

Optimisation du niveau de sécurité et de la qualité de service dans les réseaux de capteurs sans fil ¹

Abderrezak RACHEDI

Maître de conférences

Laboratoire d'Informatique Gaspard Monge (LIGM UMR 8049)



¹ Accepté pour publication dans la revue "Wireless Communications and Mobile Computing (WCMC)", John Wiley

Plan

Introduction

Contexte

Motivation

Contribution

Modèle d'optimisation du niveau de sécurité avec la QoS

Evaluation de performance

Conclusion et Perspectives

Plan

Introduction

Contexte

Motivation

Contribution

Modèle d'optimisation du niveau de sécurité avec la QoS

Evaluation de performance

Conclusion et Perspectives

Contexte

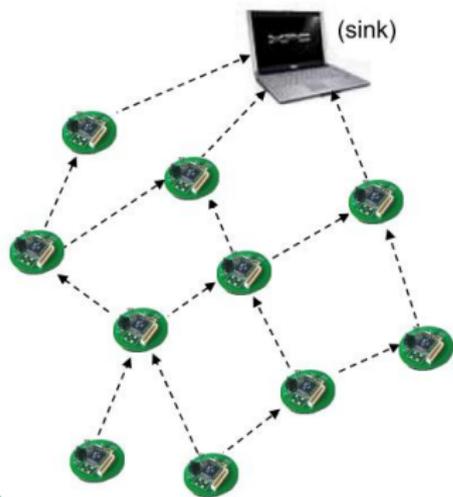


Figure : Réseau de capteurs sans fil (WSNs)

Les caractéristiques des WSNs :

- ▶ Flexibilité,
- ▶ Faible coût,
- ▶ Déploiement facile.

Contexte

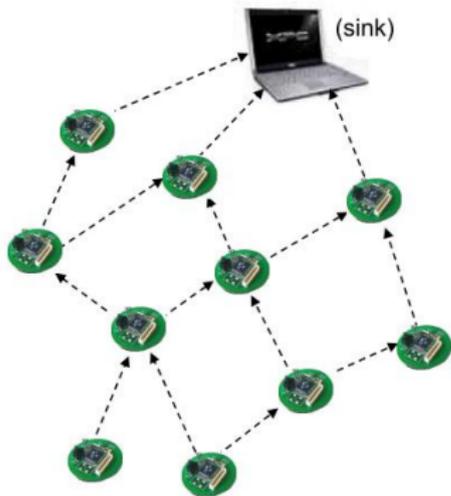


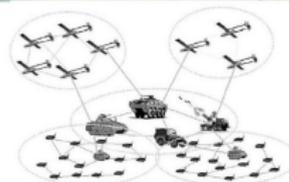
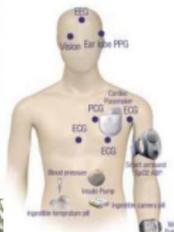
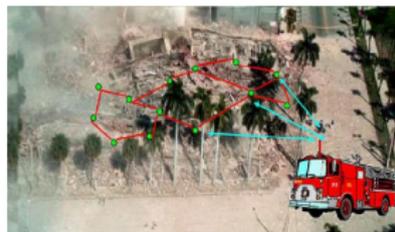
Figure : Réseau de capteurs sans fil (WSNs)

Les caractéristiques des WSNs :

- ▶ Flexibilité,
- ▶ Faible coût,
- ▶ Déploiement facile.

Domaines d'application :

- ▶ Environnement : feux de forêt, pollution, tremblement de terre,
- ▶ Sanitaire : assistance à la personne, télé-santé,
- ▶ Militaire : surveillance, localisation et suivi d'objets, etc.



Plan

Introduction

Contexte

Motivation

Contribution

Modèle d'optimisation du niveau de sécurité avec la QoS

Evaluation de performance

Conclusion et Perspectives

Motivation pour ce travail

- ▶ **Les services de sécurité nécessaires** : confidentialité des données, authentification mutuelle et intégrité des données.
- ▶ **Les contraintes** :
 - ▶ Ressources limitées : énergie et bande passante.
 - ▶ Les paramètres de la QoS et de la sécurité sont **opposés** : l'augmentation de l'un implique la diminution de l'autre.
- ▶ **Les performances** : le coût de la sécurité peut directement impacter les performances du réseau, comme la QoS et la consommation d'énergie.
- ▶ **Les travaux existants** : se focalisent sur la sécurité, la QoS, ou l'énergie **séparément**.

Plan

Introduction

Contexte

Motivation

Contribution

Modèle d'optimisation du niveau de sécurité avec la QoS

Evaluation de performance

Conclusion et Perspectives

Le régulateur PID (Proportionnel Intégral Dérivé)

- ▶ Il fait partie de la théorie de contrôle.
- ▶ Le concept de base consiste à rendre le signal de sortie proche du **signal de référence** quelle que soit la variation des paramètres du système
- ▶ Il est basé sur la combinaison de trois actions de contrôle :
 - **Partie P** : proportionnelle à l'erreur,
 - **Partie I** : proportionnelle à l'intégrale de l'erreur,
 - **Partie D** : proportionnelle à la dérivée de l'erreur.

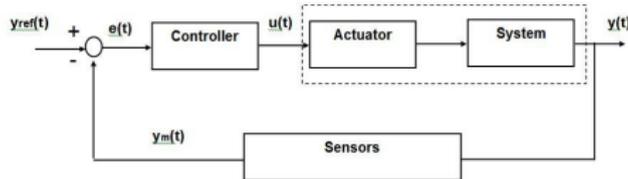


Figure : Diagramme du régulateur PID

Où $y_{ref}(t)$ est le signal de référence, $e(t)$ est l'erreur, et $u(t)$ est le signal de contrôle.

$$u(t) = K_P e(t) + K_I \int_0^t e(\alpha) d\alpha + K_D \frac{de}{dt} \quad (1)$$

Modèle d'optimisation du niveau de sécurité avec la QoS

- ▶ Le régulateur PID est utilisé pour adapter le niveau de sécurité aux ressources du réseau disponibles et aux besoins de la QoS
- ▶ L'objectif est de maximiser le niveau de sécurité sans impacter les paramètres de la QoS

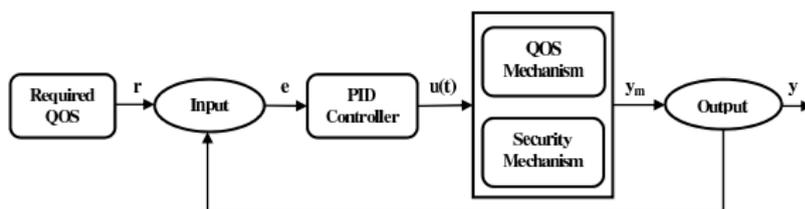


Figure : Le régulateur PID pour les paramètres de QoS et de sécurité

L'objectif final est de :

Minimiser le délai de bout-en-bout	Minimiser la consommation d'énergie
Minimiser la gigue (jitter)	Maximiser le niveau de sécurité
Maximiser le débit	

Les paramètres de la QoS

Chaque noeud calcule les paramètres suivants :

- ▶ Taux d'occupation du buffer du noeud i ($BO(i)$):

$$BO(i) = \frac{buffer.free(i)}{buffer.size} \quad (2)$$

- ▶ Energie résiduelle du noeud i ($E_r(i)$):

$$E_r(i) = E_I(i) - \sum E_k \quad (3)$$

Où E_I est l'énergie initiale, E_k est la somme des énergies consommées à la transmission, à la réception, et à l'écoute.

- ▶ Qualité du lien du noeud i avec le $SINR(i)$ (Signal Interference and Noise Ratio):

$$SINR(i) = \frac{P_r}{\sum P_{i,j} + N_p} \quad (4)$$

Où P_r est la puissance du signal reçu, $P_{i,j}$ est l'ensemble des signaux d'interférence et N_p est le bruit.

- ▶ Le débit minimum pour l'application D^*

$$D^* = \max\{D, SINR \geq S(D)\} \quad (5)$$

D est le débit de différents chemins

Les paramètres de sécurité

Les niveaux des paramètres de sécurité sont :

- L'authentification :

$$A_l = f_1(\alpha, n_1, n_2, r_m) = \sqrt{(\alpha(1 + n_1) + n_2)c_1 \frac{r_m}{r_m + c_2}} \quad (6)$$

Où α , et n_1 dépendent du type d'authentification : unilatérale ($\alpha = 1$, $n_1 = 0$), ou mutuelle. n_2 indique si l'authentification est sous un tunnel ou pas, r_m représente le taux des requêtes d'authentification. c_1 est un paramètre déterminé en fonction de r_m .

- L'intégrité :

$$I_l = f_2(x_1) = (2^{x_1/\min(x_1)} - 1) \frac{c_3}{2^{x_1/\min(x_1)} + c_4} \quad (7)$$

Où x_1 est la taille de l'empreinte numérique, c_3 et c_4 des paramètres déterminés en fonction de x_1 .

- La confidentialité :

$$C_l = f_3(x_2) = \frac{1}{2} \left[\beta(2^{x_2/\min(x_2)} - 1) + c_5 \right] \quad (8)$$

Où $\beta = \frac{8-c_5}{2^{x_2/\min(x_2)} + c_6}$ est un facteur d'impact, x_2 représente la taille de la clef. c_5 et c_6 sont déterminés en fonction de x_2 .

Niveau de sécurité

$$S_l = W_1 A_l + W_2 I_l + W_3 C_l \quad (9)$$

Introduction du modèle dans le processus de routage

Introduction du modèle dans le processus de routage (AODV) nommé QwS-AODV

Etape 1: Classification du trafic réseau

Trois classes de service principales : service garantie (GS), charge contrôlée (CL), et meilleur effort (BE).

Etape 2 : Evaluation des métriques de performance (débit, délai, SINR, énergie)

Lancement du processus de découverte de chemin : a Route Request packet (REQ) and a Route Reply packet (REP).

Etape 3: Introduction des services de sécurité avec le niveau adapté

Le régulateur PID prend la décision d'introduire le niveau et le service de sécurité adaptés.

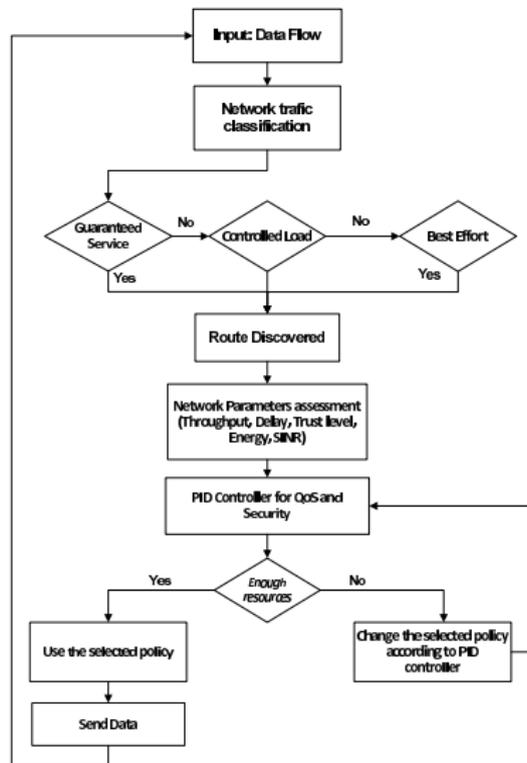


Figure : Schéma descriptif de QwS-AODV

Plan

Introduction

Contexte

Motivation

Contribution

Modèle d'optimisation du niveau de sécurité avec la QoS

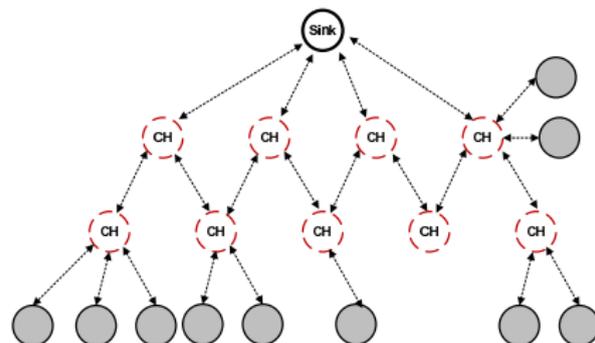
Evaluation de performance

Conclusion et Perspectives

Evaluation de performance de QwS-AODV

Paramètres de simulation - NS2

Taille de la zone	$500 \times 500m^2$
MAC/Physique	80.15.4
Taille de la file IFQ	50
Densité des noeuds	11-101
Modèle de trafic réseau	CBR/VBR
Taux CBR/VBR	16kb/s
Temps de simulation	1000 sec

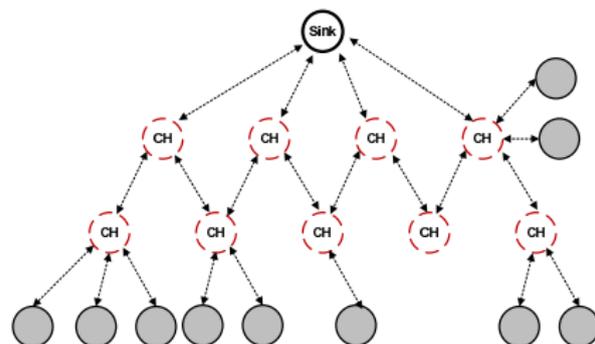


Exemple d'une topologie réseau en clusters

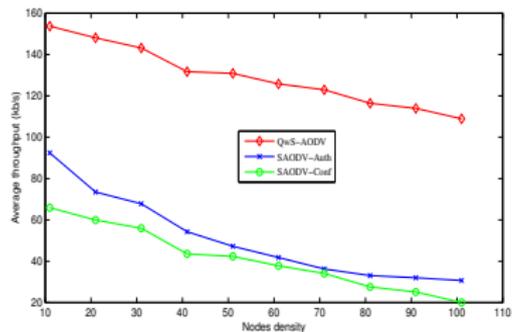
Evaluation de performance de QwS-AODV

Paramètres de simulation - NS2

Taille de la zone	$500 \times 500m^2$
MAC/Physique	80.15.4
Taille de la file IFQ	50
Densité des noeuds	11-101
Modèle de trafic réseau	CBR/VBR
Taux CBR/VBR	16kb/s
Temps de simulation	1000 sec



Exemple d'une topologie réseau en clusters

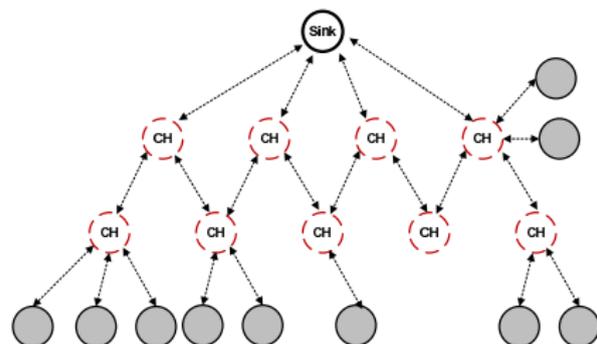


Débit moyen en fonction de la densité des nœuds

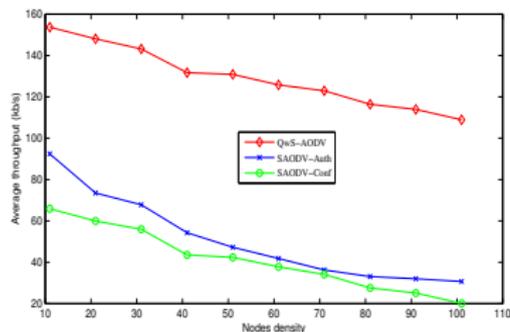
Evaluation de performance de QwS-AODV

Paramètres de simulation - NS2

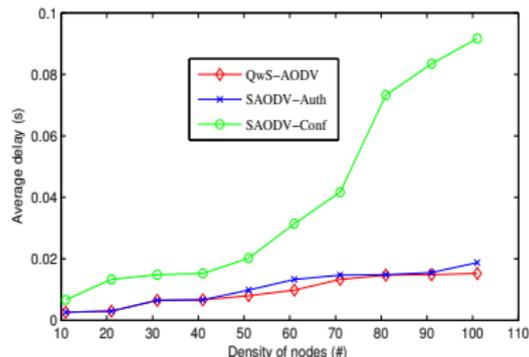
Taille de la zone	500 × 500m ²
MAC/Physique	80.15.4
Taille de la file IFQ	50
Densité des noeuds	11-101
Modèle de trafic réseau	CBR/VBR
Taux CBR/VBR	16kb/s
Temps de simulation	1000 sec



Exemple d'une topologie réseau en clusters

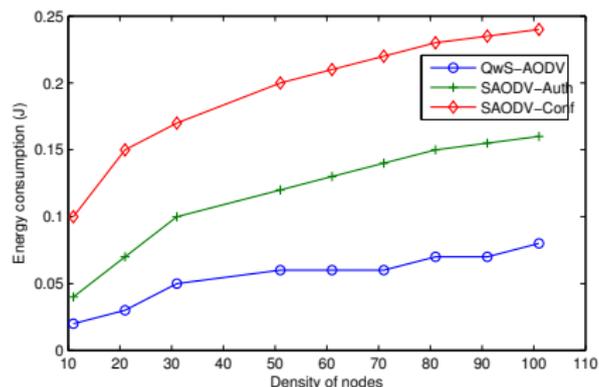


Débit moyen en fonction de la densité des nœuds



Délai moyen en fonction de la densité des nœuds

Evaluation de performance de QwS-AODV



Consommation d'énergie en fonction de la densité des noeuds

- ▶ La consommation d'énergie du protocole SAODV-Auth est moins importante que dans le cas SAODV-Conf
- ▶ La consommation d'énergie augmente rapidement dans les 2 cas de SAODV

Conclusion et Perspectives

- ▶ La solution proposée basée sur le régulateur PID permet d'adapter de manière dynamique le niveau de sécurité aux performances du réseau (QoS et consommation d'énergie).
- ▶ Les paramètres de QoS et l'énergie sont combinés avec le niveau de sécurité pour optimiser le processus de routage (QwS-AODV).
- ▶ Les résultats de simulation montrent que cette solution assure la sécurité avec moins d'impact négatif sur les performances du réseau (un gain d'environ 50% au niveau de la consommation d'énergie).

Perspectives

- ▶ Etudier l'impact de la mobilité sur le modèle proposé.
- ▶ Etendre et évaluer le modèle sur des réseaux hétérogènes (tels que l'internet des objets).

Merci pour votre attention