الجـــــــــــــــــــمـهـوريـــــة الجـــــــــــــزائـريـة الديمـــــــقـراطيـة الـشـــــــــعبيـة

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التـــــــــــــــــــــــــعـليـم العـــــــالي والبـــــــــــحث العـــــلـمـــي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جـــــــــــــــامعة أبي بكـــر بـلـقـايد– تـلمســـــــــــــــان –

Université Aboubakr Belkaïd– Tlemcen –
Faculté de TECHNOLOGIE

THESE

Présentée pour l'obtention du **grade** de **DOCTORAT 3ème Cycle**

En : Télécommunications

Spécialité : Systèmes et Réseaux informatiques et Télécommunication

Par: Mme KHEDIM Farah épouse BOUHAMED

Sujet

Détection des attaques internes dans les réseaux de capteurs sans fil

Soutenue publiquement en 2019, devant le jury composé de:

M Feham Mohammed	Professeur	Univ. Tlemcen	Président
Mme Labraoui Nabila	MCA	Univ. Tlemcen	Directeur de thèse
MAdo Adamou Abba Ari	MCA	Univ. Maroua	Co- Directeur de thèse
M Lehsaini Mohamed	Professeur	Univ. Tlemcen	Examinateur
M Ghalem Belalem	Professeur	Univ.Oran	Examinateur
M Mejdi Kaddour	MCA	Univ.Oran	Examinateur

Résumé

La sécurité dans les réseaux de capteurs sans fil (RCSFs) est devenue un domaine indissociable des autres domaines des RCSFs. Il devient en effet inenvisageable d'aborder des thématiques telles que l'agrégation, la localisation, le routage ou le clustering sans prendre en compte le côté sécuritaire. Connus pour être en effet une cible idéale pour de nombreuses attaques toujours plus sophistiquées et de plus en plus intelligentes, les réseaux de capteurs se retrouvent démunis face aux attaques internes. De telles attaques peuvent passer totalement inaperçues tout en engendrant des dégâts irréversibles pour le réseau. Les systèmes de confiance et de réputation (TRS) se présentent comme une méthode de détection efficace pour ces attaques. Cependant, ces mécanismes sont victimes de leur succès, des attaquants peuvent en effet se servir de ces mécanismes pour engendrer une multitude d'attaques internes.

Nous nous sommes intéressés dans cette thèse aux problèmes de sécurité liés aux systèmes de confiance et de réputation. Nous avons à cet effet proposé deux nouvelles approches nommées Bee-Trust Scheme et B-Smart, des méthodes intelligentes permettant de renforcer la résistance des TRS afin que ces derniers puissent soutenir efficacement la détection des attaques internes dans les réseaux de capteurs. Notre première contribution BTS résout le problème des recommandations malhonnêtes sous un nouvel angle en s'inspirant du modèle naturel du comportement des abeilles "Apis mellifera" lors de la recherche de leur nourriture. En outre, nous faisons appel à deux concepts innovateurs : une révision du modèle de nuage "cloud model" ainsi qu'un paramètre de chronométrie cognitive. Dans notre seconde contribution nous avons proposé un nouveau mécanisme de confiance et de réputation nommé B-Smart permettant une gestion intelligente des valeurs de réputation grâce à l'utilisation conjointe des notions de smart contract et de blockchain. L'association de ces deux concepts offre à notre protocole une grande résistance à un grand nombre d'attaques internes.

Mots clés : Réseaux de capteurs sans fil (RCSFs), sécurité, attaques internes, systèmes de confiance et de réputation.

Abstract

Security in wireless sensor networks (WSN) has become an inseparable area from other areas in WSN. It is indeed unthinkable to tackle topics such as aggregation, localization, routing or clustering without taking into account the security side. Known to be an ideal target for many increasingly sophisticated and intelligent attacks, sensor networks are particularly vulnerable to internal attacks. Such attacks can go completely unnoticed while causing irreversible damage to the network. Trust and reputation systems (TRS) stand out as an effective detection method for these attacks, but these mechanisms are victims of their success, attackers can use these mechanisms to generate a multitude of internal attacks.

We were interested in this thesis to the security issues related to the trust and reputation systems. We have proposed for this purpose two new approaches named Bee-Trust Scheme and B-Smart. The proposed intelligent methods are intended to strengthen the resistance of the TRS so that can effectively support the detection of internal attacks in sensor networks. Our first BTS contribution solves the problem of dishonest recommendations attacks from a new angle by drawing inspiration from the natural model of behavior of honey bees and applying two innovative concepts : a modified cloud model and a cognitive chronometry parameter. In our second contribution, we proposed a new trust and reputation mechanism called B-Smart that allows intelligent management of reputation values through the joint use of smart contract and blockchain. The combination of these two concepts gives our protocol great resistance to a large number of internal attacks.

Keywords: Wireless Sensor Networks (WSNs), security, internal Attacks, Trust and Reputation Systems.

ملخّص

أصبح الأمن في شبكات أجهزة الاستشعار اللّاسلكية مجال لا يمكن فصله عن المجلات الأخرى .أصبح من غير المعقول معالجة مواضيع مثل التّجميع أو التّوجيه دون الأخذ بعين الاعتبار الجانب الأمني .إنّ أجهزة الاستشعار المعروفة بأنّها هدف مثالي للعديد من الهجمات المتطوّرة تجد نفسها معدمة في مواجهة الهجمات الدّاخلية .هذه الهجمات تتسبب في أضرار وخيمة لا يمكن إصلاحها على الشّبكة .برزت أنظمة الثّقة والشّهرة كوسيلة فعّالة للكشف عن هذه الهجمات، ولكن هذه الآليات هي ضحايا نجاحها، حيث يمكن للمهاجمين استخدام هذه الآليات لتوليد العديد من الهجمات الدّاخلية.

نحن مهتمّون في هذه الرّسالة إلى المشاكل الأمنية المتعلّقة بأنظمة الثّقة والسّمع .اقترحنا تهجين جديدين وهما عبارة عن طريقتان ذكيتان لزيادة مقاومة أنظمة الثّقة والسّمعة حتّى تصبح وسيلة فعّالة لدعم الكشف الفعّال للهجمات الدّاخلية في شبكات الاستشعار .إنّ مساهمتنا الأولى تحلّ مشكلة التّوصيات الغير الشّريفة من زاوية جديدة من خلال تقليد النّموذج الطّبيعي لسلوك النّحل عند البحث عن الطّعام و استخدام مفهومين مبتكرين : نموذج سحابة الاستعراض و نموذج من الكرونومتر المعرفي .في مساهمتنا الثّانية، اقترحنا آلية ثقة و سمعة جديدة تسمح بالإدارة الذّكيّة لقيم السّمعة من خلال الاستخدام المشترك لمفاهيم العقد الذّكيّ و المفاتيح .الجمع بين هذين المفهومين يعطي بروتوكولنا مقاومة كبيرة لعدد كبير من الهجمات الدّاخليّة.

كلمات البحث : شبكات أجهزة الاستشعار اللاّسلكية، الأمن، الهجمات الدّاخلية، أنظمة الثقة والسّمعة.

A ma très chère maman à qui je souhaite bonheur et santé.

A mon défunt papa qui me manque trop.

A mon très cher mari pour son soutien continu et sa patience durant toutes ses années.

Aux prunelles de mes yeux mes fils Rassim et Mounir que j'aime plus que tout au monde.

A mon frère, mes sœurs, mes neveux et mes nièces qui ont toujours été là pour moi.

A ma belle-famille qui m'a toujours encouragé et soutenu.

Un grand merci à vous tous!!

Remerciements

Louanges à Dieu pour m'avoir donné la force, la patience et le courage pour réaliser cette thèse.

J'exprime ma profonde gratitude à ma directrice de thèse, Mme LABRAOUI Nabila pour son esprit scientifique, sa pédagogie et sa disponibilité. Je la remercie grandement pour avoir cru en moi et m'avoir accordé son temps, sa patience et ses précieux conseils.

Je tiens également à remercier mon co-encadrant MAdo Adamou Abba Ari pour son aide si précieuse et pour les heures de travail qu'il m'a accordé. Ses remarques ont largement contribué à l'aboutissement de cette thèse.

Je suis très honorée par la présence de M Mohamed Feham, qui a accepté de présider le jury de cette thèse. Je suis également très honorée par la présence de M Mohamed Lehsaini, M Ghalem Belalem, et M Mejdi Kaddourqui m'ont fait l'honneur d'accepter d'être les rapporteurs de cette thèse.

Qu'ils trouvent ici mes plus vifs remerciements pour l'effort qu'ils ont fourni pour lire mon manuscrit et l'intérêt qu'ils ont porté à mon travail.

Je souhaite également remercier les membres du laboratoire Systèmes et Technologie de l'Information et de la Communication (STIC) au sein duquel ce travail a été réalisé. À commencer par M Feham pour sa sympathie et pour m'avoir chaleureusement accueilli au sein du laboratoire STIC. À M Lehsaini pour sa gentillesse, sa disponibilité et ses précieux conseils. À Mme Khelif Nouria pour sa sympathie et son amitié. Enfin, à tous mes collègues enseignants et doctorants à qui je souhaite beaucoup d'épanouissement dans leur travail.

Je souhaite aussi témoigner ma gratitude et vifs remerciements envers tous ceux qui ont contribué, de près ou de loin à la réalisation de ce travail.

Bien sûr, je ne peux terminer sans remercier mes proches de tout cœur et notamment les trois hommes de ma vie pour tous leurs encouragements et leur amour. J'espère qu'ils me pardonneront les heures interminables que j'ai passé loin d'eux afin de réaliser cette thèse.

Table des matières

Table des figures

Liste des tableaux

INTRODUCTION GÉNÉRALE

1. Contexte générale

Prédestinés à devenir une partie intégrante de notre vie, les réseaux de capteurs sans fil (RCSFs) ont su se montrer à la hauteur des attentes en devenant l'une des technologies les plus populaires de ces dernières années. Un succès qui est dû en partie à la standardisation des communications sans fil mais surtout aux avancées technologiques importantes dans le domaine micro-électronique. Une telle évolution a en effet permis l'élaboration de capteurs toujours plus performants et peu couteux. Les caractéristiques intéressantes des RCSFs en termes de fiabilité, de précision, d'extensibilité et de facilité de déploiement ont fini par charmer le grand public et conquérir les grandes entreprises. La communauté scientifique s'est elle aussi intéressée de près à ce type de réseaux et de multiples projets de recherche ont été élaborés dans le domaine. Ces efforts de recherche ont permis d'améliorer les performances des RCSFs et d'étendre leur zone de couverture ainsi que leur domaine d'application grâce notamment à l'élargissement de la gamme des capteurs. Les RCSFs ont ainsi été utilisés efficacement dans de nombreux domaines incluant les applications de transport, la détection des catastrophes naturelles, la surveillance structurelle, les systèmes d'alimentation ainsi que les domaines militaire et sanitaire.

Constitués de centaines voire des milliers de capteurs s'échangeant des informations via des communications sans fil, le RCSF est fréquemment déployé pour surveiller les conditions physiques ou environnementales dans une zone d'intérêt, traiter les différentes données et transmettre les résultats à un utilisateur final. Les nœuds du réseau vont ainsi interagir avec l'environnement en détectant et en contrôlant des paramètres physiques tels que la température, la pression et le volume suivant les besoins de l'application. Souvent polyvalents, les nœuds du réseau devront non seulement traiter les données, mais également faire preuve de souplesse face aux différentes variations dans leurs tâches résultant des conditions environnementales ainsi qu'à l'épuisement de leurs batteries.

Axe de recherche très fertile ces dernières années, les RCSFs présentent toutefois quelques faiblesses liées à l'environnement hostile et sans surveillance dans lequel ils sont déployés ainsi qu'aux caractéristiques spécifiques de ces derniers. D'un côté, le cadre difficile d'accès et parfois inaccessible à l'homme dans lequel ils sont utilisés rend le remplacement manuel des nœuds endommagés chose coûteuse et difficile. D'un autre côté, les caractéristiques spécifiques des réseaux de capteurs en termes d'absence d'infrastructure, topologie

dynamique du réseau, nombre important de capteurs à la sécurité physique limitée et aux ressources énergétiques réduites influent négativement sur la stabilité ainsi que sur la durée de vie du réseau et nuisent au fonctionnement de ce dernier. De telles faiblesses ont fini par exposer les réseaux de capteurs à divers problèmes de sécurité. Ils se sont ainsi retrouvés sujets à différents types de menaces et d'attaques telles que l'écoute du canal, l'interception des données émises sur le support de communication sans fil, la modification et la suppression de ces données. L'attaquant peut également dérouter les messages, contrôler le flux de données ou endommager les équipements du réseau. De telles attaques peuvent avoir des conséquences désastreuses sur le fonctionnement global du réseau et exposent les applications mises en place à des dégâts économiques et sécuritaires importants.

La problématique de la sécurité des réseaux de capteurs est devenue depuis quelques années un axe de recherche prépondérant suscitant de nombreux défis scientifiques et techniques. L'importance accordée par la communauté scientifique à ce domaine reflète sans aucun doute les enjeux importants reposant sur la sécurité. En effet, un manquement à ce critère va non seulement influer négativement sur les capacités du réseau mais surtout sur les applications qui s'y exécutent. Les applications de routage, de localisation et d'agrégation aussi bien que les applications plus sophistiquées telles que les applications domotiques, médicales et militaires vont se retrouver exposées à des attaques multiples et à des dégâts majeurs. De ce fait, il est devenu inenvisageable de travailler sur des protocoles d'agrégation ou tout autre axe de recherche sans faire appel à une méthode de sécurisation sous peine d'avoir des données altérées et des résultats faussés. La sécurité est devenue un axe indissociable des autres axes de recherche dans les réseaux de capteurs sans fil.

Traditionnellement utilisée comme mécanisme de sécurité efficace, la cryptographie a toujours joué un rôle important dans de nombreux réseaux tels qu'internet et les MANET « Mobile Ad-hoc Networks ». Bien qu'efficaces face aux attaques externes où l'attaquant va se contenter de déclencher des attaques passives, l'efficacité des méthodes cryptographiques est anéantie face aux attaques internes. En effet, en capturant un nœud légitime du réseau, l'attaquant va obtenir toutes ses informations secrètes. Ces clés valides vont lui permettre de s'authentifier et d'interagir dans le réseau comme n'importe quel autre nœud légitime. La sécurisation contre les attaques internes est une problématique supplémentaire pour les réseaux de capteurs auxquelles des solutions efficaces doivent être proposées. Des méthodes complémentaires, qui vont permettre de réussir là où les méthodes cryptographiques ont échoué.

2. Contributions de cette thèse

Plusieurs mécanismes de sécurité découlant de divers axes de recherche ont été utilisés afin de sécuriser les réseaux de capteurs contre les attaques internes. Allant des plus classiques tels que les mécanismes de cryptographie et les systèmes de détection d'intrusions (IDS), passant par les réseaux de neurones, les machines à vecteurs de support (SVM), les mécanismes de confiance et de réputation et la théorie des jeux et jusqu'à des méthodes plus innovantes telles que les métaheuristiques ou encore la très en vogue blockchain. Cependant, aucun mécanisme n'est efficace pleinement et chaque méthode pose quelques inconvénients liés à la difficulté d'implémentation, aux besoins importants en ressources aussi bien qu'aux vulnérabilités à certaines attaques. Dans cette optique, un protocole de sécurité efficace et optimal sera celui qui combinera efficacement entre plusieurs axes afin de tirer parti des avantages et éviter les inconvénients.

Nous nous sommes intéressés dans nos travaux aux mécanismes de confiance et de réputation qui sont une solution innovante dédiée au domaine de la sécurité dans les réseaux de capteurs. Tandis que plusieurs méthodes s'intéressent uniquement au côté préventif afin d'empêcher toute attaque, les mécanismes de confiance et de réputation rendent possible la détection de ces attaques une fois présentes dans le réseau. Cependant, leurs performances peuvent facilement être altérées par des attaquants cherchant à nuire au réseau. Parmi ces attaques, nous avons : les attaques de recommandations malhonnêtes "bad mouthing, ballot stuffing et collusion", l'attaque On-Off, l'attaque de blanchiment "whitewashing", l'attaque de comportement intelligent "intelligent behavior" et l'attaque de comportement conflictuel "conflicting behavior". L'élaboration d'un mécanisme de confiance et de réputation efficace doit tenir compte de ces potentielles attaques afin d'accomplir parfaitement son rôle.

L'objectif premier de notre thèse est la détection des attaques internes dans les réseaux de capteurs sans fil. Dans cette optique, nous nous sommes intéressés aux mécanismes de confiance et de réputation vue leur efficacité dans les réseaux de capteurs et leur facilité d'implémentation. Cependant, les attaques dont sont victimes ces mécanismes, nous ont alerté sur l'impossibilité d'utiliser ces mécanismes tels quels pour la détection des attaques internes étant donné qu'ils engendrent des attaques internes supplémentaires ce qui est loin du but recherché. Notre approche est de contribuer à la sécurisation des systèmes de confiance et de réputation afin que ces derniers puissent être pleinement efficaces pour la sécurisation des réseaux de capteurs contre les attaques internes de manière générale.

Notre première contribution dans cette thèse est justement liée à la détection des attaques de recommandations malhonnêtes dont sont victimes les systèmes de confiance et de réputation dans les réseaux de capteurs sans fil. Cette contribution se résume dans le protocole BTS *(Bee-Trust Scheme)* qui est un protocole bio inspiré dédié aux RCSFs mobiles.BTS combine plusieurs mécanismes : les systèmes de confiance et de réputation comme fondement principal sur lesquels repose le protocole, les métaheuristiques comme approche générale suivant laquelle se déroule le protocole et la psychologie cognitive comme approche de détection complémentaire.

Notre deuxième contribution concerne l'élaboration d'un nouveau mécanisme de confiance et de réputation. Un protocole innovant permettant une gestion intelligente des valeurs de réputation des différents nœuds du réseau. Notre protocole B-Smart combine efficacement les propriétés intéressantes des "smart contrats" et ceux de la blockchain dans le but de permettre une détection efficace ainsi qu'une grande résistance à un grand nombre d'attaques internes.

3. Organisation du manuscrit

Ce manuscrit est organisé en cinq chapitres suivis d'une conclusion générale. Le positionnement de nos travaux est présenté sur les trois premiers chapitres et nos contributions sont détaillées dans les deux derniers chapitres.

Dans le premier chapitre, nous présentons les principales notions liées aux réseaux de capteurs en citant les différentes topologies existantes, les différents types de réseaux, les challenges de conception ainsi que la notion de mobilité dans ce type de réseaux.

Dans le deuxième chapitre, nous allons essayer de passer en revue les principaux concepts et challenges liés à la sécurité en présentant les menaces et les attaques qui peuvent toucher les réseaux de capteurs. Nous allons citer les différentes attaques internes, un moyen pour mieux les connaitre afin de mieux s'en protéger et nous survolerons par la suite les axes de recherche prometteurs pour les protocoles de sécurité.

Dans le troisième chapitre, nous investiguons notre premier axe de recherche, à savoir, les attaques de recommandations malhonnêtes. Nous commencerons par aborder les différentes méthodes de calcul de la confiance et de la réputation. Nous présenterons les besoins en sécurité de ces mécanismes. Une présentation des principales attaques touchant ces mécanismes est donnée par la suite. Nous survolerons ensuite les travaux existants concernant

les attaques de recommandations malhonnêtes, en effectuant une analyse et une classification. Cette étude approfondie, nous permettra de tracer les motivations pour la conception d'un nouveau protocole de détection des attaques de recommandations malhonnêtes.

Dans le quatrième chapitre, nous présentons notre première contribution nommée *Bee-Trust Scheme (BTS)* qui résout le problème des recommandations malhonnêtes dans les réseaux de capteurs mobiles. Une description des motivations ainsi qu'une présentation détaillée du protocole y sont données. L'évaluation des performances ainsi que les résultats de simulation ont démontré que notre proposition offre un taux de détection élevé tout en diminuant le taux de faux positifs et de faux négatifs par rapport aux protocoles existants.

Dans le cinquième chapitre, nous présentons notre deuxième contribution nommée *B-Smart* qui est un nouveau mécanisme de confiance et de réputation permettant de résoudre les problèmes de sécurité liés à ces systèmes. Nous présentons les principales étapes d'exécution du protocole ainsi qu'une analyse de sécurité pour démontrer la résistance de notre protocole face aux attaques des mécanismes de confiance et de réputation et aux attaques de routage.

Nous finalisons ce manuscrit par une conclusion générale dans laquelle nous rappelons les différentes contributions réalisées tout au long de ce travail de recherche et nous présentons les perspectives de recherche.

4. Publications

Le travail présenté dans cette thèse a été couronné par les articles suivants :

Publications internationales

- **Article -1- :** Khedim, F., Labraoui, N., & Ari, A. A. A. (2018). A cognitive chronometry strategy associated with a revised cloud model to deal with the dishonest recommendations attacks in wireless sensor networks. *Journal of Network andComputer Applications*, 123 (2018) 42–56. (**Impact Factor**= 3.991).

  DOI : 10.1016/j.jnca.2018.09.001

- **Article -2- :** Khedim, F., Labraoui, N., & Ari, A. A. A. A Comprehensive Overview on Unfair Ratings Attacks in Wireless Sensor Networks, *Computer Communications* (Soumis).

- **Article -3- :** Khedim, F., Labraoui, N., & Ari, A. A. A. B-Smart: A robust reputation based blockchain scheme in Wireless Sensor Networks, *Computers & Security* (Soumis).

Communication nationale

- **Article :** Khedim, F., Labraoui, N. (2013, Dec). Détection des Attaques par Réplication dans un Réseau de Capteurs Sans Fil. In : Conférence Nationale sur les Technologies de l'Information et les Télécommunications, Tlemcen, Algeria**.**

Communications internationales

- **Article -1- :** Khedim, F., Labraoui, N. (2014, June). The MCD Protocol for Securing Wireless Sensor Networks against Nodes Replication Attacks. In Advanced Networking Distributed Systems and Applications (INDS), 2014 International Conference on (pp. 58-63). IEEE.

  ISBN : 978-1-4799-5178-9
  DOI : 10.1109/INDS.2014.18

- **Article -2- :** Khedim, F., Labraoui, N., & Lehsaini, M. (2015, April). Dishonest recommendation attacks in wireless sensor networks: A survey. In Programming and Systems (ISPS), 2015 12th International Symposium on (pp. 1-10). IEEE.
  Prix du meilleur article.

  ISBN : 978-1-4799-7699-7
  DOI : 10.1109/ISPS.2015.7244964

PREMIERE PARTIE :

REVUE DE LITTÉRATURE SUR LA SÉCURITÉ DES RÉSEAUX DE CAPTEURS SANS FIL

"Il faut apprendre, non pas pour l'amour de la connaissance,
mais pour se défendre contre le mépris dans lequel le monde tient les ignorants".

-Charlie Chaplin-

CHAPITRE I

Les réseaux de capteurs sans fil

Sommaire

1. INTRODUCTION

Depuis quelques années, nous assistons à un engouement pour la miniaturisation électronique. Cette tendance a su bénéficier au matériel et aux réseaux informatiques en produisant en masse et à moindre coût des systèmes d'une taille extrêmement réduite et embarquant des unités de calcul et de communication sans fil. Les réseaux de capteurs sans fil sont l'une des technologies visant à résoudre les problèmes de cette nouvelle ère de l'informatique embarquée et omniprésente.

Le domaine des réseaux de capteurs connaît depuis quelques années un regain important et une évolution continue. Ce type particulier de réseaux ad hoc est utilisé de plus en plus dans de nombreux contextes et dans de nombreuses applications. Constitués d'un nombre important de minuscules dispositifs électroniques à faible coût et à faible puissance, les réseaux de capteurs sans fil (RCSFs) ont su bénéficier de la révolution dans le monde des télécommunications. En effet, dotés d'antenne radio, les nœuds capteurs peuvent échanger des informations sans nécessiter l'utilisation de connexions filaires rigides. Leur capacité d'auto-organisation, de transparence et de surveillance à distance en temps réel ont su charmer la communauté scientifique et promouvoir leur utilisation.

Nous allons présenter dans ce chapitre, les principales notions liées aux réseaux de capteurs en citant les différentes topologies existantes, les différents types de réseaux, les challenges de conception ainsi que la notion de mobilité dans ce type de réseaux.

2. RÉSEAU DE CAPTEURS SANS FIL

Hautement distribué, le réseau de capteurs est déployé en utilisant des centaines voire des milliers de nœuds compacts et peu coûteux. Ces derniers sont densément déployés soit à l'intérieur du phénomène, soit très près de celui-ci (Akyildiz et al., 2002). Le réseau ainsi déployé va permettre la surveillance des conditions physiques ou environnementales telles que la température, l'humidité, les radiations, les pressions, les vibrations ou les polluants et transmettre les données à un emplacement principal (Merad Boudia, 2014).

La popularité grandissante des réseaux de capteurs tant dans la communauté scientifique que dans les applications commerciales est due principalement à leurs nombreuses propriétés. Parmi les caractéristiques offertes par les RCSFs nous pouvons citer la capacité de communication entre les nœuds du réseau, la capacité de détection de l'environnement physique et du traitement collectif des données détectées ainsi que la capacité de fusion des données provenant de plusieurs nœuds.

D'un point de vue technologique, le RCSF est composé principalement de deux types de dispositifs : les nœuds de capteurs et les stations de base.

2.1.Nœuds

Les nœuds souvent appelés "capteurs sans fil ", "motes" ou simplement "capteurs" sont la notion de base dans un RCSF. En effet, l'évolution de l'architecture des capteurs est l'un des facteurs qui a permis l'essor de solutions basées sur ce type de réseaux. L'architecture des capteurs des générations précédentes n'avait en effet qu'une unité de captage et une unité d'alimentation ce qui limite leur utilisation. Composés actuellement de quatre éléments de base : unité de détection, unité de traitement, unité de communication et d'une unité de puissance, les capteurs peuvent traiter, échanger et transmettre les informations. Équipés de capteurs matériels, de microcontrôleurs, d'émetteurs-récepteurs et de batteries, ils sont ainsi capables de surveiller des phénomènes, de détecter des évènements relatifs à ces phénomènes, de récolter les données correspondantes de manière autonome et de traiter ces données.

En fonction de l'application et de la structure utilisée, un RCSF peut contenir différents types de nœuds comme cité dans (Kone, 2011) :

- ***Nœud régulier***. C'est un nœud doté d'une unité de transmission et d'une unité de traitement de données.
- ***Nœud capteur ou nœud source***. C'est un nœud régulier doté d'une unité de détection permettant l'acquisition de données. L'unité d'acquisition permet d'obtenir des mesures et le convertisseur analogique/numérique va permettre de convertir les informations relevées en un signal numérique compréhensible par l'unité de traitement.
- ***Nœud actionneur ou robot***. C'est un nœud régulier doté d'un mécanisme lui permettant d'exécuter certaines tâches spécifiques comme des tâches mécaniques. Ainsi, ce type de nœud peut se déplacer à travers le réseau, effectuer plusieurs actions comme par exemple combattre un incendie, piloter un automate, etc.
- ***Nœud puits***. C'est un nœud doté d'un convertisseur série connecté à une seconde unité de communication (GPRS, Wi-Fi, WiMax, etc.). Cette spécificité va lui permettre de retransmettre de manière transparente les données reçues à un utilisateur final ou à d'autres réseaux comme internet.
- ***Nœud passerelle (ou gateway).*** C'est un nœud régulier permettant de relayer le trafic dans le réseau sur le même canal de communication.

2.2.Station de base

La station de base est un périphérique plus puissant en termes de ressources de calcul, d'énergie et de communication par rapport aux autres nœuds. Elle joue un rôle important dans le réseau en se comportant comme une passerelle entre les nœuds capteurs et les utilisateurs finaux. Ainsi, elle permet de recueillir les informations provenant des nœuds capteurs, de stocker ces informations et d'émettre des ordres de contrôle aux nœuds afin de changer leur comportement. La majeure partie des applications s'exécutant dans les RCSFs utilisent une ou plusieurs stations de base. Cependant, l'architecture du réseau demeure toujours décentralisée. Il existe toutefois des réseaux spécifiques, connus sous le nom de réseaux de capteurs sans surveillance, où la station de base n'est disponible qu'à certains moments dans le temps (Lopez et al., 2010).

3. TOPOLOGIES DES RCSFs

Le déploiement ainsi que le développement d'un réseau de capteurs utilisent les architectures traditionnelles dans de nouvelles directions. Ces topologies font référence à la disposition des nœuds dans le réseau. Les topologies les plus courantes sont la topologie en étoile, la topologie maillée et la topologie hybride étoile-maillée (Selmic et al., 2016).

3.1.Topologie en étoile

Dans la topologie en étoile, les nœuds sont disposés en étoile avec la station de base en tant que centre de l'étoile (voir Figure 1.1). Cette topologie ne permet pas les communications directes entre les nœuds et tout le flux de données doit impérativement passer par la station de base. Cependant, bien que cette topologie consomme peu d'énergie, le fait qu'elle dépende d'un seul nœud pour gérer le trafic de tout le réseau impacte négativement sur la sécurité et la fiabilité globale du réseau.

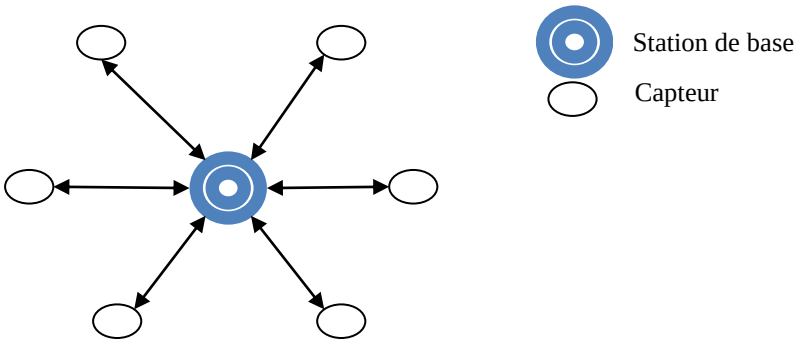


Fig 1. 1. Topologie en étoile

3.2.Topologie maillée

Dans la topologie maillée, les nœuds de capteurs sont disposés d'une manière leurs permettant de communiquer les données les uns aux autres (voir Figure 1.2). Cette topologie rend possible les communications multi-sauts en permettant aux nœuds d'utiliser d'autres nœuds pour envoyer des données hors de leur rayon de communication. Le coté maillé permet entre autre de rendre la topologie résistante aux éventuelles pannes des capteurs. Cependant, cette topologie utilise beaucoup plus de puissance que la topologie précédente en raison des transmissions redondantes des données.

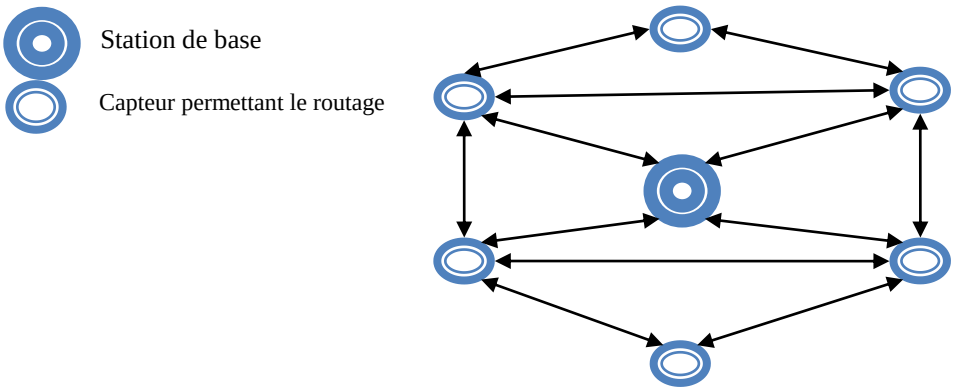


Fig 1. 2. Topologie maillée

3.3.Topologie hybride étoile-maillée

Dans la topologie hybride étoile-maillée, le réseau tire parti des avantages des deux topologies : en étoile et maillée. En effet, il bénéficie d'une part de la faible consommation d'énergie de la topologie en étoile tout en profitant de la redondance des données de la topologie maillée pour assurer la transmission des données aux nœuds destinataires. Dans cette architecture (voir Figure 1.3), les nœuds au cœur du maillage disposent d'une puissance élevée leur permettant de servir de gateway et d'assurer les transmissions entre un large nombre de nœuds. Les nœuds à l'extrémité du réseau disposent par contre d'une faible énergie vu qu'ils n'ont pas besoin d'effectuer un grand nombre de transmissions.

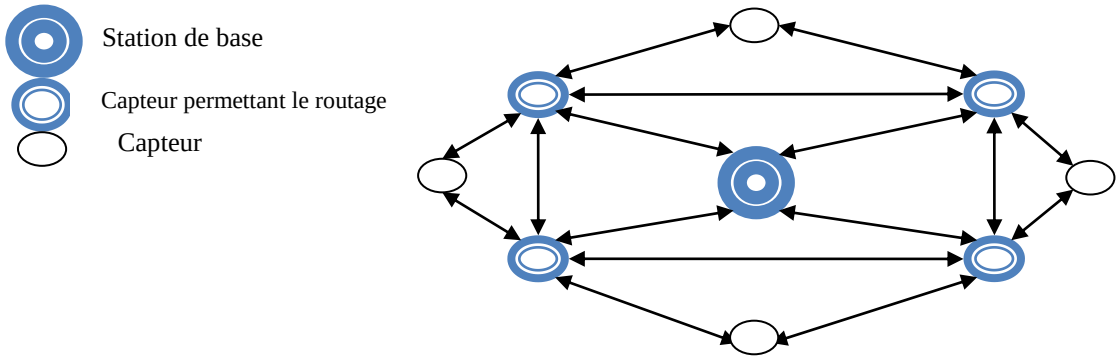


Fig 1. 3. Topologie hybride étoile-maillée

4. DIFFERENTS TYPES DE RCSFs

Pour répondre aux besoins grandissants des nouvelles applications de vouloir anticiper les événements, de détecter les phénomènes et de transmettre les informations dans n'importe quelle situation, les développeurs ont dû créer de nouveaux types de capteurs toujours plus robustes et pouvant supporter des conditions extrêmes. Suivant les caractéristiques des capteurs, quatre différents types de RCSFs ont été définit, ces derniers sont énumérés dans ce qui suit :

4.1. RCSFs terrestres

Les réseaux de capteurs terrestres se composent de centaines ou de milliers de nœuds de capteurs sans fil. Ces nœuds sont distribués de manière aléatoire dans un mode non structuré, dans une zone cible. Leur positionnement au-dessus du sol leur permet de pouvoir utiliser l'énergie solaire pour alimenter leurs batteries. En conservant leurs énergies, ces capteurs vont permettre de rallonger la durée de vie de tout le réseau. Ces réseaux sont utilisés dans diverses applications telle que : la détection des feux de forêts.

4.2. RCSFs souterrains

Les réseaux de capteurs souterrains utilisent des capteurs plus coûteux que ceux des réseaux terrestres ainsi que des équipements chers. Utilisés pour surveiller les conditions souterraines, ces réseaux utilisent néanmoins des nœuds puits présents au-dessus du sol pour transmettre les informations à la station de base. Les conditions souterraines exigent un entretien régulier pour le maintien du réseau et rendent la recharge des batteries chose difficile. Les atténuations dans l'environnement souterrain influent négativement sur la qualité

du signal provocant des pertes d'information. Ces réseaux sont utilisés par exemple dans les applications agricoles nécessitant la connaissance du degré d'humidité du sol.

4.3. RCSFs sous-marins "underwater"

Les réseaux de capteurs sous-marins utilisent des nœuds de capteurs immergés sous l'eau. La collecte des données à partir de ces nœuds nécessitent l'utilisation de véhicules sous-marins. Bien qu'utile, ce type de réseau présente néanmoins plusieurs contraintes : la difficulté de déploiement, le long délai de propagation, le dysfonctionnement de la radio, les défaillances des capteurs ainsi que l'épuisement des batteries. Différentes techniques sont développées pour résoudre ces problèmes d'utilisation et améliorer les performances. Ces réseaux sont utilisés par exemple pour mesurer le degré de la houle et ainsi être en mesure d'anticiper les tsunamis.

4.4. RCSFs multimédia

Les réseaux de capteurs multimédia utilisent des nœuds capteurs connectés à des caméras et à des microphones. Ils permettent de recueillir les informations sous forme d'image, d'audio ou de vidéo. Ces réseaux permettent de suivre et de surveiller les différents évènements qui se produisent tout en gardant un affichage visuel de ces derniers. Ils permettent aussi la compression, la récupération et la corrélation des données. Ces réseaux permettent la transmission de vidéo et d'audio, engendrant une forte consommation d'énergie et de bande passante. Ces réseaux sont largement utilisés dans les applications récentes et principalement dans le domaine de la domotique.

4.5. RCSFs mobiles

Les réseaux de capteurs mobiles utilisent des capteurs mobiles, pouvant se déplacer dans la zone cible. Grâce à cette notion de mobilité, ces réseaux peuvent interfacer avec l'environnement qui les entoure. En comparaison avec les réseaux terrestres, les réseaux mobiles sont plus polyvalents et offrent une meilleure couverture ainsi qu'une capacité de canal supérieure.

La notion de mobilité est présentée en détail dans la section 8 de ce chapitre.

5. SERVICES OFFERTS PAR LES RCSFs

Les réseaux de capteurs offrent plusieurs services. Ces services ont étendu leur utilisation dans plusieurs applications. Parmi ces applications la surveillance environnementale, la surveillance militaire ainsi que la surveillance médicale. La capacité de reprogrammer le

réseau, ou de l'utiliser comme plateforme informatique répartie sont quelques exemples de services offerts par les réseaux de capteurs. Hormis ces derniers, les services sont généralement classés en quatre catégories principales : la surveillance, l'alerte, la fourniture d'informations à la demande et l'actionnement (Lopez et al., 2010).

5.1. Surveillance

Les réseaux de capteurs offrent la possibilité de surveiller en permanence certaines caractéristiques de l'environnement. De ce fait, les capteurs seront chargés de mesurer certaines propriétés (par exemple, mesurer le degré d'humidité de l'air) et d'envoyer ces informations à la station de base en temps voulu.

5.2. Alerte

Les réseaux de capteurs permettent d'alerter les utilisateurs du système dans le cas où certaines circonstances physiques se produisent (par exemple un incendie).

5.3. Informations à la demande

Le réseau de capteurs peut fournir les valeurs actuelles d'une certaine fonctionnalité à chaque fois que l'utilisateur en a besoin.

5.4. Actionnement

Le réseau de capteurs offre la possibilité aux nœuds capteurs d'apporter des modifications au système externe en fonction du contexte (par exemple déclencher la borne à incendie une fois que la température dépasse un certain seuil).

6. TRAFIC DE DONNÉES DANS LES RCSFs

L'acheminement des données dans les réseaux de capteurs dépend essentiellement des besoins de l'application. En effet, les RCSFs proposent trois types de trafic pouvant être utilisés séparément ou conjointement selon le but recherché. Les trois types de trafic sont (Roth, 2012) :

6.1. Trafic orienté temps (time-driven)

Dans ce type de trafic, les données sont transmises à intervalle régulier par les nœuds capteurs. L'application s'exécutant sur les capteurs va permettre de fixer la fréquence d'envoi des données. Cette fréquence peut donc varier de quelques millisecondes à plusieurs heures voire plusieurs jours selon les besoins. Ce type de trafic est le plus utilisé dans les RCSFs.

6.2. Trafic orienté requêtes (query-driven)

Dans ce type de trafic, les données sont transmises en réponse à une requête envoyée par un utilisateur ou une application. En effet, l'utilisateur va pouvoir émettre une demande via une application distante ou bien installée sur la station de base du réseau à un nœud ou à un ensemble de nœuds afin d'obtenir des informations.

6.3. Trafic orienté événements (event-driven)

Dans ce type de trafic, les données sont transmises en fonction des évènements. De manière générale, les nœuds récupèrent périodiquement les données de leur environnement. Ces données sont analysées. Si un événement ou bien un phénomène physique est détecté à partir de ces analyses, le nœud va transmettre l'information au puits. Ensuite, en fonction de l'application installée sur le nœud et sur la station de base, la remontée d'information pourra s'effectuer de manière périodique ou à la demande de la station de base pour confirmer l'événement.

7. CHALLENGES LIÉS À LA CONCEPTION D'UN RCSF

Les RCSFs ont permis d'ouvrir de nouveaux horizons dans le domaine de la gestion de l'information. Cependant, la conception d'un réseau de capteurs est influencée par de nombreux facteurs. La connaissance de ces facteurs permet de servir de guide lors de la conception d'un protocole ou d'un algorithme dédié aux RCSFs. En voici une liste non exhaustive (Akyildiz et al., 2002) :

7.1. Tolérance aux pannes

La tolérance aux pannes ou fiabilité est la capacité d'un RCSF à maintenir ses fonctionnalités sans être affecté par les défaillances pouvant toucher certains de ses nœuds. En effet, les capteurs peuvent être sujets à des dommages physiques, à un épuisement d'énergie aussi bien qu'à des interférences environnementales. Ces problèmes ne doivent en aucun cas affecter le fonctionnement global du réseau. La tolérance aux pannes est fortement liée à l'environnement dans lequel est déployé le RCSF. Dans les environnements avec peu d'interférences, la tolérance aux pannes est faible car les capteurs ont peu de risque d'être endommagés. Cependant, dans les environnements hostiles tels que les champs de guerre, la tolérance doit être élevée car les données détectées sont critiques et les nœuds de capteurs peuvent être endommagés par des actions hostiles.

7.2. Passage à l'échelle

Certaines applications peuvent nécessiter l'utilisation d'une centaine voire des milliers de capteurs. Ce nombre peut atteindre la valeur extrême de millions. Par conséquent, les protocoles doivent être en mesure de fonctionner correctement même avec un grand nombre de nœuds et quel que soit la densité des nœuds à travers le réseau.

7.3. Coûts de production

Étant constitué d'un très grand nombre de nœuds capteurs, le coût d'un seul de ces capteurs est un paramètre important influençant l'utilisation ou non d'un RCSF. En effet, si le coût global du RCSF est plus élevé que celui d'un réseau traditionnel offrant des services comparables, alors, les coûts de déploiement ne sont plus justifiés.

7.4. Contraintes matérielles

Un nœud capteur est constitué de quatre unités de base : détection, traitement, émission-réception et alimentation ainsi que de composants supplémentaires tels qu'un système de localisation, un générateur d'énergie et un mobilisateur. Tous ces composants ont la contrainte de tenir dans un module de la taille d'une boite d'allumettes (Intanagonwiwat et al., 2000). Le capteur doit respecter d'autres contraintes telles que :

- Consommer le moins d'énergie possible.
- Fonctionner quel que soit les densités volumétriques.
- Avoir de faibles coûts de production.
- S'adapter à l'environnement.
- Être assez léger.
- Être autonome et fonctionner sans surveillance,

7.5. Topologie dynamique

Le réseau de capteurs subit plusieurs changements tout au long de sa durée de vie. En effet, la disparition d'un certain nombre de nœuds, les défaillances des nœuds, la rupture des liens de communication entre ces derniers ainsi que le déploiement de nouveaux nœuds rendent la topologie du réseau instable et dynamique. L'évolution d'un réseau de capteurs passe par trois étapes principales :

- *Déploiement* : Étant la première étape du cycle de vie d'un RCSF, le déploiement permet la mise en place du réseau en positionnant les nœuds capteurs suivant les besoins de l'application. Ce dernier peut se faire de différentes manières suivant l'endroit de déploiement ainsi que de l'application. Il peut par exemple, s'effectuer par

avion dans les zones difficiles d'accès, au moyen de catapulte dans les applications militaires ou bien d'une manière déterministe par un robot ou par un humain dans les zones faciles d'accès.

- *Post-Déploiement*. Lors de cette phase d'exploitation, le réseau peut subir de multiples changements. Ces changements peuvent avoir de multiples causes, tels qu': un épuisement de l'énergie, un changement de position, un dysfonctionnement ou bien des pannes de certains nœuds.
- *Redéploiement :* L'introduction de nouveaux capteurs dans un réseau existant pour remplacer les nœuds défaillant nécessite la réorganisation du réseau et la mise à jour de la topologie grâce à l'utilisation de protocoles de routage spéciaux.

7.6. Environnement

Souvent déployés dans des zones hostiles et sans surveillance, les RCSFs doivent pouvoir fonctionner correctement quel que soit l'environnement et dans différentes conditions. Ils sont ainsi utilisés dans des zones géographiques éloignées; ils peuvent fonctionner dans un milieu contaminé biologiquement ou chimiquement, à la surface d'un océan pendant une tornade, attachés à des véhicules rapides ou à des animaux aussi bien que dans les maisons et les grands bâtiments.

7.7. Sécurité

Bon nombre des contraintes précédentes influent négativement sur l'aspect de la sécurité du réseau de capteurs. D'une part, l'environnement hostile et sans surveillance dans lequel ils sont déployés les expose à différents types d'attaques. La topologie dynamique d'un autre coté rend la surveillance difficile et la détection des nœuds compromis compliquée. Enfin, les contraintes matérielles des nœuds capteurs en termes de limitation de stockage, de puissance de calcul et d'énergie rendent l'élaboration de protocoles de détection pleinement efficace chose difficile. La sécurité dans les réseaux de capteurs est expliquée en détail dans le chapitre II de cette thèse.

8. MOBILITÉ DANS LES RCSFs

Au cours des dernières années, les besoins des réseaux de capteurs sans fil ont évolué suivant les besoins des applications. En effet, les applications qui étaient à l'origine statiques et à usage unique ont évolué vers des applications nécessitant un soutien pour la mobilité et à des fins multiples. Des études récentes ont démontré que l'utilité ainsi que la fonctionnalité

d'un réseau de capteurs peuvent être largement améliorées en introduisant la mobilité à certains nœuds ou à tous les nœuds. Les capacités croissantes et les coûts décroissants des capteurs mobiles viennent faciliter cette évolution, en rendantla réalisation de réseaux de capteurs mobiles possibles et pratiques. Nous allons nous intéresser dans ce qui suit aux principaux critères liés à la mobilité.

8.1. Modèles de mobilité

Les modèles de mobilité représentent la capacité des capteurs à changer leur position initiale (Camp et al., 2002). Ils permettent de calculer comment l'emplacement, la vitesse et l'accélération de chaque capteur changent avec le temps (Mohamed et al., 2017). Un bon modèle de mobilité est donc celui qui émule de façon raisonnable le mouvement des nœuds mobiles réels. Basée sur des caractéristiques de mobilité spécifiques, la classification des modèles de mobilité se fait principalement en quatre catégories (Selmic et al., 2016) :

8.1.1. Modèles aléatoires

Dans le modèle aléatoire, les nœuds se déplacent de manière aléatoire. La direction du nœud est choisie au hasard, et le nœud se déplace dans cette direction jusqu'à atteindre la limite de la zone, fait une pause pendant un moment, puis commence à se déplacer dans une nouvelle direction (Mohamed et al., 2017). Parmi les modèles connus entrant dans cette catégorie, nous pouvons citer : le modèle de mobilité aléatoire *"random waypoint"* qui est le modèle le plus utilisé, où un nœud choisit aléatoirement une direction et une vitesse. Lorsque le nœud atteint cette destination, l'algorithme effectue une pause puis réitère. Nous avons aussi le modèle de direction aléatoire *"random direction"* et le modèle de mobilité aléatoire *"random walk mobility"*.

8.1.2. Modèles à dépendance temporelle

Dans ce type de modèle, la dépendance temporelle joue un rôle clé dans la détermination du comportement de la mobilité. En effet, les mouvements des nœuds sont susceptibles d'être influencés par leur historique de mouvement. Parmi les modèles connus entrant dans cette catégorie, nous pouvons citer : le modèle *"Gauss–Markov"* ainsi que le modèle *"smooth random mobility"*.

8.1.3. Modèles à dépendance spatiale

Dans le modèle à dépendance spatiale, les nœuds mobiles ont tendance à se déplacer de manière corrélée. Des groupes de nœuds vont donc se former et travailler en coopération. À

chaque groupe est associé un chef de groupe et c'est le mouvement de ce leader qui va déterminer le comportement de mobilité de l'ensemble du groupe (Rezazadeh et al., 2012). Les modèles de mobilité tels que le modèle de mobilité de groupe de points de référence *"reference point group mobility"*, le modèle de mobilité de groupe de vitesse de référence *"reference velocity group mobility"* et le modèle de mobilité de groupe structuré *"structured group mobility"* appartiennent à cette catégorie.

8.1.4. Modèles à contraintes géographiques

Dans ce type de modèle, les mouvements des nœuds mobiles sont contraints par les conditions géographiques. Parmi celles-ci, les rues, les autoroutes, les murs ainsi que les différents obstacles. Le modèle *"pathway model"* ainsi que le modèle *"obstacle mobility"* sont deux exemples de ce modèle de mobilité.

8.2. Avantages de la mobilité

Le déploiement d'un réseau de capteurs doit souvent faire face à de nombreux défis tels que les moyens utilisés pour déployer les nœuds capteurs ainsi que la position idéale de chacun d'eux. La distribution optimale des capteurs reste souvent inconnue jusqu'à ce que le réseau devienne fonctionnel et commence à collecter et à traiter les informations. Ce déploiement optimal est généralement infaisable sans ajouter la notion de mobilité (Rezazadeh et al., 2012). Nous allons aborder dans ce qui suit certains avantages liés à l'ajout de la mobilité dans les RCSFs (Rezazadeh et al., 2012) :

- Rallonger la durée de vie du réseau. Le fait que les capteurs puissent se déplacer à travers le réseau rend la transmission plus dispersée et l'énergie dissipée plus efficace. En effet, la présence de nœuds mobiles va permettre d'étendre la durée de vie du réseau est cela de multiples manières. D'une part, la présence de nœuds mobiles va permettre de pallier au problème de la grande consommation d'énergie des capteurs se trouvant près de la station de base. Les nœuds mobiles peuvent aussi rétablir les communications dans les RCSFs brisés ou disjoints. Enfin, l'utilisation de station de base mobile traversent la région de détection afin de collecter les données, ou se positionnant de telle sorte que le nombre de sauts de transmission est minimisé pour les nœuds de capteurs, va permettre une réduction importante de la consommation d'énergie.
- Améliorer la capacité du canal : Les gains en capacité pour les RCSFs mobiles sont nettement plus importants que ceux des réseaux statiques. En effet, la présence de

nœuds mobiles va permettre de maintenir l'intégrité des données grâce à la présence de multiples voies de communication ainsi qu'à la réduction du nombre de sauts lors des transmissions (Kansal et al., 2004).

- Améliorer la couverture et le ciblage. La présence de nœuds mobiles dans le réseau de capteurs permet d'améliorer la couverture de ce dernier et son utilité de déploiement (Wang et al., 2005 ; Ari et al., 2017). En effet, le déploiement à distance de capteurs statiques dans des zones souvent hostiles et difficiles d'accès rendait le réarrangement de ces derniers une mission impossible. Un tel réarrangement est pourtant souvent utile pour suivre les besoins évolutifs de l'application en fonction des données collectées et des évènements détectés. L'intégration des capteurs mobiles a donc permis de résoudre ce problème en rendant un tel réagencement chose facile.
- Améliorer les performances. En améliorant la qualité des communications, en augmentant la capacité du réseau et en assurant une plus grande sécurité, les réseaux mobiles permettent d'améliorer les performances globales du système.
- Meilleure fidélité des données. L'utilisation de nœuds mobiles dans le transport des données s'avère très utile lorsque le canal est en mauvais état ou lorsqu'il y'à un risque d'épuisement d'énergie. Cela permet aussi d'augmenter la probabilité des transmissions réussies en réduisant le nombre de saut.

8.3. Challenges liés à la mobilité

L'introduction d'entités mobiles dans des réseaux de capteurs statiques offre certes de nombreux avantages mais pose des challenges supplémentaires à ceux liés à la conception d'un RCSF statique. Parmi ces derniers (Rezazadeh et al., 2012) :

- Localisation. Contrairement aux réseaux de capteurs statiques où la position des nœuds est déterminée lors de l'initialisation, les nœuds mobiles doivent obtenir en permanence leur position. Cette contrainte nécessite plus de temps et d'énergie ainsi que l'utilisation d'un algorithme de localisation rapide.
- Topologie du réseau. Contrairement aux réseaux statiques, la topologie dans les réseaux de capteurs est dynamique nécessitant l'utilisation de nouveaux protocoles de routage et de contrôle d'accès au support (MAC). En effet, Dans les topologies dynamiques, les tables de routage deviennent rapidement obsolètes. La découverte d'itinéraire quant à elle doit être répétée en permanence impliquant un coût important en termes de puissance, de temps et de bande passante.

- Consommation d'énergie. Les modèles de consommation d'énergie diffèrent grandement entre les réseaux de capteurs statiques et réseaux de capteurs mobiles. Certes, la communication sans fil implique un coût énergétique important pour les deux types de réseaux et doit être utilisée efficacement, cependant, les entités mobiles nécessitent une puissance supplémentaire pour la mobilité. Ces entités sont donc souvent équipées d'une réserve d'énergie beaucoup plus grande ou disposent d'une capacité d'auto-recharge.

9. CONCLUSION

Dans ce chapitre nous avons procédé à l'étude des réseaux de capteurs sans fil. Un moyen pour nous de mieux les comprendre afin de répondre au mieux à leurs besoins. Nous avons ainsi présenté les principales notions liées à ces réseaux ainsi que les challenges de conception. Parmi ces défis, nous avons remarqué que la sécurité est un facteur important pour les RCSFs permettant de protéger les données et de préserver l'intégrité du réseau. Cependant, l'élaboration d'un protocole de sécurité efficace pour les réseaux de capteurs se heurte à plusieurs contraintes telles que : les contraintes matérielles, environnementales ainsi que la topologie dynamique du réseau.

Le chapitre suivant est consacré à la notion de sécurité dans les RCSFs. Nous allons présenter les critères de sécurité ainsi que les principaux défis de conception d'un protocole de détection efficace. Nous allons nous intéresser particulièrement aux attaques internes. Des attaques bien insidieuses et pouvant passer inaperçues tout en causant un maximum de dégâts.

CHAPITRE II

La Sécurité dans les Réseaux de Capteurs sans Fil

Sommaire

1. INTRODUCTION

L'expansion des réseaux de capteurs et leur utilisation dans des applications critiques font que la sécurité soit une problématique permanente et une question essentielle à laquelle des solutions adéquates doivent être proposées. L'élaboration de telles solutions est une tâche difficile pour plusieurs raisons. D'une part, les caractéristiques physiques des capteurs, à savoir, contrainte d'énergie, faible puissance de calcul et capacité de stockage limitée, rendent l'utilisation des protocoles de sécurité classiques connus pour être gourmand en ressources chose difficile. D'autre part, l'environnement hostile et sans surveillance dans lequel ces réseaux sont déployés présente une menace supplémentaire pour ce type de réseaux et une aubaine certaine pour les attaquants. Les RCSFs peuvent donc être sujets à différentes menaces et à une multitude d'attaques ayant la possibilité d'intercepter les données échangées sur le support sans fil, de modifier les informations, de rejouer les données, d'injecter des données erronées et de saturer ou d'endommager les équipements du réseau.

Dans ce chapitre, nous allons passer en revue les principaux concepts et challenges liés à la sécurité en présentant les menaces et les attaques qui peuvent toucher les réseaux de capteurs. Nous allons citer les différentes attaques internes, un moyen pour mieux les connaitre afin de mieux s'en protéger et nous survolerons par la suite les axes de recherche prometteurs pour les protocoles de sécurité.

2. CRITÈRES DE SÉCURITÉ

Plusieurs critères peuvent être exigés d'un protocole afin de s'assurer que les besoins en sécurité soient respectés. Les principaux critères de sécurité sont énumérés dans ce qui suit (Rathore, 2016) :

2.1. Confidentialité

La confidentialité des données est cette caractéristique d'une information de n'être jamais divulguée a des tiers non autorisés. Cela signifie pour les RCSFs que le nœud destinataire est le seul à pouvoir accéder à l'information qui lui a été transmise. Son but principal est d'empêcher toute utilisation non autorisée des données dont la révélation d'informations en transit. De ce fait, un réseau fournissant la confidentialité des données va permettre d'assurer la sécurité des échanges à travers son canal de communication en empêchant la fuite des données à partir des nœuds. Donc, plus les applications sont critiques, par exemple, application militaire, plus les informations sont sensibles, plus le nombre de nœuds autorisés à

accéder aux informations est réduit et plus le besoin de confidentialité devient grand. La confidentialité est souvent appliquée grâce à l'utilisation du chiffrement symétrique ou asymétrique (Tripathi et al., 2014).

2.2. Intégrité

L'intégrité des données vise à garantir que le contenu d'un message n'a pas été modifié par un attaquant ou bien altéré accidentellement lors du processus de transmission. Lors des communications multi-sauts dans les RCSFs, un attaquant peut compromettre un ou plusieurs nœuds entre le nœud source et le nœud de destination afin de modifier les messages véhiculés. De ce fait, un RCSF garantissant l'intégrité des données, doit permettre de garantir l'exactitude et l'exhaustivité de l'information en bloquant toute tentative d'injection de données erronées dans le réseau. Plus la fiabilité des informations d'une application est critique, plus l'intégrité des données a de l'importance. L'intégrité des données peut être réalisée grâce à l'utilisation des fonctions de hachage cryptographiques telles que la cryptographie à courbe elliptique « ECC » et DNA (Singh et al., 2017).

2.3. Disponibilité

La disponibilité des données est cette qualité d'une information d'être accessible par les utilisateurs autorisés en temps opportun. Garantir une disponibilité totale des données dans les RCSFs n'est souvent pas réalisable. L'indisponibilité de ces données peut avoir plusieurs causes, la présence d'attaquants puissants pouvant bloquer les transmissions de faible puissance des capteurs, des dysfonctionnements ou pannes des capteurs ou bien à des problèmes liés au canal de transmission tels que les brouillages. Plus les informations sont indispensables pour une application plus la prise de décision et les actions vont dépendre de ces informations et plus la disponibilité doit être précise et optimale (Sharifi et al., 2007).

2.4. Contrôle d'accès

Le contrôle d'accès va permettre d'autoriser ou bien de refuser l'utilisation de programmes ou de ressources par certains utilisateurs. Dans les RCSFs, le contrôle d'accès spécifie les politiques d'accès. De ce fait, l'accès au réseau est autorisé uniquement pour les entités éligibles, le réseau doit refuser les requêtes provenant de nœuds extérieurs afin d'empêcher d'éventuels attaquants d'interagir dans le réseau (Labraoui, 2012).

2.5. Authentification

L'authentification des données est une caractéristique permettant de s'assurer de la légitimité de la demande d'une entité accédant à une donnée. Dans les RCSFs, cette authentification est d'autant plus importante afin de repérer les paquets malicieux et les données falsifiées. Deux types d'authentification sont envisageables (Faye et al., 2014) : authentification des nœuds et celle de requêtes. Dans le premier cas, un nœud émetteur va envoyer son identifiant à un nœud récepteur pour prouver son identité, ce dernier va pouvoir décider si cet identifiant est valide ou non. Deuxièmement, l'authentification de requêtes permet de vérifier l'origine d'une requête donnée en validant sa provenance : station de base (SB), nœud capteur ou d'un utilisateur légitime.

2.6. Autorisation

L'autorisation consiste à accorder des droits d'accès à l'utilisateur afin d'établir une relation entre un utilisateur et un ensemble de services. Un réseau de capteur, doit être en mesure de donner ou de retirer l'autorisation d'accès aux utilisateurs.

2.7. Fraicheur

La fraicheur des données permet de garantir que les données échangées sont actuelles et non redondantes. Dans les RCSFs, afin d'assurer que les anciennes communications ne peuvent pas être réinjectées dans le réseau, comme c'est le cas lors de l'attaque par rejeu, un nombre aléatoire ou pseudo-aléatoire appelé nonce doit être intégrer dans chaque message échangé entre le nœud émetteur et le nœud récepteur (Drira et al., 2008).

2.8. Robustesse

La robustesse consiste à garantir que le réseau est fonctionnel et capable de gérer les erreurs dans des conditions difficiles aussi bien que dans des environnements hostiles (Rathore, 2016).

3. PRINCIPAUX DÉFIS DE SÉCURITÉ

L'application des méthodes de sécurité classiques dans les réseaux de capteurs se heurte à plusieurs obstacles. Les caractéristiques spécifiques de ces réseaux les rendent très vulnérables aux attaques. Par conséquent, un bon mécanisme de sécurité doit tenir compte de plusieurs contraintes, parmi lesquelles (Drira,et al., 2008; Djallel Eddine, 2013) :

3.1. Ressources limitées

Les ressources limitées des nœuds capteurs en termes de stockage, de bande passante, de puissance de calcul et d'énergie rendent l'élaboration de mécanismes de sécurité efficaces un réel challenge. En effet, en plus de devoir être efficaces de tels protocoles doivent traiter un minimum d'instructions compte tenu de la limitation de la mémoire, réaliser un minimum de calculs et minimiser le nombre de messages échangés afin de ne pas épuiser l'énergie des capteurs.

3.2. Communication sans fil

Bien que les réseaux sans fil offrent l'avantage de réduire le coût de l'infrastructure, le fait d'être un moyen de communication ouvert les rend moins fiables que les réseaux filaires. En effet, le médium de communication sans fil rend les échanges sensibles aux interférences, à la congestion et aux erreurs du canal. Ce type de communication facilite aussi l'accès non autorisé au réseau, l'écoute abusive, l'interception ainsi que les collisions et les dénis de service (Drira et al., 2008).

3.3. Environnement non surveillé

Les réseaux de capteurs sont souvent déployés dans des environnements ouverts et hostiles. Dans certaines applications, les nœuds capteurs sont laissés sans surveillance pendant de longues périodes. Ces conditions de déploiement exposent le réseau aux attaques physiques (Yussoff et al., 2012). Ainsi, un attaquant peut facilement capturer, compromettre ou détruire un nœud du réseau. Un attaquant peut aussi reprogrammer un nœud avant de le réintroduire dans le réseau, ce nœud compromis va pouvoir écouter les échanges, injecter des données erronées et ainsi nuire au réseau.

3.4. Déploiement aléatoire et utilisation à grande échelle

Le déploiement aléatoire des nœuds capteurs sans connaissance préalables des positions ainsi que leur utilisation à grande échelle constituent deux des plus importantes caractéristiques des RCSFs. Cependant, de telles architectures nécessitent des protocoles de sécurité plus efficaces permettant la surveillance d'un nombre important de capteurs et pouvant faire face à l'instabilité de l'environnement (Djallel Eddine, 2013).

3.5. Agrégation des données

L'agrégation des données (Drira et al., 2008) est connue comme étant une des techniques permettant d'optimiser la durée de vie d'un réseau de capteur. En effet, minimiser le nombre

de paquets transférés vers le nœud puits, en éliminant les données redondantes revient à économiser l'énergie si précieuse pour les nœuds capteurs. Cependant, l'agrégation exige l'intervention de nœuds intermédiaires dans le processus d'échange posant ainsi un défi supplémentaire pour les mécanismes de sécurité.

4. VULNÉRABILITÉS DES RÉSEAUX DE CAPTEURS SANS FIL

Dans les réseaux de capteurs deux principaux types de vulnérabilités sont exploités par les attaquants dans le but de gagner des privilèges. Ces deux types sont (Labraoui, 2012) :

4.1. Vulnérabilité physique

L'environnement non surveillé ainsi que les ressources limitées des capteurs représentent les principales vulnérabilités physiques des nœuds. En effet, un attaquant peut facilement capturer un capteur, copier ses clés cryptographiques et modifier son code de programmation afin de le rendre malicieux et l'utiliser pour lancer des attaques.

4.2. Vulnérabilité logique

Cette vulnérabilité concerne les faiblesses dans les programmes et les protocoles. Elle se présente sous quatre formes : les défauts de conception, les défauts d'implémentation, les erreurs de configuration et l'épuisement des ressources.

- Les défauts de conception laissent des brèches à l'utilisation de protocoles qui tentent de violer le mode d'utilisation, tout en se conformant aux spécifications du protocole. Par exemple, un manque d'authentification dans un protocole de sécurité peut permettre à n'importe quel attaquant de s'introduire dans le réseau.
- Les défauts d'implémentation représentent des erreurs dans le codage du logiciel ou bien dans la construction du matériel. Par exemple, une erreur de dépassement de mémoire peut causer une violation d'accès et une mise en panne.
- Les défauts de configuration sont le résultat de défauts de paramétrages pour un attaquant.
- L'épuisement des ressources est possible même si les trois étapes précédentes sont correctes. Des attaques générant trop de trafic peuvent facilement épuiser les ressources des capteurs.

5. CLASSIFICATION DES ATTAQUES DANS LES RÉSEAUX DE CAPTEURS SANS FIL

Le problème de sécurité est le souci majeur de toute application s'exécutant dans un réseau de capteurs. En effet, les ressources limitées des capteurs ainsi que l'environnement hostile dans lequel ils sont déployés les rendent extrêmement vulnérables à une variété d'attaques. Plusieurs classifications de ces attaques sont données dans la littérature : selon la cible visée par l'attaquant, selon la couche protocolaire qu'elles ciblent dans le modèle OSI, selon la nature de l'attaque ou bien de son origine. Les différentes catégories sont présentées dans ce qui suit :

5.1. Classification selon la cible visée par l'attaque

Selon que l'attaquant cherche à porter préjudice aux données ou bien à l'infrastructure du réseau, deux catégories distinctes d'attaques ont été présentées dans (Rathore, 2016) : les attaques sur les données et les attaques sur l'infrastructure.

5.1.1. Attaques sur les données

Les attaques sur les données consistent à intervenir de telle manière à perturber le réseau en provoquant un écart entre les résultats obtenus et le comportement normal attendu. Ces attaques englobent entre autres le vol de paquets, la modification des données et l'injection de paquets erronés.

5.1.2. Attaques sur l'infrastructure

Les attaques sur l'infrastructure consistent à capturer des nœuds, à prendre leurs identités et à consommer leurs ressources. En envoyant des paquets inutiles à la victime, ces attaques vont tenter d'épuiser les ressources du réseau.

5.2. Classification basée en couches

Les attaques peuvent aussi être classées selon la couche ciblée du modèle OSI comme suit (Djallel Eddine, 2013) :

5.2.1. Attaques au niveau de la couche physique

La couche physique est connue comme étant chargée des fréquences, des modulations ainsi que du cryptage des données. Deux attaques principales peuvent cibler cette couche : l'attaque de brouillage *Jamming* qui a pour but principal de consommer l'énergie des

capteurs et l'attaque d'altération *Tampering* qui cherche à nuire aux capteurs en altérant leurs circuits électroniques et extraire les clés cryptographiques.

5.2.2. Attaques au niveau de la couche liaison

La couche liaison est connue comme étant la couche responsable de la détection des trames de données, du contrôle des erreurs et de l'accès au support. La collision, l'épuisement (exhaustion)ainsi que l'allocation abusive (unfairness) sont les principales attaques ciblant cette couche. Ces attaques ont pour objectifs l'épuisement des ressources, l'allocation abusive du canal de transmission ainsi que la retransmission des données en provoquant des collisions.

5.2.3. Attaques au niveau de la couche réseau

La couche réseau est connue comme étant la couche chargée de l'attribution des adresses et de la transmission des paquets à travers le réseau. Ces deux rôles importants font de cette couche une des plus ciblées par les attaques. Certaines attaques de la couche réseau sont : l'attaque du trou noir (black hole), l'usurpation des accusés de réception (acknowledgment spoofing), l'attaque par capture de nœuds (node capture), l'attaque Sybil, etc.

5.2.4. Attaques au niveau de la couche transport

La couche transport est chargée de gérer la connectivité de bout-en-bout entre les nœuds capteurs afin d'assurer un transport fiable des paquets. Ce rôle important la rend très vulnérable aux attaques. Certaines attaques de la couche réseau sont : l'attaque d'inondation et l'attaque de désynchronisation.

5.3. Classification selon la nature

Selon la nature malicieuse des attaquants, deux catégories distinctes d'attaques peuvent être identifiées : les attaques passives et les attaques actives. Les principaux critères de chaque catégorie sont donnés dans ce qui suit (Lupu et al., 2009) :

5.3.1. Attaques passives

Les attaques passives comprennent toutes les attaques portant atteinte à la confidentialité. Dans ce type d'attaques, l'attaquant se limite à l'écoute du trafic et à la surveillance des paquets échangés dans le réseau et à l'espionnage sans apporter de modifications ni chercher à perturber le réseau. De telles attaques cherchent principalement à extraire les informations sensibles, d'analyser le fonctionnement du réseau en cherchant les nœuds les plus importants ainsi que de connaitre les mécanismes de sécurité mis en place. Ces

données analysées vont permettre à l'attaquant d'agir d'une manière ciblée et plus intelligente dans ses actions futures. Les attaques passives sont facilement réalisables tout en étant difficilement détectables, ce qui les rend très dangereuses et font d'elles une menace certaine pour les applications critiques nécessitant un besoin important en confidentialité.

5.3.2. Attaques actives

Contrairement aux attaques passives, dans les attaques actives, l'attaquant tente d'altérer les informations de routage qui transitent. Il peut ainsi détruire, modifier et obtenir des paquets, il peut aussi injecter des paquets frauduleux dans le réseau ou rejouer certains messages afin de nuire à ce dernier ou provoquer un déni de service. Portant atteinte à l'intégrité, l'authenticité et la disponibilité des informations, ces attaques obligent l'attaquant à avoir beaucoup plus de moyens et de techniques. Les attaques actives sont plus difficiles à réaliser et plus coûteuses que les attaques passives. Cependant, les dommages occasionnés au réseau sont généralement plus importants et irrémédiables.

5.4. Classification selon l'origine

Selon la localisation de l'attaquant par rapport au réseau, deux catégories distinctes d'attaques peuvent être identifiées : les attaques externes et les attaques internes. Ces attaques sont présentées dans ce qui suit (Ahmed et al., 2012) :

5.4.1. Attaques externes

Les attaques externes sont réalisées par des attaquants ne faisant pas partie du réseau. Puisque l'attaquant ne dispose pas d'informations internes sur le réseau, il va se contenter de déclencher des attaques passives telles que le *jamming* et l'attaque par rejeu. L'impact de la plupart des attaques externes est souvent limité au déni de service.

5.4.2. Attaques internes

En capturant un nœud légitime du réseau, l'attaquant obtient toutes ses données cryptographiques. Ces clés valides vont lui permettre de s'authentifier et d'interagir dans le réseau comme n'importe quel autre nœud légitime. Une définition plus détaillée est donnée dans la section suivante.

Ces différentes classifications montrent d'une part la grande considération des chercheurs pour le domaine de la sécurité et d'autre part prouvent que ces attaques sont bien réelles, sont

dangereuses et présentent une menace certaine pour n'importe quel RCSF. Dans ce qui suit, l'accent est principalement mis sur les attaques internes l'objet principal de cette thèse.

6. ATTAQUES INTERNES DANS LES RÉSEAUX DE CAPTEURS SANS FIL

Les attaques internes sont connues comme étant nettement plus insidieuses et plus dangereuses que les attaques externes. En effet, dans ce type d'attaques, l'attaquant va capturer un nœud légitime du réseau, extraire ses informations cryptographiques et ainsi pouvoir émettre de manière authentifiée des messages erronés dans le but de nuire au réseau. Capturer un nœud du réseau est ce qu'on appelle le "node compromise attack" qui est une des attaques les plus préjudiciables à un réseau de capteurs (Haddad, 2011). Cette attaque est connue comme étant le point d'entrée de toutes les attaques internes, en contrôlant le nœud capturé, l'attaquant va pouvoir effectuer bon nombre d'actions malicieuses telles que la révocation de nœuds légitimes, la corruption des données du réseau, l'injection de données erronées, etc.

6.1. Caractéristiques des nœuds compromis

Un nœud légitime du réseau capturé par un attaquant devient un nœud compromis. Les nœuds compromis ont souvent les caractéristiques suivantes (Ahmed, 2014; Ahmed et al., 2012; Shi et al., 2004) :

- Le nœud compromis est généralement reprogrammé par l'attaquant en lui injectant un code malicieux. Ainsi, le nœud compromis cherche à voler des informations à partir du réseau de capteurs ou perturber le fonctionnement normal du réseau.
- Le nœud compromis utilise la même fréquence radio que les autres nœuds légitimes du réseau afin de passer inaperçu.
- Le nœud compromis utilise l'identifiant et les clés secrètes du nœud légitime, il peut ainsi parfaitement s'authentifier lors des échanges avec les nœuds légitimes du réseau.

Compte tenu de leurs multiples caractéristiques, les attaquants internes peuvent donc passer totalement inaperçus outrepassant les méthodes cryptographiques. De ce fait, l'utilisation de protocoles de détection complémentaires efficaces reste donc l'unique moyen pour réussir là où les méthodes cryptographiques ont échoué.

6.2. Présentation des attaques internes

Connaitre les attaques internes pour mieux s'en protéger est sans doute la première étape pour la conception d'un protocole de sécurité. Nous allons présenter dans ce qui suit les différentes attaques internes selon la classification faite par (Yu et al., 2012) :

a. Usurpation, modification et retransmission des données "Spoofed, altered, or replayed routing information"

Ce type d'attaque est connu pour sa capacité à déstabiliser le protocole de routage en ciblant les informations de routage échangées entre les capteurs. L'attaquant peut répéter, retarder ou altérer le contenu des paquets en transit dans le but de nuire au réseau. Ces attaques provoquent notamment l'empoisonnement des tables de routage en engendrant la congestion et le débordement de ces dernières, en forçant la création de boucles, en générant des chemins de routage très couteux et en augmentant la latence de distribution des données.

b. Retransmission sélective "selective forwarding"

Dans ce type d'attaque, l'intrus utilise la fonctionnalité "multi-sauts" des réseaux de capteurs afin de participer dans le processus de routage. En se positionnant dans le chemin de routage ciblé, l'attaquant va soit refuser de transmettre certains messages d'un capteur donné "transmission sélective de messages", ou bien, l'attaquant va refuser de transmettre les messagesde certains capteurs choisis selon certains critères "transmission sélective de capteurs".

c. Attaque du trou noir "blackhole"

Dans cette attaque, le nœud compromis va manipuler les tables de routage en se montrant le plus attrayant possible dans le but d'attirer un maximum de flux de données. Comme un trou noir dans l'espace, l'attaquant va ensuite absorber tous les messages reçus sans jamais les transmettre aux autres capteurs. Les dégâts engendrés par cette attaque vont différés d'intensité selon le positionnement de l'attaquant dans le réseau.

d. Attaque du trou gris "grey hole"

Cette attaque est une variante améliorée et plus intelligente de l'attaque précédente. En effet, en relayant certaines informations sur le routage et en ignorant la transmission des messages importants, cette attaque rend sa détection plus difficile.

e. Attaque du trou de ver "Wormhole"

Dans cette attaque, deux ou plusieurs attaquants utilisent des tunnels de faible latence afin de faire transiter les messages d'un endroit à un autre du réseau. En permettant de fausses communications à un saut, ce type d'attaques a pour but de tromper les nœuds sur les distances en influençant les tables de routages. Ainsi, les nœuds induits en erreurs vont faire transiter leur flux de données à travers ces canaux, permettant aux attaquants de récupérer les informations.

f. Attaque du trou de base "sinkhole"

Dans cette attaque, l'intrus va se positionner sur la route du trafic amenant à la station de base. Grâce à l'utilisation d'une connexion puissante, l'attaquant va forcer le passage des données par lui-même. Les données reçues ne sont bien évidemment jamais retransmises.

g. Attaque des identités multiples "sybil"

Dans cette attaque, l'intrus peut prendre illégitimement plusieurs identifiants à la fois, lui permettant ainsi d'être présent dans plusieurs parties du réseau simultanément. Profitant de ces multiples identités, l'attaquant aura un avantage certain sur les mécanismes de sécurité utilisant le principe de vote. La présence de ce type d'attaque va déstabiliser le fonctionnement du réseau, dégrader l'intégrité des données et épuiser les ressources des capteurs.

h. Attaque par réplication "Clone attack"

Cette attaque est une des attaques internes les plus insidieuses. En capturant un nœud légitime, l'attaquant va extraire son identifiant et ses informations cryptographiques. Ces informations seront ensuite injectées dans plusieurs capteurs malicieux nommés "clones". Ceux-ci disposant du même identifiant légitime et de clés reconnues vont participer dans le fonctionnement du réseau. En passant inaperçues, ces répliques vont tenter de causer un maximum de préjudices.

i. Usurpation d'accusé de réception "acknowledgment spoofing"

Dans cette attaque, un nœud malicieux va intercepter les accusés de réception de ces nœuds voisins, les modifier et les envoyer à leurs destinataires. Cette attaque permet à l'adversaire de diffuser des informations erronées sur l'état des nœuds.

j. Attaque furtive "stealthy attack"

Dans ce type d'attaque, l'intrus injecte dans le réseau juste assez de valeurs erronées à intervalles de temps espacés afin d'éviter la détection. Les attaquants furtifs suivent étroitement le comportement normal du système et se déplacent patiemment sans causer de changements majeurs dans le réseau afin de passer inaperçus. La surveillance de telles attaques est un réel défi dans les réseaux qui évoluent en termes de taille et de vitesse.

k. Attaque de recommandations malhonnêtes négatives "Bad mouthing"

Certains mécanismes de confiance et de réputation font appel à la notion de témoins dans le calcul des valeurs de réputation. Un nœud malicieux peut s'introduire parmi ces témoins et attribuer des valeurs de réputation négatives à un nœud légitime afin de réduire sa réputation, fausser les informations et ainsi nuire au réseau.

l. Attaque de recommandations malhonnêtes positives "Ballot-stuffing"

Lors de cette attaque le nœud malicieux s'introduit parmi les témoins et attribue des valeurs de réputation positives à un autre nœud malicieux. Le but principal derrière cette attaque est de favoriser les nœuds attaquants en augmentant leurs valeurs de réputation afin d'accroitre leur poids dans le réseau.

m. Attaque On-Off

Dans ce type d'attaque, le nœud malicieux va procéder selon deux phases, une phase *on* et une phase *off*. Lors de la phase "off", l'attaquant va se comporter de manière correcte afin d'augmenter sa valeur de réputation et de gagner la confiance de son entourage. Lors de la phase "on", l'attaquant va agir négativement dans le réseau, profitant de sa valeur de réputation élevée qui va lui permettre de rester indétectable pour un moment.

n. Attaque de blanchiment "whitewashing"

Les systèmes de réputation sont connus pour être particulièrement vulnérables aux attaques de blanchiment. Dans cette attaque, un nœud malicieux dont la valeur de réputation a beaucoup diminué a la possibilité de ré-entrer dans le réseau avec une nouvelle identité et une fraiche réputation.

o. Attaque de comportement conflictuel "conflicting behavior"

Dans cette attaque, le nœud malicieux se comporte de manière différente avec les nœuds du réseau. Il va ainsi avoir un bon comportement avec quelques nœuds, ce qui lui vaudra des valeurs de réputation positives. Par contre il va se comporter de manière préjudiciable avec les

autres nœuds qui vont donc le juger négativement. Le comportement conflictuel va se produire lorsque les nœuds du premier groupe vont échanger sur la réputation de ce nœud malicieux avec les autres nœuds. Le fait de posséder des valeurs de réputation différentes va porter atteinte sur la confiance des nœuds du premier groupe par rapport à ceux du second et inversement.

p. Attaque de comportement intelligent "intelligent behavior"

Dans cette attaque, le nœud malicieux se montre extrêmement intelligent. Il va en effet adapter son comportement en fonction de sa valeur de réputation. De ce fait, il va se comporter différemment à chaque période de temps en fournissant sélectivement des services bons ou mauvais ou en attribuant des valeurs de recommandations faibles ou élevées en fonction du seuil de confiance.

7. MÉCANISMES DE SÉCURITÉ

L'élaboration d'un protocole de sécurité efficace dans les RCSFs est un réel challenge. Entre les ressources limitées des capteurs, l'environnement hostile et le nombre important d'attaques internes, il faut souvent faire un compromis entre efficacité et surcoût. Ce besoin de sécurité a cependant permis l'élaboration de plusieurs protocoles de contre-mesure. Ces protocoles découlent de plusieurs axes de recherche allant des plus classiques aux plus innovants. Nous allons nous intéresser dans ce qui suit aux principaux mécanismes de sécurité déjà utilisés dans les RCSFs ainsi qu'aux axes de recherche prometteurs, en citant leurs principaux avantages et inconvénients.

7.1. Cryptographie

Au croisement des mathématiques, de l'informatique, et parfois même de la physique, le chiffrement est une discipline à part entière. En effet, cette méthode est souvent requise pour des applications sensibles nécessitant la protection de leurs échanges. La cryptographie permet d'assurer l'authentification, la confidentialité, l'intégrité et la non-répudiation des informations dans les réseaux de capteurs. Dans la cryptographie, il existe deux types de chiffrements : le chiffrement symétrique et le chiffrement asymétrique et plusieurs primitives telles que : les fonctions de hachage et les signatures numériques. Une brève description de ces méthodes est donnée dans ce qui suit :

- Dans *le chiffrement symétrique* dit à clé secrète, les deux nœuds impliqués dans la communication vont partager une même clé secrète leur permettant d'effectuer le

chiffrement et le déchiffrement des messages. Les algorithmes symétriques les plus utilisés sont AES et RC5.

- *Le chiffrement asymétrique* dit à clé publique, une paire de clés (clé publique et clé privée) est utilisée dans la communication. Chaque nœud fait appel à sa clé publique pour chiffrer les données qui ne sont déchiffrées par la suite que par la clé privée correspondante. Les algorithmes les plus connus sont : RSA, l'algorithme Diffie-Hellman et la technique des courbes elliptiques (ECC).
- *Les fonctions de hachage* constituent une base largement utilisée lors de l'élaboration de schémas cryptographiques. Ces fonctions à sens unique, rendent possible l'obtention d'une empreinte à partir d'une donnée de taille fixe. Une telle empreinte appelée "haché" sera expédiée avec le message afin de s'assurer de son intégrité. Parmi les fonctions de hachage cryptographiques : les fonctions SHA.
- *Les signatures numériques* utilisent à la fois la cryptographie asymétrique et les fonctions de hachage. Ces signatures représentent des données ajoutées au message. Elles permettent d'assurer l'authentification des émetteurs, garantir l'intégrité ainsi que la non réutilisabilité des données.

Bien que le chiffrement symétrique est connu comme étant peu gourmand en ressources mémoire, temps et puissance de calcul, son efficacité est entravée par le problème de transmission de la clé. Le chiffrement asymétrique a quant à lui un avantage considérable en termes de gestion de clés. Cependant, ses besoins considérables en ressources et en énergie rendent son utilisation difficile dans les réseaux de capteurs. Une solution potentielle est d'utiliser un nouveau concept : les ***crypto systèmes hybrides***, qui font appel aux avantages des deux principes, alliant à la fois l'efficacité de la gestion des clés de la cryptographie asymétrique et les performances en termes de mémoire et de vitesse de la cryptographie symétrique.

Bien que largement utilisées dans les RCSFs, l'efficacité des méthodes cryptographiques est anéantie face aux attaques internes. En capturant un nœud du réseau, l'attaquant va pouvoir obtenir toutes ses informations secrètes et ainsi mettre en péril la sécurisation des échanges. Des méthodes complémentaires doivent être utilisées en parallèle avec la cryptographie afin d'assurer la sécurité du réseau.

7.2.Systèmes de détection d'intrusion (IDS)

Contrairement à la cryptographie, les IDS ne se contentent pas de protéger les données mais apportent une ligne de défense supplémentaire celle de la détection des attaques. En effet, en permettant la détection de comportements suspects, les agents IDS vont pouvoir détecter l'attaque et déclencher une alarme afin d'informer le contrôleur (Sedjelmaci, 2012). Il existe deux principales politiques de détection des intrusions dans les réseaux de capteurs : la détection à base de règles et la détection à base d'anomalies.

- Dans ***la détection à base de règles*** le comportement d'un nœud est analysé en fonction d'un ensemble de signatures d'attaques intégrées. Permettant une grande précision de détection lorsque les attaques sont connues, cette méthode par contre s'avère inefficace pour la détection de nouvelles attaques. Une mise à jour continue de la base de données d'intrusions est donc nécessaire au détriment des ressources en mémoire des capteurs.
- Dans ***la détection à base d'anomalies*** le comportement d'un nœud est modélisé et chaque déviation de ce comportement jugé "normal" est considérée comme "anomalie". Permettant une grande efficacité de détection des nouvelles attaques, cette méthode génère cependant beaucoup de fausses alarmes positives et négatives ainsi qu'un coût élevé de calcul.

Deux principales approches de prise de décision sont utilisées habituellement dans les IDS (Djallel Eddine, 2013) :

- ***Approche indépendante.*** Dans cette approche, certains nœuds sont responsables de recueillir les informations, analyser les comportements et agir en fonction des événements observés. En se basant sur des nœuds bien déterminés, cette approche est vulnérable aux attaquants et risque d'épuiser rapidement les ressources des nœuds sélectionnés.
- ***Approche coopérative.*** Dans cette approche, chaque nœud va participer dans le processus de détection et de prise de décision. Un mécanisme de coopération est initié entre nœuds voisins lors de la prise de décision. La compromission d'un des nœuds de la coopération est à ne pas négliger afin de ne pas fausser les résultats de la prise de décision.

Les IDS figurent parmi les mécanismes de détection des attaques internes dans les RCSFs les plus utilisés. Les différentes politiques de détection, les différentes approches de prise de

décision ainsi que les différentes possibilités d'emplacement des agents IDS dans le réseau de capteurs (i.e. emplacement de l'agent dans le cluster head, dans les membres du cluster ou bien dans les frontières du cluster) ont permis et permettent encore l'élaboration de plusieurs approches de détection. Cependant, choisir les bonnes associations entre ces trois critères reste un défi majeur afin de garantir l'efficacité du protocole de détection tout en diminuant ses inconvénients.

7.3. Théorie des jeux

Considérée comme un outil traitant des situations de prise de décision impliquant plusieurs entités, la théorie des jeux permet de décrire et d'analyser de nombreux systèmes sous la forme de jeux stratégiques. Il existe plusieurs types de jeux. Une brève définition des jeux les plus importants est donnée dans ce qui suit (Dominicy, 2012) :

- Dans les *Jeux simultanés* souvent appelés "synchrones", les joueurs agissent sans connaître les décisions prises par les autres joueurs ou bien ils prennent leurs décisions en même temps. Le jeu de "pierre, papier, ciseaux" est un exemple de jeu simultané.
- Dans les *Jeux séquentiels* souvent appelés "asynchrones", les joueurs jouent de manière séquentielle les uns après les autres. Chaque joueur dispose à chaque fois d'informations concernant les actions des adversaires et l'historique du jeu au moment de formuler son choix. Le jeu d'échecs est un exemple de jeu séquentiel.
- Dans les *Jeux à somme nulle,* la somme algébrique des gains des joueurs est nulle. En effet, toutes les stratégies des joueurs sont Pareto-optimales ne pouvant ni augmenter ni diminuer les gains disponibles. Le poker est un exemple de jeu à somme nulle.
- Dans les *Jeux à somme non nulle,* contrairement à leurs précédents, la somme des gains devient non nulle étant donné que certaines issues du jeu sont globalement plus profitables pour tous les joueurs ou bien plus dommageables pour tous. Le dilemme du prisonnier est un exemple de ce type de jeux.
- Dans les *Jeux à information complète*, le joueur dispose de plusieurs informations lors de la prise de décision, telles que : ses possibilités d'action et les possibilités des autres joueurs, les gains de ses actions ainsi que les motivations des autres joueurs. Si une des conditions n'est pas vérifiée, il s'agira de jeux à informations incomplètes.
- Les *jeux à information parfaite,* permettent à chaque joueur de connaître à tout moment les actions effectuées avant la prise de décision.

- Dans les *Jeux coopératifs*, les joueurs s'unissent dans le but d'obtenir le meilleur résultat possible pour chaque membre de la coalition contrairement aux *jeux de compétition (non coopératifs).*
- Dans les *Jeux répétés,* la répétition du jeu permet aux joueurs de profiter deleurs connaissances préalables des résultats intermédiaires afin d'améliorer leurs stratégies de jeu.

Les différents types de jeux existants ainsi que leurs nombreuses perspectives d'utilisation ont permis à la théorie des jeux d'être appliquée avec succès dans les réseaux de capteurs, particulièrement dans le domaine de la conception (Shi et al., 2012). L'utilisation de cette théorie dans le domaine de la sécurité tente surtout de déterminer la nature des conflits. En effet, le modèle théorique du jeu va essayer de déterminer mathématiquement le comportement des nœuds dans des situations où les décisions dépendent du comportement des autres nœuds (Rathore, 2016).

Plusieurs modèles de jeux ont été appliqués efficacement dans le domaine de la sécurité tels que : les jeux coopératifs dans la prévention des attaques de déni de service (Agah et al., 2004) et les jeux non-coopératifs dans les IDS (Reddy, 2009).

L'utilisation cependant de la théorie du jeu dans les réseaux de capteurs est connue pour sa complexité de calcul et sa difficulté de mise en œuvre. De plus, le pourcentage de détection est compris entre 30 et 60% (Rathore, 2016 ; Shen, et al., 2011).

7.4.Réseaux de neurones artificiels (RNA)

En imitant le fonctionnement des neurones biologiques, les réseaux de neurones artificiels permettent d'extraire des informations importantes à partir de données imprécises. Un réseaux de neurones artificiels (RNA) est généralement constitué d'un ensemble d'unités, chacune disposant d'une petite mémoire. Des canaux de communication relient ces unités leur permettant ainsi de communiquer. Deux étapes principales entrent dans le fonctionnement de ces réseaux : Les algorithmes d'apprentissage et la généralisation. Les algorithmes d'apprentissage permettent d'apprendre automatiquement la structure de données à partir des données représentatives collectées. La généralisation quant à elle, est cette capacité de prédire avec précision des données ne faisant pas partie des données d'apprentissage. Les architectures courantes des réseaux de neurones sont :

- *Les réseaux feedforward (non bouclés).* Dans ce type de réseaux, les neurones sont organisés en couches successives et ne sont connectés que dans un seul sens. En effet, la couche d'entrée va uniquement servir à introduire les valeurs des variables d'entrée,

les neurones des autres couches par contre sont connectés à toutes les unités des couches précédentes.

- *Les réseaux récurrents.* Dans ce type de réseau, les informations peuvent circuler dans les deux sens grâce aux interconnections des neurones qui interagissent de manière non linéaire. La présence d'au moins une boucle de rétroaction permet de conserver les données en mémoire. Ce fonctionnement ressemble plus au vrai fonctionnement du système nerveux.

Compte tenu des nombreuses applications des réseaux de neurones artificiels ainsi que leurs avantageuses caractéristiques, ces réseaux peuvent apporter un réel avantage pour les réseaux de capteurs. Les RNA ont été utilisés avec succès dans le domaine de la sécurité tel que : la détection de l'attaque par déni de service dans (Alfantookh, 2006). Plusieurs perspectives des RNA restent encore à explorer dans le domaine de la sécurité. Faire appel par exemple au pouvoir de classification des RNA afin d'analyser le comportement des nœuds et les juger en normaux/anormaux constitue un bon outil de détection de potentiels attaquants.

L'application des RNA dans les RCSFs doit cependant tenir compte de quelques inconvénients. D'une part, leur complexité de raisonnement et de fonctionnement rend leur implémentation une tâche compliquée. D'autre part, leur complexité en termes de stockage et d'énergie est importante. En effet, le coût de stockage d'un réseau de neurones dans un RCSF est de O(RT)/cycle où : R est le nombre total de neurones et T est le nombre maximale de changement d'activations (Rathore, 2016).Le coût d'énergie est aussi conséquent, il peut être cependant diminué grâce à l'utilisation de l'architecture feedforward au lieu de l'architecture récurrente. L'architecture feedforward est plus recommandée pour les RCSFs, étant donné qu'elle a un comportement stable, une grande tolérance aux fautes, plus efficace pour faire face aux problématiques concrètes et consomme moins d'énergie que l'architecture récurrente qui demande beaucoup d'échange d'informations.

7.5.Machines à vecteur de support (SVM)

Faisant partie des techniques d'apprentissage supervisé, les séparateurs à vaste marge (SVM) sont de nouvelles alternatives à la classification binaire. Leur nature, leur permet aussi de résoudre des problèmes de régression. Reposant sur la notion d'hyperlan, les SVM tentent de séparer les données en deux classes positive et négative, en garantissant que la marge entre les données d'apprentissage et l'hyperlan soit maximale. L'hyperlan représente la solution optimale et les données d'apprentissage représentent les vecteurs de support. Dans le cas où

l'échantillon d'apprentissage est linéairement séparable, cette classification se fait de manière naturelle. Dans le cas contraire, on parle de séparation non linéaire, dont la résolution nécessite l'utilisation des fonctions noyaux (kernel). Il existe deux classes principales de SVM: les SVM binaires et les SVM multi-classes (Djeffal, 2012).

- ***SVM binaires*** permettent une classification des données d'apprentissage en uniquement deux classes : positive (+1) et négative (-1).
- ***SVM multi-classes*** ont été proposées afin de répondre aux problèmes du monde réel qui nécessitent bien souvent plusieurs classes. Dans ce type de SVM, la décision n'est plus binaire d'où la nécessité d'avoir plusieurs hyperlans "bi-classes". La classe d'un nouvel exemple est déterminée en parcourant la hiérarchie des hyperplans binaires.

Reposant sur une théorie mathématique solide et permettant une classification rapide, les machines à vecteur de support constituent un outil efficace pour lutter contre les attaques internes. Leur puissance de classification peut être utilisée pour distinguer entre les comportements normaux et anormaux des nœuds capteurs. Cependant, l'utilisation des SVM dans les réseaux de capteurs doit tenir compte de quelques contraintes. D'une part, l'implémentation des SVM nécessite l'utilisation de bases de données adaptées, l'absence actuellement de base de données dédiée aux attaques internes est un frein à l'utilisation des SVM. D'un autre côté, la grande quantité d'exemples en entrée implique un calcul matriciel important (Selmic et al., 2016) influant ainsi négativement sur les ressources limitées des capteurs.

7.6. Systèmes multi agents (SMA)

Les systèmes multi agents sont constitués d'un ensemble d'agents évoluant dans un environnement commun, les interactions entre ces agents produisent un comportement global engendrant une intelligence collective. Il existe deux principaux types de systèmes multi agents : les SMA ouverts et les SMA auto-organisés (Jamont et al., 2006) :

- Dans les ***Systèmes multi agents ouverts,*** le caractère ouvert résulte du fait que les agents n'ont pas la possibilité d'avoir une vision globale sur l'environnement. Le système doit être dans ce cas-là modulaire et extensible afin de permettre la décomposition du système en plusieurs sous-systèmes, de rendre possible la mise en relation de ces sous-systèmes et de supporter le retrait et l'ajout de nouveaux éléments.

- Dans les ***Systèmes multi agents auto-organisés,*** le mot d'ordre est "l'adaptation", ce qui veut dire que le système doit être capable de rester cohérent et stable quel que soit les évènements qui s'y produisent. De tels systèmes doivent pouvoir détecter les agents instables et remplacer les agents défaillants afin d'assurer la persistance de la structure.

Depuis quelques années, il existe de plus en plus de propositions associant les réseaux de capteurs aux systèmes multi agents. En effet, les SMA ont été appliqués dans plusieurs domaines dans le contexte des réseaux de capteurs tels que : la description de services, le routage et la fusion de données. Plusieurs caractéristiques de ces deux domaines de recherche ont rendu possible cette union :

- Le côté distribué et ouvert des réseaux de capteurs rend l'approche multi agents particulièrement adaptée.
- Les SMA permettent d'apporter une vue externe sur les interactions et sur l'organisation du réseau.
- La mise en place d'un SMA au sein du réseau va permettre de relayer les informations importantes depuis ces agents vers la station de base. Étant donné que les transmissions multi-sauts sont gourmandes en ressources mémoires surtout dans les réseaux à grande échelle, déléguer les nœuds capteurs de ces transmissions importantes permet un gain de temps et d'énergie considérable.

L'utilisation des systèmes multi agents dans le domaine de la sécurité est une bonne perspective. L'autonomie, l'intelligence et la mobilité qu'offrent les agents, sont quelques-unes des caractéristiques pouvant bénéficier à l'élaboration d'un protocole de sécurité efficace. Cependant, l'élaboration de tels protocoles doit permettre de garantir la sécurité des agents en plus de la sécurité des nœuds capteurs, ce qui est doublement contraignant. Car dans le cas où quelques agents sont compromis, c'est tout le réseau de capteur qui est mis en danger.

7.7. Mécanismes de confiance et de réputation

Dédiés au domaine de la sécurité, les mécanismes de confiance et de réputation sont une solution innovante pour les réseaux de capteurs. Tandis que plusieurs méthodes s'intéressent uniquement au côté préventif afin d'empêcher toute attaque, les mécanismes de confiance et de réputation rendent possible la détection de ces attaques. Cette détection se fait suivant plusieurs étapes : la collecte d'informations, le calcul des valeurs de confiance, la sélection des entités légitimes et des transactions fiables ainsi que l'isolement des nœuds compromis.

Cependant, les performances des mécanismes de confiance et de réputation peuvent facilement être altérées par des attaquants usurpant le mécanisme afin de nuire au réseau. Parmi ces attaques, nous avons : les attaques de recommandations malhonnêtes (bad mouthing, ballot stuffing et l'attaque par collusion), l'attaque On-Off, l'attaque de blanchiment (whitewashing), l'attaque de comportement intelligent "intelligent behavior" et l'attaque de comportement conflictuel "conflicting behavior" (pour les définitions de ces attaques se référer à la section 6.2). L'élaboration d'un protocole de détection efficace doit tenir compte de ces potentielles attaques afin d'accomplir parfaitement son rôle.

Plus de détails sur les notions de confiances et de réputation ainsi que sur les méthodologies de calcul de la confiance et d'obtention des valeurs de réputation sont donnés dans le chapitre III.

7.8. Métaheuristiques

Plusieurs problèmes de la vie courante sont des problèmes d'optimisation pour lesquels des solutions alliant à la fois qualité et efficacité doivent être trouvées. Les métaheuristiques proposent des solutions optimales pour une grande variété de problèmes d'optimisation. Elles permettent de trouver une approximation de la meilleure solution en tentant d’apprendre les caractéristiques du problème. En réduisant la taille effective de l'espace de recherche et en explorant cet espace de manière efficace, ces algorithmes permettent la résolution d'une large gamme de problèmes de différentes complexités et même les problèmes jugés difficiles (NP-difficiles) (Talbi, 2009).

La plupart des métaheuristiques s'inspirent des comportements naturels, nous pouvons citer à titre d'exemple : les algorithmes génétiques qui sont les plus connus des algorithmes évolutionnaires s'inspirant de la théorie de l'évolution darwinienne, le recuit simulé qui s'inspire du recuit physique utilisé en métallurgie, l'algorithme de colonies d'abeilles, l'algorithme de colonies de fournis et l'algorithme du banc de poissons qui sont des algorithmes basés sur l'intelligence par essaim s'inspirant du comportement collectif de certaines espèces.

Il existe deux types de métaheuristiques : les métaheuristiques à solution unique et les métaheuristiques à base de population de solutions.

- Dans ***les métaheuristiques à solution unique*** le principe de base est l'exploitation de l'espace de recherche. Dans ces méthodes, des mécanismes sont utilisés afin d'empêcher le processus de recherche de tomber dans des optimaux locaux en

apportant des modifications à la solution initiale en fonction de son voisinage. Ces modifications vont permettre d'améliorer, au fur et à mesure des itérations, la qualité de cette solution. Une grande variété de méta-heuristiques à solution unique ont été proposées dans la littérature, parmi ces dernières : le recuit simulé, la recherche à voisinage variable VNS, la recherche locale itérée ILS, la recherche tabou, la recherche gloutonne aléatoire adaptative GRASP et leurs variantes.

- Dans ***les métaheuristiques à base de population de solutions*** le principe de base est l'exploration afin de renforcer la diversité de l'espace de recherche. Dans ces méthodes, la recherche débute avec un ensemble de solutions. Ces solutions seront évaluées afin de déduire la solution optimale au problème traité. L'utilisation de la recherche globale empêche le processus de recherche de converger vers l'optimum global ce qui permet d'augmenter la qualité des solutions. De nombreuses méta-heuristiques à base de population de solution ont été proposées dans la littérature, parmi lesquelles : la grande famille des algorithmes évolutionnaires et les très en vogue algorithmes d'intelligence par essaim.

Depuis quelques années, nous assistons à une ascension d'utilisation des métaheuristiques dans les réseaux de capteurs que ce soit dans le domaine du routage, l'agrégation, le clustering, l'optimisation de l'énergie ainsi que dans l'optimisation du déploiement des capteurs mais très peu dans le domaine de la sécurité. Les nombreuses caractéristiques de ces algorithmes intelligents en termes de : résolution rapide des problèmes, robustesse, souplesse, simplicité de conception, facilité de mise en œuvre et puissance de calcul limitée peuvent constituer des atouts majeurs pour les protocoles de sécurité.

7.9. Blockchain

Technologie innovante de ces dix dernières années, la blockchain est considérée comme une découverte historique suscitant l'intérêt des parties prenantes dans un large éventail d'industries. En effet, la mise en place d'une blockchain permet aux applications qui ne fonctionnaient auparavant que grâce à un intermédiaire de confiance, de fonctionner de manière autonome et décentralisée sans faire appel à une autorité centrale avec le même degré de certitude. Ce qui était impossible jusqu'alors. Constituée d'une chaine de blocs, la blockchain est une base de données distribuée contenant l'historique des paiements, des transactions et des contrats exécutés et partagés entre les entités participantes. Répliquée et partagée entre les membres d'un réseau, la blockchain est souvent associée à Bitcoin (monnaie

alternative apparue en 2008 (Nakamoto, 2008). Cependant une blockchain peut se suffire à elle-même et fonctionner sans utiliser de crypto-monnaies. Quatre critères intéressants distinguent la blockchain :

7.9.1. Architecture décentralisée

Le coté décentralisé de la blockchain agit comme une défense structurelle face aux risques de modifications volontaires ou de vol de données de la part des entités malicieuses. En effet, le fait que la blockchain ne soit pas enregistrée par un seul serveur mais par une partie des entités, rend la destruction, l'altération et la modification des données chose impossible.

7.9.2. Protection cryptographique

Plusieurs procédés cryptographiques entrent dans la sécurisation de la blockchain :

- *Chiffrement :* Les échanges dans la blockchain sont sécurisés grâce à l'utilisation des courbes elliptiques. L'application du chiffrement va ainsi permettre de garantir la confidentialité, l'intégrité, l'authentification et la non-répudiation dans le réseau des données.
- *Hashs :* La blockchain est constituée d'un ensemble de blocs où sont enregistrées les transactions de manière ordonnée et horodatée. Chaque bloc est constitué de deux parties : un en-tête et une partie consacrée à l'enregistrement des transactions. Dans le but de garantir l'intégrité des blocs et de s'assurer qu'une fois un bloc validé il ne pourra jamais être modifié, la blockchain fait appel aux fonctions de hachage. De ce fait, des fonctions telles que le *SHA-256*qui est actuellement utilisée dans le bitcoin et l'ether sont appliquées. Ces fonctions de hachage vont permettre de calculer le "hash" d'un bloc et d'insérer cette valeur dans l'en-tête du bloc qui le suit, dans le but de créer des liens entre les blocs. La moindre modification des données dans un bloc aura pour conséquence le changement de la valeur du hash qui deviendra ainsi totalement différente de la valeur de l'en-tête enregistrée. La figure II.1 montre le fonctionnement de la fonction de hachage SHA-256. Nous pouvons remarquer que l'ajout d'un seul caractère à donner un résultat complètement différent (un point d'exclamation dans notre cas).

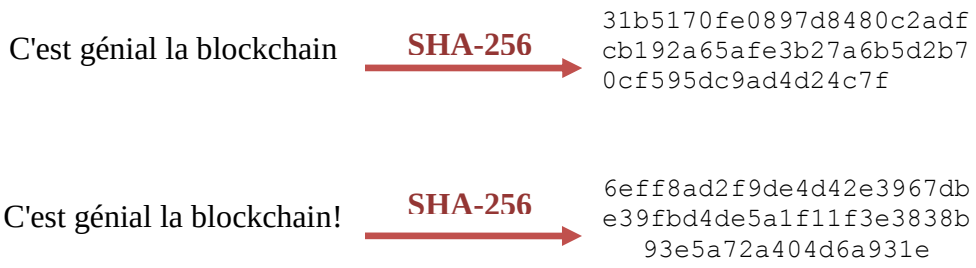


Fig 2. 1. La fonction de hachage SHA-256 dans la blockchain

7.9.3. Émission de crypto-monnaie

Souvent confondus par inadvertance, les crypto-monnaies sont pourtant différentes de la blockchain mais les deux notions restent toutefois étroitement liées. Servant de plateforme, la blockchain permet d'enregistrer les différentes transactions d'échange de ces crypto-monnaies. Depuis la création de la blockchain, plusieurs crypto-monnaies ont vu le jour, parmi ces dernières :

- ***Bitcoin :*** La publication en 2008 de l'article intitulé : « Bitcoin : A Peer-to-Peer Electronic Cash System » (Nakamoto, 2008) par un certain Satoshi Nakamoto a donné ainsi naissance au Bitcoin. Étant la première application de la blochchain, le Bitcoin a était créé afin de permettre de contourner les contrôles et de résoudre le problème du double paiement dans le but de faciliter les transactions en ligne. Le succès grandissant de Bitcoin fait de lui la star des crypto-monnaies.
- ***Ether :*** Créé en 2015 par l'entreprise Etherum, l'ether occupe la seconde place des crypto-monnaies les plus populaires. Reposant sur une blockchain permettant la mise en place de "contrats intelligents", l'ether concurrence directement le Bitcoin.
- ***Litecoin :*** Créée en 2011 par Charles Lee, le Litecoin avec ses coûts proches de zéro, fait partie des crypto-monnaies les plus populaires. En apportant des améliorations à la blockchain de Bitcoin et en accélérant notamment le processus de vérification et en augmentant la rapidité des transactions, le Litecoin se veut adapter aux transactions quotidiennes.
- ***Bitcoin cash :*** Crée en 2017, le Bitcoin cash est basé sur la même blockchain que le Bitcoin. Toutefois, plusieurs améliorations y ont été apportées telles que l'augmentation de la taille des blocs, l'utilisation d'une nouvelle fonction de hachage "SigHash", la rapidité des transactions et la diminution des frais.

7.9.4. Smart contract

Développés en 1994 par Nick Szabo (Szabo, 1994), les contrats intelligents ne sont devenus populaires que depuis quelques années grâce à la montée en puissance de la technologie blockchain. De tels contrats ont permis d'automatiser et de révolutionner les contrats traditionnels en les rendant infalsifiables et durables. Fonctionnant sur une blockchain Etherum, les smart contrats peuvent stocker des données, enregistrer des informations, prendre des décisions et exécuter automatiquement les conditions du contrat. Ils peuvent servir d'accord entre les entités et la blockchain sans que les deux parties se fassent mutuellement confiance (Bagchi, 2017). Outre ces fonctionnalités multiples, les contrats intelligents bénéficient également de la sécurité offerte par la blockchain.

La Blockchain est une technologie révolutionnaire pouvant être appliquée dans un large éventail d'applications et permettant la résolution d'un nombre important de problèmes. Son caractère désintermédié permet un fonctionnement plus sécurisé et autonome. Cependant, la blockchain ramène avec elle son lot de problèmes notamment des défis de mise à l'échelle, d'amorçage, de contrôle des activités frauduleuses ainsi que la difficulté d'adaptation face aux changements fréquents de comportement de la blockchain.

L'utilisation de la blockchain dans les réseaux de capteurs n'est qu'à ses débuts. Compte tenu de ses nombreux avantages, elle peut être une perspective intéressante pour l'élaboration de protocoles de sécurité efficaces.

8. CONCLUSION

L'engouement suscité par les réseaux de capteurs s'accompagne d'un besoin imminent en sécurité. Ce besoin de sécurité élevé doit cependant faire face aux nombreuses contraintes imposées par ces réseaux. La limitation en énergie des capteurs d'un côté et l'environnement hostile dans lequel sont déployés les réseaux de capteurs d'un autre, exigent l'élaboration de protocoles de sécurité simplifiés mais efficaces.

Dans ce chapitre nous avons commencé par présenter les principaux challenges et défis liés à la sécurité. Dans le but de mettre l'accent sur la problématique et de mesurer son importance. Nous avons présenté ensuite les principales attaques internes ainsi que leurs caractéristiques un moyen pour mieux les connaitre afin de mieux s'en protéger.

Plusieurs mécanismes de sécurité découlant de divers axes de recherche ont été utilisés afin de sécuriser les réseaux de capteurs contre les attaques internes. Allant des plus classiques tels que les mécanismes de cryptographie et les IDS, passant par les réseaux de neurones, les

SVM et la théorie des jeux et jusqu'à des méthodes plus innovantes telles que les métaheuristiques ou encore la très en vogue blockchain. Cependant, aucun mécanisme n'est pleinement efficace et chaque méthode pose quelques inconvénients liés à la difficulté d'implémentation, aux besoins importants en ressources aussi bien qu'aux vulnérabilités à certaines attaques. Dans cette optique, un protocole de sécurité efficace et optimal sera celui qui va combiner efficacement entre plusieurs axes afin de tirer parti des avantages et éviter les inconvénients.

Dans le chapitre suivant, nous allons nous intéresser aux attaques de recommandations malhonnêtes incluant l'attaque bad-mouthing, l'attaque ballot-stuffing et l'attaque collusion. Nous allons présenter les principaux travaux de recherche publiés sur ces attaques et évaluer leurs performances.

CHAPITRE III

Les attaques dans les mécanismes de confiance et de réputation

Sommaire

1. INTRODUCTION

Le rôle important que jouent les nœuds capteurs dans les diverses applications notamment la détection des données, le signalement des événements, le traitement des informations ainsi que le transfert des données via le routage multi-sauts jusqu'à la station de base, les transforment en cibles idéales pour de nombreux attaquants. De ce fait, les éléments et les protocoles du réseau doivent non seulement faire face aux conditions variables et aux nœuds défaillants mais en plus être préparés pour détecter les entités malveillantes.

Un mécanisme qui peut être utilisé pour améliorer la fiabilité, soutenir le processus de prise de décision et atténuer les attaques est le mécanisme de confiance et de réputation. En permettant la gestion de l'incertitude concernant les actions futures des autres participants, en évaluant et en conservant la réputation des autres membres, il devient alors possible de calculer le degré de confiance des différents membres pour l'accomplissement d'une tâche particulière (Lopez et al., 2010).

Cependant, les performances des mécanismes de confiance et de réputation peuvent facilement être altérées lors de la présence de certaines attaques telles que : les attaques de recommandations malhonnêtes, l'attaque On-Off, l'attaque de comportement conflictuel, etc. Il devient ainsi important de proposer des méthodes complémentaires pour soutenir ces mécanismes et améliorer leur résistance aux attaques.

Nous présenterons dans ce présent chapitre l'investigation de notre premier axe de recherche, à savoir unes des attaques les plus préjudiciables pour les protocoles de confiance et de réputation : les attaques de recommandations malhonnêtes. Nous commencerons par aborder les différentes méthodes de calcul de la confiance et de la réputation. Nous exposerons les besoins en sécurité de ces mécanismes. Une présentation des principales attaques touchant ces mécanismes est donnée par la suite. Nous allons nous intéresser aux attaques de recommandation malhonnêtes. Nous survolerons les travaux existants concernant ces attaques, en effectuant une analyse et une classification. Cette étude approfondie, nous permettra de tracer les motivations pour la conception dans nouveau protocole de détection des attaques de recommandation malhonnêtes.

Notre contribution dans ce chapitre est résumée en trois points :

1. Présentation des mécanismes de confiance et de réputation. Nous allons citer les différentes méthodes de calcul de la confiance ainsi que les principales méthodologies utilisées. Les enjeux liés à la sécurité seront présentés en mettant l'accent sur la

menace que représentent les attaques de recommandations malhonnêtes pour ces mécanismes.

2. Présentation d'un état de l'art sur les protocoles considérant les attaques de recommandations malhonnêtes. Bien que différents états de l'art ont été menés dans le domaine des protocoles de confiance et de réputation (Khedim et al., 2015), tels que :
    - (Esch, 2010)a discuté des différentes applications de la confiance dans un environnement de communication sans fil.
    - (Mármol et al., 2009) a proposé une analyse des principales menaces de sécurité pouvant être appliquées dans la plupart des schémas de confiance et de réputation dans diverses architectures réseau.
    - (Mármol et al., 2010)a proposé une approche de pré-normalisation pour les modèles de confiance et/ou de réputation dans les systèmes distribués.
    - (Yu et al., 2010)a cité les avantages et les inconvénients des modèles de confiance individuels et systémiques.
    - (Khalid et al., 2013) a étudié les progrès récents dans les mécanismes de confiance et de réputation tout en proposant une comparaison entre ces différents mécanismes.
    - (Kumar et al., 2012) a étudié les diverses méthodes appliquant les mécanismes de confiance et de réputation comme mesure de sécurité.
    - (Alzaid et al., 2013) a passé en revue les travaux actuels dans le domaine des mécanismes de confiance et de réputation.
    - (Lopez et al., 2010) a proposé une classification selon les pratiques jugées essentielles au développement d'un bon système de gestion de confiance.
    - (Han et al., 2014)a présenté une étude centrée sur les applications des modèles de confiance dans les RCSFs ordinaires.

Il n'existe cependant aucun état de l'art (à notre connaissance) dédié aux solutions et méthodes utilisées par les protocoles afin d'éviter ou de réduire l'influence des recommandations injustement positives (ballot-stuffing) ou bien injustement négatives (bad mouthing) dans les mécanismes de confiance et de réputation. Dans notre état de l'art, nous survolerons les protocoles traitant les attaques de recommandations malhonnêtes en mettant en évidence les méthodes utilisées tout en proposant une nouvelle taxonomie basée sur les stratégies de défense.

3. Présentation d’une étude comparative entre les solutions existantes en considérant plusieurs paramètres.

2. MÉCANISMES DE CONFIANCE ET DE RÉPUTATION

Les mécanismes de confiance et de réputation ont récemment été suggérés comme méthode de sécurité efficace pour les réseaux de capteurs. En effet, bien que ces mécanismes soient vulnérables à certain nombre d'attaques, les nombreux avantages offerts par ces mécanismes ainsi que leur efficacité pour résoudre les problèmes liés à l'incertitude ne peuvent être remis en cause.

Deux notions liées l'une à l'autre reviennent souvent si l'on veut expliquer la pertinence de la confiance pour les réseaux de capteurs : "la collaboration" et "l'incertitude". En effet, un réseau de capteur est constitué d'un ensemble de nœuds qui doivent collaborer afin de réaliser un service donné. Pour que la collaboration soit réussie, il est important que chaque nœud puisse être capable de déterminer les nœuds les plus susceptibles pour accomplir la tâche prévue. Permettre aux nœuds de connaitre à l'avance le comportement des différents nœuds, leur assure des prises de décision infaillibles. Cependant, l'environnement hostile ainsi que les ressources épuisables des capteurs d'un côté et la présence potentielle d'attaquants d'un autre coté font subir un grand degré d'incertitude à se pouvoir de prise de décision. Les mécanismes de confiance et de réputation permettent d'apporter une solution satisfaisante au problème de l'incertitude. Bien qu'il soit impossible de connaître le comportement futur des nœuds de manière précise, il est cependant possible d'en avoir un aperçu en considérant leurs valeurs de confiance et de réputation reflétant leurs actions passées. Si un nœud s'est comporté de façon satisfaisante dans le passé pour effectuer une certaine tâche, il est supposé qu'il sera fiable à l'avenir pour effectuer la même tâche. En conséquence, un nœud pourra démarrer un processus de coopération avec les nœuds les plus fiables.

La plupart des protocoles de gestion de confiance existants utilisent un modèle de confiance distribué permettant aux nœuds d'évaluer le comportement de leurs nœuds voisins et de prendre les décisions adéquates à leur sujet. Ces valeurs de confiance sont généralement obtenues en tenant compte de différents paramètres tels que la référence personnelle (valeurs obtenues par une interaction de première main "first-hand" avec les nœuds, également appelée confiance directe ou observation directe) et les recommandations (informations obtenues par interaction non-personnelle grâce au "second-hand" aussi appelée informations ou

observations indirectes) comme démontrer dans la Figure 3.1. L'observation directe est le taux de confiance calculé en tenant compte de nombreux facteurs, tels que le taux de livraison des paquets, la quantité d'énergie restante, l'erreur matérielle, l'écart par rapport aux lectures des capteurs, etc. Tandis que l'observation indirecte contient les observations d'autres nœuds. En se basant sur les informations de première main et les informations de seconde main, les valeurs de confiance des différents nœuds de réseau peuvent être calculées. Les systèmes de gestion de confiance les plus récents considèrent l'existence de paramètres supplémentaires, tels que la confiance dis-positionnelle (la quantité de risque que le nœud est prêt à prendre) (Lopez et al., 2010) (Momani et al., 2006). La prise en compte de paramètres additionnels permet de renforcer le mécanisme de confiance.

Nous nous intéressons dans ce qui suit aux notions de confiance et de réputation, nous allons présenter les caractéristiques ainsi que les méthodes utilisées dans la modélisation et le calcul de ces valeurs.

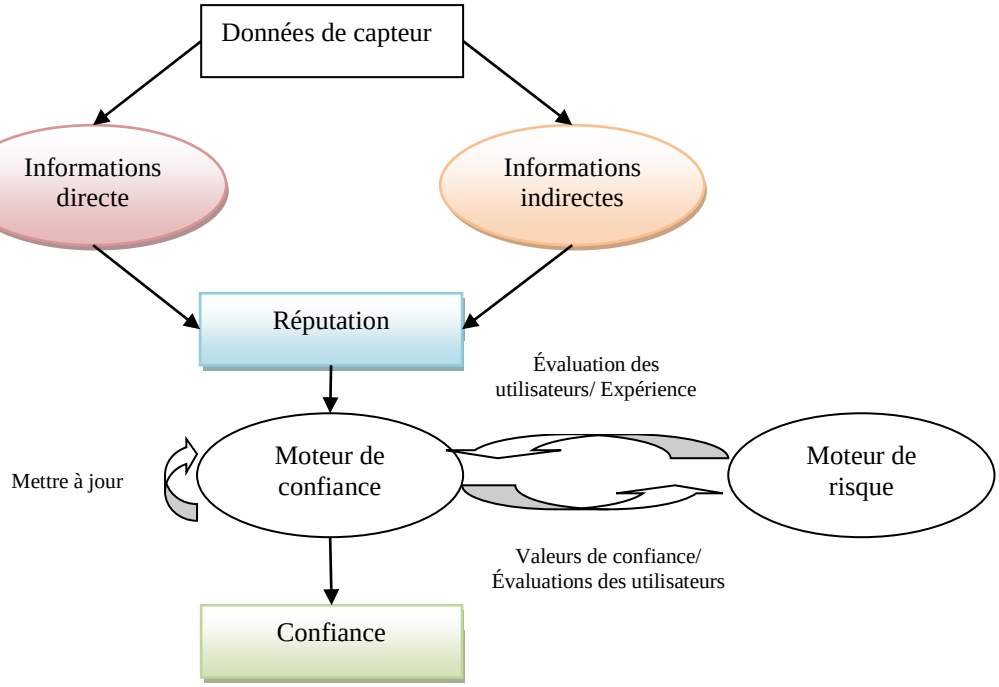


Fig 3. 1. Schéma de calcul des valeurs de confiance basé sur les informations directes et les informations indirectes (Lopez et al., 2010)

Bien qu'elles soient assez différentes, les notions de confiance et de réputation restent étroitement liées et souvent confondues. De nombreux auteurs se sont penchés sur la question et différentes définitions ont en résulté (Boukerch et al., 2007 ; Mármol, et al., 2010 ; Kumar,

et al., 2012). Cependant, Bien qu'il n'y ait pas de consensus clair, la plupart des définitions se sont généralisées comme suit :

"La confiance peut être décrite comme une valeur basée sur le comportement passé des participants. La confiance est une opinion subjective dans la fiabilité d'autres entités ou fonctions, y compris la véracité des données, la connectivité du chemin, la capacité de traitement du nœud et la disponibilité des services, etc." (Kumar et al., 2012).

En outre, bien que considérée comme étant une mesure de pertinence permettant d'évaluer la confiance en se basant sur les recommandations des autres participants, le concept de réputation est clairement différent de celui de la confiance du point de vue des définitions, comme illustré par les énoncés suivants (Jøsang et al., 2007) :

- Je te fais confiance à cause de ta bonne réputation.
- Je te fais confiance malgré ta mauvaise réputation.

Permettant de déterminer le degré de mérite du nœud et de réaliser une évaluation de sa fiabilité, le résultat de la réputation dépend d'approches concrètes pour l'évaluation de la confiance. Par exemple, si le poids de la réputation est plus élevé, nous pouvons facilement obtenir les premiers résultats. Contrairement à cela, lorsque l'expérience personnelle prend le dessus, la réputation n'est plus aussi importante (Yu et al., 2012).

2.1. Caractéristiques de la confiance

Il existe différentes caractéristiques de la confiance, ces dernières sont citées dans ce qui suit :

- Subjective : Développée en fonction de certains enregistrements de comportements passés et fournie par certains observateurs ou recommandeurs.
- Dynamique : Pouvant changer au fil du temps. La confiance du nœud décline suivant son comportement (légitime/malicieux).
- Asymétrique : Il est mutuellement indépendant entre les deux côtés, c'est-à-dire que A fait confiance à B alors que B peut se méfier de A.
- Transitive incomplète : La confiance n'est pas toujours transitive, le lien de confiance varie en fonction de la structure ou de l'étendue des relations de confiance entre les participants, c'est-à-dire que A fait confiance à B, et que B fait confiance à C, tandis que A peut faire confiance ou se méfier de C.
- Réflexive : Chaque nœud se fait confiance.
- Contextuel : La confiance est efficace dans un contexte précis.

2.2. Les valeurs de confiance

La façon de modéliser et de calculer la confiance et la réputation est très importante. Ces valeurs fournissent diverses méthodes d'évaluation. Ces valeurs peuvent être : continues ou discrètes. Pour les valeurs continues, une plage spécifique doit être utilisée telle que [-1,1] selon laquelle les valeurs de confiance peuvent être qualifiées de fiables ou de non fiables de manière dynamique. Les valeurs de confiance discrètes peuvent être représentées avec des nombres entiers tels que 0 pour non fiable ou 1 pour fiable, ou même inclure des états intermédiaires en utilisant des valeurs comprises entre 0 et 1.

2.3. Méthodes de calcul de la confiance

Il existe quatre modèles de base pour calculer la confiance (Lopez el al., 2010) :

1) Modèle basé sur la réputation : le taux de transfert de paquets est utilisé pour calculer la confiance.
2) Modèle basé sur les événements : la confiance est calculée pour des événements spécifiques de manière périodique.
3) Modèle collaboratif : les modèles sont développés pour calculer la confiance, ils sont basés sur les informations directes et indirectes.
4) Modèle basé sur l'agent : un nœud agent est introduit à partir d'un cluster, cet agent est utilisé pour stocker les informations de transfert de paquets. Il permet d'observer le comportement des nœuds et diffuser leurs évaluations de confiance.

2.4. Composants d'un mécanisme de confiance et de réputation

Un mécanisme de confiance et de réputation est généralement constitué de cinq éléments (Mármol et al., 2010) :

1) Collecte d'informations : Permet de collecter les informations relatives aux comportements des différentes entités du système afin de déterminer leurs fiabilités. Ces informations collectées peuvent provenir de plusieurs sources d'informations telles que : les informations de première main "*first hand"* obtenues grâce aux observations directes et à l'expérience personnelle, ou les informations de deuxième main *"second hand"* représentant les observations directes des autres nœuds du voisinage.
2) Notation et classement : Une fois la collecte d'informations achevée et l'historique d'une transaction recueilli et correctement pondéré, le mécanisme utilise une des

méthodologies de modélisation de la confiance (Section 2.6) dans le but d'attribuer un score de confiance et/ou de réputation à l'entité. Ce score peut être modélisé comme une valeur binaire (par exemple, fiable, non fiable), un entier mis à l'échelle (par exemple 1, 2, ..., 9, 10), un élément à partir d'un ensemble d'étiquettes linguistiques (par exemple {"très digne de confiance", "digne de confiance", "indigne de confiance", "très indigne de confiance"}), une valeur dans un intervalle continu (par exemple [0, 1]), etc.

3) Sélection d'entités : Sélectionner l'entité la plus digne de confiance ou la plus réputée de la communauté en fournissant un certain service et en interagissant efficacement avec elle (Alzaid et al., 2013).
4) Transaction : Une fois la transaction sélectionnée, la transaction va s'effectuer entre les deux entités.
5) Récompenser et punir les entités : Une fois la transaction achevée, l'entité cliente doit évaluer cette transaction afin de pouvoir récompenser ou punir l'entité qui a fourni le service.

2.5. Méthodologies de modélisation de la confiance

En général, le modèle de confiance prend en compte les observations directes et indirectes. Différents modèles ont été développés pour modéliser la confiance. Ceux-ci sont énumérés ci-dessous :

2.5.1. Modèles de confiance bayésiens

Souvent utilisé pour la gestion de la confiance, le réseau bayésien utilisant la règle de Baye comme règle principale est en totale conformité avec la procédure d'évaluation de la confiance. La théorie bayésienne est divisée en deux directions : objective et subjective. Dans la vision objective, l'analyse statistique dépend uniquement des données analysées, par contre dans la vision subjective le niveau de confiance est utilisé comme argument afin de prendre part dans la décision. Utilisant la probabilité a priori d'un événement, une mise à jour est effectuée continuellement en fonction des mises à jour des preuves pertinentes dans le but de faire une inférence a posteriori de cet événement. En utilisant le théorème de Bayes, la probabilité de la confiance totale, prenant en considération les observations directes et indirectes, peut être présentée selon l'équation (Eq.1) suivante (Momani et al., 2008) :

$$P(T\backslash D, I) = \frac{P(D\backslash T, I) * P(T\backslash I)}{P(D\backslash I)} \quad (1)$$

- Bêta distribution

Flexible et facile à estimer, la bêta distribution est adaptée pour l'analyse des risques et de la décision. Les fonctions de densité de probabilité bêta sont largement utilisées dans les protocoles de confiance pour représenter et dériver le score de réputation.
La fonction de densité pour une variable aléatoire bêta X sur le domaine [0, 1] est donnée par l'équation 2 suivante :

$$f(p\backslash\alpha+\beta)=\frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)+\Gamma(\beta)}p^{\alpha-1}(1-p)^{\beta-1} \quad (2)$$

Où $0 \leq p \leq 1$et$\alpha,\beta>0$. Avec la restriction que la variable de probabilité $p \neq 0$ si $\alpha<1$ et $p \neq 1$ si$\beta<1$. Les paramètres α et β représentent les résultats des évaluations des r positifs et s négatifs avec$\alpha=r+1$ et $\beta=s+1$ respectivement.

La valeur attendue est donnée dans l'équation 3 suivante :

$$E(p)=\frac{\alpha}{\alpha+\beta} \quad (3)$$

2.5.2. Modèle de confiance entropique

Généralement utilisée en thermodynamique, l'entropie est une mesure de l'incertitude moyenne d'une variable aléatoire. La valeur basée sur l'entropie avec une fonction de masse de probabilité *p* peut être définie comme (Mármol et al., 2010) :

$$T=\begin{cases}1-H(p) & 0.5 \leq p \leq 1\\ H(p)-1 & 0 \leq p \leq 0.5\end{cases} \quad (4)$$

Avec $T=T\{sujet:agent:action\}$ est la valeur de confiance de la relation,$p=p\{sujet:agent:action\}$ est la fonction empirique de la fiabilité et$H(p)=p\log_2(p)-(1-p)\log_2(1-p)$est l'entropie de la fonction pouvant être utilisée afin d'évaluer l'incertitude. La valeur de confiance n'est donc pas une fonction linéaire de la probabilité.

2.5.3. Modèle de confiance floue

La confiance est une relation vague dans la plupart des cas engendrant des imprécisions et des incertitudes. En effet, il est dans la majeure partie des cas difficile de traiter cette notion

en ne considérant que deux états vrai ou faux, car les preuves à prendre en charge ainsi que les politiques à appliquer peuvent être confuses. Reposant sur la logique des ensembles flous, la logique floue confère une flexibilité appréciable pour les mécanismes de confiance grâce à l'introduction de la notion de degré dans la vérification des conditions.

La logique floue permet de résoudre les problèmes de contrôle en faisant appel aux règles IF-THEN. Les principales étapes de la logique floue sont les suivantes (Boukerche et al., 2008) :

1) Prédéfinir les ensembles et les critères flous.
2) Initialiser les valeurs de la variable d'entrée du moteur flou.
3) Appliquer les règles floues pour déterminer les données de sortie.
4) Évaluer les résultats et donner quelques retours afin de modérer les critères ou les règles.

2.5.4. Modèle de confiance de la théorie des jeux

Utilisée dans les situations stratégiques dans lesquelles la décision prise par un agent va dépendre du comportement d'autres agents, la théorie des jeux tente de capturer et de modéliser mathématiquement le comportement de ces différents agents. Pouvant être considérée comme un jeu de confiance entre deux joueurs, cette théorie tente d'éliminer les nœuds non coopératifs. Le côté non prédictif de la théorie des jeux concernant le comportement des nœuds mais suggestif sur leur façon de se comporter a permis l'élaboration de plusieurs mécanismes de confiance tels que (Jaramillo et al.,2007 ; Komathyk et al.,2008 ; Papaioannou et al., 2008 ; Yu el al., 2012). Cependant, la nécessité d'une transmission bidirectionnelle rend cette approche inappropriée pour les réseaux de capteurs qui utilisent dans la majeure partie des cas une transmission unidirectionnelle.

3. PROBLEMATIQUE DE LA SÉCURITE DANS LES MÉCANISMES DE CONFIANCE ET DE RÉPUTATION

Utilisés pour sécuriser les réseaux de capteurs, les mécanismes de confiance et de réputation peuvent être la cible de plusieurs attaques. Dans cette section nous allons nous intéresser aux besoins en sécurité de ces mécanismes et présenter les différentes attaques qui menacent ces derniers.

3.1. Besoins en sécurité

Les mécanismes de confiance et de réputation constituent une approche efficace afin d'améliorer la sécurité et favoriser la collaboration entre les nœuds dans les réseaux de capteurs. Ils jouent un rôle important dans le processus de transmission de données, en permettant au nœud émetteur de choisir des nœuds de confiance pour l'acheminement d'un paquet. Ces mécanismes permettent aussi de sécuriser le routage et de traiter le problème de l'incertitude lors de la prise de décision. Cependant, l'utilisation de ces mécanismes dans les réseaux de capteurs est confrontée à plusieurs attaques qui sont dues aux caractéristiques du mécanisme de confiance et de réputation d'une part ainsi qu'aux caractéristiques du réseau d'une autre part. Parmi ces facteurs :

- Prise en compte des recommandations : Faire appel aux valeurs de recommandations des autres nœuds appelés "recommandeurs" n'est pas en soi une contrainte. En effet, l'utilisation des informations indirectes dans le calcul des valeurs de confiance permet d'améliorer le temps de convergence et d'économiser l'énergie des capteurs. Le risque de sécurité se produit lorsque des nœuds malicieux s'introduisent parmi les nœuds recommandeurs et fournissent de fausses recommandations. Ces recommandations malhonnêtes ont pour principal but de nuire au réseau en portant préjudice aux nœuds.
- Manipulation des valeurs de réputation : Les mécanismes de confiance et de réputation permettent aux nœuds d'attribuer des valeurs de réputation aux autres nœuds du réseau et de pouvoir les transmettre sous forme de recommandations. Cependant, l'absence de contrôle suite à la non-existence d'une entité centrale ayant une vue globale sur tout le système permet aux nœuds malicieux de modifier les valeurs de recommandations à leur guise afin de réduire la réputation des nœuds légitimes.
- Nature distribuée des réseaux de capteurs : La nature distribuée des RCSFs rend difficile la distinction entre les valeurs de recommandations légitimes et malhonnêtes par les nœuds du voisinage. En effet, certains nœuds du réseau peuvent ne jamais se rencontrer et même s'ils se rencontrent, la valeur de réputation attribuée ne va refléter qu'une partie du comportement du nœud et dans une certaine période de temps.

3.2. Attaques contre les mécanismes de confiance et de réputation

L'utilisation des mécanismes de confiance et de réputation apporte pour les réseaux de capteurs plusieurs avantages mais engendre plusieurs attaques. La compréhension de ces attaques est cruciale afin de garantir que l'intégration entre les systèmes de réputation et les RCSFs n'ouvre pas la porte à plus de menaces. Une fois ces attaques prises en considération,

il devient alors plus facile de renforcer ces mécanismes en y intégrant des méthodes et des paramètres supplémentaires. Les attaques ne touchant que les mécanismes de confiance et de réputation sont les suivantes :

3.2.1. Attaques de recommandations malhonnêtes

Les attaques de recommandations malhonnêtes sont parmi les attaques qui menacent les mécanismes de confiance et de réputation les plus dangereuses. Incluant les attaques badmouthing, ballot-stuffing et collusion, elles induisent en erreur les méthodes de calcul des valeurs de réputation ce qui affaiblit l'efficacité du mécanisme de confiance et menace la pérennité du réseau. Une description détaillée de chacune de ces attaques est donnée dans ce qui suit :

- ***Attaques de recommandations malhonnêtes négatives "Badmouthing"***

  Dans cette attaque, l'adversaire fournit des évaluations négatives injustes pour des nœuds fiables. Une fois que l'attaquant réussisse à compromettre un nœud, il peut s'introduire parmi les recommandeurs et influer sur le système de réputation. Il va ainsi attribuer une valeur de réputation faussement négative au nœud légitime. Ces valeurs de réputation erronées vont ensuite être envoyées sous la forme de recommandations aux nœuds voisins. En l'absence d'une vérification réelle, la prise en compte de ces valeurs malhonnêtes entraine un calcul incorrect des valeurs de réputation.

  La Figure 3.2 (a) montre la mise à jour des valeurs de réputation par les nœuds A et D. Les nœuds A et D ont la même valeur de réputation R_C pour le nœud C. Dans la Figure 3.2 (b), l'adversaire a réussi à compromettre le nœud B. Il attribue une valeur de réputation négative $-R_C$ au nœud légitime C. Une fois cette valeur négative transmise au nœud A, ce dernier va déduire que le nœud C est un nœud malicieux et réduire sa valeur de réputation (Alzaid et al., 2013).

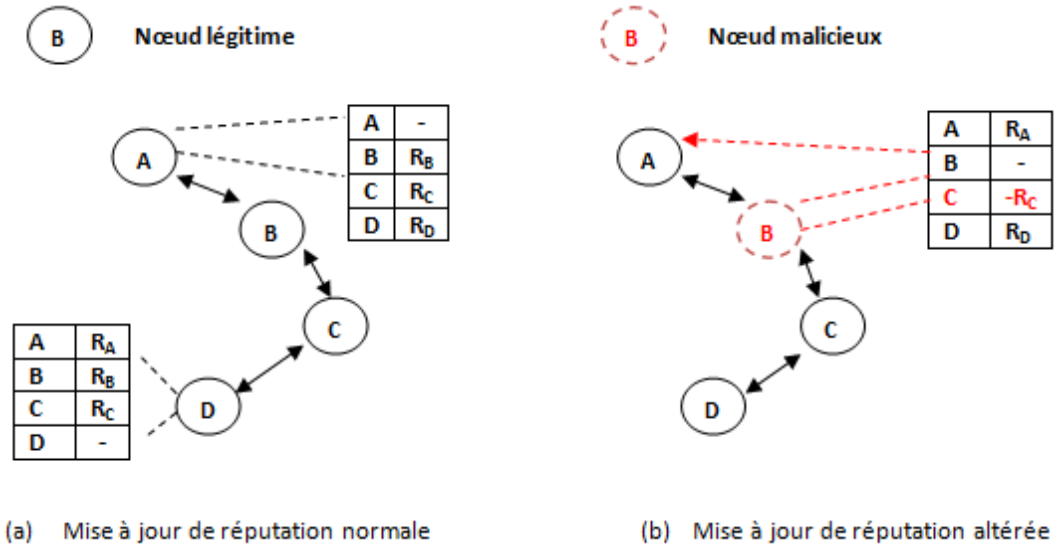


Fig 3. 2. Attaque de recommandations malhonnêtes négatives "Bad mouthing" (Alzaid et al., 2013)

- ***Attaque de recommandations malhonnêtes positives "Ballot-stuffing"***

  Cette attaque est similaire à l'attaque précédente. Cependant, lors de cette attaque, l'adversaire va tenter d'augmenter la valeur de réputation d'un autre nœud malicieux en fournissant des valeurs de recommandations faussement positives. Une fois ces valeurs prises en compte par un nœud évaluateur, le nœud malicieux complice va bénéficier d'une valeur de réputation améliorée et par conséquent d'une plus grande influence dans le système de réputation.

  La Figure 3.3 (a) montre la présence de deux nœuds malicieux B et C. Le nœud B est un recommandeur pour le nœud A et le nœud C est un recommandeur pour le nœud D. Ces nœuds compromis s'associent et s'attribuent des valeurs de réputation plus élevées comme le montre la Figure 3.3 (b).

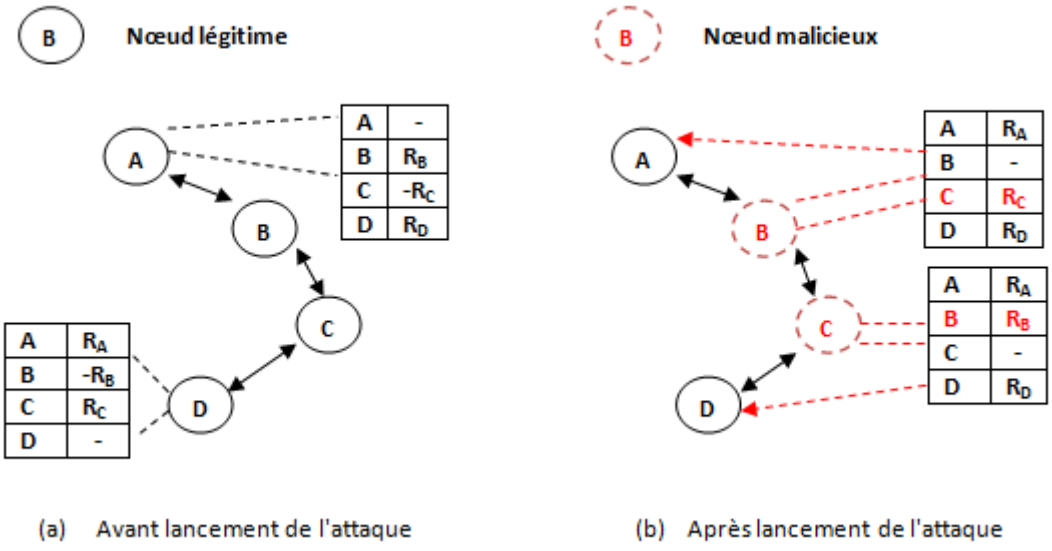


Fig 3. 3. Attaque de recommandations malhonnêtes positives "Ballot-stuffing" (Alzaid et al., 2013)

- ***Attaque par collusion***

  Cette attaque est le résultat de la collaboration de plusieurs nœuds malveillants. En combinant les deux précédentes attaques, les attaquants tentent de causer le plus de tort possible au modèle de réputation.

3.2.2. Attaque On-Off

Dans cette attaque, l'attaquant se comporte bien et mal alternativement dans le temps, en visant à perturber les performances globales du système tout en espérant rester le plus longtemps indétectable. Cette attaque comporte deux cycles on et off. Lors du cycle on, l'adversaire lance des attaques en supprimant par exemple des paquets. En revanche, lors du cycle off, l'attaquant se comporte bien afin d'augmenter sa valeur de réputation.

La Figure 3.4 (a) représente le cycle "off" de l'attaque. Dans cette phase, le nœud malicieux B va se comporter de manière normale avec ses voisins dans le but d'augmenter sa valeur de réputation R_B, une fois qu'il acquiert une valeur de réputation élevée, il peut lancer la deuxième phase de l'attaque. Dans le cycle "on" (Figure 3.4 (b)), le nœud B va se comporter de manière malicieuse afin d'apporter le plus de préjudice au réseau tout en gardant une valeur de réputation positive R'_B avec : $-R_B<R'_B<R_B$.

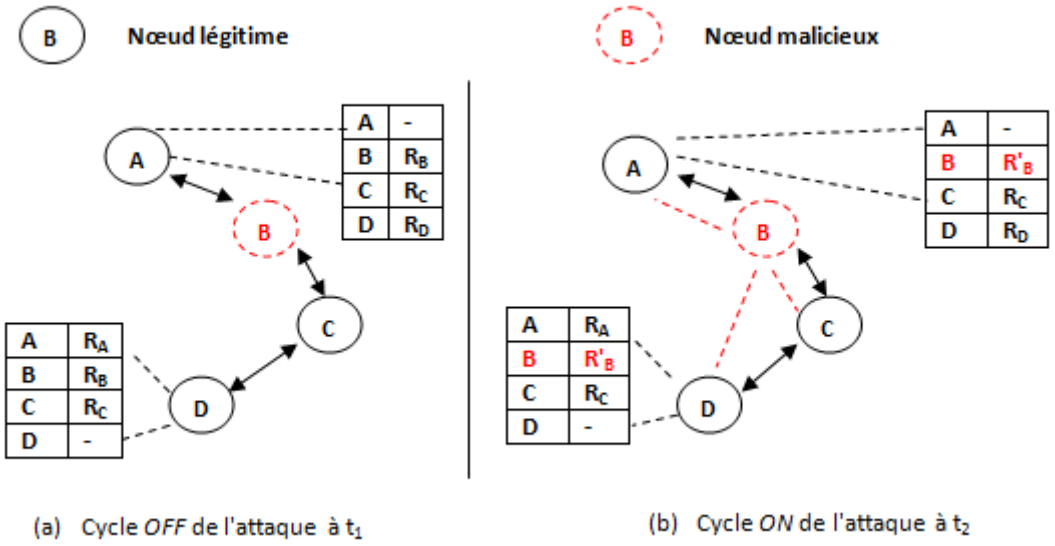


Fig 3. 4. Attaque On-Off

3.2.3. Attaque de blanchiment "whitewashing"

Dès que la valeur de réputation de l'attaquant diminue en-dessous de la valeur de seuil suite à son comportement malicieux, il ne sera plus considéré comme un nœud de confiance par ses voisins. Afin d'augmenter sa valeur de réputation, l'attaquant va ré-entrer le réseau avec un nouvel identifiant et une nouvelle réputation. Cette attaque va permettre à l'adversaire d'effacer tout l'historique de ses mauvaises actions et ainsi causer un maximum de préjudice pour le réseau.

La Figure 3.5 illustre un scénario simplifié de l'attaque de blanchiment. La valeur de réputation du nœud B sur la figure 3.5 (a)a diminué en dessous de la valeur de seuil prédéfinie. Ainsi, l'adversaire va ré-entrer le réseau avec une nouvelle identité B' et une nouvelle valeur de réputation R'_B comme représenté dans la Figure 3.5 (b).

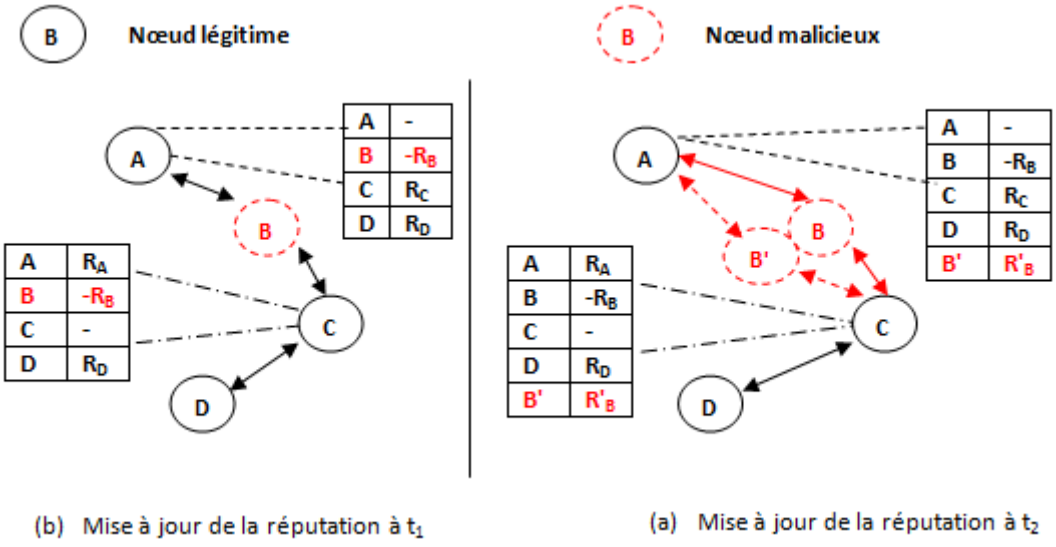


Fig 3. 5. Attaque de blanchiment "whitewashing" (Alzaid et al., 2013)

3.2.4. Attaque de comportement conflictuel "conflicting behavior"

Dans cette attaque, l'adversaire va se comporter différemment avec deux groupes de nœuds. En effet, le nœud malicieux va avoir un bon comportement avec un ensemble de nœuds qui vont lui attribuer une valeur de réputation positive. Par contre, il va se comporter d'une mauvaise manière avec un autre groupe, ce qui va lui valoir une réputation négative. Le conflit va s'effectuer une fois qu'un des nœuds du premier groupe va échanger avec un nœud du deuxième groupe sur la réputation de ce nœud malicieux.

La Figure 3.6 illustre le scénario où le nœud B va lancer une attaque de comportement conflictuel. Les nœuds A et D vont attribuer des valeurs de réputation différentes au nœud malicieux B $–R_B/R_B$ suite à son comportement mauvais avec le nœud A et bon avec le nœud D. Une fois les tables de réputation échangées entre A et D, la différence de la valeur de réputation de B va engendrer un conflit. Le nœud A va penser que le nœud D est un nœud malicieux qui a changé volontairement la réputation du nœud B et inversement.

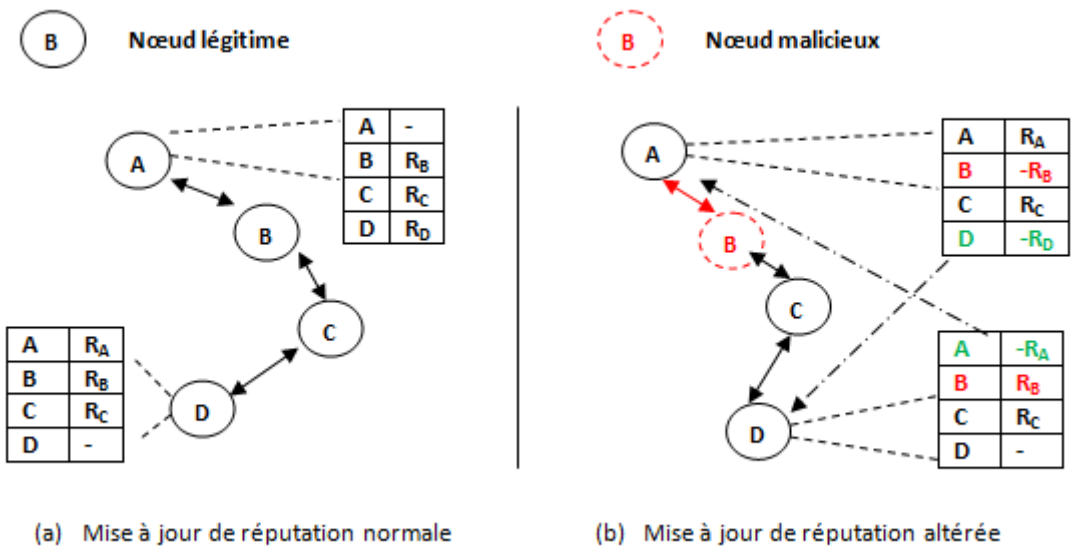


Fig 3. 6. Attaque de comportement conflictuel "conflicting behavior" (Alzaid et al., 2013)

3.2.5. Attaque de comportement intelligent "intelligent behavior"

Dans cette attaque, l'adversaire adapte son comportement en fonction de sa valeur de réputation. Son comportement intelligent va lui permettre de se comporter différemment à chaque période de temps en fournissant sélectivement des services bons ou mauvais ou en attribuant des valeurs de recommandations faibles ou élevées en fonction du seuil de confiance.

4. TAXONOMIE DES PROTOCOLES DE DÉTECTION DES ATTAQUES DE RECOMMANDATIONS MALHONNÊTES

Compte tenu de l'énorme préjudice causé par les attaques de recommandations malhonnêtes (section 3.2.1), plusieurs solutions innovantes et intuitives ont été proposées pour palier à ce problème. Dans cette section, nous survolons ces solutions en les classifiant en deux grandes familles : les algorithmes de prévention et les algorithmes de détection (Khedim et al., 2015). Voir la Figure 3.7.

4.1. Les algorithmes de prévention des attaques de recommandations malhonnêtes

Sécuriser le mécanisme de confiance et de réputation contre les attaques de recommandations malhonnêtes est un besoin vital afin d'assurer son efficacité et son exactitude ainsi qu'une protection optimale pour le réseau de capteurs. Récemment, plusieurs

protocoles se sont focalisés sur des méthodes de prévention afin d'éviter l'impact de ces attaques. Ces protocoles utilisent différentes techniques pour empêcher de telles attaques d'avoir lieu sans ce soucié de proposer des méthodes d'action si jamais celles-ci réussissent à s'introduire dans le réseau.

Deux techniques principales sont utilisées par ces algorithmes : les techniques basées sur l'utilisation des observations directes "first-hand" et les techniques basées sur l'utilisation des valeurs de réputation positives ou négatives selon l'attaque.

4.1.1. Observations directes "first-hand"

Dans les techniques de prévention des attaques de recommandations malhonnêtes basées sur l'utilisation des observations directes "first-hand", les valeurs de réputation sont calculées uniquement en fonction des observations directes du nœud évaluateur. Lorsqu'un nœud souhaite connaitre la réputation des autres nœuds de son voisinage pour des besoins de routage de paquets par exemple, il va utiliser les valeurs de réputation qu'il détient de chacun d'eux. Ces valeurs de réputation sont calculées en fonction des différents échanges que ce nœud évaluateur a eus avec ces nœuds. Selon le succès ou bien l'échec de transmission d'un paquet par nœud voisin, ou suite à l'altération ou à la modification du contenu d'un paquet par ce dernier, le nœud transmetteur augmente ou diminue la valeur de réputation correspondante.

Les travaux relatifs

Plusieurs protocoles de confiance et de réputation utilisent uniquement les observations directes lors du calcul des valeurs de réputation afin d'éviter les attaques de recommandations malhonnêtes. Dans ce qui suit nous survolons les travaux relatifs les plus significatifs.

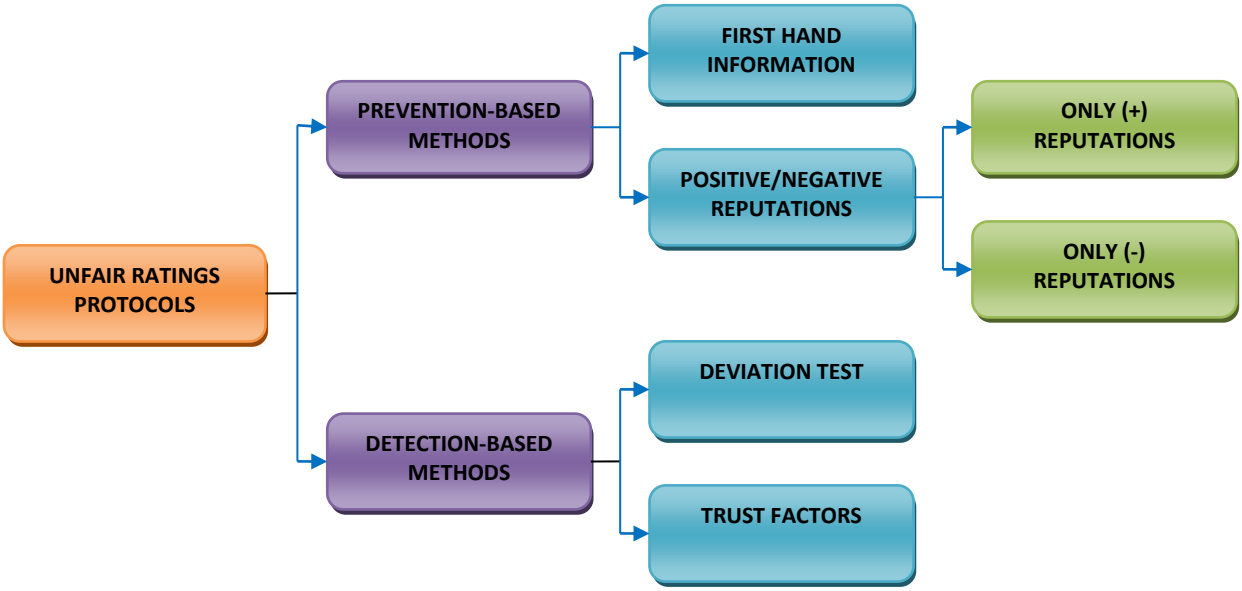


Fig 3. 7. Classification des protocoles traitant les attaques de recommandations malhonnêtes (Khedim et al., 2015)

1. ***A Framework for Trust-based Cluster Head Election in Wireless Sensor Networks (FTCH) : 2006***

Dédié à l'architecture des réseaux de capteurs en clusters, le protocole proposé par (Crosby et al., 2006) met en place un cadre distribué basé sur la confiance dans le but de garantir la fiabilité des cluster-heads sélectionnés. Dans cette architecture en cluster, chaque nœud détient une table dans laquelle il enregistre le degré de confiance de chacun de ses voisins. Ces valeurs de confiance sont obtenues grâce à l'utilisation d'un mécanisme de chien de garde "watchdog" basé sur les accusés de réception passifs. Ces valeurs sont ensuite envoyées au besoin au cluster-head. Cependant, en ne prenant en compte que les informations de première main ce mécanisme réduit l'impact de l'attaque badmouthing mais empêche le protocole de bénéficier des informations obtenues par les membres du cluster.

2. ***Agent-based Trust Model in Wireless Sensor Networks (ATSN) : 2007***

Basé sur l'utilisation des agents, le protocole ATSN proposé par (Chen et al., 2007) s'exécute sur le middleware de chaque nœud agent. Son architecture inclue l'exécution successive de plusieurs phases. La première étape va permettre la collecte des données grâce à l'utilisation du mécanisme de chien de garde dans une fenêtre de temps fixe. La vérification des données quant à elle inclue une vérification du comportement des nœuds lors du routage des informations ainsi qu'une surveillance des données de détection brutes. La dernière phase

va permettre de classer les comportements des nœuds en bon ou mauvais en fonction des résultats des phases précédentes. En se basant sur ces résultats, le nœud agent va calculer des valeurs de confiance qui seront cryptées avant d'être envoyées aux nœuds dans sa portée radio. Cependant, le protocole ATSN n'est pas adapté pour les réseaux de capteurs en raison de sa lourdeur de calcul. Supposer en plus que les agents sont résistants à toute menace de sécurité n'a pas de sens dans les réseaux de capteurs.

3. Agent-based trust and reputation management scheme (ATRM) : 2007

Basé sur une architecture de RCSFs en cluster avec backbone, le protocole ATRM présenté par (Boukerch et al., 2005)utilise une stratégie de gestion de la réputation et de la confiance localisée faisant appel à un système d'agent mobile. Dans le protocole ATRM, la gestion de la confiance et de la réputation est effectuée localement avec une surcharge minimale en termes de messages supplémentaires et de délai. La réalisation du protocole nécessite que les informations de confiance et de réputation d'un nœud soient stockées respectivement sous la forme de *t-instruments* et de *r-certificats* par le nœud lui-même. En outre, le protocole ATRM exige que chaque nœud détienne un agent mobile. Cet agent sera chargé de gérer les valeurs de confiance et de réputation de son hôte et de participer activement dans les transactions. Ce protocole permet à chaque nœud du réseau d'établir une valeur de confiance avec d'autres entités en interaction avec un coût de communication minimal et une latence d'acquisition. Cependant, ile protocole ATRM utilise de lourdes hypothèses. D'une part, il existe la présence d'une autorité de confiance responsable de la génération et du lancement des agents mobiles, en l'absence d'une telle entité c'est toute la sécurité du protocole qui est remise en jeu. D'autre part, il suppose que les agents mobiles sont résistants à l'analyse non autorisée et à la modification de leur logique de calcul, ce qui est loin d'être réaliste dans les RCSFs. Avec le relâchement de cette hypothèse, le protocole devra faire face à une multitude de menaces de sécurité.

4. Reputation Based Trust Management (RBTM) : 2008

Le schéma de gestion de confiance basé sur la réputation proposé par (Zia, 2008) utilise un mécanisme de vote afin d'établir la confiance entre les nœuds. La valeur de vote de confiance augmente avec chaque transmission de message réussie d'un nœud à un autre. Elle est compromise lorsqu'un nœud voisin entre un vote négatif pour un nœud particulier. Si le vote négatif atteint un seuil prédéterminé, ce nœud est déclaré comme nœud non sécurisé. Dans le protocole RBTM, lorsqu'un nœud A envoie un message au nœud B pour la première fois, le nœud A va créer une table de confiance afin de suivre l'acheminement de la transaction.

Lorsque le nœud B transmet le message au nœud suivant, le nœud A écoute et compare ce message avec celui qu'il a envoyé au nœud B, faisant ainsi une comparaison entre le message original et le message actuel. Si le message transmis par le nœud B est le même que l'original, le nœud A attribut une valeur de confiance positive pour le nœud B. Sinon, il lui attribue une valeur de confiance négative. La mise à jour de la table de A va s'effectuer à chaque nouvelle transaction. Une fois que la valeur de vote de confiance négative atteint un seuil prédéterminé, le nœud A déclare que le nœud B n'est pas approuvé et diffuse cette valeur aux nœuds voisins.

5. Reputation-based Secure Data Aggregation in Wireless Sensor Networks (RSDA): 2008

Alzaid et al. ont proposé un système d'agrégation de données sécurisé basé sur la réputation dans les réseaux de capteurs. Le protocole proposé (Alzaid et al., 2008) intègre les fonctionnalités d'agrégation en tirant partie des avantages des mécanismes de réputation. En se concentrant sur le modèle d'agrégateur multiple, chaque nœud dans le protocole RSDA doit surveiller le comportement des autres nœuds de la même cellule, puis leurs attribuer des valeurs de réputation en fonction de leur participation à certaines opérations de la cellule. Ce procédé va permettre de filtrer les données incohérentes en présence de plusieurs nœuds compromis. La fonction de densité de probabilité bêta est utilisée afin de mettre à jour les valeurs de réputation en fonction du comportement des nœuds. Le comportement de chaque nœud est examiné suivant trois fonctions : la détection de données, la transmission de données et l'agencement de données.

6. Connected Dominating Set (CDS) : 2008

Le protocole CDS proposé par (Srinivasan et al., 2008) est le premier protocole utilisant un backbone de surveillance basé sur un CDS "ensemble dominant connecté". L'utilisation du CDS va permettre d'agréger en toute sécurité la réputation des capteurs. Le protocole assume l'existence de deux types de nœuds : les capteurs qui sont mobiles et les moniteurs qui sont statiques. Les informations échangées sont principalement de première main; où chaque capteur maintien des valeurs de réputation pour tous les nœuds de son voisinage, ces valeurs sont fournies par son gestionnaire, c'est-à-dire, le nœud de surveillance auquel il appartient. Chaque nœud de surveillance utilise sa propre observation pour calculer la réputation de chaque nœud dans sa juridiction. Le fait d'utiliser la notion d'ensemble dominant connecté est une propriété hautement souhaitable pour les systèmes de surveillance et adéquate pour les RCSFs. En faisant en sorte que les nœuds CDS surveillent les nœuds dans leur juridiction, la surveillance de l'ensemble du réseau sera faite avec très peu de ressources. Cependant,

supposer que les moniteurs sont inaltérables et toujours fiables n'a pas de sens dans les réseaux de capteurs.

7. Task-based Trust framework for Sensor Networks (TTSN) : 2009

Le protocole TTSN (Chen et al., 2009) permet aux nœuds capteurs d'attribuer des valeurs de confiance différentes aux nœuds voisins suivant les tâches effectuées lors des transactions. En effet, un nœud peut fonctionner correctement lors de l'exécution d'une tâche, cependant, il pourra mal fonctionner lors de l'exécution d'une autre tâche. Il sera ainsi jugé positivement et négativement en fonction de ses performances. Le protocole TTSN construit les valeurs de confiance grâce à une entité appelée *"Task"* et en faisant appel au *"Trust Manager Module"* s'exécutant sur chaque nœud. Le module de gestion de tâches et de confiance comprend trois composants principaux : (1) le module de surveillance permettant de surveiller de manière indépendante les activités de transmission de paquets des nœuds voisins et de les classer suivant la tâche (2) le module de gestion de la réputation permettant d'obtenir les différentes valeurs de sortie pour les différentes tâches et (3) le module de gestion des tâches et de la confiance permettant d'associer plusieurs valeurs de confiance au nœud suivant le nombre de tâches. Le protocole TTSN est approprié pour le calcul de la confiance dans les RCSFs et peut être utilisé dans les réseaux de capteurs à grande échelle.

4.1.2. Valeurs de réputation positives ou négatives

Dans les techniques de prévention des attaques de recommandations malhonnêtes basées sur l'utilisation des valeurs de réputation positives ou négatives, les protocoles ne considèrent l'attribution que de certaines valeurs de réputation suivant le type de l'attaque. En effet, certains protocoles permettent seulement l'attribution de valeurs de réputation positives afin d'empêcher la survenue d'une attaque de type badmouthing. D'autres protocoles utilisent seulement des valeurs de réputation négatives afin d'éviter les attaques de type ballot-stuffing. Par conséquent, nous pouvons partager les protocoles utilisant cette méthode en deux catégories, ceux utilisant uniquement les réputations positives et ceux utilisant uniquement les réputations négatives comme suit :

a. Valeurs de réputation positives

Dans les protocoles utilisant cette méthode, le système ne propage que les informations de réputation positives sur les autres nœuds et, ce faisant, élimine l'attaque de recommandations malhonnêtes négatives "badmouthing". Cependant, ce procédé affecte l'efficacité du système,

car les nœuds ne peuvent pas échanger les mauvaises expériences rencontrées avec les nœuds malveillants du réseau.

Les travaux relatifs

1. Collaborative reputation mechanism (CORE) : 2002

Figurant parmi les premiers protocoles de réputation, le protocole CORE (Michiardiet al., 2002) implique l'utilisation de deux types d'entités, un demandeur et un ou plusieurs fournisseurs. Ces fournisseurs se trouvent dans la portée de transmission sans fil du demandeur. La nature distribuée du protocole et les mécanismes sur lesquels il s'appuie, y compris les informations de confiance directes, indirectes et fonctionnelles, garantissent que si un fournisseur refuse de coopérer, le système CORE réagira en diminuant sa réputation. Si ce fournisseur persiste dans son comportement non coopératif, il sera exclu du réseau. Le protocole CORE suppose que les attaques de type ballot-stuffing sont absentes du réseau et le fait de diffuser uniquement des réputations positives le rend résistant aux attaques de type badmouthing.

2. Reputation-based Framework for High Integrity Sensor Networks (RFSN) : 2004

Dans (Ganeriwal et al., 2008), les auteurs ont proposé le protocole RFSN pour les réseaux de capteurs à haute intégrité, où les nœuds maintiennent la réputation des autres nœuds afin d'évaluerleur fiabilité. Ce modèle utilise la formulation bayésienne, plus spécifiquement la distribution bêta est utilisée pour la représentation de la réputation, les mises à jour, l'intégration et l'évolution de la confiance. RFSN collecte les informations à l'aide d'un mécanisme watchdog dans le but de détecter les données invalides ainsi que les nœuds non-coopératifs. Un facteur de vieillissement est utilisé afin de pondérer différemment les anciennes des nouvelles interactions lors de la mise à jour de la confiance. Le protocole RFSN propage uniquement les informations de réputation positive sur les autres nœuds, éliminant ainsi les attaques de type badmouthing.

b. Valeurs de réputation négatives

Dans les protocoles utilisant cette méthode, le système ne propage que les informations de réputation négatives sur les autres nœuds et, ce faisant, élimine l'attaque de type ballot-stuffing. En l'absence d'une méthode de protection efficace, il sera alors difficile pour le réseau de résister à l'attaque badmouthing.

Les travaux relatifs

1. *Cooperation Of Nodes: Fairness In Dynamic Ad-hocNeTworks (CONFIDANT) : 2002*

Figurant parmi les premiers protocoles de réputation, le protocole CONFIDANT proposé par (Buchegger et al., 2002) combine plusieurs composants. Le moniteur est responsable d'enregistrer les écarts de comportements. Le système de réputation est responsable principalement de la gestion des niveaux de confiance. Le gestionnaire de chemins permet entre autre de classer les chemins suivant la réputation des nœuds et de supprimer les chemins contenant des nœuds malicieux. Enfin, le gestionnaire de confiance est responsable de la gestion du tableau des réputations. L'association de ces composants et l'utilisation des informations de première et de seconde main ainsi que d'un mécanisme *watchdog* permettent au protocole CONFIDANT de faire face aux nœuds malveillants du réseau. Le fonctionnement de ce protocole repose sur la surveillance continue du comportement des voisins du prochain saut. Si un événement suspect est détecté, l'information est donnée au système de réputation. Les nœuds sont initialisés avec des évaluations de confiance positives et ceux avec une faible réputation sont exclus du chemin de routage. Ce protocole permet d'améliorer les performances du protocole de routage DSR.

2. *Location-aware trust-based protocol : 2011*

Les auteurs utilisent dans (Crosby et al., 2011) un algorithme de formation de clusters sécurisé afin de faciliter l'établissement de clusters de confiance via des clés pré-réparties. Dans ce protocole, chaque nœud maintien des tables de confiance indépendantes basées sur les observations directes pour les nœuds de son voisinage. La fonction de réputation bêta est utilisée pour quantifier le niveau de confiance entre les nœuds. Le système permet uniquement le partage des informations négatives. Cependant, l'approche traite efficacement la menace posée par l'attaque badmouthing grâce à l'utilisation de l'interaction directe dans toute prise de décision fondée sur la confiance.

4.1.3. Discussion

Les attaques de recommandations malhonnêtes représentent à la fois une faille importante pour les mécanismes de confiance et de réputation ainsi qu'une menace certaine pour la sécurité du réseau. En effet, un attaquant lançant une attaque badmouthing va pouvoir isoler les nœuds légitimes et diminuer leur implication dans les applications critiques en détruisant

leurs réputations. Le lancement d'une attaque ballot-stuffing quant à lui, va permettre aux nœuds malicieux de gagner en pouvoir grâce à l'augmentation de leurs valeurs de réputation.

Afin de pallier à ce problème, plusieurs protocoles se sont intéressés à trouver des solutions leurs permettant d'éviter ces attaques. Deux méthodes principales se distinguent: l'utilisation des observations directes et l'utilisation des valeurs de réputation positives ou négatives. Cependant, ces méthodes présentent plusieurs inconvénients tant sur l'efficacité de la proposition que sur le fonctionnement du réseau.

Premièrement, l'utilisation uniquement des informations de première main pour le calcul des valeurs de réputation présente de sérieux inconvénients. En effet, les nœuds vont se basés sur un mécanisme watchdog afin d'obtenir des informations sur le comportement des nœuds voisins. Ainsi, ils vont mettre beaucoup de temps afin d'établir les valeurs de réputation. Ces valeurs prendront par la même occasion beaucoup de temps pour diminuer, ce qui va permettre aux nœuds malicieux de rester plus longtemps dans le système.

Deuxièmement, l'utilisation uniquement de valeurs de réputation positives ou négatives ne protège pas davantage le réseau contre les attaques badmouthing et ballot-stuffing. Ces méthodes sont inefficaces contre les attaquants intelligents. En effet, même dans un modèle de réputation où uniquement les valeurs positives sont prises en compte, l'attaque badmouthing peut être effectuée. L'attaquant n'a qu'à attribuer une valeur positive relativement faible au nœud légitime afin de diminuer progressivement sa réputation.

4.2. Les algorithmes de détection des attaques de recommandations malhonnêtes

Étant donné que les méthodes de prévention des attaques de recommandations malhonnêtes présentent plusieurs inconvénients se reflétant sur l'efficacité du mécanisme de confiance et de réputation et sur la sécurité du réseau. Il était devenu indispensable de trouver des moyens efficaces pour atténuer ou même éliminer l'influence de ces attaques. Dans ce contexte, de nombreux efforts de recherche ont été fournis ces dernières années et plusieurs algorithmes en ont résulté.

Deux techniques principales sont utilisées par ces algorithmes: les techniques basées sur l'utilisation de détection à base de déviation et les techniques basées sur l'utilisation des facteurs de confiance.

4.2.1. Test de déviation

Dans les techniques de détection des attaques de recommandations malhonnêtes basées sur l'utilisation de détection à base de déviation, les valeurs de réputation sont calculées en

fonction des informations de première main et de seconde main. Cela veut dire que si un nœud souhaite évaluer la réputation d'un autre nœud, il aura non seulement besoin des informations directes qu'il détient pour ce nœud, mais en plus, des valeurs de réputations attribuées pour ce nœud par ses recommandeurs. Le nœud choisit ses recommandeurs parmi les nœuds du voisinage avec les plus grandes valeurs de réputation. Le nombre de recommandeurs varie d'un protocole à un autre. Différents poids peuvent être attribués lors du calcul des valeurs de réputation selon les besoins des protocoles en donnant plus de poids aux informations directes ou bien plus de poids aux informations indirectes. Les méthodes de détection à base de déviation sont classées en deux catégories principales:

Premièrement, les mesures de similarité majoritaires impliquant la comparaison entre chaque recommandation et l'opinion majoritaire calculée sur l'ensemble des recommandations. Les recommandations éloignées de cette opinion majoritaire seront considérées comme malhonnêtes. Cette méthode a été efficacement utilisée dans les réseaux pair à pair (Feng et al., 2010) ainsi que dans les marchés électroniques (Dellarocas, 2000) mais à notre connaissance pas dans les réseaux de capteurs.

Deuxièmement, les mesures de similarité personnalisées impliquant une comparaison entre l'opinion personnelle du nœud demandeur "première main" et les recommandations reçues "seconde main" suivant un seuil prédéfini. Nous allons présenter dans ce qui suit les principaux travaux relatifs à cette catégorie.

Les travaux relatifs

1. A Robust Reputation System (RRS) : 2004

Dans (Boudec, 2004), les auteurs ont présenté un système de réputation entièrement distribué nommé RRS. Dans ce protocole, les nœuds surveillent leurs voisins et suivent leurs comportements en utilisant une approche bayésienne modifiée. Cette approche permet d'attribuer une moyenne pondérée mobile spécifique à chaque observation. Ces informations sont périodiquement échangées avec les autres nœuds. Pour détecter les recommandations malhonnêtes, un test de déviation est réalisé entre l'espérance de la distribution de la première main et celle de seconde main selon un certain seuil. Ce seuil ne permet qu'aux informations de seconde main qui ne sont pas incompatibles avec les informations de première main d'être acceptées. De ce fait, les informations passant ce test seront déclarées comme compatibles et fiables. Les nœuds ayants un mauvais comportement seront exclus du réseau.

2. Distributed Reputation-based Beacon trust System (DRBTS) : 2006

Le protocole DRBTS présenté dans (Srinivasan et al., 2006) est un protocole de sécurité distribué modélisant le réseau comme un graphe non orienté. Ce protocole est conçu pour fournir une méthode dans laquelle les nœuds balises peuvent se surveiller mutuellement et fournir des informations permettant aux nœuds de choisir à qui faire confiance, en utilisant une approche de vote majoritaire. Dans DRBTS, les recommandations sont jugées honnêtes ou malhonnêtes selon le résultat du test de déviation effectué entre les informations de première main et les informations de seconde main (les informations d'écoute de localisation, transmises par un autre nœud balise dans sa plage de communication). Ce test va permettre de vérifier la cohérence des informations et décourager les nœuds à publier de fausses informations.

3. Robust, cooperative trust establishment scheme (E-HERMES) : 2009

Dans (Zouridaki et al., 2009), les auteurs ont proposé un schéma d'établissement de confiance robuste et coopératif. Dans ce protocole, les informations de confiance de première main sont combinées avec celles de deuxième main dans le but de déterminer la fiabilité des nœuds. Cette fiabilité est évaluée selon l'acheminement des paquets d'un nœud à un autre. Le papier a proposé différentes définitions afin de faire la distinction entre "un nœud mauvais" et "un recommandeur mauvais". Afin de pallier au problème des attaques de recommandations malhonnêtes, le test RC est appliqué dans le but de garantir que seules les recommandations dont la valeur est suffisamment proche de la valeur de confiance de première main calculée par le nœud évaluateur sont acceptées. Cependant, le protocole E-Hermes est incapable de calculer des valeurs de confiance précises lorsque le comportement du nœud change d'un flux à un autre.

4. Beta-based Trust and Reputation Evaluation System (BTRES) : 2016

En se basant sur la surveillance du comportement des nœuds, le protocole BTRES proposé dans (Fang et al., 2016) permet de déterminer la crédibilité des nœuds et ainsi guider les interactions. Dans ce protocole, les valeurs de confiance et de réputation sont calculées en prenant en considération la confiance des communications et la confiance des données. Le protocole commence par collecter les informations directes. Ces valeurs sont synthétisées en utilisant la fonction de répartition de la réputation bêta. Un facteur de vieillissement est utilisé afin de donner plus de poids aux données récentes. Les informations indirectes sont ensuite intégrées lors du calcul final des valeurs de réputation des différents nœuds. Un seuil θ est

définit pour filtrer les évaluations indirectes s'éloignant trop des évaluations directes afin de réduire l'influence des attaques badmouthing et collusion.

5. Time Series Trust Model (TSTM) : 2018

Basé sur la confiance des données, la confiance énergétique et la confiance relative dans chaque nœud du réseau, le protocole TSTM proposé dans (Gilbert et al., 2018) s'exécute à chaque niveau du réseau que ce soit les nœuds, les têtes de cluster et la station de base. Au niveau des nœuds, la confiance totale est calculée en fonction de la confiance énergétique et de l'approbation de données en utilisant une matrice de Toeplitz. Au niveau des têtes de cluster, les données reçues de la part des nœuds sont compressés en utilisant la détection compressée. Un modèle autorégressif linéaire et non linéaire AR basé sur la confiance est utilisé par les cluster-head afin de prédire les données. Dans le but d'empêcher les données malhonnêtes de fausser les résultats du protocole, les données prédites par le modèle sont comparées continuellement aux données lues à partir des nœuds. Si la variance est supérieure à une valeur de seuil, les données prédites sont utilisées pour l'agrégation, sinon les données d'origine lues à partir du nœud sont utilisées. Enfin, la station de base va récupérer les données agrégées transmises par les différentes têtes de cluster.

4.2.2. Facteurs de confiance

Dans les techniques de détection des attaques de recommandations malhonnêtes basées sur l'utilisation de facteurs de confiance, les valeurs de confiance sont calculées en prenant en considération plusieurs paramètres. Ces facteurs sont utilisés par le nœud évaluateur afin de déterminer la fiabilité des autres nœuds. Cependant, sur qu'elle base définir ces facteurs et pour exploiter quelles données constituent le défi majeur pour cette méthode de détection.

Les travaux relatifs

1. Trust Evaluation Model for Wireless Sensor Networks: 2005

Dans (Hur et al., 2005), les auteurs ont proposé un modèle d'évaluation de confiance permettant de garantir le fonctionnement normal du réseau en présence de nœuds compromis. Le protocole est divisé en quatre étapes distinctes. Lors de la première étape, les zones de détection sont divisées en plusieurs grilles logiques, à chaque grille est assigné un identifiant unique. Dans la deuxième étape, grâce à l'utilisation du protocole ECHO, les nœuds de chaque grille vont vérifier la localisation de leurs nœuds voisins. Lors de la troisième étape, chaque nœud va évaluer la fiabilité de ses nœuds voisins en utilisant une matrice d'évaluation.

Cette matrice comprend plusieurs facteurs tels que: détection de communication, détection de résultats, consistance, etc. Finalement, des nœuds spéciaux vont agréger les données de détection de leurs grilles et transmettre les résultats calculés à la station de base.

2. Integrated trust framework (iTrust) : 2010

Les auteurs ont proposé dans (Yadav et al., 2010) un modèle de confiance distribué iTrust où les nœuds sont catégorisés en deux types : (1) les nœuds de surveillance et (2) les nœuds capteurs. Chaque nœud dans iTrust peut fonctionner soit dans le mode visible soit dans un mode de promiscuité. Les nœuds de surveillance sont chargés d'accumuler les informations de confiance, de stocker et de calculer la réputation de tous les nœuds du voisinage. Le protocole prend en compte les paramètres de toutes les couches afin d'évaluer les valeurs de confiance. Parmi ces paramètres: l'énergie disponible, la force de signal de paquet, les paquets de contrôle reçus pour le transfert, les paquets de contrôle transférés, le nombre de paquets transmis, Le nombre de collisions de paquets, etc. Le protocole utilise une phase d'apprentissage afin de connaitre le comportement normal des nœuds du voisinage. Toute déviation de ce comportement sera signalée à la station de base. L'utilisation des nœuds de surveillance dans le protocole iTrust va permettre d'étendre la durée de vie du réseau et le mode de promiscuité va contribuer à conserver l'énergie des capteurs. Cependant, le fait que le protocole iTrust repose sur l'utilisation de nœuds de surveillance non sécurisés remet en cause toute la crédibilité de ce dernier.

3. Ambient trust sensor routing (ATSR) : 2010

Le protocole ATSR présenté dans (Zahariadis et al., 2010) permet l'élaboration d'un système de gestion de confiance entièrement distribué. Ce système est dédié au routage sécurisé de paquets entre les nœuds en se basant sur la localisation. Dans ce protocole, les nœuds surveillent le comportement de leurs voisins suivant des aspects de comportement spécifiques. Les informations de confiance directes et indirectes sont combinées afin de calculer les valeurs de confiance finales. Chaque voisin est évalué sur la base d'un ensemble de facteurs de confiance comme : (1) Transfert de paquets: Pour détecter les nœuds qui refusent de transmettre les paquets ou bien transmettent sélectivement, (2) Réponse de réputation: Pour vérifier l'exécution sincère du protocole d'échange de réputation, (3) Validation de la réputation: Pour se protéger contre les fausses réputations (négatives ou positives) lors des attaques badmouthing et ballot stuffing respectivement, ainsi que des attaques de comportement conflictuel.

4. Node Behavioral Strategies Banding Belief Theory of the Trust Evaluation Algorithm (NBBTE) : 2011

Dans (Feng et al., 2011), un nouvel algorithme d'évaluation de confiance a été proposé, permettant de souligner avec succès le flou, la subjectivité et la facilité d'utilisation de la confiance. Le protocole NBBTE permet d'intégrer deux approches intéressantes: l'approche des stratégies comportementales des nœuds et la théorie des preuves modifiées. La première approche fait appel à une variété de facteurs de confiance et à différents coefficients afin d'obtenir les valeurs de confiance directes et indirectes correspondantes aux comportements des nœuds. Ces valeurs sont obtenues en combinant le degré de sécurité du réseau et le contexte de corrélation de temps. La théorie des ensembles flous quant à elle va permettre de mesurer le degré d'adhésion de la valeur de confiance à la note de confiance. Enfin, une révision de la règle de combinaison de Dempster est réalisée dans le but de moduler le coefficient de similarité en fonction des différences entre les preuves indirectes et directes. Cette dernière procédure va permettre de synthétiser la valeur de confiance des différents nœuds.

5. Recommendation Verifying scheme (RecommVerifier) : 2012

Le protocole Recomm Verifier (Chen et al., 2012)s'inspire du pouvoir de discernement humain pour la détection de tromperies dans son processus de détection. En effet, le scénario de gestion de la réputation est modélisé comme un tribunal et la notion de procès est utilisée pour traiter les recommandations malhonnêtes. Le protocole est constitué de trois modules : (1) Le test de déviation : va permettre de filtrer les recommandations malhonnêtes grâce à un algorithme de détection des valeurs aberrantes. Dans cet algorithme, un facteur de lissage est utilisé pour indiquer de combien la dis-similarité peut être réduite en supprimant une recommandation. (2) La vérification du temps : permet de vérifier chaque recommandation par rapport à un mécanisme de temps. Dans ce mécanisme, l'honnêteté d'une recommandation peut être vérifiée en s'assurant qu'elle reflète la future réputation dans le domaine temporel. Enfin (3) La vérification de la preuve : s'exécutant du côté du nœud à évaluer, elle permet de compléter le test de déviation et de vérification par rapport au temps s'exécutant tous deux du côté du nœud évaluateur. L'idée est que les recommandations reçues soient transmises au nœud à évaluer. Ce nœud va se charger de vérifier l'honnêteté des recommandeurs, en prenant l'historique comme preuve.

6. A lightweight trust management based on Bayesian and Entropy (LTMBE) : 2015

Proposé par (Che et al., 2015), le protocole LTBME utilise un algorithme léger afin de réduire la consommation d'énergie. Dans ce protocole, les valeurs de confiance directes sont calculées périodiquement en utilisant l'approche Bayésienne. La mise à jour de ces valeurs s'effectue en combinant l'historique des enregistrements avec le facteur adaptatif de décroissance. Afin de rester léger, le protocole LTBME n'utilise pas les informations de seconde main de manière systématique. En effet, en prenant en considération le niveau de confiance calculé pour les valeurs de confiance directes, le protocole décide si la confiance directe est suffisamment crédible ou bien, s'il faut y intégrer les valeurs de confiance indirectes. Afin de pallier au problème des recommandations malhonnêtes lorsque la confiance indirecte est utilisée, le protocole fait appel au facteur de poids. Pour cela, la théorie de l'entropie est utilisée pour distribuer des poids aux différentes valeurs de confiance indirectes selon leurs influences.

7. Risk-aware Reputation-based Trust (RaRTrust) : 2016

RaRTrust proposé dans (Labraoui et al., 2016) est un protocole générique permettant de combiner les valeurs de réputation avec les valeurs du risque lors du calcul des différentes valeurs de confiance. Le paramètre de risque va permettre de mettre en évidence les comportements imprévisibles et incertains des nœuds malveillants. Ce paramètre a une grande influence sur l'estimation des valeurs de réputation. Le protocole fait appel à un facteur d'équilibrage pour calculer les valeurs de confiance directes, permettant ainsi une lente augmentation de la valeur de confiance lorsque le nombre d'interactions infructueuses est considérablement élevé. Dans le but de filtrer les attaques de recommandations malhonnêtes, le protocole RaRTrust utilise un facteur de crédibilité. Ce facteur décrit à quel point un nœud peut faire confiance aux recommandations des autres nœuds. Ainsi, plus la valeur de crédibilité d'un recommandeur est grande, plus sa valeur de recommandation aura de l'influence et inversement.

4.2.3. Discussion

Compte tenu de la menace réelle que représentent les attaques de recommandations malhonnêtes pour le mécanisme de confiance et de réputation et vu l'inefficacité des protocoles de prévention, il était devenu indispensable de trouver des solutions adéquates pour pallier à ce problème. En effet, détecter et révoquer les recommandeurs malhonnêtes est sans doute le plus sûr moyen de protéger le réseau contre ce type d'attaque.

Dans cette thématique, plusieurs chercheurs se sont intéressés à trouver des solutions adaptées à la détection des attaques de recommandations malhonnêtes tout en respectant les contraintes des réseaux de capteurs. Deux méthodes principales se distinguent: les techniques de détection à base de déviation et les techniques basées sur l'utilisation des facteurs de confiance. Cependant, malgré leur efficacité, ces techniques présentent quelques inconvénients.

Les protocoles se basant sur les techniques de détection à base de déviation permettent de filtrer les recommandations s'écartant de l'opinion personnelle du nœud. Cependant, deux principales faiblesses amoindrissent l'efficacité de ces techniques. D'une part, ces techniques se basent sur les informations directes obtenues grâce aux échanges entre le nœud évaluateur et le nœud évalué. Dans les réseaux de capteurs connus pour être décentralisés il peut n'y avoir aucune interaction entre deux nœuds. D'un autre côté, les informations directes détenues par le nœud évaluateur à propos du nœud évalué ne reflètent qu'une partie des interactions de ce nœud dans le réseau et dans une certaine période de temps. Le comportement de ce nœud peut être complètement différent avec d'autres nœuds. Son comportement peut aussi totalement changer en fonction du temps surtout dans un réseau de capteurs où un attaquant peut capturer un nœud à tout moment le rendant ainsi malicieux. Les informations directes sont donc complètement obsolètes et ne peuvent pas être considérées comme une référence pour juger les autres recommandations.

Les protocoles se basant sur l'utilisation de facteurs de confiance, font appel à plusieurs facteurs afin de juger l'honnêteté ou la malhonnêteté des recommandations. Cette technique peut donner des résultats prometteurs à condition de choisir les bons facteurs.

5. COMPARAISON DES PERFORMANCES

Après avoir survolé les travaux existants et proposé une taxonomie des protocoles, nous allons présenter dans cette section une comparaison entre tous les protocoles cités dans la section précédente. La comparaison des protocoles traitant les attaques de recommandations malhonnêtes est assez difficile compte tenu des différents champs d'application de ces protocoles et des différents axes ciblés par les concepteurs. Nous ne nous attendons pas à donner une classification exhaustive et complète, mais juste une approche permettant de récapituler les principales caractéristiques que partagent la plupart d'entre eux. Pour cette raison, nous allons utiliser certains paramètres pour classer ces protocoles. Nous résumons cette comparaison dans le Tableau 3.1.

La première classification pourrait être faite selon la taxonomie que nous avons proposée pour les protocoles traitant les attaques de recommandations malhonnêtes (Figure 3.7). Cette classification va ainsi se basée sur les stratégies de défense utilisées par les protocoles que ce soit la prévention des attaques de recommandations malhonnêtes ou la détection.

Le niveau suivant de classification est la portée des informations. Incluant la source de l'information (D: Directe, de première main), (I: Indirecte, Seconde main) et le type des recommandations utilisées (Positives vs. Négatives).

Une autre catégorisation pourrait dépendre de la technique ou de la méthodologie utilisée pour développer le modèle, comme par exemple: logique floue, réseaux bayésiens, pondération, mécanisme de surveillance, etc.

Tableau 3. 1. Résumé de la comparaison entre les schémas d'attaques de recommandations malhonnêtes (Khedim et al., 2015)

	DEFENSES STRATEGIES	PROTOCOLS	SOURCE	TYPE	METHODOLOGY	APPLICATIONS	BAD MOUTHING	BALLOT STUFFING
AVOIDING DISHONEST RECOMMENDATIONS	FIRST HAND	FTCH [26]	D	+/-	Weighting; Watchdog mechanism	Clustering	***	***
		ATSN [21]	D	+/-	Weighting; Probability theory; Watchdog mechanism	Routing	***	***
		ATRM [15]	D	+/-	Weighting; Mobile backbone networks	Aggregation	***	***
		RBTM [109]	D	+/-	Weighting; Watchdog mechanism	-	***	***
		RSDA [8]	D	+/-	Weighting; Beta probability density; Watchdog	Aggregation	***	***
		CDS [95]	D	+/-	Connected dominating set; Watchdog mechanism	Aggregation	***	***
		TTSN [22]	D	+/-	Weighting; Bayes Theorem; Beta Distribution	-	***	***
	POSITIVE/ NEGATIVE REPUTATION	CORE [72]	D/I	+	Weighting; Watchdog mechanism	Routing	**	***
		RFSN [39]	D/I	+	Probability theory; Bayesian calculation; Watchdog	-	**	**
		CONFIDANT [18]	D/I	-	Weighting; Watchdog mechanism	Routing	*	**
		Location-Aware [27]	D/I	-	Weighting; Beta distribution; Watchdog	Localization	***	***
DEALING WITH DISHONEST RECOMMENDATIONS	DEVIATION TEST	RRS [14]	D/I	+/-	Moving weighted; modified Bayesian approach	-	**	**
		DRBTS [93]	D/I	+/-	Beta distribution	Localization	**	**
		E-HERMES [110]	D/I	+/-	Weighting; Bayesian approach	Routing	**	**
		BTRES [35]	D/I	+/-	Beta distribution; Watchdog mechanism	Routing	**	**
		TSTM [40]	D/I	+/-	Toeplitz matrix; Autoregressive model	Aggregation	***	***
	TRUST FACTORS	Trust Model [49]	D/I	+/-	Watchdog mechanism; Echo protocol	-	***	***
		iTrust [104]	D/I	+/-	Weighting; Watchdog mechanism	-	***	***
		ATSR [107]	D/I	+/-	Weighting; Watchdog mechanism	Routing	***	***
		NBBTE [38]	D/I	+/-	Weighting; Fuzzy theory; D–S Evidence Theory	-	***	***
		Recomm Verifier [23]	D/I	+/-	Weighting; Beta distribution; Bayesian inference	-	***	***
		LTMBE [20]	D/I	+/-	Bayesian entropy;Confidence level;Adaptative Decay factor	-	***	***
		RaRTrust [65]	D/I	+/-	Balancing factor; Risk factor; Watchdog mechanism	-	***	***

(***) Robust, **(**)** Partial damage, **(*)** Vulnerable

6. CONCLUSION

Les mécanismes de confiance et de réputation sont un outil puissant et efficace qui a fait ses preuves dans les réseaux de capteurs. Ils sont utilisés dans de nombreuses applications telles que le routage, l'agrégation et la localisation. Leur efficacité dans le domaine de la sécurité n'est plus à prouver et nombreux sont les protocoles qui s'y sont consacrés. Cependant, ces mécanismes sont victimes de leur succès. En effet, les attaquants peuvent se servir de ces mécanismes pour engendrer une multitude d'attaques internes. Ces attaques ont la possibilité de détourner le processus d'attribution des valeurs de réputation, de fausser les résultats de calcul de la confiance, de nuire aux nœuds légitimes du réseau, de promouvoir la réputation des nœuds malicieux et ainsi déstabiliser le réseau de capteurs. On compte parmi ces attaques: les attaques de recommandations malhonnêtes, l'attaque on/off, l'attaque de comportement conflictuel, etc. La conception d'un protocole de confiance et de réputation efficace doit donc non seulement tenir compte des nombreuses attaques dans il peut être victime mais aussi prendre en considération les contraintes imposées par les réseaux de capteurs en termes d'énergie, de mémoire et de puissance de calcul.

Les attaques de recommandations malhonnêtes sont parmi les attaques les plus dangereuses. En englobant les attaques badmouthing, ballot-stuffing et collusion, elles tentent de causer un maximum de dégâts pour les RCSFs. Plusieurs recherches se sont intéressées à ces attaques et de nombreux protocoles en ont résulté. Les solutions proposées sont classifiées en deux principales catégories: les algorithmes de prévention et les algorithmes de détection. D'un côté, la résistance des méthodes de prévention contre les attaques de recommandations malhonnêtes fait face à d'importantes restrictions imposées sur le fonctionnement du réseau de capteurs. D'un autre côté, les méthodes de détection à base de facteurs de confiance offrent une grande résistance à ce type d'attaque à condition de choisir les bons facteurs. Des solutions émergentes combinant entre les mécanismes de confiance et de réputation et des axes innovants tels que les méta-heuristiques ou bien la théorie des jeux semblent être de bonnes initiatives.

Dans le prochain chapitre, nous allons proposer un nouveau protocole nommé Bee-Trust Scheme (BTS). Le protocole BTS est un protocole bio inspiré permettant de résoudre le problème des attaques de recommandations malhonnêtes dans les réseaux de capteurs mobiles.

DEUXIÈME PARTIE :

LES CONTRIBUTIONS À LA RECHERCHE

"Vous n'en avez pas fait assez, vous n'en avez jamais fait assez,
tant qu'il existe encore une chose à laquelle vous pouvez contribuer"

Dag Hammarskjöld.

CHAPITRE IV

Première contribution :

Protocole de Détection des Attaques de Recommandations Malhonnêtes dans les Réseaux de Capteurs sans Fil

Sommaire

1. INTRODUCTION

La détection des attaques dites "attaques de recommandations malhonnêtes" reste parmi les principales préoccupations lors de l'utilisation des mécanismes de confiance et de réputation dans les RCSFs. En effet, les attaques de recommandations malhonnêtes incluant les attaques bad-mouthing, ballot-stuffing et collusion attaques représentent une menace réelle pour la stabilité et l'efficacité de ces derniers. Dans ce chapitre, nous présentons notre première contribution *nommée Bee-Trust Scheme (BTS)* (Khedim et al., 2018),qui résout le problème des recommandations malhonnêtes sous un nouvel angle en s'inspirant du modèle naturel du comportement des abeilles mellifères « Apis melifera »lors de la recherche de leur nourriture. En appliquant le principe de "*la survie du plus fort*", la qualité (fitness) de chaque solution est évaluée selon deux concepts : une révision du modèle de nuage (cloud model) ainsi qu'un paramètre de chronométrie cognitive.

2. MOTIVATIONS

Comme souligné dans le chapitre précédent, la majeure partie des protocoles de détection des attaques de recommandations malhonnêtes se basent sur l'utilisation des méthodes de détection à base de déviation. Ces méthodes classées en deux catégories principales, à savoir, celles utilisant *les mesures de similarité majoritaires* et celles utilisant *les mesures de similarité personnalisées* sont inefficaces pour plusieurs raisons. D'une part, la présence d'un nombre important d'attaquants fait que les recommandations malhonnêtes soient majoritaires dans le réseau induisant ainsi le système de détection en erreur. D'autre part, ces méthodes sont inefficaces face aux attaquants intelligents qui introduisent une petite déviation dans les recommandations afin de rester indétectables. Un autre inconvénient souvent omis de ces méthodes c'est qu'elles ne font aucune distinction entre les recommandations *malhonnêtes* et les recommandations *erronées* pourtant bien présentes dans des réseaux tels que les RCSFs. Compte tenu des limites des méthodes classiques, il devient primordial de proposer de nouvelles solutions qui vont venir compléter les méthodes à base de déviation afin de renforcer la détection des attaques de recommandations malhonnêtes tout en réduisant les taux élevés de faux positifs et de faux négatifs engendrés par ces dernières.

Dans ce qui suit, nous allons présenter notre protocole Bee-Trust Scheme (BTS) qui est un protocole bio inspiré, combinant à la fois l'intelligence des colonies d'abeilles en utilisant certains principes de l'algorithme *Artificial Bee Colony* (ABC), tout en faisant appel à des

paramètres innovants tels que l'utilisation d'une révision du modèle de nuage « cloud model » et d'un paramètre s'inspirant de la chronométrie cognitive.

3. L'INTELLIGENCE PAR ESSAIM-LES ABEILLES

Les algorithmes basés sur l'intelligence par essaim constituent une nouvelle branche d'algorithmes s'inspirant du comportement collectif de certaines espèces. L'étude du comportement des colonies d'insectes sociaux, telles que les fourmis, les abeilles, les guêpes, etc. ainsi que celui des bancs de poissons et des groupes d'oiseaux, a permis le développement de nouveaux algorithmes appelés "méta-heuristiques". Ces méta-heuristiques ont permis la résolution d'une multitude de problèmes d'optimisation. De plus en plus étudiés que ce soit en informatique aussi bien qu'en robotique, les phénomènes d'intelligence par essaim rendent l'élaboration de systèmes plus autonomes et plus flexibles se basant sur des interactions simples chose possible. Parmi les algorithmes d'optimisation inspirés de l'intelligence par essaim les plus populaires, nous citons l'optimisation par colonies d'abeilles.

Les abeilles sont connues comme de merveilleux insectes sociaux capables d'accomplir des tâches fascinantes. Ces insectes sont les pollinisateurs les plus importants sur terre et sont une source de matériaux diététiques, nutritifs et naturels pour la consommation humaine depuis l'Antiquité (Crane et al., 1980).Le comportement auto-organisé et collectif des abeilles leur permet d'accomplir une variété de tâches complexes qui ne sont pas réalisables par la multitude d'insectes solitaires. Le butinage est l'une des principales activités de la vie d'une colonie d'abeilles qui attire les chercheurs dans la conception d'algorithmes d'optimisation (Xing and Gao, 2014). Ce comportement est resté mystérieux jusqu'à ce que Von Frisch (1974) décode le langage de la danse des abeilles.

Le mécanisme de recherche de nourriture chez les colonies d'abeilles mellifères est utilisé comme source d'inspiration dans l'élaboration de notre protocole, dans le but de tirer parti de l'intelligence collective de ces insectes.

3.1. Recherche de nourriture chez les abeilles mellifères

L'un des principaux composants comportementaux des sociétés d'insectes sociaux, avec une prise de décision intelligente dans des environnements complexes et imprévisibles, est le comportement de recherche de nourriture (Tereshko and Lee, 2002).Les comportements de recherche de nourriture des abeilles mellifères (Apis mellifera) représentent le lien entre la colonie d'abeilles mellifères et l'environnement ambiant. Selon les ressources collectées, l'activité de butinage est classée comme nectar, eau, pollen ou butinage de la résine (Picard-

Nizou et al., 1995). Ces différentes ressources permettent de fournir la nutrition nécessaire à l'ensemble de la colonie. Le processus de recherche de nourriture comprend deux principaux modes de comportement : le recrutement de nouvelles sources de nectar et l'abandon d'une source (Tereshko and Lee, 2002). Le processus commence lorsque les ouvrières quittent leur nid pour chercher une source de nourriture. Quand une abeille trouve de la nourriture (des fleurs), elle retourne à la ruche et transmet l'information sur la source de nectar (distance de la ruche, quantité et qualité du nectar) en utilisant un ensemble de danses frétillantes connues sous le nom de *«waggle dance»*. Les autres abeilles dans le nid regardent la danse pour déterminer la rentabilité de la source de nourriture. Au bout d'un certain temps, plus d'abeilles butineuses quitteront la ruche afin de collecter le nectar de la source sélectionnée.

3.2. L'optimisation par colonies d'abeilles

L'algorithme de colonie d'abeilles artificielles (ABC : Artificial Bee Colony) proposé dans (Karaboga andBasturk, 2007) est l'un des algorithmes d'optimisation d'inspiration biologique les plus populaires. Il s'agit d'une classe de techniques de l'intelligence par essaims qui imitent le comportement de recherche de nourriture intelligente (comme l'exploration, l'exploitation, le recrutement et l'abandon) chez les colonies d'abeilles mellifères. L'excellente capacité d'optimisation globale ainsi que la facilité de mise en œuvre ont permis à l'algorithme ABC d'attirer l'attention des chercheurs et d'être ainsi appliqué à divers domaines.

Typiquement, la colonie d'abeilles artificielles de l'algorithme ABC est composée de trois types d'abeilles, à savoir, les abeilles ouvrières, les abeilles spectatrices et les abeilles scoutes. Ces trois groupes sont donnés ci-dessous :

- ***Les abeilles ouvrières :*** Ces abeilles sont responsables de l'exploitation des sources de nectar et du partage d'informations avec les autres abeilles qui attendent dans la ruche à travers la *« waggle dance »*. Dans l'algorithme ABC, une abeille ouvrière est affectée à chaque source de nourriture. Par conséquent, le nombre d'abeilles ouvrières est égal au nombre de sources de nourriture autour de la ruche (Karaboga and Basturk, 2007; Ari et al., 2018).
- ***Les abeilles spectatrices :*** Ces abeilles attendent au champ de danse pour obtenir des informations sur les sources de nourriture. Une abeille spectatrice prend la décision de choisir une source de nourriture plutôt qu'une autre, en fonction des informations partagées par les abeilles ouvrières. Plus la quantité de nectar est grande, plus la probabilité de sélectionner la source est grande aussi.

- ***Les abeilles scoutes :*** Ces abeilles exploitent l'environnement autour du nid, en lançant une recherche aléatoire afin de trouver de nouvelles sources de nourriture. L'abeille ouvrière dont la source de nourriture est épuisée devient une abeille scoute.

En conséquence, le processus de recherche peut être divisé en trois étapes : les abeilles ouvrières sont envoyées aux sources de nourriture afin de mesurer leurs quantités de nectar. Ensuite, les abeilles spectatrices recueillent les informations sur les sources de nectar trouvées par les abeilles ouvrières, choisissent les sources de nourriture et déterminent la quantité de nectar. Enfin, les abeilles scoutes sont sélectionnées puis envoyées pour découvrir de nouvelles sources de nourriture.

Les principales étapes de l'algorithme ABC sont données dans l'Algorithme 1. Ci-dessous (Karaboga and Basturk, 2007) :

Algorithme 1. Pseudo-code de l'algorithme ABC

```
Initialiser les valeurs de départ
RÉPÉTER
    Placez les abeilles ouvrières sur les sources de nourriture en mémoire;
    Placez les abeilles spectatrices sur les sources de nourriture en mémoire;
    Envoyez les abeilles scoutes à la zone de recherche pour découvrir de nouvelles sources de nourriture;
JUSQU'À (les conditions soient remplies)
```

4. MODÈLE DU SYSTÈME

Dans cette section, nous spécifions les hypothèses concernant le réseau, le modèle de l'attaquant ainsi que le vocabulaire utilisé.

4.1. Modèle du réseau

Nous supposons que le réseau de capteurs sans fil (RCSF) est hautement dynamique, ce qui peut être dû à la mobilité des nœuds, à l'environnement, aussi bien qu'aux changements de comportements des nœuds (Chen et al., 2012). Le réseau suit une architecture plate. L'identité de chaque nœud est unique et stable. De plus, chaque nœud connaît son propre emplacement (par exemple, en utilisant un GPS ou un algorithme de localisation). Un mécanisme de réputation est appliqué dans le réseau afin d'évaluer les interactions entre nœuds voisins, telles

que la réception, l'envoi, la livraison et la cohérence des paquets. Les interactions sont donc classées comme négatives ou bien positives selon la qualité du service fourni.

4.2. Modèle de l'attaquant

Dans cet article, un attaquant est supposé être un nœud propageant incorrectement des recommandations avec une intention malhonnête. Nous définissons un recommandeur malhonnête (mauvais recommandeur) comme étant un nœud qui réduit volontairement la réputation positive d'un bon nœud et/ou augmente la réputation négative d'un mauvais. Inversement, un nœud qui propage correctement les recommandations est défini comme étant un recommandeur honnête (bon recommandeur). En outre, nous supposons dans notre protocole, que le nombre de recommandeurs malhonnêtes est inférieur ou égal au nombre de recommandeurs honnêtes.

Dans ce qui suit, nous allons décrire les principaux symboles et notations utilisés dans notre protocole. Le Tableau 4.1 donne les notations considérées.

Tableau 4. 1. Notations

Symbole	Signification
S	Nœud évaluateur
X	Nœud à évalué
N	Nombre de recommandeurs
M	Nombre de recommandations
U	L'ensemble des recommandations reçues
n	Nombre des recommandations reçues
ABC	Artificiel Bee Colony
SBM	Scout Bees Module
EBM	Employed Bees Module
OBM	Onlookers Bees Module
TH	Throughput
RP	Recognition Percentage (Pourcentage de recognition)
FPP	False Positive Percentage (Pourcentage de faux positifs)
FNP	False Negative Percentage (Pourcentage de faux négatifs)

5. PROTOCOLE PROPOSÉ

Dans cette section, nous allons présenter notre protocole de détection des attaques de recommandations malhonnêtes dans les RCSFs nommé Bee-Trust Scheme (BTS). Nous commencerons par donner une description générale du protocole. Ensuite, les différents modules seront présentés et expliqués.

5.1. Description générale

Les recommandations malhonnêtes sont souvent considérées comme un problème difficile et insoluble (Zouridaki et al., 2009). Proposer une solution innovante et efficace est devenue une nécessité absolue. Notre protocole BTS résout le problème des recommandations malhonnêtes sous un nouvel angle. En effet, BTS est basé sur une nouvelle architecture s'inspirant du comportement de recherche de nourriture de l'essaim d'abeilles. Notre solution utilise certaines caractéristiques de l'algorithme d'optimisation par colonies d'abeilles artificielles (ABC) afin de tirer parti de l'intelligence collective émergeant des abeilles dans le filtrage des recommandations. BTS fait appel aux quatre composantes principales de l'algorithme ABC, à savoir, les sources de nourriture, les abeilles ouvrières, les abeilles spectatrices et les abeilles scoutes pour bénéficier de leurs avantages en termes d'exploitation et d'exploration.

La comparaison entre les principaux composants de notre protocole BTS par rapport à l'algorithme initial ABC ainsi que la cartographie du problème sont donnés dans la figure.4.1 et le Tableau 4.2 respectivement.

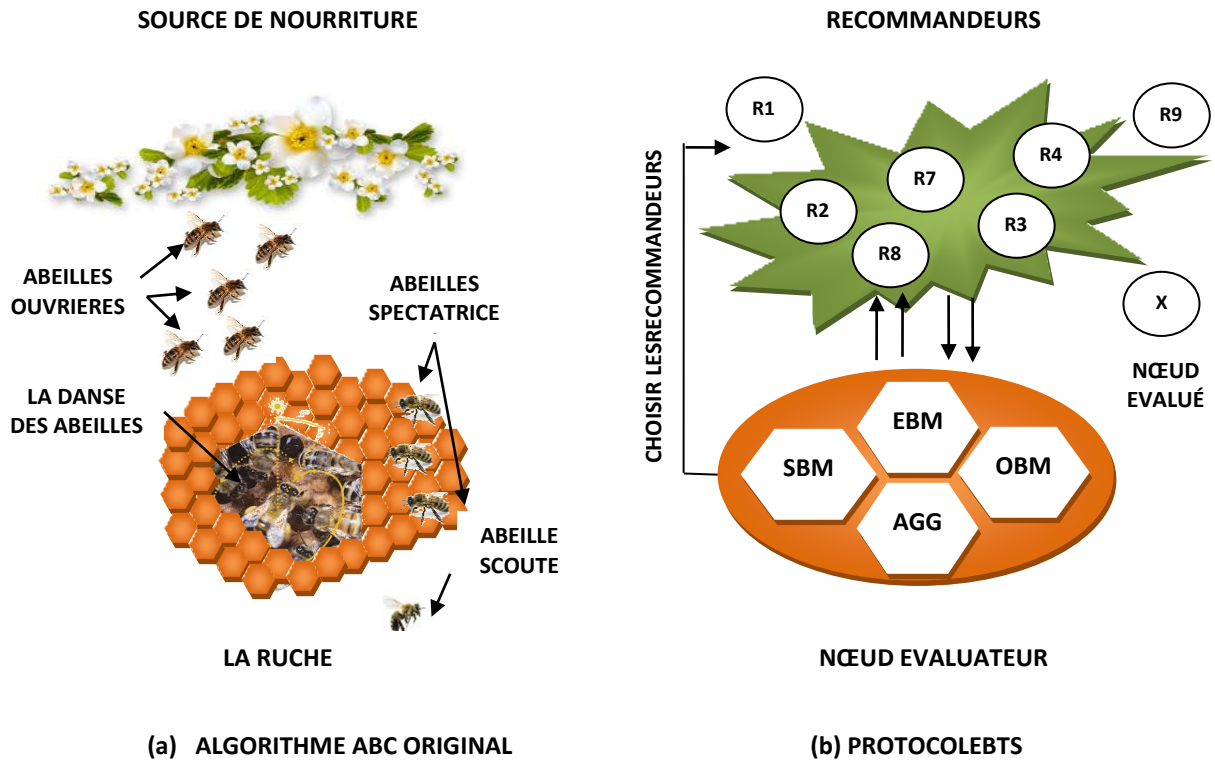


Fig 4. 1. Comparaison entre le protocole Bee-Trust Scheme et le protocole ABC

Dans notre état de l'art, nous avons souligné que le fait de se baser uniquement sur les valeurs de recommandations comme moyen de détection cause inévitablement des taux élevés de faux positifs et de faux négatifs. En effet, ces valeurs de recommandations peuvent être trompeuses si les attaquants sont nombreux ou bien intelligents. Afin de minimiser ces taux et maximiser ainsi le taux de détection des recommandations malhonnêtes, nous proposons dans notre protocole une nouvelle approche de détection. Notre solution s'intéresse au caractère malhonnête des recommandeurs ayant émis les recommandations. Il va sans dire que les recommandations malhonnêtes sont émises par des nœuds malveillants, donc, divulguer le caractère insidieux du recommandeur va nous permettre d'éviter toute échappatoire à de telles attaques.

Les recommandeurs malhonnêtes sont considérés comme la source de l'attaque; ils augmentent ou diminuent intentionnellement la réputation des nœuds en fonction de leurs besoins malveillants. Notre approche consiste à faire appel à une fonction multi-objectif. Cette fonction que nous allons appeler "multi objective fitness function" permet de mesurer la qualité "*fitness"* des recommandeurs. Afin d'exprimer cette fonction nous allons utiliser l'approche de la somme pondérée faisant appel à deux paramètres principaux. Premièrement, un facteur de détection basé sur une révision du modèle de nuage afin de détecter les recommandations malhonnêtes. Deuxièmement, un paramètre de chronométrie cognitive basé sur le calcul de la vitesse de réponse afin de détecter les recommandeurs malhonnêtes.

Le protocole Bee-Trust fonctionne comme suit : lorsqu'un nœud "S" veut évaluer la réputation d'un nœud désiré "X", il demande des recommandations aux recommandeurs "R_i" appartenant à son voisinage selon les principales étapes suivantes : Premièrement, les recommandeurs sont choisis parmi les voisins à un seul saut ayants les valeurs de réputations les plus élevées. Ces valeurs sont obtenues grâce aux observations directes *"first-hand information"* par le module Scouts Bees (SBM). Ces observations sont mises à jour après chaque interaction.

Deuxièmement, le module Employed Bees (EBM) envoie les abeilles ouvrières pour demander les recommandations du nœud "X" auprès des recommandeurs "R_i". La qualité "fitness" de chaque recommandeur est ensuite calculée en utilisant la "multi objective fitness function" proposée dans l'équation 16.

Sur la base des informations de fitness obtenues, le module Onlooker Bees Module (OBM) choisit les sources de nourriture les plus rentables.

En appliquant le principe de "la survie du plus fort", les recommandeurs ayant une valeur de *fitness* inférieure à un seuil fixé sont donc considérés comme malhonnêtes et sont ajoutés à

une liste noire. Cette liste est détenue par chaque nœud respectivement et aide ce nœud lorsqu'il agit en tant que nœud évaluateur. Les nœuds mis en liste noire ne peuvent plus être choisis comme recommandeurs durant tout le déroulement du protocole.

Les valeurs de recommandations des recommandeurs ayant des valeurs de *fitness* élevées sont ensuite agrégées afin de constituer la réputation indirecte du nœud "X".

Tableau 4. 2. Correspondance

ABC	BTS
Source de nourriture	Recommandeurs
Ruche	Nœud évaluateur
Abeille ouvrière	Employed Bees Module (EBM)
Abeille spectatrice	Onlooker Bees Module (OBM)
Abeille scoute	Scout Bees Module (SBM)
Recherche de nourriture	Demande de recommandations

5.2.Scout Bees Module (SBM)

Contrairement à l'algorithme ABC, le module SBM proposé n'effectue pas de recherche aléatoire pour identifier les sources potentielles, mais s'appuie sur les informations directes "first-hand" conservées par le nœud évaluateur sur ses voisins direct à un saut. Les recommandeurs sont choisis parmi les voisins à un saut avec les plus hautes valeurs de réputation. Dans notre modèle, choisir les recommandeurs parmi les voisins directs va permettre moins de traitement, moins de consommation de l'espace mémoire et moins de consommation d'énergie étant donné que le nœud évaluateur n'a pas besoin de conserver les informations de confiance de tous les nœuds du réseau mais d'uniquement les informations de leurs voisins (Labraoui et al., 2016). De toute évidence, le calcul du "first-hand" est à l'abri d'une attaque de recommandation malhonnête (Chen et al., 2012) étant donné qu'il ne fait pas appel à un tiers avis. Son calcul peut être réalisé grâce à plusieurs algorithmes classiques. Nous avons choisis d'utiliser l'évaluation directe de la confiance proposée par (Labraoui et al., 2016). Dans ce protocole, une gestion de confiance basée sur la réputation et tenant compte des risques est proposée pour les RCSFs. L'évaluation de la confiance directe est basée sur le concept de : "*la confiance est difficile à acquérir et facile à perdre"*. L'évaluation locale du nœud i pour le nœud j $LR_{i,j}^{k}$ pendant l'unité de temps $t_k(n \geq k \geq 1)$ est définie dans l'équation (1) comme suit :

$$LR_{i,j}^{t_k} = \left(\frac{S_{i,j}^{t_k}}{S_{i,j}^{t_k} + U_{i,j}^{t_k}}\right) * \left(1 - \frac{1}{S_{i,j}^{t_k} + 1}\right) \quad (1)$$

Où : $S_{i,j}^{tk}$ (resp. $U_{i,j}^{tk}$) est le nombre total des interactions réussies (resp. infructueuses) du nœud i avec le nœud j pendant l'unité de temps t_k.

Contrairement à la conventionnelle bêta réputation, un facteur d'équilibrage est introduit pour s'assurer que la valeur de confiance augmente lentement lorsque le nombre d'interactions infructueuses est considérablement élevé. Comme les comportements des nœuds peuvent changer de temps en temps, un facteur temps est utilisé afin d'apporter plus de poids aux actions récentes du nœud sans pour autant oublier ces derniers comportements. La valeur de confiance directe $DT_{i,j}$ est donc calculée selon la formule suivante :

$$DT_{i,j} = \frac{\lambda}{\lambda+1} \times \frac{\sum_{tk=1}^{n-1} LR_{i,j}^{t_k}}{n-1} + \frac{1}{\lambda+1} \times LR_{i,j}^{t_N} \quad (2)$$

Où : λ ($0<\lambda<1$) est le facteur de désintégration "*decay factor"* utilisé pour s'assurer que les comportements les plus récents auront plus de poids lors du calcul de la valeur de confiance directe finale. Par conséquent, la valeur de confiance directe reflète l'état du comportement le plus récent d'un nœud sans oublier aucun comportement passé.

5.3. Employed Bees Module (EBM)

Dans notre protocole Bee-Trust, le module EBM est responsable de deux tâches principales: la demande de recommandations et la dérivation de la fonction Fitness.

5.3.1. Demande de recommandations

Dans un modèle de confiance et de réputation, lorsqu'un nœud S veut évaluer la réputation d'un nœud désiré "X", il demande des recommandations auprès des recommandeurs R_i (i = 1..n) sélectionnés par le module SBM. Cette demande de recommandations va se faire par l'envoi d'un ensemble d'abeilles ouvrières. Comme dans l'algorithme ABC, le nombre d'abeilles ouvrières envoyées est égal au nombre de recommandeurs. Par conséquent, chaque abeille ouvrière sera en charge d'un recommandeur. Chaque recommandeur R_i doit transmettre à l'abeille ouvrière qui lui est affectée ses propres données, à savoir son identifiant (ID), sa position, son journal des logs correspondant à ses interactions avec le nœud évalué "X" ainsi que la valeur de réputation attribuée au nœud X ($R_{i,x}$).

Contrairement à la plupart des protocoles (Chen et al., 2012; Dellarocas,2000; Zouridaki et al., 2009; Buchegger and Boudec, 2004; Srinivasan et al., 2006; Hur et al., 2005; Zahariadis et al., 2010; Babu et al., 2014;Whitby et al., 2004) évaluant les réputations comme honnêtes ou malhonnêtes, notre protocole franchit une étape supplémentaire en considérant également les

recommandations erronées afin de palier au problème des faux positifs et faux négatifs. Ainsi, la transmission de l'historique des échanges entre le recommandeur et le nœud évalué est une des solutions proposées. Les informations contenues dans les logs vont permettre de vérifier la véracité de la valeur de réputation attribuée, ainsi que d'avoir une preuve tangible sur l'honnêteté ou la malhonnêteté de chaque recommandeur.

Les principales étapes de la procédure d'envoi des informations de chaque recommandeur sont données dans l'algorithme suivant (Algorithme 2).

Algorithme 2. Procédure d'envoi des informations

```
Début
Données
        Ri {identifiant du recommandeur i}
        Pos_Ri^t {position de Ri à l'instant t}
        History_Ri,x^t {L'historique des échanges entre Ri et le nœud évalué x
        jusqu'à l'instant t}
        Rep_Ri,x {la réputation assignée par Ri à x}

        pck.id ← Ri;
        pck.pos ← pos_Ri^t;
        pck.history ← history_Ri,x^t;
        pck.rep ← rep_Ri,x;
        Envoyer (pck);
Fin
```

5.3.2. Dérivation de la fonction Fitness

Dès que les abeilles ouvrières reviennent au nœud évaluateur, le module EBM va se charger d'analyser les informations contenues dans chaque message afin d'évaluer respectivement chaque recommandeur. En utilisant le principe de "la survie du plus fort" les recommandeurs avec les plus faibles valeurs de fitness sont déclarés comme malhonnêtes. Pour cela, nous faisons appel à une fonction multi-objectif. Nous considérons deux paramètres d'optimisation dans le calcul de cette fonction : une détection des réputations malhonnêtes basée sur une révision de la théorie du modèle de nuage (Deyi et al., 1995) et d'un paramètre de chronométrie cognitive utilisant comme indice la vitesse de réponse du recommandeur. La première contrainte à respecter est la minimisation de l'écart des réputations f^{RD}. En effet, cela a pour but de rejeter les recommandations qui s'écartent de l'opinion majoritaire et d'améliorer ainsi l'exactitude de notre protocole. De ce fait, une modification du modèle de nuage est appliquée pour gérer les incertitudes dans le domaine des recommandations. Une contrainte supplémentaire est la détection des recommandeurs

malhonnêtes en minimisant f^{lying} grâce à un paramètre inspiré de la chronométrie cognitive. Cette approche supplémentaire permet d'apporter non seulement un mécanisme de correction à d'éventuels faux positifs ou faux négatifs générés par le f^{RD}, mais offre en plus un moyen efficace de différencier entre les recommandations malhonnêtes et les recommandations erronées.

La représentation mathématique des paramètres d'optimisation est donnée dans ce qui suit :

a. Cloud model « Modèle de nuages »

Le système de confiance et de réputation permet à un nœud d'évaluer un autre nœud, à la fois positivement et négativement. Il n'est pas réaliste de confirmer que les nœuds recommandeurs dans les RCSFs sont honnêtes dans chaque recommandation attribuée. Dans la plupart des cas, il n'y a aucune garantie, principalement en raison de l'environnement hostile et sans surveillance dans lequel les capteurs sont déployés ainsi que de la nature malveillante et imprévisible des attaquants. Par conséquent, la détection des recommandations malhonnêtes est considérée comme un problème difficile et insoluble.

Nous présentons ici un mécanisme de détection de déviation basé sur un nouveau modèle hybride intégrant l'aléatoire et le flou pour la détection des recommandations malhonnêtes. Notre algorithme de filtrage utilise une théorie révisée du modèle de nuage afin de mesurer l'écart d'une recommandation reçue par rapport à une distribution de recommandations normales.

Le "modèle de nuage" connu sous le nom de *"cloud model"* introduit par le professeur Li dans (Deyi et al., 1995) est un nouveau modèle de cognition basé sur la conversion entre le concept qualitatif et les données quantitatives. Le modèle de nuages s'avère être un outil efficace pour l'exploration des données et dans la résolution des incertitudes.

Il se compose de trois caractéristiques numériques qui sont : *l'espérance E_x, l'entropie E_n et l'hyper-entropie H_e*. E_x est la mesure de la certitude qui représente le concept qualitatif; c'est la valeur attendue des gouttes de nuages. E_n représente l'entropie de l'attribut, elle reflète l'ambiguïté de E_x. Elle peut être également considérée comme la mesure de l'incertitude des concepts qualitatifs. H_e est l'hyper entropie de l'attribut, à savoir l'entropie de l'entropie, permettant de mesurer l'incertitude de l'entropie E_n.

Le modèle de nuage peut être généré par un générateur de nuages, qui est un outil de base faisant la transformation entre les concepts qualitatifs et les données quantitatives. Le générateur de nuage vers l'avant et le générateur de nuages vers l'arrière sont deux des algorithmes les plus basiques du générateur de nuages (Deyi et al., 1995). Le générateur de

nuage vers l'avant transforme un concept qualitatif avec trois caractères numériques E_x, E_n et H_e en un certain nombre de gouttes de nuages et de leurs degrés de certitude correspondants. Par contre, le générateur de nuages vers l'arrière transforme un certain nombre de gouttes de nuages sous la forme des trois caractéristiques numériques du nuage. Les générateurs de nuages avant et arrière sont représentés dans la Figure.4.2.

Dans les protocoles de détection des recommandations malhonnêtes traditionnelles, le nombre d'attaquants est supposé être inférieur ou égal à la moitié du nombre total de recommandeurs. Toutefois, le modèle de nuages original ne peut pas être appliqué lorsque le nombre de recommandeurs malhonnêtes est supérieur au quart du nombre total de recommandeurs. Afin d'équilibrer la contrainte du nombre d'attaquants dans notre mécanisme, nous proposons une révision de la formule de l'hyper entropie, de sorte que le nombre d'attaquants pris en compte dans notre mécanisme soit le même que celui des protocoles de détection traditionnels.

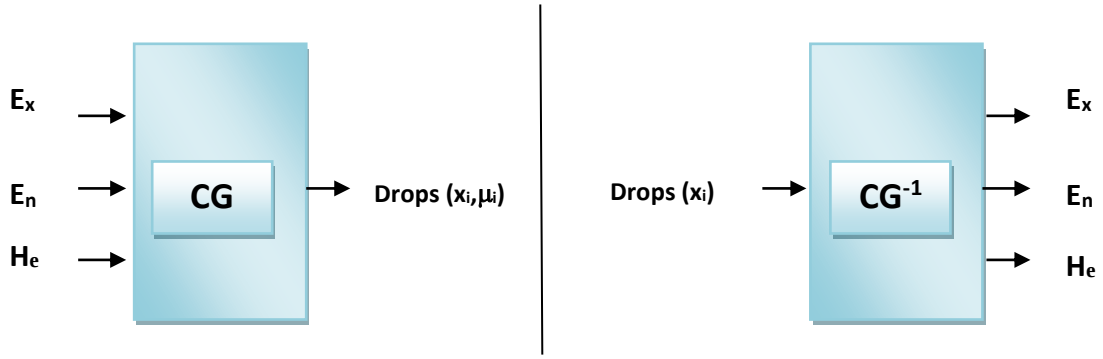


Fig 4. 2. Générateur de nuages vers l'avant (CG) et Générateur de nuages arrière (CG-1)

Notre algorithme de filtrage utilisant le modèle de nuage révisé suit deux étapes principales : (1) le calcul des caractéristiques du modèle de nuages normal et (2) le calcul du degré de certitude.

1) Pour calculer les caractéristique du modèle de nuages normal, l'algorithme de nuages arrière est appliqué afin d'obtenir les trois caractéristiques numériques du nuage C = (E_x, E_n, H_e) de l'ensemble U. Où, U est supposé être l'ensemble des recommandations envoyées par les recommandeurs et reçues par le nœud évaluateur avec : U = {x_1, x_2, ..., x_m}, $x_i \in$ U est une des recommandations reçues, m≤n et C est un concept qualitatif de U. Le calcul des caractéristiques du modèle de nuages normal est le suivant :

Étape 1. Entrer les données normales; calculer la moyenne $\bar{X}$ et la variance S^2,

$$\bar{X} = \frac{1}{m}\sum_{i=1}^{m} x_i \quad (3)$$

$$S^2 = \frac{1}{m-1}\sum_{i=1}^{m}(\bar{X} - x_i)^2 \quad (4)$$

Étape 2. Calculer E_x,

$$E_X = \bar{X} \quad (5)$$

Étape 3. Calculer E_n,

$$E_n = \sqrt{\frac{\pi}{2}} * \frac{1}{m}\sum_{i=1}^{m}|E_x - x_i| \quad (6)$$

Étape 4. Calculer H_e,

$$H_e = \sqrt{|S^2 - E_n^2|} \quad (7)$$

2) Pour calculer le degré de certitude, l'algorithme de nuage avant est appliqué. CG va d'abord utiliser les trois caractéristiques numériques du nuage C = (E_x, E_n, H_e) afin de calculer le degré de certitude. Deuxièmement, en fonction de la valeur obtenue, un facteur de déviation est calculé afin d'estimer l'écart entre chaque recommandation et le modèle de nuage normal. Le processus suit les étapes suivantes :

Étape 1. Générer un modèle de nuage normal basé sur l'entropie et l'hyper entropie d'un nombre aléatoire,

$$E_n' = NormalRandom(E_n, H_e) \quad (8)$$

Où : NormalRandom est un nombre aléatoire généré à partir de la distribution normale avec les paramètres E_n et H_e.

Étape 2. Calculer le degré de certitude correspondant à chaque recommandation x_i,

$$\mu_{x_i} = e^{-\frac{(x_i - E_x)^2}{2(E_n')^2}} \quad (9)$$

Étape 3. Calculer le facteur de déviation par rapport à chaque recommandation x_i,

$$\sigma_{x_i} = 1 - \mu_{x_i} \quad (10)$$

Par conséquent, nous définissons le critère de déviation des réputations de la fonction de fitness f^{RD} comme suit :

$$f_{Ri}^{RD} = \sigma_{x_i} \quad (11)$$

Avec : R_i un recommandeur et x_i est sa recommandation.

b. Indice de la vitesse de réponse

Bien que le modèle de nuages soit une approche efficace pour la détection des recommandations malhonnêtes, le fait qu'il soit basé sur une approche ressemblant à celle utilisées dans les techniques de "mesure de similarités majoritaires (MSM)" peut dans certains cas engendrer des confusions. Deux situations problématiques peuvent se distinguer : Premièrement, l'incapacité du modèle de nuages de discriminer entre les recommandations honnêtes et malhonnêtes lorsque l'ensemble des recommandations est auto-contradictoire.

Afin d'apprécier ce fait, considérons un petit exemple de n=6 recommandations reçues ayants les valeurs suivantes 0.3, 0.29, 0.3, 0.8, 0.8 et 0.8. La moitié des recommandations indiquent que la valeur de réputation du nœud évalué est proche de 0.3, tandis que la moitié restante indique que la valeur de réputation devrait être de 0.8. En appliquant le modèle de nuage révisé, l'espérance E_x est de 0.5483, l'entropie E_n est de 0.3146 et l'hyper entropie H_e est 0.1515. Par conséquent, les degrés de certitude des recommandations reçues sont : μ (0.3)=0.85, μ (0.29)=0.844 et μ (0.8) = 0.85 respectivement. La similitude entre ces valeurs et l'absence d'informations supplémentaires ne permettent pas au modèle de prendre une décision concernant ces recommandations. Deuxièmement, le modèle peut générer des faux positifs et des faux négatifs. Afin d'apprécier ce fait, nous considérons un autre petit ensemble de n=6 recommandations reçues avec des valeurs de 0.2, 0.25, 0.8, 0.8, 0.79 et 0.8. Nous avons le cas de figure suivant : la première recommandation (0.2) est un calcul de réputation erroné en raison d'une mauvaise communication de canal entre un recommandeur honnête et le nœud évalué. La deuxième recommandation (0.25) est en revanche une valeur aberrante générée par un recommandeur malhonnête. Les valeurs des caractéristiques du modèle de nuage sont : l'espérance E_x est de 0.6067, l'entropie E_n est de 0.3181 et l'hyper entropie H_e est de 0.1162. Par conséquent, les degrés de certitude des recommandations reçues sont : μ (0,2) = 0.56, μ (0.25) = 0.64, μ (0.8) = 0.87 et μ (0.79) = 0.89. L'absence de distinction entre les recommandations erronées et malhonnêtes a conduit à juger injustement des bons recommandeurs comme étant malhonnêtes.

Un protocole de détection des recommandations malhonnêtes efficace doit pouvoir faire la distinction entre le mensonge et la vérité, non seulement sur le plan statistique mais aussi sur

le plan sensitif (Gregg, et al., 2014). Nous introduisons dans ce qui suit un mécanisme de correction basé sur l'indice de vitesse de réponse.

Notre indice de vitesse de réponse est inspiré du TARA *"The Timed Antagonistic Response Alethiometer*". Le TARA est une tâche de classification informatisée (Gregg et al., 2007). C'est une technique permettant de diagnostiquer le mensonge. TARA met en place une situation artificielle dans laquelle les répondants disant la vérité sont capables de compléter une série de classifications compatibles plus facilement que les menteurs qui sont obligés de compléter une série de classifications incompatibles. De toute évidence, le deuxième cas est plus difficile à accomplir que le premier. Par conséquent, les réponses des répondants malhonnêtes sont plus lentes que celles des répondants honnêtes pour atteindre un niveau d'exactitude équivalent (Gregg et al., 2007).

Quand un RCSF est attaqué, les nœuds malveillants utilisent différentes stratégies pour rester indétectables. Les capteurs peuvent mentir à propos de leur position et annoncer de fausses localisations à leurs voisins, comme c'est le cas dans l'attaque "black hole"(Tseng et al., 2011). De plus, ils peuvent mentir sur leur identité, comme c'est le cas dans l'attaque "sybil" (Levine et al., 2006). Lors des attaques de recommandations malhonnêtes, les recommandeurs malveillants vont mentir sur la valeur de réputation attribuée au nœud évalué, en envoyant des recommandations faussées et malhonnêtes au nœud évaluateur. Dans notre protocole BTS, les recommandeurs doivent obligatoirement transmettre l'historique des échanges (les logs) qui ont conduit à leur jugement concernant la valeur de réputation. Alors qu'un recommandeur honnête n'a qu'à envoyer une copie du journal de ses échanges, associée à la valeur de réputation correspondante, mentir pour les recommandeurs malhonnêtes implique en plus des modifications dans les informations envoyées. La divergence entre les informations contenues dans le fichier journal et la valeur de réputation attribuée engendre une situation d'incompatibilité entre les informations contenues dans le fichier log ou bien entre le fichier log et la réputation assignée. Ces tâches incompatibles sont plus difficiles et prennent plus de temps pour se réaliser, par conséquent, des réponses plus lentes révèlent la malhonnêteté (Gregg et al., 2007). Le problème des recommandeurs malhonnêtes est une situation quelque peu similaire à celle utilisée dans TARA.

Des recherches récentes confirment qu'en répondant aux enquêtes directes de manière structurée, les gens mettent plus de temps à mentir qu'à dire la vérité (Gura et al., 2004). En utilisant le même raisonnement, nous présentons la vitesse de réponse comme un indice afin de détecter les recommandations malhonnêtes.

Pour chaque recommandeur, l'indice de vitesse de réponse peut être calculé comme suit :

$$RSI_{R_i} = \frac{D_{tr(S,R_i)}}{RT_{R_i}} \quad (12)$$

Où : RSI_{Ri} est l'indice de vitesse de réponse d'un recommandeur standard R_i, $D_{tr(S, Ri)}$ est la distance parcourue entre le nœud évaluateur S et le recommandeur R_i et RT_{Ri} est le temps de réponse approximatif du nœud R_i.

Le module EBM de notre protocole calcule la distance parcourue $D_{tr(S,Ri)}$entre le nœud évaluateur S auquel il appartient et le recommandeur R_i ayants les coordonnées (X_S^t, Y_S^t) et (X_{Ri}^t, Y_{Ri}^t) à l'instant t respectivement. L'expression de la distance est dérivée du théorème de Pythagore comme suit :

$$D_{tr(S,Ri)} = \sqrt{\left(X_{R_i}^t - X_S^t\right)^2 + \left(Y_{R_i}^t - Y_S^t\right)^2} \quad (13)$$

Pour calculer le temps de réponse approximatif RT_{Ri}, on considère que le temps de propagation est négligeable par rapport au temps de transmission, par conséquent, le temps de transmission entre les nœuds est sélectionné comme temps dominant (Lindsay et al., 2001).On supposera une synchronisation des horloges entre le nœud évaluateur et le recommandeur et pas de mise en file d'attente (Alrashed, 2017 ;Abbasy et al. 2011). Le temps de réponse approximatif du nœud R_i "RT_{Ri}" peut alors être calculé comme étant la différence entre le temps de départ des abeilles ouvrières pour demander les recommandations et leur temps d'arrivée au nœud évaluateur.

Par conséquent, l'expression finale de calcul de l'indice de la vitesse de réponse RSI_{Ri} pour chaque recommandeur R_i est :

$$RSI_{Ri} = \frac{1}{RT_{R_i}} \sqrt{\left(X_{R_i}^t - X_A^t\right)^2 + \left(Y_{R_i}^t - Y_A^t\right)^2} \quad (14)$$

Donc, plus il faut de temps au recommandeur pour modifier les données demandées avant de les envoyer (logs, réputation), plus son temps de réponse est long et plus sa vitesse de réponse est lente aussi. Par conséquent, avec l'augmentation de RT_{Ri}, RSI_{Ri} diminue de manière correspondante.

De ce fait, la fonction f^{lying} du recommandeur R_i est définie comme suit :

$$f_{R_i}^{lying} = \frac{1}{RSI_{R_i}} \quad (15)$$

Nous remarquons que f^{lying} devient minimal lorsque l'indice de vitesse de réponse RSI_{Ri} est maximal.

Nous définissons la fonction multi-objectif de notre problème d'optimisation de telle sorte que la fonction fitness devienne maximale en minimisant la fonction f^{RD} et la fonction f^{lying}. La

stratégie la plus utilisée transformant un problème multi-objectif en un objectif unique est la méthode pondérée. Ainsi, la fonction objectif pour chaque recommandeur R_i fit_{Ri} incluant le paramètre de détection de la déviation des valeurs de réputation, le paramètre de détection du mensonge des recommandeurs et les paramètres de pondération α et β, est définie comme un problème de programmation linéaire comme suit :

$$minimize fit_{R_i} = \alpha \times f_{R_i}^{RD} + \beta \times f_{R_i}^{lying} \quad (16)$$

Soumise aux contraintes données dans les équations (17) et (18) :

$$\alpha = 1 - \beta \quad (17)$$

$$0 < \beta < 1 \quad (18)$$

La forme finale de la fonction fitness de pondération linéaire f_{Ri} correspondante à chaque recommandeur est donnée selon l'algorithme ABC par la formule suivante :

$$f_{R_i} = \frac{1}{1+fit_{R_i}} \quad (19)$$

Où : f_{Ri} indique la valeur de fitness du recommandeur R_i et fit_{Ri} représente sa fonction objective.

5.4. Onlooker Bees module (OBM)

Comme les originales abeilles spectatrices dans l'algorithme ABC, le module OBM fait une classification des recommandeurs en fonction de la valeur de probabilité p_{Ri} associé à chacun d'eux. Cette probabilité est calculée selon l'expression suivante :

$$p_{R_i} = \frac{f_{R_i}}{\sum_{i=1}^{n} f_{R_i}} \quad (20)$$

Où : f_{Ri} est la valeur de fitness du recommandeur R_i évaluée par le module EBM.

Dans le cas où $p_{Ri} < \gamma$ (γ est une valeur seuil), le recommandeur est déclaré malveillant et sa recommandation est jugée comme malhonnête. Les recommandeurs déclarés malhonnêtes sont mis sur liste noire, afin d'éviter qu'ils ne soient choisis comme recommandeurs une autre fois.

5.5. Agrégation des recommandations

Après avoir décrit les principales étapes de notre protocole, nous nous intéressons maintenant à la façon d'obtenir la valeur finale de la réputation du nœud à évaluer X grâce à l'utilisation de l'agrégation des différentes recommandations. Comme nous avons déjà décrit précédemment, quand un nœud veut évaluer la réputation d'un nœud désiré, il demande des recommandations auprès des recommandeurs de son voisinage ayants les plus fortes valeurs de réputation et qui ne sont pas dans la liste noire. Le nombre de recommandeurs est fixé par chaque nœud évaluateur indépendamment, en fonction des besoins de l'application.

Afin de donner plus de poids aux informations fournies par les recommandeurs possédants les plus fortes valeurs de fitness. La réputation indirecte du nœud évalué "x" est calculée en fonction de toutes les recommandations reçues selon l'équation suivante :

$$IR_x = \frac{1}{\sum_{R_i} f_{R_i}} \times \sum_{R_i} (f_{R_i} \times Rep_{R_i,x}) \quad (21)$$

Où : f_{Ri} indique la valeur de fitness du recommandeur R_i et $Rep_{Ri,x}$ est sa valeur de recommandation.

Les principales étapes du protocole proposé Bee-Trust sont données dans l'algorithme suivant (Algorithme 3) :

Algorithme 3. Bee-Trust Scheme

```
Début
        Recevoir-les-recommandations ();
        /* EBM phase*/
            Calculer-la-fonction-fitness selon l'équation (24);
        /*OBM phase */
            Calculer-prob-pRi selon l'équation (25);
            Classifier-recommandeur-Ri en fonction de pRi;
            Mettre-liste-noire-recommandeurs-fitness la plus basse ();
        /* SBM phase */
            Remplacer-plus-faibles-recommandeurs (),
            Mise-à-jour-réputation ();
            Agrégation-réputations ();
Fin
```

6. COÛTS DE COMMUNICATION ET DE STOCKAGE

Dans cette section, nous estimons les coûts de notre protocole Bee-Trust en considérant à la fois les coûts de communication, de stockage ainsi que de la complexité temporelle.

6.1.Coûts de communication

La distribution de recommandations inclut les procédures d'envoi et de réception. Le nœud évaluateur doit envoyer n requêtes et reçoit m réponses ($m \leq n$). Nous pouvons déduire un coût moyen par nœud évaluateur de O (n + m).

6.2. Coûts de stockage

Étant donné que le nœud évaluateur n'a pas besoin de stocker les informations envoyées par les recommandeurs, c'est-à-dire (identifiants, positions, journaux ainsi que les valeurs de réputations assignées) puisque ces données seront traitées et analysées immédiatement. Et étant donné que toutes les autres étapes de cet algorithme sont constantes dans l'espace. La complexité de notre algorithme en termes de stockage est donc de O (1).

6.3. Complexité temporelle

La complexité temporelle du modèle de nuage révisé est déterminée par le nombre de gouttelettes de nuages générées associée à la complexité temporelle du mécanisme de correction. Étant donné que le nombre de gouttes de nuages est égal au nombre de recommandations "m", la complexité temporelle du modèle de nuages est de O(m).La complexité temporelle du mécanisme de correction est de O (1). Cet algorithme peut alors s'exécuter en un temps de O (m).

Ces coûts restent négligeables puisqu'ils ne concernent que le nœud évaluateur et non pas tous les nœuds du réseau étant donné que le mécanisme de détection s'exécute à la demande et non pas de manière spontanée.

7. ÉVALUATION DES PERFORMANCES

Dans cette section, une évaluation des performances de l'algorithme proposé est donnée, incluant la méthodologie de simulation ainsi que les résultats obtenus selon certaines métriques.

7.1.Méthodologie de simulation

Les expériences de simulation ont été mises en œuvre sous MATLAB afin d'évaluer les performances de notre protocole BTS dans divers scénarios d'attaques.

Le scénario de simulation considéré est le suivant : nous supposons un ensemble de 12 nœuds impliqués dans le processus de recommandation. Le nœud 2 est supposé être le nœud à évaluer tandis que le nœud 6 est le nœud évaluateur. Les nœuds 1, 3, 4, 5, 7, 8, 9, 10, 11, 12

sont les recommandeurs sélectionnés. Ces recommandeurs sont choisis parmi les voisins à un saut avec les valeurs de réputation les plus élevées. Dans les scénarios de simulation, les recommandations présentent trois types de comportement :

- **Type I :** Bons recommandeurs et bonnes recommandations.
- **Type II :** Bons recommandeurs et recommandations erronées.
- **Type III :** Mauvais recommandeurs et mauvaises recommandations.

La simulation inclue les trois types d'attaques de recommandations malhonnêtes que nous avons vu (bad mouthing, ballot-stuffing et collusion).Toutes les expériences ont été menées sur 3000 rounds, à chaque 1000 itération, les attaques ont été évaluées. 10 séries de test ont été réalisées pour chaque expérience. Le modèle de mobilité choisi est le modèle de mobilité aléatoire *"random waypoint"*, dans lequel les nœuds se déplacent vers une destination aléatoire à une vitesse uniformément répartie entre 0 m/s et une vitesse maximale spécifiée. Notre choix s'est porté sur ce modèle car il permet de refléter un mouvement aléatoire ponctué avec des pauses qui s'approche du mouvement réel des nœuds capteurs dans le réseau. Les paramètres de simulation utilisés sont donnés dans le Tableau 3.

Les effets des attaques de recommandations malhonnêtes ainsi que les performances du protocole ont été analysés en faisant varier trois indicateurs :

- Le pourcentage de la déviation des valeurs de recommandations.
- Le pourcentage des recommandeurs malhonnêtes.
- Le pourcentage des recommandations erronées.

Les performances du système ont été examinées via quatre paramètres :

- **Débit (TH) (*throughput*)** défini comme étant le débit moyen des paquets transmis avec succès à la station de base, il est mesuré en nombre de paquets de données par intervalle de temps.
- **Taux de reconnaissance (RR) (*Recognition rate*)** défini comme le nombre de nœuds détectés comme malveillants par rapport au nombre total de recommandations malhonnêtes.
- **Taux de faux positifs (FPR)** défini comme le rapport entre le nombre de recommandations honnêtes incorrectement classées comme malhonnêtes et le nombre total de recommandations honnêtes.
- **Taux de faux négatifs (FNR)** défini comme la proportion de recommandations malhonnêtes incorrectement classées comme honnêtes.

Tableau 4. 3. Paramètres de simulation

Paramètres	Valeurs par défaut
Superficie	1000m x 1000m
Mouvement	Modèle de mobilité aléatoire
Vitesse	Uniformément distribuée entre 0 et 20 m/s
Nombre de nœuds	12
Portée radio	300
α	0.3
β	0.7
γ	0.25

7.2. Résultats de la simulation

Nous avons évalué le protocole proposé BTS et examiné ses performances globales en effectuant une série d'expériences intensives dans divers scénarios. Le débit, les métriques de réputation ainsi que les indicateurs de performance définis dans la section précédente 7.1 sont simulés afin de démontrer son efficacité.

7.2.1. Performances du protocole BTS en variant le pourcentage de déviation

La déviation des valeurs de recommandation est l'un des paramètres importants influençant la détection des recommandations malhonnêtes. Plus la différence entre la réputation calculée du nœud évalué et la recommandation reçue est faible, plus la détection devient difficile et inversement. Les attaquants intelligents souhaitant rester indétectables peuvent introduire une déviation relativement faible dans leurs recommandations malhonnêtes afin de contourner les mécanismes de détection. Un protocole de détection de recommandations malhonnêtes doit rester efficace quel que soit le taux de déviation.

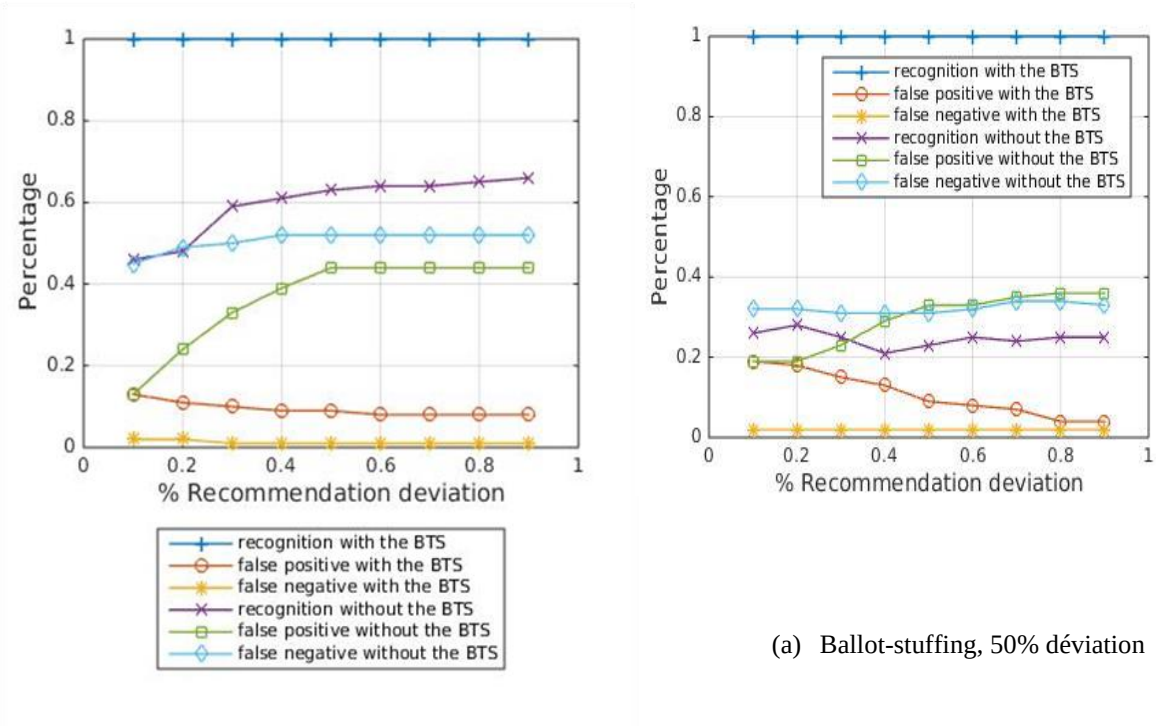
Dans cette section, nous examinons les performances de notre protocole en faisant varier le pourcentage de déviation entre les recommandations. Tout d'abord, le pourcentage des recommandeurs malhonnêtes est fixé à sa valeur par défaut de 50%. Nous examinons les résultats de la comparaison entre le cas où le protocole BTS est désactivé (c'est-à-dire un système sans protection) et quand le protocole BTS est appliqué en considérant les attaques de bad-mouthing et de ballot-stuffing, comme le montre la Figure 4.3.a-b. Nous remarquons que quelle que soit l'attaque, notre protocole obtient des performances similaires, ce qui signifie que BTS n'est pas sensible à ces 2 types d'attaque.

Lorsque le protocole BTS n'est pas utilisé, nous remarquons à partir des Figure 4.3-a et 4.3-b que le taux de reconnaissance RR est bas lorsque l'écart est faible ; par conséquent, plus

l'écart augmente, plus le RR augmente aussi. Étant donné qu'une grande déviation rend facile la détection des recommandations malhonnêtes. FPR et FNR restent élevés. La raison principale est la présence de 50% de recommandeurs malhonnêtes en l'absence d'un mécanisme de détection efficace. Le pourcentage élevé de faux positifs et de faux négatifs, ainsi que le faible taux de détection, sont intolérables pour un réseau.

Lorsque le protocole BTS est appliqué, le résultat le plus intéressant que l'on peut observer est que même dans le pire des cas où l'écart est de seulement 10%, nous obtenons de très bonnes performances avec RR = 100%, FPR = 13% et FNR = 1%. Ceci est dû au fait que notre protocole ne repose pas uniquement sur le modèle de nuage qui est basé sur une mesure de similarité majoritaire (MSM) facilement influencée par la déviation des recommandations mais qu'il utilise un paramètre supplémentaire indépendant des valeurs de recommandations. Le protocole BTS est insensible à la déviation des recommandations, il est donc efficace contre les attaquants intelligents.

Nous examinons également la métrique de débit de l'ensemble du réseau. Les résultats obtenus en variant le pourcentage de déviation des recommandations sont donnés dans la Figure 4.4. Chaque ligne représente le débit lorsque le pourcentage des recommandeurs malhonnêtes est fixé. Nous remarquons, que même en l'absence de recommandeurs malhonnêtes, le débit n'est que de 84,40%. La cause principale est la présence potentielle de mauvais nœuds générant des brouillages et des collisions. On peut observer aussi que lorsque les paramètres de (% déviation de recommandations,% recommandeurs malhonnêtes) sont inférieurs à (20%, 20%), l'impact sur le débit reste faible puisque les valeurs de réputation des mauvais nœuds sont encore beaucoup plus faibles que ceux des nœuds honnêtes. Cependant, à mesure que les paramètres (% déviation de recommandations, % recommandeurs malhonnêtes) augmentent, le débit diminue de manière significative. Par exemple à (90%, 90%), l'ensemble du réseau ne peut transmettre avec succès que 43,68% de paquets à la station de base. Ce qui prouve encore une fois l'impact négatif des recommandations malhonnêtes sur le réseau.



(a) Ballot-stuffing, 50% déviation

(b) Badmouthing, 50% déviation

Fig 4. 3. Performances du protocole BTS en variant le pourcentage de déviation

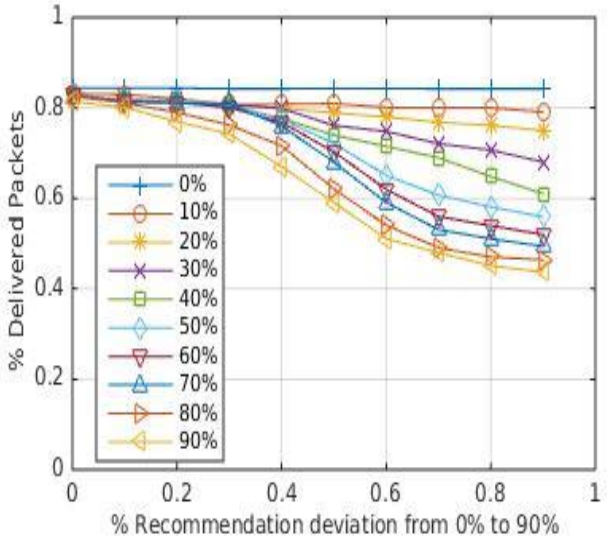


Fig 4. 4. Le débit lors de l'attaque par collusion

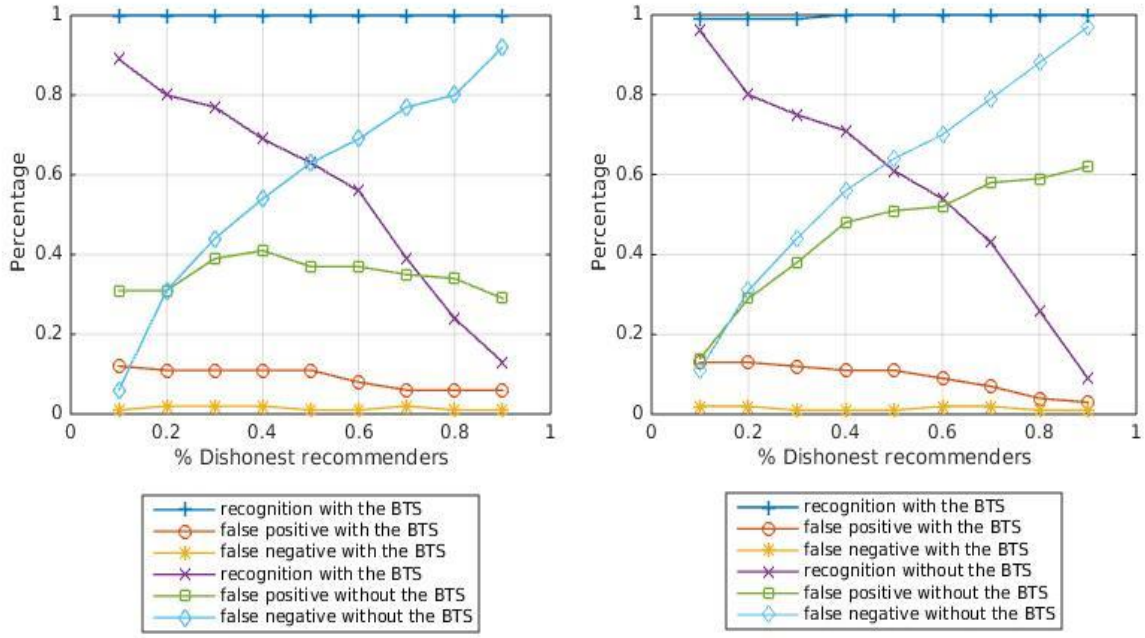
7.2.2. Performance du protocole BTS en variant le pourcentage des recommandeurs malhonnêtes

Le nombre de recommandeurs malhonnêtes est un autre paramètre important influençant le protocole de détection des attaques de recommandations malhonnêtes. Plus le nombre d'attaquants est grand, plus l'influence sur le mécanisme de confiance et de réputation est importante et plus il devient difficile de les détecter. La présence simultanée de plusieurs attaquants dans le système va les amener à collaborer et à détourner le mécanisme de réputation à leur avantage. De ce fait, un protocole de détection de recommandations malhonnêtes doit rester efficace quel que soit le pourcentage des recommandeurs malhonnêtes présents dans le réseau.

La méthodologie utilisée est similaire à celle de l'expérience précédente. Nous examinons la performance de notre protocole en faisant varier le pourcentage de recommandeurs malhonnêtes tout en fixant le pourcentage de déviation des recommandations à sa valeur par défaut de 50%. Par conséquent, les métriques RR, FPR, et FNR sont employées pour mesurer le taux de détection des recommandeurs malhonnêtes, ainsi que le taux de faux positifs et faux négatifs. Les performances du protocole BTS en faisant varier le pourcentage des recommandeurs malhonnêtes sont données dans la Figure 4.5.

Les Figures 4.5-a et 4.5-b illustrent les résultats de RR, FPR et FNR dans les deux cas étudiés : avec exécution du protocole BTS et sans l'utilisation du protocole BTS pour les attaques bad-mouthing et ballot-stuffing. Nous remarquons que les performances du protocole BTS restent stables avec des valeurs approchant les 100% pour le RR et de 2% et 1% pour le FPR et FNR respectivement, et cela quel que soit le pourcentage de recommandeurs malhonnêtes présents dans le réseau. En effet, considérer l'indice de vitesse de réponse comme un paramètre important en lui attribuant un poids élevé ($\beta = 0,7$) permet de révéler la nature du recommandeur et donc de détecter l'attaque indépendamment du nombre de recommandeurs malhonnêtes.

Une comparaison entre notre protocole BTS et quatre autres schémas de recommandation : RecommVerifier (Chen et al., 2012), Schéma de filtrage de Whitby (WFS) (Whitby et al., 2004), E-Hermes (Zouridaki et al., 2009), et RFSN (Ganeriwal et al., 2008) est réalisée en faisant appel à la métrique de débit *"throughtput"* en considérant l'attaque "collusion" qui est connue pour être l'une des attaques les plus nuisibles. Comme le montre la Fig.4.6, le débit obtenu par notre protocole BTS dépasse le débit des autres protocoles. Le protocole BTS reste stable sous différents paramètres et converge vers le débit idéal obtenu dans (Figure 4.6).



(a) Bad mouthing, 50% recommandeurs malhonnêtes (b) Ballot-stuffing, 50% recommandeurs malhonnêtes

Fig 4. 5. Performances du protocole BTS en variant le pourcentage des recommandeurs malhonnêtes

Hormis le débit du protocole RecommVerifier qui est également stable mais légèrement inférieur au notre (80,84%), le débit obtenu par les autres schémas de défense diminue quand le pourcentage des recommandeurs malhonnêtes augmente. Une faible valeur de débit laisse supposer que les recommandeurs malhonnêtes ont le contrôle sur le réseau.

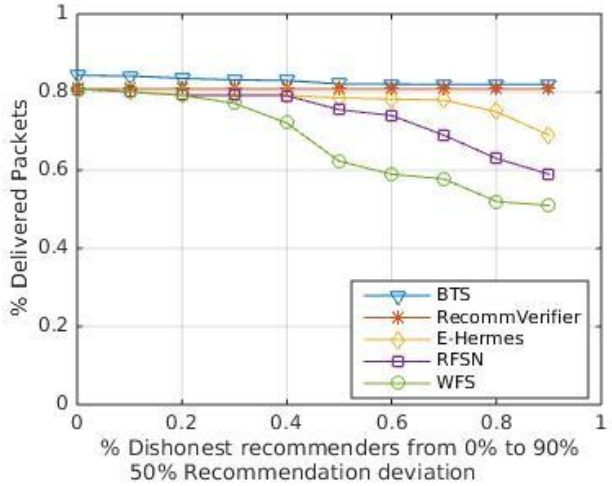


Fig 4. 6. Comparaison entre le protocole BTS et d'autres protocoles de défense

7.2.3. Performances du protocole BTS en variant le nombre de recommandations erronées

Bien que souvent négligées, les erreurs sont toujours présentes principalement dans les réseaux tels que les RCSFs. Considérer les recommandations erronées est un paramètre très important influençant le schéma de détection. Dans les RCSFs, les recommandations erronées peuvent être dues à des problèmes de communication entre les nœuds tels que de mauvais canaux de communication, des défaillances de nœuds, des pertes de paquets, etc. Des recommandations erronées peuvent aussi résulter de problèmes de sécurité comme c'est le cas lors de l'attaque "conflicting behavior". Un protocole de détection des recommandations malhonnêtes ne pouvant pas distinguer entre les recommandations erronées et malhonnêtes conduit à plusieurs problèmes. D'une part, un taux élevé de faux positifs est généré, en jugeant injustement des nœuds honnêtes fournissant des recommandations erronées comme étant malhonnêtes. D'autre part, les nœuds honnêtes seront supprimés du mécanisme de réputation, laissant ainsi plus de chance aux nœuds malhonnêtes de manipuler les systèmes de réputation et de perturber le réseau.

Afin de démontrer l'efficacité de notre protocole BTS pour distinguer entre les recommandations erronées et malhonnêtes, nous avons réalisé le scénario suivant. Comme le montre la Figure 4.7, nous avons simulé la présence de recommandations erronées et malhonnêtes dans le même scénario tout en faisant varier le pourcentage des recommandations erronées. Un des résultats intéressants pouvant être observé est que le taux de détection des recommandations erronées augmente de manière parallèle à celui du pourcentage des recommandations permettant ainsi une détection optimale.

Pour résumer toutes ces étapes de simulation, nous pouvons conclure que le protocole BTS reste efficace quel que soit les scénarios d'attaques et donne de bons résultats sous différentes métriques.

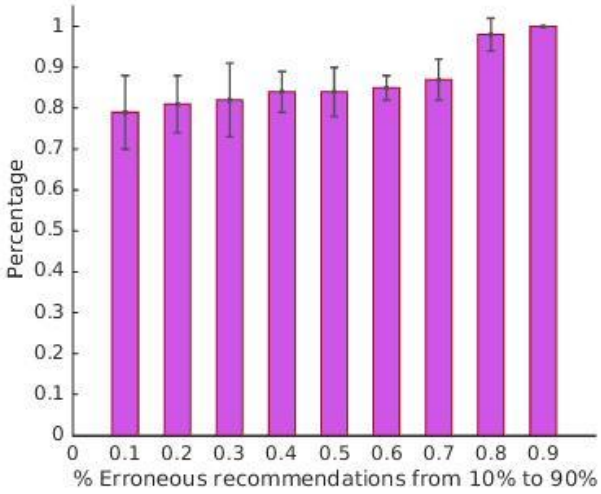


Fig 4. 7. Performances du protocole BTS en variant le nombre des recommandations erronées

8. CONCLUSION

Nous avons présenté dans ce chapitre un nouveau schéma bio-inspiré basé sur un modèle de nuages modifié et d'une stratégie de chronométrie cognitive pour les RCSFs mobiles afin d'améliorer la détection des attaques de recommandations malhonnêtes. Dans le protocole BTS, le scénario de gestion de la réputation est modélisé en s'inspirant du comportement de recherche de nourriture de l'essaim d'abeilles en utilisant certaines caractéristiques de l'algorithme (ABC). L'aptitude "fitness" de chaque recommandeur est jugée en fonction de deux paramètres importants : un modèle de nuage révisé et un indice de vitesse de réponse. La nouveauté de notre proposition est qu'elle n'est pas seulement basée sur des méthodes statistiques traditionnelles mais qu'elle introduit un paramètre cognitif efficace permettant de détecter les recommandeurs malhonnêtes qui sont considérés comme la source de l'attaque. De plus, cet indice de vitesse de réponse permet de faire la distinction entre les recommandations malhonnêtes et les recommandations erronées, diminuant ainsi le taux de faux positifs causés par les méthodes de détection à base de déviation classiques. Les différents scénarios de simulation ont prouvé l'efficacité de notre protocole sous différentes métriques. Les résultats obtenus montrent des taux de détection élevés même quand le nombre de recommandeurs malhonnêtes est important ou bien la déviation des recommandations faible.

CHAPITRE V

Deuxième contribution :

Nouveau mécanisme de confiance et de réputation pour la détection des attaques internes

Sommaire

1. INTRODUCTION

Les attaques internes sont l'une des menaces les plus graves et les plus dangereuses résultant de la capture physique des nœuds capteurs. Lors de ces attaques, l'attaquant va extraire les données cryptographiques du nœud et le reprogrammer en nœud malicieux capable d'interférer et de nuire au fonctionnement du réseau. Les mécanismes cryptographiques traditionnels étant inefficaces contre ce type d'attaque, il était devenu essentiel de trouver des méthodes complémentaires afin de distinguer les nœuds légitimes des nœuds malicieux. Les mécanismes de confiance et de réputation ont été suggérés comme une approche efficace permettant de surmonter les limites des méthodes cryptographiques. Dans ces mécanismes, des valeurs de réputation sont assignées aux nœuds voisins pour juger leur comportement. Ces valeurs sont attribuées de manière honnête ou malhonnête en fonction de la légitimité des nœuds évaluateurs. La manipulation et la modification malintentionnée de ces valeurs par des nœuds malveillants va fausser les résultats du mécanisme et détruire sa légitimité.

Nous présentons dans ce chapitre un mécanisme de réputation intelligent permettant d'automatiser le processus d'attribution des valeurs de réputation afin d'éviter que celles-ci ne soient manipulées par des attaquants. Le protocole que nous avons nommé B-Smart confie le calcul de ces valeurs à un contrat intelligent enregistré dans une structure blockchain afin de garantir l'intégrité, la durabilité et l'efficacité du système de confiance.

2. MOTIVATIONS

Nous nous sommes principalement intéressés dans cette thèse aux systèmes de confiance et de réputation TRS. Des mécanismes dont l'efficacité n'est plus à prouver, mais dont l'utilisation dans les RCSFs fait toujours face à de nombreux problèmes. Premièrement, l'environnement ouvert, non supervisé et non sécurisé dans lequel les réseaux de capteurs sont déployés, et l'absence d'une autorité centrale mettent en danger la coopération entre les nœuds et fragilisent les liens de confiance. Deuxièmement, le grand nombre de nœuds capteurs dans les RCSFs ainsi que les communications limitées entre ces nœuds en raison de l'instabilité du réseau et de la mobilité des capteurs rendent l'établissement de relations de confiance chose difficile et compliquent l'attribution des valeurs de réputation. Le troisième problème qui est un des plus cruciaux est celui de la manipulation abusive des valeurs de réputation par des nœuds malveillants participant dans le TRS. En effet, à notre connaissance, tous les protocoles présentés jusqu'à présent permettent à tous les nœuds de réseau d'attribuer

et de manipuler les valeurs de réputation. Des valeurs pourtant si précieuses sur lesquelles repose la sécurité de l'ensemble du réseau. Dans les RCSFs, connus pour être vulnérables à l'attaque "node compromise", un ou plusieurs nœuds malveillants peuvent à tout moment s'introduire parmi les nœuds légitimes en passant totalement inaperçus. Laisser ces nœuds malicieux manipuler les valeurs de réputation semble incompréhensible et contradictoire au principe des TRS.

Dans ce chapitre, nous présentons un mécanisme de réputation innovant nommé B-Smart, permettant d'automatiser le processus d'attribution des valeurs de réputation. Un protocole améliorant la fiabilité, la sécurité et la disponibilité de ces valeurs de réputation tout en déchargeant les nœuds capteurs de ce procédé fastidieux et contribuer à préserver leur énergie. En étant résistant à toutes les attaques de confiance et de réputation et à la majeure partie des attaques de routage, le protocole B-Smart permet d'apporter une grande avancée dans le domaine de la sécurité dans les RCSFs.

3. MODÈLE DU SYSTÈME

Dans cette section, nous décrivons le modèle du réseau, le modèle de l'attaquant ainsi que les hypothèses utilisées.

3.1. Modèle de réseau

Nous utilisons dans notre protocole B-Smart un RCSF basé sur la technologie blockchain où toutes les transactions effectuées par les nœuds du réseau sont enregistrées dans des blocs chainés les uns aux autres. La topologie du réseau peut être indifféremment statique ou mobile. Le réseau suit une architecture plate. L'identité de chaque nœud est unique et stable.

3.2. Modèle de l'attaquant

Dans cet article, nous supposons un modèle d'attaque active, dans lequel l'attaquant va volontairement supprimer, altérer, modifier, détourner ou rediffuser les messages qu'il est censé transmettre selon un protocole de routage donné. Nous utiliserons dans la suite du chapitre les termes "bad behavior" pour qualifier un attaquant au mauvais comportement tentant de causer le plus de dommages possible et de perturber le fonctionnement du réseau. Inversement, un nœud qui propage correctement les messages sera qualifié comme ayant "good behavior".

3.3. Suppositions

Tout schéma de gestion de la confiance et de la réputation doit initialiser les valeurs de confiance et de réputation avant le déploiement du réseau. Par conséquent, dans notre protocole B-Smart, nous supposons que : 1) les valeurs de réputation appartiennent à l'intervalle [0, 1]. 0 signifie très mauvais comportement et 1 signifie très bon comportement. 2) à l'initialisation du réseau tous les nœuds ont la même réputation égale à 0,5 et sont considérés comme trust. La raison est simple : au tout début du déploiement, l'attaquant n'a pas encore eu le temps ou l'opportunité d'influer ou de compromettre un nœud. 3) Les nouveaux nœuds apparaissant pendant la durée de vie du réseau ne sont pas entièrement approuvés, car ils pourraient être générés par un adversaire. Ces nœuds sont placés dans une "période de test" où ils devront effectuer un plus grand nombre de tâches satisfaisantes que les nœuds initiaux avant de pouvoir récupérer une valeur de réputation normale.

3.4. Vocabulaire

Dans ce qui suit, nous allons présenter les notations et les expressions considérées dans notre protocole. Le tableau 5.1 décrit les différentes notations ainsi que leurs descriptions.

Tableau 5. 1. Notations

Notation	Description
TRS	Système de confiance et de réputation
TR_X	Transaction x
S	Noeud source
D	Noeud destination
G_i	Noeud passerelle i
SK_i	Clé privée du nœud i
PK_D	Clé publique du nœud D
$Sig_{SKi}(TR_x, PK_D)$	Signature sur TR_X par le nœud i
Rec_i	Facteur de récidive du nœud i
Rep_i^{last}	Dernière valeur de réputation attribuée au nœud i

4. PRÉSENTATION DU PROTOCOLE B-SMART

Dans cette section, nous présentons notre nouveau mécanisme de réputation dédié aux réseaux de capteurs (RCSFs) nommé B-Smart. Un protocole intelligent permettant d'automatiser le processus d'assignation et de gestion des valeurs de réputation par le biais d'un contrat intelligent visant à empêcher la falsification de ces valeurs par des nœuds malveillants. Enregistrer ce contrat dans une blockchain garantira la durabilité, l'intégrité et

l'efficacité du processus. Nous présentons ci-après les objectifs de conception de notre protocole B-Smart, l'architecture du système ainsi que les principales phases d'exécution.

4.1. Objectifs de conception

Notre protocole de réputation basé sur la blockchain et la notion de contrat intelligent vise à répondre à plusieurs objectifs de sécurité, à savoir la décentralisation, l'intégrité des informations, la disponibilité des valeurs de réputation et la non-répudiation.

4.1.1. Décentralisation

Notre protocole B-Smart permet une sauvegarde de toutes les transactions de manière décentralisée dans tous les nœuds du réseau sans faire appel à une tierce partie grâce à l'utilisation d'une topologie blockchain.

4.1.2. Centralisation du calcul des valeurs de réputation

Décharger les nœuds capteurs de l'attribution des valeurs de réputation à d'autres nœuds du réseau, permet d'empêcher les attaquants d'utiliser le TRS pour manipuler les valeurs de réputation à leur guise en diminuant les valeurs de réputation des nœuds légitimes ou en augmentant celles des autres attaquants. Confier le calcul de ces valeurs à une entité centrale, le «contrat intelligent», et sauvegarder ces données dans la blockchain, facilite non seulement l'accès à ces données, mais assure également la décentralisation et la sécurité, évitant ainsi les inconvénients traditionnels des méthodes de gestion centralisée.

4.1.3. Intégrité des informations

B-Smart permet de garder une trace de toutes les transactions effectuées de manière non modifiable. L'utilisation en effet de la blockchain permet de garantir que les informations stockées dans les blocs ne peuvent être modifiées par aucun nœud du réseau.

4.1.4. Disponibilité

L'utilisation du contrat intelligent permet de garantir la disponibilité des valeurs de réputation pour les différents nœuds du réseau. En effet, tout nœud peut connaître les valeurs de réputation de ses nœuds voisins sans avoir à demander auprès de recommandeurs.

4.1.5. Non-répudiation

La non-répudiation est assurée dans notre protocole B-Smart grâce à l'utilisation de la cryptographie asymétrique. Le suivi du routage de la transaction à travers les différents nœuds

intermédiaires prouvera qu'un message a été effectivement envoyé par son expéditeur ou reçu par le destinataire.

4.2. Description générale

Le protocole B-Smart est un nouveau protocole de réputation basé sur l'utilisation de blockchain. Notre protocole résout le problème de la manipulation malveillante des valeurs de réputation en confiant la gestion de ces valeurs à un contrat intelligent. Ce smart contrat suivra ainsi l'évolution des différentes transactions du réseau et attribuera aux nœuds les valeurs de réputation correspondantes en fonction de leur comportement. Les nœuds seront ainsi jugés suivants s'ils transmettent les messages correctement ou non, la présence ou non de modifications dans les paquets de messages, la modification du chemin de routage du paquet ainsi que des éventuelles suppressions des messages en transit. Le contrat intelligent applique un facteur de récidive lors du calcul des valeurs de réputation afin de pénaliser sévèrement les nœuds malveillants en réduisant considérablement leurs valeurs de réputation. Ce facteur contribue également à motiver les nœuds intermédiaires à relayer correctement les informations afin de préserver leurs valeurs de réputation. Le contrat intelligent est enregistré dans la blockchain pour garantir sa durabilité, son intégrité et son efficacité. Ainsi enregistré, le contact est protégé des manipulations abusives des attaquants internes.

Le protocole B-Smart fonctionne comme suit : lorsqu'un nœud veut envoyer un message ou demander des informations à un autre nœud ou à la station de base. Cette communication suit les étapes principales suivantes : Tout d'abord, un protocole de routage est utilisé pour déterminer le chemin optimal entre le nœud demandeur et le nœud fournisseur. Dans les réseaux de capteurs, une telle requête doit transiter par plusieurs nœuds en mode "multi-sauts" étant donné que les communications "à un saut" nécessitent beaucoup plus de ressources. Deuxièmement, un temps est alloué pour chaque transaction et un bloc est créé pour suivre le routage de la transaction entre chaque deux nœuds successifs jusqu'à sa destination ou jusqu'à la fin du temps alloué. Une fois la transaction terminée ou le temps écoulé, le bloc est inséré dans la blockchain. Une copie personnelle de la blockchain est hébergée par chaque nœud pour garantir sa sécurité. Cependant, vu la capacité de stockage limitée des capteurs, nous supposons dans notre protocole B-Smart que les nœuds peuvent stocker la blockchain dans n'importe quel type de stockage accessible au réseau, hébergé de manière privée, tel que le stockage dans le cloud ou décentralisé tel que Swarm (Hartman et al., 1999) ou IPFS (Benet 2014) ou autres types de stockage (Bagchi, 2017). Enfin, le contrat intelligent utilise les données contenues dans son historique ainsi que les informations fournies par le bloc de la

transaction afin de mettre à jour les valeurs de réputation des nœuds participants. Les nœuds dont la valeur de réputation est inférieure à un seuil défini β sont déclarés malveillants et intégrés dans une liste noire pour empêcher leur participation dans les applications du réseau. La vue d'ensemble du protocole B-Smart est donnée dans la Figure 5.1.

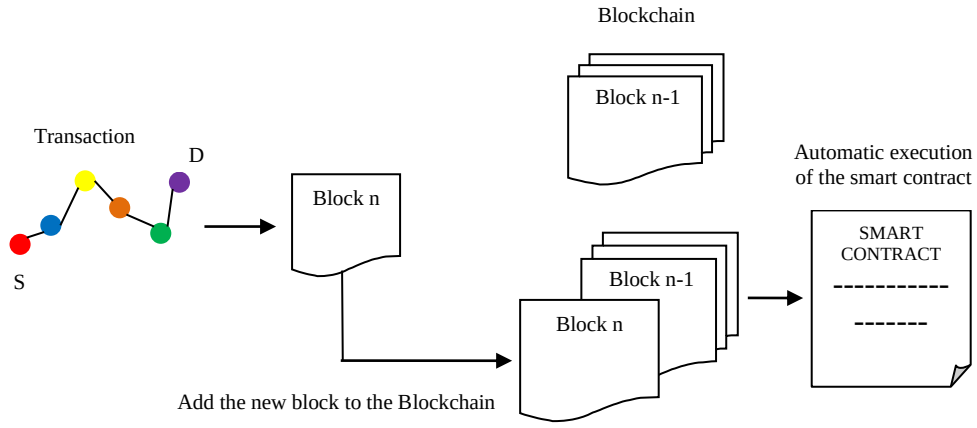


Fig 5. 1. Vue d'ensemble de notre protocole B-Smart

4.3. Architecture du système

Le protocole B-Smart repose sur le fonctionnement conjoint de plusieurs entités. Parmi ces entités, on peut citer :

4.3.1. Transaction

Les interactions entre les capteurs sont le principe de base de chaque réseau. En effet, l'échange d'informations telles que la température, l'humidité et d'autres paramètres entre ces nœuds permet la mise en œuvre de diverses applications. Une transaction est donc tout échange de données entre les nœuds, ainsi qu'entre les nœuds et la station de base. Chaque transaction dans notre protocole implique un nœud source (S), un nœud destination (D) et un ensemble de nœuds intermédiaires pour la relayée. Le nœud (D) joue le rôle de demandeur et le nœud (S) joue le rôle de fournisseur. Les transactions dans notre protocole sont stockées dans des blocs en utilisant une structure de données blockchain. Chaque transaction est signée crypto graphiquement par tous les participants afin de conserver une preuve irréfutable de la participation de chaque nœud impliqué dans la transaction.

4.3.2. Nœud

Dans notre protocole, un nœud de capteur peut jouer le rôle de nœud fournisseur, demandeur ou passerelle. En tant que demandeur, le nœud demandera la récupération de certaines données auprès du nœud fournisseur. Le fournisseur est responsable de la transmission de certains fichiers, messages ou données détectées au demandeur à l'aide des nœuds intermédiaires. Ce dernier créera un bloc qui suivra l'acheminement de la transaction entre homologues via les nœuds de passerelle en multi sauts jusqu'au nœud demandeur. Chaque nœud participant à une transaction dans notre protocole doit avoir une signature unique; cette signature est formée d'une paire de clé publique et de clé privée. Bien que la clé publique soit partagée avec tous les nœuds du réseau, la clé privée reste secrète. La cryptographie à courbe elliptique (ECC) est utilisée pour générer une clé publique à partir de la clé privée, offrant ainsi un haut degré de sécurité tout en étant adaptée aux réseaux de capteurs grâce à la taille réduite des clés par rapport à d'autres méthodes cryptographiques telles que RSA (Gura et al., 2004).

4.3.3. Bloc et Blockchain

Un bloc permet de sauvegarder toutes les informations relatives au routage de la transaction du nœud source au nœud destination. En effet, toutes les actions des nœuds lors d'une transaction sont enregistrées dans le bloc, telles que : l'envoi, la réception, la modification ainsi que la suppression de données. Dans notre protocole, chaque bloc contient une transaction. L'énoncé de la transaction et les différentes étapes de l'acheminement de la transaction avec leurs horodatages correspondants sont définis dans le corps du bloc. Pour relier les blocs entre eux et garantir ainsi l'intégrité des blocs, la fonction de hachage SHA-256 est utilisée pour calculer le "hachage" d'un bloc et insérer cette valeur dans l'en-tête de bloc suivant. Toute modification des données dans un bloc entraînera un changement de la valeur du hachage qui deviendra ainsi totalement différent de la valeur de l'en-tête enregistrée.

4.3.4. Contrats intelligents

Un contrat intelligent ou smart contrat est un bloc spécial qui exécutera le protocole de réputation. Il est automatiquement exécuté après l'ajout d'un nouveau bloc dans la blockchain. En utilisant les informations contenues dans le bloc concernant l'énoncé et le chemin de routage de la transaction par les nœuds capteurs et en utilisant son historique personnel, le contrat intelligent pourra juger les nœuds, attribuer les valeurs de réputation appropriées et mettre à jour les valeurs de réputation existantes. Accessible via une adresse de contrat, les

nœuds du réseau peuvent communiquer avec le contrat intelligent en envoyant des messages à son adresse. Ces messages peuvent être des "Transactions" ou des "Calls". Des messages de "Transactions" sont envoyés lorsque les nœuds nécessitent de stocker des informations pertinentes sur des périphériques spécifiques. Les messages d'appel sont émis lorsque les nœuds veulent interroger le contrat sur le comportement d'un nœud à un moment donné (Bagchi, 2017).

5. ÉTAPES D'ÉXECUTION DU PROTOCOLE B-SMART

Pour expliquer le fonctionnement de notre protocole, nous supposons que la transaction a lieu entre deux nœuds, c'est-à-dire, le nœud source S et le nœud de destination D de manière multi-sauts. Toutes les étapes réalisées lors de l'exécution du protocole B-Smart sont mises en évidence dans la Figure 5.2 et expliquées ci-après :

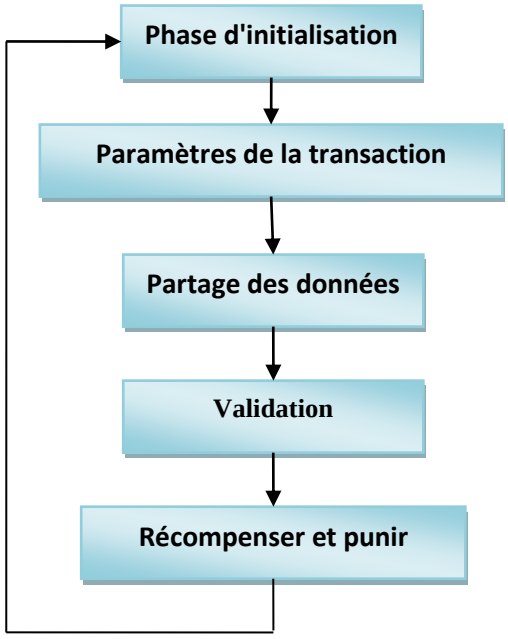


Fig 5. 2. Les principales étapes d'exécution de notre protocole par B-Smart

5.1. Phase d'initialisation

Un protocole de routage est appliqué pour déterminer le chemin le plus approprié entre le nœud source et le nœud destination. Plusieurs protocoles de routage permettant la découverte du chemin optimal ont été appliqués de manière efficace dans les réseaux de capteurs. Ces protocoles prennent en compte plusieurs paramètres tels que : le niveau d'énergie des capteurs, la fiabilité de la livraison des données, le nombre de sauts ainsi que la sécurité du

chemin. Dans notre protocole, une fois que le contrat intelligent aura plus de connaissances sur la réputation des nœuds, le protocole de routage prendra aussi en considération les informations fournies par le contrat intelligent pour choisir le chemin le plus sûr. Les protocoles de routage existants sont classés en trois catégories principales (Othmen el al., 2016) : les protocoles de routage réactifs, proactifs et hybrides. Dans les protocoles réactifs tels que (AODV) (Perkins et al., 2003) et DSR (Johnson et al., 1996), le nœud découvre un chemin vers la destination à la demande. Pour ce faire, le réseau est inondé de paquets Route REQuest (RREQ). Cela peut entraîner un temps de latence élevé dans le processus de recherche d'itinéraire. Dans les protocoles de routage proactifs tels que DSDV (Perkins et Bhagwat, 1994) et OLSR (Clausen et Jacquet, 2003), chaque nœud conserve des listes fraîches des destinations et de leurs chemins en distribuant périodiquement des messages de contrôle. Cette solution convient lorsque la topologie est statique. Cependant, il réagit lentement sur les restructurations et les échecs. Les protocoles hybrides tels que ZRP (Haas et Pearlman, 2000) et ZHLS (Hamma, et al., 2006) combinent les avantages des protocoles réactifs et proactifs. Choisir un protocole de routage au lieu d'un autre est hors de portée de notre protocole, cela dépendra des besoins de l'application.

5.2. Paramètres de la transaction

Avant d'être transmise, chaque transaction doit être cryptée et un temps lui est alloué. Ces deux notions sont expliquées dans ce qui suit :

5.2.1. Cryptage de la transaction

Une fois le chemin de routage établi, le nœud demandeur concrétise son intention d'initier une transaction en créant un bloc correspondant. L'entête du bloc créé contient l'énoncé de la transaction et le chemin défini par le protocole de routage. Le corps du bloc suivra et enregistrera toutes les étapes du routage de la transaction entre les nœuds intermédiaires et la destination. Le cryptage de la transaction est réalisé grâce à l'utilisation du cryptage asymétrique et plus particulièrement de la cryptographie à courbe elliptique (ECC). L'utilisation de la cryptographie asymétrique assurera l'authentification et l'intégrité des données relayées via les nœuds passerelles. Étant donné que chaque nœud du réseau possède une paire de clés (clé publique et clé privée), le nœud fournisseur S utilisera la clé publique du nœud demandeur D (PK_D) pour chiffrer le message qu'il veut lui envoyer. Chaque nœud passerelle G_i doit à son tour signer les données en transit afin de garder une trace du routage de la transaction. La Figure 5.3 décrit les principales étapes du chiffrement de la transaction.

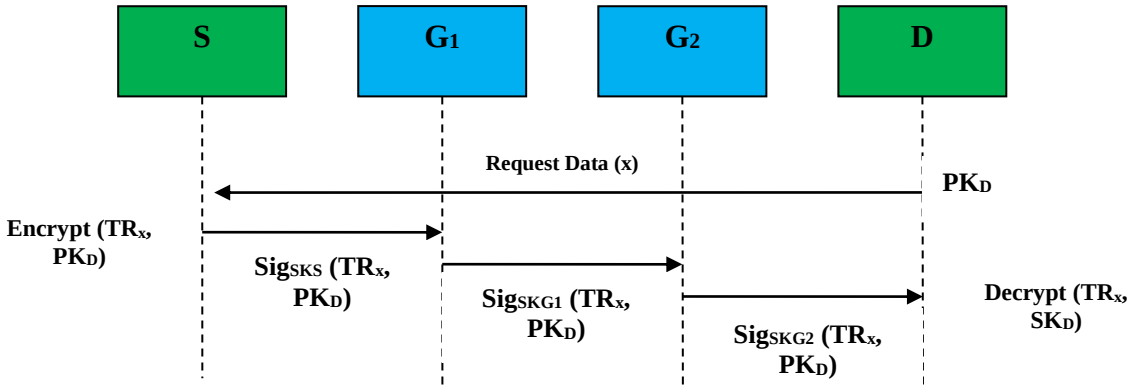


Fig 5. 3. Principales étapes du chiffrement de la transaction

5.2.2. Temps de transaction

Un temps défini est alloué à chaque transaction. À la fin de cette période, la transaction est considérée comme terminée. Ce temps limitera le temps consacré aux transactions afin de résoudre le problème des transactions qui n'atteignent jamais leur destination en raison de pannes matérielles ou de suppressions volontaires par des nœuds malveillants, évitant ainsi d'attendre indéfiniment.

5.3. Partage des données

La transaction chiffrée est envoyée en plusieurs étapes du nœud source au nœud de destination. Tous les changements et modifications, ainsi que chaque réception et chaque envoi réussis par les nœuds de passerelle, sont enregistrés dans le bloc de transaction géré par tous les nœuds participant à la transaction.

5.4. Validation du bloc

Contrairement au principe de validation utilisé dans les blockchain standards tel que celui utilisé dans (Underwood, 2016) et (Bahga et Madisetti, 2016) où la validation des blocs est effectuée par un ensemble de mineurs afin de valider le bloc avant de l'intégrer dans la blockchain globale, dans notre protocole, la validation est effectuée par le contrat intelligent une fois que le bloc de la transaction a été intégré dans la blockchain pour deux raisons principales : D'une part, l'utilisation de mineurs implique une consommation importante de la puissance de calcul des nœuds mineurs, dans les RCSFs connus pour leurs ressources limitées; de tels calculs réduiront considérablement leur énergie ce qui aura pour conséquence de réduire la durée de vie du réseau. D'autre part, dans une blockchain traditionnelle, les

mineurs vérifieront les transactions pour empêcher les opérations frauduleuses; celles considérées comme non valides ne seront jamais intégrées à la blockchain. Dans B-Smart, l'intégration dans la blockchain de toutes les transactions nous permettra de détecter les nœuds malveillants tout en ayant une preuve irréversible de leur comportement frauduleux dans l'acheminement des transactions.

Lors de la validation, le contrat intelligent vérifiera que la transaction a suivi le chemin indiqué par le mécanisme de routage ainsi que les signatures et la cohérence des informations (Torres et al., 2018). Les résultats de cette analyse seront pris en compte lors de l'étape suivante.

5.5. Récompenser et punir

Après l'étape de validation, le contrat intelligent détient suffisamment d'éléments pour évaluer le comportement des différents nœuds de la transaction et leur attribuer les valeurs de réputation correspondantes. Plus précisément, lorsqu'un bloc est ajouté à la blockchain, le contrat intelligent est appliqué de manière automatique pour vérifier que les termes du contrat ont été respectés, dans notre cas, cela signifie que la transaction a été correctement effectuée.
Le contrat intelligent détient une table de réputation de tous les nœuds du réseau. Les valeurs des nœuds ayants participé à la dernière transaction sont mises à jour suivant leurs comportements lors de la transaction. La table des réputations contient trois colonnes : Nœud (N_i, identités de tous les nœuds du réseau), Facteur de récidive (Rec_i, pour compter le nombre de fois où le nœud s'est mal comporté, plus la valeur de ce compteur est élevée, plus la valeur de réputation du nœud malveillant diminuera de manière conséquente) et la troisième colonne contient la valeur de réputation(Rep_i^{last}, qui est la dernière valeur de réputation attribuée par le contrat intelligent au nœud i). La table est facile à entretenir, par exemple, dans une transaction lorsqu'un nœud passerelle transfère correctement un paquet pour le nœud suivant son comportement est qualifié de « Bon comportement», son compteur de récidive Rec_i est inchangé et sa valeur de réputation Rep_i^{last} est augmentée d'une valeur α. Sinon, si l'un des nœuds passerelle supprime le paquet ou le modifie avant de le transférer, son comportement est qualifié de malicieux « Mauvais comportement », sa valeur Rec_i est augmentée de un et sa valeur de réputation est divisée par l'exponentielle de la valeur (Rec_i). Cette dernière opération entraîne une réduction critique de la valeur de réputation du nœud malveillant. Les nœuds dont la valeur de réputation est inférieure à un seuil défini sont déclarés malveillants et placés sur une liste noire pour empêcher leur participation aux applications réseau.

Le processus d'attribution de valeurs de réputation par le contrat intelligent, bien que simple, permet de punir sévèrement les nœuds malveillants en rendant la réputation difficile à acquérir mais facile à perdre. Cela contribue à dissuader les nœuds malveillants de perturber les opérations du réseau et fournira à notre protocole une méthode efficace pour les détecter et les isoler. Ce processus permet également de motiver les nœuds intermédiaires à relayer correctement les informations.

La Figure 5.4 représente l'architecture simplifiée du contrat intelligent. L'algorithme correspondant est donné dans l'Algorithme 1 suivant :

Algorithme 1. The attribution of reputation values process

```
Begin
    For each Transaction_sensor (i)
    if Good_Behavior (i) then
        Rec_i= Rec_i
        Rep_i^last= Rep_i^last + α else
    Rec_i= Re_c^(i+1)
    Rep_i^last= Rep_i^last / exp(Rec_i)
End
```

L'automatisation du processus d'attribution des valeurs de réputation grâce à l'utilisation de contrat intelligent permet à notre protocole B-smart de créer des transactions sécurisées sans nécessiter la présence d'une autorité de contrôle centrale et sans l'intervention de nœuds de capteurs, tout en maintenant l'intégrité, la confidentialité et une résistance à un grand nombre d'attaques internes.

En résumé, afin d'avoir une vision claire du fonctionnement de notre schéma proposé, nous fournissons dans la Figure 5.5 un organigramme illustrant les différentes phases et l'ensemble des opérations de notre protocole B-Smart.

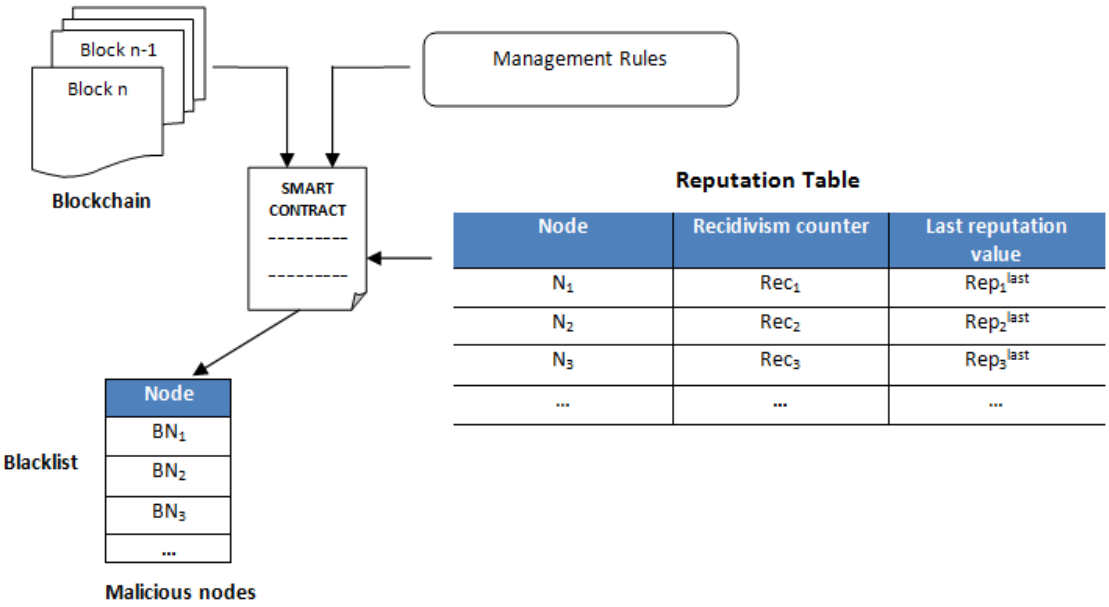


Fig 5. 4. Architecture simplifiée du smart contract dans le protocole B-Smart

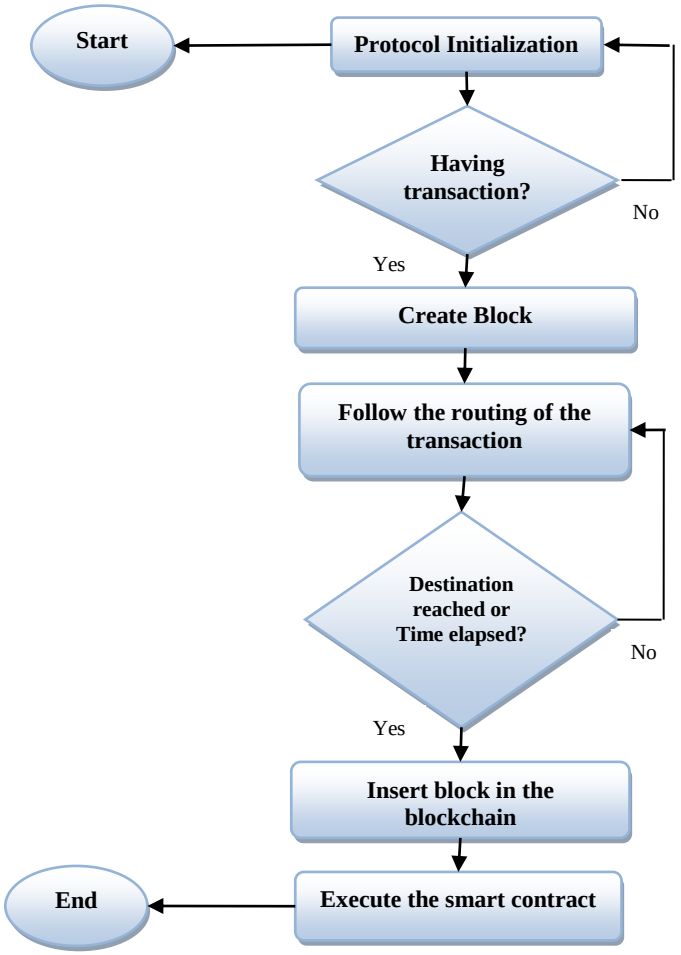


Fig 5. 5. Organigramme du protocole B-Smart

6. ANALYSE DES ATTAQUES ET DE LA SÉCURITÉ

Même si les mécanismes de confiance et de réputation sont efficaces, ils peuvent être victimes d'un grand nombre d'attaques que nous appellerons communément «attaques de confiance et de réputation». Ces attaques ont terni l'utilité de ces mécanismes et en ont découragé leur utilisation, en particulier dans les réseaux de capteurs. En effet, souffrant d'un manque important de sécurité, les réseaux de capteurs sont déjà vulnérables à un grand nombre d'attaques internes; l'utilisation de systèmes de confiance et de réputation ajoute un problème de sécurité supplémentaire. Notre protocole B-Smart aide à lutter contre les attaques de confiance et de réputation, permettant ainsi d'améliorer l'image des systèmes de confiance et de réputation afin qu'ils puissent agir efficacement pour sécuriser les réseaux de capteurs. Nous présenterons ci-dessous les principales attaques qui menacent ces mécanismes telles que définis dans (Yu et al., 2012), ainsi que les stratégies utilisées par notre protocole B-Smart afin de détecter et d'éliminer ces attaques.

6.1. Attaques de confiance et de réputation

Cette catégorie inclut toutes les attaques utilisant le mécanisme de confiance et de réputation pour effectuer des actions malveillantes. Ces attaques sont les suivantes :

6.1.1. Attaque badmouthing

Les mécanismes de confiance et de réputation utilisent souvent des nœuds recommandeurs afin d'obtenir des informations sur certains nœuds du réseau. Ces recommandeurs vont ainsi permettre de fournir des informations de seconde main très utiles pour que le nœud évaluateur puisse compléter sa vision sur un nœud qu'il connaît peu ou qu'il ne connaît pas. Dans le cas où ces recommandeurs sont honnêtes; ces informations indirectes vont améliorer considérablement l'efficacité des mécanismes de confiance et de réputation. Cependant, des nœuds malveillants peuvent s'introduire parmi ces recommandeurs, comme c'est le cas dans l'attaque badmouthing. Lors de cette attaque, l'attaquant va manipuler le système de confiance et de réputation et attribuer des valeurs de réputation injustement négatives aux nœuds légitimes du réseau. Cette attaque conduit à détruire la réputation des nœuds et à fausser les résultats du système de confiance. L'une des principales conséquences d'une telle attaque est l'isolement des nœuds légitimes des applications importantes du réseau en raison de leur valeur de réputation réduite, laissant ainsi plus de place aux nœuds malveillants, s'imposant ainsi en tant que leaders. Bien que notre protocole B-Smart ne repose pas sur des informations

de seconde main, il est tout aussi efficace, sinon plus, que les protocoles qui reposent sur ces informations indirectes, car le contrat intelligent offre une vue globale de toutes les transactions effectuées dans réseau et une disponibilité permanente des dernières mises à jour des valeurs de réputation. En n'impliquant pas de recommandation dans le calcul des valeurs de réputation, B-Smart est totalement résistant à ce type d'attaque.

6.1.2. Attaque ballot-stuffing

Comme lors de l'attaque précédente, le nœud malveillant va s'introduire parmi les nœuds recommandeurs. Cependant, contrairement à l'attaque badmouthing, il va attribuer des valeurs de réputation faussement positives à d'autres nœuds malveillants du réseau. Le but principal de cette attaque est de favoriser les nœuds malicieux en augmentant leur valeur de réputation afin d'accroître leur poids dans le réseau. L'automatisation du processus d'attribution des valeurs de réputation grâce à l'utilisation du smart contract protège notre protocole B-Smart contre ce type d'attaques.

6.1.3. Attaque on/off

Dans ce type d'attaque, le nœud malveillant procédera en deux phases, une phase "on" et une phase "off". Lors de la phase "on", l'attaquant lance l'attaque et agit négativement dans le réseau, tirant parti de sa réputation élevée lui permettant de rester indétectable pendant un certain temps. Au cours de la phase "off", l'attaquant se comportera correctement pour accroître sa réputation et gagner la confiance de son entourage. Cette attaque est efficacement gérée dans notre protocole B-Smart. En effet, lors de la phase off, l'attaquant aura un bon comportement ce qui lui vaudra une augmentation de sa valeur de réputation. Le smart contrat va donc augmenter sa valeur de réputation Rep_i^{last} d'une valeur α tant que son compteur de récidive $Rec_i = 0$. Au cours de la phase on, l'attaquant se comportera de manière malveillante; son facteur de récidive augmentera donc de 1 à chaque mauvais comportement. Le processus utilisé dans le calcul des valeurs de réputation dans notre protocole permet une légère augmentation des valeurs de réputation dans le cas de bons comportements, mais conduit à une diminution exponentielle de ces valeurs lors de comportements malicieux. Ainsi, même si le nœud malveillant générant une attaque on/off réussit à augmenter sa valeur de réputation, cette valeur passera sous le seuil d'honnêteté γ après seulement 1 à 2 mauvais comportements.

6.1.4. Attaque de comportement conflictuel "conflicting behavior"

Lors de cette attaque, le nœud malveillant va se comporter différemment avec les nœuds du réseau. En effet, il aura un bon comportement avec quelques nœuds, ce qui lui confèrera des

valeurs de réputation positives. Par contre, il se comportera de manière préjudiciable avec les autres nœuds qui le jugeront donc négativement. Le conflit se produira une fois que les nœuds du premier groupe échangeront sur la réputation de ce nœud malveillant avec les nœuds du deuxième groupe. Avoir différentes valeurs de réputation à propos du même nœud créera un conflit de confiance entre les nœuds du premier groupe par rapport à ceux du second et inversement. La problématique liée à cette attaque ne se pose pas dans notre protocole B-Smart. En effet, chaque nœud est jugé indépendamment dans chaque transaction. S'il a un bon comportement, sa réputation va augmenter, sinon celle-ci aura tendance à diminuer tragiquement. Par conséquent, quoi que l'attaquant fasse, il n'a aucun pouvoir de créer un conflit.

6.1.5. Attaque de comportement intelligent "intelligent behavior"

Dans cette attaque, le nœud malveillant est extrêmement intelligent. Il va en effet adapter son comportement en fonction de sa valeur de réputation. En conséquence, il se comportera différemment à chaque période de temps en fournissant de manière sélective de bons ou de mauvais services ou en attribuant des valeurs de recommandation faibles ou élevées en fonction du niveau de confiance. Pour tenter de rester indétectable face à notre protocole B-Smart, l'attaquant intelligent n'a pas le choix; il doit absolument adopter un bon comportement dans la majorité des cas. Dans le cas contraire, son facteur de récidive va continuellement augmenter et sa valeur de réputation aura de plus en plus de mal à être au-dessus du seuil de confiance γ. Une faible valeur de réputation implique l'isolement du réseau et l'intégration dans la liste noire. En conservant un bon comportement, l'attaquant n'aura aucun impact négatif sur le réseau.

6.1.6. Attaque de blanchiment "whitewashing"

Les systèmes de réputation sont connus pour être particulièrement vulnérables aux attaques de blanchiment. Lors de cette attaque, un nœud malveillant dont la valeur de réputation a considérablement diminué a la possibilité de ré-entrerdans le réseau avec une nouvelle identité et une nouvelle réputation. Pour parer à cette attaque, les nouveaux nœuds rejoignant le réseau après la phase d'initialisation ne sont pas considérés totalement dignes de confiance dans notre protocole. Ils doivent avant tout passer une période de test au cours de laquelle ils devront effectuer un grand nombre de tâches satisfaisantes afin d'obtenir une valeur de réputation normale. Ce processus est similaire à la procédure de «Preuve de travail» utilisée dans la blockchain et vise à décourager ce type d'attaques. En effet, en réentrant dans le réseau

avec une nouvelle identité, l'attaquant doit fournir beaucoup d'efforts et consommer beaucoup de ressources énergétiques.

En plus de résister aux attaques de confiance et de réputation, notre protocole B-Smart détecte parfaitement les attaques de routage. Nous décrivons ci-dessous les principales attaques de routage et les moyens utilisés par notre protocole B-Smart pour les combattre.

6.2. Attaques de routage

Nous incluons dans la catégorie des attaques de routage toutes les attaques qui menacent le routage des informations dans le réseau, en supprimant, modifiant, altérant ou contournant le chemin de transit des messages. Parmi ces attaques :

6.2.1. Usurpation, modification et retransmission des données

Dans ce type d'attaque, les nœuds malveillants visent à fabriquer des informations inexistantes, à modifier certaines données et à relire les messages afin de perturber le fonctionnement du réseau, en créant notamment des boucles de routage ou en augmentant le temps de latence. La détection de cette attaque dans B-Smart est réalisée en effectuant une comparaison entre les informations contenues dans l'entête du bloc (énoncé de la transaction et chemin défini par le protocole de routage) et les différentes phases d'exécution de la transaction à travers les différents nœuds. Une telle comparaison permet de constater immédiatement tout changement dans le corps ou dans l'acheminement de la transaction. B-Smart offre donc une détection efficace de ce type d’attaque.

6.2.2. Retransmission sélective

L'attaque de retransmission sélective englobe les attaques "selective forwarding" et l'attaque "grey hole" dans lesquelles le nœud malicieux refuse d'envoyer des messages à certains nœuds ou à certaines destinations respectivement. La comparaison effectuée par le contrat intelligent entre le parcours d'acheminement défini par le protocole de routage à l'initialisation et le chemin réel suivi par la transaction au cours de son exécution permet une détection efficace de tout écart par rapport au chemin initial. Le protocole B-Smart permet une détection efficace de ces deux types d’attaques et permet de punir sévèrement les nœuds responsables de comportements malveillants.

6.2.3. Sinkhole, blackcole et wormhole

Ces trois attaques partagent en commun le fait que le nœud malicieux se place dans un chemin de routage optimal afin de capturer un maximum de trafic. Les données transitant par ces nœuds malicieux sont récupérées et ne sont jamais retransmises. Dans l'attaque sinkhole, le nœud malicieux va se placer sur la route menant à la station de base afin de piéger un maximum de données. Pendant l'attaque blackhole, le nœud compromis va manipuler les tables de routage afin de paraitre plus proche et plus attrayant qu'en réalité pour attirer autant de données que possible. Lors de l'attaque wormhole, le nœud malicieux va tromper les nœuds sur les distances et influencer les tables de routage par la création de tunnels à faible latence. Le développement des chemins de routage dans notre protocole est indépendant des nœuds. Il est en effet réalisé grâce aux informations fournies par le contrat intelligent. Ainsi, un nœud souhaitant générer l'une de ces trois attaques n'a aucune influence sur les autres nœuds pour les forcer à transmettre les données par son intermédiaire. Dans le cas où l'un des attaquants est inclus dans un chemin de routage parce qu'il a une valeur de réputation élevée, sa valeur de réputation est carrément diminuée une fois qu'il effectue sa tâche malveillante. Il ne sera plus jamais choisi pour acheminer des informations.

6.2.4. Attaque Sybil

Lors de l'attaque sybil, l'attaquant introduit un grand nombre de nœuds malicieux dans le but d'avoir une influence disproportionnée dans le réseau. Bien que notre protocole B-Smart n'apporte pas une détection totale à une telle attaque, il permet néanmoins de décourager sa survenue grâce à l'utilisation du principe de "période de test". En effet, appliqué sur les nouveaux nœuds rejoignant le réseau après la phase d'initialisation, ce principe force ces nœuds à effectuer un grand nombre de tâches satisfaisantes pour obtenir une valeur de réputation normale. Similaire à la procédure de «Preuve de travail» utilisée dans la blockchain, le principe utilisé va forcer l'attaquant à fournir beaucoup d'efforts et à consommer beaucoup de ressources énergétiques dans le but de décourager la réalisation d'une telle attaque.

6.2.5. Attaque clone

Lors de cette attaque, l'attaquant va créer plusieurs répliques "clones" d'un nœud capturé du réseau. Ces répliques ont la particularité de posséder le même identifiant et les mêmes clés. Le smart contrat utilisé dans notre protocole B-Smart détient une table avec tous les identifiants des nœuds, leurs valeurs de réputation ainsi les compteurs de récidive

correspondants. Plus le nœud malveillant crée de répliques, plus le facteur de récidive du nœud cloné augmente rapidement et plus sa valeur de réputation diminue en conséquence. Dans le cas extrême où le nœud tentera de rester indétectable en ne créant qu'une seule réplique, notre protocole B-Smart détectera cette attaque tout aussi facilement étant donné que le compteur de récidive augmentera deux fois plus vite que lors des attaques générées par un seul nœud.

7. ÉVALUATION DES PERFORMANCES

Dans cette section, nous présentons les résultats de nos simulations montrant les performances de notre modèle de réputation. Tout d'abord, nous analysons le processus d'évaluation de la réputation dans notre protocole B-Smart. Deuxièmement, nous vérifions l'efficacité de notre protocole en considérant l'impact des deux principales attaques : l'attaque on/off et l'attaque conflecting behavior. A cet effet, une comparaison est effectuée entre B-Smart, RaRTrust (Labraoui et al., 2015) et RFSN (Ganeriwal et al., 2008) dans le scénario d'attaque "on/off" et entre B-Smart et ATSN (Chen et al., 2007) dans le scénario de l'attaque conflicting behavior.

Les paramètres de simulation sont configurés comme suit. Tous les nœuds du réseau sont initialisés avec la même valeur de réputation égale à 0,5 et sont considérés comme dignes de confiance. Le comportement des nœuds est évalué en fonction de toutes les transactions auxquelles ils participent. Un facteur de récidive Rec_i est attribué à chaque nœud du réseau. Ce compteur est utilisé pour enregistrer le nombre de mauvais comportements effectués par le nœud. La valeur de réputation du nœud i dépendra entièrement de la valeur de ce compteur. Les paramètres par défaut utilisés dans nos simulations sont résumés dans le Tableau 5.2.

Tableau 5. 2. Paramètres de simulation

Parameter	Default Value
Area (m^2)	100 x 100
Number of nodes	100
Radio Range (m)	25
α	0.02
β	0.3

7.1. Analyse de l'évolution de la réputation

Les protocoles de confiance et de réputation existants sont fondés sur l'utilisation des informations directes ou sur les informations directes et indirectes lors du calcul des valeurs de confiance. Les deux méthodes présentent plusieurs avantages mais surtout de nombreux inconvénients. En effet, l'utilisation exclusive des informations directes protège efficacement les protocoles de plusieurs attaques notamment des attaques de recommandations malhonnêtes. Cependant, cette approche nécessite beaucoup de temps afin d'établir les valeurs de réputation des différents nœuds et ces valeurs prendront également beaucoup de temps à diminuer, permettant ainsi à l'attaquant de rester longtemps dans le réseau. D'autre part, l'utilisation des informations indirectes obtenues grâce aux recommandeurs permet de fournir des informations supplémentaires aux nœuds sur d'autres nœuds qu'ils connaissent peu ou qu'ils ne connaissent pas. Ces informations supplémentaires vont ainsi permettre d'accélérer le processus d'établissement des valeurs de réputation dans le réseau. Cependant, l'utilisation d'une telle approche expose le réseau à l'éventuelle présence de nœuds malicieux parmi les recommandeurs. L'automatisation du processus d'attribution des valeurs de réputation dans notre protocole B-Smart permet de bénéficier des avantages des deux précédentes méthodes tout en étant résistant à leurs inconvénients. En effet, bien que ne faisant pas appel aux informations indirectes dans notre protocole, le smart contrat garantie une disponibilité et une accessibilité à ces valeurs à tout moment et pour tous les nœuds du réseau. Il offre en plus une sécurité permanente pour ces valeurs et une protection efficace contre d'éventuelles manipulations malicieuses. Notre processus est non seulement résistant aux attaques de recommandations malhonnêtes mais aussi à l'ensemble des attaques des mécanismes de confiance et de réputation.

Afin de prouver la légitimité de notre raisonnement, nous analysons dans cette section le processus d'attribution des valeurs de réputation dans notre protocole B-Smart. Nous effectuons à cet effet une comparaison entre notre protocole B-Smart et les protocoles RFSN (Ganeriwal et al., 2008) et RaRTrust (Labraoui et al., 2015) utilisant tous deux les informations directes (DT) et indirectes (IT) lors du calcul des valeurs de réputation.

- Cas (1). Le scénario est le suivant : nous effectuons une analyse sur l'évolution des valeurs de réputation d'un nœud donné i. Ce nœud est un nœud légitime du réseau, initialisé avec une valeur de réputation égale à 0,5. Ce nœud adopte un bon comportement pendant les 40 premières unités de temps. À un certain moment $t \in]40,45]$ le nœud i est capturé, reprogrammé puis réintroduit dans le réseau en tant que nœud malicieux.

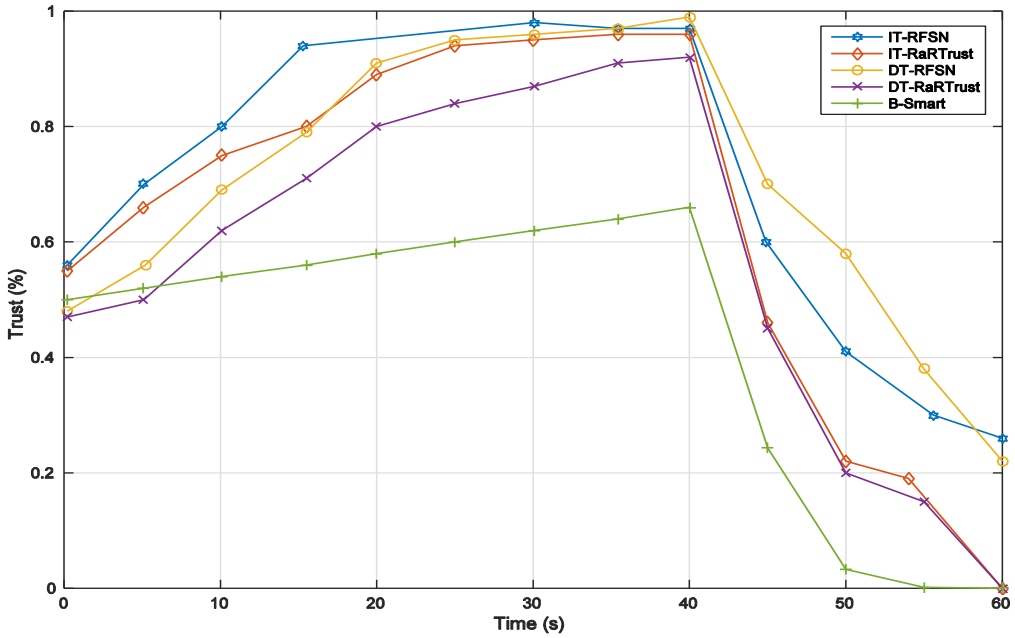


Fig 5. 6. Évolution des valeurs de réputation

La Figure 5.6 montre clairement que les valeurs de réputation du nœud i augmentent lentement dans B-Smart par rapport aux autres protocoles. Cela peut s'expliquer par le fait que la valeur de réputation augmente d'une valeur α à chaque "bon comportement" du nœud, une augmentation lente et linéaire incitant les nœuds à se comporter correctement afin d'augmenter leurs valeurs de réputation. D'autre part, au premier "mauvais comportement" la valeur de réputation du nœud diminuera plus rapidement dans B-Smart que dans les protocoles RFSN et RaRtrust, permettant ainsi une détection plus rapide des nœuds malveillants du réseau. De tels résultats sont possibles grâce à l'automatisation du processus d'attribution des valeurs de réputation dans notre protocole B-Smart grâce à l'utilisation d'une entité indépendante, impartiale et sécurisée, à savoir le «contrat intelligent». Un procédé permettantd'accélérer la détection des attaques tout en offrant une disponibilité et une sécurisation des valeurs de réputation des différents nœuds du réseau.

7.2. Analyse des attaques de confiance et de réputation

Le principal objectif de l'automatisation du processus d'attribution des valeurs de réputation dans notre protocole B-Smart est de renforcer la résistance des mécanismes de confiance et de réputation contre la manipulation abusive de ces derniers par les attaquants désireux de lancer une multitude d'attaques afin de nuire au réseau.

Dans cette section, nous analysons la résistance de notre protocole face à deux principales attaques, à savoir : l'attaque on/off et l'attaque conflicting behavior. Les attaques de recommandations malhonnêtes incluant les attaques badmouthing, ballot-stuffing et collusion ne sont pas prises en compte dans nos simulations étant donné que notre protocole est parfaitement résistant à de telles attaques. En effet, l'utilisation du smart contrat évite aux nœuds de devoir demander les valeurs de réputation auprès des recommandeurs.

7.2.1. Résistance àl'attaque "on/off"

Lors de l'attaque on/off, les nœuds malveillants se comportent correctement et malicieusement alternativement, dans l'espoir de rester indétectables tout en causant le plus de dommages possible. En effet, une fois que le nœud malveillant acquiert une valeur de réputation élevée lors de la phase « off »de l'attaque grâce à son comportement satisfaisant i.e. transmet correctement les messages, il commence la phase « on » de l'attaque en agissant de manière malveillante en supprimant ou en modifiant les messages en transit. Le scénario de simulation de cette attaque est le suivant :

- Cas (2). Nous considérons dans nos simulations un nœud malveillant i. Dans la phase « off », le nœud i transmet correctement les messages dans chaque transaction où il est impliqué. Il lance la phase « on » de l'attaque à tps=6 unités de temps. Ce cycle « on » de l'attaque est immédiatement suivi d'un cycle « off » à tps=10.

La Figure 5.7 présente les principaux résultats des simulations effectuées entre notre protocole B-Smart et les protocoles ATSN (Chen et al., 2007) et RFSN (Ganeriwal et al., 2008). Lors de la phase "off" de l'attaque, la valeur de réputation du nœud i va augmenter plus lentement dans notre protocole B-Smart que dans les deux autres protocoles. Lors de la phase active "on" de l'attaque, la valeur du compteur de récidive Rec_i va s'incrémenter à chaque mauvais comportement du nœud engendrant une diminution critique de la valeur de réputation du nœud i. Cette diminution exponentielle offre à notre protocole B-Smart une détection rapide et efficace des nœuds malveillants. De tels résultats permettent de prouver que dans notre protocole B-Smart la réputation est difficile à acquérir et facile à perdre. Bien que la valeur de réputation du nœud i décroit plus rapidement dans le protocole RFSN que dans B-Smart, cette dernière augmente plus rapidement lors de la phase "off" de l'attaque permettant ainsi au nœud i de retrouver rapidement une valeur de réputation élevée lui permettant de relancer rapidement une nouvelle phase active de l'attaque. En effet, contrairement au protocole RFSN, B-Smart se souvient du comportement malveillant du

nœud puisque la valeur du facteur de récidive associé au nœud i est stockée de manière permanente dans le contrat intelligent détenu par la blockchain. Ainsi, même si au cours de la phase suivante, le nœud malveillant parvient à augmenter légèrement sa valeur de réputation, cette dernière diminuera encore plus fortement dans la phase "on" suivante, étant donné que le compteur de récidive augmente continuellement et n'est jamais remis à zéro. Nous pouvons donc conclure que notre protocole B-Smart est plus efficace que ATSN et RFSN pour la détection de l'attaque on/off. Son principe de fonctionnement basé sur l'utilisation d'un compteur de récidive ainsi que d'un contrat intelligent permet une détection de plus en plus rapide de cette attaque d'un cycle à un autre.

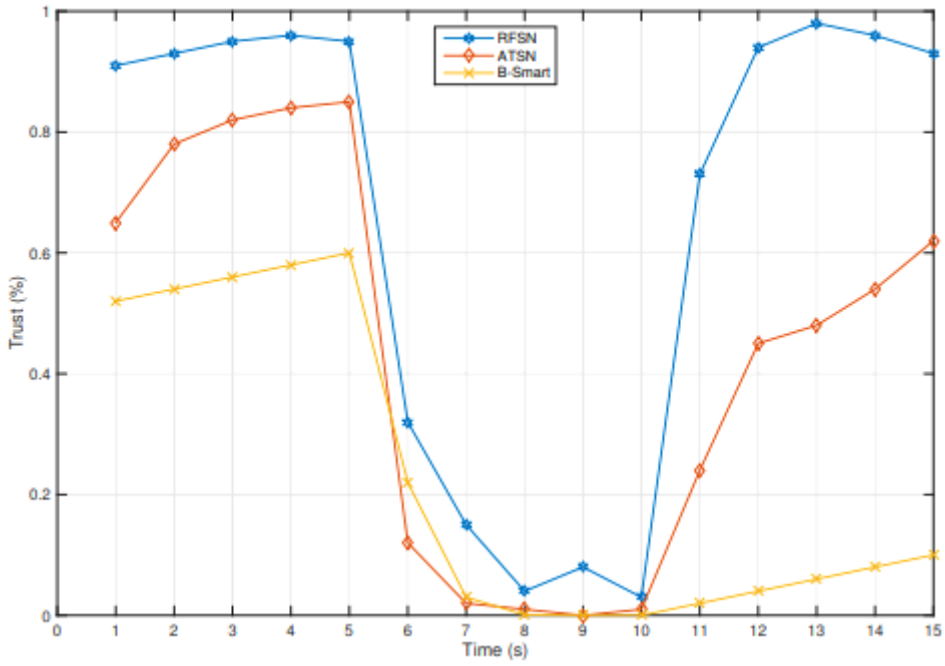


Fig 5. 7. Attaque on/off lancée par le nœud i

7.2.2. Résistance à l'attaque conflicting behavior

Bien qu'insidieuse, l'attaque conflicting behavior n'a pas suscité beaucoup d'intérêt de la part des chercheurs travaillant dans le domaine de la sécurité dans les mécanismes de confiance et de réputation dans les RCSFs. Cette attaque a le pouvoir de créer des conflits entre les groupes de nœuds, créant ainsi un manque de confiance mutuelle entre eux. Lors de cette attaque, un nœud malveillant i se comporte correctement avec un groupe de nœuds (A, B et C) en transmettant correctement les messages des transactions incluant ces nœuds, ce qui lui vaudra des valeurs de réputations élevées de ces derniers. En parallèle, ce même nœud i se comporte d'une manière malicieuse avec un deuxième groupe de nœuds (E et F), en

supprimant, altérant ou modifiant les messages de ces nœuds. Ils lui attribueront donc des valeurs de réputation négatives. Le conflit se produit lorsqu'un nœud du premier groupe (A) échange avec un nœud du deuxième groupe (E) sur la réputation de ce nœud malveillant. Le nœud A, qui est sûr que i est un nœud légitime, pensera que le nœud E est entrain de mentir sur la réputation du nœud i en tentant de la diminuer, et jugera E comme malveillant. Le nœud E de son côté va aussi penser que le nœud A est entrain d'augmenter la valeur de réputation du nœud i et jugera A comme malhonnête. De tels conflits ont pour conséquence de briser les relations de confiance entre les nœuds du réseau, perturbant ce dernier et offrant un climat d'instabilité idéal pour les attaquants.

- Cas (3). Dans ce scénario, le nœud i lance une attaque de comportement conflictuelle. Il se comportera différemment avec deux groupes de nœuds distincts.

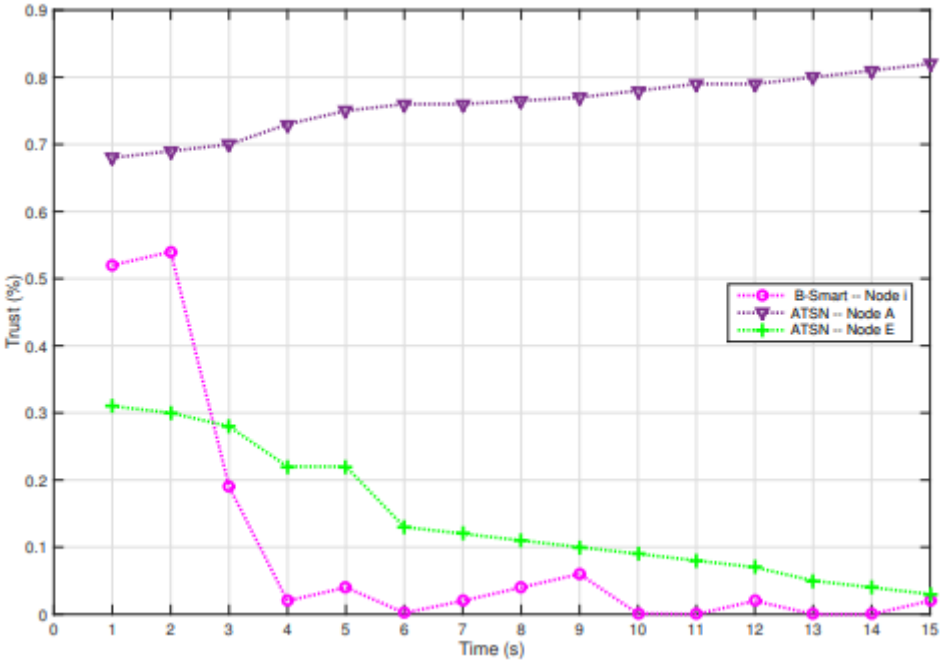


Fig 5. 8. Attaque conflicting behavior lancée par le nœud i

La Figure 5.8 montre les résultats des simulations effectuées lors de l'attaque conflicting behavior. Dans le protocole ATSN, le nœud A continue de communiquer et de juger positivement le nœud i tant que ce dernier adopte un comportement correct lors des échanges. Contrairement au nœud A, le nœud E va attribuer des valeurs de réputation négatives au nœud i en raison de son comportement malveillant et cesser de coopérer avec ce dernier. Le principe utilisé dans le protocole ATSN n'est pas tout à fait correct pour deux raisons principales : D'une part, le nœud i est un nœud malveillant et le fait de continuer à communiquer avec lui

expose le nœud A, les nœuds du premier groupe ainsi que l'ensemble du réseau à divers dommages. D'autre part, en faisant pleinement confiance au nœud malveillant i, les nœuds du premier groupe s'exposent à un conflit avec les nœuds du second groupe. Un manque de confiance mutuel pouvant engendrer une révocation des nœuds légitimes du réseau laissant ainsi plus de chance aux nœuds malicieux de prendre le contrôle du réseau. Dans notre protocole B-Smart, le contrat intelligent est chargé de calculer toutes les valeurs de réputation en détenant pour chaque nœud un compteur de récidive et la valeur de réputation appropriée. Ces valeurs sont mises à jour après chaque nouvelle transaction. Une telle automatisation d'assignation des valeurs de réputation permet de juger de manière impartiale les comportements des nœuds. Les résultats de simulation de notre protocole B-Smart démontrent clairement cet esprit de fonctionnement. En effet, le nœud est jugé indépendamment dans chaque transaction et sa valeur de réputation dépend entièrement de son comportement lors de ces transactions. Par conséquent, même s'il agit de manière malicieuse, le nœud malveillant n'a aucun pouvoir de créer un conflit.

8. CONCLUSION

L’efficacité des systèmes de confiance et de réputation dans les réseaux de capteurs n’est plus à démontrer. Cependant, le développement de tels mécanismes crée des problèmes de sécurité supplémentaires pour les RCSFs. En effet, des attaquants internes peuvent facilement s'introduire dans ces systèmes, manipuler les valeurs de réputation à leur guise et fausser le calcul des valeurs de réputation. De telles menaces qui hélas sont bien réelles peuvent engendrer des dégâts irréversibles pour tout le réseau. Nous avons présenté dans ce chapitre, un nouveau mécanisme de réputation basé sur l'utilisation de blockchain afin de résoudre le problème de la manipulation abusive des valeurs de réputation par les nœuds malveillants. Dans notre protocole B-Smart, le calcul des valeurs de réputation est confié à un smart contrat; une entité indépendante et sécurisée, permettant de juger le comportement des nœuds de manière impartiale et de leur attribuer les valeurs de réputation correspondantes. La sauvegarde de toutes les transactions effectuées dans le réseau ainsi que du smart contrat dans une structure blockchain garantira leur durabilité, leur intégrité et leur résistance à toute modification intentionnelle par des nœuds malveillants. L'automatisation du processus d'assignation des valeurs de réputation, grâce au contrat intelligent, a offert à notre protocole une grande résistance ainsi qu'une détection efficace de nombreuses attaques internes. En

effet, l'analyse de la sécurité démontre la résilience de B-Smart contre les attaques de confiance et de réputation ainsi que les attaques de routage. En outre, les différents scénarios de simulation ont prouvé l'efficacité de notre protocole dans divers scénarios d'attaques.

CONCLUSION GÉNÉRALE

➢ SYNTHÈSE

La sécurité dans les réseaux de capteurs est devenue un domaine indissociable des autres domaines des RCSFs. Il devient en effet, inenvisageable d'aborder des thématiques telles que l'agrégation, la localisation, le routage ou le clustering sans prendre en compte le côté sécuritaire. Un tel manquement va laisser planer de gros doutes et de grandes interrogations sur la véracité et l'exactitude des résultats obtenus. Connus pour être en effet une cible idéale pour de nombreuses attaques toujours plus sophistiquées et de plus en plus intelligentes, les réseaux de capteurs se retrouvent démunis face à de telles attaques agissant de manière sournoise et causant un maximum de dégâts tout en restant indétectables. La sécurisation des réseaux de capteurs contre les attaques de manière générale et particulièrement contre les attaques internes a suscité l'intérêt ces dernières années de nombreux chercheurs et une multitude de contributions ont été élaborées dans le domaine.

La première partie de cette thèse est consacrée à la présentation des bases de la thématique étudiée, à savoir, les réseaux de capteurs, la sécurité ainsi que les attaques internes.

Nous avons débuté dans le premier chapitre par une étude générale des réseaux de capteurs en présentant les principaux concepts sur lesquels reposent ces réseaux ainsi que les différents challenges liés à la conception d'un RCSF. Nous avons ensuite abordé la notion de mobilité ainsi que ses avantages et inconvénients dans les réseaux de capteurs.

Dans le second chapitre, nous avons introduit la problématique de la sécurité dans les RCSFs, les principaux défis liés à la conception de protocoles de sécurité ainsi que les vulnérabilités de ces réseaux. Nous avons ensuite présenté les attaques internes, des attaques aux profiles multiples et aux conséquences désastreuses pour le réseau. Nous avons énuméré les principaux mécanismes utilisés pour la détection de telles attaques en pointant leurs limites ainsi que les axes de recherche prometteurs. Les systèmes de confiance et de réputation se sont distingués dans notre étude comme méthode prometteuse. Cependant, de tels systèmes peuvent à leur tour être une cible potentielle d'attaquants internes. Une solution idéale serait de combiner entre ces systèmes et des axes innovants afin de profiter des avantages et réduire les inconvénients des uns et des autres.

Nous avons consacré le troisième chapitre à un état de l'art dédié aux protocoles traitant les attaques de recommandations malhonnêtes, un type particulier d'attaques internes incluant les attaques : badmouthing, ballot-stuffing et collusion. L'étude et l'analyse des protocoles

existant nous ont permis de proposer une nouvelle classification de ces protocoles, à savoir, protocoles de prévention et protocoles de détection. En se privant des informations indirectes et en n'utilisant que des valeurs positives ou négatives, les méthodes préventives préviennent l'occurrence de telles attaques mais restent toutefois vulnérables aux attaquants intelligents cherchant à rester indétectables. Les méthodes de détection incluant les méthodes de déviation et l'utilisation de facteurs de confiance, permettent de détecter ces attaques, cependant, ces protocoles confondent entre les recommandations erronées résultant d'un disfonctionnement physique et entre les recommandations malhonnêtes ayant un but malicieux. Une telle confusion engendre des taux de faux positifs et de faux négatifs élevés semant un vent de discorde entre les nœuds.

La deuxième partie de cette thèse est consacrée aux contributions que nous avons apportez dans le domaine de la détection des attaques internes dans les réseaux de capteurs. Nous avons traité dans cette thèse deux problématiques importantes, à savoir, la sécurité contre les attaques de recommandations malhonnêtes dans les RCSFs et la sécurité des systèmes de confiance et de réputation de manière générale.

Pour sécuriser les réseaux de capteurs contre les attaques de recommandations malhonnêtes, nous avons proposé un nouveau protocole de détection nommé Bee-Trust Scheme (BTS). Le protocole BTS résout le problème des recommandations malhonnêtes sous un nouvel angle en combinant entre la métaheuristique modélisant le comportement des abeilles mellifères lors de la recherche de leur nourriture et les systèmes de confiance et de réputation. En appliquant le principe de "*la survie du plus fort*", la qualité (fitness) de chaque solution est évaluée selon deux concepts : une révision du modèle de nuage (cloud model) ainsi qu'un paramètre de chronométrie cognitive. Une telle association a permis à notre protocole de distinguer efficacement entre les recommandations malhonnêtes et les recommandations erronées et garantir des taux très bas de faux positifs et de faux négatifs.

Notre deuxième contribution consiste à améliorer la résistance des systèmes de confiance et de réputation contre les attaques dont ils sont victimes. Un moyen pour nous de les rendre plus efficaces afin qu'ils puissent soutenir au mieux les réseaux de capteurs dans leur lutte contre les attaques internes. Dans cette optique, nous avons élaboré un nouveau mécanisme de réputation à la fois robuste et intelligent. Notre protocole nommé B-Smart résout le problème de la manipulation abusive des valeurs de réputation. Un problème connu pour être à l'origine de nombreuses attaques dont les attaques de recommandations malhonnêtes. L'idée principale de notre protocole B-Smart est de confier la gestion des valeurs de réputation à un contrat intelligent, un smart contrat permettant de suivre l’évolution des différentes transactions du

réseau et d'attribuer aux nœuds les valeurs de réputation correspondantes en fonction de leur comportement. Un facteur de récidive est appliqué lors du calcul des valeurs de réputation afin de pénaliser les nœuds malveillants en réduisant sévèrement leurs valeurs de réputation. L'enregistrement de ce contrat dans une structure blockchain permet de garantir sa durabilité, son intégrité et son efficacité. Ainsi sauvegardé, le contact est protégé des manipulations abusives des attaquants internes. Les différentes simulations ont prouvé l'efficacité de notre protocole face à de nombreuses attaques dont les attaques de confiance et de réputation ainsi que les attaques de routage.

➢ PERSPECTIVES

La détection des attaques internes dans les réseaux de capteurs sans fil est un axe de recherche très fertile et d'une importance capitale. Cependant, l'élaboration d'un protocole de sécurité efficace dans les RCSFs est un réel challenge. Entre les ressources limitées des capteurs, l'environnement hostile et le nombre important d'attaques internes, il faut souvent faire un compromis entre efficacité et surcoût. Ce besoin de sécurité a permis l'élaboration de plusieurs protocoles de contre-mesure. Cependant, il n'existe pas encore de solution optimale permettant de remédier à cette problématique de manière définitive. En effet, chaque proposition à ses propres limites ainsi que ses propres contraintes. Afin d'améliorer le rendement des protocoles de détection, certains axes de recherche doivent encore être explorés offrants ainsi de multiples perspectives à ce domaine.

Les métaheuristiques ont permis ces dernières années d'apporter des solutions optimales pour une large variété de problèmes d'optimisation. Elles permettent en effet de trouver une approximation de la meilleure solution en tentant d'apprendre les caractéristiques du problème, en réduisant la taille effective de l'espace de recherche et en explorant cet espace de manière efficace. L'utilisation des métaheuristiques dans le domaine de la sécurité dans les réseaux de capteurs n'est qu'à ses débuts, mais il va sans dire que le nombre important de métaheuristiques existantes aux différentes caractéristiques et aux vastes étendues offrent sans doute des dizaines de potentielles solutions pour la problématique de la détection des attaques internes dans les réseaux de capteurs sans fil.

Technologie innovante de ces dix dernières années, la blockchain est utilisée dans de nombreux domaines tels que : la location ou vente de voitures, l'authentification des diplômes, les banques, dans le domaine des prévisions et dans les contrats intelligents. Les possibilités offertes par cette technologie sans nombreuses et révolutionnaires. L'utilisation d'une

telle notion dans les réseaux de capteurs est encore au stade théorique. Nous avons réalisé dans cette thèse juste une ébauche de cette technologie, les opportunités offertes par la blockchain pour le domaine de la sécurité sont aussi vastes que variées.

Combiner entre les domaines de recherches dits classiques tels que les méthodes cryptographiques, les IDS ou les mécanismes de confiance et de réputation et les domaines innovants tels que les méthaheuristiques, la blockchain aussi bien que la psychologie ou la théorie des jeux est une autre perspective intéressante pour une détection efficace des attaques internes dans les réseaux de capteurs sans fil. Plusieurs combinaisons sont possibles afin de profiter des avantages et de minimiser les inconvénients de chaque approche. Trouver la/les combinaisons idéales permettra de se rapprocher, ou mieux encore, de trouver "la solution optimale" permettant de résoudre la problématique de la sécurité dans les réseaux de capteurs sans fil.

Un autre point essentiel, est le passage à l'échelle, pratiquement toutes les solutions de sécurité proposées sont praticables uniquement pour des réseaux dont la taille ne dépasse pas 1000 capteurs. Cela est sûrement du au surcoût induit par les primitives de sécurité. Ce sera intéressant d'examiner le comportement de ces solutions dans les applications nécessitant un très grand nombre de capteurs.

Enfin, l'utilisation de la technologie « *energy harvesting* » selon laquelle l'énergie est tirée de sources externes va permettre sans doute l'élaboration de solutions plus développées et plus robustes.

BIBLIOGRAPHIE

Abbasy, M. B., Barrantes, G., & Marín, G. (2011, December). Time delay performance analysis of sensor allocation strategies on a WSN. In Proceedings of the 1st International Conference on Wireless Technologies for Humanitarian Relief (pp. 135-140). ACM.

Agah, A., Das, S. K., & Basu, K. (2004). A game theory based approach for security in wireless sensor networks. In Performance, Computing, and Communications, 2004 IEEE International Conference on (pp. 259-263). IEEE.

Ahmed, M. R., Huang, X., & Sharma, D. (2012). A taxonomy of internal attacks in wireless sensor network. Memory (Kbytes), 128, 48.

Ahmed, M. R. (2014). Protecting Wireless Sensor Networks from Internal Attacks (Doctoral dissertation).

Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E., 2002. Wireless sensor networks: a survey. Comput. Network. 38 (4), 393–422.

Alfantookh, A. A. (2006). DoS attacks intelligent detection using neural networks. Journal of King Saud University-Computer and Information Sciences, 18, 31-51.

Alrashed, S. (2017). Reducing power consumption of non-preemptive real-time systems. Journal of Supercomputing, 73(12), 5402-5413.

Alzaid, H., Foo, E., & Gonzalez Nieto, J. (2008). RSDA: reputation-based secure data aggregation in wireless sensor networks.

Alzaid, H., Alfaraj, M., Ries, S., Jøsang, A., Albabtain, M., & Abuhaimed, A. (2013, June). Reputation-based trust systems for wireless sensor networks: A comprehensive review. In IFIP International Conference on Trust Management (pp. 66-82). Springer, Berlin, Heidelberg.

Ari, A.A.A., Labraoui, N., Yenke, B.O., Gueroui, A., 2018. Clustering algorithm for wireless sensor networks: the honeybee swarms nest-sites selection process based approach. Int. J. Sens. Netw. 27 (1), 1–13.

Ari, A.A.A., Damakoa, I., Gueroui, A., Titouna, C., Labraoui, N., Kaladzavi, G., & Yenké, B. O. (2017). Bacterial foraging optimization scheme for mobile sensing in wireless sensor networks. International Journal of Wireless Information Networks, 24(3), 254-267.

Bagchi, R. (2017). Using Blockchain Technology and Smart Contracts for Access Management in IoT devices.

Bahga, A., & Madisetti, V. K. (2016). Blockchain platform for industrial internet of things. Journal of Software Engineering and Applications, 9(10), 533.

Benet, J. (2014). IPFS-content addressed versioned, P2P file system. arXiv preprint arXiv:1407.3561.

Boudec, J. Y. L., 2004. A robust reputation system for p2p and mobile ad-hoc networks. In Proceedings of the 2nd Workshop on the Economics of Peer-to-Peer Systems.

Boukerche, A., & Li, X. (2005). An agent-based trust and reputation management scheme for wireless sensor networks. In Global Telecommunications Conference, 2005. GLOBECOM'05. IEEE (Vol. 3, pp. 5-pp). IEEE.

Boukerch, A., Xu, L., & El-Khatib, K. (2007). Trust-based security for wireless ad hoc and sensor networks. Computer Communications, 30(11-12), 2413-2427.

Boukerche, A., & Ren, Y. (2008). A trust-based security system for ubiquitous and pervasive computing environments. Computer Communications, 31(18), 4343-4351.

Buchegger, S., & Le Boudec, J. Y. (2002, June). Performance analysis of the CONFIDANT protocol. In Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing (pp. 226-236). ACM.

Camp, T., Boleng, J., & Davies, V. (2002). A survey of mobility models for ad hoc network research. Wireless communications and mobile computing, 2(5), 483-502.

Che, S., Feng, R., Liang, X., & Wang, X. (2015). A lightweight trust management based on Bayesian and Entropy for wireless sensor networks. Security and Communication Networks, 8(2), 168-175.

Chen, H., Wu, H., Zhou, X., &Gao, C. (2007, July). Agent-based trust model in wireless sensor networks. In null (pp. 119-124). IEEE.

Chen, H. (2009). Task-based trust management for wireless sensor networks. International Journal of Security and its applications, 3(2), 21-26.

Chen, S., Zhang, Y., Liu, Q., & Feng, J. (2012). Dealing with dishonest recommendation: The trials in reputation management court. Ad Hoc Networks, 10(8), 1603-1618.

Clausen, T., & Jacquet, P. (2003). Optimized link state routing protocol (OLSR) (No. RFC 3626).

Crane, E., et al., 1980. A Book of Honey. Oxford University Press.

Crosby, G. V., Pissinou, N., & Gadze, J. (2006, April). A framework for trust-based cluster head election in wireless sensor networks. In null (pp. 13-22). IEEE.

Crosby, G. V., Hester, L., & Pissinou, N. (2011). Location-aware, Trust-based Detection and Isolation of Compromised Nodes in Wireless Sensor Networks. IJ Network Security, 12(2), 107-117.

Dellarocas, C. (2000, October). Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior. In Proceedings of the 2nd ACM conference on Electronic commerce (pp. 150-157). ACM.

Deyi, L., Haijun, M., & Xuemei, S. (1995). Membership clouds and membership cloud generators [J]. Journal of Computer Research and Development, 6.

Djallel Eddine, B. (2013). Une approche Inter-Couches (cross-layer) pour la Sécurité dans les RCSF (Doctoral dissertation).

Djeffal, A. (2012). Utilisation des méthodes Support Vector Machine (SVM) dans l'analyse des bases de données (Doctoral dissertation, Université Mohamed Khider-Biskra).

Dominicy, Y. (2012). Théorie des jeux: représentations et types de jeux.

Drira, W., Bekara, C., & Laurent, M. (2008). Sécurité dans les réseaux de capteurs sans fil: conception et implémentation(Doctoral dissertation, Dépt. Logiciels-Réseaux (Institut Mines-Télécom-Télécom SudParis); Services répartis, Architectures, MOdélisation, Validation, Administration des Réseaux (Institut Mines-Télécom-Télécom SudParis-CNRS)).

Esch, J. (2010). Prolog to a survey of trust and reputation management systems in wireless communications. Proceedings of the IEEE, 98(10), 1752-1754.

Fang, W., Zhang, C., Shi, Z., Zhao, Q., & Shan, L. (2016). BTRES: Beta-based Trust and Reputation Evaluation System for wireless sensor networks. Journal of Network and Computer Applications, 59, 88-94.

Faye, Y. (2014). Algorithmes d'authentification et de cryptographie efficaces pour les réseaux de capteurs sans fil (Doctoral dissertation, Université de Franche-Comté).

Feng, J., Zhang, Y., & Wang, H. (2010). A trust management model based on bi-evaluation in p2p networks. IEICE TRANSACTIONS on Information and Systems, 93(3), 466-472.

Feng, R., Xu, X., Zhou, X., & Wan, J. (2011). A trust evaluation algorithm for wireless sensor networks based on node behaviors and ds evidence theory. Sensors, 11(2), 1345-1360.

Ganeriwal, S., Balzano, L. K., & Srivastava, M. B. (2008). Reputation-based framework for high integrity sensor networks. ACM Transactions on Sensor Networks (TOSN), 4(3), 15.

Gilbert, E. P. K., Kaliaperumal, B., Rajsingh, E. B., & Lydia, M. (2018). Trust based data prediction, aggregation and reconstruction using compressed sensing for clustered wireless sensor networks. Computers & Electrical Engineering.

Gregg, A. P. (2007). When vying reveals lying: The timed antagonistic response alethiometer. Applied Cognitive Psychology: The Official Journal of the Society for Applied Research in Memory and Cognition, 21(5), 621-647.

Gregg, A. P., Mahadevan, N., Edwards, S. E., & Klymowsky, J. (2014). Detecting lies about consumer attitudes using the timed antagonistic response alethiometer. Behavior research methods, 46(3), 758-771.

Gura, N., Patel, A., Wander, A., Eberle, H., & Shantz, S. C. (2004, August). Comparing elliptic curve cryptography and RSA on 8-bit CPUs. In International workshop on cryptographic hardware and embedded systems (pp. 119-132). Springer, Berlin, Heidelberg.

Haas, Z. J., & Pearlman, M. R. (2000). Providing ad-hoc connectivity with the reconfigurable wireless networks. Ad Hoc Networks. Addison Wesley Longman.

Haddad, E. (2011). Détection de la retransmission sélective sur les réseaux de capteurs.

Hamma, T., Katoh, T., Bista, B. B., & Takata, T. (2006, September). An efficient zhls routing protocol for mobile ad hoc networks. In Database and Expert Systems Applications, 2006. DEXA'06. 17th International Workshop on (pp. 66-70). IEEE.

Han, G., Jiang, J., Shu, L., Niu, J., & Chao, H. C. (2014). Management and applications of trust in Wireless Sensor Networks: A survey. Journal of Computer and System Sciences, 80(3), 602-617.

Hartman, J. H., Murdock, I., & Spalink, T. (1999). The Swarm scalable storage system. In Distributed Computing Systems, 1999. Proceedings. 19th IEEE International Conference on (pp. 74-81). IEEE.

Hur, J., Lee, Y., Youn, H., Choi, D., & Jin, S. (2005, February). Trust evaluation model for wireless sensor networks. In Advanced Communication Technology, 2005, ICACT 2005. The 7th International Conference on (Vol. 1, pp. 491-496). IEEE.

Intanagonwiwat, C., Govindan, R., & Estrin, D. (2000, August). Directed diffusion: A scalable and robust communication paradigm for sensor networks. In Proceedings of the 6th annual international conference on Mobile computing and networking(pp. 56-67). ACM.

Jamont, J. P., & Occello, M. (2006). Une approche multi-agents pour la gestion de la communication dans les réseaux de capteurs sans fil. Revue des Sciences et Technologies de l'Information-Série TSI: Technique et Science Informatiques, 25(5), 661-690.

Jaramillo, J. J., & Srikant, R. (2007, September). DARWIN: distributed and adaptive reputation mechanism for wireless ad-hoc networks. In Proceedings of the 13th annual ACM international conference on Mobile computing and networking(pp. 87-98). ACM.

Johnson, D. B., & Maltz, D. A. (1996). Dynamic source routing in ad hoc wireless networks. In Mobile computing (pp. 153-181). Springer, Boston, MA.

Jøsang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. Decision support systems, 43(2), 618-644.

Kansal, A., Somasundara, A. A., Jea, D. D., Srivastava, M. B., & Estrin, D. (2004, June). Intelligent fluid infrastructure for embedded networks. In Proceedings of the 2nd international conference on Mobile systems, applications, and services (pp. 111-124). ACM.

Karaboga, D., & Basturk, B. (2007). A powerful and efficient algorithm for numerical function optimization: artificial bee colony (ABC) algorithm. Journal of global optimization, 39(3), 459-471.

Khalid, O., Khan, S. U., Madani, S. A., Hayat, K., Khan, M. I., Min-Allah, N., ... & Chen, D. (2013). Comparative study of trust and reputation systems for wireless sensor networks. Security and Communication Networks, 6(6), 669-688.

Khedim, F., Labraoui, N., & Lehsaini, M. (2015, April). Dishonest recommendation attacks in wireless sensor networks: A survey. In Programming and Systems (ISPS), 2015 12th International Symposium on (pp. 1-10). IEEE.

Khedim, F., Labraoui, N., & Ari, A. A. A. (2018). A cognitive chronometry strategy associated with a revised cloud model to deal with the dishonest recommendations attacks in wireless sensor networks. Journal of Network and Computer Applications.

Komathy, K., & Narayanasamy, P. (2008). Trust-based evolutionary game model assisting AODV routing against selfishness. Journal of Network and Computer Applications, 31(4), 446-471.

Kone, C. T. (2011). Conception de l'architecture d'un réseau de capteurs sans fil de grande dimension (Doctoral dissertation, Université Henri Poincaré-Nancy I).

Kumar, G. E. P., Titus, I., & Thekkekara, S. I. (2012). A comprehensive overview on application of trust and reputation in wireless sensor network. Procedia engineering, 38, 2903-2912.

Labraoui, N. (2012). La sécurité dans les réseaux sans fil ad hoc (Doctoral dissertation).

Labraoui, N., Gueroui, M., & Sekhri, L. (2015, May). On-off attacks mitigation against trust systems in wireless sensor networks. In IFIP International Conference on Computer Science and its Applications_x000D_ (pp. 406-415). Springer, Cham.

Labraoui, N., Gueroui, M., & Sekhri, L. (2016). A risk-aware reputation-based trust management in wireless sensor networks. Wireless Personal Communications, 87(3), 1037-1055.

Levine, B. N., Shields, C., & Margolin, N. B. (2006). A survey of solutions to the sybil attack. University of Massachusetts Amherst, Amherst, MA, 7, 224.

Lindsay, S., Raghavendra, C. S., & Sivalingam, K. M. (2001, April). Data gathering in sensor networks using the energy delay metric. In Proceedings of the 15th International Parallel & Distributed Processing Symposium (p. 188). IEEE Computer Society.

Lopez, J., Roman, R., Agudo, I., & Fernandez-Gago, C. (2010). Trust management systems for wireless sensor networks: Best practices. Computer Communications, 33(9), 1086-1093.

Lupu, T. G., Rudas, I., Demiralp, M., & Mastorakis, N. (2009, September). Main types of attacks in wireless sensor networks. In WSEAS international conference. Proceedings of recent advances in computer engineering (No. 9). WSEAS.

Mármol, F. G., & Pérez, G. M. (2009). Security threats scenarios in trust and reputation models for distributed systems. Computers & security, 28(7), 545-556.

Mármol, F. G., & Pérez, G. M. (2010). Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems. Computer Standards & Interfaces, 32(4), 185-196.

Merad Boudia, O. R. (2014). Agrégation des données et sécurité des réseaux de capteurs sans fil (Doctoral dissertation).

Michiardi, P., & Molva, R. (2002). Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In Advanced communications and multimedia security (pp. 107-121). Springer, Boston, MA.

Mohamed, S. M., Hamza, H. S., & Saroit, I. A. (2017). Coverage in mobile wireless sensor networks (M-WSN): A survey. Computer Communications, 110, 133-150.

Momani, M., Agbinya, J. I., Navarrete Guzman, G. P., & Akache, M. (2006). A new algorithm of trust formation in wireless sensor networks. In International conference on Wireless Broadband and Ultra Wideband Communication. UTS.

Momani, M., Challa, S., & Alhmouz, R. (2008, August). BNWSN: Bayesian network trust model for wireless sensor networks. In Communications, Computers and Applications, 2008. MIC-CCA 2008. Mosharaka International Conference on (pp. 110-115). IEEE.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Othmen, S., Rekik, M., Zarai, F., Belghith, A., & Kamoun, L. (2016). Shortest and secure routing protocol for multi-hop cellular networks (SSRP-MCN). Security and Communication Networks, 9(18), 5346-5362.

Papaioannou, T. G., & Stamoulis, G. D. (2008, April). Achieving honest ratings with reputation-based fines in electronic markets. In INFOCOM 2008. The 27th Conference on Computer Communications. IEEE (pp. 1040-1048). IEEE.

Perkins, C. E., & Bhagwat, P. (1994, October). Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In ACM SIGCOMM computer communication review (Vol. 24, No. 4, pp. 234-244). ACM.

Perkins, C., Belding-Royer, E., & Das, S. (2003). Ad hoc on-demand distance vector (AODV) routing (No. RFC 3561).

Picard-Nizou, A. L., Pham-Delegue, M. H., Kerguelen, V., Douault, P., Marilleau, R., Olsen, L., ...& Masson, C. (1995). Foraging behaviour of honey bees (Apis mellifera L.) on transgenic oilseed rape (Brassica napus L. var. oleifera). Transgenic Research, 4(4), 270-276.

Rabaey, J., Ammer, J., Da Silva, J. L., & Patel, D. (2000). PicoRadio: Ad-hoc wireless networking of ubiquitous low-energy sensor/monitor nodes. In VLSI, 2000. Proceedings. IEEE Computer Society Workshop on (pp. 9-12). IEEE.

Rathore, H. (2016). Case Study: A Review of Security Challenges, Attacks and Trust and Reputation Models in Wireless Sensor Networks. In Mapping Biological Systems to Network Systems (pp. 117-175). Springer, Cham.

Reddy, Y. B. (2009, June). A game theory approach to detect malicious nodes in wireless sensor networks. In Sensor Technologies and Applications, 2009. SENSORCOMM'09. Third International Conference on (pp. 462-468). IEEE.

Rezazadeh, J., Moradi, M., & Ismail, A. S. (2012). Mobile wireless sensor networks overview. International Journal of Computer Communications and Networks, 2(1), 17-22.

Roth, D. (2012). Gestion de la mobilité dans les réseaux de capteurs sans fil (Doctoral dissertation, Université de Strasbourg).

Sedjelmaci, S. A. H. (2012). Mise en œuvre de mécanismes de sécurité bases sur les ids pour les réseaux de capteurs sans fil (Doctoral dissertation).

Selmic, R. R., Phoha, V. V., & Serwadda, A. (2016). Wireless Sensor Networks. Springer International Publishing AG.

Sharifi, M., Pourroostaei, S., & Kashi, S. S. (2007). Improving Availability of Secure Wireless Sensor Networks.

Shen, S., Yue, G., Cao, Q., & Yu, F. (2011). A survey of game theory in wireless sensor networks security. JNW, 6(3), 521-532.

Shi, E., & Perrig, A. (2004). Designing secure sensor networks. IEEE Wireless communications, 11(6), 38-43.

Shi, H. Y., Wang, W. L., Kwok, N. M., & Chen, S. Y. (2012). Game theory for wireless sensor networks: a survey. Sensors, 12(7), 9055-9097.

Singh, P., & Chauhan, R. K. (2017). A Survey on Comparisons of Cryptographic Algorithms Using Certain Parameters in WSN. International Journal of Electrical and Computer Engineering (IJECE), 7(4), 2232-2240.

Srinivasan, A., Teitelbaum, J., & Wu, J. (2006, September). DRBTS: distributed reputation-based beacon trust system. In Dependable, Autonomic and Secure Computing, 2nd IEEE International Symposium on (pp. 277-283). IEEE.

Srinivasan, A., Teitelbaum, J., Liang, H., Wang, J., & Cardei, M. (2007). On trust establishment in mobile ad hoc networks. Reputation and trust-based systems for ad hoc and sensor networks. New York: Wiley, 24, 696701.

Srinivasan, A., Li, F., & Wu, J. (2008, June). A novel CDS-based reputation monitoring system for wireless sensor networks. In Distributed Computing Systems Workshops, 2008. ICDCS'08. 28th International Conference on (pp. 364-369). IEEE. Talbi, E. G. (2009). Metaheuristics: from design to implementation (Vol. 74). John Wiley & Sons.

Tereshko, V., & Lee, T. (2002). How information-mapping patterns determine foraging behaviour of a honey bee colony. Open Systems & Information Dynamics, 9(02), 181-193.

Torres, W. A. A., Steinfeld, R., Sakzad, A., Liu, J. K., Kuchta, V., Bhattacharjee, N., ...& Cheng, J. (2018, July). Post-quantum one-time linkable ring signature and application to ring confidential transactions in blockchain (lattice ringct v1. 0). In Australasian Conference on Information Security and Privacy(pp. 558-576). Springer, Cham.

Tripathi, R., & Agrawal, S. (2014). Comparative study of symmetric and asymmetric cryptography techniques. International Journal of Advance Foundation and Research in Computer (IJAFRC), 1(6), 68-76.

Tseng, F. H., Chou, L. D., & Chao, H. C. (2011). A survey of black hole attacks in wireless mobile ad hoc networks. Human-centric Computing and Information Sciences, 1(1), 4.

Underwood, S. (2016). Blockchain beyond bitcoin. Communications of the ACM, 59(11), 15-17.

Von Frisch, K. (1974). Decoding the language of the bee. Science, 185(4152), 663-668.

Wang, G., Cao, G., La Porta, T., & Zhang, W. (2005, March). Sensor relocation in mobile sensor networks. In INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE (Vol. 4, pp. 2302-2312). IEEE.

Xing, B., &Gao, W. J. (2014). Innovative computational intelligence: a rough guide to 134 clever algorithms (pp. 105-121). Cham, Heidelberg, New York, Dordrecht, London: Springer International Publishing.

Yadav, K., & Srinivasan, A. (2010, March). iTrust: an integrated trust framework for wireless sensor networks. In Proceedings of the 2010 ACM Symposium on Applied Computing (pp. 1466-1471). ACM.

Yu, H., Shen, Z., Miao, C., Leung, C., & Niyato, D. (2010). A survey of trust and reputation management systems in wireless communications. Proceedings of the IEEE, 98(10), 1755-1772.

Yu, Y., Li, K., Zhou, W., & Li, P. (2012). Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures. Journal of Network and computer Applications, 35(3), 867-880.

Yussoff, Y. M., Hashim, H., Rosli, R., & Baba, M. D. (2012). A review of physical attacks and trusted platforms in wireless sensor networks. *Procedia Engineering*, *41*, 580-587.

Zahariadis, T., Leligou, H., Karkazis, P., Trakadas, P., Papaefstathiou, I., Vangelatos, C., & Besson, L. (2010). Design and implementation of a trust-aware routing protocol for large WSNs. International Journal of Network Security & Its Applications (IJNSA), 2(3), 52-68.

Zia, T. A. (2008, December). Reputation-based trust management in wireless sensor networks. In Intelligent Sensors, Sensor Networks and Information Processing, 2008. ISSNIP 2008. International Conference on (pp. 163-166). IEEE.

Zouridaki, C., Mark, B. L., Hejmo, M., & Thomas, R. K. (2009). E-Hermes: A robust cooperative trust establishment scheme for mobile ad hoc networks. Ad Hoc Networks, 7(6), 1156-1168.

Résumé

La sécurité dans les réseaux de capteurs sans fil (RCSFs) est devenue un domaine indissociable des autres domaines des RCSFs. Il devient en effet inenvisageable d'aborder des thématiques telles que l'agrégation, la localisation, le routage ou le clustering sans prendre en compte le côté sécuritaire. Connus pour être en effet une cible idéale pour de nombreuses attaques toujours plus sophistiquées et de plus en plus intelligentes, les réseaux de capteurs se retrouvent démunis face aux attaques internes. De telles attaques peuvent passer totalement inaperçues tout en engendrant des dégâts irréversibles pour le réseau. Les systèmes de confiance et de réputation (TRS) se distinguent comme méthode de détection efficace pour ces attaques, cependant ces mécanismes sont victimes de leur succès, des attaquants peuvent en effet se servir de ces mécanismes pour engendrer une multitude d'attaques internes. Nous nous sommes intéressés dans cette thèse aux problèmes de sécurité liés aux systèmes de confiance et de réputation. Nous avons à cet effet proposé deux nouvelles approches nommées Bee-Trust Scheme et B-Smart, des méthodes intelligentes permettant de renforcer la résistance des TRS afin que ces derniers puissent soutenir efficacement la détection des attaques internes dans les réseaux de capteurs.

Mots-clés : Réseaux de capteurs sans fil, sécurité, attaques internes, systèmes de confiance et de réputation.

Abstract

Security in wireless sensor networks (WSN) has become an inseparable area from other areas in WSN. It is indeed unthinkable to tackle topics such as aggregation, localization, routing or clustering without taking into account the security side. Known to be an ideal target for many increasingly sophisticated and intelligent attacks, sensor networks are particularly vulnerable to internal attacks. Such attacks can go completely unnoticed while causing irreversible damage to the network. Trust and reputation systems (TRS) stand out as an effective detection method for these attacks, but these mechanisms are victims of their success, attackers can use these mechanisms to generate a multitude of internal attacks. We were interested in this thesis to the security issues related to the trust and reputation systems. We have proposed for this purpose two new approaches named Bee-Trust Scheme and B-Smart, intelligent methods to strengthen the resistance of the TRS so that can effectively support the detection of internal attacks in sensor networks.

Keywords: Wireless sensor networks, security, internal attacks, trust and reputation systems.

ملخّص

أصبح الأمن في شبكات أجهزة الاستشعار اللّاسلكية مجال لا يمكن فصله عن المجلات الأخرى. أصبح من غير المعقول معالجة مواضيع مثل التّجميع أو التّوجيه دون الأخذ بعين الاعتبار الجانب الأمني. إنّ أجهزة الاستشعار المعروفة بأنّها هدف مثالي للعديد من الهجمات المتطوّرة تجد نفسها معدمة في مواجهة الهجمات الدّاخلية. هذه الهجمات تتسبب في أضرار وخيمة لا يمكن إصلاحها على الشّبكة. برزت أنظمة الثّقة والسّهرة كوسيلة فعّالة للكشف عن هذه الهجمات، ولكن هذه الآليات هي ضحايا نجاحها، حيث يمكن للمهاجمين استخدام هذه الآليات لتوليد العديد من الهجمات الدّاخلية. نحن مهتمّون في هذه الرّسالة إلى المشاكل الأمنية المتعلّقة بأنظمة الثّقة والسّمعة. لقد اقترحنا نهجين جديدين وهما عبارة عن طريقتان ذكيتان لزيادة مقاومة أنظمة الثّقة والسّمعة حتّى تصبح وسيلة فعّالة لدعم الكشف الفعّال للهجمات الدّاخلية في شبكات الاستشعار.

كلمات البحث: شبكات أجهزة الاستشعار اللّاسلكية، الأمن، الهجمات الدّاخلية، أنظمة الثّقة والسّمعة.