Emirates Journal for Engineering Research

Volume 28 | Issue 3 Article 3

10-29-2023

Towards Reliable Multi-Path Routing : An Integrated Cooperation Model for Drones

Ibtihel Baddari
University Mh'amed Bougara of Boumerdes, i.baddari@univ-boumerdes.dz

Abdelhak Mesbah
University Mh'amed Bougara of Boumerdes, abdelhak.mesbah@univ-boumerdes.dz

MAOHAMED AMINE RIAHLA
university of m'hamed bougara of boumerdes, ma.riahla@univ-boumerdes.dz

Recommended Citation

Baddari, Ibtihel; Mesbah, Abdelhak; and RIAHLA, MAOHAMED AMINE (2023) "Towards Reliable Multi-Path Routing : An Integrated Cooperation Model for Drones," *Emirates Journal for Engineering Research*: Vol. 28: Iss. 3, Article 3.
Available at: https://scholarworks.uaeu.ac.ae/ejer/vol28/iss3/3

1. INTRODUCTION:

In the constantly evolving wireless communication technologies era, Ad-hoc networks offer exciting opportunities to explore innovative and promising scenarios. These networks are characterized by their ability to form autonomously without centralized infrastructure [1], connecting individual nodes such as mobile devices, sensors, and drones. Their autonomous and self-organizing nature makes them suitable for various applications, from emergency search and rescue to environmental monitoring in remote areas.

However, Ad-hoc networks face challenges such as node mobility, bandwidth and energy limitations, and modest processing and memory capacities. To address these challenges, multipath routing has become a solution [2], with AOMDV (Ad-hoc On-Demand Multipath Distance Vector) [3] being one of the most widely used protocols. Our work focuses primarily on this routing protocol. The current challenge is finding the most secure path, not just the optimum route. Securing Ad-hoc routing is particularly difficult due to the need for an administrative entity at the heart of the network. Many vulnerabilities allow malicious nodes to corrupt the configuration of routing tables, modify packets in transit, or not participate in the effort of routing to save energy. Moreover, a node with limited resources will likely cooperate with expecting a reward or gain in return [4].

Our work focuses on this protocol and aims to enhance security using a cooperation model based on node reputation [4]. We chose a fleet of drones [5] as a case study to highlight the advantages and challenges of Ad-hoc networks. This article introduces a secure routing extension inspired by AOMDV, called FD-COO, which employs link-disjoint paths [3] between the source and destination. A key aspect is using drone reputation as a security layer to evaluate node behavior. The following section provides an overview of relevant work and presents our new routing approach. We then discuss the results and conduct tests of our new routing protocol using the NS2 simulator [6] before concluding with research perspectives.

1. RELATED WORK:

Firstly, we present some advances in Ad-hoc networks and their application on UAVs by highlighting the innovative solutions proposed to meet the specific challenges of communication, energy management, and decision-making:

- *Ad-hoc On-Demand Multipath Distance Vector [3]*

Authors in [3] proposed AOMDV, an Ad-hoc On-Demand Multipath Distance Vector routing protocol, as an extension of AODV [7]. AOMDV focuses on utilizing multiple disjoint paths for enhanced reliability. It allows only alternate routes with fewer hops, making the network more resilient to failures. AOMDV's route discovery and maintenance phases are similar to AODV. It initiates route discovery with broadcast requests (RREQ) and replies with route reply messages (RREP). AOMDV's route maintenance resembles AODV, forwarding RREQ only when all proposed paths are broken [3]. It uses periodic HELLO messages [8] to assess link effectiveness. The protocol prioritizes the best hop-count path for data transmission, utilizing alternate paths when the primary route fails.

AOMDV routing protocol is a sensible approach in Ad-hoc networks, particularly in scenarios where reliability, fault tolerance, and routing performance are priorities. AOMDV offers greater fault tolerance by using alternative paths in the event of a primary path failure. This is particularly useful in environments where node mobility or interference can lead to intermittent failures. AOMDV can help avoid congestion on a single path by distributing traffic over multiple paths and efficiently using available resources. Our work focuses primarily on this routing protocol.

- *AOMDV Lifetime Prolonging Routing Algorithm For Ad-hoc Networks [9]*

The authors have proposed a new algorithm dedicated to Ad-hoc networks inspired by the AOMDV multi-path routing protocol, which aims to prolong the network lifetime by managing nodes' energy, link cost, and controlling network congestion. The primary concept is to choose paths from the available multipath options using an innovative technique for replenishing the power of neighboring nodes. This approach also involves balancing nodal energy consumption to avert the depletion of energy supplies in critical nodes. Simulation results show that the AOMDV-LP routing protocol performance is better than the AOMDV protocol regarding packet loss. This enhancement is elucidated by the introduced energy recovery strategy, which avoids selecting low-energy paths to mitigate the potential for packet loss. Additionally, the strategy reduces congestion by minimizing the exchange of control packets required for energy node recovery. This aspect holds particular significance for applications sensitive to packet loss [10].

- *A Multipath Lifetime-Prolonging Routing Algorithm [11]:*

Introduces an advanced iteration of a routing algorithm exclusively tailored for mobile ad-hoc networks. Drawing inspiration from the pheromone trail-laying and following behavior observed in real ants and the ACO framework [12], this innovation carries substantial significance. Its fundamental objective is managing network congestion and significantly extending the network's lifetime by judiciously managing node energy. It's worth highlighting that the protocol introduces a pioneering approach to avoid low energy states, a strategy meticulously designed to optimize network lifetime through innovative route discovery techniques and data transmission methods. Nonetheless, it's important to note that this protocol does not merely settle for selecting routes; it aspires to harness the best possible routes, propelling it to the forefront of cutting-edge advancements in routing algorithms for mobile Ad-hoc networks.

- *Energy efficient multipath ant colony based routing algorithm for mobile Ad-hoc networks [13]*

Introduces a novel wireless routing protocol designed for mobile Ad-hoc networks and wireless sensor networks [14], utilizing a bio-inspired approach. This approach draws from behaviors observed in natural systems like ant colonies bird flocking, offering solutions to challenges posed by wireless sensor networks, such as limited bandwidth, battery life, and memory. The protocol introduces an energy-efficient multipath routing algorithm inspired by ant foraging behavior, incorporating multiple meta-heuristic impact factors to establish robust paths from source to destination. The paper demonstrates the significance of individual impact factors in routing performance analysis. It also validates the multipath routing capability by showcasing energy and statistical analyses. This proposed algorithm's performance is evaluated using metrics such as throughput, delay, packet loss, and network lifetime and compared with the AODV routing protocol [7], indicating a notable enhancement in network lifetime.

- *A new approach to realize drone swarm using Ad-hoc network [15]*

This paper presents an innovative approach to synchronize and orchestrate a set of drones based on Ad-hoc communications. Therefore, it is possible to operate a swarm of drones using a single remote control, eliminating the need for additional equipment beyond the drones, without relying on any existing infrastructure or specific sensors such as the GPS module, which can prove imprecise and inefficient in particular scenarios. In this case, an Ad-hoc network facilitates drone communication by dynamically adjusting data rates based on received signal strengths. For this, the authors use the analogy of two individuals bringing closer or moving away from each other to discuss, depending on the noise in the environment.

- *Multipath Doppler Routing (MUDOR) [16]*

Authors proposed MUDOR, a reactive routing protocol inspired by Dynamic Source Routing (DSR) [17] and designed for highly mobile Ad-hoc networks like FANETs. MUDOR focuses on identifying the most stable path with the most extended lifetime. To choose the best path, this protocol measures the frequency shift due to the Doppler effect of the received packets, which indicates the relative velocity between the source and destination nodes. Then, the users can estimate the lifetime of the link. Before starting the data delivery, MUDOR uses the flooding of RREQ to discover routes toward the target destination. The first time an aerial vehicle (node) receives the RREQ packet, it rebroadcasts this packet with its identifier and the Doppler value from the previous node. Subsequently, the destination will reply with an RREP packet by selecting the route with the most extended lifetime based on the calculated Doppler values.

- *Ad-hoc Routing Protocol for Aeronautical MANETs (ARPAM)* [18]

Introduced ARPAM, a geographical position-based routing protocol with similarities to the principle of AODV, rendering it partially reactive. ARPAM employs UAV geographic positions to determine the shortest path between source and destination UAVs. Like AODV, when a source UAV intends to transmit data packets and lacks a path to the destination UAV, a Route Request (RREQ) packet is disseminated across the network. The RREQ carries the source's velocity vector and position. These details help intermediate UAVs estimate the rapidly changing position of the source UAV due to high speeds.

Additionally, this geographical data aids in calculating packet transit distance, serving as a metric for routing decisions. Upon receiving the RREQ, the destination responds with a Route REPly (RREP) packet unicast to the source node. ARPAM incorporates an on-demand path maintenance mechanism, crucial for applications requiring low response times like voice over IP (VoIP) or video on demand (VoD). Consequently, ARPAM is a reactive routing protocol that can adopt proactive behavior on demand.

- *UAV-Assisted VANET Routing Protocol (UVAR) [19]*

In this solution, the routing paths are progressively built by choosing path segments gradually at each intersection by a scoring mechanism derived from four parameters that guide the selection process: the connectivity, the traffic density, the distance between a pair of nodes, and the real distribution of vehicles. These parameters are based on the exchanged Hello Packets [8] between vehicles and the deployed UAVs over the four road segments. This approach proves advantageous in surmounting existing obstacles and furnishing additional alternative solutions, particularly in situations where the terrestrial network exhibits sparse connectivity. Moreover, the consideration of actual vehicle distribution contributes to optimizing the selection of the most regulated road.

- *Secure UAV Ad-hoc routing Protocol (SUAP) [20]*

Authors proposed an extension secured of the AODV routing protocol for FANETs [21]. SUAP uses digital signatures to secure static fields and hash chains for dynamic fields. These packets need to be signed and verified by recipient nodes using the sender's public key. Nevertheless, the number of hop counts has to be incremented at each hop, so it cannot be indicated during transmission. We can deduce that the SUAP protocol is susceptible to wormhole attacks.

Consequently, message fields are signed to protect from malicious modifications, and geographical leashes are employed to calculate the correlation between the distance traversed and the hop-count value. To achieve this, each node must maintain a local connectivity with its adjacent neighbors. During packet transmission, each node includes its current geographical location.

- *A distributed monitoring scheme for a fleet of UAV flying drones [22]*

This article proposes a solution for UAVs in a fleet of unmanned aerial vehicles (UAVs) to work together to monitor the network and detect incidents that could compromise safety or continuity of service during their mission. The proposed scheme enables each UAV to monitor its immediate neighbors and share this information so that action can be taken in the event of an incident or service degradation. The aim is to ensure that the network is resilient and can be adapted to guarantee continuity of service without the need for a central control authority. The method used enables incidents to be detected without the need for complex security or routing solutions or constant communication with a central authority. It relies on four parameters to maintain continuity of service: link quality, transfer rate, data control rate, and mobility coordinates. This approach enables several incidents to be detected using the same scheme.

Secondly, we present the two best-known models for strengthening cooperation. These mainly address encouragement and collaboration between nodes in an Ad-hoc network. In other words, protocols are based on the reputation of nodes :

- *Confidant [23]:*

This protocol is an extension of the DSR [1] routing protocol. This version detects malicious nodes using an observation mechanism that provides a report on different types of attacks: malicious nodes are isolated and can no longer be asked to route packets. Each node has an observation mechanism to build up a database of the reputation of the other nodes in the network. CONFIDANT has an alarm mechanism for propagating information relating to reputation. However, this information is managed by a control module, which determines the degree of the information's reliability based on the reputation of the information’s source.

- *Token Based [24]:*

In this method, each node must present a token to obtain access to the ad-hoc network while neighbor nodes monitor its behavior to detect any malicious actions. Once the token's validity period expires, the node must request a renewal from its neighbors. The validity period depends on how long the node has actively participated in the network. A node that behaves appropriately will have to renew its token less and less frequently. A slightly modified version of the AODV routing protocol also uses information about a node's behavior. Routing information received from neighbors is compared with each other, and any inconsistencies detected by this comparison are reported. This redundancy makes it possible to identify nodes providing incorrect information and reduce their access token's validity period.

2. THE PROPOSED MODEL:

- *General Overview:*

This section presents the proposed model that utilizes Ad-hoc architecture to improve routing efficiency and security in a drone fleet. The advantages of choosing Ad-hoc architecture over other types are illustrated in the following *table :*

Table. 1 : Advantages of Ad-hoc Architecture for Drone Fleets

Advantage	Description
Obstacle Adaptability	When a central infrastructure or satellite system is used, the area of operation will be limited by the communication coverage area of the relay. In addition, if there are any obstacles, communication between the drones may be blocked. Ad-hoc architecture makes it possible to set up a fleet of drones to work around the obstacle.
Infrastructure-free	Adapted to areas that are isolated or in a crisis situation, where there is no infrastructure.
Multiple communication paths	Ad-hoc architecture enables the creation of multiple communication paths between drones, improving network redundancy and reliability. If one communication path is blocked or disrupted, data can be routed via alternative paths.
Distributed Network Security	The security of a mobile Ad-hoc network is distributed between the nodes, unlike a centralized cellular network. As a result, there is no single vulnerable point in the network. Responsibility for maintaining the integrity of the network is delegated to each node in the network, which, through a secure routing mechanism, can control the authentication of messages exchanged.

The effort provided to design our secure routing protocol is mainly reactive. In which a node/drone tries to discover/choose a route to a particular destination only when it has a packet to send to the latter. This on-demand routing protocol is proposed to perform better with fast topology changes.

We must choose an initial routing protocol to create our secure communication architecture. In this work, we decided to use an existing protocol in the Ad-hoc environment for the aforementioned reasons and then add security mechanisms. This choice is justified on the one hand by the maturity of routing protocols in this type of wireless network, in particular the AMODV protocol, which is recognized in the literature through many performance evaluation studies [3] (its paths are all disjoint and can guarantee loop-free routing, and also allows the shortest alternative paths to be chosen). The main idea of our strategy is to discover the best paths between source and destination in terms of energy and number of path uses, then secure them using the reputation metric in the data transmission phase. Our FD-COO routing protocol is based on two main parameters: energy recovery and calculating the reputation value for each drone to establish a more secure and efficient route. The main properties of FD-COO:

- We add the energy recovery metric in the standard AOMDV routing table.
- The paths discovered are based not only on the number of hops but also on the energy of the drones.
- The best-selected path will be secured by reputation value to detect malicious drones.
- Isolate malicious drones once they have been detected.

Figure. 1 represent the proposed model based on three core modules detailed later in this section:

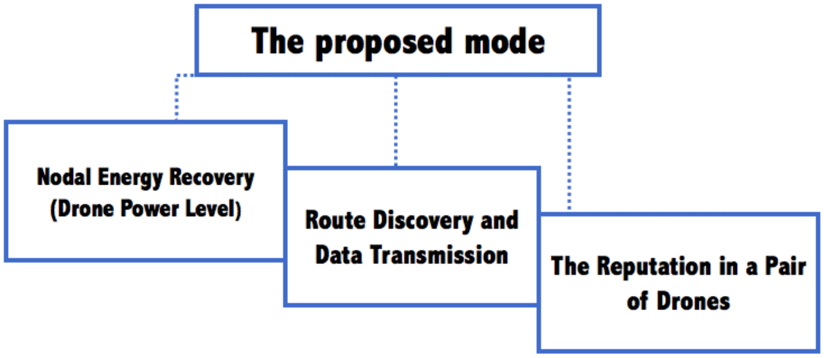

The proposed mode
Nodal Energy Recovery (Drone Power Level)
Route Discovery and Data Transmission
The Reputation in a Pair of Drones

Figure. 1 Process flow of our proposed methodology

- *Nodal energy recovery (drone power level):*

With control messages, each node maintains a neighbor table that records the state of each neighbor from which a HELLO packet has been received. We introduce an additional field in the control message that reflects the current energy recovery of the neighbor [9]. In this way, each node has a complete list of its direct neighbors and their corresponding energy levels at a given time t. As shown in Figure 2 and Figure. 3.

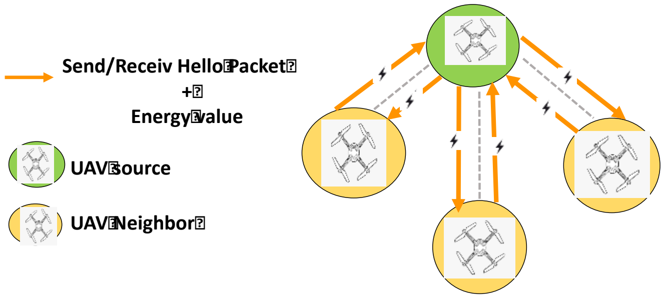


Figure. 2 Exchange of battery level information between drones/nodes.

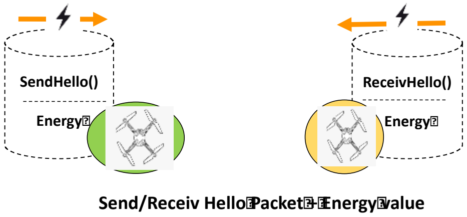


Figure. 3 Packet Sent/Received after modification.

- *Route discovery and data transmission*

- For path discovery, the FD-COO protocol is based on the following principle, depending on the quantity of RREPs received:
- If only one RREP is received, then only one path from the source to the destination will be used to send data packets.
- If many RREPs are received, the source chooses the best path based on the:
  - The adjacent neighbor's energy recovered by HELLO control message.
  - We have thought of a new, more original strategy for route discovery. The idea is to save the number of times a link NUse is used in the routing table in order to avoid saturation of the bandwidth (in Figure. 4) as well as the energy Egy of the adjacent neighbor recovered by HELLO control messages.
  - The other routes are still waiting for the RERR packet indicating the failure of the main route. In which case the optimal route of the alternative paths is used to transmit data.

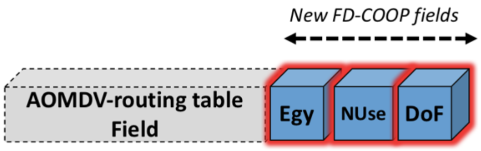


Figure. 4 New FD-COO fields

A new metric is introduced: Degree of force DoF between a node Ni, which has requested a route to the final destination Dst via its adjacent neighbor. This value is based on NUse and Egy, the energy of the neighbor drone. As shown in Eq. (1). When a path is created using the RREQ and RREP messages, the following values are assigned by default: EgyNi is the energy of the next hop that exists in the local node's neighborhood table, NUse is incremented each time a path is used to route a packet, a fill-in or a recalculation of the strength degree. During the discovery phase, the latter allows keeping different paths while controlling network congestion and reaching destinations rapidly. The rest of the path discovery procedure is similar to AOMDV [7].

$$\boldsymbol{DoF(src, Ni, dst)} = \frac{\boldsymbol{EgyNi}}{\boldsymbol{1+NUse}} \qquad \text{Eq. (1)}$$

To give importance to the hop-count, which is an essential parameter in the AOMDV[3] equation Eq. (1) can be modified as follows:

$$\boldsymbol{Pot.Link(src, Ni, dst)} = \boldsymbol{\alpha DoF + (1\text{-}\alpha)\frac{1}{1+Hcount}} \qquad \text{Eq. (2)}$$

Where Hcount represents hop-count between source src and destination Dst via Ni, the adjacent neighbor. In order to make route selection more precise, we use the potential link parameter Pot. Link combines the basic AOMDV parameter hop-count with the degree of force. As shown in Eq. (2). Depending on the routing policy in Ad-hoc networks, the parameter α=0.5 is used to provide high importance and prioritize the DoF or NumHop parameters.

Drones cooperation *:*

In an Ad-hoc network, each participant may be required to forward packets to the other stations on the network. Consequently, the network lifetime will be negatively impacted, and the network will disconnect if one of these participants decides to behave like a selfish or malicious node or not to relay packets.

A route that is nothing more than a series of drones must be evaluated for security. We considered defining a trial period for sending a specific number of packets (a threshold Pj) in order to gauge how well the drones along the path cooperated.

Equation Eq. (3) is used to evaluate the contribution of packet transmission and packet reception, taking into account the coefficient α=0.5 to adjust the importance of cooperation in the final measurement of CNj.

Several conditions might result in packets being dropped, such as queue overload, failure of the path to the next hop, or the existence of one or more malicious nodes. Our method has added a new technique to confirm the inaccessibility problem at the next hop. If the number of retransmissions reaches the maximum **MAC_RETRY_COUNT_EXCEEDED**, the packet will be dropped by the mac layer due to queue overload. We add an error counter (PER) to distinguish between queue overload and node inaccessibility.

$$\boldsymbol{CNj = 1 + \frac{PTj+PNTj}{\alpha+RECVj}} \qquad \text{Eq. (3)}$$

$$\boldsymbol{PNF = \frac{PPj}{RECVj}} \qquad \text{Eq. (4)}$$

Where the abbreviations represents :

CNj : the node cooperation

PTj : The number of packets sent by Nj.

PNTj : the number of packets not transmitted by the Nj node (transmission error).

RECVj : The received packets by Nj.

PPj : The number of packets transmitted by node Ni to node Nj and not retransmitted by node Nj.

Unforwarded Packets PNF: The ratio between the number of packets transmitted by node Ni to node Nj but not retransmitted by node Nj itself (PPj) and the total number of packets received by node Nj (RECVj) (see Eq. (4)). PNF can be used to evaluate how effectively node Nj retransmits the packets it has received from Ni, and therefore the quality of node Nj's transmission in this context.

The reputation in a pair of drones

The reputation value Rij is calculated by drone Ni for adjacent neighbor Nj ÎNGS. We used a set of counters for each neighbor station Nj to detect malicious stations. Their behavior can be judged when the number of packets Nj receives reaches the threshold Pj.

If the reputation value Rij is positive, then the node is cooperative.

Else (Rij is negative or zero), the node acts up.

The reputation of a UAV is calculated by its neighbors for a predefined period (see Figure. 4) All counters are updated according to:

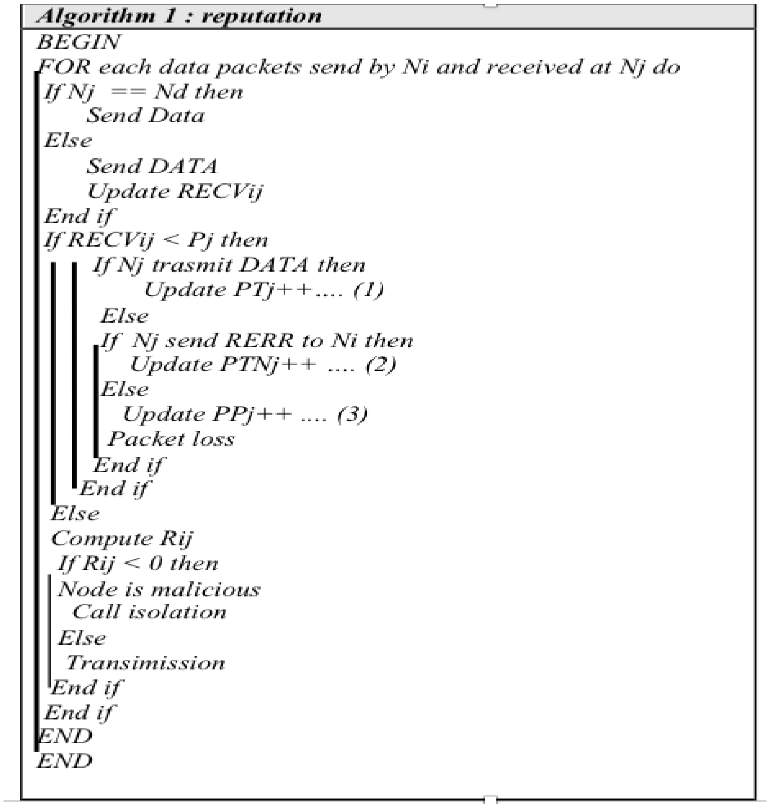
Note1: For each packet received by Nj and relayed, PTj is incremented

Note2: For each packet received by Nj and not forwarded due to queue overload or link failure, the PNTj is incremented

Note3: For each packet received by Nj and not relayed, the PPj is incremented

Note 4: Each node updates the reputation of its neighbors according to Eq (1,2,3,4). The node that joins the network receives a reputation Rinit=1.

$$\boldsymbol{Rij = CNj - PNF} \qquad \text{Eq. (5)}$$



```
Algorithm 1 : reputation
BEGIN
FOR each data packets send by Ni and received at Nj do
  If Nj  == Nd then
      Send Data
  Else
      Send DATA
      Update RECVij
  End if
  If RECVij < Pj then
      If Nj trasmit DATA then
          Update PTj++.... (1)
      Else
      If  Nj send RERR to Ni then
          Update PTNj++ .... (2)
      Else
          Update PPj++ .... (3)
          Packet loss
      End if
      End if
  Else
  Compute Rij
   If Rij < 0 then
     Node is malicious
       Call isolation
     Else
       Transimission
   End if
  End if
END
END
```

Figure. 5 Reputation Algorithm

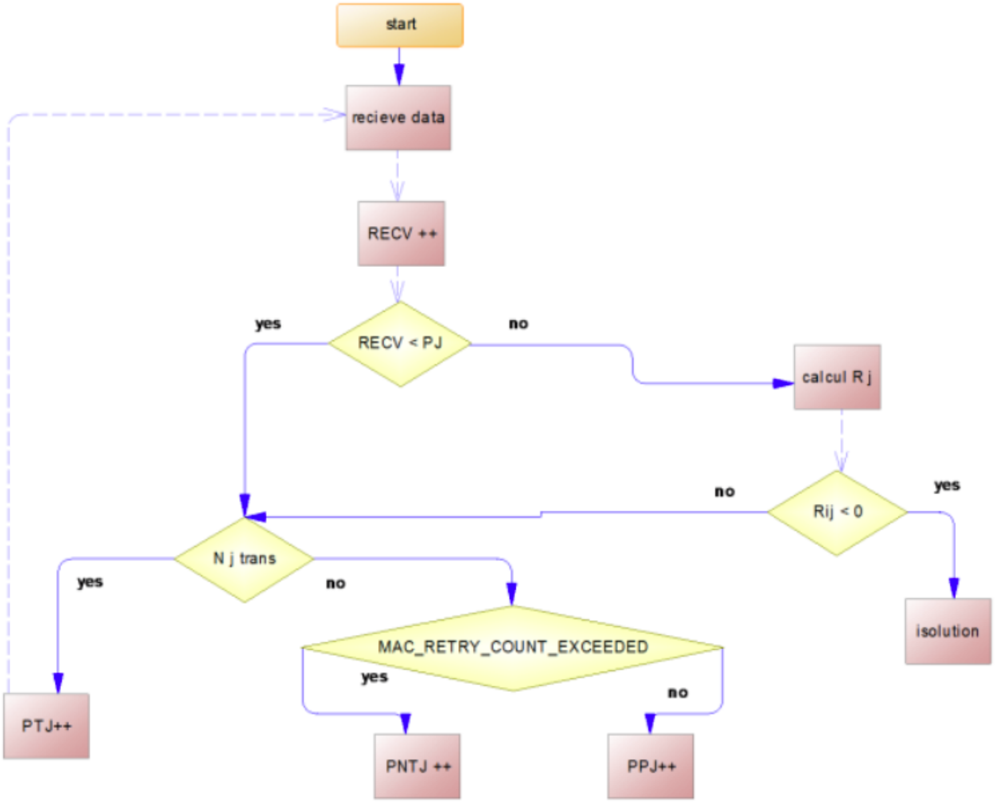


Figure. 6 Flowchart of the Improved Reputation System

Maintenance de route

The node with a reputation <= 0 is considered malicious, and an isolation process will be started. The monitoring node stops the transmission of all packets passing through this neighbor that is behaving badly. This malicious node will be added to a black_list for a certain time T_expiration. VS counter will be incremented until it reaches a threshold value VS = 3, this means that the malicious node will have 3 chances to change its behavior. The detector node sends a request to its neighbors to avoid communicating with this malicious node. As shown in Figure. 7,8 and 9.

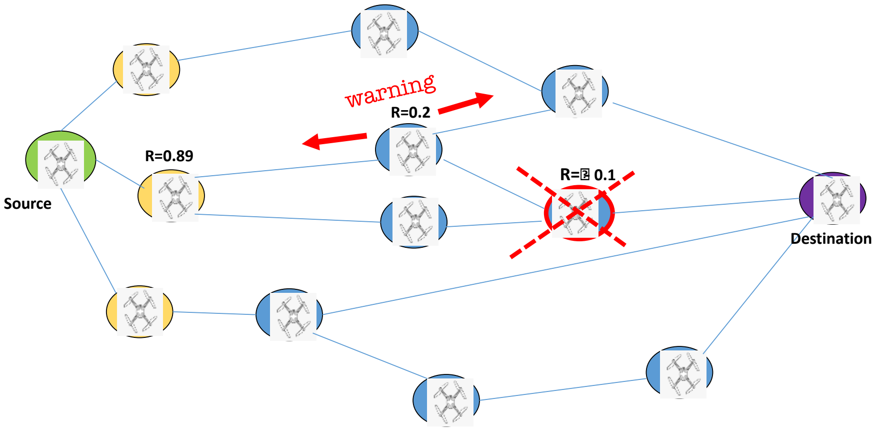


Figure. 7 The malicious nodes detection

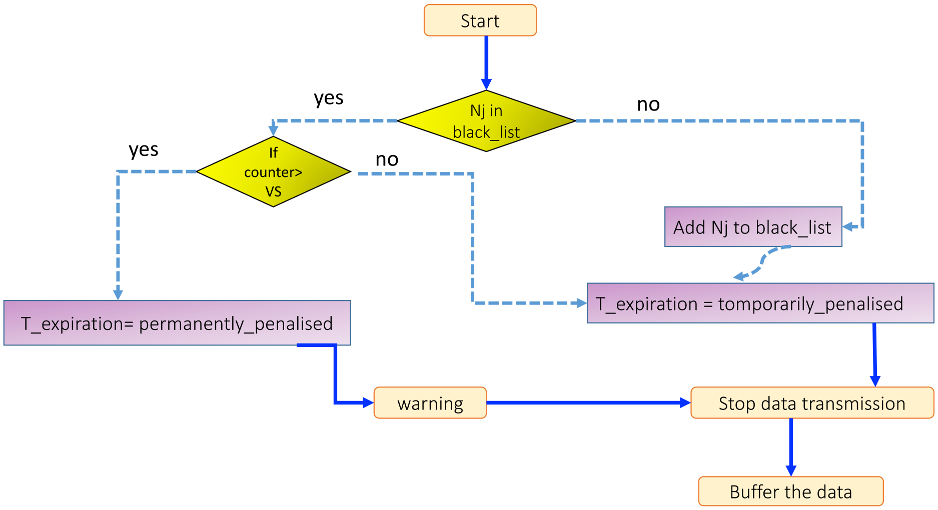


Figure. 8 Flowchart of the isolation system

3. SIMULATION RESULTS AND DISCUSSION:

Simulation is often used to test a routing protocol. In this section, we present simulation results that prove the effectiveness and performance of our new strategy, which aims to improve communication in a fleet of UAVs using a more secure Ad-hoc architecture. We take advantage of the NS-2 platform [6] for simulation experiments to test our new protocol. The agreement between our algorithm, the classical AOMDV algorithm and AOMDV-LP protocol are compared and analyzed. We consider the simulation parameters as shown in Table. 2. The performance metrics used to evaluate the performance of each algorithm are the following:

- The Packet Loss: This metric measures the number of packets not delivered to their destinations.
- End-to-End Delay: This metric represents the average Delay between the packet sending time and its reception time from source to destination.
- Throughput: this metric is calculated in bits per second and represents the number of actual data packets delivered to all destinations during the simulation.
- Total Energy Consumed.

Table. 2 Simulation Parameters

Parameter	Value
Simulation Time	100s
Max Node Speed	30m/s
Packet size	512 bytes
Number of nodes	55-110 nodes
Number of data packets	600-1200 packets
MAC type	IEEE 802.11
Simulation area	700m*700m
Protocol	UDP
Mobility Model	Random way point
Initial energy of node	5j

The performance metrics are obtained by averaging over 20 simulations run from one source to one randomly selected destination. We assume that a node consumes 0.5j while receiving and 1.02J while transmitting.

1. *The Packet Loss:*

Figure. 10 shows the variation of % packet loss as a function of the drop event time. It is clearly shown that our protocol, FD-COO, has less packet loss than the other protocols.

In AOMDV, 89% of data packets are lost from the start before they reach their destination. This is because the AOMDV basic protocol uses the diffusion process, which is made worse by the rapid multiplication of collisions. As a result, this architecture is overloaded and needs help to handle many transmissions. In the AOMDV-LP protocol, there is less packet loss because it chooses the shortest route with sufficient energy to route the packets. The link cost parameter helps to control the network congestion through load balancing, so the number of buffer overflows in the queue of intermediate nodes is reduced. In the case of our protocol, The figure shows a lower packet loss, indicating better reliability. Our protocol is based primarily on the DOF metric, the degree of force indicated in Eq. (1). Nodes with a high degree of force are more likely to transmit packets reliably, thus minimizing the risk of packet loss. Our protocol aims to lower the packet loss rate, hence increasing transmission reliability, by actively encouraging UAVs cooperation. By evaluating and assigning reputation levels to UAVs in the network, our protocol enables the selection of more reliable transmission paths, which helps reduce the packet loss rate. In addition, this can be explained by the fact that our protocol uses a more effective reactive data routing technique than AOMDV.

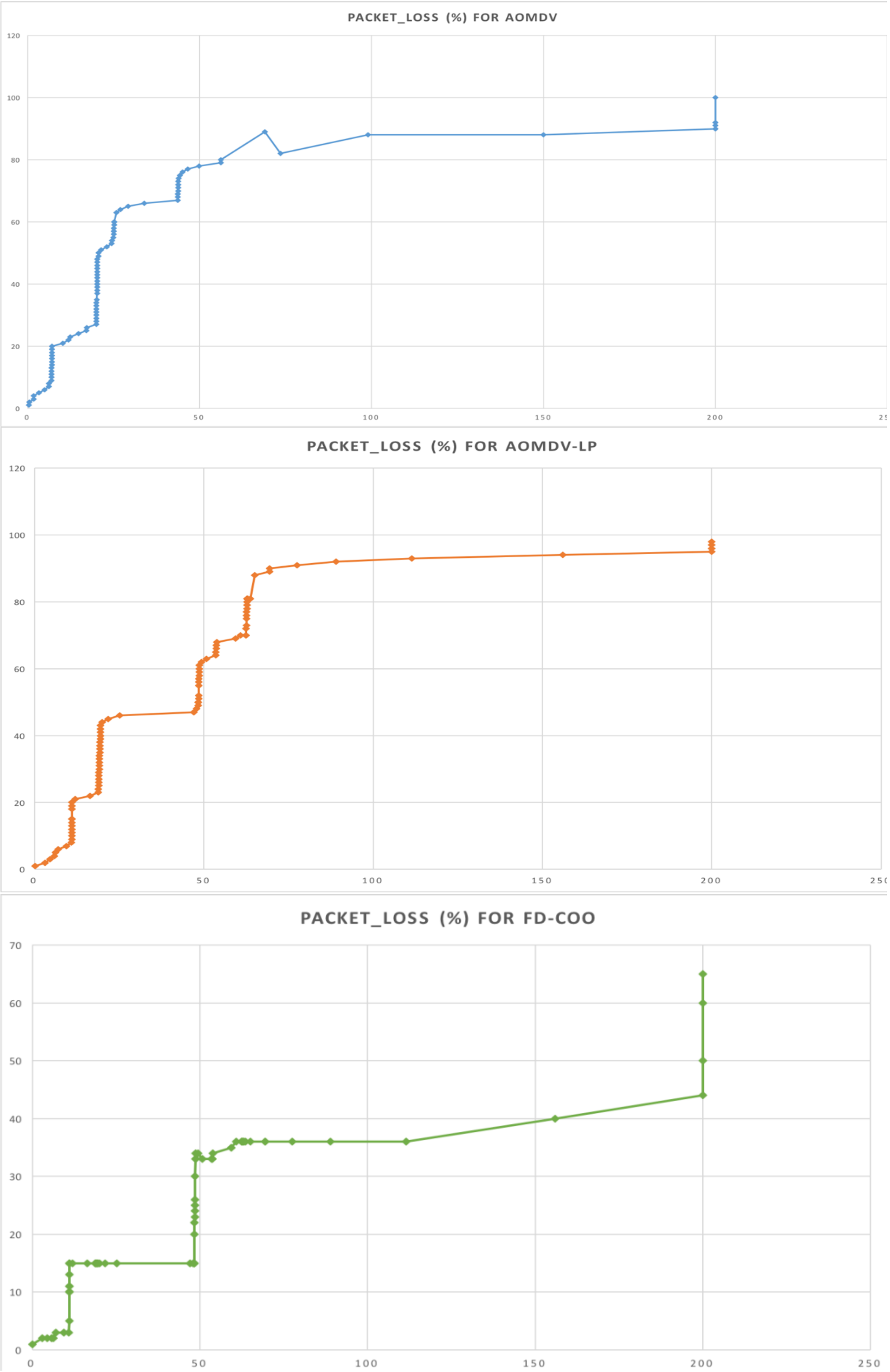


Figure. 10 Packet Loss Ratio/Drop event time

2. End to End Delay:

Figure. 11 represents the time to receive the data packet since leaving the source node in each protocol (the variation of average transmission delay). It increases as the node moves faster. Furthermore, the speed of nodes significantly impacts the network's stability. Rapid changes in topology due to high node mobility can introduce route instability, causing frequent route recalculations. This leads to increased communication overhead and raises concerns about packet loss and delivery delays. In situations where nodes move swiftly, maintaining stable and reliable routes becomes challenging. The network must continuously adapt to the changing conditions, making it more vulnerable to disruptions. These disruptions can result in route failures, necessitating the reestablishment of paths and, consequently, prolonging the average end-to-end communication delays.

We note that AOMDV-LP and our protocol FD-COO generate less important delays than those generated by the basic AOMDV protocol. Regarding our protocol, this may be due to the choice of nodes with sufficient energy and which avoid malicious nodes using the proposed technique (see Eq. (3,4,5)). The remarkable reduction in end-to-end delay observed in our protocol compared to the other Protocols underscores the efficiency of our approach in optimizing communications among drones. Our protocol incorporates advanced mechanisms based on factors such as the degree of force, cooperation, and node reputation, which help maintain reliable and stable routes even in high-mobility environments. By minimizing network disruptions and avoiding frequent route recomputation, our solution significantly reduces the time required for data transmission from one point to another, resulting in a markedly improved end-to-end delay.

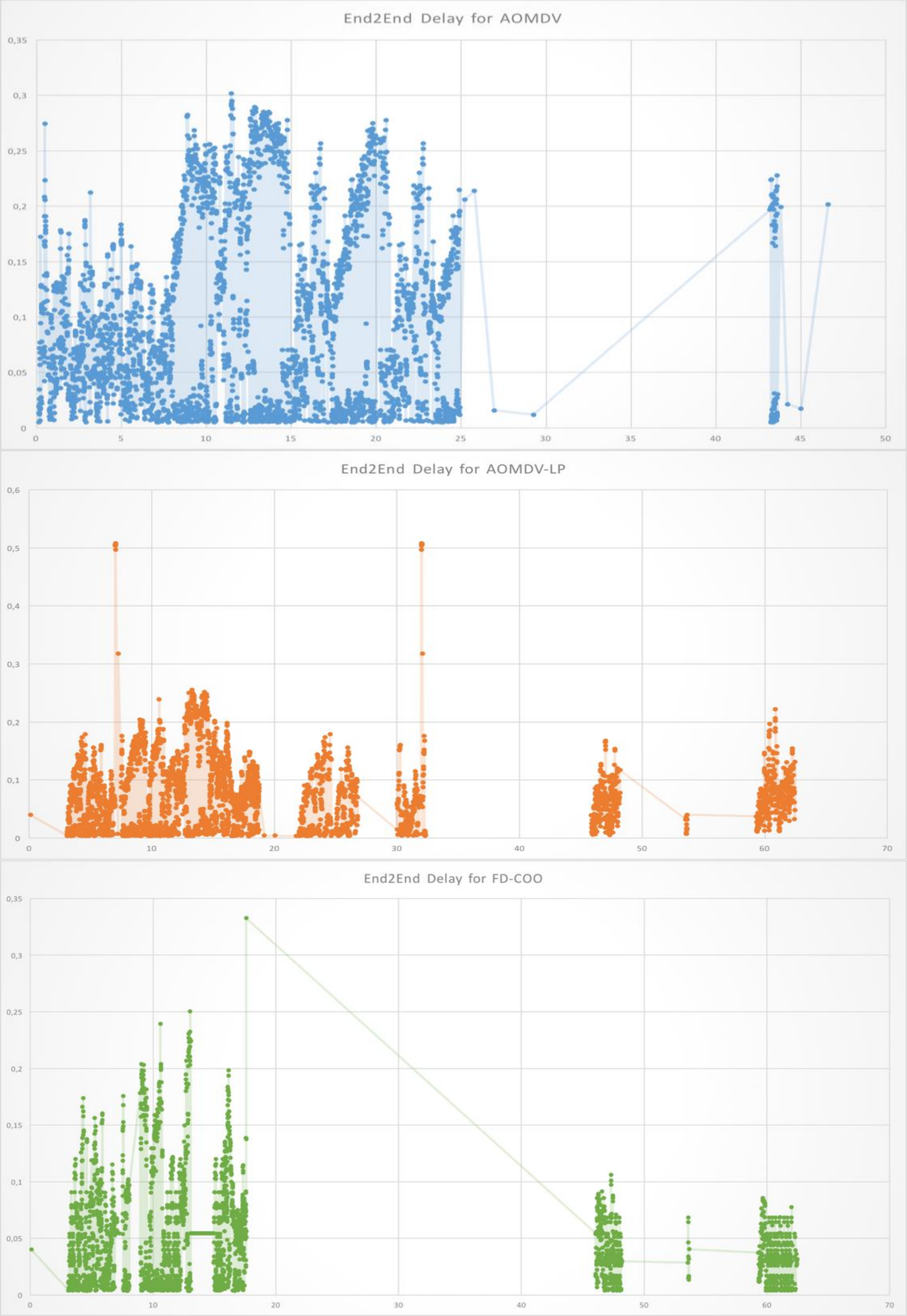


Figure. 11 End to End Delay/Packet Send Time

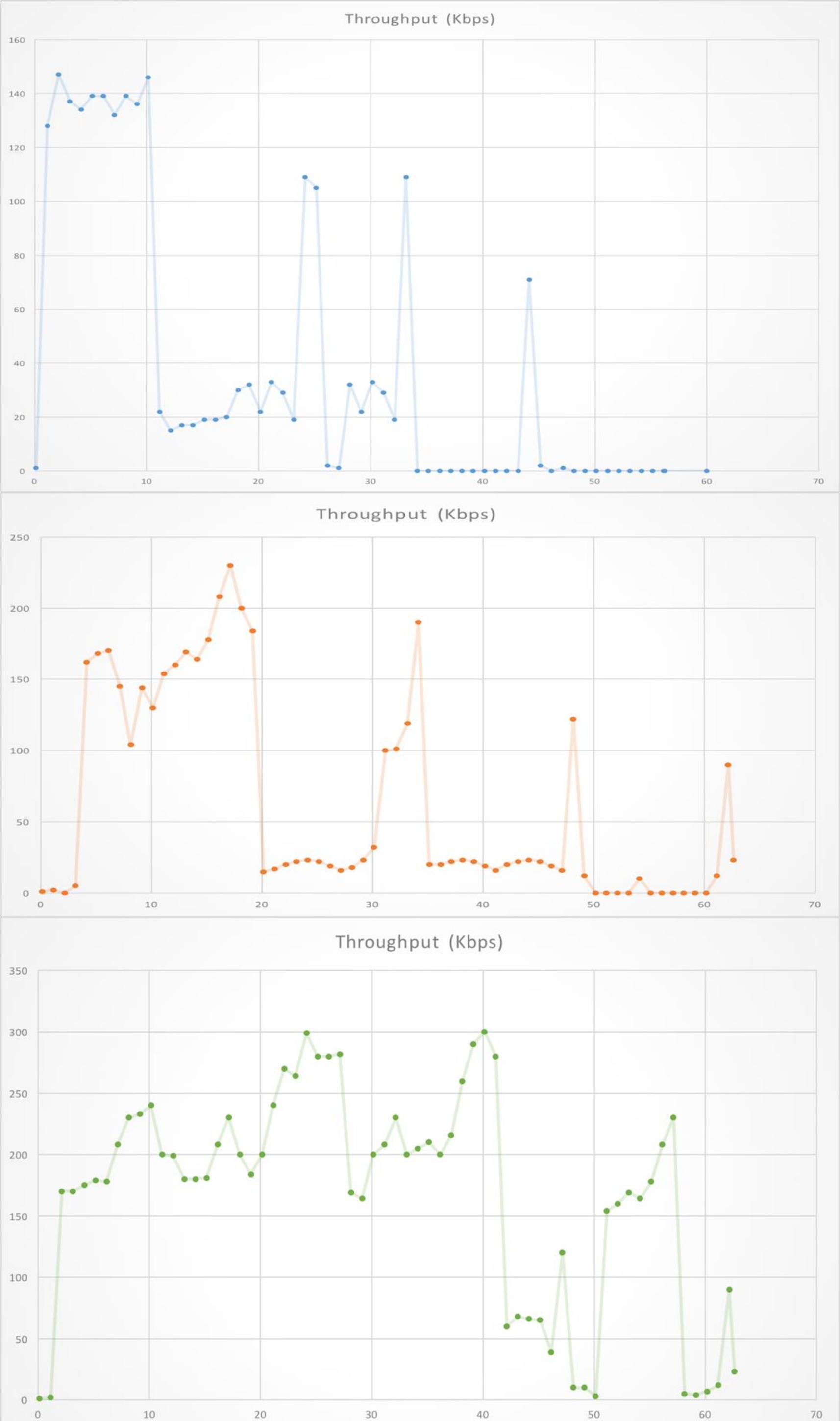


Figure. 12 Throughput/Simulation Time

3. Throughput:

Comparing the performance of our protocol FD-COO with AOMDV and AOMDV-LP in Figure. 12, we observed promising results while considering factors such as the degree of strength, cooperation, and route maintenance. Initially, both protocols showed low throughputs, which is typical at the start of the simulation when the network topology is forming. However, as the simulation progressed, our protocol outperformed AOMDV and AOMDV-LP regarding throughput. Specifically, our protocol achieved significantly higher throughputs between 10 and 40 seconds of simulation, reaching up to 290 Kbps. At the same time, AOMDV remained below 150 Kbps, and the AOMDV-LP did not exceed 230 Kbps. This improvement suggests that our protocol was more effective in establishing and maintaining stable routes for data transmission, thanks to advanced techniques for calculating the degree of force and cooperation among nodes.

4. CONCLUSION:

In our research, we have ventured into the realm of Ad-hoc networks, specifically focusing on their application in the context of drone fleets (UAVs). Drones heavily rely on Ad-hoc networks for communication in dynamic and challenging environments. This context not only enabled us to spotlight the intricacies of the problem but also allowed us to showcase the effectiveness of our proposed solution, the FD-COO routing extension.

Through extensive simulations conducted on the NS-2 platform, we have achieved compelling results that underscore the superiority of our approach over existing solutions. Our protocol outperformed the AOMDV and AOMDV-LP protocols regarding key performance metrics, including packet loss rate, end-to-end delay, and throughput. These findings reinforce the viability and promise of our FD-COO routing extension in enhancing secure and reliable communication within Ad-hoc networks. As we gaze toward the future, several exciting research avenues beckon. One promising direction is the exploration of more sophisticated reputation models to enhance the evaluation of node behavior further.

Additionally, integrating machine learning techniques, enabling adaptive routing decisions based on real-time network conditions, presents an enticing area for future investigation. Furthermore, with the proliferation of drones across various domains, scalability and adaptability become paramount. Future work will concentrate on ensuring the seamless and secure operation of Ad-hoc networks in more extensive and diverse environments.

References:

[1] Rajeswari, Alagan Ramasamy. "A mobile ad hoc network routing protocols: A comparative study." *Recent trends in communication networks* (2020): 1-24.

[2] Patel, Daxesh N., et al. "A survey of reactive routing protocols in MANET." *International Conference on Information Communication and Embedded Systems (ICICES2014)*. IEEE, 2014.

[3] Marina, Mahesh K., and Samir R. Das. "Ad hoc on-demand multipath distance vector routing." *Wireless communications and mobile computing* 6.7 (2006): 969-988.

[4] TAMI, Abdelaziz. *Sécurité du routage dans les protocoles de routage multichemins*. Diss. 2021.

[5] Tsao, Kai-Yun, Thomas Girdler, and Vassilios G. Vassilakis. "A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks." *Ad Hoc Networks* 133 (2022): 102894.

[6] Ninagawa, Chuzo. "Appendix B: Example NS Simulation Script Code for TCP." *IoT Communication Performance Analysis*. Singapore: Springer Singapore, 2022. 201-208

[7] Maurya, Prashant Kumar, et al. "An overview of AODV routing protocol." *International Journal of Modern Engineering Research (IJMER)* 2.3 (2012): 728-732.

[8] Chakeres, Ian D., and Elizabeth M. Belding-Royer. "The utility of hello messages for determining link connectivity." *The 5th international symposium on wireless personal multimedia communications*. Vol. 2. IEEE, 2002.

[9] Baddari, Ibtihel, Mohamed Amine Riahla, and Mohamed Mezghiche. "A New AOMDV Lifetime Prolonging Routing Algorithm for Ad-Hoc Networks." *International Journal of Interdisciplinary Telecommunications and Networking (IJITN)* 11.4 (2019): 48-62

[10] Tavli, Bulent, and Wendi Heinzelman, eds. *Mobile Ad hoc networks*. Dordrecht: Springer Netherlands, 2006.

[11] Riahla, Mohamed Amine, and Karim Tamine. "A multipath Lifetime-Prolonging routing algorithm for wireless ad hoc networks." *International Journal of Advanced Computer Science and Applications* 7.1 (2016).

[12] Sharvani, G. S., A. G. Ananth, and T. M. Rangaswamy. "Analysis of different pheromone decay techniques for ACO based routing in ad hoc wireless networks." *International Journal of Computer Applications* 56.2 (2012).

[13] Sharma, Arush S., and Dongsoo S. Kim. "Energy efficient multipath ant colony based routing algorithm for mobile ad hoc networks." *Ad Hoc Networks* 113 (2021): 102396.

[14] Yick, Jennifer, Biswanath Mukherjee, and Dipak Ghosal. "Wireless sensor network survey." *Computer networks* 52.12 (2008): 2292-2330.

[15] Shrit, Omar, et al. "A new approach to realize drone swarm using ad-hoc network." *2017 16th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net)*. IEEE, 2017.

[16] Sakhaee, Ehssan, Abbas Jamalipour, and Nei Kato. "Aeronautical ad hoc networks." *IEEE Wireless Communications and Networking Conference, 2006. WCNC 2006.*. Vol. 1. IEEE, 2006.

[17] Johnson, David B., David A. Maltz, and Josh Broch. "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks." *Ad hoc networking* 5.1 (2001): 139-172.

[18] Guillen-Perez, Antonio, et al. "A comparative performance evaluation of routing protocols for flying Ad-Hoc networks in real conditions." *Applied Sciences* 11.10 (2021): 4363.

[19] Oubbati, Omar Sami, et al. "UVAR: An intersection UAV-assisted VANET routing protocol." *2016 ieee wireless communications and networking conference*. IEEE, 2016.

[20] Maxa, Jean-Aimé, Mohamed Slim Ben Mahmoud, and Nicolas Larrieu. "Performance evaluation of a new secure routing protocol for UAV Ad hoc Network." *2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC)*. IEEE, 2019.

[21] Singh, Shashank Kumar. "A comprehensive survey on fanet: challenges and advancements." *International Journal of Computer Science and Information Technologies* 6.3 (2015): 2010-2013.

[22] Nouasri, Amine, and Mohamed Amine Riahla. "A distributed monitoring scheme for a fleet of UAV flying drones." *International Journal of Mobile Network Design and Innovation* 10.3 (2022): 113-120.

[23] Buchegger, Sonja, and Jean-Yves Le Boudec. "Performance analysis of the CONFIDANT protocol." *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*. 2002.

[24] Sharma, Bharti, Ravinder Singh Bhatia, and Awadhesh Kumar Singh. "A token based protocol for mutual exclusion in mobile ad hoc networks." *Journal of information processing systems* 10.1 (2014): 36-54.