# How to improve routing protocol security in a RPAS swarm?

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

# How to improve routing protocol security in a RPAS swarm?

Jean Aime Maxa[1 2], Slim Ben Mahmoud Mohamed[1], Nicolas Larrieu[1]
[1]ENAC, TELECOM/Resco, F-31055 Toulouse, France
[2]Delair Tech, Toulouse, France

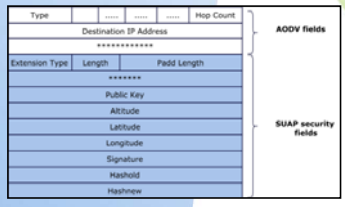
## SUANET project: Secure UAV Ad hoc NETwork

The goal of this research is to define and design a secure communication network for UAV swarm. Our objective is to design a new secure routing protocol for UAANET in order to guarantee message authentication between UAVs. This solution needs to minimize signaling overhead in order to preserve network resources for effective data exchanges between UAVs.
This proposed routing protocol called SUAP should be certified. Consequently, we contribute to its validation through the use of MDD (Model Driven Development) approach using a set of formal verification tools (i.e. Mathworks Matlab Simulink and Stateflow software) .

## SUAP routing

The SUAP (Secure UAV Ad hoc Routing Protocol) algorithm consists of **2 steps** used respectively during route maintenance and route discovery:

1. **Enhanced Beacon messages:** we use a mechanism that mathematically analyzes the correlation between the hop count and the distance traveled by *Hello* packets and *Error* packets.




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

- **T**: total distance of the legitimate route
- **Dmax**: maximum distance of one hop

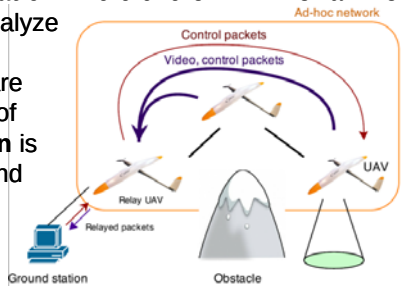
2. **Secure route discovery:**

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.

| 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]<br>CurrentNode is the address of node sending the request packet. It can be its public key or its IP Address.<br>The Nextnode is the next node public key or IP Address.<br>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 |

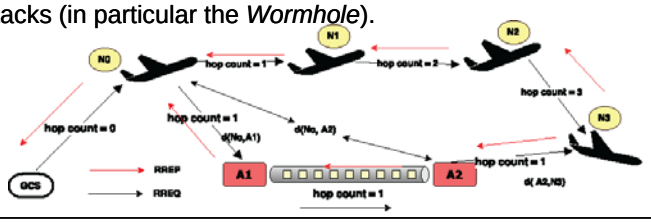
## UAANET use case

The main use case scenario identified in this project is a **search and rescue application** where one UAANET swarm is used to cartography and analyze a physical area.
**Video surveillance** flows are exchanged between UAVs of the swarm and **information** is **collected** through the ground control station.

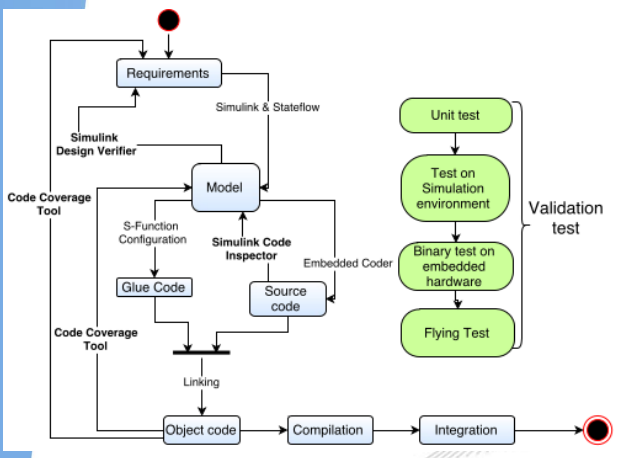



## UAANET model of attack

One of the major issues with UAV communication security is to face the *Wormhole* attack where two attackers **perform a tunnel** in an existing UAANET configuration. These attackers take place in the network as legitimate nodes and exchange information by **stealing resources and connections** of real legitimate nodes. The purpose of SUAP algorithm is to **secure the routing protocol** of the UAANET against different network attacks (in particular the *Wormhole*).




## Model Driven Development approach for UAANET routing protocol




**Experimental results:** we compared our SUAP protocol to AODV routing protocol (one of the routing protocol reference in MANET environments). Our experiments perform that SUAP is able to increase drastically both the quality of transmission and security of communication.

| Parameter | AODV | SUAP |
|---|---|---|
| Average loss duration | 7.34 s | 2.04 s |
| Packet delivery ratio | 40.5 % | 95 % |
| Average end to end delay | 5.11 ms | 35.11 ms |
| Connectivity percentage | 9.8 % | 90 % |

**Conclusion and future works**
The SUANET project enables a new secure UAANET routing **protocol providing message authentication, detection and prevention** against *Wormhole attacks*. Some additional benefits include:

- A safe routing protocol designed with MDD approach and verified through a set of formal verification tools;
- Evaluation through UAANET emulation and real world experiments;

Our future works consist to :

- **Define a key management mechanism** to enable deployment of multiple keys which will be used to implement authentication, confidentiality and integrity services.
- **Perform an extended real world outdoor experiments** with several UAVs and GCS.

**Acknowledgements**
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 (Association Nationale de la Recherche et de la Technologie).