drones

MDPI

Article

Performance Enhancement of Optimized Link State Routing Protocol by Parameter Configuration for UANET

Esmot Ara Tuli , Mohtasin Golam, Dong-Seong Kim and Jae-Min Lee *

Networked Systems Laboratory, Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi 3917, Korea; esmot@kumoh.ac.kr (E.A.T.); golam248@kumoh.ac.kr (M.G.); dskim@kumoh.ac.kr (D.-S.K.)

* Correspondence: ljmpaul@kumoh.ac.kr

Abstract: The growing need for wireless communication has resulted in the widespread usage of unmanned aerial vehicles (UAVs) in a variety of applications. Designing a routing protocol for UAVs is paramount as well as challenging due to its dynamic attributes. The difficulty stems from features other than mobile ad hoc networks (MANET), such as aerial mobility in 3D space and frequently changing topology. This paper analyzes the performance of four topology-based routing protocols, dynamic source routing (DSR), ad hoc on-demand distance vector (AODV), geographic routing protocol (GRP), and optimized link state routing (OLSR), by using practical simulation software OPNET 14.5. Performance evaluation carries out various metrics such as throughput, delay, and data drop rate. Moreover, the performance of the OLSR routing protocol is enhanced and named "E-OLSR" by tuning parameters and reducing holding time. The optimized E-OLSR settings provide better performance than the conventional request for comments (RFC 3626) in the experiment, making it suitable for use in UAV ad hoc network (UANET) environments. Simulation results indicate the proposed E-OLSR outperforms the existing OLSR and achieves supremacy over other protocols mentioned in this paper.

Keywords: enhanced optimized link state routing (E-OLSR); OPNET; routing protocols; unmanned aerial vehicles (UAVs); UAV Ad hoc network (UANET)

check for updates

Citation: Tuli, E.A.; Golam, M.; Kim, D.-S.; Lee, J.-M. Performance Enhancement of Optimized Link State Routing Protocol by Parameter Configuration for UANET. *Drones* **2022**, *6*, 22. https://doi.org/10.3390/drones6010022

Academic Editors: Abderrahmane Lakas, Mohammed Atiquzzaman, Omar Sami Oubbati, Vishal Sharma, Sahar Hoteit and Taieb Znati

Received: 30 November 2021
Accepted: 7 January 2022
Published: 13 January 2022

1. Introduction

The fast growth of unmanned aerial vehicles (UAVs) has transformed the premise of wireless communication technology. UAV networks can collect data from sensors, connect with ground users, and provide Wi-Fi coverage in areas where humans are unable to access. The application of UAVs has not been limited to only military purposes as when they were first developed. UAV networks are proving to be a beneficial and appropriate technology for a wide range of civilian and military purposes. UAVs enable us to perform risky and complex operations such as firefighting, monitoring regions affected by natural disasters, launching and tracking cruise missiles, and remote surveillance [1]. Recently, UAVs are being made more economical and smaller in size, and the availability of autopilot software raises their popularity in the public and private sectors [2]. UAVs are used for a variety of purposes, including agriculture [3], remote sensing [4], forest fire detection [5], patrolling [6], and providing communication facilities in remote and disaster-prone areas [7,8]. However, in order to carry out tough tasks, UAVs must be able to communicate effectively. Despite their numerous applications and benefits, drones are frequently referred to as "terrorism by joystick" to emphasize their negative effects [9]. Smuggling and other criminal operations, invasions of privacy, terrorist attacks, cyber assaults, surveillance, unauthentic monitoring, and so forth are all examples of UAV abuse. The growing number of crimes has highlighted the significance of identifying and disabling unlawfully deployed drones. In [10], the authors discuss techniques for identifying drones in the presence of flying objects such as birds. In [11], the authors propose a deep learning method for detecting malicious drones using image and audio data. Similarly, in [12], deep learning-based drone detection and type recognition based on radio frequency emissions are proposed. The goal of this study is to find and identify illegal drones that could endanger civilians.

UAV networks are classified into two forms based on the number of deployed UAVs: single-UAV networks and multi-UAV networks. In the case of a single-UAV network, the UAV is connected to a base station or satellite. On the other hand, in a multi-UAV network, numerous UAVs are interconnected and interact with one another to accomplish the mission. A multi-UAV network provides benefits over a single UAV network with self-recovery capabilities. As a result, in a multi-UAV network, effective UAV collaboration is required to complete tasks. This necessitates the establishment of an inter-UAV wireless communication network [13]. The current flying ad hoc networks (FANET) suffer from a lack of collaborative interaction between UAVs, emphasizing the requirement for a better routing solution to improve data transmission between UAVs. Furthermore, in the FANET network, data transfer is problematic due to the irregular distribution of UAVs, their rapid mobility in three-dimensional space, and frequent topology changes. In order to address the issue of existing FANET, a UAV ad hoc network (UANET) was established by combining mobile ad hoc networks (MANET) and vehicular ad hoc networks (VANET) to develop a novel network topology incorporating homogeneous or heterogeneous flying agents known as UAVs. The term “UANET” refers to a network comprising several UAV nodes. UANET addresses the leakage of centralized and cellular communication in the UAV communication network. UANET is predominantly a multi-UAV network with several characteristics distinct from MANET and VANET. UAVs can function as clients, routers, and servers in UANET and collaborate to complete tasks [14,15]. It is a very dynamic network, with new nodes joining and old nodes leaving very frequently. As a consequence, the network’s topology could alter at any moment, which is a key characteristic missing from wireless communication networks [14]. IEEE 802.11 was recommended for UAV communications by researchers since it can handle higher bandwidth, has fast data rates, and has long-range coverage. Due to fluctuating distances among nodes and high mobility in the UANET, connection reliability fluctuations occur. Packet delays, efficient channel use, high mobility, and varying link quality are among the difficulties that the UANET must overcome during real-time communication.

Routing protocols are one of the essential components of a UANET. In a UANET, a single node may serve as a transmitting, receiving, and forwarding node simultaneously. The transmission path is typically multi-hop, and routing greatly influences network performance. A significant amount of effort must be invested in performance analysis to select the optimal routing protocol. The simulation-based performance study for MANET is demonstrated in paper [16]. The paper explains how, by lowering the RREQ RETRIES and MAX RREQ TIMEOUT parameters, the AODV protocol performs better than the OLSR protocol. When a sender wants to transfer data to a receiver, the network responds with a route request (RREQ). The sender awaits the network’s route response, and the sender resends an RREQ a defined number of times if it is not received within a specific period of time, which is known as RREQ RETRIES. The MAX RREQ TIMEOUT is the maximum amount of time a sender node can wait before sending RREQ RETRIES. A significant amount of effort must be invested in performance analysis to select optimal RREQ RETRIES and MAX RREQ TIMEOUT values. In another paper [17], the authors compare the performance of the AODV and OLSR routing protocols by using the NS2 simulator in FANET for search and rescue (SAR). The Gauss–Markov mobility model is used to describe the motions of multi-rotor mini-UAVs used for monitoring in SAR. Similarly, in [18], the performance comparison of a UAV communication network for AODV, OLSR, DSR, and GRP routing protocols is presented.

Depending on functionality, routing protocols are classified into three categories [19,20]:

- Swarm-based routing;
- Position-based routing;
- Topology-based routing.

The characteristics of natural insects are used to inspire swarm-based routing. These traits are thought to be self-oriented, self-adaptive, and unified to choose the optimal route. However, due to the high mobility of UAVs, excessive latency is the fundamental flaw of swarm-based routing for the UANET network. Likewise, packet forwarding is performed depending on the geographic location of UAVs in position-based routing protocols [21]. However, the major downside of position-based routing is that it transmits obsolete route information due to the UAVs' constantly changing locations. On the other hand, internet protocol (IP) addresses are used by topology-based routing protocols to leverage existing network information to transmit data packets in the most efficient manner possible [22]. In order to construct and manage the optimal route, these protocols require topological information from communicating UAVs. A topology-based routing protocol for UAVs is evaluated in the paper [23]. This article provides a brief overview of the most significant topology-based routing protocols suitable for FANETs. Furthermore, the authors focus on topology-based routing protocols to enhance network performance in terms of throughput, latency, and network load. However, the previously mentioned article solely used the existing protocol for performance analysis with no improvements. In this study, a review of several routing protocols for UAV communication is provided, and an enhanced OLSR, named E-OLSR, is proposed for the UANET network.

The main contributions of this paper are as follows:

- The OLSR protocol's configuration settings have been optimized to make it appropriate for UANETs;
- Analyzes routing protocol performance in the OPNET simulator by creating realistic UANET scenarios where optimized OLSR configurations outperform the default one;
- Finally, a comparison of the existing well-known topology-based routing protocols (AODV, OLSR, DSR, and GRP) with optimized E-OLSR based on the performance metrics such as throughput, delay, and data drop rate is conducted.

The rest of the paper is arranged in the following manner: In Section 2, the basic concept of a UAV-based routing protocols and the description of the E-OLSR are presented. Research methodology is illustrated in Section 3. Section 4 describes simulation modeling of the E-OLSR routing algorithm. The performance evaluation of the E-OLSR network in terms of delay, throughput, and data drop rate, as well as comparisons to existing routing protocols, is described in Section 3.1. Finally, Section 6 brings the article to a conclusion by pointing the direction forward for future opportunities.

2. Routing Protocols for UAV Communication

Currently, UAV communication uses the MANET routing protocol. A large number of routing protocols have been proposed for ad hoc networks. Due to the different characteristics of UANET, the MANET routing protocol is not directly applicable. Therefore, the routing protocol for UANET is still a research issue. The UANET routing protocol can be divided in two ways: single-hop and multihop [24]. In the case of single-hop, there is no intermediate node. The sender UAV carries the data packet to the destination [25]. In multihop routing, data packet transfer from source to destination is performed hop by hop. Therefore, based on hop selection strategies, multihop routing is further classified into two categories: topology-based and position-based. GPS is used in a position-based routing protocol for finding the real-time position of the next hop. Topology-based routing protocols are divided into three categories: proactive routing protocols, reactive routing protocols, and hybrid routing protocols. OLSR is a proactive routing protocol, also called table-driven or active routing protocol; thus, the change in the network is immediately available due to its proactive behavior. On the other hand, AODV and DSR are reactive or on-demand routing protocols. In the on-demand protocol, routing information is exchanged only after the demand. This paper analyzes the performance comparison between routing protocols such as DSR, AODV, GRP, and OLSR, along with E-OLSR. The following is a concise outline of these protocols.

2.1. Dynamic Source Routing (DSR)

DSR is one of the first reactive routing protocols, allowing a network to self-configure and operate without the need for infrastructure [26]. In DSR, the source node only makes a connection towards the destination when required. There are two steps involved in this routing protocol, such as route discovery and maintenance. In route discovery steps, the source node discovers the path through the destination; in the case of link failure, maintenance steps are needed. The use of definite source routing across a set of nodes enables the sender to choose and control the routes employed for its own packets, hence improving network performance by allowing numerous paths for every destination (load balancing) [27]. Multiple routes between source and destination can be recovered and maintained using DSR. As a consequence, each sender may choose the optimal forwarding route based on network stability or load balancing among numerous accessible routes. Loop-free routing and support for unidirectional networks are two more features of this routing protocol. Its dynamic nature, thus, enables swift recovery whenever the topology of the network changes. Furthermore, based on the authors of the paper [28], DSR is most suitable for FANET. However, in the case of military-based UAV communication networks, the topology can be highly dynamic, and DSR is not suitable in this case.

2.2. Ad Hoc On-Demand Distance Vector(AODV)

The AODV routing protocol is an improved version of the DSR. AODV is a routing protocol that is commonly used in mobile or wireless ad hoc networks (MANETs or WANETs) [29]. An ad hoc network is a temporary distributed network comprising two or more nodes that allow packets to be sent without the need for traditional infrastructure such as routers and access points. A peer-to-peer (P2P) network is used by the nodes in the ad hoc network. In the AODV routing protocol, when a node needs to communicate, it sends a routing request to discover the communication link. Nodes find routes using defined messages by AODV, which are route requests (RREQ), route replies (RREP), and route errors (RERR). The originating node sends RREQ messages to all of its neighbors, while nodes with a route to the destination node send RREP messages back to the originating node. If the originating node's neighbor node lacks a route to a destination, it broadcasts RREQ signals while maintaining a reverse route to the originating node. Furthermore, when a node loses communication with its next-hop node source, it sends RERR messages to all nodes that received RREP messages. A route maintenance phase has been initiated to address link failure difficulties. However, due to the dynamic nature of the UANET system, network congestion is a concern with AODV.

2.3. Geographic Routing Protocol (GRP)

The GRP is an efficient and attractive approach, mostly because no end-to-end route is built before data transmission. GRP also enables each node to maintain local one-hop connectivity, which improves network scalability [30]. GRP forwards data packets in the following manner: If a source node desires to send packets to commence communication, the router sends a request-to-send (RTS) packet to its neighbors, and only neighbors within a restricted assigned sextant (forwarding area) near the destination are compatible to respond with a clear-to-send (CTS) packet, forming a set of potential forwarding nodes. The source node then chooses a single node as a subsequent relay by using a comprehensive reactive technique to transport data packets based on particular selection criteria. Furthermore, the fundamental description of the GRP approach's relay node selection takes into account unexpected scenarios. Compared to traditional ad hoc routing techniques, GRP has several advantages. Changes can be made node by node and packet by packet by taking into account extra Quality-of-Service (QoS) metrics related to the next-hop neighbors, such as latency or available bandwidth. However, one of the key drawbacks of GRP is the complexity and overheads associated with a distributed location database service.

2.4. Optimized Link State Routing (OLSR)

The OLSR protocol is an improved version of the traditional link-state algorithm. It is one of the recognized routing protocols used in MANET, VANET, and also UANET. As per table-driven routing, OLSR regularly updates and maintains the routing table of the network nodes [31]. The most important part of the OLSR protocol is the multipoint relay (MPR). Instead of sending routing messages all over the network, the OLSR protocol only keeps updating information about the MRP node [32]. MPRs are nodes that are chosen to relay broadcast messages during the flooding process. When compared to the traditional flooding method, this strategy significantly minimizes message overhead (where every node retransmits each message received). A mobile host can minimize battery consumption in this manner. Only nodes designated as MPRs generate link-state information in OLSR. Only links between an MPR node and its MPR selectors can be reported by an MPR node. As a result, in contrast to the standard link-state technique, partial link state information is spread throughout the network. This information is then utilized to calculate the path. The OLSR provides the best paths (in terms of the number of hops). Since MPRs perform effectively in this setting, the protocol is especially well suited for broad and dense networks. The fundamental functionality of the OLSR protocol is accomplished through the use of three different sorts of messages: "Hello" messages, topology control (TC) messages, and multiple interface declaration (MID) messages.

Enhanced Optimized Link State Routing (E-OLSR)

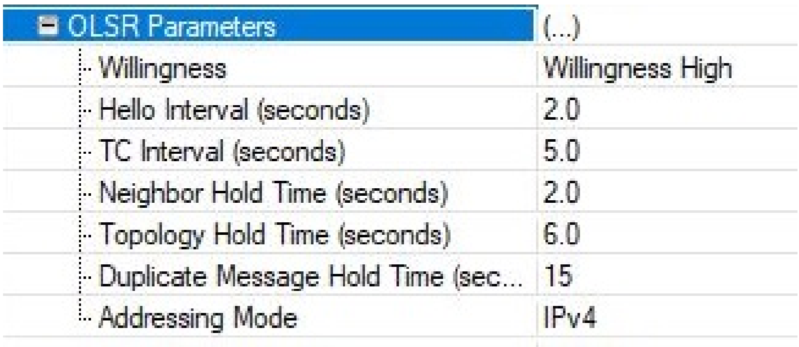
Most of the literature focuses on improving OLSR by improving the MRP selection criteria [33] or willingness concept [34]. Barki et al. [35] provides a brief survey of OLSR improvement based on MRP selection. Improving performance by tuning parameters is also an efficient method to enhance the protocol performance. The new protocol needs extensive examination and analysis before practical deployment. In this context, parameter tuning is faster and more reliable for deployment [36]. Using a tuning strategy, this research improves the performance of the OLSR. An extensive simulation has been performed based on the heuristic method to find the optimal value for the UAV network. Table 1 represents the values for standard OLSR routing protocol parameters [37], whereas Figure 1 demonstrates E-OLSR values. The E-OLSR considers willingness to be high (6) rather than the default value of (3). Willingness indicates the node's desire to forward traffic on behalf of other nodes. Batteries, power, and capacity are related to it. In UAVs, willingness is crucial, as many nodes do not want to send traffic due to preserving energy, which is called a "selfish node" [38]. A high willingness indicates that the node will actively perform data transmission and perform an MRP. It improves the possibility of better system performance. In the OLSR packet format, there are two types of holding time. Htime corresponds to the HELLO message, while Vtime refers to the data packet. Holding time holds five types of time in the message header: neighbor hold time, topology hold time, duplicate message hold time, message id hold time, and HNA message holding time. The link expiration time is specified by the neighboring hold time. If a HELLO message is not received on a link within this time frame, the link is declared lost. By reducing neighbor hold time (6 s for standard OLSR, reduced to 2 s in E-OLSR), the lost node is detected faster instead of waiting a long time. It improves UANET system throughput. The expiration time for topology table entries is defined by the topology hold time. TC messages refresh topology table entries based on their originator address and sequence number.The topology hold time in E-OLSR is reduced from 15 s to 6 s. The topology of the UANET changes frequently. If the topology changes, UAVs receive updated information more quickly in E-OLSR because of the short topology hold time. The duplicate message hold time specifies the expiration time of a duplicate set table entry. In order to avoid handling duplicate messages received within this time frame, a duplicate set table is used. The duplicate message hold time in E OLSR is reduced from 30 s to 15 s. An analytical comparison between all routing protocols is illustrated in Table 2:

Table 1. OLSR parameters and RFC 3626 [37] specified values.

Parameter	Standard Value	Range
Willingness	WILL_DEFAULT(3)	$\mathcal{R} \in [0, 7]$
HELLO_INTERVAL	2 s	$\mathcal{R} \in [1.0, 30.0]$
TC_INTERVAL	5 s	$\mathcal{R} \in [1.0, 30.0]$
NEIGHB_HOLD_TIME	3 × REFRESH_INTERVAL	$\mathcal{R} \in [3.0, 100.0]$
TOP_HOLD_TIME	3 × TC_INTERVAL	$\mathcal{R} \in [3.0, 100.0]$
DUP_HOLD_TIME	30 s	$\mathcal{R} \in [3.0, 100.0]$

Table 2. Comparative analysis between routing protocols along with proposed E-OLSR.

Parameters	DSR	AODV	GRP	OLSR	E-OLSR
Protocol type	On-demand	On-demand	Proactive	Proactive	Proactive
Multiple route	Yes	No	Yes	No	No
Routing overhead	Low	High	Medium	Medium	Medium
Route maintains	Route cache	Route table	Route table	Route table	Route table
Route structure	Flat structure	Flat structure	Flat structure	Flat structure	Flat structure
Route metric	Shortest path	Shortest path	Shortest path	Shortest distance	Shortest distance
Congestion	Low	Medium	Medium	Medium	Medium
Hop counts	Very high	Normal	High	Less	Less then OLSR



⊟ OLSR Parameters	(...)
Willingness	Willingness High
Hello Interval (seconds)	2.0
TC Interval (seconds)	5.0
Neighbor Hold Time (seconds)	2.0
Topology Hold Time (seconds)	6.0
Duplicate Message Hold Time (sec...	15
Addressing Mode	IPv4

Figure 1. E-OLSR parameters used in UANET system.

3. Research Methodology

The objective of this study is to evaluate the performance of four routing protocols (AODV, DSR, GRP, and OLSR) as well as enhance the performance of the OLSR protocol by tuning parameters for UANET. The MANET routing protocol is applied to UANET, although UANET is different from MANET. Developing a new protocol requires extensive research and practical experiments. This study's aim is to enhance the performance of the existing OLSR protocol for UANET. Standard OLSR architecture ignores wireless link quality, and route selection is dependent on the hop count measure, which ignores link quality and traffic load throughout the forward path.

By reducing hop count, the distance traveled by each hop is increased, which reduces signal strength and increases the packet loss ratio. Although the optimum route is one with the fewest hops, there may be several routes with the same minimum length but vastly different quality in a network. Most minimal hop-count measures make arbitrary decisions that are unlikely to choose the optimum path. However, as illustrated in [39], reducing the hop count will not always result in increased throughput flow. Furthermore, because the shortest path is commonly selected as the routing path in shortest path routing, nodes on the shortest path will be overloaded more than others. The resources of a node, including bandwidth, computing power, battery life, and memory storage, can be depleted by high demand. Eventually, packet loss and buffer overflow can arise if one of the overloaded nodes becomes congested, resulting in increased delay, lower throughput, and transport connection failure.

Given these considerations, this paper proposes an enhancement of OLSR by optimizing parameters that can impact the link-quality and traffic-load awareness in the routing protocol. E-OLSR is the term given to the upgraded OLSR, which has outperformed previous protocols, and simulations were carried out on the UANET network using the OPNET simulator 14.5. The simulated architecture comprises an ad hoc network of UAVs equipped with IEEE 802.11 g cards and configured as illustrated in Table 3. In order to achieve a transmission area of 1000 m and match IEEE 802.11 g-designated long-range connectivity, the transmission power is set to 0.005 W, and receiver sensitivity is set to −95 dBm. IEEE 802.11 g implementation was provided by the OPNET simulation software. The following three performance metrics are used:

Table 3. Simulation design parameters in OPNET modeler.

Parameter	Value
Simulation area	1000 m × 10,000 m
Number of UAVs	30 and 50
Directional Gain	10 dBi
Node type	Mobile
Mobility model	Random waypoint
Altitude	200 m and 50 m
UAV max speed	40 m /s and 30 m /s
Routing protocols	E-OLSR, OLSR, DSR, GRP and AODV
Physical characteristics	Extended rate PHY (802.11 g)
Data rate	1 Mbps to 24 Mbps
Transmit power	0.005 W
Simulation duration	10 min
Simulation seed	128
IP addressing	Auto-assign IPv4 addressing
Packet interval	Exponential (1) s
Reception Power Threshold	−95 dBm
Packet size	1024 byte
Large packet processing	Drop (if bigger then 2304 bytes)
Buffer size	256,000 bits
AP beacon interval	0.02 s

3.1. Performance Metrics

This paper considers throughput, delay, and data drop rate to evaluate the routing protocol's performance. Basic descriptions of these performance parameters are provided given below.

3.1.1. Throughput

The rate of successful data transmission at the destination over a given time interval divided by the duration of the time interval is known as throughput [16]. Throughput has been measured by either packets per second (pps) or bits per second (bps). In this paper, bps is considered to measure the throughput. It indicates the volume of traffic an application generates when traversing the network. Mathematically, throughput can be expressed as follows:

$$T = \frac{N_b}{T_{tst}} \tag{1}$$

where T indicates the throughput, N_b is the total number of bits sent, and T_{tst} is the total data sending time.

3.1.2. Delay

The average End-to-End Delay (EED) is a measurement of the time it takes for packets to travel from the source to the destination node's application layer. Due to the delays at various stages, the sending time of each data packet is subtracted from the receiving time at the destination node, and the result is divided by the total number of received packets. For this reason, network quality-of-service (QoS) is affected by the delay, and it is an important criterion in designing and measuring the performance of a communication network. As network delay is related to time, it is expressed in millisecond units. The average end-to-end delay is the sum of the processing, queuing, and transmission time of a packet in a network. It can be expressed as follows:

$$D_{\textit{end-to-end}} = \sum_{i=1}^{n} \frac{T_r(P_i) - T_s(P_i)}{P_i} \tag{2}$$

where $D_{\textit{end-to-end}}$ is the end-to-end delay; n denotes the total number of received packets, P_i indicates the current received packet, $T_r(P_i)$ is the receiving time for P_i, and $T_s(P_i)$ is the sending time of the packet P_i.

3.1.3. Data Drop Rate

Data drop rate means total data dropped by the MAC layer, which comes from a higher layer as a consequence of consistently failed re-transmissions. Data dropped values lower, which indicates that the network path is stable and has better transmission capability. It is an important performance measurement criteria for real-time communication systems. The data drop rate can be calculated as follows in a transmission time frame:

$$DDR = \frac{N^t - N^r}{N^{tx}} \times 100\% \tag{3}$$

where DDR is the data drop rate. N^t is the total number of transmitted data, and N^r is the total number of received data.

4. System Model and Simulation Setup

This research focuses on a collection of drones that could freely travel across a UANET employing an 802.11 g radio transceiver for wireless transmission. A random waypoint mobility model is applied in which UAVs move randomly towards the determined destination in the network with a steady speed (30 m /s and 40 m /s). The take-off and landing scenarios for UAVs are not considered in this research. Energy constraints are not considered as presumed rechargeable batteries for UAVs that can be recharged from renewable energy sources [40]. As most UAV implementations do not fly at high altitudes, we also consider that UAVs fly at a low and consistent altitude during their flight. An IPv4 auto-assign address is applied to each UAV, making it identifiable by its node address.

Simulation Setup

In this study, multiple UAV-based network structures are simulated in the OPNET modeler. OPNET is considered the optimal simulation tool with the most implementation capabilities compared with other simulation software [41]. It is used for complex network modeling and simulation. It has a user friendly graphical user interface, visual effects, a drag and drop module import facility, and all types of network devices that are used for building a specific network. If the performance of the network is not satisfactory, the OPNET modeler can find bottlenecks in service, network, or data flow. Moreover, NS-2, NS-3, and others need to write scripts in either C++, TLC, or Python, which is difficult for the complex network. Thus, OPNET 14.5 is used for network modeling and simulation in this article.

There are four simulation scenarios considered in this study, as described in Table 4. The network model of UAVs developed in the OPNET simulator is shown in Figure 2. The network model in Figure 2 contains 30 nodes as represented by UAV-1, UAV-2, . . ., and UAV-30, which are placed randomly within a 1000 m × 1000 m geographical area. For scenarios 1 and 2, UAV speed is considered at 40 m /s and an altitude of 200 m. Moreover, in scenarios 3 and 4, UAV speed is applied at 30 m /s and an altitude of 50 m. Extended rate PHY327 (802.11 g) is used as the underlying MAC layer with a data rate of 24 Mbps for scenarios two and four. In the same manner, 1 Mbps data rate is used for scenarios one and three. AODV, OLSR, DSR, GRP, and E-OLSR are considered as routing protocols' performance comparisons.

Table 4. Simulation scenarios.

Secnario Name	UAVs	Altitude	Speed	Data Rate
Scenario 1	30	200 m	40 m /s	1 Mbps
Scenario 2	30	200 m	40 m /s	24 Mbps
Scenario 3	50	50 m	30 m /s	1 Mbps
Scenario 4	50	50 m	30 m /s	24 Mbps

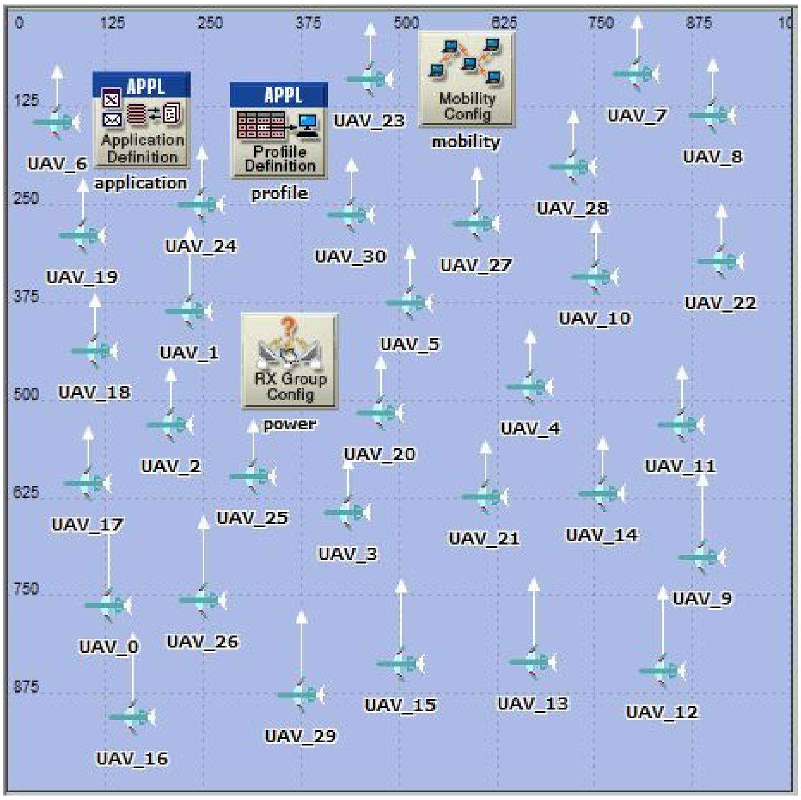


Figure 2. Simulation scenario of UAVs network model.

The MANET mobile node is changed to become a UAV node, as shown in Figure 3. The node model is applied to each node and every simulation scenario. Every square denotes a process model that handles packets. traf_src is applied to create a data packet and is forwarded to the lower layer. traf_src discards the packet if it already exists in the lower layer. The rsvp (resource reservation protocol) belongs to the transport layer used to cache resources over a network. The ip and ip_encap modules relate to the network layer. ip_encap encapsulates the transport layer segment. The ip module is used for addressing the individual device, reading the routing table, and sending IP data packets. The physical layer comprises wlan_port_tx_0_0 and wlan_port_rx_0_0. Here, wlan_port_tx_0_0 denotes the wireless transmitter, while wlan_port_rx_0_0 is the wireless receiver, and a_0 is the antenna module. The rest of the modules comprise OPNET process modules.

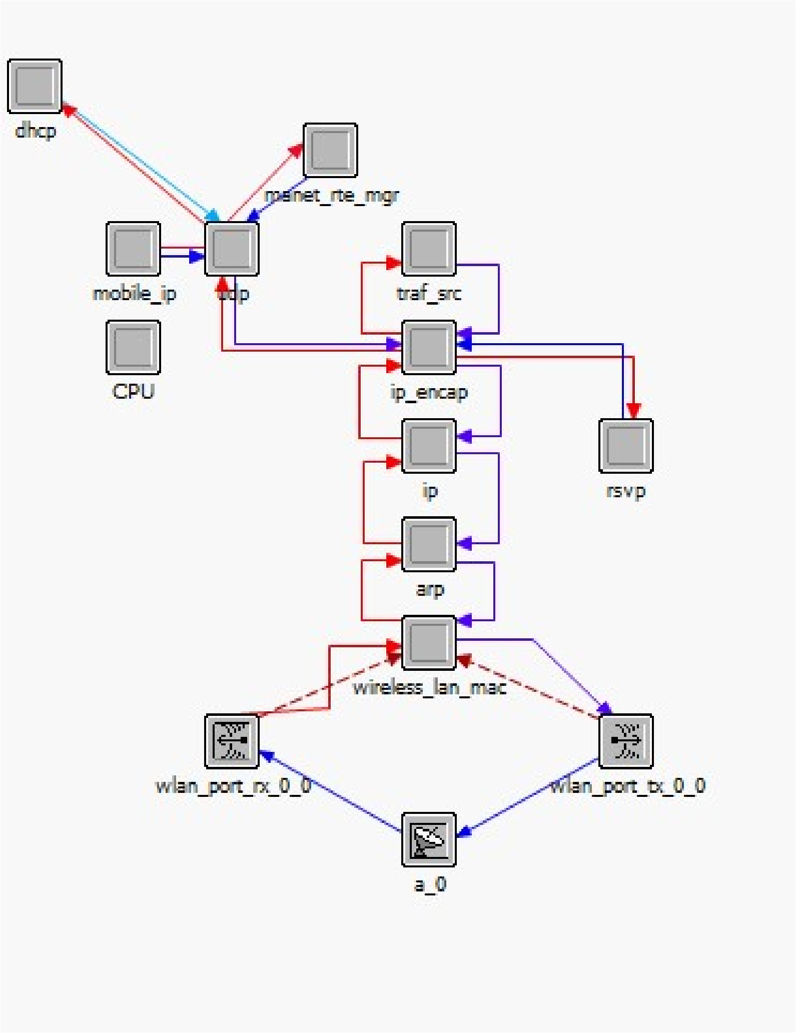


Figure 3. Node model of UAVs.

5. Results and Performance Analysis

In this paper, the performance of different routing protocols is studied; based on the study, an enhanced OLSR protocol (E-OLSR) using OPNET modeler 14.5 is designed. The paper contemplates the subsequent parameters for evaluating the comparative performance of routing protocols. Table 3 shows simulation parameters used in this study. Four different scenarios are considered in this study, as shown in Table 5.

5.1. Throughput

Figure 4a–d depict network performance in terms of average throughput in bits per second (bps). The proposed E-OLSR is compared with AODV, DSR, GRP, and OLSR in different simulation scenarios, varying the number of UAVs, speed, altitude, and data rate. Here, the x-axis indicates the simulation times, while the$y$-axis represents the throughput in bps. From Figure 4, it is observed that the performance of throughput depends on the number of UAVs. The throughput and network performance increase with an increasing number of UAVs in a fixed network area of 1000 m × 1000 m. In all scenarios, E-OLSR outperforms other existing routing protocols. While the throughput of AODV is better than others in high data rate, which is almost identical to E-OLSR in Figure 4b,d. On the other hand DSR shows the lowest throughput because of the extra routing overhead. Moreover, the proposed E-OLSR has achieved superior performance in all routing protocols.

Table 5. Performance comparison between different routing protocol.

Scenario	Performance Metrics	AODV	DSR	E-OLSR	GRP	OLSR
Scenario 1	Throughput (bits/s)	703,987	14,138	807,018	214,578	682,993
	Delay (s)	0.04603	0.03709	0.01643	0.02034	0.00112
	Data Drop Rate (bits/s)	66.10	185.27	19.60	12.38	25.16
Scenario 2	Throughput (bits/s)	618,075	10,409	791,997	178,115	682,993
	Delay (s)	0.00196	0.00358	0.00075	0.00245	0.00112
	Data Drop Rate (bits/s)	3021.12	6047.16	2993.20	5135.21	3385.23
Scenario 3	Throughput (bits/s)	976,093	15,409	1,164,725	352,092	1,046,432
	Delay (s)	0.0129	0.0376	0.0022	0.0033	0.0024
	Data Drop Rate (bits/s)	366.77	1737.6	0.43	0.76	0.58
Scenario 4	Throughput (bits/s)	1,107,482	136,878	1,141,475	347,206	1,030,007
	Delay (s)	0.00202	0.01074	0.00019	0.00773	0.00036
	Data Drop Rate (bits/s)	4350.93	10,602.72	760.71	302.96	1570.11

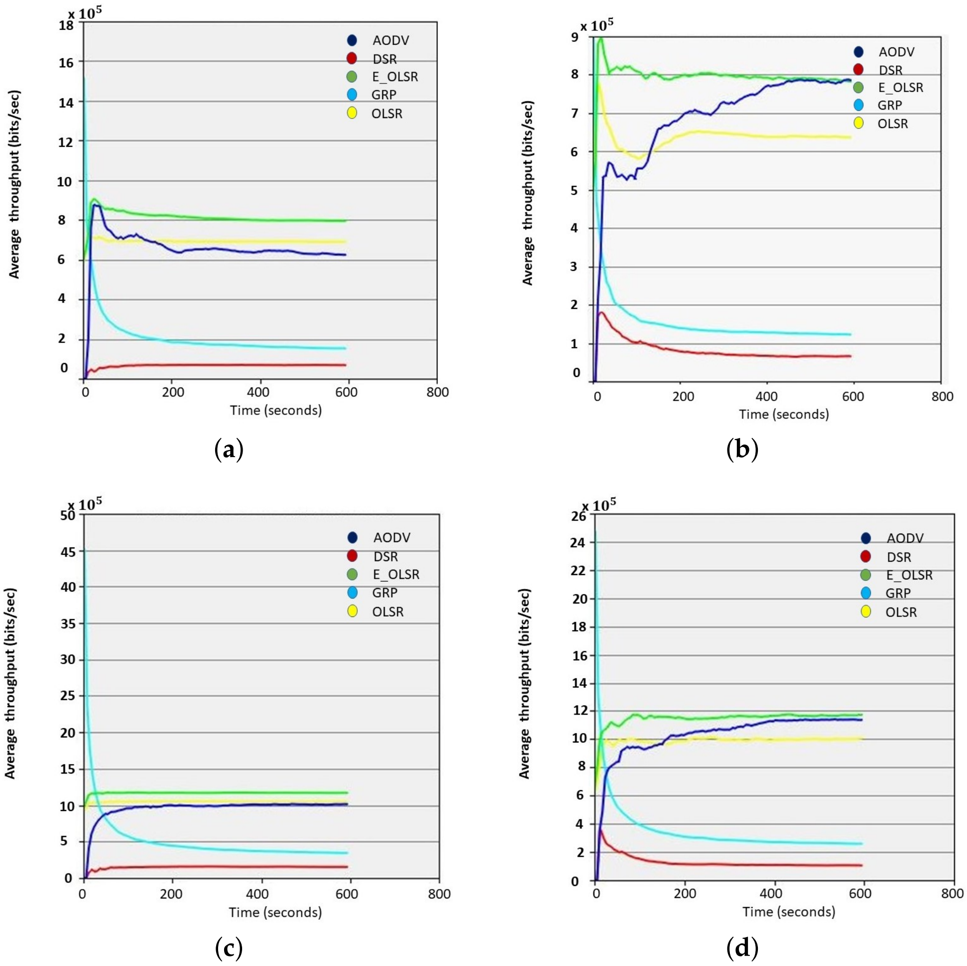


Figure 4. Average throughput comparison of different routing protocols. (**a**) Scenario 1. (**b**) Scenario 2. (**c**) Scenario 3. (**d**) Scenario 4.

5.2. Delay

Figure 5a–d demonstrate the average end-to-end delay of E-OLSR, OLSR, AODV, DSR, and GRP under a varying number of nodes, speed, and altitude. From Figure 5b,d, it can be observed that, at the same data rate of 24 Mbps, the delay of all routing protocols decreases with the increasing number of UAVs.This is because of the increasing probability of packets being routed rather waiting for transmission in the queue. From Figure 5c,d, it is shown that delay is lower at higher data rates due to faster packet transfer transmission. Among all protocols, DSR has the highest delay in all scenarios. In DSR, when a node sends a route request (RREQ), the destination replies with all the RREQs; as a result, the network becoes slower. Due to on-demand routing behavior, AODV also has higher delays. Compared to these five routing protocols, E-OLSR shows a comparatively low delay, which indicates better performance. Minimal holding time is responsible for this improved performance.

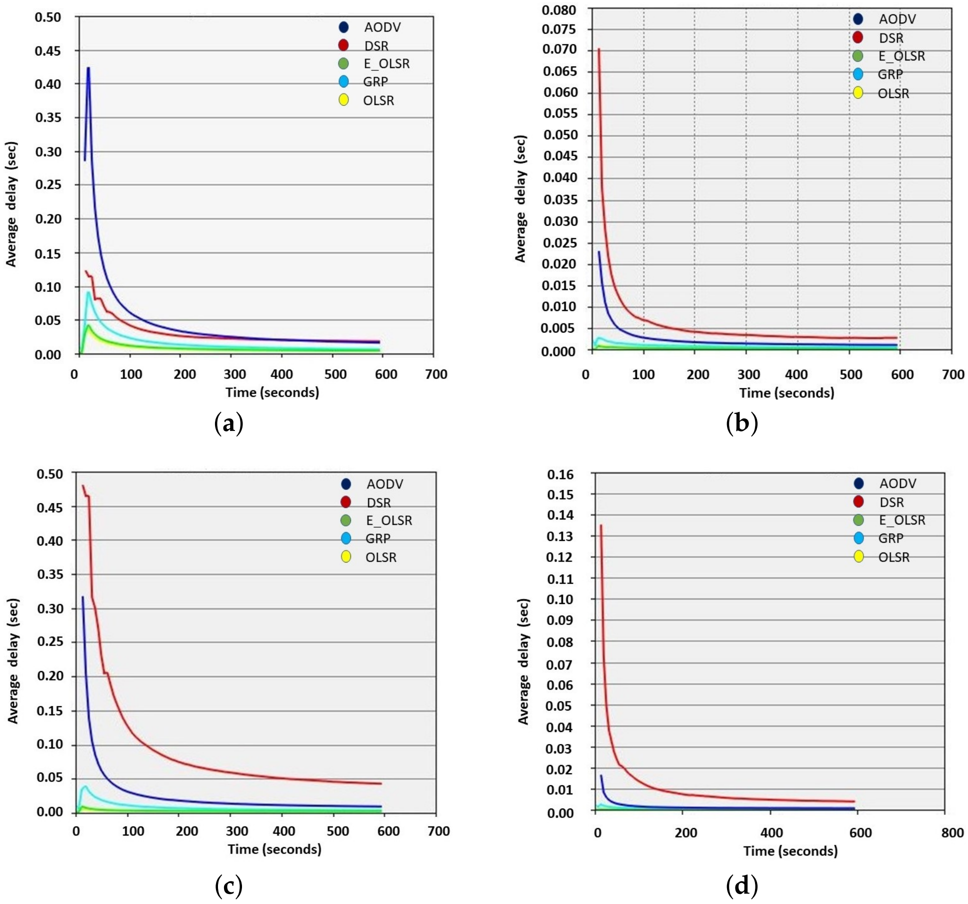
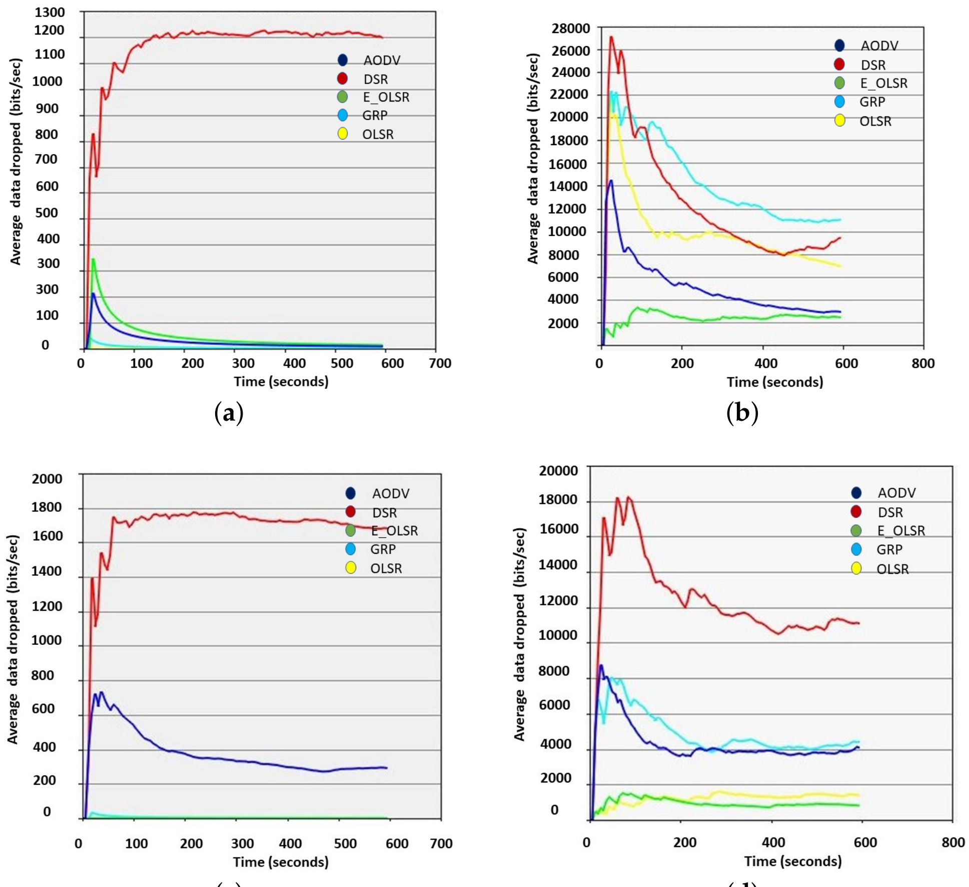


Figure 5. Average network delay comparison of different routing protocols. (**a**) Scenario 1. (**b**) Scenario 2. (**c**) Scenario 3. (**d**) Scenario 4.

5.3. Data Drop Rate

Figure 6 compares the average data dropped by E-OLSR, AODV, DSR, OLSR, and GRP when the number of nodes and data rate become varied. As observed in the contrast between Figure 6b,d, when node density is low, the data drop rate increases dramatically. From Figure 6a,b, it can be observed that the data drop rate increases with an increasing number of nodes. The UANET, based on the E-OLSR routing protocol, offers the best data drop rate performance compared to four existing routing protocols. However, DSR shows the worst result in all situations compared to other protocols. Furthermore, GRP also shows an increasing data drop rate at a high data rate Figure 6b,d.



(**a**) (**b**)

(**c**) (**d**)

Figure 6. Average data drop rate comparison of different routing protocols. (**a**) Scenario 1. (**b**) Scenario 2. (**c**) Scenario 3. (**d**) Scenario 4.

6. Conclusions

The performance of several topology-based routing protocols is examined by using simulation in this paper under various simulation environments in the UANET context. Furthermore, by tuning parameters, this paper enhances the performance of an OLSR protocol called E-OLSR, which outperforms standard ones defined in RFC 3626. In performance matrices such as throughput, delay, and data dropped, E-OLSR outperforms four other routing protocols (AODV, OLSR, DSR, and GRP). A brief qualitative analysis of the preceding routing protocols is provided based on significant parameters such as mobility, traffic density, routing overhead, and data rate. This research will assist network engineers in picking the optimal routing protocol for various UANET implementation scenarios.

Author Contributions: Conceptualization, E.A.T. and M.G.; methodology, E.A.T.; software, E.A.T.; validation, J.-M.L. and D.-S.K.; simulation, E.A.T.; data curation, J.-M.L.; writing—original draft preparation, E.A.T. and M.G.; writing—review and editing, E.A.T.; supervision, J.-M.L. and D.-S.K. 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: The data presented in this study are available on request from the corresponding author.

Acknowledgments: This work was supported by Priority Research Centers Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2018R1A6A1A03024003) and by National Research Foundation of Korea (NRF) grant funded by Korea Government (MSIT) (2019R1F1A1064055) and Grand Information Technology Research Center support program(IITP-2022-2020-0-01612) supervised by the IITP(Institute for Information communications Technology Planning Evaluation).

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

References

1. Yue, X.; Liu, Y.; Wang, J.; Song, H.; Cao, H. Software defined radio and wireless acoustic networking for amateur drone surveillance. *IEEE Commun. Mag.* **2018**, *56*, 90–97. [CrossRef]
2. Tuli, E.A.; Kim, D.S.; Lee, J.M. Performance Enhancement of UFMC Systems using Kaiser Window Filter. In Proceedings of the 2021 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea, 20–22 October 2021.
3. Oliveira, H.C.; Guizilini, V.C.; Nunes, I.P.; Souza, J.R. Failure Detection in Row Crops From UAV Images Using Morphological Operators. *IEEE Geosci. Remote Sens. Lett.* **2018**, *15*, 991–995. [CrossRef]
4. Rusyadi Ramli, M.; Lee, J.M.; Kim, D.S. Hybrid MAC Protocol for UAV-Assisted Data Gathering in a Wireless Sensor Network. *Internet Things* **2021**, *14*, 100088. [CrossRef]
5. Bushnaq, O.M.; Chaaban, A.; Al-Naffouri, T.Y. The Role of UAV-IoT Networks in Future Wildfire Detection. *IEEE Internet Things J.* **2021**, *8*, 16984–16999. [CrossRef]
6. Chen, D.Q.; Guo, X.H.; Huang, P.; Li, F.H. Safety Distance Analysis of 500kV Transmission Line Tower UAV Patrol Inspection. *IEEE Lett. Electromag. Compat. Pract. Appl.* **2020**, *2*, 124–128. [CrossRef]
7. ur Rahman, S.; Kim, G.H.; Cho, Y.Z.; Khan, A. Positioning of UAVs for throughput maximization in software-defined disaster area UAV communication networks. *J. Commun. Netw.* **2018**, *20*, 452–463. [CrossRef]
8. Shamsoshoara, A.; Afghah, F.; Blasch, E.; Ashdown, J.; Bennis, M. UAV-Assisted Communication in Remote Disaster Areas Using Imitation Learning. *IEEE Open J. Commun. Soc.* **2021**, *2*, 738–753. [CrossRef]
9. Nassi, B.; Shabtai, A.; Masuoka, R.; Elovici, Y. Sok-security and privacy in the age of drones: Threats, challenges, solution mechanisms, and scientific gaps. *arXiv* **2019**, arXiv:1903.05155.
10. Coluccia, A.; Fascista, A.; Schumann, A.; Sommer, L.; Dimou, A.; Zarpalas, D.; Méndez, M.; de la Iglesia, D.; González, I.; Mercier, J.P.; et al. Drone vs. Bird Detection: Deep Learning Algorithms and Results from a Grand Challenge. *Sensors* **2021**, *21*, 2824. [CrossRef]
11. Jamil, S.; Fawad; Rahman, M.; Ullah, A.; Badnava, S.; Forsat, M.; Mirjavadi, S.S. Malicious UAV Detection Using Integrated Audio and Visual Features for Public Safety Applications. *Sensors* **2020**, *20*, 3923. [CrossRef]
12. Akter, R.; Doan, V.S.; Lee, J.M.; Kim, D.S. CNN-SSDI: Convolution neural network inspired surveillance system for UAVs detection and identification. *Comput. Netw.* **2021**, *201*, 108519. [CrossRef]
13. Arafat, M.Y.; Moh, S. Routing Protocols for Unmanned Aerial Vehicle Networks: A Survey. *IEEE Access* **2019**, *7*, 99694–99720. [CrossRef]
14. İlker, B.; Sahingoz, O.K.; Şamil, T. Flying Ad-Hoc Networks (FANETs): A survey. *Ad Hoc Netw.* **2013**, *11*, 1254–1270. [CrossRef]
15. Singh, K.; Verma, A.K. A fuzzy-based trust model for flying ad hoc networks (FANETs). *Int. J. Commun. Syst.* **2018**, *31*, e3517. [CrossRef]
16. Priyambodo, T.K.; Wijayanto, D.; Gitakarma, M.S. Performance Optimization of MANET Networks through Routing Protocol Analysis. *Computers* **2021**, *10*, 2. [CrossRef]
17. Leonov, A.V.; Litvinov, G.A. Simulation-Based Performance Evaluation of AODV and OLSR Routing Protocols for Monitoring and SAR Operation Scenarios in FANET with Mini-Uavs. In Proceedings of the 2018 Dynamics of Systems, Mechanisms and Machines (Dynamics), Omsk, Russia, 13–15 November 2018; pp. 1–6.
18. Hussen, H.R.; Choi, S.C.; Park, J.H.; Kim, J. Performance Analysis of MANET Routing Protocols for UAV Communications. In Proceedings of the 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN), Prague, Czech Republic, 3–6 July 2018; pp. 70–72. [CrossRef]
19. Kakamoukas, G.A.; Sarigiannidis, P.G.; Economides, A.A. FANETs in Agriculture-A routing protocol survey. *Internet Things* **2020**, *2020*, 100183. [CrossRef]
20. Khan, I.U.; Qureshi, I.M.; Aziz, M.A.; Cheema, T.A.; Shah, S.B.H. Smart IoT control-based nature inspired energy efficient routing protocol for flying ad hoc network (FANET). *IEEE Access* **2020**, *8*, 56371–56378. [CrossRef]
21. 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). *Vehicul. Commun.* **2017**, *10*, 29–56. [CrossRef]
22. Hong, J.; Zhang, D. TARCS: A topology change aware-based routing protocol choosing scheme of FANETs. *Electronics* **2019**, *8*, 274. [CrossRef]
23. Khan, M.A.; Khan, I.U.; Safi, A.; Quershi, I.M. Dynamic Routing in Flying Ad-Hoc Networks Using Topology-Based Routing Protocols. *Drones* **2018**, *2*, 27. [CrossRef]

24. Jiang, J.; Han, G. Routing Protocols for Unmanned Aerial Vehicles. *IEEE Commun. Mag.* **2018**, *56*, 58–63. [CrossRef]
25. Cheng, C.M.; Hsiao, P.H.; Kung, H.T.; Vlah, D. Maximizing Throughput of UAV-Relaying Networks with the Load-Carry-and-Deliver Paradigm. In Proceedings of the 2007 IEEE Wireless Communications and Networking Conference, Hong Kong, China, 11–15 March 2007; pp. 4417–4424. [CrossRef]
26. Varshney, T.; Katiyar, A.; Sharma, P. Performance improvement of MANET under DSR protocol using swarm optimization. In Proceedings of the 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), Ghaziabad, India, 7–8 February 2014; pp. 58–63. [CrossRef]
27. Johnson, D.B.; Maltz, D.A. Dynamic source routing in ad hoc wireless networks. In *Mobile Computing*; Springer: Berlin/Heidelberg, Germany, 1996; pp. 153–181.
28. Khare, V.R.; Wang, F.Z.; Wu, S.; Deng, Y.; Thompson, C. Ad-hoc network of unmanned aerial vehicle swarms for search amp; destroy tasks. In Proceedings of the 2008 4th International IEEE Conference Intelligent Systems, Varna, Bulgaria, 6–8 September 2008; Volume 1, pp. 6-65–6-72. [CrossRef]
29. Moudni, H.; Er-rouidi, M.; Mouncif, H.; El Hadadi, B. Performance analysis of AODV routing protocol in MANET under the influence of routing attacks. In Proceedings of the 2016 International Conference on Electrical and Information Technologies (ICEIT), Tangiers, Morocco, 4–7 May 2016; pp. 536–542.
30. Lyu, C.; Gu, D.; Zhang, X.; Sun, S.; Zhang, Y.; Pande, A. SGOR: Secure and scalable geographic opportunistic routing with received signal strength in WSNs. *Comput. Commun.* **2015**, *59*, 37–51. [CrossRef]
31. Chen, X.; Tian, S.; Nguyen, K.; Sekiya, H. Decentralizing Private Blockchain-IoT Network with OLSR. *Future Internet* **2021**, *13*, 168. [CrossRef]
32. Kumar, P.; Verma, S. Implementation of modified OLSR protocol in AANETs for UDP and TCP environment. *J. King Saud Univ. Comput. Inform. Sci.* **2019**, *in press*. [CrossRef]
33. Boushaba, A.; Benabbou, A.; Benabbou, R.; Zahi, A.; Oumsis, M. Multi-point relay selection strategies to reduce topology control traffic for OLSR protocol in MANETs. *J. Netw. Comput. Appl.* **2015**, *53*, 91–102. [CrossRef]
34. De Rango, F.; Fotino, M.; Marano, S. EE-OLSR: Energy Efficient OLSR routing protocol for Mobile ad-hoc Networks. In Proceedings of the MILCOM 2008—2008 IEEE Military Communications Conference, San Diego, CA, USA, 16–19 November 2008; pp. 1–7. [CrossRef]
35. Barki, O.; Guennoun, Z.; Addaim, A. Improving the selection of MPRs in OLSR protocol: A survey of methods and techniques. *Int. J. Electr. Comput. Eng.* **2020**, *10*, 288. [CrossRef]
36. Toutouh, J.; Garcia-Nieto, J.; Alba, E. Intelligent OLSR Routing Protocol Optimization for VANETs. *IEEE Trans. Vehicul. Technol.* **2012**, *61*, 1884–1894. [CrossRef]
37. Clausen, T.; Jacquet, P. RFC3626: Optimized Link State Routing Protocol (OLSR). 2003. Available online: https://dl.acm.org/doi/pdf/10.17487/RFC3626 (accessed on 8 May 2021).
38. Mohammed, F.; Jawhar, I.; Mohamed, N.; Idries, A. Towards Trusted and Efficient UAV-Based Communication. In Proceedings of the 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), New York, NY, USA, 9–10 April 2016; pp. 388–393. [CrossRef]
39. De Couto, D.S.; Aguayo, D.; Bicket, J.; Morris, R. A high-throughput path metric for multi-hop wireless routing. *ACM Mobicom* **2003**, *3*, 134–146. [CrossRef]
40. 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]
41. AlShahwan, F.; Alshamrani, M.; Amer, A.A. Dynamic Novel Cross-Layer Performance Enhancement Approach for SIP over OLSR. *IEEE Access* **2018**, *6*, 71947–71964. [CrossRef]