REPUBLIQUE DU CAMEROUN
PAIX-TRAVAIL-PATRIE
****
UNIVERSITE DE DSCHANG
****
ECOLE DOCTORALE

REPUBLIC OF CAMEROON
PEACE-WORK-FATHERLAND
****
UNIVERSITY OF DSCHANG
****
POST GRADUATE SCHOOL

DSCHANG SCHOOL OF SCIENCES AND TECHNOLOGY
Unité de Recherche en Informatique Fondamentale, Ingénierie et Application (URIFIA)

Secure Distributed Cluster Formation in Wireless Sensor Networks

Présenté par :
TCHIO AMOUGOU Styves daudet
Matricule : CM-UDS-14SCI0251
Licencié en Informatique Fondamentale

Sous la direction de
Dr BOMGNI ALAIN Bertand
(*Chargé de Cours, Université de Dschang*)

Sommaire

Context

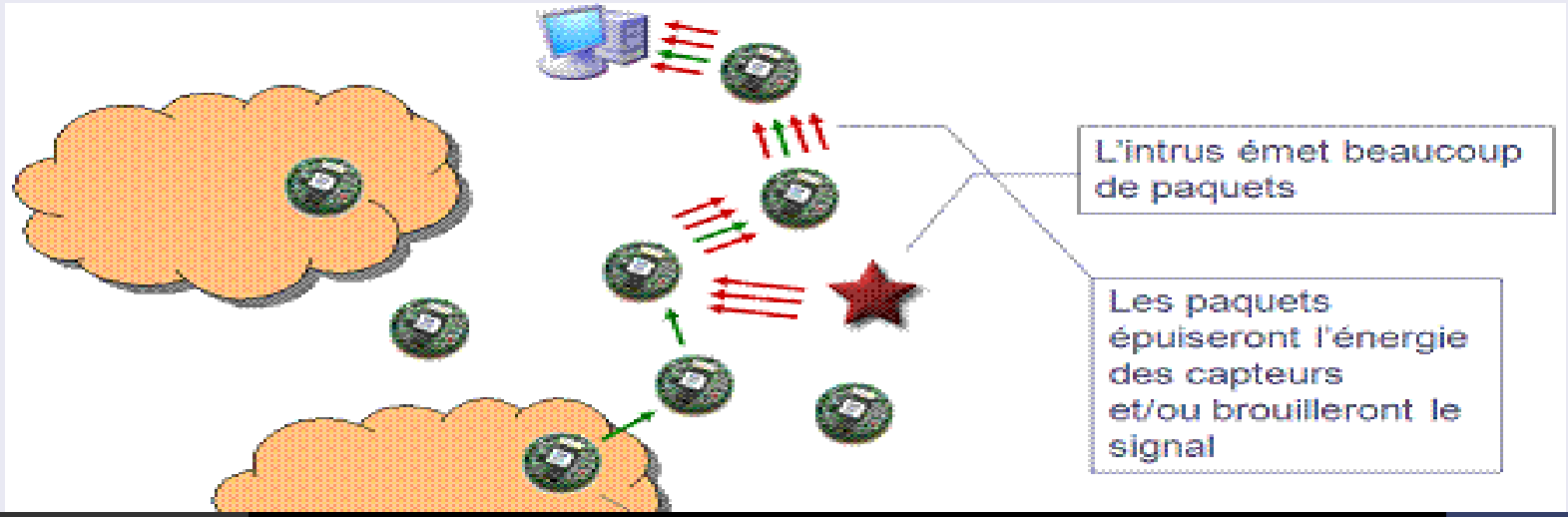
Dans les réseaux de capteurs les attaques malicieuses sont un problème réel, plusieurs protocoles proposés ne résistent pas aux attaques malicieuses dans des environnements hostiles.
En effet,Un noeud malicieux peut opérer sur deux niveaux :

- Les données échangées entre les noeuds
- La topologie du réseau créée par le protocole

Contexte

Exemple Déattaque Active :

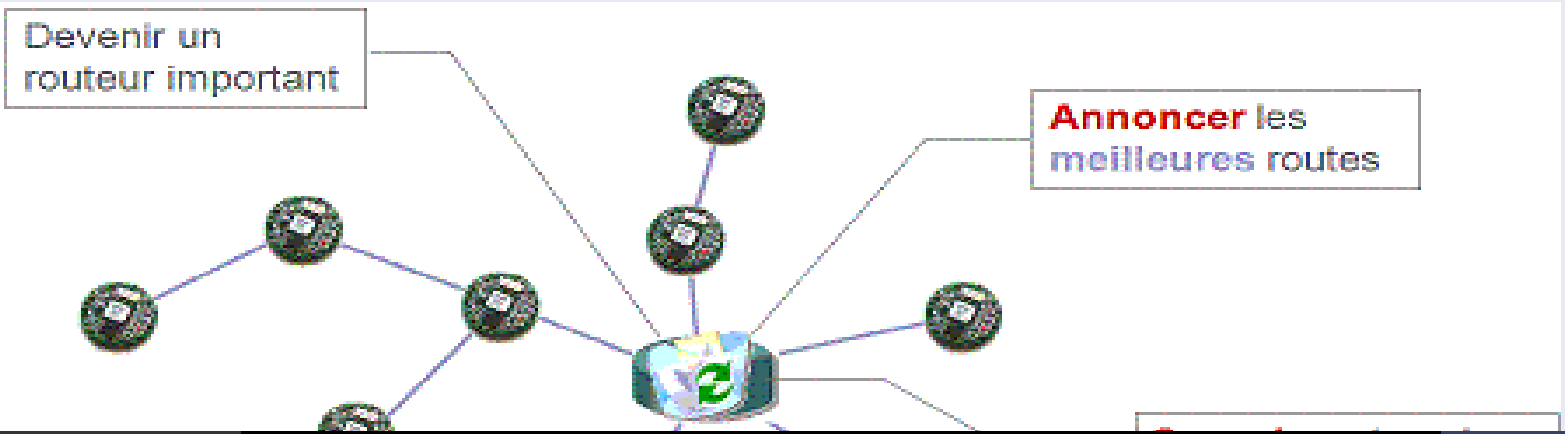
- Attaque de "jamming"
  Vu la sensibilité du média sans fil au bruit, un noeud peut provoquer un déni de service en émettant des signaux é une certaine fréquence. Cette attaque peut être très dangereuse car elle peut être menée par une personne non authentifiée et étrangère au réseau.



Contexte

Exemple D'attaque Active :

- ASink hole
  Dans une attaque sinkhole, le noeud essaye d'attirer vers lui le plus de chemins possibles permettant le contrôle sur la plupart des données circulant dans le réseau. Pour ce faire, l'attaquant doit apparaître aux autres comme étant très attractif, en présentant des routes optimales.



Problématique générale

Problématique générale

Détection des noeuds malicieux dans les réseaux de capteurs.

SECURE DISTRIBUTED CLUSTER FORMATION IN WIRELESS SENSOR NETWORKS

Propriétés

Le protocole de formation de cluster distribué sécurisé possède les propriétés suivantes même s'il y a des attaquants externes et internes

- Le protocole est entièrement distribué. Chaque noeud calcule sa clique uniquement en utilisant les informations de ses voisins ;
- La fin du protocole est garantie. Les noeuds participants qui ne respectent pas les spécifications du protocole (p. ex., envoyer des messages contradictoires) seront identifiés et retirés de toutes les cliques ;

Propriétés

Le protocole de formation de cluster distribué sécurisé possède les propriétés suivantes même s'il y a des attaquants externes et internes

- Une fois le protocole terminé,
  - Tous les noeuds normaux sont divisés en cliques disjointes.
  - Tous les noeuds normaux sont garantis d'avoir des vues cohérentes sur leurs adhésions é la clique, même dans un environnement hostile ;

propriétés

Le protocole de formation de cluster distribué sécurisé possède les propriétés suivantes même s'il y a des attaquants externes et internes

- les attaquants internes qui ne suivent pas la sémantique du protocole peuvent étre identifiés et retirés du réseau ;
- les attaquants externes peuvent être empêchés de participer au processus de formation du cluster ;
- les coûts de communication sont modéré

Hypothèses

- **Chaque** noeud connaît ses voisins 1-hop
  - Les noeuds de capteurs peuvent effectuer des opérations de signature numérique é clé publique.
  - Les horloges des noeuds normaux sont synchronisées de manière lâche, comme l'exige uTESLA.
  - Les clés publiques utilisées par les noeuds capteurs sont correctement authentifiées

Spécification du protocole

- étape 1 : Chaque noeud échange ses listes de voisins avec ses voisins et calcule sa clique maximale locale.
- étape 2 : Chaque noeud :
  - échange sa clique maximale locale avec ses voisins,
  - et met é jour sa clique maximale en fonction cliques maximales locales de ses noeuds voisins.
- étape 2 : Chaque noeud :
  - échange la clique mise é jour avec ses voisins
  - et calcule sa clique finale

Spécification du protocole

- étape 4 : Chaque noeud échange le clic final avec ses voisins.
  - Si aucune incohérence de clique n'est détectée, il se termine avec succès.
  - Sinon, il entre é l'étape 5.
- étape 5 : Chaque noeud effectue un contrôle de conformité.
  - S'il identifie les noeuds (voisins) malveillants, il les supprime du réseau et redémarre le protocole é partir de l'étape 1.
  - Sinon, il applique l'accord de clique et prend fin.

Limite

☞ Actuellement, le protocole est adapté aux réseaux de capteurs statiques, dans lesquels les noeuds ne se déplacent pas fréquemment

MERCI POUR VOTRE AIMABLE ATTENTION

REPUBLIQUE DU CAMEROUN
PAIX-TRAVAIL-PATRIE
****
UNIVERSITE DE DSCHANG
****
ECOLE DOCTORALE

REPUBLIC OF CAMEROON
PEACE-WORK-FATHERLAND
****
UNIVERSITY OF DSCHANG
****
POST GRADUATE SCHOOL

DSCHANG SCHOOL OF SCIENCES AND TECHNOLOGY
Unité de Recherche en Informatique Fondamentale, Ingénierie et Application (URIFIA)

Secure Distributed Cluster Formation in Wireless Sensor Networks

Présenté par :
TCHIO AMOUGOU Styves daudet
Matricule : CM-UDS-14SCI0251
Licencié en Informatique Fondamentale

Sous la direction de
Dr BOMGNI ALAIN Bertand
(*Chargé de Cours, Université de Dschang*)

Janvier 2021