République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin de cycle
En vue d'obtention du diplôme de master recherche en Informatique
Option : Réseaux et Systèmes Distribués

Thème

Proposition d'un modèle de confiance pour l'Internet des Objets.

Mémoire soutenu le 21/06/2015 par :

M^r^ ***AIT MOUHOUB*** **Younes**

M^r^ ***BOUCHEBBAH*** **Fatah**

Devant le jury composé de :

Président :	M^r^ ***FARAH*** **Zoubeyr**	**M.A.A, U.A.M Béjaia**
Examinateur :	M^r^ ***SKLAB*** **Youcef**	**M.A.A, U.A.M Béjaia**
Examinateur :	M^r^ ***MOHAMMEDI*** **Mohamed**	**Doctorant, U.A.M Béjaia**
Encadreur :	M^r^ ***OMAR*** **Mawloud**	**M.C.A, U.A.M Béjaia**
Co-Encadreur :	M^elle^ ***BENKERROU*** **Hayet**	**Doctorante, U.A.M Béjaia**

Promotion 2014/2015

Remerciements

« Nous remercions ALLAH qui a exaucé nos prières et qui nous a donnés non seulement le courage mais aussi la force et la patience de réaliser ce travail ».

Nous exprimons nos sincères gratitudes à nos encadreurs M^{r} OMAR Mawloud et M^{elle} BENKARROU Hayet pour nous avoir proposé ce sujet. Nous les remercions également pour la haute qualité de leur encadrement, leur suivi, leur disponibilité, leurs conseils et leurs critiques constructives.

Nous témoignons également énormément de gratitude envers tous les membres de jury et nous les remercions vivement d'avoir accepté d'évaluer notre travail ainsi que de l'enrichir avec leurs remarques.

Notre reconnaissance va particulièrement à l'ensemble des enseignants du département d'Informatique pour tout ce qui nous a été transmis tout au long de notre formation.

Nous remerciement les plus chaleureux à nos parent, pour leur soutien, les encouragements et leurs sacrifices.

Enfin, nous remercions tous nos amis, en particulier Fatiha, Ines, Kamel et Morad. Nous les remercions pour leur soutien tout au long de cette année et pour leurs encouragement et consiels notamment dans les moments difficiles.

Dédicaces

A nos chers parents, pour leur persévérance
et pour avoir suscité notre vocation
et permis d'achever nos études en tant que nous sommes actuellement,

A nos sœurs, et nos frères
pour leur soutien moral
et leur intérêt envers notre travail,

A tous nos amis et collègues,
A tous ceux qui nous ont aidés,
A tous ceux qui nous sont chers,
A tous ceux qui nous avons omis,

Nous dédions ce humble travail.

Fatah, Younes.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

TABLE DES FIGURES

LISTE DES ABRÉVIATIONS

3/4 G	3/4 Generation
6lowPAN	IPv6 over low-power Wireless Personal Area Neworks
AC	Autorité de Certification
API	Application Program Interface
CO2	Carbon dioxide
C-CRL	Compressed-Certificate Revocation List
CA	Certification Authority
CAm	Certification Authority mother
CAd	Certification Authority distribution
CAt	Certification Authority transmission
CAg	Certification Authority generation
CRL	Certificate Revocation List
ETSI	European Telecommunications Standards Institute
EU FP7	European Union Focused Project 7
EX	Expériences des nœuds
FTBAC	A Fuzzy Approach to Trust Based Access Control in Internet of Things
IdO	Internet des Objets
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IoT	Intrenet of Things
IPv6	Internet Protocol version 6

ITU-T	International Telecommunication Union-Telecommunication
KN	Connaissances des Nœuds
M2M	Machine to Machine
NFC	Near Field Communication
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
RN	Recommandations des Nœuds
RFID	Radio Frequency IDentification
RPL	Routing Protocol for Low-Power and Lossy Networks
RSA	ron Rivest, adi Shamir and leonard Adleman
STMS	Secured Trust Management System
TDDG	An Energy-aware Trust Derivation Scheme with Game Theoretic Approach in Wireless Sensor Networks for IoT Applications
TAEC	Trustworthy Agent Execution Chip
TAECM	Trustworthy Agent Execution Chip Manufacturer
TLS	Transport Layer Security
TMS	Trust Management System
TPD	Tamper Proof Device
WIMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WSN	Wirless Sensor Network
xDSL	Digital Subscriber Line

INTRODUCTION GÉNÉRALE

l'Internet des Objet (IdO) a été introduit pour la première fois par Kevin ASHTON [20]. Il désigne l'omniprésence autour de nous d'une variété d'objets qui, à travers des schémas d'adressage uniques, sont capables d'interagir les uns avec les autres et de coopérer avec leurs voisins pour atteindre des objectifs communs. Les objets intelligents, qui sont considérés comme la plateforme de base de l'IdO, sont les objets de la vie quotidienne (téléviseur, réfrigérateur, machine à laver, etc.). Ces objets sont équipés de composants électroniques tels que des supports de communication radio, des processeurs pour le traitement, des capteurs et/ou actionneurs etc. Cet ajout vise à les rendre capables d'être conscient du monde dans lequel ils se trouvent et de prendre son contrôle à un instant donné [6]. Grâce à ses potentialités et son aspect ubiquitaire, la montée en puissance de l'IdO peut s'observer dans plusieurs domaines des plus personnelles aux plus industrielles. Nous pouvons citer par exemple les smart cities, les smart homes, l'industrie, l'agriculture, la santé, etc. Ceci a conduit à des bénéfices énormes : meilleure gestion d'énergie, traçabilité des produits, amélioration du suivi de la santé, simplification des tâches quotidiennes, etc.

Néanmoins, l'IdO n'est qu'en ses débuts ; plusieurs progrès restent à faire en matière de standardisations, de routage et d'identification, d'optimisation de la consommation d'énergie et surtout de sécurité. En effet, l'omniprésence de l'Internet des Objets dans la vie quotidienne des individus impose l'établissement des solutions de sécurité robustes respectant l'hétérogénéité des objets et leurs capacités limitées. Cette forte intégrité engendre non seulement les menaces classiques d'attaque qui pèsent sur les données et les réseaux, mais aussi, l'apparition de nouvelles menaces qui touchent à l'intégrité des objets eux-mêmes, les infrastructures et processus ainsi que la privacy des personnes.

A ce fait, l'instauration de la sécurité dans l'IdO a fait l'objet de plusieurs recherches

durant les dernières années. Cependant, la satisfaction des contraintes de cette révolution technologique dans les approches de sécurité reste un défi à relever. Nous classifions les solutions proposées en deux grandes catégories : les solutions à base de certification [13], [12], [3], [16] et les solutions à base de réputation [4], [5], [21], [7], [11], [9]. Les travaux réalisés dans l'axe de la certification ont été porté essentiellement sur la réduction des charges excessives provoquées par le processus d'échange de clés, de chiffrement et de déchiffrement, et l'une des solutions invoquées est l'utilisation de la cryptographie à sens unique [13], [12]. La réputation, quant à elle, joue un rôle très important dans les approches collaboratives. Le but principal de ces approches consiste à établir une communauté d'entités éprouvée d'un réseau. Ces dernières s'aident mutuellement pour la réalisation des opérations couteuses. A ce fait, les solutions basées sur la coopération se considèrent comme les plus adaptées pour les environnements à forte hétérogénéité telle que l'IdO. Cependant, elles présentent un point faible qui limite leur performance. En effet, les approches collaboratives se basent sur la mesure de la confiance dans la désignation des entités aptes à intégrer les groupes opérationnels. La confiance est une notion qui s'influence par plusieurs facteurs mesurables et non mesurables, ce qui pose des incertitudes sur la valeur finale obtenue lors de sa dérivation.

A travers ce mémoire, nous proposons un modèle de confiance basé sur la réputation nommé STMS (pour Secured Trust Management System). Notre modèle de confiance s'appuie sur des observations négatives enregistrées sur des collaborateurs afin de sécuriser les opérations de coopérations qui se déroulent entre les objets de l'IdO. STMS est axé sur une confiance hybride et procède en quatre phases afin de garantir une meilleure exactitude lors de sa dérivation et par conséquent, il assure de meilleures performances. Dans le but d'évaluer les performances dans la sélection des collaborateurs de notre modèle, nous modéliserons notre solution par le modèle de sondage. Une simulation de ce modèle est realisée afin de comparer notre solution à un modèle concurent.

Ce mémoire est organisé en quatre chapitres. Le premier chapitre sera consacré à la présentation de l'IdO, ses vulnérabilités et les menaces relatives à son déploiement, ainsi que l'introduction de quelques notions fondamentales utilisées dans le domaine de la sécurité. Dans le deuxième chapitre, nous présenterons une étude critique de quelques solutions récemment proposées sur l'axe de la confiance dans l'IdO en termes de réputation et de certification. Nous commençerons d'abord par la description et la discussion des travaux antérieurs suivies par une classification des travaux étudiés. Ensuite, nous présenterons les critères d'analyse, une comparaison des travaux et enfin une synthèse globale. Dans le troisième chapitre nous donnerons une description détaillée de notre modèle de confiance. Le quatrième chapitre, sera consacré à la validation de notre solution.

CHAPITRE 1

PRÉSENTATION DE L'INTERNET DES OBJETS

1.1 Introduction

L'Internet des Objets (IdO) repose sur l'idée que tous les objets peuvent être connectés un jour à Internet et sont donc capables d'émettre de l'information et éventuellement de recevoir des commandes [25]. Sur le plan fonctionnel, l'IdO désigne une informatique qui se fond dans notre quotidien pour nous simplifier la vie. Toutefois, certaines Informations dont les objets disposent sont confidentielles, d'où la nécessité d'assurer un partage et une manipulation dignes de confiance de ces données afin d'assurer la sécurité des individus et des entreprises.

Dans ce chapitre, nous présentons d'abord l'IdO, son architecture, ses axes de recherche, ainsi que les vulnérabilités et les menaces relatives à son déploiement. Nous consacrons par la suite le reste du chapitre à la définition de quelques notions utilisées dans le domaine de la sécurité, notamment le concept de modèle de confiance, l'importance de la réputation et de la certification dans ces modèles.

1.2 L'Internet des Objets

1.2.1 Définition

L'internet des objets(IdO) est une infrastructure dynamique d'un réseau global. Ce réseau global a des capacités d'autoconfiguration 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 [19].

De ce fait, l'IdO ajoute une dimension *"objet"* aux deux déjà existantes (*temporelle* et

spatiale), désormais, un objet peut communiquer avec n'importe quel objet (ou personne), à n'importe quelle heure et à n'importe quelle place [14].

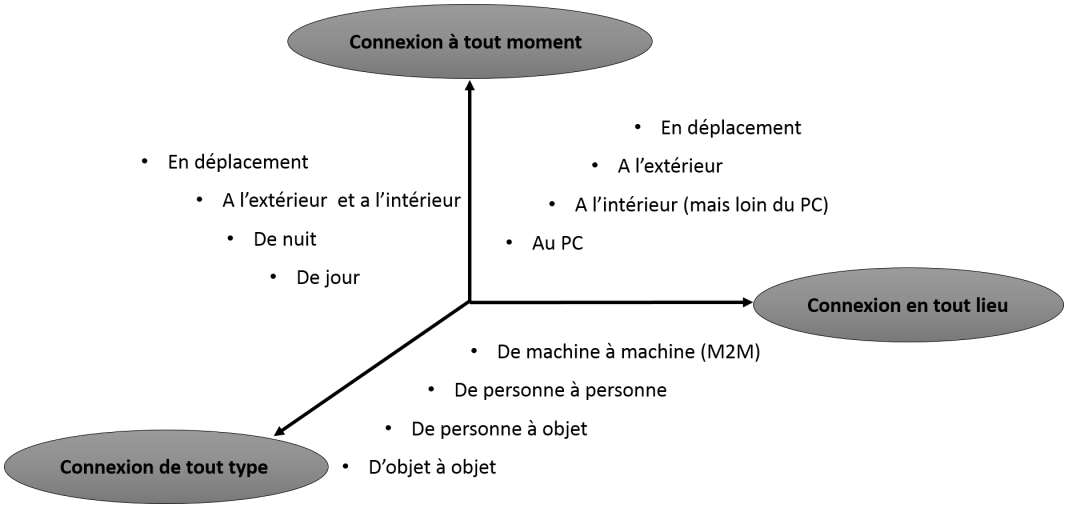

FIGURE 1.1 – Les dimensions de l'IdO [28].

1.2.2 Domaines d'application

Les potentialités offertes par l'IdO et son aspect ubiquitaire permettent de développer de nombreuses applications. Cependant, seules quelques applications sont actuellement déployées. L'utilisation de l'IdO permettra le développement de plusieurs applications intelligentes à l'avenir qui toucheront essentiellement : la domotique, les villes, le transport, la santé et l'industrie. Dans ce qui suit, nous citons brièvement des exemples d'applications de l'IdO.

1.2.2.1 La domotique en milieux urbains

L'un des domaines d'application de l'IdO les plus intéressants concerne la mise des équipements domestiques sur réseau. Cela permet d'abord d'avoir un contrôle global des différents équipements techniques d'une maison depuis une même interface (une tablette ou un téléphone intelligent par exemple), mais aussi, il offre la possibilité de contrôler à distance ces équipements via la mise à disposition d'API sur le web.

Le champ d'application de l'IdO s'étale pour toucher les villes (smart cities), l'IdO permettra une meilleure gestion de tous les réseaux qui alimentent ces villes intelligentes (eaux, électricité, gaz, etc.). Des capteurs peuvent être utilisés pour améliorer la gestion des parkings et du trafic urbain, diminuer les embouteillages et les émissions en CO2.

1.2.2.2 L'énergie

L'IdO propose des possibilités de gestion en temps réel de l'infrastructure de distribution de l'énergie, comme les réseaux électriques intelligents (smart grid). Cela contribuera d'une manière sûre à faciliter la maintenance et le contrôle de la consommation et la détection des fraudes.

1.2.2.3 Le transport

Grâce à l'IdO la communication intervéhicule et entre véhicules et infrastructures routière sera possible. De ce fait, ce domaine de l'IdO peut se considérer comme un prolongement des systèmes de transport intelligents qui a comme objectifs non seulement le renforcement de la sécurité routière et l'aide à la conduite, mais également, l'efficacité de la gestion du trafic, économie du temps, de l'énergie et le confort des conducteurs.

1.2.2.4 La santé

Ce domaine de l'IdO assurera le contrôle et le suivi des signes cliniques des patients par la mise en place des réseaux personnels de surveillance, ces réseaux seront constitués de bio-capteurs posés sur le corps des patients ou dans leurs lieux d'hospitalisation ou même dans leurs domiciles. Cela facilitera la télésurveillance des patients et apportera des solutions pour l'autonomie des personnes à mobilité réduite.

1.2.2.5 L'industrie

Le déploiement de l'IdO dans l'industrie sera certainement un grand support pour le développement de l'économie et le secteur des services, puisque l'IdO permettra d'assurer un suivi total des produits, de la chaîne de production, jusqu'à la chaîne logistique et de distribution en supervisant les conditions d'approvisionnement. Cette traçabilité de bout en bout facilitera la lutte contre la contrefaçon, la fraude et les crimes économiques transfrontaliers.

1.2.2.6 L'agriculture

L'IdO présentera des outils de choix pour la supervision de l'environnement des cultures, ce qui permettra une meilleure aide à la décision en agriculture. L'IdO servira non seulement à optimiser l'eau d'irrigation, l'usage des intrants et la planification des travaux agricoles, mais aussi, cette technologie peut être utilisée pour lutter contre la pollution (l'air, le sol et les eaux) et améliorer la qualité de l'environnement en général.

1.2.3 Importance et enjeux de l'Internet des Objets

L'importance des applications de l'IdO peut s'observer dans plusieurs domaines et activités sociales, des plus personnels aux plus industriels, il construit une continuité entre le monde réel et le monde de l'Internet, grâce à IdO, il deviendra possible aux usagers du réseau de s'informer et d'interagir en permanence avec l'ensemble des objets présents dans leur environnement immédiat. La mise en place de ces réseaux d'objets et de capteurs représente un enjeu économique très important, les flux d'informations issues des capteurs généreront une augmentation considérable des besoins en espace mémoire et en bande passante lorsque ces capteurs recueillent des informations en temps réel, ainsi l'importance de la miniaturisation et la réduction des couts associés aux nanotechnologies utilisées par l'IdO représentent un autre enjeu économique. L'IdO touche des dimensions éminemment stratégiques et des informations critiques. De ce fait, il appelle des formes renforcées de coordination et de gouvernance au niveau national ou régional, ce qui constitue un autre grand enjeu. Le dernier enjeu important de gouvernance de l'IdO concerne la protection des individus et des entreprises. Les applications de l'IdO soulèvent de manière récurrente la question de la privacy et de la protection des données pas uniquement de l'individu mais aussi les données sensibles des entreprises [22].

1.2.4 Architecture et standardisation

Les racines de l'IdO remontent aux technologies M2M (machine à machine) pour le contrôle des processus à distance. L'IdO qui est aujourd'hui un mélange de plusieurs technologies telles que la RFID, NFC, les capteurs et actionneurs sans fil, le M2M, l'ultrage bande ou 3/4G, IPv6, 6lowPAN, et RPL nécessite la définition d'une architecture et des standards afin de faciliter son développement dans le futur. L'ETSI propose une architecture découpée en trois domaines distincts, le domaine du réseau d'objets, le domaine du réseau cœur d'accès et le domaine des applications M2M et applications clientes [17].

1.2.4.1 Le domaine du réseau d'objets

Dans ce domaine nous trouvons les différentes technologies d'interconnexion des objets (M2M, RFID, Bluetooth, IETF6LowPAN, IETFRPL) et des passerelles vers les réseaux cœur de transport [17].

1.2.4.2 Le domaine du réseau coeur d'accès

Dans ce domaine nous trouvons les différentes technologies de réseaux de transport et d'accès comme xDSL, WIMAX, WLAN, 3/4G, etc [17].

1.2.4.3 Le domaine des applications M2M et applications clientes

Ce domaine est composé de platformes M2M, les Middlewares et API des applications M2M, processus métiers exploitant l'IdO, etc [17].

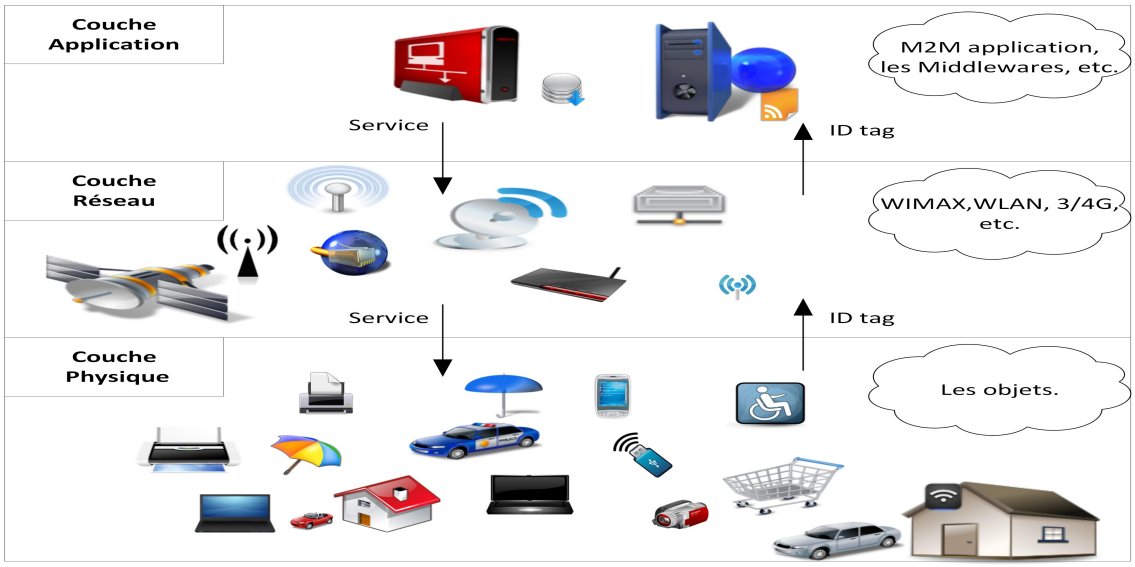

FIGURE 1.2 – Architecture de l'Internet des Objets.

1.2.5 Axes de recherche

1.2.5.1 La standardisation

L'IdO tel qu'il est aujourd'hui manque de standards et de certifications communes qui permettent d'assurer une compatibilité entre objets connectés tournant sous différents écosystèmes, une telle initiative jouera un rôle très important dans le développement de l'IdO dans le futur [17], puisqu'elle offre des solutions pour l'amélioration de l'interopérabilité et permet à des produits ou à des services de concurrencer à un niveau plus élevé ; malheureusement, les travaux de recherche des standards qui peuvent tenir face aux problèmes de l'interopérabilité, d'accès au support radio, d'interopérabilité sémantique, d'assurance de la sécurité et de la privacy sont confrontés au problème de la croissance rapide de l'IdO qui constitue un vrai souci dans les processus de standardisation.

1.2.5.2 La sécurité et la protection de la privacy

Le niveau d'acceptation des nouvelles technologies et services offerts par l'IdO au niveau de la société est fortement lié au degré de fiabilité des informations et de protection des données privées des utilisateurs. Bien que plusieurs projets aient été lancés dans le but de trouver des

solutions adéquates pour la protection de la privacy et d'assurer une protection rigoureuse aux utilisateurs finaux des technologies de l'IdO, ce domaine souffre toujours des insuffisances relatives à la confidentialité, la privacy et la gestion de la confiance [17].

1.2.5.3 La nouveauté dans les environnements de l'IdO

L'IdO est un réseau complexe géré par plusieurs parties prenantes, dans lequel certains services doivent être fournis publiquement, par conséquent, de nouveaux services (ou applications) verront le jour, ces derniers doivent être retenus dans le marché sans créer de charges excessives ou autres barrières de fonctionnement.

1.3 Vulnérabilités et menaces dans l'Internet des Objets

À cause de la forte intégration de l'IdO, les objets du quotidien deviennent des risques potentiels d'attaque sur la sécurité. L'ubiquité de l'IdO amplifiera les menaces classiques de la sécurité qui pèsent sur les données et les réseaux, de plus l'apparition de nouvelles menaces qui toucheront directement à l'intégrité des objets eux-mêmes, les infrastructures et processus et la privacy des personnes.

1.3.1 Menaces sur les données et les réseaux

Le manque de surveillance et de protection physique des objets communicants peut engendrer des attaques potentielles portées sur le matérielle telles que le vole, la corruption ou la contrefaçon de ces derniers pour récupération des données qui sont stockées sur ces dispositifs ou pour interrompre le bon fonctionnement des réseaux ou des systèmes complexes les hébergeants.

De plus, les transmissions sans fil sont réputées par leur forte vulnérabilité aux attaques de l'écoute passive et de déni de service. Les solutions cryptographiques existantes aujourd'hui ne sont pas adéquates pour tenir face à ces problèmes cités à cause de la limitation de ressources des objets communicants, de ce fait, l'adaptation de ces dernieres ou la conception de nouveaux modèles est une nécessité afin d'assurer les services de sécurité [17].

1.3.2 Menaces sur la privacy

De nombreux objets seront intégrés, portés ou même bien installés dans les lieux privés des personnes, ces objets présentent une potentielle menace pour la vie privée (privacy) de leurs utilisateurs. En effet, ces appareils électriques non seulement sont traçables, mais peuvent filmer,

écouter ou même enregistrer leur rythme cardiaque ou respiratoire ainsi que la température du corps ou sa cinématique dans le but d'un usage malicieux.

1.3.3 Menaces sur les systèmes et l'environnement physique des objets

Des objets malicieux connectés à un réseau ou intégrés dans un système complexe peuvent causer un dysfonctionnement quelconque, un déni de service ou autres types d'attaques à l'intégrité des données et les informations sensibles du système, ou pire encore prendre le contrôle du système en causant des dommages importants.

1.4 La sécurité dans Internet des Objets

1.4.1 Définition des objectifs de la sécurité

La sécurité Informatique d'une manière générale consiste à assurer que les ressources matérielles et logicielles d'une organisation sont uniquement utilisées dans le cadre prévu. Elle vise à assurer plusieurs objectifs, dont les cinq principaux sont : l'authentification, la confidentialité, l'intégrité, la disponibilité et la non-répudiation [26].

1.4.1.1 Authentification

L'authentification peut être définie comme le processus de prouver une identité revendiquée. La confidentialité, l'intégrité des données, et la non-répudiation dépendent tous de l'authentification appropriée. Un système sans cette fonctionnalité ne pouvait pas fournir les objectifs de sécurité mentionnés de manière satisfaisante.

1.4.1.2 Confidentialité

Ensemble des mécanismes permettant qu'une communication de données reste privée entre un émetteur et un destinataire. La cryptographie ou le chiffrement des données est la seule solution fiable pour assurer la confidentialité des données.

1.4.1.3 Intégrité

L'intégrité peut être vue comme un ensemble de mesures garantissant la protection des données contre les modifications et les altérations non autorisées. L'objectif des attaques sur l'intégrité est de changer, d'ajouter ou de supprimer des informations ou des ressources.

1.4.1.4 Disponibilité

La disponibilité est un service réseau qui donne une assurance aux entités autorisées d'accéder aux ressources réseaux avec une qualité de service adéquate. L'objectif des attaques sur la disponibilité est de rendre le système inexploitable ou inutilisable.

1.4.1.5 Non−répudiation

Mécanisme permettant de garantir qu'un message a bien été envoyé par un émetteur et reçu par un destinataire, c'est-à-dire aucun des correspondants ne pourra nier l'envoi ou la réception du message.

1.4.2 Définition de la confiance

La confiance fournit un mécanisme pour la mesure de la fiabilité et la disponibilité d'une entité donnée [2]. La confiance est un concept compliqué influencé par plusieurs facteurs mesurables et non mesurables [2], sa définition diffère d'un domaine scientifique à un autre [18].

Dans le domaine de la sécurité Informatique, plusieurs auteurs ont proposé leurs propres définitions de ce terme. Cependant, la plus apropriée est celle de l'ITU-T X509 qui l'a défini 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 »*** [31].

Donc à travers cette définition nous pouvons déduire que la confiance peut être vue comme une relation entre deux entités, elle exprime une croyance subjective de la première entité sur la capacité de la deuxième entité à réaliser un service qu'on lui affecte et cela en s'abstenant de tout comportement malicieux durant l'exécution de ce service.

1.4.3 Définition de la réputation

Le terme réputation exprime généralement l'opinion du publique au sujet de quelque chose ou de quelqu'un (personne, un groupe de personnes, une organisation, une ressource, etc.). Par analogie, la réputation d'un nœud dans un réseau représente l'opinion des nœuds de ce réseau vers la disponibilité et la fiabilité de ce dernier. D'une manière plus simplifiée, la réputation exprime le degré de la confiance attribuée à un nœud par l'ensemble ou une partie de l'ensemble des nœuds du réseau [9].

1.4.4 Définition de la certification

La certification permet de prouver la validité d'une liaison existante entre une clé publique et une entité, cette validation se fait grâce à un document électronique appelé *un certificat* qui

atteste que cette clé est bien liée à cette entité, cette dernière peut être une organisation, une personne physique, une machine ou une application. Les certificats sont délivrés par une tierce partie de confiance dite *une autorité de certification (AC)*, et possèdent généralement le format du standard X.509v3 dont les champs les plus essentiels sont : un numéro de série, une clé publique, l'identifiant du propriétaire de la clé publique, la date de validité (date de début et date de fin de validité), l'identifiant de l'autorité de certification qui a délivré le certificat, la signature du certificat à l'aide de la clé privée de l'autorité de certification [32].

1.4.5 Définition des capacités (capabilities)

Une capacité est un jeton (un document électronique) transmissible et infalsifiable, elle contient un identificateur d'un objet et une liste d'opérations permises sur ce dernier. Elle représente une permission à auto-authentification pour accéder à cet objet spécifié afin d'effectuer un ensemble d'opérations d'une façon bien décrite. De ce fait, les propriétaires de la capacité peuvent accéder à l'objet spécifié sans aucune authentification [10].

1.4.6 Définition d'un modèle de confiance

Un modèle de confiance peut se définir comme une tentative formelle de modéliser mathématiquement les aspects d'une relation de confiance. Ils sont employés généralement pour l'établissement et l'administration des relations de confiance entre les nœuds d'un réseau, dans le but d'assurer les objectifs de sécurité [23].

1.4.6.1 Modèles de confiance à base de réputation

La confiance est un concept intégral qui se considère comme l'élément le plus important dans un modèle de confiance, elle indique le degré d'acceptation d'un nœud dans un réseau. En d'autres termes, c'est selon cette valeur de la confiance que les autres nœuds du réseau décident de leur coopération avec le nœud.

La valeur de la confiance d'un nœud augmente au fur et à mesure de sa participation au bon fonctionnement du réseau, dans ce cas, les autres nœuds seront plus disposés à coopérer avec ce nœud. Dans le cas contraire, sa valeur de la confiance diminuera rapidement, par conséquent, aucun nœud n'acceptera de coopérer avec ce dernier, ce qui engendre son isolement du reste du réseau.

Pour décider si un nœud sera isolé ou accepté dans un réseau, le modèle de confiance calcule la valeur de confiance à base des valeurs de confiance directe (historique) ou indirecte (recommandations) d'un nœud, une valeur finale sera obtenue par la combinaison de ces deux dernières ; ensuite, cette valeur finale sera comparée à un seuil, si la valeur finale de la confiance

est plus grande que le seuil déclaré, cela signifie que le nœud sera accepté, sinon il sera isolé [15].

De ce fait, nous pouvons résumer les objectifs d'un modèle de confiance à base de réputation en trois éléments essentiels :

- Être capable d'enregistrer chaque comportement effectué par un nœud dans un réseau, cela permettra de distinguer entre les nœuds fiables et les nœuds malicieux au sein de ce réseau.
- Encourager la collaboration entre les nœuds appartenant à un même réseau.
- Sécuriser un réseau en isolant les nœuds suspectés en les empêchant de participer aux activités réalisées dans ce réseau.

1.4.6.2 Modèles de confiance à base de certification

Les modèles de confiance à base de certification sont employés, généralement, pour garantir les objectifs de la sécurité par la délivrance d'un certificat, ils sont classifiés selon deux types d'approches : des modèles utilisant une tierce partie de confiance et des modèles sans ou à faible dépendance d'une tierce partie de confiance [23].

La première catégorie (les modèles avec tierce partie de confiance) s'appuient sur une autorité de certification dans les systèmes à clé publique ou d'un gardien des clés dans les systèmes à chiffrement symétriques. Parmi ces modèles, nous pouvons citer les PKI (Public Key Infrastructure) et Kerberos [23].

Dans la deuxième catégorie, chaque utilisateur est le centre de son propre monde, la fonction de confiance est distribuée entre plusieurs entités dans le réseau, comme le cas du modèle PGP (Pretty Good Privacy) et les modèles basés sur la cryptographie à seuil [23].

1.5 Conclusion

Ce chapitre a été découpé en deux parties, la première partie a été consacrée à la présentation de l'IdO, ses domaines d'application ainsi que son importance, ses enjeux et ses axes de recherche. Aussi, nous avons décrit en détail dans cette partie les menaces relatives à son déploiement. Dans la deuxième partie, nous avons mis l'accent sur quelques concepts liés à la sécurité, nous avons défini les notions de confiance et de réputation. Le chapitre est clôturé par la définition d'un modèle de confiance en précisant l'importance de la certification et la réputation au sein de ce modèle.

Le chapitre suivant sera consacré à l'étude de quelques travaux récents réalisés dans le contexte des modèles de confiance dans l'IdO.

CHAPITRE 2

TAXONOMIE DES MODÈLES DE CONFIANCE DANS L'IDO

2.1 Introduction

L'Internet des Objets (IdO) prévoit de nouveaux défis de sécurité qui appellent à une révision substantielle des solutions de sécurité existantes ou le développement de nouvelles approches. Parmi les solutions de sécurité et des mécanismes qui doivent être révisés et innovés nous pouvons citer l'évaluation de la confiance vu son importance dans la gestion des relations de confiance et la prise de décision.

Ce chapitre sera consacré à la présentation et l'étude critique de quelques solutions récemment proposées sur l'axe de la confiance dans l'IdO en termes de réputation et de certification. Pour cela, nous commençons d'abords par déterminer nos critères d'analyse ; suivie par notre propre classification des solutions étudiées, par la suite, nous présentons une description et une discussion de ces derniéres et enfin, une comparaison des travaux analysés et une synthèse sont proposées pour la clôture du chapitre.

2.2 Les critères de comparaison des solutions

Afin de bien évaluer les articles et les travaux que nous avons lus et en se basant sur les objectifs, ainsi que les besoins et les contraintes de l'Internet des Objets, nous avons établie une liste de critères d'évaluation la plus pertinente !. Notre liste comprend les quatre éléments suivants :

2.2.1 La résistance aux attaques

Un modèle de confiance doit être résistant aux attaques, nous envisageant évaluer les travaux analysés sur la résistance aux attaques qui touchent aux points sensibles de l'Internet des Objets, qui sont : la vie privée des utilisateurs (privacy), les données et les services.

2.2.2 La consommation énergétique

La forte contrainte de ressources qui caractérise les objets de l'internet des objets, nous pousse vers la conception des modèles de confiance peu consommateurs en termes d'énergie.

2.2.3 La scalabilité

La scalabilité est l'une des caractéristiques essentielles d'un modèle de confiance dans l'Internet des Objets, elle permet d'assurer son bon fonctionnement lors des changements dynamiques de la taille du réseau d'objets [24].

2.2.4 Exactitude de la dérivation de la confiance

Ce critère d'analyse est spécifique aux solutions basées sur la réputation. La réputation d'un nœud peut être calculée à base de plusieurs informations, la décision d'accepter ou de refuser un objet dans un réseau dépend de sa réputation, à ce fait, l'exactitude de la dérivation de la confiance joue un rôle très important car elle tente de minimiser au maximum le taux des fausses acceptations et le taux des faux rejets.

2.3 Classification des travaux

Nous classifions les travaux que nous avons analysés en une structure hiérarchique à deux niveaux. Le premier niveau représente la catégorie de la solution proposée (à base de certification ou à base de réputation) et le deuxième niveau décompose les solutions à base de réputation que nous avons traitées selon le type de la confiance utilisé, ce niveau est associé à un tableau de deux lignes qui spécifie si la solution proposée se base sur l'usage d'un gestionnaire de confiance ou non. La figure 2.1 montre notre classification.

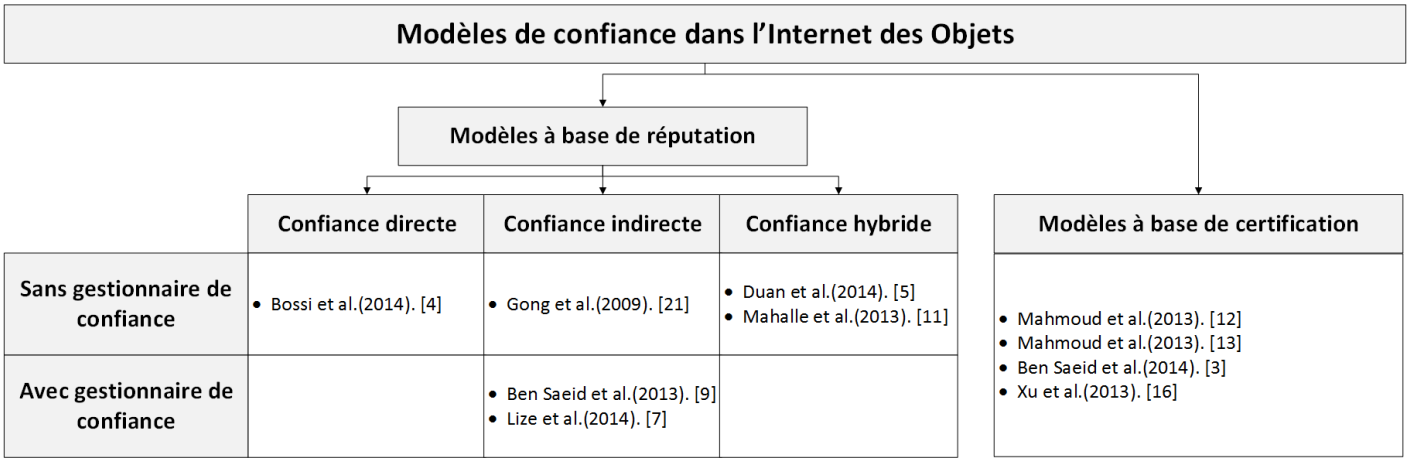

FIGURE 2.1 – Le schéma de classification des solutions des modèles de confiance dans l'IdO.

2.4 Les modèles de confiance dans l'Internet des Objets

La confiance est l'un des facteurs essentiels pour l'établissement de la sécurité au sein de l'IdO, plusieurs recherches ont été menées afin de réaliser un modèle de confiance qui répond aux exigences de l'IdO. Dans ce qui suit, nous présentons une partie des travaux les plus pertinents qui ont été réalisés dans ce contexte.

2.4.1 Les modèles à base de réputation

Notre étude des travaux sur les modèles à base de réputation montre que la confiance dans ce domaine peut être répartie en trois catégories : confiance directe, indirecte et hybride. La confiance directe est l'observation locale des comportements d'un objet, tandis que dans la confiance indirecte l'observation des comportements de l'objet se fait par ses voisins. Dans la confiance hybride, la dérivation de confiance est calculée en se basant sur les deux catégories précédentes.

2.4.1.1 Les solutions à base de la confiance directe

Multidimensional reputation network for service composition in the Internet of Things

Bossi et al. [4], ont proposé un modèle de choix de fournisseurs de services basé sur la réputation. Un utilisateur propose un plan de travail qui contient les types de service dont il a besoin, le modèle de Bossi et al s'appuie sur ce plan afin de construire une unité de travail composée d'un ensemble de fournisseurs qui offrent ces services, en tenant compte de la réputation la plus élevée et de la distance par rapport à l'utilisateur.

Le processus de calcul de la réputation d'un fournisseur P_f par rapport à un service **S** par un autre fournisseur P_i se fait comme suite : P_i construit un multi-graphe '**G**', un arc '**e**' de ce dernier possède un poids **r(e)** et une étiquette '**s**' qui désigne un service. Ensuite, il calcule le plus court chemin qui le relie à P_f avec l'algorithme de Djikstra et en tenant compte seulement des petites valeurs des nouveaux poids des arcs calculés par **1/ (l(s(e),s).(2+r(e)))**, finalement la réputation de P_f est la valeur minimale d'un arc figurant dans le plus court chemin calculée par **(l(s,s(e)).r(e))** tel que '**l**' est la fonction d'interchangeabilité de deux services.

La réputation d'une unité de travail est la moyenne des réputations (calculées dans le processus précédent) de l'ensemble des fournisseurs qui la compose. Enfin, les auteurs ont proposé un algorithme qui prend en entrée un plan de travail **WP** et produit en sortie une unité de travail **WU**, non seulement cette **WU** possède la réputation la plus élevée mais aussi les fournisseurs qui la composent sont à une distance proche de l'utilisateur qui propose le plan de travail. En effet, pour chaque type de service figurant dans le plan de travail, on établit une liste de fournisseurs de services '**SPs**' qui sont à une distance 'd' de l'utilisateur et qui présentent un service d'une valeur d'interchangeabilité avec le service demandé incluse dans [0.5, 1]. Ensuite, lorsqu'il existe au moins un service dans le plan de travail qui n'a aucun fournisseur, le résultat est un échec. Sinon l'algorithme détermine toutes les unités de travail possibles, puis, il calcule la réputation de chaque unité et retourne celle qui possède la valeur la plus élevée.

Discussion et critiques

Le modèle proposé se base sur des calculs simples, donc il ne consomme pas trop d'énergie. Néanmoins, il ne vérifie pas l'existence réelle des services proposés par les fournisseurs, par exemple un attaquant peut proposer un faux service dans le but est d'avoir des informations privées d'un utilisateur, donc ce modèle est vulnérable aux attaques. De plus, la scalabitité n'est pas assurée dans le cas où la taille du multigraphe est très grande et l'utilisateur est muni d'un objet à faible ressources puisque le calcul de la réputation dans ce cas exige un grand espace mémoire pour stocker le multigraphe. Enfin, le modèle proposé ne prend en considération que l'interchangeabilité entre le service offert et le service demandé afin de calculer la réputation, d'autres mesures importantes telles que la fiabilité, la qualité de service et la sensibilité au contexte sont ignorées dans ce travail ce qui influance négativement l'exactitude de la valeur de la confiance dérivée.

2.4.1.2 Les solutions à base de la confiance indirecte

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

Les nœuds à capacités limitées dans l'IdO nécessitent la collaboration avec d'autres nœuds moins contraints pour établir des communications sécurisées (ex : partage de secret, vérification de la signature, etc.). Sur cet axe, Ben Saeid et al. [9], ont proposé un TMS (Trust management system) basé sur la connaissance du contexte, ayant comme objectif, l'évitement des nœuds égoïstes (refus de participation dans le but de sauvgarder leur ressources) et malins qui peuvent lancer des attaques internes lors de la collaboration telles que la modification des données ou l'injection des bugs sans qu'ils soient identifiables. Le processus de selection de des nœuds collaboratifs contient cinq phases (voir la figure 2.2). :

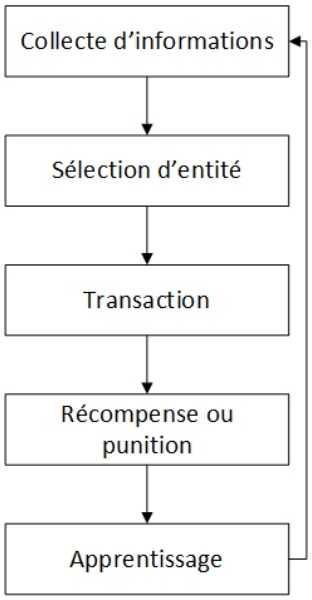

FIGURE 2.2 – Le modèle de TMS proposé [9].

La première phase consiste à collecter les informations de contexte (le services S_j auquel P_i a fournit de l'assistance, la capacité de P_i lors de la fourniture de S_j, le score N_j affecté par le nœud demandeur à P_i pour l'évaluer et le temps T_j d'exécution de S_j) intégrées dans le rapport R_{ij} envoyé par un noeud témoin 'j' pour évaluer un nœud assistant (proxy) P_i. La deuxième phase permet de selectionner les meilleurs proxy en 5 étapes : (1) restreindre le nombre de proxy selon les exigences du service, (2) restreindre le nombre de rapports R_{ij} liés à chaque proxy choisi dans l'étape (1) pour calculer la confiance. Cette restriction se fait en calculant la similarité du contexte entre un rapport donné et le rapport cible en termes de service et de capacité, à base d'une distance contextuelle 'd_{ij}' permettant de selectionner les rapports les plus proches du rapport cible, (3) calculer un poids $W_{R_{ij}}$ pour chaque rapport selectionné dans

l'étape précédente pour favoriser les rapports les plus récents et les plus proches du rapport cible, (4) calculer la confiance T_i du proxy P_i selon la somme des poids des rapports, les scores du proxy et la qualité de recommendation des nœuds témoins. À partir de cette valeur, l'étape (5) fournira les meilleurs proxy (collaborateurs) au nœud demandeur. La troisième et la quatrième phase permettent au nœud demandeur de récompenser (score positif) ou de punir (score négatif) un proxy selon la qualité de service offert. Enfin, la phase d'apprentissage met à jour en premier lieu la qualité de recommendations des nœuds témoins en comparant leurs notes par rapport à la note du demandeur à propos du collaborateur ; ensuite, calculer la réputation du nœud comme étant la somme des scores et la qualité des recommendations.

Discussion et critiques

Le TMS proposé permet de remédier aux attaques on-off, bad mouthing et comportement sélectif. Cependant, nous avons constaté une imprécision dans la similarité du contexte en terme des services. Aussi, dans la phase d'évaluation (punish and reward), seulement le comportement égoïste est détecté et aucune méthode n'est prise en considération pour vérifier les résultats renvoyés par les proxy. L'usage du gestionnaire de confiance permet de remédier à la contrainte d'énergie, cependant il limite la scalabitité du TMS.

Trust Management Mechanism for Internet of Things

Dans cet article, Lize et al. [7] ont proposé un mécanisme de gestion de la confiance basé sur la modélisation d'architecture de l'IdO. Cela consiste à décomposer l'IdO en trois couches : couche physique, couche réseau et couche application. Chaque couche est contrôlée par la gestion de confiance, la couche physique comporte une série de dispositifs physiques et des réseaux de capteurs sans fil, le rôle principal de cette couche et la collecte d'informations et la transmission à la couche réseau, cette dernière inclut réseaux d'accès et Internet, son rôle est l'interconnexion et le routage des informations. La couche application a pour but le traitement et le stockage des informations. Le modèle en couches et le flux d'information sont représentés dans la figure 2.3.

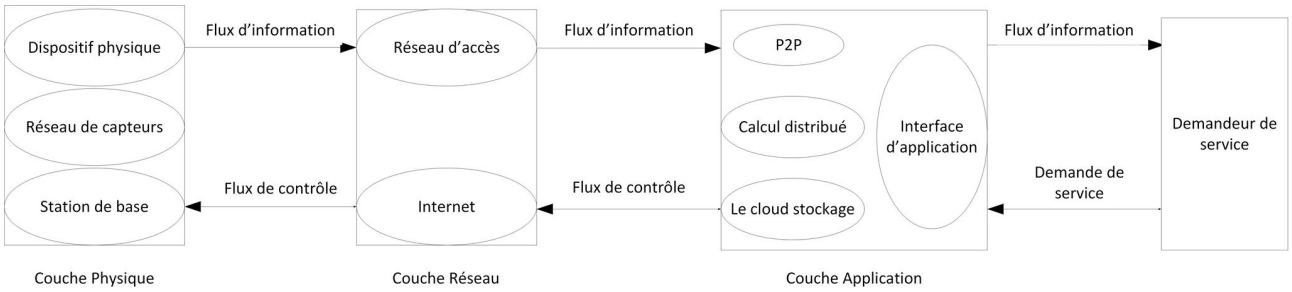

FIGURE 2.3 – Le modèle en couches et le flux d'information pour IdO [7].

La procédure de gestion de la confiance proposée par les auteurs comporte trois étapes, la première étape consiste à envoyer les informations de contrôle de la confiance aux couches d'IdO, la deuxième étape permet d'extraire ces informations et de calculer la valeur de confiance au niveau de chaque couche. La troisième étape est la prise de décision finale basée sur les valeurs de confiance calculées au niveau de chaque couche. Ces étapes permettent la sélection d'un ensemble d'objets dignes de confiance afin d'accomplir un service conformément à la politique du demandeur et au contexte spécifique. La figure ci-dessous illustre le mécanisme de gestion de confiance proposé par les auteurs.

Lorsqu'un service est demandé, l'identité du demandeur sera vérifiée ainsi que ces droits d'accès aux informations de confiance, ensuite le service lui sera offert selon une politique de contrôle basé sur la confiance distribuée, dans laquelle chaque couche participe au calcul de la valeur de confiance (voir la figure 2.4).

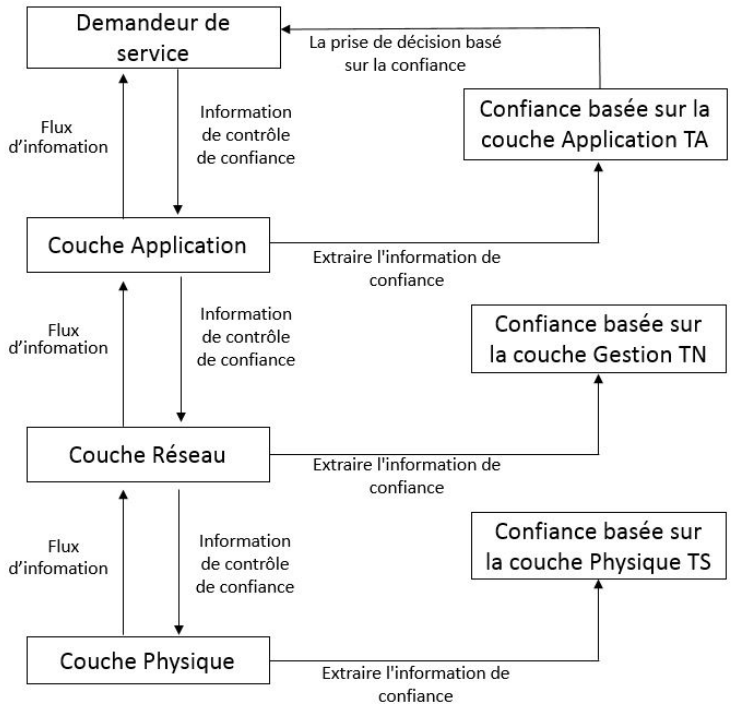

FIGURE 2.4 – Mécanismes de gestion de la confiance [7].

Discussion et critiques

Le modèle en couches proposé par les auteurs provoque une consommation d'énergie due à l'overhead. Le critère de scalability est respecté vu que le modèle proposé est distribué. Les auteurs n'ont pas défini une politique de sécurité contre les attaques, tandis que la couche physique fait usage à des réseaux de capteurs sans fil, l'attaque homme au milieu peut affecter la prise de décision, l'utilisation des ensembles flous dans le calcul de la confiance permet d'avoir des valeurs de confiance fiables mais ces valeurs sont inefficaces en matière de la prise de décision.

A Trust Model Combining Reputation and Credential

Le modèle de confiance proposé par Gong et al. [21] se compose de trois modules : module de réputation, module d'étude de compétence et module d'intégration. La structure générale est représentée dans la figure 2.5. I (u, v) désigne la pair u avec la recommandation v, et I(v) désigne toutes les pairs avec la recommandation dans le réseau.

Le module de réputation permet de calculer le score global de la réputation de I (u, v) en considérant les évaluations de toutes les autres pairs qui ont interagi avec I (u, v), les auteurs ont choisi l'approche Bayesienne [30] pour calculer la réputation d'une pair. Le module d'étude de compétence calcule la valeur de confiance des pairs ayant la recommandation v, en considérant

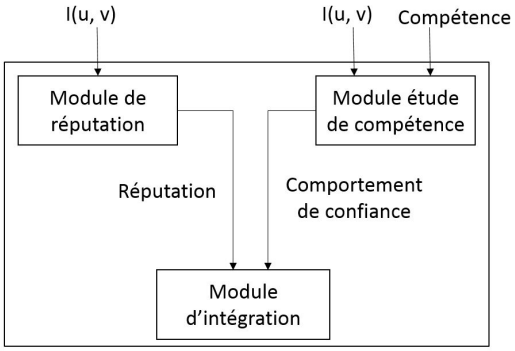

FIGURE 2.5 – La structure du modèle de confiance [21].

les évaluations de toutes les autres pairs qui ont interagi avec I (v), la valeur du comportement de confiance peut être représenté sous forme de vecteur (gi(v),bi(v)) tel que gi(v) et bi(v) représentent réspectivement les bons et les mauvais comportements. Le module d'intégration permet de combiner la réputation et la confiance pour obtenir la confiance globale de I(u, v).

Discussion et critiques

Les auteurs ont fait usage à l'approche Bayesienne [30], ce dernier permet de fournir une base théorique solide pour le calcul de la réputation, mais il est couteux en terme de consommation d'énergie, le modèle proposé est scalable vu qu'il est distribué. Pour la résistance aux attaques, aucun mécanisme n'a été défini.

2.4.1.3 Les solutions à base de la confiance hybride

An Energy-aware Trust Derivation Scheme with Game Theoretic Approach in Wireless Sensor Networks for IoT Applications (TDDG)

L'évaluation de la confiance est un outil important dans l'établissement des relations de confiance au sein de l'Internet des Objets [2]. Néanmoins, les processus de dérivation présentent un inconvénient majeur qui est la consommation élevée d'énergie. Dans cet article, Duan et al. [5], présentent un modèle de dérivation de la confiance (TDDG), basé sur la théorie des jeux, tout en essayant de réduire au maximum la consommation de l'énergie en contrôlant l'overhead provoqué par le processus de dérivation de la confiance indirecte. Le modèle proposé repose sur l'observation directe du nœud à évaluer (Watchdog) et le mécanisme de recommandations.

La valeur de la réputation du nœud évalué est périodiquement calculée à base des deux valeurs de confiance directe et indirecte ; cette valeur sera mise à jour au fur et à mesure du fonctionnement du réseau. En effet, chaque nœud enregistre les bonnes et les mauvaises actions de son voisin. Les mauvaises actions sont reconnues par la tentative de sauvegarde de l'énergie

en effectuant un comportement égoïste.

La valeur de la réputation calculée à la période (L) est déduite à partir des anciennes informations collectées à la période (L-1), pour se faire, le nœud évaluateur 'i' qui veut calculer la réputation d'un nœud 'j' suit le processus si dessous après avoir attribué un poids pour chaque action (bonne ou mauvaise).

La première étape du processus servira à calculer la réputation directe de 'j'. En se basant sur les poids des actions observées directement sur 'j' (les actions enregistrées) et l'ancienne valeur de la réputation de 'j', le nœud évaluateur 'i' calculera la nouvelle valeur de la réputation de ce dernier.

Dans la deuxième étape, le nœud 'i' procédera au calcul de la valeur de la réputation indirecte de 'j'. Après la réception des messages de recommandations (les observations faites par les voisins de 'j' sur 'j') par un nœud évaluateur 'i', le calcul de la nouvelle valeur de la réputation indirecte de 'j' se fait en utilisant les recommandations reçues, les actions de 'j' que 'i' a enregistré et les poids de ces dernières.

Pendant la troisième étape, le nœud 'i' calculera la réputation finale de 'j' en utilisant les deux valeurs de la réputation (directe et indirecte). En fin, Le nœud 'i' ne fera confiance à 'j' que si et seulement si la nouvelle réputation de 'j' à la période (L) est supérieur à un certain seuil. Ce seuil est déduit en utilisant une valeur fixe, le totale d'énergie sauvegardée en effectuant une action malicieuse et un facteur désignant le rapport entre l'énergie sauvegardée et la perte de réputation.

Pour collecter des recommandations sur un nœud tout en évitant l'inondation dans le réseau, les auteurs ont attribué aux nœuds voisins du nœud cible le droit de choisir entre répondre à une requête de recommandation ou non. En effet, la décision de répondre à la requête ou non est propre à chaque nœud selon l'état de sa batterie, le nombre minimum $\mathbf{K}$ de recommandations obligatoire afin de calculer la réputation indirect du nœud cible et le nombre total de nœuds voisins de ce dernier. Dans ce contexte les auteurs ont appuyé sur la théorie des jeux pour calculer la probabilité de sélection de stratégie (répondre ou non) ; l'équilibre de Nash en stratégie mixte a conclu que le tout se repose sur la valeur d'un certain rapport $\mathbf{G/f_e(s)}$, où $\mathbf{f_e(s)}$ est l'énergie consommée à l'envoie d'une recommandation et $\mathbf{G}$ est le gain tel que $\mathbf{G>Kf_e(s)>0}$. La simulation a montré que le rapport $\mathbf{G/f_e(s)}$ doit être petit pour une consommation d'énergie réduite mais suffisamment grand pour atteindre un taux de livraison des paquets élevé afin de maintenir l'exactitude de calcul de la confiance.

Discussion et critiques

La solution proposée par Duan et al assure la scalabitité puisqu'elle se repose sur une approche décentralisée. Les auteurs ont proposé l'utilisation de la théorie des jeux pour minimiser

le nombre de messages échangés dans le calcul de la confiance indirecte par conséquent réduire la consommation d'énergie. Néanmoins, si on réduit la valeur du rapport $\mathbf{G/f_e(s)}$ la solution ne sera pas résistante aux attaques et la dérivation de la confiance sera moins exacte puisque les auteurs ont affirmé que l'exactitude de la dérivation de la confiance et la résistance aux attaques exigent que le rapport $\mathbf{G/f_e(s)}$ soit élevé.

A Fuzzy Approach to Trust Based Access Control in Internet of Things (FTBAC)

Dans le contexte d'attribution des droits d'accès à base de la confiance, Mahalle et al. [11], ont proposé FTBAC utilisant la logique floue, basée sur trois variables linguistique : expériences (EX) des nœuds, des connaissances (KN) et des recommandations (RC) dans l'estimation de la confiance.

La confiance d'un objet 'A' en un objet 'B' liée à EX se calcule avec le rapport du nombre d'intéractions réussies par le nombre total d'intéractions. La connaissance directe et la connaissance indirecte sont utilisées pour le calcul de la valeur de confiance en terme de KN. La troisième évaluation basée sur RC est obtenue par la somme des valeurs RC des objets à propos de 'B'. La valeur floue de la confiance est souvent prise dans l'interval $[-1, 1]$ qui est divisé par chaque variable linguistique en trois parties affectées à trois valeurs linguistiques de sens : confiance faible, moyenne ou élevée.

Expériences	Connaissances	Recommandations	Les palges des 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 [11].

La fonction d'appartenance d'un ensemble flou A retourne un résultat qui est le degré d'appartenance dans l'interval $[0, 1]$.

Pour obtenir le score final de la confiance, 9 règles d'inférence sont utilisées par le modèle de Mamdani exploitant la combinaison de trois résultats de la confiance obtenus dans les évaluations par EX, KN et RC.

La valeur nette de la confiance obtenue est découpée en K intervalles qui est égale à la cardinalité de l'ensemble des permissions d'accès, par exemple si l'ensemble de droits d'accès comporte quatre types d'accès (ϕ , {lire}, {lire, écrire}, {lire, écrire, effacer}), une valeur de confiance nette T sera subdivisée en quatre intervalles T= { T1, T2, T3, T4 } avec la correspondance suivante : T1 est considéré faible donc pas de permissions qui lui y sont associées, T2 bénéficie de la lecture seulement, T3 de la lecture et l'ecriture et enfin T4 considéré comme le plus fiable donc supportera toutes les permissions possibles.

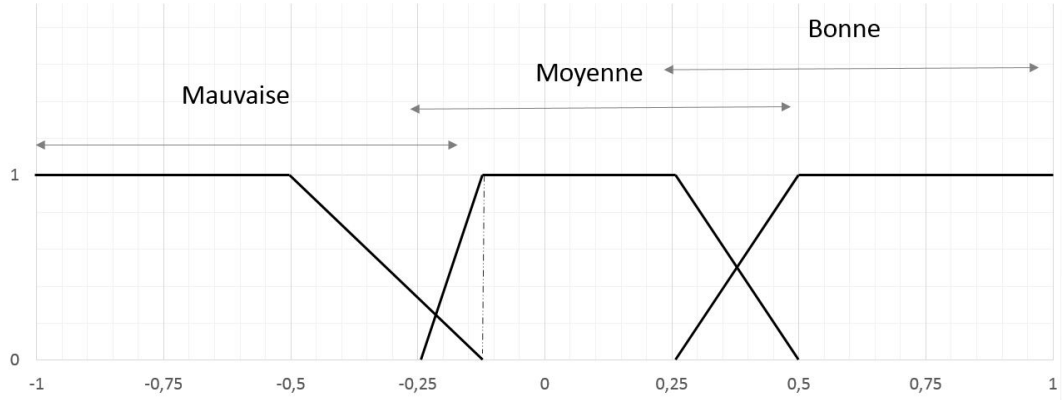

FIGURE 2.6 – Fonction d'appartenance des valeurs floues de la confiance [11].

Discussion et critiques

La scalabitité est assurée car FTBAC se base sur une approche décentralisée, la valeur de la confiance est déduite à partir de trois informations : l'expérience, la connaissance et les recommandations ce qui assure l'exactitude de la dérivation de la confiance. Cependant, le processus de collection des recommandations provoque un overhead important, ce qui induit à une consommation énergétique élevée. En plus, aucun mécanisme assurant la sécurité n'est utilisé dans ce modèle, à ce fait, FTBAC n'est pas résistant aux attaques.

2.4.2 Les modèles à base de certification

A Scalable Public Key Infrastructure for Smart Grid Communications

Les réseaux électriques intelligents (Smart Grid) sont une modernisation des réseaux existants, ils visent à détecter, prévenir et corriger les erreurs dans une auto-reprise en cas de perturbation. L'infrastructure à clé publique existante ne peut être utilisée d'une manière efficace pour la communication dans le smart grid, en raison de la complexité, l'immobilité des nœuds et la grande dispersion géographique des réseaux de communications.

Dans cet article, Mahmoud et al. [12] ont proposé une infrastructure à clé publique spécialement conçue pour le smart grid, avec un nouveau format de certificats et nouveau système de leur renouvellement. Dans le schéma proposé, l'infrastructure à clé publique est hiérarchique et entièrement connectée, chaque autorité de certification (CA) est responsable de la gestion des certificats pour une zone géographique limitée. La racine de l'hiérarchie est appelée 'CAm', le deuxième niveau de la hiérarchie contient les CAs des grandes divisions qui sont 'CAd' (gèrent les certificats du système de distribution électrique), 'CAt' (gèrent les certificats du système de transmission), et 'CAg' (gèrent les certificats du système de production), les autres nivaux réduisent la zone géométrique et le dernier niveau certifie les appareils. La figure 2.7 représente

le nouveau format proposé pour le certificat dans un smart grid.

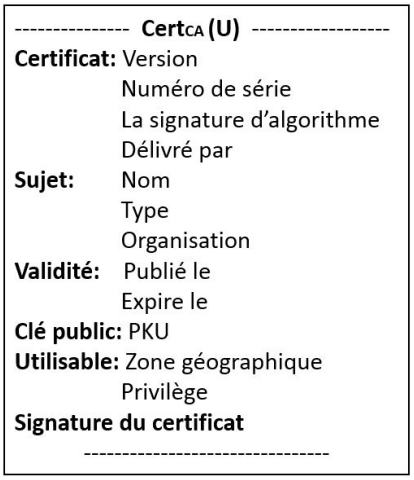

FIGURE 2.7 – Le nouveau format du certificat [12].

Les certificats révoqués figurent sur la liste des certificats révoqués CRL jusqu'à l'expiration de leurs durées. Dans le cas d'un certificat permanent, l'identifiant est toujours conservé dans la CRL, ce qui augmente progressivement la taille de cette dernière invoquant ainsi une consommation élevée d'énergie lors de sa distribution et de son stockage. Pour éviter la complexité des calculs de vérification de la signature dans chaque renouvellement de certificat, les auteurs ont proposé que l'autorité de certification crée une chaine de hachage pour chaque certification, en hachant itérativement un nombre aléatoire secret (Sn) n fois pour obtenir la valeur de hachage racine S0, qui sera ajouté à la partie données et à la partie signature dans le certificat. Lors du renouvellement du certificat, seulement les opérations de hachage assurent sa validité, la signature n'est alors vérifie que lors de la génération du certificat.

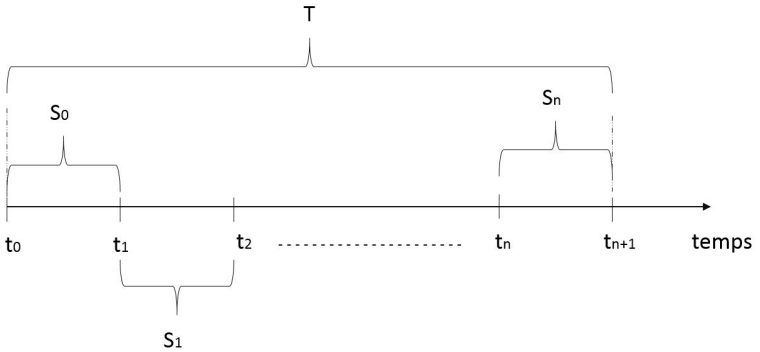

FIGURE 2.8 – Le schéma de renouvellement de certificats basé sur la chaine de hachage [12].

Discussion et critiques

L'utilisation de la chaine de hachage lors du renouvellement des certificats permet de réduire la consommation énergétique et de renforcer la résistance aux attaques. Cependant dans l'IdO, les objets changent souvent de privilège et dans ce cas leurs certificats sont révoqués à chaque fois, ce qui provoque l'augmentation de l'overhead. Le critère de scalabitité est respecté vu que le modèle proposé est hiérarchique.

Efficient Public-Key Certificate Revocation Schemes for Smart Grid

Dans un smart grid, il existe plusieurs situations qui nécessitent la révocation du certificat avant son expiration (ex : la clé compromise, perte du support de sécurité, changement d'affiliation ou d'un privilège, fin de l'objectif du certificat, comportement malveillant, changement de politique de sécurité et les appareils défectueux). Dans cet article, Mahmoud et al. [13] ont proposé un nouveau système de la révocation des certificats pour le smart grid. Des solutions novatrices et innovantes sont proposées pour gérer la révocation des certificats. Les auteurs ont présenté cinq régimes de révocation de certificats : (1)système fondé sur les certificats a courte durée, (2)tamper-proof-device (TPD), (3)serveur de statuts du certificat, (4) liste de certificats révoqués (CRL) ayant comme inconvénient la taille qui augmente au fil du temps, provoquant ainsi des problèmes de stockages et d'overhead lors de sa distribution. Pour y remédier, les auteurs ont proposé (5) C-CRL (compressed CRL) sur laquelle notre étude se focalise.

Pour une C-CRL, la CA génère un groupe d'identifiants pour les certificats par une chaine de hachage. Ces identifiants sont liés l'un à l'autre en hachant itérativement un nombre aléatoire secret 'R' en utilisant une clé secrête 'K' et une fonction de hachage 'h()'tel que, le premier identifiant= H^0 = h(K, R) et H^i = h(K, H^{i-1}) et $1 \leqslant i \leqslant S$ où 'S' représente la taille de la chaine.

En effet, pour révoquer une liste de certificats, la CA envoie le premier identifiant de la liste 'H^F', le nombre de certificats à révoquer et la clé 'K' pour créer la chaine. Les noeuds récepteur pourront alors calculer la liste complète des identifiants des certificats révoqués en faisant le hachage itératif de l'entrée 'H^F' 'n' fois avec 'K'.

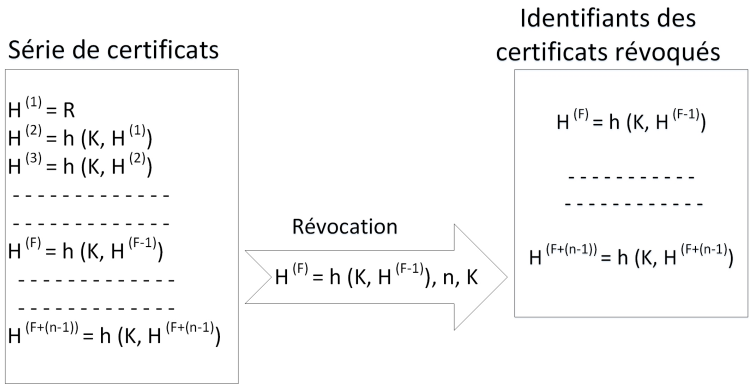

FIGURE 2.9 – Le schema de la C-CRL [13].

Discussion et critiques

Cette solution permet de réduire le trafic (overhead) réseau car seulement l'entrée de la CRL est envoyé au lieu de toute la liste. Mais, à chaque révocation ou renouvellement de certificats, le C-CRL réorganise (recalcule) les identifients de tous les certificats, ce qui provoque plus de consommation d'énergie si la taille de la liste est importante et des révocations sont fréquentes.

Lightweight collaborative key establishment scheme for the Internet of Things

Ben Saeid et al. [3] ont proposé un schéma collaboratif léger pour l'établissement de clés qui exploite l'hétérogénéité des objets afin d'effectuer des opérations cryptographiques lourdes et d'assurer la sécurité de bout en bout entre les paires. Pour se faire, les auteurs ont sélectionné les deux protocoles IKE (Internet Key Exchange) et TLS Handshake (Transport Layer Security) comme les protocoles les plus adaptés aux caractéristiques de l'IdO. L'idée de ce travail consiste à modifier les schémas des deux protocoles pour les rendre plus adaptés aux spécifications de l'IdO. Le processus d'échange de clé collaboratif prend en considération deux classes : le transport de clés collaboratif et la négociation(mise en accord) de clés collaboratives, la première classe définie deux modes : le transport de clés collaboratif à une seule phase et le transport de clés collaboratif à deux phases. Le premier mode utilise deux techniques pour distribuer les calculs nécessaires afin de délivrer la clé secrète : le partitionnement simple où le nœud à forte contraintes de ressources découpe le secret X en n parties x_1, x_2,...x_n et envoie chaque partie x_i à un proxy (moins contraint en ressources), ce dernier chiffre et signe sa partie x_i et envoie le résultat au serveur. Après avoir reçu tous les messages envoyés par les proxys, le serveur reconstituera le secret initial. Contrairement au cas simple, dans la technique de distribution de secret à seuil, par l'application d'un schéma de redondance d'erreurs aux fragments de la clé secrète, seulement un nombre k (avec $k < n$) de paquets est suffisant pour reconstruire le

message dans le serveur. Pour le transport de clé collaboratif à deux phases, le serveur et le nœud contraint en ressources génèrent tous les deux un secret aléatoire (X, Y respectivement), le client délivre le secret X au serveur en appliquant la méthode expliquée précédemment, le serveur reconstitue le secret X, génère la clé de session Y et envoie cette clé au client ; des proxys reçoivent la clé Y et vérifient l'intégrité et l'authentification du message à la place du nœud contraint en ressources.

La négociation de clés nécessite le calcul de deux exponentiations modulaires pour générer la clé publique de deffie-hellman et configurer son partage. L'approche collaborative dans ce travail présente deux techniques : la première technique est le partitionnement de l'entier exposant secret où chaque proxy effectue une partie des deux exponentiations modulaires, et la deuxième est la distribution de l'exposant secret à seuil qui nécessite la réception de k (avec $k < n$) parties en utilisant un partage polynomiale au lieu de partitionner les éléments avec l'interpolation de Lagrange.

Discussion et critiques

La solution proposée dans ce modèle exploite l'hétérogénéité des objets pour établir un schéma collaboratif, en d'autre termes, exploiter les capacités de calcul, de stockage et les ressources énergétiques de certains nœuds pour effectuer des services couteux en termes de ressources à la place des autres nœuds caractérisés par une forte contrainte de ressources, cette approche est décentralisée ce qui assure la scalabilité. Cependant, le schéma d'échange de clé de deffie-hellman n'authentifie pas les participants à un échange de clé, à cet effet, il ne résiste pas à certaines attaques tel que l'attaque homme au milieu. De plus, un objet contraint en ressource doit diviser à chaque fois le secret X en n parties x_1, x_2,...x_n et envoyer chaque x_i à un proxy, ce qui génère trop de messages et une consommation d'énergie très élevée.

An Autonomic Agent Trust Model for IoT Systems

Xu et al. [16] ont proposé un modèle de confiance utilisant des agents autonomes qui s'exécutent sur des environnements TEAC. Une TEAC (Trustworthy Agent Execution Chip) est une puce en silicone possédant une architecture bien spécifiée, conçue pour offrir une plateforme logicielle et matérielle sécurisées et à coût réduit pour l'exécution des agents, le rôle de cette puce est double : protéger les agents et les nœuds sur lesquels elle est installée. De son coté, un agent est un programme transmissible, composé de modules permettant d'encapsuler les codes des tâches et les données à transférer dans son propre programme, ainsi que des modules pour la protection des informations encapsulées et une interface pour gérer les communications avec son environnement d'exécution.

Les principaux composants du modèle de Xu et al. [16] sont : les nœuds collaborateurs, des

puces TAEC, un proxy et un constructeur de puce TAEC appelé TEACM (TAEC manufacturer).

Le TAECM fabrique des puces TAEC et les fournies aux utilisateurs munies d'un certificat qui assure la validité de la clé publique de la TAEC. Ensuite, ces puces seront installées sur des nœuds. Une fois cette procédure est terminée, chaque nœud enregistrera ses informations et le certificat de sa propre TAEC sur un proxy. Un nœud désirant collaborer avec un autre nœud récupérera les informations de ce dernier et le certificat de sa TAEC depuis le proxy, encapsulera les tâches à envoyer dans un agent, chiffrera cet agent avec la clé publique de la TAEC trouvée dans le certificat récupéré avant de l'envoyer à la destination (le nœud collaborateur). Dès que le nœud collaborateur reçoit l'agent chiffré, il le transférera à sa TEAC qui constituera son environnement d'exécution. La figure 2.10 montre le schéma général du modèle de Xu et al.

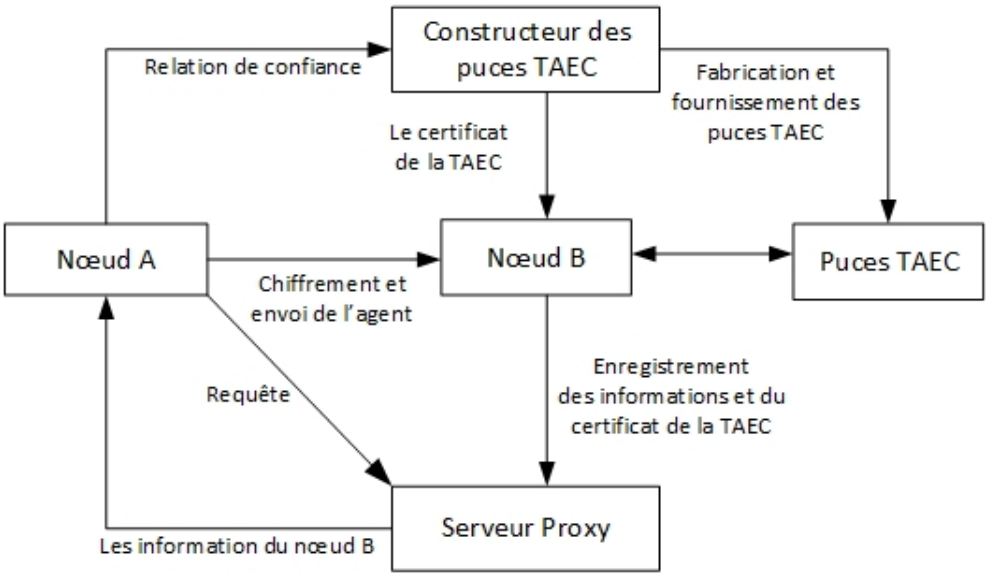

FIGURE 2.10 – Le schéma générale du modèle de Xu et al. [16].

Discussion et critiques

Le modèle proposé se base sur l'utilisation des puces insérées dans des objets, donc il assure la scalabilité. La confiance entre les objets est établie grace à un certificat délivré par une autorité à laquelle les utilisateurs font confiance (La TAECM). Les puces TAEC sont délivrée avec une paire de clés non renouvlable et non révocable, si cette dernière est divulguée à l'insue de l'utilisateur cela mettra en danger les informations sensibles contenues dans les agents, les resutlats d'executions des fragments de codes et les nœuds. De ce fait, le modèle de Xu et al. n'est pas résistant aux attaques.

Les processus du chiffrement et du dechiffrement des agents ajoutent des coûts supplimentaires relatifs à la consommation énergétique, puisque la cryptographie asymétrique est réputée d'être lourde en calcul et consomme trop d'énergie.

2.5 Analyse des surveys

Dans cette section nous présentons une étude des deux surveys existants dans le contexte des modèles de confiance dans l'IdO.

Security, privacy and trust in Internet of Things : The road ahead

Sicari et al, 2015. [1] ont réalisé un état de l'art sur les travaux faits au sujet de l'IdO en termes de sécurité, de privacy et de confiance. Grâce à une étude approfondie de la littérature les auteurs ont déduit une classification des travaux axés sur la confiance en quatre catégories : l'approche coopérative, la logique floue, les relations sociales et les méthodes à base d'identité.

L'approche coopérative est fondée sur le fait que tous les objets coopèrent afin de réaliser le service demandé. Les travaux utilisant les ensembles flous dans le calcul de la confiance ont été classés dans la catégorie logique floue. Une autre catégorie des travaux a été étudiée par les auteurs fondés sur l'établissement et la gestion des relations sociales entre les objets afin d'assurer la confiance dans le réseau. Les méthodes à base d'identité permettent d'assurer la confiance en se basant sur l'identité des objets.

Survey on trust management for Internet of Things

Yan et al, 2014. [8] ont réalisé une étude analytique et critique des solutions proposées en littérature relatives à la gestion de la confiance dans l'IdO, l'étude est basée sur dix taxonomies : les relations de confiance et les prises de décision, la confiance dans la perception de données, la préservation de la vie privée, la confiance dans l'extraction et la fusion des données, la confiance dans les transmissions et les communications, la qualité de service, la robustesse et la sécurité du système, la généralité, la confiance dans les interactions Homme-Machine, la confiance dans la géstion des identités.

Cette analyse a montré qu'aucune solution ne prend en considération une gestion complète de la confiance qui permet de gérer la confiance dans chaque couche et les inter-couches du modèle architectural défini pour l'internet des objets. Les auteurs ont soulevé un ensemble d'insuffisances trouvées dans les travaux étudiés : manque de sensibilité au contexte, les solutions de collections de données existantes sont lourdes et compliquées, les propositions pour la préservation de la privacy des utilisateurs sont spécifiques à des couches et la privacy dans les inter-couches n'a jamais été abordée. Aussi, aucun travail ne prend en considération la confiance

dans les interactions Homme-Machine malgré qu'elle est considérée comme un élément décisif dans l'évolution de l'IdO.

Des problèmes ouverts restent encore à résoudre dans la thématique de la gestion de la confiance dans l'IdO ; à partir de ces problèmes, les auteurs ont défini les axes qui feront l'objet des recherches dans le futur. En effet, l'IdO est un réseau fortement hétérogène composé d'objets de capacités différentes, donc l'économie d'énergie, la définition des algorithmes cryptographiques légers pour minimiser les charges de calcul et d'assurer une bonne gestion de clés sont des points décisifs pour une gestion révolutionnaire de la confiance. De plus, les auteurs ont invoqué la possibilité de coopérer les différentes solutions existantes dans chaque couche afin d'établir une gestion complète et autonome. Et enfin, la préservation de la privacy des utilisateurs de l'IdO et la confidentialité de leurs transactions commerciales dans toutes les étapes du traitement de l'information en commençant de la collection de données jusqu'au service final.

Les auteurs ont défini un cadre de travail complet pour la gestion de la confiance dans l'IdO basé sur l'architecture de référence proposée dans le projet EU FP7 IoT-A dans le but est de renforcer leurs état de l'art et d'inspirer les futures recherches, ce cadre de travail défini les besoins de la gestion de la confiance de chaque couche ainsi que les inter-couches et supporte des modules qui permettent d'assurer une gestion complète de la confiance ainsi que des modules pour assurer la production des services et des applications fiables et digne de confiance qui s'appuient sur les relations sociales.

Le cadre de travail établi par Yan et al. [8] se repose sur la coopération des solutions proposées pour chaque couche afin de produire une gestion de la confiance complète. À ce fait, il risque d'être lourd car il supporte trop de modules et parfois ces derniers sont dupliqués (routage pour les réseaux ad hoc et pour les WSNs). De plus, la synchronisation des solutions n'a pas été prise en considération dans ce cadre de travail, et l'hétérogénéité ainsi que la consommation d'énergie n'ont été recommandées que dans la couche réseaux alors qu'elles doivent être présentes dans toutes les couches de l'architecture. Aussi, ce cadre de travail de Yan et al a totalement négligé l'autonomie de la gestion de la confiance et sa scalabilité.

2.6 Comparaison des approches étudiées

Le tableau 2.2 illustre la comparaison entre les travaux présentés précédemment.

		Résistance aux attaques	Scalability	Consommation d'énérgie	Exactétude de la dérivation de la confiance
Certification	Mahmoud et al. [12], [13]	Oui	Oui	Non	Non étudié
	Ben Saeid et al. [3]	Non	Oui	Non	Non étudié
	Xu et al. [16]	Non	Oui	Non	Non étudié
Réputation	Duan et al. [5]	Non	Oui	Oui	Non
	Mehalle et al. [11]	Non	Oui	Non	Oui
	Bossi et al. [4]	Non	Non	Oui	Non
	Ben Saeid et al. [9]	Oui	Non	Oui	Non
	Lize et al. [7]	Non	Oui	Non	Oui
	Gong et al. [21]	Non	Oui	Non	Oui

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

Notre étude des travaux basés sur la réputation montre que les solutions proposées se divisent en deux catégories : sans gestionnaire de confiance et avec gestionnaire de confiance. Les solutions à gestion décentralisée (sans gestionnaire de confiance) sont généralement scalables, mais vulnérables aux attaques et gourmandes en énergie. Les solutions qui font l'usage d'un gestionnaire de confiance, les dérivations de la confiance se font au niveau de ce dernier distingué par sa robustesse et ses ressources élevées qui lui permettent de supporter des charges de calculs et de résister aux attaques. Cependant, il ne peut gérer qu'un nombre fini d'objets (non scalable).

2.7 Synthèse

Notre étude révèle deux axes de recherche essentiels : la certification et la réputation, chacun des axes se caractérise par un ensemble de points forts et de points faibles.

2.7.1 La certification

La certification assure une bonne résistance aux attaques. Cependant, elle se base sur la cryptographie asymétrique, ce qui explique sa lourdeur et son énorme consommation d'énergie. De ce fait, l'amélioration des anciennes solutions cryptographiques pour les faire adaptées aux caractéristiques de l'IdO ou la mise en œuvre de nouveaux mécanismes de sécurité plus légers demeure une nécessité (Mahmoud et al. [12], [13] ont proposé la chaine de hachage pour éviter

la vérification de la signature avec RSA et la distribution de toute la CRL, Ben Saeid et al. [3] a exploité l'hétérogénéité des objets pour établir un schéma collaboratif léger, cela consiste à sélectionner un ensemble d'objets non contraints en ressources afin d'assister les objets contraints en ressources dans les opérations cryptographiques lourdes).

2.7.2 La réputation

La réputation des nœuds joue un grand rôle dans les approches collaboratives qui sont indispensables pour l'internet des objets. Néanmoins, elle souffre des problèmes liées à l'imprécision de la dérivation de la confiance et une forte vulnérabilité aux attaques. Aussi, nous avons constaté que les méthodes de calcul de la réputation provoquent un overhead important lors de l'échange des recommendations et des connaissances. Plusieurs auteurs ont proposé des mécanismes de limitation du nombre de messages échangés, tel que la théorie des jeux par Duan et al. [5].

2.8 Conclusion

Les modèles à base de réputation s'appuient sur la notion de la confiance, un terme difficile à définir et sa valeur exacte est influencée par plusieurs éléments mesurables et non mesurables, ce qui complique la conception des méthodes qui fournissent des résultats exactes et précis lors du calcul de la réputation d'une entité. Donc, le défi majeur est de trouver des méthodes de calcul formelles qui assurent non seulement l'exactitude et la précision des résultats, mais aussi la satisfaction des exigences imposées par les caractéristiques de l'internet des objets (résistance aux attaques, consommation énergétique, scalabitité, etc.). Plusieurs travaux ont été publiés en littérature mais la solution révolutionnaire recherchée n'a pas encore vu le jour.

Pour cela, nous avons réalisé une classification et une synthèse des solutions analysées, qui nous seront utiles par la suite pour l'amélioration d'une solution spécifique ou la conception de notre modèle de confiance.

Le chapitre suivant sera consacré à la description détaillée de notre contribution.

CHAPITRE 3

SECURED TRUST MANAGEMENT SYSTEM

3.1 Introduction

Dans le chapitre précédent, nous avons analysé quelques travaux publiés sur l'axe des modèles de confiance dans l'IdO ; cette étude nous a conduits vers deux axes complémentaires, la certification et la réputation, chacun permet de remédier aux insuffisances de l'autre.

Dans ce chapitre nous proposons un modèle de confiance nommé STMS (pour *Secured Trust Mangement System*). Notre modèle est destiné à assurer la sécurité dans des opérations de collaboration qui se passent entre les objets de l'IdO et cela en se basant sur la réputation. L'idée générale de notre modèle de confiance consiste à hybrider la confiance directe et indirecte afin de satisfaire les exigences des approches collaboratives en terme de sécurité.

3.2 Motivations

L'IdO est un mélange de plusieurs technologies qui forment un réseau hétérogène, les objets d'un tel environnement sont souvent confrontés à effectuer de différents services. Cependant, la réalisation de certains de ces services nécessite beaucoup de ressources dont l'objet ne dispose pas, c'est dans ce contexte que les approches collaboratives sont souvent sollicitées. Le principe de telles approches consiste à trier l'ensemble des objets qui composent un environnement afin de former des communautés d'objets s'aidant mutuellement pour la réalisation des services coûteux. Par conséquent, l'exactitude de la sélection des objets collaborateurs demeure un point très important.

Parmi les moyens utilisés pour assurer cette exactitude, la mesure de la confiance comme dans [9]. Néanmoins, la confiance dans ce modèle n'est reliée qu'à la capacité d'un objet à accomplir une tâche qui lui a été affectée, une démarche insuffisante, car l'aspect sécurité est

totalement négligé ce qui implique que le modèle proposé est vulnérable aux attaques. Le but de notre travail consiste à proposer un modèle de confiance pour remédier à ce problème. Notre modèle est nommé STMS (Secured trust management system). STMS supervise le comportement des objets collaborateurs lors de la réalisation des tâches, ce qui lui permettra de **détecter et d'exclure** du réseau **les objets malicieux**, par conséquent, les résultats des sélections seront **des objets compétents et honnêtes**.

3.3 Préliminaires

- **La confiance :** dans le cadre de notre travail, nous définissons la confiance comme étant la capacité d'un objet à réaliser un service correct **sans comportements malicieux**.
- **Un gestionnaire de confiance :** un gestionnaire de confiance est une entité de confiance caractérisée par des capacités très élevées de stockage et de calcul.
- **Un demandeur de service :** un demandeur de service est un objet qui a envoyé une demande de service auprès du gestionnaire de confiance.
- **Demande de service :** une demande de service est une requête envoyée par un objet au gestionnaire de confiance afin de demander une assistance sur un service.
- **Un objet collaborateur :** un objet collaborateur est un objet sélectionné par le gestionnaire de confiance pour participer dans la réalisation d'un service.
- **Un objet témoin :** lorsqu'un demandeur d'un service évalue les collaborateurs, il devient témoin pour les prochaines collaborations.
- **La qualité de recommandation :** est le score de fiabilité d'un objet témoin sur l'exactitude de ses anciennes évaluations.

3.4 Modèle physique

L'objectif principal du STMS est de gérer la coopération dans une architecture hétérogène impliquant des objets ayant des capacités différentes afin d'établir une communauté d'objets performants est dignes de confiance qui s'aident en ce qui concerne la réalisation d'un ensemble d'opérations liées à un service. La figure 3.1 illustre le modèle physique du STMS.

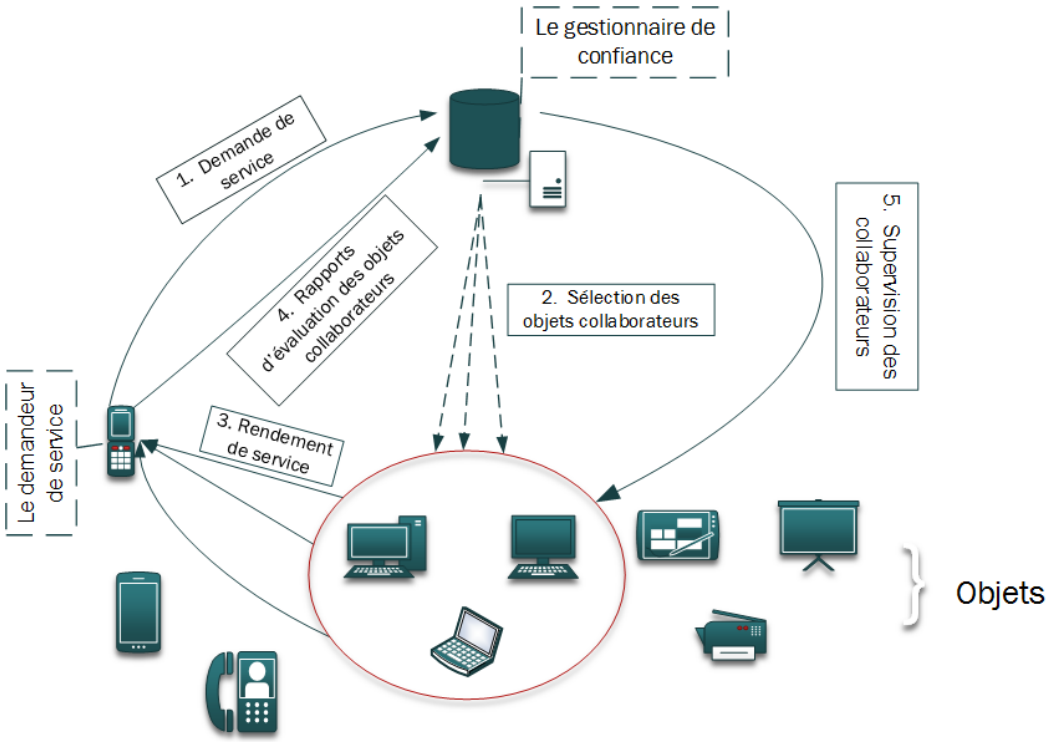

FIGURE 3.1 – Le modèle physique du STMS.

Lorsqu'un objet du réseau a besoin d'un service, il envoie une requête au gestionnaire de confiance, ce dernier vérifie cette requête et sélectionne un ensemble d'objets non contraints en ressources (mémoire et calcul) afin d'assister l'objet demandeur dans son service. Chaque collaborateur exécute les tâches qui lui ont été attribuées et envoie le résultat de cette exécution à l'objet demandeur. Une fois ce résultat a été bien reçu par le demandeur il l'évalue et il envoie un rapport d'évaluation au gestionnaire de confiance, ce rapport est positif lorsque le demandeur est satisfait du rendement de ce collaborateur et négatif dans le cas contraire. Les rapports d'évaluation sont sous forme d'un compte rendu et contiennent toutes les informations suivantes : la complexité du service effectué, le taux de ressources du collaborateur avant le début de l'exécution de ce service, la date de terminaison de l'exécution des tâches et la note attribuée au collaborateur.

Durant l'exécution du service demandé, le gestionnaire de confiance surveille à son tour chaque collaborateur et enregistre ses comportements. A la fin de la collaboration, il note ces collaborateurs selon les observations directes enregistrées, si un collaborateur a exécuté une tâche suspectée ou il s'est comporté d'une manière égoïste, il lui attribue une note négative sinon il le récompense par une note positive.

L'ensemble des rapports seront stockés dans le gestionnaire de confiance et seront utilisés pour ajuster la qualité de recommandation des témoins.

3.5 Hypothèses

Notre modèle de confiance repose sur une architecture centralisée, qui s'appuie sur l'utilisation d'une entité de confiance caractérisée par des capacités énormes de calcul et de stockage appelé le gestionnaire de confiance.

Dans le cadre de notre travail, nous admettons que l'IdO est un réseau dense composé d'objets hétérogènes déployés aléatoirement, les canaux de communication sont fiables et les tâches dans ces objets s'exécutent en séquentiel. Un service est décomposé en un nombre fini de tâches, chaque tâche est associée à un et un seul collaborateur. Le gestionnaire de confiance est supposé être capable d'estimer le pourcentage de ressources et de temps que devrait consommer une tâche, ainsi que le pourcentage réel des ressources et de temps consommé par un objet collaborateur pour exécuter cette tâche.

3.6 Attaques au modèle

Afin de mieux sécuriser notre modèle, nous avons fait l'inventaire des attaques qui pourront nuire à son bon fonctionnement, nous les résumons en ce qui suit :

3.6.1 Attaques menées par l'objet demandeur

Notre modèle se sert des rapports envoyés par les objets demandeurs des services afin de calculer la confiance indirecte des objets collaborateurs, toutefois, ces rapports peuvent être falsifiés dans le but d'un usage malicieux, par exemple pour faire diminuer la confiance indirecte d'un objet compétent ou pour la faire augmenter pour des objets égoïstes.

3.6.2 Attaques menées par l'objet collaborateur

Notre modèle se repose sur une approche collaborative pour aider les objets faibles en ressources à effectuer des tâches couteuses. A cet effet, le choix des objets collaborateurs est extrêmement sensible, car une fois un objet faible en ressources a transmis ses tâches, il perd le contrôle sur ces dernières et l'objet collaborateur devient le seul maître des informations qu'il détient, ce qui lui permettra de mener des attaques actives et/ou passives sur les informations qu'il contient et les résultats de leurs exécutions. Le demandeur de service n'a aucun moyen de vérifier les résultats envoyés par ses collaborateurs. A ce fait, sélectionner des collaborateurs qui constitueront des environnements d'exécution fiables pour les services collaboratifs est primordial pour assurer la sécurité dans notre modèle.

3.7 Secured Trust Management System (STMS)

Notre modèle de confiance introduit l'utilisation de la confiance directe et procède en quatre phases : initialisation et collecte d'informations, sélection des objets, transaction et évaluation et enfin la phase apprentissage.

3.7.1 Description de notre modèle STMS

La figure 3.2 illustre les différentes phases de notre modèle de confiance.

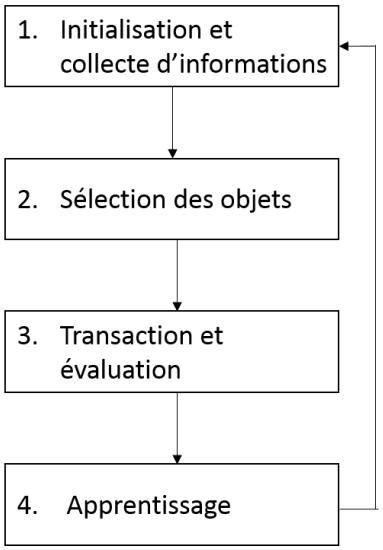

FIGURE 3.2 – Les phases de STMS.

3.7.2 Initialisation et collecte d'informations

La première phase du modèle est la phase initialisation et collecte d'informations. C'est la période d'amorçage, durant cette phase le gestionnaire de confiance prend connaissance du réseau. En créant des fausses transactions, le gestionnaire de confiance évalue chaque objet du réseau et détecte ceux qui sont défaillants. Un objet est considéré comme défaillants s'il ne retourne pas le resultat de la fausse transaction qui lui a été confiée par le gestionnaire de confiance.

3.7.3 Sélection des objets

Lors de la réception d'une requête d'aide envoyée par un objet contraint en ressources, le gestionnaire de confiance débute la deuxième phase qui consiste à sélectionner un ensemble d'objets selon les exigences du service demandé. Ces exigences concernent le niveau de ressources

contenu dans les objets qui doit être suffisant pour réaliser le service en question, ainsi que tous les objets assistants doivent appartenir au même groupe multicast, cela facilite énormément la mise en contact de l'objet demandeur avec ses collaborateurs.

Notre modèle de confiance procède comme TMS et sélectionne les collaborateurs selon leur valeur de confiance ; les collaborateurs ayant les valeurs de confiance les plus élevées possèdent plus de chance d'être sélectionné afin de collaborer dans la réalisation d'un service. TMS s'appuie sur les scores obtenus par ces collaborateurs, les poids des rapports envoyés par les demandeurs des services et la qualité de recommandation des objets témoins pour dériver cette confiance. Le calcul de la confiance d'un objet i dans TMS se fait par la formule (3.1) :

$$CI = \frac{1}{\sum_{j=1}^{n} WR_{ij}} * \sum_{j=1}^{n} (WR_{ij} * QR_j * N_j) \qquad (3.1)$$

Critiques

La formule (3.1) ne prend en considération que la performance des objets collaborateurs pour le calcul de la valeur de confiance. Cependant, la performance d'un objet ne reflète pas sa dignité de confiance, un objet est capable de réaliser des services tout en effectuant des attaques. Le demandeur de service n'évalue les objets collaborateur que pour le service réalisé, d'où les objets collaborateurs malicieux ne seront pas punis.

Amélioration Dans STMS

Nous avons pris en considération la problématique du TMS signalée ci-haut, pour y remédier, nous appuyant sur l'adoption d'un nouveau type de confiance qui est *la confiance directe*.

Afin d'expliquer cette partie de notre contribution, nous dressons le tableau 3.1, ce tableau contient la signification de tous les paramètres utilisés dans nos formules de la dérivation de la confiance directe et de la réputation.

Paramètre	Signification
R_{ij}	Un rapport d'évaluation d'un collaborateur j, ce rapport à été envoyé par un témoin i.
WR_{ij}	Le poids du rapport R_{ij}.
QR_j	La qualité de recommendation de l'objet témoin j.
N_j	Le score contenu dans un rapport d'évaluation, ce score est donné par le témoin j.
$\gamma > 0$,$\gamma = e^{t_c - 1 - t_c}$	Formule utilisée pour favoriser les dérivations recentes de la confiance.
t_c	Le temps actuel.
t_{c-1}	Le temps du dernier calcul de confiance directe.
$CD^{t_{c-1}}$	La valeur de la confiance directe d'un objet donné à l'instant t_{c-1}.
$f(O(o))$	Une fonction qui calcul la moyenne des observations enregistrées sur un objet.
$O_i(o)$	Une obsérvation enregistrée sur un objet. Cette observation est égale à -1 si les ressources consommées par le collaborateur ne sont pas conformes aux exigences du service demandé. Sinon, cette observation est la même note contenue dans le rapport rendu par le demandeur du service pour évaluer ce collaborateur.
α	Un facteur désignant l'importance de la confiance directe.
β	Un facteur désignant l'importance de la confiance indirecte.
N^{Fj}	Le score d'un collaborateur, ce score lui a été attribué par le témoin F_j.
QR_{Fj}	La qualité de recommandation du témoin F_j.
$O^T(i)$	L'observation enregistrée par le gestionnaire de confiance sur un objet i.
C_j	Le poids de la note $note_j$, dans le cadre de STMS nous adoptons la même formule utilisée dans [9] pour le calcul de ce poids.

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

Notre modèle STMS supervise les comportements de chaque collaborateur. A la fin de chaque service, le gestionnaire de confiance vérifie l'état des ressources de chaque collaborateur désigné pour ce service ainsi que le temps d'exécution consommé pour la réalisation de ce service. Dans le cas où la consommation des ressources et le temps d'exécution auraient été conformes aux exigences du service, le gestionnaire de confiance lui attribuera la note contenue dans le rapport d'évaluation envoyé par le demandeur du service (1 ou -1), Sinon il le punit directement par un score négatif (-1). Ces supervisions directes sont utilisées plus tard pour le calcul de la confiance directe selon la formule (3.2) :

$$CD^{t_c} = \gamma * CD^{t_{c-1}} + f(O(o)) \qquad (3.2)$$

Avec :

$$f(O(o)) = \frac{\sum_{i=1}^{n_j} (O_i(o))}{n_j} \qquad (3.3)$$

La formule (3.2) permet de détecter et de punir les collaborateurs malicieux, cela constitue une procédure préventive afin d'assurer la sécurité des opérations de collaboration qui se déroulent entre les objets. En effet, cette formule fait diminuer la valeur de la confiance directe des collaborateurs malicieux, tout en assurant que les bons collaborateurs auront des valeurs éle-

vées, cela isole ces mauvais collaborateurs et les empêche de participer dans des collaborations et par conséquent il fait diminuer leur chance de mener des attaques.

Désormais, nous avons tous les éléments nécessaires pour exprimer notre formule complète du calcul de la confiance hybride :

$$T_i = \underbrace{\alpha\,(e^{t_{c-1}-t_c} * CD^{t_{c-1}} + \frac{\sum_{i=1}^{n_j}(O_i(o))}{n_j})}_{CD} + \underbrace{\beta\,(\frac{1}{\sum_{j=1}^{n} WR_{ij}} * \sum_{j=1}^{n}(WR_{ij} * QR_j * N_j))}_{CI} \tag{3.4}$$

Avec :

$$\alpha + \beta = 1 \text{ où } \begin{cases} \alpha > \beta & \text{l'importance est donnée à la confiance directe.} \\ \alpha < \beta & \text{l'importance est donnée à la dérivation indirecte.} \end{cases}$$

Les deux facteurs α et β servent à ajuster la dérivation de la confiance selon l'importance et les caractéristiques d'un service demandé, par exemple, lorsqu'un service exige un niveau élevé de confidentialité, le paramètre α doit être supérieur à β, dans le cas où un objet demandeur d'un service ne s'intéresserait qu'à la performance des collaborateurs, le paramètre β doit être élevé. Cet équilibrage offre plus de souplesse au STMS en lui permettant de s'adapter aux différentes exigences des services.

3.7.4 Transaction et évaluation

A la fin de chaque collaboration, l'objet demandeur évalue le rendement de chaque collaborateur et envoie un rapport d'évaluation au gestionnaire de confiance, dans lequel, soit il récompense (score positif) ou punit (score négative) ce collaborateur. Cette évaluation sera enregistrée dans le gestionnaire de confiance et sera utilisée ultérieurement pour calculer la dérivation de la confiance indirecte.

Le demandeur du service n'a aucun moyen de vérifier la justesse du résultat envoyé par les objets collaborateurs. Le résultat envoyé peut-être incomplet ou faux si l'objet est égoïste ou malicieux. Pour remédier à cela, le gestionnaire de confiance procède à l'évaluation des objets collaborateurs en vérifiant l'état de ressources de chaque objet et le temps d'exécution des tâches qui lui ont été attribuées. Lorsque les résultats de vérification sont conformes aux exigences du service, le gestionnaire de confiance récompense l'objet sinon, il le punit. Ces évaluations sont enregistrées dans le gestionnaire de confiance et utilisées ultérieurement pour calculer la dérivation de confiance directe.

3.7.5 Apprentissage

Cette phase contient deux étapes : la mise à jour de la qualité de recommandation et la mise à jour de la réputation.

3.7.5.1 La mise à jour de la qualité de recommandation

Après avoir reçu les rapports d'évaluation, le gestionnaire de confiance apprend davantage sur les intentions de chaque témoin et peut alors mettre à jour sa qualité de recommandation. Un témoin ayant donné une mauvaise note pour un collaborateur ayant reçu un bon score sera considéré comme mauvais recommandeur et sa qualité de recommandation QR sera diminuée. Lorsque la note du témoin à propos du collaborateur est conforme à celle du demandeur, sa qualité de recommendation sera augmentée. Dans le cadre de notre modèle STMS nous adoptons la même formule utilisée dans [9].

3.7.5.2 La mise à jour de la réputation

La réputation d'un objet exprime l'opinion de l'ensemble des objets d'un réseau sur la fiabilité de ce dernier après avoir fourni une assistance pour divers services. Elle sert à éliminer du réseau les objets malicieux et incompétents et cela en comparant la réputation de chaque objet à un seuil d'acceptation, lorsque cette dernière est au-dessous de ce seuil, l'objet concerné sera exclu immédiatement du réseau, il ne pourra pas demander ou participer à la réalisation d'un service.

TMS utilise la formule suivante pour calculer cette valeur de réputation :

$$R_i = \sum_{j=1}^{n} (C_j * N^{Fj} * QR_{Fj}) \qquad (3.5)$$

Critiques

Etant donné que les collaborateurs sont des objets moins contraints en ressources, la formule (3.5) ne favorisera que les collaborateurs défaillants, puisque, si la réputation d'un collaborateur diminue à cause de ses ressources épuisées, elle augmentera progressivement lorsqu'elles seront rechargées quand les collaborateurs ne sont pas défectueux. Par ailleurs, cette formule présente un problème, elle n'exclue pas les collaborateurs malicieux, ce qui provoque un état d'insécurité dans le réseau.

Améliorations de la formule de la réputation dans STMS

Dans le cadre de notre modèle STMS, nous ajoutons les observations enregistrées par le gestionnaire de confiance afin d'assurer plus d'exactitude, nous exprimons cette amélioration

par la formule (3.6) :

$$R_i = \sum_{j=1}^{n} (C_j * note_j) \qquad (3.6)$$

Avec :

$$note_j = \begin{cases} ((N^{F_j} * QR_{F_j}) + O^T(i)) - 1 & \text{Si } (N^{F_j} * QR_{F_j}) > 0 \text{ et } O^T(i) > 0 \\ (|N^{F_j} * QR_{F_j}| - |O^T(i)|) - 1 & \text{Sinon} \end{cases}$$

Le paramètre $note_j$ est égale à -1 si l'objet i a une observation négative ou un rapport négatif sur un même service, sinon sa valeur est à 1. La formule (3.6) permet de raffiner encore plus la composition du réseau, car elle élimine tous les collaborateurs malhonnêtes et ceux qui sont défaillants.

3.8 Conclusion

Dans ce chapitre, nous avons proposé un modèle de confiance nommé STMS (pour Secured Trust Management System) qui est une amélioration du modèle TMS [9].

Notre modèle de confiance introduit l'utilisation de la confiance directe, ce qui lui permet d'abord d'assurer plus d'exactitude dans la dérivation de la confiance. L'idée d'hybridation de la confiance directe et indirecte contribue énormément dans la sécurité des opérations de collaboration, car elle permet de réduire la chance d'être selectionné aux collaborateurs malicieux. STMS permet aussi de minimiser le taux de fausses acceptations dans le réseau, vu que les observations directes enregistrées par le gestionnaire de confiance assurent que tous les objets malicieux seront punis à chaque participation dans la réalisation d'un service donné, ce qui diminue leur réputation rapidement.

Le chapitre suivant sera consacré à la validation des performances de notre modèle STMS.

CHAPITRE 4

SIMULATION ET ÉVALUATION DES PERFORMANCES

4.1 Introduction

Ce chapitre est consacré à l'analyse des performances de STMS (*Secured Trust Management System*). Pour ce faire, nous analysons ses performances en comparaison avec celui du TMS (*Trust Management System*) proposé par Ben Saeid et al. [9], qui est une solution proposée dans l'axe des approches collaboratives qui se basent sur la notion de confiance et de réputation dans la désignation des collaborateurs adéquats pour un service demandé.

4.2 Sondage à probabilités inégales

4.2.1 Définition

Les méthodes de sondage ont pour objectif de tirer dans une population concrète des échantillons destinés à estimer avec la meilleure précision possible des paramètres d'intérêt. Les sondages réels portent sur des populations finies et sont effectués par tirage sans remise, pour ne risquer d'interroger deux fois la même entité. Les échantillons ne sont plus constitués de variables indépendantes et le tirage ne se fait pas toujours avec les mêmes probabilités [27].

4.2.2 Notations

$\mathsf{U} = \{1...\mathsf{N}\}$ une population d'entités (appelée aussi base de sondage), tel que N est la taille de la population. Chaque entité de cette population est désignée par un identifiant i. Nous notons Y la variable d'intérêt dont les valeurs sont (Y_1, Y_2,...,Y_n). Nous supposons que Y_i est

obtenue sans erreurs si l'entité i est sélectionnée.

Un échantillon est un sous-ensemble de n entités de la population et $\tau = \frac{n}{N}$ est le taux de sondage. Il y a C_N^n échantillons distincts possibles, chacun est noté par s.

Dans un sondage aléatoire chaque entité i de la population a une probabilité de tirage, où la probabilité d'inclusion Π_i qui est bien définie ne doit pas être nulle sous peine de ne pouvoir faire des estimations sans biais.

Nous notons que la somme des probabilités d'inclusion vaut à $\sum_{i=1}^{N} \Pi_i = n$ et que Π_i est égale à la somme des probabilités des échantillons qui contiennent l'entité $i : \Pi_i = \sum_{s(i \in s)} P(s)$. Un plan de sondage correspond à une distribution de probabilités sur l'ensemble des échantillons [27].

4.2.3 Le sondage aléatoire simple

Il constitue la base des autres méthodes. C'est un tirage équiprobable sans remise : nous avons, donc, $\Pi_i = \frac{n}{N}$ et tous les échantillons C_N^n sont équiprobables [27].

4.2.4 Sondage à probabilités inégales

Nous disposons d'une variable auxiliaire $x_i > 0 / \ i \in U$, suffisamment proportionnelle à la variable Y_i. Nous sélectionnons les unités à probabilités inégales proportionnelles aux x_i. Pour ce faire, nous calculons les probabilités d'inclusion selon la formule suivante : [29]

$$\Pi_i = \frac{n x_i}{\sum_{i=1}^{N} x_i} \qquad (4.1)$$

Si la formule ci-dessus fournit des $\Pi_i > 1$, les entités correspondantes sont sélectionnées dans l'échantillon avec une probabilité d'inclusion égale à 1 et les Π_i sont recalculés selon la même formule sur les entités restantes.

4.3 Modélisation

Dans cette section, nous modélisons notre solution en utilisant le modèle de sondage précédemment défini. L'objectif de cette modélisation est l'estimation de l'exactitude de la dérivation de la confiance et de la réputation de notre modèle. Pour ce faire, nous calculons les probabilités d'inclusion des objets dans les groupes de collaborateurs sélectionnés afin d'assister les objets à fortes contraintes de ressources dans les services qu'ils demandent, ainsi que la probabilité d'inclusion des collaborateurs malicieux dans l'ensemble des objets malicieux.

4.3.1 Le calcul des probabilités de sélection

4.3.1.1 Probabilité de sélection pour le premier service

La base de sondage est constituée de N objets, qui ont initialement la même valeur de confiance. Nous tirons aléatoirement un échantillon (un groupe de collaborateurs) de n objets afin d'assister le premier demandeur dans le service qu'il a proposé. Le tirage est sans remise car un collaborateur doit figurer une et une seule fois dans l'échantillon. Donc, ceci fait l'objet d'un sondage aléatoire simple. Dans ce cas, tous les échantillons sont équiprobables et le taux de sondage est $\tau = \frac{n}{N}$.

4.3.1.2 Probabilité de sélection pour les prochains services

Quand le système est en plein activité, des objets exécutent des services et par conséquent, les valeurs de confiance changent. Chaque objet i dispose d'une variable T_i qui représente sa valeur de confiance. A cet effet, il suffit de sélectionner les objets à probabilités inégales proportionnelles aux T_i. Cependant, les valeurs $T_i \in \mathbb{R}$, ce qui les rend inadaptées pour ce type de sondage qui exige des valeurs dans $\mathbb{N}^*$. Pour cela, nous procédons à la normalisation de ces valeurs. La normalisation consiste à transformer les valeurs T_i des objets de $\mathbb{R}$ vers $\mathbb{N}^*$ tout en gardant la précision d'écart entre les valeurs. Soit T_i la valeur de confiance d'un objet i, nous identifions tout d'abord le minimum des valeurs T et nous normalisons les valeurs en utilisant la formule suivante :

$$T_i^{'} = (T_i + |min + 1|) * 10^{\omega} \qquad (4.2)$$

Tel que $T_i^{'}$ est la valeur normalisée, min est la valeur minimale de l'ensemble des valeurs de confiance et ω est un facteur de précision. Enfin, la probabilité de sélection de chaque objet i est calculée avec $\Pi_i = \frac{n * T_i^{'}}{\sum_{i=1}^{N} T_i^{'}}$.

4.3.2 Le calcul des probabilités d'exclusion

En se basant sur une population de N objets, nous calculons les probabilités d'inclusion des objets dans l'ensemble des objets malicieux à exclure du réseau (ou probabilité d'exclusion). Nous supposons que le nombre d'objets malveillants est m. Donc, l'échantillon à sélectionner possède une taille de m. Chaque objet a sa propre valeur de réputation. Par conséquent, la modélisation mène vers un sondage à probabilités inégales. La normalisation des valeurs de réputation des objets est nécessaire afin de les adaptées à notre modèle. La normalisation se fait par la formule ci-dessous :

$$R_i^{'} = (R_i + |max + 1|) * 10^{\omega} \qquad (4.3)$$

Avec $R_i^{'}$ est la nouvelle valeur normalisée de réputation de l'objet i, max est la valeur maximale de l'ensemble des valeurs de réputation. Les probabilités d'exclusion sont calculée avec $\Pi_i = \frac{m * R_i^{'}}{\sum_{i=1}^{N} R_i^{'}}$.

4.4 Simulation du modèle

4.4.1 Paramètres de simulation

Pour simuler notre solution, nous avons développé le modèle sous java. Les simulations ont été réalisées avec 200 objets dont 100 sont non contraints en ressources et 10 % sont malicieux. Nous avons initialisé la qualité de recommandation des objets à 1. A chaque opération collaborative, un demandeur est choisi aléatoirement parmi les objets à fortes contraintes de ressources pour demander un service tiré aléatoirement parmi 6 types de services différents. 40 collaborateurs sont sélectionnés par le system pour assister l'objet demandeur dans son service, et le coût de ce dernier est déterminé d'une manière uniforme. Les résultats obtenus sont la moyenne de 100 itérations simulées.

4.4.2 Résultats obtenus

Dans ce qui suit nous présentons les résultats de la simulation de notre modèle. Afin de l'évaluer, nous comparons ses performances par rapport aux celles du modèle TMS proposé par Ben Saeid et al. dans [9].

4.4.2.1 Les probabilités de sélection

La figure 4.1 illustre la variation de la probabilité de sélection d'un bon collaborateur en fonction du nombre de services.

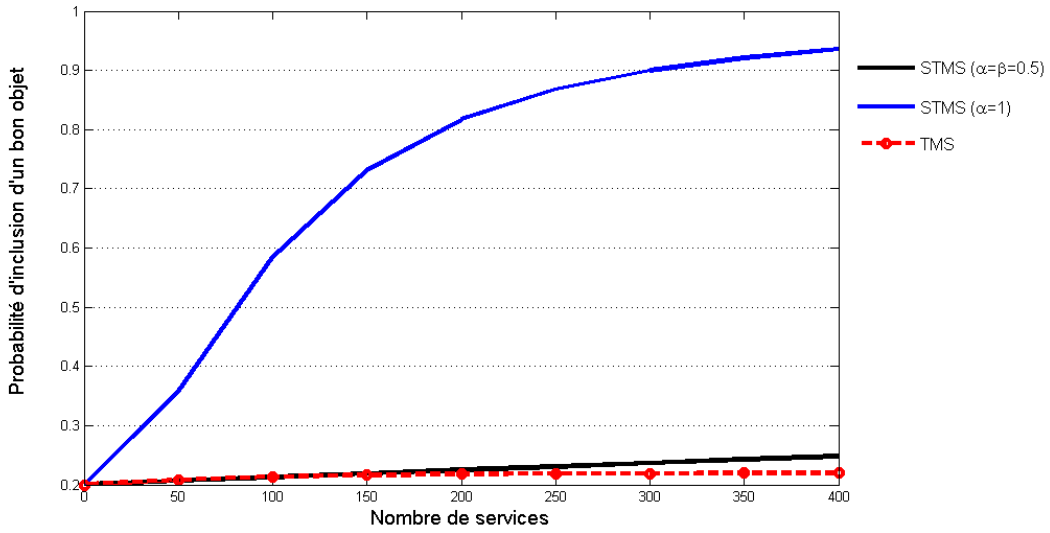

FIGURE 4.1 – Probabilité d'inclusion d'un bon collaborateur avec $\omega = 2$.

Pour STMS, la probabilité de sélection d'un bon collaborateur augmente avec l'augmentation du nombre de services demandés et elle est meilleure par rapport à celle de TMS. Notre modèle prend en considération les bons collaborateurs lors de l'exécution des services, ce qui permet de mieux les récompenser. Cela crée une large différence entre les valeurs de confiance des bons et des mauvais collaborateurs et par conséquent, les probabilités de sélection des bons collaborateurs sont élevées, contrairement à TMS qui ne se focalise que sur la performance des objets. TMS note tous les collaborateurs de la même manière, ce qui résulte des valeurs de confiance et des probabilités de sélection rapprochées.

La figure 4.2 illustre l'évolution de la probabilité de sélection d'un mauvais collaborateur en fonction du nombre de services.

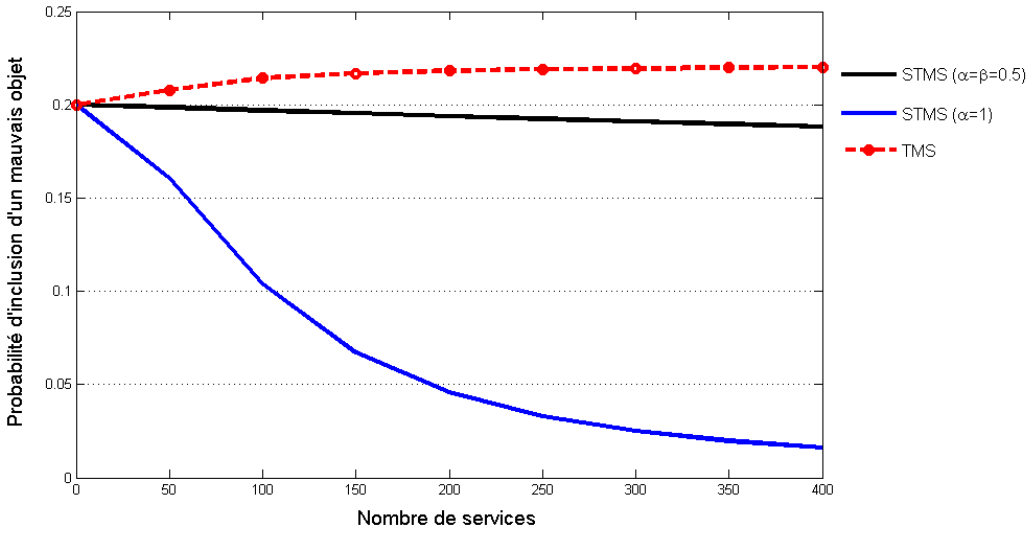

FIGURE 4.2 – Probabilité d'inclusion d'un mauvais collaborateur $\omega = 2$.

Nous constatons que la probabilité de sélection d'un mauvais collaborateur dans le cas de TMS est presque la même que celle d'un bon collaborateur, vu qu'il ne marque pas de différence entre les bons et les mauvais collaborateurs. Contrairement à STMS, nous remarquons la chute des valeurs de probabilité de sélection due aux observations négatives enregistrées sur les mauvais collaborateurs qui permettent de les punir et diminuer ainsi leur valeur de confiance, ainsi que leurs probabilités de sélection pour les prochains services.

Nous constatons qu'à chaque fois que la valeur du facteur α augmente, les probabilités de sélection deviennent intéressantes. Cela est justifié par l'écart que crée ce facteur dans les valeurs de confiance des collaborateurs permettant ainsi de faciliter la distinction entre un bon et un mauvais collaborateur. Ces résultats montrent l'importance de la confiance directe adoptée dans notre modèle.

4.4.2.2 Les probabilités d'exclusion du réseau

Il est important d'avoir que les meilleurs collaborateurs dans le réseau afin d'alléger le processus de calcul des distances de similarité, les poids des rapports et la sélection des collaborateurs aptes pour un service demandé. Une opération permettant d'aboutir à cette situation consiste à exclure du réseau les collaborateurs dont les valeurs de réputation sont inférieures à un seuil donné. La figure 4.3 illustre l'évolution de la probabilité d'exclusion d'un bon collaborateur en fonction du nombre de services.

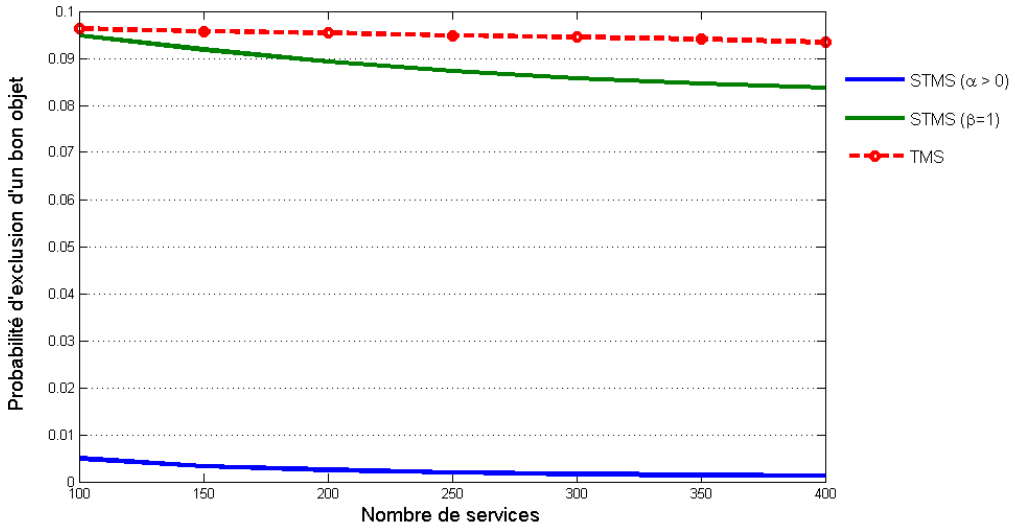

FIGURE 4.3 – Probabilité d'exclusion d'un bon collaborateur $\omega = 2$.

Nous constatons que quelles que soient les valeurs des facteurs α et β, notre modèle assure une meilleure protection contre l'exclusion des bons collaborateurs comparant à TMS. Ça revient aux observations directes enregistrées qui garantissent une dérivation de réputation plus exacte, ce qui minimise le risque de confusion entre les bons et les mauvais collaborateurs.

La figure 4.4 illustre la variation de probabilité d'exclusion d'un mauvais collaborateur en fonction du nombre de services.

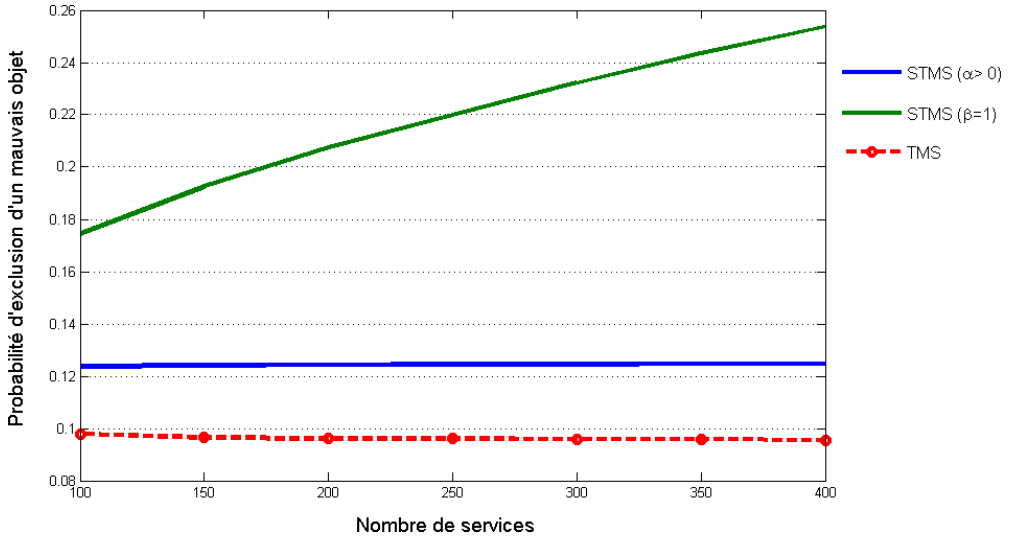

FIGURE 4.4 – Probabilité d'exclusion d'un mauvais collaborateur $\omega = 2$.

Nous constatons que le STMS affiche les meilleures performances. En effet, les probabilités d'exclusion d'un collaborateur malicieux sont largement importantes dans notre modèle que dans le modèle TMS. Cet écart de probabilités d'exclusion est obtenu grâce à la même raison du cas précédent.

4.5 Conclusion

Ce chapitre est axé sur la validation et l'analyse de performances du modèle proposée. Nous avons évalué les performances de notre modèle en se basant la confiance et la réputation en le comparant au TMS. Les résultats obtenus sont encourageons et montrent que notre modèle sélectionne des collaborateurs de confiance pour la réalisation des services.

CONCLUSION GÉNÉRALE ET PERSPECTIVES

L'Internet des Objets est un concept qui repose sur l'idée que tous les objets seront connectés un jour à Internet et seront donc capables d'émettre de l'information et éventuellement de recevoir des commandes. En quelques années seulement depuis son apparition, il est fut adopté dans divers secteurs et cela grâce à son potentiel énorme. Cependant, sa forte intégration soulève plusieurs interrogations dont la principale est « comment assurer la privacy et instaurer une sécurité robuste pour cette nouvelle technologie fortement hétérogène et ubiquitaire ? »

Dans ce travail, nous avons mené une étude critique des travaux menés dans l'axe des modèles de confiance dans l'Internet des Objets. Nous avons constaté que la réputation offre des solutions plus adaptées aux contraintes de l'IdO (ressources limitées, hétérogénéité des objets, etc.). Nous avons contribué à ce sujet en proposant un modèle de gestion de la confiance nommé STMS (*Secured Trust Management System*). Notre modèle de confiance se base sur la réputation et vise à sécuriser les opérations de collaboration qui se déroulent dans l'IdO et cela en s'appuyant sur une confiance hybride. Nous avons évalué notre modèle en le comparant avec TMS (*Trust Management System*) et les résultats ont été très encourageants.

Pour la clôture de ce document, nous présentons des perspectives qui feront l'objet de nos futures recherches. A commencer d'abord par la proposition d'un mécanisme permettant de détecter l'exécution d'une tâche supplémentaire par un objet et enfin, nous envisageons à instaurer un modèle théorique pour l'estimation de l'énergie consommée lors d'un traitement donné.

BIBLIOGRAPHIE

[1] S.Sicari, A.Rizzardi, L.A.Grieco and A.Coen-Porisini. Security, Privacy and Trust in Internet of Things : The Road Ahead. *Computer Networks,* 76 :146-164, 2015.

[2] G.D.Tormo, F.G.Mérmol and G.M.Pérez. Dynamic and Flexible Selection of a Reputation Mechanism for Heterogeneous Environments. *Future Generation Computer Systems,* 49 :113-124, 2015.

[3] Y.Ben Saeid, A.Olivereau, D.Zeghlache and M.Laurent. Lightweight Collaborative Key Establishment Scheme for the Internet of Things, *Computer Networks,* 64 :273-295, 2014.

[4] L.Bossi, S.Braghin and A.Trombetta. Multidimensional Reputation Network for Service Composition in The Internet of Things. In *International Conference on Services Computing*, pages 685-692. IEEE, 2014.

[5] J.Duan, D.Gao, D.Yang, C.H.Foh and H.Chen. An Energy-aware Trust Derivation Scheme with Game Theoretic Approach in Wireless Sensor Networks for IoT Applications. In *Internet Of Things Journal*, IEEE, 2014.

[6] G.Fortino and P.Trunfio. *Internet of Things Based on Smart Objects.* Springer, 2014.

[7] G.Lize, W.Jingpei and S.Bin. Trust Management Mechanism for Internet of Things. In *China Communications*, pages 148-156. ICT Management, 2014.

[8] Z.Yan, P.Zhang and A.V.Vasilakos. A Survey on Trust Management for Internet of Things. *Journal of Network and Computer Applications*, 42 :120-134, 2014.

[9] Y.Ben Saeid, A.Oliverau, D.Zaghlache and M.Laurent. Trust Management System Design for the Internet of Things : A Context-aware and Multiservice Approach. *Computers and Security*, 39 :351-865, 2013.

[10] S.Gusmeroli, S.Piccione and D.Rotondi. A Capability—based Security Spproach to Manage Access Control in the Internet of Things. *Mathematical and Computer Modelling*, 58 :1189-1205, 2013.

[11] 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 *conference*. IEEE, 2013.

[12] M.Mahmoud, J.Misic and X.Shen. A Scalable Public Key Infrastructure for Smart Grid Communications. In *Communication and Information System Security Symposium*, pages 806-811. Globecom, 2013.

[13] M.Mahmoud, J.Misic and X.Shen. Efficient Public-Key Certificate Revocation Schemes for Smart Grid. In *Communication and Information System Security Symposium*, pages 800-805. Globecom, 2013.

[14] Z.Sheng, S.Yang and Y.Yu. A survey on the IETF Protocol Suite for the Internet of Things : Standards, Challenges, and Opportunities. In *IEEE Wireless Communications*, 91-98, 2013.

[15] H.Wu and H.Dong. A Trust Model Based on Reputation in P2P Network. In *Proceedings of the Second International Conference on Innovative Computing and Cloud Computing*, pages 208-212, 2013.

[16] X.Xu, N.Bessis and J.Cao. An Autonomic Agent Trust Model for IoT Systems. *Procedia Computer Science*, 21 :107-113, 2013.

[17] Y.Challal. *Sécurité de l'Internet des Objets : Vers une Approche Cognitive et Systèmique*. PhD thesis, Université de technologie de Compiègne, 2012.

[18] J.Dumortier and N.Vandezande. Trust in the Proposed EU Regulation on Trust Services ?. *Computer Law and Security Review*, 28 :568-576, 2012.

[19] Cluster of European Research Projects on the Internet of Things. Vision and Challenges for Realising the Internet of Things. Report, 2010.

[20] K.Ashton. That 'Internet of Things' Thing. In *The Real World Things Matter More than Ideas*. RFID Journal, 2009.

[21] J.Gong, J.Chen, H.Deng and J.Wang. A Trust Model Combining Reputation and Credential. In *WASE International Conference on Information Engineering*, pages 635-638. IEEE, 2009.

[22] P.J.Benghozi, S.Bureau, and F.Massit-Folea. L'Internet des Objets. Quels Enjeux Pour les Européens ?. Technical report, Orange Ecole Polytechnique et TELECOM Paris Tech, 2008.

[23] M.Omar, Y.Challal and A.Bouabdallah. Infrastructure de Confiance Pour Les Architectures de Réseaux Mixtes. *Sécurité et Architéctures Réseaux / Sécurité des Systemes d'Information*, 2007.

[24] T.Schlossnagle. Scalable Internet Architectures. Kindle edition, 2007.

[25] A.Greebfield. Everyware : the Dawning Age of Ubiquitous Computing. New Riders, 2006.

[26] C.Llorens, L.Levier and D.Valois. Tableau de Bord de la Sécurité Réseau. Eyrolles, 2006.

[27] G.Saporta. Probabilités Analyse des Données et Statistiques. Technip, 2006.

[28] International Telecommunication Union. The Internet of Things. Report, 2005.

[29] P.Ardilly and Y.Tillé. Exercices Corrigés de Méthodes de Sondage. Ellipses, 2003.

[30] A.Josang and R.Ismail. The Beta Reputation System. In *Bled Electronic Commerce Conference*. Proceedings, 2002.

[31] ITU-T Recommendation. *Public-key Attribute Certificate Fram Works*. 4 edition, 2001.

[32] R.Housley, W.Ford, W.Polk et D.Solo. Internet X.509 Public Key Infrastructure Certificate and CRL. In *Profile*, 1999.

Résumé

Grâce aux progrès récents dans le domaine de la micro-électronique et l'émergence des technologies de communication sans fil et d'identification, l'Internet des Objet (IdO) a vu le jour. L'IdO est un réseau mondial qui relie tous les objets qui nous entourent à l'Internet. Par ailleurs, l'un des problèmes majeurs de ce type de réseaux, est la sécurité. En effet, la sécurité et la privacy dans l'IdO soulèvent des défis et des challenges plus importants que les réseaux classiques, cela est due à la fois aux contraintes qui caractérisent ses objets (hétérogénéité, mobilité, ressources limitées), ainsi que sa forte intégration dans la vie quotidienne des individus. Dans ce travail, après une étude critique menée sur les solutions proposées dans la littérature, nous proposons un modèle de confiance basé sur la réputation, nommé STMS (Secured Trust Management System). Le modèle de confiance proposé enregistre les tâches malicieuses effectuées lors de l'exécution des services et hybride la dérivation de la confiance pour assurer la sécurité des opérations de coopération qui se déroulent entre les objets de l'IdO. Les résultats de la modélisation de la sélection des collaborateurs dans STMS par un modèle de sondage sont très encourageants.

Mots clés : Modèle de confiance, Internet des Objets, Confiance, Réputation, Collaboration, Sécurité.

Abstract

Thanks to the recent developments in micro-electronics technologies and wireless communication and identification technologies, Internet of Things (IoT) have emerged. IoT is a global network connecting any objects around us to the Internet. Moreover, one of the major issues of such networks is security. Indeed, security and privacy issues in IoT scenarios would be much more challenging than what is being used in the conventional networks, this fact is due to both the constraints that characterize its objects (heterogeneity, mobility and limited resources) and its high implementation in the individual's daily life. In this work, after discussing some proposed solutions in the literature, we suggest a reputation based model, named STMS (Secured Trust Management System). The suggested trust model records the malicious tasks performed by the objects during the execution of services and hybrids trust derivation to ensure security in cooperative operations happening between IoT's objects. The modeling by the survey model of collaborators' selection performed by STMS shows encouraging results.

Keywords : Trust model, Internet of Things, Trust, Reputation, Collaboration, Security.