

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTRE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE
SCIENTIFIQUE
UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE HOUARI
BOUMEDIENE USTHB / ALGERIE

Faculté D'Electronique et D'Informatique
Département d'Informatique



Mémoire pour l'obtention du Diplôme d'Ingénieur d'Etat en Informatique

Thème du sujet :

**Implémentation d'un modèle d'attaques sur le
routage dans les réseaux de capteurs**

Proposé et encadré par : Mr. KHELLADI L. - attaché de recherche
Commission de suivi : Melle. BENZAÏD C.

Le jury :

Présidente du jury : Melle. BENZAÏD C.
Membre du jury : Melle. BOUZIANE N.
Membre du jury : Melle. CHENAIT M.

Réalisé par :

ARAB M^{ed} Arezki
MEZINE Samir

Année universitaire : 2007 ~ 2008

Sommaire

Introduction générale	1
Chapitre 1 : Environnements mobiles et réseaux de capteurs	
1. Introduction	3
2. Les réseaux sans fil mobiles	4
2.1 Définition	4
2.2 Caractéristiques des environnements mobiles	4
2.3 Les Domaines d'exploitations des réseaux sans fil	6
3. Classification des réseaux sans fil	6
3.1 Les réseaux cellulaires (avec infrastructure)	6
3.2 Les réseaux Ad Hoc (sans infrastructure)	8
3.2.1 Les caractéristiques des réseaux ad hoc	9
3.2.2 Modélisation d'un réseau ad hoc	10
4. Les réseaux de capteurs	11
4.1 Définition	11
4.2 Qu'est-ce qu'un capteur ?	12
4.3 Applications des réseaux de capteurs	16
4.4 Spécificités des réseaux de capteurs	17
4.5 Pile protocolaire des réseaux de capteurs	19
5. Présentation de quelques projets de réseaux de capteurs	21
5.1 Le projet « Smart Dust »	21
5.2 Etude d'une forêt de séquoia	22
5.3 Projet "Common Sense Net"	23
6. Conclusion	24

Chapitre 2 : Le routage et sa sécurité dans les réseaux de capteurs

1. Introduction	25
2. Le routage dans les réseaux de capteurs	26
1.1 Définition	26
1.2 Les défis du routage dans les réseaux de capteurs	26
1.3 Classification des protocoles du routage dans les réseaux de capteurs	29
1.3.1 Les protocoles centrés-données	29
1.3.2 Les protocoles hiérarchiques	30
1.3.3 Les Protocoles basés sur la localisation	31
1.3.4 Les protocoles orientés qualité de service	33
2. Sécurité du routage dans les réseaux de capteurs	33
2.1 Définition de la sécurité	34
2.2 Objectifs de la sécurité	34
2.3 Mécanismes de sécurité	35
2.3.1 Chiffrements symétriques	35
2.3.2 Chiffrement asymétrique	36
2.3.3 Signature numérique	37
2.3.4 Fonction de hachage	38
2.4 Modèles d'attaques dans un réseau de capteurs	39
2.5 Attaques sur les mécanismes du routage dans les réseaux de capteurs	40
2.5.1 Usurpation d'information du routage	40
2.5.2 Relais sélectif des paquets	40
2.5.3 Attaque du trou noir	41
2.5.4 Attaque du trou de ver	41
2.5.5 Attaque de l'identité multiple	42
2.5.6 Attaque de l'inondation de HELLO	43
2.6 Les contres mesures	44
2.6.1 Relais sélectif	44
2.6.2 Attaques de trou de ver et de trou noir	44
2.6.3 L'identité multiple	45

2.6.4	Attaque d'inondation HELLO	45
3.	Conclusion	46
Chapitre 3 : Étude du protocole Directed Diffusion Fonctionnement et Sécurité		
1.	Introduction	48
2.	Fonctionnement	49
2.1	Dissémination d'intérêt et établissement des gradients.....	49
2.2	Propagation des données	50
2.3	Renforcement des chemins.....	51
2.4	Maintenance locale des chemins défaillants	53
2.5	Création des routes pour plusieurs sources et plusieurs puits.....	53
3.	Sécurité de Directed Diffusion	55
3.1	Attaque de clonage	55
3.2	Attaque du trou de ver	56
3.3	Attaque de relais sélectif des paquets	57
3.4	Attaque du trou noir	59
4.	Conclusion	60
Chapitre 4 : Implémentation du protocole de routage et des modèles d'attaques		
1.	Introduction.....	61
2.	Description de l'environnement de développement.....	62
2.1	Systèmes d'exploitation.....	62
2.1.1	Description du TinyOS.....	62
2.1.2	Propriétés de TinyOS	62
2.1.3	Allocation de la mémoire.....	63
2.1.4	L'ordonnanceur TinyOS.....	64
2.2	Le langage de programmation	64
2.2.1	Description du nesC.....	64
2.2.2	Compilation	65
2.3	Le simulateur TOSSIM.....	65
2.1.1	Description.....	65

2.1.2 Propriétés de TOSSIM	66
2.1.3 Avantage du TOSSIM	67
2.1.4 Inconvenant du TOSSIM	67
3. Implémentation	68
3.1 Le protocole Directed Diffusion	68
3.2 Structures de données du protocole Directed Diffusion	70
3.3 Format des paquets	69
3.4 Modèles d'attaque	71
3.4.1 <i>Attaque de clonage</i>	71
a. <i>Utilisant un renforcement positif</i>	71
b. <i>Utilisant un renforcement négatif</i>	73
c. <i>Utilisant le message d'intérêt</i>	75
3.4.2 <i>Attaque de trou de ver</i>	77
3.4.3 <i>Attaque de trou noir</i>	79
4. Conclusion	81

Chapitre 5 : Impact des attaques sur les performances du protocole

Directed Diffusion (Résultats et interprétations)

1. Introduction.....	82
2. Paramètres de simulation.....	83
3. Métriques de performances évaluées	83
4. Résultats et interprétation.....	84
4.1 Attaques du clonage utilisant l'intérêt et le renforcement positif.....	84
d. <i>Impact sur la consommation d'Energie</i>	84
e. <i>Impact sur le taux de trafic contrôlé par les nœuds malicieux</i>	85
f. <i>Impact sur le temps de réponse moyen</i>	86
4.2 Attaque du clonage utilisant un renforcement négatif	87
a. <i>Impact sur la consommation d'énergie</i>	87
b. <i>Impact sur le taux de satisfaction de l'intérêt</i>	89
4.3 Attaque du trou de ver	90

<i>a. Impact sur le temps de réponse moyen</i>	90
<i>b. Impact sur le taux de trafic contrôlé par les nœuds malicieux</i>	91
4.4 Attaque du trou noir	92
<i>a. Impact sur le taux de trafic contrôlé par les nœuds malicieux</i>	92
<i>b. Impact sur le taux de livraison des données</i>	93
5. Conclusion	94
Conclusion générale	95
Perspectives	96
Bibliographie	97

Résumé

Le travail effectué dans notre projet de fin d'études, s'inscrit dans le cadre d'un projet de recherche sur la sécurité de routage dans une nouvelle classe particulière des réseaux *ad hoc*, il s'agit des réseaux de capteurs sans fil (RCSF). Ces derniers, sont caractérisés par l'absence de toute infrastructure préexistante, le déploiement d'un très grand nombre de nœuds sans identificateur global, la consommation d'énergie est un facteur déterminant.

Le but de ce projet est de définir des modèles d'attaques sur un protocole de routage des réseaux de capteurs, précisément le protocole « diffusion dirigée » (*directed diffusion*), afin d'étudier l'impact de ces attaques sur les performances du réseau. Pour cela, on a procédé à la simulation des différentes attaques implémentées, en utilisant le simulateur des réseaux de capteur TOSSIM. Ce dernier se caractérise par : une simulation du code réel de l'application ; une capacité de simuler un réseau de plusieurs milliers de nœuds avec précision et performance ; l'utilisation d'un modèle d'énergie complet et réaliste, car il simule la consommation d'énergie dans les capteurs réels (capteurs Mica) ; de plus, il permet un affichage graphique des échanges radios grâce à l'outil TinyViz, cela permet à chaque instant de la simulation d'avoir une vue globale de l'activité du réseau étudié. Ce qui est non réalisable sur la plupart des autres simulateurs.

Les résultats de simulation obtenus confirment l'effet des attaques sur la robustesse du protocole *directed diffusion*. Ce travail servira par la suite pour évaluer les solutions de sécurité de ce protocole pour faire face aux attaques.
