Performance evaluation of a new secure routing protocol for UAV Ad hoc Network

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

▶ **To cite this version:**

Jean-Aimé Maxa, Mohamed-Slim Ben Mahmoud, Nicolas Larrieu. Performance evaluation of a new secure routing protocol for UAV Ad hoc Network. DASC 2019 : 38th Digital Avionics Systems Conference, Sep 2019, San Diego, United States. 10.1109/DASC43569.2019.9081613 . hal-02301110

HAL Id: hal-02301110
https://enac.hal.science/hal-02301110

Submitted on 25 May 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Performance evaluation of a new secure routing protocol for UAV Ad hoc Network

Jean-Aimé Maxa[1] , Mohamed Slim Ben Mahmoud[2] and Nicolas Larrieu[2]
[1] APSYS (Innovation team), F-31700 Toulouse, France
[2] ENAC, TELECOM/Resco, F-31055 Toulouse, France
jean.maxa@airbus.com
slim.ben.mahmoud@gmail.com
nicolas.larrieu@enac.fr

***Abstract*---**

UAANET (UAV Ad hoc Network) is defined as an autonomous system made of swarm of UAVs (Unmanned Aerial Vehicle) and GCS (Ground Control Station). Compared to other types of MANET (Mobile Ad hoc network), UAANET have some unique features and bring several challenges. One of them is the design of routing protocol. It must be efficient for creating routes between nodes and dynamically adjusting to the rapidly changing topology. It must also be secure to protect the integrity of the network against malicious attackers.

In this paper, we will present the architecture and the performance evaluation (based on both real-life experimental and emulation studies) of a secure routing protocol called SUAP (Secure UAV Ad hoc routing Protocol). SUAP ensures routing services between nodes to exchange real-time traffic and also guarantees message authentication and integrity to protect the network integrity. Additional security mechanisms were added to detect Wormhole attacks. Wormhole attacks represent a high level of risk for UAV ad hoc network and this is the reason why we choose to focus on this specific multi node attack.

Through performance evaluation campaign, our results show that SUAP ensures the expected security services against different types of attacks while providing an acceptable quality of service for real-time data exchanges.

***Index Terms*---UAV Ad hoc NETwork, Security Architecture, Real-world experiment, Routing Protocol, Performance evaluation**

I. Introduction

An Unmanned aerial vehicle (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, several civilian applications have emerged for small UAVs. Examples are: weather monitoring, infrastructure inspection and aerial monitoring. To support UAV developments, communities such as Dronecode[1] or px4[2] have emerged to provide an open source platform. Through these collective efforts, UAVs are expected to play a major role in supplying both data acquisition and dynamic data streaming for different civilian applications.

Typically, it is possible to deploy and establish the collaboration between several UAVs through a wireless communication network. There are several utilities for a UAV swarm. For example, it would allow to extend the duration of a Unmanned Aerial System (UAS[3]) mission. Such a network is called UAANET for UAV Ad hoc Network and is considered as a subcategory of Mobile Ad hoc Network (MANET).

Ad hoc networks are considered suitable for UAV based networks because of their self-forming, self-healing and self-organizing features. Once UAVs have been configured, they can form their network structure with the guidance from the GCS. Thus, the network becomes resilient to eventual failures of nodes. Ad hoc networks have been largely investigated by the research community for a bunch of mobile systems such as sensors, cars, or civil aircraft. However, much of the work carried out in these areas does not take into account some specific features of UAANET (detailed in section 2) which raises some networking issues.

Furthermore, from a network security perspective, routing protocol traffic needs to be protected against attackers. Typically, there are several reasons to suggest that UAANET is prone to several vulnerabilities. To name a few, the use of wireless links render the communication channel vulnerable. Also, the lack of a fixed infrastructure and the need for cooperation between nodes enable an attacker to breach and disrupt the network integrity. As a result, control packets need to be authenticated to verify both the identity of the message originator and the fields integrity.

A. Contributions

In this paper, we focus on the performance evaluation of a secure routing protocol for UAANET called SUAP (Secure Uav Ad hoc routing Protocol). This routing protocol allows to find routes between swarm of UAVS and GCS. This architecture has been designed through a model-based approach. Each main feature of our architecture belongs to a specific partition. The routing partition (first) is based on the AODV protocol [1]. In addition, message authentication and integrity

[1] https://www.dronecode.org/
[2] https://px4.io/

[3] A Unmanned Aircraft System is composed of UAVs, communication links, ground control stations, launch and recovery system, and any other system elements that may be required during flight operation

are ensured with asymmetric cryptography based mechanisms and hash chains approaches (second partition). The third partition of the protocol is allocated for the detection and the prevention of Wormhole attacks [2]. Due to the complexity of this attack, two distinct mechanisms are combined. The first one is used during route maintenance to analyze and monitor the correlation between the hop count and the distance traveled by each packet. The second mechanism is used during route discovery phase to compute hash values of IP address of forwarding nodes. These mechanisms are detailed in Section 3.

Moreover, for performance evaluation purposes, we will describe the experimental testbeds and the test results. Two types of experiment were realized.

- hybrid simulation&emulation based experiments as described in [3].
- real world experiments performed with several UAVS and GCS.

B. Structure of the paper

This paper is organized as follows. In Section 2, we highlight the state of the art on UAANET, routing and security. Section 3 describes the SUAP routing protocol by specifying the structure of route discovery and route maintenance packets. In Section 4, we present the performance evaluation of the SUAP protocol. Finally, we draw the conclusions and the future work in Section 5.

II. UAANET routing and security state of the art

Ad hoc drone network is a sub-category of the MANET mobile network. It involves the deployment of a fleet of drones and ground stations through a wireless ad hoc network. Drones work together with the ground control station(s) to exchange data, which may relate specifically to routing (control packets) or contain information specific to the UAS.

UAANETs do not require a fixed infrastructure and are based on nodes working together to exchange data. However, they have certain specific characteristics which set them apart from other types of ad hoc network. These specific features concern the network connectivity, the node densisty, the energy consumption and the strict delay constraints related to the exchange of real-time traffic.

A. Routing protocol for UAANET

Routing is a method used to transmit data from an emitting node to a recipient or recipients. In mobile ad hoc networks, routing is based on a packet re-sending approach. The challenge lies in identifying an optimal pathway. Routing involves calculating the best pathway between two given nodes in a network. A certain metric thus needs to be assigned to connections so that the route identification process may, for example, simply involve calculating the shortest pathway between a source and a destination.

It should be noted that the high level of node mobility is a particularly important feature of ad hoc drone networks. Frequent changes in topology lead to route changes and create a management overhead in the routine mechanism. Lost routes need to be restored rapidly in order to avoid packet loss or sub-optimal bandwidth usage resulting from retransmission. As the traffic is critical, a rapid and effective backup mechanism is necessary. These constraints mean that a routing protocol needs to have excellent overhead properties and and the lowest time of execution. A number of routing protocols for ad hoc drone networks have been published in response to this context; most are extensions of routing protocols used for MANET networks [4] such as AODV, OLSR [5], DSR [6] and Geographical routing, as surveyed in [7].

The question that needs to be answered is which routing protocols fit the best the UAANET environment. To provide an answer to this question, in [3], we have introduced an emulation-based performance evaluation of MANETs routing protocols for UAANETs. This realistic study considers the Linux kernel networking stack requirements, the protocol implementation issues, the background traffics, the real time execution features and a realistic UAVs mobility model that was deduced from real UAS flights. Our results showed that AODV suits better in UAANET compared to OLSR and DSR.

Based on these findings, in [8], we have introduced the model design of SUAP (Secure Uav Ad hoc routing Protocol). Then, a first preliminary outdoor experiment has been carried out in [9] to evaluate its network requirements and performances.

B. Security Challenges for UAANET

1) Vulnerabilities: spontaneous environments of UAANET are subject to a number of security issues. These different weak points are:

- **Vulnerable communications channels**: wireless connections are used to send and receive signals in a UAANET network. These radio links may be subject to a variety of attack types, including illicit listening or active interference [10]. Given that all traffic is airborne, the attacker simply needs to adopt a position in the zone covered by the target nodes in order to intercept traffic.
- **Uncontrolled environment**: generally, wireless ad hoc networks operate in a distributed and dynamic environment. This means that communications between nodes participating in the routing process are shared and operate in an opportunistic manner. This makes it hard to control nodes coming into or leaving the network, and a malicious node may be able to connect to the network and participate in packet transfer.
- **Dynamic topology**: the high travel speed of UAVs means that the topology of the network is not stable and changes continuously. This characteristic creates security issues, as routing protocols do not have the intrinsic ability to differentiate between interrupted communications (or a broken link) caused by drone movements and those caused by an attacker acting on the network [11].
- **Cooperation issues**: in an ad hoc wireless network, routing algorithms do not intrinsically require the use of a node pre-association algorithm prior to execution.

This is based on the hypothesis that nodes are cooperative and not malicious; situations involving a malicious node compromising the network are not taken into account. Consequently, node authenticity is not guaranteed, allowing malicious nodes to enter the network.

- **Limited resources**: the calculation and memory capabilities of drones are limited by their size. This fact may be exploited to attack the network by exhausting drone resources. The sleep deprivation attack [12], for example, consists of transmitting a constant stream of control messages toward network nodes. Once all resources have been used up, drones may be captured or diverted by an attacker.
- **Existence of attacks**: ad hoc networks are generally targeted by attacks directed against a subset of the protocol layer of the OSI model [13]. These attacks may be grouped into two classes: rational and irrational. Irrational attacks aim to disrupt the operation of network services without deriving any benefit from the results, whilst rational attacks are designed to provide a direct or indirect benefit for the attacker. For example, an attacker may aim to violate a network security policy in order to falsify functions and sensitive data. Violating the integrity of this critical information may lead to a variation in network connectivity, causing a UAV mission to fail.

III. SUAP routing protocol

In this section, we will propose a new routing protocol, designed to respond to the reliability and security requirements for communications within a UAV swarm.

During the design step of our secure communication architecture, we needed to choose an existing routing protocol as a starting point. We selected a protocol used in the MANET environment, adding our own security mechanisms. In order to select a protocol, we needed to evaluate the different classes of routing protocol and to identify those which come closest to the real implementation conditions of a UAANET network. The details of our evaluation process are set out in [3]. We recommend this paper as it presents the full architecture of the targeted secure communication architecture. The simulation experiment of the SUAP protocol had been also detailed. Our results showed that the AODV protocol performs better in these conditions than OLSR or DSR, given our specific scenario and considering metrics including the connectivity rate, end-to-end delay, average re-creation delay and overhead rate.

We therefore chose to use the AODV protocol as the basis for our secure routing protocol. The mechanisms in the SUAP protocol which relate directly to route creation in a network are based on AODV.

The network model and attacks considered in designing the SUAP protocol are detailed in [14]

A. Description of the SUAP protocol

SUAP is characterized by security mechanisms which guarantee the authentication of non-mutable fields (i.e. fields within the routing protocol which remain static from emission to reception of a packet by the receiver, such as the address fields of the source and destination nodes), the integrity of mutable fields (such as the hop count) and non-repudiation. It also includes mechanisms for detecting Wormhole attacks.

In what follows, we will: (1) describe the Wormhole attacks, (2) highlight the vulnerabilities encountered and (3) discuss the specification of the SUAP protocol.

1) Wormhole attacks: Wormhole attack is a serious attack which targets the routing process. It is effective against reactive routing protocols using hop counts as their route selection metric. The attack creates a disturbance in the packet routing process, as distant nodes are led to believe that they are neighbors. Genuine nodes are obliged to follow the routing protocol algorithm, choosing the shortest available route, and thus transmit packets through the Wormhole.

Figure 1 shows an example of a Wormhole attack. In this case, nodes N0 and N3 are led to believe that they are neighbors. Attacker A1 transfers all packets from node N0 directly to N3, via a second attacker A2. Node 3 thus believes that N0 is in range, i.e. a neighbor. All AODV control packets (Hello, RREQ, RREP, RERR) are then transmitted along this route. Even with no knowledge of cryptographic keys or of the selected hash function, attackers are able to damage the integrity of the network by transferring control packets, and subsequently capture data traffic.

B. SUAP security features

SUAP routing protocol is based on public key cryptography, hash chains and geographical leashes [15]. It uses digital signatures for non-mutable fields and hash chains for mutable fields (i.e the hop count). A node that generates a routing message signs it with its private key, and the nodes that receive the message verify the signature using the sender's public key. The hop count cannot be signed by the sender, because it must be increased at every hop. A mechanism based on hash chains is used instead for mutable fields.

Intrinsically, the routing protocol is still vulnerable against Wormhole attacks. Accordingly, a version of geographical leashes based security algorithm is used to estimate the correlation between the traveled distance and the hop count value. In order to do so, SUAP requires each node in the network to be tightly synchronized and maintains a local connectivity with its direct neighbor.

C. Enhanced Beacon message mechanism

Beacon message is sent by broadcast to one-hop neighbors to maintain the local connections updated. Our objective with SUAP is to protect these packets from Wormhole attacks. Hence, besides signing all the data fields, we use a mechanism that analyzes the correlation between hop count and distance traveled by the packet. When sending messages, each node includes its actual location information. To protect from malicious modification, message fields are signed (including the geographical position).

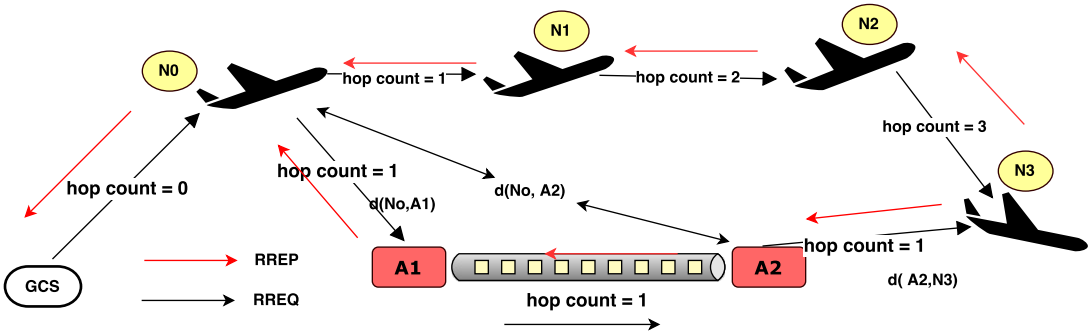

Figure 1 Illustration of Wormhole Attack in UAANETs

The mathematical proof of our demonstration is detailed in [14].

Table I is then created in order to detect Wormhole attacks.

Table I Correspondence table between geographical distance T and hop count

Value of T	Hop count hc
$0 < To \leq Dmax$	0
$D_{max} < T1 \leq 2Dmax$	1
.....	.....
$(n-1)D_{max} < T_{n-1} \leq (n+1)Dmax$	n-1

From this table, we obtain:

$$\frac{T}{Dmax} - 1 \leq hc < \frac{T}{Dmax} + 1 \qquad (1)$$

To detect a Wormhole attack, we can either use the correspondence table or use this inequality to see whether the hop count falls within the interval given above.

D. Securing route discovery

In order to implement an hop-by-hop authentication, each node must verify the incoming message from its one-hop neighbors before sending it by unicast to its neighbors. Each node must ensure that the packet is authenticated and was not forwarded through Wormhole link. Thus, each node should make sure that it has a trust relationship with its neighbors. Such secure relationship between each pair of nodes relies on the exchange of beacon messages between neighbors as explained previously. In SUAP, the route discovery process is similar to that of standard AODV, but two hash extensions are appended to the end of route discovery packets as explained in the following.

During the route discovery process route request and response are exchanged. In this mechanism, nodes do not need to send its geographical position. Instead, each node assumes that its local connectivity is secure thanks to the neighbor information provided by the previous mechanism. Each node then sends in unicast all route discovery packets to its direct neighbors. Each node also includes the address of the next hop to which the message is forwarded and apply a hash chain to the packet mutable fields. The non-mutable fields are signed as stated previously. An illustration of the request message is shown in Table II. The source node appends its own address and the next node address to the hash chain called *Hashnew*. It also includes the *Hashold* (which is the previous *Hashnew*) within the packet.

Table II SUAP Request Packet Signature Extension Fields

Field	Value
Type	64
Hash function	hash function selected by the sender node. It is used to compute the hash chain field
Signature	The signature of all the non-mutable fields
Hashnew	Hashnew = H [CurrentNode, NextNode, Hashold] CurrentNode is the address of node sending the request packet. It can be its public key or its IP Address. The Nextnode is the next node public key or IP Address. Hashold is the previous chain element received from the previous node
Hashold	It is the previous chain element received from the previous node. When receiving packets, nodes change the value of *Hashnew* into *Hashold*
Hop Count	The actual hop count of the packet. It is the number of times the hash is performed

The operation is repeated until the packet reaches the destination. The same mechanism is also used for the response packet. As regards to the exact value of the hop count values, it can be inferred from the number of times that the hash was used for verification. It can also be included in the hash chain computation. Note that this mechanism can also be efficient against man in the middle attacks in which malicious nodes tries to breach route discovery mechanisms by forwarding control packets from one point to another.

E. Limitations of the SUAP protocol

The hash function principle used in SUAP protocol falls down in failing to consider Kerchoffs's principle. In SAODV, a hash function table is created, and is only known by genuine nodes, permitting them to identify the function chosen by the source node. This may be seen as a form of security by obfuscation, as the function is only initially known by genuine nodes.

If an attacker is able to gain knowledge of this function, a number of attacks on the SUAP protocol are possible.

First, an attacker may use the hash function to increase the hop count in order to prevent a packet from being transmitted over an optimum route. For example, an attacker may forcibly increase the hop count for a genuine route so that packets are transmitted over a different, non-optimal route, thus reducing network performance.

Second, one or more wormhole attackers may also modify the value of the *Hashnew* and *Hashold* stamps to avoid detection. This more sophisticated form of attack consists of not only creating a tunnel, but also modifying the packet exchanged through the tunnel. Attacks of this kind have not been considered for this study, as we have only considered wormholes which do not modify packets, as defined in [2]. In the case of a modification attack, if the attacker manages to deduce the value of *Hashnew* from *Hashold* by taking account of the identity of genuine nodes, packets passing through a wormhole may not be detected. However, this type of attack involving value modification has limited effects in a real-time context, particularly when a more robust hash function is used. If the hash function in question results from a composition of functions (as described in [16]), the function may be public, as the time needed for an attacker to calculate the function would be too high for them to have an impact on the integrity of routing messages (executed in real time during the mission).

IV. Performance evaluation of SUAP

In this section, we will present the validation of security functions of the SUAP protocol through performance evaluations.

Figure 2 indicates the security functions and the selection of experiment realized in our study.

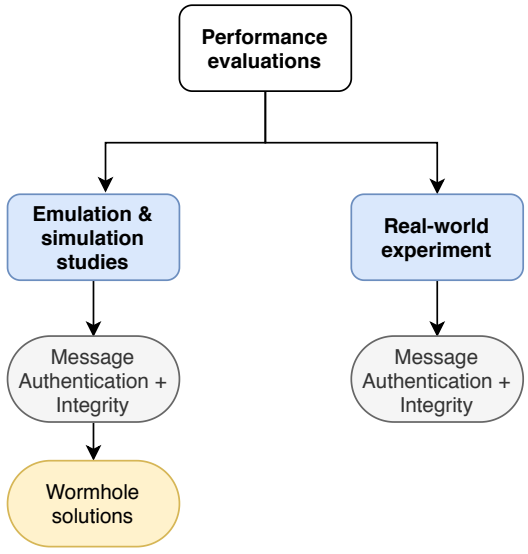

Figure 2 Performance evaluations of SUAP

According the figure 2, the Wormhole solutions are only validated through simulation studies. This is due mainly to the difficulty that we encountered to set up a tunnel between the two attackers during the real-world experiment. As for the message authentication solutions, we were able to validate them through both real-world experiment and simulation&emulation studies. In the following, we will focus on the evaluation of the Wormhole solutions (validated through emulation studies) and the evaluation of the message authentication functions validated through real-life experiments with DT 18 drone.

A. Validation of the security partition (message authentication) in a real-world experiment

The topology used here is shown in figure 3. It is made up of 4 nodes: three DT18 drones and a ground control station. We added a second ground station, acting as a black hole attacker. For the purposes of this test, we needed to place an attacker near the emitting node Dr3 to verify whether the genuine route through nodes Dr1 and Dr2 would be chosen throughout the test period. We therefore reduced the power of the modem antenna to give us a range less than or equal to 500m. Station 4 (the black hole attacker) has a maximum emission power of up to 1.5km. In other terms, the attacker has the capacity to contact all of the nodes in the network, notably the most distant drone. This topology allows us to verify whether or not the SUAP protocol is able to defend against black hole attacks in real conditions.

It is important to note that other equipment could have been used to play the part of the attacker. The choice of a ground station avoided the need to implement the black hole attack code in a different machine architecture. The previous configurations remained unchanged. The traffic exchanged between nodes is summarized in table III.

Table III Different flows exchanged during the flight test

Type	Source ----- Destination	Packet size	Exchange rate
Tick	Station1 ----- Dr1 Station2 ----- Dr2 Station3 ----- Dr3	64 bytes	1 packet/sec
Georef	Dr1 ----- Station1 Dr2 ----- Station2 Dr3 ----- Station3	80 bytes	3 packets/sec
Command	Station 1 ------ Dr1 Station 2 ------ Dr2 Station 3 ------ Dr3	80 bytes	1 packet/sec
Video	Dr3 --------- Station1	1400 bytes	25 UDP datagrams/sec width=720, height=576

Packet loss rate: The packet loss rate is shown in table IV. As we can see, losses are concentrated around the connection between the three drones. The mobility and different movement patterns of the drones during the test resulted in connections being lost and re-established over the course of the test. The total observed loss rate is 5.57 % for data packets sent from node Dr3 to node station 1. This result is acceptable compared to the results obtained through emulation.

Overhead: The results for the overhead are shown in table V, and are also similar to those obtained through emulation. The reactive nature of the routing protocol means that few traffic signaling packets are exchanged within the network.

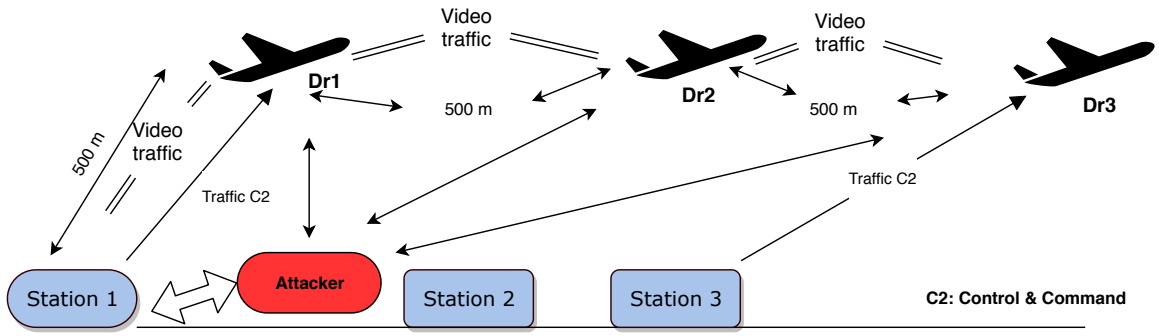

Figure 3 Topology used to validate the security partition in a real environment

Table IV Loss rates (%) measured between each node

Source	Destination	loss rate
Station 1	Dr1	0.53
Dr1	Dr2	2.32
Dr2	Dr3	2.70
Total (Station 1 --- Dr3)		5.57

The protocol only acts if a route creation request is emitted. The low density of nodes means that drone movement speed has no direct impact on this value.

Table V Overhead for the 16 minute test period

Source	Destination	Size of control packets (in bytes)	Percentage of total traffic
Station 1	Dr1	89 760	0.075 %
Dr1	Dr2	153 653	0.093 %
Dr2	Dr3	153 321	0.0927 %
Total			0.270 %

Table VI Route stability in the presence of a black hole attacker

Delay	Value
Average delay	15.15 s
Maximum delay	20.44 s

Average route lifespan: Our results for the average lifespan of routes between station 1 and Dr3 are shown in table VI and figure 4. We can observe that the average lifespan of a route remains within an acceptable value and in the same range with and without security as described in [14]. This indicates that our routing protocol behaves in the same way as AODV in performance terms, and that the addition of security mechanisms does not have a detrimental effect on network performance, whilst providing defense against attacks in this configuration.

The delay involved in re-establishing a route in response to a loss of connectivity between one or more nodes, causing route loss, is shown in table VII. We obtained an average delay value of 2.23 milliseconds, which is sufficient to compensate for frequent connectivity losses in the network. This result is in the same range as the route re-establishment value obtained

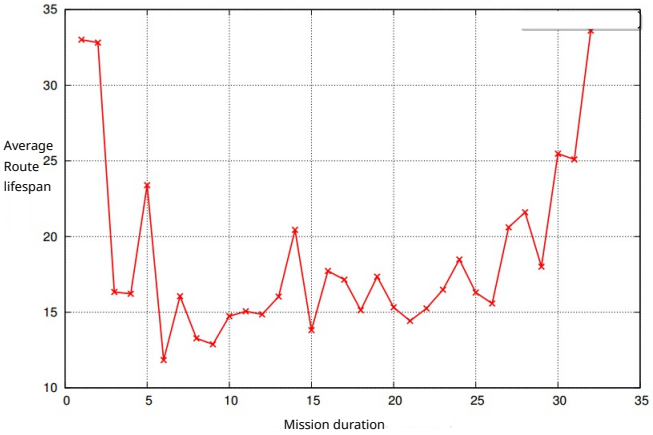

Figure 4 Route stability in the presence of a black hole attacker

for the AODV protocol through real testing (2.23 ms compared with 2.08 ms).

Table VII Route re-establishment delay following a loss of connection

Delay	value
Average delay	2.23 ms
Maximum delay	5.79 ms

Table VIII End-to-end delay for control packets and real-time traffic

End-to-end delay for signalling traffic exchanges	Value	End-to-end delay for payload traffic exchanges	Value
Average delay	7.43 ms	Average delay	9.2 ms
Maximum delay	100 ms	Maximum delay	104 ms

End-to-end delay: The end-to-end delay for each traffic type is shown in table VIII. This value is generally low (under 10 ms on average) and does not have a negative impact on real-time traffic exchanges. However, it is higher than

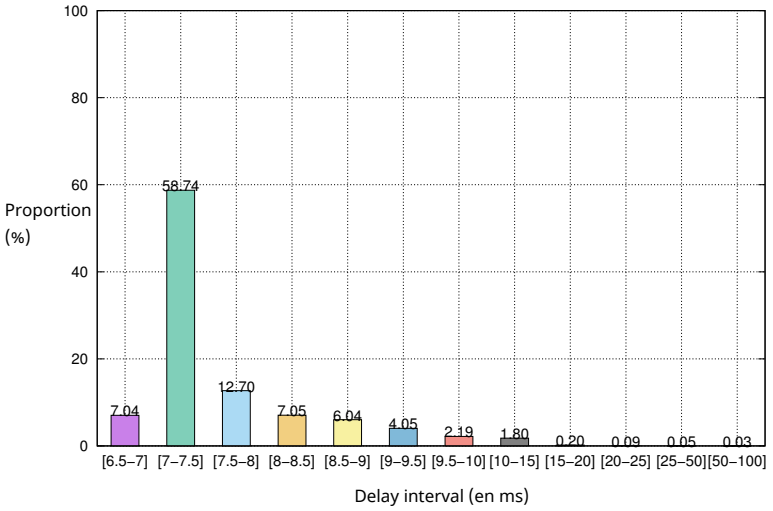

Figure 5 Distribution of end-to-end delay values over the course of the mission

the result obtained for the AODV routing protocol. This is due to the non-negligible time taken by the LIBGCRYPT cryptography library[4], used to create and verify signatures and hashes. Figure 5 shows the evolution of the end-to-end delay over the course of the mission, illustrating the proportion of packets with a delay of over 10 ms. We see that our results are concentrated in the interval [7, 7.5]. Delays of over 100 ms only occurred on 7 occasions during the mission.

B. Evaluation of the AODV protocol in a real environment with a black hole attacker

To gain a clearer understanding of the results we obtained for our message authentication mechanisms, we tested the AODV protocol in a real environment with a black hole attacker. This test was carried out using the same configuration used for SUAP, as shown in table III and figure 3. Our results are summarized in table IX. These results are shown alongside those obtained for the SUAP protocol, as seen above. Note that only those metrics for which AODV and SUAP produced significantly different results are shown here.

Note that drone mobility was not the same in this case as in our evaluation of the SUAP protocol, due to the difficulty involved in reproducing exactly the same movement patterns in a real environment. However, our results clearly show the weakness of the AODV protocol to black hole attacks in a real environment. These results may be explained as follows:

- for the loss rate, the majority of data packets are lost in this case, because each time a route request is sent, the black hole attacker intervenes and emits fake packets, leading to erroneous routes.
- the percentage of routes established between station 1 and node Dr3 is only 1.7 % for the whole mission, as the vast majority of established routes included the black hole attacker.
- the overhead value obtained for the AODV protocol is smaller than that for the SUAP protocol (cf. the results presented in table V). The additional traffic results from the security mechanisms included in the latter protocol. However, it is not sufficiently high to have a negative impact on data exchange, as we saw above (cf. the end-to-end delay results presented in table VIII).

Table IX Summary of results obtained for real environment evaluations of the AODV protocol with a black hole attacker

Parameter	Real test of the AODV protocol with a black hole attacker	Real test of the SUAP protocol with a black hole attacker
Loss rate	98.20 %	5.57 %
Percentage of routes established between Station 1 and Dr3	1.76 %	100 %
Overhead	210 kb	397kb

C. Discussion for the security functions of SUAP to counter black hole attacks

We have presented our validation study for the message authentication partition of the SUAP protocol. The results obtained show that the SUAP protocol offers a robust defense against black hole attacks. We focused on black hole attacks as they allow us to check whether each node in the network is able to verify the security level of messages before processing them. The black hole attack can be seen to have no direct influence on the performance of the SUAP protocol, whilst having a significant effect on the AODV routing protocol. We may thus state that our secure routing protocol demonstrates the high-level behaviors set out in the specification. These first results are positive but not sufficient to validate all of the security functions of the SUAP protocol. In the following section, therefore, we will consider the Wormhole detection mechanism proposed earlier in this chapter, which constitutes one of the main components of our security architecture.

D. Validation of the Wormhole detection mechanism with emulation studies

In this section, we shall analyze the precision of Wormhole attack detection offered by the SUAP protocol. This validation study was carried out by emulation alone with the tool presented in [14]. To validate the partition, we considered a topology made up of 5 genuine nodes and two attackers, as shown in figure 6. We used emulation for this phase of validation due to limited access to mobile nodes and to embedded systems compatible with the DT18's communications systems, which meant that we did not have the means to envisage a real-environment validation approach. The possibility of carrying

[4]For more information, see https://www.gnupg.org/software/libgcrypt/index.html

out real-world tests of this nature will be discussed in the following chapter.

The parameters used in our scenario are shown in table X.

Table X Evaluation parameters used in validating the Wormhole attack detection mechanism

Parameters	**Value**
Number of genuine nodes	5 (4 drones and 1 ground station)
Mobility	Real mobility replay
Routing protocol	SUAP and AODV
MAC protocol	802.11
Radio range	100m
Simulation duration	600 s
Channel capacity	54 Mbit/s

We compared the SUAP and AODV protocols to study the influence of the attack. To do this, we verified that the route passing through the tunnel between A1 and A2 was not used for data transmission. We considered two metrics in assessing the relevance of our mechanism:

1) firstly, we measured the quantity of data (sent from drone Dr4) received by the ground station (traveling over the two alternative routes). This allowed us to compare the quantity of data passing through the wormhole and the quantity of data passing through a genuine connection.
2) secondly, we evaluated the number of established routes passing through the wormhole and the number of routes passing through the legitimate connection.

These two metrics are complementary, and sufficient to demonstrate the relevance of our security mechanism in defending against Wormhole attacks.

For validation purposes, we decided to simulate two stationary attackers, with A1 located close to the ground control station and A2 close to the most distant node, Dr4. In this way, the attackers were located near the target nodes, making it easier to evaluate the impact of the attack.

Tables XII and XIII show the quantity of information exchanged by genuine nodes and by attackers, respectively. We see that, using the SUAP protocol, the wormhole tunnel only transmits routing information for the target nodes. The fact that attackers receive routing packets is not important, as these messages do not contain any secret information relating to the mission.

We also see that no video information is transmitted between A1 and A2. Here, detection is carried out by the ground station, which identifies an anomaly between its relative distance from node Dr4 and the hop count in the neighborhood discovery packet received from thus node. In this case, Hello packets are protected by a geographical leash algorithm which compares the hop count and the relative distance between neighbors. Request and response packets are protected by a hashing function. Our results show that SUAP is effective in choosing a genuine route, despite routes with better metrics being offered through the wormhole.

Table XI Generated traffic: 1=Dr1, 2=Dr2, 3=Dr3, 4=Dr4

Type	Source→Destination	Packet size	Frequency
Tick	1→2,1→3,1→4	64 bytes	1.0 packets/s
Georef	2→1,3→1, 4→1	64 bytes	1.8 packets/s
Command	1→2,1→3, 1→4	64 bytes	0.034 packets/s
Video	2→1,3→1,4→1	4 Mbit/s	

Comparing these results with table XIII, which indicates the quantity of data received by the two attackers using the AODV protocol, we see that the wormhole succeeds in transmitting video from node Dr4. In this case, the other genuine nodes only exchange signaling traffic, receiving only a tiny part of the useful data (0.18 % of the total traffic). This is explained by the fact that the route through the malicious nodes is always chosen as it offers a better hop count metric. The value of 0.18 % is due to the fact that node Dr4 may, on occasion, be out of range of A2 due to its mobility, and in this case, the genuine route may be used for video transmission over a short period of time, corresponding to 0.18 % of the total quantity.

Figure 7 shows our results for data delivery rates over both routes (genuine and wormhole) as presented in tables XII and XIII. We see that using the SUAP protocol, only the genuine route is used to transmit data packets. This leads us to conclude that the SUAP protocol is robust against Wormhole attacks.

a) : To improve our understanding of these results, we measured the route creation rate along the legitimate route (Dr4, Dr3, Dr2, Dr1 and the ground control station) and the route creation rate through the wormhole (Dr4, A1, A2 and the ground station). As we see from figure 8, the creation rate along the genuine route is around 85 % for the whole duration of the simulation, whilst the result for the wormhole route is 0 %. The route creation rate using SUAP does not add up to 100 %, as in this case, node mobility comes into play and creates fluctuations in connections between neighbors. These values should be compared to our results for the AODV protocol, shown in the same figure. Without the detection mechanism, the route establishment rate is around 90 % over the wormhole connection. This total is higher than that achieved by SUAP, as the two attackers are stationary and the links along the route are thus subject to less fluctuation. The Wormhole attack may thus appear to improve performance depending on the network topology and the selected metric. That being said, without our detection protocol, video traffic is directed toward the wormhole.

Furthermore, the route creation rate over the genuine route using AODV is significantly lower, being close to 0 %. This 0% value is never achieved, as the mobility characteristic of node Dr4 may cause it to be out of range of the attacker A2 for a short period of time, during which it communicates with its genuine neighbor Dr3. This exchange is negligible, however, as the route creation rate over the connection (Dr4, Dr3, Dr2, Dr1, GCS) is around 0.18 % for the whole period of communication.

These results demonstrate the capacity of our approach to retain a genuine route through active, legitimate nodes, and to ignore routes through a wormhole. We thus obtain a packet delivery rate of around 85 %, similar to that obtained for AODV through simulation (88 %). We also note that, in the

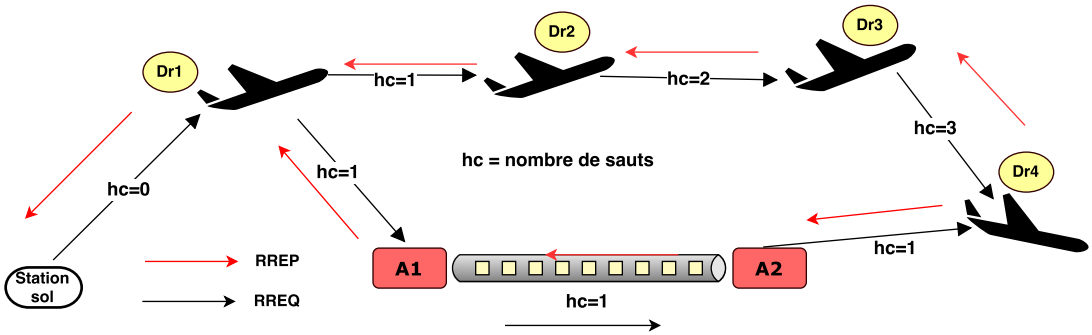

Figure 6 Validation topology for the Wormhole attack

Table XII Summary of data sent and received in communications between Dr4 and the ground control station using the SUAP protocol

Source	Quantity of signaling traffic generated	Video traffic generated	Destination	Quantity of signaling traffic received	Quantity of data traffic received
Dr4	146783 bytes	23 02 289 kb	Dr3	146783 bytes	23 02 111 kb
Dr3	140782 bytes	23 02 111 kb	Dr2	140782 bytes	23 00 011 kb
Dr2	142345 bytes	23 00 011 kb	Dr1	142345 bytes	22 98 245 kb
Dr1	130011 bytes	22 98 245 kb	GCS	140011 bytes	22 97 988 kb
Dr4	146783 bytes	23 02 289 kb	A1	146783 bytes	**0 bytes**
A1	146783 bytes	**0 bytes**	A2	146783 bytes	**0 bytes**

Table XIII Summary of data sent and received in communications between Dr4 and the ground control station using the AODV protocol (no security)

Source	Quantity of signaling traffic generated	Video traffic generated	Destination	Quantity of signaling traffic received	Quantity of data traffic received
Dr4	146783 bytes	23 02 289 kb	Dr3	146783 bytes	13450 kb
Dr3	140782 bytes	13450 kb	Dr2	140782 bytes	13450 kb
Dr2	142345 bytes	13450 kb	Dr1	142345 bytes	13450 kb
Dr1	130011 bytes	13450 kb	GCS	140011 bytes	13450 kb
Dr4	146783 bytes	23 02 289 kb	A1	146783 bytes	22 98 839 kb
A1	146783 bytes	22 98 839 kb	A2	146783 bytes	22 98 839 kb

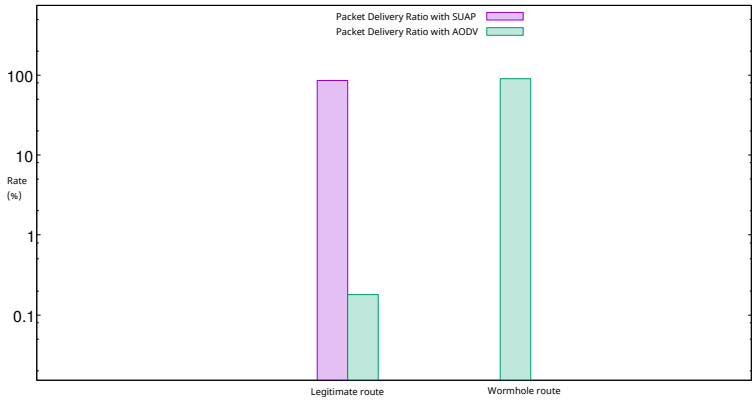

Figure 7 Packet delivery rate in the context of a Wormhole attack

absence of a Wormhole detection mechanism, the percentage of established routes passing through the genuine node is markedly lower. Our results therefore show the SUAP protocol to be effective against Wormhole attacks, as described above.

V. Conclusion and future research

In this paper, we have described the validation of the security partitions of the SUAP protocol. This validation by performance evaluation was carried out, on the one hand, using a tool which combines emulation (virtual machines) with simulation (the OMNET++ tool), and, on the other hand, in a real environment using Delair-Tech DT18 drones. Our test architecture was made up of three UAVs and three ground stations, one of which was a communicating network node. Our test configuration involved a communications system featuring a fleet of cooperating drones, piloted by ground stations.

The performance of the SUAP protocol was validated through a series of tests. The results, as given above, indicate that SUAP is able to ensure the security of communications between nodes by providing message authentication services. It is also able to detect the presence of wormholes, and ensures that only genuine nodes can transmit data packets. Furthermore, it respects the time constraints imposed by the

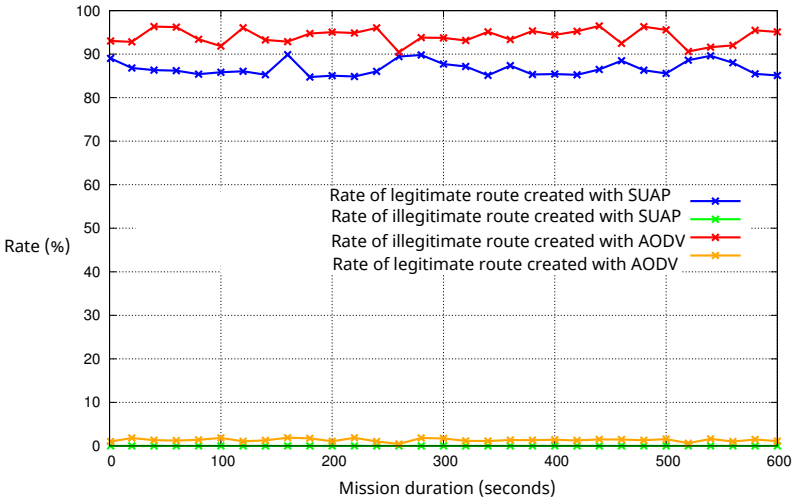

Figure 8 Creation rate for genuine and attack nodes

use of real time traffic, with acceptable route re-establishment and end-to-end delays. The SUAP protocol offers more than satisfactory performance in comparison with the AODV protocol presented in [14]. The values obtained here are sufficient to implement a secure communications architecture for a fleet of drones.

As future works, we have planned to focus on public-key infrastructure that will allow to exchange cryptographic keys among the team of UAVs.

References

[1] Charles Perkins, E Belding-Royer, Samir Das, et al. "RFC 3561-ad hoc on-demand distance vector (AODV) routing". In: *Internet RFCs* (2003), pp. 1–38.

[2] Reshmi Maulik and Nabendu Chaki. "A study on wormhole attacks in MANET". In: *International Journal of Computer Information Systems and Industrial Management Applications* 3.1 (2011), pp. 271–279.

[3] Jean-Aimé Maxa, Gilles Roudiere, and Nicolas Larrieu. "Emulation-based performance evaluation of routing protocols for uaanets". In: *Communication Technologies for Vehicles*. Springer, 2015, pp. 227–240.

[4] Koray Sahingoz. "Networking Models in Flying Ad-Hoc Networks (FANETs): Concepts and Challenges". In: *Journal of Intelligent & Robotic Systems* 74.1-2 (2014), pp. 513–527.

[5] Philippe Jacquet et al. "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.

[6] David B Johnson et al. "The dynamic source routing (DSR) protocol for mobile ad hoc networks". In: *IETF Draft, draft-ietf-manet-dsr-009. txt* (2003).

[7] Atekeh Maghsoudlou, Marc St-Hilaire, and Thomas Kunz. "A survey on geographic routing protocols for mobile ad hoc networks". In: *Carleton University, Systems and Computer Engineering, Technical Report SCE-11-03* (2011).

[8] Jean-Aimé Maxa, Mohamed Slim Ben Mahmoud, and Nicolas Larrieu. "Secure routing protocol design for uav ad hoc networks". In: *2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC)*. IEEE. 2015, 4A5–1.

[9] Jean-Aimé Maxa, Mohamed Slim Ben Mahmoud, and Nicolas Larrieu. "Joint model-driven design and real experiment-based validation for a secure uav ad hoc network routing protocol". In: *2016 Integrated Communications Navigation and Surveillance (ICNS)*. IEEE. 2016, 1E2–1.

[10] Bounpadith Kannhavong et al. "A survey of routing attacks in mobile ad hoc networks". In: *IEEE Wireless communications* 14.5 (2007), pp. 85–91.

[11] Jack Elston et al. "Net-centric communication and control for a heterogeneous unmanned aircraft system". In: *Journal of intelligent and Robotic Systems* 56.1-2 (2009), pp. 199–232.

[12] Matthew Pirretti et al. "The sleep deprivation attack in sensor networks: Analysis and methods of defense". In: *International Journal of Distributed Sensor Networks* 2.3 (2006), pp. 267–287.

[13] Zubair Muhammad Fadlullah, Tarik Taleb, and Marcus Schöller. "Combating against security attacks against mobile ad hoc networks (MANETs)". In: *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET* 173 (2010), pp. 1–13.

[14] Jean-Aimé Maxa, Mohamed Slim Ben Mahmoud, and Nicolas Larrieu. "Extended verification of secure UAANET routing protocol". In: *2016 IEEE/AIAA 35th Digital Avionics Systems Conference (DASC)*. IEEE. 2016, pp. 1–16.

[15] Yih-Chun Hu, Adrian Perrig, and David 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.

[16] René Ndoundam and Juvet Karnel Sadie. "Collision-resistant hash function based on composition of functions". In: *arXiv preprint arXiv:1108.1478* (2011).