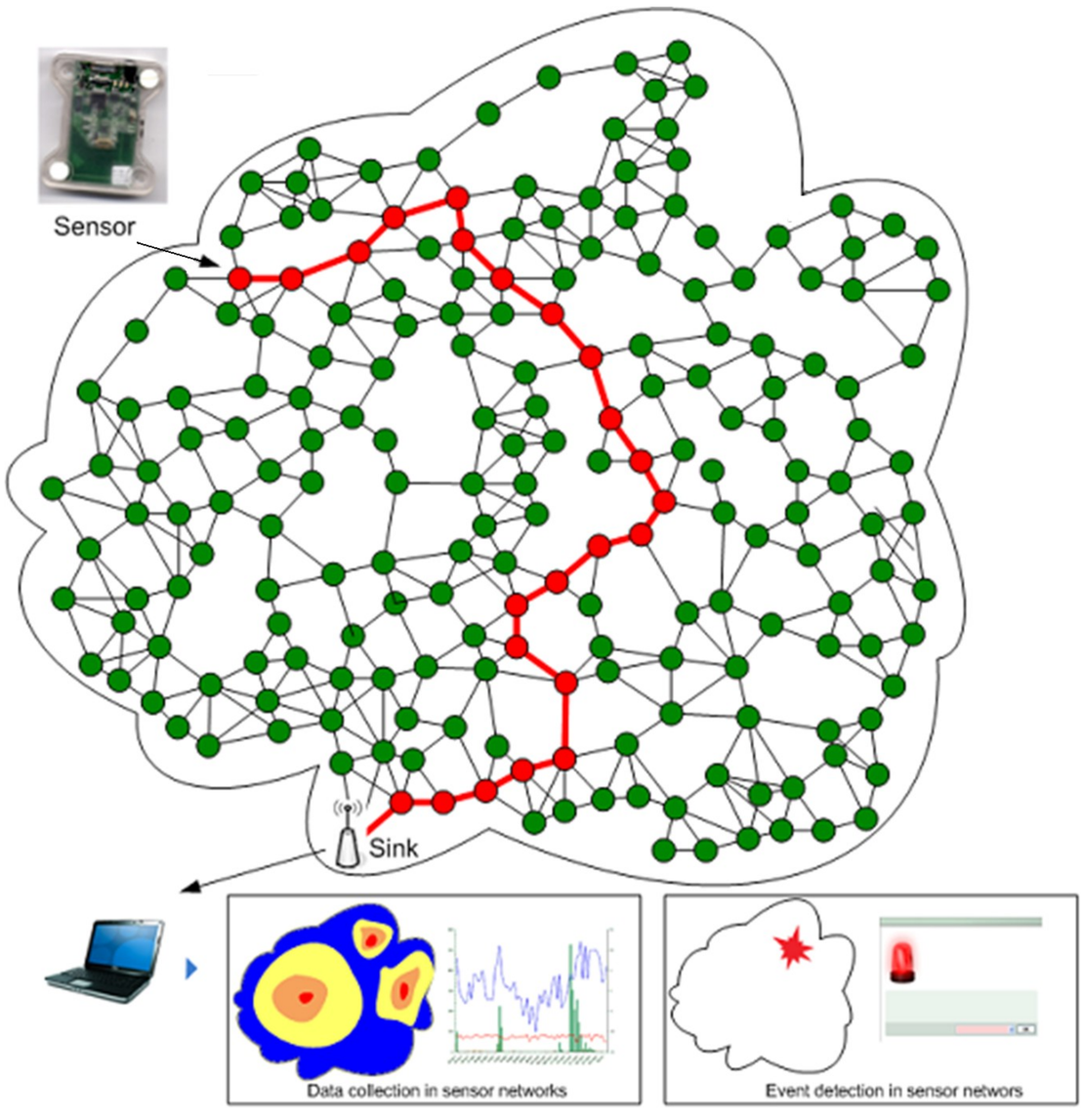
Protocoles de communjcation résilients pour les réseaux de capteurs

O. ERDENE-OCHIR
M. MINIER, F. VALOIS, A. KOUNTOURIS
INRIA SWING / CITI, INSA-Lyon et FTR&D, Meylan



Contexte

- Réseaux de capteurs (WSNs)
- Propriétés de résilience aux attaques de niveau 3 (Sécurité)
- Projet ANR VERSO ARESA2

Résilience :

Capacité des protocoles de communication à maintenir leur service en présence de k attaquant(s).

Motivations

- Compromission de nœuds simple dans les WSNs
  - accès aux données internes, réplication, Sybil attaque,…
- Cryptographie n'est pas toujours une solution

But

- **Analyse et création de protocoles de communication intrinsèquement résilients aux attaques de la couche réseau**

Etude de cas

- Analyse de 4 protocoles de routage (DSR, Gradient based, Greedy Forwarding, Random Walk) au sens de la résilience aux attaques :
  - Faux paquets *hello*
  - Faux paquets de *control*
  - *Black hole & Grey hole*

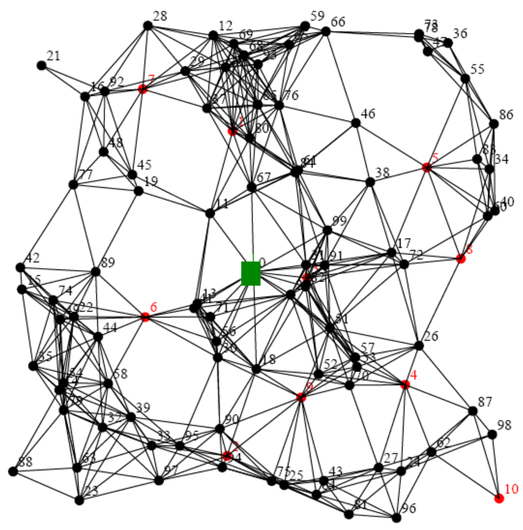
Simulations

- Environnement WSNet
- Topologie aléatoire et uniforme de 100 nœuds (1 puits)
- Sans interférence, sans collision (considère seulement l'impact des attaques)

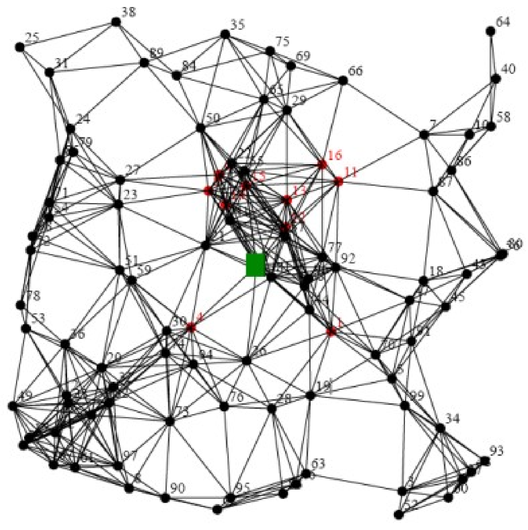
Analyses des résultats

- Comportement moins résilient:
  - Découverte des routes (flooding)
- Comportement plus résilient:
  - Plus court chemin
  - Démarche aléatoire

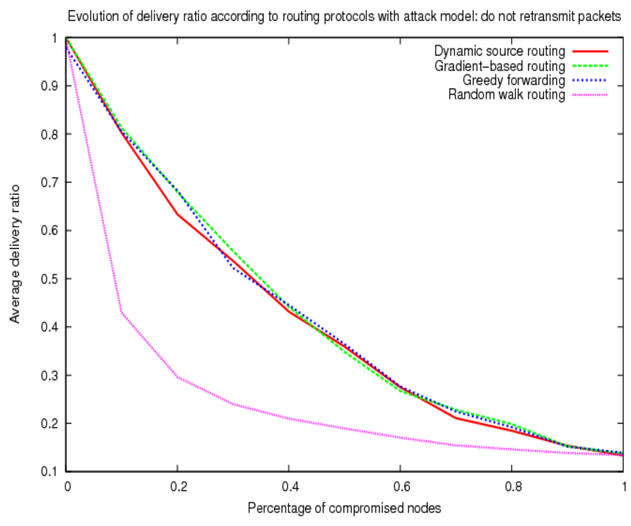
Distribution aléatoire des nœuds corrompus

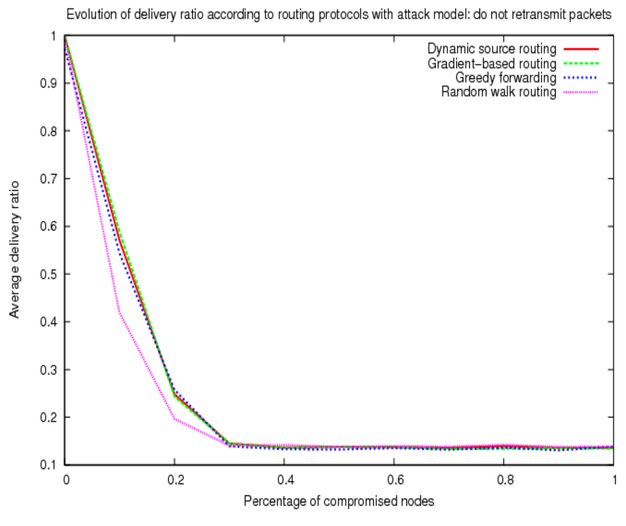


uniformément dans le réseau



autour du puits





Futures directions

- Etendre nos simulations en prenant en compte différentes distributions des nœuds, différentes cardinalités du réseau, interférences, collisions, protocoles proactifs etc.

- Quantifier une mesure de la résilience : quelle métrique ?
- Comparer la résilience des protocoles considérés
- Définir / concevoir une méthode pour augmenter la résilience des protocoles (et/ou proposer un nouveau protocole)

- Utilisation de l'entropie pour détecter localement une attaque
- La médiane est la fonction d'agrégation de données la plus résiliente : par analogie, est-ce qu'ils existent des fonctions similaires pour les protocoles de routage (approche théorique) ?