Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE LA DÉFENSE

Les réseaux de capteurs

10/06/08

DGA

DÉLÉGATION GÉNÉRALE POUR L'ARMEMENT

Avant propos

- Cette présentation n'est qu'un point de vue SSI des problématiques des WSN

- Cette présentation ne se prétend pas exhaustive sur les emplois possibles par la Défense des WSN

Plan

- Définition
- Quelques contextes d'emplois possibles
- Problématiques de SSI
- Quelques autres voies

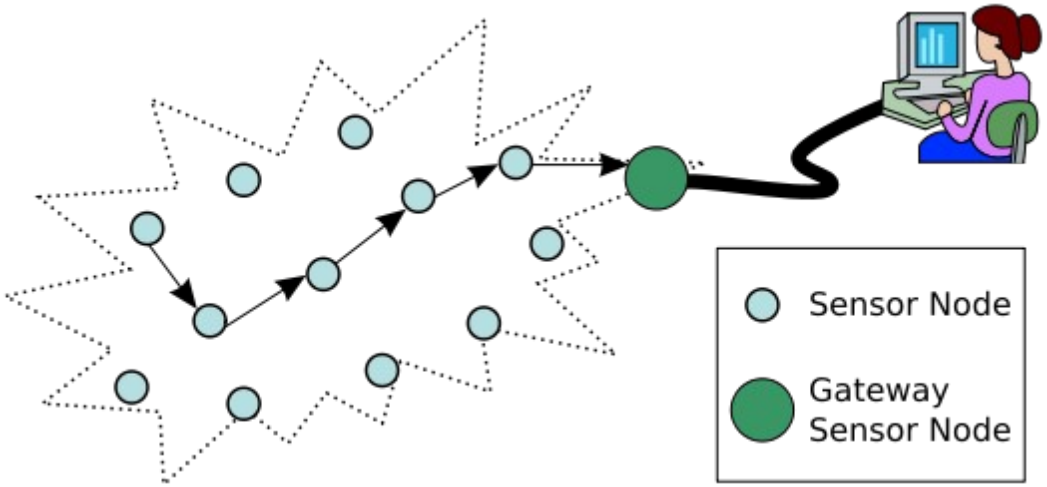
Définition

- Réseau de capteurs (WSN : Wireless Sensor Networks)
  - Un type spécial de réseaux ad hoc

- Les nœuds de ces réseaux consistent en un grand nombre de micro-capteurs :
  - Capables de récolter et de transmettre des données environnementales d'une manière autonome
  - Dispersés aléatoirement à travers une zone géographique (champ de captage)
  - Mettant en œuvre un routage multi-saut jusqu'à un nœud considéré comme un « point de collecte »

Le capteur

- Capteurs : éléments de base des systèmes d'acquisition de données.
  - Distance
  - Lumière
  - Sons
  - Température
  - Pression
  - Débit
  - Courant
  - Niveau
  - Déplacements
  - Contrainte
  - Inertiels



Idées d'applications militaires

- Renseignements
  - Interception d'origine électromagnétique
  - Surveiller toutes les activités des forces ennemies
- Surveillance de zone
  - Détection des mouvements ou caractéristiques indiquant une intrusion
- Observations avant déploiement
  - Analyse du théâtre d'opération avant d'y envoyer des troupes (détection d'agents chimiques, biologiques ou de radiations)

Idées d'applications militaires

- Capteurs volants
  - Parachutages (mission air-sol)
  - Capteurs sondes
  - …
- Capteurs au sol
  - Application terrestre
  - …
- Capteurs flottants
  - Activité acoustique
  - …
- Capteurs sous-marins

Atouts des WSN

- Déploiement rapide
- Coût réduit
- Auto-organisation
- Tolérance aux pannes

Objectifs de Sécurité pour les données captées

- Confidentialité
  - S'assurer que l'information n'a pas été divulguée
- Intégrité
  - S'assurer que l'information n'a pas été modifiée
- Authentification
  - S'assurer qu'une entité est bien ce qu'elle prétend être
  - S'assurer qu'une information provient d'où elle est censée provenir
- Disponibilité
  - S'assurer que l'information est présente et utilisable au moment ou l'on en a besoin
- Non-Rejeu
  - S'assurer qu'un message n'a été transmis qu'une seule fois
- Non-Répudiation
  - S'assurer qu'une entité ne puisse pas répudier ses actes

Points difficiles

- Énergie limitée
  - Algorithmes (crypto, comm., calculs) prenant en considération la consommation énergétique
    - Impact sur la durée de la mission
    - Impact sur les capacités et performances des capteurs
    - Impact sur la « dispersabilité » des capteurs (portée)
  - Routage à minimum d'énergie
- Débit faible
- Portée limitée
- Capacités de calculs limitées
- Faible capacité de stockage
- Vulnérabilités
  - liées aux réseau ad hoc

Problématiques SSI

- Vulnérabilités de la Liaison
  - Brouillage
- Vulnérabilités Réseau
  - Attaques sur la confidentialité et l'authenticité des paquets transmis
  - Attaques sur le protocole de routage
- Vulnérabilités Applicatives
  - Agrégation des données
- Gestion des clés
  - Crypto Symétrique / Asymétrique
- Vulnérabilités Matériels
  - Matériel pouvant être perdu
  - Compromission d'un nœud / Capture

TRANSEC : Transmission Security

- Capacité du capteur à rester discret
  - Ne pas se faire localiser/détecter afin d'assurer la mission
- Capacité du capteur à transmettre
  - Sans être brouillé afin d'assurer la mission
- Mais :
  - Tout en optimisant sa bande passante
  - Et en augmentant sa portée

- Modèles ?
- Lois descriptives imposant des limites ?

Attaques Réseau

- Déni de service / Flooding
- Attaques du Routage
  - Misdirection
  - Sinkhole attack
  - Selective forwarding attack
  - Création de Black hole
  - Routing table overflow
  - Faux transit pour épuiser les batteries
- Sybil attack
  - Prendre plusieurs identités
- Wormhole attack
- Rushing attack
- Stealthy attack
  - Contre l'agrégation

Gestion des éléments secrets

- Gestion des clés
  - Crypto Symétrique / Asymétrique (RSA/ECC) ?
  - **La gestion standard des clés est impossible**

- Plusieurs questions
  - Qui crée les clés ?
  - La compromission d'un nœud (ou plusieurs) ne doit pas compromettre les autres
  - Comment les clés sont-elles distribuées ?
  - Protocoles d'établissement de clés ?
  - Confiance mutuelle : combien d'éléments doivent-ils se faire confiance ?

Perdabilité

- Éviter le clonage de nos solutions
  - Propriété intellectuelle
- Garantir la protection des nos savoir-faire nationaux
  - Souveraineté
- Ne pas faire « tomber le système »
- Ne pas permettre la localisation des autres nœuds
- Ne pas compromettre la mission et surtout les futures missions
  - L'analyse des senseurs ne doit pas remettre en cause la sécurité apportée par les autres
- Les capteurs doivent être résistants aux attaques physiques

Détection d'Intrusion

- Détection d'un intrus dans le réseau
  - Afin d'éliminer les données qu'il transmet
  - Afin d'identifier une attaque sur les senseurs déployés
- Attaques
  - Attaques physiques : captures
  - Attaques réseau
- Problème des généraux byzantins

Réalisation

- Quels types de plate-forme ?
  - Objectif : Coût réduit
- Quels protocoles ?
  - Chiffrement / Routage / Signature / Agrégation à minimum de consommation
- Quels types de systèmes d'exploitation ?
  - Liés aux applications ?
  - OS à minimum de consommation ?
- Quels types de batteries ?
  - Alimentation solaire ?
- Quels types de formes d'onde ?
  - Zigbee, meilleur candidat ?

Clauses environnementales

- **Logique de développement durable**
  - Les capteurs doivent-ils être biodégradables ?
  - Ou n'avoir aucun impact sur la Nature
    - Batteries
    - Plastiques
    - …

Pour aller plus loin

- Pas uniquement des remontées d'information, mais aussi :
  - Activation/désactivation des capteurs
  - Reprogrammabilité de leurs capacités/missions

- Mobilité des senseurs
  - Impacts ?

Fin