Vérification étendue d'un protocole de routage sécurisé pour les réseaux UAANET

Jean Aimé Maxa, Nicolas Larrieu, Mohamed Slim Ben Mahmoud

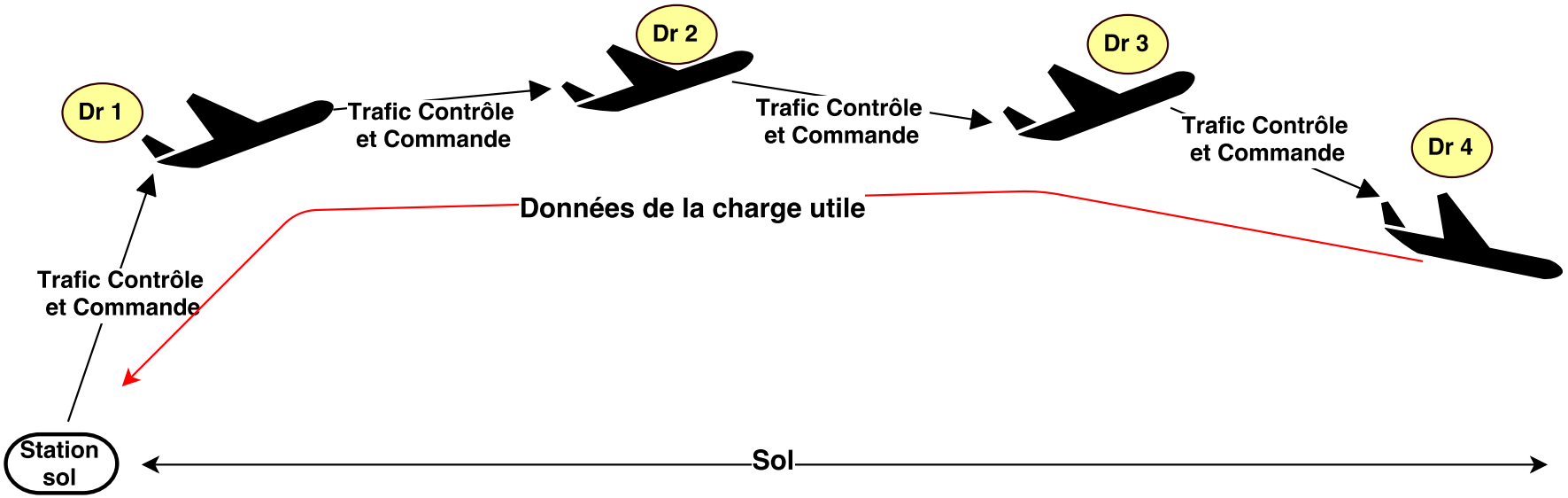
Journée de présentations des doctorants

Chantier Sécurité et Vie Privée du RTRA STAE

Laboratoire d'accueil: ENAC, axe ResCo de l'équipe TELECOM
Ecole doctorale: Systèmes (EDSYS)

Plan

Pourquoi un réseau Ad hoc ?



Réseau UAANET (UAV Ad hoc Network)

- Réseau ad hoc mobile (MANET - Mobile ad hoc Network) où les nœuds sont des drones et des stations sol
- Caractéristiques spécifiques :
  - Faible densité de nœuds, mobilité spécifique (3D), connectivité intermittente.

Besoins de sécurité

Vulnérabilités des réseaux MANET

- Canal de communication vulnérable
- Absence d'une ligne de défense
- Problème de coopération

Attaques sur le routage

- Attaque Blackhole : génération de paquets falsifiés permettant d'établir une route erronée
- Attaque Wormhole : coordination entre deux ou plusieurs attaquants pour créer un tunnel et intercepter le trafic

Besoins de sécurité

Vulnérabilités des réseaux MANET

- Canal de communication vulnérable
- Absence d'une ligne de défense
- Problème de coopération

Attaques sur le routage

- Attaque Blackhole : génération de paquets falsifiés permettant d'établir une route erronée
- Attaque Wormhole : coordination entre deux ou plusieurs attaquants pour créer un tunnel et intercepter le trafic

Contexte UAANET

- Le protocole de routage doit être robuste aux différentes attaques
  1. L'authentification des paquets de routage est primordiale pour la survie de la mission
  2. Les attaquants ne doivent pas pouvoir falsifier le choix d'une route

Besoins de sécurité

Vulnérabilités des réseaux MANET

- Canal de communication vulnérable
- Absence d'une ligne de défense
- Problème de coopération

Attaques sur le routage

- Attaque Blackhole : génération de paquets falsifiés permettant d'établir une route erronée
- Attaque Wormhole : coordination entre deux ou plusieurs attaquants pour créer un tunnel et intercepter le trafic

Contexte UAANET

- Le protocole de routage doit être robuste aux différentes attaques
  1. L'authentification des paquets de routage est primordiale pour la survie de la mission
  2. Les attaquants ne doivent pas pouvoir falsifier le choix d'une route

Contexte de travail : vérification et validation de la sûreté pour une flotte de drones

Sûreté de fonctionnement

- Anticiper les défaillances et les pannes
- [DO 178 B], [DO 178 C] : normes de certification du logiciel pour l'avionique
- Vérification de conformité entre le code source et l'architecure logicielle durant la conception

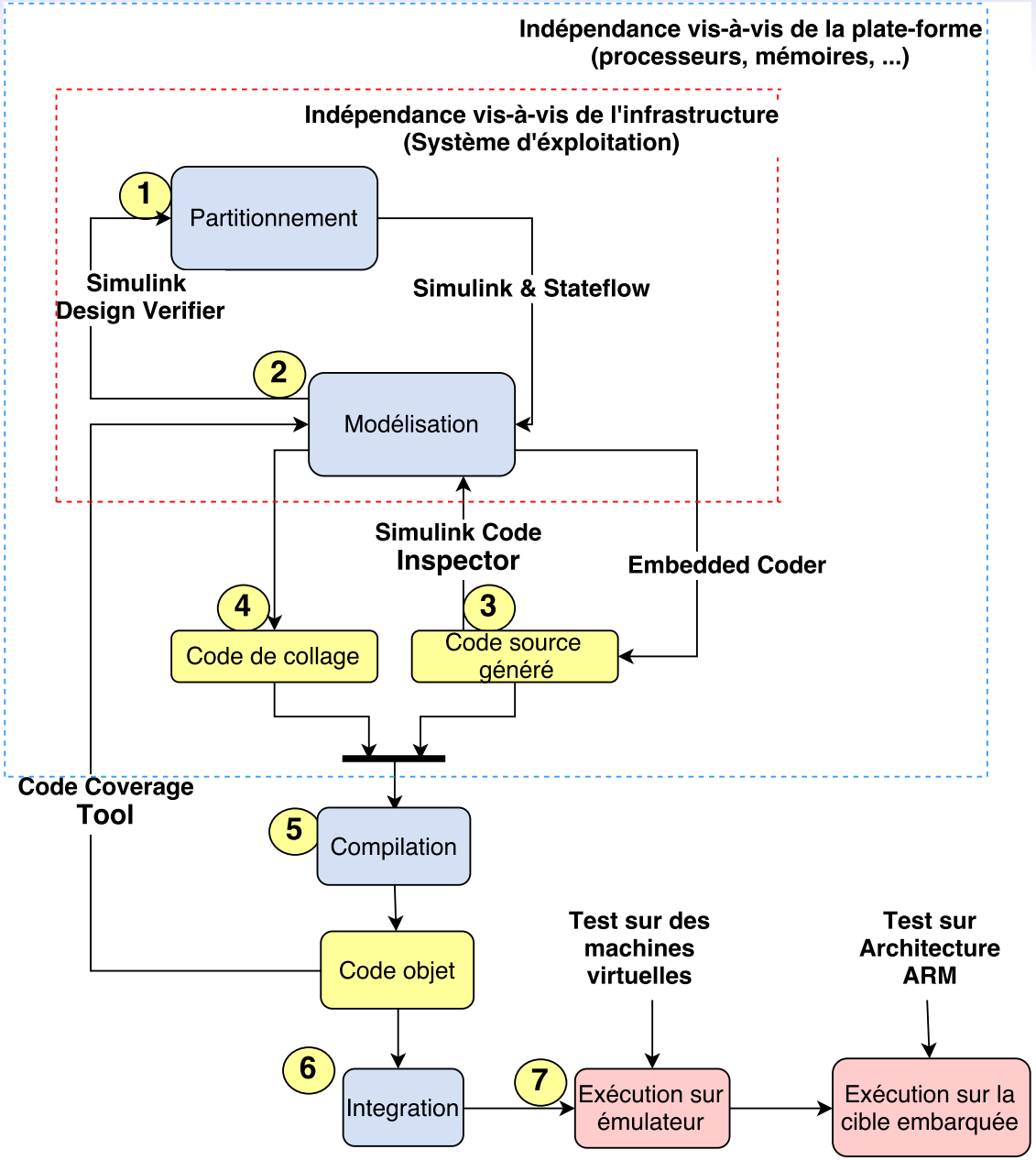
Besoin de validation

- Assurer que la flotte de drones n'entre pas en collision avec d'autres systèmes (UTM : UAS Traffic Management)
- Nécessite une méthodologie qui prenne en compte l'évaluation et la certification du logiciel produit

Contribuer à la validation (dans le but d'obtenir une certification) du système UAS utilisé

Plan

Méthodologie de développement



Plan

Objectif du protocole SUAP

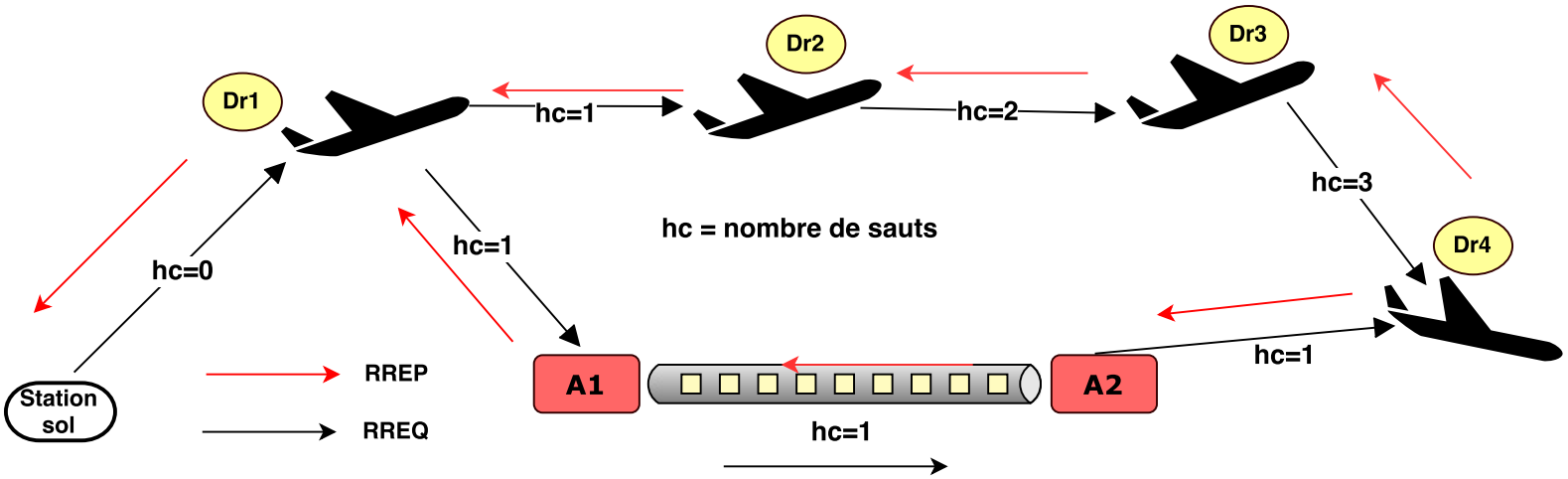
Proposer une route fiable

1. Authentifier les messages de routage
   - Eviter les modifications non autorisées des messages de routage
   - Eviter les attaques conduisant à la dégradation de performance
2. Protéger contre l'attaque wormhole
   - Assurer que les paquets de routage ne passent pas par un tunnel wormhole

Objectif du protocole SUAP

Proposer une route fiable

1. Authentifier les messages de routage
   - Eviter les modifications non autorisées des messages de routage
   - Eviter les attaques conduisant à la dégradation de performance
2. Protéger contre l'attaque wormhole
   - Assurer que les paquets de routage ne passent pas par un tunnel wormhole



Mécanismes de sécurité mis en oeuvre dans SUAP

Champs non mutables

- Utilisation d'une signature numérique
- Algorithme utilisé RSA

Champs mutables

- Utilisation d'une chaine de hachage (en incluant l'identité du prochain nœud dans la table)
- Algorithme utilisé SHA-256 (peut également utiliser les autres variantes SHA)

La contribution porte sur l'implémentation orientée modèle de ces mécanismes et les validations formelles qui en découlent

Nouveaux mécanismes de sécurité proposés pour SUAP

Raisonnement

- L'attaque wormhole diminue d'une manière significative le nombre de sauts d'une source vers une destination.
- Il est possible de connaitre la distance relative entre deux voisins (synchronisation des nœuds)
- On considère le problème en deux dimensions

Proposition

- Relation entre le nombre de sauts et la distance géographique entre les nœuds
- Inclusion de l'identité des nœuds légitimes dans le calcul de l'empreinte (valeur de hash)

Nouveaux mécanismes de sécurité proposés pour SUAP

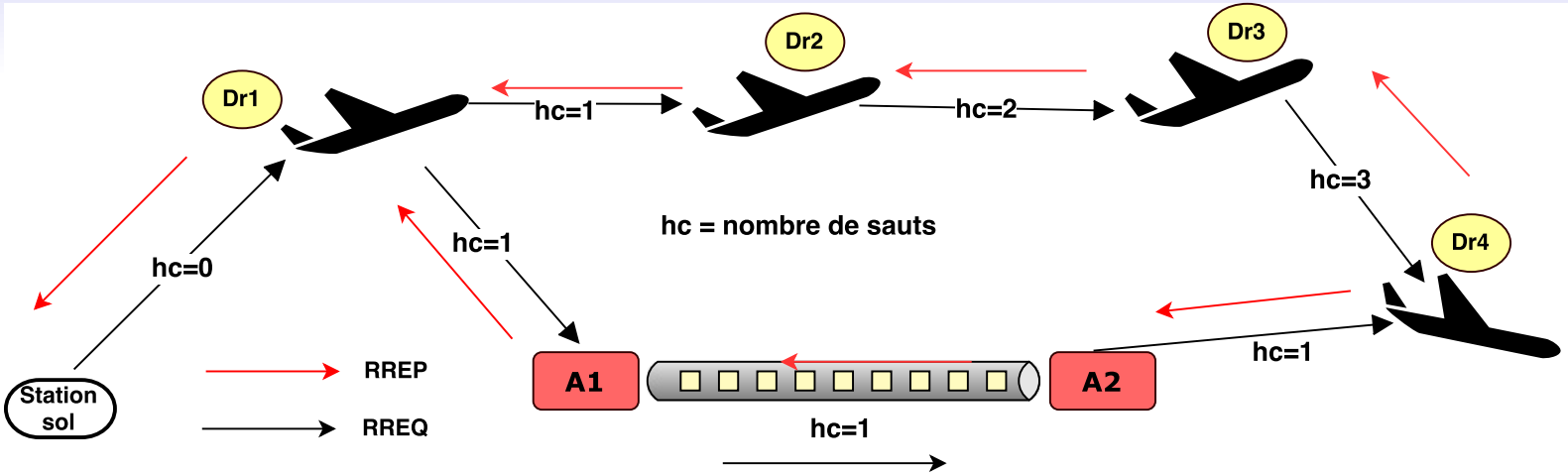
Fonctionnement du mécanisme

ETAPE 1 (à l'initialisation) :

Découverte de voisin

Rélation entre nombre de sauts et distance rélative

Illustration de l'échange des paquets Hello



T = distance totale de la route légitime
hc = valeur virtuelle du nombre de sauts

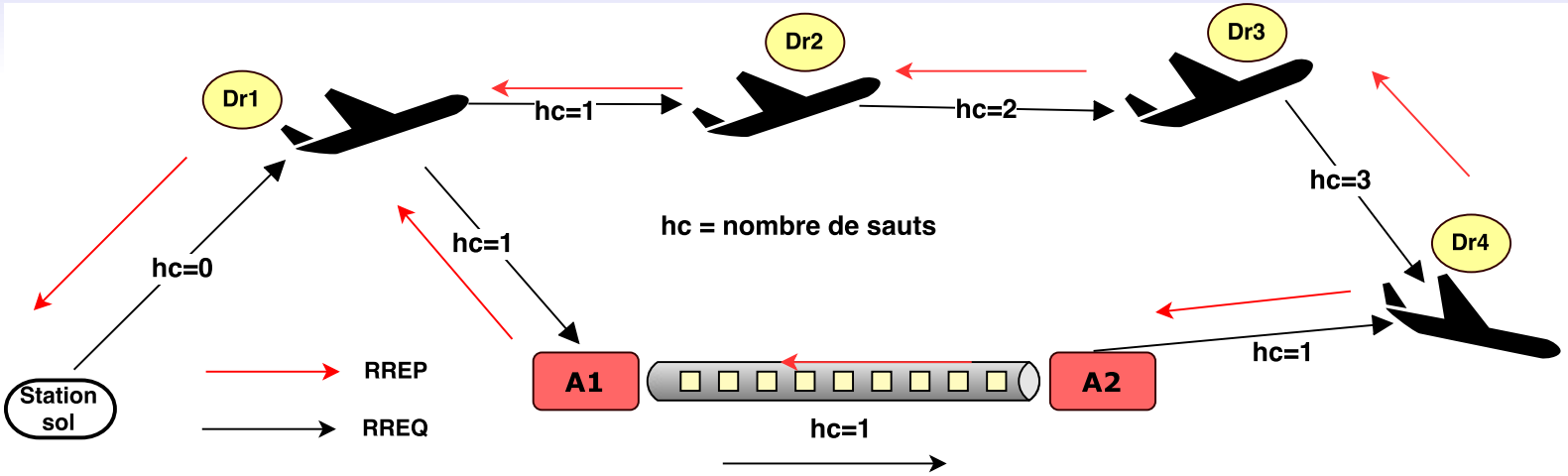
$$\frac{T}{Dmax} - 1 \leq hc < \frac{T}{Dmax} + 1 \quad (1)$$

avec

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

- Dr1 envoi un paquet Hello au nœud Dr2
- Dr2 calcule la distance relative et déduit la valeur virtuelle du nombre de sauts
- Dr2 compare le nombre de sauts virtuel avec le nombre de sauts inclus dans le paquet.

Illustration de l'échange des paquets Hello



T = distance totale de la route légitime
hc = valeur virtuelle du nombre de sauts

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

avec

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

- Dr1 envoi un paquet Hello au nœud Dr4 à travers le tunnel
- Dr4 calcule la valeur virtuelle du nombre de sauts
- Dr4 compare les deux valeurs de nombre de sauts et constate l'anomalie

Mécanismes de sécurité contre l'attaque wormhole

Fonctionnement du mécanisme

ETAPE 1 (à l'initialisation) :

Découverte de voisin

Rélation entre nombre de sauts et distance rélative

Authentification (des messages) entre voisin et vérification de l'existence d'un tunnel wormhole

Mécanismes de sécurité contre l'attaque wormhole

Fonctionnement du mécanisme

ETAPE 1 (à l'initialisation) :

Découverte des voisins

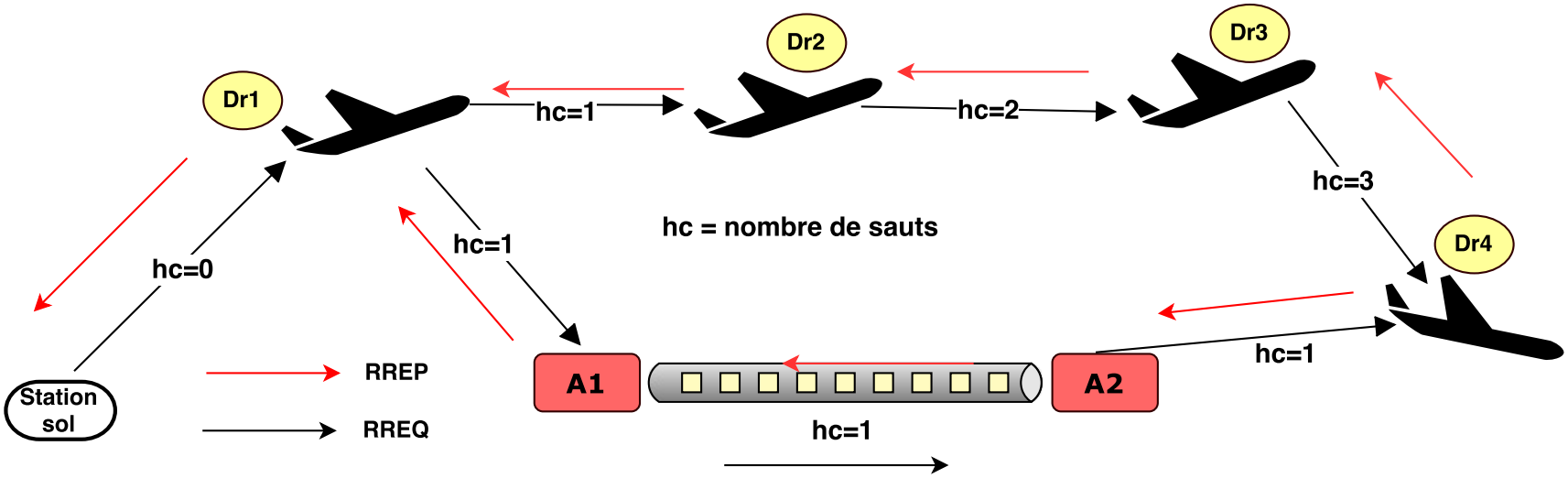
- **Rélation entre nombre de sauts et distance rélative**
- **Authentification (des messages) entre voisins et vérification de l'existence d'un tunnel wormhole**

ETAPE 2 :

Découverte de route

- **Prise en compte de l'identité des noeuds dans le calcul de hash**

Illustration de l'échange des paquets de découverte de route



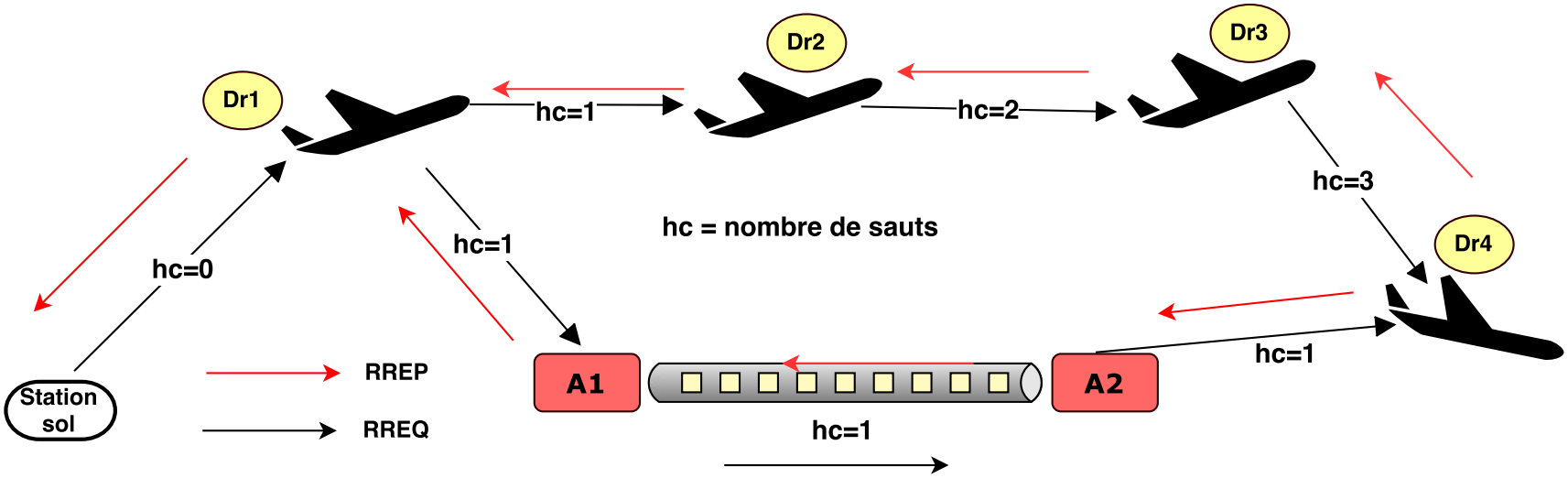
Opération sur le nœud Dr1

- Calcul de *Hashold*
- Calcul de *Hashnew* = $H(Dr1, Dr2, Hashold)$
- Dr1 $\Rightarrow$ $Dr2$: $[64, H, sign, Hashnew, Hashold]$

Opération sur le nœud Dr2

- Calcul de *Hashverifier* = $H[Dr1, Dr2, Hashlold]$
- Comparaison de Hashverifier et Hashnew
- Si Hashverifier = Hashnew $\Rightarrow$ il n'y a pas de tunnel wormhole

Illustration de l'échange des paquets de découverte de route



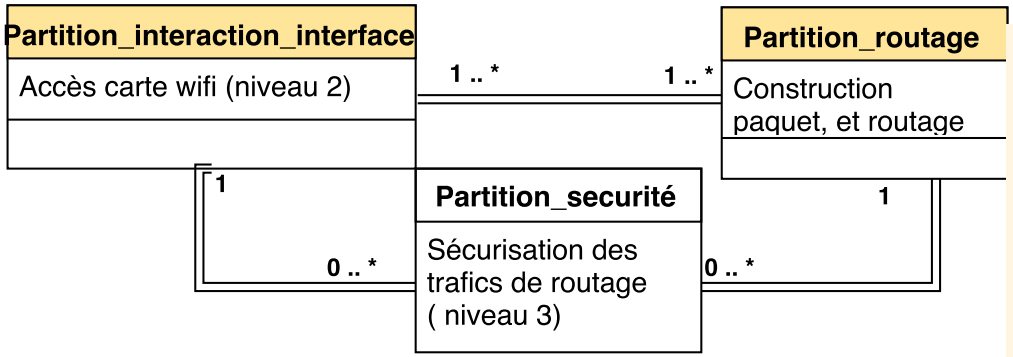
Opération sur le nœud Dr1

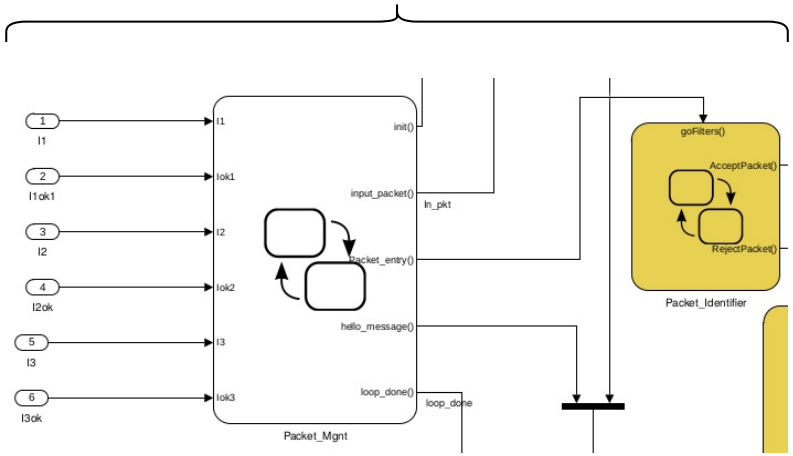
- Calcul de *Hashold*
- Calcul de $Hashnew = H(Dr1, Dr2, Hashold)$
- Dr1 $\Rightarrow Dr2$: $[64, H, sign, Hashnew, Hashold]$

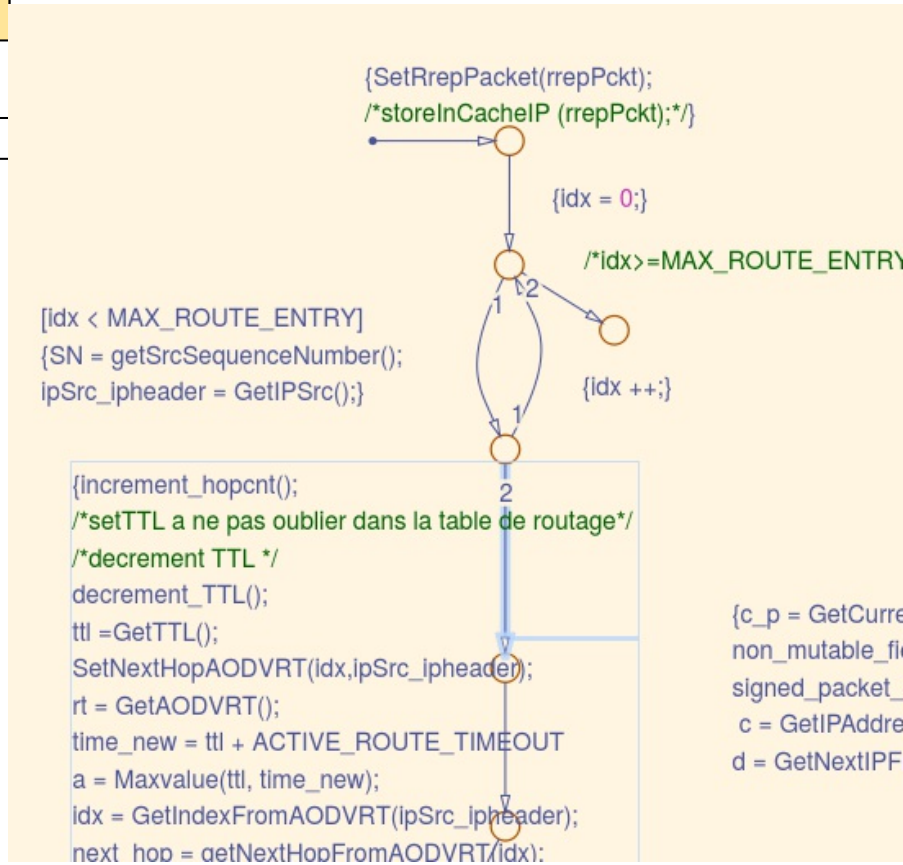
Opération sur le nœud Dr4

- Calcul de $Hashverifier = H[Dr1, Dr4, Hashlold]$
- Comparaison de Hashverifier et Hashnew
- Hashverifier $\neq$ Hashnew $\Rightarrow$ il y un tunnel wormhole

Mise en œuvre grâce à des modèles à états-transitions








```
/* Initial conditions for function-call system: '<Root>/Sta
void AODV_delair_StatisticsMgmt_Init(void)
{
  int32_T i;
  AODV_delair_DW.bitsForTID0.is_active_c4_AODV_delair = 0U;
  AODV_delair_DW.bitsForTID0.is_c4_AODV_delair = AODV_delai
  for (i = 0; i < 5; i++) {
    AODV_delair_Y._statisticsAodv_out[i] = 0U;
```

Usage de modèles

=> Vérification de propriétés

=> Génération de code

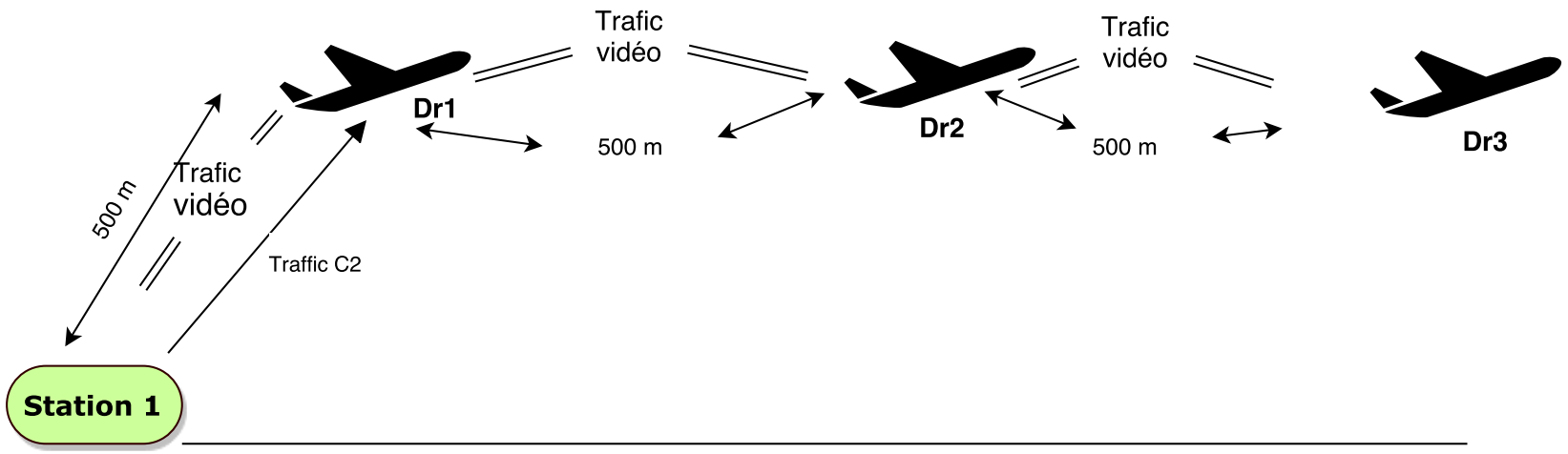
Vérification étendue du protocole SUAP

Vérification formelle des propriétés de sécurité avec AVISPA

- Objectifs
  - Vérifier l'utilité des contre-mesures
  - Trouver des variantes d'attaques auxquelles SUAP serait vulnérable
- Résultats
  - Propriétés du protocole SUAP conformes aux objectifs de sécurité attendus

Plan

Topologie de test pour les fonctions de sécurité

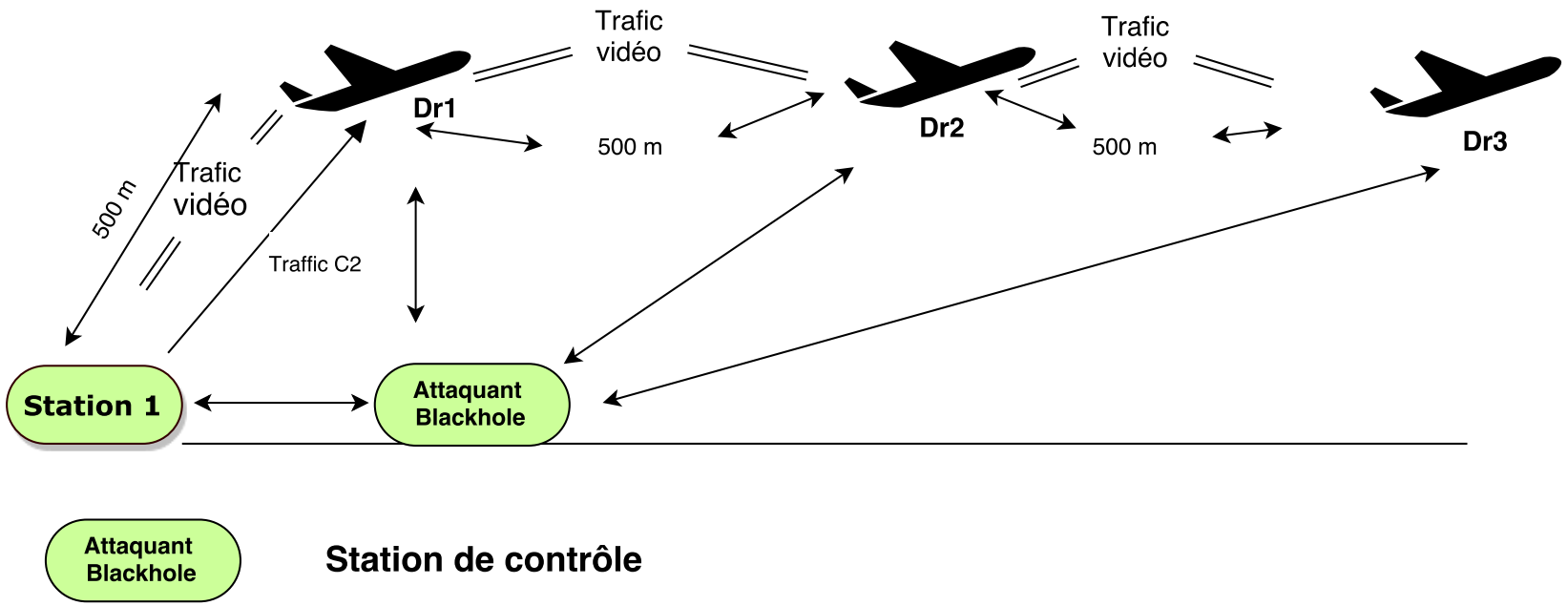


Permet de valider les classes de partition de sécurisation des trafics de routage

- Fonctions d'authentification et d'intégrité

- Protocole AODV modélisé et SUAP modélisé
- IEEE 802.11g

Topologie de test pour les fonctions de sécurité

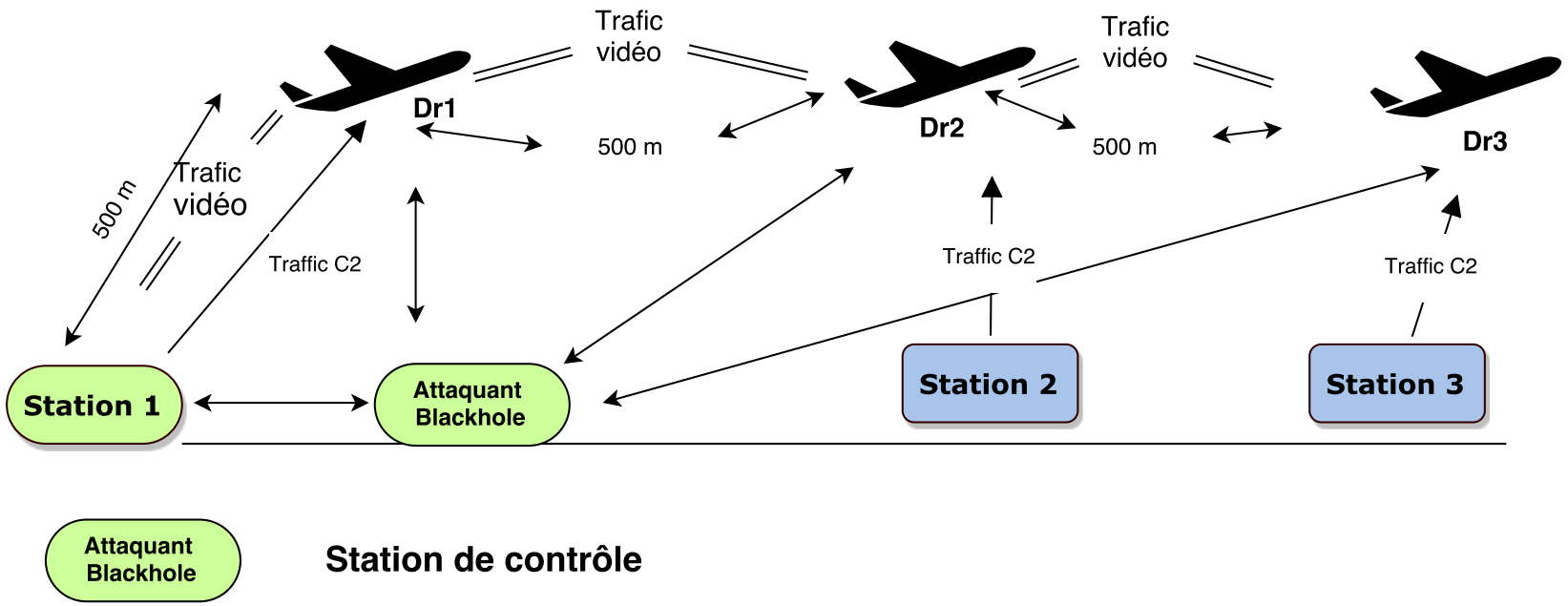


Permet de valider les classes de partition de sécurisation des trafics de routage

- Fonctions d'authentification et d'intégrité

- Protocole AODV modélisé et SUAP modélisé
- IEEE 802.11g

Topologie de test pour les fonctions de sécurité

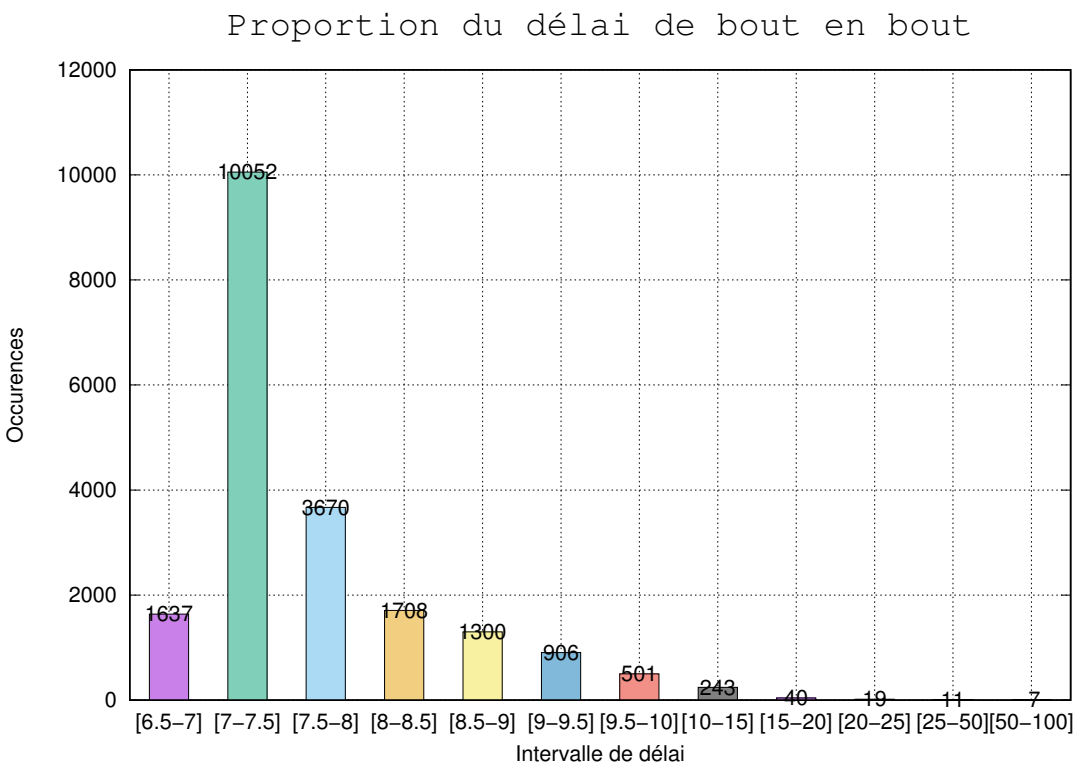


Permet de valider les classes de partition de sécurisation des trafics de routage

- Fonctions d'authentification et d'intégrité

- Protocole AODV modélisé et SUAP modélisé
- IEEE 802.11g

Délai de bout en bout et délai d'acheminement des trafics vidéo

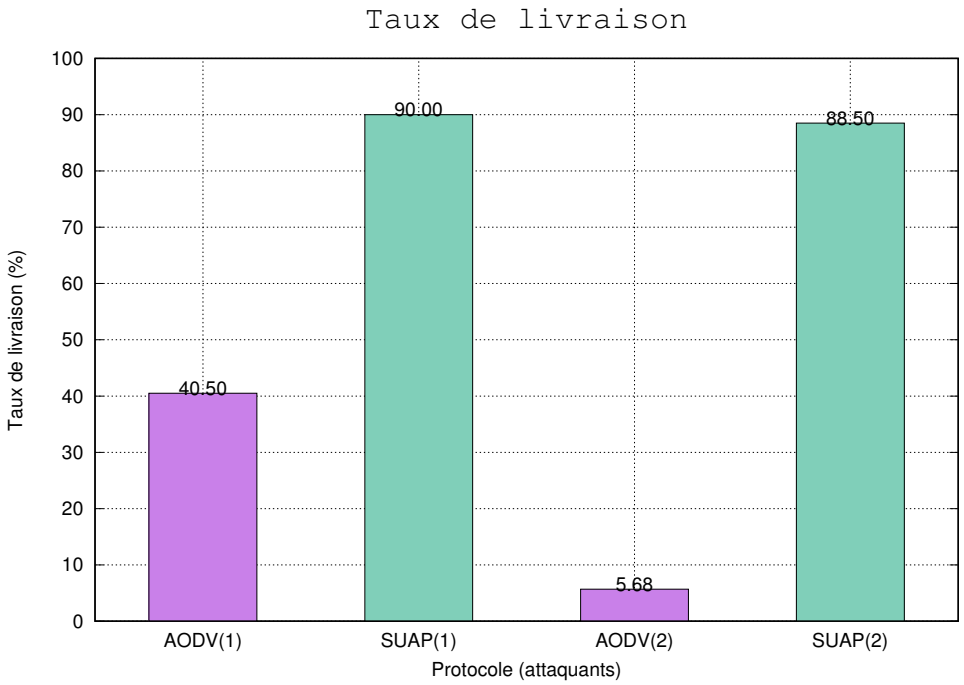


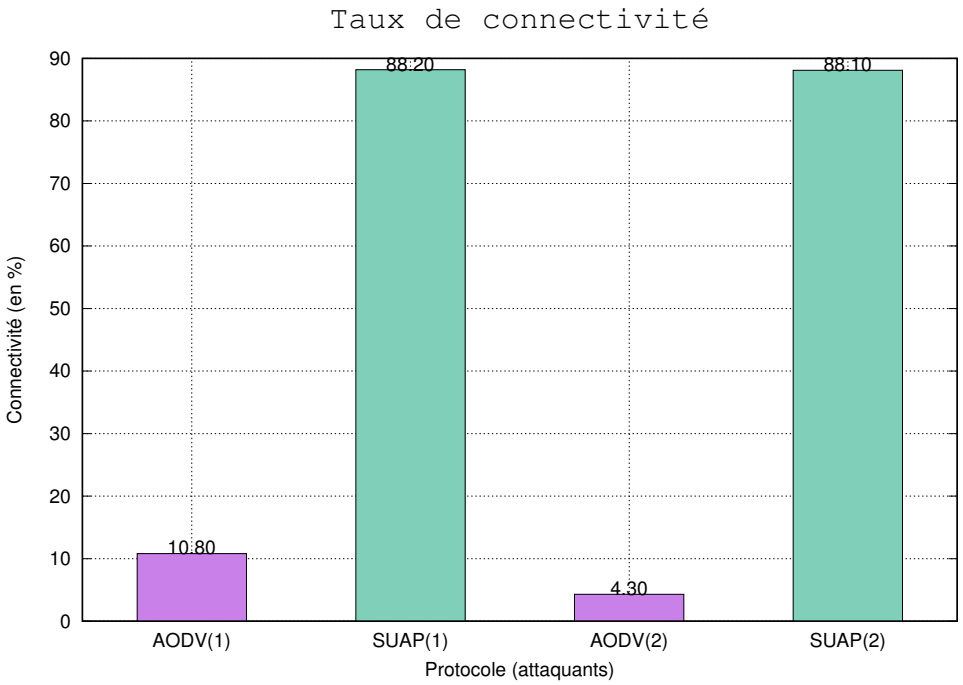
Délai pour trafic de signalisation	**Valeurs**
Délai moyen	7.43 ms
Délai maximum	100 ms
Délai pour trafic de charge utile	**Valeurs**
Délai moyen	9.2 ms
Délai maximum	104 ms

Conclusion

- Le délai nécessaire pour authentifier les paquets **ne pénalise pas** l'échange des trafics temps réel

Taux de connectivité et de livraison des données

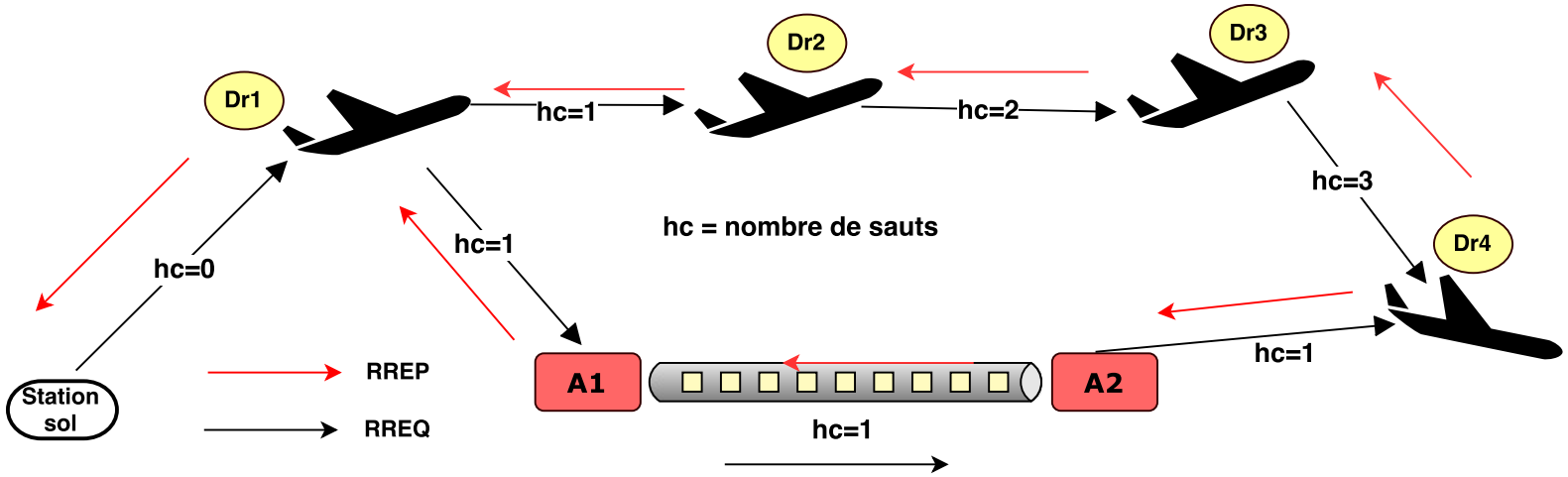




Conclusion

- **AODV souffre** de l'effet de l'attaque blackhole.
- Avec SUAP, **la connectivité est maintenue**

Validation des mécanismes contre l'attaque wormhole



Paramètres	Valeur
Nombre de nœuds légitimes	5 (4 drones et une station sol)
Mobilité	Rejeu de scénarios de mobilité réels
Protocole de routage	SUAP et AODV modélisé
Protocole MAC	Couche d'accès idéale
Trafic applicatif généré	trafic C2 et vidéo

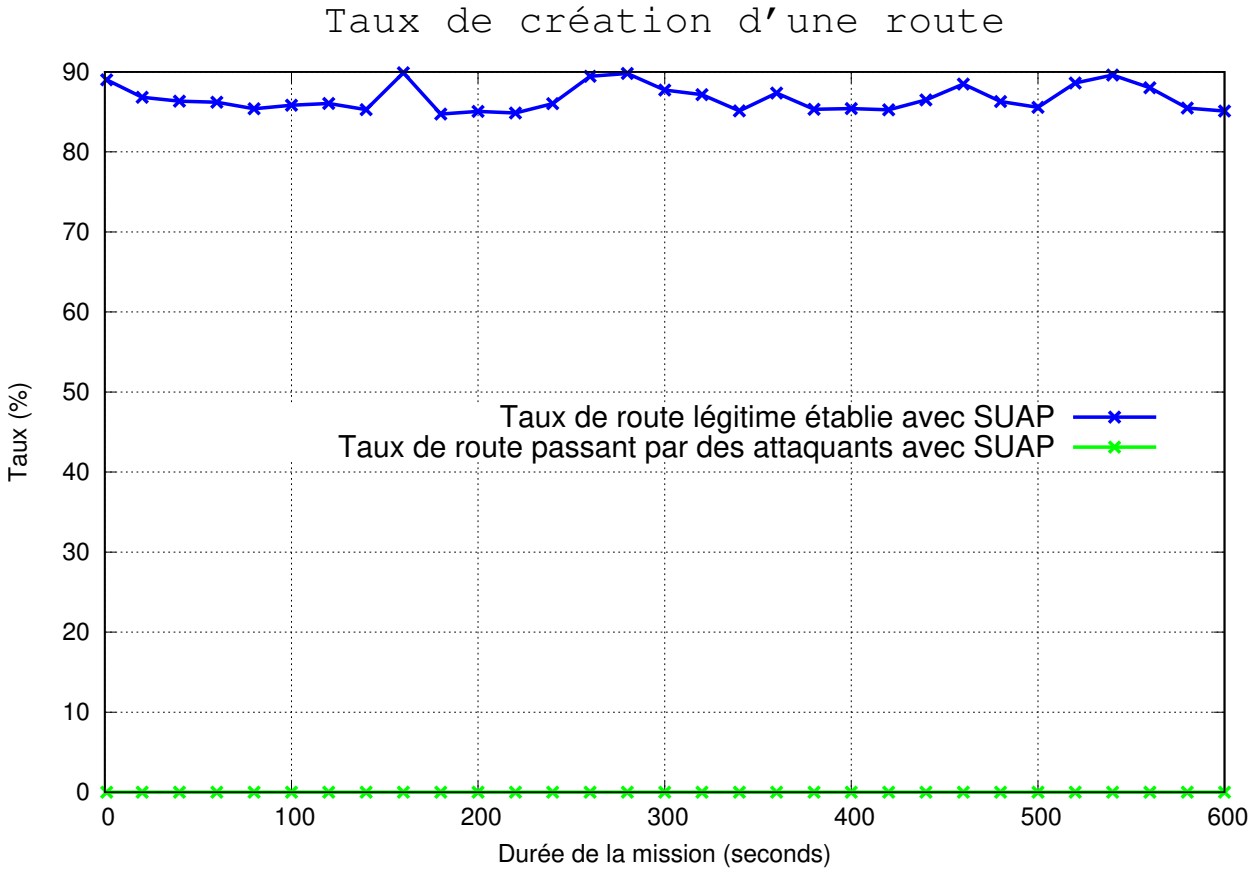
Validation des mécanismes contre l'attaque wormhole

Objectif

1. Étudier la capacité de SUAP à
   - détecter l'attaque wormhole
   - prendre des décisions sur le choix d'une route
2. Métrique choisie
   - Taux de création d'une route sur le chemin légitime

Paramètres	**Valeur**
Nombre de nœuds légitimes	5 (4 drones et une station sol)
Mobilité	Rejeu de scénarios de mobilité réels
Protocole de routage	SUAP et AODV modélisé
Protocole MAC	Couche d'accès idéale
Trafic applicatif généré	trafic C2 et vidéo

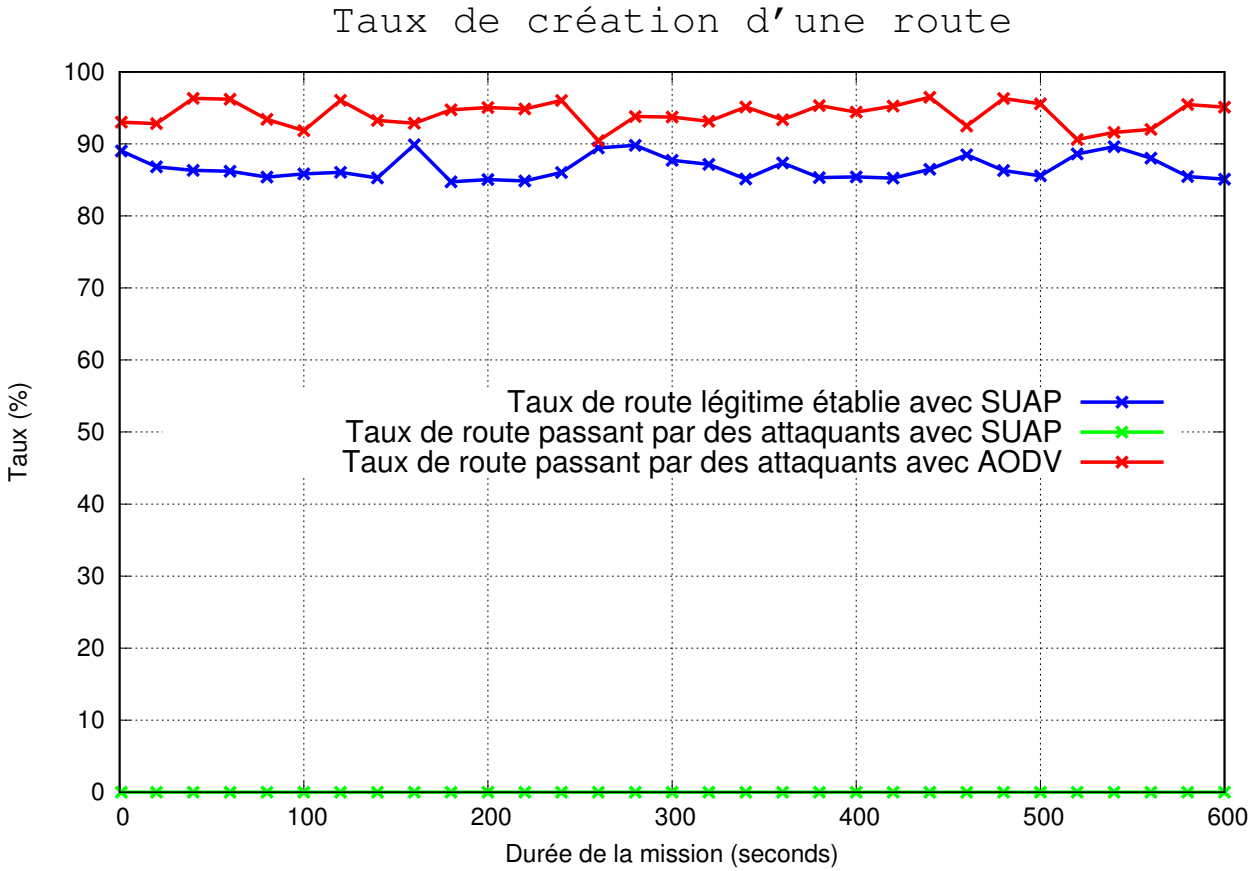
Taux de création d'une route passant par les nœuds légitimes



Conclusion

- Taux de création d'une route légitime est de 85 % avec SUAP contre 0 % avec AODV
- Avec SUAP, les paquets de données ne sont échangés que sur la

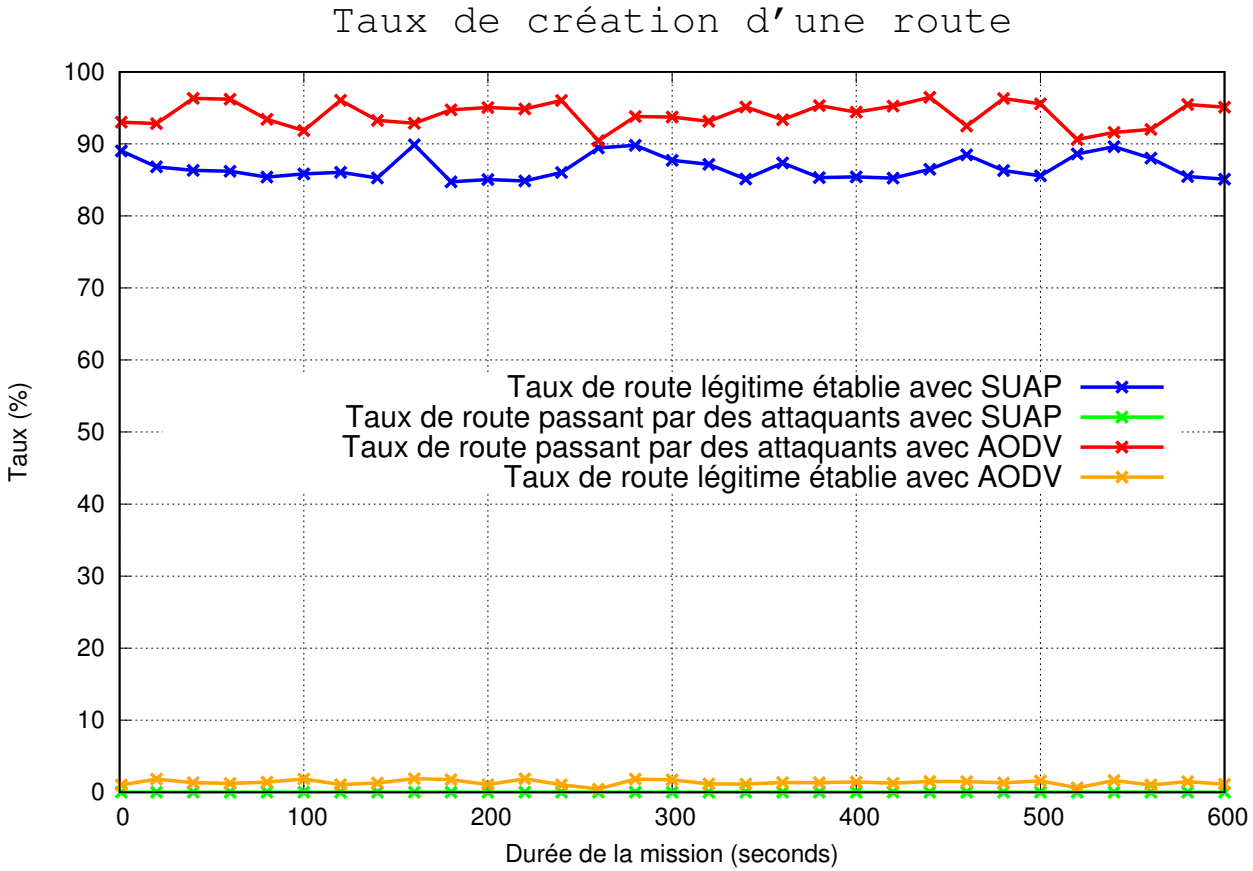
Taux de création d'une route passant par les nœuds légitimes



Conclusion

- Taux de création d'une route légitime est de 85 % avec SUAP contre 0 % avec AODV
- Avec SUAP, les paquets de données ne sont échangés que sur la

Taux de création d'une route passant par les nœuds légitimes



Conclusion

- Taux de création d'une route légitime est de 85 % avec SUAP contre 0 % avec AODV
- Avec SUAP, les paquets de données ne sont échangés que sur la

Plan

Conclusions

Génie logiciel

- Élaboration et validation d'une méthodologie de développement de systèmes embarqués critiques
- Utilisation de modèles pour concevoir l'architecture détaillée du système
- Vérification formelle des modèles et du code source généré

Sécurité des réseaux UAANET

- Élaboration et validation du protocole SUAP
- Nos résultats valident que SUAP authentifie les messages et protège contre l'attaque wormhole
- SUAP offre un niveau de service acceptable

Perspectives

Infrastructure de gestion de clé adaptée au contexte UAANET

- Proposer une architecture de gestion de clé pour les réseaux UAANET afin de gérer le cycle de vie des clés cryptographiques utilisées dans la solution SUAP

Sécurité des trafics utiles échangés

- Définir une solution de sécurité applicative pour la confidentialité des données utiles

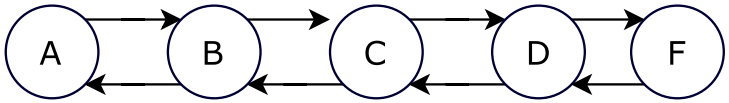
Etude de performance complémentaire du protocole SUAP

- Augmenter le nombre de nœuds durant l'expérimentation réelle
- Déployer un attaquant mobile en environnement réel
- Tester l'attaque wormhole en environnement réel

Merci pour votre attention

Spécification du protocole SUAP avec AVISPA

Analyse de l'authentification des messages



A ----> B: { SREQ, NA, A, id}_inv(Ka), oldhash, newhash}

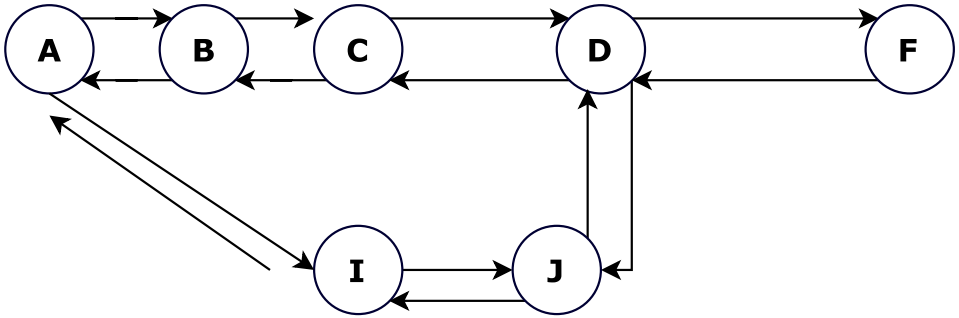
B ----> C: { SREQ, NA, A, id}_inv(Ka), oldhash, newhash}

.....

D----> F: { SREQ, NA, A, id}_inv(Ka), oldhash, newhash}

B ----> A: { SREP, NF, F, id}_inv(Kf), oldhash, newhash}

Analyse de l'attaque wormhole

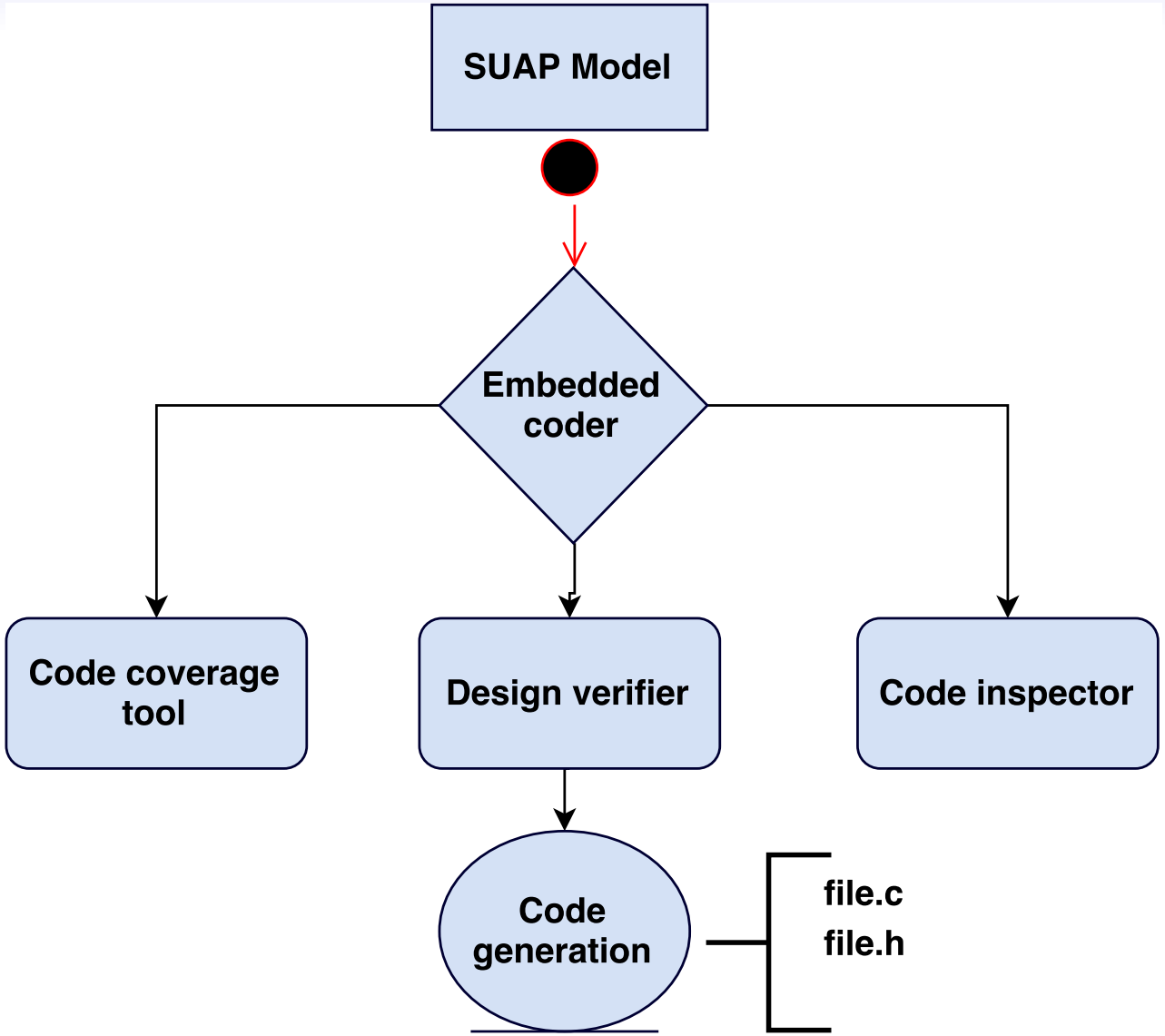


1) A → I : {SREQ, F, N a ′ } inv(Ka), Hash, certA
2) A → B : {SREQ, F, N a ′ } inv(Ka), Hash, certA
3) I → J : {SREQ, F, N a ′ } inv(Ka), Hash, certA
4) J → D : {SREQ, F, N a ′ } inv(Ka), Hash, certA
5) D → F : {SREQ, F, N a ′ } inv(Ka), Hash, certA, certD
6) F → D : {SREP, A, N d ′ } inv(Kf), Hash, certF
7) D → J : {SREP, F, N d ′ } inv(Kf), Hash, certF, certD
8) J → I : {SREP, F, N d ′ } inv(Kf), Hash, certF, certD
9) I → A : {SREP, F, N d ′ } inv(Kf), Hash, certF, certD

Résultats

- Le protocole SUAP assure l'authentification des messages
- L'attaque wormhole n'est pas solutionnée

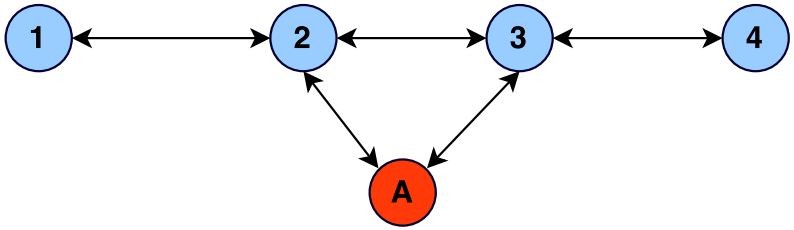
Illustration des étapes de vérification formelle



Description de l'attaque Blackhole

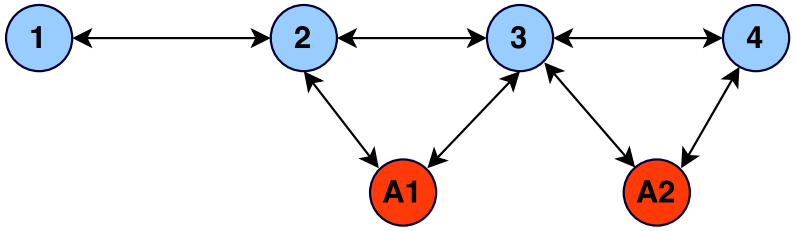
Single blackhole

- L'attaquant jette tous les paquets de donnés qu'il reçoit
- L'attaquant propose de meilleures routes (en jouant sur le nombre de sauts)



Collaborative blackhole

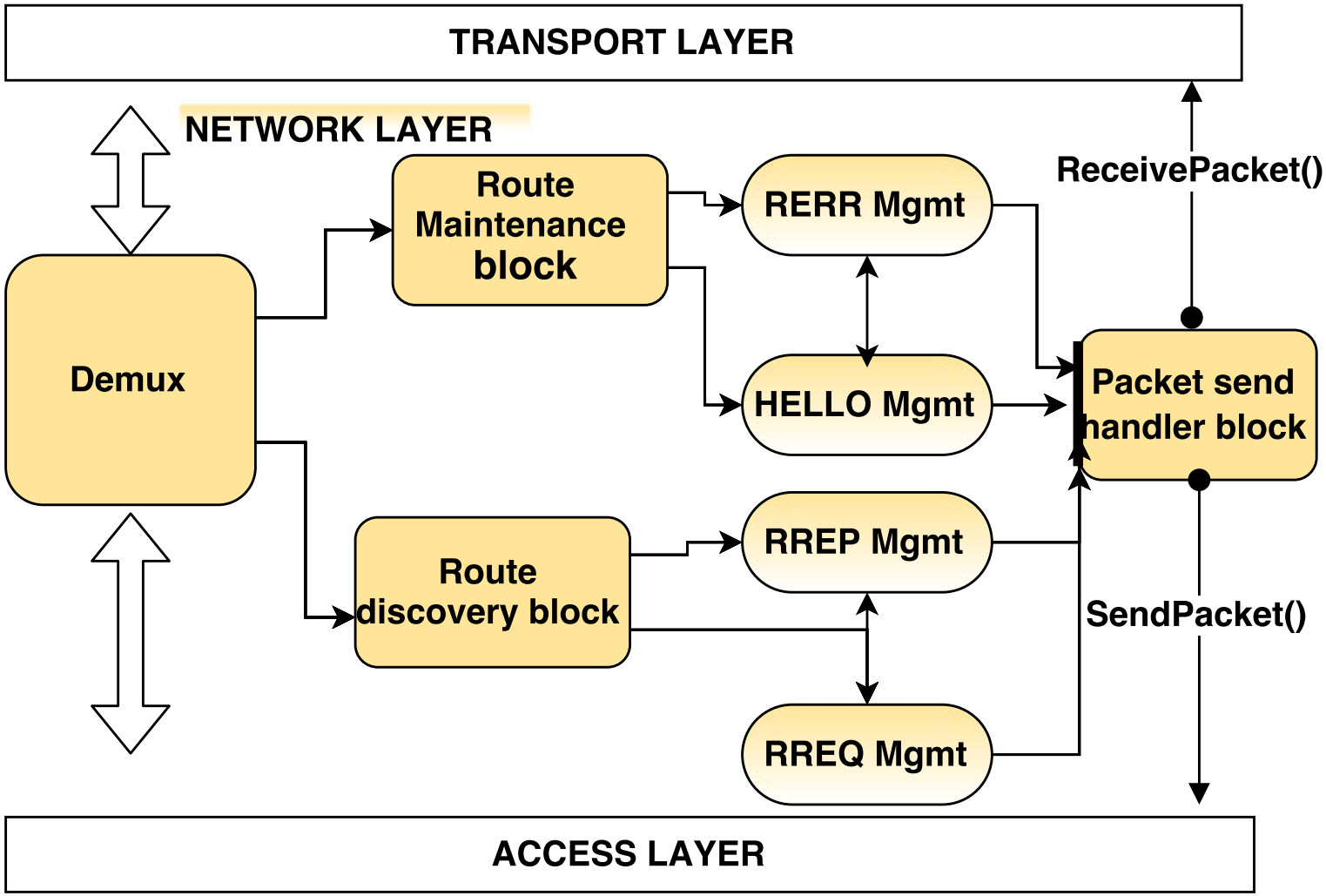
- Plusieurs nœuds malveillants attaquent le réseau simultanément



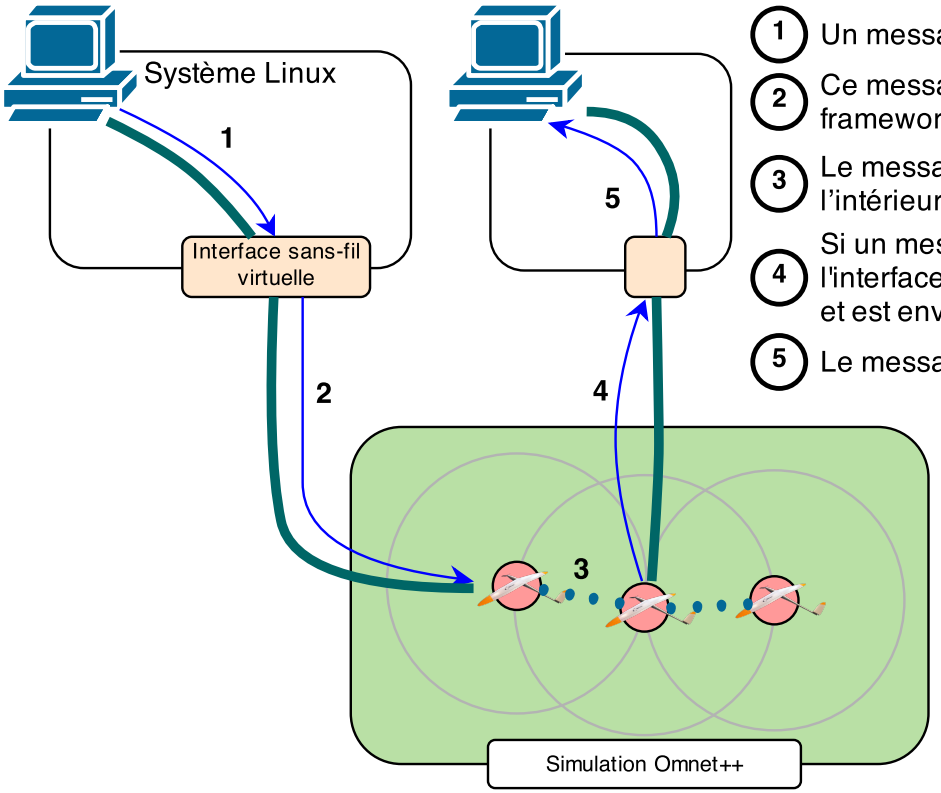
Format du paquet requête

Type	Length	Hash function	Max hop count
Top hash			
Sign Method	H	Reserved	Padd Length
Public Key			
Padding (optional)			
Signature			
Hashnew			
Hashold			

Architecture générique de conception pour la partition de routage

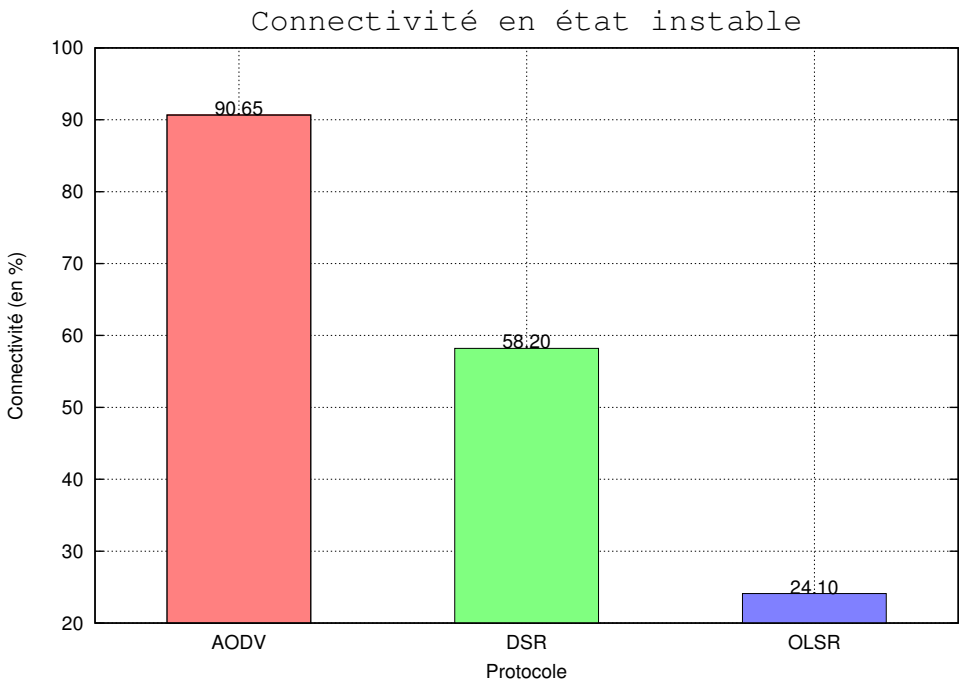


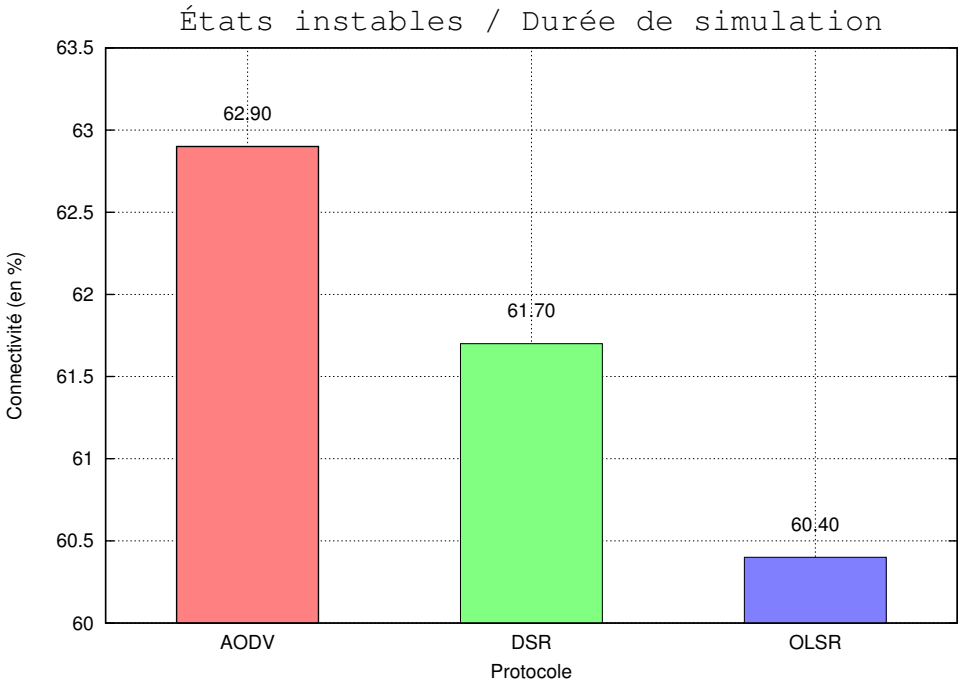
VirtualMesh : lien entre tests réel et tests en simulation



1. Un message IP est envoyé à travers l'interface virtuelle
2. Ce message est transmis, encapsulé par un protocole propre au framework, et est envoyé à la simulation OmNet++
3. Le message est décapsulé, puis est émis au sein de la simulation à l'intérieur d'une trame MAC.
4. Si un message reçu a une adresse MAC de destination correspondant à l'interface virtuelle de l'agent connecté. Il est ré-encapsulé par le framew et est envoyé à l'interface virtuelle de l'agent.
5. Le message IP est bien reçu, il est traité par le système Linux.

Taux de connectivité des protocoles en environnement émulé

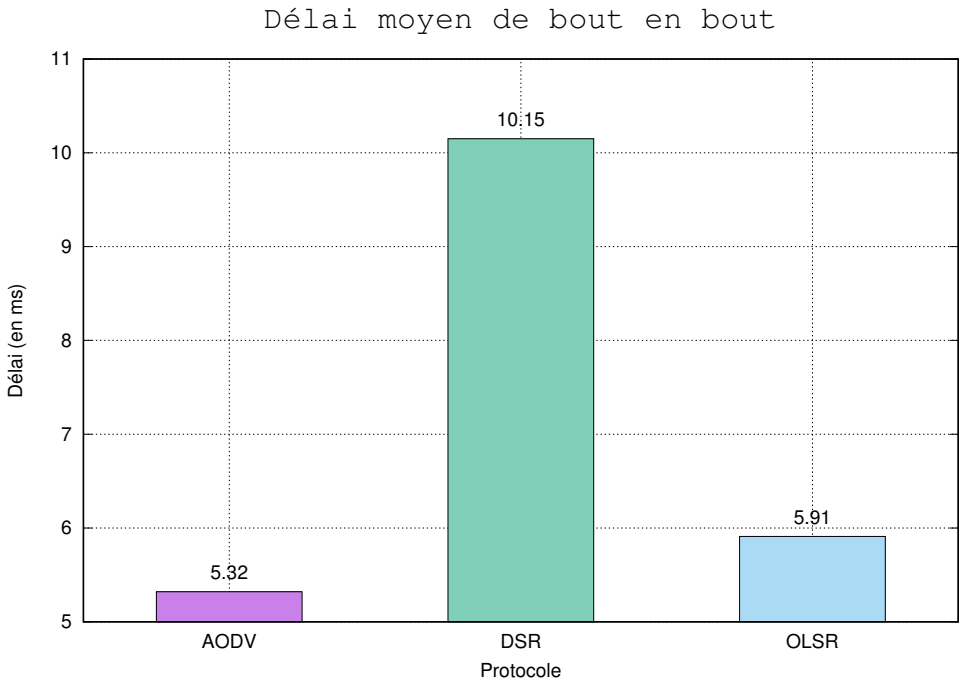


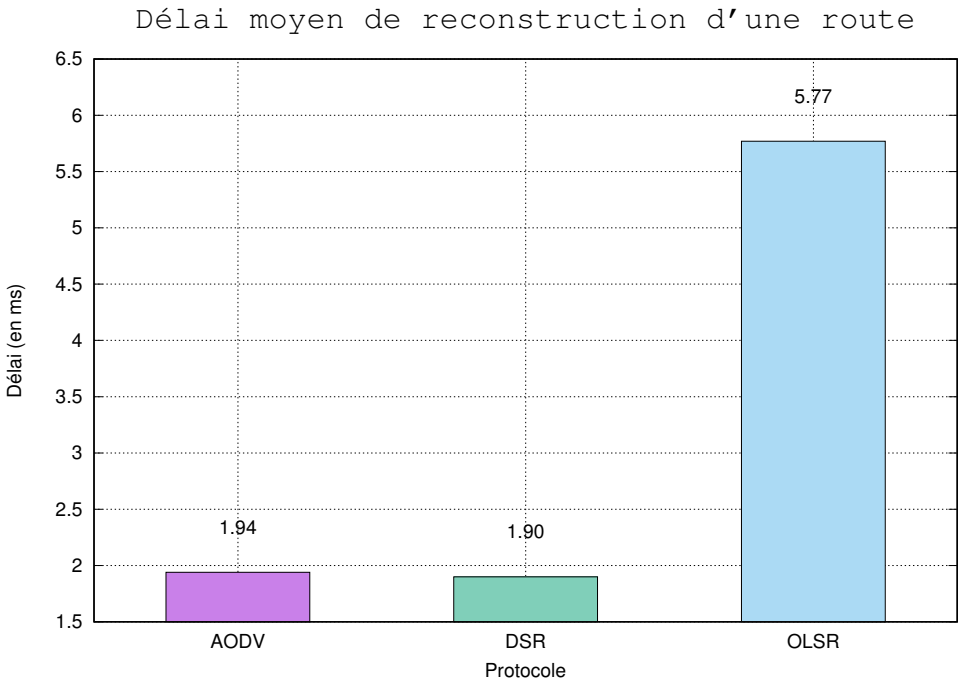


Conclusion

AODV présente de meilleures connectivités en états instables

Délai moyen de bout en bout et délai de reconstruction d'une route en environnement émulé

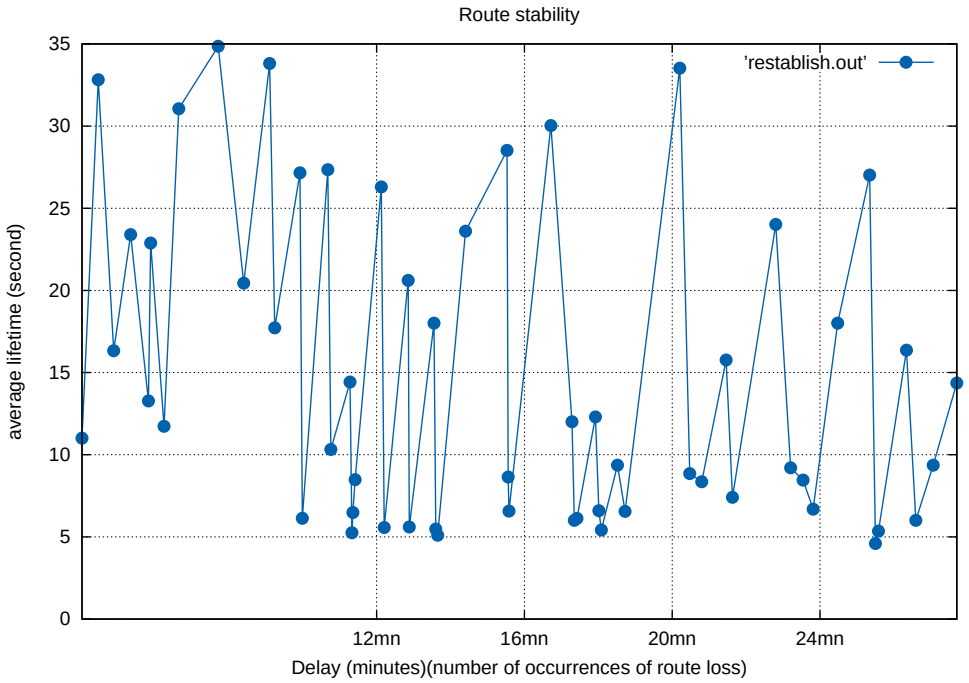




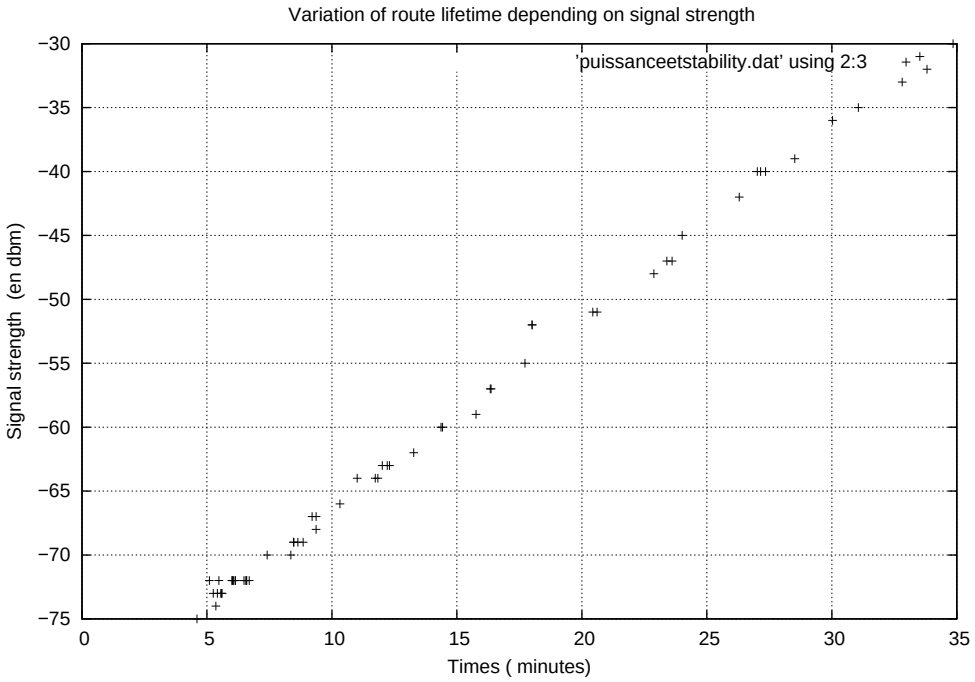
Durée de vie moyenne d'une route

Stabilité d'une route

- Durée de vie moyenne d'une route : 14.328955 s



Variation de la durée de vie de route en fonction de la force du signal reçu



Délai de rétablissement d'une route après une perte de route