REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Mohamed Khider – BISKRA
Faculté des Sciences Exactes, des Sciences de la Nature et de la Vie
Département d'informatique

N° d'ordre : RTIC/M2/2020

Mémoire

Présenté pour obtenir le diplôme de master académique en

Informatique

Parcours : Réseaux de Technologie et l'Information

de la Communication**(RTIC)**

La gestion de la confiance dans Internet social des objets

Par :

Zaaboubi Salima

Soutenu le Septembre 2020, devant le jury composé de :

		Président
Hamida Ammar	M.A.A	Rapporteur
		Examinateur

Dédicaces

Je dédie ce travail

À Mes chers parents

Aucune dédicace ne saurait exprimer mon respect, mon amour éternel et ma considération pour les sacrifices que vous avez consenti pour mon Instruction et mon bien être.

Je vous remercie pour tout le soutien et l'amour que vous me portez

Depuis mon enfance ma mère, je prie pour que Dieu la préserve pour moi.

Et mon père, que Dieu ait pitié de lui, a souhaité qu'il soit à mes côtés en ce moment, mais cette épidémie "**COVID 19**" l'a emporté avec la sagesse de Dieu .. Dieu repose son âme j'espère que votre bénédiction m'accompagne toujours.

À mon frère Mourad.

À mes sœurs Zineb Nadjette Fadhila Hafida.

Et la femme de mon frère Asma pour ces soutiens moral et leurs conseils précieux tout au long de mes études et à tout ma famille.

Remerciements

Je remercie tout d'abord « Allah » de m'avoir donné le courage d'entamer et de finir ce mémoire

Je remercie vivement mon encadreur, ***M. HAMIDA AMMAR***, d'avoir encadré ce travail avec beaucoup de compétences.

Merci pour votre patience et sa volonté.et la confiance que vous m'avez accordée au cours de l'élaboration de ce mémoire ;

Merci pour l'acuité de vos critiques et pour vos conseils éclairés.

Je remercie également les membres du jury d'avoir accepté d'évaluer ce travail

J'adresse mes sincères remerciements à tous les professeurs, intervenants et toutes les personnes qui par leurs paroles, leurs écrits, leurs conseils et leurs critiques ont guidé mes réflexions et ont accepté de me rencontrer et de répondre à mes questions durant mes recherches.

Je remercie mes très chers parents, qui ont toujours été là pour moi. Je remercie mes sœurs, et mon frère, pour leurs encouragements.

À tous ces intervenants, je présente mes remerciements, mon respect et ma gratitude.

Table des matières

Liste des Figures

Liste des Tableaux

Introduction générale

L'Internet des objets (IoT) a été introduit pour la première fois par Kevin ASHTON [9]. Il désigne l'omniprésence autour de nous d'une variété d'objets qui, à travers des schémas d'adressage uniques, ces éléments inter connectés sont capables de fournit une variété de données qui peuvent être agrégées, fusionnées, traitées, analysées et exploitées afin d'extraire des informations utiles [18].

La principale force de la vision de l'IoT est son fort impact sur plusieurs aspects de la vie quotidienne et du comportement des utilisateurs potentiels. Cependant, de nombreux problèmes difficiles empêchent la vision de l'IoT de devenir réalité, comme l'interopérabilité, la navigabilité, la confiance, la gestion de la confidentialité et de la sécurité et la découverte de ressources dans un réseau aussi hétérogène et décentralisé. Pour résoudre certains des problèmes cités, un nouveau paradigme appelé internet social des objets (SIoT) est né.

L'internet social des objets est un paradigme qui intègre les réseaux sociaux dans internet des objets ; selon lequel les objets sont capables d'établir de manière autonome des relations avec d'autres objets, de rejoindre des communautés et de construire leurs propres réseaux sociaux qui peuvent différer de ceux de leur propriétaire [10]. Adopter une telle vision est donc une nouvelle tendance prometteuse, avec de nombreux avantages. Premièrement, la navigabilité et la découverte des ressources sont améliorées en réduisant leurs portées à un réseau social gérable [8]. Deuxièmement, l'évolutivité est garantie comme dans les réseaux sociaux humains [12]. Troisièmement, l'hétérogénéité des appareils, des réseaux et des protocoles de communication est résolue par l'utilisation des réseaux sociaux [8]. Et une source de données plus grande devient disponible car elle provient d'un ensemble d'utilisateurs. L'alimentation continue des données des communautés nous donne du big data [28]. La quantité et la variété des données contextuelles ont augmenté, ce qui a permis d'améliorer l'intelligence des services et l'adaptabilité aux besoins situationnels des utilisateurs [8]. par exemple, les ordinateurs et les téléphones portables, travaillent ensemble pour rendre la vie humaine plus confortable. Avec ce nombre croissant des appareils connectés, il est difficile de supposer que quel appareil est fiable .

En effet, sans fondations efficaces de gestion de la confiance, les attaques et les dys-

fonctionnements d'IoT l'emporteront sur tous ses avantages [46].

À cause de cela, la gestion de la confiance devenue un défi majeur dans soi garantir une analyse fiable des données, des bons services et une sécurité accrut des utilisateurs. Il aide les gens à affronter et à dépasser leurs peurs et incertitudes et favorise l'acceptation et la consommation des utilisateurs sur les services et applications IoT. En effet dans ce contexte que nous orientons notre recherche sûre comment gérer la confiance dans d'environnement SIoT à cet effet, nous sommes basés sur les connaissances et les techniques déjà existant pour situer la question principale de recherche. L'hypothèse principale qui sous-tend la présente recherche repose sur déterminer les nœuds honnêtes et les nœuds malhonnêtes. Nous estimons alors qu'il est nécessaire d'utiliser un meilleur modèle de confiance dans l'environnement SIoT qui permettre d'éviter les nœuds malhonnêtes dans communication entre les nœuds pour cela on a utilisé l'algorithme DTrustInfer qui calcule dynamiquement la confiance des nœuds et utilise des codes secrets pour fournir une communication sécurisée et fiable entre les nœuds pour garantir que le réseau SIoT comprend la majorité des nœuds honnêtes. Peu de nœuds malveillants peuvent être présents dans le réseau, car le réseau SIoT doit être robuste et un contrôle de robustesse doit être effectué périodiquement. Puis on a ajouté les valeurs de rétroaction qui rendre, le nœud demandeur récompense ou punit le nœud fournisseur de services selon que son service était satisfaisant ou insatisfaisant. La récompense et la punition sont données sous forme d'augmentation ou de diminution, respectivement, de la valeur de fiabilité ou de la réputation du nœud du fournisseur de services.

Ce mémoire comporte quatre chapitres organisés comme suit : Dans le premier chapitre,On a décomposé par deux partie dans le premier partie qui présenté internet des objet(IoT) ,les technologies utilisée pour son fonctionnement et les domaine d'applications, puis dans la deuxième parties on a parler sur internet des objets social (SIoT) qui présenté d'abord les principales facettes d'un système SIoT, son architecture, les types de relations entre les objets, domaine d'applications,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 la confiance dans internet des objet social et encore faire une taxonomie des modèles des confiance dans IoT et SIoT .

Le second chapitre nous allons entamer sur les différent types attaques qui sont spécialement conçus pour perturbez les systèmes de gestion de confiance et les différents solutions ont été proposées dans la littérature pour atténuer ces attaques.

Le troisième chapitre est réservé à la conception de notre système, son architecture globale et détaillée. Le dernier chapitre nous proposons une simulation dans ce modèle pour assure la confiance de l'environnement SIoT. Nous avons présenté le logiciel de simulation,

décrit son architecture, méthode de son installation, ses principaux fichiers et enfin . Le mémoire est terminé par une conclusion générale contenant les perspectives envisagées.

Chapitre 1

Présentation sur internet des objets social (SIoT)

1.1 Introduction

Le monde a été confronté à trois révolutions des technologies de l'information et de la communication (TIC) , la troisième vague des TIC a conduit à L'internet des Objets(IoT) [36] L'IoT est un réseau qui relie et combine des objets avec l'Internet en suivant des protocoles qui assurent leur communication et échange d'informations à travers une variété de dispositifs [59] en utilisant la technologie filaire ou sans fil tels que RFID, ZigBee, WSN, NFC, Bluetooth, GPRS . 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 ont d'assurer la sécurité des individus et des entreprises cela afin de trouver un système fiable qui exclut les nœuds malveillants . Dans ce chapitre,on a décomposé par deux partie dans le premier partie qui présenté internet des objet(IoT) ,les technologies utilisée pour son fonctionnement et les domaine d'applications, puis dans la deuxième parties on a parler sur internet des objets social (SIoT) qui présenté d'abord les principales facettes d'un système SIoT, son architecture, les types de relations entre les objets, domaine d'applications,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 la confiance dans internet des objet social et encore faire une taxonomie des modèles des confiance dans IoT et SIoT et terminer par une conclusion

1.2 Internet des objets (IoT)

1.2.1 Définition de internet des objets (IoT)

L'Internet des objets(IoT) devrait être dominé par un grand nombre d'interactions entre des milliards des objets intelligents ou personnes et des communications hétérogènes entre les hôtes. Il fournit une variété de données qui peuvent être agrégées, fusionnées, traitées, analysées et extraites afin d'extraire des informations utiles [2]. une autre définition d'après les auteurs Keyur et Sunil [44] qui défini L'Internet des objets (IoT) représente une vision dans laquelle tous les objets physiques sont reliés entre eux à tout moment, en tout lieu, avec n'importe quoi et n'importe qui utilisant idéalement n'importe quel chemin réseau et n'importe quel service.

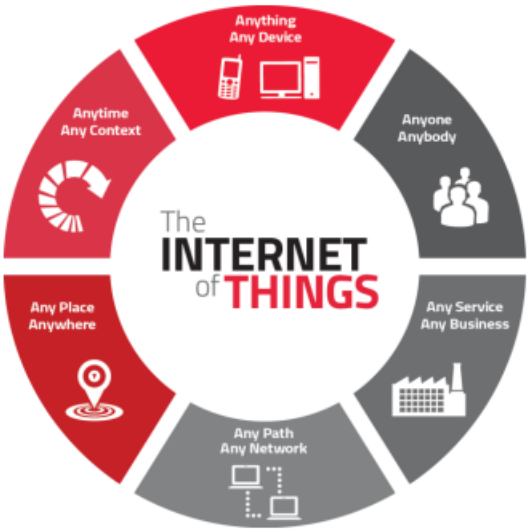

FIGURE 1.1 – Internet des objets (IoT) [44]

1.2.2 Les Technologies de l'IoT

L'IoT nécessite plusieurs systèmes technologiques pour son fonctionnement. Afin de permettre l'interconnexion de différents objets intelligents via l'Internet.

1.2.2.1 RFID (Radio Frequency Identification)

Le RFID se compose d'étiquettes RFID et de lecteurs RFID. Les appareils sont équipés de micropuces qui transmettent des informations via des réseaux sans fil. Ces informations sont ensuite traitées par des lecteurs RFID pour identifier et surveiller des objets ou des appareils avec des étiquettes RFID[19], cette technologies utilisant les ondes radio pour identifier des objets ou des personnes. Le fonctionnement de la technologie RFID est

représenté sur la figure 1.2.

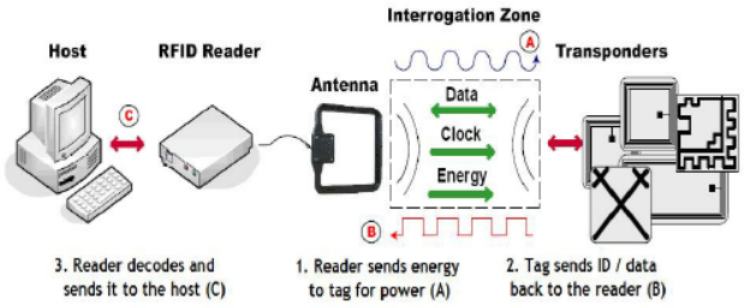

FIGURE 1.2 – Technologie RFID [7]

1.2.2.2 WSN (Wireless Sensor Network)

C'est un ensemble de nœuds organisés en un réseau coopératif qui communiquent sans fil, où chacun possède une capacité de traitement et peut contenir différents types de mémoires : un émetteur-récepteur (Radio fréquence RF) et une source d'alimentation, comme il peut aussi tenir compte des divers capteurs et des actionneurs. Il constitue alors un réseau de capteurs sans fil nécessaire au fonctionnement de l'IoT [50].

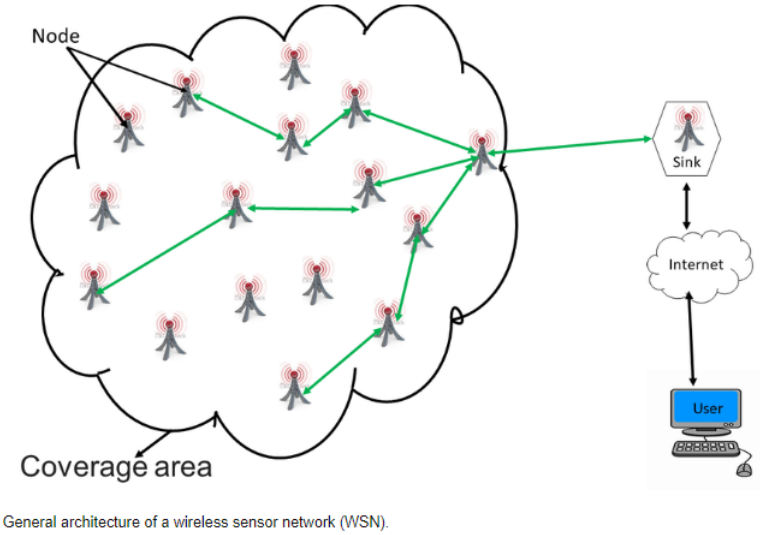

FIGURE 1.3 – Réseau de capteurs sans fil pour la communication entre différents nœuds de capteurs [26]

1.2.2.3 M2M (Machine to Machine)

C'est l'association des technologies de l'information et de la communication avec des objets intelligents dans le but de donner à ces derniers les moyens d'interagir sans intervention humaine avec les systèmes d'information [43].

1.2.3 Domaine d'Application

Les applications potentielles de l'IoT sont nombreuses et diverses, imprégnant pratiquement tous les domaines de la vie quotidienne des individus, des entreprises et de la société dans son ensemble. L'application IoT couvre les environnements / espaces «intelligents» dans des domaines tels que : transport, bâtiment, ville, mode de vie, commerce de détail, agriculture, usine, chaîne d'approvisionnement, urgence, soins de santé, interaction avec les utilisateurs, culture et tourisme, environnement et énergie. Voici quelques-unes des applications IOT. [53]

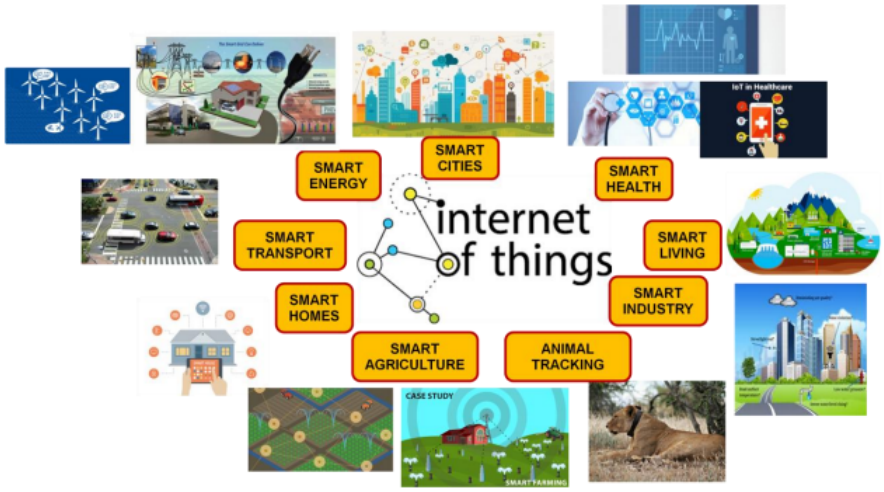

FIGURE 1.4 – Domaine d'application dans IoT [44]

1.2.3.1 IOsH (Internet de la santé intelligente) :

- **Surveillance des patients** : surveillance de l'état des patients à l'intérieur des hôpitaux et au domicile des personnes âgées,
- **Réfrigérateurs médicaux :** contrôle des conditions à l'intérieur des congélateurs stockant les vaccins, les médicaments et les éléments organiques,
- **Détection des chutes :** assistance aux personnes âgées ou handicapées vivant en autonomie,
- **Dentaire :** la brosse à dents connectée Bluetooth avec l'application Smartphone analyse les utilisations du brossage et donne des informations sur les habitudes de brossage sur le Smartphone pour des informations privées ou pour afficher des statistiques au dentiste,
- **Surveillance de l'activité physique :** des capteurs sans fil placés à travers le matelas détectent les petits mouvements, comme la respiration et la fréquence cardiaque et les grands mouvements provoqués par les mouvements et les retournements pendant le sommeil, fournissant des données disponibles via une application sur le smartphone.

‘

1.2.3.2 IOsC (Internet des villes intelligentes) :

- **Santé structurale :** surveillance des vibrations et des conditions matérielles des bâtiments, ponts et monuments historiques,
- **Foudre :** éclairage intelligent et adaptable aux conditions météorologiques dans les réverbères,
- **Sans encombre :** Surveillance vidéo numérique, gestion de la lutte contre les incendies, systèmes d'annonces publiques,
- **Transport :** routes intelligentes et autoroutes intelligentes avec messages d'avertissement et déviations en fonction des conditions climatiques et des événements inattendus comme les accidents ou les embouteillages,
- **Parking intelligent :** suivi en temps réel de la disponibilité des places de stationnement en ville permettant aux habitants d'identifier et de réserver les places disponibles les plus proches,
- **Gestion des déchets :** détection des niveaux de déchets dans les conteneurs pour optimiser les itinéraires de collecte des déchets. Les poubelles et les bacs de recyclage avec des étiquettes RFID permettent au personnel de l'assainissement de voir quand les ordures ont été jetées.

1.2.3.3 IOsI (Internet de l'industrie intelligente) :

- **Gaz explosifs et dangereux :** détection des niveaux de gaz et des fuites dans les environnements industriels, les environs des usines chimiques et à l'intérieur des mines, surveillance des niveaux de gaz toxique et d'oxygène à l'intérieur des usines chimiques pour assurer la sécurité des travailleurs et des marchandises, surveillance des niveaux d'eau, de pétrole et de gaz en stockage réservoirs et citernes,
- **Maintenance et réparation :** les premières prévisions de dysfonctionnements de l'équipement et de maintenance peuvent être programmées automatiquement avant une défaillance réelle de la pièce en installant des capteurs à l'intérieur de l'équipement pour surveiller et envoyer des rapports.

1.2.3.4 IOsA (Internet de l'agriculture intelligente) :

- **Maisons vertes :** contrôler les conditions micro-climatiques pour maximiser la production de fruits et légumes et sa qualité.

1.2.3.5 IOsE (Internet de l'énergie intelligente)

- **Smart Grid :** surveillance et gestion de la consommation d'énergie.
- **d'éoliennes / centrale électrique :** surveillance et analyse du flux d'énergie des éoliennes et de la centrale électrique, et communication bidirectionnelle avec

les compteurs intelligents des consommateurs pour analyser les modes de consommation.

1.3 Internet des Objets Social(SIoT)

1.3.1 Définition

L'Internet social des objets (SIoT) est un nouveau paradigme où l'IoT fusionne avec les réseaux sociaux, permettant aux personnes et aux appareils connectés ainsi qu'aux appareils eux-mêmes d'interagir dans un cadre de social pour soutenir une nouvelle navigation sociale [4]

1.3.2 Les principales facettes d'un système SIoT

D'apres 'Pallavi Sethi' et les autres [48]le système SIoT se compose principalement de trois facettes tel que :

- **Navigabilité :** par exemple Nous pouvons commencer avec un seul appareil et parcourir tous les périphériques qui y sont connectés. Il est facile de découvrir de nouveaux appareils et services en utilisant un réseau social de dispositifs IoT.
- **Fiabilité** grâce des relations social entre les objets (force de la relation) les valeur de fiabilité est plus exact.
- **Sociale :** à l'étude des réseaux sociaux humains pour étudier également les réseaux sociaux des dispositifs IoT.

1.3.3 Architecture système internet des objets social(SioT)

1.3.3.1 Architecture globale du SIoT

Pour une meilleure compréhension, nous considérons que les éléments suivants font partie de l'architecture de SIoT [27] :

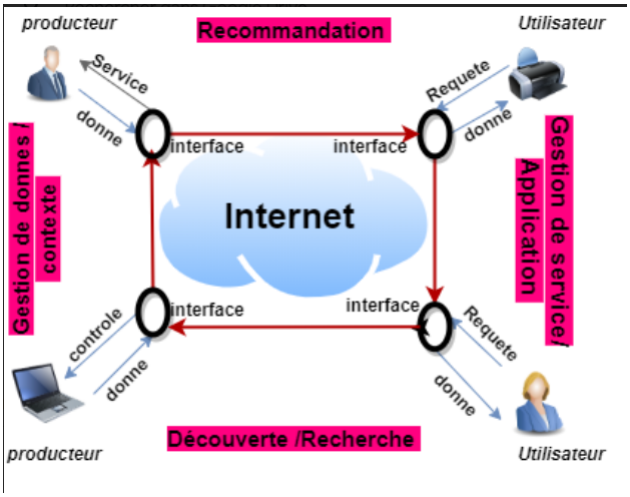

FIGURE 1.5 – schéma globale de SIoT [27]

1. **Les acteurs (les objets intelligentes) :** chaque objet peut participer de manière égale en publiant des données et en recevant des commandes de contrôle permettant de gérer les données en cours de production qui peuvent être représentées sous forme de données de profilage ou simplement de réponses à des requêtes envoyées par des utilisateurs et / ou des périphériques ;
2. **Le système intelligent :** responsable de la gestion et de l'orchestration de l'ensemble des interactions entreprises par les acteurs telles que la gestion des services et des applications, les données et de contexte, la recommandations, la recherche et la découverte de services et gestion de contexte ;
3. **L'interface :** sert d'intermédiaire entre les acteurs et le système intelligent ;les interactions avec le système ont lieu via l'interface. Elle permet la saisie de données et de requêtes et la sortie demandée telles que les commandes de contrôle ou de services ;
4. **L'internet :**c'est un moyen de communication et de lien entre les appareils intelligents avec leurs services et les utilisateurs

1.3.3.2 Architecture proposée par Luigi Atzori michele Nitti

Luigi Atzori, Al[13] propose une architecture à trois couches pour SIoT, Ces couches sont : la couche de détection, la couche réseau et la couche application

1. **Couche détection :**est la couche physique qui a des capteurs pour détecter et recueillir des informations sur l'environnement,et à la collaboration des noeuds dans les réseaux locaux et à courte portée.
2. **Le couche réseau :**est responsable de la connexion à d'autres objets intelligentes, les périphériques réseau et les serveurs ses caractéristiques sont également utilisées pour la transmission et le traitement des données de capteurs.
3. **Couche application :** où les applications IoT sont déployées avec les fonctionnalités middleware, cette couche est subdivisée en trois couches, à savoir la sous-couche de base, la sous-couche de composant et la sous-couche d'interface.

   La figure 6 montre l'architecture à trois couches. Les trois éléments de base du système proposé sont : **le serveur SIoT, la passerelle et l'objet** [13] :

   (a) **Côté serveur à gauche :** la partie serveur est composée de trois sous couches, les composants et fonctionnalités de ces sous-couches sont décrits ci-dessous :

   i. **La sous-couche de base (Base Layer) :** comprend la base de données pour le stockage et la gestion de données avec les descripteurs pertinents, la base de données d'ontologies, les moteurs sémantiques et les communications.

ii. **la sous-couche Composants (the Component Sub-layer)** comprend les outils qui implémentent la fonctionnalité principale du système SIoT tels que :

La gestion des identifiants (The ID management) : vise à attribuer un identifiant qui identifie universellement toutes les catégories possibles d'objets (UUID,MAC, N de Série, ePC,. . .), et conserver les schémas d'identification d'objets existants habituellement définis par le fabricant de l'objet. Un protocole simple basé sur XML peut être mis en oeuvre, permettant de spécifier le mécanisme d'identifiant adopté autre que l'identifiant lui-même. Ce système comprend : les adresses IPv6, le code universel de produit (UPC), le code électronique de produit (EPC), le code ubiquitaire (Ucode), OpenID, l'URI.

Le profil d'objet (Object profiling OP) : vise à configurer manuellement et automatiquement une information (statique ou dynamique) sur les objets qui doivent être organisés en classes sur la base de leurs principales caractéristiques.

Le contrôle du propriétaire (The owner control OC) : Ce module permet la définition des éléments suivants en utilisant différents langages de politique de sécurité et de contrôle d'accès déjà disponibles : des activités pouvant être exécutées par l'objet ; des informations pouvant être partagées et auxquelles peut accéder l'objet ;du type de relation à mettre en place.

La gestion des relations (The relationship management RM) : est le module clé du réseau. Sa tâche principale est de permettre aux objets de démarrer, de mettre à jour et de mettre fin à leurs relations avec d'autres objets sur la base des paramètres de contrôle du propriétaire.

Découverte de service (The service discovery SD) : Cet élément détermine les FSs requis de la même manière que les êtres humains en recherchant des amitiés et toute information contenue dans les services de réseau social.

Composition de service (The service composition SC) : Active les interactions entre les objets ainsi que le service souhaité et trouvé par l'élément de découverte de services en s'appuyant sur les relations d'objets.

Gestion de confiance (the trustworthiness management TM) : vise à comprendre comment doivent être traitées les informations fournies par les autres membres et savoir à quels services et objets faire confiance. La confiance est basée sur le comportement de l'objet et

strictement liée au module de gestion des relations.

iii. **Sous-couche Interface (Interface Sub-layer) :** les interfaces avec les objets, les humains et les services s'y trouvent. Elle peut être mappée sur un seul site, déployée de manière fédérée par différents sites ou déployée dans un nuage.

(b) **Côté Passerelle et objets à droite :**quant aux systèmes de passerelles et d'objets, la combinaison des couches peut varier selon les caractéristiques du périphérique. Nous prévoyons l'un des 3 scénarios suivants [13] :

i. **Premier scénario** : un objet simple (ex : l'étiquette RFID), un dispositif de détection équipé d'une fonctionnalité de la couche la plus basse est autorisé à envoyer des signaux à la passerelle qui est équipée des fonctionnalités des 3 couches.

ii. **Deuxième scénario :** un dispositif (ex : la caméra vidéo) est capable de détecter les informations physiques et d'envoyer les données associées sur une IP réseau. L'objet serait alors défini avec les fonctionnalités de la couche réseau autres que celles de l'application. Par conséquent, Une couche d'application sur un serveur avec la fonctionnalité de couche d'application de passerelle serait suffisante.

iii. **Troisième scénario :** un objet intelligent (ex : Smartphone) peut implémenter la fonctionnalité des 3 couches de sorte que la passerelle ne soit pas nécessaire. Mais certaines installations de communication sont nécessaires pour maintenir la connectivité de l'objet. Il dispose suffisamment de puissance de calcul pour effectuer toutes les opérations pour les 3 couches et nécessite une passerelle pour une connectivité réseau omniprésente.

Quel que soit le scénario mis en oeuvre, la couche application englobe les applications SIoT, **l'agent social et l'agent de gestion de service** présentés ci-dessous [13] :

L'agent social (The social agent) : Prévu pour la communication avec les serveurs afin de mettre à jour son profil et ses amitiés, de découvrir et de demander des services et d'implémenter les méthodes permettant de communiquer directement avec d'autres objets lorsqu'ils sont proches géographiquement ou lorsque la composition du service nécessite des communications directes entre les objets.

L'agent de gestion de services (the service management agent) est responsable des interfaces avec les humains qui peuvent contrôler le comportement de l'objet lors de la communication au sein de son réseau social.

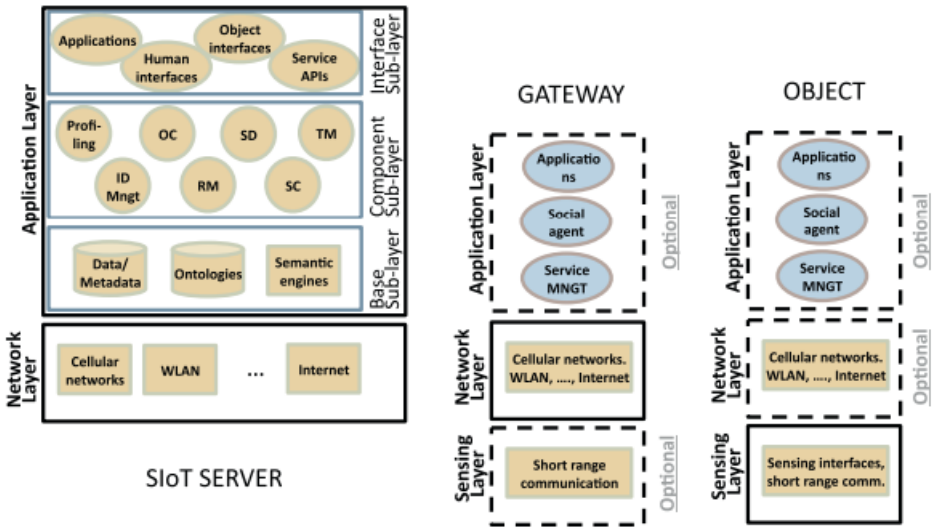

FIGURE 1.6 – Architacture de SIoT proposée par Luigi Atzori et michele Nitti [13]

1.3.4 Les Types de relations entre objets

1.3.4.1 Approche sociologique de Mandler

Par analogie aux types de relations entre les individus, des travaux (Mandler et al., 2015) ont proposé une classification des types de relations relatives aux objets communicants sur la base de 5 types de relations qui sont [14] :

1. **Relation de Co-localisation (Co-Location Object Relationship C-LOR) :** établie lorsque des objets (tels que capteurs, actionneurs, étiquettes RFID, etc.) sont présents simultanément au même endroit (sur une machine, dans un atelier, une maison, une ville) pour proposer des services d'automatisation résidentielles ou industrielles.
2. **Relation de Co-travail (Co-work object relationship C-WOR) :** établie lorsque des objets coopèrent ensemble dans une même application ou un même processus, pour réaliser une tâche ou un but collectif telles que : intervention d'urgence, télémédecine.
3. **Relation de Parent (Parent Object Relationship : POR) :** établie lorsque des objets appartiennent à une même famille (objets similaires, même catégorie, construits à la même période, même fabricant, appartenant à un même lot). Elle est implémentée lors de la production de l'article, ne changera pas au fil du temps et ne sera mise à jour que par des événements d'interruption ou d'obsolescence d'un périphérique donné .
4. **Relation de Propriétaire (Ownership object relationship OOR) :**établie entre des objets hétérogènes appartenant au même utilisateur et interagissent entre eux (téléphones portables, lecteurs de musique, consoles de jeux, etc.). L'objet peut

être porté par son utilisateur (personne, machine ou autre objet) qui peut stimuler l'interaction des objets .

5. **Relation Sociale (Social Object Relationship SOR) :**établie lorsque des objets entrent en contact au travers de la rencontre physique de leurs propriétaires de la même manière que les personnes qui échangent leurs contacts (n de Tel, adresses e-mail, etc.). L'appareil, s'il y est autorisé, échange son profil social de manière autonome.

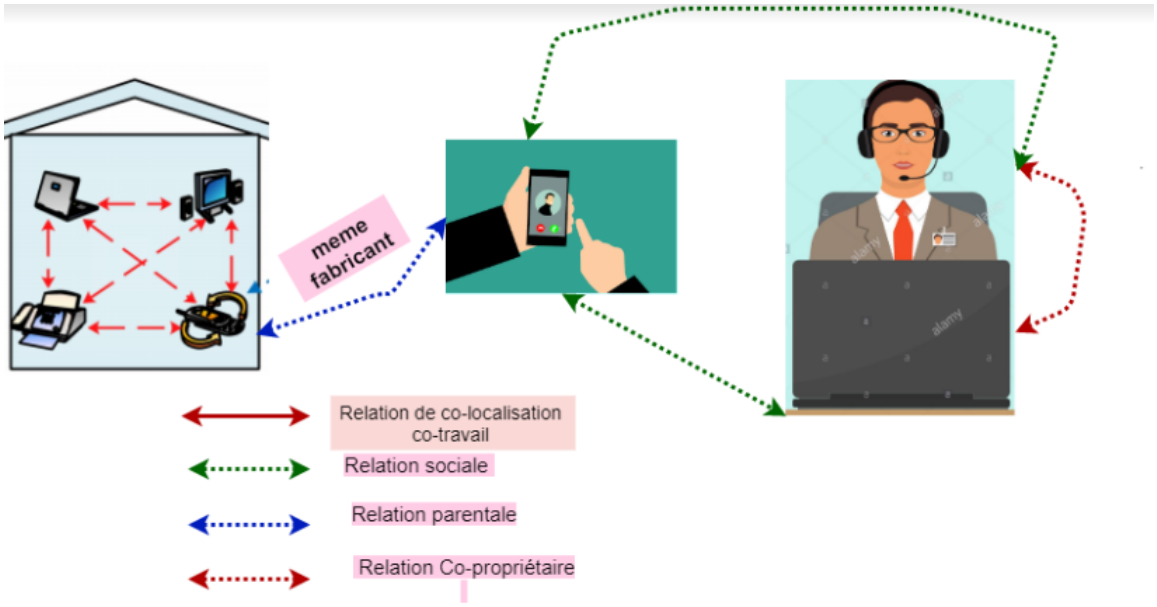

FIGURE 1.7 – Les types de relations social entre les objets[19]

1.3.4.2 Approche sociologique de Chen R. et al

Une autre structure de relation a été proposée par Chen R. et al [22], qui proposent un réseau SIoT basé sur 3 types de relations sociales reliant les propriétaires d'objets :

1. **Relation d'amitié :** Elle représente l'intimité ;
2. **Relation de contact social :** Elle représente la proximité ;
3. **Relation de communauté d'intérêts :** fait référence à des connaissances ou expériences communes.

1.3.5 Domaine D'application dans SIoT

L'SIot a des applications dans divers secteurs. Elle conduit à une meilleure circulation de l'information et de la gestion, ce qui à son tour conduit à une meilleure

prestation de services. Les exemples de scénarios dans différents domaines d'application sont donnés ci-dessous, qui fournissent des preuves de l'utilité et de l'impact potentiels du SIoT dans divers secteurs.[19]

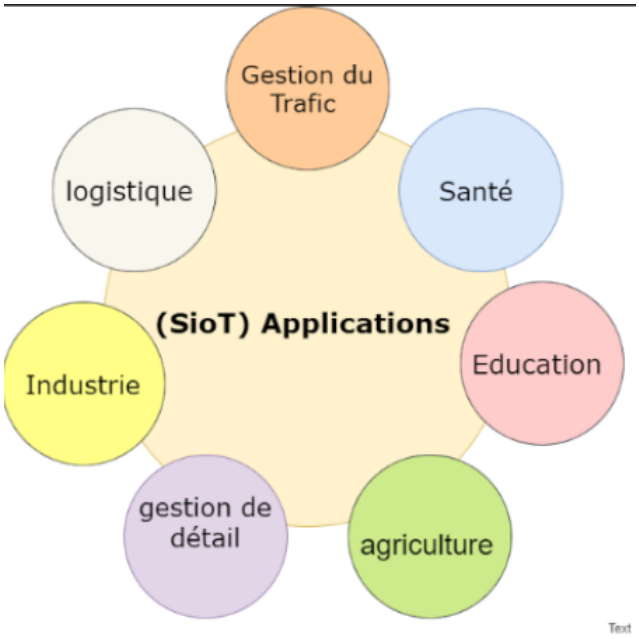

FIGURE 1.8 – Domaine application de internet social des objets (SioT)

— **Industrie :** soit exemple suivante "Albert" dirige une industrie textile et est confronté à un problème technique dans l'une de ses machines. Avant d'appeler un mécanicien, il essaie de trouver lui-même des solutions. Il contacte les appareils d'autres propriétaires d'industries similaires qui peuvent avoir rencontré un problème similaire dans leurs unités industrielles. Il peut utiliser la relation de co-travail pour sa cause où les appareils de différents propriétaires de l'industrie travaillent ensemble pour fournir un service de dépannage de la machine.
— **Éducation :** "Joe" est un lycéen et a des doutes en mathématiques. Aucun de ses amis n'est capable de résoudre son problème. "Joe" essaie ensuite de trouver des solutions via son appareil en envoyant des messages à d'autres appareils de son réseau social avec les propriétaires desquels "Joe"aurait pu aller à l'école ou à des cours de coaching mais qu'il ne connaît pas autrement.
— **Santé :** "Ben" fait face à un problème de santé et souhaite consulter un spécialiste. L'appareil de Ben (par exemple, téléphone ou bracelet de santé) peut consulter ses appareils amis pour trouver le médecin et faire rapport des résultats à Ben. En particulier, la co-localisation ou les relations sociales peuvent être exploitées dans ce cas.
— **Gestion du trafic :** "Fred" est un vendeur qui doit beaucoup voyager à travers la ville pour son travail. La voiture de Fred peut demander à d'autres voitures de

son réseau social des mises à jour du trafic le long de différents itinéraires vers une destination particulière. La voiture de Fred peut exploiter l'un des cinq types de relations autorisés par SIoT, en fonction des politiques définies par Fred pour son appareil (la voiture dans ce cas).

1.3.6 Vulnérabilités et menaces dans l'Internet social des Objets

À cause de la forte intégration de l'IoT, les objets quotidien deviennent des risques potentiels d'attaque sur la sécurité. L'ubiquité de l'IoT 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 les processus et la privacy des personnes[6]

1. **Menaces sur les données et réseaux**
   - Manque de la surveillance et de la protection des objets communication cité a cause des attaque potentielle portées sur le matérielle (vole ,corruption ,la contrefaçon de ces données pour récupération des données qui sont stockées sur ces dispositifs)
   - Transmission sans fil sont réputes pour leur forte vulnérabilité aux attaque(passive ,déni de service DoS)
   - Limitation de ressources des objets communication

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.car les appareils électronique non seulement sont traçable mais peuvent filmer écouter ou même enregistrer leurs rythme cardiaque ou respiratoire ,la température du corps dans le but d'un usage malicieux

1.3.7 La sécurité dans Internet des Objets

D'une manière générale la sécurité Informatique consiste à assurer que les ressources matérielles et logicielles d'une organisation sont uniquement utilisées dans le cadre prévu.

La Sécurité vise à assurer plusieurs objectifs, dont les cinq principaux sont : l'authentification, la confidentialité, l'intégrité, la disponibilité et la non-répudiation [17]

- **La confidentialité :**dans la littérature, la confidentialité semble être la qualité la plus importante dun système sûr. Elle a été est la première préoccupation des militaires. Assurer la confidentialité des données consiste à faire en sorte que les informations restent secrètes et que seules les personnes autorisées y aient accès.

Les utilisateurs du système ont besoin d'avoir la garantie que leurs informations ne risquent pas dêtre divulguées à des personnes non autorisées.

— **L'authentification :** fournir deux preuves en parallèle, lune est aussi importante et indispensable que lautre : Prouver quun sujet (site, personne, système, processus, etc.) est celui quil prétend être et que les informations reçues sont conformes à celles fournies.

Pratiquement, dans le cas dun simple message, le service dauthentification assure que le message provient de lendroit doù il prétend venir. Dans le cas dun échange bidirectionnel, deux aspects sont à vérifier. Il faut assurer que les deux entités communicantes sont bien ce quelles affirment être. De plus, le service dauthentification doit montrer que la connexion ne peut être brouillée par une troisième entité essayant de se faire passer pour un des deux correspondants.

— **L'intégrité : :**outre la confidentialité des informations, lintégrité évite la corruption, laltération et la destruction des données dans le réseau de manière non autorisée. Lintégrité reste un domaine très large couvrant à la fois les modifications, les moyens de modification mais également laprès-modification et donc la cohérence des données.

— **La disponibilité :** assurer aux utilisateurs légitimes une continuelle disponibilité des informations, des services et des ressources dans le réseau (les temps de réponse, la tolérance aux fautes, le contrôle de concurrence, le partage équitable de ressources, etc.). En somme,veiller à la disponibilité dun système, cest prévenir contre les perturbations et les interruptions de son fonctionnement et aussi contre toute utilisation abusive des services et des ressources du système.

— **La non répudiation :**la technique de non répudiation vise à éliminer le risque qu'un émetteur puisse nier avoir envoyé un message alors que réellement tel a été le cas.

A titre d'exemple, lors dune transaction commerciale électronique, le service de la non répudiation de lorigine oblige le client à ne pas démentir le fait qu'il a adressé une requête dachat au fournisseur.

1.3.7.1 La confiance Dans Internet Social Des Objets

1.3.7.1.1 Définition de la confiance

La confiance fournit un mécanisme pour la mesure de la fiabilité et la disponibilité d'une entité donnée ,dans le domaine de la sécurité Informatique, plusieurs auteurs ont proposé leurs propres définitions de ce terme,en suivant certaines des définitions existantes :

— **Neisse et al [39]** : ont défini la confiance comme « *c'est la croyance mesurée par un trustor (qui accorde sa confiance)en ce qui concerne la compétence, l'honnêteté, la sécurité et l'habilité d'un trustée (à qui on fait confiance) dans un contexte*

donné. »

— **Daubert et al [24]** ont défini « *la confiance dans le contexte de l'IoT comme la confiance des appareils, la confiance des entités et la confiance des données ; où l'informatique de confiance et la confiance de calcul pourraient être utilisées pour établir la confiance des appareils. la confiance d'entité fait référence au comportement attendu des participants tels que des personnes ou des services. et les données de confiance peuvent être dérivées de sources non fiables par agrégation ou peuvent être créées à partir de services IoT où les données nécessitent une évaluation de la confiance.* »

Donc à travers ces définition on peut 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.

1.3.7.1.2 Objectifs De La Confiance

Yan et al [58] ont mis en évidence les objectifs auxquels la gestion de la confiance dans l'IoT devrait répondre. Ces objectifs sont résumés comme suit

1. **Relation de confiance et de la décision (Trust Relationship and Decision (TRD)) :** une relation de confiance est basée sur le contexte qui indique toutes les informations qui définissent la situation des acteurs impliqués. Ainsi, la relation de confiance n'est pas absolue. En d'autres termes, l'objet de la confiance, l'environnement de confiance (par exemple, le temps et le lieu), le rôle des acteurs évolués et le risque de confiance sont définis a priori. Par exemple, un a trustor (qui accorde sa confiance) peut faire confiance à un trustee(à qui on fait confiance) pour transférer un paquet de données dans un contexte ; cependant, le même trustor ne peut pas faire confiance à un trustee pour effectuer une autre tâche dans un autre contexte.
2. **La confiance de la perception des données(Data perception trust (DPT)) :** la fiabilité des données détectées et collectées doivent être garanties. Dans ce contexte, les propriétés objectives du dépositaire doivent être prises en compte dans la couche de détection physique.
3. **Fusion de données et confiance minière(Data fusion and mining trust (DFMT)) :** les données détectées doivent être traitées et analysées de manière précise et fiable tout en garantissant la fiabilité et la préservation de la confidentialité.
4. **Confiance en matière de transmission et de communication des données(Data transmission and communication trust (DTCT) :) :**les données détectées et traitées doivent être transmises et communiquées en toute sécurité et de manière fiable. Ainsi, un routage basé sur la confiance et une gestion sécurisée des clés sont

nécessaires pour répondre à l'objectif de confiance de transmission de données et de communication.

5. **préservation de la confidentialité (Privacy preservation (PP)) :** les utilisateurs et la confidentialité des données sont des problèmes clés qui doivent être résolus pour atteindre les objectifs de confiance.
6. **Qualité des services IoT (Quality of IoT services(QIoTS)) :**la qualité des services IoT doit être assurée tout en maintenant un haut niveau de sécurité.
7. **La sécurité et robustesse du système (System security and robustness(SSR)) :**la fiabilité contre les attaques et la disponibilité du système IoT doivent être assurées pour gagner la confiance des utilisateurs.
8. **Généralités (Generality (G)) :**il est plus souhaitable d'avoir un système générique de gestion de la confiance, qui ne dépend ni du contexte ni d'autres exigences spécifiques.
9. **La confiance d'identité (Identity Trust (IT)) :** la confiance dépend de l'identité. En fait, avoir une identité permet de construire l'histoire des interactions liées à cette identité.

1.3.7.1.3 La confiance Dans SIoT

Systeme SIoT est implique des choses connectées les unes aux autres via Internet et les réseaux sociaux se développent énormément chaque année et donc les utilisateurs malveillants se développent également de ce fait chaque nœud doit calculer la confiance entre ces voisins afin de permettre des communications fiables, un moyen de communication sécurisé entre les nœuds d'un SIoT peut être atteint en gérant la confiance entre les nœuds [2]. En conséquence la gestion de la confiance est une caractéristique importante des systèmes de réseau tels que SIoT.

1.3.7.1.4 Propriétés De La confiance

Dans la littérature, la confiance a été calculée de plusieurs manières en fonction des différents propriétés ces propriétés peuvent être résumées comme suit [4]

- **La confiance peut être directe :**cette propriété indique que la confiance est basée sur des interactions, des expériences ou des observations directes entre le trustor (qui accorde sa confiance) et le trustee(à qui on fait confiance).
- **La confiance peut être indirecte :**le trustor (qui accorde sa confiance) et le trustee(à qui on fait confiance) n'ont pas d'expérience ni d'interaction dans le passé. La confiance ici repose sur l'opinion et la recommandation d'autres nœuds. dans ce cas on a parler de confiance transitive.
- **La confiance peut être locale :**elle dépend du couple trustor (qui accorde sa confiance) / trustee(à qui on fait confiance) pris en compte et qui diffère d'un

couple à l'autre, ce qui signifie qu'un nœud (i) peut faire confiance à un nœud (j) si un autre nœud (k) peut se méfier du même nœud (j).

— **La confiance peut être globale :**la confiance globale également appelée réputation signifie que chaque nœud a une valeur de confiance unique sur le réseau qui peut être connue de tous les autres nœuds.
— **La confiance devrait être asymétrique :**ce qui signifie que deux personnes liées par une relation peuvent avoir différents niveaux de confiance. Le fait que A fasse confiance à B ne signifie pas que B devrait faire confiance à A [40].
— **La confiance devrait être subjective :** la confiance est intrinsèquement une opinion personnelle qui repose sur divers facteurs ou preuves, et dont certains peuvent avoir plus de poids que d'autres [29].
— **La confiance peut être objective :** dans certains cas, par exemple lorsque la confiance est calculée en fonction des propriétés de qualité de service d'un périphérique.
— **La confiance peut dépendre du contexte :** la confiance d'un nœud (i) dans un nœud (j) varie d'un contexte à l'autre.
— **La confiance peut être une propriété composite :** la confiance est en réalité une composition de nombreux attributs différents : la fiabilité, la fiabilité, l'honnêteté, la véracité, la sécurité, la compétence et la rapidité, qui peuvent être considérées en fonction de l'environnement dans lequel la confiance a été spécifiée. [29].
— **La confiance peut dépendre de l'histoire :** cette propriété implique que l'expérience passée peut influencer le niveau actuel de confiance [57].
— **La confiance doit être dynamique :** la confiance évolue de façon non monotone avec le temps. Il peut être périodiquement actualisé ou révoqué, et doit pouvoir s'adapter aux conditions changeantes de l'environnement dans lequel la décision de confiance a été prise [29].

1.3.7.1.5 Les éléments De La Confiance

La confiance contient plusieurs éléments chaque sa propriétés diffèrent sont illustre au suivant :

— **Honnêteté :** le degré de fiabilité des recommandations fournies par une entité [20].
— **Intérêt à la communauté :** déterminé par l'appartenance à la même communauté.
— **Interaction :** l'action menée en commun par des acteurs au sein d'un système [55].
— **Contrôle d'accès :** méthode de gestion de l'accès aux ressources [55].
— **Certificat :** document électronique qui associe une clef publique à une identité en

utilisant la notion de signature numérique [55].

— **Réputation :**comportement attendu d'une entité d'après des informations relatives à son comportement passé [5].
— **Recommandation :** une entité peut évaluer la qualité et la fiabilité d'une collaboration avec une autre entité et fournir cette information à une 3ème entité [5].
— **La coopérativité :** déterminé par l'interaction d'un nœud avec ses amis ou leurs amis.
— **Logique floue :**une extension de la logique booléenne avec des valeurs de vérité [30].

1.3.7.1.6 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 noeuds d'un réseau, dans le but d'assurer les objectifs de sécurité [42].

1.3.8 Taxonomie Des Modèles De Confiance Dans l'IoT Et SioT

Dans la littératures ,Différents critères d'analyse et de comparaison des différents modèles de gestion de confiance sont proposés, puis nous avons classés pour finir par une synthèse dans laquelle nous avons exposé leurs avantages et leurs inconvénients,

1.3.8.1 Critères de comparaison des solutions

Nous fonderons notre comparaison sur un ensemble de critères qui sont :

— **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 social des Objets, qui sont : la vie privée des utilisateurs (privacy), les données et les services. Les préoccupations sont les attaques pouvant perturber le système de gestion de confiance et ainsi causer une perte de précision dans l'évaluation de confiance.
— **Consommation énergétique :**la majorité des dispositifs du SIoT sont limités en termes de mémoire et des capacités énergétiques [45]. Alors, la gestion de confiance doit être à moindre consommation d'énergie.
— **Évolutivité (Scalabilité) :**c'est une caractéristique essentielle d'un modèle de confiance dans SIoT. Elle permet d'assurer un correct fonctionnement lors de changement dynamique de la taille du réseau [47].
— **Précision dans le calcul de la confiance :**représente le degré de similarité entre le score de confiance d'un nœud calculé par le système de gestion de confiance avec la confiance effective qui doit être attribuée au nœud.

— **Monitorage :**représente la capacité de suivi du comportement de tout objet, ce qui permet d'utiliser l'historique de ses agissements pour calculer avec précision son score de confiance.

1.3.8.2 Classification aux modèles de gestion de confiance

La gestion de confiance considère comme une solution aux problème de sécurité dans IoT et SIoT , il est nécessaire de faire une distinction entre la gestion de confiance et la modélisation de confiance (décrit l'établissement de la confiance et technique de calcule ensuite il estimer le niveau de fiabilité entre les appareils au sein d'un système)

1. **modèles proposé par Moyano et al** Moyano et al [38], ont présenté deux classes : **les modèles de décision et les modèles d'évaluation.**

   La première classe comprend : les modèles de politique et les modèles de négociation, tandis que la seconde classe comprend : les modèles de propagation (flux), les modèles de réputation et les modèles de comportement.

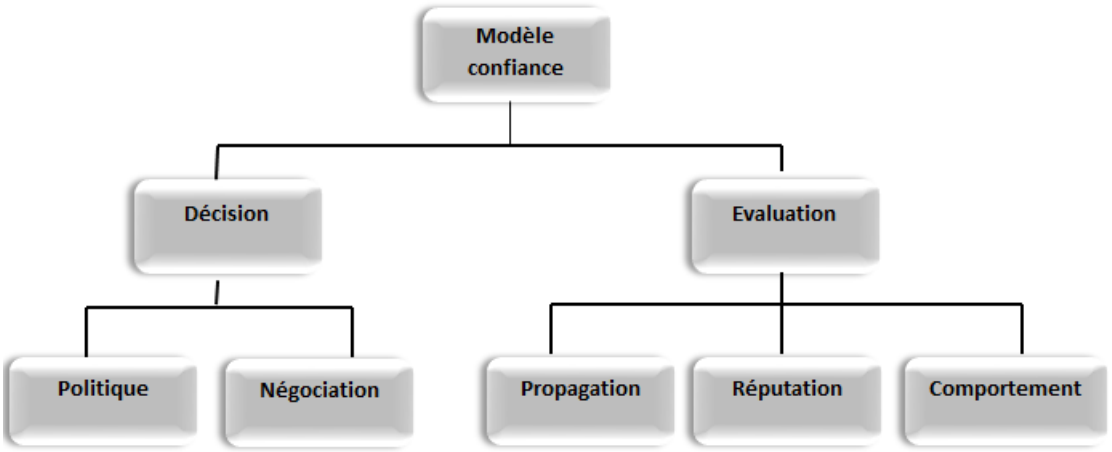

FIGURE 1.9 – Modèles de confiance selon Moyano et al[38]

(a) **Modèles de décision de confiance :** ces modèles apportent des solutions unifiées pour la décision de contrôle d'accès et la gestion du processus d'authentification et d'autorisation en les transformant en une seule tâche.

— **Modèles de politique :** le but de ces modèles est d'accorder l'accès aux ressources en utilisant les conditions prédéfinies dans les politiques.

— **Modèles de négociation :** dans ces modèles, deux entités effectuent un échange d'informations d'identification et de politiques, étape par étape, guidé par la négociation jusqu'à ce qu'elles décident de se faire confiance ou non.

(b) **Modèles d'évaluation de la confiance :** ces modèles sont également appelés modèles de confiance informatique. Contrairement aux modèles de décision,

les modèles d'évaluation utilisent la mesure pour quantifier la confiance. Ils évaluent et quantifient les attributs des entités tels que la fiabilité, l'honnêteté et l'intégrité pour calculer la valeur de confiance.

— **Modèles de comportement :** dans ces modèles, à chaque relation d'approbation est associée une valeur d'approbation indiquant le degré de confiance du trustor dans le trustee. Les valeurs de confiance sont calculées à l'aide des métriques de confiance choisies.

— **Modèles de propagation :** ces modèles indiquent la manière dont une entité diffuse les informations de confiance à d'autres entités. La propagation de la confiance peut être distribuée ou centralisée [32] ;

Distribuée : les entités calculent et propagent l'observation de confiance à d'autres entités de manière autonome. L'entité centralisée n'est pas nécessaire.

Centralisée : les entités ne peuvent pas propager l'observation d'approbation. Seule l'entité centralisée est responsable de la propagation de la confiance.

— **Modèles de réputation :** dans ces modèles, différentes entités échangent des informations de confiance et collaborent entre elles pour l'évaluation d'une entité. Ainsi, chaque entité prend en compte la recommandation des autres pour évaluer une autre entité.

2. **modèles proposé par Guo et al**

Guo et al [32] ont proposé une classification basée sur la combinaison des différents modèles suivants. : **composition de confiance, propagation de confiance, agrégation de confiance et mise à jour de confiance et formation.**

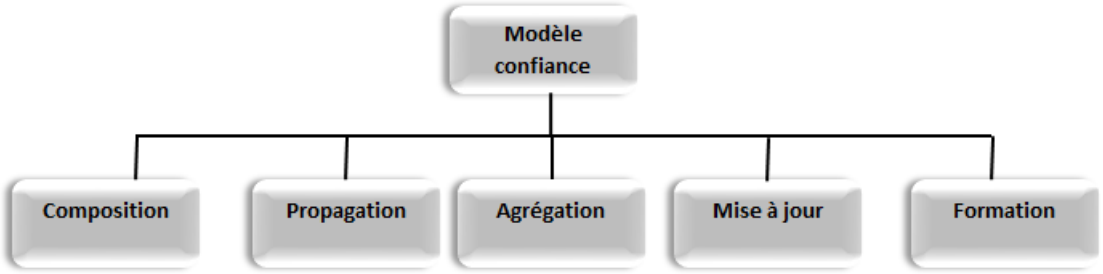

FIGURE 1.10 – Modèles de confiance selon Guo et al[32]

(a) **Modèles de composition :** dans ces modèles, les entités doivent savoir quelles propriétés de confiance utiliser dans le calcul de confiance. Les modèles de composition incluent des modèles de confiance de qualité de service (QoS) et des modèles de confiance sociale.

Modèles de confiance de qualité de service :la confiance QoS fait référence au niveau d'attente d'une entité selon laquelle une autre entité IoT est capable de réaliser correctement ses fonctionnalités. Ces modèles utilisent certaines propriétés de confiance telles que la compétence, la coopération, la fiabilité et la capacité d'achèvement des tâches pour mesurer les valeurs de confiance [15]

Modèles de confiance sociale : la confiance sociale découle de la relation sociale entre les propriétaires d'appareils IoT et se mesure en termes d'intimité, d'honnêteté, de confidentialité, de centralité et de connectivité, etc. La confiance sociale est particulièrement répandue dans les systèmes sociaux IoT où les appareils IoT doivent être évalués non seulement pas la confiance QoS , mais aussi basée sur le degré de confiance de leurs propriétaires [15].

(b) **Modèles de propagation :**déjà définis dans les sections précédentes.

(c) **Modèles d'agrégation :**indiquent la meilleure façon d'agréger les informations de confiance évaluées par l'entité elle-même (évaluation directe) ou par d'autres entités (évaluation indirecte) [15]

Dans [4] l'agrégation de confiance consiste à agréger des observations de confiance pour obtenir une valeur convergente unique. les principaux techniques d'agrégation étudiées sont la somme pondérée statique (SWS), la somme pondérée dynamique (DWS), le modèle bayésien (BM) et la logique floue (FL).

(d) **Mise à jour :**la mise à jour de confiance concerne le moment où la confiance doit être recalculé. En général, il existe deux schémas : schéma basé sur les événements et schéma basé sur le temps.[25]

Axé sur les événements : dans le schéma basé sur les événements, toutes les données de confiance d'un nœud sont mises à jour après une transaction ou un événement.

Axé sur le temps :dans le schéma basé sur le temps, les observations de confiance sont collectées périodiquement et la confiance est mise à jour en appliquant une technique d'agrégation de confiance.

(e) **Modèles de formation :**ces modèles indiquer le calcul de la confiance est basée sur une seule propriété de confiance (Single-trust) ou si elle est basée sur l'utilisation des propriétés multiples (Multi-trust). En outre, les modèles de formation devraient indiquer les poids à mettre sur les propriétés de la confiance sociale et de qualité de service pour former la confiance [15].

1.3.8.3 La Gestion De Confiance Dans l'SIoT Et Iot

La gestion de confiance est définie comme étant l'activité de création de systèmes et de méthodes pour permettre aux utilisateurs de faire des évaluations et de prendre des

décisions concernant la fiabilité des opérations, et de leur permettre ainsi qu'aux propriétaires du système d'augmenter et représenter correctement la fiabilité de leur système [35].

1. **Gestion de services basée sur la confiance pour les systèmes SIoT :**

   Chen et al.[21] ont présenté de gestion de confiance pour SIoT autonome, adaptif et distribué basé sur trois paramètres : **l'honnêteté**, **la coopératives** et **l'intérêt à la communauté** suffisants pour la résistance aux attaques .

   Le calcul de la confiance est effectué par des processus distribués et implémentés dans chaque objet, utilisant des sommes pondérées avec des coefficients dynamiques prenant en compte les expériences subjectives ainsi que les recommandations d'autres objets, tout en accordant un poids supérieur aux évaluations les plus récentes. La propagation et la mise à jour de la confiance s'effectuent après chaque interaction.

   Les évaluations de confiance des objets et celles attribuées à d'autres nœuds sont échangées, sachant qu'un objet ne garde en mémoire que celles des objets avec lesquels il a interagit.

   — **Avantages :**

   - Une modeste consommation en énergie due à l'utilisation de simples calculs (sommes pondérées) combinés avec une mise à jour de confiance orientée événement, ce qui diminue le nombre de messages échangés entre les noeuds.
   - Le modèle s'adapte bien à l'environnement dynamique en ajustant avec précision les meilleurs paramètres de confiance.

   — **Inconvénients :**

   - Le monitorage n'est pas assuré, étant donné l'absence d'infrastructure centralisée pour la sauvegarde de la réputation de chaque objet

2. **Gestion de la Confiance dans le SIoT :** Michèle Nitti et al [41] ont proposé deux modèles de gestion de confiance pour le SIoT, le 1ère est subjectif, le 2 ème objectif. Les deux utilisent la QoS ainsi que les caractéristiques du SIoT pour la composition de la confiance.

   (a) **Gestion de confiance subjective :** Chaque noeud calcule la fiabilité de ses amis a a base de sa propre expérience et de l'opinion de ses amis avec fournisseurs de service potentiels. la mise à jour des valeurs de confiance est orientée événement, telle que chaque interaction entre 2 nœuds est suivie d'une évaluation mutuelle des valeurs de confiance.

   — **Avantages :**

   - Résiste aux attaques de type"Self-Promoting"(SPA), "Bad-Mouthing"(BMA) et "Ballot-Stuffing"(BSA), grâce à l'utilisation de la crédibilité comme poids pour les recommandations.
   - Garantit l'évolutivité par sa nature distribuée

— **Inconvénients :**

- N'est pas adapte dans un environnement dynamique où les intérêt peuvent évaluer dans le temps(réponse transitoire plus lente).

- Le monitorage n'est pas possible à cause de l'absence de stockage centralisé des valeurs de confiance des noeuds du réseau .

(b) **Gestion de confiance objective :**

Les informations sur chaque noeud sont distribues et stockées a laide d'une structure de table de hachage distribuée (DHT) de sorte pour touts les noeuds puisse utilise les mêmes informations .la mise à jour des informations sauvegardées dans la DHT est effectuée après chaque interaction, tel que chaque nœud A recevant un service de la part du nœud B, émet un rapport décrivant le service fourni.

— **Avantages :**

- Permet de retirer le fardeau de calcul aux noeuds du réseau, ce qui implique une moindre consommation de ressources.

- Assure le monitorage grâce au stockage des informations de confiance de chaque noeud du réseau et leur disponibilité .

— **Inconvénients :**

- Ne résiste pas aux attaques de type "On-Off"(OOA), ce qui cause une perte de précision lors du calcul de la confiance.

3. **Modèle de confiance fondé sur la réputation et la garantie pour SIoT** Hannan Xiao et al [56] ont proposé un modèle hiérarchique de gestion de confiance pour le SIoT utilisant deux paramètres :

(a) **La réputation :**employée pour déterminer le niveau de fiabilité d'un nœud dans l'accomplissement d'un service donné ;

(b) **Le crédit :**fait office de commission à céder pour obtenir un service digne ou de caution dans le cas contraire afin de détecter les nœuds malicieux ;

La gouvernance du système est assurée au niveau de la couche application en utilisant une chaîne de serveur de deux types différents :

— **Le premier type :**

représente les serveurs de réputation chargés du calcul, la mise à jour et la propagation des valeurs de réputation des nœuds du réseau ;

— **Le second type :**

représente les serveurs de bases de données prenant en charge la découverte de services ainsi que le choix des meilleurs chemins pour y'accéder :

i. **Envoi d'une requête :**un Demandeur l'envoie au gestionnaire de confiance à travers son point d'accès dans laquelle il indique le service, la commission qu'il est prêt à payer en échange de sa réalisation, ainsi que le

forfait que le fournisseur lui cédera si sa réalisation est jugée de mauvaise qualité.

ii. **La réception de la requête :**le gestionnaire de confiance interroge le serveur de bases de données pour avoir l'ensemble des objets pouvant fournir ce service, puis sélectionne parmi eux l'objet qui a la réputation la plus élevée.

iii. **Fourniture de service :**l'objet sélectionné fournit le service au demandeur , qui procède après à l'évaluation du QoS reçu qui sera envoyée sous forme de rapport au serveur de réputation.

Notes : En cas de réalisation d'un bon service, le Demandeur de service paye la commission convenue au fournisseur de service , et sinon le fournisseur de service cède un forfait qui est une sorte d'indemnisation. Si un objet malicieux fournit de faux rapports à propos d'un objet, alors ce dernier conteste auprès du gestionnaire de confiance afin que l'émetteur du rapport soit sanctionné.

— **Avantages :**
- Faible consommation d'énergie des nœuds.
- Les nœuds sont exempts de services de calcul de réputation et de découverte de chemin .

— **Inconvénients :**
- Le critère d'évolutivité n'est pas garanti.
- Aucun moyen précis de décider si un service reçu est bon ou mauvais

4. **Gestion dynamique de la confiance pour des communications sécurisées dans l'internat social des objets (SIoT)**

Meena Kowshaly et al [36] ont proposé un modèle de gestion de confiance dynamique pour les communication sécurité dans (SioT) basé sur quatre paramétré telles que **l'honnêteté, la coopération, l'intérêt de la communauté et l'énergie d'un nœud** sont prises en compte pour le calcul de la confiance.

En utilisant ces propriétés,la confiance directe et la confiance indirecte sont calculées. La confiance calculée est analysée en fonction de divers facteurs de pondération afin de maximiser les performances de l'application et d'établir une communication sécurisée ,Le processus se déroule selon cinq phases :

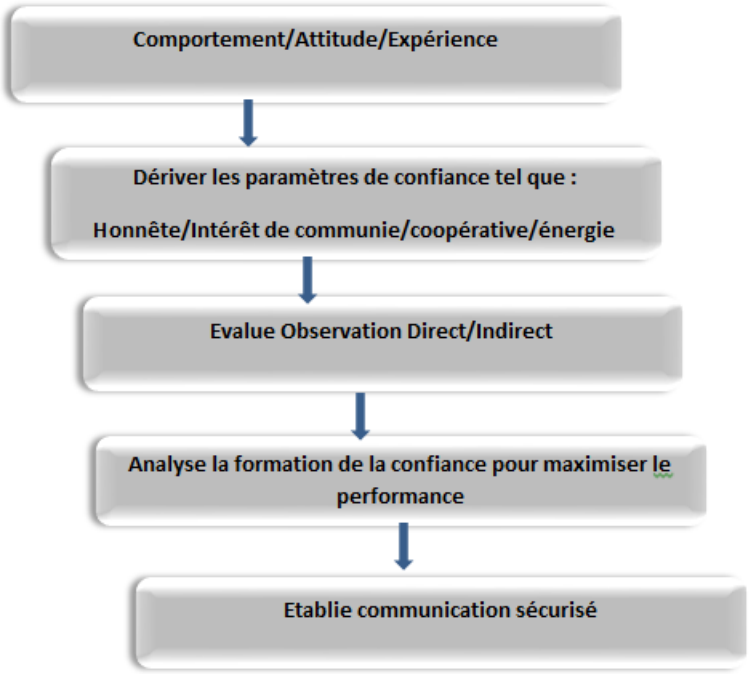

FIGURE 1.11 – Processus d'obtention de la confiance [36]

Les paramètres de confiance sont utiles pour caractériser un nœud en fonction de son **comportement**, de son **attitude** et de **son expérience**.

- chaque propriété de confiance (honnêteté, coopérative, l'intérêt communautaire et de l'énergie) est complémentaire à l'autre et doit donc être évaluée séparément.

(a) **Honnêteté :**l'honnêteté d'un nœud dans la plage (0,1) est considérée comme un facteur primordial car un nœud honnête est supposé toujours donner des recommandations correctes et correctes sur ses voisins , de plus il garantit que le noeud n'est pas malveillant

(b) **Coopérative :** dans un environnement SIoT, la coopérative des nœuds peut être prédite par ses liens sociaux. Les nœuds socialement coopératifs améliorent les performances de système. Chaque appareil objet possède une liste d'amis susceptibles d'être coopératifs. Cette liste sera mise à jour périodiquement par les propriétaires.

(c) **L'intérêt communautaire :** les objets sont classés en fonction de leurs relations parentales,de leurs relations de travail(CWOR) ou de colocalisation(CLOR). Les objets ayant le même intérêt communautaire sont censés interagir très souvent,ce qui entraîne une augmentation des performances des applications.

(d) **L'énergie :**l'énergie d'un nœud joue également un rôle important dans la communication et le partage d'informations.presque tous les objets de SIoT sont des objets à faible consommation et des appareils moins efficaces en énergie. Ainsi, l'énergie d'un nœud doit recevoir une importance primordiale à des fins

de collaboration

— **Avantages :**

- Calculer dynamiquement la valeur de confiance des noeuds utilise code secret et la facteur de fiabilité pour assure une communication sécurité entre les noeuds(la confiance et authentification rendent SIoT plus robuste).

- Résiste aux attaques de type SPA BMA, BSA OOA grâce l'utilisation de l'honnêteté comme paramètre lors du calcul de la confiance .

— **Inconvénients :**

- Les nœuds sont responsable pour calculer la valeur de confiance (plus de consommation d'énergie).

- Le monitorage n'est pas possible 'a cause de l'absence de stockage centralisée des valeurs de confiance des noeuds du réseau

1.3.9 Discussion et comparaison

Dans la sous-section précédente, on a parler sur la majorité des travaux dans le domaine de la gestion de la confiance sur les environnements SIoT. On a souligne également leurs avantages et leurs inconvénients.

Dans cette section, on a fait une classification de ces travaux connexes en fonction de critères spécifiques. Dans le 1ère tableau on a classé les travaux en fonction des propriétés de confiance adoptées. Dans le 2ème tableau,on a fait une Comparaison entre différents systèmes de gestion de confiance basés sur la fonction objectifs de confiance Dans le 3 ème tableau,nous les comparons en fonction de leur volonté de répondre aux critères spécifiques du SIoT. Et enfin, dans le 4ème tableau , on a classer selon les dimensions du modèle de confiance.

	Direct	In_ direct	Local	Global	Sub_ jectif	Ob_ jectif	His_ torique	Contexte	Dyna_ mique	Composite
[41]	No	Yes	No	Yes	Yes	Yes	No	Yes	No	Yes
[21]	Yes	No	Yes	No	Yes	Yes	No	Yes	Yes	Yes
[56]	Yes	Yes	No	Yes	Yes	No	No	No	No	Yes
[36]	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes

TABLE 1.1 – classification des propriétés de confiance basées sur les œuvres existantes

	TRD	SSR	DTCT	DPT	DFMT	QIoTS	PP	G	IT
[41]	Yes	Yes	No	No	No	No	No	Yes	Yes
[21]	Yes	Yes	No	No	No	No	No	Yes	Yes
[56]	Yes	Yes	No	No	No	No	No	Yes	Yes
[36]	Yes	Yes	Yes	No	No	Yes	No	Yes	Yes

TABLE 1.2 – Comparaison entre différents systèmes de gestion de la confiance en fonction des objectifs de la fonction de confiance

	Résistance aux Attaque	Consommation énergétique	Évolutive	Précision dans le calcul	Monitorage
[41]	Yes	No	No	No	Yes
[56]	Yes	Yes	No	No	Yes
[21]	Yes	Yes	Yes	No	No
[36]	Yes	No	Yes	Yes	No

TABLE 1.3 – Classification des ouvrages existants en fonction des critères SIoT considérées

	Composition	**Propagation**	**Agrégation**	**mise a jour**	**Formation**
[41]	QoS/Social	Distribue	somme pondéré statique(SWS)	Évènement	Multi-valeur
[21]	QoS/Social	Contralisé	(SWS)/(DWS)	Évènement	Multi-valeur
[56]	Social	Distribué	la logique floue(FL)	Évènement	Multi-valeur
[36]	QoS/Social	Distribué	somme pondéré dynamique(DWS)/(SWS)	Évènement	Multi-valeur

TABLE 1.4 – Classification des ouvrages existants en fonction des dimensions du modèle de confiance

Cette comparaison nous a permet d'affirmer qu'il y a beaucoup de progrès dans le domaine du gestion de la confiance dans les systèmes SIoT. Cependant, la majorité des travaux connexes prouvent leur efficacité face aux attaques liées à la confiance. Plus de ça le modèle [36] il prenne en compte la nouvelle structure et les nouvelles contraintes liées au SIoT(Dynamique .authentification)qui a rendu le système plus robuste . cependant ce modèle a établit une conversation sécurisé et fiable entre les noeuds en utilise des simple codes secrets ,assurée l'évolutivité ,malheureusement l'efficacité énergétique est pratiquement ignorée(car les noeuds de faible puissance et moins économique d'énergies sont responsables de calculer la valeur de confiance). pour cette raison la on a réalisé une architecture dont le quelle le serveur est responsable de faire le calcul qui est permet de retirer le fardeau de calcul aux noeuds du réseau, ce qui implique une moindre consommation de ressources.et assure le monitorage grâce au stockage des informations de confiance de chaque noeud du réseau et leur disponibilité.

1.4 Conclusion

Dans ce chapitre, nous avons souligné tout d'abord un aperçu du paradigme SIoT,ses avantages et ses évolutions et sa structure de réseau. puis, nos abordé la notion de confiance et ses concepts associés et l'importance de la gestion de la confiance dans l'environnement SIoT.et finalement nos exposé une classification des modèles de confiance SIoT basée sur des critères spécifiques.
Dans le chapitre suivant, on a parler sur les principales attaques liées à la confiance et les solution qui ils proposent pour éviter ces attaques.

Chapitre 2

Les attaques dans internet social des objets(SIoT)

2.1 Introduction

Différents modèles d'évaluation de la confiance sont proposés pour garantir la confiance dans différents types de systèmes. Leur rôle consiste à fournir (calculer) un score de confiance, qui aidera les acteurs à prendre la décision d'invoquer ou non les services fournis par d'autres participants. Il existe plusieurs attaques qui sont conçues pour briser spécifiquement cette fonctionnalité. Dans ce chapitre nous allons entamer sur les différent types attaques qui sont spécialement conçus pour perturbez les systèmes de gestion de confiance et les différents solutions ont été proposées dans la littérature pour atténuer ces attaques.

2.2 Définition une Attaque

Une attaque est un comportement malveillant établi par un nœud malveillant lancé pour briser les fonctionnalités de base d'un système donné et pour atteindre diverses fins malveillantes. Un nœud malveillant, en général, peut effectuer des attaques de protocole de communication pour perturber les opérations du réseau.[3]

2.3 Motivation des attaques

Les motivations des attaques peuvent être de différentes sortes[16] :

— obtenir un accès au système
— voler des informations, tels que des secrets industriels ou des propriétés intellectuelles
— troubler le bon fonctionnement d'un service
— récupérer des données bancaires ;
— s'informer sur l'organisation (entreprise de l'utilisateur, etc.)

— utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée.

2.4 Les différentes types attaques

1. **Attaque par déni de service (Denial of Service(DoS))**

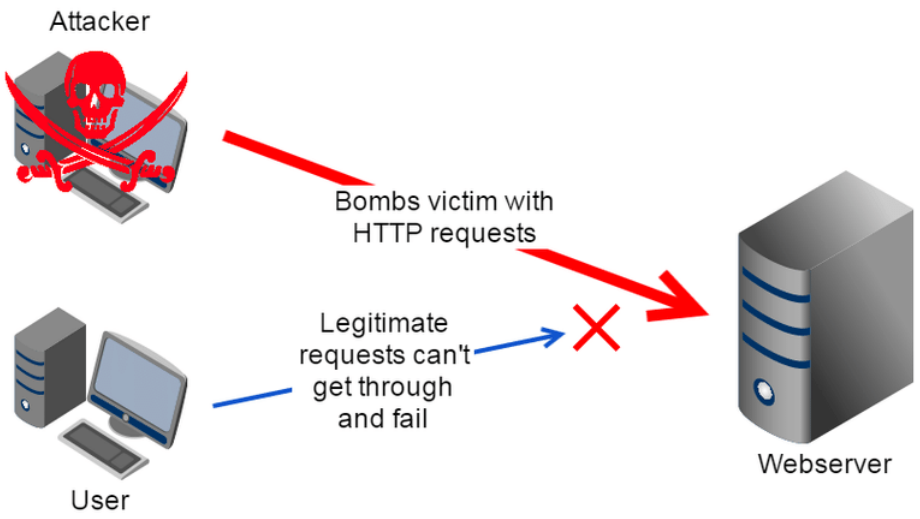

FIGURE 2.1 – Attaque dénis de service (DoS)[52]

(a) **Définition :**une « attaque par déni de service » (DoS) est un type d'attaque visant à rendre indisponible pendant un temps indéterminé les services ou ressources d'une organisation. Il s'agit la plupart du temps d'attaques à l'encontre des serveurs d'une entreprise, afin qu'ils ne puissent être utilisés et consultés [52].

(b) **Le but de ce d'attaque :**les attaques par déni de service sont un fléau pouvant toucher tout serveur d'entreprise ou tout particulier relié à internet. Le but d'une telle attaque n'est pas de récupérer ou d'altérer des données, mais de nuire à la réputation de sociétés ayant une présence sur internet et éventuellement de nuire à leur fonctionnement si leur activité repose sur un système d'information [16].

(c) **Les diffèrent types :**on distingue habituellement deux types de dénis de service [16] :

— **Les dénis de service par saturation,** consistant à submerger une machine de requêtes,afin qu'elle ne soit plus capable de répondre aux requêtes réelles

— **Les dénis de service par exploitation de vulnérabilités,** consistant à exploiter une faille du système distant afin de le rendre inutilisable.

Lorsqu'un déni de service est provoqué par plusieurs machines, on parle alors de «Déni de Service Distribué(DDoS) »

(d) **Le principe de ce d'attaque :**le principe des attaques par déni de service consiste à envoyer des paquets IP afin de provoquer une saturation ou un état instable des machines victimes et de les empêcher ainsi d'assurer les services réseau qu'elles proposent,la figure 2.1 montre que la fonctionnalité de ce type attaque [16].

(e) **Protéger d'un déni de service :**pour se protéger de ce type d'attaque, il est nécessaire de récupérer sur internet des correctifs logiciels (patchs) «http ://windowsupdate.microsoft.com/»

2. **L'usurpation d'adresse IP (IP spoofing)** L'usurpation d'adresse IP est une technique consistant à remplacer l'adresse IP de l'expéditeur IP par l'adresse IP d'une autre machine[54] ,comme l'illustre la figure 2.2 . et ainsi cette technique permet à un pirate d'envoyer des paquets anonymement.

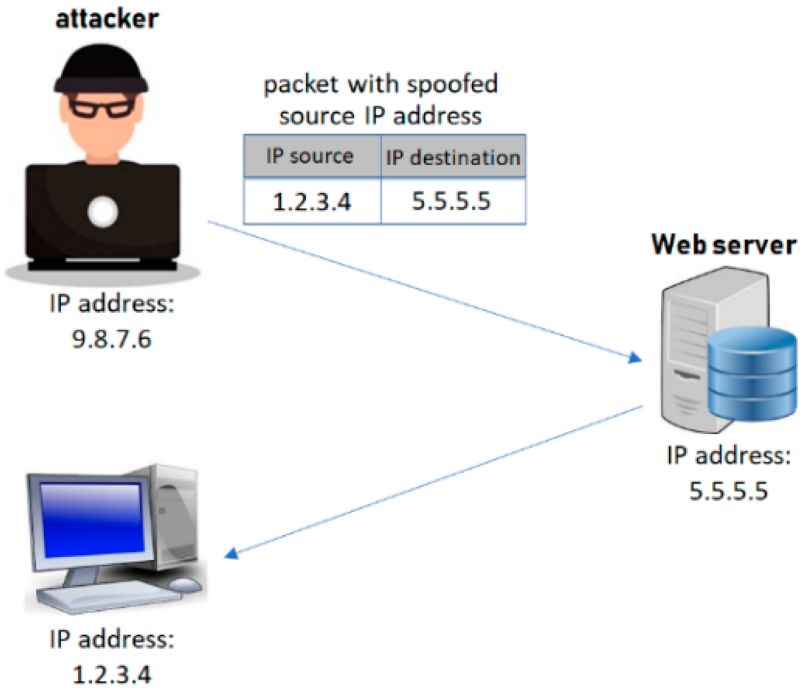

FIGURE 2.2 – Attaque IP Spoofing [54]

2.5 Les attaques contre le système de gestion de la confiance

Il existe différents types d'attaques qui peuvent affecter un système de gestion de confiance et compromettre son authenticité. on a considéré six types d'attaques qui sont discutés ci-dessous.

Ces attaques sont globalement classées en deux catégories [19], comme le montre la figure suivante :

— **Les attaques individuelles**, dans lesquelles les nœuds peuvent mener l'attaque sans la coopération d'autres nœuds

— **Les attaques de collusion,** dans lesquelles les nœuds malveillants s'entendent entre eux pour porter sur l'attaque.

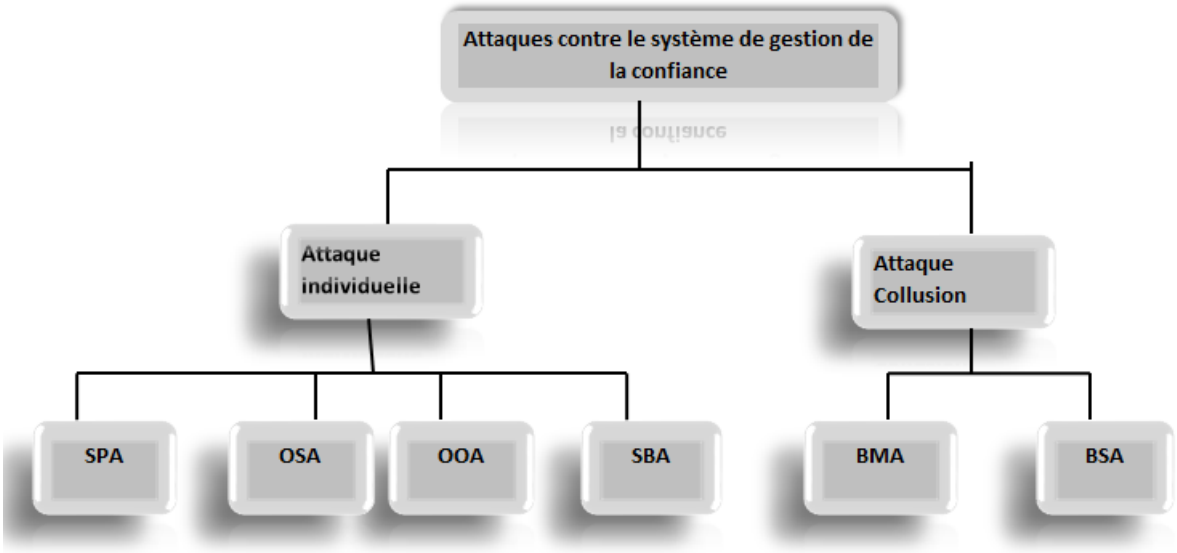

FIGURE 2.3 – Types d'attaques contre les systèmes de gestion de la confiance[19]

Dans ce type d'attaques, un noeud malveillant peut promouvoir sa propre réputation pour accéder à des fonctions supérieures ou perturber le système de manière à réduire son efficacité. Ainsi, un dispositif IoT malveillant (sous contrôle d'un propriétaire malveillant) peut effectuer les attaques suivantes [1].

1. **Les attaques individuelles**

   (a) **Self Promoting Attacks (SPA) :** est une attaque dans laquelle des noeuds malveillants, fournissant des services de mauvaise qualité, tentent de renforcer leur réputation (en s'octroyant des votes élevés) afin d'être sélectionnés comme fournisseurs de services[33].

   (b) **Attaques on-off (OOA) :** le nœud malveillant fournit alternativement un bon et un mauvais service. Le but est de garder sa bonne réputation et il peut compromettre le réseau en fournissant une bonne recommandation pour les nœuds malveillants ou une mauvaise recommandation pour les nœuds de confiance. Ces attaques semblent plus difficiles à détecter [25].

   (c) **Selective Behavior Attack (SBA) :** dans cette attaque, un nœud malveillant fonctionne bien pour un service particulier ou des types de services

particuliers, alors qu'il fonctionne mal pour d'autres services, par exemple des services gourmands en ressources [49]. Ce faisant, le nœud maintient son niveau de réputation tout en se comportant malicieusement [51].

(d) **Opportunistic Service Attack (OSA) :** Dans ce type d'attaque, les nœuds malveillants saisissent l'opportunité de savoir quand fournir un bon service et quand fournir un mauvais service. Lorsqu'un nœud remarque que sa réputation diminue, il commence à fournir un bon service afin d'augmenter sa réputation [23]. Lorsque sa réputation augmente, il profite alors de cette opportunité pour fournir de mauvais services ou s'entendre avec d'autres nœuds malveillants afin de mener à bien BSA ou BMA [31].

2. **les attaques de collusion :**

(a) **Bad Mouthing Attacks (BMA) :** est une attaque dans laquelle des noeuds malveillants tentent de détruire la réputation des noeuds bienveillants (en leur donnant de mauvais votes) afin de diminuer leurs chances d'être sélectionnés comme fournisseurs de services[1].

(b) **Ballot Stuffing Attacks (BSA) :** est une attaque dans laquelle des noeuds malveillants tentent de promouvoir la réputation d'autres noeuds malveillants afin d'augmenter leurs chances d'être sélectionnés comme fournisseurs de services [3].

2.6 État de l'art

Dans ce tableau 2.1 qui montre les différents solutions ont été proposées dans la littérature pour atténuer ces attaques .

Travail	SPA	BMA	BSA	OSA	OOA	SBA
[21]	Honnêteté Métrique et mécanisme de rétroaction	Poids attribué pour contrôler l'impact et trouver des recommandations directes	Poids attribué pour contrôler l'impact et trouver des recommandations directes	La confiance directe et la confiance indirecte sont toutes deux considérées pour mesurer la fiabilité mesurer la fiabilité	NA	NA
[41]	Mécanisme de confiance directe et de rétroaction	Crédibilité pour l'évaluation des recommandataires	Crédibilité pour l'évaluation des recommandataires	Considérations de confiance directe à long terme et à court terme	Considérations de confiance directe à long terme et à court terme	NA
[56]	Commission et forfait fournis par le nœud récepteur à calculer la réputation	Commission et forfait fournis par le nœud récepteur à calculer la réputation	Commission et forfait fournis par le nœud récepteur à calculer la réputation	NA	NA	NA
[36]	Honnêteté Métrique utilise comme paramètre lors du calcul de la confiance	Poids attribué pour contrôler l'impact et trouver des recommandations directes	Poids attribué pour contrôler l'impact et trouver des recommandations directes	La confiance directe et la confiance indirecte sont toutes deux considérées pour mesurer la fiabilité	Honnêteté Métrique utilise comme paramètre lors du calcul de la confiance	Différent valeur de confiance calcule par différent type de service

TABLE 2.1 – Les différent solution pour éviter les attaque lié au confiances

‘

2.7 Conclusion

Nous avons évoqué dans ce chapitre les différentes solutions apportées par la littérature pour éviter au maximum les attaques à des comportements malveillants afin de détruire le réseau. Après avoir comparé ces solutions,
Nous concluons que le type fourni par[36] est le meilleur pour éviter le maximum les types attaquent lié aux gestions de confiance pour cela on a choisi ce modèle .

Chapitre 3

Conception

3.1 Introduction

Dans ce chapitre, nous visons à concevoir et à expérimenter un modèle de confiance dynamique pour les communications sécurité dans (SIoT) basé sur 4 paramétré telles que l'honnêteté, la coopération, l'intérêt de la communauté et l'énergie d'un nœud sont prises en compte pour le calcul de la confiance .
En utilisant ces propriétés, la confiance directe et la confiance indirecte. La sous-section suivante décrit l' architecture générale de SIoT, la seconde illustre l'architecture d'un mécanisme de gestion de la confiance et la troisième décrit les éléments de base du modèle de confiance et la quatrième décrit les attaques contre la gestions de confiance et encore l'algorithme DTrustInfer puis les diagrammes de séquence et a la fin une conclusion.

3.2 Architecture générale de SIoT

Sur la base des services et des composants définis ci-dessus, nous proposons une architecture généralisée à trois composants tel que :les Objet ;les Objet malveillant ;serveur. Comme le montre dans la figure 3.1

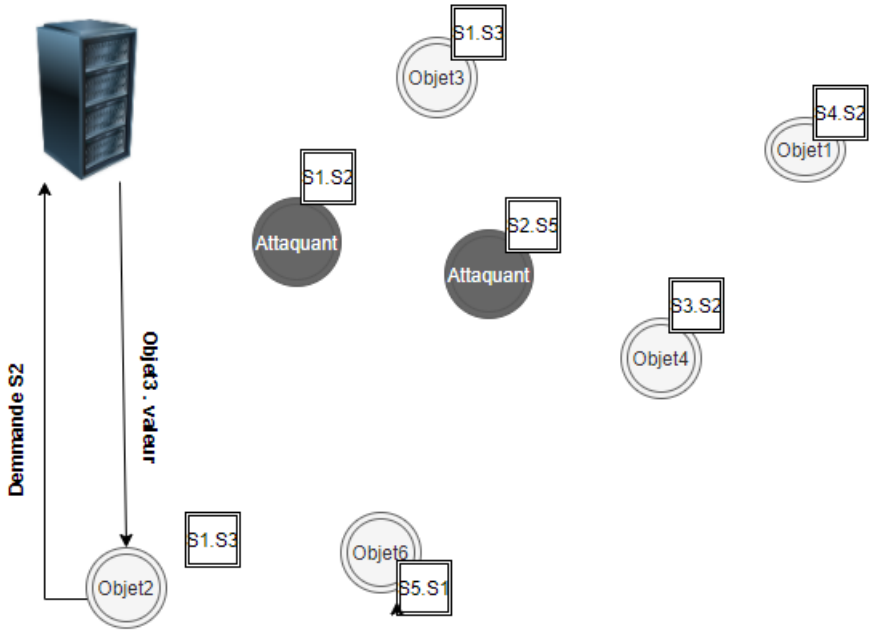

FIGURE 3.1 – Architecture générale de SIoT

3.2.1 Décomposition de l'architecture SIoT

Les composants de nos modèles et leur fonctionnalités sont décrits ci-dessous :

1. **Les Objet :** soit il s'agit du demandeur ou du fournisseur de services il représente les appareils et les dispositifs équipés de capteurs pour détecter et recueillir des informations sur l'environnement, Ces appareils peuvent collaborer et communiquer les uns avec les autres via internet [11].

2. **Les Objet malveillant :** il donne de mauvais services, de fausses références et de faux commentaires.le nœud malveillant peut alors être celui qui demande le service, celui qui fournit le service ou,celui qui donne son avis sur un autre nœud. Dans le premier cas, il fournit une rétroaction négative à chaque nœud impliqué dans la transaction ; dans le second cas, il fournit le mauvais service et devrait alors recevoir un retour négatif ; enfin, dans le troisième cas, il donne un avis négatif sur les autres nœuds.

3. **Le Serveur :** est responsable pour faire l'exécution des activités liées a la gestion de confiance a savoir(collecte d'information ,calcule la valeur de confiance,le stockage sa valeur et faire mise a jours).

3.3 Architecture d'un mécanisme de gestion de la confiance

La gestion de confiance est nécessaire dans deux scénarios [19] :

— Lorsqu'un nœud (nœud demandeur, disons ri) veut bénéficier d'un service particulier (d'un nœud fournisseur de services, disons sj)

— Lorsqu'un nœud (ri) reçoit des informations de un autre nœud (nœud fournissant des informations, (sj) .Il souhaite vérifier si ces informations peuvent être fiables ou non

Quel que soit le scénario qui se produit le système de gestion de la confiance aide (ri) à calculer la valeur de fiabilité de (sj)

La gestion de la confiance dans n'importe quel environnement comprend quatre phases, à savoir l' Établissement de la confiance, le propagation,la récompense et la punition,la mise à jour de la confiance qui sont illustrées à la figure 3.2. .

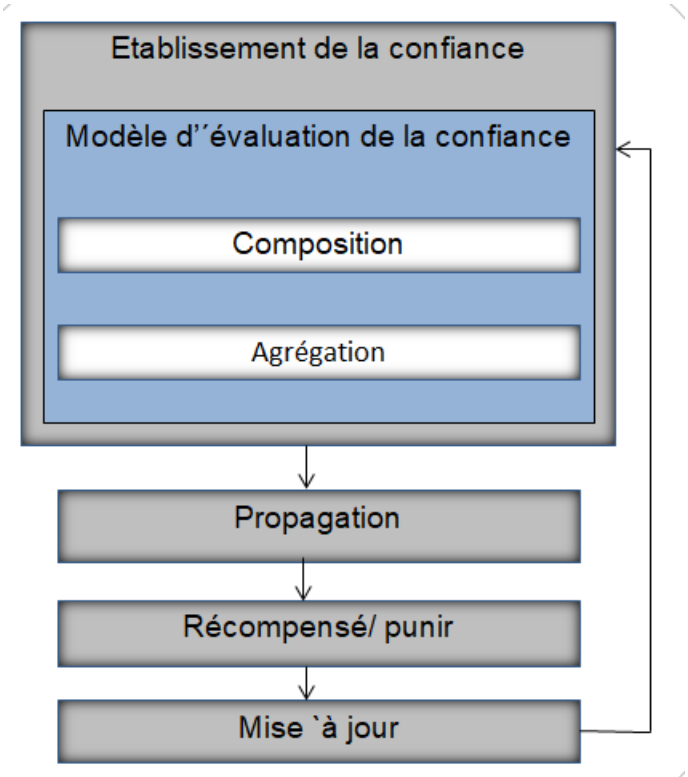

FIGURE 3.2 – Architecture d'un mécanisme de gestion de la confiance [1]

3.3.1 Gestion de la confiance

Les mécanismes de gestion de la confiance (MGC) permettent d'assurer le processus d'établissement, de propagation et rétroaction et de mise à jour de la confiance [32]. La figure 3.2 montre les différentes étapes d'un MGC. L'étape d'établissement de la confiance se base sur "un modèle d'évaluation de la confiance" qui est construit en deux premier

étapes [1] :

1. **L'étape de composition** consiste à sélectionner les facteurs à prendre en compte dans le calcul des valeurs de confiance.

   Plusieurs facteurs ont été proposés dans la littérature, dans ce modelé on a utilisé ces facteurs tel que : l'honnêteté, la coopération, les intérêts de communies et l'énergie... Ces derniers peuvent être classés selon différentes dimensions : (indirect /direct). Pour les mesurer, on a utilisé des informations relatives aux nœuds, telles que leur localisation ou leur historique d'interaction.

2. **L'étape d'agrégation** Cette méthode est utilisée pour agréger les valeurs des différents facteurs afin d'obtenir la valeur de confiance unique.A cette fin on utilise la moyenne pondérée (ajouter attributs des pondération a ces facteurs en fonction de leur importance ou leur pertinence).

3. **L'étape de propagation** Cette méthode est utilisée pour propager dans le réseau les valeurs de confiance obtenues après l'étape d'agrégation. Deux méthodes sont utilisées. Dans la méthode dite centralisée une entité centrale fait les différents calculs pour tous les nœuds du réseau. Dans la méthode dite décentralisée, chaque nœud fait ses propre calculs. On a utilise la méthode de propagation centralisée, arguant que les nœuds impliqués dans les réseaux SIoT ont une capacité limitée (en termes de de calcul, de stockage, etc. ...).

4. **Récompensé/ punir** Le nœud demandeur récompense ou punit le nœud fournisseur de services selon que son service était respectivement satisfaisant ou insatisfaisant. La récompense et la punition sont données sous forme d'augmentation ou de diminution, respectivement, de la valeur de fiabilité ou de la réputation du nœud du fournisseur de services ,on a utilisé la méthode basé sur un seuil [19].

5. **L'étape de mise à jour** Cette méthode est utilisée pour mettre à jour les valeurs de confiance. On a utilisé la méthode dirigée par les évènements, les mises à jour se font à chaque fois qu'un nouvel évènement se produit.

3.4 Éléments de base du modèle de confiance

Nous utilisons le modèle qui proposé par [36] ils utilisent les propriétés de confiance suivants telle que (l'honnêteté ,la coopération , l'intérêt de communie et l'énergie d'un nœud chaque propriété de confiance est complémentaire à l'autre et donc doit être évalué

- **Honnêteté :** Dans la gamme (0,1) considérée comme un facteur primordial car un nœud honnête est supposé donner toujours une bonne recommandation et correcte de ses voisins.et puis il garantit que le nœud n'est pas malveillant.

  Il est calculé comme le quotient entre le nombre d'interactions positives et le nombre total d'interactions (eq 3.1), les interactions positives sont des interactions ayant reçu des valeurs de vote élevée.

Le facteur honnêteté, combiné à d'autres facteurs, permet de révéler des attaques de type BMA, BSA, SPA .

$$D_{ij}^{honnête} = \frac{Nombre\ expérience\ positive}{Total\ des\ expériences\ collecté} \tag{3.1}$$

- **La coopérative** La coopérative des nœuds peut être prédite par ses liens sociaux. Les nœuds socialement coopératifs améliorent les performances de système
  Chaque objet possède une liste d'amis susceptibles d'être coopératifs. Cette liste sera mise à jour périodiquement par les utilisateurs.
  Il est calculé comme le quotient entre le nombre d'amis le noeuds demandeur (i) et le nombre d'amis le noeuds fournisseur de service (j)(eq 3.2).

$$D_{ij}^{coopération} = \frac{amis(i)\ \cap\ amis(j)}{amis(i)\ \cup\ amis(j)} \tag{3.2}$$

- **l'intérêt de communie :** Intérêt communautaire est un autre facteur qui permet la communication entre des objets d'intérêt commun .
  Les objets sont classés en fonction de leurs relations parentales, de leurs relations de travail(collaboration) ou de Co-localisation.Les objets ayant le même intérêt de la communauté sont censés interagir les uns avec les autres, ce qui entraîne souvent une augmentation des performances de l'application [36].
  Il est calculé comme le quotient entre le nombre d'amis le noeuds demandeur (i) et le nombre d'amis le noeuds fournisseur de service (j)(eq 3.2). ‘

$$D_{ij}^{l'intérêt\ de\ communie} = \frac{communauté(i)\ \cap\ communauté(j)}{communauté(i)\ \cup\ communauté(j)} \tag{3.3}$$

- **L'énergie** l'énergie d'un nœud joue également un rôle important dans la communication et le partage d'informations. Presque tous les objets de SIoT sont des objets à faible consommation et des objets moins efficaces en énergie. Ainsi, l'énergie d'un nœud doit recevoir une importance primordiale à des fins de collaboration.
  La raison pour laquelle l'énergie est considérée comme un facteur de confiance est que, si un nœud effectue une attaque de transfert sélectif On Off, son niveau d'énergie sera plus faible (puisque le nœud passe à l'état Off pendant les transactions essentielles) par rapport à d'autres pairs dans le groupe faisant la même tâche [37]

$$E\ résultat_j = E\ initial_j(t - \Delta t) – E\ consomme_j(\Delta t) \tag{3.4}$$

- **Centralité (Gij)** est représenté à quel point (pj)est central dans la «vie» de(pi)et non à quel point il est considéré comme central pour tout le réseau [40]. Cette

mesure empêche les nœuds malveillants qui créent de nombreuses relations dans le réseau aient des valeurs de centralisé élevées .

$$G_{ij}^{x} = \frac{|C_{ij}|}{|F_i| - 1} \tag{3.5}$$

- **Le facteur de fiabilité ($\mathbf{DP}_{ij}^{X}$)**
  Le facteur de fiabilité se situe dans la plage (0, 1) qui est obtenue par le fournisseur de services d'un autre environnement SIoT similaire. Le comportement du même nœud (historique) dans un environnement différent est utilisé pour évaluer la fiabilité [36].
  Le facteur de fiabilité sera égal à 0 si les mêmes objets ne participent nulle part dans le monde extérieur.
- **Valeur de rétroaction ($\mathbf{f}_{ij}$)**
  permet à un nœud pi de fournir une évaluation du service qu'il a reçu par le fournisseur pj, qui fait référence à chaque transaction et peut être exprimé on utilisant des valeurs dans une plage continue [0, 1] pour évaluer différents niveaux de satisfaction.

  Si demandeur est satisfaite alors
  La valeur de fiabilité +X
  Sinon
  La valeur de fiabilité –X

  X : valeur prédéterminé par lequel la fiabilité d'un nœud est être augmente ou diminué

Le tableau 3.1 illustre les paramètres utilisés pour calculer la confiance :

Paramètre	Signification
X	Honnête, l'intérêt communautaire, coopération,l'énergie
$\mathrm{D}_{ij}^{X}(t)$	la confiance direct de I vers J au temps t dans X
$\mathrm{R}_{kj}^{X}(t)$	Recommandation que le noeud K fournit au noeud I a propos du noeud J
$\mathrm{T}_{ij}^{X}(t)$	Confiance entre I etJ au temps T dans X
G_{ij}^{X}	Centralisé d'un noeud
$\mathrm{D}_{ik}^{X}(t)$	confiance direct entre I et K au temps T dans X
Dp_{ij}^{X}	Facteur de fiabilité
α, β, γ	Facteur de pensée
$\mathrm{T}_{ij}^{X}(t)(t - \Delta t)$	valeur de confiance passé
C_{ij}	amis commun entre I et J
F_i	Les amis de I

TABLE 3.1 – Les paramètres utilisés dans les formules de dérivation de la confiance

Lorsque les nœuds (i) et (j) interagissent directement l'un avec l'autre, la confiance est calculée comme suit :

$$T_{ij}^{X}(t) = \alpha T_{ij}^{X}(t)\ (t - \Delta t)\ +\ \alpha D_{ij}^{X}(t)\ +\ \beta G_{ij}^{X}\ +\ \beta\alpha DP_{ij}^{X} \tag{3.6}$$

où X = honnêteté, coopération, intérêt communautaire et énergie.dans cette équation le nœud (i) utilisera l'observation directe et sa confiance passée vers le nœud (j). Avec ces deux paramètres noeud (i) utilise aussi le facteur de la centralité et la facteur de fiabilité pour calculer la confiance.
Le nœud (i) n'aura aucune interaction directe avec le nœud (j), donc utilisera la recommandation de (k)vers (j) (nœud (k) est ami commun entre noeud(i) et (j) avec la valeur de centralisé plus élevé par rapport les autre amis commun entre noeud (i) et (j) et aussi nœud (k) déjà fait une transaction avec le nœud (j)) la confiance est alors calculée selon l'équation Suivante :

$$T_{ij}^{X}(t) = \gamma T_{ij}^{X}(t)\ (t - \Delta t)\ +\ \gamma D_{ik}^{X}(t)\ +\ \gamma R_{Kj}^{X}(t)\ +\ \beta G_{ij}^{X} \tag{3.7}$$

Il est possible que le nœud (k) soit malveillant :
Si le nœud (k) n'est pas malveillant alors

$$R_{Kj}^{X}(t) = D_{ik}^{X}(t) \tag{3.8}$$

Sinon le nœud(k)est malveillant alors
il peut effectuer de mauvaises attaques et les propager au nœud (i).
Pour éviter cela, le nœud (i) utilise la confiance directe pour accéder au nœud (k) $\mathrm{D}_{ik}^{X}(t)$

3.5 Les Attaques contre la gestions de confiance

Dans le réseau SIoT n'a pas toujours tous nœuds est honnête, des nœuds malveillants peuvent également être présents dans le réseau. Il existe de nombreux nœuds malveillants dans le réseau qui exécutent un comportement malveillant afin de détruire la fonction de base du réseau Ces noeuds peut être le demandeur, le fournisseur de services ou un nœud intermédiaire entre le demandeur et le fournisseur de services. Nous expliquerons chaque cas séparément ;

- Dans le cas du nœud malveillant qu'est le demandeur, dans ce cas, il existe de nombreux types d'attaques que nous avons mentionnés précédemment, et dans notre travail nous nous concentrerons sur le type **Bad Mouthing Attaques (BMA)** c'est une attaque dans laquelle des noeuds malveillants tentent de détruire la réputation des noeuds bienveillants (en leur donnant de mauvais votes) àfin de diminuer leurs chances d'être sélectionnés comme fournisseurs de services [1]
- Dans le cas où le nœud malveillant est le fournisseur de services, il envoie de fausses

informations au demandeur ou utilise le type attaqué **Self Promoting Attaques (SPA)** c'est une attaque dans laquelle des noeuds malveillants, fournissant des services de mauvaise qualité, tentent de renforcer leur réputation (en s'octroyant des votes élevés) afin d'être sélectionnés comme fournisseurs de services [33] .

— Dans le cas du nœud malveillant, il s'agit d'un nœud intermédiaire entre le demandeur et le fournisseur de services, de sorte qu'il ouvre le message entrant du fournisseur de services, le modifie, puis l'envoie au demandeur

3.6 L'algorithme DTrustInfer

Cette algorithme est proposé pour calcule la confiance sur la base d'une observation direct et indirect utilise d'un facteur de centralité et de fiabilité d'un nœud. Les propriétés de confiance telles que l'honnêteté, la coopération, l'intérêt de la communauté et l'énergie d'un nœud sont prises en compte pour le calcul de la confiance. on a utilisé cette algorithme pour garantit une communication sécurisée entre les nœuds SIoT grâce à de simples codes secrets.

Les auteurs [36] ont propose ce algorithme qui connaissait le réseau SIoT est un graphe G (V, E) où V représente le nombre de sommets (objets) et E représente les arêtes entre eux.

L'algorithme DTrustInfer prend l'entrée d'un sous-graphe G (V, E). Lorsqu'un nœud souhaite établir une communication avec un autre nœud, il calcule et estime la fiabilité du nœud voisin.

Le nœud avec la centralisé la plus élevée est choisi comme authentificateur Ai. le nœud d'authentification Ai gère la génération et la distribution des codes secrets qui doivent être remplis avec les messages. il vérifie également les informations d'identification de l'utilisateur lors de l'attrition de l'utilisateur.

L'algorithme commence par calculer la confiance entre les nœuds qui doivent communiquer, Lorsqu'il est digne de confiance, le nœud de l'expéditeur remplit la clé secrète avec le message. À la destination, le nœud destiné sépare le message et la clé secrète compare la clé secrète avec celle qui a été distribuée par l'authentificateur Ai.

Ainsi, une vérification est effectuée pour assurer l'authentification des messages. La confiance et l'authentification rendent le réseau SIoT plus robuste.

Haifeng Yu [60] est prouvé que les nœuds honnêtes se mélangent rapidement et que ceux de Sybil ne se mélangent pas assez rapidement comme les nœuds honnêtes.

En raison de cette nature, il existe une petite coupure dans le graphique entre la région honnête et Sybil région. Cela ils aide à identifier facilement la région de Sybil.

Algorithme DTrustInfer

Input sous graph G (V, E)
Out put score de confiance entre les nœuds et la région Sybil
Si nœud(i) veux communiquer direct avec (j) alors
Applique la formule (3.6)
Sinon
Applique la formule (3.7)
Choisir le nœud avec la centralisé plus élevé pour être le nœud authentificateur A
Applique la formule (3.5)
Pour tous les nœuds voisins de A
Alloue un code secret à chacun
Pour nœud(i) établir communication vers nœud (j)
- Vérifier la fiabilité entre (i) et (j)
- effectue des promenades sur le sous graph pour identifier les petites coupures

Si coupure présente alors
La région Sybil et contient des bords d'attaque
Sinon
Commencer la communication en remplissant le code secret le long l »unité de réputation du message

FIGURE 3.3 – Les Algorithmes DTrustInfer [36]

3.7 Les Diagrammes de séquence

On a utilisé cette section qui permet de comprendre d'une façon claire ce modèle pour obtenir le meilleur fournisseur de service .

Un diagramme de séquence, c'est un l'abstraction d'une fonction typique du système à modéliser sur la figure 3.4,

Cette figure illustre que le demandeur envoie au serveur une requête contenant le ID de demandeur et le service dont il a besoin.

Le serveur, après avoir reçu le message, cherché dans la table des propriété du objet les objets qui fournissent le service requis,après avoir extrait les objets, il vérifie s'il existe une relation sociale entre les fournisseurs de services et demandeur. en cas d'absence de relation sociale ne calcule pas la valeur de la confiance entre demandeur et le fournisseur de service.

Dans le cas où il y a une relation ici, il calcule la valeur de confiance pour extraire le meilleur fournisseur de services qui a la plus grande valeur de confiance.puis envoie ID de fournisseur avec le valeur de confiance au demandeur le demandeur faire communication avec le fournisseur après avoir mis fin à la communication, le demandeur transmet son rétroaction et son avis sur le fournisseur de service au serveur pour le serveur faire le mise a jour sur la valeur de confiance concernant le fournisseur de service .

notre modèle est composé de deux types de communication principaux telle que communication directe entre le demandeur et fournisseur de service ou communication indirect qui le demandeur n'aura aucune interaction directe avec le fournisseur de service , nous expliquerons chaque type séparément ;

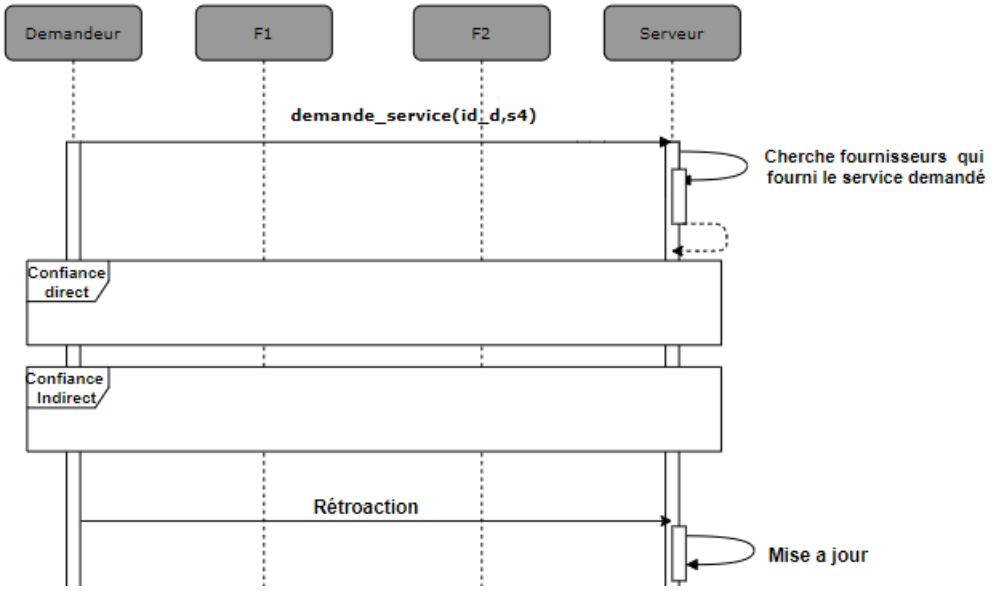

FIGURE 3.4 – Diagramme de séquence générale pour obtention la valeur de confiance unique

— **Communication Direct** cette propriété indique que la confiance est basée sur des interactions, des expériences ou des observations directes entre le demandeur et le fournisseur .
Dans la figure 3.5 montre que le serveur est responsable de collecter les informations et le compte pour extraire le meilleur fournisseur de services puis envoie un message à demandeur contenant le ID du meilleur fournisseur de services avec la valeur de confiance.
Après réception du message, le demandeur envoie sa demande au fournisseur pour lui fournir le service souhaité.

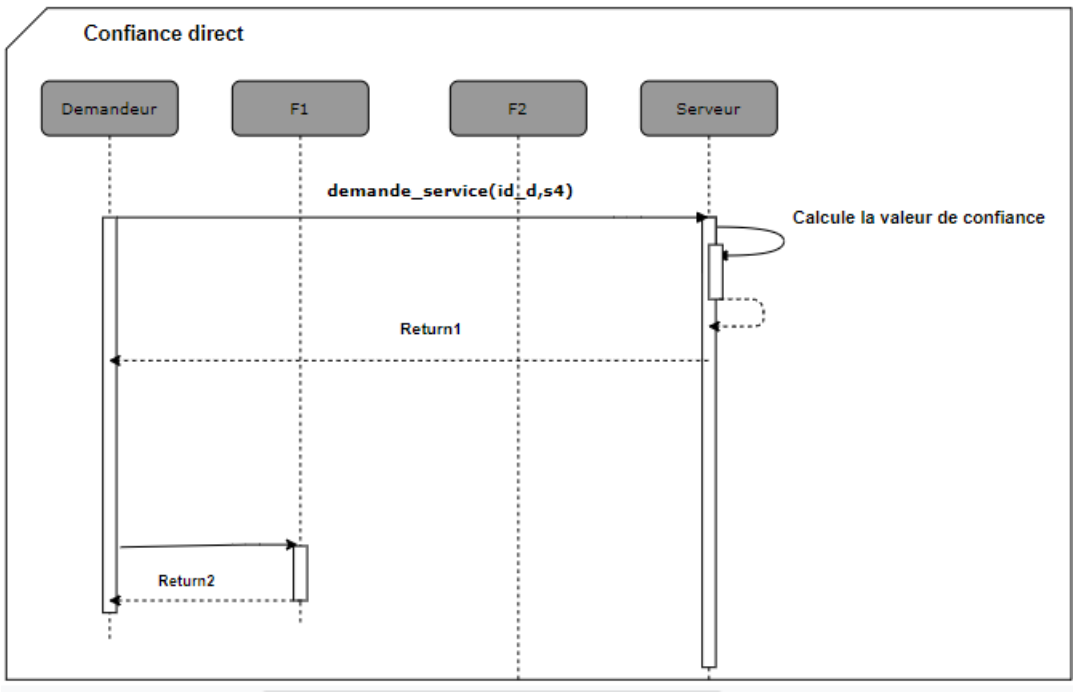

FIGURE 3.5 – Interaction Direct entre les noeuds

— **Communication Indirect** le demandeur et fournisseur n'ont pas d'expérience ni d'interaction dans le passé. la confiance ici repose sur l'opinion et la recommandation d'autres noeuds. dans ce cas on a parler de confiance transitive.
Dans la figure 3.6 le serveur est calculer la valeur de centralisé entre le demandeur et chaque fournisseur de service ,le nœud avec la centralisé la plus élevée est choisi comme authentificateur Ai.
Le nœud d'authentification Ai gère la génération et la distribution des codes secrets qui doivent être remplis avec les messages.
serveur commence par calculer la confiance entre les nœuds qui doivent communiquer, Lorsqu'il est digne de confiance, le nœud de l'expéditeur remplit la clé secrète avec le message. À la destination, le nœud destiné sépare le message et la clé secrète compare la clé secrète avec celle qui a été distribuée par l'authentificateur Ai. Ainsi, une vérification est effectuée pour assurer l'authentification des messages.

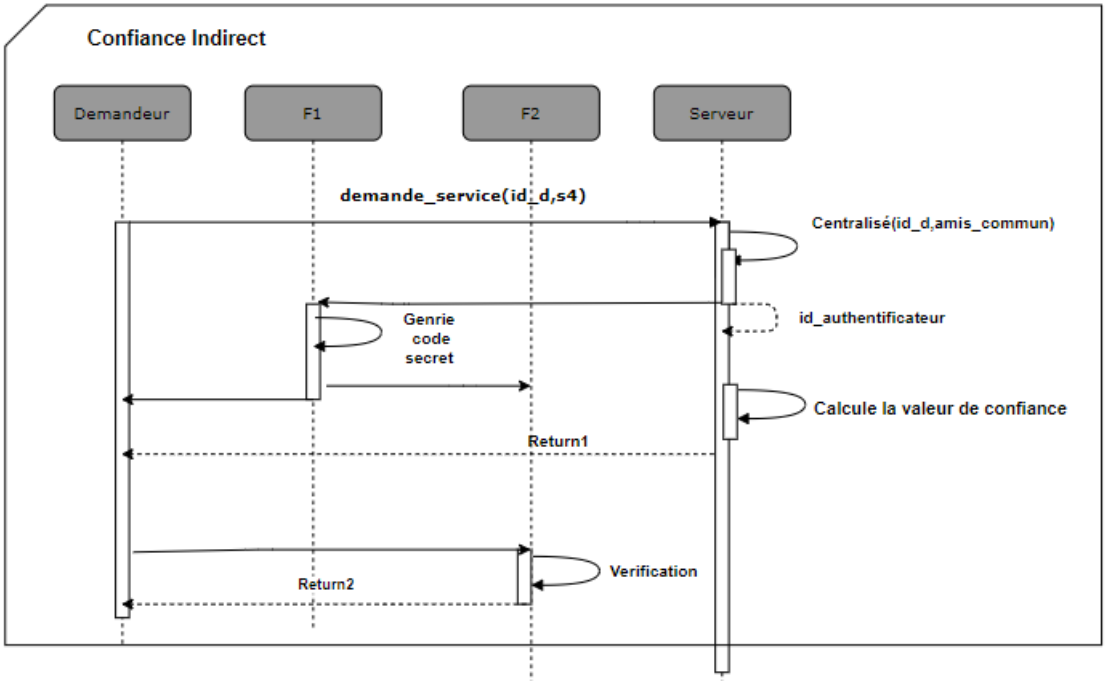

FIGURE 3.6 – Interaction Indirect entre les noeuds

3.8 Conclusion

Dans ce chapitre, nous concevoir et exprimé un modèle de confiance dynamique pour évaluer le niveau de fiabilité des nœuds et éviter le maximum les nœuds malhonnêtes qui fournirent des services malveillant afin d'assuré que la communication entre les nœuds plus sécurisé.

On a utilisé dans ce modèle , le facteur de centralisé et de fiabilité qui permet un meilleur calcul de la confiance et avec l'authentification rendent le réseau SIoT plus robuste.

Dans le chapitre suivant, nous allons présenter la mise en œuvre de notre conception,les moyens utilisés et les résultats obtenus.

Chapitre 4

Simulation et Implémentation

4.1 Introduction

Dans nos jours la simulation connaît un essor considérable grâce à l'intérêt que présente les modèles informatiques des systèmes simulés ; car le déploiement d'un réseau exige une étape de simulation avant son déploiement sur site. La simulation permet de tester à moindre coût les performances d'une solution.

OMNET++ sera notre environnement de simulation. Il s'agira d'étendre la simulation grâce à son architecture modulaire en implémentant un nouveau modèle pour la gestion de confiance .

Dans ce chapitre,nous allons présenter la mise en œuvre de notre conception,les moyens utilisés et les résultats obtenus.

4.2 L'environnement De Développement

OMNET++ est un environnement de simulation à évènements discrets basé sur le langage C++ : une application open source et sous licence.

Il est totalement programmable paramétrable et modulaire grâce à son architecture flexible et générique il a été utilisé avec succès dans divers domaines d'applications ,notamment :

— La modélisation des protocoles de communications ;
— La modélisation des réseaux filaires et sans fils ;

— La modélisation des systèmes répartis ;
— Les architectures HardWare ;

En général, il peut être utilisé pour n'importe quel système à évènements discrets pouvant être modélisé selon des entités communiquant par envoient de messages.

OMNET++ est basé sur la plateforme Eclipse. Il fournit des outils pour la création et la configuration des modèles de réseaux (fichiers NED et INI) et des outils pour l'exécution d'un lot de programmes ainsi que pour l'analyse des résultats de simulation.

4.3 Les principaux fichiers d'OMNET

1. **Fichiers (.NED)**

   Le langage NED (programmé à l'aide de fichiers NED avec des extensions .ned) permet de définir la structure des modules et la topologie du réseau. Au niveau le plus élémentaire, nous pouvons diviser grossièrement le contenu du fichier NED en deux composants fondamentaux, à savoir la partie de définition des modules et la partie de définition de la topologie du réseau. Les modules sont de deux types, c'est-à-dire simples (actifs) et composés, qui représentent finalement la structure de chaque nœud qui ferait partie de l'analyse de simulation. Les modules simples expriment fondamentalement l'interface du module (c'est-à-dire les portes et les paramètres). Les modules actifs sont programmés en C ++ et l'imbrication hiérarchique de modules simples forme un module composé. D'autre part, un groupe de modules actifs peut être encapsulé pour former des modules composés où les niveaux de hiérarchie ne sont pas limités. Les modules composés contiennent généralement des définitions de sous-modules et une interconnexion. La partie réseau décrit la topologie / la disposition de tout scénario de réseau ou l'emplacement de certains nœuds dans un scénario de simulation. Les autres fonctionnalités du fichier NED incluent l'héritage (pour les modules, les canaux, etc.), les notations de métadonnées et les informations sur les packages [34].

   Des exemples de fichier Ned en ses deux modes sont présentés dans la figures 4.1 et la figure 4.2.

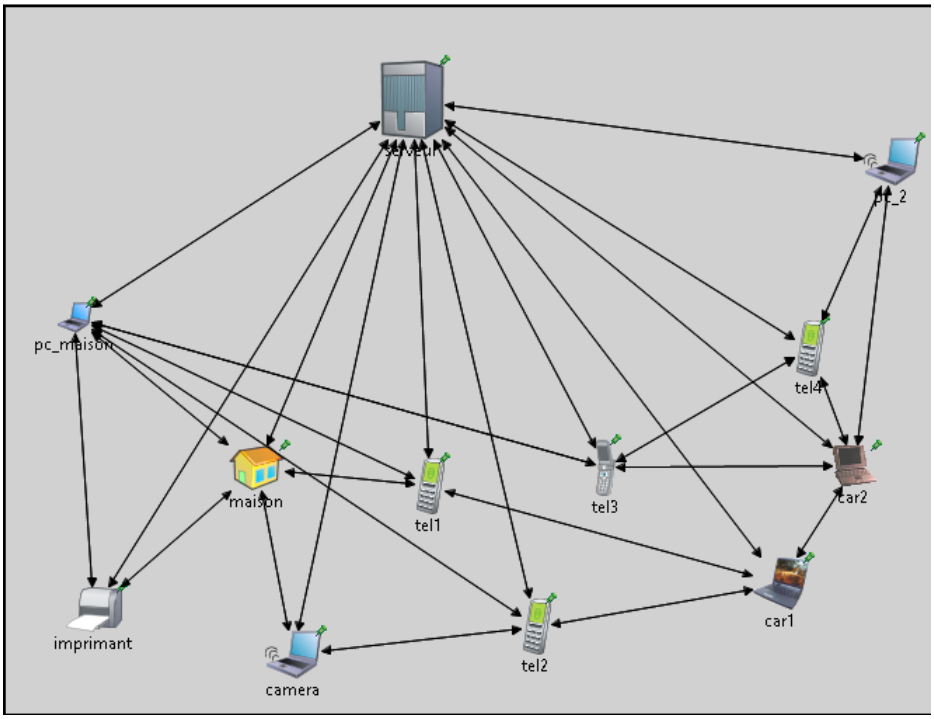

FIGURE 4.1 – Le fichier NED en mode Design

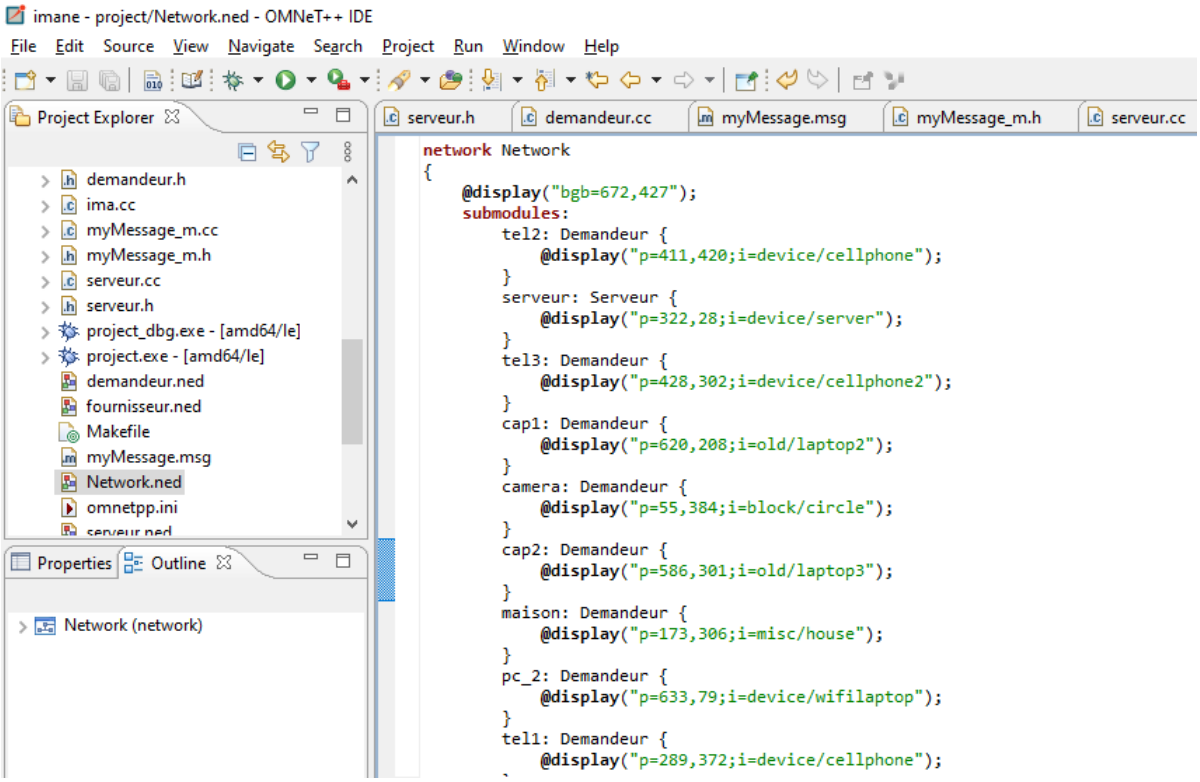

FIGURE 4.2 – Vue de la source du fichier NED du réseau composé de plusieurs objets

2. Le fichier (.ini)

Une tentative d'exécution après l'écriture de fichiers .ned et .cc dans un projet

OMNeT ++ produira une erreur concernant l'absence de fichier de configuration, c'est-à-dire un fichier avec une extension .ini. omnetpp.ini est la configuration clé que ce fichier offre la possibilité d'exécuter le réseau spécifié dans un projet OMNeT ++ (car plusieurs réseaux peuvent exister dans le même projet OMNeT ++)[34].

En outre, l'utilisateur peut également transmettre des valeurs en tant que paramètres (définis dans .ned) à partir du fichier omnetpp.ini. Associé à un réseau défini du fichier .ned (illustré à la figure **??**), un simple extrait de code du fichier omnetpp.ini est illustré à la figure 4.3.

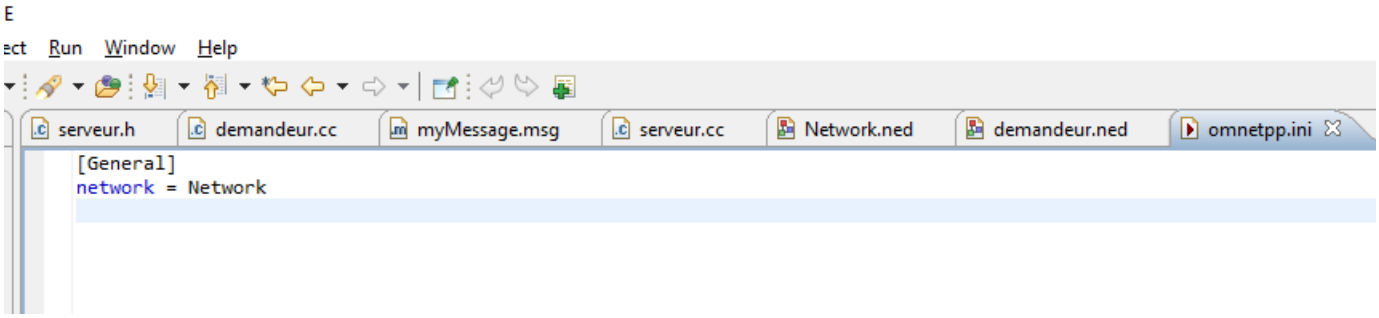

FIGURE 4.3 – Vue source de omnetpp.ini pour nos projet

3. **Le fichier (.msg)**

   Les modules communiquent en échangeant des messages qui peuvent être déclarés dans un fichier d'extension (.msg) où l'on peut ajouter des champs de données. OMNeT++ traduira les définitions de message en C++.

   Un exemples sur le fichier msg présenté sur la figure 4.4

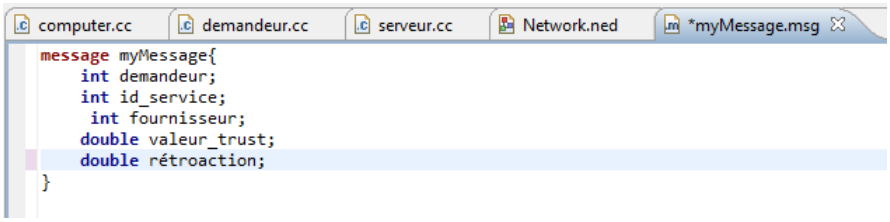

FIGURE 4.4 – Vue source de la fichier myMessage.msg

La figure 4.9 est une aide détaillée sur le développement d'exécution d'une simulation sous OMNET.

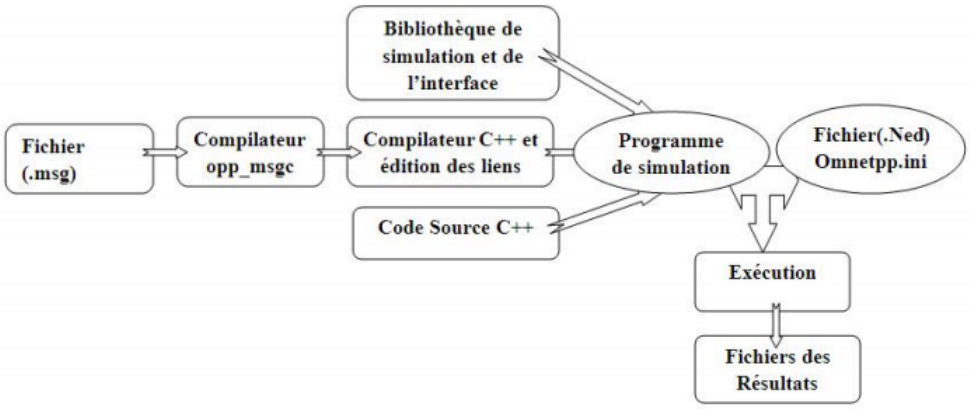

FIGURE 4.5 – Exécution d'une simulation sous OMNET++

4.4 Structure de Données

Dans notre modèle on a utilisé trois tables qui l'utilise par le serveur tel que : première table statique qui s'appelle la propriété d'objet qui contient la description des objets et pour la deuxième table statique qui s'appelle la table de relation sociale indique chaque objet et ses relation associe aux autres objets et dernier table c'est une table dynamique dans cette table on a enregistrée chaque transaction avec ID de demandeur et ID de fournisseur de service avec la valeur de confiance pour cette transaction

4.4.1 Table de propriété d'objet

Le nombre total d'objets comprend un total de 30 périphériques, dont 10 d'utilisateurs

Propriété	Signification
$\mathrm{Id}_{o}bjet$	Reference de l'appareil ;
$\mathrm{id}_{u}ser$	$\mathrm{id}_{u}serIDdepropriétairedel'appareil(nousindiquonslacommuneavecuser1)$;
Type	Type d'objet telque (portable,voiture,pc...)
Amis	Liste d'amis associe a chaque objets
Service	l'ensemble des services possibles offerts par chaque objet
Comportement	Si comportement est 1 alors l'objet est bienveillant (fourni bon service) Sinon malicieux(fourni mauvaise service)

TABLE 4.1 – Table de propriété d'objet

4.4.2 Table de Relation Sociale

Selon (SIoT), les noeuds établissent des liens sociaux et créent des réseaux sociaux. Nous proposons pour chaque relation et pour le réseau SIoT la matrice d'adjacence produite avec nos paramètres. Comme suit, nous décrivons les relations et leurs paramètres

Les relations	Description	Paramètres
Relationship (POR)	Établie si les objets ont le même fabricant et construits à la meme période	Seuil de 2 à 2.5 km
Colocalion objet	Établie si les objets partagent leur emplacement ;	+ de 13 fois
COWork objet	Établi lorsque la nature du travail pour les objets est identique ;	
Ownership object	Établie si les objets appartiennent à la même personne ;	Wi-Fi (400 m)
Social objects relationship	Établie lorsque la liaison entre les objets est fréquente ou récurent N : nombre de réunions TM : durée de réunions TI :intervalle entre réunions	N=3 ; TM = 1minute TI = 1h

Table 4.2 – Table de Relation Sociale

Dans le tableau 4.3, nous présentons un ensemble des objets que nous avons utilisé et les relation sociale qui les lies

id demandeur	id fournisseur	type de relation
id2	id4	POR
id6	id2	CWOR
id7	id2	OOR
id4	id6	CWOR
id8	id4	SOR
id5	id2	CWOR

Table 4.3 – Exemple table de Relation Sociale qui utilisé

4.4.3 Table de confiance

Une fois chaque transaction terminée, le serveur enregistre dans ce tableau le ID du fournisseur de services, le ID du demandeur avec la valeur de la confiance entre eux.

4.5 Les algorithmes

Concernant l'architecture logique d'OMNeT ++, les modules Simple et Compound communiquent entre eux par passage de messages. Le passage de messages entre les modules est possible via des connexions. Les connexions existent sous la forme de portes, qui sont des interfaces de module d'entrée / sortie. Les portes de modules simples et composés peuvent être inter connectées et généralement un message passe à travers une chaîne de connexion [34].

Dans cette section, nous présenterons un ensemble d'algorithmes qui montrent les étapes que nous avons franchies dans notre projet pour obtenir le meilleur fournisseur de services.

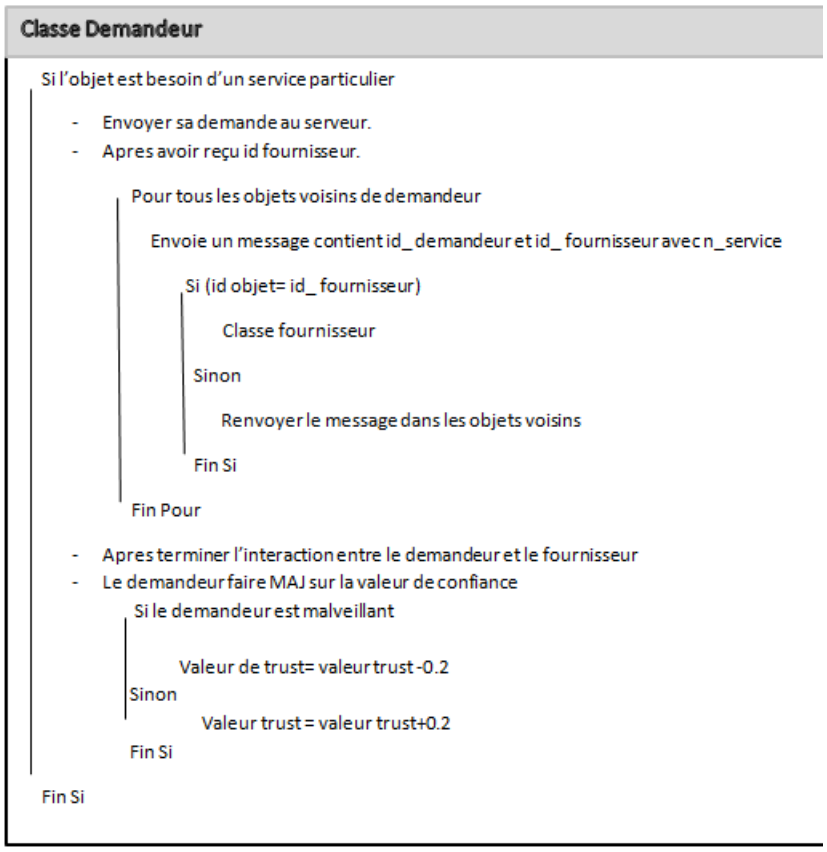

FIGURE 4.6 – L'algorithme de demande service

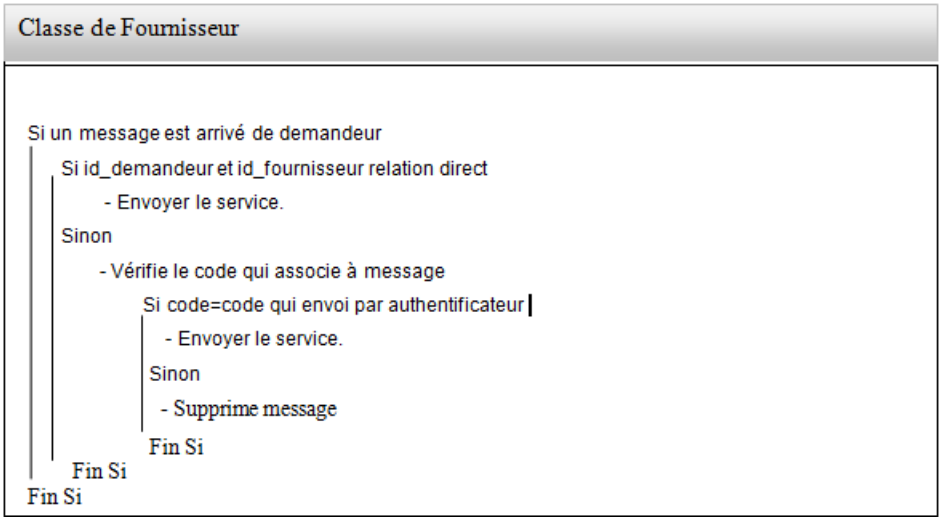

FIGURE 4.7 – L'algorithme qui explique le fonction d'objet fournisseur

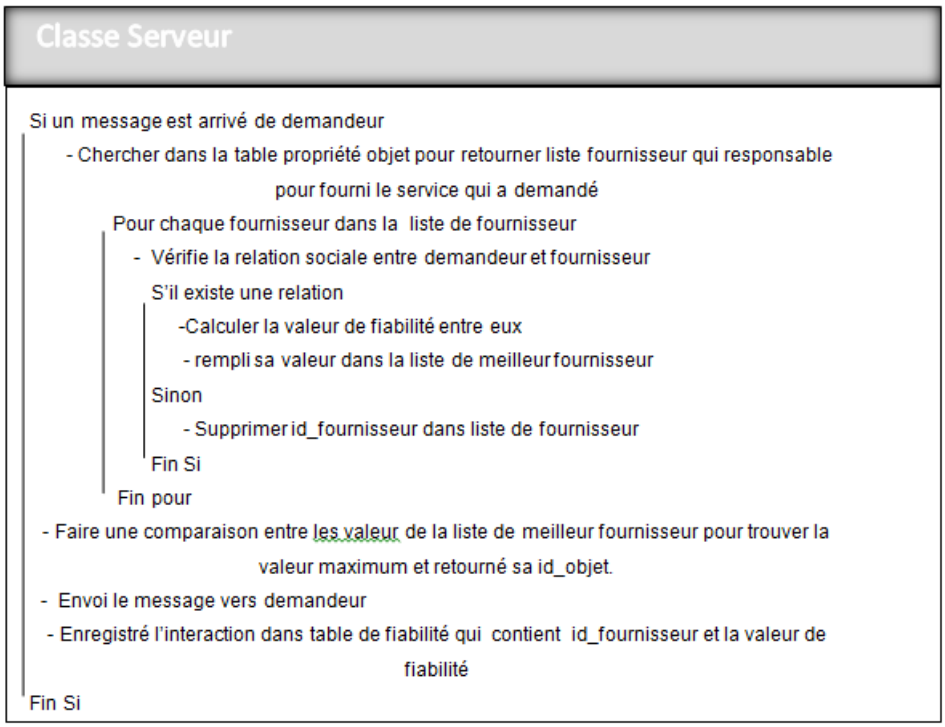

FIGURE 4.8 – L'algorithme qui explique le fonction de serveur

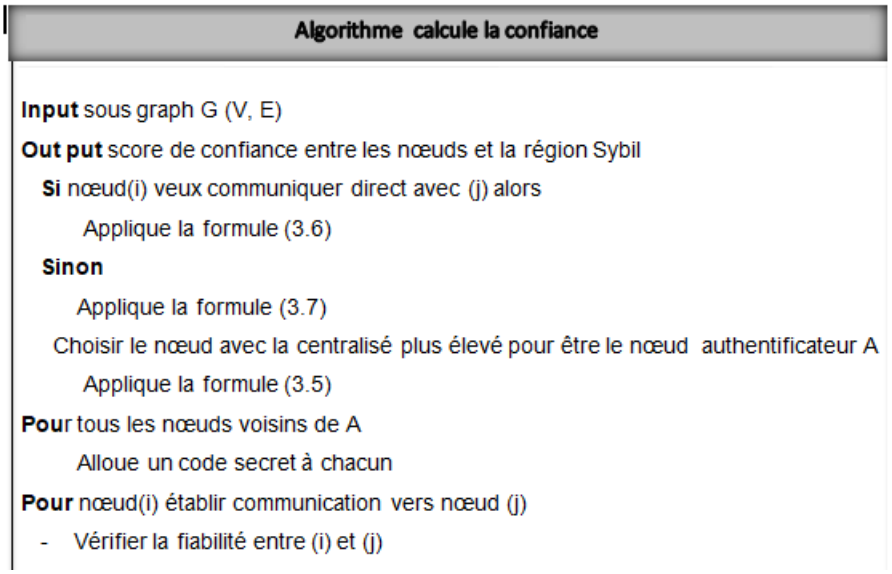

FIGURE 4.9 – L'algorithme pour obtenir la valeur de fiabilité

4.6 Simulation du modèle

4.6.1 Paramètres de simulation

Pour simuler notre solution, nous avons développé le modèle sous omnet++. Les simulations ont été réalisées avec 50 objets et le pourcentage de nœuds malveillants est fixé par défaut à 20% ; c'est a dire 10 objets malveillants.

Au début de chaque transaction, on a choisit le nœud demandant le service puis envoi cette demande au serveur,puis le serveur retrouve les noeuds fournisseur qui peuvent fournir le service ensuite,il effectue des calculs entre eux pour obtenir le meilleur fournisseur de services.

Concernant les objets malveillants on a utilisé le type attaque qui indique le noeud demandeur est malveillant,il est fournit une rétroaction négative à chaque nœud impliqué dans la transaction.

Le tableau 4.4 présente les paramètres de simulation du système et les différents poids utilisés .

paramètre	value
nombre des objets	50
% de noeud malveillant	20%
valeur de rétroaction(V_r)	0.2
α	0.2
β	0.3
γ	0.1

TABLE 4.4 – Les paramètres de simulation du système

4.6.2 Résultats obtenus

Dans ce qui suit nous présentons les résultats de la simulation de notre modèle. Afin de l'évaluer, nous essais plus de 20 interaction pour voir après certain temps ce qui va se passer. La figure 4.10 montre le taux de réussite pendant plusieurs interaction .

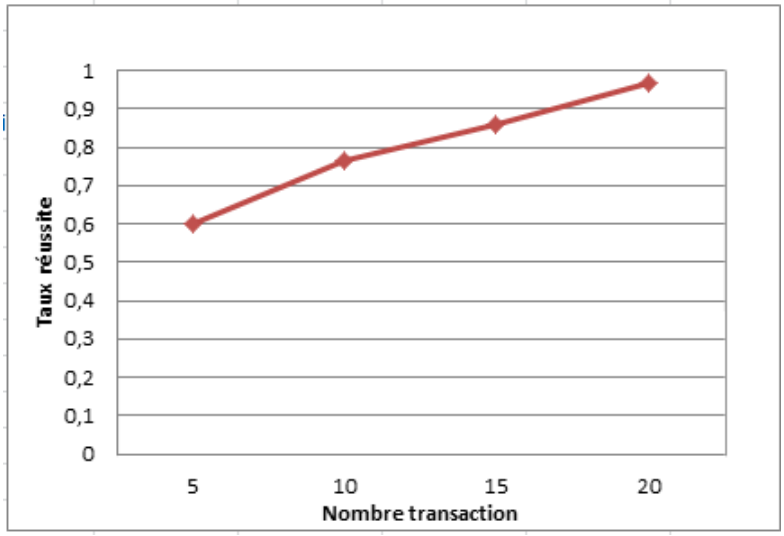

FIGURE 4.10 – courbe représenter l'évolution des bonnes objets

L'illustration figure 4.10 montre l'évolution de taux réussite dans une moyenne de 20 interaction , taux réussite c'est le résultat de la division de la moyenne des valeurs des bonnes transaction par la moyenne de toutes les transaction .

La figure 4.11 montre que le taux d'échec démunie avec le temps . le taux de d'échec est le résultat de la division de la moyenne des valeurs des mauvais transaction par la moyenne de toutes les transaction .

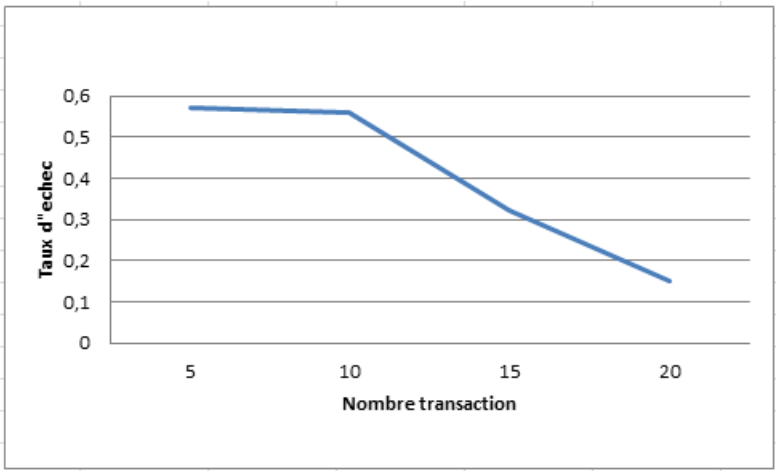

FIGURE 4.11 – courbe représenter dégradation des mauvaise objets

4.7 Conclusion

Ce chapitre est axé sur la validation et l'analyse de performances du modèle . Nous avons évalué les performances de notre modèle en se basant sur la confiance .
Concernant Les résultats obtenus sont succès pour choisir le meilleur fournisseur mais non pas à détecter les nœuds malveillants.

Chapitre 5

Conclusion générale

L'intégration de la composante sociale dans l'Internet des Objets a donné naissance à l'Internet des Objets Social (SIoT).
Le SIoT est apparu suite à un processus évolutif qui a transformé les objets du quotidien en objets pseudo-sociaux capables d'interagir avec leur environnement,
L'objet sociaux, ayant la possibilité d'établir des relations avec d'autres objets, d'une manière autonome.
La gestion de la confiance devenu un défi majeur dans SIoT ,avec son objectif est établir la fiabilité entre les noeuds, d'échanger des informations de confiance en fonction de leur relation, et de construire un système intelligent dans lequel on sait à qui se connecter pour un service particulier . Pour cela dans nos travail, nous avons faire une étude critique des travaux menés dans l'axe des modèles de gestion de la confiance dans l'Internet social des Objets ,A travers cette étude nous concevoir et exprimé un modèle de confiance dynamique pour évaluer le niveau de fiabilité des nœuds et éviter le maximum les nœuds malicieux qui fournier des services malveillant , Afin d'assuré que la communication entre les nœuds plus sécurisé.On a utilisé le facteur de centralisé et de valeur fiabilité qui permet un meilleur calcul de la confiance et avec l'authentification rendent le réseau SIoT plus robuste.
Nous avons remarqué que la majorité des systèmes de gestion de confiance actuels sont intéressés à classer les meilleurs nœuds du réseau et à éviter les nœuds malveillants, mais non pas à détecter les nœuds malveillants. Cela permet de les isoler et d'obtenir un système de confiance.

Bibliographie

[1] Wafa Abdelghani et al. “Détection des attaques de confiance dans l’Internet des Objets Social.” In : *INFORSID*. 2020, p. 155-170.

[2] Wafa Abdelghani et al. “Trust evaluation model for attack detection in social internet of things”. In : *International Conference on Risks and Security of Internet and Systems*. Springer. 2018, p. 48-64.

[3] Wafa Abdelghani et al. “Trust evaluation model for attack detection in social internet of things”. In : *International Conference on Risks and Security of Internet and Systems*. Springer. 2018, p. 48-64.

[4] Wafa Abdelghani et al. “Trust management in social internet of things : a survey”. In : *Conference on e-Business, e-Services and e-Society*. Springer. 2016, p. 430-441.

[5] Alfarez Abdul-Rahman et Stephen Hailes. “Supporting trust in virtual communities”. In : *Proceedings of the 33rd annual Hawaii international conference on system sciences*. IEEE. 2000, 9-pp.

[6] Younes Ait Mouhoub, Fatah Bouchebbah, Mawloud Omar et al. “Proposition d’un modèle de confiance pour l’internet des objets.” Thèse de doct. Université A/Mira de Bejaia, 2015.

[7] ME Ajana et al. “FlexRFID : A flexible middleware for RFID applications development”. In : *2009 IFIP International Conference on Wireless and Optical Communications Networks*. IEEE. 2009, p. 1-5.

[8] Dina Hussein Ali. “A social Internet of Things application architecture : applying semantic web technologies for achieving interoperability and automation between the cyber, physical and social worlds”. Thèse de doct. 2015.

[9] Kevin Ashton et al. “That ‘internet of things’”. In : *RFID journal* 22.7 (2009), p. 97-114.

[10] Luigi Atzori, Antonio Iera et Giacomo Morabito. “From” smart objects” to” social objects” : The next evolutionary step of the internet of things”. In : *IEEE Communications Magazine* 52.1 (2014), p. 97-105.

[11] Luigi Atzori, Antonio Iera et Giacomo Morabito. “Siot : Giving a social structure to the internet of things”. In : *IEEE communications letters* 15.11 (2011), p. 1193-1195.

[12] Luigi Atzori et al. “The social internet of things (siot)–when social networks meet the internet of things : Concept, architecture and network characterization”. In : *Computer networks* 56.16 (2012), p. 3594-3608.

[13] Luigi Atzori et al. “The social internet of things (siot)–when social networks meet the internet of things : Concept, architecture and network characterization”. In : *Computer networks* 56.16 (2012), p. 3594-3608.

[14] Eddy BAJIC et Oussama HAJLAOUI. “APPORTS DES PARADIGMES SOCIAUX DANS L’INTERNET DES OBJETS INDUSTRIEL : VERS DES OBJETS COMMUNICANTS INDUSTRIELS SOCIAUX”. In : ().

[15] Fenye Bao et al. “Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection”. In : *IEEE transactions on network and service management* 9.2 (2012), p. 169-183.

[16] Pierre-François Bonnefoi. “Cours de Sécurité Informatique”. In : *Université de Limoges* (2012).

[17] Djemaa Boukhlouf. “Une approche à base d’agents mobiles pour la sécurité des systèmes d’informations sur le web”. Thèse de doct. Université Mohamed Khider-Biskra, 2016.

[18] Gaëlle Calvary et al. *Computer science and ambient intelligence*. Wiley Online Library, 2013.

[19] Rajanpreet Kaur Chahal, Neeraj Kumar et Shalini Batra. “Trust management in social Internet of Things : A taxonomy, open issues, and challenges”. In : *Computer Communications* 150 (2020), p. 13-46.

[20] Ray Chen, Fenye Bao et Jia Guo. “Trust-based service management for social internet of things systems”. In : *IEEE transactions on dependable and secure computing* 13.6 (2015), p. 684-696.

[21] Ray Chen, Fenye Bao et Jia Guo. “Trust-based service management for social internet of things systems”. In : *IEEE transactions on dependable and secure computing* 13.6 (2015), p. 684-696.

[22] Ray Chen, Jia Guo et Fenye Bao. “Trust management for SOA-based IoT and its application to service composition”. In : *IEEE Transactions on Services Computing* 9.3 (2014), p. 482-495.

[23] Ray Chen, Jia Guo et Fenye Bao. "Trust management for SOA-based IoT and its application to service composition". In : *IEEE Transactions on Services Computing* 9.3 (2014), p. 482-495.

[24] Joerg Daubert, Alexander Wiesmaier et Panayotis Kikiras. "A view on privacy & trust in IoT". In : *2015 IEEE International Conference on Communication Workshop (ICCW)*. IEEE. 2015, p. 2665-2670.

[25] Nabil Djedjig et al. "Trust management in the internet of things". In : *Security and Privacy in Smart Sensor Networks*. IGI Global, 2018, p. 122-146.

[26] Asside Christian Djedouboum et al. "Big data collection in large-scale wireless sensor networks". In : *Sensors* 18.12 (2018), p. 4474.

[27] Deboleena Dutta et al. "Social Internet of Things (SIoT) : transforming smart object to social object". In : *NCMAC 2015 Conference Proceedings*. 2015.

[28] S Geetha. "Social internet of things". In : *World Scientific News* 41 (2016), p. 76.

[29] Tyrone Grandison et Morris Sloman. "A survey of trust in internet applications". In : *IEEE Communications Surveys & Tutorials* 3.4 (2000), p. 2-16.

[30] Jia Guo et Ray Chen. "A classification of trust computation models for service-oriented internet of things systems". In : *2015 IEEE International Conference on Services Computing*. IEEE. 2015, p. 324-331.

[31] Jia Guo et Ray Chen. "A classification of trust computation models for service-oriented internet of things systems". In : *2015 IEEE International Conference on Services Computing*. IEEE. 2015, p. 324-331.

[32] Jia Guo, Ray Chen et Jeffrey JP Tsai. "A survey of trust computation models for service management in internet of things systems". In : *Computer Communications* 97 (2017), p. 1-14.

[33] Kevin Hoffman, David Zage et Cristina Nita-Rotaru. "A survey of attack and defense techniques for reputation systems". In : *ACM Computing Surveys (CSUR)* 42.1 (2009), p. 1-31.

[34] Muhammad Azhar Iqbal et al. *Computer Network Simulation Using OMNeT++*. 2017.

[35] Audun Jøsang, Claudia Keser et Theo Dimitrakos. "Can we manage trust ?" In : *International Conference on Trust Management*. Springer. 2005, p. 93-107.

[36] A Meena Kowshalya et ML Valarmathi. "Dynamic trust management for secure communications in social internet of things (SIoT)". In : *Sādhanā* 43.9 (2018), p. 136.

[37] A Meena Kowshalya et ML Valarmathi. "Trust management for reliable decision making among social objects in the Social Internet of Things". In : *IET Networks* 6.4 (2017), p. 75-80.

[38] Francisco Moyano, Carmen Fernandez-Gago et Javier Lopez. “A framework for enabling trust requirements in social cloud applications”. In : *Requirements Engineering* 18.4 (2013), p. 321-341.

[39] Ricardo Neisse, Maarten Wegdam et Marten van Sinderen. “Trust management support for context-aware service platforms”. In : *User-Centric Networking*. Springer, 2014, p. 75-106.

[40] Michele Nitti, Roberto Girau et Luigi Atzori. “Trustworthiness management in the social internet of things”. In : *IEEE Transactions on knowledge and data engineering* 26.5 (2013), p. 1253-1266.

[41] Michele Nitti, Roberto Girau et Luigi Atzori. “Trustworthiness management in the social internet of things”. In : *IEEE Transactions on knowledge and data engineering* 26.5 (2013), p. 1253-1266.

[42] Mawloud Omar, Yacine Challal et Abdelmadjid Bouabdallah. “ICARM : Infrastructure de Confiance pour les Architectures de Réseaux Mixtes”. In : 2007.

[43] Sang Min Park et al. “Software-defined-networking for M2M services”. In : *2013 International Conference on ICT Convergence (ICTC)*. IEEE. 2013, p. 50-51.

[44] Keyur K Patel, Sunil M Patel et al. “Internet of things-IOT : definition, characteristics, architecture, enabling technologies, application & future challenges”. In : *International journal of engineering science and computing* 6.5 (2016).

[45] Hauke Petersen, Emmanuel Baccelli et Matthias Wählisch. “Interoperable services on constrained devices in the internet of things”. In : 2014.

[46] Rodrigo Roman, Pablo Najera et Javier Lopez. “Securing the internet of things”. In : *Computer* 44.9 (2011), p. 51-58.

[47] Theo Schlossnagle. *Scalable internet architectures*. Pearson Education India, 2006.

[48] Pallavi Sethi et Smruti R Sarangi. “Internet of things : architectures, protocols, and applications”. In : *Journal of Electrical and Computer Engineering* 2017 (2017).

[49] Antesar M Shabut et al. “Recommendation based trust model with an effective defence scheme for MANETs”. In : *IEEE Transactions on mobile computing* 14.10 (2014), p. 2101-2115.

[50] John A Stankovic. “Wireless sensor networks”. In : *computer* 41.10 (2008), p. 92-95.

[51] Yan Sun, Zhu Han et KJ Ray Liu. “Defense of trust management vulnerabilities in distributed networks”. In : *IEEE Communications Magazine* 46.2 (2008), p. 112-119.

[52] PS Suryateja. “Threats and vulnerabilities of cloud computing : a review”. In : *International Journal of Computer Sciences and Engineering* 6.3 (2018), p. 297-302.

[53] Ovidiu Vermesan, Peter Friess et al. *Internet of things-from research and innovation to market deployment*. T. 29. River publishers Aalborg, 2014.

[54] Natalija Vlajic, Mashruf Chowdhury et Marin Litoiu. “IP Spoofing in and out of the public cloud : from policy to practice”. In : *Computers* 8.4 (2019), p. 81.

[55] Van-Hoan Vu. “Infrastructure de gestion de la confiance sur internet”. Thèse de doct. 2010.

[56] Hannan Xiao, Nitin Sidhu et Bruce Christianson. “Guarantor and reputation based trust model for social internet of things”. In : *2015 international wireless communications and mobile computing conference (IWCMC)*. IEEE. 2015, p. 600-605.

[57] Zheng Yan et Silke Holtmanns. “Trust modeling and management : from social trust to digital trust”. In : *Computer security, privacy and politics : current issues, challenges and solutions*. IGI Global, 2008, p. 290-323.

[58] Zheng Yan, Peng Zhang et Athanasios V Vasilakos. “A survey on trust management for Internet of Things”. In : *Journal of network and computer applications* 42 (2014), p. 120-134.

[59] Mehdi YOUSSEF et al. “Formalisation du cycle de vie des produits de l’Usine du Futur étendue : vers l’Ingénierie Système élargie”. In : ().

[60] Haifeng Yu et al. “Sybilguard : defending against sybil attacks via social networks”. In : *IEEE/ACM Transactions on networking* 16.3 (2008), p. 576-589.