

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

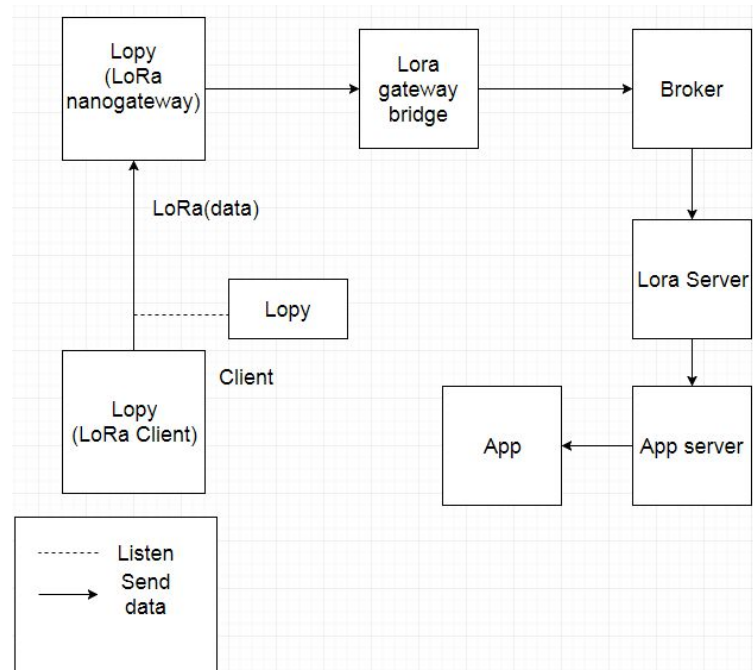
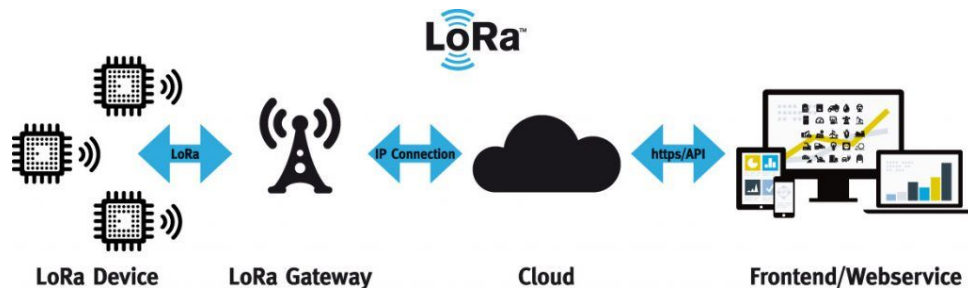
american fuzzy lop 0.47b (readpng)			
process timing		overall results	
run time : 0 days, 0 hrs, 4 min, 43 sec		cycles done : 0	
last new path : 0 days, 0 hrs, 0 min, 26 sec		total paths : 195	
last uniq crash : none seen yet		uniq crashes : 0	
last uniq hang : 0 days, 0 hrs, 1 min, 51 sec		uniq hangs : 1	
cycle progress		map coverage	
now processing : 38 (19.49%)		map density : 1217 (7.43%)	
paths timed out : 0 (0.00%)		count coverage : 2.55 bits/tuple	
stage progress		findings in depth	
now trying : interest 32/8		favored paths : 128 (65.64%)	
stage execs : 0/9990 (0.00%)		new edges on : 85 (43.59%)	
total execs : 654k		total crashes : 0 (0 unique)	
exec speed : 2306/sec		total hangs : 1 (1 unique)	
fuzzing strategy yields		path geometry	
bit flips : 88/14.4k, 6/14.4k, 6/14.4k		levels : 3	
byte flips : 0/1804, 0/1786, 1/1750		pending : 178	
arithmetics : 31/126k, 3/45.6k, 1/17.8k		pend fav : 114	
known ints : 1/15.8k, 4/65.8k, 6/78.2k		imported : 0	
havoc : 34/254k, 0/0		variable : 0	
trim : 2876 B/931 (61.45% gain)		latent : 0	

American fuzzy lop : fuzzer with genetic algorithms

LoRa

Qu'est-ce que LoRa ?

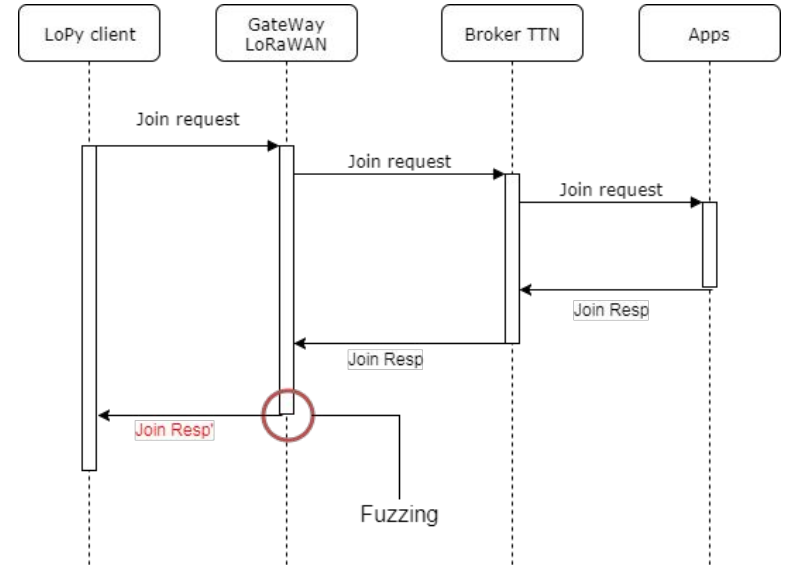
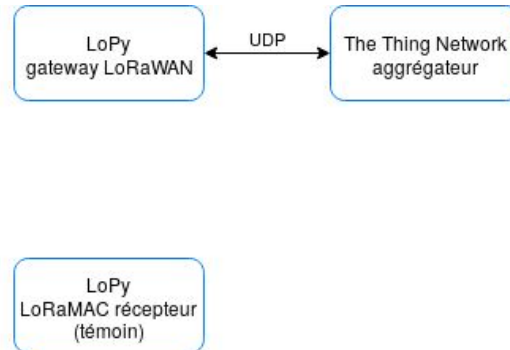
- Protocole radio (WAN)
- Communication entre objets connectés
- LoRaWAN (Couche 3)
- LoRaMAC (Couche 2)



Travail réalisé

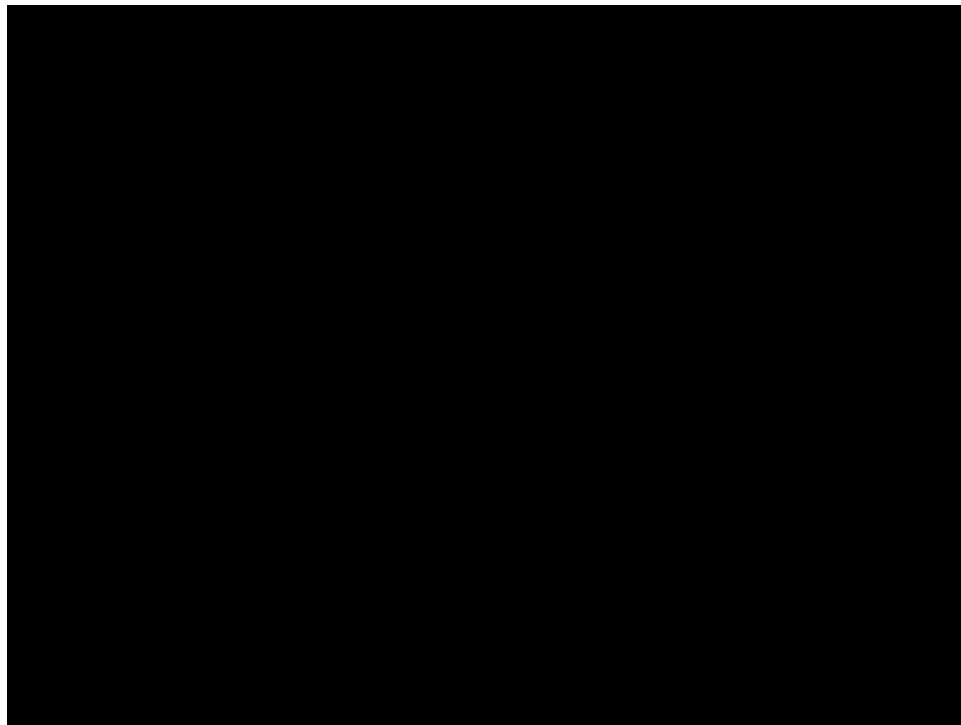
Quel est le travail réalisé ?

- 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