Survey on UAANET Routing Protocols and Network Security Challenges

Jean-Aimé Maxa, Mohamed-Slim Ben Mahmoud, Nicolas Larrieu

Survey on UAANET Routing Protocols and Network Security Challenges

Jean-Aimé Maxa[1] [2] , Mohamed Slim Ben Mahmoud[1] and Nicolas Larrieu[1]
[1] ENAC, TELECOM/Resco, F-31055 Toulouse, France
[2] Univ de Toulouse, F-31400 Toulouse, France
{$maxa, slim.ben.mahmoud$}@recherche.enac.fr
nicolas.larrieu@enac.fr

***Abstract*—UAV Ad hoc Networks (UAANETs) is a subset of the well-known mobile ad hoc network (MANET) paradigm. It refers to the deployment of a swarm of small Unmanned Aerial Vehicles (UAVs) and Ground Control Stations (GCS). These UAVs collaborate in order to relay data (command and control traffic and remotely sensed data) between each other and to the Ground Control Station (GCS). Compared to other types of ad hoc networks, UAANETs have some unique features and bring several major challenges to the research community. One of these is the design of UAANET routing protocol. It must establish an efficient route between UAVs and adjust in real time to the rapidly changing topology. It must also be secured to protect the integrity of the network against malicious attackers.**

Security of routing protocols has been widely investigated in wired networks and MANETs, but as far as we are aware, there is no previous research paper dealing with the security features of UAANET routing protocols. This paper focuses on characteristics of UAANETs and provides a review of the literature on associated routing protocols. We also highlight the analysis of the security features of these protocols. Security requirements, potential threats and countermeasures are all described.

***Index Terms*—UAV Ad hoc NETwork (UAANET), Security Architecture, Routing Protocol.**

I. Introduction

UAV investigations began after the First World War with preliminary prototypes. Since then, technological and research advances in embedded systems have helped to produce small UAVs with highly effective capacities. A UAV, also called Drone or Remotely Piloted Aircraft System (RPAS), is a pilotless aerial vehicle which can be controlled either autonomously by an on-board computer or remotely by a pilot on the ground.

Recently, their popularity has drastically increased in commercial and government applications. Their use is not limited to the military domain and they can also be used for civilian applications for example, for weather monitoring [1] or infrastructure inspection [2]. To support UAV developments, a large community has emerged and continues to share open source platforms for UAVs such as: PX4 [3], Qgroundcontrol [4], Pixhawk [5]. A recent example is the collaborative Dronecode [6] project supported by the Linux foundation [7] aiming to provide autopilot and GCS software for UAV users. In the near future, because of those efforts, UAVs are expected to play a major role in effective infrastructure management and intelligent traffic management by supplying both static data acquisition and dynamic data streaming.

Typically, a small UAV is equipped with a set of micro-electromechanical systems, including but not limited to low capacity batteries, cheap airframes, microprocessors, micro radio-devices (limited radio range) and have a limited payload volume and weight capacity. As a consequence, its capabilities is limited in space and time. Such constraints can be an issue for complex missions, for example an aerial monitoring during natural disaster assessment. In such a case, the scalability and the duration of the mission (UAV energy level and computation capacity) are the key factor in the success or the failure of the mission.

An alternative solution is to deploy multi-UAV systems that make UAVs and GCS collaborate through an ad hoc wireless network called UAANET. The collaboration and coordination between UAVs enhance the capability of the Unmanned Aircraft System (UAS) by creating a communicating group of UAVs. Ad hoc networks have been largely investigated by the research community for a set of mobile systems such as sensors [8], cars [9], or civil aircraft [10]. UAANET is considered as subcategory of Mobile Ad hoc Networks (MANETs). However, it raises some networking issues that must be addressed to allow efficient communication between nodes. A UAANET routing protocol has to provide route discovery, data forwarding and route maintenance services by taking into account all the specific characteristics of the UAANET (cf. Section V). For this reason, typical routing protocols initially designed for other classes of MANET cannot be directly used for UAVs without amendment [11].

Moreover, from a network security point of view, both data traffic and the routing protocol traffic need to be protected. Indeed, in a wireless environment, attacks are likely to occur: control packets need to be authenticated to verify both the identity of the message originator and the message integrity. It is also necessary to ensure payload traffic confidentiality to ensure privacy and to avoid traffic analysis [12]. Traffic analysis consists of confidentiality violation in which data traffic is captured and analyzed to deduce a set of information related to the UAS deployment (e.g., node mobility pattern).

In this paper, we propose to provide an overview of current UAANETs state of the art with an emphasis on routing

protocols and associated security issues. In the routing survey, we will detail the existing routing protocols specifically designed for UAANET, and also some routing protocols intended for MANET but used in some UAANET simulations. With regard to security aspect, we will analyze the vulnerability of existing communication architecture and summarize some security techniques that can protect UAANETs.

It should be noted that, we mainly focus on civil, commercial and research-dedicated UAVs. Military units are out of the scope of the paper. Section II provides an overview of existing UAANET survey. We highlight what is lacking in these surveys and present a UAANET state of the art with a focus on network properties in section III. In section IV, we discuss routing protocols for UAANETs. In section V, we identify the UAANETs security requirements and potential attacks on the network layer. In section VI, we provide a selection of tools that can be used to avoid such vulnerabilities. In section VII, we conclude by giving some directions for future work.

II. Overview of UAANET Technology and Existing Communication

This paper provides a survey of both UAANET routing protocols and network security. We believe these two topics should be subject to the same analysis as there is a trade-off to establish between routing efficiency and security overheads.

Some UAANET survey papers exist in the literature. These works either give a general overview of communication architectures for UAVs or relate a particular solution that responds to a specific need (such as quality of service). To the best of our knowledge, no previous work addresses UAANET routing protocols while linking them to network security. However, some papers that are considered to be among the first works in the field have specially treated UAANET communication architecture design challenges and issues. Among these papers, we quote [13], in which Bekmezci et al. were interested in the concept and the challenge of creating a UAANET architecture. They give a detailed overview of requirement tools and algorithms in each layer of the protocol stack (physical layer, MAC layer, network layer and transport layer).

In [14], Frew et al. presented a set of operational requirements for building a swarm of UAVs. They analyzed the networking systems of small UAVs by characterizing multiple communication architectures of such swarms. They emphasized delay tolerant network architecture advantages to ensure data delivery and network service discovery between UAVs. Similarly, in [15] Li, Jun, et al., were interested in the classification of potential communication architectures for UAV swarms. They analyzed each one individually and discussed the pros and cons. They placed special attention on the UAANET architecture because of its high applicability among multiple groups of heterogeneous UAVs. They also provided a detailed survey of data link technologies for UAV swarm.

In [16], Gupta et al. proposed a survey paper on important issues in UAV communication networks. The authors focused on three specific topics. The first topic covered the special features of UAANET compared to MANETs and VANETs which induce the challenges of UAV networks. These differences lies in the mobility model, topology types and changes, energy constraints and typical use cases. The second topic consist of an analysis of how the Software Defined Network (SDN) could be used to increase performances within UAANET deployment. Lastly, they studied UAANET routing requirements to meet their specific requirements.

In [17], Namuduri et al., have reviewed the prerequisite requirements that must be addressed before deploying a UAANET. In this paper, they assessed the requirements for UAV networking and communications, situational awareness, mobility patterns, sense-and-avoid, coordination and control. Furthermore, they also stress the certification issues on multiple UAVs to enable full deployment in national airspaces.

In survey papers [18], [19], respectively, Sahingoz and Shashank surveyed the research in UAV networking and related issues. They focused on classifying MANET and VANET routing protocols and discussed its theoretical applicability in UAANET.

Similarly, in paper [20], Maghsoudlou focused on a geographical routing protocol state of the art and an analysis for UAANET perspectives.

In survey paper [21] , Song et al. presented a state of the art in UAANET MAC protocol and quality of service difficulties. A number of security aspects were briefly presented.

In [22], Zhao et al. presented a detailed state of the art schemes on topology control and mobility strategy for UAV Ad-hoc Networks. Among the works related to the security of UAANET, but focused on a specific issue, we quote: [23] of Bekmezci et al. reserved for security limitation analysis of FANET. They listed some well-known attacks on ad-hoc networks and their existing countermeasures.

The surveys discussed above are summarized in table I according to the topic coverage they provide. Such a summary shows that UAANET is currently an active field of investigation. However, network security has been ignored in all these works. Besides, none of them has been entirely written to cover routing protocols in mind. Thus, we provide in this article a complete state of the art dedicated to UAANET routing protocols. In the next section, we first provide a description of the UAS focusing on its components, communication architectures, and characteristics along with some application scenarios.

III. UAANET State of the Art

A. Unmanned Aircraft System

A UAS is a system composed of UAVs, communication links, ground control stations, a launch and recovery system, and any other system elements that may be required during flight operation. Although the International Civil Aviation Organization (ICAO) advises using the term Remotely Piloted Aircraft System (RPAS) [25], the literature quotes many other terms to designate such a heterogeneous system. For clarity, table II summarizes these terms:

Survey	Communication architecture	QoS	Routing protocol	Data link Technology	Network Security	Mobility Model
[[13]]	yes	No	yes	yes	No	yes
[[14]]	yes	No	yes	No	No	No
[[15]]	yes	No	No	yes	No	No
[[17]]	yes	No	No	No	No	Yes
[[18]][[24]][[19]]	yes	No	yes	No	No	No
[[20]]	yes	No	yes	No	No	No
[[21]]	yes	yes	No	yes	No	No
[[22]]	yes	No	No	No	No	yes
[[16]]	yes	No	yes	No	No	No
[[23]]	No	No	No	No	yes	No

Table I
EXISTING UAANET SURVEY RELATED WORK

Given name	Meaning
UAS	Unmanned Aircraft System
UAV system	Unmanned Aerial Vehicle System
RPAS	Remotely Piloted Aircraft System
RPV System	Remotely Piloted Vehicle System

Table II
DIFFERENT TERMS USED TO INDICATE UAS

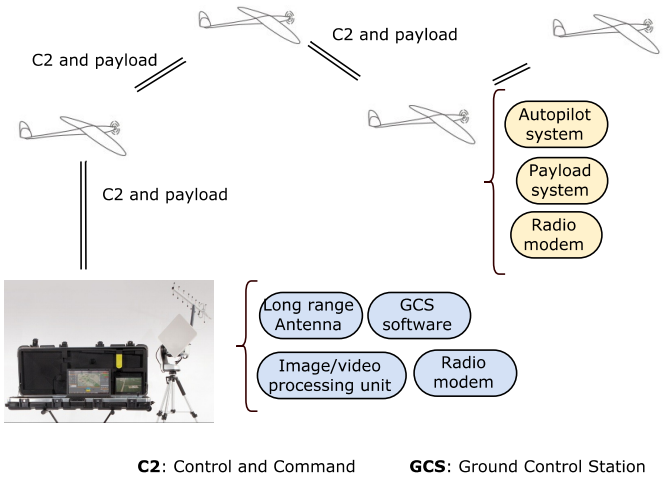


Figure 1. Example of UAS architecture

The architecture of a typical UAS is shown in figure 1.

1) Unmanned Aerial Vehicle: The main component of a UAS is the UAV which can be remotely controlled or fly autonomously based on a pre-programed or predetermined flight plan. It is usually required to fly out of sight of the operator and is able to communicate in real time with the controller sending back the payload data. It must also periodically return information about its flight conditions (e.g. position, speed, heading or altitude). This data helps the operator to evaluate the flight conditions and accordingly if needed, allows him to modify the flight settings. In addition, some UAVs may also be equipped with on-board decision-making capabilities to support automatic corrective responses in case of component failures.

It is important to emphasize the existence of several kinds of UAVs, each designed for a different purpose. It is possible to categorize them in many ways using different metrics (e.g., size, shape, autonomy, operational altitude, operating conditions and certification approaches). UAV classification is important from a regulatory perspective as different requirements may be imposed on UAV categories according to their features. A detailed survey of UAV classification can be found in [26].

2) Payload: Each UAV usually carries a payload[1], which is the most significant part of the UAS since it is the ultimate reason for having such a system. It should be noted that in order to deploy a payload for small UAVs, a trade-off between communications, power, sensors and autopilot subsystems must be found so that the overall UAV system balance of weight and volume is preserved. Typically, the payload used in civilian UAVs is a digital camera that streams or records a video (for reconnaissance and surveillance missions). It should be noted that in this case, the digital camera must be placed under the front of the UAV in order to detect any obstacle during the landing phase [27]. Depending on the UAV size and the application requirements, the payload traffic is then sent to the GCS in real time. The payload may also be a special sensor used to collect samples or gather information related to a specific field (e.g. a temperature sensor). Another type of UAV payload is a communication platform device for data and communications. In this case, the objective is to extend the coverage of the radio frequency systems, including the set of data links used to exchange payload and control traffic [28]. Interested readers can refer to [29] for more details of UAV payload design requirements and capabilities.

3) Ground Control Station: a GCS is a combination of multiple entities that form an independent infrastructure to monitor UAV movements. It allows the operator to adjust waypoints, flight paths, altitude, airspeed and landing zones. The GCS communicates with UAVs through the communication system uplink and waits for information in return on the downlink. Typically, a GCS is composed of the following three entities:

1) GCS Desktop software: this is one of the crucial parts of the UAS. The software allows the operator to control

[1]In order to avoid misunderstanding, it should be noted that the payload from an UAS point of view is quite different from the payload traffic, which is the amount of additional data required by traffic control

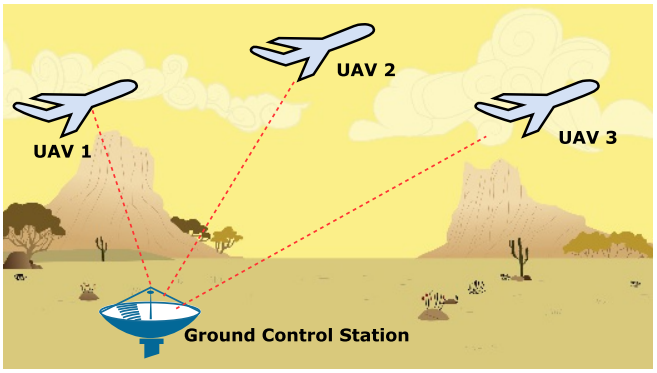


Figure 2. Centralized architecture

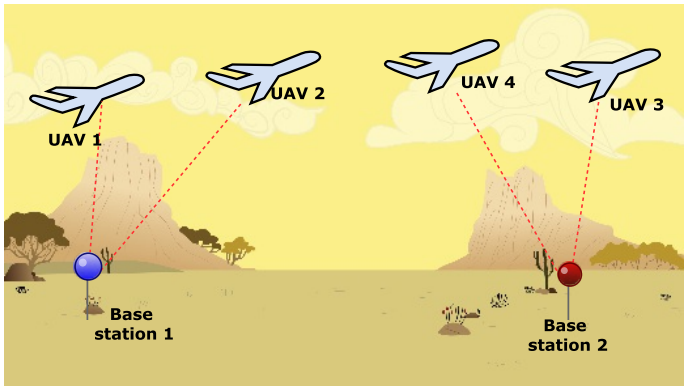


Figure 3. cellular based architecture

the UAVs during all the flight phases and to analyze the features of the surrounding zones in order to give a predictive signal strength map. It also enables the operator to monitor and adjust sensor payloads during UAV missions.

2) GCS infrastructure : the physical part of the GCS. It includes a transmitter to transmit and receive data traffic respectively. This infrastructure supports communication between the GCS and the nearest UAV through a two-way communication link: the uplink provides control of the UAV flight and commands for its payload, whereas the downlink provides acknowledgements to (air) traffic control and transmits UAV status information (e.g. altitude, speed, direction, etc.). Furthermore, in order to be sure of the effectiveness of the mission, it is desirable that the data link provides an anti-interference capability [30].

B. UAV Communication Architectures

A UAANET communication architecture is defined by a set of rules and mechanisms that determine how information should be exchanged between GCS and multiple UAVs. In this section, we will analyze existing communication architectures that can be used for a swarm of UAVs. Their strengths and weaknesses are highlighted. We show why UAANET communication architecture is a promising solution for the future of UAVs.

Firstly, a direct communication scheme [14] [15] can be used to communicate UAVs. Each UAV is connected directly to the ground station with a dedicated link. The GCS is considered as a central node and communicates with each UAV simultaneously. As the scheme is centralized, UAV-to-UAV communications are not possible as data traffic must be routed to the GCS. An illustration of such network architecture is shown in Figure 2.

Such centralized architecture has numerous flaws. First, since a certain amount of bandwidth is dedicated for each UAV, the total amount used is expected to scale to be proprotional to the number of UAVs in the network. As a consequence, the system has to provide large bandwidth capacities to support a high node density in the network. Another drawback is the long transmission delay between two UAVs because data must always be routed to the GCS. From a reliability point of view, geographic obstructions (e.g. mountain) can block the signal and prevent control and command (c2) traffic to be sent. As a result, either UAVs cannot fly too far from the GCS or an advance radio devices is deployed to generate high transmission power, which is not suitable for small UAVs. Moreover, from a security point of view, the use of the GCS as a central point of communication in the network represents a vulnerability and a single point of failure. Indeed, if the GCS is somehow out of service, all UAVs in the network will be unable to communicate further. In case two UAVs need to communicate with each other, they need to send the traffic through the GCS, which can saturate the UAV system and adds latency to the communication.

Cellular networks represent another communication architecture that can be used for UAV communications (represented in Figure 3). As stated in [14], this refers to the use of a base station infrastructure which forms multiple cellular beams where one or multiple UAVs are located. Each cell uses a different frequency value to that of the neighboring cell in order to avoid interference. When combined together, the cellular network can provide the required signal coverage over a wide geographic area. Typically, in such topology, it is possible for two UAVs to communicate through the base station.

However, the expensive implementation of these base stations is expensive and represents a financial handicap. Indeed, a positive return on investment is not guaranteed because as unlike mobile telecommunication, UAS flights are infrequent and irregular. Thus, the cost is not recovered. Moreover, cellular mechanism is only relevant for specific application scenarios where the mission zone is initially known. In cases where the area is initially unknown (e.g. natural disaster assessment), and if there is no base station in the vicinity, the use of the cellular network paradigm is not feasible. From a security point of view, such a solution is still vulnerable due to the presence of numerous fixed points that can be attacked.

Traffic	Link type
Configuration (GCS, camera settings, autopilot, ...)	Uplink
Hearbeat, Joystick	Uplink
Geographical location	Downlink
Command and control	Uplink
Data (image, video stream)	Downlink

Table III
DIFFERENT TYPES OF APPLICATIVE STREAMS IN UAANET

References	Name
[31] [32] [33] [34]	UAANET (UAV Ad hoc Network)
[35]	Mobile UAV ad hoc network
[36]	Mobile Ad-Hoc Unmanned Aerial Vehicle Communication Network
[13]	Flying ad hoc network
[21]	Ad Hoc Networks with UAV Node
[37]	Airborne network
[38]	Network Aerial Robots
[39]	Unmanned Aeronautical Ad-Hoc Network
[40]	Aerial Communication Network
[41]	Networks of UAVs
[42]	Distributed Aerial Sensor Network
[43]	UAV fleet networks

Table IV
UAANET TERMINOLOGY IN THE LITERATURE

In order to address the weaknesses of the communication architectures discussed above, an UAANET can be used for a swarm of UAVs (depicted in Figure 4). This network architecture is a sub-category of the well-known MANET in which nodes communicate with each other without the need for a fixed infrastructure. Each UAV acts as an end system. All UAVs are required to cooperate and thus have to organize themselves to relay information. The ad hoc architecture can cope well with the constant changing topology that results from UAV mobility. In UAANETs, the GCS is considered as a regular end node which can have a fixed or non-fixed geographical position. It communicates with the nearest UAV which acts as a gateway. Thus, there are three types of communication to consider in UAANETs (see Figure 5): UAV-to-UAV, UAV-to-GCS and GCS-to-UAV.

In UAV-to-UAV communication, UAVs can communicate with each other directly in wireless range or indirectly in a multi-hop mode. As for UAV-to-GCS communication, this refers to the wireless exchange of telemetry (data captured through the payload) and heartbeat[2] messages. In UAANET, such communication exists between the GCS and the nearest UAV. GCS-to-UAV communication refers to the exchange of critical command and control (c2) traffic. The different types of applicative streams are depicted in Table III

Furthermore, we should remember that in the literature, there are several ways to name an ad hoc network formed by UAVs. For a matter of clarity, these names are listed in Table IV.

Compared to other communication networks cited above, UAANETs have several advantages. The scalability is ensured thanks to the mobility of UAVs which enables them to cover a vast area rapidly. In addition, the reliability is improved because the failure of one UAV does not affect the whole network. Bandwidth can be reused more often and thus more efficiently due to multi-hop communication. From a security viewpoint, the absence of a central node within the network decreases the risk of attack on a single point of failure. Each end system (UAVS and GCS) is responsible for network integrity and confidentiality. However, it is important to mention that several security issues need to be addressed even without a centralized node. In section V, security challenge is discussed.

Furthermore, different types of communication architecture have been inspired by the UAANET scheme. In [44], different Delay Tolerant Networking (DTN) architectures have been proposed for the UAV swarm. In such a network, we make the assumption that an end-to-end path may not always exist due to the inherent characteristics of the wireless connections and the variable distance between nodes. DTN architecture allows UAVs to begin the data exchanges process even if there is only a partial path available. The DTN protocol allows intermediate nodes to store data until it finds a neighbor in his range. The major drawback of this architecture is that it cannot suit real time traffic requirements as route discovery may require additional time.

Net-centric communication for a heterogeneous UAS provided in [45] is another example of network architecture for UAANETs. In such a network, different clusters are formed with various types of UAVs. The heterogeneous paradigm suggests that UAVs may use different hardware, software or data link technologies. In such a scheme, the main objective is to have a unique communication system that can work transparently on top of a variety of physical layers. A hierarchical control architecture is used as UAVs are regrouped into several clusters. The communication is coordinated by the cluster head, which supervises a set of UAVs.

Moreover, another organization of UAANET architecture is the multi-cluster UAV Ad hoc Network [15]. It makes the assumption that different UAV backbones (major UAV elements) communicate with the GCS. Different groups of UAVs are constructed and form an ad hoc network. The UAV backbone acts as a cluster head and is responsible for sending and receiving traffic within its group. There is an intra-group communication and an inter-group communication as suggested in [46]. This architecture is considered as semi-centralized and therefore still lacks of robustness as explained previously.

Lastly, in [36], a cross-layer design for mobile ad hoc UAV networks is proposed. The cross-layer solutions have been developed by breaking the principles of layering and by allowing interdependence and joint development of protocols involving various different layers of the protocol stack. Alshbatat et al. have created interaction algorithm between non-adjacent layers to share various information such as bit error rate, altitude, geographical position in order to meet UAANET QoS requirements.

[2]There is a requirement for the UAV to send the heartbeat packet periodically. On the GCS, the user can monitor the heartbeat packet sequence number and determine packet loss statistics and the UAV mode is in.

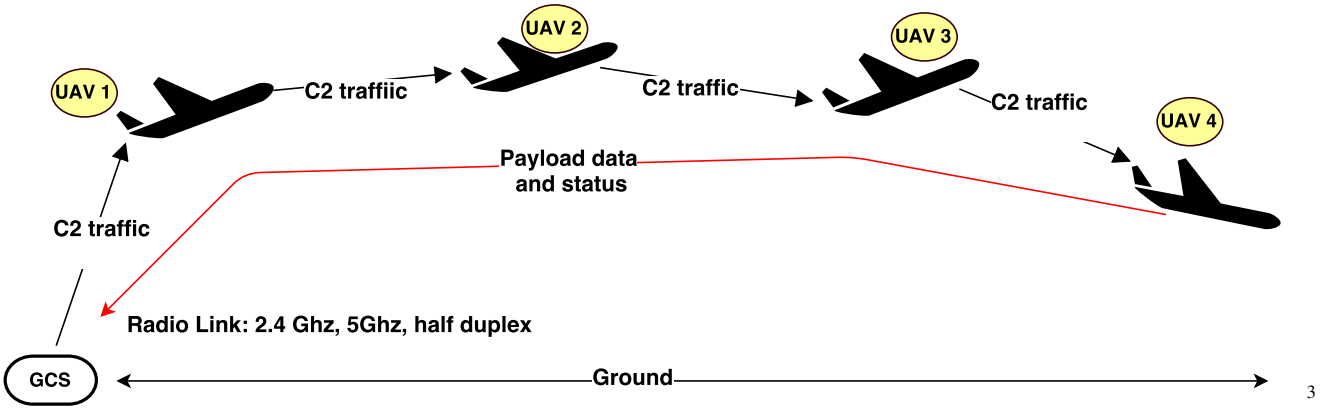


Figure 4. UAANET Architecture

	Strength	Weakness
Direct architecture	- Reliability of data delivery with low latency	- Depending on the number of nodes, it requires a large amount of bandwidth. - Ineffiency of UAV-to-UAV communication. - High probability of obstruction due to obstacles. -Vulnerable to network attacks due to the centralized scheme (for instance eavesdropping [47], blackhole [48]).
Cellular based Architecture	- Reliable data delivery. - Network connectivity is ensured due to the number of base stations. - Coverage extended as a result of base station number. - Link switch possibility. - Require special transceiver hardware to exchange data with Base Station.	- Costly. - Not always operational as it necessitates a prior existing infrastructure. - Vulnerable to attacks targeting GCS and base stations (packet forwarding attack [49]). - Ineffiency of UAV-to-UAV communication.
UAANET Architecure	- Bandwith can be reused more frequently and thus more efficiently. - Efficiency of UAV-to-UAV communication - Coverage extended due to the number of UAVs. - Possibility of using COTS off-the-shelf hardware. - Scalability. - Network reliability (failure of one node does not affect the system).	- Vulnerable to network attacks. - Need to set up a pre-determined mobility pattern, auto-configuration and an initial auto-formation techniques for the network. - Need to set up swarm intelligence for UAVs.

Table V
COMPARISON OF UAV COMMUNICATION ARCHITECTURE

Table V summarizes the major strengths and weaknesses of the different communication architectures discussed above.

C. UAANET Projects

In order to investigate the UAV ad hoc paradigm, research projects and industry efforts have been started as explained in the following. In [50], Chaumette, S., et al. presented the CARUS project (Cooperative Autonomous Reconfigurable UAV swarm). CARUS aims to find a group of target points located on the ground with a swarm of 5 UAVs. Consequently, a UAANET is deployed with 6 nodes (5 UAVs and the GCS). Each UAV of the swarm cooperates with each other to achieve the mission objective. Each UAV is responsible for decision to perform a specific task when approaching the target. These UAVs exchange periodically with their respective neighbor information concerning the zone structure to survey. They also exchange their previous searching zone, so that each node concentrates only on a new area which has not yet been scanned. A distributed delay routing protocol with a broadcast asynchronous communication mode has been used to allow nodes to exchange data traffic. Each swarm member has a unique ID for collision avoidance and way point resolution. A formal model has been used to validate the correctness of algorithms managing the distributed broadcast-based communication approaches.

In [28], an ad hoc UAV-Ground Network is described. The AUGNet project consists in forming an ad hoc network with ground nodes and a swarm of UAVs. The objective is to use the UAANET to increase the communication range of ground nodes. The swarm of UAVs is used as a gateway for the ground disconnected network. A specific mesh network radio is embedded within UAVs to run a modified version of DSR (Dynamic Source Routing) [51] routing protocol. DSR is modified to include embedded monitoring and to address the specific UAANET requirements.

In [52], Kai Daniel et al., describe the AirShield project, which aims to deploy a network architecture for multiple micro UAVs for disaster supervision. They capitalize the fact that using a swarm of UAVs during critical missions improves the data transmission rate and delay. The objective is to enable small delays for the control packets and high data rates for the payload traffic. The deployed UAANET network architecture includes three interdependency algorithms to ensure high reli-

ability. An inter Drone links (IDL) maintains a mesh network between nodes by exchanging topology information (it is also used to transmit payloads among neighbors). Secondly, a Drone-to-Ground-Station Links (DGSL) is used to share UAV related information (telemetry, speed, power levels) to the GCS. Lastly, a back end network topology communication subsystem is used to ensure efficient communication between the different components of the back-end system.

In [53], the Sensing, Unmanned and Autonomous Aerial Vehicle (SUUAVE) project is described. The aim of the project is to deploy a collaborative communication architecture between UAVs for rescue mission. The aim is to minimize the total delay for the target search and identification. The communication architecture uses the 802.11 protocol and implements the multi-agent Partially Observable Markov Decision Process (POMDPs) [54] for network routing. Moreover, a decentralized algorithm for multiple UAVs management is designed to search, detect and locate mobile ground targets [55].

In [56], Sabine Hauert et al., describe the SMAVNET (Swarming Micro Air Vehicle Network) project, which aims to develop a UAV swarm that can be deployed in an inaccessible area hit by a natural disaster. The project aims to propose a partially connected mesh with ad-hoc network topology that enables UAVs to create multi-hop communication with the GCS. To exchange data packets between nodes, the author proposes a new UAANET routing protocol called : P-OLSR [11] based on the well-known OLSR protocol [57]. P-OLSR tries to predict the UAV movements and forwards the packet to UAVs that will travel to the destination (discussed in detail in section IV).

In [32], the Secure UAV Ad hoc NETwork (SUANET) project is presented. The project aims to propose a secure ad hoc communication architecture of UAVs. It has three technical objectives. The first is to define a key management mechanism within UAANETs to enable deployment of multiple keys between UAVs, which will be used to implement authentication, confidentiality and integrity services. The second objective is to design a secure routing protocol for UAANETs in order to guarantee that all UAVs collaborating in the routing process are authenticated and able to find the shortest path toward the destination quickly and efficiently. The final aim is to design an additional mechanism on a layer other than the network layer to secure data communications between UAVs. The SUANET project is currently the only known project that investigates routing protocol security. It brings together the French company Delair-Tech[4] and the French civil aviation university ENAC[5]. Related to SUANET, a performance evaluation of existing MANET protocols in a UAANET realistic scenario has been investigated in [33] and a secure routing protocol design through model driven development approach is presented in [34]. An extended verification of the secure routing protocol is detailed in [58]

[4]http://www.delair-tech.com/

[5]http://www.enac.fr/

To summarize, cooperation, control and communication architecture and QoS improvements are the primary aspects investigated in existing UAANET projects. There are no existing UAANET security-related projects other than SUANET. We summarize in Table VI the objectives and the features of existing UAANET related projects.

D. UAANET characteristics

Similar to MANETs, the UAANET architecture is an infrastructure-less network which uses multiple nodes to forward data packets. It also shares other characteristics such as self-organized abilities, self-managed information in a distributed fashion, communications and cooperation between nodes to perform data delivery. However, UAANETs also have some specific features that differentiate them from MANET :

1) **Network connectivity**: The intermittent degree of UAANET network connectivity is more significant than in MANETs or VANETs [14]. This mainly results from UAV mobility. The interruption of the communication could be critical when transmitting important information (control/command traffic). In addition, UAV failure may cause connectivity failure, which results in routing failure, and therefore communication failure or longer delay. Another aspect that affects connectivity is connection outages. Due to UAV movements and variations of distances between UAVs, link quality fluctuates and may cause loss of connectivity and performance degradations.
2) **Number of nodes** : When a UAV deployed in a given mission has a relatively high speed, it can be sufficient to cover a restricted mission area. In such a case, the need for a large number of UAVs is not justified. Usually, a UAV mission involves an average of 3 to 4 UAVs [52] [53].
3) **Sufficient energy**: Depending on their size and type, UAANETs nodes are usually assumed to have enough energy and computing power compared to nodes in MANETs. This is due to the fact that the level of energy required to move an UAV is much greater than the energy needed to compute data.
4) **Mobility (3D)**: The mobility model plays a significant role in designing network protocols for ad-hoc networks. UAV mobility patterns are different from those of other vehicles. A UAV movement is above all three dimensional. This brings challenges at the physical level, for antenna behavior and for security (e.g., misbehavior detection). On the last point, several existing misbehavior detection techniques often rely on node position to determine if their refusal to forward data packets is justified. The existing techniques take into account their position based on 2D. Thus, a study should be performed to take altitude information into account in the misbehavior detection algorithm. Furthermore, depending on the mission, the UAV movement can follow different types of pattern. It can be straight following a waypoint, circular staying in a specific zone, or oval and scan when patrolling around a given circuit. Accordingly, an

Project	Objective	Features
CARUS	Target Search	- Nodes: swarm of 5 UAVs and GCS - Ground visualization algorithm - Delay routing protocol with broadcast asynchronous communication mode
AUGNET	Relay for ground network	- Use of DSR routing protocol - 802.11b data link
Airshield	Disaster supervision	- QoS enhancement- Use of interdependencies - Three data links to ensure high reliability - An inter Drone link to maintain a mesh network between UAVs - A UAV to Ground station links is used to share UAVs related information to the GCS - A back end data link is used to ensure efficient communication between the different components of the back-end system.
SUAAVE	Rescue mission	- 802.11 data link - Multi-agent Partially Observable Markov Decision Process (POMDPs) algorithm implemented for data exchange between nodes
SMAVNET	Inaccessible area supervision	- Partially connected mesh ad-hoc networks between UAVs - P-OLSR used as UAANET routing protocol
SUANET	Secure ad hoc communication architecture	- Define a key management mechanism within UAANETs to enable deployment of multiple keys between UAVs. - Secure routing protocol for UAANETs - Secure payload traffic exchanges between UAVs

Table VI
EXISTING UAANET PROJECTS

innovative approach has been proposed in [59] where the author provided a mobility pattern for UAVs based on real traces. An illustration of this mobility model is shown in Figure 5

5) **Environment**: In the majority of MANETs, nodes usually move close to the ground (like in VANETs or sensor networks). As UAANETs are composed of flying nodes, they usually move in large free spaces. Consequently, the free-space path loss model is often used to model the physical layer. Nevertheless factors like large obstacles, ground reflections or weather conditions can affect connectivity between UAVs. The propagation model used should take into account these factors.
6) **Strict delay constraints**: Generally, UAANETs are used for real-time applications, such as aerial photography and video capture. Accordingly, the control/command traffic should arrive on time and be computed by the UAV with small latency to avoid loss of control.

Table VII compares UAANETs with other types of ad hoc network such as VANET, AANETs and MANETs.

E. UAANET Applications

Multiple UAV application scenarios range from commercial or humanitarian to experimentation for research and development. In this section we provide a non-exhaustive list of UAANET applications. Indeed, UAVs can be used reasonably for several operations since they are portable and cheap to run. We believe that as soon as the regulations preventing free UAANET deployment are lifted, it is just a matter of time before UAANETs enter service in many fields.

1) UAANET for surveillance: A UAANET can be used to perform surveillance of an area struck by natural disaster.

It can also be used for *industrial infrastructure surveillance* in order to detect potential failures or dangers. For example, to inspect large power-lines for electricity companies. Such tasks have been undertaken by manned helicopter in the past, which is considered an expensive solution and potentially dangerous for the pilot. Data (image, video) traffic is forwarded node by node and sent in real time to the operators to allow them to take decisions in unusual situations. Mini-UAVs can also collect data on the ground (concentration of certain gases or radioactivity for instance) using special sensors and forward the data to the GCS.

2) UAANET for environmental monitoring : It is also possible to use UAANETs for meteorological and environmental measurement. In such cases, small UAVs are scattered in the airspace and follow a zone perimeter. The objective is then to ensure data precision. According to the payload type onboard, the UAV can take aerial photographs, produce thermal mapping, measure concentrations of gas or radioactivity and wind speed.

Another application is monitoring a natural phenomenon such as volcanic eruption for instance. Since human intervention is not possible in these situations, a UAV swarm can capture the required information and send it to the GCS for processing.

Another UAANET use related to Research and Development is wildlife research. A UAV swarm can be used to monitor and track wildlife, providing information such as animal behavior and protection from proachers and other predators. With thermal payload sensors, UAANET can be deployed at night to have a better view of wildlife.

3) UAANET for humanitarian applications : UAANET communication can also be used for search and rescue operations in order to find lost or trapped humans after events such as a natural disaster. Indeed, with thermal sensors, UAANET allows rescuers to quickly discover the location of lost persons even in a large and challenging zone (e.g., cliffs). In this context each node monitors a portion of the target zone and shares data to dynamically move to another location.

UAANET can also be used to provide communication support for stricken areas where there is no telecommunication

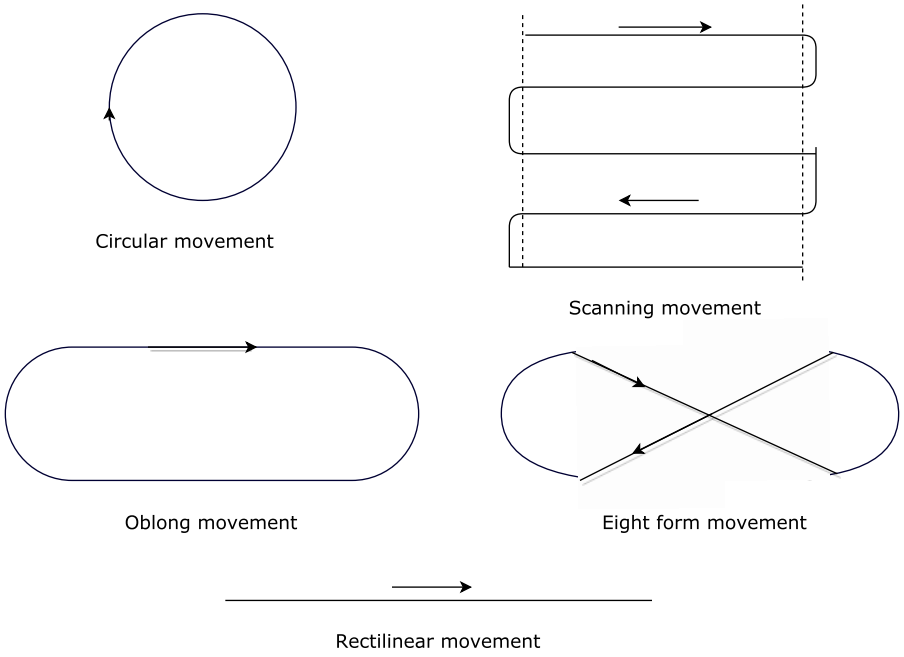


Figure 5. Illustration of PPRZM mobility models

	MANET	VANET	AANET	UAANET
Mobility model	- 2D - Random	- 2D - Regular - Mostly linear trajectory	- Can be 2D and 3D with regular linear trajectory	- 3D - Can be predetermined - Realistic mobility model (e.g. Paparazzi Mobility Model)
Node speed	Low	High	Very high	Very high
Propagation model	- On the ground - No LOS	- On the ground - Depends on the application, can be LOS and no LOS	- In the air - LOS	- In the air - Depends on the application, can be LOS and no LOS
Energy capacity	Low	High	High	High (depends on UAV size)
Node speed	Low	High	Very high	High
Number of nodes	High	High	Low	Low
Security requirements	Low	High	High	High
Network topology update	Infrequent	Frequent	Frequent	Frequent

Table VII
DIFFERENCE BETWEEN MANET, VANET, AANET AND UAANET

LOS: Line of Sight

infrastructure. In such a case, UAVs must be placed in a pre-planned location and perform a specific task following a pre-programed mobility pattern (circular, way-point) [60].

4) Data Measurement: UAANETs can be used for mining where each UAVs are dispatched into the mining area and equipped with specialized payloads. Each UAV can inspect pit walls or compute a map in 3D and forward it to the CCS. In addition, UAANETs can also be implemented for monitoring construction sites where they can provide an aerial view of the project. For this application, a small number of UAVs may be sufficient depending on the size of the construction site. UAVs can therefore perform 3D aerial photography of inaccessible points.

Another UAANET use is *the agriculture monitoring* for crop monitoring, crop sowing and spraying. The principle is to survey the field to identify any malicious intrusion but also to evaluate the crop state for harvesting using a special sensor. Crop survelillance is performed by infrared cameras to detect crop color changes. Information on crop health would allow farmers to react and improve conditions locally with fertilizers and insecticide.

F. Physical and Medium Access Control Requirements for UAANETs

Physical and MAC layers are not the focus of this paper. However, it is helpful to briefly introduce some of the aspects of UAANET Physical and MAC technologies that exist in order to understand the assumptions selected on the lower level of the existing UAANET routing protocol.

The UAANET physical layer deals with the radio propagation model and the antenna structure used. While the propagation model depends on many factors (variations of distance

between two nodes, ground reflection effects, environmental conditions, interference, etc.) [13], an antenna structure can be either omnidirectional or directional. Each provide a different level of routing protocol efficiency [61].

Furthermore, the crucial role of the MAC layer in UAANETs is to provide an interface protocol and parameters for high-speed UAV communication using one or more of the available transmission channels. It must also satisfy the latency requirements of data traffic that have different priorities. This is why traffic classes in/within UAANETs should be differentiated. [62]. It is important to underline that the 3D features of UAANET mobility patterns which differ from MANET mobility patterns (2D) must be considered when designing MAC technology for UAANETs [63].

The major problem that arises in MAC layer in ad hoc communication is transmission collision management. Different MAC layer protocols have been proposed in MANETs [64], but due to the high mobility and fast topology changes of UAVs, their use in UAANET is not suitable [65]. For example, it is not possible to reserve the transmission channel before the sending process when Carrier Sense Multiple Access (CSMA/CA) is used. In general, the control traffic requires a low delay and high availability. The well-known IEEE 802.11 standard [66] is widely used in some UAANET projects as quoted previously. However, it raises a problem of interference in urban areas since the standard is used by many mobile devices (mobile phones, laptops, etc.).

Nonetheless, other types of MAC protocols have recently been specifically proposed for UAV communications such as the Common Data Link (CDL), Tactical Common Data Link (TCDL), Link-11, Link-14, Link-16, and Link-22. For a detailed description of these MAC technologies, see [15]. However, most of these protocols have been developed for military usage and their application on small UAVs for civilian applications still needs to be investigated. .

From standard perspective, unlike VANETs, there is currently no UAANET standard to homogenize UAANET deployment. Such a standard would be helpful to define a protocol stack for future developments. That is already the case for VANETs as: DSRC (Dedicated Short Range communication) [67], WAVE (Wireless Access in vehicular Environments) [68] and IEEE.802.11p [69] are used to allow interoperability between different manufacturers. The research and standardization entities are still working on such standards for UAANETs, which means that interoperability issues are yet to be solved. As a result routing protocol, a main component of the protocol stack in any MANET network, needs to be defined. In the next section, we provide an in-depth analysis of such UAANET routing protocols and discuss their challenges.

IV. Routing protocols in UAANETs

To perform UAANET missions, UAVs and GCS must relay control and data traffic. Accordingly, an adapted UAANET routing protocol is required to find routes between nodes in a timely manner. This routing protocol must take into account the UAANET specific features as stated in Section III-D to ensure efficient communications between UAVs and the GCS. For instance, a noticeable delay during transmission must be avoided as control traffic flows in real-time between entities. Indeed, if a control packet forwarding process is delayed, it can create instability and therefore unexpected behavior of the UAV swarm.

In order to design such routing protocol, there are two possibilities. Either it can be created from scratch by defining how route discovery, packet forwarding and route maintenance will be performed, or an existing routing algorithm which has been initially proposed for MANETs can be adapted to meet UAANET requirements. The first approach would allow a routing protocol design that covers all UAANET specific features. However, the second design choice has attracted greater research attention since it offers the advantage of sustaining interoperability between other types of nodes (e.g. ground vehicles, sensor nodes) in case a UAANET is deployed to extend ground node communication [28].

As a result, most existing UAANET routing protocols are an extension of the following well-known MANET routing protocols: Ad-hoc On-demand Distance Vector (AODV) [70], Optimized Link State Routing Protocol (OLSR) [57] and DSR (Dynamic State Routing) protocol [51]. Nonetheless, it should be noted that there are some routing protocols that have been built from a new concept taking into account UAANET requirements.

From a practical perspective, all the protocols discussed in this paper have their own advantage in a specific test scenario where they outperform their competitors. As a result, no single protocol outperforms the others. The main purpose of these protocols is similar as they seek to maximize throughput and minimize packet loss and control both overhead generated by the protocol itself and end-to-end delay. The difference lies in the priority given to these metrics based on the user application.

In this paper, a survey of main routing protocol approaches for UAANETs is presented by introducing a taxonomy of UAANET routing protocols. We have divided the UAANET protocols into five categories: (i) reactive, (ii) pro-active, (iii) hybrid, (iv) geographical routing and (v) hierarchical. For each of these classes, we have reviewed and given feedback on their strengths and weaknesses while considering UAANET requirements.

A. Taxonomy of UAANET routing protocols

In this part of the paper, we will illustrate a taxonomy of UAANET routing protocols. There are different methods to construct a taxonomy. Here the approach is to classify the protocol based on their routing strategy.

- Reactive (Source-initiated)
- Proactive
- Hybrid
- Hierarchical
- Geographical

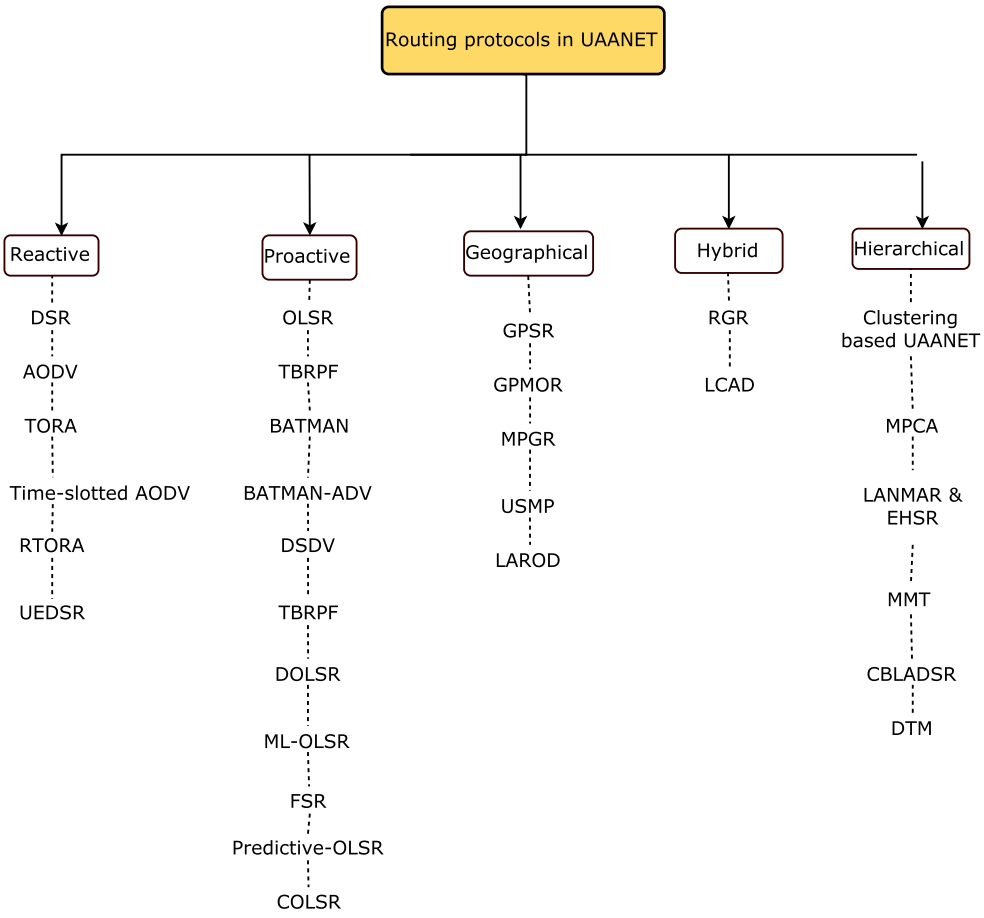


Figure 6. Categories of UAANET routing protocols.

B. *Proactive routing protocols*

Proactive routing implies that each node maintains fresh network state information with all nodes before sending data packets. It requires that each node relays control packets periodically. As a result, all nodes always have a route to join any node in the network. Typically, a routing table is required so that nodes can establish routes based on a predefined criteria. Among these criteria, we can mention the shortest path metric, the forwarding delay between nodes or the bandwidth size of the calculated route [71]. It is important to underline that this category of routing protocol uses either a link state or distance vector routing strategy. As depicted in [71], this class of routing algorithm is not well adjusted for highly dynamic and low density networks like UAANETs because of the large amount of packet overhead generated. The overhead tends to increase proportionally with the number of nodes and the mobility degree. There is also a negative impact on energy level as nodes do not have an idle phase and continuously listen to the wireless medium. In [33], it was proved that under UAANET realistic scenario, proactive protocols tend to generate too much overhead compared to reactive protocols. However, in spite of these drawbacks, proactive routing has the advantage of offering fast connections between nodes since routing information is immediately available in the routing table, so there is no delay when data traffic has to be sent. The existing UAANET proactive protocols are summarized in Table VIII.

1) Proactive MANET routing protocols used in UAANETs:

a) OLSR: Existing studies [72] [73] [74] [33] have been conducted during simulation experiments in order to assess OLSR performance within a UAANET environment. Clausen et al. designed the OLSR algorithm [57] which is a unicast and link state routing algorithm that build routes regardless of data packet transmission. In OLSR, each node declares their direct links with only a subpart of their neighbors to create a neighbor list. This list is created thanks to the periodic exchange of Topology Control (TC) packets and Hello messages between neighbors. After building a neighbor list, each node selects one node as Multi-Point Relays (MPRs). Only these MPR nodes can generate link state information and forward data packets to other MPRs. According to [33] [74], compared to AODV and DSR, OLSR has a slightly better performance in terms of end-to-end-delay in UAANET environments. This can be explained by the continuous exchange of Hello and TC packets which inform UAVs of all possible paths to join a given destination.

However, the overhead generated by OLSR and its ability to find a new route following a route loss is inferior to AODV. This is caused by the repeated broadcast of multiple packets (Topology Control, Hello, MAC control, etc) between UAVs under high data rates.

b) TBRPF (Topology Broadcast based on Reverse-Path Forwarding): TBRPF [75] is a proactive MANET link-state routing protocol, which provides communication through the shortest path metric. With TBRPF, using the Dijkstra algorithm [76] each node computes a source tree that is based on partial topology information stored in a topology table. This source tree contains the link state information to all reachable nodes. A combination of periodic and differential updates is used to disseminate the source tree. This enables smaller sized Hello packets to be sent if there is not much topology change in the network. Moreover, TBRPF allows each node to quickly detect neighbors with a bidirectional link requirements mechanism. It therefore detects when the current link breaks or becomes unidirectional (asymmetric). According to [77], TBRPF can induce less overhead compared to OLSR when used in UAANET environments, but can still suffer from inaccurate routing information with a high degree of UAV mobility. Similarly, in [46], a UAANET field experiment has been conducted with TBRPF protocol. Their metric based on minimum hop count gives inconsistent route discovery results. This is because of the oscillation of the wireless interface which is not considered. Consequently, the work in [46] supports the idea of introducing link quality as part of the routing metric to discover routes. This approach should be tested in UAANET environments to assess network performances.

c) BATMAN /BATMAN-ADV (Better Approach To Mobile Adhoc Networking) [78]: BATMAN introduces routing loop management to handle high node density while inducing low processing and traffic cost. BATMAN algorithm also has a particularity of not discovering the entire network topology, but only learns of its direct neighbor by exchanging a BATMAN control packet also called "Originator Message" (OGM). During topology discovery each node maintains only the link which offers the best route towards all other nodes by exchanging OGM packets. OGM packets are small with a typical raw packet size of about 52 bytes, including IP and UDP overhead. During data forwarding, a sender computes the number of OGM packets received from its neighbors and picks one neighbor that had sent more regularly and which has a fresh sequence number value. This neighbor is then selected as next hop toward the destination node.

Furthermore, BATMAN advanced (shortened as BATMAN-ADV) is an improvement of the B.A.T.M.A.N routing protocol by the creation of a kernel module that operates in the kernel stacks. As a result, the routing information is no longer encapsulated within a UDP socket, but within raw ethernet frames. Thus, all nodes have a link which local and unconcerned with any topology changes.

BATMAN has been used in UAANETs either in simulation [79] or real word implementation [80]. In [74], Pojda et al, have analyzed the performance of four mesh routing protocol implementations (Batman, Batman advanced, OLSR and OPEN80211s [81]) in a UAANET scenario in which 2 control stations maintain the same geographical position and 2 UAVs cover a specific zone. The purpose of their study was to compare BATMAN performance in the context of a UAV swarming application. Based on this scenario, their results show that within a low entity network, the layer-2 protocols (open80211s and BATMAN-ADV) outperformed the layer-3 protocols (BATMAN and OLSR) in terms of goodput and packet loss ratio. This can be attributed to the reduced control overhead and routing oscillation generated by layer-2 protocols.

d) DSDV (Destination-sequenced distance vector): DSDV (C. Perkins and P. Hagwat, 1994) [82] is based on the Bellman-Ford algorithm. It adds two parameters to distance-vector routing. The first is the sequence number parameter which helps to avoid routing loops, and the second is the Damping parameter which holds advertisements for any topology modification of short duration.

Moreover, DSDV exchanges two types of packet: full dump packets and incremental update packets. Full dump packets carry all routing table information and infrequently transmitted over the network due to its size. As for incremental update packets, they are used to bring in new information since the exchanged of last full dump packets.

DSDV is used for UAANETs in [83]. The author objective was to assess LANMAR [84] routing protocol performances compared to DSDV. LANMAR routing protocol combine landmark ad hoc routing techniques and a hierarchical scheme that includes backbone architecture (further discussed in section IV). The results show that DSDV eliminates routing loops and problems caused by counting to infinity problems in the network. However in terms of end to end delay, DSDV suffers from the long delay to reassemble the latest updates. Indeed, before beginning routing process to join any destination, each node must wait for all latest updates from neighbors to reset the local routing table. In addition, in order to decide between full-dump packets and incremental packets, a UAV must continuously listen to events within the network (for instance, if there was a radical change with the topology). This can generate excessive packet control that could saturate the network under high workload.

e) FSR (Fish State Routing): The FSR routing algorithm (Guangyu Pei, Mario Gerla and Tsu-Wei Chen in 2000) [85] is an enhanced version of the GSRP (Global State Routing Protocol) [86]. It is based on fish vision which captures the points near the focal view in great detail. It aims to reduce routing update overhead by decreasing routing table update frequency with distance to destination. It means that updates are generated more frequently for near destination nodes compared to distant destinations. It maintains accurate routing information for direct neighbors and progressively less detail as distance increases.

The major strength of FSR lies in decreasing overhead within small size networks. However, it still suffers from rout-

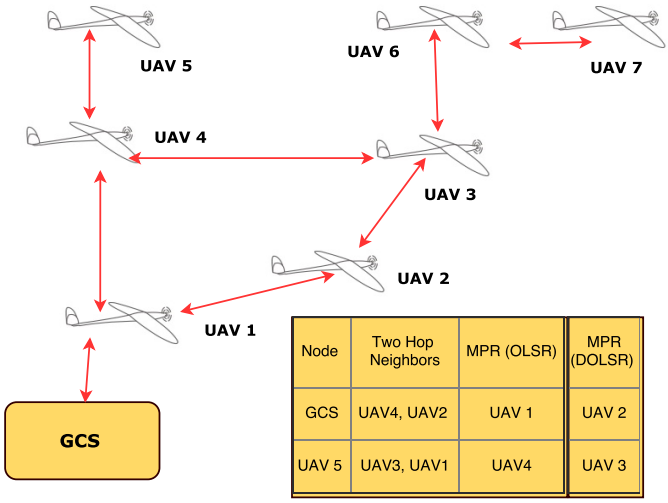
ing table overflow with higher network size. This might induce out of date path to distant destinations. Another noticeable drawback is its non-optimal management when dealing with the destination node that is out of range of the source node. In such a case, it would take too long to search a route and might never find the full path to the destination node. A potential solution would be to implement the DTN algorithm to keep the message during the routing process and to transfer it to neighbors when there is a communication opportunity. In [87] FSR is assessed in a new UAANET testbed called UCSS (UAV Communication Simulation System). The main concern of this study is to evaluate the testbed rather than FSR performance.

2) Proactive UAANET routing protocols:

a) DOLSR (Directional Optimized Link State Routing Protocol): The DOLSR [88] routing protocol is an extension of OLSR protocol. It makes the assumption that each UAV of the swarm is equipped with a directional antenna to improve the communication range. In this work, Alshabtat, Abdel Ilah, et al. capitalize on this capability to reduce the overhead by minimizing the number of MPR (Multi-Point Relay) nodes compared to the usual OLSR MPR selection. An illustration of MPR selection with DOLSR is depicted in Figure 7. In this figure, all nodes are equipped with a directional antenna. Accordingly, these nodes cover all the unreachable two-hop neighbors. The GCS will build its routing table based on the OLSR selection (as shown in Figure 7). Accordingly, the GCS has two routes to reach UAV3 either through UAV1 and UAV2 or UAV1 and UAV4. In this situation, DOLSR scheme computes the distance between the GCS and nodes UAV2 and UAV4; and takes the longer one. If we assume that UAV2 is the further from the GCS than UAV4, then UAV2 is considered as a MPR for the node GCS. The same approach is applied for UAV5 and the others.

DOLSR has the advantage of optimizing end-to-end delay which is beneficial for real time data traffic. It also offers enhanced security compared to unidirectional protocols by leveraging its robustness to signal jamming. However, its hardware requirements do not allow its use when UAVs are only equipped with omnidirectional antenna. Moreover, as in general proactive routing protocols, the periodic exchange of topology control consumes power and bandwidth resources. This can be an issue for a UAV which has low power capacity and computation embedded devices (e.g., PPZUAV [89]).

b) P-OLSR: Predictive-OLSR (P-OLSR) [11] is another extension of OLSR protocol. As its name suggest, it consists of predicting the quality of links between UAVs and choosing the one that gives the smallest percentage of datagram loss. Rosati et al, introduce another routing metric called Speed-Weighted ETX (Expected Transmission Count) based on the usual ETX [90] to select the best route. This routing metric combines the link state information and the relative speed between two UAVs (speed, position and direction of the UAV compared to its neighbors). The UAV obtains this information through GPS devices embedded on board . Likewise, as in original OLSR, each UAV broadcasts a Hello message to advertise link state information in order to detect neighbors. The Hello packet is



Node	Two Hop Neighbors	MPR (OLSR)	MPR (DOLSR)
GCS	UAV4, UAV2	UAV 1	UAV 2
UAV 5	UAV3, UAV1	UAV4	UAV 3

Figure 7. Illustration of multipoint relays in DOLSR

redefined by adding GPS information (position and direction information) of the sender.

P-OLSR, by its prediction algorithm copes well with the dynamic topology of UAANET. Indeed, the speed-Weighted ETX takes into account UAV velocity and the speed between two neighbors. As a result, the intermittent connectivity is reduced. Nonetheless, the computation might be heavy for some CPU and thus the protocol is unable to calculate in real time the prediction algorithm, which is required. This can induce an inconsistency between the real topology and the predicted computation result. UAV mobility also significantly affects the performance evaluation of this solution. To be effective, a specific mobility model is used which may change in real-implementations. A possible extension of this work would be to integrate a set of realistic mobility model as has been proposed in [31].

It is important to underline that a real experiment with two UAVs and one GCS had been carried out. The results show that P-OLSR outperforms OLSR in terms of goodput and outage time rate. P-OLSR tends to react well in case of topology changes. However, the network settings lacks realism with only 3 nodes. The node density should be increased to evaluate the protocol because of its proactive features. In Figure 8, the topology construction in P-OLSR is shown.

c) Mobility and Load Aware OLSR (ML-OLSR): ML-OLSR [91] is a proactive routing protocol based on OLSR that improves on three important features: MPR selection algorithm, neighbor discovery and route selection process. It uses mobility aware and load aware algorithms to select neighbor and route data packets.

Firstly, the mobility aware algorithm takes into account the mobility pattern and uses two new routing metrics called the Stability Degree of Node (SDN) and Reachability Degree of Node (RDN). On the one hand, the SDN represents the

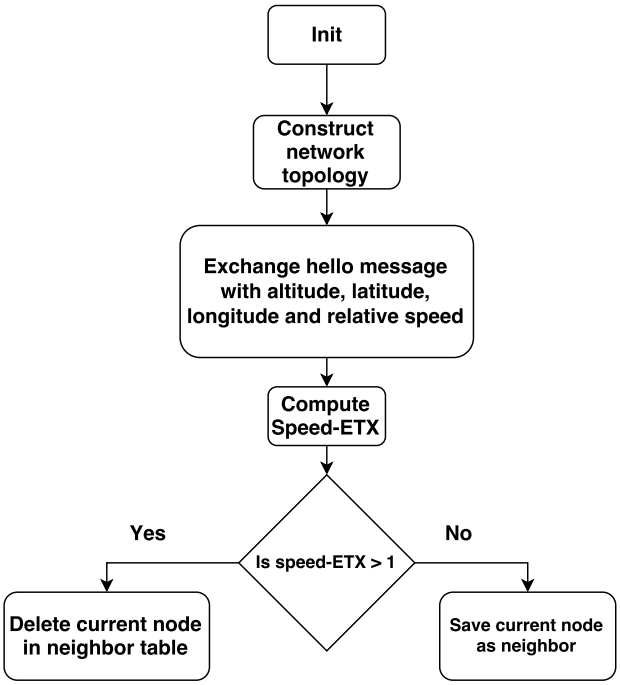


Figure 8. Topology construction in P-OLSR

connection stability of the communication link between nodes. It represents the metric (also called weight) of the link between two UAVs. Given that, the objective is to select the most stable node, SDN selects the node which possesses the smallest distance to its neighbor. On the other hand, the RDN represents the weight of the nodes. This value represents the number of nodes that have selected the current node as the most suitable (stable) one.

Secondly, the load aware algorithm is added to compensate the problematic feedback when using IEEE 802.11 mechanisms. It avoids the scenario where a sender has entered data into a buffer before retrieving communication in cases of medium contention. It helps to optimize the packet delivery ratio and transmission delay during packet collision.

Furthermore, in ML-OLSR, the location information[6], the SDN value, and the mac factor (load aware algorithm metric) are added to the Hello packets. Typically, upon reception of hello packets, each UAV computes the SDN, RDN and the load aware weight. As a result, each UAV will be aware of the distance, load information, and mobility pattern of its neighbor. As with the MPR selection process, the stability of network topology is included in the metric choice by considering the SDN and the mac factor value of one hop away neighbors.

ML-OLSR routing protocol can help to find the most stable route because it avoids selecting nodes that have a tendency to have an unpredicted movement as MPR. Consequently, it can provide a higher packet delivery ratio than OLSR with an acceptable end-to-end delay. However, a noticeable drawback of ML-OLSR is its energy efficiency. The mobility and load aware algorithm require more computation by the CPU. Another drawback of ML-OLSR is also the beacon message size which increases with UAV movements. Indeed, each time a link between two UAVs A and B fluctuates, it generates a new value of SDN(AB) and RDN(AB), which must be encapsulated within a hello packet to be disseminated within the network. As a result, protocol overhead may increase drastically if disconnection is frequent.

d) Contention-Based Optimized Link State Routing Protocol (COLSR): In [65], The COLSR protocol is proposed by Yan Li et al. It is a cross layer protocol based on geographic information that combines network, link and PHY layers for cooperative communication. A network-link cross layer mechanism is used for routing selection while a link-layer cross layer mechanism handles relay selection. Unlike OLSR, a periodic exchange of Hello packets is necessary as complete neighbor information is not required. It rather uses two beaconless techniques : namely Beaconless Greedy forwarding (BGLF) and Beaconless Recovery Forwarding (BLRF) for route selection.

Firstly, the source node sends broadcast data packets following the BLGF algorithm to find the best forwarder among its neighbours. The first node with an expired timer gives maximum progress toward the destination and is selected as the best forwarder. This selected node then sends a clear to forward (CTF) message to the source. The other candidate nodes overhearing the CTF message will halt their timer and switch to idle state. To avoid the hidden terminal problem, the source node sends a message SELECT after receiving the CTF message.

Secondly, BLGF may suffer from a local minimum problem [92]. In such cases, the Beaconless Recovery Forwarding (BLFR) algorithm is activated to apply the Beaconless Forward Planarization algorithm (BFP) [93] which consists of choosing the next hop following a graph planarization principle [94]. In the situation if the next hop cannot forward the message properly after a given period of time, a relay selection is performed to find another next hop. This is done by the MAC-Phy cross layer mechanism. During this process, a new timer is configured. The metric used is based on the SEP (Symbol Error Probability) metric [95] which is computed from each neighbor candidate. The node that provides maximum coding gain and minimum SEP is selected as the next hop. An evaluation study shows that COLSR achieves a lower packet error rate and throughput than the traditional geographic protocol BOSS [96]. BOSS is a beacon-less on demand strategy for geographical routing. It uses a three way handshake mechanism to select and forward messages in a similar way to the RTS/CTS scheme used in IEEE 802.11. It uses the data packet being routed to discover neighbors.

The major strength of COLSR protocol lies in its cross layer features between network, link and Physical layers which allow data related to the UAVs (altitude, speed, pitch, roll and the like) to be considered. Another advantage is the spatial diversity concept among distributed nodes. The interaction between link and network layers gives a better insight into

[6]Obtained thanks to a GPS on board of UAVs

configuring link and network parameters.

Nonetheless, a synchronous timer between nodes should be set so that the algorithm operates properly.

C. Reactive routing protocols

In this type of routing protocol, a route is created only when a node wants to send a packet to a destination node. To search for a route, a node first sends a route request packet which will be broadcasted through the network. When a node receives the route request packet, it adds its address to the list of nodes that have processed the packet. When one (or several) route request packets reach the destination node, a route response packet is sent back to the source using the shortest route discovered. The source node uses this route to reach the destination. The existing UAANET proactive protocols are summarized in Table IX.

1) Reactive MANET routing protocol used in UAANETs:

a) AODV (Ad hoc On Demand Distance Vector) : This is a popular reactive protocol, used by many researchers in literature in MANETs as well as in UAANETs. For AODV, the route is only calculated when there is a need to send data packets. During the route discovery process, the initiator node checks its routing table if a route has been established in the past for the destination node. If such a route exists, the data packet will be sent through this route. However, if it does not exist, a route request is initiated using a request packet (RREQ: Route REQuest) and a response packet (RREP : Route Response). During route maintenance, a Hello message is sent periodically one hop away to ensure link connectivity.

According to [33], AODV outperformed OLSR and DSR in terms of end-to-end delay, packet delivery and time to retrieve a new route after route loss in a realistic UAANET scenario. This is justified by the reactive nature of its topology changes and its limited overhead. Similarly, in [73], under a UAANET scenario, AODV has slightly better performance than OLSR in terms of packet delivery ratio, but can create higher delays wit low workload. However, it is important to underline that this evaluation is based on simulations and does not consider real system related issues. In addition, it considers a large number of nodes using unrealistic mobility patterns (e.g Random waypoint).

b) DSR (Dynamic Source Routing): DSR is a source routing protocol, which means that the whole path of a data packet is placed in the packet header. In source routing, only the sending node determines the complete sequence of nodes through which data packets will be sent. The complete path is then included in the packet header. It is worth noting that during route discovery, if an intermediate node does not have a route in the source node, it broadcasts the packet after appending its own address in the source route. It also kept and save the request ID for a further reception to prevent the packet from being forwarded over and over again in the network. The intermediate node can discard the message if the message has the same ID as a message that the node has already seen previoulsy or if it finds its own address in the route record. DSR is used by many UAANET implementations [33]. In [28], it is used in a real environment to create an ad hoc network between UAVs and multiple Ground Control Stations. Their objective is to communicate moving ground nodes with multiple UAVs forming a UAANET. Their results show that DSR tends to generate a significant amount of overhead and adds latency due to the need for link-level acknowledgement in each packet sent. Such performance is justified by the source routing of DSR. The full path is included within the packet and creates latency.

c) TORA: The TORA (Temporally Ordered Routing Algorithm) is an on-demand routing protocol that has been proposed in [97]. The principal feature of TORA is to limit control message propagation. It is based on Link Reversal Algorithms and works with the height metric. It mostly finds multiple routes between source and destination. The idea is to create a Directed acyclic Graph (DAG) within each node with the "height" metric before searching for a route. It is important to underline that time synchronization is required between the source and the destination before creating a DAG.

Moreover, TORA uses three types of messages: The query packet for route discovery, the UPD packet for route maintenance and the CLR packet for route deletion. To create a route, a query packet is created and broadcasted across the network. Upon reception, each node along the way increases its height by one. At the same time, each node verifies if it has a downstream link to the destination. Then, it decides whether it will send back a reply packet to the source or drop the packet. When the reply packet is captured in the source, it revises its height and verifies whether it has already received the current reply packet. If not, the packet is accepted and its height is compared to another reply packet. The one that characterized less height is assigned as the valid packet, and the route is created.

Furthermore, it should be noted that a route maintenance process is triggered when the last link towards the destination is lost. The purpose of route maintenance is to reverse some of the links, so that the network reorients itself to a state where each node has a path to the destination. The process consists of adjusting height levels and propagating the updates through the network. It might also be necessary to re-calculate a DAG to create a new route. In case of route deletion, all the information related to the deleted route is flooded across the network in broadcast mode to erase all paths that contain that route.

TORA is used for UAANET in [98]. A noticeable advantage of TORA is that it only creates a DAG when necessary. Thus, it generates less overhead within the network. Moreover, multiple paths are created and can be used when the current path is lost. However, the time required to build the DAG is harldy negligible when the network is dense.

2) Reactive UAANET routing protocol: In this section, we will give an overview of reactive routing protocols that have been proposed explicitly for UAANET.

a) Time-slotted AODV: In [99], Forsmann et al, have proposed a time slotted protocol based on AODV protocol. As its name suggests, it incorporates the time slotted principle [100] into the original AODV. This is because a large number

Protocol	Performance consideration for UAANET
Proactive protocols	- Generate large amount of packet overhead for maintaining tables up-to-date
OLSR	- Inconsistency between real topology and information within topology control packets because of frequent topology changes - Compared to AODV and DSR, OLSR has better performance in terms of end-to-end-delay
TBRPF	- The minimum hop count gives inconsistency of the route discovery -Induce less overhead compared to OLSR -Generate inaccurate routing information with the UAVs high mobility degree
BATMAN	- Packet loss values increase above two hops Accordingly, throughput and data decrease sharply
DSDV	- Eliminate any routing loop and counting to infinity problems within UAANET - Add additional delay during updates - Consume network and energy resources to decide between full dump and incremental packets (because each UAV must continuously listen to events within the network)
FSR	- Decrease packets overhead within small size networks - Suffer routing table overflow with high workload - Non-optimal management when dealing with node destination far from the source node
DOLSR	- Optimize end-to-end delay compared to OLSR - Security enhancement because of use of unidirectional antenna - Hardware limitation: cannot operate with omnidirectional antenna
P-OLSR	- Functionality depends on mobility model type (mathematical model for correct prediction)
ML-OLSR	- Able to find the most stable route - Generate high overhead under high workload - Consume large network bandwidth
COLSR	- Require a synchronous timer. As processing delay can be bigger than propagation delay, it can generate false positive

Table VIII
UAANET PROACTIVE ROUTING PROTOCOLS COMPARISON

of UAVs is assumed in the network and therefore at some point during routing discovery, a collision will occur which may increase the packet loss rate. Such loss of data packets (including C2 traffic) may have a severe effect during missions. The main motivation is then to control network congestion by finding a trade-off between the bandwidth consumption and network congestion risk. Accordingly, the protocol attributes time-slots for each UAV and allows collision-free communication between neighbors. The duration of the time-slot is selected to be large enough depending on the number of nodes. In addition, in order to manage topology changes, the time-slot window is dynamically adjusted in case of link-failure detection. Each message type has its own time-slots sizes to enable a large time-slot for the routing protocol, while minimizing unsused bandwidth during C2 traffic and payload transmission.

An evaluation test has been carried out to compare Time slotted AODV and AODV under a UAANET scenario. The results show that the use of time-slot allocation to manage communication between UAVs enhances the data delivery rate while significantly reducing packet collision. Furthermore, by dynamically allocating time-slots, communication reliability is ensured. However, its use is only beneficial if several UAVs are deployed. Such a scenario is unlikely in real deployment as mentioned in section III-D.

b) RGR (Reactive-greedy-reactive): RGR [101] is a UAANET routing protocol that combines reactive and geographical modes. AODV is used as the reactive part and GGF (Greedy Geographic Forwarding) [102] for the geographical concerns.

RGR is based on the following hypotheses: each UAV is able to receive its position, its neighbor position and the destination position without implementing a position sharing mechanism. The position sharing process is achieved by incorporating position information in the request packet during neighbor discovery. Indeed, reactive routing is primarily used and the greedy forwarding is only activated in cases where the UAV source fails to find a path reaching the destination. During the route discovery phase, the source node sends a Request packet RREQ in which the node adds its position information, so that the neighbor and the destination aware of its location. This is also the case with a response packet RREP.

Furthermore, during a data forwarding phase, AODV forwarding techniques are used. If there are link breaks, the routing protocol uses the greedy forwarding algorithm in which the packet is sent to the nearest neighbor to the destination. In the meantime, a route request is launched to find a new route.

A noticeable advantage of this routing protocol lies in its property of being executed without a sharing position technique. Another advantage is that RGR handles the frequent UAANET topology changes well as it can switch into another mode that consider link failures. However, the drawback is that network congestion may be created because of the overhead size and the increased number of control packets.

c) RTORA: In [98], The Rapid-reestablish Temporally Ordered Routing Algorithm (RTORA) is proposed. This routing protocol is based on the TORA algorithm and adopts the reduced-overhead mechanism to correct link reversal failures in TORA. As in TORA, RTORA uses the height and link re-

versal mechanism during route discovery and data forwarding phases. Each UAV has the height list of its neighbors and information about link-status. However, it is implemented in a different manner as explained in the following. A height of a given node can be defined as a 5-tuple (t, oid, r, v, id) in which: (t) is the time reference of level creation, (oid) is the identity of the reference creator, (v) is the hop count to the destination node, (r) is the reflection bit and (id) is the identity of the node itself. In RTORA, this height becomes 4-tuple (r, oid, v, id) as (t) as the reflexion bit is deleted. This deletion suggests that once a node has a NULL height value, it cannot participate in communication. As a result, only useful control packets are exchanged within UAANETs.

Furthermore, during routing maintenance, RTORA uses the "reduced-overhead" mechanism. A node that receives a UDP packet or CLR[7] (Cleared Packet) updates the reachability status list and the height value of its neighbor. In cases where another downstream[8] link exists with a greater value of height, an update is operated, otherwise, the link reversal is launched. If the node performing the link reversal is not the source node, it sets to height into NULL and sends a CLR packet. Otherwise, it will update its height to the highest value and sends a UDP packet. As for a source node that does not have any neighbors, it will create and process a new query packet.

A simulation comparison between RTORA and TORA shows that RTORA offers better performance in terms of overhead and end-to-end delay. This is justified by the improved routing maintenance (reduced-overhead) mechanism which allows RTORA to rapidly reestablish a new route and avoid flooding control packets.

D. Geographical UAANET routing

As far as geographical routing is concerned, it uses node positions to find the best route from a source to a destination. Usually,there are two distinct mechanisms: greedy forwarding and a backup mechanism in case the former fails.

The greedy forwarding consists of selecting as a next hop the closest node to the source node position. Alternatively, when no node within geographical range close to the destination is found, a backup mechanism is automatically launched. We can cite as an example "Face Routing" used by GFG [103], a mechanism which consists in creating a planar graph of the network interconnections, and then uses the right hand rule to reach the destination. It is important to mention that for the full deployment of geographical protocols an additional mechanism is required to exchange the different node positions through the network (otherwise we would have to use another communication medium, which is unavailable most of the time). The main existing position sharing mechanisms are detailed in [104].

Table X summarizes the protocols reviewed in this section and compares some of their features.

[7]CLR is used to delete route and to set the height value as NULL

[8]A downstream link is from a higher to a lower height

a) GPSR (Greedy Perimeter Stateless Routing for Wireless): This is a geographic routing protocol that uses two routing approaches such as Greedy mode and Perimeter mode. The former is used when a node communicates directly with a neighbor that is closer to the destination. As a result the closest neighbor to the destination node is selected as a next hop during the packet forwarding process. The latter consists of a protocol recovery mode that is used when the greedy mode fails. Such failure occurs when the closest node to the destination is the node itself. When this happens, a local maximum is declared and points to the latest node during the greedy mode. A planarized graph is constructed with the implementation of the right hand rule mechanism in case the local nodes does not offer a better routing metric to reach the destination. As depicted in Figure 8, at a given node u1, from u2, the right hand rule principle consists of choosing the next traversed edge as the one that is sequentially counter-clockwise about u1 from the edge (u1, u2). GPSR is evaluated in [105] and [106] in simulation in a realistic UAANET scenario. Their results show a strong correlation with the mobility model being used. In these studies, they found that GPSR is outperformed by GPMOR and MPRG in terms of packet delivery ratio and delay.

b) GPMOR: Greographic Position Mobility Oriented Routing: GPMOR [105] is fbased on the following assertion: each UAV is equipped with an embedded GPS that allows each node to obtain its position, its neighbor position and the destination node position within the network. During neighbor discovery, each node periodically exchanges a beacon message that includes their own coordinate information, time stamp and velocity. The neighbor table is then created. In order to reduce the packet loss ratio (caused by intermitent network connectivity), there is a compromise to find between the time to launch the broadcast and the overhead size. This issue is settled with a movement prediction algorithm to select the next hop. Note that the Gauss-Markov mobility [107] model is used to make the prediction.

The routing strategy based on the mobility prediction can be summarized as follows. First, the euclidean distance between UAV is computed. The result is compared to the maximum coverage of the source node. If the result is more than the maximum coverage of the communication range, then, it suggests that the two nodes cannot communicate and it is wise not to select the node as a next hop. Otherwise, if the result is within the maximum coverage interval, the node is selected as next hop. The second step consists of computing the metric to connect (MTC). The MTC metric is used to assess mobility compatibility between a sending node and its neighbor. If the MTC value is a positive or zero, it indicates that the neighbor is out of the communication range of the sending node. Consequently, there is no possible communication. However, if it is negative, there will be communication as this neighbor will probably move towards destination node. The last step consists of combining these two metrics to assess the communication probability with the given neighbor.

Figure 9 below gives an illustration of this algorithm. A

Protocol	MR	Route metric	Route repository	Route rebuilding	Performance
DSR	Yes	Shortest path or next available	Route cache	Searches for new route, informs one hop neighbor and notifies source	- High overhead under high network load - Add latency during fresh route discovery
AODV	No	Minimum hop count	Routing table	Generate route error, local repair and informs source node	- High overhead under high network load - Provides low end-to-end delay with low node density - A good route stability with low node density
TORA	Yes	Shortest path or simply next neighbor	Routing table	Reverse link and repairs route	- High overhead under high network load - Less overhead in cases of low node density - Add latency to construct the DAG
Time-slotted AODV	No	Minimum hop count	Routing table	Generates route error and uses local repair	- Minimum packet loss rate - Collision-free communication - Only valuable in cases of high node density
RTORA	Yes	Shortest path or the next neighbor	Routing table	Reverse link and repair route	- Generates less packet overhead
RGR	No	- Minimum hop count - Next closest node	Routing table	Greedy forwarding followed by local repair	- Generates high overhead during topology changes - Minimum packet loss rate due to back up route

Table IX
REACTIVE ROUTING PROTOCOLS COMPARISON

simulation study was performed to compare GPMOR with GPSR and GLSR(Geographic Load Share Routing) [108]. The results suggest that GPMOR outperforms GPSR and GLSR in terms of PDR and delay.

c) MPGR (Mobility Prediction Geographic Routing) : MPGR [106] is a mobility prediction geographic routing used for battlefield application based on the GPSR algorithm [109]. The choice of prediction algorithm is justified by the need to properly choose the next hop and thus to select a stable route within UAANETs.

The particularity of this routing protocol lies in its position sharing mechanism. Indeed, an on demand position acquisition technique is used. It means that if the UAV does not send a message, the UAV will navigate silently without enabling the routing protocol daemon. If one UAV has a message to send, it will begin by broadcasting Neighbor Discovery packet (ND). It contains desination position, delivery mode parameter (either greedy or perimeter), and distance from destination. Each neighbor then responds by putting their respective neighbor list information to the sender. This will eventually allow the sender to construct its own neighbor table.

Furthermore, during the packet forwarding phase, a prediction method is merged into the geographic algorithm. If routing void occurs, MPGR switches to two-hop perimeter forwarding algorithm. Its principle is to calculate the euclidean distance between the node and its two hop neighbors and select the one that proposes a better feedback in terms of prediction function result. It should be noted that a Gaussian mobility model is used during prediction computing. A simulation study on the Gauss mobility model has been carried out to compare MPGR with GPSR and AODV. The results show that MPGR outperforms GPSR and AODV in terms of PDR, end-to-end delay and overhead.

Even though a promising result has been obtained, it is important to remark that it depends heavily on the GAUSS mobility model implemented. Accordingly, the results should be verified and validated with other mobility models in the same test scenario. Another noticeable drawback is that the load balancing of heavy traffic (for instance video traffic) is not considered in this study.

d) USMP (UAV Search Mission Protocol): USMP [110] is a geographical routing protocol used specifically for UAANETs in a search mission application. It is also based on the well-known GPSR routing protocol, which is enhanced with a cross-layer mechanism.

The USMP protocol has two features that give uniform information on each UAV: Location Update and Waypoint conflict. The former helps to build a distributed decision among UAVs by exchanging node positions. Thus, each node is able to determine the location that has not been scanned. The GPSR location sharing algorithm is used to accomplish such a task. The second property of USMP is waypoint conflict resolution. Waypoint conflict occurs when two or more UAVS move towards the same direction and collide. Waypoint resolution consists of calculating the search metric "Expected Arrivals rule" for each node involved in the conflict. The algorithm then selects the one that has a greater probability value of arriving at the waypoint.

A simulation study has been carried out to compare USMP and GPSR protocols. The results show that USMP improves performance by as much as 188 % compared to scenarios without inter-UAV communication. GPSR degrades performance by approximately 20% in searches and distance traveled.

e) LAROD (Location Aware Routing for opportunistic Delay Tolerant Network): LAROD [111] is a delay tolerant protocol. The UAV that holds the packet (the custodian) uses greedy packet forwarding when there are other UAVs nearby. The custodian should make sure that the packet has been received by other UAVs. To forward messages, nodes that provide some minimum progress towards the destination are

eligible. They create the Forwarding Area. After receiving a packet, the nodes in the forwarding area set a timer. The node with the timer that expires first is the best forwarder (custodian). This node will then broadcast the packet again.

Furthermore, overhearing this transmission, the other nodes remove their copy of the packet. If there is no node in the forward area, no such retransmission is heard by the sender and it regularly broadcasts the packet until a forwarder becomes available relying on UAV mobility. When a packet reaches its destination, the destination sends an acknowledgment packet to stop transmission, and to prevent the indefinite forwarding of the packet between nodes.

It is important to point out that this protocol is not robust to node loss. If a node fails, all packets stored in the node will be lost unless they happened to be duplicated in another diverging path.

E. Static UAANET routing protocol

Static routing protocols are based on static routing tables, which are configured and loaded at the start and mostly on the ground. As a result, the routing table will not be modified during the mission, which limis its applicability in real UAANET deployment.

a) MLHR(Multi Level Hierarchical Routing) [18]: This consist of ensuring the scalability of large-scale ground networks such as MANETs or VANETs. These networks are normally organized as flat structures since performance degrades when node density increases. One approach to limit this performance degeneration is to organize the network as a hierarchical structure which will increase the capability to extend the operation area. Accordingly, UAANET can be deployed in clusters where only the cluster head has connections to one of the ground nodes. The cluster head disseminates data traffic to other UAVs in the cluster. One noticeable drawback of such as approach is that under high network load and frequent topology changes, the cluster head will be frequently renewed which would impose large overhead on the network.

b) LCAD (Load Carry and Deliver) : Static Routing protocol for UAANET: LCAD [60] is a static routing protocol for UAANET. This means that the route is configured on the ground before takeoff. Such routing protocol is sometimes used for repetitive tasks like repetitive area check ups (border surveillance missions). It is also used for delay tolerant networks (DTN). The objective of LCAD is to maximize throughput by configuring node swarm position. One such configuration example could be one UAV flying from the ground position to a specific point while carrying data packets. After that, another UAV takes the packets when the UAVs are within range of each other. The communication paradigm is divided into three steps. The first is the load stage where the GCS transmits the packet to the first UAV. The second is the carriage step in which the UAV takes care of the data packets and sometimes transmit them to other UAVs. The last step consists of transmitting the data to the final destination which can be a central point located in the ground. It should be noted that this paradigm does not involve a routing table algorithm.

Consequently, the protocol only works when no failures occur with the UAV during transmission, which is unlikely in a context of real deployement. An ideal communication system and hardware are therefore taken as a prerequisite which is unlikely to occur during real UAANET deployment.

F. Clustering based UAANET routing protocols

In this category, UAVs are organized as a cluster. Each cluster is supervised by a "cluster-head", which manages care of intra and inter cluster communications. Cluster head selection is therefore particularly important in this category of routing mechanisms.

a) Clustering algorithm of UAV networking [112]: This is a hierarchical routing protocol that uses the cluster principle. It builds the clusters on the ground, and then updates it during the operation of the multi-UAV system. Initially, the ground control station adjusts the initial cluster of the UAV swarm based on the mission application. It is important to underline that this routing protocol requires an aerostat node to fly above the UAVs. An aerostat (or balloon) is a flying vehicles which floats due to its buoyancy. It can propel itself in the air in a controlled manner. The ground station then communicates directly to the aerostat node which in turn exchanges with the UAV nodes. An illustration of this architecture is depicted in Figure 15. The main drawback of this approach is the necessity of an aerostat which is not only costly but also unlikely is some case of UAANET deployment [9]. It is also vulnerable to attacks as it is considered as semi-centralized.

b) Mobility Prediction Clustering Algorithm for UAV Networking [113]: MPCA routing protocol tries to predict the cluster formation based on the mobility prediction of UAVs. This choice can be explained by the need to construct a stable cluster and thus to stabilize the network. The mobility prediction used is based on link expiration time (LTE) and on Dictionary Trie Structure. The former allows to evaluate whether or not the transmission link between them will be interrupted. To calculate this metric, they make the assumption is made that a GPS is available on-board that can provide position information. With this information available, two UAV neighbors can compute the link expiration time between the two UAVs. Furthermore, the dictionary tree structure consists of computing the probability of a node remaining in the cluster. These two features are used to construct more stable cluster formations. Simulation results comparing MPCA and HD [114] have been carried out. Their results show that MPCA offers stable prediction results that improve network performance. The number of clusters formed by MPCA increases constantly as connectivity and mobility prediction are considered. In addition, the duration of cluster formation in MPCA is longer than in HD. This is the result of mobility prediction reliability which ensures stable cluster structure. Lastly, MPCA offers a lower reaffiliation frequency compared to HD. This is due to the fact that in MPCA, nodes do not change clusterhead even if other clusterheads appear in the

[9]In an emergeny for example, an aerostat is not available.

Protocol	Forwarding strategy	Route metric	Loop-free	Scalability	Performance
Geographical routing					- Requires location information sharing methodology which may become unrealistic in some applications - Uses random way point mobility model which is not efficient to measure its performance
GPSR	Greedy	Shortest path	Yes	Yes	- It decreases packet delivery ratio in the presence of high node mobility - It adds delay during face routing and does not suit UAANET real time application
MPGR	Flooding	Maximum progress	Yes	Yes	- With Gauss mobility model, it outperforms GPSR and AODV in terms of packet delivery ratio, end-to-end delay and overhead - Different result with different mobility model and therefore in real deployment
GPMOR	Flooding	Maximum progress	Yes	Yes	- With Gauss mobility model, it outperforms GPSR and GLSR in terms of packet delivery ratio and end-to-end delay - Different result with different mobility model and therefore in real deployment
LAROD	Greedy	Maximum progress	No	Yes	- In case of node failure, all packets stored and exchanged will be lost
USMP	Greedy and directional forwarding	Expected arrivals rule probability	Yes	No	- Protocol designed for a specific case of target search application only

Table X
GEOGRAPHICAL ROUTING PROTOCOLS COMPARISON.

Protocol	Performance consideration in UAANET
Static	- Fixed tables, - Not suitable for dynamic topology as found in UAANETs - Does not handle topology changes
LCAD	- Higher delivery delays - High risk of data traffic loss
MLHR	- Cluster head becomes a single point of failure - Generates high overhead when the cluster head is changed

Table XI
UAANET STATIC ROUTING PROTOCOL PERFORMANCE CONSIDERATION

vicinity. A node only search a new cluster head when the links of the original clusterhead fail.

c) Landmark Routing In Large wireless Battlefield networks using UAVs: In [83], an improvement of the LANMAR protocol [84] is proposed. This routing protocol is based on an extended version of HSR (Hierarchical State Routing) protocol. The latter is a hierarchical link state routing that organizes nodes as a cluster in the network. Each node is identified with a hierarchical ID (HID). EHSR has three levels which are a ground ad hoc network, a UAV network and a backbone network.

A landmark is responsible for tracking other nodes that have a common interest. Compared to DSDV and LANMAR protocols, this protocol has the advantage of scalability by including a backbone and UAV links.Moreover, its route discovery delay is shorter. This can be explained by the combination of backbone and UAV links which discover optimal routes (minimum distance) in real time.

d) Multi Meshed Tree Protocol (MMT): In [115], an Integrated Routing and Medium Access Control framework for Surveillance Networks is proposed for UAANETs. The aim of this cluster based protocol is to ensure efficient communication during surveillance. The routing metric used is an end-to-end delay along with file delivery latency. This provides a solution for the routing and MAC layer functions. The MMT uses a clustering scheme in which a cluster head (CH) is elected and a group of UAVs (also called cluster clients or simply "CC") are placed in a cluster formation. By applying the mesh tree principle, the branch connecting the CC and CH allow data to be exchanged between them. A UAV may either stay on a branch or may leave and connect to another cluster. The stay duration on a branch therefore depends on their mobility pattern and speed. This suggests that when CC loses connectivity to the CH, the CC will still be able to interact with the CH via another path. Consequently, this scheme allows several multipaths to be created based on the number of clusters. Simulation results have shown that this routing protocol provides connectivity to cluster clients moving across clusters. It also helps extend the coverage area of the surveillance network to address scalability. As a result, it improves the management of frequent route failures due to node mobility.

e) CBLADSR (Cluster-Based Location- Aided Dynamic Source Routing): In [43], CBLADSR is proposed. It is a hybrid routing protocol combining three routing algorithms: the reactive DSR protocol, a cluster mechanism and a geographic routing. Route discovery and route maintenance are performed based on the cluster architecture. Initially, this routing algorithm creates one or more stable clusters of UAV swarms. Then it uses location information acquired through a GPS device to perform route discovery and route maintenance. It uses the Node-Weight heuristic algorithm [116] to select cluster heads. The node-weight heuristic algorithm measures the suitability of the node to endorse the cluster head's responsibility. It considers connectivity degree, speed and power level. As in general cluster based routing protocols, it uses short range communication with its neighbor and long-range-transmission with a distant destination.

Simulation results show that CBLADSR outperforms DSR in terms of packet delivery ratio and end-to-end delay. It also offers good scalability and dynamic performance compared to

Protocol	Performance consideration in UAANET
Cluster based	- Difficult to use in real deployment (low density node) - Only valid with some UAANET application - Cluster represents a single point of failure
Clustering algorithm of UAV Networking	- Requires an aerostat which is costly
MPCA	- Performance results shows a strong correlation with mathematical prediction model used - Its performance may vary when used in real deployment where node movements are unpredictable (due to a variety of factors)
EHSR	- Requires a ground backbone - Scalability
MMT	- Scalability - Improves the management of frequent route failures due to node mobility
CBLADSR	- Provides better performance in terms of packet delivery ratio and end-to-end delay compared to DSR - Generates high overhead in cases of high node density
DTM	- Its delay tolerant principle is not suitable for highly sensitive traffic (e.g. C2 traffic). It should only be considered for specific UAANET applications in which delays does not matter.

Table XII
UAANET CLUSTER BASED ROUTING PROTOCOLS

DSR.

f) DTM (Disruption Tolerant Mechanism): In [117], a cluster-based reactive routing protocol is proposed for UAANETs. The DTM routing protocol combines the well-known AODV algorithm and cluster management techniques to form a hierarchical routing structure. The purpose of DTM is to alleviate the possible overhead and significant delay caused by AODV to find a more stable route while limiting flooding packets during route creation. To create the appropriate topology, the flat structure formed by AODV is partitioned into several clusters and assigned with a cluster ID called CID and a cluster head node. Moreover, during route discovery, AODV algorithm is used, but only inside a given cluster to avoid network congestion by the multiple control packets. If the destination node is in the cluster, the packet is transmitted directly. If it is not in the cluster it is transmitted hop by hop. On the other hand, if the node is beyond the cluster range, it is transmitted to the cluster head, which in turn modifies the packet header with cluster ID. Finally the packets are sent to the cluster destination. As for route maintenance, each cluster head automatically exchanges periodic beacon messages called cluster control messages (CCM). The CCM contains the ID of the cluster head, the ID of the cluster class and the Time-To-Live (TTL) field to asses cluster lifetime. It is important to underline that there is no periodic communication required between the cluster head and its members. The broadcast transmission of the CCM by each cluster head is sufficient to acknowledge inter connectivity. According to [117], using DTM, the overhead is limited in each cluster. This can be explained by the transmission of CCM instead of hello packets. The CCM is relatively short and only sent by the cluster head. In addition, thanks to the Delay tolerant principle, DTM increases resiliency in case of temporary link or node failures. However, DTM is not valid when used with real time applications such as video monitoring. When one node fails or if link breaks, packets may never reach the desination.

G. Comparison and discussion of issues related to UAANET routing protocols.

Designing an efficient routing algorithm for UAANETs that can deliver payload traffic and control packets while ensuring a certain QoS and a high level of security services is a difficult challenge. This is particularly due to UAV mobility which induces a rapid topological change in UAANETs. As we have seen previously, several researchers have proposed a routing protocol based mostly on either AODV, OLSR DSR or GPSR. These 4 routing protocols were often used as basis of new UAANET routing protocols. A synthetic study has enable the identification of three common issues that can be addressed to improve these existing algorithms and to render them more suitable for UAANETs. The first is the lack of real experiments which are crucial to assess routing protocols based on realistic requirements. Indeed, routing protocol performances have often been evaluated in a simulation which is easy to establish but does not represent the real UAANET environment accurately. As a consequence, several authors claim to have the best performing protocol without providing real implementation results. Therefore, we believe that outdoor flight experiments should be performed for several propositions in order to have a clear understanding of the impact of UAV mobility on the routing protocol. The second issue is the lack of consideration of security which is a highly significant due to the inherent characteristics of the wireless medium which allows different routing attacks to be launched. In addition, there is a critical security level of control traffic which requires authentication, integrity and confidentiality of the routing protocol control packets. Indeed, a UAV can be used as a weapon and threaten human lives if hijacked. This second factor is yet to be addressed in all of the existing UAANET routing protocols (detailed in the next section). Lastly, a major drawback is the lack of consideration for the certification of the routing algorithm. Indeed, UAANET certification is mandatory for UAV to be integrated into civil airspace. This certification includes different parts of the UAV

System (UAS) such as the autopilot, the operating system and the communication system. It appears therefore that a set of tools and methodologies should be used that can contribute to the certification of UAANET routing as suggested in [118]. An example of such methodology is the Model Driven Development (MDD) which enables cost-effective and fast development of complex systems. The principle is to begin the design with models rather than software algorithms. The model is an executable specification that can continuously be modified during the development step. In addition, MDD allows the generation of code for hardware implementation requirements by minimizing coding errors. These steps help not only for modularity and reusability of the final code, but also contribute to the certification of the entire UAS communication system [119].

V. UAANET Security Challenges

Similar to MANETs, securing UAANETs is a challenging task due to the use of wireless links, cooperativeness characteristics, the uncontrollable environment and the absence of a fixed infrastructure to separate nodes originating inside from those arriving from outside. Typically, there can be different motivations for attackers to breach a UAANET. For instance, an attacker may attempt to take control of one or multiple UAVs by capturing the control and command traffic. It should be understood that regardless of their motivation, an attacker usually wants to break one or a set of the standard security services: confidentiality, authentication, integrity and availability (detailed in the next section).

The UAANET security research topic is currently at its early stages, as most of the UAANET research has focused on how to enhance communication performance capabilities between UAVs. Nonetheless, from our point of view, the security context should be considered as the critical level of traffic exchange is relatively high and cannot be ignored. While acknowledging such lack of interest, it should be noted that some UAS security studies have been proposed by the likes of FAA[10] and EASA[11]. However,the majority of their work cannot be applied in UAANETs because of the direct architecture assumptions that have been made between UAVs and the GCS. Nonetheless, there are some papers that are considered to be among the first leading works in the field of security and which emphasize the importance of UAANET security. Among these papers, the work in [120] highlighted the control and command traffic security requirements. In this paper, Akram et al, have analyzed how this traffic can be vulnerable to routing attacks as it provides rational adversary and network models.

In [121], Phuoc et al., analyzed the importance of securing each component of the UAS to sustain UAANET integrity. They suggest that each individual module is a potentially vulnerable to attackers and therefore must be protected either through physical or software embedded secure elements.

[10]Federal Aviation Administration

[11]European Aviation Safety Agency

In [122], Phillips et al., investigates the application of a secure group communication architecture to a UAV swarm. They have proposed a multicast secure group communication architecture algorithm for a UAV swarm.

In [123], Yokoyama et al., studied UAV swarm security by proposing an architecture that protects UAVs position by using RSSI (Received Signal Strength Indicator)-based distance estimation. This approach is used to counter a false location attack which consists of forging the GCS position to gain access to a UAV.

In [124], Javaid et al. analyze various UAS cyber security threats. They place emphasis on wireless communication channel vulnerabilities, which enable attacks not only from aerial intruders flying in the coverage zone, but also from ground based adversaries equipped with a powerful antenna. Then, they analyze the vulnerability of each UAV communication module by determining which component is at risk and how it can induce confidentiality attacks, integrity attacks and availability attacks.

All of these papers reinforce the major importance of securing UAS communication. Despite such rise of interest, the research in the field of UAANET security is currently in its early stages. The next section details UAANET vulnerabilities and the different type of network attacks that can be performed against these networks.

A. Vulnerabilities in UAANETs

There are various reasons why UAANETs are at risk from a security perspective. In the following, we will discuss the features that make these networks vulnerable to attack. Attacks can be defined by a set of operations that are executed by unauthorized entities to disrupt network accuracy and reliability.

- Wireless links: similar to MANETs, UAANETs use wireless links to send and to receive radio signals. Generally, wireless links can be prone to links attacks, which consist of passive eavesdropping, active interfering, leaking secret information, data tampering, message replay, message misuse, impersonation and denial of service. These attacks might give an adversary access to vulnerable information, thus violating data confidentiality. Typically, with commercial high-gain antennas configured on specific frequencies, anyone can listen to a frequency and receive the signals (e.g. GPS signal) send by the GCS and UAVs. Moreover, considering that the GCS provides real time control and command traffic on the uplink to the UAVs, one only needs to detect the signal and generate a noise signal the radio communication. If such an attack is successfully performed and the pilot does not react rapidly, the UAV will not be able to receive any command during a certain period of time which can be sufficient for an attacker to capture a UAV. The same scenario can happen to the downlink in which aerial observations are transmitted from flying UAVs to the GCS. Furthermore, depending on data-link characteristics, UAANET wireless links often have lower bandwidths than wired networks. Consequently, an attacker can exploit this feature by

sending unnecessary packets to UAVs. These packets could consume the network bandwidth and prevent normal communication between entities [125].

- Uncontrolled environment: as for MANETs, UAANETs do not have any central authority like in wired networks to handle incoming and outcoming packets. However, even if such system were assumed to exist, it could be a point of failure that makes the network much more vulnerable. Due to the lack of key management system, attacks can happen from inside as well as outside the network. Once an attacker is in transmission range of a UAV, it can send and receive data traffic.
- Dynamic topology: another problem that arises in UAANETs is the correct detection of the adversary node (or action). Indeed, it is usually challenging to distinguish between a truly misbehaving node and a legitimate node that appears to be misbehaving because of poor link quality. For example, there may be little difference between a loss of route caused by an attacker and a loss of route caused by an outdated routing information (or a data link break due to dynamic topology). Additionally, an adversary node may operate correctly for a while to gain trust, but, at the same time create inconsistency in the routing protocol to corrupt the route discovery or the route maintenance process. In such a case, an attacker can forge new routing messages or advertize non-existent links. Such attacks are especially difficult to resolve since they may come from seemingly legitimate nodes, whose the true identity have not yet been discovered.
- Cooperativeness: routing algorithms for UAANETs require that all nodes participate in the routing process (topology discovery and data forwarding). No prior security association is considered between nodes. Accordingly, when a node searches a route to a given destination, it broadcasts the message without paying attention to the identity of the recipient. Unfortunately, there is no guarantee that a path between two nodes will be free of adversary nodes. The mechanisms currently deployed in UAANET routing protocols cannot survive disruptions due to malicious behavior. As a result, an attacker can easily participate in the routing process and disrupt UAANET topology by filtering or blocking control traffic.
- Limited resources: depending on their size, UAVs can have limited computing and storage capacities (For instance, Paparazzi UAVs [89] have a energy level of approximately 10 minutes during flight). Accordingly, an attacker can launch a sleep deprivation attack [126] which aims to drain UAV battery power. Furthermore, implementation of a security solution, always requires a trade-off between network performance and security robustness. The security solution implemented in a UAANET depends on the power and storage capacity of UAVs. For example, the working memory of UAV must be sufficient to hold all the variables that are required to perform asymmetric cryptographic algorithms. For a low power UAVs, this can be a particular challenge because of authentication security methodologies that are based on digital signatures [127]. In such cases long signatures with large communication overhead per packet are required and this may be impractical. As network performance is important in UAANETs due to the strict delay constraints of data traffic, all the functional and security requirements must be considered together.

The above discussions reveal that UAANETs are inherently insecure and require effective security schemes that take into account the special features of UAANET. When proposing a security scheme, the fundamental security objectives should be discussed. In the next section, the essential UAANET security needs will be described.

B. Security requirements for UAANETs

1) Authentication: It is crucial to authenticate all nodes and messages which transit within UAANETs. This ensures that only authenticated nodes are allowed to participate in the routing process. Without authentication, an adversary could act as a legitimate node, could acquire access to sensitive information and could even interfere with network operation. Generally, there are two types of authentication services in standard MANET architecture: Node authentication and Message Authentication.

- Node authentication ensures that only authorized UAVs and GCS(s) which have authorization to access the resource and the inherent network information can process messages. If provided, it disallows any attempt by a flying UAV attacker or ground attackers to take part in the routing process and thus eliminates any danger of UAVs being captured.
- Message authentication is used to authenticate the message originator and to provide message integrity.

2) Integrity: This involves the consistency, accuracy, and trustworthiness of data packets over their entire passage through the network. It ensures that an attacker cannot alter by insertion, deletion or modification data traffic during transfer. When sending data packets, the majority of current UAANET routing protocols require that mutable fields (e.g., hop count, sequence number, etc....) are updated hop by hop. This implies that neighbour nodes need to ensure that a security mechanism of integrity is launched to detect adversary nodes that are able to modify data packets. If the integrity mechanism of routing messages is weak, the integrity of the entire UAS could be at risk as attackers can send forged c2 traffic.

3) Confidentiality: This is roughly equivalent to privacy. Measures used to ensure confidentiality are designed to prevent sensitive information from reaching the wrong node, while making sure at the same time that this information can be received by the appropriate node. This, it ensures that sensitive information is not shared with unauthorized nodes. Within UAANETs, it guarantees that payload traffic, control and command traffic are not revealed to unauthorized entities. When there is no confidentiality mechanism, an attacker can launch passive and internal attacks such as the improper

collection of clear information [128]. The confidentiality of a UAANET is violated when an adversary is able to access C2 traffic sent to the UAV from the ground station as well as location information and other data sent in the opposite direction.

4) Availability: This guarantees that all services provided by the UAS are always available even in the presence of attackers. It ensures that the network is functional and useful information such as control and command traffic is always available at any given time during UAANET mission. This is indeed very challenging because of the strict delay constraints and the critical characteristic of a UAV mission.

5) Timeliness: Routing updates should be delivered on time to avoid delays. Since C2 traffic is exchanged in real time, routing messages must arrive on time to reflect the true state or network links. Otherwise, they can cause incorrect forwarding or propagate false information.

6) Self-stabilization: A UAANET routing protocol should be able to recover automatically and rapidly from any attacks without rebooting the system or requiring human intervention. That is to say, it must not be possible to permanently damage the network with malicious packets. If the routing protocol is self-stabilizing, an attacker who tries to inflict continuous damage must remain in the network and continue sending malicious packets to the nodes. This makes the attacker easier to detect.

Having discussed basic UAANET security needs, we will now introduce a possible attacker model to be considered in UAANET security.

C. Attacker model in UAANET Security

In order to accurately compare a set of properties of a given security UAANET protocol, a common attacker model is necessary which allows for proper evaluation. Such a model can provide complete knowledge of attacker capabilities. Accordingly, in order to describe the UAANET adversary model, we consider Dolev-Yao model [128] and the work of Cordasco et al. in [129] in which they present a topology and protocol agnostic model that takes into account real world scenario. Dolev-Yao is a model in which the attacker has full send and receive capabilities (i.e., control over the transmission medium).

1) Communication capability: The following are a comprehensive list of an attacker's communication capabilities.

- The attacker can be equipped with the same hardware used for communication as the GCS or a UAV.
- There can be one or more attacker within the network that has different heterogeneous hardware. They might also be equipped with the same equipment as stated previously. Typically, collusion among several attackers increases the attacker communication capabilities.
- An attacker has the ability to listen to a message within a typical radio range or listen to the entire network.
- It is possible for an attacker to send messages in broadcast mode to the entire network. It can also choose to limit sending messages to nodes within a typical radio range to avoid detection.
- The attacker's maximum transceiver capabilities are symmetrical, this suggests that an attacker will always use receiver device capabilities at least equal to its sender device capabilities.

2) Computation: The computational abilities of an attacker consist of decrypting incoming messages or encrypting outgoing messages. This essentially depends of hardware capabilities and knowledge.

- The attacker can only perform operations that are feasible in a reasonable amount of time. It means that the cost of the attacks is lower than the cost of the information that the attacker intends to obtain. Such a model is commonly used in the cryptographic community.
- The information available for the attacker can come from many different sources. These may be messages (or chunks of messages) that are previously exchanged unencrypted.
- Collusion among several attackers increases the information available as colluding attackers share all key material, nonces, hash chain seeds, etc. in order to be more powerful.
- Considering attacking strength, we assume that an attacker has the capabilities and knowledge to perform several attacks targeting different layers of the protocol stack. For instance, a software attack targeting the application layer, a UDP SYN Flood attack [130] targeting the transport layer, wormhole attacks [131] on the network layer and DoS targeting [47] the access layer.

While assuming these communication, computation and knowledge capabilities, the following attack objectives are possible within UAANETs:

- Data traffic disclosure: The attacker can collect data traffic transmitted by UAVs such as the payload traffic (video stream), GPS information, heartbeat messages or UAV mobility waypoints. All of this sensitive information can be obtained by eavesdropping if any confidentiality mechanism is employed.
- Routing information disclosure: The attacker can obtain information related to the network such as routing or topology information. They can be collected if the message confidentiality is not protected.
- Performance degradation: The attacker can degrade UAANET performance by rejecting or modifying the order of delay-sensitive traffic, or by adding delay during transmission. An attacker can also add unnecessary traffic to slow the network. This attack can be launched if any authentication mechanism is used.
- Topology modification: An attacker can also disrupt UAANET connectivity. This can be achieved by inserting an additional node or by invalidating a reliable link. An attacker can also forge false routing information and forward it within the network.

- UAV exclusion (i.e. capture of a UAV by an attacker): An attacker can exclude UAVs from the network by inserting false routing information or by modifying the routing metric. Once a UAV is removed from the network, the attacker is able to take control of the UAV and perform other types of attacks. This can be achieved if data integrity is not protected.

D. Analysis of security issues in existing UAANET routing protocols

Without security mechanism, UAANETs are inherently vulnerable to a variety group of attacks. In the following, we give a non exhaustive list of security issues faced by existing UAANET routing protocols.

a) Information disclosure: This combines illegal collection of information related to the network, such as routing information, topology information, UAV positions, C2 and payload traffic. When an attacker obtain these information (mostly by eavesdropping), it shows that confidentiality is not protected. The majority of existing UAANET routing protocols are vulnerable to this attack.

However, depending on the application, in some cases the information disclosed may not be critical to the whole UAS since the interpretation of information related to the UAVs will only be relevant at the time when it is sent from the GCS. This means that it will not have value in the future. For example, in C2 traffic when a certain command is sent from the GCS and is eavesdropped by an attacker, its action on that specific data is limited since UAVs interpret command and control in real time. As a result, routing information confidentiality is not usually protected even in the presence of secure routing algorithm. This is due to the fact that it is difficult to carry out UAANET information protection while still guaranteeing route performance (as is also the case for MANETs).

Nonetheless, the operator must be aware of the confidentiality issues within the network and apply the appropriate security block if necessary on data traffic. To solve this problem, a measure that can be applied is to encrypt data exchanged between nodes with the public key of the destination node and then decrypting the packet with the neighbor or destination's private key. If we assume that all nodes are trustworthy, encryption and decryption delays are reduced to a minimum, and that there is a valid PKI within UAANET, such a mechanism (already applied in MANETs) would be effective. Some proposition created on the basis of the mechanism above have been proposed in [132].

b) C2 and data traffic disclosure: Another attacker goal within a UAANET consists in collecting c2 and data traffic. This attack is possible due a the lack of authentication and integrity mechanisms. For this attack to be successful, an attacker must attract control packets during route discovery. Traffic attraction is relatively easy with the existing UAANET routing protocols without security extensions. Therefore, attackers can:

- control the interconnection points that join different nodes by disconnecting a specific or group of links. If successful, communication between nodes will be controlled by malicious nodes.
- launch colluding attacks [133], in which a private link is deployed between 2 valid nodes to reduce route length. As a result, the wormhole link appears faster and is therefore selected as the shorter and valid path to exchange data traffic.
- modify control packets [134] which aim of rejecting legitimate routing messages and validating forged messages by an attacker. Typically, an attacker can increase the sequence number or other message identifier (for reactive routing protocols) to attack the routing protocol using message identifiers. The attacker could also reduce the hop count value to attack, routing protocols using hop count as a routing metric (e.g., Time slotted AODV, UEDSR, RGR, CBLADSR).
- rushing attack [49] by hurrying route discovery messages to nodes to reject valid packets.
- launch route cache poisoning [135] by inserting incorrect routing information into route caches of valid nodes. This attack could be harmful for source routing protocols such as DSR, UEDSR and CBLADSR.
- launch RERR dropping by systematically blocking all RERR packets in order to make routes always valid. If the routing protocols do not require an end-to-end acknowledgment, as is the case with reactive approaches, this attack could be harmful.
- declare non existent nodes as neighbors in Hello messages. As a result, when applying the MPR algorithm if proactive approach is used, the attacker increases its chance of selection.

c) Performance degradation: Other attacks aims to breach existing UAANET routing protocols are also to degrade the performance of the network, which can be achieved by perturbing the ad hoc routing algorithm or by launching a DOS attack.

- By applying data reduction, data traffic can suffer from data loss and can be used to reduce the routing performance.
- Traffic addition: an attacker can also decide to add redundant traffic to UAANETs to increase routing load thus decreasing performance. To add traffic, an attacker could replay data messages or create a message loop within the network.
- Delay addition: an attacker can also decide to add delay to data delivery by providing a non-optimal route or by modifying the data packet header.

d) Topology modification: The vulnerability of existing UAANET routing protocols also lies in the possibility of the attacker modifying network connectivity. To perform such an attack, an attacker could:

- exclude a legitimate node by disconnecting its communication with other nodes. Such disconnection can be achieved through sleep deprivation attack [126], Sybil

attack [136], packet modification attack [134] and blackmail attack [137].
- introduce non-existent nodes into routing tables or route caches.
- invalidate legitimate routes or links by forging fake control packets or degrading a symmetrical link into an asymmetrical one.
- route/link forging [138]: attempts are made to inject forged information into UAANETs.

Having discussed the existing vulnerabilities of current UAANET routing protocols, we will analyze in the next section the various possible attacks on UAANETs. This will aid the discussion about designing the security schemes for such attacks in subsequent sections.

E. Network attacks within UAANETs

UAANET routing protocols are exposed to different types of threats and attacks. This is caused by its inherent characteristics as we have previously seen (section V-A).The purpose of attack targeting the network layer consists of absorbing and controlling network traffic, disrupting the routing function and injecting malicious nodes. A diversity of attacks in a MANET environment have been extensively described in the literature. Examples are Wormhole attacks, Rushing attacks [49], Colluding attacks [139] and Sybil attacks. A detailed overview of the existing attacks on MANETs is given in [140].

Given the diversity of possible threats and attacks to UAANETs, they should be classified. Several classifications have been proposed in the literature for MANETs. One such classification is to distinguish external threats and attacks from internal ones [141]. External attacks attempt to cause congestion in the network by propagating incorrect routing information or by preventing network services from working properly. As for internal attacks, these consist of insider attacks that are executed by insider nodes that already belong to the network.

Passive and active classification is also possible [142]. Passive attacks involve only eavesdropping (e.g, traffic analysis) on data being exchanged in the network while active attacks consist of specific actions performed by adversaries such as replication, modification, or deletion of data packets being exchanged between nodes.

In the following, we will instead classify threats and attacks based on basic routing functionalities to illustrate the attack targeting the different traffic between UAVs: route discovery attacks (category I), route maintenance phase attacks (category II) and data forwarding phase attacks (category III). The first category refers to attacks which could harm traffic control. The second category is relevant to routing control packets (e.g beacon messages). Lastly, the third category is relevant to payload traffic (image and (real time) video traffic for instance).

1) UAANET routing discovery phase attacks: Based on the routing strategy during the routing discovery process, a sender node searches for a route to a destination node to control packets. For instance, in AODV, the sender broadcasts a RREQ (Route Request) and waits for a RREP (Route Response). The route discovery process is crucial as it conditions other routing processes. Accordingly, if these packets are properly exchanged without malicious manipulation, a reliable route will be found. Otherwise, a false route containing malicious nodes will be established. Typically, the ultimate objective of routing discovery attacks is to deliberately modify the network topology. From the attacker's point of view, this can be achieved by excluding a reliable node, by adding nodes, by invalidating either a link or a route, and by forging either a link or a route.

a) Blackhole attack in UAANETs: As the name suggests, this consists of an attacker that attempts to advertise that it has a fresh route. By generating forge control packets, the adversary node may succeed in becoming part of the network route. Then, once chosen as intermediate node, the attacker drops the packets instead of processing them. As shown in Figure 9 where we suppose that the AODV routing protocol is executed to create routes, an adversary node claims to possess an optimum route toward a given destination, and transmits its forged routing information to other UAVs. The attacker generates and sends its neighbors a false RREP packet that has a non-existing destination, sequence number random value and a forged lifetime value. Consequently, nodes are convinced that the optimum route is through the blackhole attacker. This prompts the GCS to choose the route involving the adversary node as the better one. To avoid detection from its neighbors, the attacker can selectively forward some packets and discard others (greyhole attack [143]).

b) Sleep deprivation attack in UAANETs: This is a denial of service attack in which an adversary attempts to behave as a legitimate nodes in the network. The purpose of this attack is to exclude a UAV from the network by suspending its communication with other nodes. The attacker continuously generates data packets and sends them to target UAVs to drain their energy. This can be extremely hamrful for small size UAVs with limited storage and capacity. To perform this attack, an adversary node broadcasts a RREQ demanding a route for a non existent node. This will compel all the nodes to forward the request since none have the requested route. To illustrate this attack, we consider the figure 10. In this scenario, the intruder generates a RREQ (including a TTL large value) with a destination IP address for UAV6 which does not exist in the network. Nodes UAV1, UAV2, UAV3 and UAV4 which are within the coverage of the intruder, will receive the request and check their routing table entries for routes to the destination. Since they do not have the route for UAV6, they will repeatedly rebroadcast the RREQ packet. When the packet arrives at node UAV5, it will also rebroadcast the RREQ and create a loop in the network.

c) Link with-holding and Link-Spoofing attacks within UAANET: This attack is specific to routing protocols that use link quality as a metric. On one hand, an attacker voluntarily ignores the requirement to advertise the route to a specific UAV or a group of UAVs. As a result, the GCS is unable to find links to communicate with those UAVs. Therefore, this

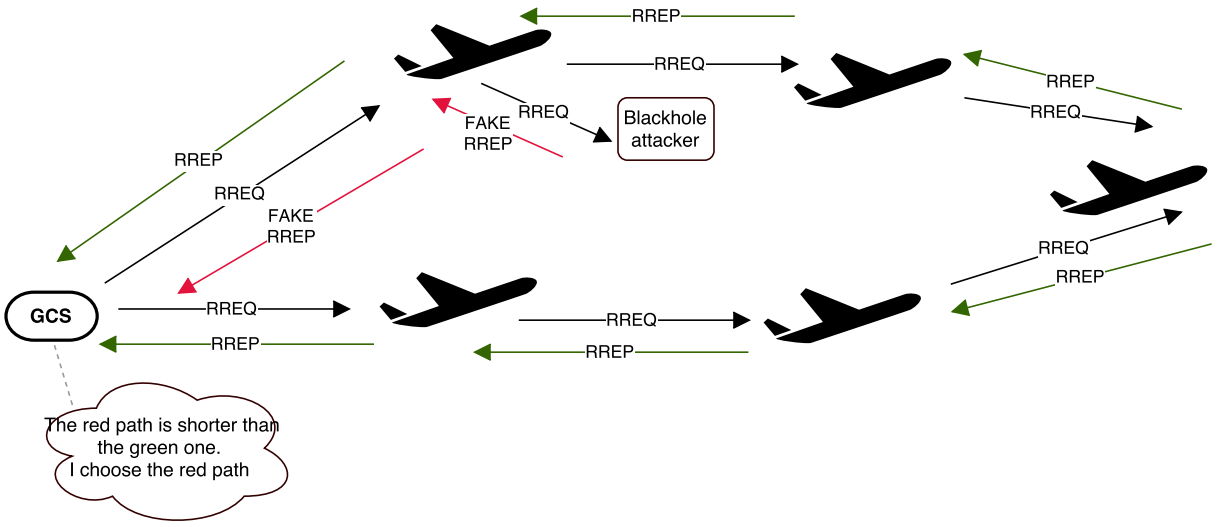


Figure 9. Illustration of blackhole attack in UAANETs

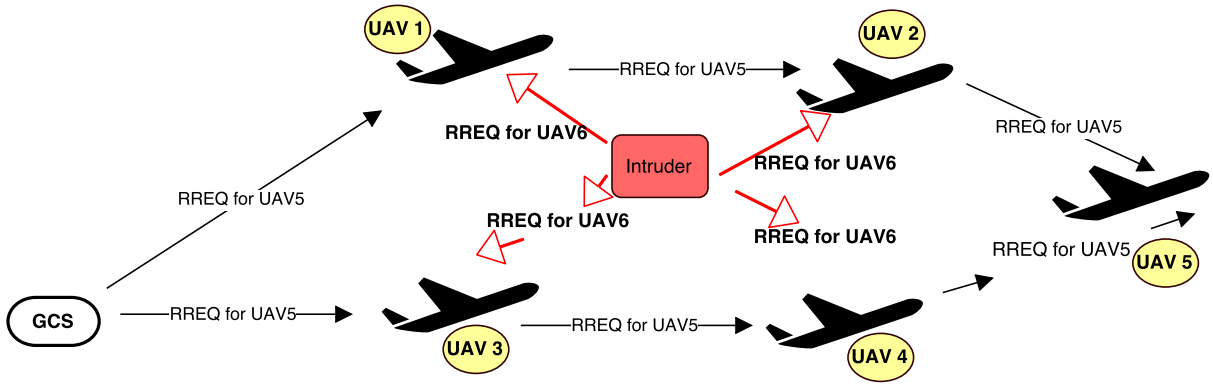


Figure 10. Illustration of sleep deprivation attack in UAANETs

attack can isolate UAVs and prevent them from communicating with other nodes in the network. On the other hand, in cases of OLSR based routing protocol, an intruder advertises forged routes by broadcasting a forged link. As a result, the victim may choose the malicious node as its MPR. In addition, the attacker can delete or modify TC messages and other routing traffic from the victim. It can also discard the payload traffic arriving from the victim intended for a different destination.

d) Sybil attack on UAANET: Within an UAANET, nodes are required to have unique IP address to participate in routing. Since there is no central authority to verify this rule, an attacker can attempt to send multiple control packets using different identities. This is called Sybil attack. The adversary node could use random identities or the identity of another node to create confusion in the routing process. Moreover, this attack could used to disable all links related to a UAV or a set of UAVs. An attacker may pretend to be all the neighbors of a set of UAVs by generating and sending beacon messages with an optimized value (fresh sequence number and TTL values) to invalidate communication links.

e) Wormhole attack in UAANETs: The wormhole attack involves two attackers which perform a colluding attack. One attacker records packets at a particular location and replays them to another attacker by using a high-speed private network. This tunnel between two colluding attackers is referred to as a wormhole. Due to the wireless links, attackers are able to receive data packets not addressed to them. It should be noted that if wormholes are created purely for packet relaying purposes, no harm is done. However, it is unlikely that the attackers will remain passive after gaining the other nodes' trust. In such cases, the attackers can perform additional types of attack such as blackhole, flooding attacks or rushing attacks. Figure 11 demonstrates an example scenario of this attack within UAANETs, where *A1* and *A2* are the colluding attackers while the GCS is the victim node. When the GCS broadcasts a RREQ message to find a route to UAV4, the immediate neighbor UAV1 (one hop away) forwards the message to its respective neighbors. However, the attacker

eavesdrops the message and forwards it through the tunnel to its colluding partner A2 without modifying the packets. The latter performs the same operation and broadcasts the request to the destination node UAV4. As a consequence UAV1 will believe that UAV4 is in its vicinity as the route GCS-UAV1-UAV4 is shorter than the route GCS-UAV1-UAV2-UAV3-UAV4. Once the wormhole tunnel is selected as a path, the malicious attackers can discard, or modify data traffic.

f) Rushing attack in UAANETs [49]: This is a DoS-type attack against all conventional on-demand MANET routing protocols. In [144], it is stated that even security protocols such as SAODV [145] and SUCV [146] were shown vulnerable to rushing attacks. It consists of deleting or modifying the random emission delay that is used by each node before rebroadcasting a received RREQ in on-demand routing protocols. A malicious node can then prioritize its own request packet and cause the automatic rejection of other legitimate RREQ packets by the route discovery algorithm itself. As a result, the route containing the attacker will have a greater chance of being chosen to deliver traffic.

g) Route cache poisoning: In route cache poisoning [135] attacks, attackers take advantage of the promiscuous mode of routing table updating, where a node overhearing any packet may add the routing information contained in that packet header to its own route cache, even if that node is not on the path. If a malicious node M wants to poison routes to node X, M could broadcast spoofed packets with the source route to X via M itself. Thus, neighboring nodes that overhear the packet may add the route to their route caches. This attack consists in inserting incorrect routing information into routing caches of reliable nodes. It targets source routing algorithms (e.g: DSR).

h) Routing table overflow attack: The attacker advertises routes towards non-existent nodes. In this manner the attacker tries to build enough routes to prevent new valid routes from being created. It should be noted that this attack can impact the proactive routing more heavily since it attempts to discover topology information before data sending. As a result, the attacker can easily send excessive route advertisement in the target vicinity to overflow its routing table.

i) Byzantine attack [147]: A compromised intermediate node works alone, or a set of compromised intermediate nodes works in collusion and carry out attacks such as creating routing loops, forwarding packets through non optimal paths, or selectively dropping packets. These actions result in the disruption or degradation of routing services.

j) Packet forwarding attack in UAANET: This is used to breach integrity and availability. Technically, it consists of delivering packets irregularly by dropping, duplicating or modifying routing packets. This causes the UAVs either not to respond to route request or to execute forged packets inserted by an attacker.

k) Replay attack [148]: The UAANET topology frequently changes because of UAV mobility. This dynamic change means that the current network topology may not even last a few seconds. In UAANETs, the replay attack enables adversary nodes to record legitimate control messages, store and retransmit them at a later time when it is advantageous to manipulate the UAS. Consequently, routing tables are updated with old and stale routes. The route will then be disrupted.

l) Flooding attack on UAANET [134]: This aims to exhaust the network resources such as bandwidth, and consume UAVs and GCS resources such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. For example, in AODV protocols, a malicious node can send a large number of Route Requests (RREQs) in a short period to a destination node that does not exist in the network. AS there will be no reply, these requests will flood the whole network. Typically, in [149], it was shown that a flooding attack can decrease the network throughput by up to 84%.

2) UAANET route maintenance phase attacks: Route maintenance consists of updating routes after route loss or when a link breaks due to node movement. It is processed when there is a better route in the network. Route maintenance is necessary to achieve stability in the network and to reduce the excessive overhead required in discovering a new route. It is triggered by beacon messages exchanged periodically. Attacks targeting this phase consist mainly on performance degradation. The goals of these attacks are to reject control packets, to add redundant and irrelevant traffic into UAANETs, to increase routing load, and finally to add processing delay. As an example, we can refer to the routing algorithm based on AODV and DSR in which Hello messages are exchanged. An error packet is also generated to publish broken routes. These packets are generated to address the mobility of the nodes within the network. A malicious node may exploit these mechanisms by willingly broadcasting false route error or Hello messages, and and thereby preventing the source node (i.e. the victim node in this case) from communicating with the destination.

3) Data forwarding phase attacks: In this case, the malicious nodes have been able to participate in the previous routing protocol process: the routing discovery and maintenance phases. Their focus is on how to disrupt the forwarding of payload traffic in order to make the mission fail. For instance, a malicious node may drop silently or replay or even modify the C2 traffic. In addition, time sensitive communications may be disrupted by delaying the relaying of data packets to their respective next-hop destinations or simply by injecting and forwarding dummy packets

4) Taxonomy of security attacks in UAANETs: Figure 12 illustrates an example of the taxonomy of UAANET routing attacks presented in this section. The successive groups of yellow boxes indicate the action of the attacker. The blue ones show the effect and the white boxes describe the procedure used by the attacker. In Table XIII, the current security solution to these attacks in MANET is presented.

VI. How to secure UAANETs

Many security mechanisms have been proposed in ad hoc literature to ensure network integrity and reliability. These

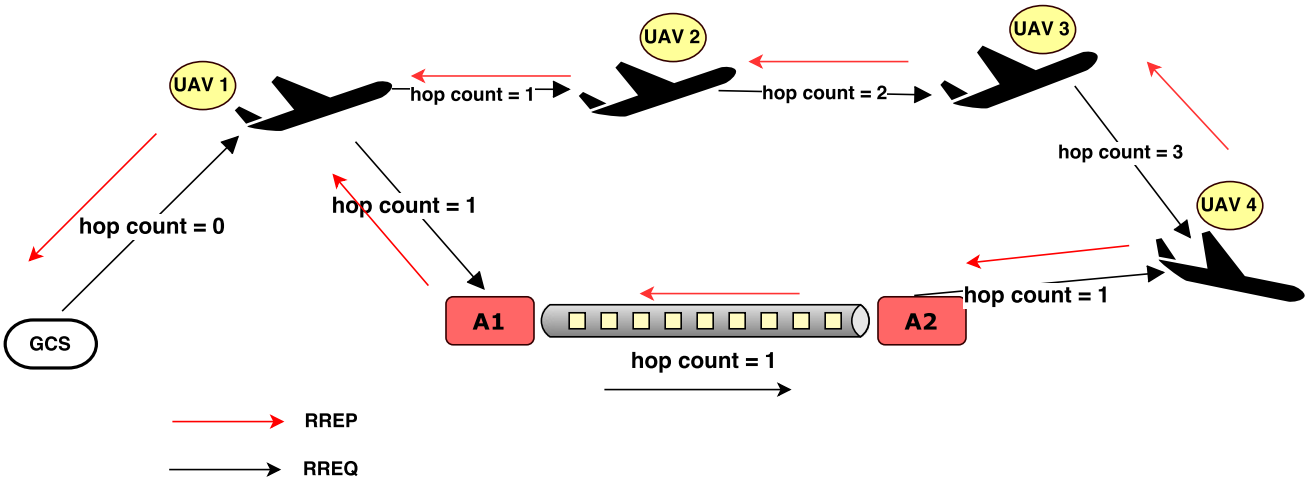


Figure 11. Illustration of wormhole attack in UAANETs

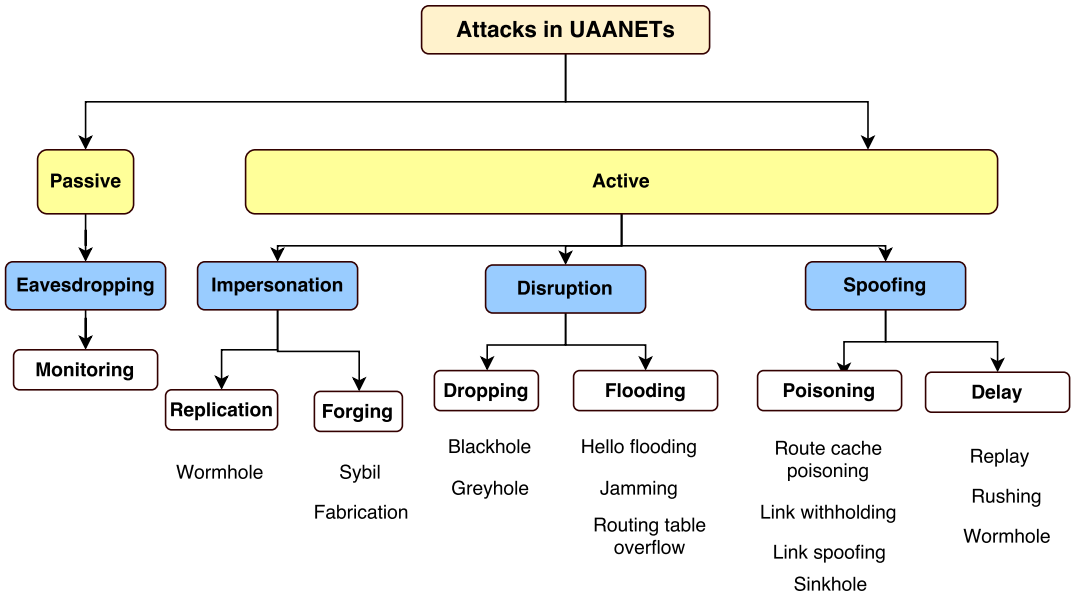


Figure 12. UAANET attack taxonomy

solutions include the use of cryptographic techniques for route discovery and maintenance, the use of reputation-based schemes to select a path from trusted nodes, the use of location and distance information and the use of anomaly detection algorithms. In the following, we will analyze how these different approaches perform in UAANET security.

A. Cryptography technique approach

Cryptography is the science of writing and reading coded messages that will be sent to a recipient through an insecure channel. It plays a major role in achieving secure communications between peers by encrypting messages using cryptography implementations (keys, software or a specific hardware). The original information is then restored from those encoded during decryption. The objective is for data to reach the destination without modification.

Typically, there are two types of cryptography: symmetrical and asymmetrical. A taxonomy of cryptographic mechanisms used in ad-hoc networks is depicted in Figure 13.

1) Symmetrical and asymmetrical cryptography: In symmetrical cryptography, each entity has an encryption/decryption key that is used to encrypt and to decrypt messages from the sender to the destination.

In contrast, in asymmetrical cryptography, the encryption and decryption keys are different. One of the keys (secret key) is memorized and used only by one node, while the other (public key) is distributed to all other nodes. Generally, the public key is used during encryption and the private key during

Routing attacks	Impacted security services	Security solutions
Black hole	- Availability	- Security-aware ad hoc routing protocol (SAR) [150] uses security metric in RREQ packet. It also uses a shared secret to generate a symmetrical cryptographic key
Wormhole	- Availability - Authentication - Confidentiality - Integrity	- Packet leashes [151]
Rushing	- Availability	- Route Discovery Protocol (RAP) [49] that combines secure neighbor discovery mechanism, secure delegation acceptance protocol, and randomized selection of the RREQ to be forwarded
Replay	- Authentication - Integrity	- Solution based on time stamps and asymmetrical encryption. it consists of comparing current time with time stamp embedded in packets from neighbors [152].
Byzantine	- Availability - Confidentiality	- Robust Source Routing (RSR) [153] protocol
Sybil	- Authentication - Confidentiality	- Registration, radio resource testing [154], and position verification [155] - Position-based routing solution [156]
Sleep deprivation	- Availability	- Every node monitors and computes respective RREQ rates of its neighbors. If predefined threshold is exceeded, node places neighbor on blacklist and drops further RREQs [125] - Anomaly-based detection mechanism which learns from statistical analysis of different rates of RREQ packets and computes threshold on the fly [157]
Link Withholding Link Spoofing	- Availability - Integrity	- Detection scheme that relies on spatial information obtained from GPS and time stamp that is encrypted. Each node publishes its GPS coordinates and the time stamp. Each node computes inter nodal distances [158]
Grey hole	- Availability - Confidentiality	Identical to blackhole defense mechanism

Table XIII
SECURITY SOLUTIONS FOR MANET ATTACKS AND VULNERABILITIES

decryption. The advantage is that it is mathematically impossible to deduce the private key from the public key. However, its drawback lies in the complexity of the mathematical function used which may induce a large overhead and long delay.

The UAANET attacks described previously could be avoided with powerful authentication mechanisms in routing protocol between nodes. The key idea is to ensure that only nodes that have been authenticated (trusted nodes) are allowed to exchange routing information. Additionally, other security services such as confidentiality, integrity, non-repudiation and availability can be achieved by encryption and decryption algorithms.

2) Hashing: Hash functions are used to compress an arbitrary length message to a fixed size output, called the hash value. This is generally applied to the message and does not commonly use keys. The hash value is representative of the original data, but smaller than the original. A Message Authentication Code (MAC) is a one-way hash function whose hash value depends both on the message content and the key used.

Good cryptographic hash functions "h" must have the following properties:

- A given hash value is only associated with one piece of data. Any character difference must induce a different hash value.
- It must be a one way hash function, meaning that it is mathematically impossible to obtain the original data from the hash value.

By sending the message with its associated hash value, the recipient node is able to deduce whether or not the data has been modified. Several hash functions are known in literature, such as MD2, MD4, MD5, Secure Hash Algorithm (SHA) and HMAC.

3) Hash chains: Hash chains are based on one way hash functions. A hash chain of length N is constructed by applying a hash function "h" N times to a random value "seed".

$$\begin{Bmatrix} h_i(Y) = h(h_{i-1}(Y)) \\ h_0(Y) = seed \end{Bmatrix}$$

The destination node only applies the hash function once to verify the received hash value which is used to for data integrity verification.

4) Authentication techniques: UAANET security protocols are based on communication exchange rules between UAVs and GCS that must be respected in different security applications. As in MANET, the authentication solution applied in UAANET should be accurately selected as a minor modification of the rules or a slight rearrangement in the configuration may lead to unexpected results.

a) Digital Signatures: The digital signature mechanism can be used to achieve authentication between nodes in UAANETs. It binds the signature to the message before sending data packets. Since forging of electronic communication is relatively easy, a verification mechanism on the recipient side must be set up. This verification can be achieved with a public verification algorithm. This algorithm has some important features which allow the authentication mechanism to take place:

- Unforgeability: It shows the commitment of the sender;
- Authenticity: It shows the authenticity of the message being sent to the receiver;
- Non-reusability: It ensures that the signature cannot be reused ;
- Non-alterability: It guarantees that the message will not be modified on the route between the sender and the receiver

It should be noted that it is crucial to deploy shorter signatures to maintain a low communication overhead. Additionally, one must take into account the real-time requirements of UAANET communication. Care should be taken to minimize signature binding delay to optimize end-to-end delays between two nodes and therefore to limit packet loss and robustness against DoS attacks. The following requirements should be satisfied.

- Fast generation of authentication information, and fast verification of receiver.
- Instant authentication without packet buffering
- Robustness to packet loss
- Minimum communication overhead
- Scalability (with number of nodes)

b) Message authentication: Message authentication consists of protecting the integrity of a message and validating the identity of the message originator. Usually, a message authentication code (MAC) is sent along with the message. The MAC is generated through an algorithm which depends on both the message and on some (private or public) keys that are known only to the sender and receiver. It is important to underline that the MAC length should preferably be of fixed size, requiring the use of a hash function mechanism to shorten the message size.

c) Node authentication: There are 3 existing security approaches for node authentication in the MANET family.

1) The Key agreement in which nodes agreed on a secret key beforehand [159]. Existing schemes are mostly key agreement protocols such as the two-party Diffie-Helman (DH) scheme [160], a common key for group communications [161], and the Encrypted Key Exchange (EKE) protocols [162] which generate a long-term key from a shared password.
2) The Duckling Security Policy model [163] in which RoSS Anderson et al. use the master-slave principle to share secret keys.
3) Public key infrastructure: the main objective for developing a PKI for UAANETs is to enable secure, convenient, and efficient acquisition of public keys between UAVs. Such a key management scheme includes key distribution and key revocation. Key distribution shares the secret keys to UAVs for secure communication while key revocation securely enlists and removes compromised keys.

   The prerequisites of implementing such an operation are: (i) the presence of a CA (Certificate Authority) to manage the life-cycle of digital certificates; (ii) a distribution method for CA capabilities among entities; and (iii) the availability of the CA to the nodes. It should be noted that existing MANET solutions rely on a distributed Certificate Authority (CA) based on threshold cryptography [164]. Each public key belonging to a given node is segregated into **n** shares issued among **n** nodes. A number k<n of nodes must sign the certificate to be valid. In such a scheme, each node generates its signature and gathers signatures from the others. Using such scheme, a UAANET is robust against attackers which can compromise no more than k-1 nodes.

B. Reputation and Trust based systems

Reputation and trust can be used to handle forwarding decisions in UAANETs in which nodes are heterogeneous. It is often used to reinforce MANET security in cases where the cryptographic security block has somehow been compromised. Typically, reputation techniques consist of an opinion made by one node of another. As for trust, this represents the expectation of one node concerning the actions of another node. This approach is generally used in heterogeneous network nodes in which we assume that a node may eventually try to be selfish and ignore the network pattern. Such a case can indeed happen in a UAANET in which multiple UAVs and GCS from different manufacturers can exchange information as described in [45].

C. Intrusion detection in UAANETs

In traditional wired networks, prevention techniques can be limited and ineffective. As a result, an IDS has been introduced to detect violations of security system. An intrusion in a network can be defined as "any set of actions that attempt to compromise network integrity, confidentiality or availability of resources". To mitigate an intrusion, many prevention techniques have been proposed either based on authentication and encryption or on demand monitoring. Once an attack is detected, a response can be initiated to minimize system damage. Among IDS based approaches proposed for MANET, we can refer to specification-based, specification-based intrusion detection [165], anomaly-based intrusion detection [166], misuse-based intrusion detection [167], and promiscuous monitoring-based intrusion detection [168].

Specification-based intrusion detection consists of detection based on the violation of routing protocol specification. It is used to detect modification and forged attacks. In [169], this mechanism is used for AODV and OLSR protocols. Each node monitors its direct neighbors during route request and route response exchanges. The objective is to verify whether or not the next hop forwarded the route discovery packets. Typically, specification-based IDSs cannot detect attacks that violate protocol specification directly [170]. As a result, several propositions have been made in which a signature analysis tool is introduced to detect DoS attacks.

Anomaly-based intrusion detection is used to measure the difference between normal and abnormal behaviors of a given system. Measurement can be applied to several metrics such as the frequency of commands launched, the CPU usage, the time required to launch a program, and the usual output of a command. These measures can be obtained through various techniques such as statistical approaches, data mining, etc.... The accuracy of this technique relies on what is specified as normal behavior. It means that to avoid false positives, each node must know the normal registered activities and adapt in case of change.

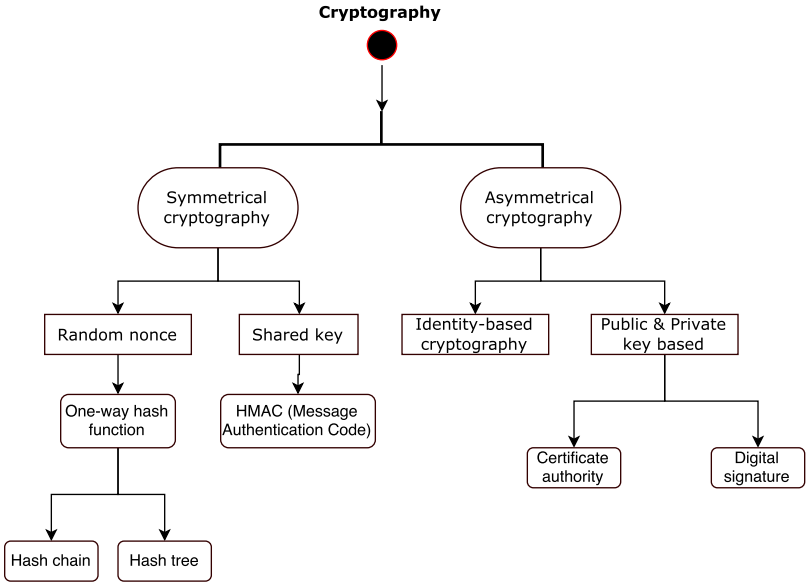


Figure 13. Cryptographic techniques used in MANETs and and suitable for UAANETs

Misuse-based IDSs consist of comparing current system activities with a known attack strategy. As a result, they can only useful for a known attack and becomes obsolete in face of new attacks.

Promiscuous monitoring-based intrusion detection takes advantage of the promiscuous capabilities of each node. It can detect nodes that are dropping or modify data packets before forwarding them. The weakness of this approach is that it can generate false positives when an ambiguous collision occurs or during network queuing.

VII. Summary of secure mechanisms for improving routing protocols in UAANETS

A routing protocol is defined as secure if it preserves routing algorithm accuracy and reliability in the presence of malicious attackers. On one hand, accuracy properties refer to routing protocol abilities to find valid routes that respect routing process rules and on the other hand, reliability refers to routing protocol capacity to return accurate routes in the face of malicious or non-malicious failures (mobility, hardware failure). Indeed, to preserve efficiency in a malicious environment, a routing protocol must be able to find valid routes and at the same time mitigate route failures when they occur.

Several secure routing protocols exist for MANETs and VANETs [171]. In this paper, we will focus on the AODV routing protocol specifically as it seemed to emerge specifically as, regarding performances, it compared well to other well known routing protocols [33]. It should also be noted that as far as we know, there has not yet been a secure routing protocol proposed for UAANETs.

The choice of AODV is motivated by the followings:

- Network characteristics: During a UAANET mission, each UAV will be assigned to a specific role. It can be a forwarder node (node that forwards data packets) that is used to extend scalability or the node that actually performs the aerial monitoring. This implies that most of the time, each node will have a specific role until the end of the mission and mode density will neither decreased nor increased.
  Accordingly, nodes are not required to maintain connectivity with all other nodes but only with direct neighbors. Therefore, routing protocol should be reactive so that routing protocol packets do not consume bandwidth (which should be allocated to c2 and payload traffic)
- Optimized end-to-end delay, overhead, and connectivity ratio values: with low density and realistic mobility models, AODV outperforms DSR and OLSR as studied in [33] [72] [73].

A. Existing secure AODV routing protocols

The set of existing secure extensions in MANET is represented in table XIV.

B. Security solutions for UAANETs based on AODV

A routing protocol provides security if it preserves protocol accuracy and reliability in the face of malicious attackers. It must find valid routes by securing the routing process. It must also mitigate route failures once they occur by securing the data forwarding phase. Similarly, the route maintenance phase should be protected to avoid topology modification caused by attacks.

Furthermore, a UAANET routing protocol is secure if at least the message authentication and data integrity are ensured. Control packet confidentiality is not mandatory compared to the security strength it may provide. Indeed, routing packets are processed in real time by a set of flying of UAVs. As such, even if an attacker is able to eavesdrop the message, its action

Routing protocols	Authentication	Integrity	Availability	No-repudiation	Security primitives
SAODV [172]	Yes	Yes	No	Yes	- Digital signature - Packet double signature - Hash chains
AODV-SEC [173]	yes	yes	No	Yes	- Digital signature - HMAC - Hash chain
MSAODV [174]	yes	yes	No	Yes	- Asymmetrical cryptography
RAODV [175]	Yes	Yes	No	Yes	- Additional control packets (RRPDU, RRPDU-REP) and data fields
ISAODV [176]	Yes	Yes	No	Yes	- Additional fields - IDS system
SAR [150]	Yes	Yes	No	Yes	
A-SAODV [177]	Yes	Yes	No	Yes	- Digital signature - Hash chains
DPRAODV [48]	Yes	No	No	No	- Sequence number verification - Blacklist
RIDAN [178]	No	Yes	No	No	- Timed finite state machines (TF-SMs)
NDTAODV [179]	Yes	No	No	No	- Broody list - RREQ count table
ARAN [180]	Yes	Yes	No	Yes	- PKI - Digital Signature - Hash function - Asymmetrical cryptography
TAODV [181]	Yes	Yes	No	Yes	- Digital signature - Hash chains

Table XIV
EXISTING SECURE AODV ROUTING PROTOCOLS

is limited in passive mode because in the future, the previous information is no longer valuable.

1) Solution for message authentication: Message authentication ensures that within the network, a node must prove its identity for every communication session with any other node in the network. This implies that an adversary node cannot impersonate authenticated node in the network. Consequently, the network is protected against compromised nodes.

One of the methods that can be used is the principle of asymmetrical key cryptography, e.g. with digital signatures. As in SAODV, a node generating a route discovery message signs it with its private key, The nodes that receive this message verify the signature using the sender's public key. This mechanism can be used for all message fields, as in ARAN protocol [180]. However, it will induce a large amount of overhead and expensive authentication computation. Depending on UAV size, such an approach may not be a problem for certain types of UAVs (e.g. Delair Tech UAV [182]) as the speed of signature encapsulation and verification lies in the computation capability and storage capacity. For UAVs that have energy limitation, one candidate is required to differentiate the variable and static fields of the packets as in SAODV. Static fields regroup the chunk of non-mutable data from the sender to the receiver, such as sender or/and destination address. A digital signature can be applied to these fiels since a hop by hop signature encapsulation is not required. For the mutable fields (the hop count), we can apply a symmetrical cryptography approach based on hashing. However, such an approach is not robust against wormhole attacks [183]. Moreover, it is important to underline that in this case, each node requires a public/private key pair, a certificate binding its identity to its public key (signed by a trusted certificate server), and the public key of the trusted certificate server. All nodes are deployed with the private part of a public/private key pair. Prior to deployment, each node will request a certificate from a trusted certificate server T. The certificate binds node identity with its public key and is signed by T. The certificate is time stamped and has an expiration time. Each node will possess T's public key so it can decrypt certificates of other nodes. This allows a node N1 to inform another node N2 of its public key, assuming node N2 was deployed correctly with T's public key to decrypt certificates.

Furthermore, another technique that can be used is the use of symmetrical cryptography based on hashing on all fields of routing packets as in [184]. Such an approach would be lightweight and computationally efficient as only a one-way hash chain mechanism is involved. These mechanisms require key generation and distribution during bootstrapping. Generally, two key hierarchies are needed [185]: one for unicast communication to its direct neighbors and one for broadcast communication. Considering Figure 14, each UAV must generate a single group key called uK and one pairwise key for each neighbor, called bK. When the GCS wants to broadcast a message to all its neighbors, it generates a MAC (or a modified HMAC in [184]) for each individual neighbor using the broadcast key bk. UAV1 and UAV2 use their private

key uK to authenticate the message.

Typically, such a mechanism would wor but only if the key exchange mechanism and distribution are secure. If not, the keys can be compromised and the entire network becomes vulnerable. Accordingly, the TESLA authentication protocol [186] is used in [187]. However, it can induce a high probability of false positive because it requires synchronization with secure time synchronization protocol and time servers. As a result, the synchronization mechanism must be secure to avoid DoS attacks. In addition, the propagation delay is shorter than the processing delay. Therefore, a specific hardware should be deployed on-board UAVs to avoid false positive alerts. Similarly, the work in [185] proposes the idea of computing a broadcast key association between neighbors using hello messages. Nonetheless, such an approach would still be vulnerable against wormhole attacks. A potential solution is to include packet leashes [188] in the packet.

2) Solution for routing packet integrity: To ensure data integrity, a common method is to use symmetrical cryptography through a hashing mechanism. A digital signature can also be used as in [180]. However, as stated previously, this is not suitable for small sizes UAVs as it induces computational overhead. When hashing is used, it is applied to mutable fields as in SAODV. A hash tree can also be used when several individual mutable fields need to be secured. An example is the Merkle authentication tree [189] where different secret values are committed to a full binary tree. Furthermore, the hash tree chain can also be used to enforce the hash tree property. A hash tree chain is a hybrid hashing between a hash tree and a one-way chain. In such a case, the one way chain is used to protect the routing metric, while the hash-tree authenticates node identities.

3) Solution for confidentiality: To ensure control packet confidentiality, hybrid encryption techniques can be used as it is the case in [190]. In this scheme, some assumptions about the presence of valid and trusted CA are made. During neighbor discovery, a source node generates and signs a hello message and includes its certificate. When neighbor nodes receive the beacon message, they verify the signature before replying with a signed hello message. During route discovery, the source node generates a signed RREQ. This packet is firstly encrypted with random symmetric key and then signed a second time with the public key of each node in the trusted neighbor table. When the destination node receives the message, it decrypts the symmetrical key using its private key and uses it to decrypt the message. This approach ensures confidentiality because a given node does not have the private key associated with the public key stored in the predecessor node. However, the use of hybrid encryption introduces considerable computational overhead and additional delay.

In [191], Wu et al., proposed to split the data packets into different flows, each forwarded through different paths. By splitting the traffic in a random way, the traffic pattern can be hidden from any malicious node, thus providing traffic confidentiality. However, this technique depends on the use of a multi-path routing protocol that can find multiple routes between source and destination. Consequently, this solution is only relevant with high network density. Otherwise, it may be beneficial to split the channel into multiple component channels and use diversity coding as explained in [192]. However, message splitting and reconstructing may introduce additional delay and overhead.

4) Secure data forwarding: Once routes are established through previous service route discovery, the routing protocol can be vulnerable in the face of certain types of attacks such as Byzantine or wormhole attacks. Detecting these attacks is difficult as attackers behave correctly and follow the routing rules. Once malicious or suspicious activity occurs, the secure routing protocol must take steps to mitigate the effects. Accordingly, mitigation techniques may include utilizing multipath routing protocols or using protocols based on a trust metric to monitor links for malicious activity. This would enable the identifcation of suspicious nodes in the network and eliminate them to ensure future route discovery reliability and accuracy.

5) A case study: SAODV: SAODV is an enhancement of the AODV routing protocol to prevent malicious actions from external nodes. The extension message includes a digital signature of the AODV packet using the private key of the sender and a hash value of the hop count. It uses asymmetrical cryptography to authenticate all static fields of routing messages and symmetrical cryptography (hash chain) for the mutable fields. Neighbor nodes authenticate the variable fields using the public key of the sender. If the signature is verified, the integrity of the hop count is checked through the computation of the hash value of the actual hop count. If these match, the routing message is accepted as valid and processed. If it reaches the destination node, it will be processed and a response packet will be generated. Otherwise, it will be forwarded with an incremented hop count value and a new hash value. The same process is used for the RREP packets. As for RERR messages, all of the fields are signed by every node since it does not contain mutable fields.

The SAODV mechanism is robust against impersonation and modification attacks(e.g. blackhole, greyhole). However, the existence of colluding attackers performing wormhole attacks cannot be detected. A detailed comparison of existing wormhole detection techniques for MANETs is presented in [193]. In the following, we will present a possible solution for wormhole attacks that could work on UAANETs.

a) Packet leashes: One way to defend the network against wormhole attacks is to use packet leashes. Their use is not recommended by the literature with most MANETs nodes because of synchronization requirements that are difficult to fulfill in constraint environment. However, this is not the case in UAANETs because all of the UAVs are equipped with a GPS which is principally used for navigation. Accordingly, it is relevant to rely on such leverage to obtain node synchronization. The purpose of packet leashes is to add additional information to the packet to restrict maximum allowed transmission distance. Two types of packet leashes exist in the literature:

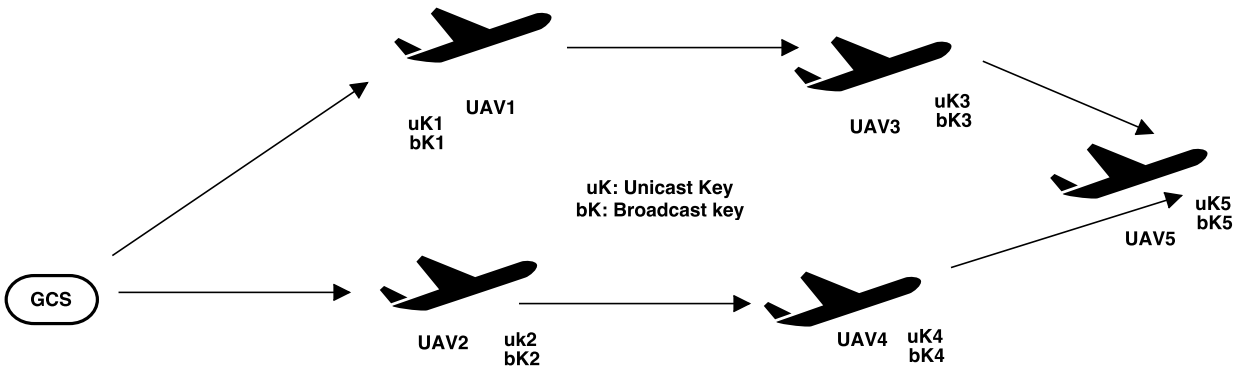


Figure 14. Cryptographic techniques used in MANETs and which can be used in UAANETs

temporal leashes and geographical leashes.

On one hand, temporal leashes consist of including an expiration time in the packet so that it will not processed by the receiver if the timer expires. Even though clock synchronization is feasible in UAANETs, this solution will induce too much false positive because the propagation delay is not greater than the processing delay and the queuing delay, thus the difference will depend more on those variables than the propagation delay. This is the case as data packets are exchanged with the speed of light ($c = 3 * 10^8 ms^{-1}$). When interference occurs, data will be delayed for a number of milliseconds which is greater than the nanoseconds of the propagation delay. It is also trivial to estimate the processing and queuing delay as it depends on the presence of interference. A workaround would be to deploy a special hardware to eliminate the difference delay (queuing and processing) in the MAC layer.

On the other hand, geographical leashes consist of bounding the distance between two neighbor nodes by the formula: $dsr \leq ||ps - pr|| + 2V(tr - ts + \alpha) + \delta$

where dsr is the distance between the sender and the receiver; ps and pr represent respectively, the location information of the source and destination node. The variable tr and ts represent the reception and sending time. And V represents the upper bound of node velocity. This method only works when the network is free of obstacles, which is unlikely considering UAANET topology. Accordingly, one solution is to compute a mathematical relationship between the distance traveled by the packet and the hop count that should be included included in the packet. Since wormhole attacks consist of replaying packets without modification, a packet tends to travel further with a low hop count value.

b) Directionnal antenna: For UAVs that are equipped with a directional antenna, it is possible to use directional antenna, directional antenna capabilities maybe used to implement a strick neighbor discovery protocol [194]. Nodes are oriented with different directional zones of transmission, and the zone of transmission is included in route discovery packets. When receiving data packets, the directional antennas allow a node to establish the zone from which a transmission is received. If the direction of transmission is the opposite of the direction zone in which the transmission is received, the packet is accepted. Otherwise, it will be ignored.

VIII. Conclusions

The UAV Ad hoc Network (UAANET) is becoming a popular type of network in the MANET networks family. Compared to other possibilities of UAV swarm network architecture, it has several advantages such as scalability reliability improvement, effective bandwidth uses and inter-drone communication. etc. Given the specific features of UAANET, an adaptive routing protocol is required to satisfy UAANET requirements as explained previously. These requirements consists of ensuring a small delay during communication, a recovery mechanism to repair routes in case of route loss and a large bandwidth for C2 traffic exchanges. Accordingly, in this paper we highlight UAANET communication architecture. We also present a taxonomy of UAANET routing protocols which we have divided into five categories: (i) reactive, (ii) pro-active, (iii) hybrid, (iv) geographical routing and (v) hierarchical. For each of these classes, we have reviewed and given feedback about their strengths and weaknesses. They usually share common goals which are to reduce control packet overhead, maximize throughput and minimize end-to-end delay. The main differentiating factor between protocols is route discovery and maintenance mechanisms. Nonetheless, one of their common features is the lack of consideration for security. Since each node is required to cooperate and exchange messages through wireless links, the lack of a fixed infrastructure to separate the inside from the outside enables attacks within. As a result, UAANETs are vulnerable to different types of attacks which can have severe consequences considering that UAVs are flying in national airspace. Therefore, securing UAANET routing is crucial. In this paper, we have presented a comprehensive state-of-the-art regarding UAANET security challenges. Some security issues such as security requirements, adversary profiles and attacks on UAANETs have been pointed out. We have also pointed out some potential candidates to improve routing security

We hope this research represents a step towards the design and development of accurate and reliable security routing

protocols to support the protection of critical traffic exchanged between UAVs and GCS.

REFERENCES

[1] W. M. DeBusk, "Unmanned aerial vehicle systems for disaster relief: Tornado alley," in *AIAA Infotech@ Aerospace Conference, AIAA-2010-3506, Atlanta, GA*, 2010.

[2] D. Hausamann, W. Zirnig, G. Schreier, and P. Strobl, "Monitoring of gas pipelines-a civil uav application," *Aircraft Engineering and Aerospace Technology*, vol. 77, no. 5, pp. 352–360, 2005.

[3] L. Meier, D. Honegger, and M. Pollefeys, "Px4: A node-based multithreaded open source robotics framework for deeply embedded platforms."

[4] E. Zurich, "Qgroundcontrol: Ground control station for small air land water autonomous unmanned systems," 2013.

[5] L. Meier, P. Tanskanen, L. Heng, G. H. Lee, F. Fraundorfer, and M. Pollefeys, "Pixhawk: A micro aerial vehicle design for autonomous flight using onboard computer vision," *Autonomous Robots*, vol. 33, no. 1-2, pp. 21–39, 2012.

[6] "dronecode," https://www.dronecode.org, 2015, [Online; accessed 09-octobre-2015].

[7] G. KroahHartman, J. Corbet, and A. McPherson, "Linux kernel development," *the Linux foundation*, 2008.

[8] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer networks*, vol. 52, no. 12, pp. 2292–2330, 2008.

[9] H. Hartenstein and K. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *Communications Magazine, IEEE*, vol. 46, no. 6, pp. 164–171, 2008.

[10] Q. Vey, A. Pirovano, J. Radzik, and F. Garcia, "Aeronautical ad hoc network for civil aviation," in *Communication Technologies for Vehicles*. Springer, 2014, pp. 81–93.

[11] S. Rosati, K. Kruzelecki, L. Traynard, and B. Rimoldi, "Speed-aware routing for uav ad-hoc networks," in *Globecom Workshops (GC Wkshps), 2013 IEEE*. IEEE, 2013, pp. 1367–1373.

[12] J.-F. Raymond, "Traffic analysis: Protocols, attacks, design issues, and open problems," in *Designing Privacy Enhancing Technologies*. Springer, 2001, pp. 10–29.

[13] I. Bekmezci, O. K. Sahingoz, and Ş. Temel, "Flying ad-hoc networks (fanets): A survey," *Ad Hoc Networks*, vol. 11, no. 3, pp. 1254–1270, 2013.

[14] E. W. Frew and T. X. Brown, "Networking issues for small unmanned aircraft systems," *Journal of Intelligent and Robotic Systems*, vol. 54, no. 1-3, pp. 21–37, 2009.

[15] J. Li, Y. Zhou, and L. Lamont, "Communication architectures and protocols for networking unmanned aerial vehicles," in *Globecom Workshops (GC Wkshps), 2013 IEEE*. IEEE, 2013, pp. 1415–1420.

[16] L. Gupta, R. Jain, and G. Vaszkun, "Survey of important issues in uav communication networks."

[17] K. Namuduri, Y. Wan, and M. Gomathisankaran, "Mobile ad hoc networks in the sky: state of the art, opportunities, and challenges," in *Proceedings of the second ACM MobiHoc workshop on Airborne networks and communications*. ACM, 2013, pp. 25–28.

[18] O. K. Sahingoz, "Networking models in flying ad-hoc networks (fanets): Concepts and challenges," *Journal of Intelligent & Robotic Systems*, vol. 74, no. 1-2, pp. 513–527, 2014.

[19] S. K. Singh, "A comprehensive survey on fanet: Challenges and advancements."

[20] A. Maghsoudlou, M. St-Hilaire, and T. Kunz, "A survey on geographic routing protocols for mobile ad hoc networks," *Systems and Computer Engineering, Technical Report SCE-11-03.–Carleton University.–2011.–49 p*, 2011.

[21] L. Song and T.-L. Huang, "A summary of key technologies of ad hoc networks with uav node," in *Intelligent Computing and Integrated Systems (ICISS), 2010 International Conference on*. IEEE, 2010, pp. 944–949.

[22] Z. Zhao and T. Braun, "Topology control and mobility strategy for uav ad-hoc networks: A survey," in *Joint ERCIM eMobility and MobiSense Workshop*, 2012, pp. 27–32.

[23] I. Bekmezci, E. Senturk, and T. Turker, "Security issues in flying ad-hoc networks (fanets)."

[24] O. K. Sahingoz, "Mobile networking with uavs: opportunities and challenges," in *Unmanned Aircraft Systems (ICUAS), 2013 International Conference on*. IEEE, 2013, pp. 933–941.

[25] I. Annex, "to the convention on international civil aviation," *Volume II, Heliports*, 14.

[26] K. Dalamagkidis, "Classification of uavs," in *Handbook of Unmanned Aerial Vehicles*. Springer, 2014, pp. 83–91.

[27] R. Loh, Y. Bian, and T. Roe, "Uavs in civil airspace: Safety requirements," *Aerospace and Electronic Systems Magazine, IEEE*, vol. 24, no. 1, pp. 5–17, 2009.

[28] T. X. Brown, B. Argrow, C. Dixon, S. Doshi, and P. Nies, "Ad hoc uav-ground network (augnet) test bed," in *4th Scandinavian Workshop on Wireless Ad-hoc Networks, May*, 2004, pp. 4–5.

[29] S. Gruber, H. Kwon, C. Hager, R. Sharma, J. Yoder, and D. Pack, "Uav handbook: Payload design of small uavs," in *Handbook of Unmanned Aerial Vehicles*. Springer, 2014, pp. 143–163.

[30] P. Fahlstrom and T. Gleason, *Introduction to UAV systems*. John Wiley & Sons, 2012.

[31] O. Bouachir, A. Abrassart, F. Garcia, and N. Larrieu, "A mobility model for uav ad hoc network," in *Unmanned Aircraft Systems (ICUAS), 2014 International Conference on*. IEEE, 2014, pp. 383–388.

[32] J.-A. Maxa, B. Mahmoud, M. Slim, and N. Larrieu, "Secure routing protocol design for uav ad hoc networks," in *Digital Avionics Systems Conference (DASC), 2015 IEEE/AIAA 34th*. IEEE, 2015, pp. 4A5–1.

[33] J.-A. Maxa, G. Roudiere, and N. Larrieu, "Emulation-based performance evaluation of routing protocols for uaanets," in *Communication Technologies for Vehicles*. Springer, 2015, pp. 227–240.

[34] J.-A. Maxa, "Model-driven approach to design a secure routing protocol for uav adhoc networks," in *EDSYS 2015, 15ème Congrès des doctorants*, 2015.

[35] K. Zhang, W. Zhang, and J.-Z. Zeng, "Preliminary study of routing and date integrity in mobile ad hoc uav network," in *2008 International Conference on Apperceiving Computing and Intelligence Analysis*, 2008.

[36] A. I. Alshbatat and L. Dong, "Cross layer design for mobile ad-hoc unmanned aerial vehicle communication networks," in *Networking, Sensing and Control (ICNSC), 2010 International Conference on*. IEEE, 2010, pp. 331–336.

[37] B.-N. Cheng and S. Moore, "A comparison of manet routing protocols on airborne tactical networks," in *MILITARY COMMUNICATIONS CONFERENCE, 2012-MILCOM 2012*. IEEE, 2012, pp. 1–6.

[38] F. A. Aloul and N. Kandasamy, "Sensor deployment for failure diagnosis in networked aerial robots: a satisfiability-based approach," in *Theory and Applications of Satisfiability Testing–SAT 2007*. Springer, 2007, pp. 369–376.

[39] R. Shirani, M. St-Hilaire, T. Kunz, Y. Zhou, J. Li, and L. Lamont, "Combined reactive-geographic routing for unmanned aeronautical ad-hoc networks," in *Wireless Communications and Mobile Computing Conference (IWCMC), 2012 8th International*. IEEE, 2012, pp. 820–826.

[40] L. Reynaud and T. Rasheed, "Deployable aerial communication networks: challenges for futuristic applications," in *Proceedings of the 9th ACM symposium on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks*. ACM, 2012, pp. 9–16.

[41] Y. Li, M. St-Hilaire, and T. Kunz, "Improving routing in networks of uavs via scoped flooding and mobility prediction," in *Wireless Days (WD), 2012 IFIP*. IEEE, 2012, pp. 1–6.

[42] S. Rohde, N. Goddemeier, K. Daniel, and C. Wietfeld, "Link quality dependent mobility strategies for distributed aerial sensor networks," in *GLOBECOM Workshops (GC Wkshps), 2010 IEEE*. IEEE, 2010, pp. 1783–1787.

[43] N. Shi and X. Luo, "A novel cluster-based location-aided routing protocol for uav fleet networks," *International Journal of Digital Content Technology and its Applications*, vol. 6, no. 18, p. 376, 2012.

[44] R. Laplace, "Applications et services dtn pour flotte collaborative de drones," Ph.D. dissertation, Université Sciences et Technologies-Bordeaux I, 2012.

[45] J. Elston, E. W. Frew, D. Lawrence, P. Gray, and B. Argrow, "Net-centric communication and control for a heterogeneous unmanned aircraft system," *Journal of intelligent and Robotic Systems*, vol. 56, no. 1-2, pp. 199–232, 2009.

[46] B. Bellur, M. Lewis, and F. Templin, "An ad-hoc network for teams of autonomous vehicles," in *Proceedings of the First Annual Symposium on Autonomous Intelligence Networks and Systems*. Citeseer, 2002.

[47] R. H. Jhaveri, S. J. Patel, and D. C. Jinwala, "Dos attacks in mobile ad hoc networks: A survey," in *Advanced Computing & Communica-*

tion Technologies (ACCT), 2012 Second International Conference on. IEEE, 2012, pp. 535–541.

[48] P. N. Raj and P. B. Swadas, "Dpraodv: A dyanamic learning system against blackhole attack in aodv based manet," *arXiv preprint arXiv:0909.2371*, 2009.

[49] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," in *Proceedings of the 2nd ACM workshop on Wireless security*. ACM, 2003, pp. 30–40.

[50] S. Chaumette, R. Laplace, C. Mazel, R. Mirault, A. Dunand, Y. Lecoutre, and J.-N. Perbet, "Carus, an operational retasking application for a swarm of autonomous uavs: First return on experience," in *MILITARY COMMUNICATIONS CONFERENCE, 2011-MILCOM 2011*. IEEE, 2011, pp. 2003–2010.

[51] D. Johnson, Y. Hu, and D. Maltz, "The dynamic source routing protocol (dsr) for mobile ad hoc networks for ipv4," Tech. Rep., 2007.

[52] K. Daniel, B. Dusza, A. Lewandowski, and C. Wietfeld, "Airshield: A system-of-systems muav remote sensing architecture for disaster response," in *Systems Conference, 2009 3rd Annual IEEE*. IEEE, 2009, pp. 196–200.

[53] S. Cameron, S. Hailes, S. Julier, S. McClean, G. Parr, N. Trigoni, M. Ahmed, G. McPhillips, R. De Nardi, J. Nie *et al.*, "Suaave: Combining aerial robots and wireless networking," in *25th Bristol International UAV Systems Conference*, 2010, pp. 1–14.

[54] R. Nair, M. Tambe, M. Yokoo, D. Pynadath, and S. Marsella, "Taming decentralized pomdps: Towards efficient policy computation for multiagent settings," in *IJCAI*, 2003, pp. 705–711.

[55] D. J. Pack, P. DeLima, G. J. Toussaint, and G. York, "Cooperative control of uavs for localization of intermittently emitting mobile targets," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, vol. 39, no. 4, pp. 959–970, 2009.

[56] S. Hauert, S. Leven, J.-C. Zufferey, and D. Floreano, "The swarming micro air vehicle network (smavnet) project," 2015.

[57] T. Clausen and P. Jacquet, "Optimized link state routing protocol (olsr)," Tech. Rep., 2003.

[58] J.-A. Maxa, M.-S. B. Mahmoud, and N. Larrieu, "Extended verification of secure uaanet routing protocol," in *DASC 2016, 35th Digital Avionics Systems Conference*, 2016.

[59] O. Bouachir, F. Garcia, A. Abrassart, and N. Larrieu, "A mobility model for uav ad hoc network," in *International Conference on Unmanned Aircraft Systems (ICUAS), 2014*. IEEE, 2014.

[60] C.-M. Cheng, P.-H. Hsiao, H. Kung, and D. Vlah, "Maximizing throughput of uav-relaying networks with the load-carry-and-deliver paradigm," in *Wireless Communications and Networking Conference, 2007. WCNC 2007. IEEE*. IEEE, 2007, pp. 4417–4424.

[61] ——, "Performance measurement of 802.11 a wireless links from uav to ground nodes with various antenna orientations," in *Computer Communications and Networks, 2006. ICCCN 2006. Proceedings. 15th International Conference on*. IEEE, 2006, pp. 303–308.

[62] O. Bouachir, F. Garcia, N. Larrieu, and T. Gayraud, "Ad hoc network qos architecture for cooperative unmanned aerial vehicles (uavs)," in *Wireless Days (WD), 2013 IFIP*. IEEE, 2013, pp. 1–4.

[63] A. Bürkle, F. Segor, and M. Kollmann, "Towards autonomous micro uav swarms," *Journal of intelligent & robotic systems*, vol. 61, no. 1-4, pp. 339–353, 2011.

[64] R. Jurdak, C. V. Lopes, and P. Baldi, "A survey, classification and comparative analysis of medium access control protocols for ad hoc networks," *Communications Surveys & Tutorials, IEEE*, vol. 6, no. 1, pp. 2–16, 2004.

[65] Y. Li and X. Luo, "Cross layer optimization for cooperative mobile ad-hoc uav network," *International Journal of Digital Content Technology and its Applications*, vol. 6, no. 18, p. 367, 2012.

[66] G. Bianchi, "Performance analysis of the ieee 802.11 distributed coordination function," *Selected Areas in Communications, IEEE Journal on*, vol. 18, no. 3, pp. 535–547, 2000.

[67] J. Yin, T. ElBatt, G. Yeung, B. Ryu, S. Habermas, H. Krishnan, and T. Talty, "Performance evaluation of safety applications over dsrc vehicular ad hoc networks," in *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*. ACM, 2004, pp. 1–9.

[68] Y. J. Li, "An overview of the dsrc/wave technology," in *Quality, Reliability, Security and Robustness in Heterogeneous Networks*. Springer, 2012, pp. 544–558.

[69] D. Jiang and L. Delgrossi, "Ieee 802.11 p: Towards an international standard for wireless access in vehicular environments," in *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*. IEEE, 2008, pp. 2036–2040.

[70] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (aodv) routing," Tech. Rep., 2003.

[71] S. Mohseni, R. Hassan, A. Patel, and R. Razali, "Comparative review study of reactive and proactive routing protocols in manets," in *Digital Ecosystems and Technologies (DEST), 2010 4th IEEE International Conference on*. IEEE, 2010, pp. 304–309.

[72] D. S. Vasiliev, D. S. Meitis, and A. Abilov, "Simulation-based comparison of aodv, olsr and hwmp protocols for flying ad hoc networks," in *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*. Springer, 2014, pp. 245–252.

[73] M. Hyland, B. E. Mullins, R. O. Baldwin, and M. A. Temple, "Simulation-based performance evaluation of mobile ad hoc routing protocols in a swarm of unmanned aerial vehicles," in *Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on*, vol. 2. IEEE, 2007, pp. 249–256.

[74] J. Pojda, A. Wolff, M. Sbeiti, and C. Wietfeld, "Performance analysis of mesh routing protocols for uav swarming applications," in *Wireless Communication Systems (ISWCS), 2011 8th International Symposium on*. IEEE, 2011, pp. 317–321.

[75] R. G. Ogier, F. L. Templin, B. Bellur, and M. G. Lewis, "Topology broadcast based on reverse-path forwarding (tbrpf)," *draft-ietf-manettbrpf-05. txt*, vol. 1, 2002.

[76] S. Skiena, "Dijkstra's algorithm," *Implementing Discrete Mathematics: Combinatorics and Graph Theory with Mathematica, Reading, MA: Addison-Wesley*, pp. 225–227, 1990.

[77] A. Boukerche, B. Turgut, N. Aydin, M. Z. Ahmad, L. Bölöni, and D. Turgut, "Routing protocols in ad hoc networks: A survey," *Computer Networks*, vol. 55, no. 13, pp. 3032–3080, 2011.

[78] D. Johnson, N. Ntlatlapa, and C. Aichele, "Simple pragmatic approach to mesh routing using batman," 2008.

[79] L. Barolli, M. Ikeda, G. De Marco, A. Durresi, and F. Xhafa, "Performance analysis of olsr and batman protocols considering link quality parameter," in *Advanced Information Networking and Applications, 2009. AINA'09. International Conference on*. IEEE, 2009, pp. 307–314.

[80] M. Abolhasan, B. Hagelstein, and J.-P. Wang, "Real-world performance of current proactive multi-hop mesh protocols," in *Communications, 2009. APCC 2009. 15th Asia-Pacific Conference on*. IEEE, 2009, pp. 44–47.

[81] L. Carlos, "open80211s," *HHhttp://www. open80211s. org/index. html*, 2008.

[82] C. E. Perkins and P. Bhagwat, "Dsdv routing over a multihop wireless network of mobile computers," in *Ad hoc networking*. Addison-Wesley Longman Publishing Co., Inc., 2001, pp. 53–74.

[83] K. Xu, X. Hong, M. Gerla, H. Ly, and D. L. Gu, "Landmark routing in large wireless battlefield networks using uavs," in *Military Communications Conference, 2001. MILCOM 2001. Communications for Network-Centric Operations: Creating the Information Force. IEEE*, vol. 1. IEEE, 2001, pp. 230–234.

[84] G. Pei, M. Gerla, and X. Hong, "Lanmar: landmark routing for large scale wireless ad hoc networks with group mobility," in *Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing*. IEEE Press, 2000, pp. 11–18.

[85] G. Pei, M. Gerla, and T.-W. Chen, "Fisheye state routing: A routing scheme for ad hoc wireless networks," in *Communications, 2000. ICC 2000. 2000 IEEE International Conference on*, vol. 1. IEEE, 2000, pp. 70–74.

[86] T.-W. Chen and M. Gerla, "Global state routing: A new routing scheme for ad-hoc wireless networks," in *Communications, 1998. ICC 98. Conference Record. 1998 IEEE International Conference on*, vol. 1. IEEE, 1998, pp. 171–175.

[87] D. Wu, X.-g. ZHAO, and F.-x. ZHU, "Simulation study and realization of uav ad hoc network in reencounter scenario [j]," *Journal of system simulation*, vol. 20, no. 23, pp. 6409–6413, 2011.

[88] A. I. Alshabtat, L. Dong, J. Li, and F. Yang, "Low latency routing algorithm for unmanned aerial vehicles ad-hoc networks," *International Journal of Electrical and Computer Engineering*, vol. 6, no. 1, pp. 48–54, 2010.

[89] U. Paparazzi, "Url http://paparazzi. enac. fr/wiki."

[90] M. E. M. Campista, P. M. Esposito, I. M. Moraes, L. H. M. Costa, O. C. Duarte, D. G. Passos, C. V. N. De Albuquerque, D. C. M. Saade, and

M. G. Rubinstein, "Routing metrics and protocols for wireless mesh networks," *Network, IEEE*, vol. 22, no. 1, pp. 6–12, 2008.

[91] Y. Zheng, Y. Wang, Z. Li, L. Dong, Y. Jiang, and H. Zhang, "A mobility and load aware olsr routing protocol for uav mobile ad-hoc networks," in *Information and Communications Technologies (ICT 2014), 2014 International Conference on*. IET, 2014, pp. 1–7.

[92] M. Mabrouk and C. McInnes, "Solving the potential field local minimum problem using internal agent states," *Robotics and Autonomous Systems*, vol. 56, no. 12, pp. 1050–1060, 2008.

[93] H. Kalosha, A. Nayak, S. Ruhrup, and I. Stojmenovic, "Select-and-protest-based beaconless georouting with guaranteed delivery in wireless sensor networks," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. IEEE, 2008.

[94] R. Jayakumar, K. Thulasiraman, and M. N. Swamy, "o (n 2) algorithms for graph planarization," *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on*, vol. 8, no. 3, pp. 257–267, 1989.

[95] P. Anghel, M. Kaveh *et al.*, "Exact symbol error probability of a cooperative network in a rayleigh-fading environment," *Wireless Communications, IEEE Transactions on*, vol. 3, no. 5, pp. 1416–1421, 2004.

[96] J. Sanchez, R. Marin-Perez, P. M. Ruiz *et al.*, "Boss: Beacon-less on demand strategy for geographic routing inwireless sensor networks," in *Mobile Adhoc and Sensor Systems, 2007. MASS 2007. IEEE International Conference on*. IEEE, 2007, pp. 1–10.

[97] S. Bradner, "temporally-ordered routing algorithm (tora) routing ietf," Internet Draft, draft-ietf-manet-tora-spec-04. txt, RFC 2026, Tech. Rep., 2001.

[98] J. D. Zhai, Zhongqiang and Y. Ren, "The application and improvement of temporally ordered routing algorithm in swarm network with unmanned aerial vehicle nodes," in *ICWMC 2013, The Ninth International Conference on Wireless and Mobile Communications*, 2013.

[99] J. H. Forsmann, R. E. Hiromoto, and J. Svoboda, "A time-slotted on-demand routing protocol for mobile ad hoc unmanned vehicle systems," in *Defense and Security Symposium*. International Society for Optics and Photonics, 2007, pp. 65 611P–65 611P.

[100] F. Baccelli, B. Blaszczyszyn, and P. Mühlethaler, "An aloha protocol for multihop mobile wireless networks," *Information Theory, IEEE Transactions on*, vol. 52, no. 2, pp. 421–436, 2006.

[101] R. Shirani, "Reactive-greedy-reactive in unmanned aeronautical ad-hoc networks: A combinational routing mechanism," Ph.D. dissertation, Carleton University Ottawa, 2011.

[102] R. Shirani, M. St-Hilaire, T. Kunz, Y. Zhou, J. Li, and L. Lamont, "The performance of greedy geographic forwarding in unmanned aeronautical ad-hoc networks," in *Communication Networks and Services Research Conference (CNSR), 2011 Ninth Annual*. IEEE, 2011, pp. 161–166.

[103] Y.-J. Kim, R. Govindan, B. Karp, and S. Shenker, "Geographic routing made practical," in *Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation-Volume 2*. USENIX Association, 2005, pp. 217–230.

[104] I. Stojmenovic, "Position-based routing in ad hoc networks," *Communications Magazine, IEEE*, vol. 40, no. 7, pp. 128–134, 2002.

[105] L. Lin, Q. Sun, J. Li, and F. Yang, "A novel geographic position mobility oriented routing strategy for uavs," *Journal of Computational Information Systems*, vol. 8, no. 2, pp. 709–716, 2012.

[106] L. Lin, Q. Sun, S. Wang, and F. Yang, "A geographic mobility prediction routing protocol for ad hoc uav network," in *Globecom Workshops (GC Wkshps), 2012 IEEE*. IEEE, 2012, pp. 1597–1602.

[107] N. Meghanathan, "Impact of the gauss-markov mobility model on network connectivity, lifetime and hop count of routes for mobile ad hoc networks," *Journal of networks*, vol. 5, no. 5, pp. 509–516, 2010.

[108] D. Medina, F. Hoffmann, F. Rossetto, and C.-H. Rokitansky, "A crosslayer geographic routing algorithm for the airborne internet," in *Communications (ICC), 2010 IEEE International Conference on*. IEEE, 2010, pp. 1–6.

[109] B. Karp and H.-T. Kung, "Gpsr: Greedy perimeter stateless routing for wireless networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking*. ACM, 2000, pp. 243–254.

[110] R. L. Lidowski, B. E. Mullins, and R. O. Baldwin, "A novel communications protocol using geographic routing for swarming uavs performing a search mission," in *Pervasive Computing and Communications, 2009. PerCom 2009. IEEE International Conference on*. IEEE, 2009, pp. 1–7.

[111] E. Kuiper and S. Nadjm-Tehrani, "Geographical routing in intermittently connected ad hoc networks," in *Advanced Information Networking and Applications-Workshops, 2008. AINAW 2008. 22nd International Conference on*. IEEE, 2008, pp. 1690–1695.

[112] L. Kesheng, Z. Jun, and Z. Tao, "The clustering algorithm of uav networking in near-space," in *Antennas, Propagation and EM Theory, 2008. ISAPE 2008. 8th International Symposium on*. IEEE, 2008, pp. 1550–1553.

[113] C. Zang and S. Zang, "Mobility prediction clustering algorithm for uav networking," in *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*. IEEE, 2011, pp. 1158–1161.

[114] C. R. Lin and M. Gerla, "Adaptive clustering for mobile wireless networks," *Selected Areas in Communications, IEEE Journal on*, vol. 15, no. 7, pp. 1265–1275, 1997.

[115] N. Martin, Y. Al-Mousa, and N. Shenoy, "An integrated routing and medium access control framework for surveillance networks of mobile devices," in *Distributed Computing and Networking*. Springer, 2011, pp. 315–327.

[116] M. Chatterjee, S. K. Das, and D. Turgut, "Wca: A weighted clustering algorithm for mobile ad hoc networks," *Cluster Computing*, vol. 5, no. 2, pp. 193–204, 2002.

[117] B. Fu, L. DaSilva *et al.*, "A mesh in the sky: A routing protocol for airborne networks," in *Military Communications Conference, 2007. MILCOM 2007. IEEE*. IEEE, 2007, pp. 1–7.

[118] N. Larrieu, "How can model driven development approaches improve the certification process for uas?" in *Unmanned Aircraft Systems (ICUAS), 2014 International Conference on*. IEEE, 2014, pp. 253–260.

[119] N. Larrieu and A. Varet, "Methodology for rapid prototyping avionic software," *Rapid Prototyping of Software for Avionics Systems*, pp. 23–60.

[120] R. N. Akram, P.-F. Bonnefoi, S. Chaumette, K. Markantonakis, and D. Sauveron, "Improving security of autonomous uavs fleets by using new specific embedded secure elements a position paper."

[121] P. Luong, "Securing embedded systems for autonomous aerial vehicles," Ph.D. dissertation, WORCESTER POLYTECHNIC INSTITUTE, 2013.

[122] A. N. Phillips, "A secure group communication architecture for a swarm of autonomous unmanned aerial vehicles," DTIC Document, Tech. Rep., 2008.

[123] R. S. Yokoyama, B. Y. L. Kimura, and E. dos Santos Moreira, "An architecture for secure positioning in a uav swarm using rssi-based distance estimation," *ACM SIGAPP Applied Computing Review*, vol. 14, no. 2, pp. 36–44, 2014.

[124] A. Y. Javaid, W. Sun, V. K. Devabhaktuni, and M. Alam, "Cyber security threat analysis and modeling of an unmanned aerial vehicle system," in *Homeland Security (HST), 2012 IEEE Conference on Technologies for*. IEEE, 2012, pp. 585–590.

[125] P. Yi, Z. Dai, S. Zhang, and Y. Zhong, "A new routing attack in mobile ad hoc networks," *International Journal of Information Technology*, vol. 11, no. 2, pp. 83–94, 2005.

[126] M. Pirretti, S. Zhu, N. Vijaykrishnan, P. McDaniel, M. Kandemir, and R. Brooks, "The sleep deprivation attack in sensor networks: Analysis and methods of defense," *International Journal of Distributed Sensor Networks*, vol. 2, no. 3, pp. 267–287, 2006.

[127] D. Westhoff, B. Lamparter, C. Paar, and A. Weimerskirch, "On digital signatures in ad hoc networks," *European transactions on telecommunications*, vol. 16, no. 5, pp. 411–425, 2005.

[128] I. Cervesato, "The dolev-yao intruder is the most powerful attacker," in *16th Annual Symposium on Logic in Computer Science—LICS*, vol. 1. Citeseer, 2001.

[129] J. Cordasco and S. Wetzel, "An attacker model for manet routing security," in *Proceedings of the second ACM conference on Wireless network security*. ACM, 2009, pp. 87–94.

[130] W. M. Eddy, "Syn flood attack," in *Encyclopedia of Cryptography and Security*. Springer, 2011, pp. 1273–1274.

[131] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole attacks in wireless networks," *Selected Areas in Communications, IEEE Journal on*, vol. 24, no. 2, pp. 370–380, 2006.

[132] H. Aldabbas, T. Alwada'n, H. Janicke, and A. Al-Bayatti, "Data confidentiality in mobile ad hoc networks," *arXiv preprint arXiv:1203.1749*, 2012.

[133] K. S. Win, "Analysis of detecting wormhole attack in wireless networks," in *World Academy of Science, Engineering and Technology*. Citeseer, 2008.

[134] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," *Wireless communications, IEEE*, vol. 14, no. 5, pp. 85–91, 2007.

[135] B. Wu, J. Chen, J. Wu, and M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc networks," in *Wireless Network Security*. Springer, 2007, pp. 103–135.

[136] J. R. Douceur, "The sybil attack," in *Peer-to-peer Systems*. Springer, 2002, pp. 251–260.

[137] G. Peng and Z. Chuanyun, "Routing attacks and solutions in mobile ad hoc networks," in *Communication Technology, 2006. ICCT'06. International Conference on*. IEEE, 2006, pp. 1–4.

[138] N. Kang, E. M. Shakshuki, and T. R. Sheltami, "Detecting forged acknowledgements in manets," in *Advanced Information Networking and Applications (AINA), 2011 IEEE International Conference on*. IEEE, 2011, pp. 488–494.

[139] F. Kandah, Y. Singh, and C. Wang, "Colluding injected attack in mobile ad-hoc networks," in *Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on*. IEEE, 2011, pp. 235–240.

[140] A. K. Abdelaziz, M. Nafaa, and G. Salim, "Survey of routing attacks and countermeasures in mobile ad hoc networks," in *Computer Modelling and Simulation (UKSim), 2013 UKSim 15th International Conference on*. IEEE, 2013, pp. 693–698.

[141] A. K. Rai, R. R. Tewari, and S. K. Upadhyay, "Different types of attacks on integrated manet-internet communication," *International Journal of Computer Science and Security*, vol. 4, no. 3, pp. 265–274, 2010.

[142] Z. M. Fadlullah, T. Taleb, and M. Schöller, "Combating against security attacks against mobile ad hoc networks (manets)," *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*, vol. 173, 2010.

[143] F.-H. Tseng, L.-D. Chou, and H.-C. Chao, "A survey of black hole attacks in wireless mobile ad hoc networks," *Human-centric Computing and Information Sciences*, vol. 1, no. 1, pp. 1–16, 2011.

[144] A. Ivanov, "Side-channel attacks," 2005.

[145] M. G. Zapata, "Secure ad hoc on-demand distance vector routing," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 6, no. 3, pp. 106–107, 2002.

[146] G. Montenegro and C. Castelluccia, "Statistically unique and cryptographically verifiable (sucv) identifiers and addresses," in *In Proceedings of the 9th Annual Network and Distributed System Security Symposium (NDSS*. Citeseer, 2002.

[147] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, "Mitigating byzantine attacks in ad hoc wireless networks," *Department of Computer Science, Johns Hopkins University, Tech. Rep. Version*, vol. 1, 2004.

[148] P. Syverson, "A taxonomy of replay attacks [cryptographic protocols]," in *Computer Security Foundations Workshop VII, 1994. CSFW 7. Proceedings*. IEEE, 1994, pp. 187–191.

[149] R. V. Boppana and S. Desilva, "Evaluation of a stastical technique to mitigate malicious control packets in ad hoc networks," in *Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks*. IEEE Computer Society, 2006, pp. 559–563.

[150] S. Yi, P. Naldurg, and R. Kravets, "Security-aware ad hoc routing for wireless networks," in *Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing*. ACM, 2001, pp. 299–302.

[151] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol. 3. IEEE, 2003, pp. 1976–1986.

[152] C. Adjih, D. Raffo, and P. Mühlethaler, "Attacks against olsr: Distributed key management for security," in *2nd OLSR Interop/Workshop, Palaiseau, France*, 2005.

[153] C. Crepeau, C. R. Davis, and M. Maheswaran, "A secure manet routing protocol with resilience against byzantine behaviours of malicious or selfish nodes," in *Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on*, vol. 2. IEEE, 2007, pp. 19–26.

[154] B. N. Levine, C. Shields, and N. B. Margolin, "A survey of solutions to the sybil attack," *University of Massachusetts Amherst, Amherst, MA*, 2006.

[155] B. Xiao, B. Yu, and C. Gao, "Detection and localization of sybil nodes in vanets," in *Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks*. ACM, 2006, pp. 1–8.

[156] C. Harsch, A. Festag, and P. Papadimitratos, "Secure position-based routing for vanets," in *Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th*. IEEE, 2007, pp. 26–30.

[157] S. Desilva and R. V. Boppana, "Mitigating malicious control packet floods in ad hoc networks," in *Wireless Communications and Networking Conference, 2005 IEEE*, vol. 4. IEEE, 2005, pp. 2112–2117.

[158] D. Raffo, C. Adjih, T. Clausen, and P. Mühlethaler, "Securing olsr using node locations," in *Wireless Conference 2005-Next Generation Wireless and Mobile Communications and Services (European Wireless), 11th European*. VDE, 2005, pp. 1–7.

[159] N. Asokan and P. Ginzboorg, "Key agreement in ad hoc networks," *Computer Communications*, vol. 23, no. 17, pp. 1627–1637, 2000.

[160] W. Diffie and M. E. Hellman, "New directions in cryptography," *Information Theory, IEEE Transactions on*, vol. 22, no. 6, pp. 644–654, 1976.

[161] M. Steiner, G. Tsudik, and M. Waidner, "Diffie-hellman key distribution extended to group communication," in *Proceedings of the 3rd ACM conference on Computer and communications security*. ACM, 1996, pp. 31–37.

[162] S. M. Bellovin and M. Merritt, "Encrypted key exchange: Password-based protocols secure against dictionary attacks," in *Research in Security and Privacy, 1992. Proceedings., 1992 IEEE Computer Society Symposium on*. IEEE, 1992, pp. 72–84.

[163] F. Stajano and R. Anderson, "The resurrecting duckling: Security issues in ad-hoc wireless networks. 1999," in *Security Protocols, 7th International Workshop Proceedings, Lecture Notes in Computer Science, Springer-Verlag. http://www. cl. cam. ac. uk/fms27/duckling*.

[164] Y. G. Desmedt, "Threshold cryptography," *European Transactions on Telecommunications*, vol. 5, no. 4, pp. 449–458, 1994.

[165] M. May, "Specification-based intrusion detection," 2004.

[166] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *computers & security*, vol. 28, no. 1, pp. 18–28, 2009.

[167] T. Bass, "Intrusion detection systems and multisensor data fusion," *Communications of the ACM*, vol. 43, no. 4, pp. 99–105, 2000.

[168] R. V. Boppana and X. Su, "An analysis of monitoring based intrusion detection for ad hoc networks," in *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*. IEEE, 2008, pp. 1–5.

[169] C. H. Tseng, S.-H. Wang, C. Ko, and K. Levitt, "Demem: distributed evidence-driven message exchange intrusion detection model for manet," in *Recent Advances in Intrusion Detection*. Springer, 2006, pp. 249–271.

[170] Y.-a. Huang and W. Lee, "A cooperative intrusion detection system for ad hoc networks," in *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*. ACM, 2003, pp. 135–147.

[171] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on vanet security challenges and possible cryptographic solutions," *Vehicular Communications*, vol. 1, no. 2, pp. 53–66, 2014.

[172] M. G. Zapata and N. Asokan, "Securing ad hoc routing protocols," in *Proceedings of the 1st ACM workshop on Wireless security*. ACM, 2002, pp. 1–10.

[173] S. Eichler and C. Roman, "Challenges of secure routing in manets: A simulative approach using aodv-sec," in *Mobile Adhoc and Sensor Systems (MASS), 2006 IEEE International Conference on*. IEEE, 2006, pp. 481–484.

[174] A. A. Hanafy, S. H. Noureldin, and M. A. Azer, "Immunizing the saodv protocol against routing information disclosure," in *Internet Technology and Secured Transactions (ICITST), 2011 International Conference for*. IEEE, 2011, pp. 330–334.

[175] S. Khurana, N. Gupta, and N. Aneja, "Reliable ad-hoc on-demand distance vector routing protocol," in *Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, 2006. ICN/ICONS/MCL 2006. International Conference on*. IEEE, 2006, pp. 98–98.

[176] L. Bononi and C. Tacconi, "Intrusion detection for secure clustering and routing in mobile multi-hop wireless networks," *International journal of information security*, vol. 6, no. 6, pp. 379–392, 2007.

[177] D. Cerri and A. Ghioni, "Securing aodv: the a-saodv secure routing prototype," *Communications Magazine, IEEE*, vol. 46, no. 2, pp. 120–125, 2008.
[178] I. Stamouli, P. G. Argyroudis, and H. Tewari, "Real-time intrusion detection for ad hoc networks," in *World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium on a*. IEEE, 2005, pp. 374–380.
[179] A. Aggarwal, S. Gandhi, N. Chaubey, N. Tada, and S. Trivedi, "Ndtaodv: Neighbor defense technique for ad hoc on-demand distance vector (aodv) to mitigate flood attack in manets," *arXiv preprint arXiv:1405.6216*, 2014.
[180] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "Authenticated routing for ad hoc networks," *Selected Areas in Communications, IEEE Journal on*, vol. 23, no. 3, pp. 598–610, 2005.
[181] J. Li, M. Lyu, and J. Liu, "Taodv: A trusted aodv routing protocol for mobile ad hoc networks," in *Proceedings of Aerospace Conference*, 2004.
[182] B. Mancini, "The great reconnaissance: A uav project in niger," *GeoInformatics*, vol. 17, no. 6, p. 6, 2014.
[183] L. Lazos, R. Poovendran, C. Meadows, P. Syverson, and L. Chang, "Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach," in *Wireless Communications and Networking Conference, 2005 IEEE*, vol. 2. IEEE, 2005, pp. 1193–1199.
[184] R. Akbani, T. Korkmaz, and G. Raju, "Heap: A packet authentication scheme for mobile ad hoc networks," *Ad Hoc Networks*, vol. 6, no. 7, pp. 1134–1150, 2008.
[185] C. Li, Z. Wang, and C. Yang, "Seaodv: A security enhanced aodv routing protocol for wireless mesh networks," in *Transactions on computational science XI*. Springer, 2010, pp. 1–16.
[186] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The tesla broadcast authentication protocol," *RSA CryptoBytes*, vol. 5, 2005.
[187] Q. Li, Y.-C. Hu, M. Zhao, A. Perrig, J. Walker, and W. Trappe, "Sear: a secure efficient ad hoc on demand routing protocol for wireless networks," in *Proceedings of the 2008 ACM symposium on Information, computer and communications security*. ACM, 2008, pp. 201–204.
[188] A. Perrig and D. B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless ad hoc networks," in *IEEE INFOCOM*, 2003, pp. 1976–1986.
[189] H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen, "An efficient merkle-tree-based authentication scheme for smart grid," *Systems Journal, IEEE*, vol. 8, no. 2, pp. 655–663, 2014.
[190] A. Hanafy, M. A. Azer, S. H. Noureldin *et al.*, "Saodv and modified saodv performance comparison," in *Computer Engineering & Systems (ICCES), 2013 8th International Conference on*. IEEE, 2013, pp. 95–98.
[191] T. Wu, Y. Xue, and Y. Cui, "Preserving traffic privacy in wireless mesh networks," in *Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks*. IEEE Computer Society, 2006, pp. 459–461.
[192] S. Bouam and J. Ben-Othman, "Data security in ad hoc networks using multipath routing," in *Personal, Indoor and Mobile Radio Communications, 2003. PIMRC 2003. 14th IEEE Proceedings on*, vol. 2. IEEE, 2003, pp. 1331–1335.
[193] A. Patel, N. Patel, and R. Patel, "Defending against wormhole attack in manet," in *Communication Systems and Network Technologies (CSNT), 2015 Fifth International Conference on*. IEEE, 2015, pp. 674–678.
[194] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks." in *NDSS*, 2004.