Secure Routing Protocol Design for UAV Ad Hoc Networks

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

Secure Routing Protocol Design for UAV Ad Hoc Networks

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 (UAANET) are a new form of ad hoc networks in which nodes are Unmanned Aerial Vehicles (UAVs) and Ground Control Station (GCS). Although this field generated a certain interest in the scientific community, it has only received a modest contribution . Compared to Mobile Ad hoc NETworks (MANET), this new network paradigm has some unique features and brings specific challenges such as node mobility degree, network connectivity patterns, delay-sensitive applications and network security. Indeed, some UAV communication architectures have been proposed, but none of them has been designed with security in mind. This lack of scientific investigation can make the certification of UAANETs difficult to obtain. In this paper, we present our vision of such a challenge and the research that we are conducting to reach this objective. The aim is to propose an original secure routing protocol for UAVs using a MDD (Model Driven Development) approach which will ease the certification of final UAV products. The first preliminary results concerning our secure-routing protocol design will be presented. This paper describes our ongoing research which will provide secure communications for UAV ad hoc networks at the end of the SUANET (Secure Uav Ad-hoc NETwork) project.**

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

I. Introduction

An Unmanned Aerial Vehicle (UAV) is a pilotless aerial vehicle which can be controlled either autonomously by on-board computers or remotely controlled by a pilot. When several UAVs are communicating with each other via wireless links, they dynamically form a temporary multi-hop radio network called UAV Ad hoc Network (UAANET).

In UAANETs, the relatively low number of UAVs, their high mobility and frequently changing topology challenge network connectivity and differentiate them from usual Mobile Ad hoc NETworks (MANETs). These characteristics induce difficult challenges for building a reliable and secure communication architecture solution. It is worthwile to underline that some communication architectures [1] have been proposed by the UAVs research community for UAANET, but none of these has been designed to provide defense against malicious attackers. Moreover, due to some specific features (described in detail in Section II) which differentiate UAANETs from other MANETs, implementing a secure communication architecture has become a daunting task. An example of such a challenge is the resource constraints (e.g, very low communication throughput) and limited physical security[1] offered by the current UAANET communication infrastructure. Also, safety in UAANET is of major importance because UAVs can be used as a weapon[2][3]. Consequently, human lives can be at stake in case of security failures. It is therefore crucial to ensure that the control traffic cannot be either modified or deleted by an unauthorized entity during the mission. It must be securely exchanged and on time because a noticeable delay in the traffic exchanged may cause considerable damage such as collision of UAVs.

This is the challenge that we intend to solve within our research collaboration with the DELAIR-TECH company [4]. The objective is to propose a new secure communication architecture for UAVs taking into account the unique specifications of UAANETs (described in section II-A). This new architecture depends mostly on the definition of a secure routing protocol which provides authentication, confidentiality and integrity services. This network protocol must also induce as little signaling overhead as possible in order to preserve network resources for effective data exchanged between UAVs.

Furthermore, it is important to underline that UAANETs will have to be certified in the near future to fully enable its commercial applications. The procedure involved in obtaining such certification is long and complex, as it includes different parts of the UAS (Unmanned Aerial System). Indeed the validation and verification range from the electronic part (autopilot hardware, GCS hardware, etc.) to the embedded software (autopilot software, operating system, communication system, etc.). The certification authorities require that every UAANET component must be reliable, safe and conforms exactly to the technical specifications. In our work, we considered such complexity by using a qualified tool for the communication software design. As a result, in order to be compliant with the French Civil Aviation Administration (DGAC[2]) for the certification requirements, we use a Model Driven Development (MDD) approach (this design approach will be detailed in Section III).

[1]UAVs used in UAANETs are deployed in untrustworthy environments in which external attacks can occur due to the absence of fixed infrastructure

[2]DGAC: Direction Générale de l Aviation Civile which is equivalent to FAA (Federal Aviation Administration) but at a French scale.

The paper is organized as follows. In Section II, we describe UAANETs specifications and their security requirements. In Section III, we describe our research collaboration with DELAIR-TECH company, then we provide an analysis of a potential security architecture in Section IV. The first preliminary results related to our new secure routing protocol for UAANET will be described in Section IV. Finally, in Section V, we provide our conclusions and an overview of our future research perspectives.

II. UAANET COMMUNICATION ARCHITECTURE AND SECURITY PRINCIPLES

A. UAANET Specifications

Similar to MANETs, the architecture of UAANETs is an infrastructure-less network which uses several nodes to forward data packets. It shares some common features with standard mobile ad hoc networks such as self-organized connection pattern, self-managed information distribution and communication between nodes without a centralized authority. However, UAANETs have also specific features that can be listed as [1]:

- **Network connectivity**: depending on the mobility degree, the connectivity between two UAVs could be lost while they are transmitting critical information (e.g. control/command traffic). In addition, UAV platform failures can also affect the network topology. Indeed, when a UAV fails, the different links with that UAV also fail, and it results in a topology maintenance. Furthermore, link quality inconsistency may also affect UAANET topology. Because of the UAV movements and variations of distance, link quality fluctuates and may cause loss of connectivity and performance degeneration.
- **Number of nodes:** Compared to some MANETs (for instance VANET - Vehicular Ad hoc NETwork), the node density in UAANETs is relatively low because the high speed of a UAV help to quickly cover a restricted area. Consequently, a large number of UAVs is not required. Commonly, UAANET missions deploy an average of 3 to 4 UAVs [5] [6] [7].
- **Sufficient energy and storage**: depending on their sizes, UAVs are usually assumed to have more energy and computing power than nodes in MANETs. For instance, in wireless sensor networks, nodes are subject to power and storage limitations, which restrict the network lifetime. This issue is frequently not considered as a dominant factor in UAANETs because the UAV itself is a source of electricity for the autopilot and payload infrastructure. As such, the energy used to fly the UAV is supposed to be much greater than the energy used to perfom networking.
- **Mobility**: mobility model plays an important role in designing network protocols in UAANETs. The UAV mobility is specifically 3D based and quite different from other vehicles. Random Way Point (RWP) model is one of the most common ones used to simulate node movements in MANETs [8]. It assumes that the path is chosen randomly. However, as stated in [9], such pattern is not suitable for UAVs as they will navigate with a predefined direction based upon the mission. Therefore, the mobility model should be rebuilt from scratch. Accordingly, an innovative approach has been proposed in [10] where authors provided a mobility pattern for UAVs based on real traces.
- **Propagation model**: in VANETs and MANETs, the propagation model is not free of obstacles [11] as nodes are moving close to the ground. In contrast, a Line of Sight (LOS) usually exists in UAANET environments. However, as stated in [1], the propagation model depends on several factors such as the variation in communication distance, the ground reflection effects and weather conditions.
- **Strict delay constraints**: generally, UAANETs are used for real-time application exchanges, such as, aerial photography and video capture in case of remote monitoring and environmental measurements. In addition, the control/command traffic has also to arrive on time and be computed by the UAV in order to avoid loss of control.

B. Security for UAANET

UAANET security is necessary to verify that nodes are trustworthy before exchanging data packets. It is also needed to ensure that no malicious entity can disturb the transmission of data messages during UAANET mission. Moreover, as stated previously, UAANETs security is of special concern because its failure may compromise human lives. Indeed, in today's world, ensuring safety of civilians is of major importance. Since a UAV can be used as a weapon [3], an appropriate security solution is mandatory and can be a key factor for certification. Consequently, before deploying UAANET, we have to make sure that the control traffic as well as heartbeat messages (GPS information, UAV onboard state, battery level, UAV identification, etc ...) cannot be either modified or deleted by an attacker. Along with payload traffic, this information must be exchanged securely and at the right time to prevent unexpected behavior of the swarm.

However, the deployment of an exhaustive security system for UAANET is not an easy task as there are several challenges and security breaches to overcome. Indeed, in addition to classical network security issues, the specific features of UAANETs mentioned above raise additional challenges from a security point of view. For instance, due to UAANET intermittent connectivity and UAV movements, it is difficult to perform a reliable formation flight[3] for small UAVs. Also, deploying a Public Key Infrastructure (PKI) to handle cryptographic keys is an obstacle to overcome. Indeed, the high mobility of UAV nodes and the low air-ground network resources require us to develop a specific PKI solution for UAANETs.

Moreover, several security solutions for MANETs have been proposed but most of them cannot be used directly

[3]An efficient formation flight of UAV swarms is necessary to increase mission coverage and optimize mission duration.

for the UAANET paradigm, given its specific features stated previously (see section II-A for details). Consequently, security should be taken into account at an early stage of the UAV network design. So far, communication architectures have been proposed for UAVs [12]. They mostly focus on performance enhancements rather than security. As a result, UAANETs are vulnerable to many attacks [13]. These attacks could occur on any layer of the protocol stack. For instance jamming at the physical layer [14], traffic analysis at the data link layer [15], flooding at the network layer [16], UDP[4] flood attack at the transport layer [17] and data corruption at the application layer [18]. This section focuses solely on attacks targeting the communication system (i.e, the network layer) since it is part of our research project specifications (the SUANET project collaboration will be described in more detail in the next section).

1) Routing attacks on UAANETs: The purpose of attacks targeting the network layer consist 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 [19], Rushing attacks [20], Colluding attacks [21] and Sybil attacks [22]. Denial of Service (DoS) attacks and Eavesdropping attacks are also possible on MANETs. A detailed overview of the existing attacks on MANETs is given in [18]. Since a UAANET is a subcategory of MANET, these attacks could well be applied in UAANETs.

In order to block these attacks, the UAANET secure routing protocol has to be able to identify trustworthy nodes and find a reliable route from the sender to the destination node. An extended description of the wormhole attack is described in figure 1 to illustrate the needs of the security mechanisms in UAANETs. We have decided to highlight this attack since it is especially sophisticated and makes vulnerable different types of existing routing protocol in MANET[23]. The wormhole attack involves two attackers who perform a colluding attack. One attacker record packets at a particular location and replay them at another attacker by using a high-speed private network. As a result, a UAV could unconsciously decide to forward traffic through the corrupt route to seek better performance. Consequently, all traffic sent from the GCS to the UAV4 which are supposed to go through UAV1 and UAV2 will end up captured by the two attackers. Note that once this collaborative attack successfully performed, it gives the attacker nodes a possibility for future attacks (for instance route disruptions or traffic unauthorized access, etc.). Obviously, to avoid such attack within UAANETs, the different UAVs needs to deploy an efficient authentication security mechanism that provides a strong authentication between each other. This ensures that only authenticated UAVs are able to participate on routing information. Thus, the attackers (attacker nodes 1 and 2) cannot prove their identity and will not be able to communicate with the different UAVs.

[4]User Datagram Protocol

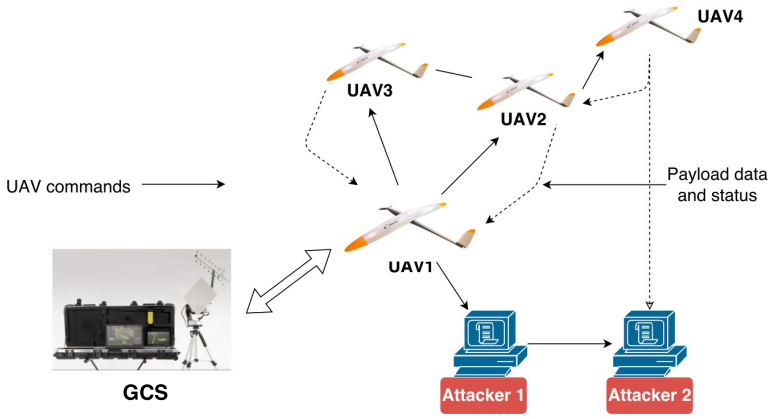

Figure 1. The Wormhole attack process

Moreover, different classifications can be defined to understand UAANET attacks. For instance, active attack versus passive attack or internal versus external attacks can be used to categorize them. In the following, we will instead classify them based on the basic routing functionalities to illustrate the attack targeting the different exchanged traffic between UAVs: route discovery attacks (category I) and data forwarding attacks (category II). Attacks within these categories are shown in figure 2. The first category (left of figure 2) refers to the attacks which could harm the traffic control, while the second category (right of Figure 2) is relevant to the payload traffic (image and (real time) video traffic for instance).

We consider that a corrupted configuration packet could have a significant impact on the entire UAS because it directly corrupts the route finding process. Therefore, the first category is considered to be more critical. Likewise, the second category of attacks has an impact essentially on network performances. These potential attacks happen only after the route finding process, which can therefore be detected by a security mechanism. For instance, with a hash chain mechanism [24] which allows each node to verify the integrity of a message hop count, a node is able to detect a forged message and recognize if the message has been originated or forwarded from an untrusted node.

For illustrative purposes, we highlight in figure 3 one of our research project application scenario involving three UAVs (DT1, DT2 and DT3). We consider that DT3 is dedicated to capture video from a coverage area and send it back to the GCS. As for DT1 and DT2, they are used as a relay node and forward traffics between the GCS and DT3. This use case requires that the GCS continuously sends control traffic to all UAVs. In this specific case, if any attacker between DT1 and DT3 manages to capture and modify the control packet, it will lead to a misconfiguration of DT3 and thus, will induce a failure of the mission. One way to achieve such attack is to corrupt the route discovery algorithm. Consequently, the security of the route finding process is a primary prerequisite for secure communication within UAANETs. Therefore, we

need to the prioritize route discovery attacks among the several existing attacks to ensure data transmissions by an efficient and secure routing mechanism.

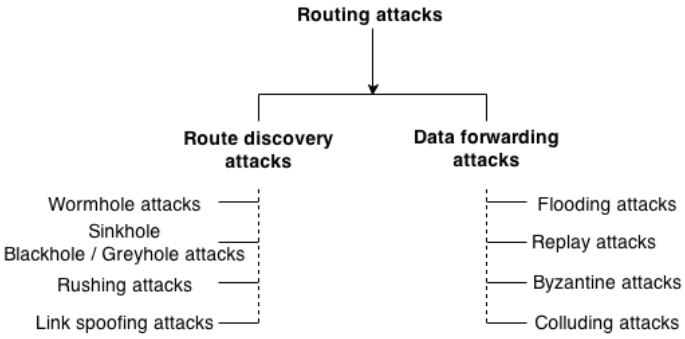

Figure 2. Attacks category during routing process

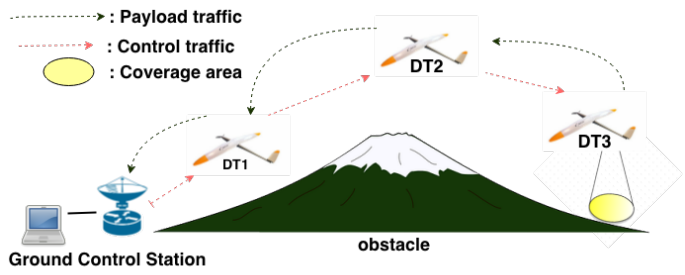

Figure 3. A use case for UAANETs

2) Security requirements in UAANETs: Security goals of UAANETs are not different from other ad hoc networks. The aim is always to ensure the five security services: authentication, integrity, confidentiality, availability and non-repudiation.

Without authentication, an attacker could masquerade a UAV, thus being able to have unauthorized access to the resources and secret information, and may overtake the control of the network.

Likewise, without integrity, an adversary could manipulate critical data by insertion, deletion or modification.

Confidentiality ensures that information content is never revealed to entities that are not authorized to receive it.

The non-repudiation service refers to a property that entities in the network cannot deny sending or receiving a message. Availability guarantees that all of the services provided by the system are always available.

3) Secure routing protocols for UAANETs: Many of the attacks described above can be avoided by considering the security requirements of UAANETs in the routing protocol. The aim is not only to guarantee that all UAVs wishing to participate in the routing process are correctly authenticated but also to prevent unauthorized nodes from taking part in the routing operations. It is important to note that no secure routing protocol has been developed currently for UAV communications. For this reason, one of our research objectives is to propose a new secure routing protocol for UAANETs. Furthermore, several secure routing protocols have been created for MANET. They are either trust based or cryptographic based. An extensive survey can be found in [25]. Since we envisioned to deploy homogeneous UAVs from a same manufacturer, a trust metric implementation does not bring any significant advantages in our study. Thus, we only address our solution through cryptography techniques. Nevertheless, it must be made clear that, the implementation of cryptography algorithms necessitates a key management for issuing, exchanging and revoking keys [26]. Keys are the basic credentials of symmetric and asymmetric cryptography functions. However, similarly to MANETs, key management in UAANETs is more difficult to provide than in traditional networks. This is because of several factors related to UAANET features such as the propagation conditions, lack of a certification authority (CA), and resource constraints such as power, memory, and bandwidth availability.

4) Secure data communication: This is a primary function needed by the entities in the network. This strategy concerns essentially the design of a security mechanism on a different layer from the network layer. Thus, it can be applied, for instance, to the application layer or the link layer. The main objective is to ensure that each UAV is able to securely exchange data messages. It should also be interoperable with the under performing routing protocol and add additional security block if the routes is still not free of adversaries.

III. SUANET: Secure UAV Ad Hoc Network

A. Research Collaboration Context

Our work is part of a scientific collaboration between the French company **Delair-Tech** and **ENAC** (the French Civil Aviation University), funded by the French scientific foundation ANRT[5]. This collaboration started in December 2013, and is planned to last for 36 months. The aim is to define and implement a secure architecture for UAANETs. Figure 4 summarizes the different research objectives we wish to achieve. The first objective is to define a key management mechanism to enable deployment of multiple keys which will be used to implement authentication, confidentiality and integrity services.

We focused solely on these three security attributes as they are sufficient to ensure the security of the communication between UAVs.

The second objective is to design a new 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 routing algorithm will rely on the key distribution protocol defined in the first step. Note that the solution has to induce the minimum signaling overhead in order to preserve network resources for effective data exchange between UAVs.

[5]ANRT: Association Nationale de la Recherche et de la Technologie

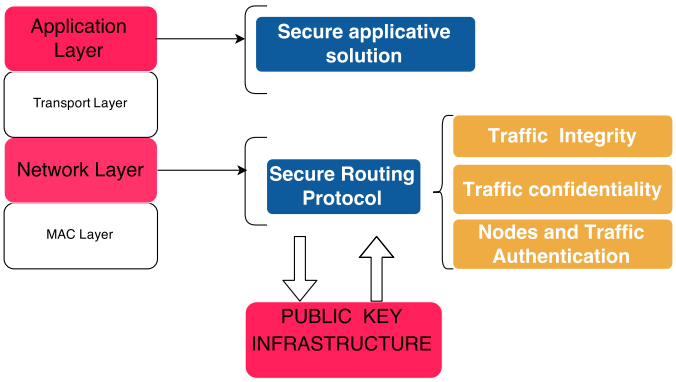

Figure 4. SUANET research objectives

Lastly, the third contribution will be the design of an additional mechanism to secure data communications between a pair of entities. This security extension would probably need to be added onto a layer other than the network layer (the application layer for instance).

These different security solutions assume that a Public Key Infrastructure (PKI) is available in the network. Air-ground PKI is a dedicated research field and we will not describe it in this paper. In this paper, we assume that a dedicated PKI is deployed in the network and reachable by each UAV.

Note that different UAV applications are already implemented within the Delair Tech company, such as video surveillance, aerial photography, precision farming and environmental measurements. In our current research, we focus on using UAANETs in order to improve video monitoring of geographical areas where natural disasters can occur (see the SUANET use case described in Figure 3).

Furthermore, it is important to underline that the specificity of the UAV hardware has to be taken into account when designing the solution. Our secure routing protocol design depends on specific characteristics (e.g. CPU capacity, energy consumptions) of the system. Table I describes the main technical characteristics of DT-18[6] UAVs, provided by the DELAIR TECH company for the development of the communication architecture.

Finally, this paper will focus on the secure routing protocol design but the reader needs to consider this work as a piece of something bigger: the final goal of the SUANET research work is to propose to the UAS community a secure communication architecture for UAVs.

B. An application scenario: real-time video surveillance in disaster areas

The considered application scenario is an emergency situation where the UAANET is used to cover a geographical area using remote monitoring. As shown in Figure 3, the scenario involves 3 UAVs (DT1, DT2 and DT3) communicating with each other. In the beginning, the three UAVs are moving in accordance with their flight plans while being connected to the ground control station (GCS). We then assume that based on the mission plan update, the node DT3 has to move into another location to cover a specific geographic zone. Its communications are then impossible with the GCS due to the loss of coverage (inducing a disconnection). Additionally, we assume that an obstacle prevents a direct connectivity between DT3 and the GCS. In this case, DT1 and DT2 act as relays to ensure communications towards the GCS. The monitoring data are therefore exchanged between DT3 and the GCS through DT1 and DT2.

Table I
DRONE DT-18 CHARACTERISTICS

Characteristic	Value
Model	DT-18
Cruising speed	50 km/h
Range	100 km
Autonomy	2 hours
Wingspan	1.80 m
Length	1.20 m
Data-link range	15 km
Unloaded weight	1.7 kg
Load capacity	0.3 kg
Propulsion	1 electric engine
Wind resistance	45 km/h
Autopilot	Delair-Tech technology

C. Secure routing UAANET protocol: a Model Driven Development approach

To act as autonomous systems (without a dedicated safety pilot) or to be simply authorized to fly in general air space, UAANET needs to be certified before deployment[7]. This certification process is a very long procedure and involves different parts of the UAS such as the autopilot, the operating system and the communication system. In this context, we focus on the certification for the final software of our communication system and use a Model-Driven Development (MDD) approach in our design process. The main advantage of MDD approaches is to bring less error-prone properties and to lead to a higher quality and meaningful validation [27] of the final embedded software.

MDD is a paradigm in software development which claims the use of models as primary artifacts in the development process. The main idea is to focus on creating models rather than software codes and algorithms [28]. Indeed, a system model is the focus of the development process, from requirements specification, development through model design, simulation testing and integration. Additionally, MDD allows us to generate high level code in order to verify and to test

[6]DT-18 website: http://www.delair-tech.com/packages/observer/

[7]The website http://www.developpement-durable.gouv.fr/Demarches-pour-effectuer-des.html gives extra information for flying a UAV inside the French airspace.

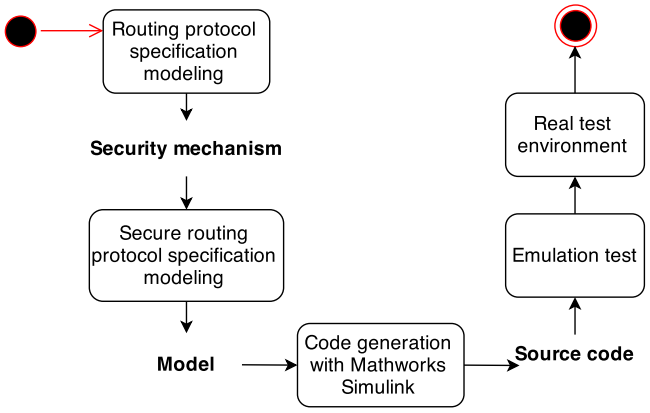

Figure 5. Using an MDD approach to design this secure routing protocol for UAANETs

the coverage of the model and therefore the conformance in line with the project requirements. It also allows us to create unitary tests and execute model-and-code consistency checking for system verification purposes. Note that it takes time and effort to develop models. However, reusing them by generating code for implementation and integration is another advantage of using MDD.

It is important to emphasize that the autopilot for flight missions beyond the line of sight of the GCS haq already been certified by the DGAC for DT-18 UAVs. However, since the new secure communication architecture that we are designing implies a modification of the communication system, a new certification is therefore needed to cover the new functionalities.

In order to do so, we use the Matlab Simulink framework which is a modern tool for domain expert's development of the system model. This software system will be integrated directly into the ARM board of the UAV in order to automatically generate a C/C++ code.

Figure 5 shows how we used the MDD approach to design a secure routing protocol for UAANETs. Figure 6 gives detailed information about the different Matlab Simulink and ad hoc tools used to produce the final binary. The modeling process begins with the design of the routing protocol with Matlab Simulink. The next step is to add a set of security mechanisms in order to obtain a secure protocol. Based on the modeling results, the automatic generation feature provided by Simulink is used to get the source code. Moreover, Matlab Simulink provides full automatic test procedures that improve the design of our secure routing protocol model. For instance, they provide automatic logical coverage verification procedures which increase the robustness of the final software. The validation procedures are then eased and final binary tests will be less numerous (this is investigated further in Section IV-D2).

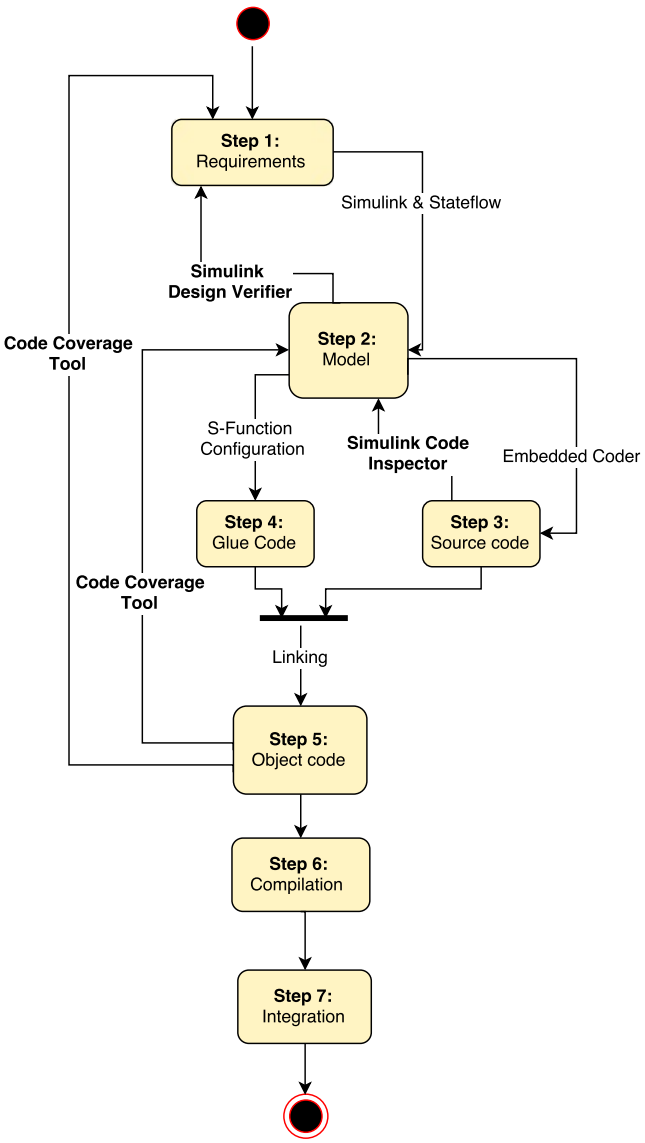

Figure 6. Set of MDD tools used to design this secure routing protocol for UAANETs

IV. SUANET SECURE ROUTING PROTOCOL SELECTION PROCESS

In this section, we focus on the design of the new secure routing protocol for UAANETs. The first part of this design was dedicated to a selection process which has been divided into three complementary studies:

1) Survey of existing UAANET routing protocols and selection of the best performing ones;
2) Emulation testbed results of the different routing protocol candidates selected in study 1;
3) Literature based security robustness selection.

The main objective of this selection process has been to consider the most performing routing protocol which exists in the MANET field. This protocol will be the starting point of the new secure routing protocol that we plan to propose. These three steps of the selection process are described below.

A. Survey of existing UAANET routing protocols

This survey has been conducted to identify the starting point of our protocol design. Most of the current UAANET routing protocols are extensions of well-known MANET routing protocols such as Ad hoc On demand Distance Vector (AODV) [29], Optimized Link State Routing protocols (OLSR) [30] and the Greedy Perimeter Stateless Routing (GPSR) [31]. We conducted an in-depth study of each UAANET routing protocol and we compared them based on their concordance with the SUANET requirements and performances in terms of end-to-end delay, overhead and packet delivery ratio.

Based on our survey (Figure IV-A summarizes the state of the art of routing protocols for UAANET), it seems that the Reactive-Greedy-Reactive (RGR) protocol [32] would provide better performances than existing protocols for UAANET. RGR combines both reactive routing AODV and Greedy Geographic Forwarding (GGF) [33] mechanisms. It uses location information as well as reactive end-to-end paths in the route selection process. The geographic part of RGR is mostly used as a backup when AODV fails to route packets.

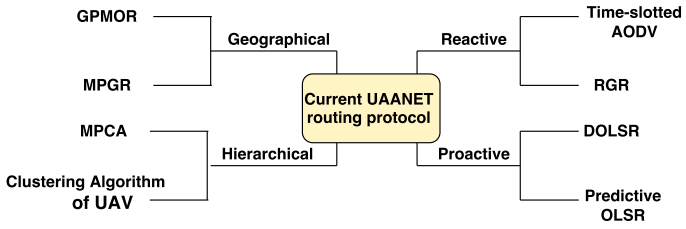

Figure 7. State of the art of UAANET routing protocols

B. Emulation Testbed Results

As explained above, among the existing UAANET routing protocols in the literature, RGR appeared to best fit our requirements in terms of specifications and performances. This leads us to start with AODV which is the first component of RGR, as a starting point of our protocol design. However, RGR testbed environments are different from what we would have in the SUANET use case (see Figure 3 for more detail). Indeed, RGR protocol was implemented in OPNET Modeler [34] and tested with unrealistic test parameters such as a low degree of mobility, several nodes and a non real-time traffic. The choice to directly select a routing protocol based on RGR performance evaluation results is not enough to justify our selection. Therefore, we performed an evaluation performance with a hybrid tool that combined emulation and simulation testbeds. This tool is created during SUANET project and was presented in a different paper [35]. It helped us to emulate a real UAANET experimental scenario (chosen in the SUANET project and described in Figure 3) as closely as possible and use a realistic mobility model[8]. For this purpose, we utilized three virtual machines running on the same ad hoc network. These virtual machines mimic the UAV behaviors in terms of exchange data packets and connectivity through wireless links. The objective is to evaluate and compare the performance of AODV protocol, DSR (Dynamic Source Routing) protocol [36] and OLSR protocol.The testbed specifications of our project are detailed in Table II.

We chose *VirtualBox*[9] as a hypervisor because it enables us to easily establish a communication between multiple virtual machines through a virtual network. Also, we chose the 11.04 version of the *Ubuntu* operating system since it is the version that runs on 2.6.38 *Linux* kernel version. This variant was chosen for convenience, because it corresponds to our developing machine and also to the type of *Linux* kernel deployed in the DT-18 UAV ARM mainboard.

Regarding the performance parameters, we decided to evaluate each protocol according to basic parameters commonly used to characterize routing protocols:

- The routing overhead metric: allows us to measure the amount of extra generated packets by each protocol. It shows us how much bandwidth is occupied by the application data.
- The end-to-end delay metric: allows us to measure the time needed for a packet to cross the network.
- The route retrieval time metric: enables us to measure the routing protocol speeds to find new routes in case of route loss.

Furthermore, passive measurements have also been performed in order to have an accurate data estimation throughout the virtual network. Hence, we use *Tcpdump* to capture the traffic passing over each interface. Additionally, to analyze the traffic recorded by *Tcpdump*[10], we decided to use *Wireshark* [37] which is a powerful analysis tool to extract several metrics from network traces.

Regarding the traffic generation, we use real-time traffic composed of control and payload data generated in previous Delair Tech UAV missions. The control/command data flow concerns the configuration, geo-referencing and camera settings, while the payload traffic gathers real time video, infrared video and image streams.

Based on the specifications detailed above, emulation results are shown in Table III. We can see that AODV has better performance while DSR performance drops because of a large overhead and OLSR performance drops also because of a significant increase of the retrieval time. The value of the end-to-end delay and the retrieval time in case of route failure are particularly important to the SUANET requirements because of the real-time constraints of the data traffic exchanged in this project (for instance video monitoring in real time of devastated geographical areas).

[8]This data is provided by the Delair-Tech company.

[9]Virtual Box website: https://www.virtualbox.org/

[10]http://www.tcpdump.org/

Parameters	Value
Operating system	Ubuntu 11.04
Kernel version	2.1.38
Hypervisor	VirtualBox
Number of VM	Three
Performance parameters	• routing overhead • loss link retrieval time • end to end delay
Passive measurement tools	• Tcpdump • Wireshark
Traffic generator	Real-time traffic pattern

Table II
TEST BEDS SPECIFICATIONS

	AODV	DSR	OLSR
Overhead	33.1 ko	7749.4 ko	32.8 ko
End-to-end delay	0.0038 s	0.0060 s	0.0052 s
Retrieval time in case of link route loss	0.68 s	0.46 s	5.54 s

Table III
EMULATION-BASED RESULTS FOR UAANET ROUTING PROTOCOL COMPARISON

C. Security Robustness Selection

Our security architecture starts with the creation of a new secure routing protocol for UAVs. Therefore, this solution should be robust in the face of the maximum number of attacks and should guarantee security services (authentication, integrity and confidentiality).

It is worth mentioning that UAANET can be seen as a sub-category of MANET (see Section II-A for some details of this justification). Many secure routing approaches have been proposed so far by the MANET research community. Thus, we can consider the state of the art of security attacks for MANET as a starting point for our security robustness evaluation. The reason for such an interest is the very large number of existing attacks for this environment as mentioned in Section II-B1.

1) Security context for future validation purposes: Our new secure routing protocol is currently implemented through the MDD approach previously stated in this paper. When this implementation will be done, we will realize tests on real UAVs in a real environment. This environment will have to take into account the different features of the network system model and the attacker model summarized in Table IV in order to consider a realistic security validation context. This work is part of the future research investigations we are going to enumerate in the next section.

Concerning our network system model, we assume that UAVs and GCS are the only nodes within the network which are homogeneous. It suggests that they are coming from the same manufacturer. This implies that there will be no selfish node within UAANETs. Additionally, we also consider that the application data exchanged is a real time video traffic. As for energy consumption and computation capability, we would like to highlight that all nodes have a required amount of energy and equipped with a powerful processor to run efficiently our cryptographic algorithm presented in Section V.

As for attacker model, we assume that an attacker is capable of the following actions:

- 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 ensured.
- Routing information disclosure: The attacker can obtain information related to the network such as routing information or topology information. They can be collected if the message confidentiality is not protected.
- Performance degradation: The attacker can degrade UAANET performance by rejecting 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 ensured.
- Topology modification: An attacker can also disrupt UAANET connectivity. This can be achieved by inserting additional node or by invalidating a reliable link. An attacker can also forge a false routing information and forward it within the UAANET.
- UAV exclusion (i.e. capture of UAV by an attacker): An attacker can exclude UAVs from the network by inserting false routing information or by modifying 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.

2) Selection process criteria: First of all, because of the real-time traffic exchanged in the SUANET project, the route finding process has to be realized within a short period of time depending on the mobility of UAVs and the number of hops in the route. For all of these reasons, our first evaluation parameter is the routing algorithm vulnerabilities. The aim is to select the supporting algorithm criteria which is the most robust in the face of attacks targeting the route finding process (belonging to category I and detailed in Figure 2).

Furthermore, our second selection criteria is based on the strength of the security mechanism characterized by the considered routing protocol. Based on security requirements, we focus on cryptography. The cryptography based approach can be divided into two categories namely symmetric and asymmetric cryptography. As stated in [38], the public key cryptography is usually considered as more robust in terms of security but adds an extra time overhead while computing the key used in the cryptography process. We make the assumption that this additional burden is negligible in terms

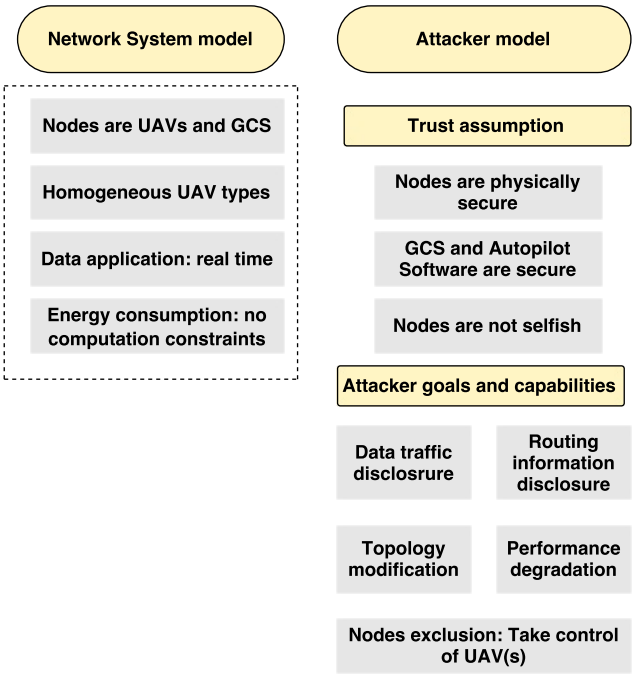

Table IV
NETWORK AND SECURITY CONTEXT OF VALIDATION

of the computing capacity of DT-18. However, we plan to validate this assumption in future real experiments.

3) Mechanism composition to design a better secure routing protocol for UAANET: AODV-SEC [39] is a secure reactive ad hoc routing protocol based on AODV, it is an enhanced version of SAODV [40]. It uses PKI, digital signatures and hash chain functions to ensure the authentication and the integrity of messages. Moreover, it uses a specific certification type mCert [41] which contains only the relevant data of the certificate. This certificate is compatible with the X.509 standard and reduces the overhead by 50 % [42].

Moreover, to guarantee the confidentiality of messages, we propose to combine the two cryptography approaches (symmetric and asymmetric) as they are presented in the protocol MSAODV [24]. Until now this solution seemed robust and efficient but it is still vulnerable against Wormhole attack. To cope with this attack, we propose to add the Packet Leashes algorithm of the protocol TIK (TESLA with Instant Key Disclosure) [43], said to be robust against Wormhole, Blackhole, Rushing and Spoofed attacks. This set of attacks represents the most important part of security vulnerabilities identified for the SUANET project and listed in Section II-B. TIK algorithm offers the possibility to calculate the expiration time and the distance traveled of the packets [44]. This information is then included in the packets, so that the other UAVs can infer whether or not the packet has been altered. Typically, the Packet Leashes mechanism strengthens the authentication of the packet by putting additional information onto the packets in order to restrict maximum transmission of the packet. To implement this method, we use the TIK protocol which uses temporal leashes algorithm with packet expiration times [44] as a metric. This metric is computed by taking into account the maximum distance that the packet should travel.

Security services	**Cryptographic mechanism**	**Algorithm**
Authentication Integrity	- Digital signature, mCert - Hash function	- RSA - SHA-1
Confidentiality	- Symmetric and Asymmetric cryptography	- AES - RSA
Against Wormhole attack	- Packet Leashes	- TIK

Table V
SECURE ROUTING PROTOCOL MECHANISMS DESIGNED FOR THE SUANET PROJECT

Considering the parameters cited above, we have come to the conclusion that AODV-SEC is the most prominent and reliable routing protocol. This protocol is an extension to the AODV algorithm which fulfills several security requirements and tries to secure all possible aspects of the route discovery process. This includes the authentication of the two end nodes as well as the intermediate nodes. The integrity of the route discovery packets (i.e. RREQ, RREP and RRER packets) is protected in such a way that intermediate nodes cannot advertise a potentially fake packet that leads to a shorter route than the one that actually exists.

We chose to extend AODV-SEC security mechanisms with the TIK protocol in order to cope with Wormhole attacks which represent an important threat for UAANET.

Finally, we summarize the different security algorithms selected in our secure routing protocol in Table V. This set of mechanisms handle the different malicious attacks such as: Wormhole, Blackhole, Rushing and Spoofed. It also deals with the following security services: authentication, integrity and confidentialy. Consequently, the different security requirements of SUANET project are covered by this theoretical solution. It is important to note that the different mechanisms have been implemented through the MDD process previously described.

D. Secure routing protocol features

In this subsection, we will detail the features of the secure routing protocol that we will implement and test in the scope of the SUANET research collaboration. As stated previously, this protocol is essentially based on AODV, and combines some of MSAODV and AODV-SEC properties. It is therefore a reactive based protocol which only searches a route when there is a data traffic to send within the UAANET. By choosing AODV protocol, the end-to-end delay value and the retrieval time value in case of route loss will be optimized.

On the one hand, considering the performance parameters, the AODV protocol will be enhanced by including the link quality of the wireless medium as a routing metric. Indeed, in case, where more than 3 UAVs are deployed within UAANETs, it is advisable to select the most stable route rather than the shorter. This is investigated in V-A subsection.

One the other hand, concerning the security criteria, the AODV-SEC algorithm will be implemented to ensure authentication and integrity services. The confidentiality of both data and control traffic will be added through the addition of MSAODV protocol. This protocol is an extension of AODV-SEC and brings confidentiality features by using hybrid cryptographic mechanisms. Furthermore, note that, AODV-SEC does not have a countermeasure against Wormhole attacks. To tackle this specific attack, let us remind that the Packet Leashes (as known as TIK algorihm) mechanism will be added. Figure 8 summarizes the different components we propose to compose in order to design our new secure routing protocol for UAANET.

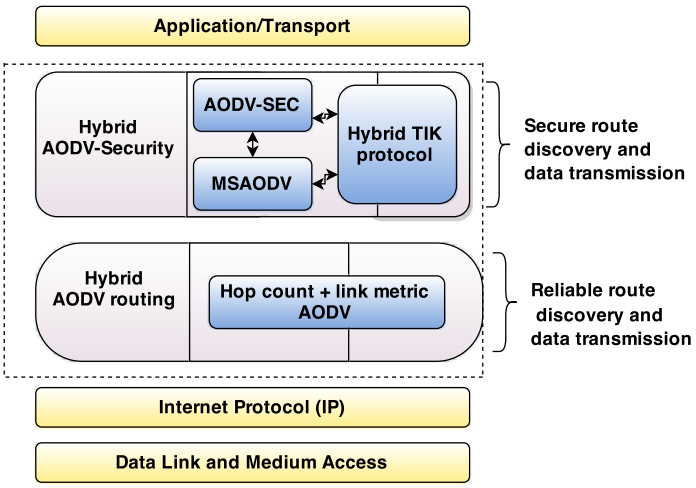

Figure 8. Secure communication protocol suite for UAANET

1) PKI implementation assumptions: As already stated in the introduction, we also need to implement a PKI as a key management infrastructure. The principal objective for developing a PKI for UAANETs is to enable secure, convenient, and efficient acquisition of public keys between UAVs. Such key management scheme includes key distribution and key revocation. The key distribution shares the secret keys to UAVs for secure communications while the key revocation securely enlisting and removing compromised keys.

The prerequisites of implementing such an operation in SUANETs are :

- the presence of a CA (Certificate Authority) to manage life-cycle of digital certificates;
- a distributed method for distributing CA capabilities among entities;
- the security and availability of the CA to the nodes.

These prerequisites point out the challenge of certificate distribution that we will encounter with application security within our future work.

2) Secure routing protocol implementation details: In this section, we will run through the methodology used to design our secure routing protocol. We will first present how we use the MDD methodology to develop the core of our routing protocol algorithm, and then we will give a detailed overview of how we intend to implement our secure routing protocol extension. It is important to consider that several steps have been carried out applying MDD methodology (as shown in Figure 6).

The first step is to validate our requirements specification. Since the AODV protocol was the most efficient in our realistic test scenario (as it has been shown in IV-A), our model requirements are therefore mainly based on the AODV RFC specifications [29]. The main functionalities have been modeled except for few ones which were too complex to develop in high level modeling. We would rather prefer to directly add them during the glueing step (see step 4 described further in this section). Note that the secure routing protocol functionalities can be divided into three partitions:

i a partition to interface the high level software with the to kernel space;
ii a partition to handle information routing;
iii a security partition to protect network traffic.

Figure 9 shows this segmentation. The routing and security partitions are developed with the MDD methodology while the low level network interface handler is processed manually during glueing step .

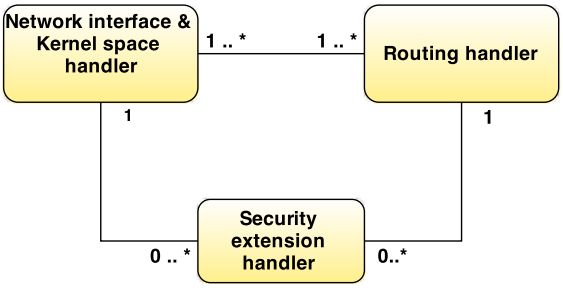

Figure 9. Secure routing protocol design segmentation

The next step is to model the high level requirements with *Simulink* and *Stateflow* toolbox. Thereafter, to get full benefits of MDD through *Matlab Simulink* and *Stateflow*, we employ verification measures with *Simulink Design Verifier* toolboxes. It allows us to check the compatibility of the model, its traceability and certification with respect to the reference document DO-178C [45] used in aeronautical design of embedded systems. Consequently, at the end of this step, we obtained a model verified and validated. Figure 10 gives an illustration of *Matlab Simulink* diagrams and *Stateflow* models developed to implement the different mechanisms of our secure routing algorithm.

Afterwards, the step 3 corresponds to the automatic generation of code. This step consists of enabling the *Embedded Coder* tool offered by *Matlab*. Moreover, the verification of the source code, whether automatically or manually, requires a code review as part of the DO-178C recommendation. This operation is run automatically with *Simulink Code Inspector*

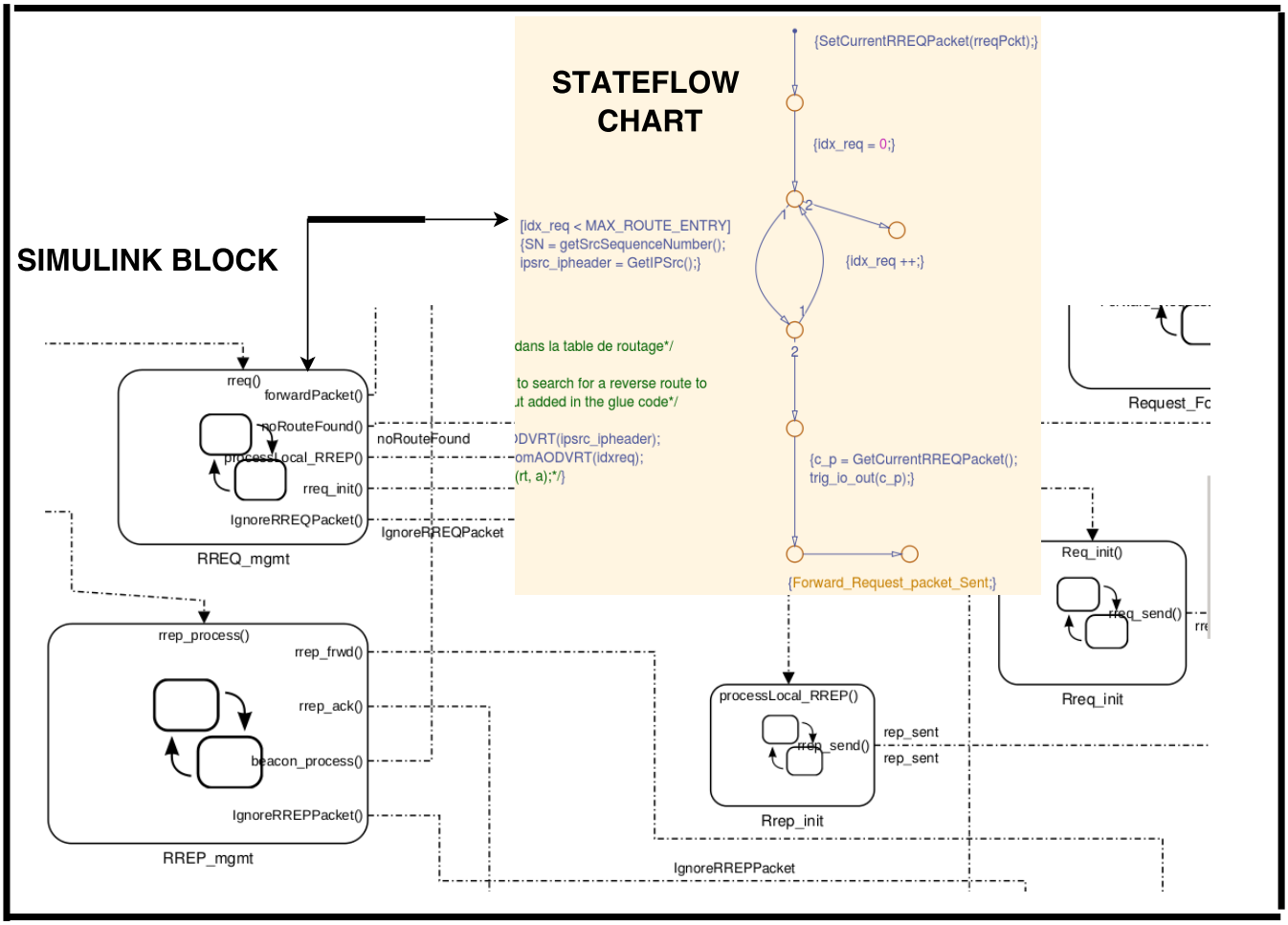

Figure 10. MDD design for secure routing protocol mechanims

toolbox. It compares the generated code with its source model to test specification conformances. The code inspector systematically examines blocks, state diagrams, parameters, and settings in the model to determine whether they are structurally equivalent to operations, operators, and data in the generated code. Ultimately, it generates a traceability documentation that can be used for certification purposes by certification authorities.

The next step (called glueing) consists of linking the previous generated code with the kernel space. Generally, the glue code consists of specifying how the generated code will exchange inputs and outputs with the operating system (in our case *Linux*) kernel by calling the requested library functions. It also specifies how the source code exchanges with the different hooks of the *Netfilter Linux* module. This kernel communication interface can be manually written or automatically generated with a predefined tool. In order to ease this programming task, we decided to use a dedicated toolbox called *Matlab S-Function*[11] which is a description language of *Simulink* blocks and allows to encompass external C code into the model environment.

Afterwards, the fifth step is to generate the object code. This step is automated with *Matlab Code Generation* toolbox with an appropriate compiler in the program preferences. In our work, we decided to stick with the usual *gcc* compiler. However, when integrating the object into our specific embedded systems (Phytec ARM mainboard [46]), it is necessary to cross-compile with cross-compiler and linker tools. Additionally, we have also been able to test the object code and achieve structural coverage compared to the model and to the requirements. This task is automatically executed by the *Matlab Model Coverage* tool.

Finally, the last two steps consist of compilation processes respectively on the emulation tool (detail of the emulation testbed in Section IV-B) and the Phytec ARM mainboard.

Furthermore, having explained how we have used the MDD methodology in our routing protocol design, we will detail how our selected security extension guarantees security requirements. As stated in Section IV-C3, the secure routing protocol we proposed in this paper (detailed in Section IV-D) is an improved security version of the well-known AODV protocol. It combines three security mechanism (AODV-SEC, MSAODV and TIK) to provide comprehensive security solu-

[11]Mathworks online documentation: http://fr.mathworks.com/help/simulink/-matlab-s-functions-1.html

tions which guarantee authentication, integrity and confidentiality security services. In order to ensure these requirements, we use symmetric and asymmetric cryptographic methods. The set of cryptographic mechanism is depicted in Table V.

a) Solution for integrity: The one-way hash chain mechanism is used to ensure that important fields in AODV messages used to find and to maintain route (i.e. the **hop count** and the **lifetime** fields) could not be forged during transmission. This is an asymmetric cryptographic mechanism which has an irreversible function which helps to hide real information under a constant data length. For this purpose, the hash chain is used with a specific field as shown in the following:

- **Hop count**: to prevent any malicious node to present itself as the best next hop;
- **Lifetime**: to prevent any malicious node to invalidate a reliable route;
- **Type**: to prevent any malicious node to modify this field in order to automatically enable other node to reject packets[12].

b) Solution for authentication: Foremost, it is important to note that there are two types of authentication in traditional MANET architectures: *node authentication* and *message authentication*. In the SUANET project, we tackled these two authentication services. On the one hand, the *node authentication* is used to ensure that each UAV and GCS are allowed to participate in the routing process. Among the multiple solutions found in the literature [47], one approach that mostly fitted our project is to verify the node's identity (thanks to certificate verification) through a PKI. As previously mentioned, this point is part of our project objectives but yet to be tackled. On the other hand, *message authentication* is used to authenticate the message originator and also to provide message integrity sureness. For this purpose, we use digital signatures (asymmetric cryptography mechanism) to protect the following fields of the different exchanged packets:

- **Originator IP Address**,
- **Last-Hop IP Address**,
- and **Packet Signature**.

It is important to mention that, as in [39], we add a field called **Packet signature**[13] in order to allow the signature of the entire packet.

Moreover, to ensure that only authorized UAVs and GCS can communicate within the UAANET, an hybrid encryption solution is used for authentication. We make the assumption that each UAV has a set of public and private keys given by a reliable and trusted PKI. We intend to implement them as explained in the following. Firstly, we perform a symmetric encryption during *hello* packet process. For this purpose, each UAV generates a set of *hello* packets for their respective neighbors and signs them with their respective private key. They also append their unique validated and updated certificate before sending them. Thereafter, upon receiving such a packet, the receiving node uses its own private key to decrypt the packet and to verify the certificate of the transmitting node. If this certificate is valid, the current node marks the link through the sender as valid and then sends back a signed *hello* packet with the same method.

c) Solution for confidentiality: We use an hybrid encryption for *route discovery* packets. For this purpose, a node starts by generating *route request* packets (as in the regular AODV mechanism) and then attaches signatures and certificates (as explained previously for the authentication and integrity services). Afterwards, it ciphers each packet with a random symmetric session key. Such a key is generated for each UAV and GCS during the initialization phase (on the ground and before the UAV flights). The next step is to encrypt this symmetric session key with the public key of each trusted node and finally to append it to the packet. Thereafter, the originating node sends in unicast mode each message to the respective neighbors (according to each public key). Furthermore, in the other side of the network, upon reception of the packet, a node performs the reverse operation by first decrypting the symmetric key with the public key of the transmitting node and afterwards by decrypting the RREQ with a symmetric key. If these steps are well processed, it indicates that the node has the right to be in the network and therefore, it can decrypt the message information and also it can process the packet by checking its authentication and integrity (as explained previously).

d) Solution for Wormhole attacks: The previous hybrid (symmetric + asymmetric) security algorithm is able to counter several MANET well-known attacks (e.g, Blackhole, Flooding, Greyhole or Rushing) except the Wormhole. As stated previously, in the Wormhole attack, an attacker tries to intercept a packet from one location and he tunnels them to another location (which can locate another attacker). This information forwarding lets the Wormhole link be faster than the legitimate link within the network, which may trigger other nodes to choose an unreliable link for the routing process.

To counter this powerful attack, the **Packet Leashes** mechanism has been introduced in literature. Note that, in order to get TIK algorithm executed properly, it is required that all UAVs and GCS share a common time reference (this is an additional implementation assumption to the PKI related assumptions listed in Section IV-D1). This can be achieved through the available on-board embedded GPS devices on each UAV and GCS. Once this time is computed, we ensure its truthfulness by a digital signature as an authentication method.

To illustrate our approach, the following flow chart illustrates the sending request process and the receiving event process (Figures 11 and 12) . We only show the RREQ packet as it is the same with other types of AODV packets (i.e. RERR and RREP packets).

[12]Indeed, in case where a UAV is waiting to receive a response packet following its route request, if a malicious node modifies the type value of the RREP packet header into 1 instead of 2, the UAV will always reject the response packet even if a valid route is found.

[13]For instance, for the RREQ packet, we add a new field called RREQ signature.

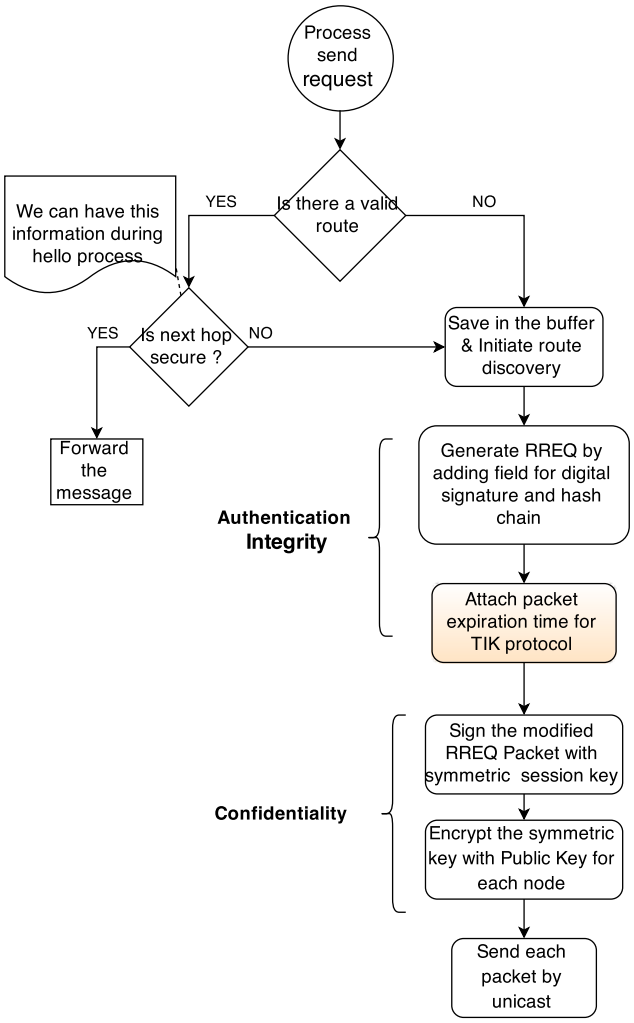

Figure 11. Flow chart for process send request

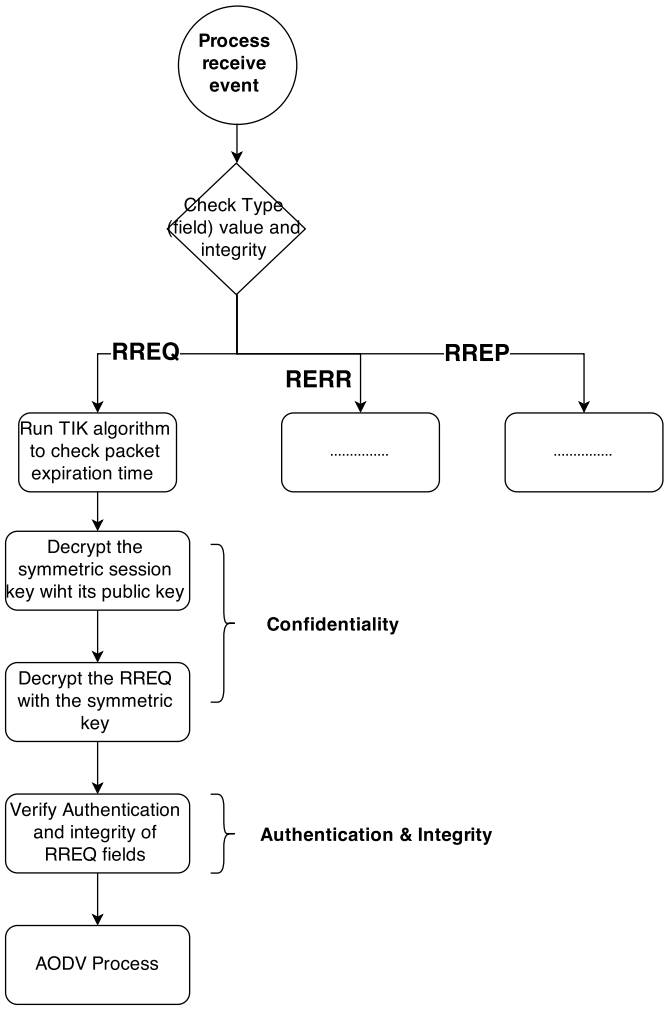

Figure 12. Flow chart for process receive event

V. Conclusion and future research

In this paper, we have presented a new approach to secure a swarm of UAVs. We have detailed the specific features of UAANETs which make this new type of mobile ad hoc network very challenging to secure. From the routing point of view, many protocols which have been proposed for MANETs cannot be applied directly to UAANETs. Therefore, it is necessary to design new efficient routing protocols that appropriately address these high mobility features of UAANET. Accordingly, we have described the SUANET collaboration th at we are currently working on to investigate secure routing research field. Moreover, the MDD approach is used as a security architecture design tool to contribute to the certification of the final UAV communication system. Furthermore, since the secure communication architecture has to provide confidentiality, authentication and integrity, the implementation of a PKI will be undertaken to make these purposes possible by issuing, exchanging and revoking keys for the UAVs. We have introduced three complementary studies based on emulation testbed and literature-based evaluations helping us to choose AODV as the starting point of our process design regarding our project requirements.

Based on this initial design choice we have been able to propose a new secure routing protocol which is a combination of different security mechanisms and which will be able to cope with the different vulnerabilities of UAANET.

A. SUANET project perspectives

The SUANET research collaboration has recently started, and we still have several tasks to complete. Indeed, the routing protocol implementation discussed in Section IV has to be finalized. The next step will be the integration on the Phytec ARM mainboard of DT-18 UAV which is the final product architecture. The challenging part will be the test of our proposed software solution in a real environment with 3 mini-UAVs provided by the DELAIR TECH company.

1) Routing performance enhancements: link quality as a routing: Additionally, we will describe our short term perspectives to strengthen our communication architecture. In order to have a stable route within UAANETs when the number of nodes increases, we would like to add the quality of the wireless link between nodes as a routing metric. This was not initially addressed because, we planned to deploy no more than 3 UAVs into the network. In this case, the usual hop count metric performs well with homogeneous single-radio environments. However, for future deployments, it can be possible to have more than 3 UAVs into the network (with different link settings). In this situation, the hop count metric might not be accurate to find the best route. Indeed, in a heterogeneous and multi-radio environment, the link quality between UAVs is different and the shortest path does not always provide the best available route. For instance, as shown in figure 13, when a UAV can be reached through two paths with the same hop count value, the routing algorithm selects one route arbitrarily without measuring links' quality. As a result, UAV1 can select UAV3 as next hop rather than UAV2 which gives better throughput to transmit video traffic. Another reason to enhance the routing metric assessment is also the disparate conditions of the propagation model. It is important to remember that in UAANET, a propagation model is conditioned by various factors such as variations in communication distance, ground reflection effects and weather conditions. Consequently, there is a possibility that the link quality fluctuates unexpectedly and creates inaccuracy of route discovery.

Because of these issues, it is essential to take into account the link quality to get accurate information about path selection. Furthermore, note that several link metric exist in literature [48]. A non-exhaustive list is given in table VI.

In our future work, we would like to evaluate the existing link metrics and select one or a group of link metrics which are the most relevant with UAANET features. We plan to integrate these metrics with the traditional hop count to form a hybrid metric.

To implement this solution, we envision to use the basic functionalities of AODV. Only the route discovery process will be modified. The hybrid metric is then used to select the most efficient route. Some fields will be added to the RREQ packet, RREP packet and the routing table. Typically, all fields related to hop count will be updated. The RERR packet will not be modified because it does not interfere with the selection process.

Furthermore, once this hybrid routing metric is configured, it will be necessary to ensure its security to avoid any modification from adversary node. Accordingly, its integrity would be protected with an hash chain mechanism (see Section IV-D2a for details).

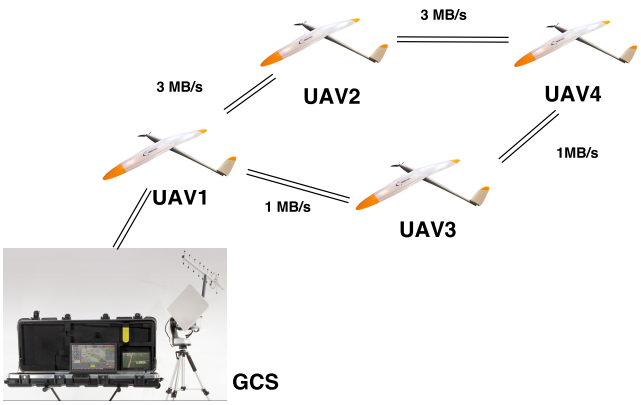

Figure 13. Use case where hop count metric is not sufficient

Link metric	Characteristics
ETX [49]	- Compute link quality during path selection - Find paths with the fewest expected number of total transmissions
ETT [50]	- Compute the time a data packet needs to be successfully transmitted on a link - Consider the expected number of transmission, packet size and raw bandwidth of the link
WCETT [51]	- Find routes with less intra-flow interference
MIC [52]	- Find routes with less inter-flow interference

Table VI
SOME EXISTING LINK QUALITY METRICS

REFERENCES

[1] İ. 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.

[2] E. Miasnikov, "Threat of terrorism using unmanned aerial vehicles: Technical aspects," *Moscow, Russia: Center for Arms Control, Energy, and Environmental Studies, Moscow Institute of Physics and Technology*, 2005.

[3] K. Hartmann and C. Steup, "The vulnerability of uavs to cyber attacks-an approach to the risk assessment," in *Cyber Conflict (CyCon), 2013 5th International Conference on*. IEEE, 2013, pp. 1–23.

[4] D. Tech, *Delair-tech Website*, 2014 (accessed February 3, 2014). [Online]. Available: http://www.delair-tech.com

[5] 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.

[6] S. Rosati, K. Kruzelecki, G. Heitz, D. Floreano, and B. Rimoldi, "Dynamic routing for flying ad hoc networks," *arXiv preprint arXiv:1406.4399*, 2014.

[7] 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.

[8] F. Bai and A. Helmy, "A survey of mobility models," *Wireless Adhoc Networks. University of Southern California, USA*, vol. 206, 2004.

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

[10] 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.

[11] A. I. Alshbatat and L. Dong, "Performance analysis of mobile ad hoc unmanned aerial vehicle communication networks with directional antennas," *International Journal of Aerospace Engineering*, vol. 2010, 2011.

[12] 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.

[13] N. Butcher, A. Stewart, and S. Biaz, "Securing the mavlink communication protocol for unmanned aircraft systems."

[14] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: a tutorial," *Wireless Communications, IEEE*, vol. 18, no. 2, pp. 66–74, 2011.

[15] S. Sen, J. A. Clark, and J. E. Tapiador, "Security threats in mobile ad hoc networks," *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET, Auerbach Publications*, pp. 127–147, 2010.

[16] D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defenses," *Pervasive Computing, IEEE*, vol. 7, no. 1, pp. 74–81, 2008.

[17] P. M. Jawandhiya, M. M. Ghonge, M. Ali, and J. Deshpande, "A survey of mobile ad hoc network attacks," *International Journal of Engineering Science and Technology*, vol. 2, no. 9, pp. 4063–4071, 2010.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

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

[23] R. Maulik and N. Chaki, "A study on wormhole attacks in manet," *International Journal of Computer Information Systems and Industrial Management Applications ISSN*, pp. 2150–7988, 2011.

[24] 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.

[25] L. Abusalah, A. Khokhar, and M. Guizani, "A survey of secure mobile ad hoc routing protocols," *Communications Surveys & Tutorials, IEEE*, vol. 10, no. 4, pp. 78–93, 2008.

[26] A.-S. K. Pathan, *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC press, 2010.

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

[28] O. Pastor, S. España, J. I. Panach, and N. Aquino, "Model-driven development," *Informatik-Spektrum*, vol. 31, no. 5, pp. 394–407, 2008.

[29] C. Perkins, E. Belding-Royer, S. Das *et al.*, "Rfc 3561-ad hoc on-demand distance vector (aodv) routing," *Internet RFCs*, pp. 1–38, 2003.

[30] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "Optimized link state routing protocol for ad hoc networks," in *Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century. Proceedings. IEEE International*. IEEE, 2001, pp. 62–68.

[31] 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.

[32] 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.

[33] 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 *Proceedings of the Ninth Annual Communication Networks and Services Research Conference, CNSR 2011, Ottawa, Ontario, Canada, 2-5 May 2011*, 2011, pp. 161–166. [Online]. Available: http://dx.doi.org/10.1109/CNSR.2011.31

[34] O. Modeler, "Opnet technologies inc," 2009.

[35] J. Maxa, G. Roudiere, and N. Larrieu, "Emulation-based performance evaluation of routing protocols for uaanets," in *Communication Technologies for Vehicles - 8th International Workshop, Nets4Cars/Nets4Trains/Nets4Aircraft 2015, Sousse, Tunisia, May 6-8, 2015. Proceedings*, 2015, pp. 227–240. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-17765-6_20

[36] D. B. Johnson, D. A. Maltz, Y.-C. Hu, and J. Jetcheva, "The dynamic source routing (dsr) protocol for mobile ad hoc networks," *IETF Draft, draft-ietf-manet-dsr-009. txt*, 2003.

[37] G. Combs *et al.*, "Wireshark," *Web page: http://www. wireshark. org/last modified*, pp. 12–02, 2007.

[38] B. A. Forouzan, *Cryptography & Network Security*. McGraw-Hill, Inc., 2007.

[39] 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.

[40] S. Lu, L. Li, K.-Y. Lam, and L. Jia, "Saodv: a manet routing protocol that can withstand black hole attack," in *Computational Intelligence and Security, 2009. CIS'09. International Conference on*, vol. 2. IEEE, 2009, pp. 421–425.

[41] C. Boyd and A. Mathuria, "Key establishment protocols for secure mobile communications: A selective survey," in *Information security and privacy*. Springer, 1998, pp. 344–355.

[42] T. Zia, A. Zomaya, and N. Ababneh, "Evaluation of overheads in security mechanisms in wireless sensor networks," in *Sensor Technologies and Applications, 2007. SensorComm 2007. International Conference on*. IEEE, 2007, pp. 181–185.

[43] 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.

[44] A. Perrig and J. Tygar, "Tesla broadcast authentication," in *Secure Broadcast Communication*. Springer, 2003, pp. 29–53.

[45] Y. Moy, E. Ledinot, H. Delseny, V. Wiels, and B. Monate, "Testing or formal verification: Do-178c alternatives and industrial experience," vol. 30, no. 3. IEEE, 2013, pp. 50–57.

[46] A. Bauer, "Realtime capabilities of low-end powerpc and arm boards for embedded systems," in *Real-Time Linux Workshop*, 2007.

[47] R. S. Puttini, L. Me, and R. T. De Sousa, "Certification and authentication services for securing manet routing protocols," in *In Proceedings of the Fifth IFIP TC6 International Conference on Mobile and Wireless Communications Networks*. Citeseer, 2003.

[48] M. A. Rahman, F. Anwar, M. S. Azad *et al.*, "Integrated metric-ad hoc on-demand distance vector: a routing protocol over wireless mesh networks," *Journal of Computer Science*, vol. 5, no. 7, p. 511, 2009.

[49] N. Javaid, A. Javaid, I. A. Khan, and K. Djouani, "Performance study of etx based wireless routing metrics," in *Computer, Control and Communication, 2009. IC4 2009. 2nd International Conference on*. IEEE, 2009, pp. 1–7.

[50] S. Biaz, B. Qi, and Y. Ji, "Improving expected transmission time metric in multi-rate multi-hop networks," in *Consumer Communications and Networking Conference, 2008. CCNC 2008. 5th IEEE*. IEEE, 2008, pp. 533–537.

[51] L. Ma and M. K. Denko, "A routing metric for load-balancing in wireless mesh networks," in *Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on*, vol. 2. IEEE, 2007, pp. 409–414.

[52] S. Ghannay, S. M. Gammar, F. Filali, and F. Kamoun, "Multi-radio multi-channel routing metrics in ieee 802.11 s-based wireless mesh networksand the winner is," in *Communications and Networking, 2009. ComNet 2009. First International Conference on*. IEEE, 2009, pp. 1–8.

ACKNOWLEDGMENT

We would like to thank Rita ZGHEIB, Master's student at Toulouse University, who helped to design and implement some parts of this secure routing protocol.