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 Bertrand
(*Chargé de Cours, Université de Dschang*)

Sommaire

Contexte

Dans les réseaux de capteurs sans fil, le regroupement des n ?uds de capteurs en Les petits groupes sont une technique efficace pour atteindre l'extensibilité, l'auto-organisation, l'économie d'énergie, l'accès aux canaux, le routage, etc.
protocoles de formation de clusters peuvent être regroupé en deux grandes catégories :

Contexte

- Lead-First :
  - Dans l'approche lead-first, les clusters head sont d'abord élus selon certaines métriques (batteries restantes, degré de connectivité).
  - Ensuite, les clusters heads s'accordent sur comment assigner les noeuds à différents clusters.
- Cluster-first
  - Dans cette approche, tous les n ?uds sont d'abord regroupés en clusters,
  - Et ensuite chaque cluster sélectionné son cluster head sur la coordination de tous les n ?uds du cluster.

Contexte

Un certain nombre de protocoles de formation de clusters ont été proposés récemment mais Cependant, la plupart des protocoles existants supposent des environnements sans risque et sont vulnérables aux attaques de noeuds malveillants.

Problématique

Problématique

Comment regrouper les n ?uds d'un réseau de capteurs sans field dans different cluster tout en assurant la sécurité du réseau face des attaques malveillantes même dans un environnement hostile.

SECURE DISTRIBUTED CLUSTER FORMATION IN WIRELESS SENSOR NETWORKS

Définitions

- ☞ Le protocole propose ici est : un protocole sécurisé de formation de cluster distribuées pour organiser les réseaux de capteurs en cliques mutuellement disjointes
- ☞ Clique : est cluster dans lequel chaque noeud peut communiquer avec tous ses voisins à un saut.

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 à 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 à 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

Objectif

L'objectif premier de ce protocole est de diviser tous les noeuds du réseau en des cliques mutuelles disjoints de telle sorte que chaque noeud dans un même clique puisse communiquer directement avec chacun de ses voisins

Spécification du protocole

On définit par :

- C_i = Clique local du noeud i.
- Clique Agreement : pour chaque noeud j $\in C_i$, $C_j = C_i$
- Clique inconsistency : il existe j $\in C_i$ tel que $C_j \neq C_i$

Spécification du protocole

Algorithm 1 Heuristic Algorithm to Find the Local Maximum Clique

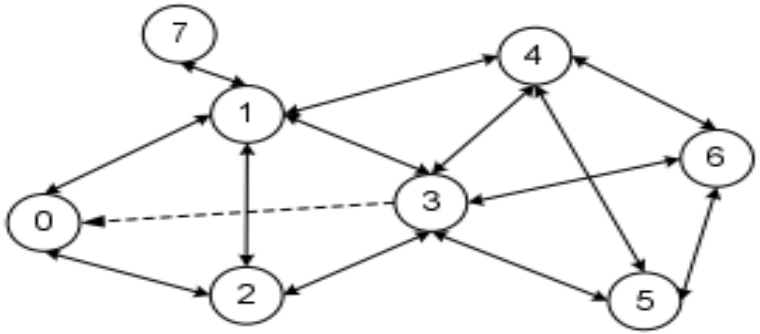
INPUT: $G_i = \{V_i, E_i\}, i \in V_i$
OUTPUT: C_i
STEPS:
$S_i = \{j | (i,j) \in E_i\}; C_i = \{i\};$
while ($S_i \neq \emptyset$) **do**
  Find $k \in S_i$ with maximum $|L_i \cap L_k|$
  $L_i \leftarrow L_i \cap L_k$
  $C_i \leftarrow C_i \cup \{k\}$
  $S_i \leftarrow S_i - \{k\} - \{j | (j,k) \notin E_i, j \in S_i\}$
end while

Spécification du protocole

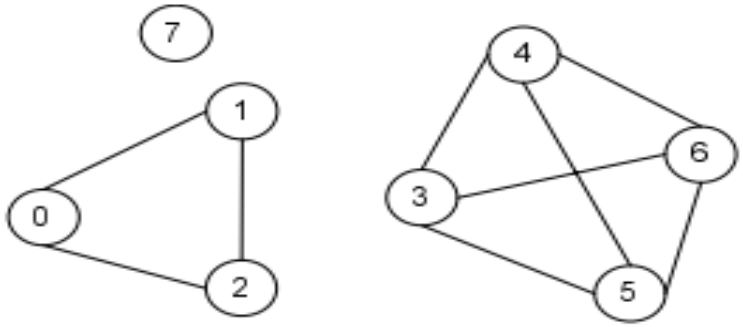
- L_i = liste des voisins de i à 1 saut
- $V_i = \{i\} +$ la liste de voisins de i
- $E_i =$ ensemble des bidirections entre les noeuds dans V_i
- $C_i^k =$ Clique de i a l'étape k, avec $1 \leq k \leq 4$

Spécification du protocole

Exemple :



(a) A network with 8 nodes



(b) Cluster formation

Spécification du protocole

Etape 1 : Chaque noeud échange ses listes de voisins avec ses voisins et calcule sa clique maximale locale.

Spécification du protocole

$S_0 = \{1, 2\}$, $L_0 = \{1, 2\}$, $C_0 = \{0\}$
$L_1 = \{0, 2, 3, 4, 7\}$, $|L_0 \cap L_1| = |\{2\}| = 1$
$L_2 = \{0, 1, 3\}$, $|L_0 \cap L_2| = |\{1\}| = 1$
comme les noeuds 1 et 2 ont le meme monbre d'element
on choisie le noeud 1
$L_0 = \{2\}$, $C_0 = \{0, 1\}$, $S_0 = \{2\}$
$|L_0 \cap L_2| = |\{1\}| = 1$
$L_0 = \Phi, C_0 = \{0, 1, 2\}$, $S_0 = \Phi$
$C_0^1 = \{0, 1, 2\}$, De même, nous avons
$C_0^1 = C_1^1 = C_2^1 \{0, 1, 2\}$,
$C_3^1 = C_4^1 = C_5^1 = C_6^1 = \{3, 4, 5, 6\}, C_7^1 = \{1, 7\}$,

Spécification du protocole

Etape 2 : Chaque noeud :

- échange sa clique maximale locale avec ses voisins,
- après avoir reçu les cliques maximales locales de ses voisins, le noeud i vérifie s'il existe une clique C_j^1 qui soit "meilleure" que sa clique C_i^1
- si le noeud i recois n clique contenant i,il ordonne les cliques comme
  $C_{\alpha 1}^1 \prec^i \ldots \prec^i C_{\alpha i}^1 \prec^i \ldots \prec^i C_{\alpha n}^1, C_i^2 = C_{\alpha n}^1$

Pour comparer les cliques calculées par différents noeuds, nous utilisons cette relation $\prec^i$ sur les cliques comme suit

Spécification du protocole

Definition 3 $C_j \overset{i}{\prec} C_k$ *if and only if*

1. $i \in C_j$, $i \in C_k$, *and*

2. *a).* $|C_j| < |C_k|$, *or*

   b). $|C_j| = |C_k|$, *but* $c_j < c_k$, *where* $c_j = min\{a_i | a_i \in C_j \wedge a_i \notin C_k\}$ *and* $c_k = min\{b_i | b_i \in C_k \wedge b_i \notin C_j\}$, *or*

   c). $C_j = C_k$, *but* $j < k$.

Spécification du protocole

$C_0^1 = C_1^1 = C_2^1 = \{0, 1, 2\}$,
$C_3^1 = C_4^1 = C_5^1 = C_6^1 = \{3, 4, 5, 6\}, C_7^1 = \{1, 7\}$,
Noeud 1 :
$|C_7^1| < |C_0^1|$, $C_7^1 \prec^i C_0^1$
$|C_0^1| = |C_1^1| = |C_1^2|$ et $0 < 1 < 2$ donc on a :
$C_7^1 \prec^1 C_0^1 \prec^1 C_1^1 \prec^1 C_2^1$ Donc on a : $C_1^2 = C_2^1 = \{0, 1, 2\}$
De même, nous avons
$C_0^2 = C_1^2 = C_2^2\{0, 1, 2\}$,
$C_3^2 = C_4^2 = C_5^2 = C_6^2 = \{3, 4, 5, 6\}, C_7^2 = \{1, 7\}$,

Spécification du protocole

Etape 3 : Chaque noeud :

- échange la clique mise à jour avec ses voisins
- Pour chaque noeud j dans C_2^1, le noeud i vérifie s'il est inclus dans j clique C_2^j Sinon, le noeud i retire j de sa clique C_2^i .
- Si le noeud i ne reçoit pas la clique actualisée du noeud j, le n ?ud i garde simplement le n ?ud j dans sa clique.

Exemple : $C_1^2 = \{0, 1, 2\}$, $C_7^2 = \{1, 7\}$
C_2^1 ne contient pas 7 donc le noeud 7 retire 1 de sa clique et on a : $C_7^3 = \{7\}$

Spécification du protocole

Etape 4 : Chaque noeud échange sa clique final avec ses voisins.

- Si $j \in C_i^3$, node i rediffuse la clique C_j^3 . L'objectif de cette rediffusion est de prévenir les attaques silencieuses.
- Chaque Noeud i vérifie que, pourtous $j \in C_i^3$, $C_j^3 = C_i^3$
- Si aucune incohérence de clique n'est détectée, il se termine avec succès.
- Sinon, il entre à l'étape 5.

Spécification du protocole

étape 5 : Chaque noeud effectue un contrôle de conformité.
Cette étape se déroule en deux temps. Dans la première étape,

- Conformity Checking : le noeud i effectue le contrôle de conformité pour identifier les noeuds malveillants qui ont envoyé des messages incohérents au cours des quatre étapes précédentes
- Consistency Enforcement : permet de faire respecter l'accord de clique, et terminer le protocole de formation de la clique.

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 Bertrand
(*Chargé de Cours, Université de Dschang*)

Janvier 2021