Model driven development of a secure routing protocol for UAANET

Nicolas LARRIEU, Jean Aimé MAXA, Antoine VARET

SSIV workshop – Toulouse – June 28, 2016

French Civil Aviation University (**ENAC**)
TELECOM Laboratory

Outline

1. **Scientific context**: certification of complex systems
2. **State of the art** of model driven development (MDD) approaches
3. **SUANET project**: **S**ecure **U**AV **A**d hoc **NET**work
4. **MDD case study**: secure communication network design for Unmanned Aerial Systems

Outline

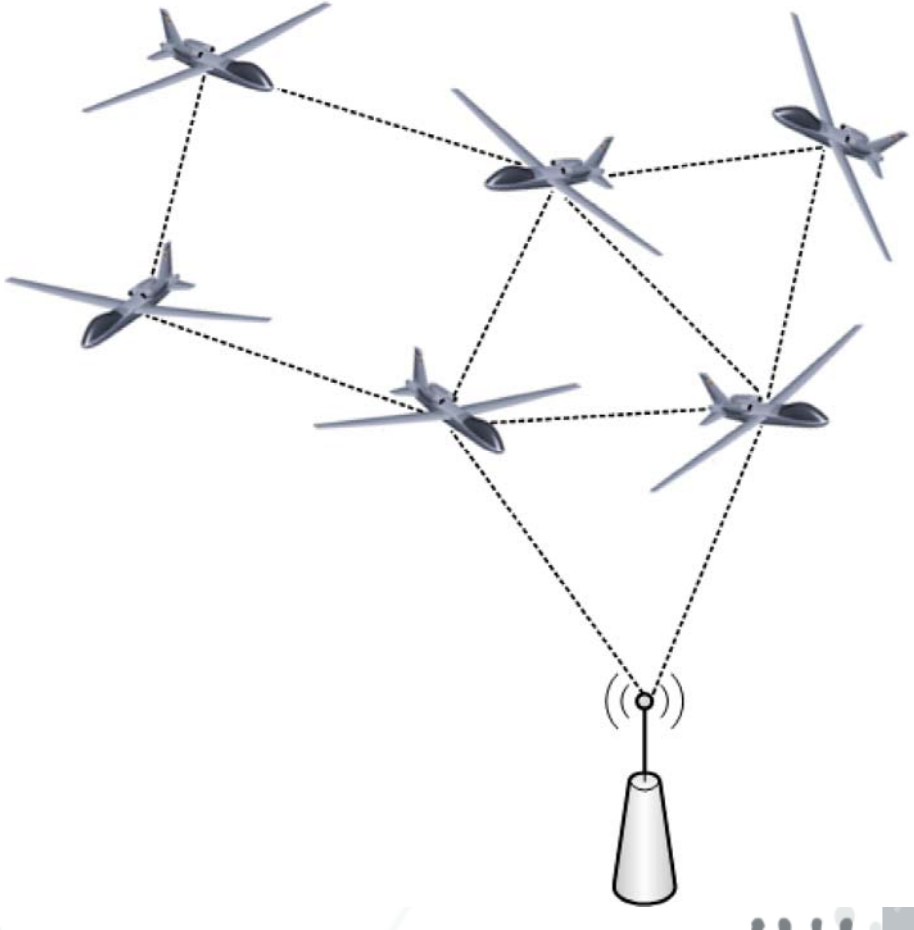
1. **Scientific context: certification of complex systems**
2. State of the art of model driven development (MDD) approaches
3. SUANET project: Secure UAV Ad hoc NETwork
4. MDD case study: secure communication network design for Unmanned Aerial Systems

UAV and civil air space

- UAV DT-18
- Flight
  - **B**eyond **L**ine **O**f **S**ight (BLOS)
  - Full autonomy
- Integration in the civil air space

Scope of the scientific contribution (1)

- **Communication network** between several UAVs
  - ***UA**v **A**d hoc communication **NET**work (UAANET) also known as FANET (**F**lying **A**d Hoc **NET**work) in the literature*
- **Security** of the UAANET
- **Validation** of communication and security functions for UAANET
  - *MDD based certification process*



Scope of the scientific contribution (2)

UAANET Challenges

Network routing

- Data must be exchanged in timely manner
- Minimum signaling overhead
- Optimize route retrieval time

Certification requirements

- To ensure software quality (Modularity and Reusability) and compliance
- To generate code with a qualified auto-generator and formal verification tools.

Security requirements

- C2(Control and command) and Data traffics are vulnerable to attacks if not protected
- There is no secure routing protocol proposed for UAANET

Outline

1. Scientific context: certification of complex systems
2. **State of the art of model driven development (MDD) approaches**
3. SUANET project: Secure UAV Ad hoc NETwork
4. MDD case study: secure communication network design for Unmanned Aerial Systems

Overview of model driven development approaches

- UML: Unified Modelling Language
  - ☺ Widely used in traditional industry
  - ☹ Does not fit specific aeronautical certification procedures

- Aeronautical software design
  - **DO 178 C:** Software Considerations in Airborne Systems and Equipment Certification
  - **DO 331:** Model-Based Development and Verification

- Taking advantage of aeronautical model driven approaches
  - **Accelerate** certification procedures
    - **Validation:** theorem proving
    - **Verification:** model checking

Outline

1. Scientific context: certification of complex systems
2. State of the art of model driven development (MDD) approaches
3. **SUANET project: Secure UAV Ad hoc NETwork**
4. MDD case study: secure communication network design for Unmanned Aerial Systems

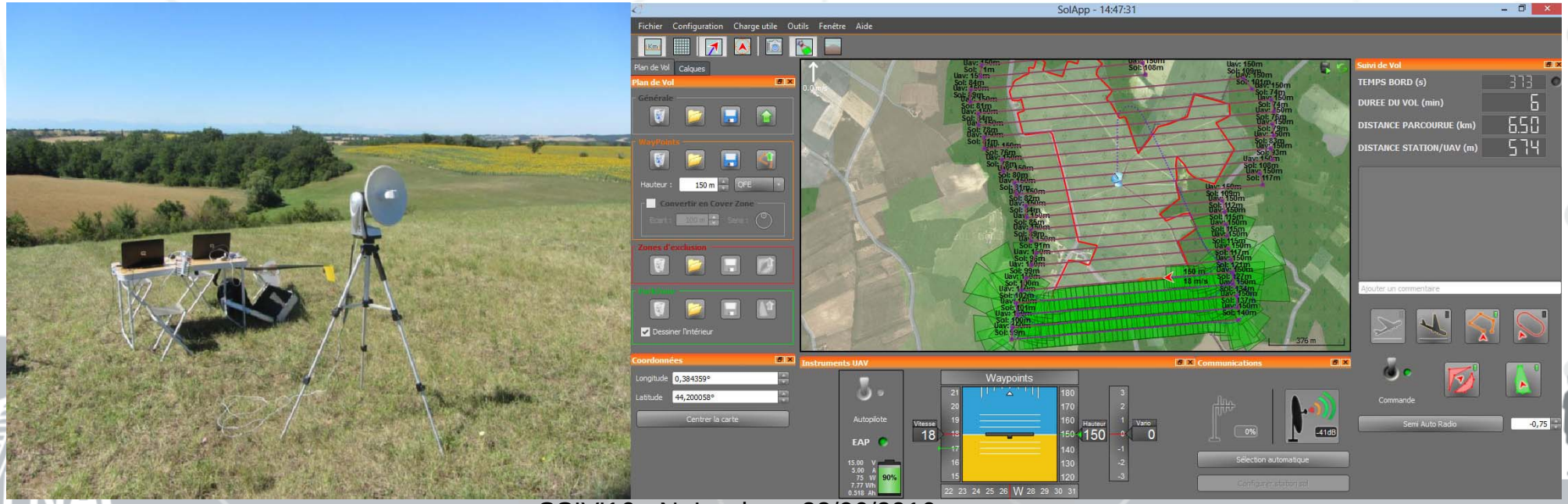
SUANET project description (1)

- Actors:
  - Delair Tech company
  - French Civil Aviation University (ENAC)
- 36 months duration (2014-2017)
- UAV DT-18

Characteristic	Value
Range	100km
Cruise speed	50km/h
Wind	up to 45km/h
Photo	5 to 10cm resolution
Video	20cm resolution
Infra-red video	30cm resolution
Field deployment	< 10 minutes
Price	15 k€

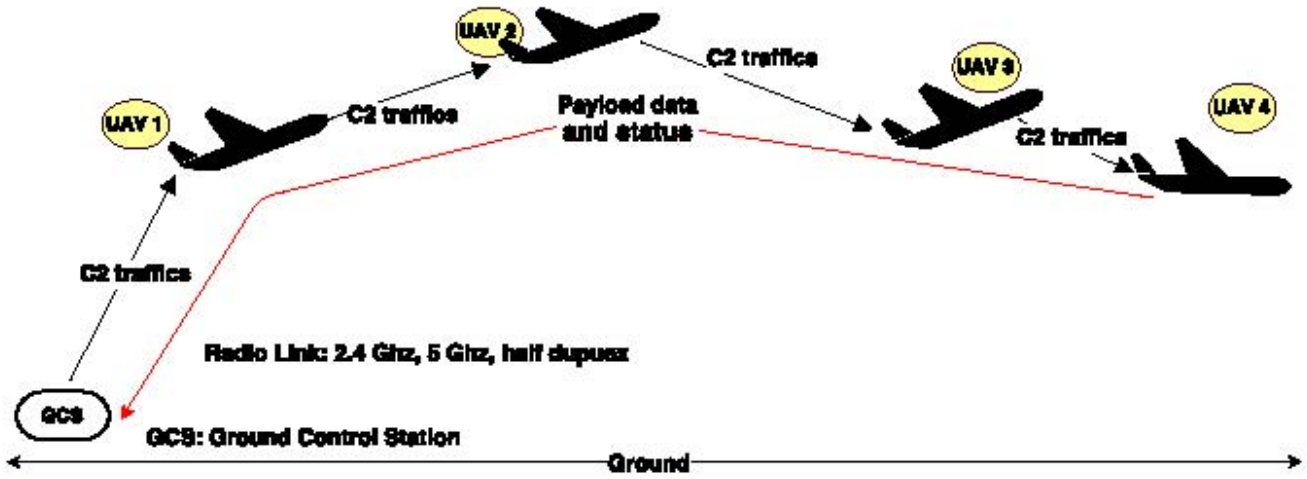
SUANET project description (2)

- Fields of application
  - Video surveillance
  - Cartography
  - Search and rescue network



SUANET: video surveillance use case (1)

UAANET : UAVs and GCS connected through an ad-hoc network



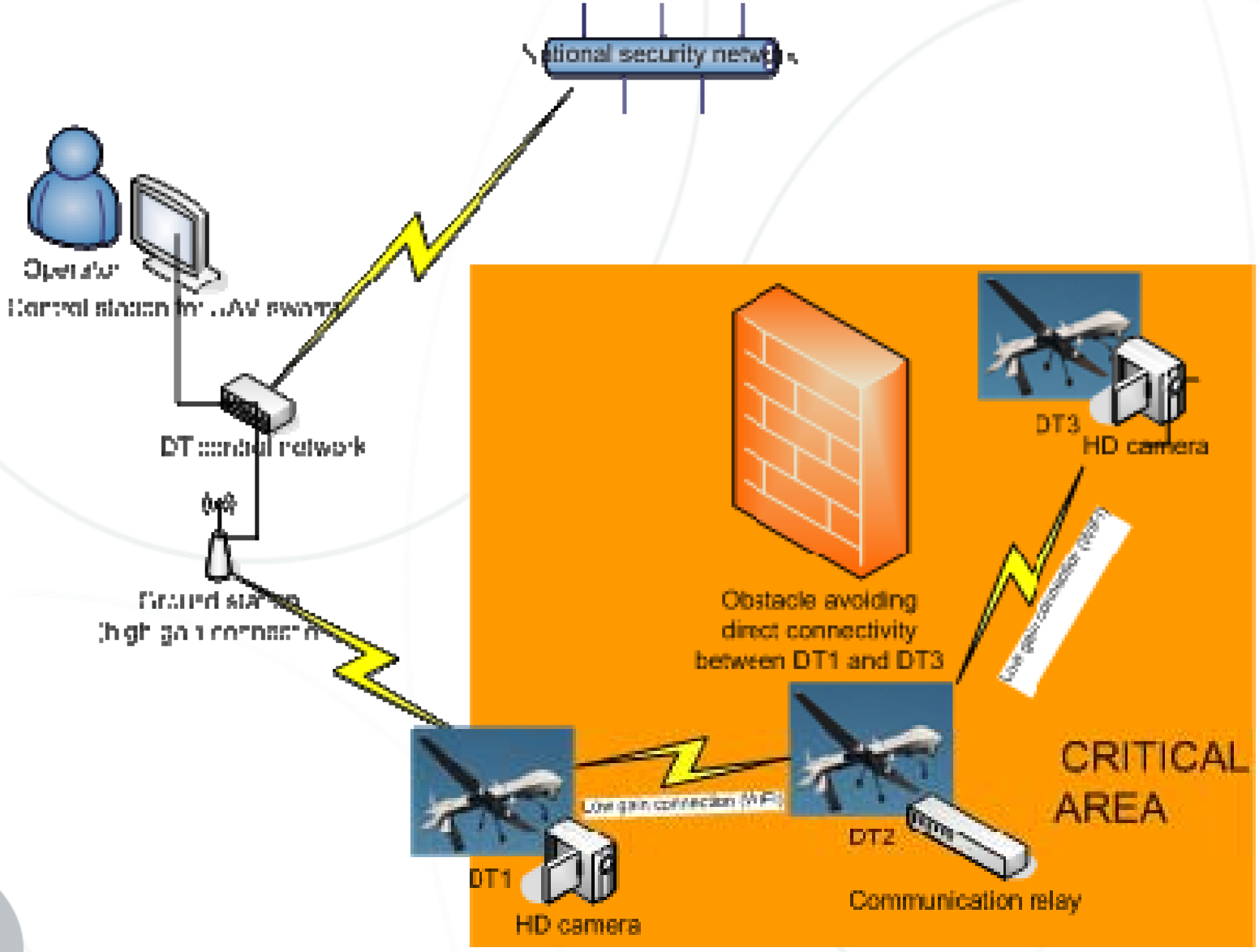
UAANET Characteristics

- Low density node, 3D mobility, dynamic topology, no authentication requirements

SUANET Objectives

- Safe (validation) and Secure routing protocol (authentication and integrity) : SUAP (Secure UAV routing Protocol)
- Efficient and Secure Key management

SUANET: video surveillance use case (2)



Outline

1. Scientific context: certification of complex systems
2. State of the art of model driven development (MDD) approaches
3. SUANET project: Secure UAV Ad hoc NETwork
4. **MDD case study: secure communication network design for Unmanned Aerial Systems**
   1. **MDD methodology**
   2. **SUAP protocol design**
   3. **SUAP test and validation**

Outline

1. Scientific context: certification of complex systems
2. State of the art of model driven development (MDD) approaches
3. SUANET project: Secure UAV Ad hoc NETwork
4. **MDD case study: secure communication network design for Unmanned Aerial Systems**
   1. **MDD methodology**
   2. SUAP protocol design
   3. SUAP test and validation

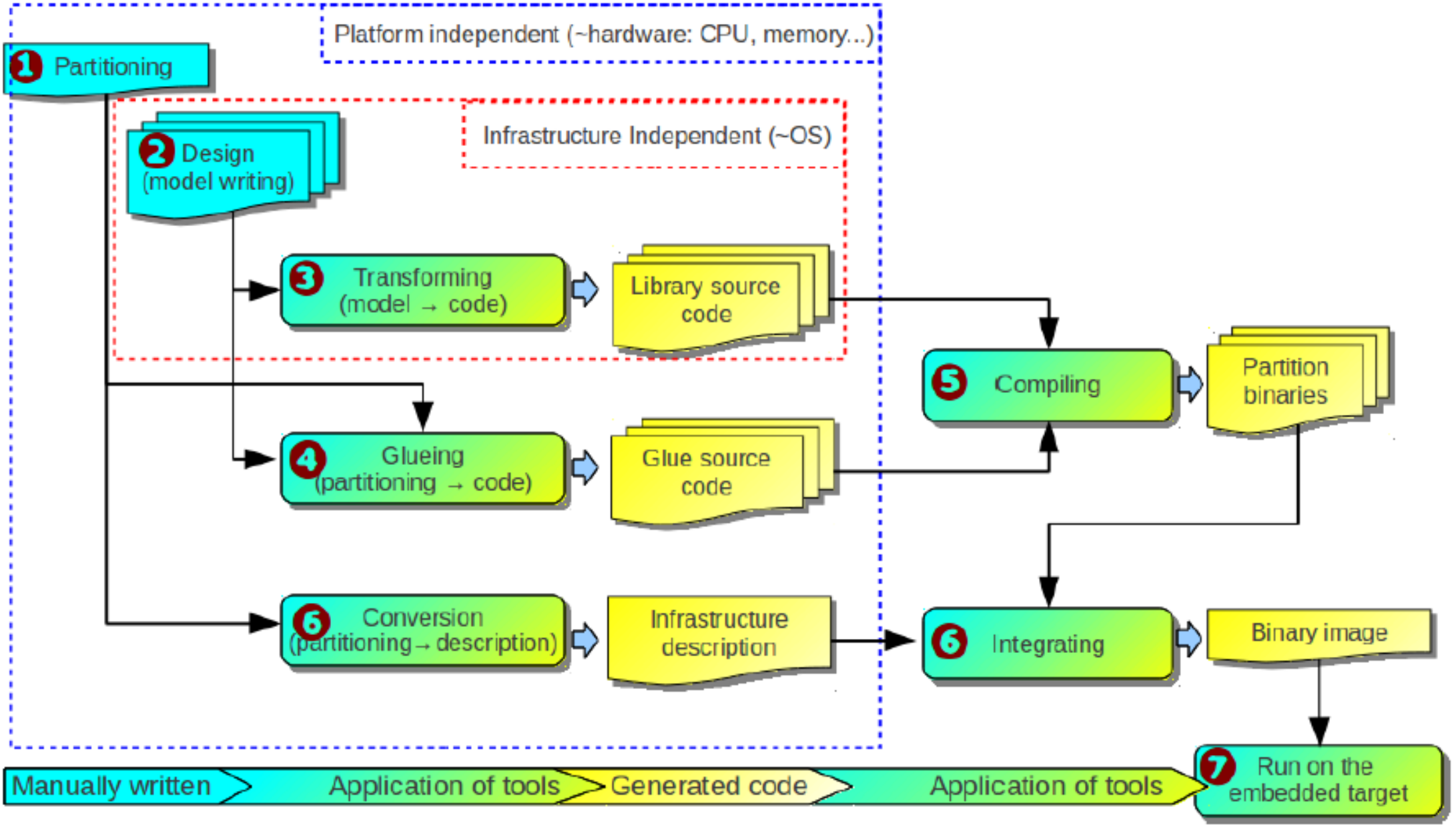
MDD principles

1. **Partitioning step:** this is the architecture design where each (or a set of) feature(s) of the global system is (are) grouped into the same functional partition

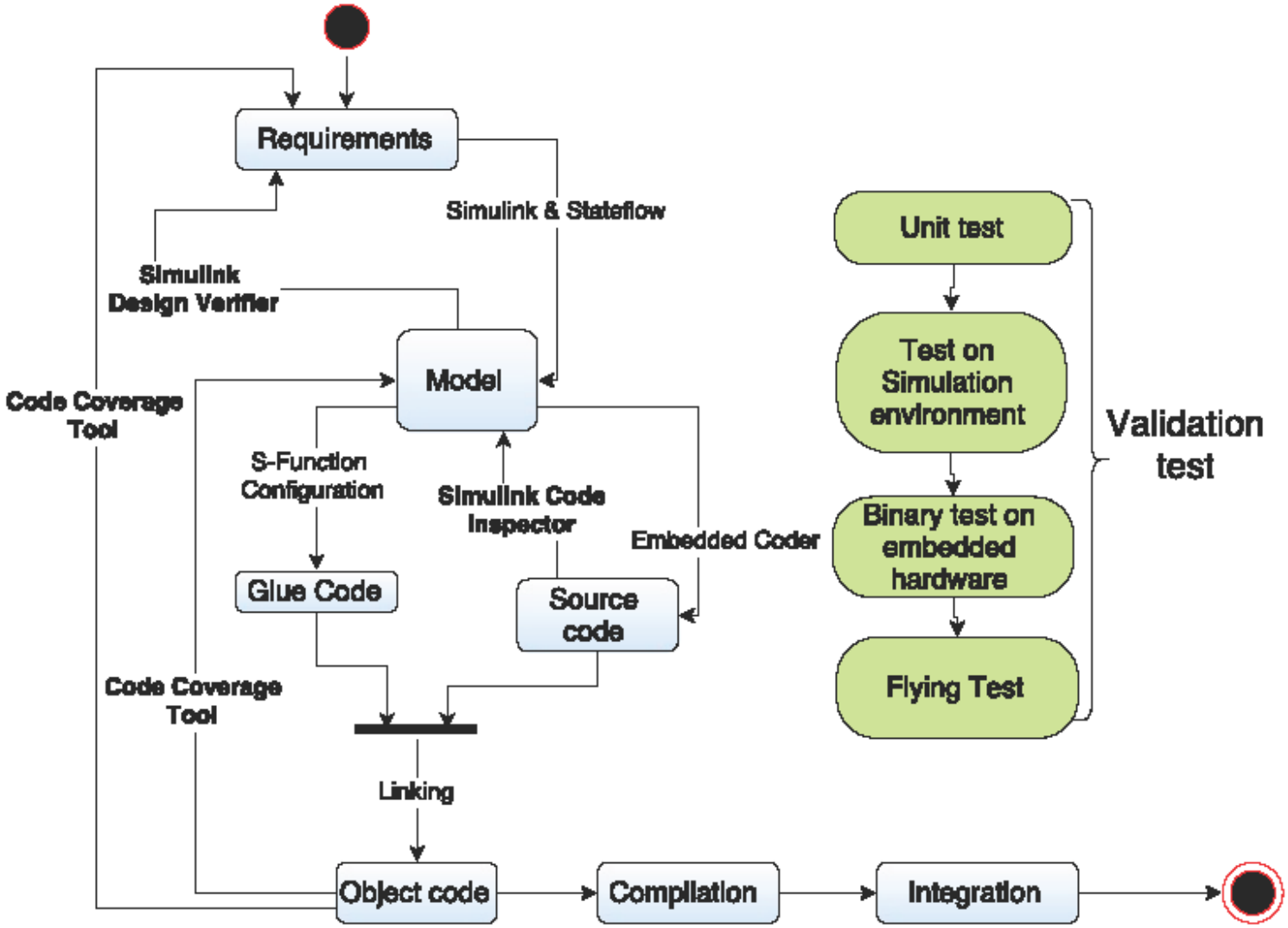
2. **Design step:** for each functional partition we produce one high level model which represents the behaviour of the different agents and processes acting together

3. **Transformation step:** based on an auto-generator of software code we are able to transform the high level model into software code in C language

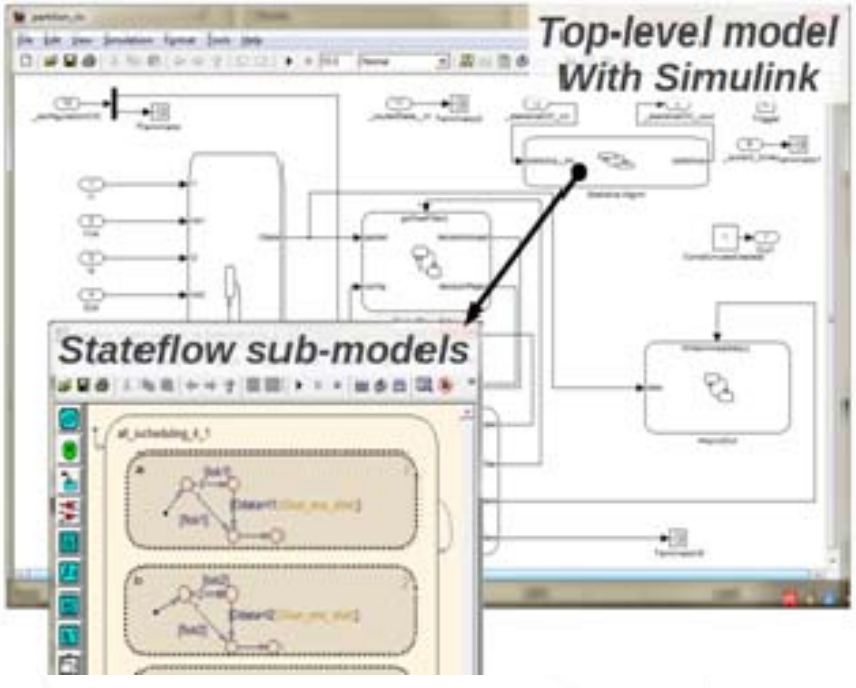
MDD methodology (1)

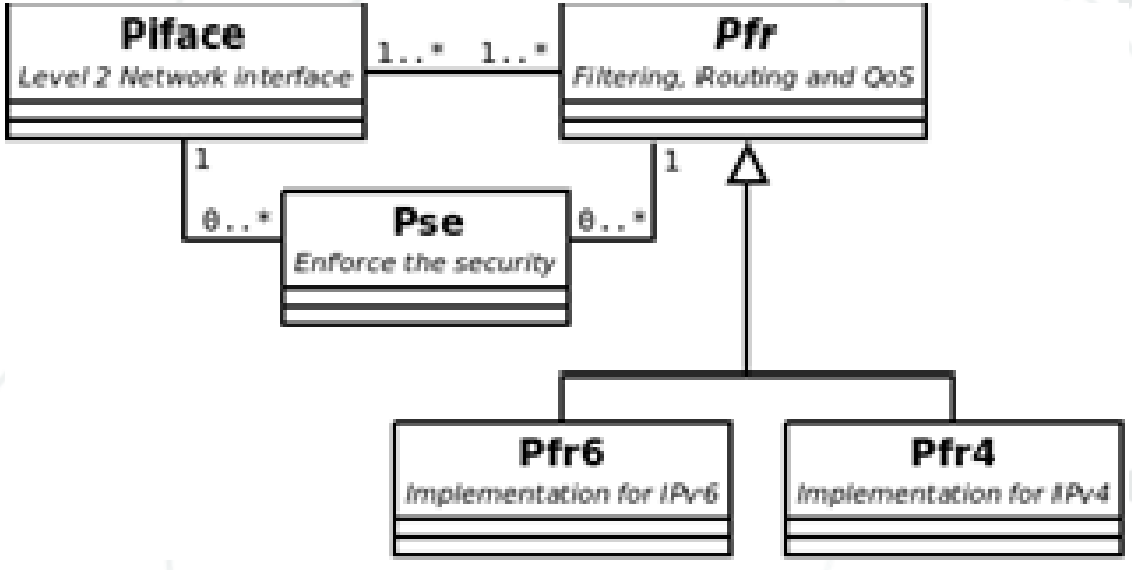


MDD methodology (2)



MDD design





- Tools :
  - Matlab **Simulink** and **Stateflow**
  - **Model driven** code **autogeneration** (C language)

MDD advantages

- **Modularity**
  - **Oriented-Object Design**: class & object definition
  - **Segregated design** based on the different system features: routing, security, signal processing…
- **Reusability**
  - **Certification** documents and procedures can be **inherited** from previous research projects
- **Verification and validation** at an early stage of development
  - **Model** based **auto validation** (Matlab **model checking** features)

Outline

1. Scientific context: certification of complex systems
2. State of the art of model driven development (MDD) approaches
3. SUANET project: Secure UAV Ad hoc NETwork
4. **MDD case study: secure communication network design for Unmanned Aerial Systems**
    1. MDD methodology
    2. **SUAP protocol design**
    3. SUAP test and validation

Security consideration

Network and security model

- Homogeneous nodes (UAVs and GCS)
- Sufficient energy power and network resources
- Each UAV has omnidirectional antennas
- Nodes are clocked synchronized
- There is an efficient and reliable key management within the network to manage keys
- Node's current position is included in each packet sent

Security services provided by SUAP

Message Authentication

- Digital signatures to authenticate non-mutable fields (Originator IP Address)
- Algorithm RSA

Data integrity

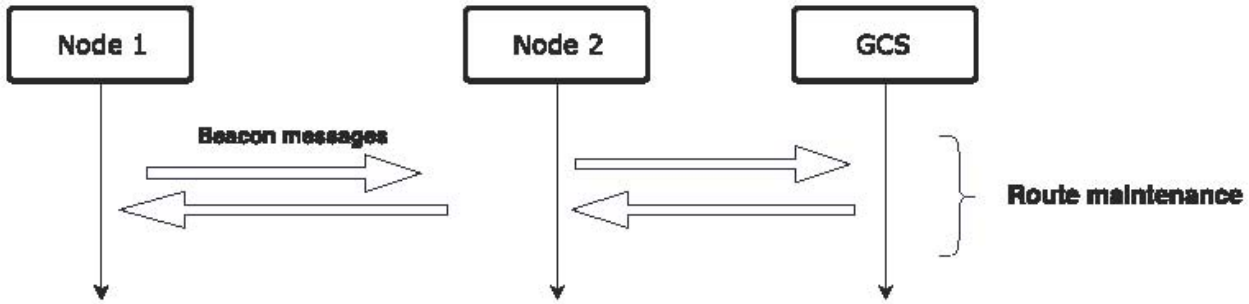
- Hash chains to secure mutable fields (e.g., hop count).
- Algorithm SHA-1

Wormhole attack solution

- Geographical leashes to restrict packet maximum transmission distance
- Location knowledge (ok)
- Compute relative distance between nodes

Beacon messages exchanges

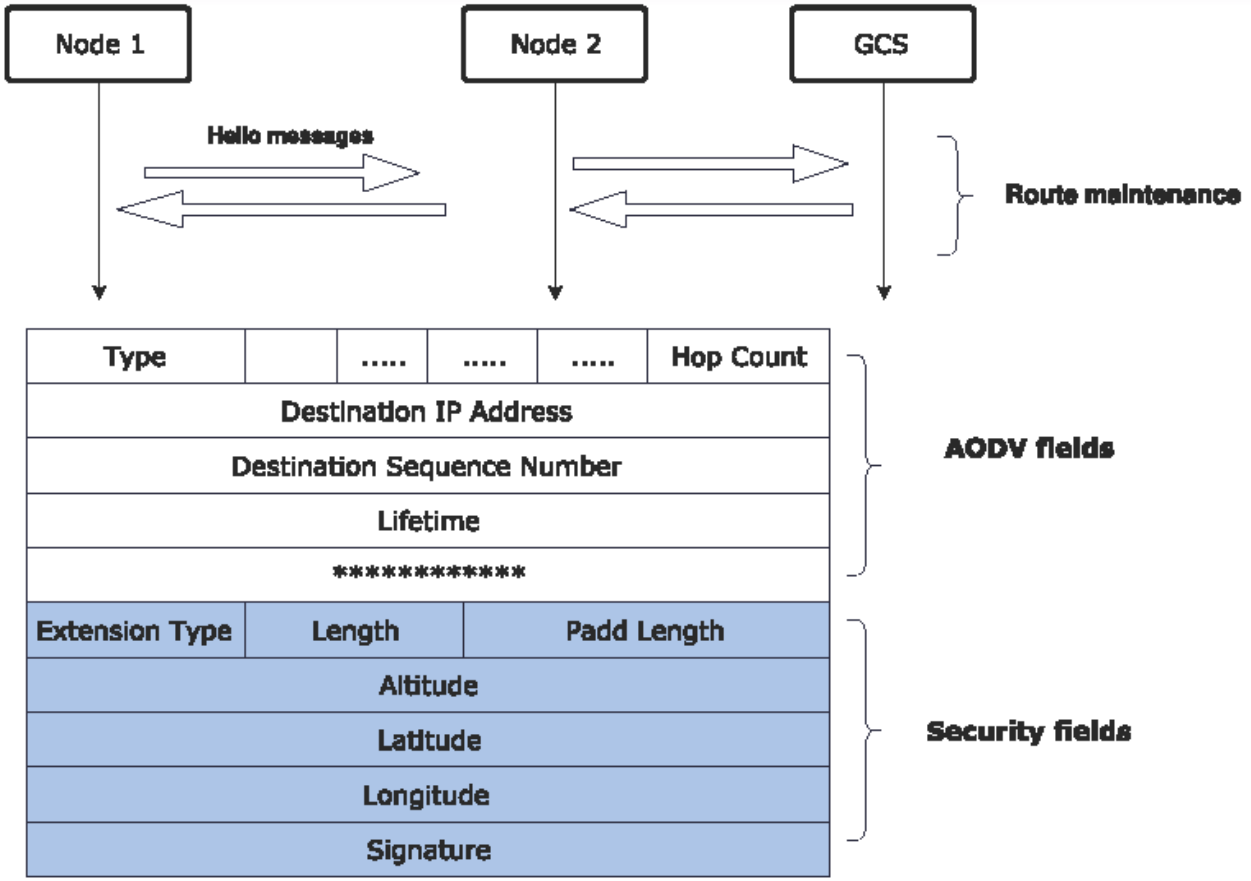
Beacon messages are exchanged at the initializing phase



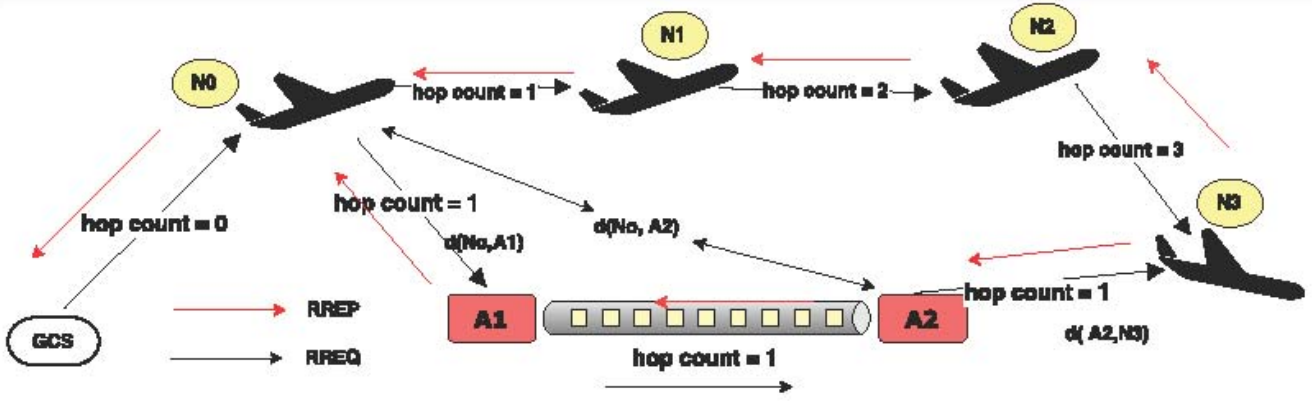
Procedures

- Node builds beacon messages by including its current position
- Recipient node compute the relative distance traveled by the packet
- Recipient node compute the associated hop count and compare it to the current hop count value

Beacon messages format



Beacon messages exchanges



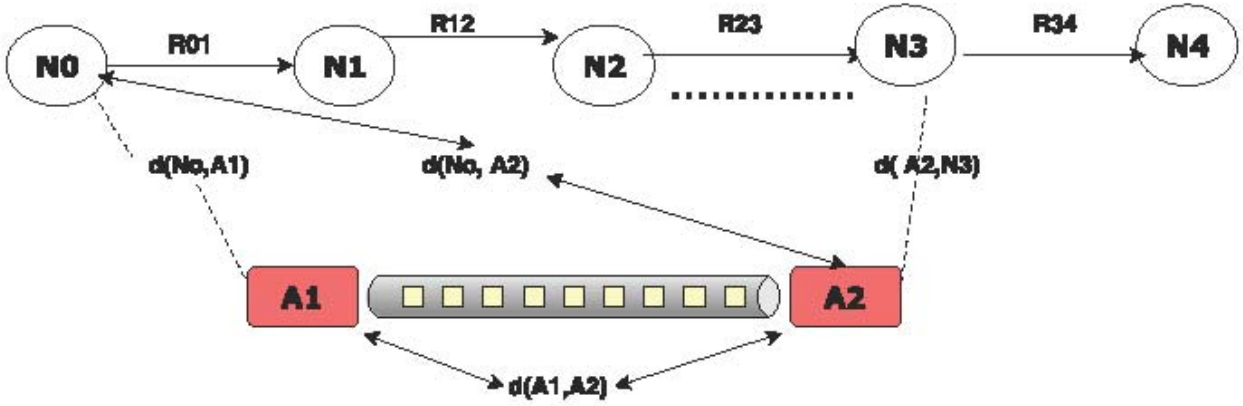
$$\frac{T}{Dmax} - 1 \leq hc < \frac{T}{Dmax} + 1 \quad (1)$$

with

$$T = \sum_{i=0,j=0}^{n} R_{i,j}$$

- N0 send beacon packets to N1
- N1 computes the relative distance and induce the hop count value
- N1 compare the hop count value to the one included in the packet

Hash chain based mechanism to prevent wormhole



GCS node

- Compute $Oldhash = H(seed)$
- Compute $Hashnew = H(GCS, N0, Oldhash)$
- GCS $\Rightarrow$ $N0$: $[64, H, sign, Hashnew, Oldhash]$

N0 node

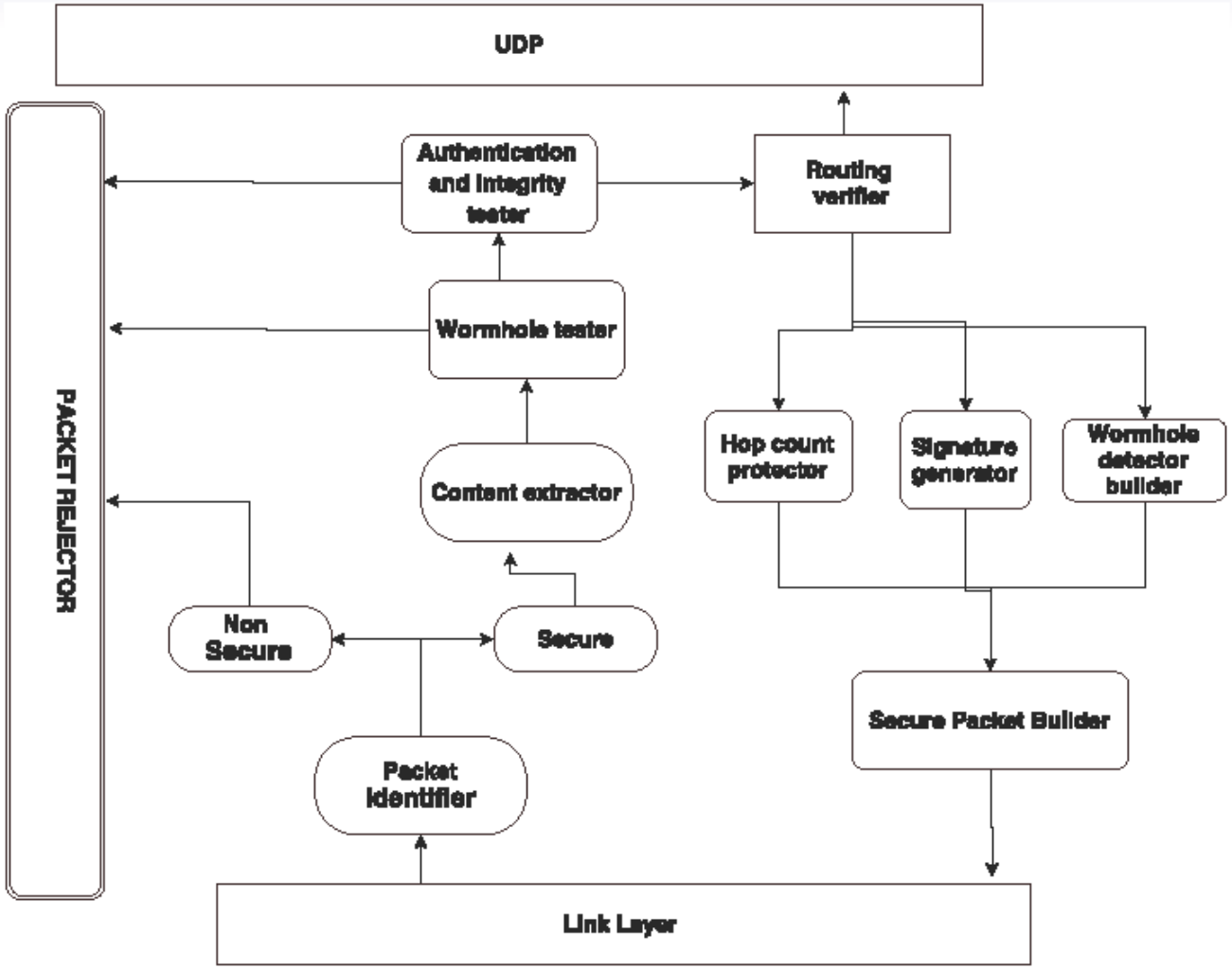
- Integrity verification by computing $Hashverifier = H[GCS, NO, Oldhash]$
- If Hashverifier = Hashnew $\Rightarrow$ wormhole free

Hash chain based mechanism to prevent wormhole

Procedures

- Thanks to geographical leashes, one hop neighbors are authenticated
- Each node sends in unicast route discovery packets by including
  1. Next node identity (ip address or public key)
  2. Current node identity
  3. Compute hashold (previous received hash initialized with a seed value)
  4. Compute a new hash called Hashnew : H [previous-node-identity, myidentity, hashold]
- The hop count value is induced by the number of times the hash is performed

Secure block design architecture



Outline

1. Scientific context: certification of complex systems
2. State of the art of model driven development (MDD) approaches
3. SUANET project: Secure UAV Ad hoc NETwork
4. **MDD case study: secure communication network design for Unmanned Aerial Systems**
    1. MDD methodology
    2. SUAP protocol design
    3. **SUAP test and validation**

Routing protocol design

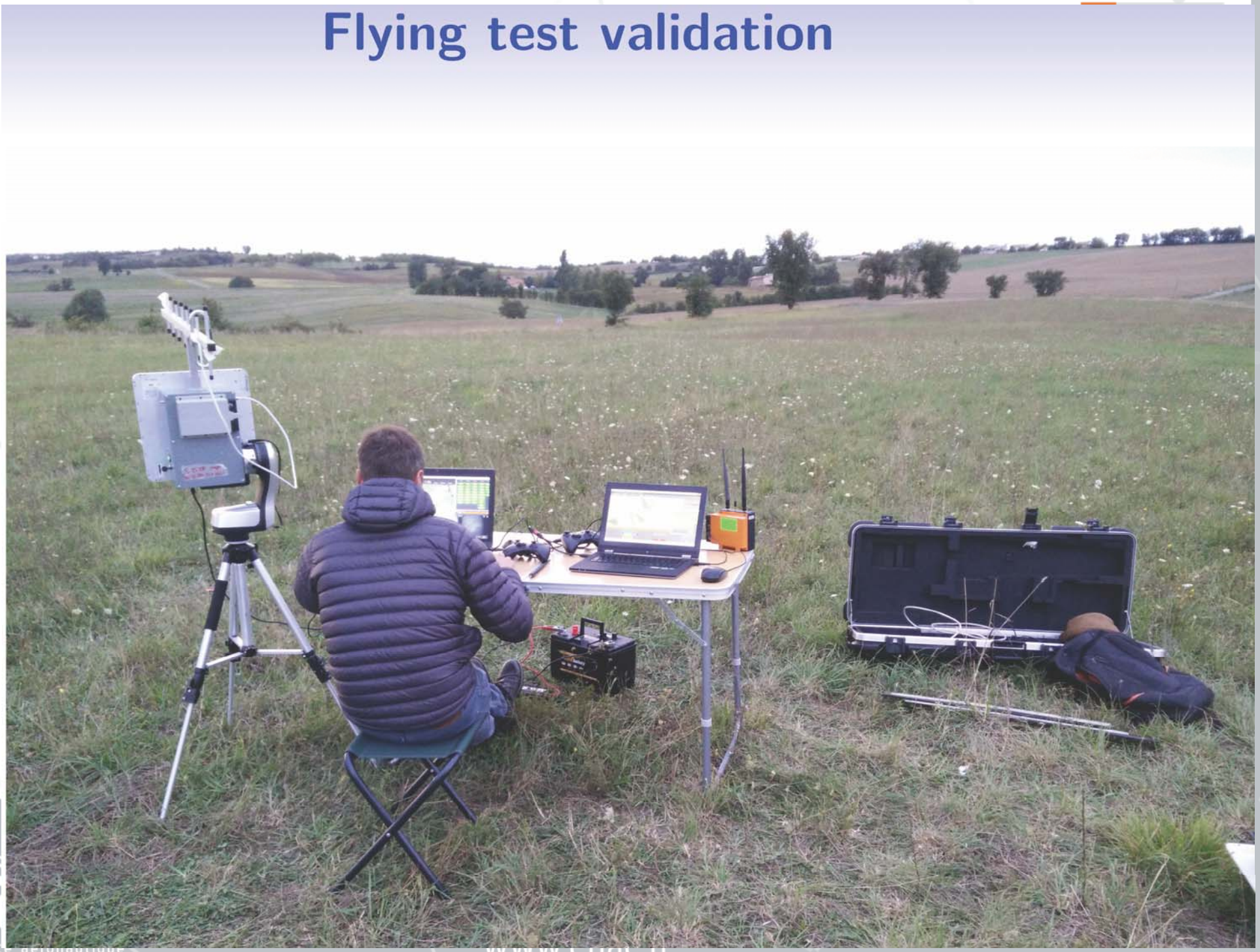
Secure routing protocol design steps

- Performance evaluation of MANET routing protocols under UAANET scenario
  - Performed with a hybrid tool (simulation and emulation)
  - AODV Routing protocol selected
- Security routing protocol implementation
  - Through Model Driven Development

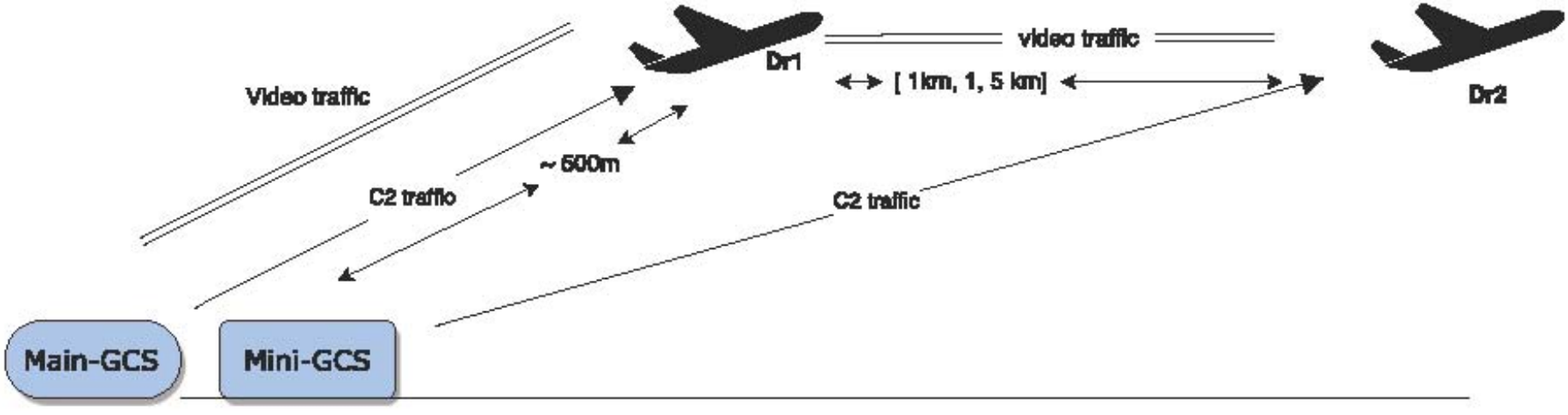
	AODV	DSR	OLSR
Delay	5.32 ms	10.15 ms	5.91 ms
Overhead	501 kB	759.99kB	438kB
Connectivity	90.65 %	58.2 %	24.1 %

TABLE : Performance results

Flying test validation



Testbed Architecture



Main GCS

DT-18

Mini GCS

Testbed environment

Type of traffic	Source —- Destination	Size	Rate
Heartbeat or Tick	GCS —- Dr1 GCS —- Dr2	64 Bytes	1 packet/s
Geographical Reference (Georef)	Dr1 —— GCS Dr2 —— GCS	80 Bytes	3 packets/s
C2	GCS—- Dr1 GCS —- Dr2	80 Bytes	1 packet/s
Video	Dr2 ——Dr1—— GCS	1400 Bytes	25 UDP packets/second width=720,height=576
Network	Exchanged between Dr1, Dr2 and the GCS	Request : 66 bytes Response : 62 bytes Hello : 62 bytes Error : 54 bytes	1 packet/s for the hello Request and Response and Error packets are exchanged during disconnection (route loss)

Experimental results

Overhead

It represents the amount of control packet sizes added to data packets.

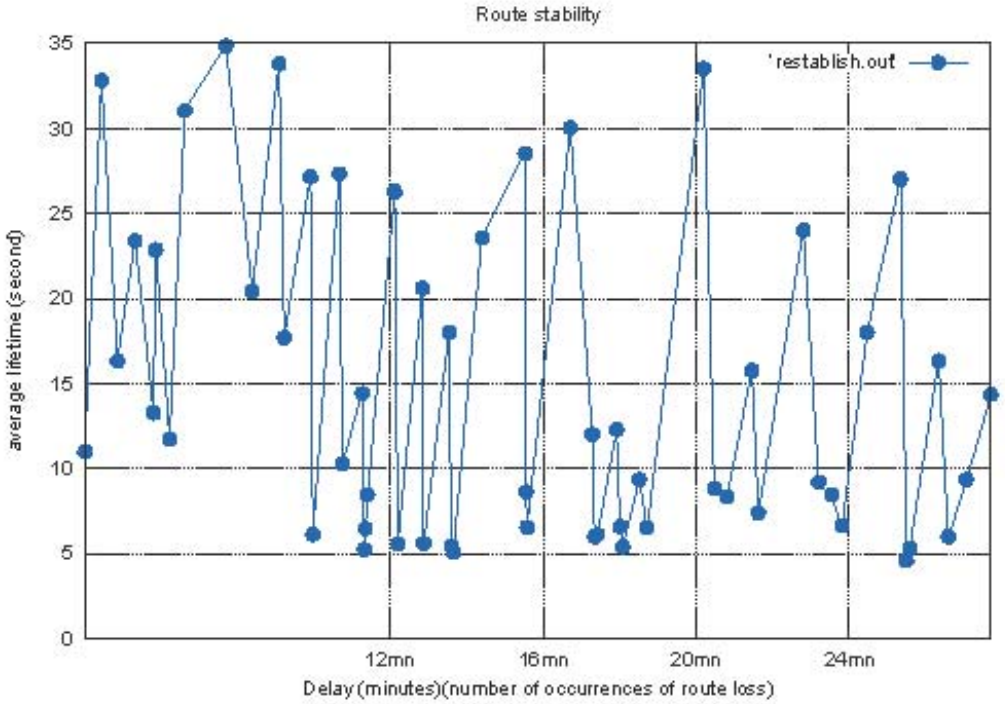
Overhead	Protocole
Control packets	352 ko
Traffic % (bytes)	2.15 %

Experimental results

Route (Link) stability

It evaluates the delay during which the connectivity is uninterrupted.

- Average route lifetime : 14.328955s

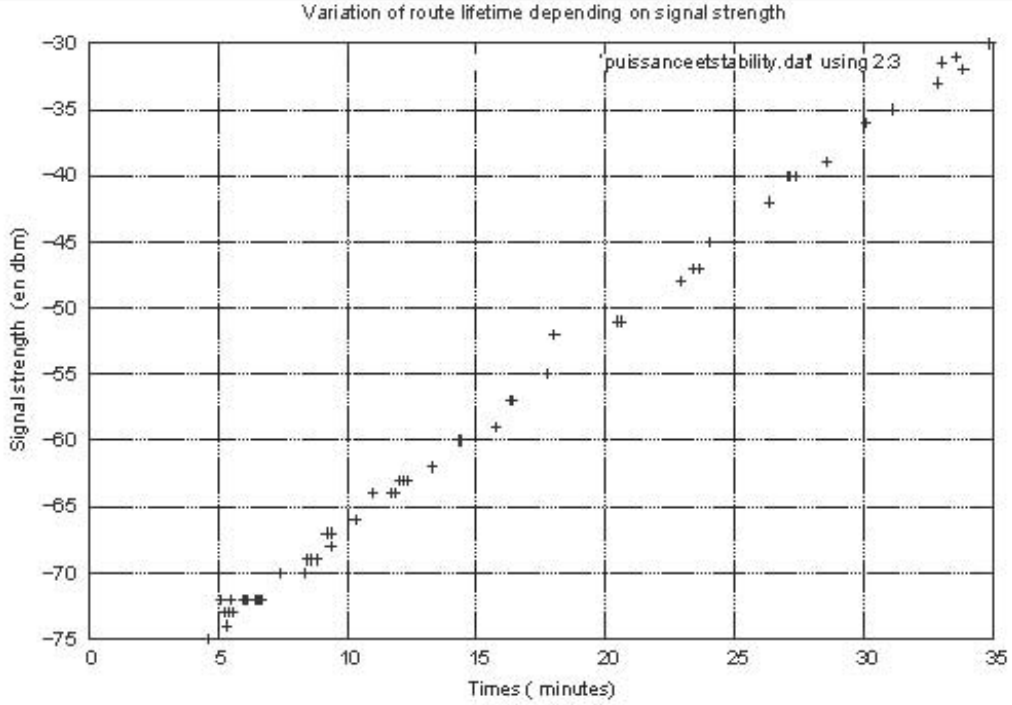


Variation of route lifetime depending on signal strength

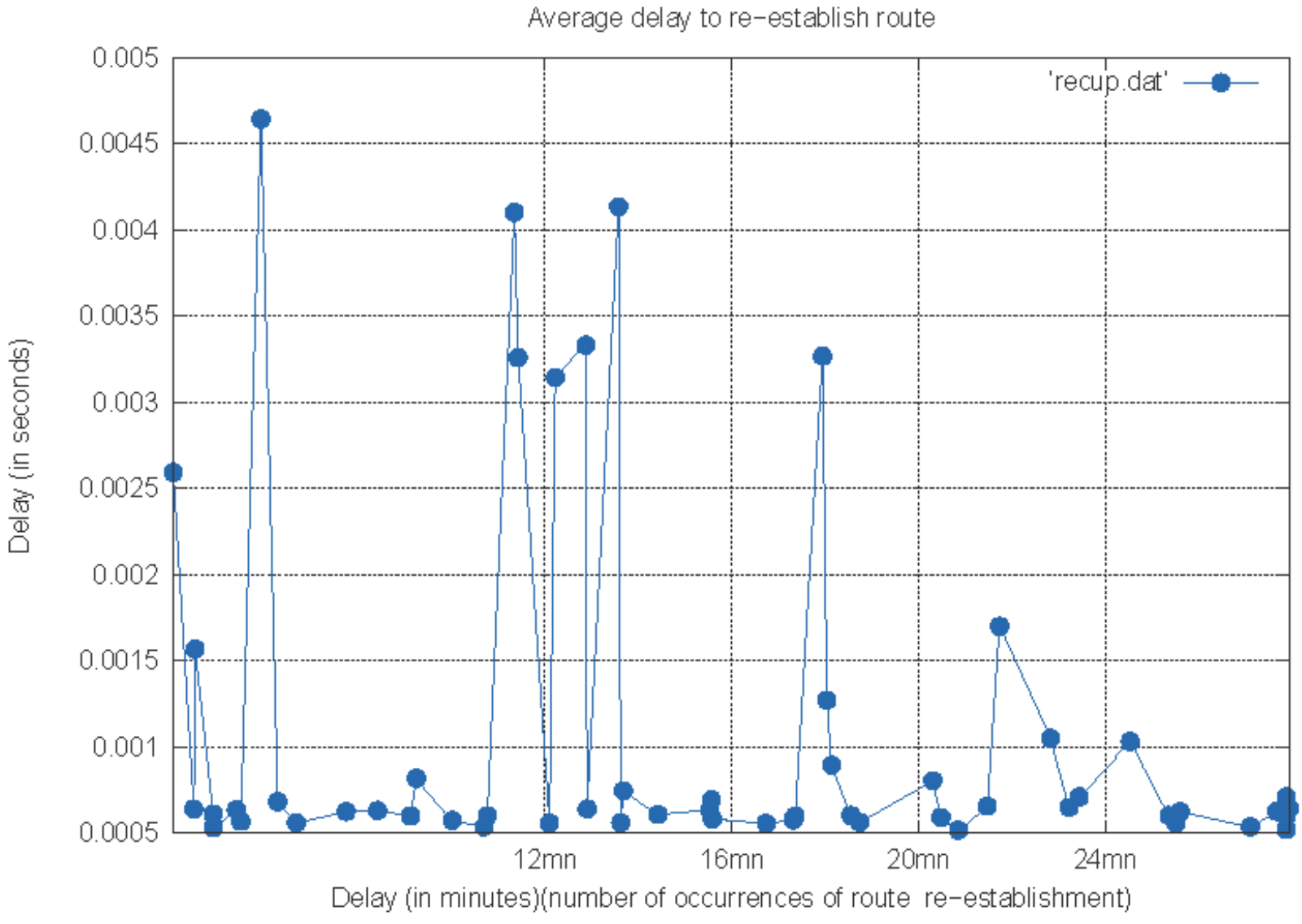
Route (Link) instability causes

It helps understand the route stability fluctuation

- Propagation loss and signal attenuation (caused by nodes mobility) cause momentary link breakages



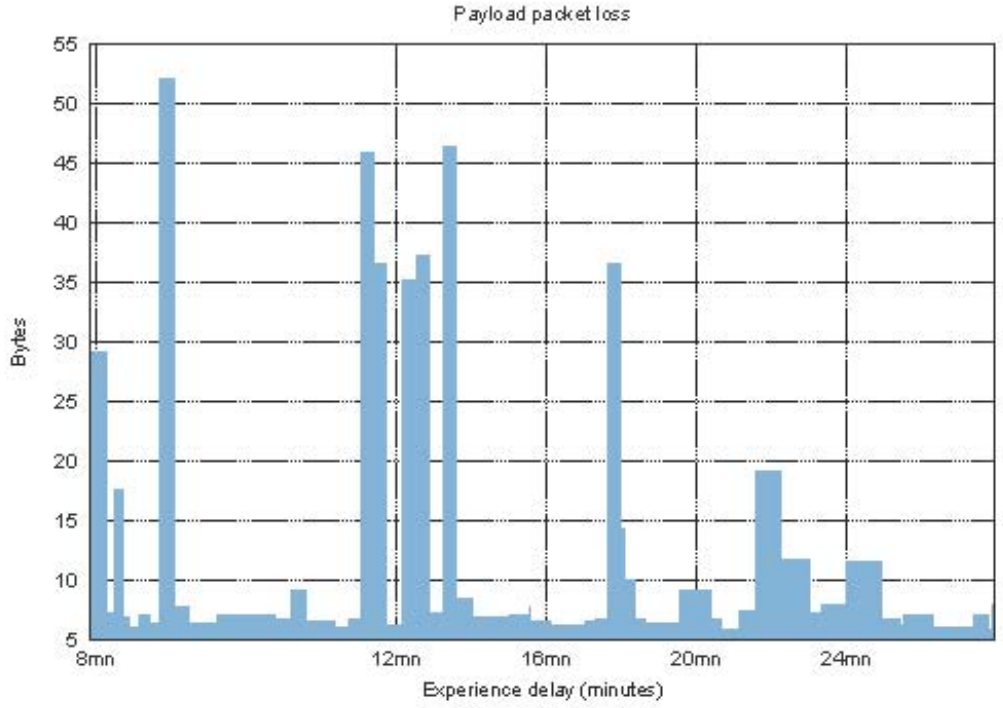
Delay to re-establish route in case of route loss



Payload packet loss

We measure :

- how many routing control packets are lost during the mission
- the size of payload packets being lost by the time the route is repaired
- unstable states : 3.8 % (1.2 minutes)
- average payload packet loss : 52 Bytes (3.7 %)



Outline

1. **Scientific context**: certification of complex systems
2. **State of the art** of model driven development (MDD) approaches
3. **SUANET project**: Secure UAV Ad hoc NETwork
4. **MDD case study**: secure communication network design for Unmanned Aerial Systems

Conclusion (general)

- **Model driven development** approaches
  - Inherited from airspace and aeronautical systems
  - Reused in UAS design

- **Demonstration** of how a model driven design can **improve** UAS system **robustness** and **facilitate** the validation (both **simulation and real flight tests**)

- **Case study** (SUANET research project)
  - Main advantages for UAS environments: modularity and reusability

Conclusion (SUAP)

- Development of software based routing protocol for UAAANET
  - Designed with model driven development and validated with formal internal verification tools
  - Models for AODV and SUAP routing protocol
- Secure routing protocol ensures
  - data authentication and integrity
  - Defense against wormhole attacks
- Real world experiment validation
  - Routing validated
  - Routing protocol fits well to UAANET unexpected and dynamic topology
  - Route is unstable but the recovery delay is small

Future work

- Performance improvements (stability)
  - Optimization during different steps of the process
  - Data (c2 and payload traffics) confidentiality
- Formal verification of security services provided by SUAP using AVISPA
- More flying validation stages :
  - Different scenario including more nodes and different mobility
- Key management implementation (ongoing ...)

Questions?

Contacts:

Nicolas LARRIEU (nicolas.larrieu@enac.fr)

Jean Aimé MAXA (maxa@recherche.enac.fr)

ENAC / Telecom Laboratory