République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira de Béjaia

Faculté des Sciences Exactes
Département de Recherche Opérationnelle

Mémoire de fin détude
Option : Modélisation Mathématique et Évaluation des Performances Réseaux

Thème

Routage sécurisé dans les réseaux FANETs : L'attaque WORMHOLE

Réalisé par :

SAIDANI Lynda

Soutenu le 14 juillet 2022 devant le jury composé de :

M^{me}**BOULFKHER Samra**	MCA	Université de Béjaia	Promotrice
M^{me} **LEKADIR Ouiza**	professeur	Université de Béjaia	Présidente
M^{me}**BACHIRI Lyna**	MCA	Université de Béjaia	Examinatrice
M^{me}**BELAMRI Fatima**	Doctorante	Université de Béjaia	Examinatrice

Promotion 2021-2022

Résumé

L'avancement des recherches dans le domaine des réseaux Ad hoc (MANET) et des technologies de communication ont favorisé la naissance des réseaux FANETs (Flying Ad hoc Networks), où les nœuds sont des drones. Les applications liées à ses réseaux sont devenues de plus en plus populaires, comprenant les services militaires, la photographie aérienne, les levés géologiques et topographiques, la surveillance des catastrophes,... Par conséquent, il est très important de construire un FANET hautement fiable et tolérant aux pannes. Cependant, l'architecture du réseau très différente des architectures réseau précédentes, car les drones volants à grande vitesse, la topologie se varie également rapidement, se qui complique le routage des données. Par conséquent, il faut concevoir des protocoles de routage efficace et qui garantissent la sécurité du système, notamment de l'attaque WORMHOLE. Ce manuscrit présente un nouveau schéma de sécurité contre l'attaque WORMHOLE qui est une amélioration du protocole SUAP (Secure UAV Ad hoc Network Protocol), avec une modélisation de réseau de Pétri coloré, qui est implémenté sur CPN-Tools.

Mots clés : MANETS, FANETs, UAVs, Routage, Sécurité, SUAP, réseau de Pétri

---

Abstract

The advancement of research in the field of Ad hoc networks (MANET) and communication technologies has favored the birth of FANETs (Flying Ad hoc Networks), where the nodes are drones. Applications related to its networks have become increasingly popular, including military services, aerial photography, geological and topographical surveys, disaster monitoring,... Therefore, it is very important to build a highly reliable and fault-tolerant FANET. However, the very network architecture different from previous network architectures, because drones fly at high speed, the topology also varies quickly, which complicates the routing of data. Consequently, it is necessary to design effective routing protocols and which guarantee the security of the system, in particular from the WORMHOLE attack. This manuscript presents a new security scheme against the WORMHOLE attack which is an improvement of the SUAP protocol (Secure UAV Ad hoc Network Protocol), with a colored Petri net modeling, which is implemented on CPN-Tools.

Keywords : MANETS, FANETs, UAVs, Routing, Security, SUAP. Petri Network.

Table des matières

Table des figures

Liste des tableaux

Liste des sigles et acronymes

AODV	*Ad hoc On Demand Distance*
DOLSR	*Directional Optimized Link State Routing*
DSDV	*Destination Sequenced Distance Vector*
DSR	*Dynamic source routing*
FANET	*Flying Ad hoc network*
GPMOR	*Geographic Position Mobility Oriented Routing*
GPS	*Global Positioning System*
HPR	*Hybrid routing protocol*
IA	*Intelligence Artificielle*
MAC	*Medium access control*
MANET	*Mobile ad hoc network*
OLSR	*Optimized Link State Routing Protocol*
OSI	*Open System Interconnection*
RERR	*Route error*
RREP	*Route reply*
RREQ	*Route request*
RGR	*Reactive greedy reactive routing protocol*
RPR	*Reactive Routing Protocol*

SUAP *Secure UAV Ad hoc Network Protocol*

TCP/IP *Transport Control Protocol/ Internet Protocol*

TORA *Temporary Ordered Routing Algorithm*

UAV *Unmanned Aerial Vehicles*

VANET *Vehicular ad hoc network*

Introduction générale

Contexte

Les réseaux Ad hoc (MANETs) sont des types de réseaux à sauts multiples et auto-organisé et qui sont largement utilisé sur différents secteurs. La constante évolution des technologies de l'information et le penchant vers l'utilisation des machines sans fil qui se sont imposées ces dernières années ont fait émerger de nouveaux types de réseaux MANETs : les réseaux VANETs (Vehicule Ad hoc Networks) et les réseaux FANETs (Flying Ad hoc Networks).

Les FANETs sont un groupe de véhicules aériens sans pilote (UAV) communiquant entre eux sans avoir besoin de point d'accès, mais au moins l'un d'entre eux doit être connecté à une base au sol ou à un satellite.Les véhicules aériens sans pilote (UAV) ou les drones volants sont des entités contrôlables à distance ou de manière autonome sans humain à bord. Ils ont été largement étudié dans différents domaines, pas seulement pour un usage militaire mais aussi dans des applications civiles telles que la recherche et le sauvetage missions, détection de cibles, télédétection et surveillance.

Ils sont utilisés dans de nombreuses applications critiques, ce qui en fait la cible de nouvelles attaques. Car, ses réseaux se distingue de l'utilisation de liaisons sans fil se qui rend le réseau vulnérable aux écoutes clandestines et aux attaques d'interférences actives. De plus, les protocoles de routage conçus pour ces réseaux reposent sur la coopération des noeuds, ce qui rend les attaques internes très efficaces dans de tels réseaux. La grande mobilité de ces réseaux pourrait également affecter la sécurité de différentes manières. D'une part, la mobilité permet aux attaquants d'échapper aux solutions de sécurité tout en endommageant le réseau.

En effet, ce routage est un problème d'optimisation sous des contraintes telles que les changements de topologies, la volatilité des liens, la capacité limitée de stockage, de traitement et de bande passante, la sécurité, le niveau d'énergie, etc. Un certain nombre de protocoles de routage sécurisés dans FANETs ont été proposés dans le but de prévenir différents types de attaques (par exemple, falsification de message, largage de message, message rejouer, attaque de trou de ver, attaque de trou noir). La plupart de ces protocoles sont analysés et modélisés en utilisant des outils et techniques de recherches opérationnelles.

Ce mémoire est organisé comme suit :

Le premier chapitre "**Généralité sur les réseaux FANETs**" on présentera les ca-

ractéristiques liées aux environnements mobiles Ad hoc, quelques concepts sur les réseaux VANETs et nous passerons par la suite à la présentation des réseaux Flying Ad hoc Network (FANETs), leur évolution, caractéristiques ainsi que les différentes applications associées et les défis.

Le deuxième chapitre "**Mécanismes de sécurité dans les réseaux FANETs**" on citera les outils et les requis de base de la sécurité, la vulnérabilité des FANETs, les problèmes lié à la sécurité et les attaques existantes enfin les techniques et solutions qui peuvent être mises en oeuvre afin de sécuriser les informations échangées à travers ces réseaux et assurer la qualité des missions.

Le troisième chapitre "**Protocoles de routage sécurisés dans les FANETs**" dans une première partie on parlera sur le routage dans les réseaux Ad hoc et ses protocoles associés, ensuite le routage dans les FANETs, les critères de conception d'un protocole de routage, les différentes classes de schémas de routage, une section dédié aux attaques liées à la couche réseau enfin les protocoles de routage sécurisés contre l'attaque WORMHOLE.

Le quatrième chapitre "**Mécanisme de sécurité contre l'attaque WORMHOLE**" dans cette partie de notre travail, nous détaillerons le protocole SUAP : Secure UAV Ad hoc Network Protocol, son fonctionnement, ses avantages, ses inconvénients, et sa sécurité. Par la suite, nous introduirons les mécanismes de sécurité contre l'attaque WORMHOLE, puis nous présenterons un protocole TEE-SUAP : Time Energetic Efficiency SUAP, qui est une amélioration du protocole SUAP, son impact sur l'attaque WORMHOLE, enfin une modélisation avec un réseau de Pétri pour un mécanisme de détection et prévention de l'attaque WORMHOLE implémenté sur le logiciel CPN-tools.

Chapitre 1

Généralités sur les réseaux FANETs

1.1 Introduction

L'apparition récente mais remarquable des véhicules aériens sans pilote (UAV ou drone) qui occuperont bientôt la majeure partie de nos systèmes de service constitue la clé de l'expansion des nouvelles technologies de communication et des réseaux sans fil. Ces engins dans un premier temps étaient associés à l'armée, mais aujourd'hui elles sont utilisées dans un large éventail des rôles civils, allant de la recherche, le sauvetage, la surveillance, de la vidéo graphie, à l'agriculture et même aux services de livraison.
La mise en place d'un réseau Ad hoc de drones est un problème difficile, et les exigences peuvent différer des réseaux traditionnels (MANETs et VANETs) en termes de mobilités des nœuds, routage des messages, connectivité et la qualité de service.

Dans ce chapitre, nous allons commencer par présenter les caractéristiques liées aux environnements mobiles Ad hoc, quelques concepts sur les réseaux VANETs et nous passerons par la suite à la présentation des réseaux Flying Ad hoc Network (FANETs), leur évolution, caractéristiques ainsi que les différentes applications associées et les défis.

1.2 Réseaux Ad hoc

Les réseaux Ad hoc appelés aussi réseau MANET (Mobile Ad hoc Netwok) ou WANET (Wirless Ad hoc Network).

1.2.1 Définition d'un réseau Ad hoc

Un réseau Ad hoc est un type de réseau sans fil décentralisé, il se compose de systèmes informatique divers, plus ou moins complexes : appelés **nœuds**. Ils peuvent communiquer et coopérer entre eux de manière autonomes par ondes radio pour échanger les services [3].

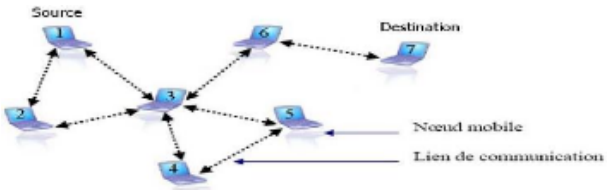

FIG. 1.1 : *Réseau Ad hoc.*

1.2.2 Caractéristiques d'un réseaux Ad hoc

Un réseau Ad-hoc est constitué d'entités, mobiles, qui communiquent entre elles, et son fonctionnement le différencie notablement des autres réseaux, d'où les caractéristiques suivantes :

- ***Topologie Dynamique :*** les nœuds se déplacent indépendamment les uns des autres [1].
- ***Absence d'infrastructure :*** l'absence de tout genre d'administration centralisée.
- ***Capacité limitée des liens :*** l'utilisation d'un médium de communication partagée, ce partage fait que la bande passante réservée à une hôte soit limitée [4].
- ***Ressources énergétiques limitées :*** les nœuds dans les réseaux Ad hoc sont alimentés typiquement par des batteries dont la capacité et l'énergie sont limitées.
- ***Sécurité limitée :*** les réseaux Ad hoc sont plus vulnérable par rapport aux autres réseaux à cause de la nature du médium qui rend certaines attaques malicieuses, ainsi que la topologie du réseau qui peuvent être redoutable.
- ***Nœuds cachés :*** le problème du noeud caché se produit lorsque deux unités mobiles ne peuvent pas s'entendre l'une et l'autre du fait qu'un obstacle les empêche de communiquer entre elles ou que la distance qui les sépare est trop grande.

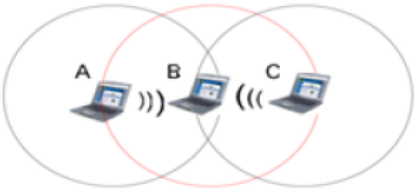

FIG. 1.2 : *Problème du nœud caché.*

1.3 Réseaux VANETs

Parmi les principaux types de réseaux Ad hoc on a : les réseaux de capteurs (en anglais WSN : Wirless Sensor Networks), les réseaux maillés (en anglais WMN : Wirless Mesh Networks). Les réseaux Ad hoc véhiculaires (en anglais VANETs : Vehicular Ad hoc

Networks) et les réseaux Ad hoc volants (en anglais FANETs : Flying Ad hoc Networks). Les derniers deux réseaux sont des types particuliers des réseaux Ad hoc et qui possèdent les mêmes caractéristiques.

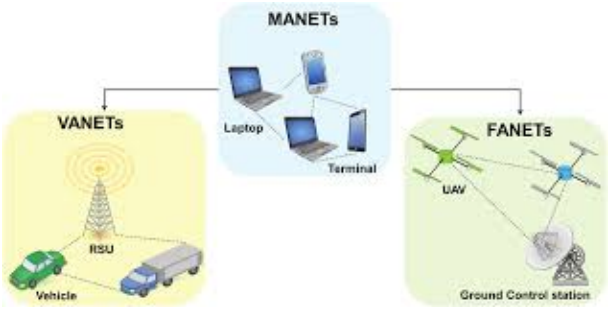

FIG. 1.3 : *Les sous réseaux de MANET*

1.3.1 Définition des réseaux VANETs

Un réseau VANET est un réseau dont les nœuds sont des véhicules terrestres intelligents, équipés de matériels à très hautes technologies (Calculateurs, radars, systèmes de géolocalisation (GPS), différents types de capteurs et périphériques réseau). Ils permettent des communications entre les véhiculaires (V2V) et véhicules à infrastructure (V2I). Les différents nœuds s'échangent les alertes ou les informations utiles pour améliorer la sécurité de la circulation routière, ainsi que des données (musique, vidéo, publicités…),pour rendre le temps qu'on passe dans nos véhicules plus agréable,moins ennuyeux et plus sécurisé [5].

1.3.2 Applications des réseaux VANETs

Le développement des véhicules intelligents a apporté de nouvelles possibilités d'application dans les réseaux VANETs. Ces applications peuvent être catégorisées en : Application de transport intelligent et en application de confort et de maintenance [31].

- **Les applications de transport intelligent** englobant les applications de sûreté et de transport efficace (Éviter des collisions, réduire les longues files sur la route à la suite d'un accident,...)

- **Les applications de confort** (Les applications de jeux en ligne, le partage de music et de vidéo, l'accès à la messagerie web, les communications interactives, l'accès aux informations utiles tel que le restaurant le plus proche, la stations de service à proximité, les parking disponibles dans les environs,...)

- **Les applications de maintenance** (Les automobilistes qui rencontrent des problèmes mécaniques et qui nécessitent une aide urgente, ils pourraient de ce fait bénéficier d'une aide à distance).

1.4 Réseaux FANETs

Les réseaux FANETs (Flying Ad hoc Network) ou les Réseaux Ad hoc Volants sont une solution prometteuse pour les scénarios d'application impliquant des drones.

1.4.1 Définition des réseaux FANETs

C'est un type de réseau sans fil décentralisé ne reposant pas sur une infrastructure préexistante, comme les routeurs dans les réseaux câblés ou des points d'accès dans les réseaux sans fil. Où les nœuds sont des drones, chaque nœud participe au routage en transférant les données pour d'autres nœuds, de sorte que la détermination des nœuds qui transmettent les données soit effectuée de manière dynamique sur la base de la connectivité réseau et de l'algorithme de routage.

1.4.2 Systèmes aéronautiques coopératifs sans pilote

Véhicules aériens télépilotés (Remotely Piloted Vehicle RPV), aéronef télépiloté (Remotely Piloted Aircraft RPA), aéronef télécommandé (Remotely Operated Aircraft ROA), véhicules aériens sans pilote (UAV Unmanned Aerial Vehicles) : ce sont des acronymes administratifs avancés désigné par la fédérale de l'aviation américaine, Federal Aviation Admnistration (FAA), pour regrouper les différentes dénominations associé à des avions sans pilote.
Le système aéronautiques sans pilote,en anglais Unmanned Aircraft System (UAS) est composé de drones, de différentes liaisons de communication et de transfert de données, d'une ou plusieurs stations sol et de systèmes additionnels sécurisant la mission.

1. **Drones**
   Les drones ou les aéronefs se sont des véhicules sans pilote à bord. Ils sont constitués d'un auto pilote qui leur permet d'exécuter des commandes envoyées depuis une station sol ainsi que d'un ensemble de systèmes micro-électromécaniques qui inclue des microprocesseurs, des adaptateurs radio sans fil et des charges utiles généralement limitées en poids et en taille.

2. **Flotte de drones**
   La taille et le poids limités des drones sont un obstacle à la réalisation des missions de longue durée (Exemple de surveillance sur une vaste zone) ; d'où le déploiement d'un système multi-drones permettant la mise en oeuvre d'un réseau de communication coopératif entre les drones et apporte plus de valeur en termes de performances et de productivité [39].

   Cette amélioration est rendue possible grâce à un algorithme de coordination fiable, qui échange en continu des trafics de signalisation. Dans ce cas, le réseau est appelé réseau Ad hoc de Drones en anglais UAANET (Unmaned Areal Ad hoc Network).

3. **Station de sol**
   Les stations de sol sont considérées comme un nœud central et communique avec tous les drones simultanément, en incluant les entités physique et logiciels.

4. **Charge utile**
   Les charges utiles regroupent les différents systèmes embarqués qui lui permettent de réaliser sa mission, comme : un appareil photo, une caméra vidéo, une caméra thermique, des sondes ou tout autre type de capteurs,...

1.4.3 Évolution des drones

Cela fût plus d'un siècle que le premier aéronef sans pilote (UAV) décollait de la base militaire d'Avord (le 2 juillet 1917) par le français Max Boucher qui a réussit le décollage d'un avion de type Voisin 150 HP sans pilote.

Ces engins sans pilote à bord ont été construits et ils ont volé pour des tests et des missions militaires. Trois décennies plus tard, à l'occasion du conflit Coréen et de la guerre du Vietnam dans les années 50, des drones ont été développés par les États-Unis pour réaliser diverses missions allant de la surveillance et de la collecte de renseignements, à l'intervention militaire en terrain ennemi (David et Panhaleux).

Ce n'est que dans les années 2000 que les UAV font leur véritable entrée dans le secteur civil. Aujourd'hui les drones sont accessibles au grand public ainsi qu'aux entreprises grâce au progrès technologique et la miniaturisation des systèmes informatiques, les caméras et les batteries dotant ces machines de capacités énormes.La multitude d'utilisations possibles offerte par les drones ne cesse de croître d'année en année [15].

1.4.4 Caractéristiques des réseaux FANETs

Les FANETs ont hérité les caractéristiques des réseuax MANETs, mais ils possèdent ses propres attributs qui le distingue des autres réseaux, dans ce qui suit nous résumons ses particularités :

- ***La rapidité :*** la fréquence et la rapidité des fluctuations topologiques dues à la grande mobilité des noeuds, les UAVs.
- ***Densité :*** la densité c'est le nombre moyen de drones dans une zone unitaire. En fonction de plusieurs critères la densité des drones se varie : Si les UAV ont la capacité de fournir à la fois une large transmission et se déplacent à des vitesses élevées, leur la densité devient faible .D'où le déploiement d'un grand nombre de drones coopérant entre eux.
- ***Station de base au sol (GBS) :*** le GBS (Ground Base Station) est capable d'envoyer ou collecter le trafic de données de vol (La vitesse, l'altitude et l'état de la batterie).Tout comme il peut à la fois communiquer avec tous UAV à sa portée et calculer la qualité des liaisons de communication entre eux.
- ***Système LUNCH :*** Le système LUNCH fournit aux UAV leurs vitesses de vol initiales en une distance et un temps très courts.
- ***Accès à des endroits où l'homme ne peut pas atteindre :*** les réseaux FANETs peuvent accédé à des zones que l'homme peut pas atteindre, par exemple les zones de guerres.

- ***Respecte l'environnement :*** les UAVs circulent sans émission de CO_2
- ***Stable en matière de qualité*** : les équipements dont les drones servent (Les caméras, les capteurs,...) favorisent la prise de vue de qualité, de sons, ect.

1.4.5 Contraintes de conceptions des réseaux FANETs

La conception d'un système aérien sans pilote nécessite un ensemble de mécanismes et de règles qui définissent comment l'information doit être échangés entre les UAVs et les stations de bases. Il y a un certain nombre d'organisations de communication qui sont utilisées selon les applications que les drones envisagent d'accomplir [7].

1. **Organisation centralisée**

   L'ensemble des drones sont directement connectés à un ou plusieurs GBS qui peut communiquer avec chaque UAV simultanément. Cet organisation a pour avantages :

   - L'augmentation de la tolérance aux pannes dans le cas d'échec des drones.
   - Le parallélisme des tâches.
   - L'amélioration des capacités de calcul et de stockage.

   D'une autre part cette se trouve face à trois grands défauts :

   - L'augmentation des UAVs nécessite plus de liaisons descendantes de bande passante coûteuses.
   - La latence élevée à cause de la centralisation du trafic
   - Le GBS constitue un point de défaillance représentant une vulnérabilité contre les défaillances et sa panne génère la perturbation du réseau.

2. **Organisation multigroupe**

   Les drones ont la possibilité de communiquer entre eux de manière Ad hoc tout en conservant l'organisation centralisée, et des groupes sont formé où chacun des UAVs désigné joue le rôle passerelles reliant les groupes aux GBS . Cette configuration améliore la performance et prend en charge les communications pour un grand nombre d'UAVs ayant des vols de différents fonctionnalités.

3. **Organisation cellulaire**

   Les cellules contenant les UAVs sont considérées comme solution prometteuse pour faciliter le déploiement de nombreuses applications civiles et militaires. Une fréquence unique est utilisée par chaque cellule pour éviter les interférences entre les cellules . Ces dernières peuvent fournir une couverture du signal importante sur des zones spécifiques. Cependant, les cellules ne sont pas une solution rentable en raison de la mise en œuvre coûteuse des GBS. De plus,elle est vulnérable car les GBS fixes peuvent échouer à tout moment, provoquant la perte de contrôle des UAVs.

1.4.6 Applications des réseaux FANETs

Les exemples d'applications peuvent se diviser en plusieurs grandes catégories à partir d'un large éventail de clients utilisateurs, publics et parapublics, tels que la Police, la Gendarmerie, les Pompiers (évaluation de sinistres, repérage de réfugiés dans un immeuble ou sur le toit), la Sécurité civile, etc. On cite les catégories suivantes [22] :

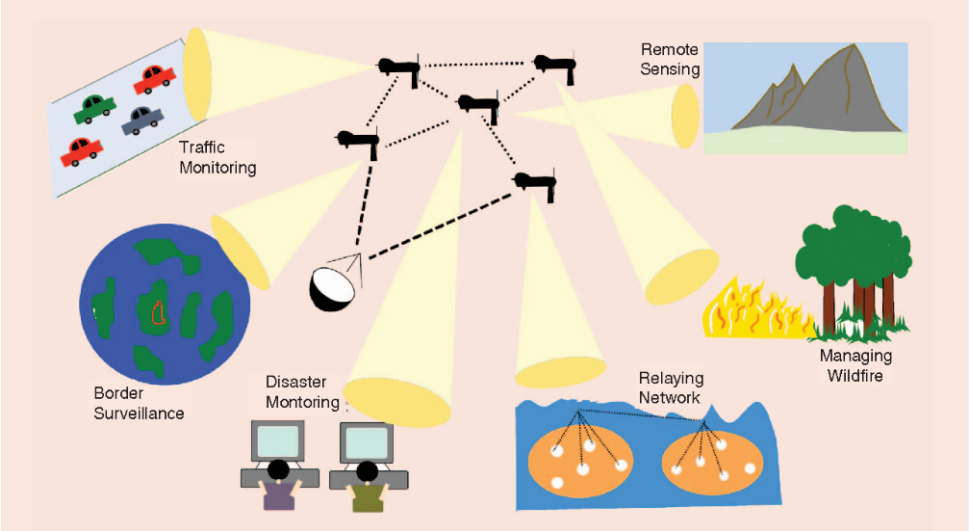

FIG. 1.4 : *Application des réseaux FANETs.*

✓ **La surveillance et l'observation**

- **Études scientifiques** (atmosphère, des sols, océans, prévisions météorologiques...)
- **Surveillance d'urgence** :

  1. Incendies de forêts, avalanches , volcans, tornades,...ect
  2. Recherche et sauvetage
  3. Évaluation des dégâts en cas de catastrophe naturelle (inondation, éruption, tremblements)

- **Surveillance civile**

  1. Surveillance des cultures et épandage agricole
  2. Surveillance maritime (voies maritimes, trafic de drogue, détection des pollutions par hydrocarbures, localisation pour sauvetage).
  3. Surveillance urbaine, des manifestations, ainsi que des frontières.
  4. Surveillance du trafic routier et du transport de matières dangereuses.

✓ **Exploration aérienne**

- Transport de fret

- Cartographie
- Utilisation par l'industrie cinématographique
- Largages de vivres et d'équipements de sauvetage en zones hostiles

✓ **Autre missions spécifiques**

- Relais de communications
- Missions dangereuses (détection de gaz toxiques, radiations)
- Recherche et sauvetage (mer, montagnes, désert...)

1.4.7 Architecture de communication dans les réseaux FANETs

L'architecture de communication détermine le mode d'échange d'informations entre le les stations de base et les drones et les plus remarquables des systèmes multi-UAV sont :

- Architecture de communication centralisé.
- Architecture de communication satellitaire.
- Architecture de communication réseau cellulaire.
- Architecture de communication réseau Ad hoc.

Le tableau 1.1 compare les différentes architectures de communication des réseaux FANETs [2].

Cette comparaison a été faite par rapport :

1. **Latence de transfert des paquets :** l'architecture centralisé et satellitaire souffrent de latence de transfert des paquets de données entre deux drones voisins en raison du relais obligé par la station sol, et aussi dans le cas de présence d'un obstacle entre un drone et la station sol (Par exemple les montagnes), le signal peut être bloqué . En conséquence, les nœuds ne peuvent s'éloigner que d'une distance maximale de la station sol, limitant ainsi la distance d'opération des drones [8].
2. **Sécurité :** la sécurité dans l'architecture satellitaire dépend d'un seul point et dans l'architecture cellulaire dépend des infrastructures fixes .Par contre la sécurité dans l'architecture Ad hoc est distribuée entre les noeuds.
3. **Coût :** l'architecture Ad hoc est la moins coûteuse par rapport aux autres architectures.
4. **Mobilité et flexibilité :** grâce à la mobilité des nœuds (libre et arbitraire), l'architecture Ad hoc assure la mobilité et la flexibilité.

	Centralisé	Satellitaire	Cellulaire	Ad hoc
Avantage	-Découverte de service - Aptitude à contrôler l'entrée et la sortie des noeuds	-Connectivité	-Connectivité -Mise à l'échelle en fonction du nombre de stations de base -Possibilité de choisir le meilleur lien parmi ceux situés entre les stations de base	-Coût faible -Facile à déployer -Tient compte de la mobilité des noeuds -Communication autonome sans infrastructure -Optimisation de l'utilisation de la bande passante
Inconvénients	-Latence d'échange entre deux noeuds -Blocage possible des signaux -La sécurité dépend d'un seul point -Blocage des signaux	-Latence d'échange entre deux noeuds -Puissance d'émission importante -Coût élevé -La sécurité dépend d'un seul point	-Coût élevé de déploiement -Indisponibilité des infrastructures dans quelques situations -La sécurité dépend des infrastructure fixes	-Communication intermittente -Non contrôle de l'entrée et de la sortie des noeuds -Nécessite des protocoles de communication dynamiques

Tab. 1.1 : Comparaison des différentes architectures de communication dans les FANETs

1.4.8 Problèmes et défis ouverts dans les réseaux FANETs

Malgré plusieurs avancées au cours de ces dernières années, les FANETs ont encore des restrictions qui peuvent être critiques pour leur fonctionnement selon l'application :

- **Consommation d'énergie :** elle limite le temps de vol des drones, la vitesse de connexion et la portée du signal transmis par eux. Alors, l'exploration et la recherche de solutions à ces limitations sont nécessaire [20].
- **Mobilité :** L'un des plus grands différentiels des UAVs est la grande mobilité et la variation de vitesse dont ils disposent, ce qui leur permet d'accéder à des endroits difficiles d'accès et de parcourir de longues distances en peu de temps. Il est nécessaire que des informations critiques pour la mobilité entre les nœuds soient transmises aux réseau ou à la station de base comme les alertes de prévention de collisions, GPS, temps de vol, conditions environnementales et climatiques, ainsi que la transmission des commandes de pilotage du drone s'ils sont contrôlés par une station de base.
- **Routage :** les protocole de routage sont le cerveau des FANETs, ils contrôlent tous les flux entre les UAVs et les autres appareils qui leur sont connectés, et bien qu'il existe déjà plusieurs protocoles de routage disponibles, mais parfois ne peuvent pas faire face à la mobilité et à la vitesse des aéronefs, ce qui provoque un taux élevé

d'erreurs dans la connexion et jusqu'à la chute du réseau dans certains cas. De ce contexte, de nouveaux protocoles ont été développés et d'autres en cours de création.

- **Réglementations nationales :** les drones sont de plus en plus utilisé dans de nombreux domaines d'application, ils trouvent leur place dans l'information moderne et ils deviennent de plus en plus une partie de l'espace aérien national de chaque pays . La plupart des réglementations aériennes dans les pays n'autorisent pas les opérations d'UAVs contrôlées dans l'espace aérien civil. Cela peut être vu comme le plus grand obstacle actuel au développement de UAS dans les zones civiles. Par conséquent, il existe un grand besoin de définir des règles distinctives et réglementations pour intégrer les vols des drones dans le l'espace aérien national [4].

- **Planification de trajectoire :** dans une zone de mission à grande échelle, la coopération et la coordination entre les drones ne sont pas seulement caractéristique souhaitable mais aussi cruciale pour augmenter l'efficacité. Durant les opérations, il peut être des changements dynamiques comme l'ajout/ suppression des drones et des obstacles physiques statiques, menaces dynamiques (telles que les radars mobiles). Dans de tels cas, chaque UAV doit changer son chemin précédent, et les nouveaux devraient être recalculé dynamiquement. C'est pourquoi de nouveaux algorithmes/ méthodes de planification dynamique des chemins sont nécessaires pour coordonner les flottes de drones.

- **Qualité de service (QoS) :** un réseau FANET peut être utilisé pour de nombreux types d'applications, il transporte différents types de données, qui incluent localisations GPS, streaming vidéo/voix, images, messages texte simples,etc. Pour le succès de transmissions de données ces réseaux ont besoin de prendre en charge certaines qualités de service pour satisfaire un ensemble de performances prédéterminées et des contraintes comme le délai, la bande passante, la gigue, perte de paquets, et la sécurité.
  ✓ **Sécurité :** à cause de l'importance des informations envoyées/transmises par les véhicules aériens, la sécurité des communications dans les réseaux FANETs ne consiste pas seulement à assurer les objectifs de la sécurité , mais d'autres objectifs et contraintes doivent être pris en compte pour éviter les vulnérabilités induites ainsi que les différents attaques.

1.5 Conclusion

Dans ce chapitre, nous avons évoqué dans un premier temps quelques notions sur les réseaux Ad hoc et des réseaux VANETs puis on s'est focalisé sur les réseaux FANETs, allant de leur définition, leur convergence vers la flotte de drones qui a permet une coordination autonome entre plusieurs drones pour améliorer la capacité du système UAS, leurs types et leurs architectures de communication.

Les FANETs se trouvent face à des problèmes et des défis car leur champs d'applications est divers et ils sont cibles pour différentes attaques. Pour se protéger de ses actions malveillantes, les exigences et les mécanismes de sécurité doivent être attribués pour sauvegarder et garantir les services du réseau.

Les notions de sécurités, les attaques liées aux réseaux FANETs et les solutions proposées feront l'objet du prochain chapitre.

Chapitre 2

Mécanismes de sécurité dans les réseaux FANETs

2.1 Introduction

Les communications véhiculaires aérien constitueront dans le futur des réseaux Ad hoc. A cause de l'importance des informations échangées et la sensibilité des donnée , l'environnement des réseaux FANETs sera plus qu'hostile. En effet, les messages liés à la sécurité peuvent être falsifiés ou éliminés par des entités malveillantes afin de causer des accidents et mettre en péril les situations. Donc, avant le déploiement de ces réseaux, des mécanismes de sécurité appropriés doivent être mis en oeuvre afin d'éviter ces mauvais scénarios et d'identifier les entités responsables de ces activités malveillantes.

Dans ce chapitre, nous parlerons des outils et des mécanismes de base de la sécurité, la vulnérabilité des FANETs, les problèmes lié à la sécurité et les attaques existantes enfin les techniques et solutions qui peuvent être mises en oeuvre afin de sécuriser les informations échangées à travers ces réseaux et assurer la qualité des missions.

2.2 Notions de bases de la sécurité

La sécurité est l'un des facteurs clés de la réussite de la mise en œuvre de tout type réseau. De nombreuses organisations et chercheurs travaillent depuis plusieurs années pour protéger ses systèmes de sécurité et minimiser les attaques associées.

2.2.1 Sécurité

La sécurité informatique est une discipline qui se veut de protéger l'intégrité et la confidentialité des informations stockées dans un système informatique. Quoi qu'il en soit, il n'existe aucune technique capable d'assurer l'inviolabilité d'un système.

Parmi les outils les plus courants de la sécurité informatique : programmes antivirus, les firewalls (pare-feu), le cryptage de l'information et l'utilisation des données d'accès (mots de passe).

2.2.2 Requis de la sécurité

La sécurisation des communications nécessite la mise en oeuvre de mécanismes permettant d'atteindre un certain nombre d'objectifs généraux de sécurité. Ces objectifs comprennent [5] :

- Authentification : cela permet aux membres du réseau de s'assurer de la bonne identité des membres avec lesquels ils communiquent.
- Non-répudiation : elle permet de s'assurer qu'aucun émetteur ne peut nier d'être à l'origine d'un message. Cet objectif est indispensable dans les transactions électroniques et dans toutes les communications sensibles.
- Confidentialité : elle garantit que seules les parties autorisées peuvent accéder aux données transmises à travers le réseau. Ces données peuvent concerner la couche applicatrice ou les couches inférieures.
- Intégrité : elle assure que les données échangées ne sont pas soumises à une altération volontaire ou accidentelle. Donc, il permet aux destinataires de détecter les manipulations de données effectuées par les entités non autorisées et rejeter les paquets correspondants.
- Disponibilé : elle vise à garantir aux entités autorisées d'accéder aux ressources du réseau avec une qualité de service adéquate [33].

2.2.3 Primitives crypthographiques

La cryptologie c'est la science caché, et la crypthographie c'est une des discipline de la cryptologie qui est l'art de cacher l'information [35].

- **La cryptographie symétrique (ou cryptographie à clé secrète) :** elle consiste à utiliser une seule clé secrète partagée entre l'expéditeur et le destinataire pour chiffrer et déchiffrer les données.
- **La cryptographie asymétrique(ou cryptographie à clé publique) :** elle se repose sur l'utilisation d'une clé publique (qui est diffusée) et d'une clé privée (gardée secrète), l'une permettant de coder le message et l'autre de le décoder.
- **Le hachage :** consiste à déterminer une information de taille fixe et réduite (appelée l'empreinte ou le condensé) à partir d'une donnée de taille indifférente.
- **Les fonctions de hachage à sens unique :** c'est une fonction irréversible qui fournit l'empreinte à partir d'une chaîne fournie en entrée. La particularité de cette fonction est qu'il est aisé de calculer l'empreinte d'une chaîne donnée, mais il est difficile de retrouver ou déduire la chaîne initiale à partir de l'empreinte.
- **La signature numérique :** c'est un code numérique associé à un message électronique afin que les destinataires puissent en authentifier les origines et en vérifier l'intégrité. Son implémentation fait appel aux fonctions de hachage et à clé privée du signataire.

- **Le MAC (Message Authentification Code) :** un code qui accompagne les données qui assurent les mêmes fonctionnalités de la signature numérique, mais son implémentation se base sur l'utilisation de la clé secrète et sur des fonctions similaires à celles de hachage.

- **Le certificat numérique :**c'est une sorte de structure de données qui permet de prouver l'identité du propriétaire d'une clé publique. Les certificats numériques sont signés et délivrés par un tiers de confiance appelé l'autorité de certification (AC).

2.3 Sécurité des réseaux FANETs

Les véhicules aériens sans pilote (UAV) ont récemment suscité un intérêt considérable dans le domaine de la recherche et du commerce. Cependant dans la pratique, ces systèmes présentent de nombreux défis à relever avant de profiter pleinement de ces avantages. L'un des plus importants et qui fait l'objet de notre chapitre c'est la sécurité.

2.3.1 Vulnérabilité des réseaux FANETS

Les causes de vulnérabilité des UAVs sont, d'une part, intrinsèques à l'environnement du système UAS, autrement ils sont liées à l'architecture physique des nœuds, des différents liens de communication et à la condition de déploiement du système aérien sans pilote. D'autre part, la présence de nœuds malveillants dans le réseau peut également être une source de vulnérabilité du réseau. Dans ce qui suit, nous allons analyser ces différents points de vulnérabilité [14] :

- ***Canal de communication vulnérable***

  Les liens sans fil sont utilisés pour l'envoi et la réception des signaux dans les FANETs, ils sont soumis à diverses attaques (écoute illicite, interférence active). Étant donné que l'ensemble du trafic passe dans l'air, il suffit alors à l'attaquant de se positionner dans la zone de couverture des noeuds cibles pour intercepter les trafics. Aussi l'utilisation d'une antenne à fort gain à portée d'un drone peut permettre à l'attaquant l'écouter illicite de toute la flotte.

- ***Environnement non contrôlé***

  L'environnement des FANETs est dit distribué et dynamique. Cela signifie que la communication est partagée et opportuniste. Il est donc difficile de contrôler l'entrée et la sortie des noeuds dans le réseau, ce qui offre la possibilité aux noeuds malveillants de se connecter au réseau et de participer au transfert des paquets et usurper l'identité d'un noeud légitime et falsifier le mécanisme de routage.

- ***Topologie dynamique***

  À cause de la vitesse importante des drones la topologie du réseau n'est pas stable, ce qui engendre des problématiques de sécurité puisque, un protocole de routage ne peut différencier une coupure de communication (ou de lien) déclenchée par les mouvements des drones et l'action d'un attaquant dans le réseau . Ce qui provoque la déconnexion d'un groupe de noeuds dans le réseau . De plus, le noeud malveillant coopère pour créer des incohérences dans le protocole de routage.

- ***Ressources limitées***

  En fonction de leur taille, les drones peuvent avoir des capacités de calcul et de mémoire limitées. Cette dernière peut être exploitée par des attaquants pour épuiser les ressources. Par ailleurs, l'introduction des mécanismes de sécurité dans le réseau pour se prémunir des attaques peut diminuer la performance du réseau en augmentant la charge des microprocesseurs . Il y a donc des compromis à trouver entre la fiabilité du réseau de communication et le choix d'une solution de sécurité.

2.3.2 Attaques existantes dans les réseaux FANETs

Il existe des catégories différentes de ces attaques, cela par rapport aux différentes couches du modèle TCP-IP, telles que l'attaque matérielle, l'attaque sans fil, l'usurpation de capteur, l'attaque par déni de service, l'attaque par déni de service distribué, ect.

- **Attaque matérielle**

  Les attaques s'exécutant sur la couche physique concernent les matériels utilisés, il y a un accès direct aux composants du pilote automatique du drone par l'attaquant. Pour cette raison, l'attaquant cible les données stockées à bord par le pilote automatique. Il est possible que l'attaquant installe des composants supplémentaires qui peuvent entraîner la corruption du flux de données de ces réseaux. Typiquement, les attaques observées à ce niveau sont :Intervention, brouillage, perturbation de trafic l'écoute illicite, et l'attaque jamming [36].

  – *Attaque jamming (brouillage) :*Dans cette attaque, l'attaquant perturbe le canal de communication dans FANETs en utilisant un signal fortement alimenté avec une fréquence équivalente. Il s'agit de l'attaque la plus dangereuse pour les applications de sécurité, car elle ne suit pas l'alerte de sécurité valide. Pour toute attaque de brouillage réussie, en effectuant une action, le brouilleur peut bloquer le signal utile dans le même délai de survenance d'un événement.

- **Attaques sans fil**

  les canaux de communication sans fil sont utilisés par l'attaquant pour collecter ou modifier des données stockées à bord. Un attaquant peut obtenir un contrôle complet

sur les systèmes UAV lors de la présence de ce type d'attaque dans le cas où la connaissance du protocole de communication est connue de l'utilisateur ;tout comme les données présentes à bord peuvent être mises en mémoire tampon. L'attaquant peut mener les attaques depuis des endroits éloignés, ce qui est un problème très préoccupant [13].

- **Attaques par déni de service (Dos)**

  Ce type d'attaques au niveau de la couche de liaison,les attaques à ce niveau sont diverses et variées [34]. Cela peut concerner,l'épuisement des ressources ou la capacité du canal de transmission par des attaques de déni de service(DOS).Se sont un type d'attaque qui sont causées par les initiés et les étrangers du réseau et fournissent un réseau qui n'est pas disponible pour les vrais utilisateurs. Cela se fait en inondant le canal de contrôle avec une grande quantité de messages générés naturellement et en arrêtant ainsi la connexion. on a aussi :

  – Attaque par déni de service distribué : DDOS est plus nocif que l'attaque DOS car il est de manière distribuée, autrement dit de différents types de lieux sont utilisés par l'attaquant pour lancer l'attaque. DDOS est possible entre UAV à UAV. Son objectif principal est de ralentir et bloquer le réseau.

- **Usurpation de capteur**

  Sur la base de l'environnement entourant le réseau, les attaques d'usurpation de capteur sont dirigées vers les capteurs embarqués. Avec l'aide des canaux GPS, les fausses données peuvent être envoyées via les canaux GPS par l'attaquant.

- **Attaques liées aux protocoles de routage**

  Ce type d'attaques est au niveau de la couche réseau, et les différentes attaques liées seront étudiées dans le prochain chapitre.

On a cité quelques types particuliers des attaques, bien que il existe d'autres qui n'ont pas été mentionné.

2.3.3 Conséquences des attaques sur les réseaux FANETs

La particularité de l'intérêt de l'utilisation des UAVs vient du fait de leur capacité énorme à s'adapter à des environnements dynamiques et à réaliser différents types de tâches, mais tout de même ils ne peuvent s'échapper des effets que les attaques engendrent [38]

- **Modification de la topologie du réseau**

  elle est atteinte en invalidant des liens valides (usurpation d'identité) par l'exclusion des nœuds légitimes et incluant des nœuds malveillants.

- **Menace de performance et de fiabilité du réseau**

  les performances d'un réseau sont liées à plusieurs critères. L'injection/suppression de faux messages, ou en rejouant des messages non à jour sont parmi les conséquences des attaques qui diminuent la qualité de service.

- **Divulgation d'informations de charge utile**

  lorsque la route qui est utilisée est corrompue, Cela veut dire qu'un attaquant est arrivé à rompre le mécanisme de sécurité mis en place. Il est donc nécessaire d'ajouter une brique de sécurité qui vienne assurer la confidentialité des données.

- **Divulgation des informations de routage**

  la révélation des coordonnées de routage est atteinte en interceptant ou en analysant les trafics de routage échangés sur le médium sans fil.

2.3.4 Solutions existantes aux attaques dans les réseaux FANETs

Il existe une variété de solutions proposées aux attaques, en utilisant différents mécanismes et technologies pour empêcher les scénarios de menaces. Ci-dessous nous décrivons un ensemble de solutions pour ces dernières :

- **Solutions pour les attaques par déni de service**

  Il y a de différentes approches de détection de déni de service ont été proposées . La plupart d'entre elles se focalisent sur la détection de manipulation de backoff en appliquant des mécanismes de mesure de confiance entre les noeuds ; autrement chaque noeud surveille la valeur de la variable backoff de son voisin. La formation de cette chaîne permet d'évaluer la variation de la performance du réseau durant la communication.

- **Solutions pour les attaques d'usurpation de capteur**

  Pour ces types d'attaques, les systèmes de détection d'intrusion (IDS) sont des systèmes capables de déceler les attaques. Ils utilisent différents mécanismes pour déceler les attaques parmi : les signatures et la recherche de motif (détection d'anomalie)

- **Autres solutions**

  Ci-dessous nous ajoutons d'autres en générale, par rapport aux autres couches :

  - **Compromis de performance :** sur tous les niveaux des drone, lors de la mise en œuvre de solutions de sécurité, nous devons évaluer les performances du système de drone (les coûts de communication, les coûts de calcul, les frais généraux de stockage et l'énergie) Cependant, l'ajout d'une couche de sécurité supplémentaire pour chaque niveau sans tenir compte des paramètres susmentionnés de performances.
  - **Les technologies émergentes :** Il y a eu une utilisation extensive des technologies émergentes pour sécuriser les UAVs : intelligence artificielle, technologie Blockchain, SDN et Fog Computing. Ces technologies sont appliquées dans diverses applications civiles. Par exemple, l'architecture distribuée de la technologie Blockchain ajoute une couche de sécurité supplémentaire au niveau de la communication. Avec les contrats intelligents, les fonctions de hachage cryptographique pour stocker les données sous forme de chaîne de blocs et les mécanismes de consensus, il devient difficile pour l'adversaire de falsifier la communication des drones.
  - **Analyse du comportement de l'attaquant :** Cela aide à étudier le comportement post-attaque des drones en cas de types particuliers d'attaques. Afin de déterminer quels types d'attaques étaient les plus efficaces, diverses études ont également été réalisées à travers lesquelles les différents scénarios ont été compris et utilisés selon les besoins.

2.4 Conclusion

Ce chapitre nous a permis de présenter les notions de bases de sécurité (les requis et les primitives crypthographiques), la vulnérabilité des réseaux FANETs, quelques types d'attaques et leur solutions. Les études reliant aux réseaux FANETs présentent un énorme progrès, mais malheureusement il y a bien des embarras existants à résoudre, notamment dans le routage et la sécurité liés aux protocoles de routage que nous verrons dans le chapitre suivant.

Chapitre 3

Protocoles de routage sécurisés dans les FANETs

3.1 Introduction

Le routage est une fonction primordiale dans les MANETs, où les nœuds du réseau coopèrent pour la découverte et la maintenance des routes. Le type d'informations échangées durant cette phase sont cibles pour les attaquants, de ce fait, l'utilisation des algorithmes de routage est indispensable pour assurer la sécurité des informations échangées et déterminer les chemins optimales pour les paquets d'une source à une destination donnée, en utilisant différents métriques pouvant être le nombre de sauts, le coût, le délai, etc.
Dans ce chapitre, nous allons voir dans une première partie le routage dans les réseaux Ad hoc et ses protocoles associés, ensuite le routage dans les FANETs, les critères de conception d'un protocole de routage, les différentes classes de schémas de routage, une section dédié aux attaques liées à la couche réseau enfin les protocoles de routage sécurisés contre l'attaque WORMHOLE.

3.2 Routage dans les réseaux Ad hoc

Afin d'acheminer une information entre un ou plusieurs nœuds intermédiaires, ces derniers coopèrent entre eux pour transmettre les données jusqu'à leurs destinations. De ce fait, les protocoles de routage sont responsables de choisir la meilleure route vers la destination, qui optimise les critères de la qualité du service (délai, débit bande passante gigue,..etc). Ces protocoles peuvent être classifiés en trois grandes catégories [23] :

3.2.1 Protocoles de routage proactifs

Les protocoles de routages proactifs sont des protocoles qui tentent de maintenir à jour dans chaque nœud les informations de routage concernant tous les autres nœuds du réseau [8].
Les routes sont sauvegardées même si elles ne sont pas utilisées. Le sauvegarde des chemins

de routage est assuré par un échange continu de messages de mise à jours des chemins. Exemple de protocoles de ce type : OLSR, DSDV, ect [6].

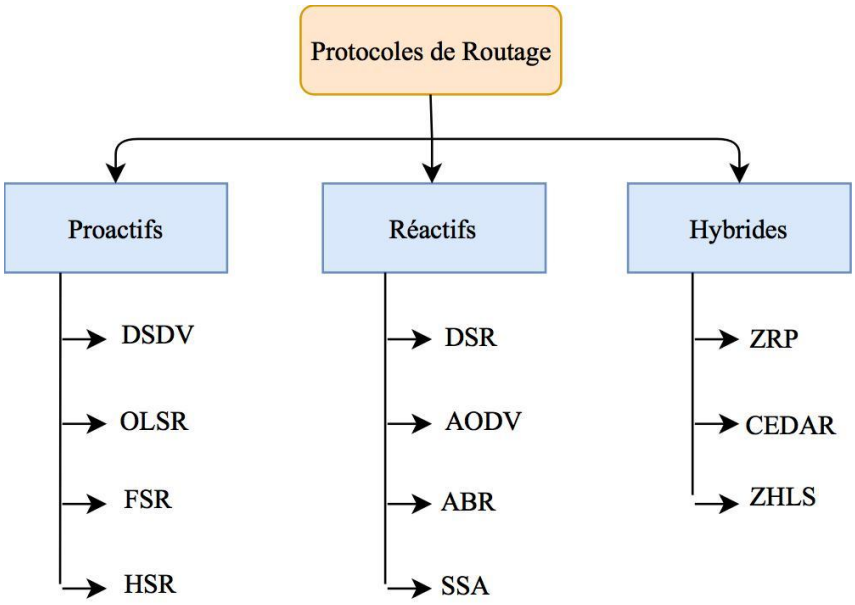

FIG. 3.1 : *Classification des protocoles de routage dans les réseaux Ad hoc.*

3.2.2 Protocoles de routage réactifs

Un protocole réactif est un protocole qui construit une table de routage lorsqu'un nœud en effectue la demande. Il détermine le chemin à prendre pour accéder à un nœud du réseau lorsqu'on lui demande.Il économise la bande passante et l'information sur la topologie est plus fraîche. C'est une approche plus adaptée aux environnements Ad hoc. On peut cité les protocoles : AODV, DSR, ect[26].

3.2.3 Protocoles de routage hybrides

En plus des protocoles de routage proactifs et réactifs, il existe une famille de protocole de routage qui est une combinaison des deux précédents et appelée protocole hybride. Il utilisent le protocole proactif pour apprendre à chaque nœud son voisinage à un, deux ou trois sauts, d'où le requis des routes dans le voisinage. Le protocole hybride fait appel aux techniques des protocoles réactifs pour chercher des routes. Quelques types de protocoles de cette catégorie :ZRP, ZHLS, ect [21].

3.3 Routage dans les réseaux FANETs

Il existe de nombreux protocoles de routage pour les réseaux Ad hoc, la plupart de ces protocoles ne sont pas directement applicables aux réseaux FANETs. Les UAVs devraient développer ses propres techniques de routage en raison de leur caractéristiques spécifiques et l'environnement dans lequel ils opèrent.

3.3.1 Critères de conception d'un protocole de routage pour les réseaux FANETs

Les exigences de conception du protocole de routage pour les FANETs vont au-delà de celles des réseaux traditionnels tels que MANET et VANET. Celle-ci doit tenir compte des ces propos suivantes [10] :

- **Domaines d'applications**

Les applications de surveillance des données télémétriques environnementales se caractérise par un faible retard de transmission, bande passante faible et de gigue moyenne.

- **Trafic de données**

Le trafic de données de détection en temps réel, de stockage et retransmission,... Chaque type a ses particularités concernant la bande passante, le délai de retard et la gigue.

- **Exigences des QoS**

Les protocoles désignés doivent tenir compte des exigences de sécurité car ils transmettront des messages critiques tels que la détection, la commande, le contrôle et le trafic du protocole de routage.

- **Adaptation aux caractéristiques des FANETs**

Le protocole de routage conçu pour FANET doit être adaptable aux liaisons intermittentes, aux changements de topologie fréquents, au partitionnement du réseau et à la mobilité des drones.

- **Amélioration de la fiabilité**

Les limitations de puissance, l'équilibrage de charge, la gestion des liaisons instables, le retrait et l'ajout fréquents d'UAVs, les fonctionnalités de mobilité et la localisation des UAVs doivent être pris en compte pour améliorer la fiabilité des communications des UAVs vers la station au sol ainsi qu'entre les UAVs.

3.3.2 Classes des protocoles de routage des réseaux FANETs

Les protocoles de routage peuvent être classés dans différents groupes selon leurs caractéristiques en fonction de leur objectif, comportement, ou bien ses techniques utilisées. La figure **??** montre la taxonomie des protocoles de routage dans FANETs en quatre grandes classes : topologie, positon géographique, hybride, enfin bio-inspiré. Dans ce qui suit, nous donnons quelques concepts de ses schémas.

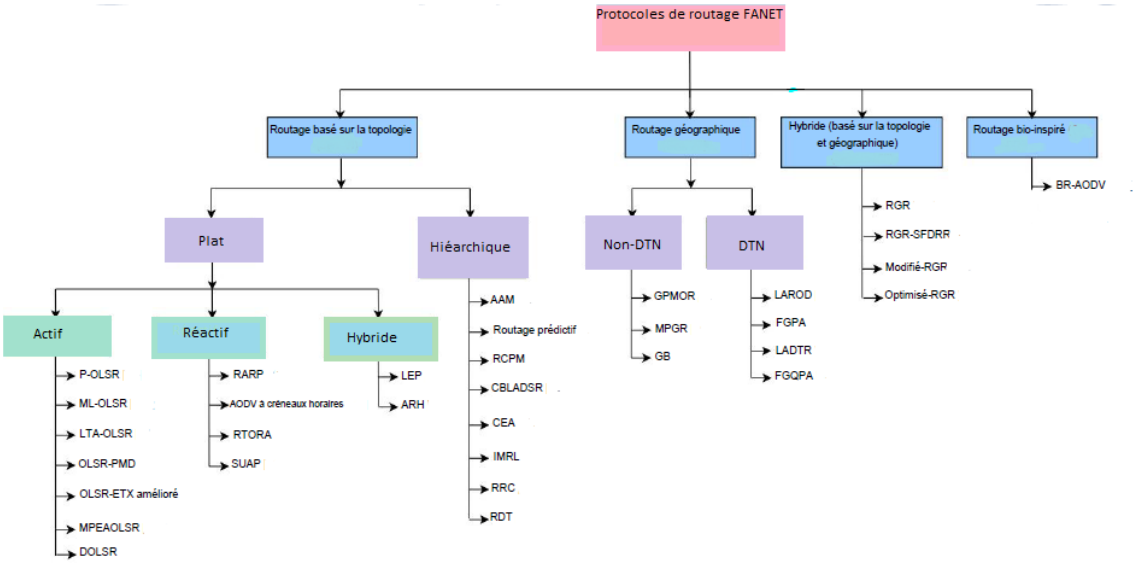

FIG. 3.2 : *Classification des protocoles de routages dans les réseaux FANETs. [10]*

1. **Routage basé sur la topologie**

Dans cette classe de protocole, les informations de topologie des nœuds du réseau sont utilisés pour envoyer des paquets. Un chemin de routage correct de la source à la destination est requis avant que le transfert de données commence, on distingue deux sous-classes :

• **Plat :** Un algorithme de routage plat utilise une approche d'adressage plat, autrement les UAVs participent au routage à rôles égaux . Selon la manière dont les informations de routage sont obtenues et conservées par les UAVs dans le réseau, les schémas de routage plats sont classés en schémas de routage proactifs, réactifs et hybrides.
• **Hiérarchique :** Les protocoles de routage hiérarchiques (basés sur des clusters) sont plus avantageux en termes de flexibilité et d'évolutivité. Ils conviennent aux FANETs de grande taille constitués de drones hétérogènes avec des capacités de communication, d'énergie, de stockage, de traitement et des tailles différentes.

Les stratégies et algorithmes de clustering ont des objectifs :

- Une durée de vie maximale d'UAVs.
- Une stabilité maxilame de cluster.
- Une élection de tête de cluster minimale.

Les protocoles hiérarchiques se trouvent face aux défis de l'énergie limitée embarquée et la grande mobilité des UAVs dans la plupart des scénarios d'application des FANETs [11].

2. **Routage basé géographique**

   Cette classe de protocoles de routage est basée sur la connaissance des positions géographiques, que chaque noeud est capable de définir à l'aide du GPS. Pour calculer la position et la destination, le nœud peut utiliser les service de localisation tel que le Reactive Location Service (RLS) , le Grid Location Service pour les réseaux hautement dynamiques tels que les FANETs. Les routage le plus pertinents dans cette catégorie sont [18] :

   • **Les réseaux tolérant aux délais (DTN) :** Les protocoles de routage dans les réseaux tolérant aux délais emploient des techniques gourmandes de protection, où chaque nœud sélectionne le nœud gardien suivant la plus proche destination parmi ses voisins pour transmettre les paquets. Cependant, ce mécanisme de transfert échoue dans les situations où un le nœud ayant un paquet de données à transmettre n'a pas de nœud voisin proche de la destination prévue autre que le nœud même. Cette approche des DTN est destinées à traiter les problèmes techniques des réseaux souffrant de pannes de connexions telles que les FANETs en raison du degré élevé de mobilité des nœuds.
   • **Les réseaux non tolérant aux délais (Non DTN) :** Ce type de protocoles fonctionne plus efficacement sur des réseaux bien connectés où la densité de nœuds est relativement élevée parce qu'elle ne tient pas compte du problème de déconnexion. L'objectif principal de ces protocoles est pour transmettre des paquets de données au récepteur aussi rapidement que possible en utilisant la technique multi-sauts via le nœud dans le cas où le récepteur n'est pas dans la portée de transmission de l'expéditeur[18][10].

3. **Routage Hybride (basé sur la géographie et la topologie)**

   Cette approche combine entre des schémas de routage basés sur la topologie en particulier les routages plat, et les techniques de routage géographique. Ils sont plus évolutifs et adaptés aux scénarios d'application FANET hautement dynamiques et volumineux. Cependant, dans le schémas de routage géographique gourmand, les performances du réseau diminuent en raison de la difficulté à trouver un prochain UAV transitaire approprié, en particulier si les UAV se déplacent de manière aléatoire sans planification de chemin préalable. De plus, la densité du réseau dépend non seulement du nombre de drones formant des FANETs, mais sera également affectée par les différents scénarios d'applications. Dans cette famille de protocole on a RGR, Optimisé RGR,...

4. **Routage Bio-inspiré**

   Ces algorithmes de routage sont inspirés des comportements biologiques des insectes, tels que les abeilles, les fourmi, l'essaim de particules...ect. Il constitue un support important pour différentes problématiques dans les FANETs, et notamment pour établir communications entre drones. De nombreux protocoles de routage bio-inspirés ont été proposés dans la littérature en essayant de résoudre différents types de problèmes de routage tel-que : APAR, BR-AODV,...

3.4 Routage avec sécurité dans les réseaux FANETs

Le routage est un procédé dans lequel un dispositif trouve un meilleur chemin entre la source et le réseau de destination. Pour garantir ses services il utilise une variété de protocoles précautionné de techniques de sécurité qui vont faire face aux attaques pouvant se produire durant les différentes phases de routage [9].

3.4.1 Attaques liées au routages des réseaux FANETs

Ces attaques peuvent être divisées en deux sous catégories :

- La première c'est les attaques pouvant être exécutées durant la phase de découverte de routes, un émetteur cherche à la base une route vers sa destination en diffusant des requêtes. Il s'agit dans ce cas d'une diffusion par inondation pour atteindre tous les noeuds actifs (attaque blackhole, attaque wormhole, attaque rushing,..).
- La deuxième catégorie c'est des attaques pouvant être exécutées durant la phase de maintenance La phase de maintenance de route consiste en l'échange de messages de contrôle entre les nœuds participants à la formation de la topologie. Les attaques exécutées durant cette étape consistent en la diffusion de faux paquets conduisant à la reconfiguration des routes déjà établies (rejeu, byzantine,..).

1. **Attaque blackhole (trou noir)**

   Un problème de trou noir signifie qu'un nœud malveillant utilise le protocole de routage pour prétendre d'être le chemin le plus court vers le nœud de destination, mais abandonne et ne transmet pas ces paquets à leurs voisins ou destination. La figure suivante représente l'attaque blackhole avec un nœud [16].

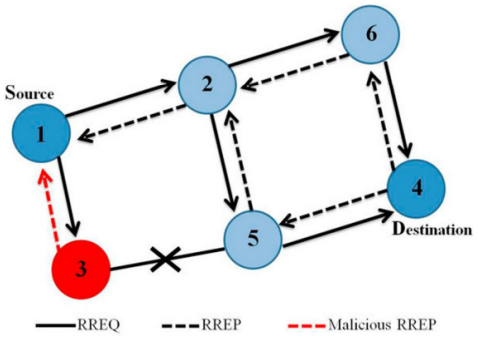

FIG. 3.3 : *Attaque blackhole* .

2. **Attaque rushing (précipitée)**

   Le principe de base de l'attaque rushing consiste à prioriser la première requête et les autres sont mises en attente ou ignorées. L'objectif de l'attaquant est donc de faire passer ses requêtes avant celles des autres nœuds en se plaçant géographiquement entre deux nœuds communicants [28].

3. **Attaque playback (rejeu)**

   Elle est une forme d'attaque réseau dans laquelle une transmission est malicieusement répétée par un attaquant qui a intercepté la transmission. Il permet aux nœuds adverses d'enregistrer des messages de contrôle légitimes, de les stocker et de les retransmettre ultérieurement.

4. **Attaque byzantine**

   Cette-ci vise à créer des boucles de routage, et à acheminer des paquets via des chemins non optimaux, ou à abandonner sélectivement des paquets. Ces actions entraînent la perturbation ou la dégradation des services de routage[25].

5. **Attaque Man-in-the-Middle**

   Le principe de cet attaque est que tous les messages échangés entre les drones et les stations de bases transitent par l'attaquant qui croient que leur communication entre eux est via une connexion privée alors qu'en réalité, l'ensemble de la communication est contrôlée par l'attaquant.

6. **Grayhole (trou gris)**

   Elle peut être considérée comme une variation de l'attaque blackhole, avec une base différente dans laquelle les paquets sont supprimés de manière sélective. Dans l'attaque du trou gris, les paquets provenant d'une source unique ou d'une adresse IP sont ignoré et les autres paquets de données restants sont transmis .

7. **Attaque wormhole (Trou de ver)**

   Dans cette menace, un attaquant reçoit des paquets dans un point du réseau, puis les encapsule vers un autre attaquant, pour les réintroduire dans le réseau. Dans ce genre d'attaque, les adversaires coopèrent pour fournir un canal à basse latence, pour la communication, en utilisant une radio pour communiquer avec une puissance plus élevée et des liens à longue portée. Ceci favorise les nœuds voisins à acheminer leurs données à travers ses attaquants [24].

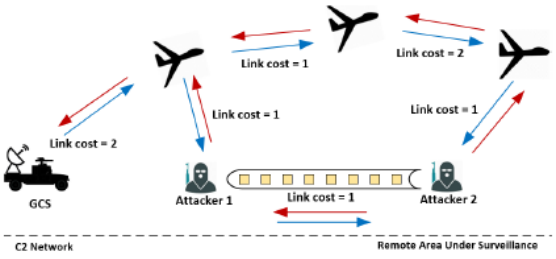

FIG. 3.4 : *Attaque WORMHOLE.*

3.4.2 Classification des menaces basés sur les exigences de sécurité

Les réseaux FANETs nécessitent que la sécurité durant le routage soit mise en avant comme un aspect crucial. Ainsi, le tableau suivant 3.2 répertorie les attaques potentielles du routage, ciblant la stabilité des services de sécurité [13] :

Attaques	Phase	Services
Blackhole	Découverte	Diponibilité
Rushing	Découverte	Diponibilité Authentification
Playback	Maintenance	Disponibilité Authentification
Byzantine	Maintenance	Disponibilité Confidentialité
MIMA	Découverte	Disponibilité Authentification Confidentialité Intégrité
Grayhole	Découverte	Disponibilité
Wormhole	Découverte	Disponibilité Confidentialité Intégrité Authentification

Tab. 3.1 : Classification des attaques selon les exigences de sécurité

Le tableau nous montre au niveau de quelle phase les attaques se produisent, par exemple l'attaque Byzantine est dans la phase de découverte. De plus il nous précise les services de sécurité que ces attaques affectent, l'attaque Grayhole atteint le service de disponibilité.

3.5 Protocoles de routages dans FANET contre l'attaque WORMHOLE

La défense contre les attaques de trous de ver se font à l'aide de plusieurs mécanismes comme : les laisses de paquets, les antennes directionnelles, les pare-feu, les systèmes de détection d'intrusion et les preuves de collocation.
Les protocoles suivants ont les caractéristiques pour éviter et résoudre les attaques de trou de ver :

1. **Protocol DOLSR**

   C'est un protocole de routage proactif, Directional Optimized Link State Routing est basé sur le protocole OLSR conçu pour les réseaux Ad hoc, mais avec l'aménagement

d'une antenne directionnelle il est recommandé dans les FANETs. . Ces antennes avec une technique heuristique sont utilisées pour minimiser le nombre de MPR, réduire le nombre total de messages de contrôle à échanger dans les FANETs et servent aussi à protéger le système des attaques WORMHOLE.

Ce protocole présente les avantages suivants :

- Le gain de temps lors d'une demande de route.
- Amélioration du taux de livraison de paquets.
- Réduit les latences.

Néanmoins, La taille des tables de routage croit linéairement en fonction du nombre de noeud, se qui implique le gaspiallage de la capacité du réseau.

2. **Protocole AODV-SEC**

Le AODV-SEC (Ad hoc On-demand Distance Vector- Secure) est une version sécurisée de l'AODV : protocole de routage réactif pour les réseaux Ad hoc, et il est appliqué aux réseaux FANETs. Les clés publiques et les certificats sont utilisés comme ancre et outil de confiance dans ce protocole. Le SAODV est utilisé contre l'attaque **WORMEHOLE** , cela en assurant :

- Sécurité du processus de découverte tout au long des transmissions avec les paquets de contrôle échangés.
- Authentifications des nœuds communicants.
- Élimination des nœuds non fiables.

D'autre part, SEC-AODV consomme une grande partie de la bande passante et un grand nombre de paquets est généré quand une rupture de lien se produit.

Dans l'exemple illustré à la figure suivante, la découverte de route dans AODV-SEC est similaire à celle du AODV classique. Cependant, la différence réside dans l'utilisation d'un nouveau type de paquets de contrôle appelé RREQ-ACK qui est envoyé avant le paquet RREP. Les paquets RREQ-ACK sont tous deux utilisés pour éviter faux paquets RREP et de valider leur réception.

3. **Protocole SRPU**

Protocole de routage sécurisé pour les drones (Secure Routing Protocol for UAVs) est un protocole de routage basé sur le protocole AODV et il est dédié aux réseaux FANETs. Dans cet algorithme, le modèle de développement piloté (**MDD** :Model Driven Development) est utilisé pour rendre l'échange de paquets plus sécurisés. C'est un protocole réactif (c'est-à-dire qu'un processus de découverte n'est exécuté que lorsqu'une communication est nécessaire), où plusieurs mécanismes adoptés sont inspirés du protocole AODV-SEC[11].
Ce protocole :

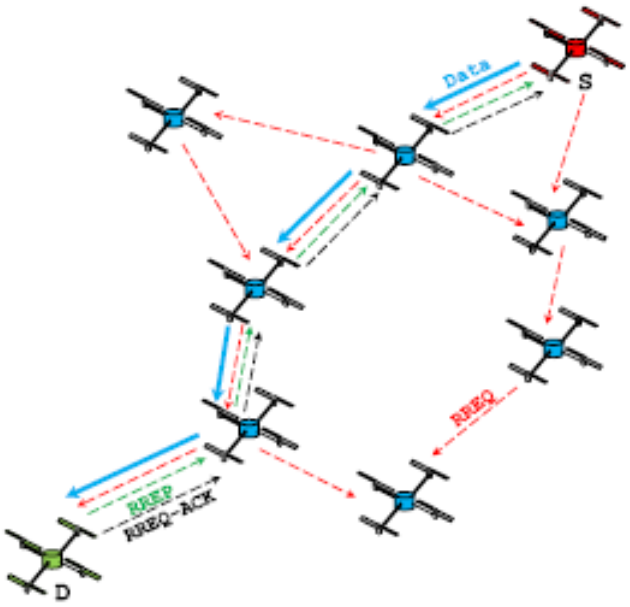

FIG. 3.5 : *Mécanisme du protocole AODV-SEC.*

renforce les mécanismes de sécurité notamment les attaques internes.

- Il introduit plus de frais de mise œuvre
- Des latences d'un niveau non négligeable.

4. **Protocole SAUAV**

Les drones qui se comportent mal peuvent être retiré des réseaux FANETs en utilisant un agent sécurisé pour les UAVs (Secure Agent UAV), il se déroule en deux phases pour protéger le réseau :

- Durant la première phase, un drone malveillant est identifié puis supprimé à l'aide d'un ensemble de règles.
- Durant la deuxième phase un processus de négociation est mis en œuvre avec un agent mobile. Cet agent permet aux drones de découvrir les voisins et fournit aux drones du même réseau les informations nécessaires sur les nœuds malveillants[12].

SAUAV fournit une énergie résiduelle élevée et une faible livraison de faux paquets. Par ailleurs, il consomme plus de bande passante.

5. **Protocole SUANET**

Le protocole de routage sécurisé dédié aux réseaux Ad hoc de drones (Secure UAV Ad-hoc NETwork), utilise une stratégie de gestion de clés, qui sont déployées entre les UAVs afin de prendre en charge le service d'identité, d'authentification et d'intégrité. En outre, le processus de routage est sécurisé pour s'assurer que tous les

drones impliqués sont authentifiés et peuvent établir efficacement le chemin de routage le plus court vers la destination cible. Les liaisons entre drones sont maintenues et sécurisées à l'aide de plusieurs paramètres de sécurité pour éviter toute attaque (**WORMHOLE**) et supprimer tout drone malveillant.
Ce protocole fournit :

- Authentification des drones impliquées dans le réseau.
- Établissement d'un chemin de routage optimal

En outre, ce protocole consomme une grande partie des recours de la bande passante[19].

6. **Protocole PASER**

Les véhicules aériens sans pilote (UAV) à basse altitude combinés aux réseaux maillés WLAN (WMN) ont facilité l'émergence d'applications aéroportées assistées par réseau. PASER (Position-Aware, Secure, and Efficient mesh Routing) est un protocole de routage sécurisé est indispensable pour rendre possible le déploiement de UAV-WMN[15].

Il est dédié aux attaquantes externes(Exemple Wormhole),internes, de relecture et temporelles, mais la taille et le poids limités des drones limite quelques applications de ce protocole. En outre, PASER offre :

- L'authentification et la fraîcheur des messages.
- Un schéma de gestion dynamique des clés plus confidentes et qui garantissent la détection ou la révocation des nœuds.

7. **Protocole ARAN**

Le protocole d'analyse de rouage authentifié (Analyzing security of Authenticated Routing Protocol) est un protocole réactif. Le nœud source produit un package appelé RREQ dans lequel il détermine le nœud source et cible. Il envoie ces paquets par inondation. En recevant un package RREQ de chaque nœud, s'il ne connaît pas la route cible, il ajoute son nom à la liste des packages et le diffuse. Bien qu'il s'agisse d'une bonne méthode et certainement applicable, notamment la diffusion des packets pour préciser le chemin vers la destination mais il :

- Augmente la charge du réseau ce qui provoque des latences et des déconnexions de transmissions.
- Utilise une bande passante élevée, ce qui entraîne la charge du transport.

8. **Protocole ARIADNE**

Le protocole sécurisé à la demande pour les réseaux ad hoc (A Secure On-Demand Routing Protocol for Ad Hoc Networks) est un protocole augmenté du DSR et adéquat pour les FANETs. Dans Ariadne, chaque nœud qui reçoit RREQ est authentifié ainsi que le message joignant le code d'authentification. Dans ce code, le propre ID individuel et la fonction Hash du message précédent sont utilisés. ARIADNE offre :

- La sécurisé dans des circonstances particulières contre les attaques de trous de ver.
- Assure l'authentification des messages jusqu'à leur destination.

Mais le principal problème est la nécessité d'échanger la clé entre les nœuds du réseau pour effectuer le chiffrement avant que le protocole ne commence à fonctionner.

9. **Protocole SEAD**

Dans le routage sécurisé pour les réseaux Ad hoc(A Secure Routing Protocol for Mobile Ad Hoc Networks), une table de routage est disponible dans chaque nœud dans laquelle se trouve une liste de tous les cibles dans le réseau. Chaque tableau enregistre l'adresse des cibles, la distance connue et les nœuds voisins qui peuvent être atteints à cette cible par le prochain saut. Le premier développement de sécurité de SEAD convenable pour les FANETs est qu'il :
• Ajoute un numéro consécutif à chaque élément de la table de routage. Ces numéros consécutifs évitent de créer des boucles, qui peuvent entraîné des mise à jour de routes hors du temps.
• Ce protocole utilise une série hachée unidirectionnelle pour fournir des fonctions de chiffrement de sécurité. Cependant, il dispose d'une grande quantité de latences [2].

10. **Protocole SUAP**

Protocole sécurisé pour les UAVs est un protocole adressé aux réseaux FANETs, basé sur le protocole réactif AODV. Les paquets de contrôles échangés dans les champs statiques (par exemple, des adresses IP) et dynamiques (par exemple, le nombre de sauts) sont protégés à l'aide de signatures numériques et les chaînes de hachage, respectivement. Ces paquets sont déchiffrés par les drones qui les reçoivent sur la base d'une clé publique de l'expéditeur. De plus. L'objectif du SUAP permet d'assurer à la fois la détection et la prévention contre les attaques de trous de ver. Mais tout comme autre protocole de routage, il se trouve face à quelques lacunes :

- Il ne fournit pas une méthode efficace pour faire face à la grande mobilité des drones.
- Il ne garantie pas la sécurité des échanges de paquets lors des différentes déconnexions.
- SUAP consomme une grande partie de la bande passante[10].

3.5.1 Comparaison entre les protocoles de routage sécurisés étudiés

Pour assurer la confidentialité et la sécurité des données lors transmission, il est important d'inclure des mécanismes de sécurité dans les protocoles de routage pour se protéger

des actes malveillants et assurer les exigences de QoS.

Protocole	MR	PD	BP	LT	EE	DF	SC
DOLSR	Haut	Non	Faible	Moyen	Non	Non	Non
S-AODV	Moyen	Oui	Haut	Haut	Non	Non	Oui
SRPU	Moyen	Oui	Moyen	Haut	Non	Non	Oui
SAUAV	Moyen	Oui	Haut	Faible	Non	Non	Oui
SUANET	Moyen	Oui	Haut	Moyen	Non	Non	Oui
PASER	Moyen	Oui	Moyen	Moyen	Non	Non	Oui
ARAN	Moyen	Oui	Haut	Haut	Non	Oui	Non
ARIADNE	Moyen	Oui	Moyen	Haut	Non	Oui	Non
SEAD	Faible	Non	Faible	Haut	Non	Non	Non
SUAP	Haut	Oui	Haut	Moyen	Non	Non	Oui

Tab. 3.2 : Comparaisons des protocoles étudiés dans les FANETs

Le tableau 3.2 compare les protocoles de routage pour éviter contraire l'attaque WORMHOLE, par rapport à plusieurs critères :

✓ **Mémoire requise (MR) :** Le calcul des délais de transmissions et le traitement des données exige un niveau de mémoire. Les protocoles DOLSR et SUAP ont un haut niveau, tandis que les autres protocole varient entre une mémoire faible et moyenne.

✓ **Processus de découverte (PD) :** Il est nécessaire de découvrir les positions futures des relais afin de sélectionner l'adéquat. Dans le cas général, la demande de route (RREQ) est diffusée pour retrouver tous les chemins possibles vers le drone de destination . Les protocoles DOLSR et SEAD ne fournissent pas la diffusion des paquets (RREQ).

✓ **Bande passante (BP) :** Les paquets de contrôle dans un protocole de routage devraient être minimum que possible,cails consomment la largeur de bande passante et peuvent causer des collisions avec des paquets de données,diminution de débit. Les protocoles S-AODV, SAUAV, SUANET, ARAN et SUAP consomment plus de ressources en bande passante. Cela est dû à l'utilisation des entêtes de sécurité.

✓ **Latence (LT) :** Les latences sont une des mesure de la quantité de temps nécessaire à un paquet pour traverser le chemin réseau de l'émetteur au destinataire. plus avantageux d'avoir de faibles latences, notamment dans le protocole SAUAV.

✓ **Efficacité d'énergie (EE) :** Comme on le sait déjà, les drones ont une capacité énergétique restreinte avec piles, et les protocoles étudié souffrent de cette obstacle.

✓ **Diffusion (DF) :** Pour assurer la transmission de données, le paquet de données est diffusés sur le réseau depuis le drone source jusqu'à l'UAV de destination. Cependant, la diffusion peut introduire un surcoût sur le réseau et provoquer une tempête de diffusion. Uniquement les protocoles ARAN et ARIADNE qui se trouvent face à ce propos.

✓ **Sécurisé (SC) :** Les différents mécanismes de sécurité sont utilisés pour protéger

les liens existants dans le réseau et détecter les drones malveillants. SEC-AODV,SRPU, SAUAV, SUANET, PASER et SUAP garantissent les requis de sécurité.

Bien que les schémas de routage existants proposés pour la détection et la prévention de l'attaque WORMHOLE dans les FANETs montrent des résultats prometteurs sur la base de différentes critères. Mais il y a quelques algorithmes qui garantissent pas les caractéristiques idéals pour augmenter l'efficacité contre les attaques de trou de ver. Le tableau précédant 3.2, en se basant sur les différents indices nous a aidé à opter pour le choix du protocole SUAP.

3.6 Conclusion

Le routage est un élément essentiel de l'architecture de communication des FANETs, car les UAVs doivent relayer les trafics de contrôle et de données entre eux vers les GBS. Dans notre chapitre, on a pu examiné les classification de routage (réseau Ad hoc et FANET), les critères qui doivent être prises en compte avant le choix et la conception des schémas de routage ainsi que les attaques qui peuvent croiser cette partie. L'attaque Wormhole, est dangereuse, cela dû à sa difficulté de détection et de prévention. On a proposé quelques protocole qui aident à empêcher et prévenir de cet critique, et depuis une comparaison entre ses schémas on a opté pour le protocole SUAP. SUAP offre des mécanismes de sécurité qui peuvent détecter l'attaque WORMHOLE, mias tout comme autre protocole, il souffre de certains faiblesse. Le prochain chapitre sera dédié à l'étude formelle de ce protocole ainsi que des améliorations à proposer pour faire face à ses inconvénients.

Chapitre 4

Mécanisme de sécurité contre l'attaque WORMHOLE

4.1 Introduction

La gestion de l'acheminement des données consiste à assurer une stratégie de routage qui garantie la connexion entre n'importe quelle paire de nœuds appartenant au réseau. Elle doit prendre en considération les changements de la topologie ainsi que les autres caractéristiques du réseau (bande passante, nombre de liens, ressources du réseau,etc). Plusieurs protocoles de routage pour les réseaux FANETs ont été développés, certains ont été présenté dans le chapitre précédent pour améliorer la sécurité des schémas de routage. Le résultat de la comparaison entre ses derniers nous a guidé vers le protocole SUAP. C'est un protocole de routage sécurisé conçu pour les attaques de WORMHOLE et garanti la qualité de service dans les réseaux FANETs.
Dans ce chapitre, nous détaillerons ce protocole (fonctionnement, avantages, inconvénients, sécurité), les mécanismes de sécurité contre l'attaque WORMHOLE, puis nous présentons un protocole TEE-SUAP, qui est une amélioration du protocole SUAP et nous l'implémentons sur le logiciel CPN-Tools.

4.2 Fonctionnement du SUAP

En plus de trouver un chemin fiable et efficace entre les drones dans les réseaux FANETs et dans un délai raisonnable, le protocole d'acheminement doit être sécurisé lors de la transmission des messages décisifs tels que la détection, la commande et le contrôle, et routage du trafic de protocole. Les auteurs de [30] ont présenté le protocole SUAP (Secure UAV Ad Hoc Routing Protocol) pour les FANETs, qui se base sur le le protocole réactif SAODV (Secure Ad hoc On Demand Distance Vector). De plus, il intègre les laisses géographiques, les chaînes de hachage et les outils de cryptographie.
Le protocole SUAP se compose de deux parties :

- Partie routage.
- Partie sécurité.

4.2.1 Partie routage dans SUAP

Cette partie est consacrée pour gérer le routage, comme le montre la figure 4.1, elle est divisé en séquences de tâches :

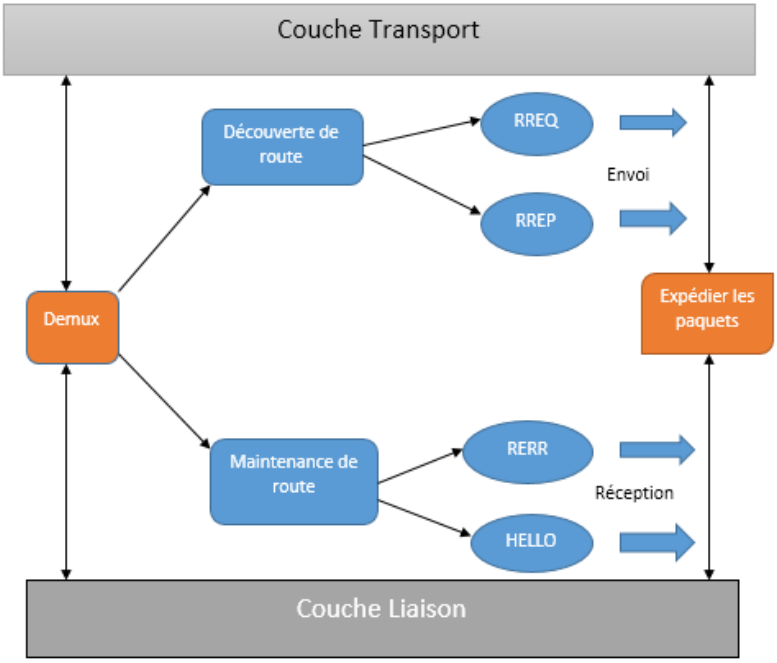

FIG. 4.1 : *La partie routage dans SUAP.*

- **Un démultiplexeur (Demux)**

  Un démultiplexeur réceptionne les paquets des couches voisines (couche liaison et transport), ensuite il vérifie l'existence d'un chemin. S'il existe une route il l'envoie vers le bloc de maintenance de route ; sinon, le paquet est transféré vers le bloc de découverte de route.

- **Découverte de routes**

  Cette partie doit vérifier la nature du paquet qu'elle reçoit (un message HELLO, requête). Chaque nœud du réseau découvre ses voisins en diffusant une série de messages, pour faire un choix du prochain saut. SUAP hérite les paquets de contrôle de SAODV, en garantissant leur authentification pour éviter la génération de faux paquets :

  ✠ *Message Route Request et Reply (RREQ/RRER) :* lorsqu'un nœud a des données à transmettre au nœud de destination, il vérifie sa table de routage. S'il existe une route active vers cette destination, il transmet directement les données. S'il y a pas d'itinéraire actif pour la destination, il diffuse alors le message RREQ. Chaque fois qu'un nœud envoie un nouveau message, SUAP utilise un nouveau

numéro de séquence qui augmente de manière monotone.
Le format de l'extension du message RREQ et RRER sont similaires.

- **Maintenance de routes**

  Cette partie aussi se charge de vérifie la nature des paquets qu'elle reçoit (réponse ou erreur).

  ✠ *Message HELLO* : ce paquet est diffusé en incluant les informations sur la longueur, latitude et altitude, vers les nœuds voisins à un saut, pour connaître le prochain voisin. Le nœud ayant reçu le paquet HELLO calcule la distance relative qui le sépare de l'émetteur pour savoir si le paquet n'a pas emprunté une route illégitime.

  ✠ *Message d'erreur de route (RERR)* : comme son nom l'indique, c'est un message qui signale une erreur. Ce message est diffusé dans deux cas :

  – Si un nœud reçoit un paquet de messages(RREQ/RRER) que sa table de routage ne contient pas.
  – La perte d'un lien sur une route active.

  Lorsque un nœud est déconnecté du réseau,les autres nœuds doivent le déclarer en informant ces voisins (en étendant son identité : adresse IP). Ce dernier sera effacé de la table de routage.

- **Expédier les paquets**

  Ce bloc fait la mise à jour de tout les champs des paquets en fonction de leur état, c'est à dire les envoyer vers les couche destinataire voisines

4.2.2 Partie sécurité

Ce modèle peut être expliqué comme suit : Une fois qu'un paquet est reçu, le paquet bloque identifie et supprime les paquets routés sans extensions de sécurité. C'est la première étape de filtrage pour éliminer les paquets non autorisés. Cette suppression est implémenté par le bloc Packet Denier.
Ensuite, on procède à la désencapsulation du paquet sécurisé, en Bloc extracteur de contenu. Dans ce bloc, nous allons effectuer diverses vérifications Coffre-fort de paquet. Tout d'abord, appelez le bloc de test de trou de ver (les calculs de distance et de fonction de hachage dans la section suivante). Bloc de trou de ver test : identifie le type de paquet (découverte de route ou maintenance) et s'applique donc le traitement est approprié. Si le testeur de trous de ver échoue, le paquet sera rejeté par le module de rejet de paquets.

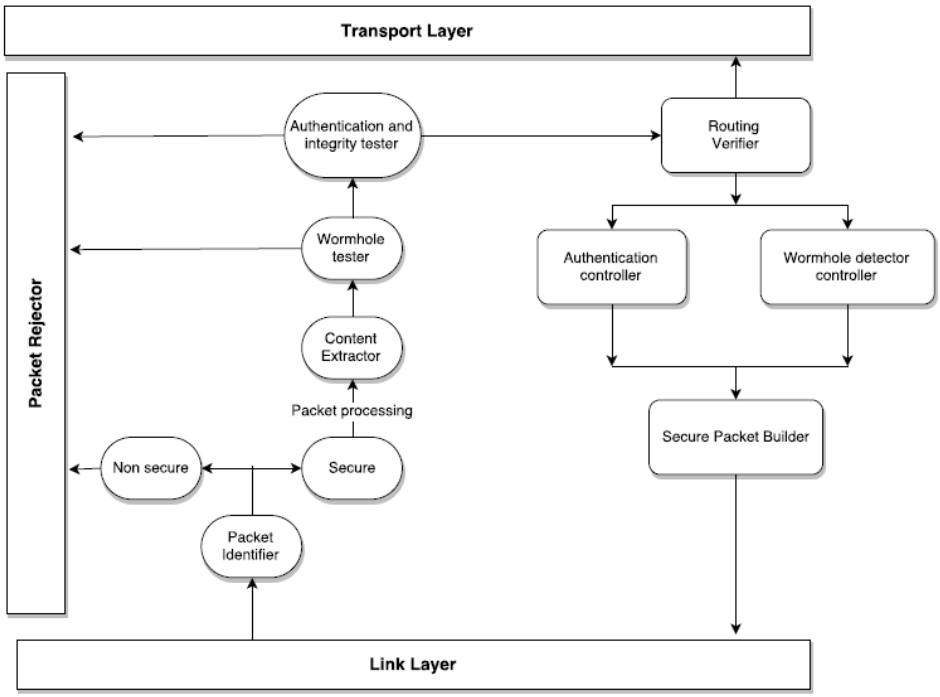

FIG. 4.2 : *La partie sécurité dans SUAP.*

4.2.3 Vulnérabilité de SUAP

Pour garantir la sécurité dans SUAP, il faut qu'il contrarie les attaques actives et les comportements égoïstes des nœuds malveillants. De plus, il doit éviter la dégradation de performance causée par les mécanismes de sécurité.
Mais, quand les attaquants coopèrent entre eux et utilisent des techniques puissantes, SUAP échoue de garantir un routage sécurisé et ne parvient pas à faire face aux attaques (Wormhole, Blackhole). Les manipulations pouvant affectées un message de routage sont :

- Effacer un paquet ;
- Modifier un ou plusieurs champs du paquet avant de le retransmettre ;
- Fabriquer une réponse à la réception d'une demande de route RREQ ;
- Fabriquer activement des paquets de routage sans même avoir reçu de messages de routage.

Cela apportera des changement sensible au réseau, et peuvent arriver à :

- Paralysation totale du réseau dans le cas de génération de plusieurs tunnels de trou de ver.
- Blocage,crises du trafic et l'extension avec les autres nœuds dans le cas de la présence d'un trou noir.
- Modification de la topologie du réseau, et divulgation des informations de routage
- Dégradation de la performance du réseau.

4.3 Protocole SUAP pour contrer l'attaque WORMHOLE

Le protocole étudié est exposé aux attaques de trous de ver, celle-ci qui se déroule en enregistrant un paquet à une position ou un tunnel, à travers un réseau privé haut débit d'un autre poste.
Les résolutions que fait SUAP pour contrarier l'attaque WORMHOLE et l'arrêter sont décrites comme suit :

- La corrélation du nombre de sauts avec la distance parcourue est calculé en utilisant les laisses géographiques. Chaque drone doit préserver sa connectivité locale avec ses voisins directs. Lors de l'envoi de paquets, chaque drone intègre les informations de sa position. Les champs de message et les informations de localisation sont signés pour empêcher toute altération malveillante.

- Les attaquants peuvent obtenir les paquets diffusés et cela dû à la caractéristique du diffusion des réseaux sans fil. Afin de résoudre ce problème, SUAP met en œuvre un ensemble de techniques de vérification qui inspectent la corrélation de la distance parcourue par le paquet avec le nombre de sauts.

4.3.1 Modèle de l'attaque WORMHOLE contre SUAP

Les mécanismes du protocole SUAP se rapportent à ceux de protocole SAODV. SUAP utilise les paquets de messages améliorés et la découverte des route sécurisées, de plus, il inclut quelques fonctionnalités spécifiques de sécurité, notamment pour contrer l'attaque WORMHOLE.

1. ***Les laisses géographiques***

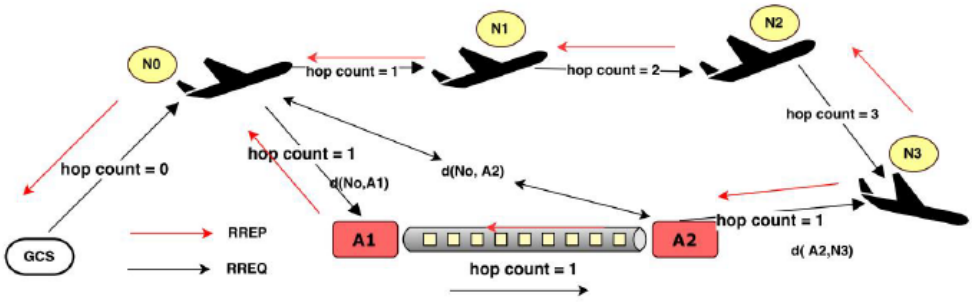

FIG. 4.3 : *Aperçu de l'attaque de trou de ver dans les FANETs.*

Les champs de message de routage qui ne changent pas tout au long du réseau. Par exemple, adresse IP de destination, adresse IP source, (y compris la position géographique) sont signées.
Les auteur dans [31] pour élucider leur proposition et l'étude, ils ont considéré la figure 4.3 et la notation dans le tableau 4.1 .

Abréviation	**Représentation en français**	**Représentation en anglais**
n	Nombre de noeuds dans le réseau	Number of nodes in the network
hc	Nombre de sauts	Hop count
D_{max}	Distance maximale d'un saut	One hop distance maximum
R_{ij}	Distance entre les noeuds i et j	Distance between nodes i and j
$c(i,j)$	État de connectivité entre le noeud i et le noeud j	connectivity state between node i and node j
$d(No, A1)$	Distance entre la première cible et le premier attaquant	Distance between the first target and the first attacker
$d(A1, A2)$	Distance entre les deux attaquants	Distance between the two attackers
$d(No, A2)$	Distance entre la première cible et le deuxième attaquant	Distance between the first target and the second attacker
$d(A2, D)$	Distance entre la deuxième cible et le deuxième attaquant	Distance between the second target and the second attacker
T	La distance totale de l'itinéraire légitime	The total distance of the legitimate route
D_w	La longueur totale du chemin à travers le lien du trou de ver	The total length of the path through the wormhole link

Tab. 4.1 : Les notations et leur correspondances [31]

Dans SUAP, On a la distance qui sépare deux nœuds i et j est inférieure ou égale à la distance maximale d'un saut ($\forall i, j \in [0, n] : R_{ij} \leq D_{max}$), et la connectivité entre deux nœuds légitimes peut être exprimée comme suit :

$$c(i,j) = \begin{cases} 1 & if \quad R_{i,j} \leq D_{max} \\ 0 & if \quad R_{i,j} > D_{max} \end{cases}$$

La présence de lien de trou de ver modifie une condition de l'équation précédente à :

$$c(i,j) = \begin{cases} 1 & if \quad R_{i,j} \leq D_{max} \\ 1 & if \quad R_{i,j} > D_{max} \end{cases}$$

On traduit les distances entre les attaquants et les nœuds comme suit :

$$\begin{gathered} \mathrm{d(No\,;A1)} \leq D_{max} \\ \mathrm{d(A2;N3)} \leq D_{max} \\ \mathrm{d(No\,;A2)} > \mathrm{D}_{max} \\ \mathrm{d(A1;N3)} > \mathrm{D}_{max} \end{gathered}$$

Il en résulte que :

$$d(No; A1)^2 + d(A1; A2)^2 > D_{max}^2$$

Alors :

$$d(A1; A2) > D_{max} - (No; A1)$$

De l'équation de connectivité dans la présence d'un trou de ver :

$$\begin{gathered} D_w = d(A1; A2) + d(No; A1) + d(A2; N3) \\ D_v > D_{max} \end{gathered}$$

On sait que :

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

- Lorsque le nœud $N0$ envoie le paquet, $To = R_{o1}$ qui correspond à $hc = 1$ avec $x \in$N ;
- Lorsque le nœud N1 envoie le paquet, $T1 = To + R_{12}$qui correspond à $hc = 2$;
- Lorsque le nœud N2 envoie le paquet, $T2 = T1 + R_{23}$ qui correspond à $hc = 3$;

$$\frac{T}{D_{max}} - 1 \leq hc < \frac{T}{D_{max}} + 1$$

T	**Nombre de sauts** hc **(Hop count)**
$0 \prec T_0 \preceq D_{max}$	0
$\mathrm{D}_{max} \prec T_1 \preceq 2D_{max}$	1
...	...
$(n-1)D_{max} \prec T_{n-1} \preceq (n+1)D_{max}$	(n-1)

TAB. 4.2 : Les paquets de signatures de vérification dans SUAP

On peut comparer la valeur du nombre de sauts présente dans le paquet et la valeur du nombre de sauts calculée sur la distance parcourue en suivant la valeur correspondante décrite dans le tableau 4.2 et l'inégalité précédente. S'il y a une différence,

le lien WORMHOLE est détecté, et le paquet est rejeté. Dans le cas contraire, le lien est considéré comme libre de trou de ver et le processus de vérification de signature commence.

2. ***Vérification de signatures***

La figure **4.3** montre une illustration de l'attaque WORMHOLE. Dans cet figure, les noeuds $N0$ et $N3$ sont amenés à croire qu'ils sont voisins. L'attaquant $A1$ transfère tous les paquets du noeud $N0$ directement vers $N3$, via un deuxième attaquant $A2$. Le noeud $N3$ croit donc que $N0$ est un voisin. Tous les paquets de contrôle (Hello, RREQ, RREP, RERR) sont alors transmis le long de cette route.

Le tableau 4.3 résume les messages de demande d'informations échangés entre les drones :

Champs	**Valeur**
64	Paquet de requête
Signature	La signature de tout les champs non modifiables
$Hashnew$	$Hashnew = [CurrentNode, NextNode, Hashhold]$ $CurrentNode$: est l'adresse du nœud envoyant le paquet de requête. Il peut s'agir de sa clé publique ou de son adresse IP $NextNode$: Le nœud suivant est la clé publique ou l'adresse IP du nœud suivant. $Hashhold$: est l'élément de chaîne précédent reçu du nœud précédent
$Hashold$	C'est l'élément de chaîne précédent reçu du nœud précédent. Lors de la réception de paquets, les nœuds changer la valeur de $HashnewenHashold$
$Hopcount$ (nombre de sauts)	Le nombre réel de sauts du paquet. C'est le nombre de fois que le hachage est effectué

Tab. 4.3 : Les paquets de signatures de vérification dans SUAP

Le nœud source ajoute sa propre adresse et celle du nœud suivant à la chaîne de hachage appelé $Hashnew$. Il comprend également le $Hashold$ (qui est le précédent $Hashnew$) dans le paquet. Lorsqu'un nœud intermédiaire affirme la réception d'une requête, il vérifie sa signature et vérifier sa chaîne de hachage. Il recalcule la chaîne $Hash$ avec $H[previousnode, MyIPAddress, Hashold]$ et vérifiez s'il a le même résultat que celui inclut dans le paquet.
La chaîne de hachage sera calculer suivants les étapes suivantes :

Le nœud GCS exécute ces opérations :

- Sélectionnez une fonction de hachage H ;

- Compter $Oldhash = H(seed)$, $seed$ étant une valeur sélectionnée aléatoirement par l'expéditeur ;
- Calculer $Hashnew = H(GCS, N0, Oldhash)$, $N0$ est l'adresse du nœud suivant ;
- Calculer le message de S à $N0$: $[64, H, signature, Hashnew, Oldhash]$

Lorsque le nœud $N0$, reçoit le paquet, il traite les étapes suivantes :

- Vérification de l'intégrité en calculant $Hashverifier = H[previousnode, actualnode, Oldhash$ et vérifie le résultat par rapport à $Hashnew$.
- Si $Hashverifier = H[GCS, N0, Oldhash] \neq Hashnew$, cela signifie que le paquet a été transmis via un tunnel de WORMHOLE. Le paquet est alors rejeté.
- Attribuez le nouveau $Oldhash = Hashnew$;
- Calculer le nouveau $Hashnew = H[N1, N2, Oldhash]$

L'opération est répétée jusqu'à ce que le paquet atteigne la destination. Le même mécanisme est également utilisé pour la réponse au paquet (RREP). En ce qui concerne la valeur exacte de nombre de sauts, elle peut être déduite du nombre de fois que le hachage a été utilisé pour la vérification[29].

4.3.2 Avantages et Inconvénients du SUAP

Parmi les avantages que le protocole SUAP présente, on cite :

- SUAP convient pour les applications ayant des exigences de sécurité élevées(Exemple applications militaire : surveillance automatisée).
- SUAP fournit les services de sécurité (Authentification, intégrité, la non-répudiation)
- Efficacité en protection des routes de découverte au long du processus.
- SUAP contient des fonctionnalités améliorées contre les attaque de trou de Ver.

De plus, il présente plusieurs inconvénients, on peut mentionner ce qui suit :

- Il ne fournit pas un mécanisme robuste pour se remettre face aux déconnexions fréquentes entre les drones en raison de leur grande mobilité.
- Le délai pour rétablir une nouvelle route après les pannes n'est pas négligeable, en particulier pour les applications en temps réel (la capture vidéo, télésurveillance, etc).
- SUAP ne prend pas en considération le type de drone capturé comme attaquant, qui peut avoir un fort potentiel d'attaque .
- Les frais informatique généreux de déploiement.
- Faible en scalabilité.

4.3.3 Discussion

Les problèmes de sécurité doivent être pris en compte lors de la conception des protocoles de routage, le protocole de routage sécurisé SUAP garantit l'authentification des champs mutables et non mutables, avec des approches de sécurité pour contrer les variantes des attaquants, notamment l'attaque WORMHOLE.

- Cependant, la latence élevée due à la procédure d'exploration d'itinéraires est le principal inconvénient de ce protocole de routage.
  Car si le délai moyen de transition des paquets augmente, les attaquants de WORMHOLE, créent des de faux transitions avec des latences moins élevées pour tromper les nœuds

- De plus, l'inondation des paquets RREQ et RERR dans les phases de découverte et de maintenance des routes, respectivement, entraîne une congestion, une consommation d'énergie et une bande passante élevées, ce qui est favorisant aux attaquants WORMHOLE, car lors de la diffusion d'une quantité des messages de contrôles, ils peuvent falsifier certains de ces paquets et les renvoyer.

- D'une autre part, le temps perdu dans le rétablissement des routes après les déconnexions permet à ces attaquants de créer d'autres tunnels avec les nœuds du reste de réseau.

Pour cela, des améliorations plus approfondies pour SUAP sont nécessaires, assurer la sécurité et empêcher le réseau de l'attaque WORMHOLE, ainsi que les autres attaques pouvant se générer (déni de service, paquet HELLO,…) et garantir une meilleure QoS. En prenant en considération l'énergie limitée à bord des drones et de la bande passante, on peut ajuster le schéma de routage pour avoir un protocole sécurisé et économe en énergie et en bande passante.
De plus, on peut attribuer un mécanisme adaptative de créneaux horaires qui peut ajuster sa fenêtre temporelle pendant le trajet des phases de découverte et de maintenance.

4.4 Protcole TEE-SUAP Amélioré de SUAP

En s'inspirant des travaux [32] et [33], nous présentons une amélioration du protocole SUAP, qui est TEE-SUAP (Time Energy Efficient Secur UAV Ad hoc Protocol), il hérite les mêmes étapes de SUAP, de plus il est efficace en énergie et réduit le taux de perte de paquets, dans le but est d'éviter ou de contrarier l'attaque WORMHOLE.

4.4.1 Nouvelles techniques améliorées

L'idée pour notre protocole amélioré est d'inclure un procédé pour vérifier l'énergie des nœuds. Comme on le sait déjà la complexité de la sélection du meilleur chemin augmente de manière exponentielle, en particulier lorsque les nœuds sont mobiles et peuvent

se déplacer dans les trois directions (3D : axes x, y et z) comme dans les réseaux FANETs. Les informations qu'on obtient sur la localisation des nœuds et leur énergie se trouvant dans les charges utiles (capteurs) nous aident à calculer un équilibrage de l'énergie.

1. **Équilibrage de l'énergie** :

   Une mesure importante pour évaluer les performances du protocole de routage est l'équilibrage de l'énergie . Son objectif est de conserver l'énergie des drones et d'améliorer la durée de vie globale du réseau, la qualité de service (QoS) en limitant le transfert de paquets qui est un état avantageux pour les attaquants de WORMHOLE. Nous décrivons l'équilibrage d'énergie dans les deux parties du routage :

   - **Découverte de routes :** comme on a vu déjà, le processus de découverte commence lorsque le nœud source diffuse les paquets RREQ pour envoyer ses données . Tous les nœuds à l'exception du nœud source et le nœud destination, vont résoudre le problème d'énergie en ajoutant au paquets RREQ/RRER la métrique de l'énergie pour transmettre un paquet, qui se calcule par l'équation suivante :

   $$E_{ep} = \frac{T_p + S_U}{B}$$

   Où :

   - E_{ep} : énergie de pour transmettre un paquet.
   - T_p :la puissance de transmission de paquet ;
   - S_u :la taille des paquets ou chaque type a une taille unique ;
   - B :la bande passante ;

   - **La maintenance de route :** dans cette phase, on trouve l'équilibrage d'énergie en ajoutant au paquet HELLO la métrique de l'équilibrage d'énergie se calculant comme suit :

     L'énergie efficace E_e doit être inférieur ou égale au seuil de l'énergie de chaque drone :

     $$E_e \leq LE - hold$$

     Où :

     $$LE - hold = \frac{ie}{e^{\frac{n}{ie}} * \frac{a+b}{c}}$$

     Tel que :

     - $LE - hold$: le seuil de l'énergie.
     - n : le nombre total de noeuds
     - ie : l'énergie initiale des noeuds
     - a : taille de la topologie en dimension x
     - b : taille de la topologie en dimension y
     - c : taille de la topologie en dimension z

Le nœud ne relaie les paquets de données que si son énergie résiduelle est supérieure à un certain seuil $LE-hold$, c'est-à-dire que chaque nœud surveille la diminution de son énergie résiduelle.

2. **Créneau horaire :**
L'utilisation des créneaux de temps pour coordonner la communication entre les nœuds dans un protocole de routage améliore la qualité de service (QoS) de la communication des nœuds en minimisant les pertes de paquets de données. De plus, il ajuste la durée de la tranche de temps pour qu'elle soit suffisamment grande pour faciliter le transfert du plus gros paquet et du message de routage de différentes exigences tout en évitant les collisions de paquets, ce qui maximise la fiabilité de la communication[37].

Le créneau T_{ls} nous permet de savoir le temps de transmissions des paquets entre deux voisins, comme suit :

$$T_{ls} = C * D * P * \beta$$

où :

- T_{ls} : créneau horaire ;
- C : période de backoff ;
- D : la longueur de paquet de contrôle ;
- P : débit de données ;
- β : le décalage maximal, obtenu des données de GPS.

Alors que le nombre des messages qui peuvent être envoyés est diminué par cette méthode, et se traduit par un taux de transfert de données inférieur, le débit de communication soutenu par le protocole d'acheminement par créneaux temporels est suffisant pour maintenir le vol en formation. L'important de cette technique est quelle assure la fiabilité de la communication, l'évolutivité des nœuds dans la formation. Cela en évitant les dangers d'un paquet de navigation abandonné qui peut potentiellement perturber ou modifier la mission, et facilite les attaques de trou de ver.

4.4.2 Impact de TEE-SUAP sur l'attaque WORMHOLE

Le protocole SUAP est conçu pour la détection et la prévention de l'attaque WORMHOLE, de même, pour le protocole proposé TEE-SUAP qui ajoute en plus des laisses géographiques et les chaînes de hachage, l'équilibrage de l'énergie et le temps de transmission des paquets entre les nœuds. Dans les paragraphes suivants, nous citons quelques effets de ses deux technique sur l'attaque WORMHOLE :

1. L'efficacité énergétique :

- Limiter la diffusion des paquets de contrôle(RREQ, RRER, etc), ce qui réduira les risques de génération de faux paquets et le blocage dans les parties de routage.
- Vérifier le nombre de sauts et la distance parcourue, ainsi on vérifie l'énergie du nœud légitime, pour éviter les drones malveillants.
- La coopération entre les nœuds du réseau permet d'optimiser l'énergie de calcul et de consommation dans la communication, ce qui augmentera le bon fonctionnement du protocole.
- Contrôler la gamme de transmission et regrouper efficacement le réseau contre les attaquants.

2. Le créneau horaire :

- Ajuster les tranches de temps pour différents paquets de contrôles, cela nous aide à la reconnaissances des nœds du réseau.
- Éviter la perte de paquets, car en connaissant le temps de transmission nous permettra de contrôler plus la réception et la transmission des messages de contrôle dans le réseau, et de supprimer les faux paquets.
- Les nœuds sont évolutifs dans la formation du chemin et de nœds.
- Éviter le danger des paquets abandonnés, et qui sont risque la perturbation et la modification du réseau.
- Détecter les défaillances et mettre à jour la table de routage.
- Améliorer la qualité de service (QoS) de la communication des nœuds et un bon fonctionnement de routage.

4.4.3 Modélisation de TEE-SUAP par le CPN-Tools

Dans la section précédente, nous avons proposé la version améliorée du protocole SUAP qui est TEE-SUAP avec deux nouvelle technique : l'efficacité énergitique et le créneau horaire.
Dans cette partie, nous modélisons le paquet RREQ de la phase de découverte de route avec un modèle de réseau de pétri coloré, par la suite nous l'implémentons sur le logiciel CPN-Tools, qui nous donnera à la fin le nombre moyen de paquets RREQ sécurisés diffusés après vérification [28].

1. **Modèle proposé de réseau de petri coloré**

   Le modèle que nous avons proposé décrit la vérification de l'énergie dans la phase de découverte de route (paquet RREQ). Dans ce modèle, nous avons supposé que cette vérification passe plusieurs sous étapes, pour éliminer les paquets malveillants. Ceci se traduit par les transitions et les places montrées dans le modèle de la figure 4.4.
   Le réseau de petri coloré se compose de quatre place(P1, P2, P3, P4) et de trois transitions (T1,T2, T3)

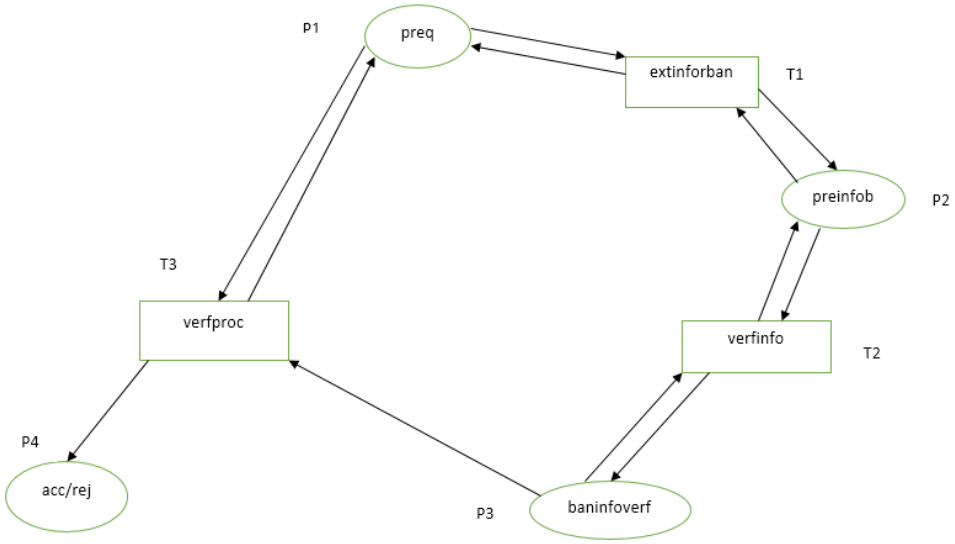

FIG. 4.4 : *Modèle proposé de réseau de Petri coloré*

2. **Modèle proposé implémenté sous CPN-Tools** Notre modèle a été implémenté sous Color Petri Networks-Tools (CPN-Tools), ce qui donne la figure 4.5 suivante. Dans la partie index nous avons déclaré quatre différentes places :

   - **preq :** c'est la place représentant le paquet RREQ (closet RQ), avec la variable i.
   - **preinfob :** c'est la place chargé de prise d'informations du paquet RREQ (closet EIC), avec la variable eic.
   - **baninfoverf :** c'est la place illustrant la vérification d'informations (closet BIV), avec la variable biv.
   - **acc/rej :** c'est la place de nombre de paquets acceptés à être transférer (closet AR), avec la variable rq.

   De plus, on a la description de ses trois transitions utilisées :

   - **extinforban :** cette transition extrait les informations du paquet concernant l'énergie du nœud.
   - **verfinfo :** cette transition vérifie les informations obtenu du nœud.
   - **verfproc :** cette transition vérifie le processus d'acceptation et de rejet de paquet RREQ.

3. **Résultat de simulation** Après l'insertion des place et transitions, de plus les variables associées aux places, nous enregistrons le travail dans un dossier, puis nous utilisons la fenêtre de simulation qui se trouve sur l'interface de logiciel CPN-Tools pour commencer la simulation en précisant les nombres de steps, dans notre cas 100steps, 1000steps, 10000steps.

   D'après la figure 4.6 obtenue lors de la vérification avec CPN tools, on constate que le nombre de nœuds dans SCC Graph est 1, car uniquement le nœud AR (closet AR) qui nous donne le résultat final, qui est le nombre de paquets sécurisés diffusés.

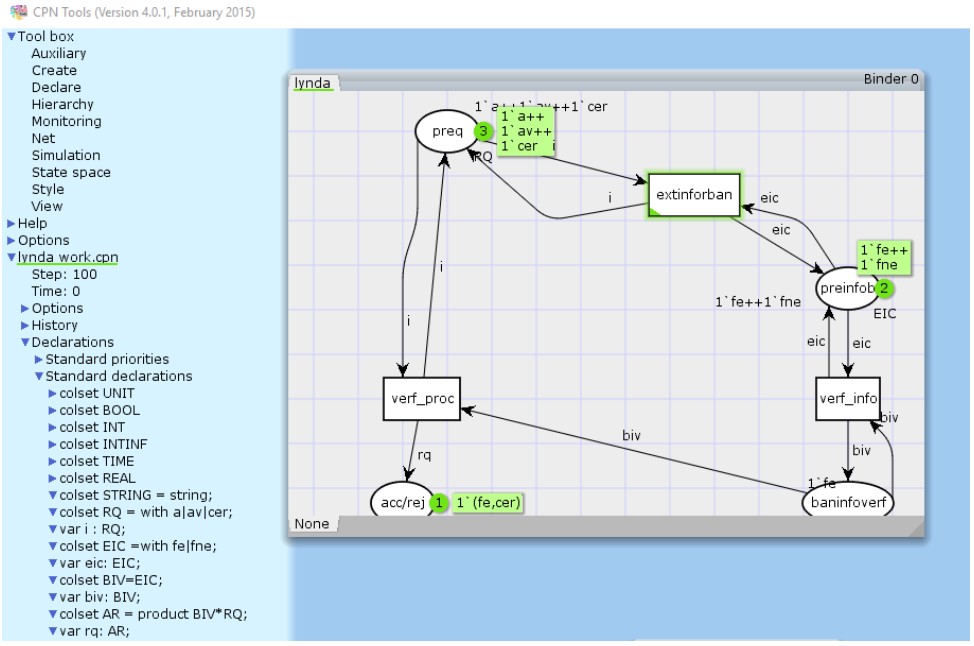

FIG. 4.5 : *Modèle proposé sur CPN-Tools*

```
CPN Tools state space report for:
/cygdrive/C/Users/PC/Desktop/projet fin d/lynda work.cpn
Report generated: Tue Jul 12 00:34:07 2022


 Statistics
------------------------------------------------------------------------

  State Space
     Nodes:  1
     Arcs:   6
     Secs:   0
     Status: Full

  Scc Graph
     Nodes:  1
     Arcs:   0
     Secs:   0


 Boundedness Properties
------------------------------------------------------------------------
```

FIG. 4.6 : *Rapport -1- de simulation*

Dans la figure 4.7 montre que le système envoie toujours des paquets RREQ (fe,av). Les transitions de notre modèle sont dans tous les cas franchissables alors elles sont vivantes, par conséquent notre modèle est vivant (réinitialisable). Le modèle est validé (vivacité, bornitude, réversibilité).

Nombre de simulation	Nombre moyen de paquet envoyé
100	0,980198
1000	0,995005
10000	0,999900

TAB. 4.4 : Nombre moyen de paquet RREQ envoyés

```
------------------------------------------------------------------------

  Best Integer Bounds
                              Upper      Lower
     lynda'acc 1              1          1
     lynda'baninfoverf 1      0          0
     lynda'preinfob 1         2          2
     lynda'preq 1             3          3

  Best Upper Multi-set Bounds
     lynda'acc 1         1`(fe,av)
     lynda'baninfoverf 1 empty
     lynda'preinfob 1    1`fe++
1`fne
     lynda'preq 1        1`a++
1`av++
1`cer

  Best Lower Multi-set Bounds
     lynda'acc 1         1`(fe,av)
     lynda'baninfoverf 1 empty
     lynda'preinfob 1    1`fe++
1`fne
     lynda'preq 1        1`a++
1`av++
1`cer


 Home Properties
------------------------------------------------------------------------
```

FIG. 4.7 : *Rapport -2- de simulation*

```
  Home Markings
     All


 Liveness Properties
------------------------------------------------------------------------

  Dead Markings
     None

  Dead Transition Instances
     lynda'verf_info 1
     lynda'verf_proc 1

  Live Transition Instances
     lynda'extinforban 1


 Fairness Properties
------------------------------------------------------------------------

  Impartial Transition Instances
     lynda'extinforban 1

  Fair Transition Instances
     lynda'verf_info 1
     lynda'verf_proc 1

  Just Transition Instances
     None

  Transition Instances with No Fairness
     None
```

FIG. 4.8 : *Rapport -3- de simulation*

La simulation sur le CPN-tools pour le modèle proposé commence de 100 step - 10000 step, et nous avons résumé les résultats dans le tableau 4.4. Il nous montre le nombre moyen des paquets RREQ sécurisé et optimisé en énergie dans le système qui sont envoyés dans la phase de découverte, le nombre augmente, cela indique qu'il y a une diffusion des paquets de contrôle RREQ, et l'augmentation est à valeurs faible à cause de rejet des paquets vulnérables.

4.5 Conclusion

Dans le présent chapitre, nous avons vu le protocole de routage SUAP, ses fonctionnalités, son effet sur l'attaque WORMHOLE, ses avantages et ses inconvénients. Puis on a présenté une amélioration pour ce protocole qui est TEE-SUAP : Time Energy Efficient, qui inclut une technique de calcul de l'énergie et un créneau pour coordonner la communication entre les nœuds.
Enfin, nous avons modélisé le paquet RREQ, qui vérifie l'énergie du nœud pendant le processus de découverte de route, ainsi que le créneau horaire, avec un réseau de petri coloré. On l'a implémenté sur le logiciel CPN-Tools. Les résultas montrent le nombre moyen de paquets diffusé qui augmente faiblement, ceci indique le rejet de la partie des paquets d'attaquants de WORMHOLE.

Conclusion générale

Les avantages que les FANETs peuvent offrir sont incommensurables (extension de couverture, application dans les communications d'urgence, recherche et sauvetage, agriculture, etc.). Lors du déploiement de ses réseaux, il est essentiel de pouvoir trouver le chemin qu'un paquet doit suivre pour atteindre sa destination. En raison des changements constants caractéristiques de la topologie, la sélection du protocole de routage est une tâche cruciale pour un déploiement efficace et un fonctionnement réussi.

Cependant, les FANETs sont cible en raison de leur utilisation dans des applications critiques, leur nature déploiement et des protocoles de routage coopératif qu'ils utilisent. De plus, ils nécessitent de nouvelles solutions de sécurité ou l'adaptation des solutions de sécurité existantes des réseaux mobiles ad hoc (MANET), car ils ont une mobilité beaucoup plus élevée que les MANET. Étant donné que la mobilité peut affecter la sécurité de différentes manières, il convient d'abord d'analyser la vulnérabilité des FANETs.

Dans un premier temps, nous avons présenté dans les diverses attaques contre les FANETs, à savoir les attaques de déni de service, usurpation, trou noir,trou de ver (WORMHOLE),... sont analysées.

Puis, nous avons présenté et comparé les protocoles de routage sécurisés dans FANET contre l'attaque WORMHOLE. Par la suite nous avons choisi d'élargir les notions et fonctionnalités du protocole SUAP, et de présenter une amélioration pour ce protocole qui est TEE-SUAP, qui hérite les mêmes étapes de SUAP en ajoutant deux techniques.

- La première, c'est l'ajout de calcul d'énergie dans les deux partie de routage (découverte de route et maintenance de route) inspiré des algorithmes métaheuristiques et des protocole de routage des réseaux de capteurs (WSN).
- La deuxième technique, c'est l'ajout d'un créneau horaire, qui calcule le temps de transsmission des paquets entre deux voisins.

Le protocole TEE-SUAP, rétabli les temps de déconnexions mieux que le protocole SUAP, et ceci grâce au calcul de temps de transmission entre les deux nœuds, limite la diffusions de paquets de contrôles, et préserve l'énergie du système pour assurer son fonctionnement.

Dans une dernière partie de notre travail, nous avons proposé une modélisation du paquet RREQ et la vérification de l'énergie se trouvant dans le nœud avec un réseau de petri coloré, puis nous l'avons implémenté sur le logiciel CPN-TOOLS. Le résultat de la

simulation nous donne le nombre moyen de paquets RREQ sécurisé diffusé qui augumente faiblement et cela dû à la diffusion de faux paquets qui interrompe les transmissions.

Il est à noter que dans un travail futur, nous espérons comparer les deux protocoles SUAP ET TEE-SUAP en conditions réelles. De mêmes, nous souhaitons modéliser tout le protocole TEE-SUAP, ainsi que son évaluation de performance. De plus, amélioré les solutions proposées pour maximiser la prévention contre l'attaque WORMHOLE, et proposer des solutions à bases de d'autres scénarios et algorithmes, en incluant les mécanismes de sécurité afin de rendre la détection plus efficace et performante.

Bibliographie

[1] **B.Ait-salem**, UNIVERSITÉ DE LIMOGES. thèse doctorat : Sécurisation des Réseaux Ad hoc : Systèmes de Confiance et de Détection de Répliques 2011.

[2] **J.A Maxa**, UNIVERSITÉ TOULOUSE 3. Thèse doctorat : Architecture de communication sécurisée d'une flotte de drones 2017.

[3] **T. Abbas Mounir** , UNIVERSITÉ d'Oran. Thèse doctorat : Proposition d'un protocole à économie d'énergie dans un réseau hybride GSM et Ad hoc 2011 .

[4] **A.BERRABAH, H.Saidi** , Université Abou Bakr Belkaid– Tlemcen . Mémoire de fin d'études pour l'obtention du diplôme de Master en Informatique Option : Réseaux et Systèmes Distribués (R.S.D). Sous le thème Balancement de charges dans les réseaux Ad Hoc 2013 .

[5] **N. Chaib**, UNIVERSITE ELHADJ LAKHDER – BATNA. Magister en Informatique .Option : Ingénierie des systèmes informatiques (ISI) : La sécurité des communications dans les réseaux VANET 2011.

[6] **A.Koffi** , École de technologie supérieure UNIVERSITÉ DU Quebéc. Mémoire à l'obtention de la maîtrise avec mémoire en génie concentration, réseaux de télécommunications sous le thème : optimisation d'un réseau ad hoc de véhicules aériens sans pilote (uav) dans un environnement urbain : positionnement des uav à l'aide de l'apprentissage automatique 2021.

[7] **O.z.K Sahingoz, O. K. Sahingoz**, Computer Engineering Department, Turkish Air Force Academy, Istanbul, Turkey. Networking Models in Flying Ad-Hoc Networks (FANETs) : Concepts and Challenges.

[8] **S.Yahi**, UNIVERSITÉ Mouloud Maameri. Mémoire Master 2 sous le thème : Étude et Conception d'une Plate-Forme de Diffusion d'un Bouquet Numérique TV Radio Par Satellite 2011.

[9] **D.Jaye Segui Agron, J.Min Lee, D.Kim**, Kumoh National Institute of Technology, South of Korea. Conférence : Secure Ground Control Station-based Routing Protocol for UAV Networks 2019.

[10] **D.SLakew, U.Sa'ad, N.N Dao, W.Na, and S.Cho**, Article : Routing in Flying Ad Hoc Networks A Comprehensive Survey, University of Canberra 2020.

[11] **M.Bani Yassein and N.Damer**, Jordan University : Flying Ad-Hoc Networks : Routing Protocols, Mobility Models, Issues.

[12] **R.Fotohi , E.Nazemi, F.Aliee**, University, Evin. Article : An Agent Based Self Protective Method to Secure Communication between UAVs in Unmanned Aerial Vehicle Networks.

[13] **S.GOUMIRI, M.Amine RIAHLA et M.HAMADOUCHE**, Security issues in self-organized ad-hoc networks (MANET, VANET, and FANET) : A survey, University of Boumerdes.

[14] **F.Hamad, N.Hussam et O.Rababah**, University of Jordan, Amman, Jordan. Article : Comprehensive Overview of Security and Privacy of Data Transfer, centre canadien de science et éducation 2018.

[15] **Mohamad Sbeiti, Daniel Behnke**, PASER : Secure and Efficient Routing Approach for Airborne Mesh Networks, Germany 2016.

[16] **Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao**, National Ilan University, Taiwan. A survey of blackhole attacks in wireless mobile ad hoc networks 2011.

[17] **O.S.Oubbatia, A.akasb, Z.Fen ,G. Mesut , M.Bachir** , University of Laghouat, United Arab Emirates University, University of Avignon, France, Ottovon-Guericke-University, Germany 2019.

[18] **M.Fahad Khan, K.Alvin Yau, R. Noor ,M.Ali Imran 4**, Sunway University, COMSATS University Islamabad, University of Malaya, University of Glasgow. Routing Schemes in FANETs : A Survey 2019.

[19] **A. Sawalmeh, N,Othman**, Universiti Tenaga, Malaysia. An overview of collision avoidance approaches and network architecture of unmanned aerial vehicles (uavs).

[20] **O.Oubbati , M.Atiquzzaman, MD. Hasan et S.hohrab hossain**,

University of Haute Alsace, University of Laghouat, University of Oklahoma. Article : Routing in Flying Ad Hoc Networks : Survey, Constraints, and Future Challenge Perspectives 2015.

[21] **I.Maleki, R.Habibpour, M.Ahadi, A.Kamalinia**, Islamic Azad University, Iran. Article : security in routing protocols of ad-hoc networks : a review 2013.

[22] **Ons Bouachir**, Conception et mise en oeuvre d'une architecture de communication pour minidrones civils. Réseaux et télécommunications. Université Toulouse 3 Paul Sabatier en 2014. France.

[23] **H.Redouane**, Protocoles de routage pour les réseaux Ad hoc, université de Montréal 2004.

[24] **R.A Sajano**, The resurrecting duckling, security issues for ad- hoc wireless networks.

[25] **C.Cheng, J.Chun-Wei Lin, L.Ying Chen**, un protocole de consensus pour les réseaux de véhicules aériens sans pilote en présence de failles byzantines, Taiwan 2022.

[26] **A. Perrig Y.C. Hu and D. B. Johnson. Rushing**, attacks and defense in wireless ad hoc network routing protocols, San Diego,USA, 2003

[27] **Cite internet CPN-TOOLS**, http ://cpntools.org/2018/01/16/documentation-2/.

[28] **T.M.Andriamanjara**, Université D'Antanario, sécurisation de données à bord dans un système drone.

[29] **J.A Maxa, M.S Ben Mahmoud, N. Larrieu** , Extended Verification of Secure UAANET Routing Protocol.Digital Avionics Systems Conference, Sacramento, United States 2016.

[30] **J.A Maxa, M.S Ben Mahmoud, N. Larrieu** , Security Challenges

Survey on UAANET Routing Protocols and Network 2017.

[31] **J.A Maxa, M.S Ben Mahmoud, N. Larrieu** , Joint model-driven design and real experiment-based validation for a secure UAV ad hoc network routing protocol . Conference, Herndon, United States 2016.

[32] **I.Ullah Khan, I.M URESHI , M.ADNAN AZIZ**, martiot control based nature inspired energy efficient routing protocol for flying ad hoc network fanet.

[33] **I.Chihi**, Université de Trois rivières CANADA. Étude de l'attaque « Black Hole » sur le protocole de routage VADD, 2017.

[34] **K.Moghrawi**, Université de Trois rivières CANADA. Gestion de la communication anonymyats dans les (VANETs)

[35] **C.Bensaid**, Université Djillali Liabès de Sidi Bel Abbès 2020. Gestion des certificats dans les réseaux véhiculaire.

[36] **E.Walia, B.Vinay , G.Kaur**, Département ECE Baddi University of Emerging Science and Technology, Inde. Détection de noeuds malveillants dans une annonce volante 2019.

[37] **J. Hope, F.Robert, E. Hiromoto, J.Svoboda**, A Time-Slotted OnDemand Routing Protocol for Mobile Ad Hoc Unmanned Vehicle Systems.

[38] **A. Rovira-Sugranes, A.Razi b, F. Afghah, J.Chakareski** , A review of AI-enabled routing protocols for UAV networks : Trends, challenges, and future outlook, Arizona University, USA

[39] **A.Ziou**, université Guelma, Réalisation d'un système de suivi d'objets basé sur les Drones

Annexes

Annexe A

CPN-TOOLS

A.1 Bref historique

CPN Tools est destiné à remplacer Design/CPN qui est un progiciel répandu pour les CP-nets, Design /CPN a été publié pour la première fois en 1989 avec un support pour l'édition et la simulation de réseaux CP. CPN Tools est le résultat d'un projet de recherche, le projet CPN à été développé , à l'Université d'Aarhus de 2000 à 2010. Les principaux architectes derrière l'outil sont Kurt Jensen, Søren Christensen, Lars M. Kristensen et Michael Westergaard. À partir de l'automne 2010, CPN Tools est transféré au groupe AIS, Université de technologie d'Eindhoven, Pays-Bas. L'objectif du projet CPN était de profiter de l'évolution de l'interaction homme-machine, et d'expérimenter ces techniques dans le cadre d'une refonte complète de l'IHM pour Design/CPN. La dernière version est apparue en 2015.

A.2 Définition du logiciel CPN-TOOLS

CPN Tools est un outil d'édition, de simulation et d'analyse de réseaux de Petri colorés. L'outil propose une vérification incrémentielle de la syntaxe et la génération de code, qui ont lieu pendant la construction d'un réseau. Un simulateur rapide gère efficacement les filets non chronométrés et chronométrés. Des espaces d'état complets et partiels peuvent être générés et analysés, et un rapport d'espace d'état standard contient des informations, telles que les propriétés de limite et les propriétés de vivacité.

A.3 Interface du logiciel

La colonne de gauche s'appelle l'index et le reste de l'interface c'est l'espace travail. Comme le montre l'image ci-dessous. La colonne de gauche (index) contient une zone qui s'appelle outil . Elle même contient une liste des Palettes disponibles create(crée), simulation,... .

Dans l'image (A.2) on vas voir toutes les palettes disponible dans l'espace travail.

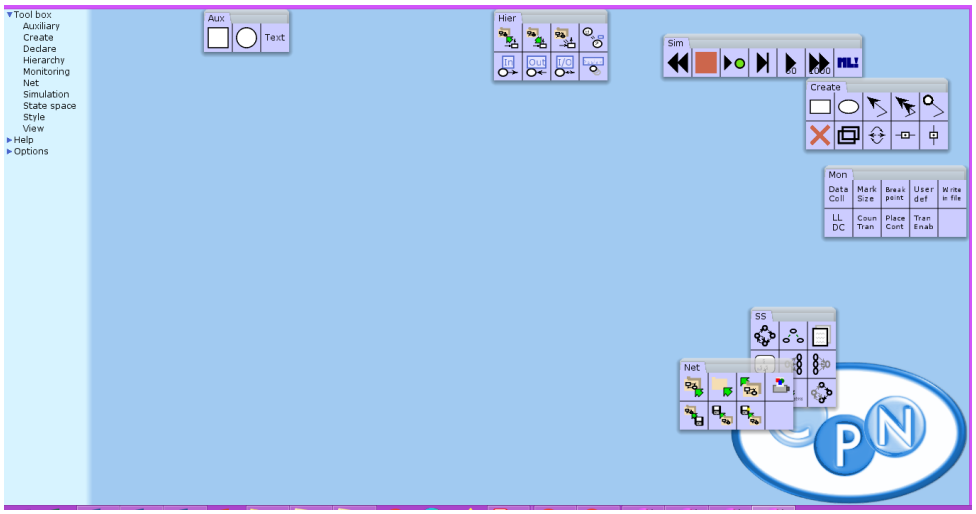

FIG. A.1 : *Interface du CPN-TOOLS.*

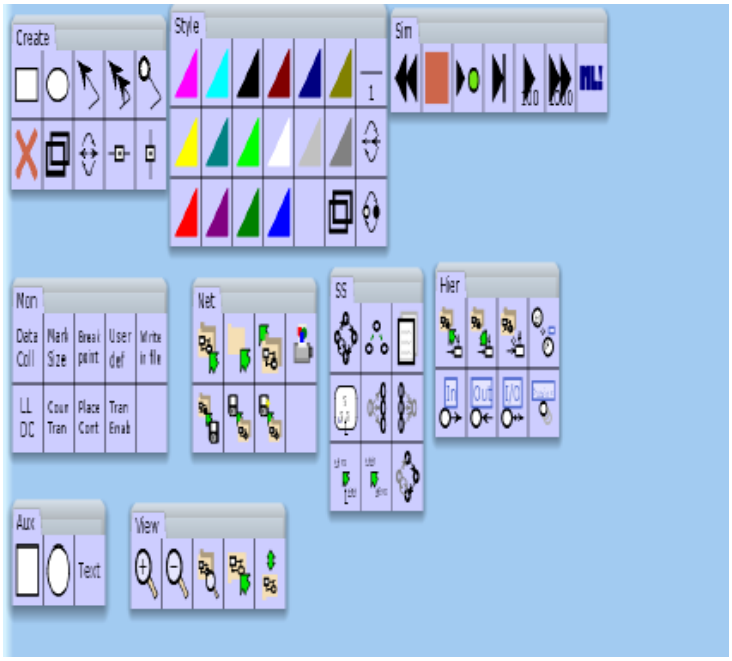

FIG. A.2 : *Palettes disponibles sur l'interface*

- **Outils auxiliaires :** sont utilisés lors de la création d'éléments auxiliaires.

FIG. A.3 : *Outils auxiliaires*

- **Outils de création :** sont utilisés lors de la création de la structure de réseau.

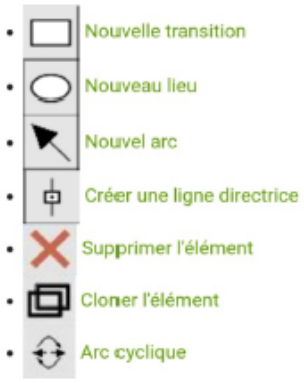

FIG. A.4 : *Outils auxiliaires*

- **Outils de simulation :** sont utilisés pour simuler le réseau.

FIG. A.5 : *Outils auxiliaires*

Annexe B

Réseaux de Pétri coloré

B.1 Réseau de Pétri

Un réseau de Pétri (RdP) est un graphe biparti constitué de 2 sortes de nœuds : Les places (représentées par des ronds) et les transitions (représentées par des barres).
Le graphe est orienté : des arcs vont d'une sorte de nœuds à l'autre (jamais de places à places, ou de transitions à transitions directement).
Graphe formé de :

- ensemble de places $P = P1, P2, P3, ...$
- ensemble de transition $T = T1, T2, T3, ...$
- marquage initial $M = m1, m2, m3, ...$

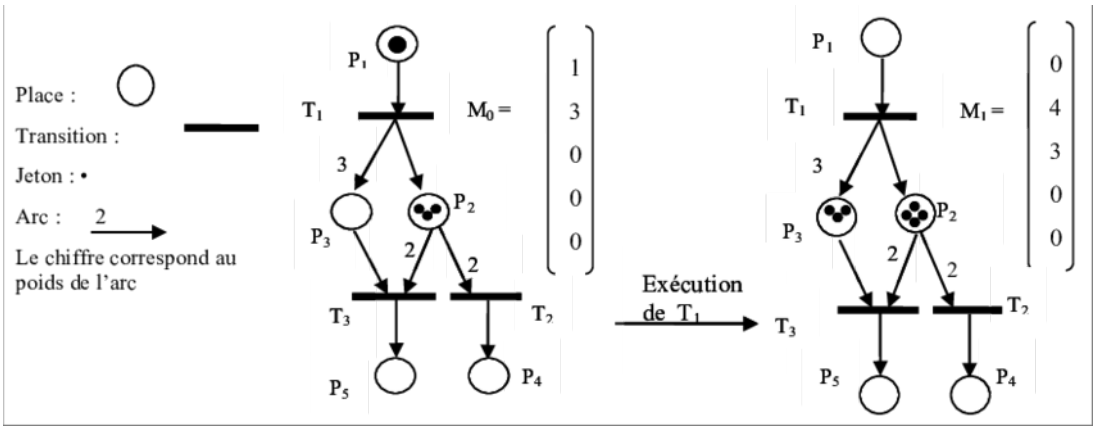

FIG. B.1 : *Une transition franchissable dans un Rdp.*

B.2 Réseau de Pétri coloré

La coloration des modèles comporte une autre facette très intéressante qui consiste en ce fait que les jetons gagnent une identité. Lors de leur circulation dans la structure, les

jetons sont toujours identifiables, ceci assurant leur suivi en temps réel.
Un réseau coloré est constitué :

- de places, transitions et arcs, comme les réseaux de places et transitions,
- de marques individuelles differentiables les unes des autres, par leur couleur par exemple, d'ou le nom de réseau coloré,
- d'un marquage initial indiquant pour chaque place le type de marques qu'elle comporte,
- d'étiquette sur les arcs faisant référence à des types de marques données.

Dans un réseau de ce type, on dira qu'une transition t est franchissable ou tirable :

pour toute place d'entrée P de t, une marque de type indiqué sur l'arc reliant P à t (si places de sortie à capacité finie),

si une transition t est tirable et tirée :

- pour toute place d'entrée P de t on supprime dans P une marque de type indiqué sur l'arc reliant P à t.
- pour toute place de sortie P de t, on ajoute dans P une marque de type indiqué sur l'arc reliant t à P

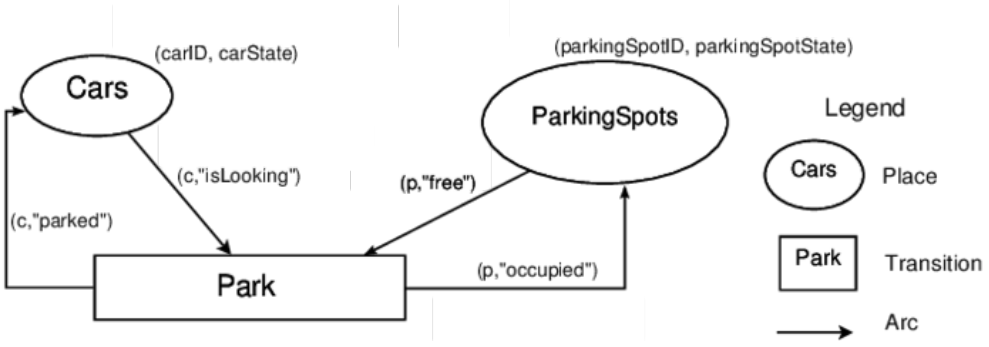

FIG. B.2 : *Exemple de réseau de petri coloré.*

La figure B2 montre une modélisation d'un parking en utilisant un réseau de petri coloré. Il est composé de deux places $P1 = Cars$ et $P2 = ParkingSpots$, d'une transition $T = Park$ et de quatre arcs.

- La place $Cars$ contient des jetons représentant les différentes voitures. Sa couleur est définie sous la forme de tuple : (carID, carState) où carID est une chaîne caractères et carState est un type énuméré représentant les différents états d'une voiture.
- La place $ParkingSpots$ contient des jetons qui représentent les différentes places de parking.

Lorsqu'une voiture est à la recherche d'une place et qu'une place est libre, la transition $Park$ est franchie, alors l'état de la voiture devient *parked* et l'état de la place est modifié à *occupied*. Les jetons $(c, "isLooking")$ et $(p, "free")$ sont consommés et les nouveaux jetons $(c, "parked")$ et $(p, "free")$ sont insérés dans les places $Cars$ et $ParkingSpots$. Les jetons sont consommés et insérés de façon atomique.