Contents

Preface ix

Introduction and Approach xi

Chapter 1. State of the Art of Model-driven Development (MDD) as Applied to Aeronautical Systems 1

1.1. Principle of MDD 1
1.2. Use in avionics 2
1.2.1. System virtualization: Integrated Modular Avionics 3
1.2.2. MILS: divide and conquer to ensure security 3
1.2.3. Combined treatment of safety and security considerations 6
1.2.4. Certification of an avionics system 7
1.3. The case of drones (UAS - Unmanned Aerial Systems) 9
1.3.1. The need for a new rapid prototyping methodology for UAS design 9
1.3.2. Safety standards 11
1.3.3. Software development lifecycle 12

Chapter 2. Original Rapid Prototyping Method for Embedded Systems for UAVs 15

2.1. Using models to auto-generate a system 15
2.1.1. Presentation of different steps 15

2.2. Formal verification of models 18
2.2.1. Model analysis 19
2.3. Advantages of MDD (Model-driven Development) methodologies 21
2.4. MDD contributions to UAS certification 22
2.5. Choice of tools for applying MDD methodology 26
2.6. AVISPA: a formal verification tool for security protocols 32
2.7. The need for verification 33
2.7.1. Why use AVISPA? 34
2.8. Additional tools: simulation and experimentation 36
2.8.1. Testing and validation using emulation and network simulations 36
2.8.2. Testing and validation using real experiments 41

Chapter 3. Application to Communications in a Drone Fleet 43

3.1. Introduction 43
3.2. Cooperating unmanned aeronautical systems 44
3.2.1. Unmanned Aircraft/Aerial Systems 45
3.2.2. Payload 46
3.2.3. Ground station 46
3.2.4. Drone fleets 46
3.3. Ad hoc communications architecture for a drone fleet 47
3.3.1. Ad hoc drone network 49
3.4. Routing protocols in an ad hoc drone network 52
3.4.1. Hierarchical protocols 54
3.4.2. Reactive protocols 54
3.4.3. Proactive protocols 55
3.4.4. Geographic protocols 56
3.4.5. UAANET networks and routing protocols: discussion 57
3.5. Security in an ad hoc drone network 59
3.5.1. Weaknesses in UAANET networks 60
3.5.2. Attacks on UAANET networks 62

3.5.3. SAODV secure ad hoc routing protocols 68
3.6. Designing a new secure routing protocol for UAANETs (SUAP: Secure UAANET Routing Protocol) 74
3.6.1. Choosing an initial routing protocol 75
3.6.2. The SUAP protocol 76
3.6.3. The SAODV protocol 79
3.6.4. Wormhole attacks 84
3.6.5. Single attacker variant 84
3.6.6. State of the art: solutions for defense against wormhole attacks 86
3.6.7. A new method for detecting and defending against wormhole attacks 91
3.6.8. Defense mechanism for single-attacker wormhole attacks 97
3.6.9. Limitations of the SUAP protocol 99
3.7. Using the AVISPA tool to verify the security properties of the SUAP protocol 100
3.7.1. Application of the SUAP protocol 101
3.7.2. Analysis of the specification of the SUAP protocol 103
3.8. Implementation of the SUAP protocol 104
3.8.1. Software architecture of the SUAP algorithm 105
3.8.2. Modeling the SUAP protocol 106
3.8.3. Use of the model-driven approach in developing the SUAP protocol 114
3.8.4. Implementation of the SUAP protocol 116
3.9. Validation of the SUAP protocol by performance evaluation 118
3.9.1. Validation of the routing partition 119
3.9.2. Validation of the security functions of the SUAP protocol 131
3.9.3. Validation of the wormhole detection mechanism 145
3.9.4. Validation by performance evaluation: discussion 150

Conclusions and Perspectives 153

Bibliography 159

Index 169