La sécurité des systèmes embarqués et des objets connectés – un panorama

Eric Alata

INSA - LAAS/CNRS

Journée CAPTRONIC - Toulouse - 18 février 2016

Contexte et motivation des travaux

Sécurité des systèmes embarqués “critiques”

Sécurité des équipements grand public connectés à Internet

Sécurité dans l’IoT

Bilan

Contexte et motivation des travaux

Sécurité des systèmes embarqués “critiques”

Sécurité des équipements grand public connectés à Internet

Sécurité dans l'IoT

Bilan

Sécurité des systèmes informatiques – 1/2

Etat des lieux

- L'informatique est présente dans de nombreux secteurs
  - Moyens de transports – avions, voiture, etc
  - Objets connectés du quotidien – téléphones, systèmes d'alarmes, fridigaires, compteurs, systèmes de santé, Smart TV, etc
- Utilisation de moyens de communications très variés
  - Filaires et non filaires
  - Supportés par de multiples technologies

$\Rightarrow$ Envisager la sécurité des systèmes informatiques aujourd'hui ne se limite pas aux PCs de bureau et aux serveurs

- La sécurité des ces "nouveaux systèmes informatiques" est-elle réellement considérée sérieusement ?

Sécurité des systèmes informatiques – 2/2

Travaux du de l'équipe TSF du LAAS

- S'intérese depuis toujours à la sécurité des systèmes informatiques
- Diversification de nos travaux vers ces "nouveaux systèmes"
  - Sécurité des systèmes embarqués avioniques
    collaboration avec Airbus
  - Sécurité des communications dans les véhicules
    collaboration avec Renault
  - Sécurité des équipements grand public connectés à Internet
    nos premiers "objets connectés"
    collaboration avec Thalès

⇒ Trois thèses soutenues

  - Vient s'y ajouter une étude sur la sécurité des réseaux Lora
    collaboration avec D. Dragomirescu de l'équipe MINC

Contexte et motivation des travaux

Sécurité des systèmes embarqués “critiques”

Sécurité des équipements grand public connectés à Internet

Sécurité dans l'IoT

Bilan

Sécurité des systèmes embarqués “critiques”

Systèmes avioniques (2010-2014)

Thèse d'Anthony Dessiatnikoff

Projet ANR SOBAS

Contexte des travaux – 1/2

Les systèmes avioniques d'aujourd'hui – l'IMA

- Evolution vers une architecture de type IMA (*Integrated Modular Avionics*)
  - Fin de l'isolation complète des fonctions avioniques
  - Partage de ressources et communications via un bus (AFDX)
  - Utilisation de COTS
- Historiquement, nombreuses normes pour la *safety*
- ... mais peu concernant la *security*

$\Rightarrow$ Les malveillances sont sérieusement considérées

Contexte des travaux – 2/2

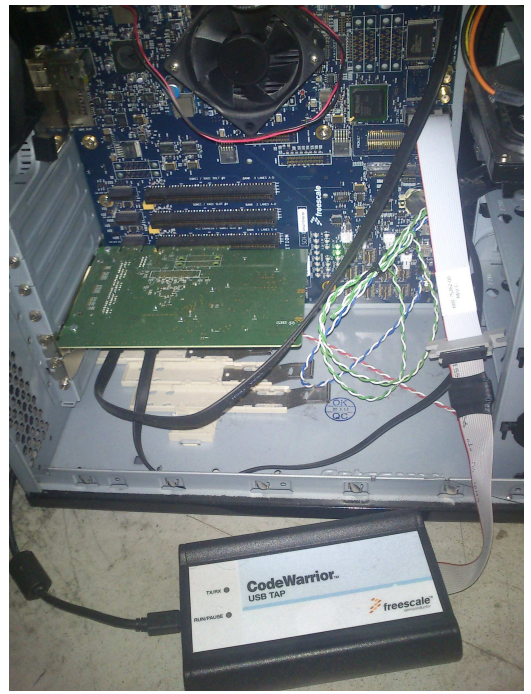
Le projet SOBAS

- Projet ANR *Securing On-Board Aerospace Systems*
- Objectif : étudier les vulnérabilités des couches basses du logiciel durant le développement
- Tests sur un noyau embarqué expérimental fourni par Airbus France
  - Réalisation d'un certain nombre d'expérimentations visant à mettre en évidence des vulnérabilités
  - Expérimentations qui peuvent influer sur le développement du noyau (qui est en cours) – **un des objectifs de SOBAS**

La plateforme de tests

Caractéristiques du noyau

- Minimaliste
- Partitions utilisateurs – faible niveau de criticité
- Partitions système – haut niveau de criticité
- Partitionnement spatial et temporel assuré par la MMU (*Memory Management Unit*) et le MPIC (*Multicore Programmable Interrupt Controller*)



Caractéristiques du matériel

- Plateforme P4080 de FreeScale
  - Fonctionnalités de télécom.
  - 8 cœurs, MMU, caches, PAMU, etc
- CodeWarrior et un port JTAG
  observation et injections d'attaques

Expérimentations

Hypothèses d'attaques

- Une partition utilisateur non-critique est malveillante et essaie de corrompre une autre partition ou le noyau lui-même

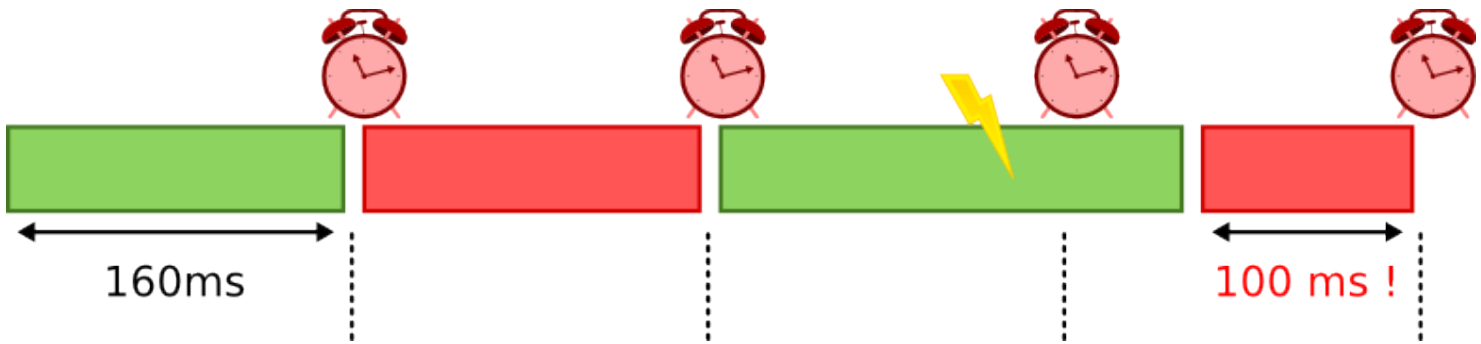
Attaques réalisées

- Ciblant les fonctions de base d'un calculateur (processeur, gestion de la mémoire, gestion du temps, etc)
- Ciblant les mécanismes de tolérance aux fautes (diagnostic de fautes)

Exemple d'attaque – 1/2

Mécanismes de gestion du temps

- Objectif de l'attaque : modifier le temps de cycle d'une partition critique depuis une partition non-critique
- Ordonnancement des partitions géré par le MPIC
  - ⇒ Impossible de générer des interruptions depuis une partition utilisateur
- Idée : augmenter la durée d'exécution de la partition malveillante pour réduire la durée d'exécution de la partition critique qui suit
  - ⇒ Déclenchement d'une exception de façon à exécuter du code noyau non interruptible, le plus long possible



Exemple d'attaque – 2/2

Diagnostic de fautes

- Mise à l'épreuve de la gestion des exceptions à l'aide d'un programme de type `crashme`
- Programme exécuté sur 1 million de cycles de la partition : exécution de 100 instructions aléatoires à chaque cycle
- Pas de crash du noyau mais ...
  - Beaucoup d'exceptions provoquent à tord le redémarrage de la partition, du noyau ou du système complet

  $\Rightarrow$ Nécessité d'améliorer l'analyse des causes d'exceptions pour prendre des décisions moins radicales

- Les attaques peuvent cibler les spécificités de ces systèmes
- Les études durant le développement permettent de consolider l'architecture

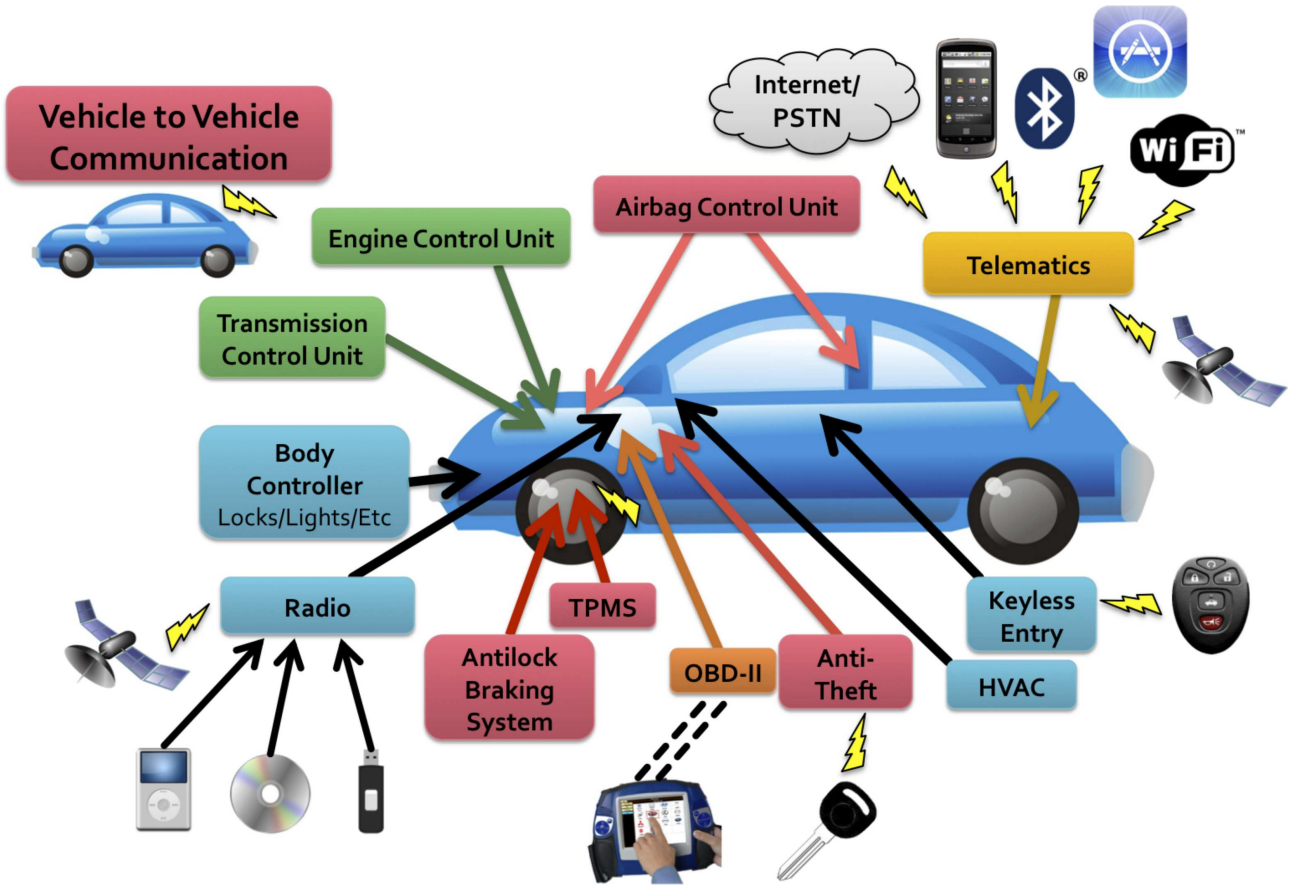
Sécurité des systèmes embarqués “critiques”

Systèmes automobiles (2012-2015)

Thèse de Ivan Studnia

Cifre Renault

Contexte des travaux



Comprehensive Experimental Analyses of Automotive Attack Surfaces Stephen Checkoway, Damon McCoy, Brian Kantor et al.

- De plus en plus d'informatique et d'électronique embarquées
- *Electronic Control Unit*
- Communications réseau inter-ECU sur Bus CAN

De multiples attaques

Attaques locales

- L'attaquant possède un accès au réseau

⇒ Lire du trafic

⇒ Emettre des trames

⇒ Interrompre le trafic

Attaques distantes

- Attaque physique indirect
  (lecteur multimédia, valise de diag.)
- Attaque à courte portée
  (bluetooth, ouverture à distance)
- Attaque à longue portée
  (réseaux mobiles)

⇒ **Classification des attaques**

Objectifs

- Défi intellectuel
- E-tuning
- Vol
- Sabotage
- Vol de données

Un IDS sur Bus CAN – 1/5

Hypothèse d'attaque

- L'attaquant contrôle un ECU
- Il connaît le système
- Il interagit avec le réseau

Attaques considérées

- Trames inconnues ou ne respectant pas les spécifications
- Trames périodiques en supplément du trafic légitime
- Trames périodiques substituées au trafic légitime
- Trames ponctuelles, apériodiques

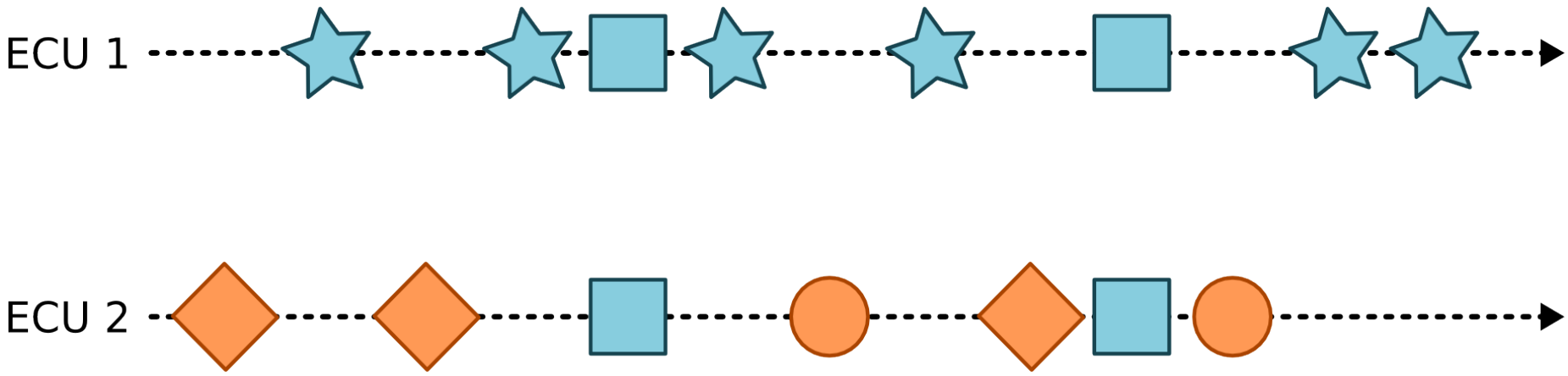
Un IDS sur Bus CAN – 2/5

Les contraintes

- Pas d'instrumentation des ECU
- Pas de modification de la topologie
- Réutilisable (utilisation de COTS)
- Ressources limitées
- Maintenance longue (20 ans)
- Traitement rapide (système temps réel)

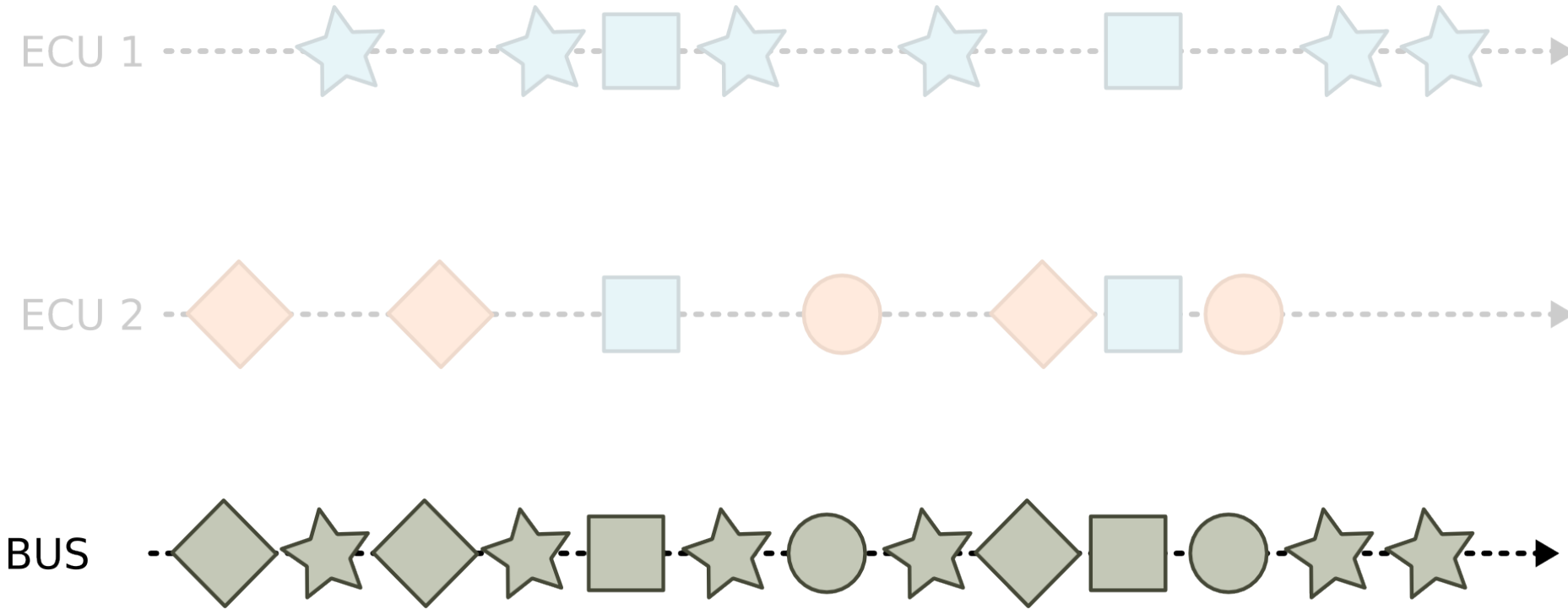
Un IDS sur Bus CAN – 3/5

Principe de l'IDS



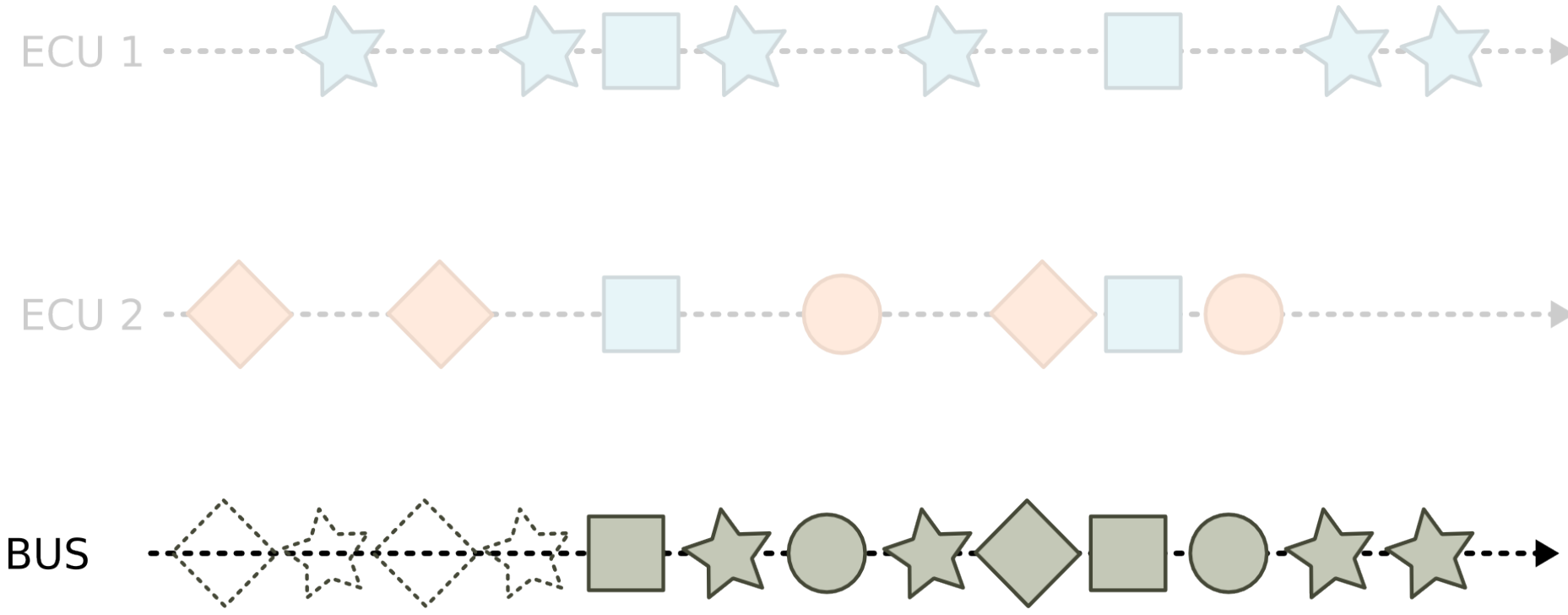
Un IDS sur Bus CAN – 3/5

Principe de l'IDS



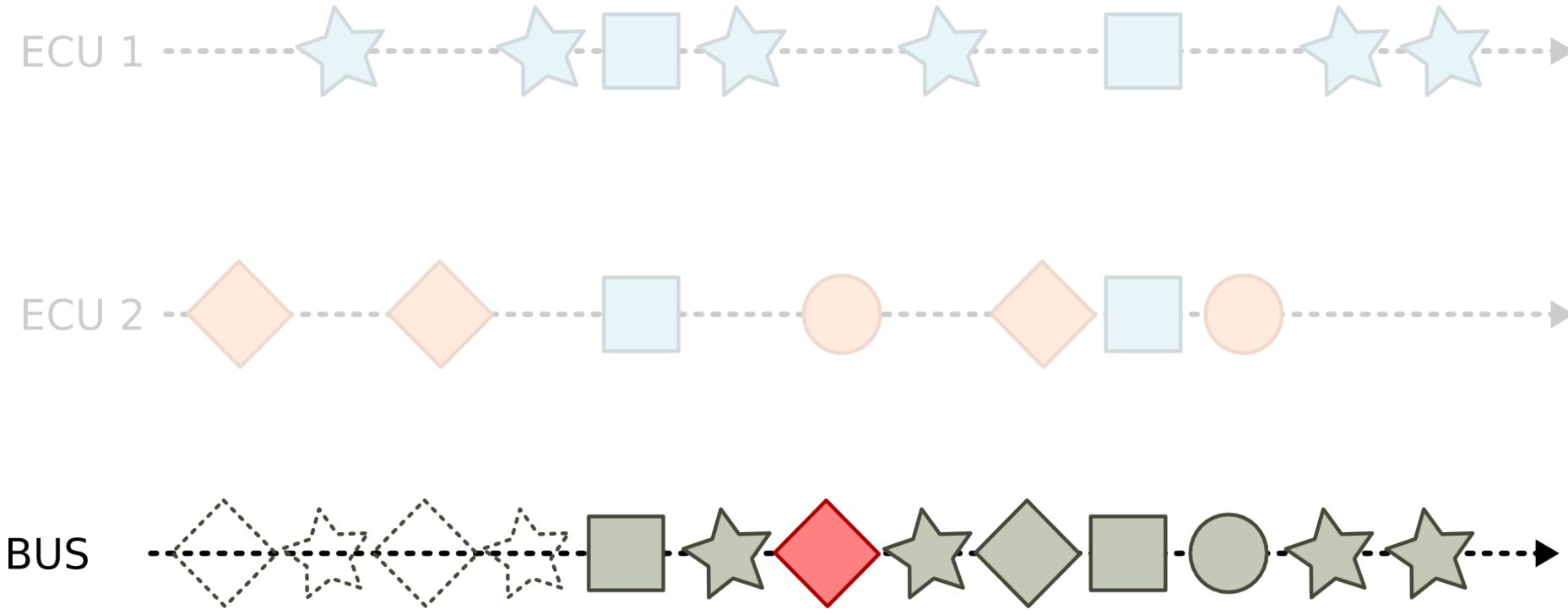
Un IDS sur Bus CAN – 3/5

Principe de l'IDS



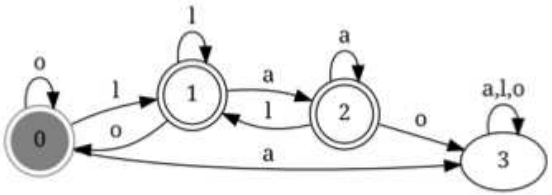
Un IDS sur Bus CAN – 3/5

Principe de l'IDS

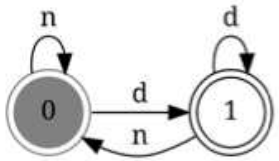


Un IDS sur Bus CAN – 4/5

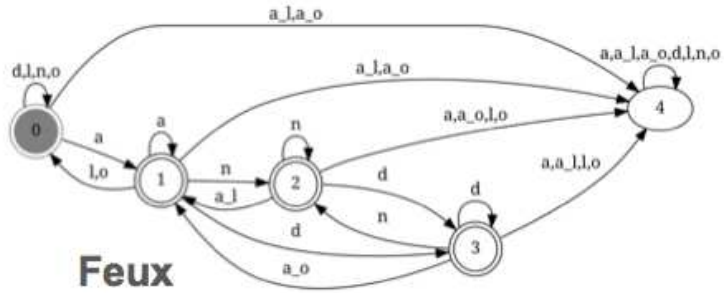
Approche orientée langage



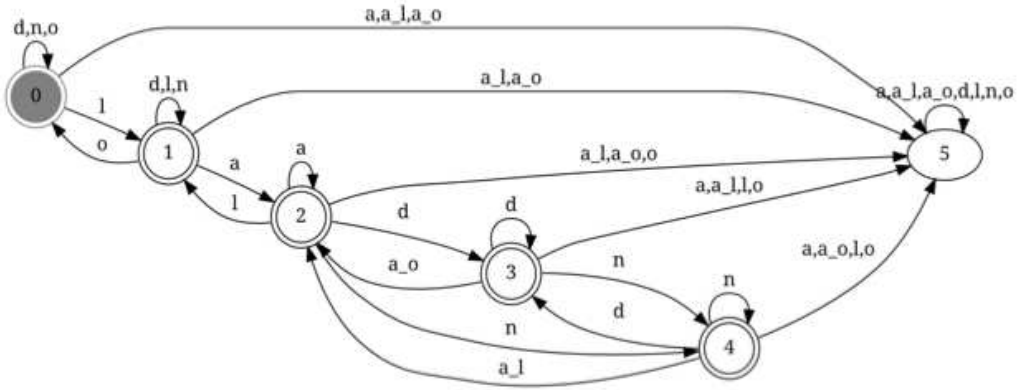
Commande



Capteur

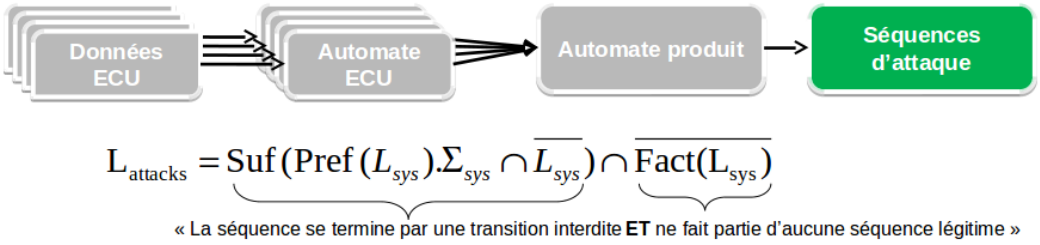


Feux

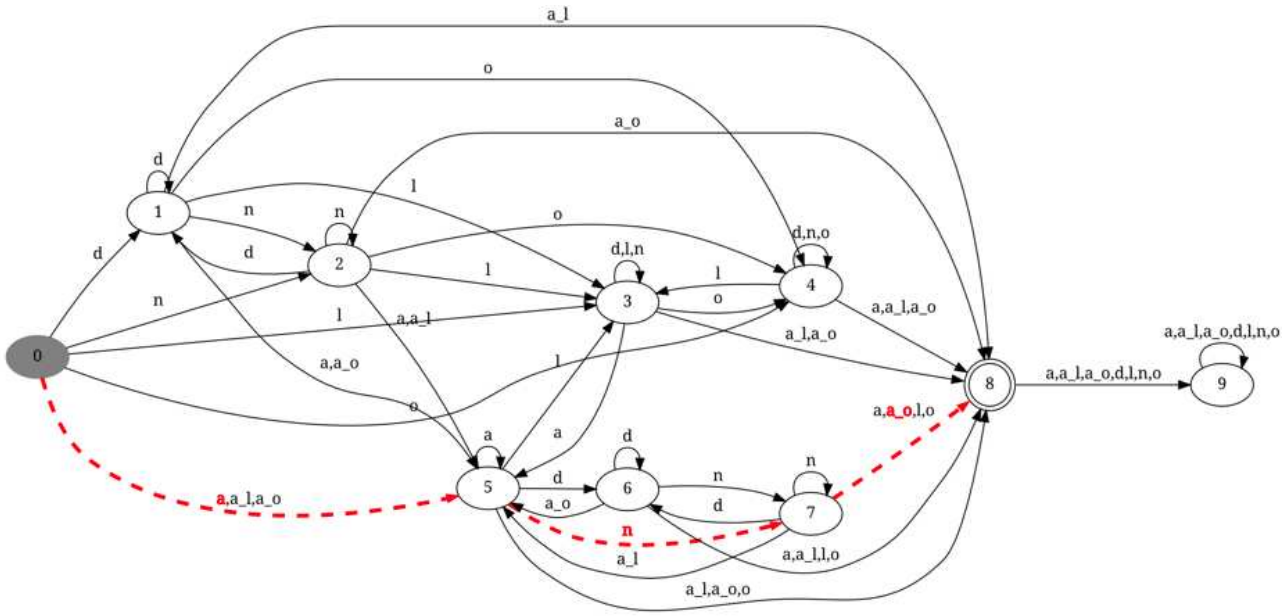


Un IDS sur Bus CAN – 5/5

Approche orientée langage



$$L_{attacks} = \underbrace{Suf(Pref(L_{sys}).\Sigma_{sys} \cap \overline{L_{sys}})}_{\text{« La séquence se termine par une transition interdite ET ne fait partie d'aucune séquence légitime »}} \cap \overline{Fact(L_{sys})}$$



- Contrairement au domaine IT, on peut se baser sur la connaissance du comportement des *petits* composants pour mieux se protéger

Sécurité des équipements grand public connectés à Internet

Systèmes grand public (2012-2015)

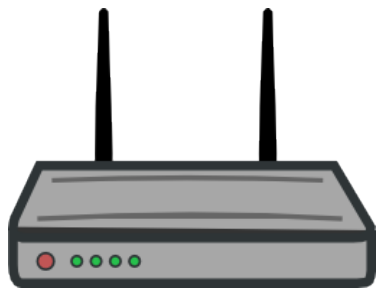
Thèse de Yann Bachy

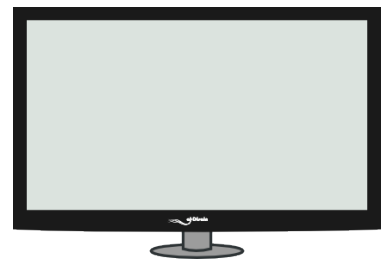
Cifre Thalès

Émergence des équipements grand public connectés

Les risques ?

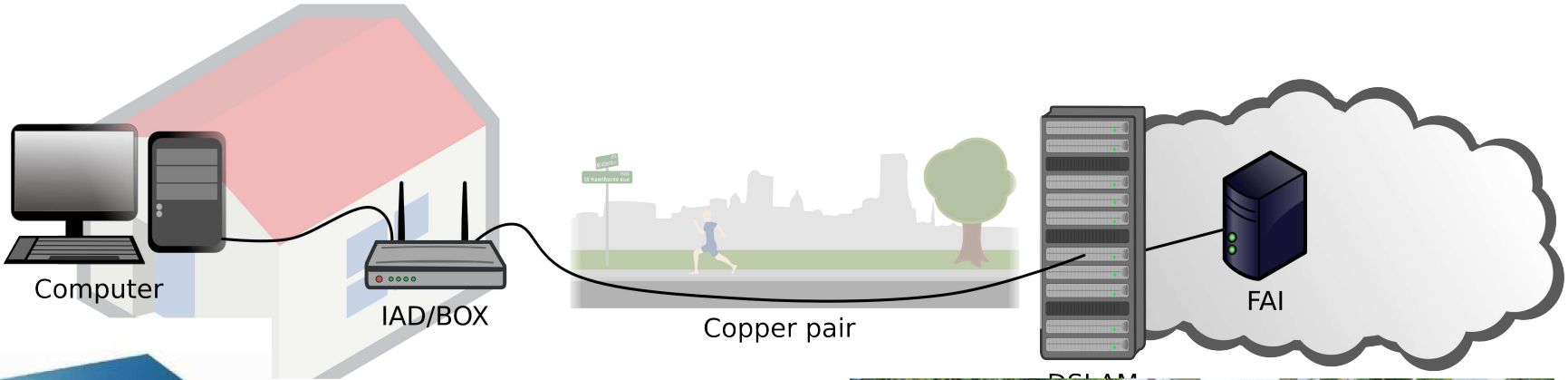
- Pas de réelle prise en compte de la sécurité ni de la protection de la vie privée par les constructeurs de ces matériels
- Cible de notre étude : équipements connectés possédant plusieurs interfaces de communication, pouvant être utilisés comme relai dans le cas d'attaque – deux cas d'étude



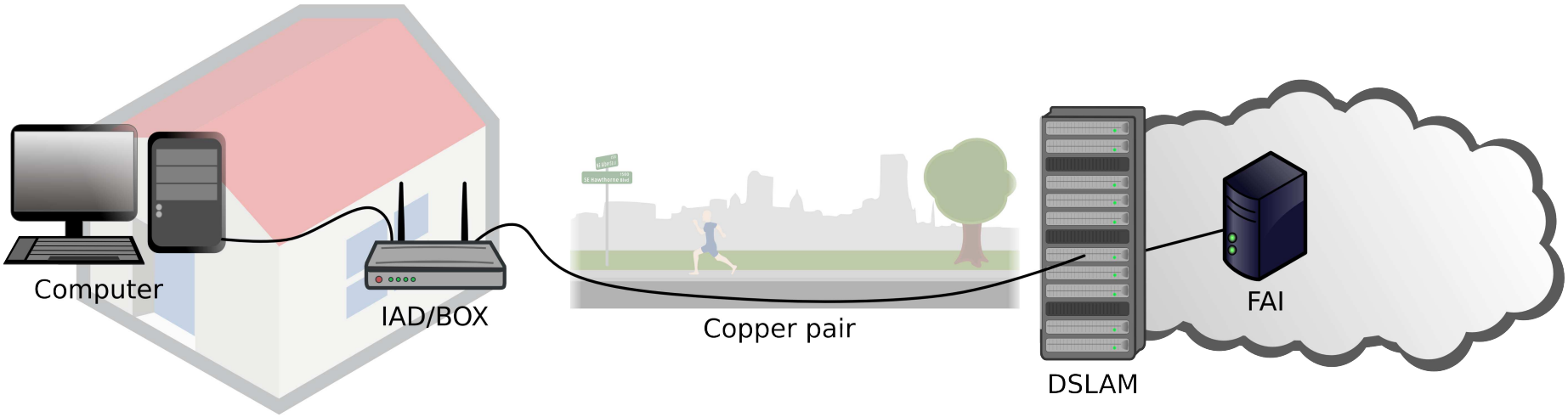


- Hypothèse d'attaque : exploitation de la communication avec les fournisseurs de service qui est insufisamment sécurisée

La Box ADSL – 1/2

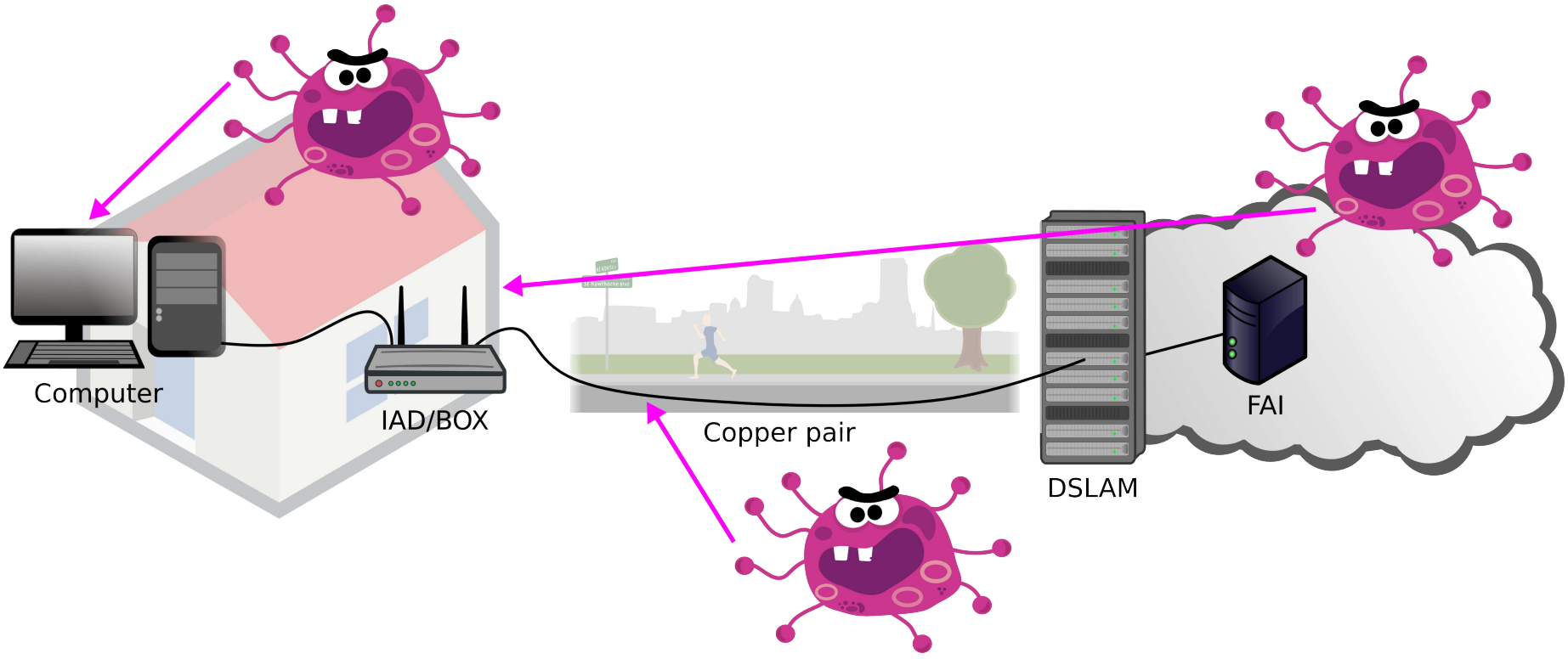


La Box ADSL – 2/2



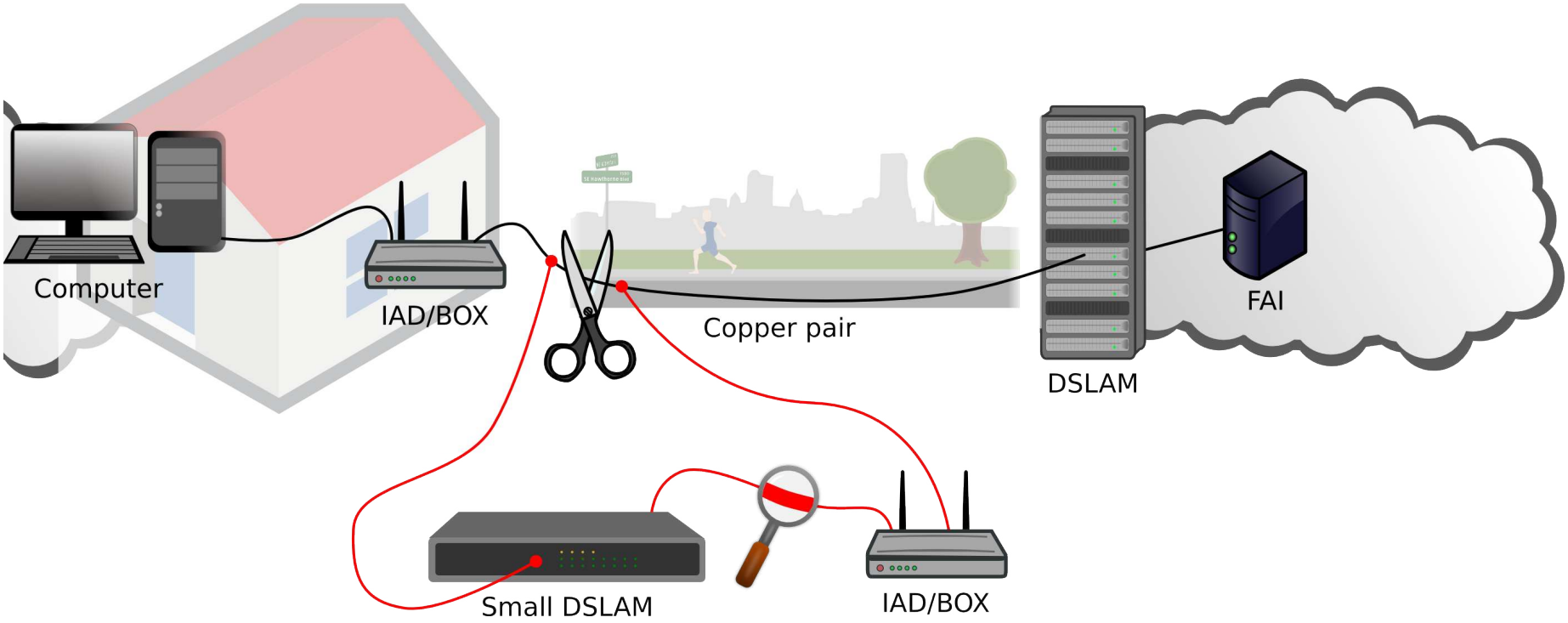
- La Box ADSL *pense* être connectée au DSLAM via la paire cuivrée
- Cette paire cuivrée véhicule deux types de messages
  - Messages du FAI : **lien virtual de confiance**
  - Messages échangés avec Internet

Les chemins d'attaque



- Attaques depuis Internet
- Attaques locales
- Attaques sur la paire cuivrée

Expérimentations



- **Man in the middle attack**

Résultats obtenus

Remplacement du firmware

- Désactivation (partielle) du pare-feu
- Ajout d'un compte super-utilisateur
- Désactivation des mises à jour
- Installation de logiciel "soft-phone"

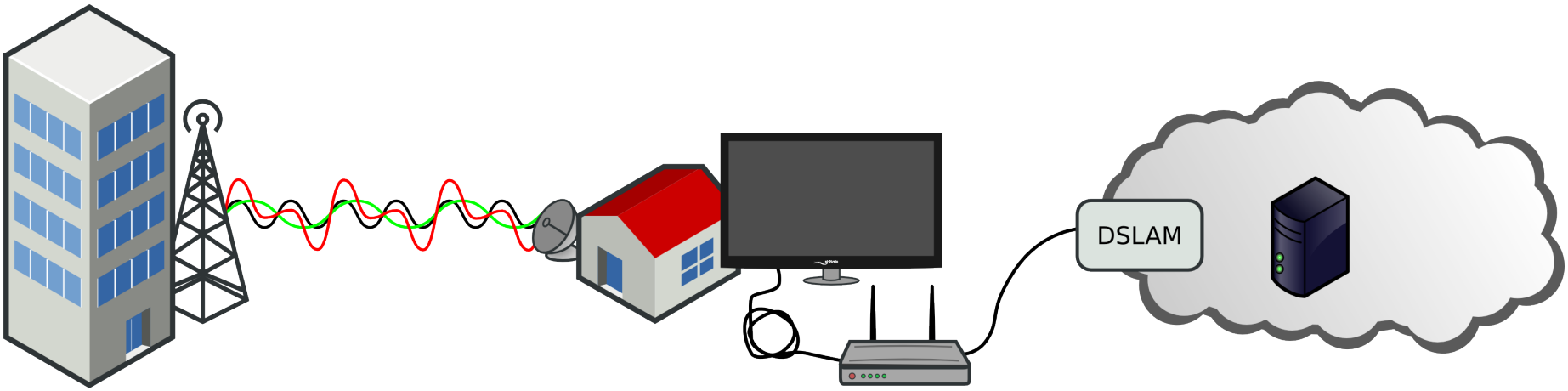
Exploitations réalisées

- Utilisation à distance de la Box pour émettre des appels "surtaxés"
- Connexion à distance sur la Box (via porte dérobée)

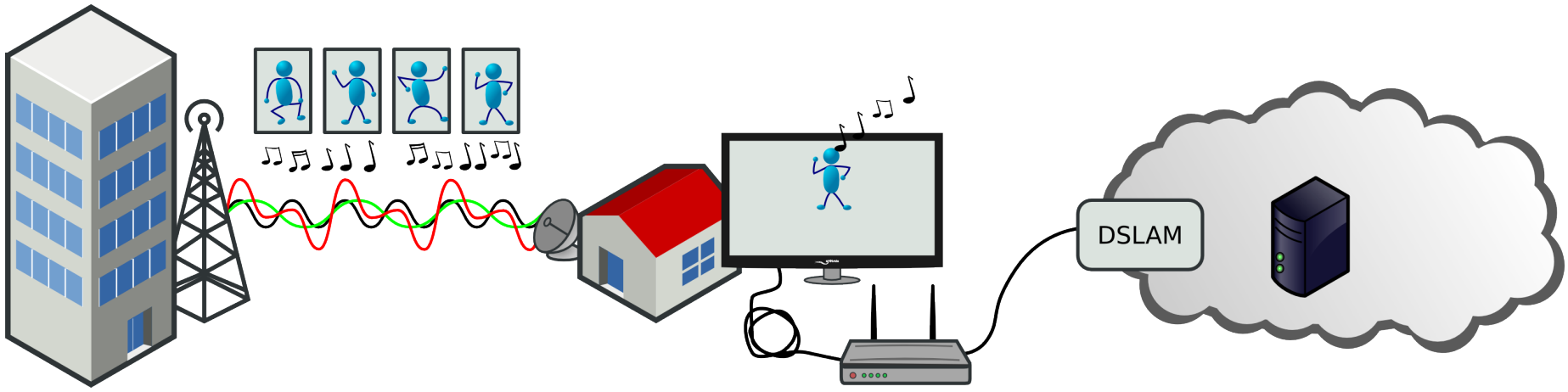
Autres exploitations envisagées

- Réalisation d'un botnet
- Attaques DDos
- Proxy

Utilisation d'une Smart TV

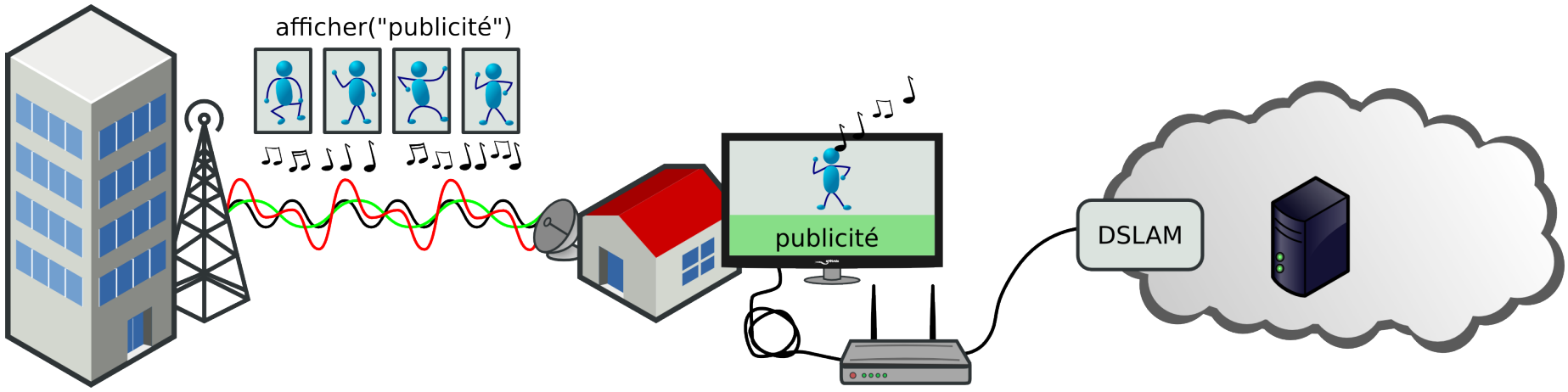


Utilisation d'une Smart TV



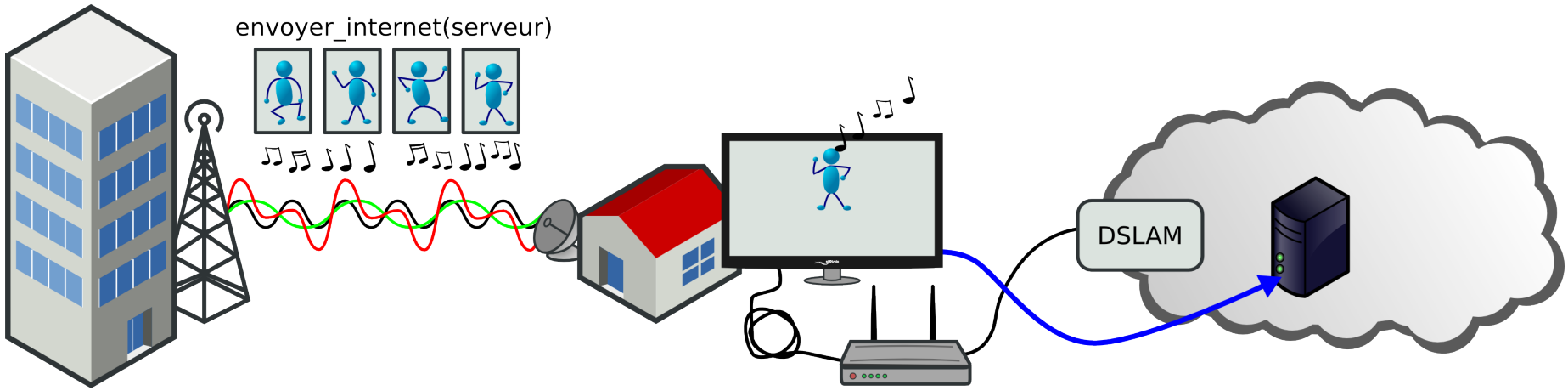
- Envoi d'une séquence vidéo et audio multiplexée

Utilisation d'une Smart TV



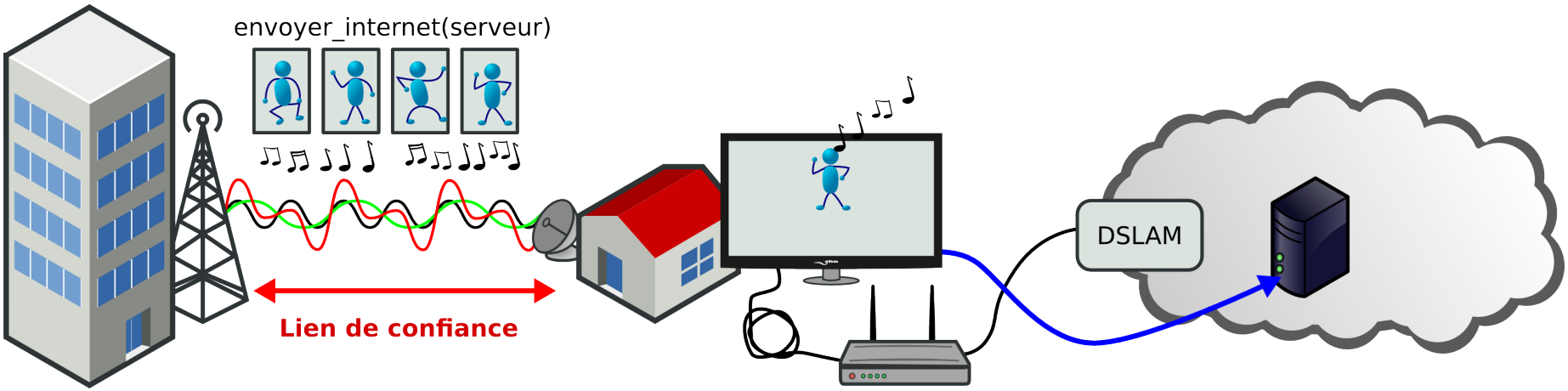
- Envoi d'une séquence vidéo et audio multiplexée
- Ajout d'un flux de données pour contrôler la manière dont le contenu est rendu
  - Affichage d'informations contextuelles (publicité, informations, ...)

Utilisation d'une Smart TV



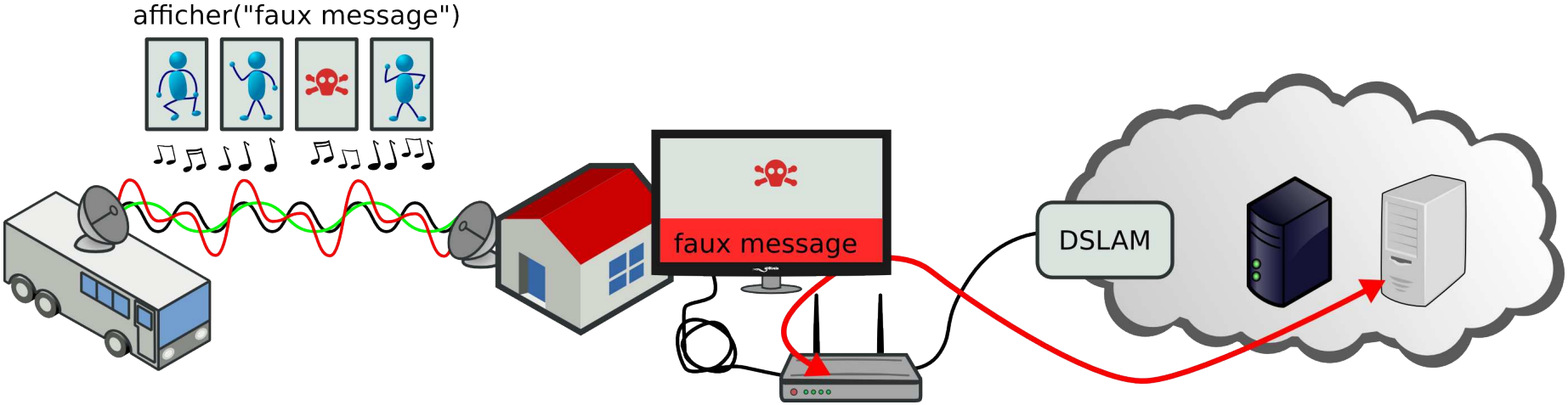
- Envoi d'une séquence vidéo et audio multiplexée
- Ajout d'un flux de données pour contrôler la manière dont le contenu est rendu
  - Affichage d'informations contextuelles (publicité, informations, ...)
  - Interrogation de serveurs distants (vote, sondage, audimat, ...)

Chemin d'attaque envisagé



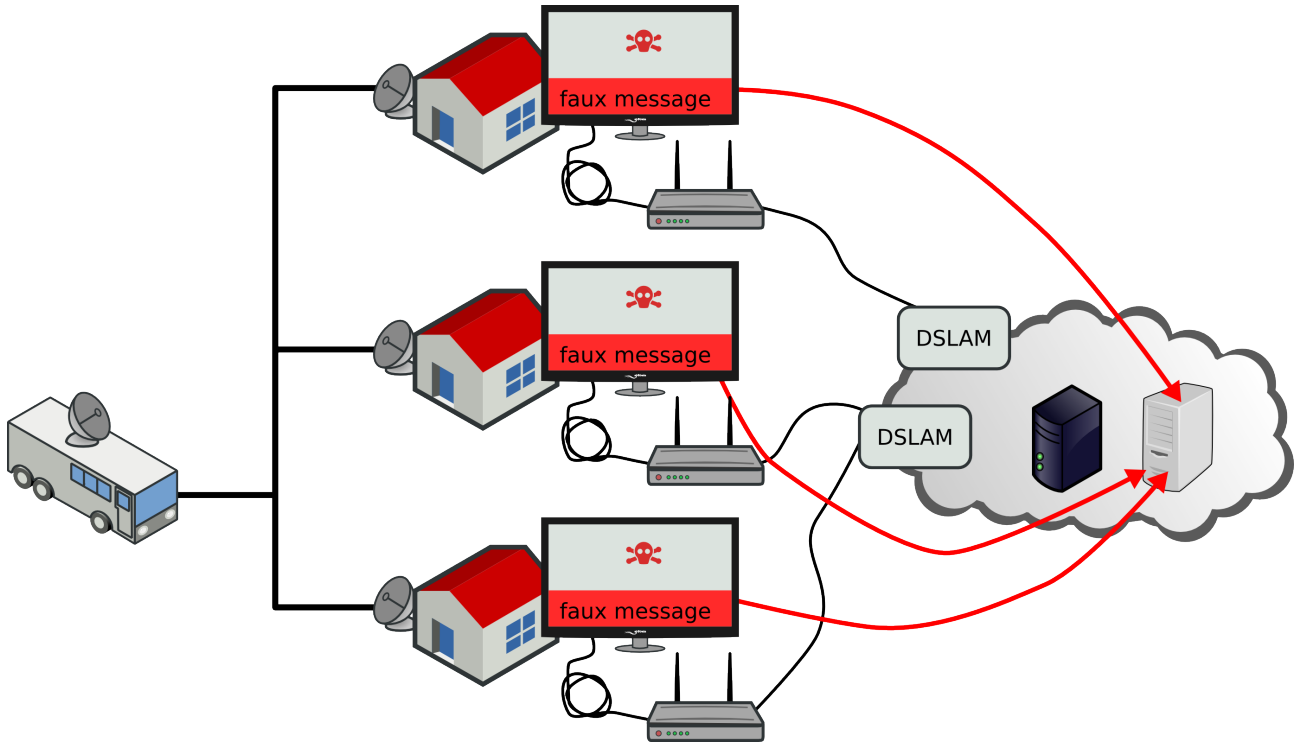
- Lien de confiance de l'antenne vers la TV – confiance légitime ?
- Pas d'authentification du fournisseur de service par la TV

Scénario d'attaque



- Inclusions de données malveillantes dans le flux de données
- La TV exécute les actions correspondant à ces données
  - Relai pour cibler un équipement de la maison (Box, ...)
  - Reconfiguration depuis la TNT de la Box pour ouvrir lun flux réseau depuis l'extérieur

Scénario d'attaque



- Diffusion depuis un point fortement habité
- Prise de contrôle de plusieurs TV ⇒ Constitution d'un *botnet* de TV

- Toute évolution nécessite de remettre en cause les choix historiques

Sécurité dans l'IoT

Réseaux LoRa (2015-2016)

Stage de Gabriel Mabille

et de Frédéric Recoules

Collaboration avec l'équipe MINC (D. Dragomirescu)

Objectifs de l'étude

Problématique

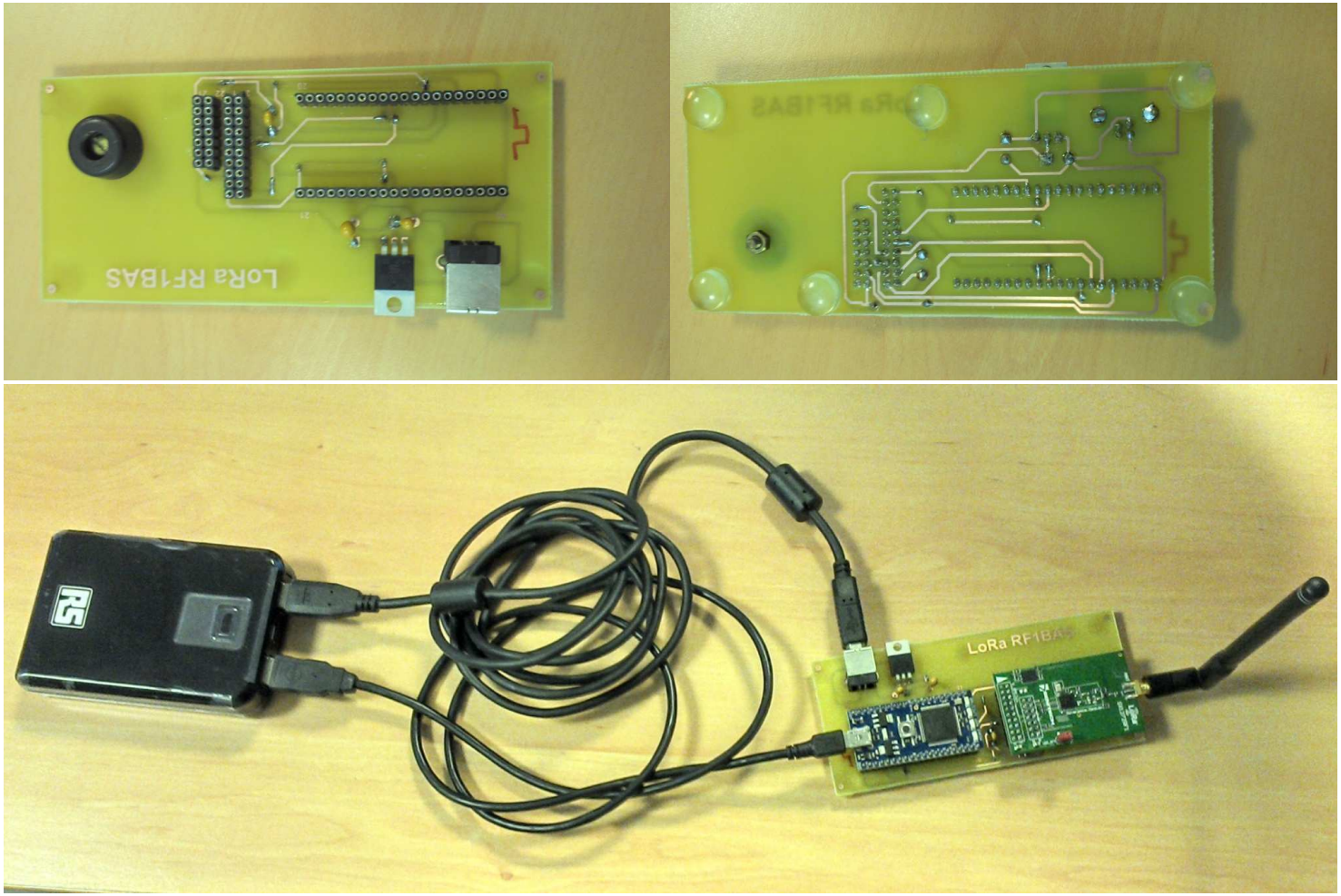
- Les composants qui implémentent le protocole LoRa disposent de ressources limitées
- Ces composants sont déployés dans des environnements ouverts
- Leur emplacement n'est pas forcément physiquement protégé

$\Rightarrow$ La sécurité de ces composants est plus qu'une question de logiciel

Objectifs

- Conception d'un objet communicant LoRa
- Analyse de la couche physique
- Expérimentations et tests

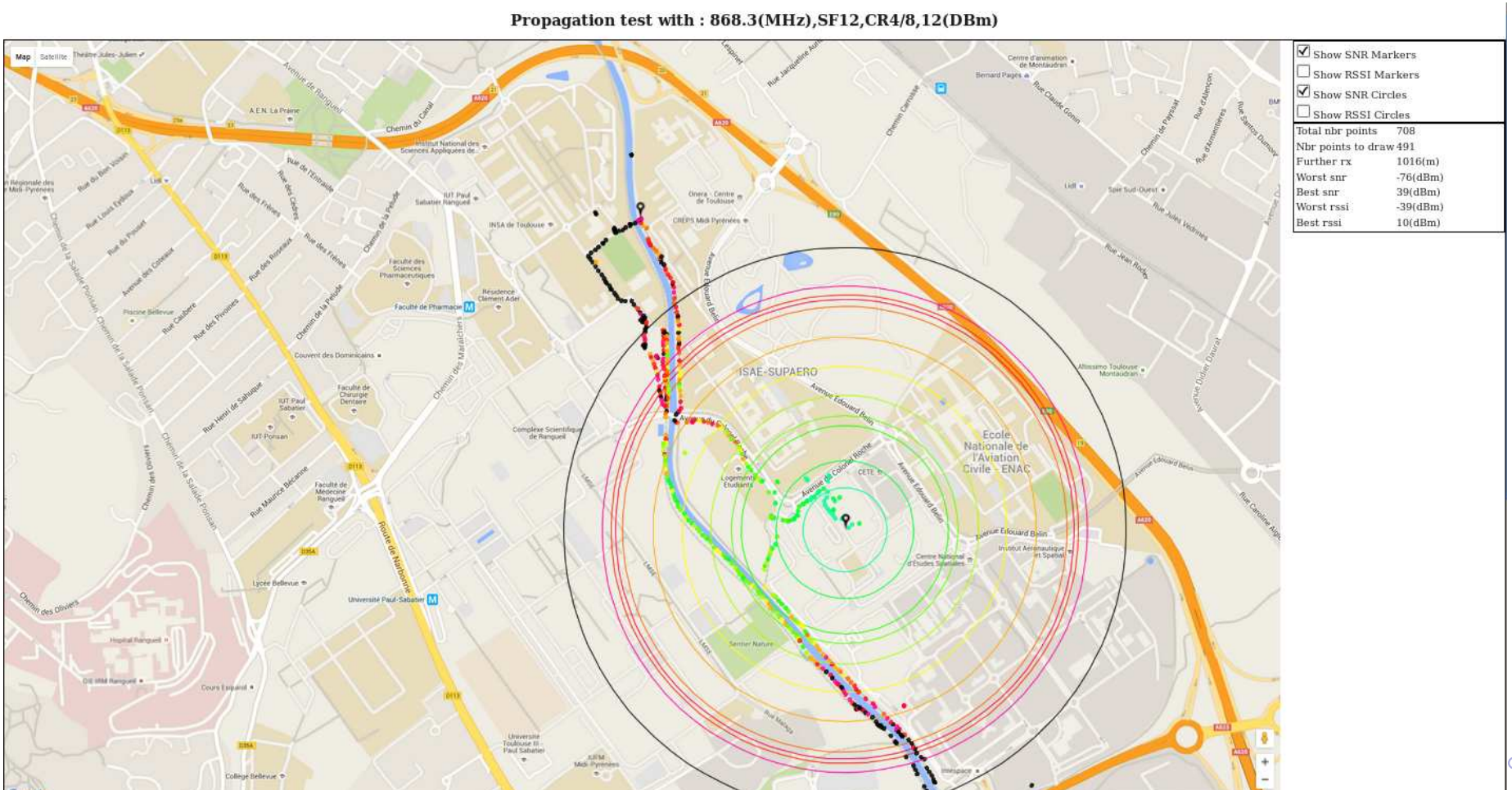
Maquette d'un objet LoRa



Analyse du composant – 1/2

Analyse de la portée du composant

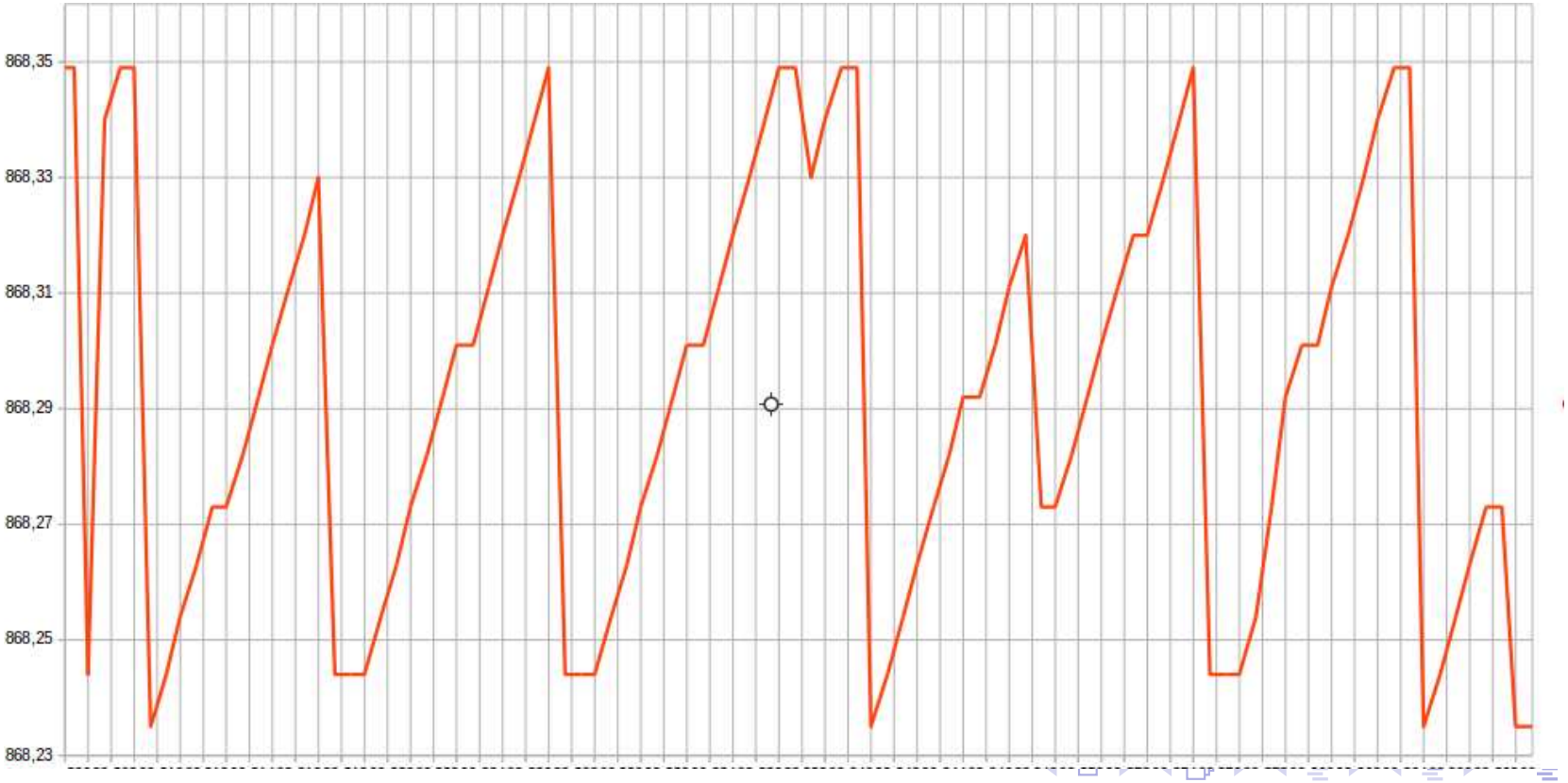
- Mesure de la qualité du signal en fonction de la distance entre le composant et la borne
- Expérience réalisée proche du LAAS



Analyse du composant – 2/2

Début du *reverse* du protocole de communication

- Analyse de la spécification : usage de mécanisme cryptographique
  Mais, il existe des implémentations qui ne suivent pas compplètement la spécification !
- Utilisation d'un analyseur logique pour caractériser les couches physiques et MAC



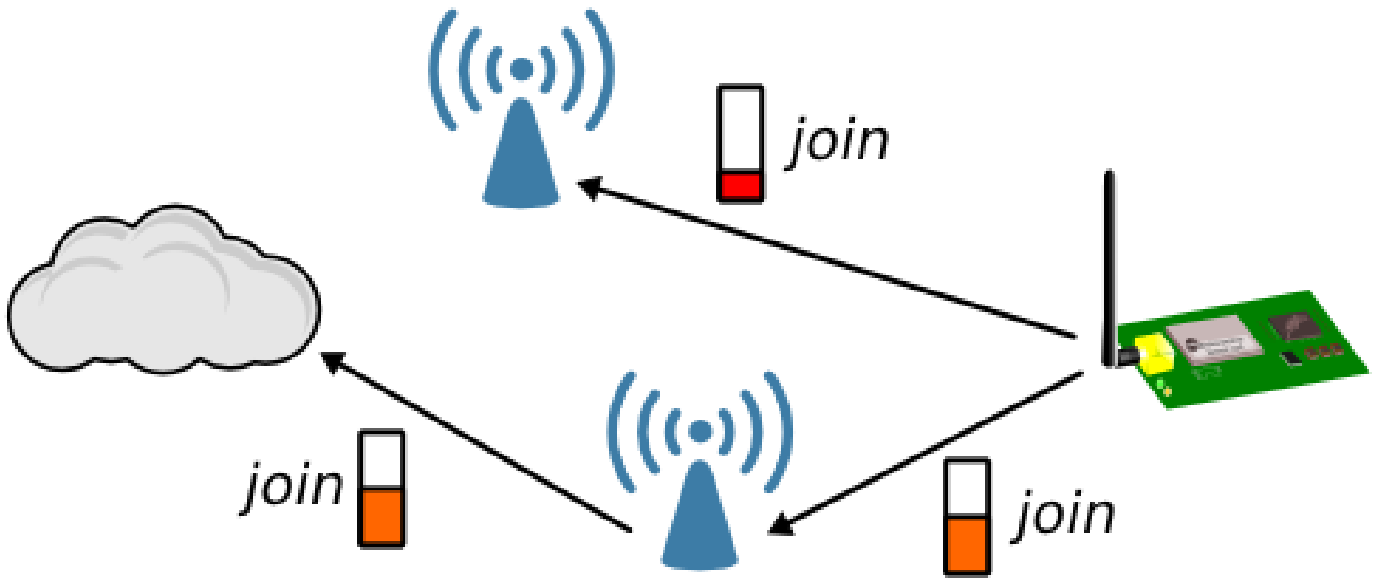
Expérimentations – 1/2

- Installation d'une borne malveillante / compromission d'une borne
- Borne privilégiée par l'infrastructure pour contacter le composant
  En fonction de la qualité du signal

⇒ Rupture dans le canal de communication

⇒ Atteinte à la disponibilité

- Piste de réflexion : *geo-privacy*, *distance bounding protocol*, etc



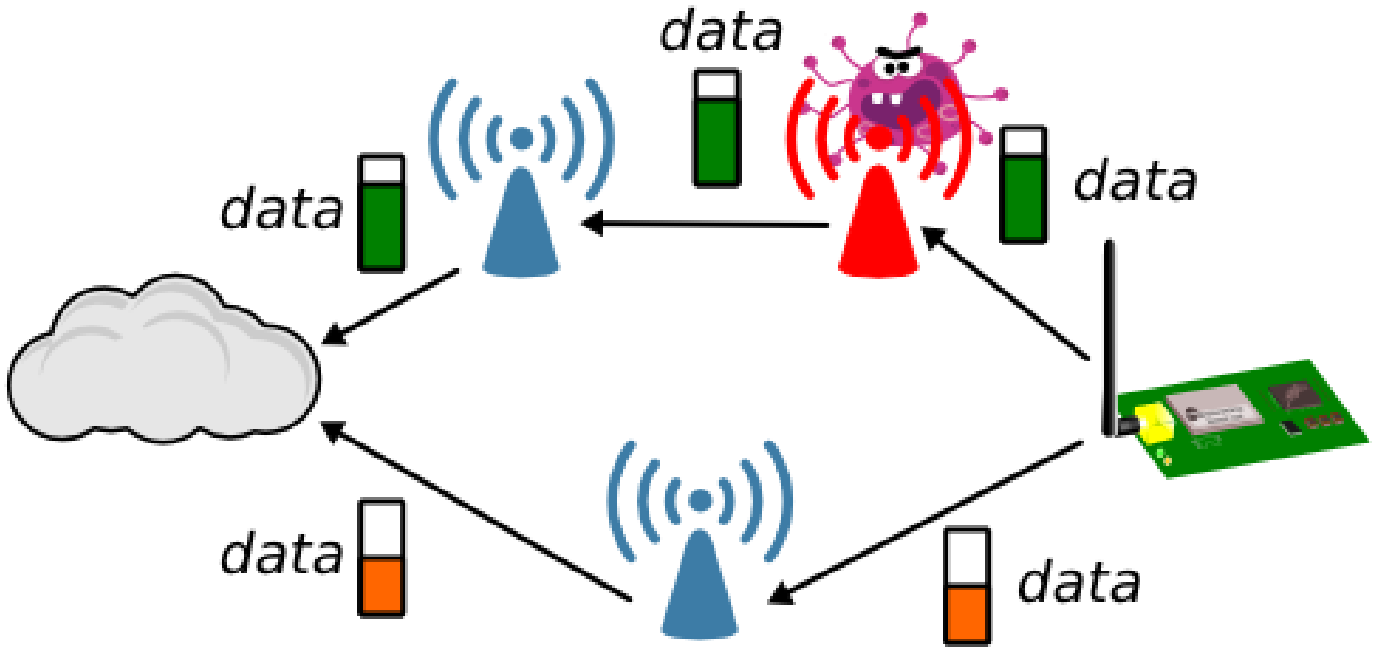
Expérimentations – 1/2

- Installation d'une borne malveillante / compromission d'une borne
- Borne privilégiée par l'infrastructure pour contacter le composant
  En fonction de la qualité du signal

⇒ Rupture dans le canal de communication

⇒ Atteinte à la disponibilité

- Piste de réflexion : *geo-privacy*, *distance bounding protocol*, etc



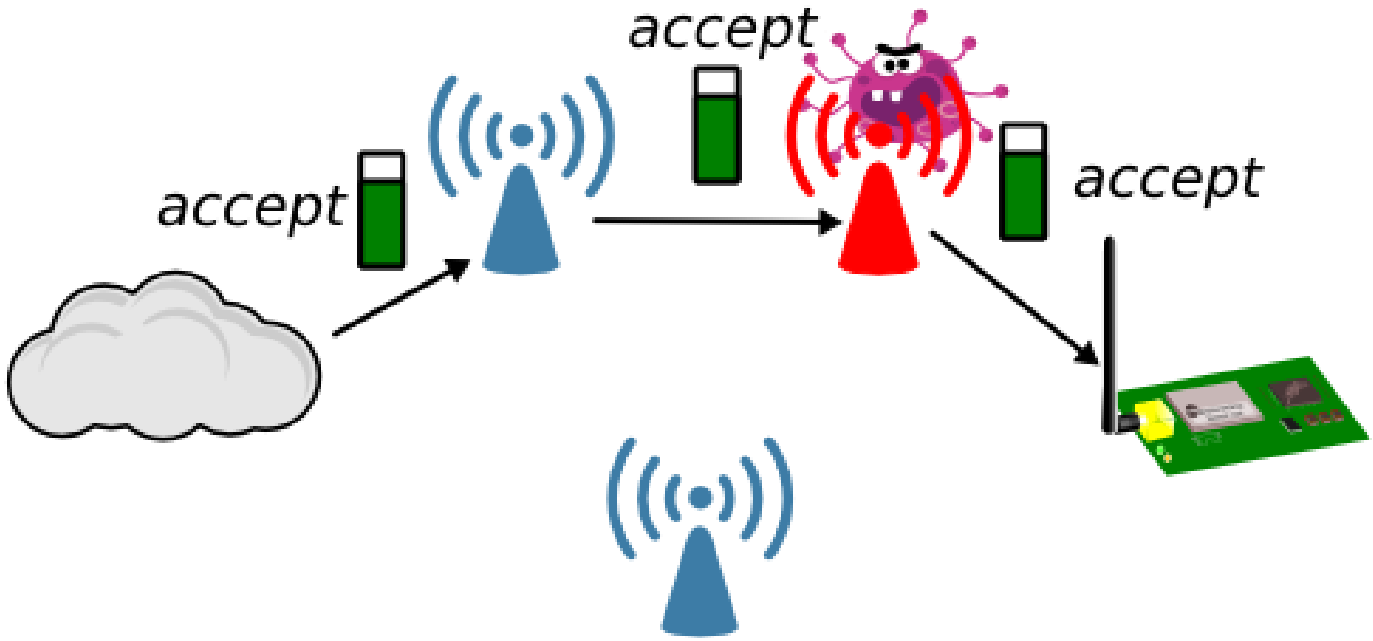
Expérimentations – 1/2

- Installation d'une borne malveillante / compromission d'une borne
- Borne privilégiée par l'infrastructure pour contacter le composant
  En fonction de la qualité du signal

⇒ Rupture dans le canal de communication

⇒ Atteinte à la disponibilité

- Piste de réflexion : *geo-privacy*, *distance bounding protocol*, etc



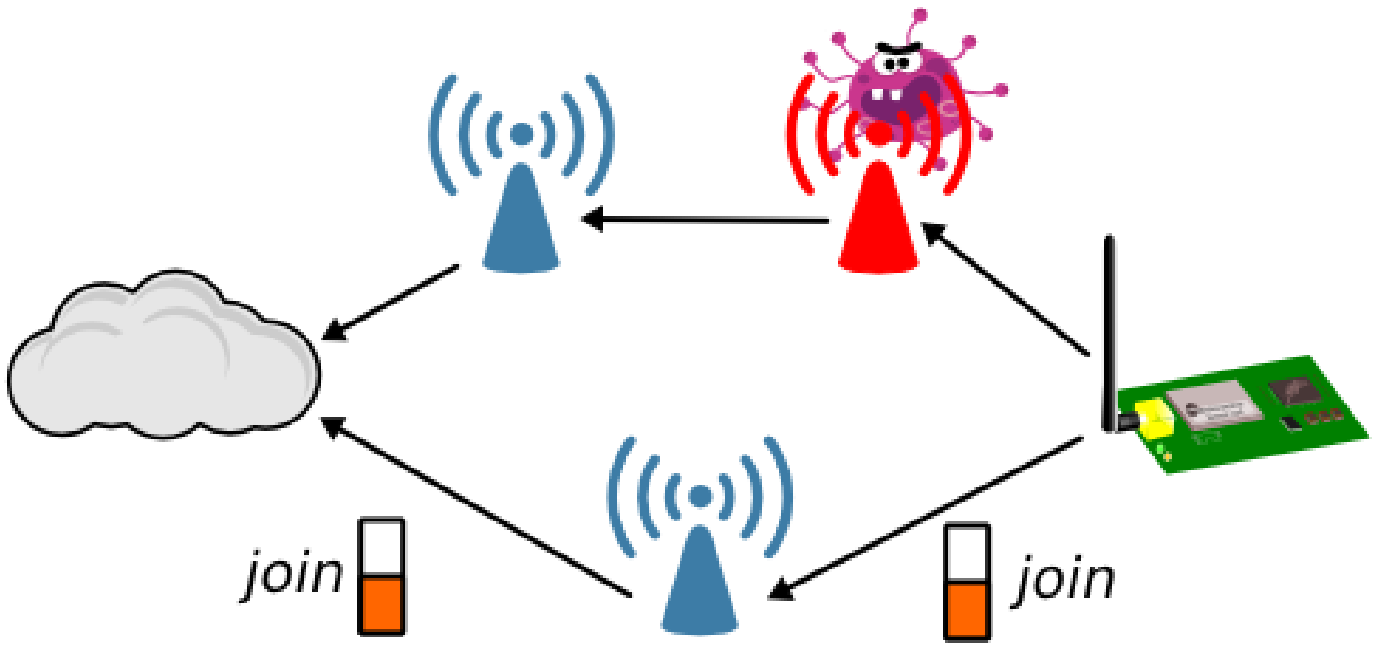
Expérimentations – 1/2

- Installation d'une borne malveillante / compromission d'une borne
- Borne privilégiée par l'infrastructure pour contacter le composant
  En fonction de la qualité du signal

$\Rightarrow$ Rupture dans le canal de communication

$\Rightarrow$ Atteinte à la disponibilité

- Piste de réflexion : *geo-privacy*, *distance bounding protocol*, etc



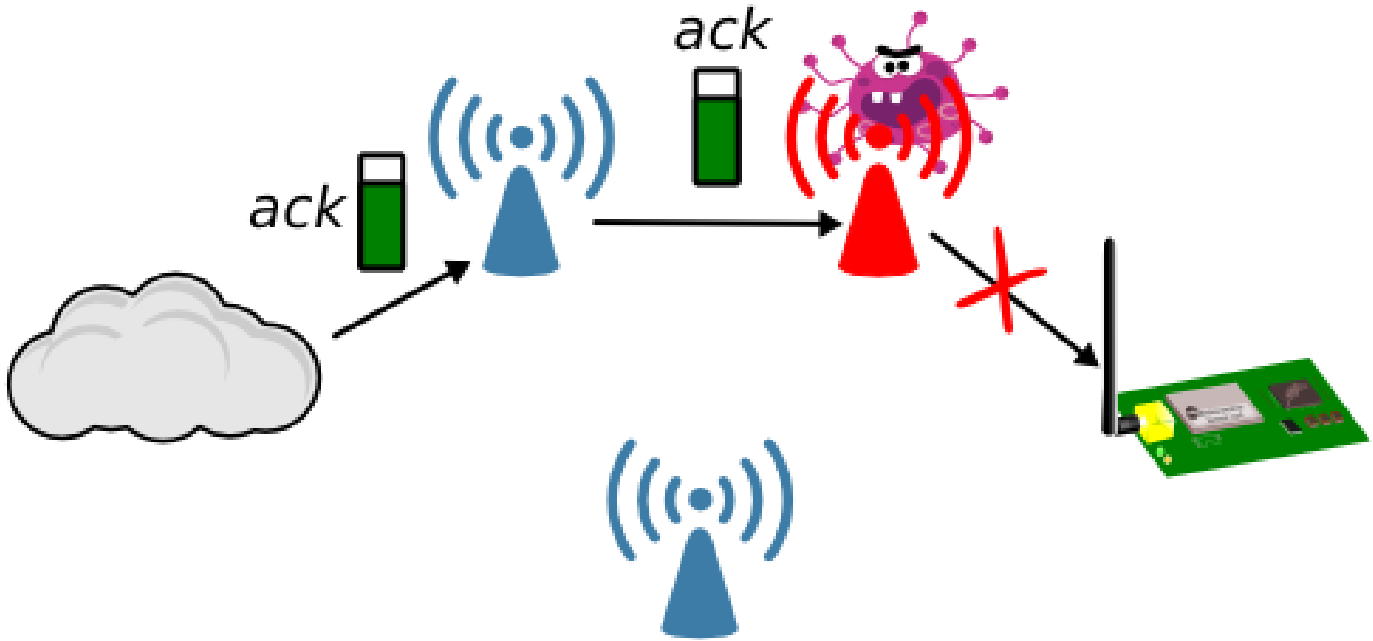
Expérimentations – 1/2

- Installation d'une borne malveillante / compromission d'une borne
- Borne privilégiée par l'infrastructure pour contacter le composant
  En fonction de la qualité du signal

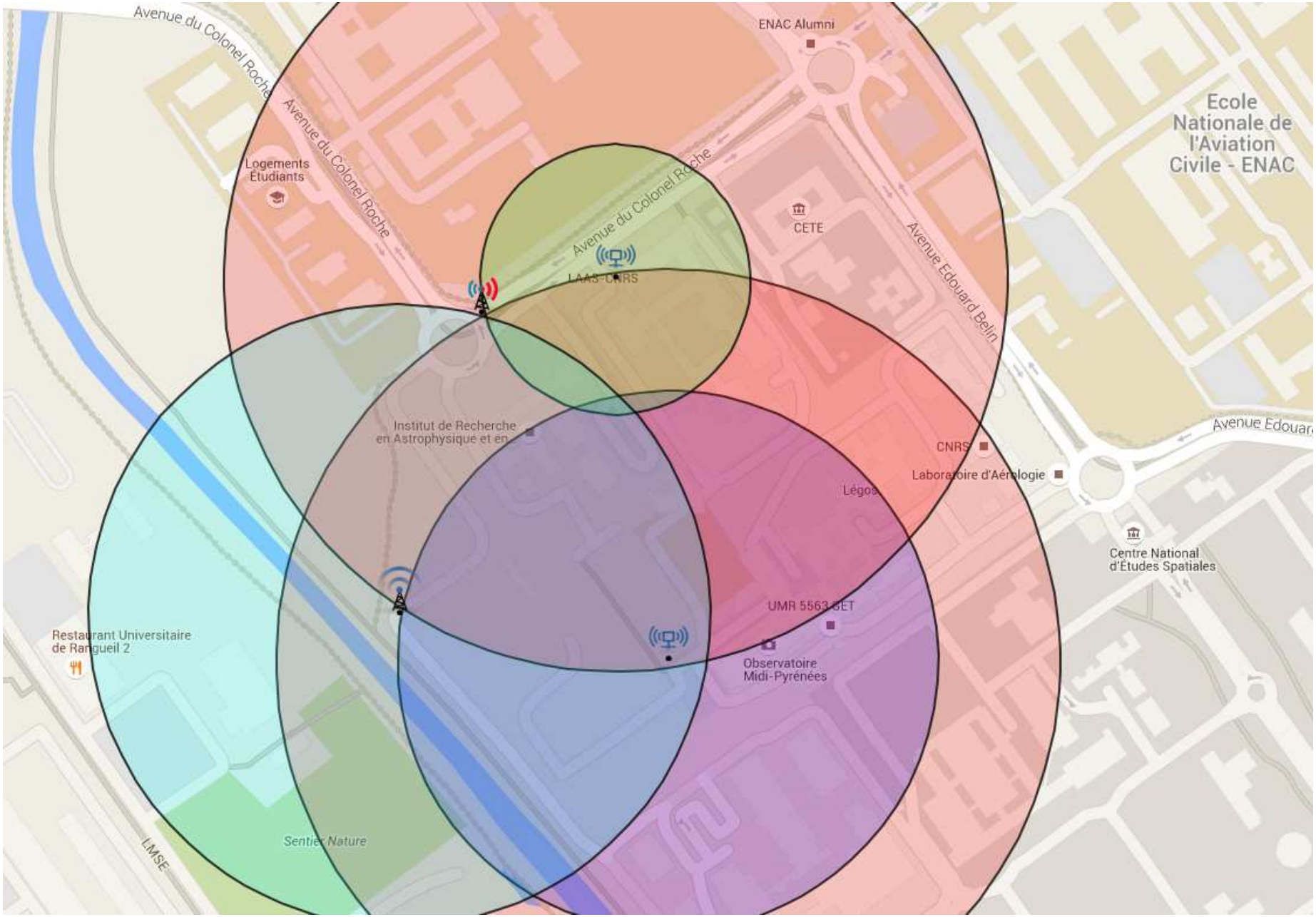
⇒ Rupture dans le canal de communication

⇒ Atteinte à la disponibilité

- Piste de réflexion : *geo-privacy*, *distance bounding protocol*, etc



Expérimentations – 2/2



Conclusion

Importance des études de sécurité pour l'IoT

- Equipements de plus en plus intelligents
- Connectivité des équipements de plus en plus importante
- *Le risque peut se cacher derrière des équipements associés à un usage banal*

$\Rightarrow$ La prise en compte la sécurité de ces objets est fondamentale

$\Rightarrow$ Besoin de méthodes pour évaluer ces objets

Perspective

Approches envisageables

- Utilisation de moyens issus du domaine IT
- Besoin de développer des approches spécifiques
- Etude indispensable de toutes les couches du composant

Perspectives de recherche

- Géneraliser les travaux à l'ensemble des objets connectés
- Proposer une classification des risques en fonction des caractéristiques des objets
- Proposer des architectures génériques "sûres" pour chaque classe