RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITÉ ABDERRAHMANE MIRA DE BÉJAÏA

Mémoire de Fin de Cycle

En vue d'obtention du diplôme de Master Recherche en Informatique
Option : Réseaux et Systèmes Distribués

Thème

Vers un modèle de confiance pour l'Internet des Objets

Présenté par :
HADDAD Syphax

Soutenu le : *30/06/2016*

Devant le jury composé de :

Président :	Mme. TAHAKOURT Zineb	M.A.A, U.A.M Béjaia
Examinateur :	Mr. AKILLAL Abdellah	Doctorant, U.A.M Béjaia
Examinateur :	Mr. BOUCHEBBAH Fatah	Doctorant, U.A.M Béjaia
Encadreur :	Dr. OMAR Mawloud	M.C.A, U.A.M Béjaia
Co-Encadreur :	Mlle. BENKERROU Hayet	Doctorante, U.A.M Béjaia

Année universitaire : 2015-2016

Remerciments

***A**u terme de ce travail, je tiens à exprimer ma profonde gratitude et mes sincères remerciements à tous qui par leur présence, leur soutien et leur disponibilité m'ont encouragé.*

***M**es profonds remerciements vont à mes encadreurs Dr. OMAR Mawloud et Mlle. BENKARROU Hayet pour tout le temps qu'ils m'ont consacré, leurs nombreux conseils, et pour la confiance qu'ils m'ont accordé.*

***J**e tiens à remercier également les membres du jury en l'occurrence Mme. TAHAKOURT Zineb, Mr. AKILLAL Abdellah et Mr. BOUCHEBBAH Fatah pour l'intérêt qu'ils ont porté á ce travail en acceptant de l'examiner et de l'enrichir par leurs propositions.*

***J**e remercie aussi l'ensemble des enseignants du département d'Informatique pour m'avoir formé et encadré tout au long de ma formation.*

***U**n grand merci à mes parents, mon frère et ma sœur, mes amis et tous ceux qui ont contribué à l'aboutissement de ce travail. Ainsi que toute la promotion 2015-2016 Master 2 Recherche Informatique de l'Université Abderrahman Mira.*

***J**e remercie enfin toutes les personnes intéressées par ce travail, en espérant qu'elles puissent y trouver des explications utiles pour leurs propres travaux.*

Dédicaces

***J**e dédis ce travail*

***À** mes chers parents qui m'ont toujours entouré avec tout leur amour et se sont sacrifié pour veiller à m'offrir le meilleur et m'encourager à avancer, j'espère avoir été à la hauteur de tous qu'ils m'ont apporté.*

***À** mon frère et ma sœur avec qui j'ai grandit, rit et tout partagé.*

***À** toute ma famille et mes amis pour leur présence et tous ces moments de bonheurs passés à leurs cotés.*

H. Syphax

Table des matières

Table des figures

Liste des tableaux

Notations et symboles

6lowPAN : IPv**6** over **low**-power **W**ireless **P**ersonal **A**rea **N**eworks
BDD : **B**ase **D**e **D**onnées
DHT : **D**istributed **H**ash **T**able
DoS : **D**enial **o**f **S**ervice
DS : **D**emandeur de **S**ervice
EX : **Ex**périence
FS : **F**ournisseur de **S**ervice
GPS : **G**lobal **P**ositioning **S**ystem
GSM : **G**lobal **S**ystem for **M**obile Communication
IDA : **I**nfocomm **D**evelopment **A**uthority (Singapore)
IdO : **I**nternet **d**es **O**bjets
IoT : **I**nternet **o**f **T**hings
ITU : **I**nternational **T**elecommunication **U**nion
ITU-T : **ITU** standards for **T**elecommunications
KN : **Kn**owledge (Connaissances)
LAN : **L**ocal **A**rea **N**etwork
LTE : **L**ong **T**erm **E**volution
LTE-A : **L**ong **T**erm **E**volution **A**dvanced
M2M : **M**achine **to** **M**achine
P2P : **P**eer-**to**-**P**eer
PAN : **P**ersonal **A**rea **N**eworks
RFID : **R**adio **F**requency **ID**entification
RC : **R**ecommandations
SIoT : **S**ocial **I**nternet **o**f **T**hings
UMTS : **U**niversal **M**obile **T**elecommunications **S**ystem
UWB : **U**ltra **W**ide**B**and
WAN : **W**ide **A**rea **N**etwork

Introduction générale

Le terme Internet des objets a été introduit pour la première fois par Kevin Ashton [5] (1999), il ne désignait alors simplement qu'une technologie permettant l'identification d'objets du monde physique de manière unique grâce aux puces RFID. Le concept a toutefois évolué avec le temps et s'est généralisé vers une approche consistant à connecter un très grand nombre d'objets du quotidien(téléphones, montres, appareils ménagers, etc.) au réseau Internet, les dotant ainsi d'une identité propre et leur permettant, entre autres, d'offrir des services et de collecter des informations de manière autonome grâce à l'intégration de capteurs, d'actionneurs et de capacités de communication, faisant ainsi le lien entre le monde physique et le monde virtuel. Tout ceci se traduit actuellement par l'omniprésence d'objets capables de mesurer l'environnement et d'agir sur celui-ci. Cet aspect ubiquitaire en fait un concept très prometteur dans la perspective d'intégrer pleinement la technologie à notre quotidien à travers les objets dans une multitude de domaines : ville intelligente, e-santé, domotique, transport, logistique, sécurité, etc.

Néanmoins, comme tout concept émergent, l'Internet des objets soulève un nombre considérable de problématiques représentant des obstacles ralentissant sa progression et l'atteinte de son plein potentiel. En effet, la communauté scientifique se penche dors et déjà sur des axes de recherche tels que l'interopérabilité dans le système Internet des objets pour lequel il n'existe pas encor de standard ou de norme, la préservation et la protection de la vie privée des utilisateurs dont les données sont quotidiennement recueillies et traitées, et enfin le chalenge que représente déjà la sécurité pour les technologies de l'information en général, se voit amplifié du fait des caractéristiques exceptionnelles de l'Internet des objets, à savoir la très grande échelle du système, la nature ubiquitaire, l'hétérogénéité des données et des systèmes le composant et enfin la pauvreté des objets en termes de ressources de calcul, stockage, et d'énergie.

Parmi les mécanismes permettant de garantir la sécurité dans un système se basant sur la collaboration dans la réalisation des services tel que l'Internet des objets, la gestion de confiance représente un aspect primordial devant être assuré afin de garantir un fonctionnement sure du système. Cependant, les modèles de gestion de confiance traditionnels, généralement à base de credentials (certificats) ne peuvent pas être utilisés pour l'Internet des objets car ils font appel à la

cryptographie asymétrique dont les processus sont très couteux en termes de ressources. C'est Pour cela que la majorité des solutions proposées dans la littérature sont à base de réputation utilisant des architectures hiérarchiques ou complètement distribuées impliquant des métriques telle que la qualité de service, les relations sociales ou une hybridation des deux dans la dérivation de la confiance. Cependant, malgré la pertinence de certaines de ces solutions, elles présentent chacune des faiblesses du point de vue d'un critère donné.

Dans l'optique de proposer une solution plus complète pour la gestion de la confiance et ainsi participer à la concrétisation de l'Internet des objets, nous nous sommes inspiré des modèles proposés dans la littérature et de leurs points forts. Plus concrètement, nous proposons un modèle de confiance hiérarchique à base de crédit et d'honnêteté dans le but de garantir une meilleure précision dans le calcul de la confiance tout en s'adaptant au contexte de l'internet des objet.

Les différentes étapes de ce travail sont présentées dans ce mémoire en trois chapitres. Le premier chapitre est consacré à la présentation de l'Internet des objets, ses spécificités, les risquent inhérents à son déploiement ainsi que quelques notions relatives à la confiance et à la sécurité. Le deuxième chapitre expose une étude critique, une classification et une comparaison de quelques unes des solutions les plus récemment proposées dans la littérature pour la gestion de confiance dans l'Internet des Objets. Dans le troisième chapitre, nous proposons notre propre modèle de gestion de confiance.

Chapitre 1

Présentation de l'Internet des Objets

1.1 Introduction

L'internet des objets introduit un système où des entités appartenant au monde physique sont connectées à internet, cela afin d'utiliser des applications tirant partie de la collecte et du partage d'information dans le but de fournir des services plus avancés mais aussi plus intelligents à l'humanité. Cependant, la nature décentralisée et distribuée du système, impose de grands défis en termes de sécurité.

Ce chapitre, ayant pour rôle d'introduire l'environnement de ce travail, sera consacré à la présentation de l'Internet des objets, ses spécificités, les types d'attaques auxquelles il est exposé ainsi que quelques notions relatives à la confiance et à la sécurité.

1.2 L'Internet des Objets

1.2.1 Définition

Le CERP-IoT, *Cluster des projets européens de recherche sur l'Internet des objets* , définit l'Internet des objets comme : " une infrastructure dynamique d'un réseau global. Ce réseau global a des capacités d'auto-configuration basée sur des standards et des protocoles de communication interopérables. Dans ce réseau, les objets physiques et virtuels ont des identités, des attributs physiques, des personnalités virtuelles et des interfaces intelligentes, et ils sont intégrés au réseau d'une façon transparente " [22].

Cette vision de l'Internet des objets introduira une nouvelle dimension aux technologies de l'information et de la communication : en plus des deux dimensions temporelle et spatiale qui permettent aux personnes de se connecter de n'importe où à n'importe quel moment, nous aurons une nouvelle dimension "objet" qui leur permettra de se connecter à n'importe quel objet [9].

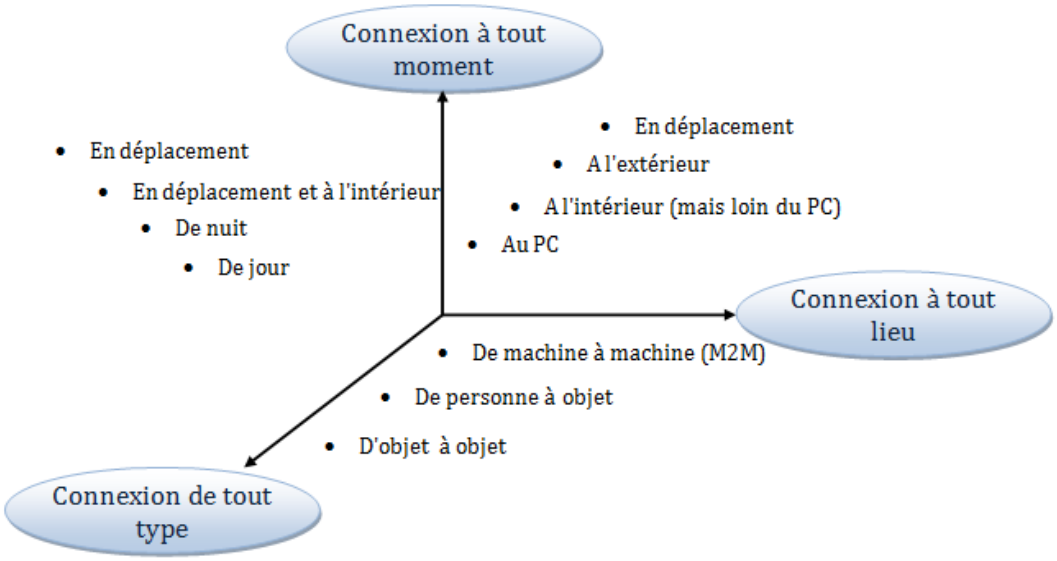

FIGURE 1.1 – Dimensions de l'IdO.

1.2.2 Domaines d'application

Les potentielles applications de l'IdO sont très nombreuses, elles imprègnent pratiquement tous les domaines de la vie quotidienne des individus, ce qui permettra l'émergence d'espaces intelligents autour d'une informatique omniprésente [9]. Parmi ces espaces intelligents nous citons quelques exemples :

1.2.2.1 Aérospatial et aviation

Dans ce domaine l'IdO permettra d'améliorer la sécurité des services, en assurant l'identification des produits et des éléments contrefaits grâce à l'élaboration de pédigrée des pièces critiques des appareils, cela par le biais d'implantation de tag RFID.

1.2.2.2 Santé

L'IdO aura maintes applications dans ce secteur destinées à préserver et améliorer la santé publique, notamment grâce au déploiement de réseaux personnels dédiés au suivi des paramètres médicaux et l'administration des médicaments. Ce qui permettra une meilleure prévention et contrôle des maladies au sein de la société, ainsi que des diagnostiques instantanés en cas d'urgence.

1.2.2.3 Transport

Le suivie en temps réel du déplacement des populations, des biens et des moyens de transport dans le monde, permettra l'élaboration d'un système de transport plus intelligent et efficace ga-

rantissant une meilleure sécurité, plus de confort et facilité de déplacement, tout en privilégiant l'économie d'énergie et de temps.

1.2.2.4 Industrie

Dans l'industrie l'IdO permet un suivi total des produits, de la chaine de production jusqu'à la chaine logistique et de distribution en supervisant les conditions d'approvisionnement. Cette traçabilité de bout en bout permet de repérer rapidement les problèmes, minimiser les déchets et rationaliser les processus de gestion.

1.2.2.5 Agriculture

Les capteurs déployés connectés à l'application peuvent être utilisés pour la supervision de l'environnement de culture, ceci en fournissant un tableau de bord destiné à faciliter la prise de déscision pour l'agriculteur concernant les besoins imminents de la plantation, assurant ainsi une optimisation de l'usage de l'eau, des engrais et la planification des travaux agricoles, et par conséquent économiser les ressources et préserver l'environnement en diminuant la pollution [9].

1.2.2.6 Ville

Les villes intelligentes permettent d'améliorer la qualité de vie de la municipalité, en assurant l'optimisation du remplissage des parkings dans la ville grâce à l'identification en temps réel des places libres, l'éclairage intelligent qui varie en fonction de l'intensité lumineuse ou des déplacements également. La gestion du trafic est facilitée par une vision fine et en temps réel des flux [24].

1.2.3 Enjeux socio-économiques de l'Internet des objets

La montée en puissance des applications de l'IdO peut s'observer dans plusieurs secteurs ou registres des activités sociales : des plus personnels (animaux, familiers, santé) aux plus industriels (gestion, logistique). Le large spectre des applications d'ores et déjà observables indique que nous sommes aujourd'hui face à une tendance bien ancrée.

Le poids et l'intérêt économiques de certaines applications contribuent à stimuler les investissements de recherche et développement et à installer durablement les utilisations de l'IdO. Ensuite, par son caractère très global, l'IdO est porté par des mouvements profonds de la société : la convergence grandissante, la communication en réseau et les systèmes d'information, le développement de la mobilité, le renforcement de la traçabilité et des processus de contrôle des activités et des personnes [8].

1.2.4 Architecture

L'architecture de l'IdO consiste en un mélange de technologies destiné à supporter ce système doté de besoins spécifiques. Dans la perspective de garantir l'interopérabilité et la coexistence de ces technologies dans l'IdO, l'IDA [12] en s'inspirant de l'architecture proposée par l'ITU-T a défini une architecture composée des quatres couches illustrées par la figure 1.2 :

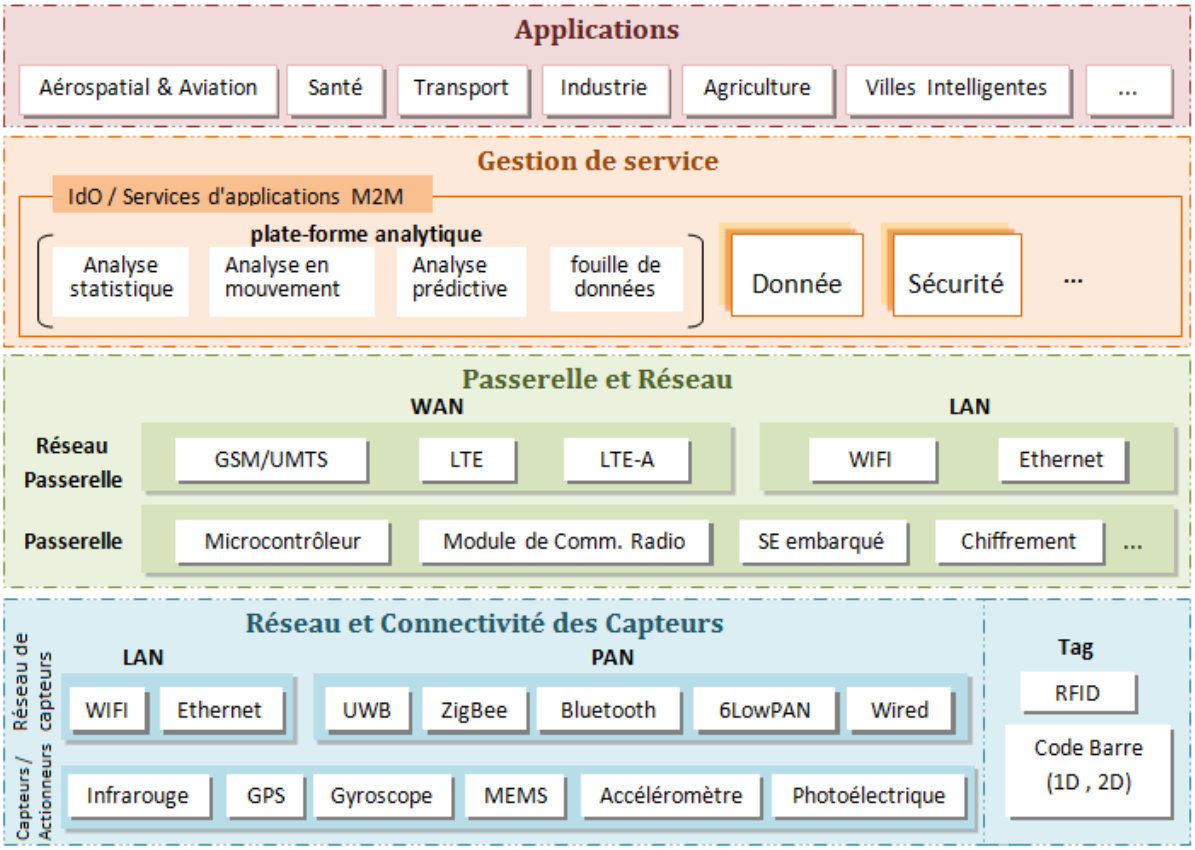

FIGURE 1.2 – Architecture de l'IdO.

1.2.4.1 Couche physique

Au sein de cette couche nous retrouvons des objets intelligents intégrant des capteurs et des actionneurs destinés à interconnecter le monde physique au monde digital, ceci en permettant la collecte et le traitement d'informations sur le monde physique en temps réel. Il existe différents types de capteurs destinés à différent usages, les capteurs ont la capacité de mesurer des propriétés physiques, puis les convertir en signal compréhensible par un instrument. La majorité de ces capteurs nécessitent une connectivité à un agregateur de capteurs (point d'accès), et sont ainsi organisés sous forme de LAN, WIFI ou PAN tel que ZigBee, Bluetooth et Ultra-Wideband (UWB). Les capteurs ne nécessitant pas une connectivité à un agregateur de capteurs, utilise directement des technologies WAN tel que GSM, GPRS et LTE, pour ce connecter aux serveurs d'applications.

Nous retrouvons aussi dans cette couche des technologies utilisant des tags RFID, des Codes-barre ainsi que les réseaux de capteurs sans fils.

1.2.4.2 Couche Reseaux

Le volume colossal de données qui sera généré par les capteurs de la couche Physique requier une infrastructure réseau câblée et sans fil robuste et performante, afin d'assurer le transport des données collectées jusqu'à la couche application. Dans le but de répondre aux besoins de l'IdO en termes de latence, bande passante et sécurité, des réseaux multiples utilisant des technologies et des protocoles d'accès variés et appartenant à des organisations différentes devrons convergés afin de former un seul support de communication. Cette abstraction du réseau permettra à plusieurs organisations de partager et d'utiliser le même réseau sans compromettre leurs exigences de confidentialité, de sécurité et de performance.

1.2.4.3 Couche gestion des services

La couche gestion des services rend le traitement de l'information possible grâce à des analyses, des contrôles de sécurité, la modélisation des processus et la gestion des périphériques, ainsi cette couche représente le superviseur du système.

1.2.4.4 Couche Application

Cette couche utilise les services fournis par la couche gestion des services comme une plateforme sur laquelle sont exécutées des applications destinées à mettre l'IdO au service de divers domaines.

1.2.5 Challenges imposés par l'IdO

Des progrés considérables ont déjà été accomplis dans la perspective de concrétisation de l'IdO, mais le chemin à parcourir est encore long, notamment dans les domaines suivants :

1.2.5.1 Securité

En tenant compte du nombre pharamineux d'objets qui seront interconnectés, leur faiblesse en ressources combiné à l'aspect ubiquitaire de l'IdO, engendre un accroissement considérable des vulnérabilités ainsi que des opportunités d'exploitation de ces dernières. Les mécanismes de sécurité traditionnels ne répondant pas aux besoins spécifiques et uniques de l'IdO, la communauté de chercheurs scientifiques et industriels sont ainsi sollicités afin d'adapter ou de proposer de nouveaux mécanismes destinés à assurer la sécurité dans le système IdO.

1.2.5.2 La Privacy

Il y a un certain nombre de conséquences sur la vie privée découlant de l'ubiquité et omniprésence des dispositifs IdO, car une grande partie des informations collectées et traitée dans IdO sont des données personnelles, donc il est nécessaire de soutenir l'anonymat et la manipulation restrictive de ces données.

1.2.5.3 Interopérabilité et standardisation

L'Internet des Objets ambitionne de faire communiquer chaque système avec tous les autres au moyen de protocoles communs ; la mise en application, à une large échelle, du concept d'Internet des Objets apparaît largement tributaire d'une standardisation de la communication entre objets, dite M2M. Près de 140 organismes dans le monde sont aujourd'hui concernés, directement ou indirectement, par la normalisation de la communication dite M2M. La normalisation représente en effet l'un des facteurs cruciaux de l'évolution de l'Internet mobile vers l'Internet des Objets [13].

1.3 Social Internet des Objets

1.3.1 Définition

Représente un système IdO au sein du quel les objets peuvent établir des relations social entre eux de manière autonome. La motivation de choix d'une approche axée sur le social est la mise en avant de la découverte, la sélection et la composition de services, mais aussi des renseignements fournis par les objets distribués et les réseaux ayant accès au monde physique. L'objectif clé est de publier des informations, des services, puis pouvoir les retrouver ou découvrir de nouvelles ressources afin de supporter la mise en œuvre de services et d'applications complexes [19].

1.3.2 Métriques sociales

Contrairement à l'IdO, le social IdO prend en considération des critères sociaux et fait donc appel à des métriques d'ordre social comme l'honnêteté, l'intérêt à la communauté, etc.

1.4 Confiance dans l'internet des objets

1.4.1 Définitions préliminaires

1.4.1.1 Honnêteté

Représente le degré de fiabilité (vérité) dans les recommandations fournies par une entité [10].

1.4.1.2 Interaction

Une interaction est une action menée en commun par plusieurs acteurs au sein d'un système [23].

1.4.1.3 Contrôle d'accès

Le contrôle d'accès est une méthode de gestion de l'accès à des ressources. On n'autorise l'accès aux ressources qu'à certaines entités privilégiées [23].

1.4.1.4 Certificat

Un certificat est un document électronique qui utilise la notion de signature numérique pour associer une clef publique à une identité. L'association clef publique/identité est réalisée sous le contrôle de l'entité qui signe le certificat [23].

1.4.1.5 Réputation

Comportement attendu de la part d'une entité d'après des informations relatives à son comportement passé [3].

1.4.1.6 Recommandation

Une entité peut évaluer la qualité et la fiabilité d'une collaboration avec une autre entité tierce et fournir cette information à une troisième entité [19].

1.4.2 Confiance

Il existe différentes définitions de la confiance dans la littérature.

Selon Neisse et al. [18] la confiance est : " la croyance mesurée par un trustor (celui qui doit accorder sa confiance) en ce qui concerne la compétence, l'honnêteté, la sécurité et la fiabilité d'un trustée (celui à qui l'on doit faire confiance) dans un contexte donné ".

Selon l'ITU-T X. 509 [14] la confiance est définit par : "On dit qu'une entité fait confiance à une deuxième entité si et seulement si cette dernière se comporte exactement comme la première le prévoit ".

Ainsi nous pouvant déduire que la confiance représente une relation entre deux agents, tel que le premier agent associe à l' avance au deuxième un niveau de probabilité subjectif dans la réalisation d'une action donnée de manière sûre et fiable dans un contexte spécifique.

1.4.3 Gestion de la confiance

La gestion de confiance est définit comme étant l'activité de création de systèmes et de méthodes permettre aux parties utilisatrices de faire des évaluations et de prendre des décisions concernant la fiabilité d'opérations éventuelles à risque, et qui permettent également à l'utilisateur ainsi qu'aux propriétaires du système d'augmenter et représenter correctement la fiabilité de leur système [15].

1.4.4 Importance de la confiance dans l'internet des objets

La confiance et la sécurité sont étroitement liées et les processus de décision de la confiance traitent de manière identique ces deux notions. Il existe une relation stricte entre les notions de sécurité et de confiance. Si la transaction que nous allons entreprendre peut se faire en toute sécurité, alors nous considérons que nous ne prenons aucun risque et le problème de la confiance ne se posera donc pas. Il est nécessaire de se préoccuper des problèmes de confiance dès lors que la sécurité des relations n'est plus assurée. Dans le cas général, le mécanisme de sécurité protège les ressources contre les accès malveillants par un contrôle qui en restreint l'accès aux personnes autorisées. Mais nous devons aussi nous protéger contre la partie qui nous offre le service ou les ressources car ce fournisseur de services pourrait lui aussi nous donner des informations erronées dans le but de nous tromper [23].

Dans le contexte de l'IdO où les services sont basés principalement sur la collaboration de billions d'objets hétérogènes, la confiance est un pilier fondateur visant à assurer la sécurité du système et améliorer la qualité des services en assurant une composition de services optimal. De plus, la confiance peut être utilisée pour garantir d'autres critères de la sécurité, tel que le contrôle d'accès et l'autorisation.

1.4.5 Modèles de gestion de confiance

En étudiant l'état de l'art concernant les modèles de gestion de la confiance, nous pouvons distinguer trois familles d'approches principales :

1.4.5.1 Confiance à partir de Credentials (Certifiaction)

Ce cadre repose sur la mise en place d'une ou plusieurs politiques de sécurité et d'un système de certificats : les nœuds utilisent la vérification des certificats pour établir un lien de confiance avec

les autres nœuds [7]. Ainsi un nœud à confiance en un nœud seulement si ce dernier à un certificat valide.

1.4.5.2 Confiance à partir de réputation et de recommandation

Dans ce cadre, la gestion de la confiance repose sur un modèle de réputation et/ou de recommandation. La réputation peut-être vue comme l'espérance portée dans la réalisation d'un objectif fictif. La recommandation serait la qualité supposée d'un nœud qu'il détiendrait d'un tiers et qu'il présenterait à un autre nœud. De tels systèmes fournissent un mécanisme pour lequel un nœud demandant une ressource peut évaluer la confiance qu'il porte au fournisseur à la lui fournir, Chaque nœud établit ainsi des relations de confiance avec les autres nœuds et assigne des valeurs de confiance à ses relations [26].
La valeur assignée à la relation de confiance est fonction d'une combinaison entre la réputation globale du nœud et l'évaluation de la perception du nœud, c'est-à-dire basée sur son expérience propre.

1.4.5.3 Confiance à partir d'un réseau social

Les relations sociales sont utilisées pour calculer les valeurs de réputation et de recommandation pour chaque nœud. De tels systèmes analysent le réseau social qui représente les relations existantes dans chaque communauté dans le but de tirer des conclusions sur les niveaux de confiance à accorder aux autres nœuds, Ils reposent sur des mécanismes de réputation, de crédibilité, d'honnêteté et également des procédés de recommandations [7].

1.4.6 Attaques sur la confiance

Un gestionnaire de confiance a pour objectif principal de fournir des scores de confiance, ces derniers sont utilisés par la suite dans la prise de décision concernant le choix de collaborateurs dans le système IdO. Cependant, il existe une variété d'attaques exécutées par des entités malicieuses destinées à casser ou perturber les services assurés par le système de gestion de confiance. Les attaques les plus courantes sont les suivantes :

1.4.6.1 L'attaque "Self-Promoting "

Un nœud malveillant peut promouvoir son importance (en fournissant de bonnes recommandations à son egard) de manière à être sélectionné en tant que FS, mais peut fournir des mauvais services [11].

1.4.6.2 L'attaque "Bad-Mouthing"

Un nœud malveillant peut ruiner la réputation d'un nœud honnête (en fournissant des mauvaises recommandations contre lui) de façon à diminuer la probabilité que ce nœud soit sélectionné pour la réalisation de services [11].

1.4.6.3 L'attaque "Ballot-Stuffing"

Un nœud malveillant peut promouvoir la confiance d'un autre nœud malveillant (en fournissant de bonnes recommandations sur ce dernier) de manière à augmenter la probabilité que ce nœud soit sélectionné en tant que fournisseur de services [11].

1.4.6.4 L'attaque "On-Off "

Un nœud malveillant effectue un mauvais service une fois de temps en temps afin d'éviter d'être étiqueté comme un nœud de confiance faible et risquer lui-même de ne pas être sélectionné en tant que fourniseur de services, ainsi que de ne pas pouvoir effectuer efficacement des attaques de type "Bad-Mouthing " et "Ballot-Stuffng" [11].

1.4.6.5 L'attaque "White-Washing "

Un nœud malveillant peut disparaitre puis rejoindre l'application pour laver sa mauvaise réputation [2].

1.4.6.6 L'attaque "Discriminatory"

Présente dans les systèmes IdO sociaux où un nœud malveillant peut mener une attaque discriminante sur les nœuds non-amis ou sans liens sociaux forts (sans beaucoup d'amis communs), ce comportement est similaire à celui des humains qui préfère interagir avec leurs Amis plutôt que des inconnus [10].

1.4.6.7 L'attaque "Déni de service"

Un nœud malveillant agit dans l'intérêt de rendre un autre nœud incapable d'assurer un service [4].

1.4.7 Logique floue

La logique floue est une extension de la logique booléenne ; Par rapport à des ensembles binaires traditionnels, les variables de logique floue peuvent avoir une valeur de vérité qui varie en degré entre 0 et 1, elle confère ainsi une flexibilité aux raisonnements qui l'utilisent. La logique floue a

été étendue pour gérer le concept de vérité partielle, où la valeur de vérité peut se situer entre tout à fait vrai et complètement faux.

En outre, lorsque les variables linguistiques sont utilisées, ces degrés peuvent être gérés par des fonctions spécifiques d'appartenance. La réputation ou la confiance est représenté comme une mesure floue avec des fonctions d'appartenance décrivant les degrés de confiance, par exemple, une valeur de confiance dans l'intervalle (1,25, 1,25) dénote une très faible confiance, (0, 2.5) faible confiance, (1,25, 3,75) confiance moyenne, (2,5, 5) une confiance élevée, (3,75,6,25) une confiance élevée, etc.

Par conséquent, un nœud avec une valeur de confiance de 0,25 est de 75% à très faible confiance (une fonction d'appartenance) et de 25% à faible confiance (une autre fonction d'appartenance). La logique floue fournit des règles pour raisonner avec des mesures floues et permet ainsi la modélisation des imperfections des données et se rapproche dans une certaine mesure de la flexibilité du raisonnement humain [11].

1.5 Conclusion

Dans ce chapitre, en vue d'éviter toute ambigüité, nous avons présenté le vocabulaire de base utilisé dans les modèles de gestion de confiance, cela en définissant chaque concept rencontré dans la littérature ou dans le modèle que nous proposons.

Chapitre 2

Taxonomie des modèles de confiance dans l'Internet des objets

2.1 Introduction

Le paradigme émergeant de l'Internet des objets intégrant des technologies hétérogènes et servant de plateforme à une myriade d'applications a imposé un éventail de défis de sécurité à relever, ce qui exige une révision substantielle des solutions de sécurité existantes ou le développement de nouvelles approches. Parmi les mécanismes de sécurité devant être assurer dans un système basé sur la collaboration tel que l'IdO, nous retrouvons la confiance.

Dans ce chapitre, nous avons étudié les modèles de gestion de confiance récemment proposés dans la littérature afin d'en faire une critique sur laquelle nous nous baserons par la suite dans notre proposition. Pour ce faire, nous avons commencé par la définition des critères d'analyse et de comparaison des différentes solutions, ensuite nous avons procédé à leur classification pour finir par une synthèse dans laquelle nous avons repris l'essentiel des avantages et des inconvénients des modèles proposés.

2.2 Critères de comparaison des solutions

Dans le but de mener une étude objective des solutions proposées dans la littérature en tenant compte des besoins et des contraintes spécifiques de l'IdO, nous avons introduit un ensemble de critères sur lesquels nous fonderons notre comparaison, et qui sont les suivants :

2.2.1 Résistance aux attaques

Dans un système IdO, chaque objet peut être fournisseur (FS) ou demandeur (DS) de service, par conséquent, tout objet veut être sélectionné pour fournir un service à but lucratif quand il est un FS ou recevoir des services des meilleures FSs dans le cas ou il est un DS.

Un nœud FS malveillant agit dans le but d'être sélectionné pour la réalisation du service même si la qualité de service qu'il peut fournir est inferieure à celle assurée par d'autres objets. Dans le contexte de l'IdO, les préoccupations sont les attaques pouvant perturber le système de gestion de confiance et ainsi causer une perte de précision dans l'évaluation de confiance attribuée aux objets.

2.2.2 Consommation énergétique

La majorité des dispositifs présents dans l'IdO sont sévèrement limités en termes de mémoire, CPU ainsi que des capacités énergétiques [1]. De ce fait le mécanisme de gestion de confiance doit être à moindre consommation d'énergie.

2.2.3 Évolutivité (Scalabilité)

L'évolutivité est l'une des caractéristiques essentielles d'un modèle de confiance dans l'Internet des Objets, elle permet d'assurer un fonctionnement correct lors des changements dynamiques de la taille du réseau [21].

2.2.4 Précision dans le calcul de la confiance

Représente le degré de similarité entre le score de confiance d'un nœud calculé par le système de gestion de confiance avec la confiance effective qui doit être attribuée au nœud.

2.2.5 Monitorage

Représente la capacité de suivie du comportement de tout objet dans le système, ce qui permet d'utiliser l'historique des agissements d'un objet pour calculer son score de confiance et ainsi augmenter la précision du calcul de confiance.

2.3 Classification des travaux

Dans cette section nous avons proposé une classification des modèles de confiance étudiés, pour ce nous avons utilisé un arbre à deux branches. La première branche représente les modèles distribuées, la deuxième représente les modèles hiérarchiques décomposés en deux sous ensembles :

Modèles hiérarchiques virtuelle : correspondant à une architecture dans laquelle le mécanisme est distribué sur plusieurs serveurs.

modèles hiérarchiques physique : correspondant à une implémentation du mécanisme de gestion de confiance sur un serveur physique. Au sein de chaque branche nous retrouvons deux

niveaux correspondant au type de métriques utilisées pour le calcul de la confiance, dans lequel le modèle utilise soit la qualité de service soit la qualité de service combinée avec les critères sociaux qu'on retrouve généralement dans le SIoT.

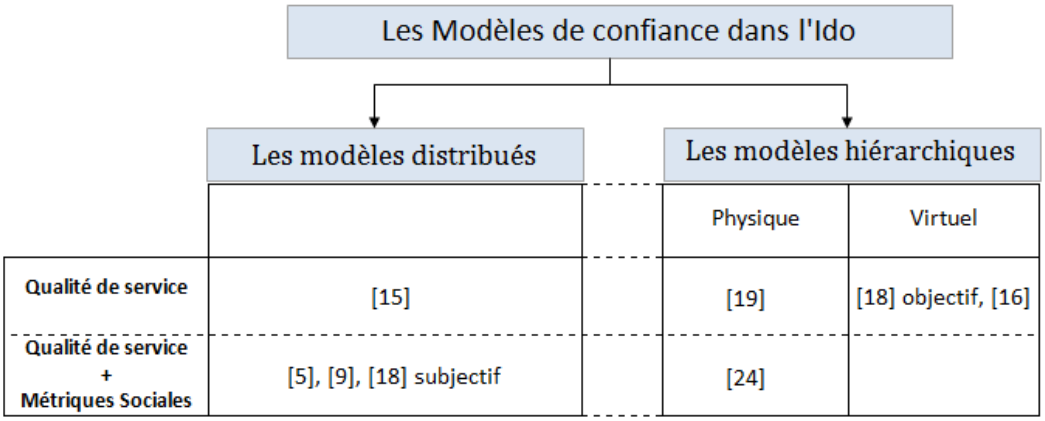

FIGURE 2.1 – Le schéma de classification des solutions des modèles de confiance dans l'IdO.

2.4 Modèles de confiance dans l'Internet des Objets

2.4.1 Modèles distribués

2.4.1.1 "Trust management mechanism for internet of things"

Gu Lize et al. [16] ayant considéré l'Internet des Objets comme un ensemble ou chaque nœud peut être demandeur ou fournisseur de service, ont proposé un mécanisme de gestion de confiance dans le but d'assurer des services plus qualifiés et adéquats.
Compte tenu de la complexité liée à la définition d'un modèle de gestion de confiance pour le système tout entier, les auteurs ont opté pour la distribution du mécanisme sur les trois couches composant l'architecture de l'IdO et qui sont les suivantes : La couche physique, réseau et application.
Le processus de gestion de la confiance se déroule conformément aux étapes décrites dans la figure 2.2

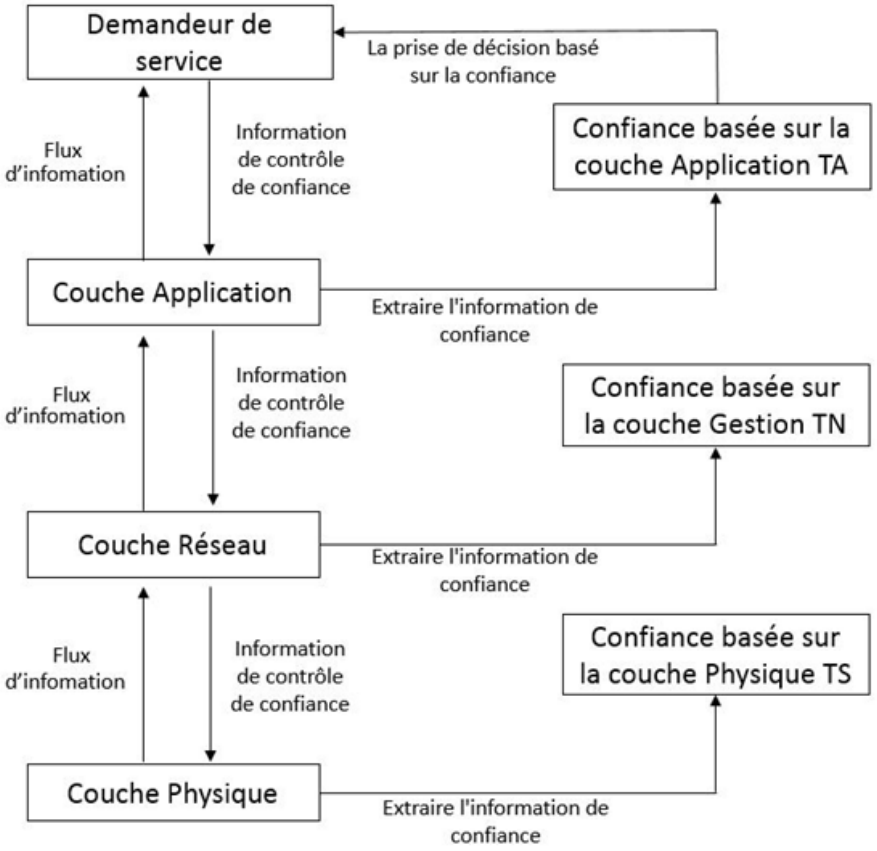

FIGURE 2.2 – Schéma du processus de gestion de la confiance [16].

D'abord un nœud demandeur de service émet une requête que le mécanisme de gestion de confiance traduit en informations de contrôle contenant le service requis, les facteurs de contrôle ou attributs qui serviront au calcul de la confiance ainsi que le contexte qui sont envoyés aux trois couches constituant l'architecture de l'IdO. Ensuite les nœuds de contrôle de chaque couche à la réception de ces informations, collectent les informations de confiance de plusieurs objets candidats à la réalisation du service, puis évaluent le niveau de confiance de chacun d'entre eux pour les combiner aux attributs spécifiés dans les informations de contrôle reçues, ceci en utilisant la théorie des ensembles flous tout en prenant compte du contexte spécifié pour aboutir à un sous ensemble de nœuds jugés aptes à réaliser le service requis, ce résultat représentant la confiance de la couche est transmis à la couche supérieure pour être combiné avec la confiance des autres couches en utilisant la theorie des ensembles flous afin de sélectionner le meilleur triplet de fournisseur de services destiné à réaliser la requête du demandeur de service. De surcroît le mécanisme proposé permet d'assurer le contrôle d'accès en se basant sur la confiance attribuée à un utilisateur sachant qu'il appartient au système IdO.

Discussion et critiques

Le modèle proposé assure une bonne évolutivité grâce à son architecture distribuée, ainsi que la sensibilité au contexte vue l'implication de ce dernier dans le calcul de confiance. Néanmoins, il provoque une grande consommation d'énergie due à l'overhead en terme de messages échangés lors du calcul de la confiance et la prise de décision.
De plus le critère de monitorage n'est pas assuré compte tenu de la nature distribuée du mécanisme, ajouté à cela l'absence de sauvegarde des évaluations de confiance des nœuds.
Enfin, la résistance aux attaques n'ayant pas été considérée dans le modèle, engendre une perte de précision dans le calcul de la confiance.

2.4.1.2 "Trust-based Service Management for Social Internet of Things Systems"

Dans cet article Ing-Ray Chen et al. [10] ont présenté un modèle autonome, adaptive et distribué de gestion de confiance pour le SIoT destiné à la gestion des services dans le système.
La composition de la confiance au sein de ce modèle est basée sur les trois paramètres suivants :

- L'honnêteté, représente le degré de similarité entre la qualité de service qu'un nœud prétend pouvoir assurer et la qualité de service effective dans la réalisation d'un service donné, combiné au degré de vérité dans les recommandations qu'il émet au sujet d'autres nœuds ;
- La coopérativité, un nœud est considéré comme coopératif dans le cas ou il interagit avec ses amis ou les amis de ses amis, ou bien non coopératif dans le cas d'interaction avec d'autres nœuds ;
- L'intérêt à la communauté, déterminé par l'appartenance à la même communauté ainsi que la similarité des capacités en termes de ressources.

Les auteurs ont jugé que les trois paramètres précédents sont suffisants pour le calcul de la confiance de manière juste tout en permettant la résistance aux attaques.
Le calcul de la confiance est effectué par des processus distribués et implémentés dans chaque objet, utilisant des sommes pondérées avec des coefficients dynamiques prenant en compte les expériences subjectives ainsi que les recommandations d'autres objets, tout en accordant un poids supérieur aux évaluations les plus récentes dans le temps.

La propagation et la mise à jour de la confiance, étant orientées événement s'effectuent après chaque interaction entre deux objets. En plus d'une évaluation mutuelle des valeurs de confiance de ces derniers, celles attribuées à d'autres nœuds sont échangées, sachant qu'un objet garde en mémoire uniquement les valeurs de confiance des objets avec lesquels il interagit le plus souvent.

Disscussion et critiques

Le modèle proposé de par son architecture distribuée garantie une bonne évolutivité ainsi que l'adaptation au contexte grâce à l'utilisation de coefficients dynamiques dans les sommes pondérées. La consommation de ressources est modérée par l'utilisation de calculs simples (sommes pondérées) combinés avec une mise à jour de confiance orientée événement, ce qui diminue le nombre de messages échangés entre les nœuds composant le réseau.
Le monitorage n'est pas assuré, étant donné l'absence d'infrastructure centralisée pour la sauvegarde de la réputation de chaque objet, par conséquent le modèle ne résiste pas aux attaques de type *"White-Washing"*,. Cependant, il résiste aux attaques de type *"Self Promoting"* , *"Bad Mouthing "*, *" Ballot Stuffng"* et *"On-Off "* grâce à l'utilisation de l'honnêteté comme paramètre lors du calcul de la confiance, de plus les attaques de type *"Discriminatory"* sont évitées en se basant sur les propriétés de coopérativité et d'intérêt à la communauté pour calculer la confiance, Ce qui permet au nœuds honnêtes ayant récemment rejoint le réseau de se construire une bonne réputation et pouvoir intégrer la communauté d'intérêt.

2.4.1.3 "A Fuzzy Approach to Trust Based Access Control in Internet of Things"

Dans le but de garantir le contrôle d'accès dans l'Internet des Objet, Mahalle et al. [17] ont proposé un modèle à base de confiance, utilisant un Framework chargé du calcul de la réputation de chaque nœud, puis de lui faire correspondre les permissions associées.
Le mécanisme se déroule en trois étapes :

La première étape consiste à collecter les informations suivantes sur chaque objet du réseau : D'abords l'expérience (EX) représentant le rapport du nombre d'interactions réussies par le nombre total d'interactions prenant les valeurs linguistiques suivantes (Mauvaise, Moyenne, Bonne). Ensuite, les connaissances (KN) calculées à partir des évaluations directes et indirectes prenant les valeurs linguistiques suivantes (Insuffisante, Assez, Complete). Enfin les recommandations (RC) obtenues en agrégeant les avis des autres objets prenant les valeurs linguistiques suivantes (Négative, Neutre, Elevée).
Les valeurs linguistiques précédentes sont traduites en valeurs floues appartenant à l'intervalle [-1,1] en plus de l'introduction de fonction d'appartenance prenant des valeurs dans l'intervalle [0,1] et permettant de représenter le degré de vérité d'une valeur linguistique.

Expérience	**Connaissances**	**Recommandations**	**Les plages de noyaux**	**Les valeurs floues**
Mauvaise	Insuffisante	Négative	Au dessous de -0.5	(-1, -1, -0.5, -0.1)
Moyenne	Assez	Neutre	-0.1, 0.25	(-0.25, -0.1, 0.25, 0.5)
Bonne	Complète	Elevée	Au dessus de 0.5	(0.25, 0.5, 1, 1)

TABLE 2.1 – Division des variables linguistiques en valeurs linguistiques.

La deuxième étape consiste à utiliser des règles d'inférences définies par les auteurs en se basant sur le modèle de Mamdani, tel que chaque règle prend en entrées les valeurs linguistiques de EX, KN et RC afin de produire en sortie une valeur de confiance, cette dernière appartient à un des ensembles flous prenant les valeurs linguistiques (bonne, moyenne ou mauvaise), ainsi le résultat retourné par la règle d'inférence est considéré comme l'évaluation de confiance associée au nœud.

La troisième et dernière étape consiste à faire un mappage des évaluations de confiance sur les autorisations d'accès, cela en répartissant les droits d'accès dans des sous-ensembles réunis au sein d'un seul ensemble ayant une cardinalité égale au nombre de valeurs linguistiques en sortie du système d'inférence utilisé, ce qui permet de fournir l'accès aux ressources ou aux appareils avec le principe du moindre privilège.

Discussion et critiques

Le modèle proposé permet une bonne évolutivité sachant que c'est un modèle distribué. Par contre, la résistance aux attaques n'ayant pas été considérée, engendre une grande perte en terme de précision dans le calcul de la confiance. Le processus de collecte d'informations sur chaque nœud provoque un overhead en terme de messages, ce qui induit une consommation énergétique élevée. Enfin, aucun mécanisme de monitorage n'à été défini.

2.4.1.4 "Scalable, Adaptive and Survivable Trust Management for Community of Interest Based Internet of Things Systems"

Dans cet article Fenye Bao et al. [6] ont proposé un modèle de gestion de confiance pour le SIoT utilisant la qualité de service ainsi que les métriques spécifiques au SIoT (honnêteté, coopérativité, internet à la communauté) comme composantes de la confiance.
La propagation de la confiance est distribuée, en effet chaque nœud sauvegarde en mémoire les valeurs de confiance attribuées aux nœuds avec lesquels il a interagit, cela conformément à une politique d'enregistrement définie dans le mécanisme, permettant ainsi de privilégier le maintien en mémoire des évaluations de confiance des nœuds ayant une bonne réputation ou bien ceux avec lesquels il a récemment interagit.
Les informations stockées servirons à agréger les observations subjectives en confiance directe en utilisant des sommes pondérées, mais aussi à agréger les recommandations en confiance indirecte, cela en utilisant la similarité sociale ainsi que les sommes pondérées dynamique pour ajuster le poids associés à la confiance directe et indirecte dynamiquement, ce qui permet la maximisation des performances et la sensibilité au contexte.
La mise à jour de la confiance étant orientée événement, s'effectue après chaque interaction, tout en privilégiant les interactions récentes par rapport au plus anciennes en leur attribuant un poids plus fort dans la somme pondérée, ce qui donne au modèle la possibilité d'adaptation au

dynamisme du SIoT tout en évitant la discrimination des nouveaux nœuds qui rejoignent le réseau.

Discussion et critiques

Le modèle propose permet de garantir une évolutivité élevée grâce à ça nature distribuée, cependant, la mobilité n'est pas garantie à cause de l'absence d'infrastructure centrale dédiée à la sauvegarde des valeurs de confiance de tous les nœuds du réseau. L'utilisation de sommes pondérées dans le calcul de la confiance ainsi que la nature orienté événement de la mise à jour de ces valeurs, permet une économie d'énergie considérable au niveau des nœuds du réseau très faibles en ressources. La résistance aux attaques est assurée en combinant les trois paramètres honnêteté, coopérativité et intérêt à la communauté pour détecter les nœuds malicieux ce qui permet de garantir une bonne précision lors du calcul de la confiance.

2.4.2 Modèles hiérarchiques

2.4.2.1 "Guarantor and Reputation Based Trust Model for Social Internet of Things"

Hannan Xiao et al. [25] ont proposé un modèle hiérarchique de gestion de confiance pour le SIoT utilisant deux paramètres, le premier est la réputation employée pour déterminer le niveau de fiabilité d'un nœud dans l'accomplissement d'un service donné, le second ayant pour but de détecter les nœuds malicieux est le crédit faisant office de commission à céder pour obtenir un service digne de ce qui à été convenu ou de caution dans le cas contraire.

La gouvernance du système est assurée au niveau de la couche application de l'IoT, ceci en utilisant une chaine de serveur de deux types différents. Le premier type représente les serveurs de réputation chargés du calcul, la mise à jour et la propagation des valeurs de réputation des nœuds du réseau. Le second type représente les serveurs de bases de données prenant en charge la découverte de services ainsi que le choix des meilleurs chemins pour y accéder.

Un objet nécessitant un service envoi une requête destiné au gestionnaire de confiance à travers son point d'accès dans laquelle il indique le service, la commission qu'il est prêt à payer en échange du service, ainsi que le forfait que l'objet fournisseur de service lui cédera dans le cas de réalisation d'un service jugé de mauvaise qualité. A la réception de la requête le gestionnaire de confiance interroge le serveur de bases de données pour avoir l'ensemble des objets pouvant fournir ce service, puis selectionne parmi eux celui dont la réputation est la plus élevée. L'objet sélectionné fournit le service au demandeur du service, qui procède par la suite à l'évaluation de la qualité du service reçu, cette dernières sera envoyée sous forme de rapport au serveur de réputation.

Dans le cas de réalisation d'un bon service le demandeur de service paye la commission convenue au fournisseur de service, dans le cas contraire le fournisseur de service cède un forfait qui est une sorte d'indemnisation. Si un objet malicieux fournit de faux rapports à propos d'un objet, alors ce dernier conteste au près de du gestionnaire de confiance afin que l'émetteur du rapport soit sanctionné.

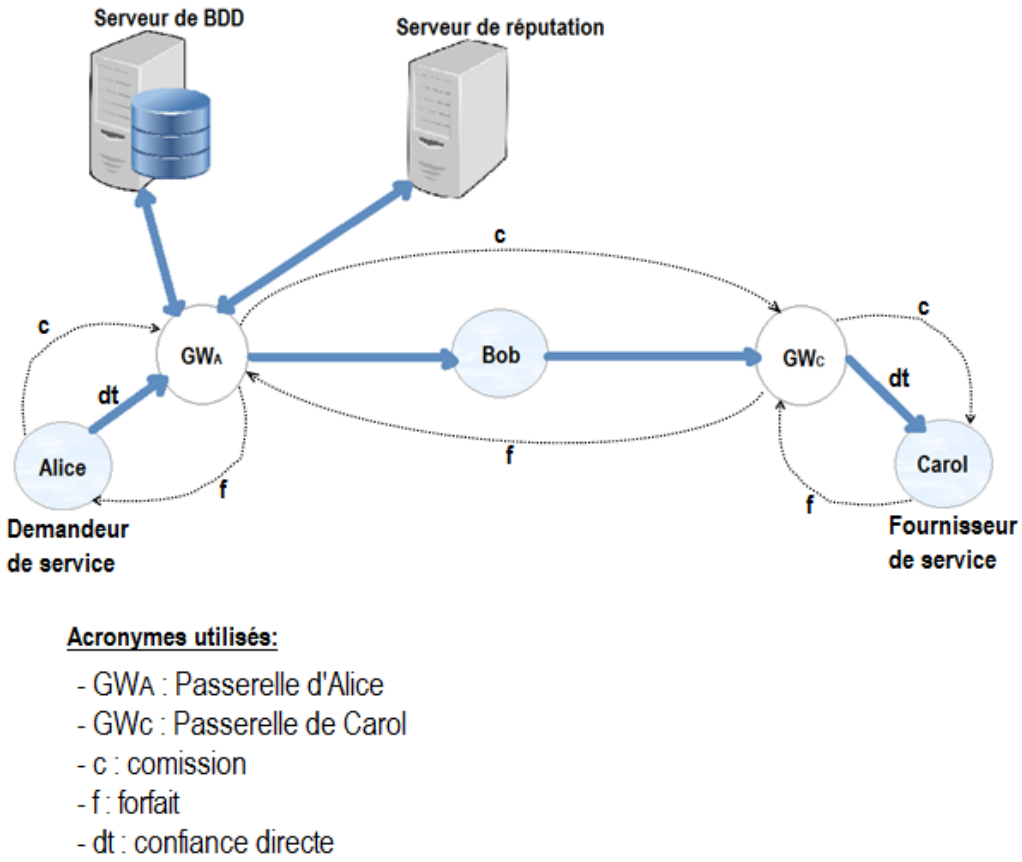

FIGURE 2.3 – Modèle de confiance à base de garantie et réputation [25].

Disscussion et critiques

Le modèle proposé permet le monitorage grâce à la centralisation de la sauvegarde des évaluations de chaque nœud de l'IdO. En ce qui concerne la consommation de ressources, la charge de calcul est transmise à la couche application qui est très riche en ressources. Cependant, le critère d'évolutivité n'est pas garanti et la résistance aux attaques étant sensée être assurée par l'utilisation du crédit présente de nombreuses lacunes relevant, d'une part, de l'absence de politique de gestion et distribution de crédits entre les nœuds ainsi qu'un moyen de vérification de la qualité de service, et d'autre part de la détection des nœuds malicieux effectuée par les nœuds. Enfin, le

fait que le mécanisme proposé ne soit pas résistant aux attaques engendre une perte considérable de précision dans le calcul de la confiance.

2.4.2.2 "Trustworthiness Management in the Social Internet of Things"

Dans cet article, Michele Nitti et al. [19] ont proposé deux modèles de gestion de confiance pour le SIoT, le premier est subjectif, le second objectif. Les deux utilisent la qualité de service ainsi que les caractéristiques du SIoT pour la composition de la confiance.

Dans la première approche (subjective), chaque nœud A calcul la valeur de confiance qu'il attribue à un nœud B avec lequel il à interagit, puis sauvegarde cette valeur, en plus d'un bilan lié à la qualité de service assuré pour pouvoir le diffuser à la demande à un autre nœud C ayant un lien social avec A. Les informations transmises font office de recommandation sur ce dernier. Le nœud C, afin d'évaluer B, utilise la recommandation apportée par A, sa centralité, et son expérience directe avec A comme facteurs dans une somme pondérée. La mise à jour des valeurs de confiance est orientée événement, tel que chaque intéraction entre deux nœuds est suivie d'une évaluation mutuelle des valeurs de confiance.

Dans la deuxième approche (objective), les auteurs ont opté pour une structure centralisée où les informations liées à la qualité de service assuré par chaque nœud sont envoyées à une entité centrale, utilisant une table de hachage dynamique (DHT), sur le réseau afin de maintenir la réputation globale de chaque nœud. Un nœud ayant besoin de la valeur de confiance d'un nœud quelconque du réseau procède à l'émission d'une requête destinée à la DHT qui cherchera cette valeur dans la base de données et la retournera au demandeur.
L'agrégation de la confiance est faite en utilisant des sommes pondérées statiques prenant comme facteurs la centralité, la qualité de service direct et indirect.
La mise à jour des informations sauvegardées dans la DHT est effectuée après chaque interaction, tel que chaque nœud A recevant un service de la part de du nœud B, émet un rapport décrivant le service fourni.

Discussion et critiques

L'approche subjective permet de garantir l'évolutivité de par sa nature distribuée. Par contre, le monitorage n'est pas possible à cause de l'absence de stockage centralisé des valeurs de confiance des nœuds du réseau. Le modèle résiste aux attaques de type *"Self-Promoting"*, *"Bad-Mouthing"* et *"Ballot-Stuffing"*, grâce à l'utilisation de la crédibilité comme poids pour les recommandations, mais aucun mécanisme de résistance aux attaques de types *"On-Off"* et *"white-waching"* n'a été défini, ce qui engendre une perte de précision lors du calcul de la confiance. Enfin, ce modèle permet une économie d'énergie grâce à l'utilisation de sommes pondérées pour le calcul de la confiance.

L'approche objectif permet de retirer le fardeau de calcul aux nœuds du réseau, ce qui implique une moindre consommation de ressources en plus de l'assurance de l'évolutivité en tenant compte du fait que le modèle a été inspiré des technologies utilisées dans les réseaux P2P. Le monitorage est assuré grâce au stockage des informations de confiance de chaque nœud du réseau et leur disponibilité. Cependant, elle ne résiste pas aux attaques de type *"On-Off"*, ce qui cause une perte de précision lors du calcul de la confiance.

2.4.2.3 "Trust management system design for the Internet of Things : A context-aware and multiservice approach"

Ayant comme objectif de garantir une composition de services précise, optimale et sensible au contexte pour l'Internet des objets, Ben saied et al. [20] ont proposé un modèle de gestion de confiance hiérarchique à base de réputation. Le processus se déroule selon les cinq phases décrites à la figure 2.4.

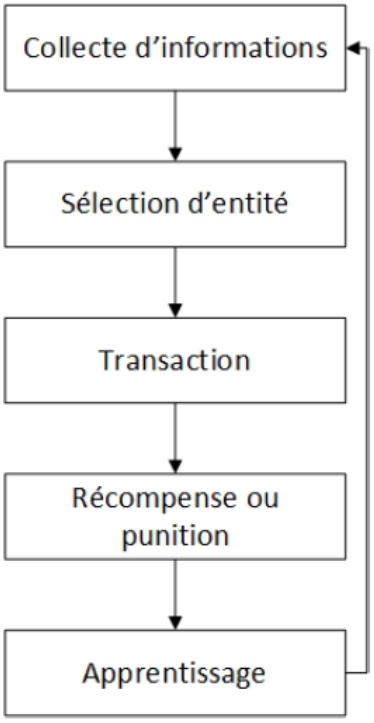

FIGURE 2.4 – Processus de gestion de la confiance dans l'IdO [20].

La première étape est la collecte d'information représentant les témoignages émis par de objets ayant reçu un service d'un autre objet, chaque rapport contient le service fournit, son temps d'exécution, le score affecté par le témoin à l'objet fournisseur du service ainsi que son état courant (vieillissement, capacité en ressources), permettant de savoir dans quelle conditions le nœud coopérant a obtenu l'évaluation rapportée.
La seconde étape est la sélection des meilleurs proxy en tenant compte du service spécifié, mais

aussi du contexte et ceci en privilégiant les nœuds ayant fourni le même service dans des conditions équivalentes, ou en utilisant la similarité de contexte représentant le rapport entre le service et la capacité en ressource pour sa réalisation, tout en favorisant les services les plus récents dans la sélection.
La troisième et la quatrième phase sont la fourniture du service suivie de l'évaluation des objets fournisseurs du service représentant une récompense ou une punition. La dernière phase est subdivisée en deux étapes, la première est la mise à jour de la qualité de recommandation des nœuds ayant fourni les rapports, en effectuant la comparaison entre ces dernières, suivie de la mise à jours des réputations des nœuds fournisseurs de service en calculant la somme des scores attribués par les nœuds demandeurs de service pondérés avec leur qualité de recommandation.

Discussion et critiques

Le modèle proposé permet le monitorage ainsi qu'une moindre consommation d'énergie grâce à sa nature hiérarchique. Cependant, en plus de ne pas garantir l'évolutivité, il ne résiste pas aux attaques de type " *On-Off* " puisque le mécanisme de punition implémenté ne prend pas en compte le comportement à long terme des nœuds, causant une perte de précision dans le calcul de la confiance.

		Résistance aux attaques	**Evolutivité**	**Monitorage**	**Moindre consommation de ressources**	**Précision du calcul de la confiance**
Distribué	G. Lize et al. [16]	Non	Oui	Non	Non	Non
	I. R. Chen et al. [10]	Oui	Oui	Non	Oui	Oui
	M. Nitt et al. [19] Subjectif	Non	Oui	Non	Oui	Non
	P. N. Mahalle et al. [17]	Non	Oui	Non	Non	Non
	F. Bao et al. [6]	Oui	Oui	Non	Oui	Oui
Hiérarchique	H. Xiao et al. [25]	Non	Non	Oui	Oui	Non
	M. Nitti et al. [19] Objectif	Non	Non	Oui	Oui	Non
	Y. Ben Saied et al. [20]	Non	Non	Oui	Oui	Non

TABLE 2.2 – Comparaison des solutions basées sur la confiance dans l'IdO.

2.5 Synthèse

Les modèles distribués

Inspirés par les solution proposées pour les réseaux P2P , ces modèles permettent une autonomie des objets, une très forte évolutivité mais s'avèrent de faible efficacité du point de vue de la résistance aux attaques, ce qui influence de manière négative sur l'exactitude de la dérivation de la confiance et ne garantissent pas le monitorage car il n'existe pas d'entité centrale destinée a la supervision des nœuds du réseau.

Les modèles hiérarchiques

Les modèles hiérarchiques présentent des avantages quant à la possibilité de monitorage, à la faible consommation d'énergie et à la résistance aux attaques, permettant ainsi une grande précision

dans le calcul de la confiance mais se voient désavantagés par une faible évolutivité compare aux modèles complètement distribués.

2.6 Conclusion

De cette analyse nous avons retenu que de toutes les solution proposées aucune ne garanti l'ensemble des critères préalablement définis mais aussi la résistance aux attaques de type DoS. Ces modèles représentent ainsi des solutions partielles aux problématiques rencontrées dans la gestion de confiance dans l'internet des objets.

Autrement dit, afin qu'une solution soit complète, elle devra garantir à la fois tous les critères mais aussi la résistance aux attaques de type DoS.

Chapitre 3

Modèle de gestion de confiance à base de crédit et d'honneteté pour l'Internet des Objets

3.1 Introduction

Dans le chapitre précédent, nous avons étudié quelques-unes des solutions les plus récentes proposées pour la gestion de confiance dans l'IdO. Ce qui nous a permis d'une part la déduction d'une certaine prédominance de l'aspect social dans les modèless proposés, d'une autre part l'identification des faiblesses présentes dans la littérature.

En restant dans la perspective d'une approche sociale de l'Internet des objet, nous avons proposé un modèle de gestion de confiance hiérarchique combinant le crédit et l'honnêteté, dans le but de palier les carences perçues dans les travaux antérieurs et ainsi garantir un calcul de confiance précis et fiable tout en s'adaptant aux caractéristiques exceptionnelles du système d'IdO.

3.2 Motivations

L'Internet Des Objets étant un réseau hétérogène composé pour la plus part d'entités fortement limitées en termes de ressources, la réalisation de services dans un tel environnement fait appel à une approche collaborative. Cette méthode engendre un nombre considérable d'interactions durant lesquelles chaque objet cherche à interagir avec les objets les plus efficaces dans la réalisation d'un service donné. La prédominance de l'aspect social dans le système fait de la confiance le critère prépondérant dans le choix d'un fournisseur de service, de ce fait le score de confiance associé à chaque objet doit refléter précisément et réellement le degré de son implication ainsi que la qualité des services qu'il a précédemment accompli, afin de garantir un fonctionnement correct du système.

Cependant la gestion de confiance dans un tel système représente un véritable challenge, étant donné qu'il est doté de caractéristiques exceptionnelles qui amplifient les risques d'attaques et rendent la mise en place de mécanismes de sécurité très complexes.

Les travaux proposés dans la littérature présentent pour la plupart des faiblesses, ces dernières sont dues à l'attribution d'une priorité dans la résolution des problèmes rencontrés lors de l'élaboration d'un système de gestion de confiance. De ce fait, les solutions existantes ne représentent que des résolutions partielles de la problématique.

Nous avons choisi cet axe de recherche dans la perspective de proposer un modèle de gestion de confiance plus adapté aux besoins spécifiques de l'IdO et ainsi participer à sa concrétisation.

3.3 Hypothèses

Dans le cadre de notre travail, nous admettons que l'IdO est un réseau dense composé d'objets hétérogènes déployés aléatoirement et regroupés en communautés.
Chaque objet peut jouer le rôle de fournisseur ou demandeur de service dans une interaction, chaque objet a une identité unique et appartient à une seule communauté gérée par un serveur de confiance, un objet sollicité pour la réalisation d'un service peut soit accepter ou refuser de le fournir. Les canaux de communication sont fiables ceci est concrétisé grâce à l'utilisation d'une infrastructure réseau et des protocoles de communication adaptés aux spécifications et aux besoins de l'Internet Des Objets.
Nous supposons aussi que toutes les variables destinées à contenir le crédit, l'honnêteté et le score de confiance des objets sont stockées et gérées au niveau du serveur de communauté, de façon à garantir leur intégrité et ainsi préserver les ressources des objets.

3.4 Modèle de gestion de confiance à base de crédit et d'honnêteté pour l'internet des objets

3.4.1 Modèle physique

Notre modèle de confiance repose sur une architecture hiérarchique s'appuyant sur l'utilisation d'une entité de confiance caractérisée par des capacités énormes de calcul et de stockage appelée le gestionnaire de confiance. Ce dernier est composé de plusieurs serveurs de communauté entre lesquels il existe des relations de confiance, ceci dans le but de garantir l'évolutivité du model.

Le serveur de communauté assure la gestion de confiance et la découverte des services assurés par les objets qu'il supervise. Un objet nécessitant un service envoi une requête à travers son point d'accès, cette dernière est transmise au serveur de communauté à laquelle il appartient. À la réception de la requête un objet fournisseur de service est sélectionné sur la base du son score de confiance.

Idéalement, le fournisseur de service choisi appartient à la même communauté (interaction intra-communauté), car il est privilégié par rapport aux objets des autres communautés, de manière à réduire la charge sur la couche réseaux du système et ainsi garantir une bonne scalabilité du modèle.

Dans le cas où la requête ne peut être satisfaite par un objet de la même communauté, le serveur la transmet à une autre communauté avec laquelle il entretient une relation de confiance (interaction inter-communauté), d'où l'utilité de la répartition du système de gestion de confiance sur plusieurs serveurs physiques afin de créer une seule entité de gestion virtuelle, à savoir le gestionnaire de confiance.

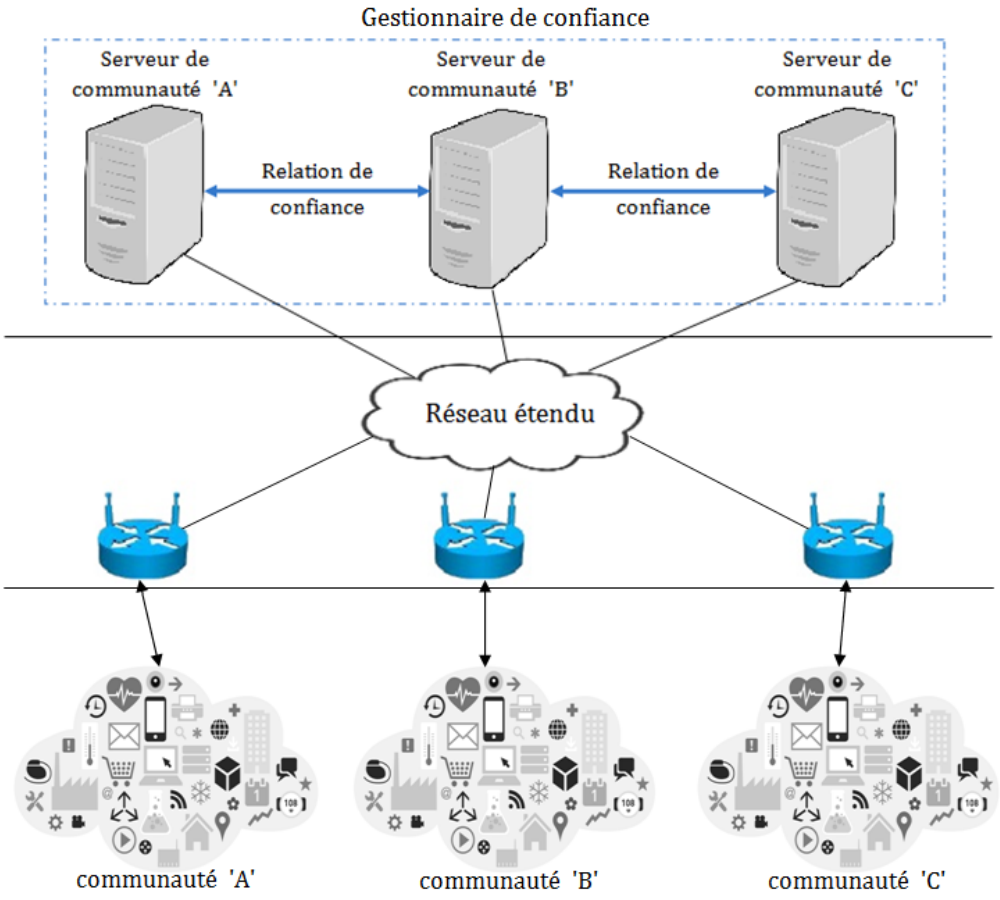

FIGURE 3.1 – Modèle physique du system de gestion de confiance.

3.4.2 Fonctionnement du gestionnaire de confiance

Notre modèle de confiance procède conformément aux cinq phases decrites dans la figure 3.2.

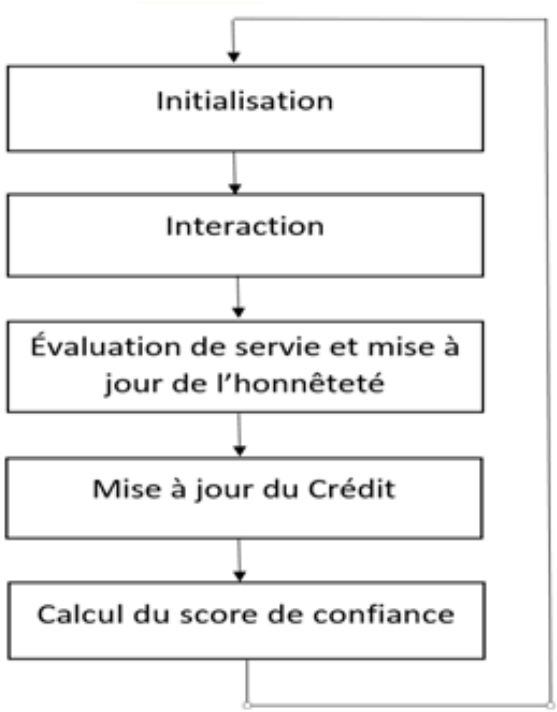

FIGURE 3.2 – Les différentes phases de notre modèle de confiance.

Le tableau suivant représente les différents paramètres contenus dans les formules utilisées dans notre modèle de confiance.

Paramètre	**Signification**
C_i	Crédit initial affecté à un objet.
C_d	Valeur de crédit minimum néczssaire pour une interaction.
C_{ap}	Capacité d'un objet (relative aux ressources).
ρ	Facteur permettant d'ajuster le poids de l'energie d'un objet par rapport aux autres ressources.
E	Energie d'un objet.
λ	Facteur permettant d'ajuster le poids de la capacité de stockage d'un objet par rapport aux autres ressources.
M	Capacité de stockage d'un objet
μ	Facteur permettant d'ajuster le poids de la puissance de calcul d'un objet par rapport aux autres ressources.
P	Puissance de calcul d'un objet.
S	Service.
S'	Service similaire au service S (soit même service soit complexité équivalente).
$St_f^d(s)$	Similarité du taux de satisfaction émis par l'objet d sur un service S fourni par un objet f avec les autres taux émis à propos du même service(ou un service similaire en terme de complexité) fournis par le même objet f.
$T_f^d(s)$	Taux de satisfaction émis par l'objet d sur un service S fourni par un objet f.
$T_f^i(s')$	Taux de satisfaction émis par l'objet i sur un service s' fourni par un objet f.
N	Nombre total d'appréciations émises sur le service S ou un service similaire en termes de complexité par un objet quelconque.
$H^d(t)$	Honnêteté d'un objet d à l'instant t.
σ	facteur permettant d'ajuster le poids de l'évaluation récent de l'honnête par rapport à l'ancienne valeur.
$C^d(t)$	Crédit associé à l'objet d demandeur de service a l'instant t.
t_l	Instant de la dernière interaction.
$Co_f^d(s)$	Commission négocié par le demandeur de service d avec un fournisseur de service f concernant le service S.
$C^f(t)$	Crédit associé à l'objet f fournisseur de service a l'instant t.
φ	Facteur représentant la fréquence de mauvais service effectué .
Bs^d	Nombre de bons services fournis par d.
Ts^d	Nombre total de services fournis par d.
F_f^d	Forfait négocié par le demandeur de service d avec un fournisseur de service f concernant le service S.
t_0	temps d'oisiveté toléré.
ω	Facteur permettant d'ajuster la punition infligé.
$CF_0(t)$	Score de confiance d'un objet o à l'instant t.
γ	Facteur permettant d'ajuster le poids de l 'honnêteté dans le calcul de la confiance.
$H^0(t)$	Évaluation de l'honnêteté d'un objet o à l' instant t.
$C^0(t)$	Évaluation du crédit d'un objet o à l' instant t.

TABLE 3.1 – Les paramètres utilisés dans la formule de dérivation de la confiance directe et de la réputation.

3.4.2.1 Initialisation

Après le déploiement du réseau, le gestionnaire de confiance procède à l'initialisation de la réputation, du score de confiance et du crédit affecté à chaque objet du système IdO. Sachant que tous les objets sont considérés comme neutres au début, les valeurs affectées à la réputation ainsi

qu'un score de confiance sont celles représentatives de la neutralité dans les intervalles de notation choisis.

Le crédit, étant la monnaie d'échange de services, doit être initialisé sur tout objet pour lui permettre d'interagir. Cependant, l'hétérogénéité des objets du système IdO et l'implication du crédit dans le calcul du score de confiance ont rendu nécessaire la définition d'un mécanisme d'initialisation proportionnel aux capacités des objets en termes de ressources (Énergie, capacité de stockage, puissance de calcul).

En effet un objet riche en ressources à tendance à acquérir du crédit plus facilement, car il peut fournir des services supérieurs en nombre et en genre, c'est pour cela que le crédit qui lui sera initialement affecté sera le minimum pour pouvoir démarrer des interactions.

En revanche un objet pauvre en ressources, pour lequel le gain de crédit est plus difficile, se verra affecté un crédit initial supérieur à celui d'un objet riche en ressources. Le calcul du crédit initial affecté à un objet est définit par la formule :

$$C_i = C_d * (1 + \frac{1}{C_{ap}}) \qquad (3.1)$$

La formule ci-dessus permet de garantir une proportionnalité dans l'affectation du crédit, ceci en assurant une corrélation négative entre la capacité d'un objet (C_{ap}) et son crédit initial, tel que la capacité (C_{ap}) d'un objet est calculée en utilisant une somme pondérée faisant intervenir trois paramètres qui sont l'énergie, l'espace de stockage et la puissance de calcul, ceci conformément à la formule suivante :

$$C_{ap} = \rho.E + \lambda.M + \mu.P \qquad (3.2)$$

Où les facteurs ρ, λ et μ permettent d'ajuster les poids de chaque paramètre selon les besoins de l'application, afin de garantir la sensibilité et l'adaptation au contexte.

3.4.2.2 Interaction

Un objet nécessitant un service, génère une requête contenant : le service, le seuil minimum de confiance que doit avoir son fournisseur, la commission qu'il est prêt à payer en contrepartie ainsi que le forfait que le fournisseur de service lui cèdera dans le cas de la réalisation d'un mauvais service.

A la réception d'une requête, débute la deuxième phase qui consiste à sélectionner l'objet satisfaisant les exigences du service demandé dans la même communauté s'il existe. Dans le cas contraire la requête sera retransmise au serveur d'une autre communauté avec laquelle il entretient

une relation de confiance. Un objet ayant reçu une requête de service peut soit :

- **Accepter la réalisation du service :** en le fournissant au demandeur de service qui par la suite procèdera à son évaluation.
- **Refuser la réalisation du service :** en répondant au gestionnaire avec un message de refus de service, le gestionnaire de confiance sélectionnera un autre fournisseur de service, de manière transparente au demandeur de service.

3.4.2.3 Évaluation de service et mise à jour de l'honnêteté

A la fin de chaque interaction, l'objet demandeur évalue le service effectué et envoie un rapport au gestionnaire de confiance, dans lequel il émet une appréciation (taux de satisfaction) positive ou négative sur le fournisseur du service. Cette évaluation sera enregistrée pour déduire l'honnêteté de l'émetteur du rapport, puis être utilisée ultérieurement pour le calcul de la confiance du fournisseur de service.

L'honnêteté d'un objet (d) à l' instant t est calculée en utilisant une somm1e pondérée, combinant l'ancienne valeur d'honnêteté ainsi que la similarité de taux de satisfaction sur un même service ou un service ayant une complexité semblable fournie par un même objet.

$$St_f^d(s) = \frac{T_f^d(s)}{\sum_{i=1}^{N} \frac{T_f^i(s').H^i}{N}} \qquad (3.3)$$

La formule 3.3 permet de calculer la similarité de taux de satisfaction, en comparent le taux de satisfaction émis par l'objet demandeur (d) sur l'objet fournisseur (f) ayant fourni un service s avec tout les taux de satisfaction émis par d'autres objets sur le fournisseur de service (f) concernant le même service ou un service dont la complexité est semblable *s'*.
La valeur calculée appartient à l'intervalle]0, 1], tel que cette valeur représente le pourcentage d'honnêteté de l'objet demandeur de service dans le jugement du fournisseur de service.

L'utilisation de la similarité de taux de satisfaction permet ainsi d'éviter les attaques de types *Bad-mouthing, Good-mouthing et Ballot-stuffing*, un objet ne peut pas mentir sur la qualité de service effective d'un autre objet, car dans le cas contraire il est directement sanctionné en diminuant son honnêteté et finira par être exclu du réseau dans le cas de récidive.

$$H^d(t) = (1 - \sigma) * H^d(\Delta t) + \sigma[St_f^d(s)] \qquad (3.4)$$

Le facteur σ est introduit afin d'ajuster le poids de la valeur d'honnêteté récente par rapport à l'ancienne valeur, de cette manière la précision de calcul est garantie car elle reflète l'honnêteté

d'un objet à long terme, ainsi le gestionnaire de confiance est protégé contre les attaques de type *On-Off*. Dans le cas où l'honnêteté d'un objet est inférieure à un seuil S_H, il est exclu du réseau en le considérant comme malicieux.

3.4.2.4 Mise à jour du crédit

Le processus de mise à jour du crédit est un facteur déterminant dans le calcul de la confiance, par conséquent il est exécuté après chaque interaction, tel que le fournisseur du service est soit récompensé (commission) dans le cas d'une bonne prestation, ou bien punit (forfait) dans le cas contraire.

- **Récompense**

Dans le cas où le service fourni est conforme à ce qui a été convenu dans la requête de demande de service, le serveur de communauté déduit un nombre de crédit du demandeur de service (commission) et l'additionne au crédit du fournisseur de service, cela conformément aux formules suivantes :

$$C^d(t) = C^d(\Delta t) - Co_f^d(s) \qquad (3.5)$$

La formule ci-dessus permet de calculer le crédit d'un demandeur de service d ayant bénéficié d'un service $s$réalisé par un fournisseur de service f , tel que la commission $Co_f^d(s)$ est déduite de son crédit avant l'interaction $C^d(\Delta t)$ pour aboutir à la valeur de crédit restant après l'interaction $C^d(t)$.

$$C^f(t) = C^f(\Delta t) + Co_f^d(s) \qquad (3.6)$$

Dans le cas ou un objet fournit un bon service, il est récompensé en additionnant la commission qu'il a reçu depuis l'objet demandeur de service à son crédit, cela conformément à la formule 3.6.

- **Punition**

Un Objet est puni dans les deux cas suivants :

1. **Fourniture d'un mauvais service :** Dans le cas où un fournisseur de service ne satisfait pas les conditions convenues dans la prestation de service offerte à un objet, il est sanctionné en diminuant sont crédit conformément à la formule 3.7.
   Le demandeur de service bénéficie du forfait convenu dans la requête de service comme le montre la formule 3.8.

$$C^f(t) = C^f(\Delta t) - \varphi F_f^d(S) \qquad tel \quad que \qquad \varphi = \frac{Bs^d}{Ts^d} \qquad (3.7)$$

La punition d'un fournisseur de service est proportionnelle, tel que le facteur φ représente la fréquence des mauvais service au sein de tous les services réalisés, ainsi plus un objet fournis de mauvais service plus couteuse en crédit sera la punition, par conséquent un nœud fournissant de mauvais services finira par épuiser son crédit.

$$C^d(t) = C^d(\Delta t) + F_f^d(S) \qquad (3.8)$$

Dans le cas de fourniture d'un mauvais service, le demandeur de service reçoit un forfait qui est additionné à son crédit, conformément à la formule 3.8, cette valeur représente une indemnisation.

Remarque : la punition est toujours plus sévère que la récompense afin d'éviter les attaques de type *On-Off*.

2. **Oisiveté :** Un objet est oisif car il ne fournit pas de service pendant une certaine durée ou indéfiniment, parce qu'il est soit malveillant ou bien défectueux.

Dans le but d'encourager les objets bienveillants à interagir et détecter les nœuds malveillants ou défectueux, le gestionnaire de confiance diminue le crédit des objets n'ayant pas interagi pendant un temps fixé t_0, ce dernier est calculer en procédant à une soustraction entre l'instant actuel t et le temps de la dernière interaction, ce qui permet de déduire le temps pendant lequel l'objet est resté sans interagir, puis si le temps de oisiveté déduit est supérieur à t_0 alors le neoud est puni conformément à la formule suivante :

$$Si \qquad t - t_l > t_0 \qquad Alors \qquad C^f(t) = C^f(t) - \omega C^f(t) \qquad (3.9)$$

Le facteur ω est défini afin d'ajuster le coût de la punition selon les besoins de l'application.

Dans les modèles ne mettant pas en œuvre le crédit, un nœud malicieux peut épuiser les ressources d'un ou plusieurs objets en effectuant une attaque de déni de service. Par contre, dans notre modèle, la mise en place de ce type d'attaques est exclue car tout service à un coût, par conséquent un nœud voulant attaquer un autre nœud se doit d'être un bon fournisseur de services afin de gagner assez de crédit pour demander des services, ainsi un nœud malveillant devra épuiser ses propres ressources pour pouvoir attaquer un autre objet.

3.4.2.5 Mise à jour du score de la confiance

Après que l'honnête ainsi que le crédit soient mis à jour, le gestionnaire de confiance calcule le score de confiance des deux nœuds ayant interagit en utilisant la formule suivante :

$$CF_0(t) = (1 - \gamma)H^0(t) + \gamma C^0(t) \qquad (3.10)$$

Le facteur γ représente un pourcentage servant à ajuster le poids d'honnêteté ainsi que le crédit dans le calcul de confiance. Dans le cas où le score de confiance d'un objet diminue en-dessous d'un seuil prédéfini, il est ajouté à un ensemble de nœud malades.

3.5 Conclusion

Dans ce chapitre, nous avons proposé un modèle de confiance combinant l'honnêteté et le crédit dans le calcul de la confiance, ceci dans le but de tirer parti de la complémentarité existante entre ces deux paramètres pour garantir un calcul de confiance précis et adaptif aux caractéristiques spécifiques de l'IdO.

En effet l'utilisation de l'honnêteté dans le calcul permet non seulement de garantir une bonne qualité de recommandation mais aussi la résistance aux attaques sur la réputation des nœuds. L'idée du crédit permet d'attribuer une valeur aux services et de cette manière encourager l'interaction et éviter les attaques de déni de services sur les objets.

Conclusion générale et perspectives

Ce travail nous a montré l'influence des caractéristiques de l'Internet des objets, à savoir la pauvreté en termes de ressources des objets, l'ubiquité et l'hétérogénéité, sur les solutions devant être proposées pour la gestion de la confiance. En effet, ces spécificités accroissent considérablement les risques d'attaques, que ça soit des attaques traditionnelles sur la confiance ou de type DoS, visant à altérer le bon fonctionnement du système de gestion de confiance en particulier et de tout le système en général.

A travers les différents modèles étudiés dans ce travail, nous avons constaté une certaine priorité dans les critères à prendre en considération dans la proposition d'une solution ainsi que l'avantage des modèles hiérarchiques quant à la garantie d'un maximum de ces critères, à la différence des modèles distribués qui malgré la forte autonomie qu'ils procurent présentent un besoin en ressources et des risquent en termes de sécurité trop élevés.
Pour cela, nous avons opté pour une approche hiérarchique qui apporte une solution permettant d'éviter, premièrement, les attaques de type DoS en attribuant un coût à chaque service, de part l'utilisation du crédit qui oblige un nœud malveillant à accomplir d'abord un bon service pour ensuite effectuer une attaque, et deuxièmement, les attaques sur la confiance en utilisant l'honnêteté comme paramètre dans le calcul de la confiance.

À l'origine de ce travail, les critères qu'un modèle de gestion de confiance pour l'Internet des objets devait remplir ont été énuméré et nous avons proposé un modèle théorique pour lequel nous avons comme perspective d'effectuer une simulation afin d'évaluer ses performances sur la base de ces critères, notamment la scalabilité, la consommation de ressources et la résistance aux attaques.

Bibliographie

[1] https://www.w3.org/2014/02/wot/papers/baccelli.pdf (accèdè le 26/03/2016).

[2] S. Abbas, M. Merabti, and D. Llewellyn-Jones. Deterring whitewashing attacks in reputation based schemes for mobile ad hoc networks. In *Wireless Days*, pages 1–6. IEEE, 2010.

[3] A. Abdul-Rahman and S. Hailes. Supporting trust in virtual communities. In *System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on*, pages 9–pp. IEEE, 2000.

[4] A. Aris, S. F. Oktug, and S. B. O. Yalcin. Internet-of-things security : Denial of service attacks. In *Signal Processing and Communications Applications Conference (SIU), 2015 23th*, pages 903–906. IEEE, 2015.

[5] K. Ashton. That 'internet of things' thing. *The Real World Things Matter More than Ideas. RFID Journal*, 2009.

[6] F. Bao, I. R. Chen, and J. Guo. Scalable, adaptive and survivable trust management for community of interest based internet of things systems. In *Autonomous Decentralized Systems (ISADS), 2013 IEEE Eleventh International Symposium on*, pages 1–7, March 2013.

[7] A. Beghriche and A. Bilami. Modélisation et gestion de la confiance dans les réseaux mobiles ad hoc. In *CIIA*, 2009.

[8] P. J. Benghozi, S. Bureau, and F. Massit-Folea. L'internet des objets. quels enjeux pour les européens ? Technical report, HAL, 2011.

[9] Y. Challal. *Sécurité de l'Internet des Objets : vers une approche cognitive et systémique*. PhD thesis, Université de Technologie de Compiègne, 2012.

[10] I. R. Chen, F. Bao, and J. Guo. Trust-based service management for social internet of things systems. *IEEE Transactions on Dependable and Secure Computing*, PP(99) :1–1, 2015.

[11] J. Guo and I. R. Chen. A classification of trust computation models for service-oriented internet of things systems. In *SCC*, pages 324–331. IEEE Computer Society, 2015.

[12] IDA. https://www.ida.gov.sg/~/media/Files/Infocomm%20Landscape/Technology/TechnologyRoadmap/InternetOfThings.pdf (accèdè le 16/04/2016).

[13] INHESJ. Sécurité des objets connectés. http://www.inhesj.fr/sites/default/files/sececo/securite_objets_connectes.pdf (accèdè le 27/04/2016).

[14] Recommendation X ITU-T. 509,âœ. *Draft Revised ITU-T Recommendation X*, 509 :9594–8, 1997.

[15] A. Jøsang, C. Keser, and T. Dimitrakos. Can we manage trust ? In *Trust management*, pages 93–107. Springer, 2005.

[16] G. Lize, W. Jingpei, and S. Bin. Trust management mechanism for internet of things. *China Communications*, 11(2) :148–156, Feb 2014.

[17] P. N. Mahalle, P. A. Thakre, N. R. Prasad, and R. Prasad. A fuzzy approach to trust based access control in internet of things. In *Wireless Communications, Vehicular Technology, Information Theory and Aerospace Electronic Systems (VITAE), 2013 3rd International Conference on*, pages 1–5, June 2013.

[18] R. Neisse, M. Wegdam, and M. van Sinderen. Trust management support for context-aware service platforms. In *User-Centric Networking*, pages 75–106. Springer, 2014.

[19] M. Nitti, R. Girau, and L. Atzori. Trustworthiness management in the social internet of things. *IEEE Transactions on Knowledge and Data Engineering*, 26(5) :1253–1266, May 2014.

[20] Y. Ben Saied, A. Olivereau, D. Zeghlache, and M. Laurent. Trust management system design for the internet of things : A context-aware and multi-service approach. *Computers & Security*, 39, Part B :351 – 365, 2013.

[21] T. Schlossnagle. *Scalable internet architectures*. Pearson Education, Londres, 2006.

[22] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelfflé. *Vision and challenges for realising the Internet of Things*, volume 20. EUR-OP, 2010.

[23] V. H. Vu. *Infrastructure de gestion de la confiance sur internet*. PhD thesis, Ecole Nationale Supérieure des Mines de Saint-Etienne, 2010.

[24] O. Wyman. Internet des objets, les business models remis en cause ? `http://www.oliverwyman.com/content/dam/oliver-wyman/global/en/2015/jun/IoT%20Part%201_screen.pdf''` (accèdè le 14/04/2016).

[25] H. Xiao, N. Sidhu, and B. Christianson. Guarantor and reputation based trust model for social internet of things. In *Wireless Communications and Mobile Computing Conference (IWCMC), 2015 International*, pages 600–605, Aug 2015.

[26] G. Zacharia and P. Maes. Trust management through reputation mechanisms. *Applied Artificial Intelligence*, 14(9) :881–907, 2000.

RÉSUMÉ

Avec l'accroissement exponentielle du nombre d'objets connectés à Internet, gérer la sécurité, et plus spécialement la confiance devient un challenge. Maintenir et sécurisé un réseau hétérogène à une aussi grande échelle que l'Internet des objets est une tache complexe. Dans ce contexte, après avoir étudié les solutions proposées dans la littérature pour pallier le problème de gestion de la confiance, nous proposons un modèle de gestion de confiance basé sur le crédit et l'honnêteté pour l'Internet des objets. Ce modèle intègre l'honnêteté comme paramètre lors du calcul de la confiance pour l'évaluer au mieux et utilise le crédit pour assigner un coût à chaque service et ainsi permettre d'éviter des attaques de type DoS.

Mots clés : Internet des objets, gestion de confiance, securité, honnêteté, crédit.

ABSTRACT

With the exponential growth of devices connected to Internet, manage security, and specially trust becomes a challenge. Maintain and secure a heterogeneous network on a large scale is a complex task. In this context, after studying proposed solutions in the literature to address trust management issue, we proposed a credit and honesty based trust management model for Internet of Things. This model includes honesty as a parameter to gain accuracy in trust computation and uses credit to assign a concrete cost to each service and thus allow to avoid DoS attacks.

Key words : Internet of things, trust management, security, honesty, credit.