REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

N° d'ordre : .....

UNIVERSITE MOHAMED BOUDIAF-M'SILA
FACULTE DES MATHEMATIQUES ET DE L'INFORMATIQUE

Département d'Informatique

MEMOIRE de fin d'étude

Présenté pour l'obtention du diplôme de MASTER

Domaine : Mathématiques et Informatique
Filière : Informatique
Spécialité : Réseaux
Par : MILOUDI Mokhtar

SUJET

Analyse des attaques d'intégrité des données dans les réseaux de capteurs sans fil

Soutenu publiquement le : / / 2015 devant le jury composé de :

.....	**Université de M'sila**	**Président**
Mr. ATHMANI Samir	**Université de M'sila**	**Rapporteur**
.....	**Université de M'sila**	**Examinateur**
.....	**Université de M'sila**	**Examinateur**

Promotion : 2014/2015

Table des matières

CHAPITRE 4

PROPOSITION D'UN PROTOCOLE DE DETECTION DES ATTAQUES D'INTEGRITES

INTRODUCTION GENERALE

Les progrès réalisés lors de ces dernières décennies dans les domaines de la microélectronique, de la micromécanique, et des technologies de communication sans fil, ont permis de produire avec un coût raisonnable des composants de quelques millimètres cubes de volume. Ces derniers, appelés micro-capteurs, intègrent : une unité de captage chargée de capter des grandeurs physiques (chaleur, humidité, vibrations) et de les transformer en grandeurs numériques, une unité de traitement informatique et de stockage de données et un module de transmission sans fil. Un grand nombre de ces dispositifs (micro-capteurs) sont déployés dans la nature afin de créer un réseau de capteurs à des fins aussi bien de contrôle que de monitorisation. Le fort potentiel d'applications des réseaux de capteurs en font un domaine de recherche très actif.

Cependant le grand problème de ces réseaux est la sécurité, les travaux de recherche indique que les réseaux sans fil sont plus vulnérables que les réseaux filaires en raison de leurs caractéristiques tels que le milieu ouvert, la topologie dynamique, l'absence d'administration centrale, la coopération distribuée, et la capacité restreinte (en termes de puissance et de calcul). L'utilisation de liaisons sans fil rend ces réseaux plus sujets à des menaces de sécurité physiques que les réseaux câblés, allant de l'écoute passive à l'interférence active. Sans aucune sécurité adéquate, les hôtes mobiles sont facilement capturés, compromis et détournés par des nœuds malveillants. L'adversaire peut écouter et /ou modifier les messages dans le canal de communication, injecter des messages erronés, supprimer des messages, et même passer par d'autres nœuds. Par conséquent, les mécanismes de sécurité dans de tels réseaux sont essentiels pour protéger les données émises par les utilisateurs.

Dans le cadre de ce mémoire, nous nous intéresserons au problème d'intégrité, ou les attaques d'intégrité dans le RCSF. Dans cette optique nous projetons de proposer un protocole de détection des attaques d'intégrités dans les réseaux de capteurs sans fils

Ce rapport est organisé en quatre chapitres. Chaque chapitre aborde des points spécifiques. Il est et structuré comme suit :

Le premier chapitre présente une introduction aux réseaux de capteur sans fil, et les différents concepts liés à ces réseaux. Le deuxième chapitre explique les mécanismes de sécurité fondamentaux utilisés dans la sécurisation des réseaux sans fil. Dans le troisième chapitre Nous allons étudier en détails les attaques les plus dangereuses pour l'intégrité dans le RCSF et retracer les solutions préalablement proposer et présenter les avantages et la faiblesse de chaque solution. Le dernier chapitre est réservé à la description du protocole proposé et l'analyse de ses performances, le but de ce protocole est la sécurisation des échanges des données dans les réseaux de capteur sans fil. Enfin, nous terminons le mémoire par une conclusion générale dans laquelle nous résumons l'essentiel de notre travail et nous donnons quelques orientations des travaux futurs.

CONCLUSION GENERALE

Les RCSFs constituent des sujets de recherche innovants pour diverses disciplines des sciences et techniques de l'information et de la communication mais avec toutefois des contraintes spécifiques s'érigeant en défis certains à relever.

Dans ce projet de fin d'études, nous étions intéresser à l'analyse d'attaque d'intégrité Pour cela, il nous a fallu étudier les différentes attaques d'intégrité. Cela nous a permis d'offrir un protocole efficace, nous avons utilisé seulement des concepts simples. Le MAC le chiffrement et un algorithme simples pour trouvée la zone exacte de attaquant, Cela signifie que la consommation d'énergie est simple, En fait, cela est le point fort fondamentale du protocole.

Bibliographie

[1] Mémoire, KAZI TANI Chahrazad, BENHADDOUCHE Wiam, implémentation et test d'un protocole de prévention de l'attaque clone dans un réseau de capteurs sans fil , Master, 2013-2014

[2] Mémoire, nadia boungta, approche distribuée pour la sécurité d'un réseau de capteurs sans fils, ingénieur ,2010-2011

[3] mémoire, Melle Khedim Farah épouse Bouhamed, détection des attaques par réplication dans un réseau de capteurs sans fil, 2013-2014

[4] thèse, Christina Boura, analyse de fonctions de hachage cryptographiques, 19 dec 2012

[5] Mémoire, Y. Challal, routage multichemin securise pour un reseau de capteurs sans fil video. attaque wormhole:etude et contre mesure. 29/05/2012

[6] mémoiré, dealing with sinkhole attacks in wireless sensor networks, 2012-2013

[7] john r. douceur. the sybil attack. in peer-to-peer systems, first international workshop, iptps 2002, cambridge, ma, usa, march 7-8, 2002, revised papers, pages 251–260. springer, 2002

[8]mémoire, protocole de routage pour les rcsf 2007-2008

[9] mémoire protocole pour la sécurité des réseaux sans fil peer to peer 19 dec 2012

[10]mémoire, la sécurité dans les réseaux sans fil ad hoc

[11]. jeyanthi hall, michel barbeau, and evangelos kranakis. enhancing intrusion detection in wireless networks using radio frequency fingerprinting. in international conference on communications, internet, and information technology, november 22 - 24, 2004, st. thomas, us virgin islands, pages 201–206. iasted/acta press, 2004

[12]. chris karlof and david wagner. secure routing in wireless sensor networks : attacks and countermeasures. ad hoc networks, 1(2-3) :293–315, 2003.

[13]. brian neil levine, clay shields, and n. boris margolin. a survey of solutions to the sybil attack. tech report 2006-052, university of massachusetts amherst, ma, usa, october 2006.

[14] shaohe lv, xiaodong wang, xin zhao, and xingming zhou. detecting the sybil attack cooperatively in wireless sensor networks. in international conference on computational intelligence and security, cis 2008, 13-17 december 2008, suzhou, china, volume 1 - conference papers, pages 442–446, washington, dc, usa, 2008.ieee computersociety.

[15] debapriyay mukhopadhyay and indranil saha. location verification based defense against sybil attack in sensor networks. in distributed computing and networking, 8th international conference, icdcn 2006, guwahati, india, december 27-30, 2006, pages 509–521. springer, 2006.

[16] james newsome, elaine shi, dawn xiaodong song, and adrian perrig. the sybil attack in sensor networks : analysis & defenses. in proceedings of the third international symposium on information processing in sensor networks, ipsn 2004, berkeley, california, usa, april 26-27, 2004.

[17] indranil saha and debapriyay mukhopadhyay. security against sybil attack in wireless sensor network through location verification. in distributed computing and networking, 10th international conference, icdcn 2009, hyderabad, india, january 3-6, 2009. proceedings, pages 187–192. springer, 2009.

[18] haifeng yu, michael kaminsky, phillip b. gibbons, and abraham d. flaxman. sybilguard : defending against sybil attacks via social networks. ieee/acm ton, transactions on networking, 16(3) :576–589, 2008.

ملخـــص

موضوع بحثنا هو الأمن في شبكات الاستشعار اللاسلكية ,وبالضبط تحليل هجمات النزاهة في شبكات الاستشعار اللاسلكية , وقد قمنا باقتراح بروتوكول ناجع وفعال في هذا النوع من الهجمات ,ويعتمد أساسا علي أفكار بسيطة وفعالة ,حيث اعتمدنا علي التشفير وال "م ا ك" بالإضافة إلي خوارزمية بسيطة تمكننا من معرفة موقع المهاجم بدقة كبيرة مما يتيح لنا تجنبه.

الكلمات البحث: الأمن في شبكات الاستشعار اللاسلكية, هجمات النزاهة, التشفير, "م ا ك "

Résumé

L'objet de notre recherche est la sécurité dans les réseaux de capteurs sans fil, et exacte l'analyse des attaques d'intégrité dans les réseaux de capteurs sans fil, et nous devons proposer un protocole efficace dans ce type d'attaques, repose essentiellement sur des idées simples et efficaces, où nous comptons sur le chiffrement et le MAC En plus de l'algorithme base nous permet de connaître le position de l'attaquant avec une grande précision qui nous permet évitons

Mots-clés: sécurité dans les réseaux de capteurs sans fil, les attaques d'intégrité, chiffrement, MAC.

Summary

The purpose of our research is security in wireless sensor networks, and accurate analysis of integrity attacks in wireless sensor networks, and we must propose a viable and effective protocol in this type of attack mainly based on simple and effective ideas, where we rely on encryption and MAC Besides the basic algorithm allows us to know the position of the striker with great precision which allows us avoid.

Keywords: security in wireless sensor networks, attacks of integrity, encryption, MAC