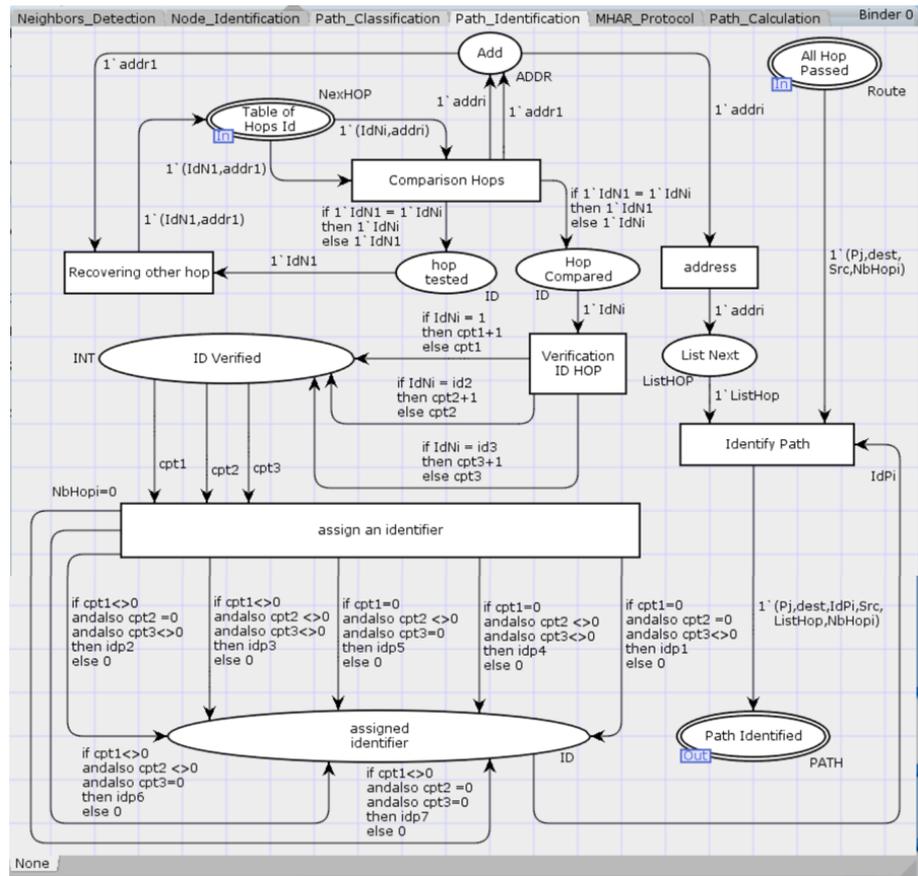


Figure 6. Path identification module.

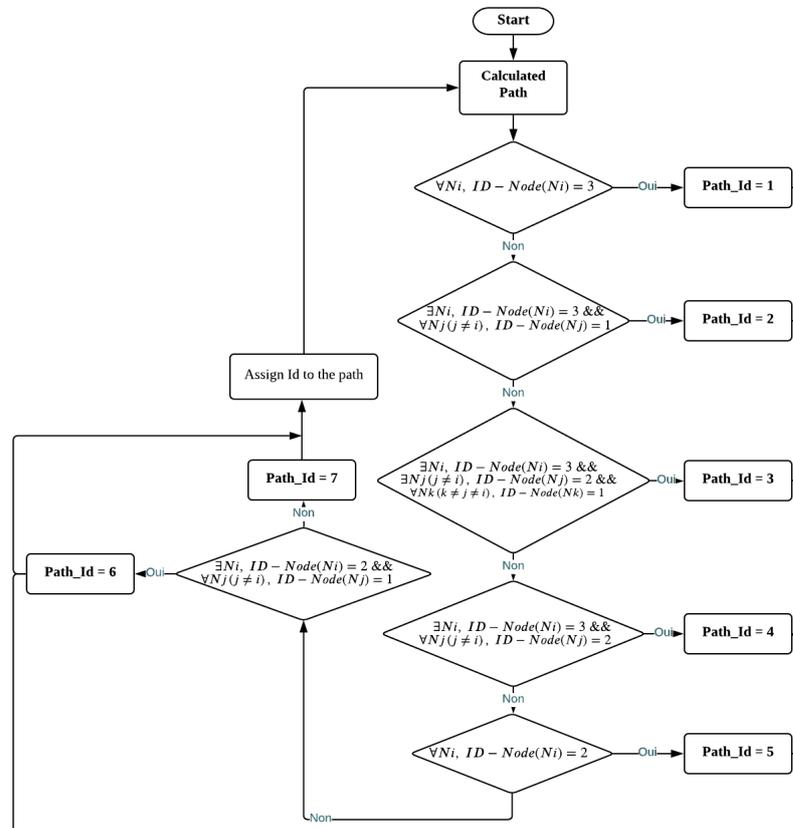


Figure 7. Path classification flowchart.

Each “Path-Id” indicates the route quality that ensures sending a specific type of data. For example, identifier “1” represents that this path is the fastest and most reliable, then it is reserved for critical data. While Path-Id = 7 is given to the longest and least reliable itinerary where informative data can be transmitted. This type of classification allows us to have several paths with the same identifier.

5. Case Study: Application of MHAR-OLSR

In this work, the network HAdN_MVF is assumed to be composed of mobile, vehicular, and UAV nodes (c.f., Figure 8). It is divided into the ground area whose size depends on the communication range of vehicles (300 m) and mobiles (100 m). As for the aerial zone, we have two different cases: small aerial zones and large aerial zones depending on the communication range of the drones, which is 400 m and 1000 m, respectively [36,37]. The communication between two nodes can be successfully established if they are within the communication range of each other.

The choice of drones that fly at low and constant altitudes [38] ensures a wide coverage that supports more terrestrial devices (cars and mobiles) [39,40]. Each node in the network is equipped with a GPS system that specifies its current geographical position.

On the energy side, vehicles and drones are equipped with rechargeable batteries that can be powered by solar energy, gasoline, or electric energy [41].

The exchange of data packets over the network is done by means of integrated wireless interfaces using IEEE 802.11p at the MAC layer [42] and MHAR-OLSR at the network layer. The last protocol uses the same principle as standard OLSR routing [43] by exchanging Hello and TC messages between its nodes:

- The Hello message allows each node to have an overview of its first and second neighborhoods (discovery of neighbors). Each device sends a Hello message including all the necessary information and utilities: type of connection, will of the node, neighbors’ information, etc.
- The topology control message (Tc message) is broadcasted periodically within the network. It’s the structure where nodes insert the list of their neighbors to build the routing tables.

In the HAdN_MVF network, we have six possible types of links (c.f., Figure 9): Vehicle-to-Vehicle “V2V”, Vehicle-to-Mobile “V2M”, Vehicle-to-UAV “V2U”, UAV-to-Mobile “U2M”, UAV-to-UAV “U2U”, and Mobile-to-Mobile “M2M”.

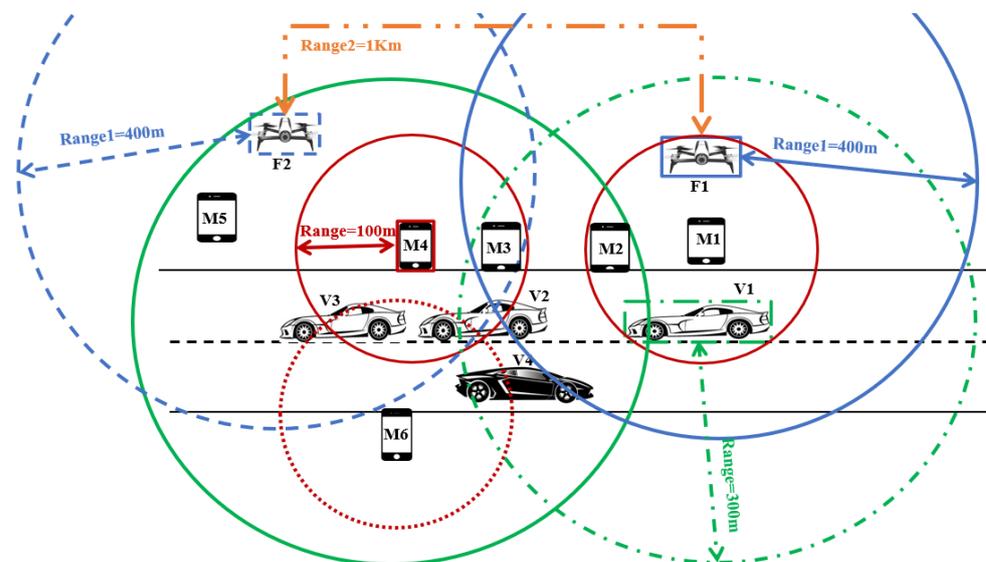


Figure 8. Example of HAdN_MVF network.

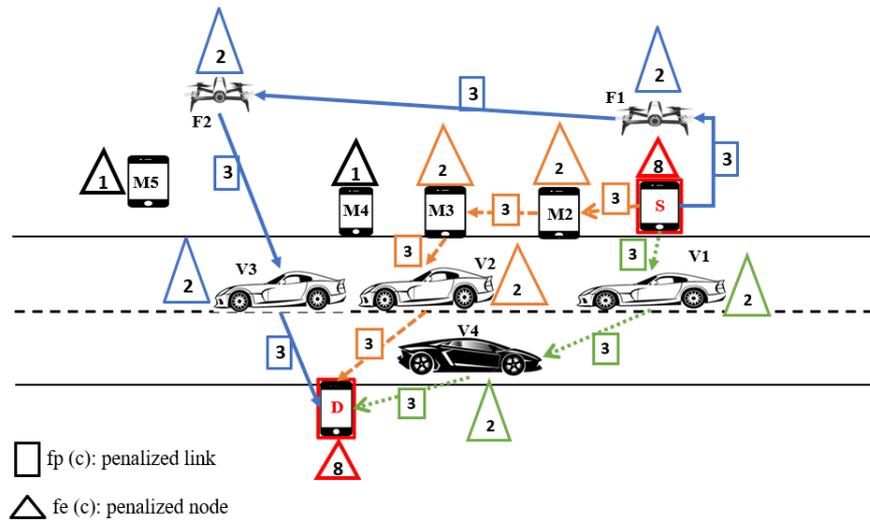


Figure 9. Example of MHAR-OLSR communication within an HAdN_MVF network.

5.1. “Node Identification Step”

Combining the MHAR principle and OLSR, we obtain the routing protocol MHAR-OLSR with new structures.

(a) MHAR-OLSR Hello message structure:

The new Hello message (Figure 10) will contain the node position in three dimensions: the latitude, the longitude, and the altitude. This information allows the node to calculate the instantaneous speed of its neighbors in the first neighborhood. To obtain this speed, we apply the following Equation (4):

$$\begin{cases} V_{(ij)}(t) = \tilde{V}_{(ij)}(t) + V_{(ij)}(t - 1) \\ V_{(ij)}(0) = 0 \end{cases} \quad (1)$$

We need the instantaneous relative velocity represented as follows:

$$\tilde{V}_{(ij)}(t) = \frac{d_{(ij)}(t) - d_{(ij)}(t - 1)}{\delta t} \quad (2)$$

where:

* $d_{(ij)}(t)$ and $d_{(ij)}(t - 1)$ are the distances between two neighboring nodes (i and j) at two successive instants, or:

$$d_{(ij)} = \sqrt{(x_j - x_i)^2 + (y_j - y_i)^2 + (z_j - z_i)^2} \quad (3)$$

* x, y, z : Cartesian coordinates equivalent to the geographic coordinates of a node.

* δt : is the difference between the arrival time of the first and last message Hello.

For having a more precise speed value, we add an exponential average (Alpha) to give more importance to all historical movements of the nodes since the beginning of the communication and to filter abrupt speed variations. Alpha ranges between 0 and 1 and is defined in a manner that makes sense to the application field. Then, the filtered instantaneous speed takes this new form:

$$\begin{cases} V_{(ij)}(t) = \alpha \tilde{V}_{(ij)}(t) + (1 - \alpha)V_{(ij)}(t - 1), \\ 0 \leq \alpha \leq 1 \\ V_{(ij)}(0) = 0 \end{cases} \quad (4)$$

The node range will be inserting too in this new structure of hello message.

Byte 0 0 1 2 3 4 5 6 7		Byte 1 0 1 2 3 4 5 6 7		Byte 2 0 1 2 3 4 5 6 7		Byte 3 0 1 2 3 4 5 6 7	
Reserved		HTime		Willingness			
Altitude		Range					
Latitude							
Longitude							
Link Code	Reserved	Link Message Size					
Neighbor Interface Address							
Neighbor Interface Address							
...							

Figure 10. MHAR -OLSR Hello message format.

The latitude and longitude have the same form, a floating-point number stocked in 4 bytes. The altitude and range are each represented by fixed-point numbers occupying 16-bits. These 12 bytes added to the standard hello message haven't any impact on the frames size in medium and large networks.

(b) MHAR-OLSR identification structure:

Adding an intelligent and dynamic structure will ensure the store of the neighbors' identifiers. This structure allows the node to gather the maximum amount of information on all topology components.

After each exchanged hello message, the node updates its identification structure by verifying the existence of a neighbor, the change of its position indices (which will act on its identification), or the presence of a new neighbor.

After each calculation of the paths, the source node structure will add the identifiers of the nodes, which constitute the calculated paths. If one of them becomes its neighbors in an instant, it can, therefore, just update its identifier.

We are going to give this structure the aspect of a database of identifiers that we can use to have a precise vision of our network.

5.2. Path Calculation Step

The OLSR principle requires nodes to renew their routing tables after each new Tc message is received. A routing table saves routes to all possible destinations.

However, the multipath version does not always keep the routing table. When exchanging data packets, it applies the Dijkstra Multipath algorithm to fill a multipath routing table with the calculated paths that connect the source "S" to the specified destination "D".

According to Figure 9, S has three neighbors in its communication range: F1, V1 and M2, thus three potential paths.

- The first and shortest path calculated is: $S \rightarrow V1 \rightarrow V4 \rightarrow D$, since V4 is inside the range of V1 and D at the same time.
- The second established route is: $S \rightarrow F1 \rightarrow F2 \rightarrow V3 \rightarrow D$. F2 is connected to F1 via U2U, and to V3 using U2V. Then V3 is among D neighbors.
- The Last path is: $S \rightarrow M2 \rightarrow M3 \rightarrow V2 \rightarrow D$.

In Figure 9, the source node (S) finds three paths to its destination (D) with disjoint links and nodes by applying the second case of the cost functions (Section 4.2.2, Equation (2)). Knowing that, initially, all costs for links and nodes are set to 1, thus the cost of each associated arc in these detected paths passes from 1 to 3 by using fp, and each cost of node takes value 2, by mean of fe.

5.3. Paths Classification Step

After detecting the shortest paths in the previous step, we can now classify them. To do so, we apply the classification algorithm (Figure 7) based on the components nature of each route. Then the detected paths are classified as follows:

- $S \rightarrow V1 \rightarrow V4 \rightarrow D$, receives the Path_Id = 5, the path comprises just VANETs nodes (ID-Node = 2).

- $S \rightarrow F1 \rightarrow F2 \rightarrow V3 \rightarrow D$, is tagged by Path_Id = 4, this route contains the FANET and VANET nodes (respectively: ID-Node = 3 and ID-Node = 2).
- $S \rightarrow M2 \rightarrow M3 \rightarrow V2 \rightarrow D$, takes Path_Id = 6, the presence of MANET and VANET nodes (respectively: ID-Node = 1 and ID-Node = 2).

The path with identifier 6 is less reliable than the others. It consists of MANET nodes with a limited range and VANET nodes characterized by their high speed. Therefore, there is a risk of losing the link on these itineraries. This is why they have a minimum priority.

But the second one (Path_Id = 4) remains more reliable because it contains UAVs. These devices are characterized by high power and controlled mobility.

6. Evaluation Performances

The implementation and simulation of the MHAR protocol concept shows the impact of its added functionalities on the QoS metrics. Based on that, we can enhance our proposition to have the best results. Afterward, we will develop our internal architecture of the MHAR protocol: packets and messages.

6.1. Implementation

This section introduces the MHAR algorithms of the implemented code into the OLSR protocol:

- Algorithms 1 and 2 show the node identification and path calculation functions,
- The path classification function (Algorithm 3) aims to assign an identifier to every calculated path using the path identification function and to mark the ones having the smaller number of hops with the short path tag,
- The path identification function (Algorithm 4) dispatches identifiers to all routes based on the nature of their components (nodes).

Algorithm 1: Node identification function

1: Initial

2: NeighborTuple: Tuple of neighboring nodes grouping their important characteristics

3: RANGE_FANET: Range value of FANET nodes

4: $Speed_{(1,i)}$: Instantaneous relative velocity between N1 and its neighbors

5: HUMAN_SPEED: Speed max value of MANET nodes

6: N_1 : Current node

7: $ID - N_i$: Node identifier

8: IDNList: List of all identified node

9: Begin

10: Identification(NeighborTuple)

11: $N_i \leftarrow \text{GetNeighbor}(\text{NeighborTuple})$

12: $(X_i, Y_i, Z_i) \leftarrow \text{GetCoordinates}(\text{NeighborTuple})$

13: $Range_i \leftarrow \text{GetRange}(\text{NeighborTuple})$

14: $Speed_{(1,i)} \leftarrow \text{RelativeVelocity}(X_i, Y_i, Z_i)$

15: **for** all neighbor N_i **of** NeighborTuple **do**

16: **if** $Range_i > \text{RANGE_FANET}$ **then**

17: $ID - N_i \leftarrow 3$

18: **else if** $Speed_{(1,i)} \leq \text{HUMAN_SPEED}$ **then**

19: $ID - N_i \leftarrow 1$

20: **else**

21: $ID - N_i \leftarrow 2$

22: **end if**

23: **end if**

24: **end for**

25: **return** IDNList

26: End

Algorithm 2: Path calculation function

```

1: Initial
2: src: the source
3: dest: the destination
4: NoP: number of routes
5: V: set of the graph vertices or nodes
6: E: set of arcs e of  $V \times V$  (i.e., a relation on V)
7: c: arc cost
8: G: the graph composed of (V; E; c)
9:  $P_i$ : the path
10: PathTree: set of calculated path ( $P_1, \dots, P_{NoP}$ )
11: Begin
12: function MultiPathDijkstra (src, dest, G, NoP)
13:    $c_1 \leftarrow c$ 
14:    $G_1 \leftarrow G$ 
15:   for i  $\leftarrow$  1 to NoP do
16:     SourceTreei  $\leftarrow$  Dijkstra( $G_i$ , src)
17:      $P_i \leftarrow$  GetPath(SourceTreei, dest)
18:     for all arcs e in E do
19:       if e is in  $P_i$  OR Reverse(e) is in  $P_i$  then
20:          $c_{i+1}(e) \leftarrow f_p(c_i(e))$ 
21:       else if vertexHead(e) in  $P_i$  then
22:          $c_{i+1}(e) \leftarrow f_e(c_i(e))$ 
23:       else
24:          $c_{i+1}(e) \leftarrow c_i(e)$ 
25:       end if
26:     end if
27:   end for
28:    $G_{i+1} \leftarrow (V, E, c_{i+1})$ 
29: end for
30: return PathTree
31: End

```

Algorithm 3: Path classification function

```

1: Initial
2: HopTuplei: tuple of address and identifier of hops composing a path i
3:  $P_i$ : the path
4: PathTree: set of calculated path ( $P_1, \dots, P_{NoP}$ )
5: IDHListi: list of identified hops in a path i
6: ID –  $P_i$ : path i identifier
7: NbHopi: number of hops in path i
8: ShPList: list of shortest paths
9: Tag –  $P_j$ : tag of path j inserted in the ShPList
10: SP: shortest path tag
11: NbShP: number of shortest paths
12: ClassPathTuple: set of classified path composed by ( $P_i, ID - P_i, Tag - P_i$ )
13: Begin
14: Path_Classification (PathTree, IDNList)
15:   for i  $\leftarrow$  1 to NoP do
16:      $P_i \leftarrow$  GetPath(PathTree)
17:     NbHopi  $\leftarrow$  GetNbHop ( $P_i$ )
18:     IDHListi  $\leftarrow$  GetID(IDNList, NbHopi)
19:     HopTuplei  $\leftarrow$  Browse_Hops( $P_i, IDHList_i$ )
20:     ID –  $P_i \leftarrow$  Path_Identification(HopTuplei, NbHopi)
21:   end for
22:   ShPList  $\leftarrow$  Shortest_Paths(PathTree)
23:   NbShP  $\leftarrow$  GetSize(ShPList)
24:   for j  $\leftarrow$  1 to NbShP do
25:     Tag –  $P_j \leftarrow$  "SP"
26:   end for
27: return NbShP, ClassPathTuple
28: End

```

Algorithm 4: Path identification function

1: Initial
 2: HopTuple: tuple of hops composed by the address of each hop and its identifier
 3: Cpt: counter
 4: $Cpt1 \leftarrow 0, Cpt2 \leftarrow 0, Cpt3 \leftarrow 0$
 5: $ID - N_i$: identifier of Node i
 6: ID-P: path identifier
 7: NbHop: number of hops
 8: Id: identifier
9: Begin
10: Path_Identification(HopTuple, NbHop)
 11: **for** $i \leftarrow 1$ **to** NbHop **do**
 12: $ID - N_i \leftarrow \text{GetID}(\text{HopTuple})$
 13: **if** $ID - N_i = 1$ **then**
 14: $Cpt1 \leftarrow Cpt1 + 1$
 15: **else if** $ID - N_i = 2$ **then**
 16: $Cpt2 \leftarrow Cpt2 + 1$
 17: **else**
 18: $Cpt3 \leftarrow Cpt3 + 1$
 19: **end if**
 20: **end if**
 21: **end for**
 22: $ID - P \leftarrow \text{Assign_ID}(Cpt1, Cpt2, Cpt3)$
 23: **return** ID-P
24: End

6.2. Simulation

To evaluate and compare MHAR-OLSR and OLSR routing protocols efficiency, we use the NS3 [44] version 3.29. This network simulator provides an open, extensible platform for networking research and education. It generates important files; .xml describes the simulation environment with a GUI, and .csv contains the simulation parameters and calculated metrics.

6.2.1. Simulation Scenario

We experimented different simulations with different densities of heterogeneous nodes moving randomly within a 2000 m × 2000 m area for 400 s. The simulation parameters are summarized in Table 2.

Table 2. Simulation parameters.

Parameters	Values
Routing protocol	OLSR, MHAR-OLSR
Traffic model	UDP
PHY/MAC layer	IEEE 802.11p
Range of MANET	≈100 m
Range of vehicules	≈300 m
Range of UAV	R1 ≈ 400 m and R2 ≈ 1000 m
Area size	2000 × 2000 m ²
Simulation time	400 s
Mobility generator	BonnMotion

Table 2. Cont.

Parameters		Values									
MANET nodes speed		[0, 2] m/s (≈ 7 km/h)									
VANET nodes speed		[0, 17] m/s (≈ 61 km/h)									
UAV nodes speed		[0, 5] m/s (≈ 18 km/h)									
Alpha (α)		0.5									
Network components	Number of Nodes	20	40	60	80	100	120	140	160	180	200
	“50%” MANET	10	20	30	40	50	60	70	80	90	100
	“40%” VANET	8	16	24	32	40	48	56	64	72	80
	“10%” FANET	2	4	6	8	10	12	14	16	18	20

6.2.2. Studied Metrics

Packet Delivery Ratio (PDR): allows revealing in percentage whether a protocol can send all outgoing data. Its calculation of the lost packets is the ratio between received ones by the destination node D_p and those sent by the source node S_p (Equation (5)). Higher values of PDR illustrate better performance. So PDR of 100% signifies that the network has high reliability and availability.

$$PDR = \frac{D_p}{S_p} \times 100 \tag{5}$$

End-to-End delay (E2E): describes the transfer time of the packet from the source to destination. It must be respected, otherwise the contained data in the transmitted packet becomes useless for the application. Equation (6) allows us to determine the E2E value:

$$E2E = \frac{t_R^P}{\sum D_p} \tag{6}$$

where:

t_R^P : Time of receiving the packet by the destination node

Energy cost per packet (E_{cpp}): gives the ratio between the total consumed energy over the number of successfully received packets at the destinations (Equation (7)).

$$E_{cpp} = \frac{E_{total}}{D_p} \tag{7}$$

where

$$E_{total} = E_{trans} + E_{rec} + E_{idle} \tag{8}$$

6.3. Results and Discussion

To study the impact of density, we vary the number of nodes from 20 (low density) to 200 (important density).

Figure 11 shows the percentage of data packets received at the destination as a function of node numbers. We remark that both protocols have the same shape with a minor difference in value within the interval of 20–60 nodes. In fact, MHAR-OLSR does not provide a considerable improvement to the communication since it can not detect more than two distinct paths, including a VANET or FANET device.

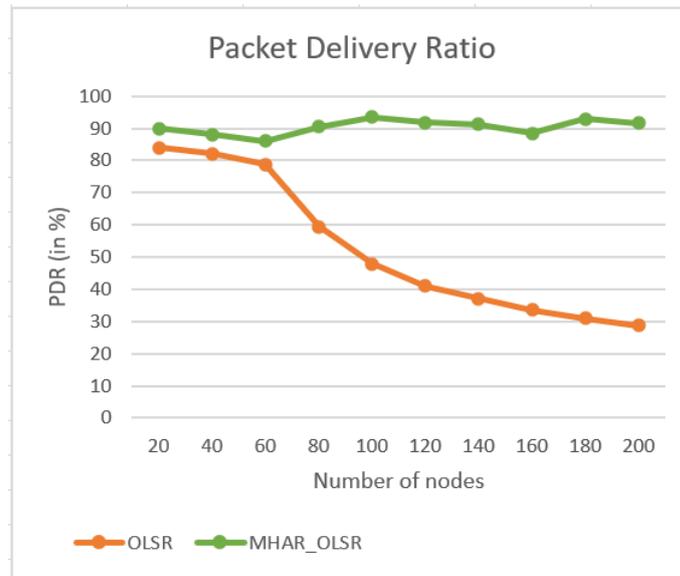


Figure 11. Packet delivery ratio as function of density.

From 80 nodes on, the single route in OLSR takes a long time before the node drops the packets as the time-out of the path expires. Moreover, the PDR ratio in OLSR is also influenced by the presence of more possible heterogeneous routes in the network, due to the increase in the proportion of VANET and FANET components, according to Table 2.

With this being said, the MHAR-OLSR protocol delivers more packets linking to the fact that the multipath establishes more paths between the source and the destination without being affected by the heterogeneity of the network.

Moreover, according to PDR results shown in article [10] (figure 10: Ratio of Delivered Packet), it is clear that the presence of ATR nodes influences the outcome of the PDR. We notice then that the PDR obtained in our simulation results is more significant than those of ATR. So we can say that MHAR-OLSR is more efficient in term of packet delivery ratio than ATR as a routing protocol within heterogeneous ad hoc networks.

Figure 12 presents the achieved end-to-end delay as a function of node density for each routing protocol tested. We observe inside the interval 20–60 nodes that the OLSR has an E2E delay between 50–200 ms. However, when the density increases, the single path becomes longer, and the values of the metric can reach up to 1700 ms in the network composed of 200 devices.

The presence of VANET and FANET nodes gives a plus to MHAR-OLSR that accepts their characteristics and benefits from their big range. In fact, the curve shows that the E2E delay values are between 30–150 ms within a network of 20 to 100 nodes, and the peak equals 700 ms at 200 nodes.

We conclude that the density impacts this metric for both protocols. However, the MHAR-OLSR offers better performance compared to the original OLSR.

Figures 13 and 14 allow us to evaluate the energy efficiency of the studied protocols. Based on the Equation (5), we deduce:

$$D_p = PDR \times S_p \tag{9}$$

So, we can write the Equation (7) in the following format:

$$E_{cpp} = \frac{E_{total}}{PDR \times S_p} \tag{10}$$

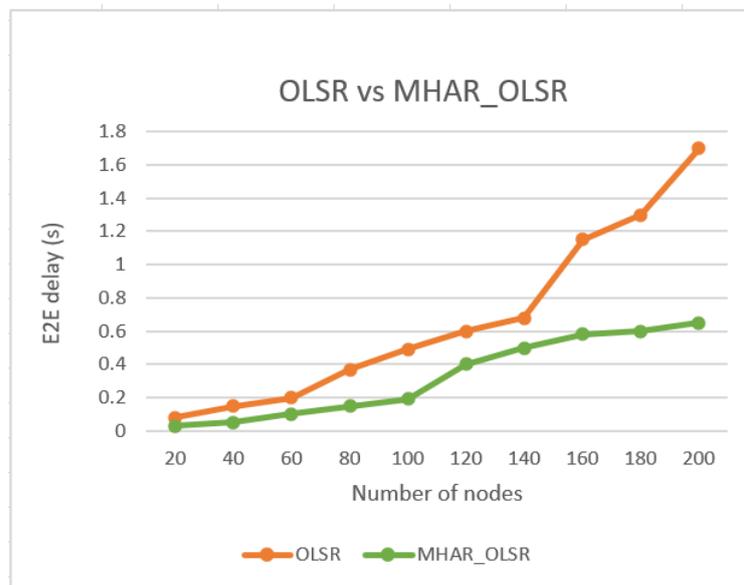


Figure 12. End-to-End delay as function of density.

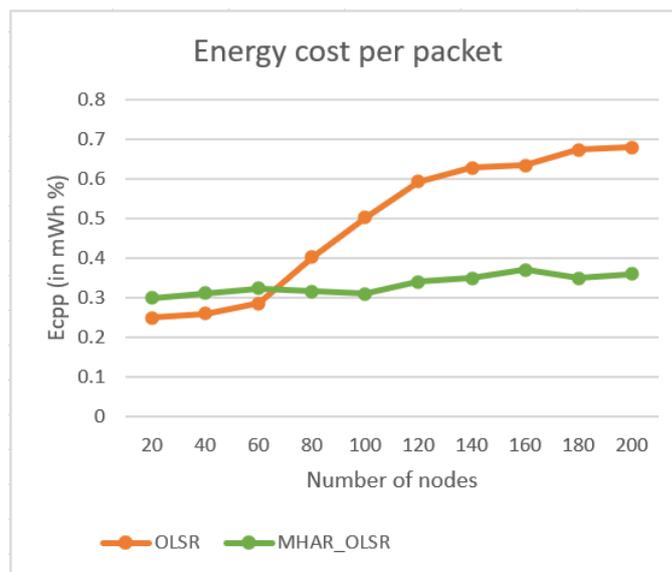


Figure 13. Energy cost per packet as function of density.

The energy cost per packet (Figure 13) keeps the same shape as the packet delivery ratio (Figure 11) in the range of 20–60 nodes since both protocols provide approximately the same results. On the other side, from 80 nodes on, the obtained curve illustrates exactly the representation of Equation (10), where the E_{cpp} is inversely proportional to the PDR.

Figure 14 gives an overview of the total energy consumed in the network based on its density. We see that the MHAR-OLSR consumes more energy than the OLSR protocol in general. Nevertheless, we notice that the energy consumption in OLSR decreases in the high density [120–200 nodes], which is expected since the E_{rec} decreases too.

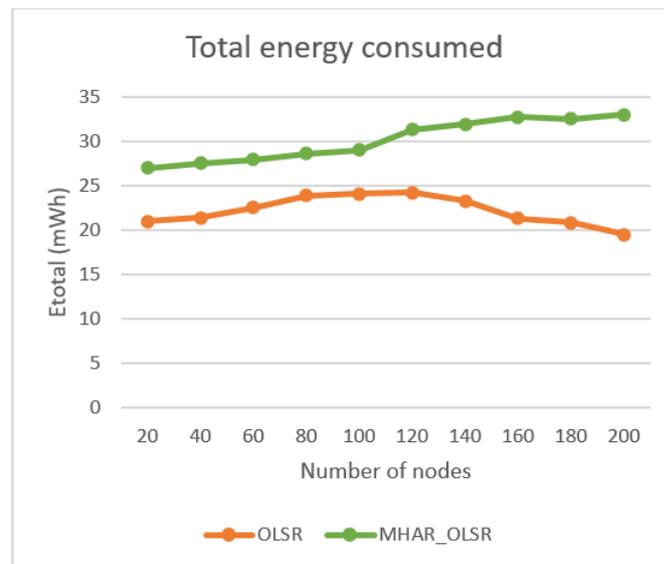


Figure 14. Total energy consumed as a function of density.

The main reasons for consuming energy in the MHAR-OLSR protocol vs. the OLSR protocol are its ability to manage route changes and the complexity of the implemented Dijkstra and path classification algorithms.

7. Conclusions & Perspectives

This research work addressed the problem of communication within heterogeneous ad hoc networks. These are constituted by multiple types of devices not having the same characteristics.

The study gives an overview of different protocols used in this specific network. It also presents our original multi-path heterogeneous routing protocol (MHAR) divided into four steps to ensure direct communication between the mixed nodes. Its concept has been combined with the OLSR protocol, creating a new version named MHAR-OLSR.

The modelization of this new proposition within the framework of colored Petri nets has the important advantage of understanding the pros and cons of its functional behavior.

The application of MHAR-OLSR in a chosen case study, like a heterogeneous ad hoc network composed of the MANET, VANET, and FANET nodes (HAdN_MVF), gives a clear idea of the estimated results.

According to the result analysis, we can say that the MHAR-OLSR performs better in the HAdN_MVF network compared to the OLSR routing protocol, although it consumes more power.

So far, we have seen in this study the MHAR concept and the integration of its three steps (node identification, path calculation, and path classification) in the standard OLSR protocol. And we have also tested the impact of the MHAR-OLSR version on QoS of the network compared to the OLSR protocol.

In future work, we will add the path choice function of the MHAR concept in our case study and test its influence on network performance. Based on all the results we will obtain, we will discuss the design of an appropriate MHAR protocol architecture that will be suitable for all types of ad hoc networks: terrestrial (WSN, MANET, VANET, wireless body area network “WBAN” [45]), airborne (FANET), and maritime (optical WSN “OWSN” [46]). Our protocol will ensure that heterogeneous ad hoc networks grouping the different ad hoc networks categories will be able to communicate reliably with better performance while always respecting the nature of each component.

Author Contributions: Conceptualization, C.B.; Supervision, A.H.; Validation, A.H. and N.M.; Writing—original draft, C.B.; Writing—review & editing, C.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

Abbreviations

List of used acronyms

AI	Artificial Intelligence
ATR	Ad hoc Traversal Routing
CPN	Colored Petri network
D_p	Packet received by the destination
E_{cpp}	Energy cost per packet
E_{total}	Energy total
E_{trans}	Energy transmitted
E_{rec}	Energy received
E2E	End-to-End delay
FANET	Flying Ad hoc Network
GFR	Geographic Forwarding Rules
HAdN_MVF	Heterogeneous Ad hoc Network MANET VANET FANET
IoT	Internet of Things
M2M	Mobile-to-Mobile
M3S	Mobile Smart Security Systems
MANET	Mobile Ad hoc Network
MHAR	Multi-path Heterogeneous Ad hoc Routing protocol
MHAR-OLSR	Multi-path Heterogeneous Ad hoc Routing OLSR protocol
MPOLSR	Multi-Path OLSR protocol
OLSR	Optimized Link State Routing protocol
OWSN	Optical Wireless Sensor Network
PDR	Packet Delivery Ratio
QoS	Quality of Service
RAT	Radio Access Technologies
S_p	Packet sent by the source
Tc	Topology Control message
UAV	Unmanned aerial vehicle
U2M	UAV-to-Mobile
U2U	UAV-to-UAV
U2V	UAV-to-Vehicle
VANET	Vehicular Ad hoc Network
V2M	Vehicle-to-Mobile
V2U	Vehicle-to-UAV
V2V	Vehicle-to-Vehicle
WBAN	Wireless Body Area Network
WMN	Wireless Mesh Network
WSN	Wireless Sensor Network

References

1. Piechowiak, M.; Zwierzykowski, P.; Owczarek, P.; Wasłowicz, M. Comparative analysis of routing protocols for wireless mesh networks. In Proceedings of the 10th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP), Prague, Czech Republic, 20–22 July 2016; pp. 1–5.
2. Kashyap, V.K.; Astya, R.; Nand, P.; Pandey, G. Comparative study of AODV and DSR routing protocols in wireless sensor network using NS-2 simulator. In Proceedings of the International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 5–6 May 2017; pp. 687–690.
3. Krishna, B.H. Study of Ad hoc Networks with Reference to MANET, VANET, FANET. *Conf. Proc.* **2017**, *7*, 390–394.

4. Rosati, S.; Kruzelecki, K.; Heitz, G.; Floreano, D.; Rimoldi, B. Dynamic Routing for Flying Ad Hoc Networks. *IEEE Trans. Veh. Technol.* **2016**, *65*, 1690–1700. [[CrossRef](#)]
5. Rani, V.; Dhir, R.; Ambedkar, B.R. A Study of Ad-Hoc Network: A Review. *Int. J. Adv. Res. Comput. Sci. Softw. Eng.* **2013**, *3*, 135–138.
6. Cui, H.; Feng, W.; Wang, Y.; He, Y. Balancing Interference and Delay in Heterogeneous Ad Hoc Networks With MIMO. *IEEE Access* **2017**, *5*, 19225–19232. [[CrossRef](#)]
7. Das, S.K.; Tripathi, S. Adaptive and Intelligent Energy Efficient Routing for Transparent Heterogeneous Ad-Hoc Network by Fusion of Game Theory and Linear Programming. *Appl. Intell.* **2018**, *48*, 1825–1845. [[CrossRef](#)]
8. Ganesh, S.S.; Ramar, K. A Cluster Based Intrusion Detection System for Homogeneous and Heterogeneous Mobile Ad Hoc Network. *J. Comput. Theor. Nanosci.* **2017**, *14*, 4249–4254. [[CrossRef](#)]
9. Zhao, P.; Yu, W.; Yang, X.; Meng, D.; Wang, L. Buffer Data-Driven Adaptation of Mobile Video Streaming Over Heterogeneous Wireless Networks. *IEEE Internet Things J.* **2018**, *5*, 3430–3441. [[CrossRef](#)]
10. Fujiwara, S.; Ohta, T.; Kakuda, Y. An Inter-domain Routing for Heterogeneous Mobile Ad Hoc Networks Using Packet Conversion and Address Sharing. In Proceedings of the 32nd International Conference on Distributed Computing Systems Workshops, Macau, China, 18–21 June 2012; pp. 349–355.
11. Okano, K.; Aoki, Y.; Ohta, T.; Kakuda, Y. An Autonomous Clustering-Based Inter-domain Routing Protocol for Heterogeneous Mobile Ad Hoc Networks. In Proceedings of the 10th International Conference on Mobile Ad-Hoc and Sensor Networks, Maui, HI, USA, 19–21 December 2014; pp. 144–150. [[CrossRef](#)]
12. Wang, J.N.; Narula-Tam, A.; Byan, R. Interconnecting Heterogeneous MANET Networks at the Tactical Edge. In Proceedings of the IEEE Military Communications Conference, Baltimore, MD, USA, 6–8 October 2014; pp. 1152–1159.
13. Rekha, B.; Ashoka, D. SRHM: Sustainable routing for heterogeneous ADHOC environment in IOT-based mobile communication. *IJACT* **2019**, *8*, 3003–3010.
14. Benjbara, C.; Habbani, A.; Mahdi, F.E. Procédé de Communication basé sur la Classification des Chemins Multiples. MA Patent 42342 IPC H04W 4/00, 29 November 2019.
15. Souidi, M.; Habbani, A. Zonage Dynamique et déCentralisé dans les réSeaux pour Réduire le Traffic Broadcast basé sur des Règles de Diffusion Géographiques (GFR). MA Patent 40652 IPC H04W 4/00, 31 January 2019.
16. Mahdi, F.E.; Habbani, A.; Benjbara, C. Procédé de Localisation et Isolation des trous noirs dans un Réseau Mobile Ad Hoc. MA Patent 42357 IPC H04W 4/00, 28 February 2020.
17. Oubbati, O.S.; Chaib, N.; Lakas, A.; Lorenz, P.; Rachedi, A. UAV-Assisted Supporting Services Connectivity in Urban VANETs. *IEEE Trans. Veh. Technol.* **2019**, *68*, 3944–3951. [[CrossRef](#)]
18. Fendji, J.L.E.K.; Samo, S.D. Energy and performance evaluation of reactive, proactive, and hybrid routing protocols in wireless mesh network. *arXiv* **2019**, arXiv:1903.06875.
19. Tabbana, F. Performance Comparison and Analysis of Proactive, Reactive and Hybrid Routing Protocols for Wireless Sensor Networks. *Int. J. Wirel. Mob. Netw. (IJWMN)* **2020**, *12*. Available online: <https://ssrn.com/abstract=3694426> (accessed on 24 December 2021). [[CrossRef](#)]
20. Muhammad, H.A.; Yahiya, T.A.; Al-Salihi, N. Comparative Study Between Reactive and Proactive Protocols of (MANET) in Terms of Power Consumption and Quality of Service. In *Computer Networks*; Springer: Cham, Switzerland, 2019; pp. 99–111.
21. Sallum, E.; Santos, G.; Alves, M.; Santos, M. Performance analysis and comparison of the DSDV, AODV and OLSR routing protocols under VANETs. In Proceedings of the 2018 16th International Conference on Intelligent Transportation Systems Telecommunications (ITST), Lisboa, Portugal, 15–17 October 2018; pp. 1–7. [[CrossRef](#)]
22. Kadadha, M.; Otrouk, H.; Barada, H.; Al-Qutayri, M.; Al-Hammadi, Y. A street-centric QoS-OLSR Protocol for urban Vehicular Ad Hoc Networks. In Proceedings of the 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, Spain, 26–30 June 2017; pp. 1477–1482. [[CrossRef](#)]
23. Sharma, S. P-OLSR: Position-based optimized link state routing for mobile ad hoc networks. In Proceedings of the 2009 IEEE 34th Conference on Local Computer Networks, Zurich, Switzerland, 20–23 October 2009; pp. 237–240. [[CrossRef](#)]
24. Singh, K.; Verma, A.K. Experimental analysis of AODV, DSDV and OLSR routing protocol for flying adhoc networks (FANETs). In Proceedings of the 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, India, 5–7 March 2015; pp. 1–4. [[CrossRef](#)]
25. Guillen-Perez, A.; Montoya, A.-M.; Sanchez-Aarnoutse, J.-C.; Cano, M.-D. A Comparative Performance Evaluation of Routing Protocols for Flying Ad-Hoc Networks in Real Conditions. *Appl. Sci.* **2021**, *11*, 4363. [[CrossRef](#)]
26. Rosati, S.; Kruzelecki, K.; Traynard, L.; Mobiler, B.R. Speed-aware routing for UAV ad-hoc networks. In Proceedings of the 2013 IEEE Globecom Workshops (GC Wkshps), Atlanta, GA, USA, 9–13 December 2013; pp. 1367–1373. [[CrossRef](#)]
27. Benjbara, C.; Habbani, A.; Mahdi, F.E.; Essaid, B. Multi-path routing protocol in the smart digital environment. In Proceedings of the 2017 International Conference on Smart Digital Environment, Rabat, Morocco, 21–23 July 2017; pp. 14–18.
28. Westergaard, M.; Maggi, F.M. Modeling and Verification of a Protocol for Operational Support Using Coloured Petri Nets. In *International Conference on Application and Theory of Petri Nets and Concurrency*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2011; Volume 6709, pp. 169–188.

29. Clausen, T.; Dearlove, C.; Jacquet, P.; Herberg, U. *The Optimized Link State Routing Protocol Version 2*; RFC 7181. In Proceedings of the 2010 IEEE International Conference on Wireless Communications, Networking and Information Security, Beijing, China, 25–27 June 2010; doi:10.17487/RFC7181. [[CrossRef](#)]
30. Yi, J.; Parrein, B. Multipath Extension for the Optimized Link State Routing Protocol Version 2 (OLSRv2); RFC 8218. Available Online: <https://datatracker.ietf.org/doc/rfc8218/> (accessed on 24 December 2021).
31. Barbehenn, M. A note on the complexity of Dijkstra’s algorithm for graphs with weighted vertices. *IEEE Trans. Comput.* **1998**, *47*, 263. [[CrossRef](#)]
32. Zheng, Y.; Hou, K.; Liao, W.; Yang, L. The Shortest Path Algorithm Based on Petri Net. In Proceedings of the The 19th International Conference on Industrial Engineering and Engineering Management, Changsha, China, 27–29 October 2012; Springer: Berlin/Heidelberg, Germany, 2012; pp. 221–229. [[CrossRef](#)]
33. Kadri, H.; Zouari, B. A high-level Petri nets approach for multi-objective optimization in pipeline networks. In Proceedings of the 4th International Conference On Simulation And Modeling Methodologies, Technologies And Applications (SIMULTECH), Vienna, Austria, 28–30 August 2014; pp. 211–218. [[CrossRef](#)]
34. Shah, P.A.; Hasbullah, H.B.; Rafique, S.; Rehman, S.U.; Jung, L.T. Fuzzy logic based link status classification for efficient multipath routing in multi-hop wireless mesh networks. In Proceedings of the International Conference on Computer and Information Sciences (ICCOINS), Kuala Lumpur, Malaysia, 3–5 June 2014; pp. 1–6. [[CrossRef](#)]
35. Laouid, A.; Dahmani, A.; Bounceur, A.; Euler, R.; Lalem, F.; Tari, A. A distributed multi-path routing algorithm to balance energy consumption in wireless sensor networks. *Ad Hoc Netw. J.* **2017**, *64*, 53–64. [[CrossRef](#)]
36. Guillen-Perez, A.; Maria-Dolores, C. Flying Ad Hoc Networks: A New Domain for Network Communications. *Sensors* **2018**, *18*, 3571. [[CrossRef](#)] [[PubMed](#)]
37. Sharma, A.; Vanjani, P.; Paliwal, N.; Basnayaka, C.M.W.; Jayakody, D.N.K.; Wang, H.-C.; Muthuchidambaranathan, P. Communication and networking technologies for UAVs: A survey. *J. Netw. Comput. Appl.* **2020**, *168*, 102739. [[CrossRef](#)]
38. Gupta, L.; Jain, R.; Vaszkun, G. Survey of important issues in UAV communication networks. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 1123–1152. [[CrossRef](#)]
39. Oubbati, O.S.; Lakas, A.; Zhou, F.; Güneş, M.; Lagraa, N.; Yagoubi, M.B. Intelligent UAV-Assisted Routing Protocol for Urban VANETs. *Comput. Commun.* **2017**, *107*, 93–111. [[CrossRef](#)]
40. Muruganathan, S.D.; Lin, X.; Maattanen, H.-L.; Zou, Z.; Hapsari, W.A.; Yasukawa, S. An Overview of 3GPP Release-15 Study on Enhanced LTE Support for Connected Drones. *arXiv* **2018**, arXiv:1805.00826.
41. Oubbati, O.S.; Lakas, A.; Zhou, F.; Güneş, M.; Yagoubi, M.B. A survey on position-based routing protocols for Flying Ad hoc Networks (FANETs). *Veh. Commun.* **2017**, *10*, 29–56. [[CrossRef](#)]
42. Clausen, T.; Jacquet, P. Optimized Link State Routing Protocol (OLSR), RFC 3626, Project Hipercom, INRIA, Oct. 2003. Available online: <https://tools.ietf.org/html/rfc3626> (accessed on 24 December 2021).
43. The Network Simulator NS-3. Available online: <https://www.nsnam.org/> (accessed on 24 December 2021).
44. Dijkstra, E.W. A Note on Two Problems in Connexion with Graphs. *Numer. Math.* **1959**, *1*, 269–271. [[CrossRef](#)]
45. Thakur, M.; Kaur, M. Ad-Hoc Network Routing Protocols for Wireless Body Area Network. In Proceedings of the ICAICR ’19: Proceedings of the Third International Conference on Advanced Informatics for Computing Research, Shimla, India, 15–16 June 2019; pp. 1–7. [[CrossRef](#)]
46. Li, X.; Hu, X.; Zhang, R.; Yang, L. Routing Protocol Design for Underwater Optical Wireless Sensor Networks: A Multiagent Reinforcement Learning Approach. *IEEE Internet Things J.* **2020**, *7*, 9805–9818. [[CrossRef](#)]