

# Table des matières

<b>Avant-propos</b> . . . . .	1
<b>Introduction et positionnement de l'ouvrage</b> . . . . .	3
<b>Chapitre 1. État de l'art des méthodes orientées modèles (MDD – <i>Model Driven Development</i>) appliquées aux systèmes aéronautiques</b> . . . . .	7
1.1. Principe du MDD . . . . .	7
1.2. Cas des systèmes avioniques . . . . .	8
1.2.1. Virtualisation des systèmes : <i>Integrated Modular Avionics</i> . . . . .	9
1.2.2. MILS : diviser pour mieux régner sur un monde sûr . . . . .	9
1.2.3. Traitement conjoint des aspects sûreté et sécurité . . . . .	11
1.2.4. Certification d'un système avionique . . . . .	13
1.2.4.1. Qualification d'outils pour la certification . . . . .	13
1.2.4.2. Les approches de développement orientées modèle dans l'aéronautique . . . . .	13
1.2.4.3. DO-178C : <i>Software Considerations in Airborne Systems             and Equipment Certification</i> . . . . .	14
1.2.4.4. DO-331 : <i>Model-Based Development and Verification</i> . . . . .	14
1.3. Cas des drones (UAS – <i>Unmanned Aerial System</i> ) . . . . .	14
1.3.1. Besoin d'une nouvelle méthodologie de prototypage rapide pour la conception d'un système UAS . . . . .	15
1.3.2. Norme de sûreté . . . . .	16
1.3.3. Cycle de vie de développement logiciel . . . . .	17

<b>Chapitre 2. Méthode originale de prototypage rapide de système embarqué pour les drones</b> . . . . .	<b>21</b>
2.1. Auto-génération du système à partir de modèles . . . . .	21
2.1.1. Présentation des différentes étapes . . . . .	21
2.2. Vérification formelle des modèles . . . . .	24
2.2.1. Analyse des modèles . . . . .	25
2.3. Avantages de l'utilisation de la méthodologie MDD ( <i>Model Driven Development</i> ) . . . . .	27
2.4. Apport de l'approche MDD dans la certification UAS . . . . .	27
2.5. Choix d'outils pour l'application de la méthodologie MDD . . . . .	31
2.6. Un outil spécifique de vérification formelle de protocole de sécurité : AVISPA . . . . .	37
2.7. Nécessité des procédures de vérification . . . . .	37
2.7.1. Pourquoi le choix de l'outil AVISPA ? . . . . .	39
2.8. Complément à la vérification formelle : simulations et expérimentations . . . . .	40
2.8.1. Test et validation par émulation et simulation réseau . . . . .	40
2.8.2. Pourquoi un test par émulation et simulation ? . . . . .	41
2.8.3. Protocole expérimental pour les réseaux UAANET . . . . .	42
2.9. Architecture de l'outil de test . . . . .	42
2.9.1. Test et validation par expérimentation réelle . . . . .	45
<b>Chapitre 3. Application au domaine de la communication d'une flotte de drones</b> . . . . .	<b>47</b>
3.1. Introduction . . . . .	47
3.2. Systèmes aéronautiques coopératifs sans pilote . . . . .	48
3.2.1. <i>Unmanned Aircraft/Aerial Systems</i> . . . . .	49
3.2.2. Charge utile . . . . .	49
3.2.3. Station sol . . . . .	50
3.2.4. Flotte de drones . . . . .	50
3.3. Architecture de communication <i>ad hoc</i> pour une flotte de drones . . . . .	51
3.3.1. Réseau <i>ad hoc</i> de drones . . . . .	52
3.3.1.1. Connectivité réseau . . . . .	54
3.3.1.2. Densité des nœuds . . . . .	54
3.3.1.3. Consommation énergétique . . . . .	54
3.3.1.4. Délai strict et contraint . . . . .	54
3.3.2. Protocoles de routage dans un réseau <i>ad hoc</i> de drones . . . . .	55
3.3.2.1. Protocole hiérarchique . . . . .	57
3.3.2.2. Protocole réactif . . . . .	57
3.3.2.3. Protocole proactif . . . . .	58
3.3.2.4. Protocole géographique . . . . .	59

3.4.5. Discussions sur les réseaux UAANET et les protocoles de routage . . . . .	60
3.5. Sécurité dans un réseau <i>ad hoc</i> de drones . . . . .	62
3.5.1. Vulnérabilités des réseaux UAANET . . . . .	63
3.5.2. Attaques dans les réseaux UAANET . . . . .	65
3.5.2.1. Attaques au niveau de la couche physique . . . . .	65
3.5.2.2. Attaques au niveau de la couche liaison . . . . .	66
3.5.2.3. Attaques liées aux protocoles de routage . . . . .	67
3.5.2.4. Solutions existantes et limites . . . . .	70
3.5.3. Protocoles de routage <i>ad hoc</i> sécurisé SAODV . . . . .	71
3.5.3.1. Discussions sur les protocoles de routage sécurisés existants . . . . .	72
3.6. Conception d'un nouveau protocole de routage sécurisé (SUAP : <i>Secure UAANET routing Protocol</i> ) pour les UAANET . . . . .	76
3.6.1. Choix d'un protocole de routage de départ . . . . .	77
3.6.2. Protocole SUAP . . . . .	78
3.6.2.1. Modèles réseau et d'attaques considérés dans la conception du protocole SUAP . . . . .	78
3.6.2.2. Description du protocole SUAP . . . . .	79
3.6.2.3. Analyse des solutions existantes . . . . .	79
3.6.3. Protocole SAODV . . . . .	80
3.6.3.1. Signature numérique dans SAODV . . . . .	81
3.6.3.2. Chaîne de hachage dans SAODV . . . . .	83
3.6.4. Attaque <i>wormhole</i> . . . . .	85
3.6.5. Attaque avec un seul attaquant . . . . .	86
3.6.6. État de l'art des solutions contre l'attaque <i>wormhole</i> . . . . .	87
3.6.6.1. Synthèse des travaux existants . . . . .	91
3.6.7. Proposition d'une nouvelle méthode pour détecter et contrer l'attaque <i>wormhole</i> . . . . .	92
3.6.8. Détails du mécanisme permettant de contrer l'attaque <i>wormhole</i> réalisée par un seul attaquant . . . . .	96
3.6.9. Limites du protocole SUAP . . . . .	98
3.7. Utilisation de l'outil AVISPA pour vérifier les propriétés de sécurité du protocole SUAP . . . . .	100
3.7.1. Cas d'application du protocole SUAP . . . . .	101
3.7.2. Analyse de spécification du protocole SUAP . . . . .	102
3.8. Mise en œuvre du protocole SUAP . . . . .	104
3.8.1. Architecture logicielle de l'algorithme SUAP . . . . .	104
3.8.2. Modélisation du protocole SUAP . . . . .	105
3.8.2.1. Partition de routage . . . . .	105
3.8.2.2. Partition de sécurisation . . . . .	110
3.8.2.3. Partition d'interfaçage du matériel avec la partition de sécurisation et de routage . . . . .	113

3.8.3. Apport de l'approche orientée modèle dans la conception du protocole SUAP . . . . .	113
3.8.4. Mise en œuvre du protocole SUAP . . . . .	115
3.9. Validation par évaluation des performances du protocole SUAP . . . . .	116
3.9.1. Validation de la partition de routage . . . . .	117
3.9.1.1. Topologie de test pour la partition de routage . . . . .	117
3.9.1.2. Métriques de performance considérées . . . . .	118
3.9.1.3. Résultats obtenus et interprétation des performances de la partition de routage . . . . .	120
3.9.1.4. Discussions sur la phase de validation de la partition de routage . . . . .	128
3.9.2. Validation des fonctions de sécurité du protocole SUAP . . . . .	129
3.9.2.1. Validation de la partition de sécurisation (authentification des messages) en environnement émulé . . . . .	129
3.9.2.2. Validation de la partition de sécurisation (authentification des messages) en environnement réel . . . . .	134
3.9.3. Validation du mécanisme de détection de l'attaque <i>wormhole</i> . . . . .	142
3.9.4. Discussions sur la validation par évaluation des performances . . . . .	147
<b>Conclusions et perspectives . . . . .</b>	<b>149</b>
<b>Bibliographie . . . . .</b>	<b>153</b>
<b>Index . . . . .</b>	<b>163</b>