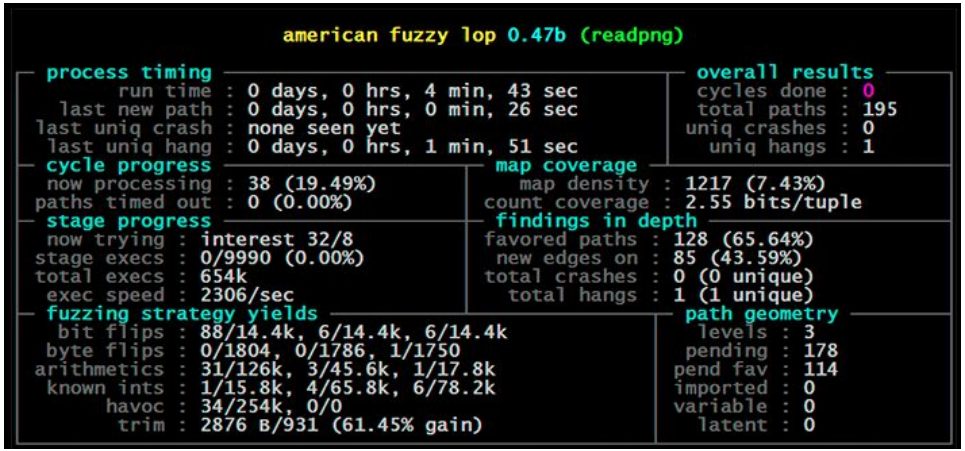
Test de protocole LoRaWAN

Tristan CLAVERIE
Thomas DEMANY
Manutea HUANG

Fuzzing

Qu’est-ce que le fuzzing ?

- Boite noire
- Injection de données aléatoires (paramètres, variables, ...)
- Comportement du programme
- Détection d’erreur
- Sécurité

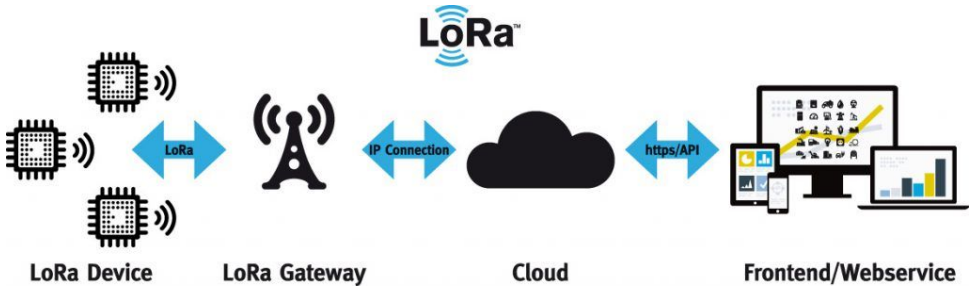


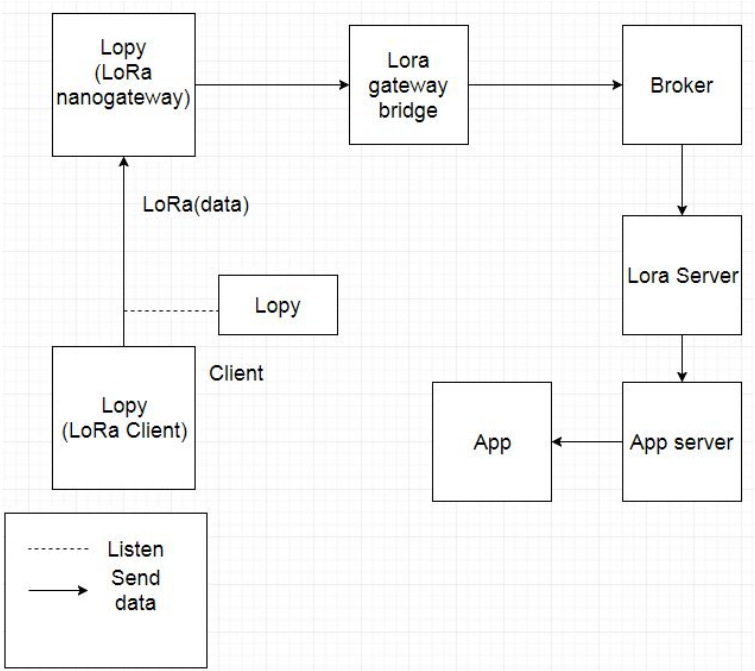
American fuzzy lop : fuzzer with genetic algorithms

LoRa

Qu’est-ce que LoRa ?

- Protocole radio (WAN)
- Communication entre objets connectés
- LoRaWAN (Couche 3)
- LoRaMAC (Couche 2)

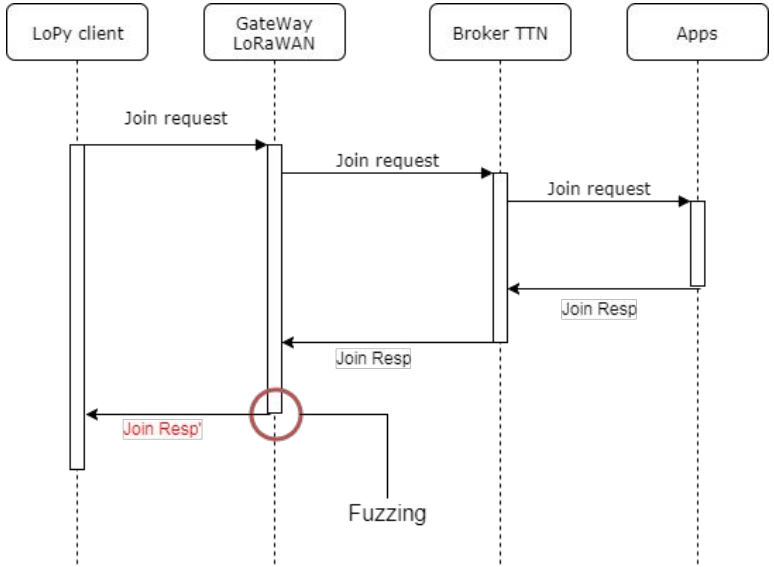


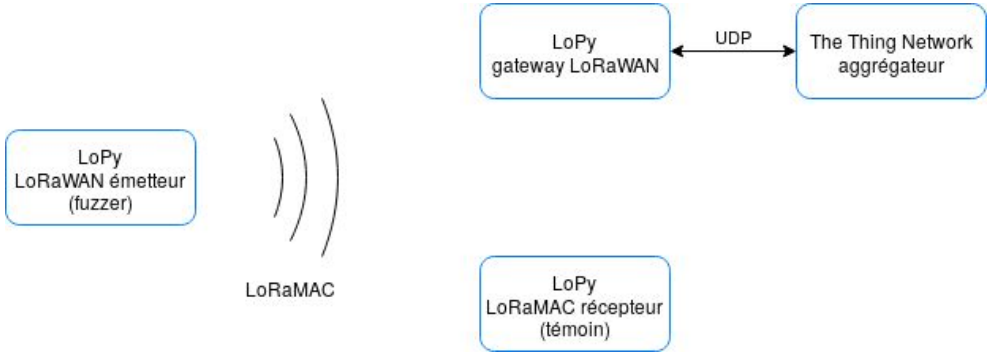


Travail réalisé

Quel est le travail réalisé ?

- Découverte de la LoPy
- Découverte du protocole LoRa
- Définir une architecture
- Implémentation fuzzer sur le client
- Implémentation du fuzzer sur la GateWay





Démonstration

Demo time

Conclusion

Quelle est la conclusion ?

- Tester sans interface de debug, c’est compliqué
- Pour tester les protocoles RF, il n’y a pas de Wireshark
- Créer une architecture Client/Gateway/Broker avec LoPy est relativement simple
- Réutilisation possible des outils développés pendant ce projet

Pistes d’amélioration

Quelles sont les pistes d’améliorations ?

- Fuzzer partie spécifique de la trame
- Tester le matériel (puissance d’émission, résistance au brouillage, ..)
- Supporter d’autres protocoles radio