REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'enseignement supérieur et de la recherche
Scientifique
Université Mentouri de Constantine
Faculté des sciences de l'ingénieur
Département d'Informatique

Ecole Doctorale de l'Est en Informatique
Pôle Constantine

Mémoire présenté en vue de l'obtention du diplôme magister en Informatique
Option : Génie Logiciel

N°d'ordre : 397/Mag/2008
Série :012/info/2008

Protection de l'Agent Mobile : Identification des Métriques Permettant l'Estimation de la Confiance

Présenté par : ***M^{elle} Zaiter Meriem***

Soutenu publiquement le : 06 / 12 /2008, devant le jury composé de :

Président: ***Mr M. Benmohamed***	Professeur, Université Mentouri de Constantine
Rapporteur: ***Mme Z. Boufaida***	Professeur, Université Mentouri de Constantine
Examinateur : ***Mme F. Belala***	Maître de conférences, Université Mentouri de Constantine
Examinateur : ***Mr R. Maamri***	Maître de conférences, Université Mentouri de Constantine
Invitée : ***Mme S. Hacini***	Docteur, Université Mentouri de Constantine

Remerciements

Je remercie avant tout, d'abord Dieu pour m'avoir prodigué la force morale et physique et m'a permis d'achever ce travail.

D'un point de vue professionnel je commence par mon encadreur professeur Zizette Boufaida pour avoir accepté de diriger ce travail ainsi que pour ses précieux conseils.
Je remercie aussi le Docteur Salima Hacini pour sa contribution dans la réalisation de ce mémoire ainsi que pour sa patience et sa disponibilité.
Mes remerciements vont aussi au Professeur Mahmoud Boufaida, à Mme Aicha Choutri, et Mr Mohemed Chihoub pour l'aide qu'ils m'ont prodiguée.

Je remercie ainsi, les membres de Jury, le professeur Mohemed Benmouhamed, Docteur Faiza Belala et Docteur Ramdane Maamri, Maitres de conférences, pour avoir bien voulue accepter de juger ce travail.

D'un point de vue personnel, Je remercie mes parents et mes sœurs pour leur soutient, confiance et je pris Dieu de me les garder auprès de moi.

Je remercie enfin, tous les enseignants qui ont participé à ma formation, et tous les collègues qui m'ont aidé de prés ou de loin...

Que Dieu les récompense tous

Dédicace

Je ne veux surtout pas rater cette occasion pour dédier ce mémoire

A

Ma merveilleuse mère qui est ma source de courage, de joie, et qui a toujours crus en moi je pris dieu de me la garder, prés de moi.

A

Mon père qui est ma source de confiance et qui a toujours eu confiance en moi.

A

Mes inestimables soeurs Hanene, Ikram et Khadidja, sans oublier les petits Roufaida, Manel, Rahma, Maria, Yasmine, Simou, Marame et Amani Loulou.

A mes deux grandes _mère Zhore et Yamena et mon grand _père Abd_Ahamid

A tous mes tantes Dalila, Hayette et ses Maries, sans oublier la belle Soumia.

A ma tante Djamila et ses enfants et A la mémoire de son marie mustafa.

A tous mes tontons, ses épouses et ses enfants, et spécialement A Mourad et son épouse Amel je les remercie pour leur aide sans oublier, Abd_Allah, Hamada et Boulaam Zakaria.

A toute ma famille à Annaba, djidjel et à Constantine (La famille Zaiter, kihel, twafek, khelassi…)

A tous mes amis: Sabrina, Nawel, khouloud, Nabila, Sara, Souhaila, Soumia, Zakaria Laaboudi, Moussa, Hamza… mes collègues de sports mes collègues au mosquée, à mes entraîneurs Mustafa et Bachir

A

Tous qui m'ont appris quelques choses…

Résumé:
La confiance est un concept important de la vie quotidienne. Il s'agit d'une notion assez naturelle que chaque personne acquiert et utilise systématiquement pour décider si un échange avec un autre individu est envisageable ou non. Elle est alors présente dans tous les types de communication ou d'interaction englobant deux parties. Par ailleurs, l'Internet est devenu un moyen incontournable fournissant un ensemble de services aux utilisateurs distants avec un coût raisonnable et un délai minimal. L'infrastructure de l'Internet se base sur le modèle client/serveur et se trouve exposée à un ensemble de problèmes tels que la surcharge, la défaillance, ou la congestion de réseau. De tels problèmes ont tendance à être résolus par une solution de mobilité du code ou encore celle de l'emploi des agents mobiles. Cependant, le problème de leur sécurité constitue un frein à leur emploi. La majorité des applications distribuées employant le concept d'agent mobile exigent leur exécution par des hôtes de confiance. L'objectif principal de ce mémoire, se concentre sur l'exploitation des différentes facteurs de confiance afin d'établir des métriques pour l'estimation du degré de confiance de l'hôte visité. La valeur estimée permettant à un agent mobile de décider d'interagir ou non avec l'hôte d'accueil en vue d'une transaction électronique.

***Mots clés** : agent mobile, estimation de la confiance, confiance, sécurité des agents.*

Abstract:

Trust is an important concept in our daily life. It deals with the natural notion that every person use systematically to decide if an exchange with another person will be possible or not. So, it is found in all kinds of communication in all what gathered two parts. Moreover, the Internet has become a powerful tool. It provides a set of services to different users in a short period of time and with a minimal cost. The Internet's infrastructure is based on customer /server model which suffers from a set of problems such as the overloading, the network congestion, and the shortcoming. These problems are partially solved by the use of the mobiles agents' paradigm. However, they bring a serious security risk. The majority of distributed applications that employ the agents mobile concept require an honest host for there execution. The main objective of our work is focus on the investigation of different metrics of trust that contribute to estimate the trustworthiness degree of the visited host. Trust metric value indicates whether the electronic transaction between the mobile agent and the received host will be completed or not.

***Key words**: Mobile agents, trust, trust metric, security of mobile agent.*

ملخص:

الثقة مفهوم دو أهمية في الحياة اليومية. إنها مفهوم يستعمله الإنسان في كل عمليات التبادل التي تجمع عنصرين و هدا لتحديد قابلية تنفيذ عملية التبادل. من جهة أخرى, أصبح الانترنت وسيلة لا مفر منها يستعملها الإنسان لتنفيذ الكثير من العمليات في زمن قصير و بثمن معقول. البنية التحتية للانترنت تعتمد على تقنية (الزبون/المزود) هده التقنية تعاني من نقائص مثل : العجز, الاختناق أو الاحتقان, هده المشاكل حلت بصفة نسبية باستعمال البرنامج المتحرك أو بالأحرى استعمال الوكيل المتحرك. لكن ضمان أمن هدا الأخير يشكل عائق في استعماله. معظم التطبيقات أو العمليات الموزعة التي تستعمل مفهوم الوكيل المتحرك تفرض وجوب تنفيذ هدا الأخير في مواقع تتسم بالثقة. هدفنا في هده المذكرة هو استغلال عوامل الثقة في الانترنت لإنشاء معادلات لتقييم نسبة الثقة الموضوعة في الموقع المستقبل للوكيل. بناءا على هده القيمة المحسوبة يتم اتخاذ القرار ادا كان الوكيل المتحرك سوف يتم تنفيذ العملية الالكترونية المبرمجة مع الموقع المستقبل أم لا .

الكلمات المفتاح: *الوكيل المتحرك, الثقة, تقييم الثقة, أمن الوكيل المتحرك.*

TABLE DES MATIÈRES

INTRODUCTION GENERALE
1. Le contexte 1
2. La problèmatique 2
3. Notre contribution 2
4. Organisation du memoire 3
CHAPITRE 1: Agent mobile et sécurité
1. Introduction 5
2. Definition et caracteristiques 5
2. 1 Le cycle de vie d'un agent mobile 7
2. 1.1 Les domaines d'application des agents mobiles 7
3. Exemple d'un agent mobile adaptable 8
4. La sécurité dans les systèmes d'agents mobiles 10
4.1 Les types d'attaques. 10
4.1.1 Les attaques des agents visant les hôtes 11
4.1.2 les attaques des hôtes contre l'agent 12
4.2 Les techniques de protection 15
4.2.1 La protection de l'hôte 15
4.2.2 La protection de l'agent. 17
5. conclusion 21
CHAPITRE 2: Notion de la confiance et métriques
1. Introduction 23
2. Les notions de confiance et de métrique 24
2.1 Définition et avantages de la confiance 24
2.2 Les catégories de la confiance 25
2.3 La confiance et la réputation 30
3. La relation entre la confiance et le risque 33
3.1 Le risque et la confiance agissent indépendament sur le comportement 33
3.2. Une relation de médiation 34
3.3. Une relation modérée 34
4. Conclusion 36

CHAPITRE 3: Technique de protection proposée
1. Introduction 37

2. La délimitation du cadre de travail 38
3. La technique de protection 39
3.1 L'identification 39
3.2 La bienveillance 40
3.3 La réputation 42
3.4 Le risque 44
3.5 La disponibilité 46
3.6 Algorithme d'estimation de la confiance 46
4. Conclusion 49
CHAPITRE 4: Expérimentation
1.Introduction 51
2. Definition du commerce électronique 51
3. Agent mobile et commerce électronique 52
4. La discription générale de l'application 53
4.1 le scénario d'aquisition des paramètres 54
4.2 Le scénario de vérification du certificat 55
4.3 Le scénario de vérification des informations reçus 56
5. l'environnement de dévelopement 59
6. Expérimentation… 60
6.1 Exemples expérimentaux 60
6.2 L'apport de notre technique de protection 68
7. Conclusion 70
CONCLUSION GENERALE 71
PERSPECTIVES 72
References bibliographiques 73

TABLE DES FIGURES

Fig. 1.1 le Fonctionnement d’un agent. 6
Fig1.2 le cycle de vie d’un agent mobile 8
Fig1.3 Architecture adaptative de l’agent mobile 9
Fig1.4 le sandbox. 16
Fig1.5 la Signature numérique du code 17
Fig2.1 un modèle représente l'effet indépendant de la confiance et le risque sur le comportement. 33
Fig2.2 un modèle qui représente la relation de médiation entre le risque et la confiance et leur effet sur le comportement 34
Fig2.3 un modèle qui représente la relation modérée entre le risque et la confiance et leur effet sur le comportement 34
Fig4.1 la forme générale d’une transaction sur internet 51
Fig4.2 la description générale de la simulation 53
Fig4.3 Une interface pour récupérer les paramètres liées au caractéristique du produit . 60

LISTE DES TABLES

Table 1.1 Les catégories de la confiance 27
Table 3.1. Paramètres intervenant dans le calcul de la réputation 43
Table 3.2.Algorithme du comportement de l'agent mobile 47
Table 3.3.Algorithme de l'exécution de l'émetteur de l'agent mobile 48
Table 3.4. Utilisation de la disponibilité pour le traitement du manque de confiance 49
Table 4.1 les données stocké au niveau de la base de donnée locale de l'émetteur de l'agent mobile..... 61
Table 4.2 les valeurs précisé par l'émetteur de l'agent mobile..... 61
Table 4.3 les valeurs reçus de l'agent mobile 61
Table 4.4 les poids associé à chaque métrique..... 62
Table 4.5 les valeurs des métriques du scénario 1 62
Table 4.6 les informations reçus du scénario2 63
Table 4.7 les valeurs des métriques du scénario 2 64
Table 4.8 les informations reçus du scénario4 64
Table 4.9 les informations reçus du scénario4 65
Table 4.10 les informations reçus du scénario4 66
Table 4.11 les métriques calculées du scénario4 (modifié) 67
Table 4.12 les informations reçus du scénario4 (modifié)..... 67
Table 4.13 les informations reçus du scénario comparatif..... 68
Table 4.14 les métriques calculées du scénario comparatif 69

LA LISTE DES GRAPHES

Graphe4.1 la représentation graphique des résultats du premier scénario 63
Graphe4.2 la représentation graphique des résultats du scénario2 64
Graphe4.3 la représentation graphique des résultats du scénario3 65
Graphe4.4 la représentation graphique des résultats du scénario4 66
Graphe4.5 un graphe montrant la sensibilité de métrique en cas d'une altération au niveau des informations reçues 67
Graphe4.6 représentation graphique des résultats du scénario5 69
Graphe4.7 représentation graphique du scénario 5 montrant l'apport de la prise en compte de l'aspect multi dimmensionnelle de la confiance 70

INTRODUCTION GENERALE

Introduction générale

1. Le contexte

L’Internet est devenu un outil essentiel et incontournable qui permet une liaison avec le monde entier en fournissant un ensemble de services aux utilisateurs distants avec un coût raisonnable et un délai minimal. D'autre part, le développement croissant de la technologie informatique est amené à supporter l'exécution d'un grand nombre d'applications pouvant avoir des contraintes d'exécution spécifiques telles que le commerce sur Internet. L’infrastructure de l’Internet, qui est un réseau des réseaux (web), se base sur le modèle client serveur et se trouve exposé à un ensemble de problèmes tels que la surcharge, la défaillance ou la congestion de réseau.

De tels problèmes ont tendance à être résolus par une solution : la mobilité du code et en particulier l'utilisation des agents mobiles.

Un agent mobile est un logiciel particulier qui a des capacités de flexibilité, d’autonomie, de mobilité et d’adaptabilité. Cet agent se déplace à travers le réseau (en particulier l’Internet) d’un site vers un autre dans le but de fournir un service précis à son propriétaire.

Il y a évidemment plusieurs domaines d'application des agents. Ceci est du au fait que les architectures basées sur les agents fournissent une manière bien particulière afin d'aborder des problèmes rapidement. À titre d’exemple, en utilisant les caractéristiques de l’autonomie, l’adaptabilité et la flexibilité, cet agent permet une meilleure utilisation des ressources de réseau ainsi qu’une réduction de communication en ce qui concerne la latence, la largeur de la bande passante et le temps de connexion. C'est pour cette raison que les agents sont largement utilisés dans les domaines tels que la robotique (les robots coopératifs), la gestion de réseaux, le commerce électronique ou la recherche d'information.

Cependant, l'utilisation du paradigme agent présente des insuffisances puisque des problèmes d’insécurité dus à des actes de malveillance de différentes natures et catégories se posent tels que l’accès au code de l’agent par l’hôte et le risque de sa modification ou encore l'attaque d'un hôte par un virus.

2. La problématique

Les travaux de recherche relatifs à la sécurité des agents mobiles suivent principalement deux axes [Bob 2000]. Le premier axe concerne la protection de l'hôte contre des agents mobiles malicieux tandis que le second axe concerne la protection de l'agent mobile contre la malveillance des hôtes visités. On cite à titre d'exemple, la technique du bac à sable (sandboxing) [Con 2005] ou l'estimation de l'état (state appraisal) [Far 1996, Gre 1998]. Dans cette thèse, on s'intéresse au second volet où plusieurs approches de protection des agents mobiles contre un hôte malveillant ont été présentées [Wil 1997, Hoh 1998, San 1998, Esp 2003, Vig 1998]. Ces techniques sont intéressantes mais elles sont appliquées dans un cadre restreint. C'est le cas de la technique basée sur la limitation du temps d'exécution [Esp 2003] qui ne peut être utilisée que dans une application où l'agent mobile retourne à son propriétaire ou à l'hôte originaire.

En analysant ces différentes approches, on voit bien que la conception d'une solution générique de sécurité pour les agents mobiles reste un problème ouvert.

3. Notre contribution

L'objectif de cette thèse est d'assurer l'exécution de l'agent mobile uniquement dans un environnement de confiance. Dans cette optique, nous proposons un mécanisme de protection qui offre la possibilité de contrecarrer les éventuelles attaques de l'hôte visité [Zai 2008]. Ce mécanisme de protection est une des perspectives de la thèse de Doctorat de Mme Hacini [Hac 2008] au niveau de laquelle elle a proposé une architecture flexible et adaptable pour l'agent mobile qui lui permet de s'adapter dans un environnement donné afin de se protéger contre les attaques des hôtes visant l'analyse de son code.

La technique de protection proposée par Hacini et al [Hac 2006] est liée de manière intrinsèque à la confiance placée en l'hôte visité. Notre objectif est de renforcer cette technique en identifiant l'ensemble des métriques nécessaires à l'estimation de la confiance. Cette dernière est utilisée comme base de décision a partir de laquelle l'agent interagit ou non avec l'hôte visité.

Par ailleurs, la confiance est un concept important qui permet de pallier au problème de l'incertitude. Il s'agit d'une notion naturelle que chaque être acquiert et utilise systématiquement pour décider si un échange avec un autre individu, quel que soit sa nature, est envisageable ou non. Il faut remarquer que, de façon générale, la confiance que nous plaçons en une personne ne dépend pas uniquement de notre propre connaissance de celle-ci mais aussi de celle que possèdent les personnes qui nous entourent. La confiance est alors présente dans tout type de communication ou d'interaction englobant deux parties. Il semble donc raisonnable que les réseaux informatiques procèdent de manière identique.

La notion de la confiance a été largement utilisée ces dernières années dans des domaines tels que les réseaux had hoc, les systèmes pair à pair, les systèmes multi agents, etc.

L'objectif de ce mémoire est donc de définir les différentes métriques de la confiance afin de protéger l'agent mobile en lui permettant de s'exécuter uniquement dans des environnements de confiance.

4. Organisation du mémoire

Ce travail de recherche, nous a obligé à étudier tout d'abord un nombre assez important de concepts qui sont l'objet des deux premiers chapitres (état de l'art) de cette thèse. Ensuite, la technique proposée est présentée et une simulation permettant de prouver sa faisabilité est effectuée. Nous pouvons résumer le contenu de cette thèse comme suit:

Chapitre 1 : Agent mobile et sécurité. Il est consacré à la définition de la notion d'agent mobile, de quelques types d'agents mobiles et de leurs divers domaines d'application. Ce chapitre englobe aussi les différents aspects de la sécurité et la présentation de quelques problèmes ainsi qu'un aperçu assez détaillé sur les attaques possibles et les techniques utilisées pour y remédier.

Chapitre 2 : Les métriques de la confiance. A ce niveau**,** la notion de la confiance est détaillée par l'exposé de quelques définitions existant dans la littérature et quelques formes de catégorisation. De plus, les différentes métriques utilisées dans les systèmes distribuées ainsi que les facteurs affectant chaque métrique sont recensés.

Chapitre 3 : Technique de protection proposée. Ce chapitre constitue le fruit de toute une étude puisqu'il présente notre proposition pour la protection de l'agent mobile qui se base sur la confiance ainsi que toutes les métriques et les paramètres nécessaires pour son évaluation en précisant éventuellement les différents facteurs rentrant en jeu.

Chapitre 4: Simulation et expérimentations. Dans ce chapitre, notre objectif est d'expérimenter l'approche proposée afin de vérifier sa faisabilité à travers la simulation d'une application du commerce électronique.

Conclusion générale : C'est une synthèse et une évaluation du travail réalisé tout au long de ce projet ainsi que la suggestion d'un certain nombre de perspectives pour des travaux futurs.

Chapitre 1: AGENT MOBILE ET SECURITE

1. INTRODUCTION

La communication basée sur le modèle « client/serveur » et activée par envoie de messages provoquant ainsi l'exécution de programmes en fonction des services demandés. Ce mode a l'inconvénient d'être coûteux, de nécessiter de connexion permanente entre le client et le serveur et de surcharge du réseau. Afin, pour pallier à ces problèmes, une alternative est adoptée. Elle est basée sur le concept de la mobilité du code qui peut être effectuée par une entité particulière appelée « agent mobile ».

Durant ces dernières années le concept d'agent est utilisé dans plusieurs applications distribuées telles que, les systèmes de télécommunication, la gestion de l'information ou la vente aux enchères etc. Pour cette raison, un fort et un rapide développement des recherches sur les agents afin d'améliorer ses performances. Le terme agent est un terme générique qui se rapporte à différentes entités [Fra 1996]:

- ✓ Des entités biologiques.
- ✓ Des robots autonomes.
- ✓ Des composants ou des logiciels informatiques qui sont intégrés dans des systèmes d'exploitation ou des systèmes informatiques complexes.

Ce chapitre est consacré à la présentation des notions de base et des propriétés relatives au concept d'agent ainsi qu'à l'aspect de sécurité qui y est associé.

Les différentes formes d'attaques seront présentées en insistant sur celles relatives aux systèmes à base d'agents mobiles. Enfin, quelques approches de protection seront discutées.

2. DEFINITIONS ET CARACTÉRISTIQUES

Il n'existe pas une définition de l'agent qui fasse foi dans le monde de l'intelligence artificielle distribuée. Il est donc nécessaire, pour avoir une bonne vision de ce concept, de confronter plusieurs de ces définitions.

- ➢ Du point de vue linguistique, le mot « agent » est un dérivé du verbe « agir » qui signifie faire quelque chose, s'occuper ou produire un effet [petit Larousse].

On peut aussi trouver le mot latin « agent : celui qui agit », qui veut dire « personne chargée des affaires et des intérêts d'un individu, d'un groupe ou d'un pays, pour le compte desquels elle agit ».

Trois caractéristiques de l'agent sont déduites à partir de ces définitions :

- ✓ Un agent accomplit une tâche.
- ✓ Un agent a un propriétaire.
- ✓ Un agent agit à la demande de son propriétaire.

- ➢ Du point de vue informatique, nous allons exploiter trois définitions:

✓ Une définition classique est celle de Jacques Ferber [Ferber 1995] qui a défini un agent comme étant une entité physique ou virtuelle évoluant dans un environnement dont il n'a qu'une représentation partielle et sur lequel il peut agir (Fig1.1). Il est doté d'un comportement autonome et capable de communiquer avec d'autres entités.

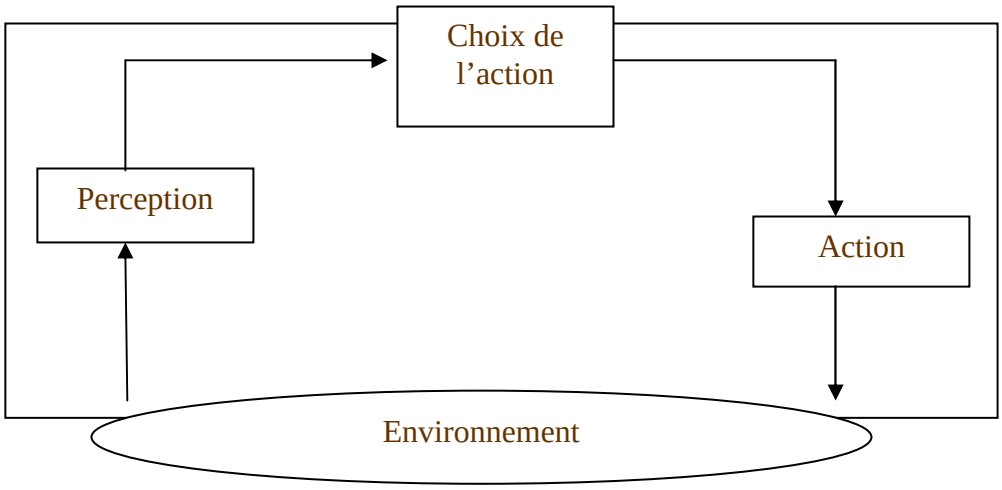


Fig. 1.1 *le Fonctionnement d'un agent*

Cette définition met en évidence deux nouvelles caractéristiques :

- l'autonomie: En effet, ce concept est au centre de la problématique des agents. L'autonomie est la faculté d'avoir ou non le contrôle de son comportement sans l'intervention d'autres agents ou d'êtres humains.
- Une autre caractéristique importante abordée par cette définition concerne la capacité d'un agent à communiquer avec d'autres entités.

✓ Selon Yves Demazeau [Dem 1996], un agent est une entité réelle ou virtuelle dont le comportement est autonome, évoluant dans un environnement qu'il est capable de percevoir et sur lequel il est capable d'agir, et d'interagir avec les autres entités.

Cette définition introduit l'interaction (la communication et l'action sur le monde) qui suppose la présence d'agents capables de se rencontrer, de communiquer, de collaborer et d'agir.

✓ Pour Mickael Wooldridge [Woo 1999], un agent est un système informatique capable d'agir de manière autonome et flexible dans un environnement.

Par flexibilité, il entend :

- Réactivité : un système réactif maintient un lien constant avec son environnement et répond aux changements qui y surviennent.
- Pro-activité : un système pro-actif (appelé aussi téléonomique) génère et satisfait des buts. Son comportement n'est donc pas uniquement dirigé par des événements.
- Capacités sociales : un système social est capable d'interagir ou coopérer avec d'autres systèmes.

L’exemple formel suivant peut clarifier le concept d’agent [Pat 2005]. L’agent prenant rendez-vous pour faire changer mes pneus est :

- Autonome : il prend conscience que le printemps arrive et que mes pneus d’hiver sont encore installés. Il peut alors lancer le processus de prise de rendez-vous.
- Réactif : peut repousser mon rendez-vous si une tempête de neige exceptionnelle est annoncée.
- Proactif : peut prendre l’initiative d’acheter de nouveaux pneus si les miens sont trop usés.

2.1 Le cycle de vie d’un agent mobile

L’accomplissement de la tâche affecté à l’agent mobile l’oblige à passer par plusieurs états selon la compétence et les paramètres de disponibilité de l’hôte visité tels que l’espace mémoire, ou encore la technique d’ordonnancement du processeur (le scheduling) etc. A cet effet, l’agent bascule, à titre d’exemple, d’un état actif vers l’état d’attente lorsque il attend une entrée de l’hôte visité. La figure 1.2 illustre les états possibles par lesquels un agent peut passer durant son exécution.

2.1.1 Les domaines d’application des agents mobiles

Les applications utilisant les agents mobiles sont diverses, elles peuvent concerner les réseaux pair à pair, le commerce électronique et nous citons ainsi, à titre d’exemple,

a. La recherche d’information

Dans ce cas la tache de recherche des informations est déléguée à un ou plusieurs agents mobiles qui visitent les sites web, ces agents peuvent coopérer et rechercher les sites intéressent puis choisir les meilleurs résultats.

b. La méthode de mise à jour de ressources distribuées

Dans ce cas, un agent possède la mise à jour à appliquer et va se déplacer de site en site, que se soit un ordinateur hôte ou un routeur, et va actualiser tous les éléments trouvés. En se déplaçant, les agents peuvent plus facilement accéder aux éléments appartenant aux infrastructures décentralisées et surtout peuvent, grâce à leur traitement local, appliquer la mise à jour sans craindre d’être interrompus [Pau 2001].

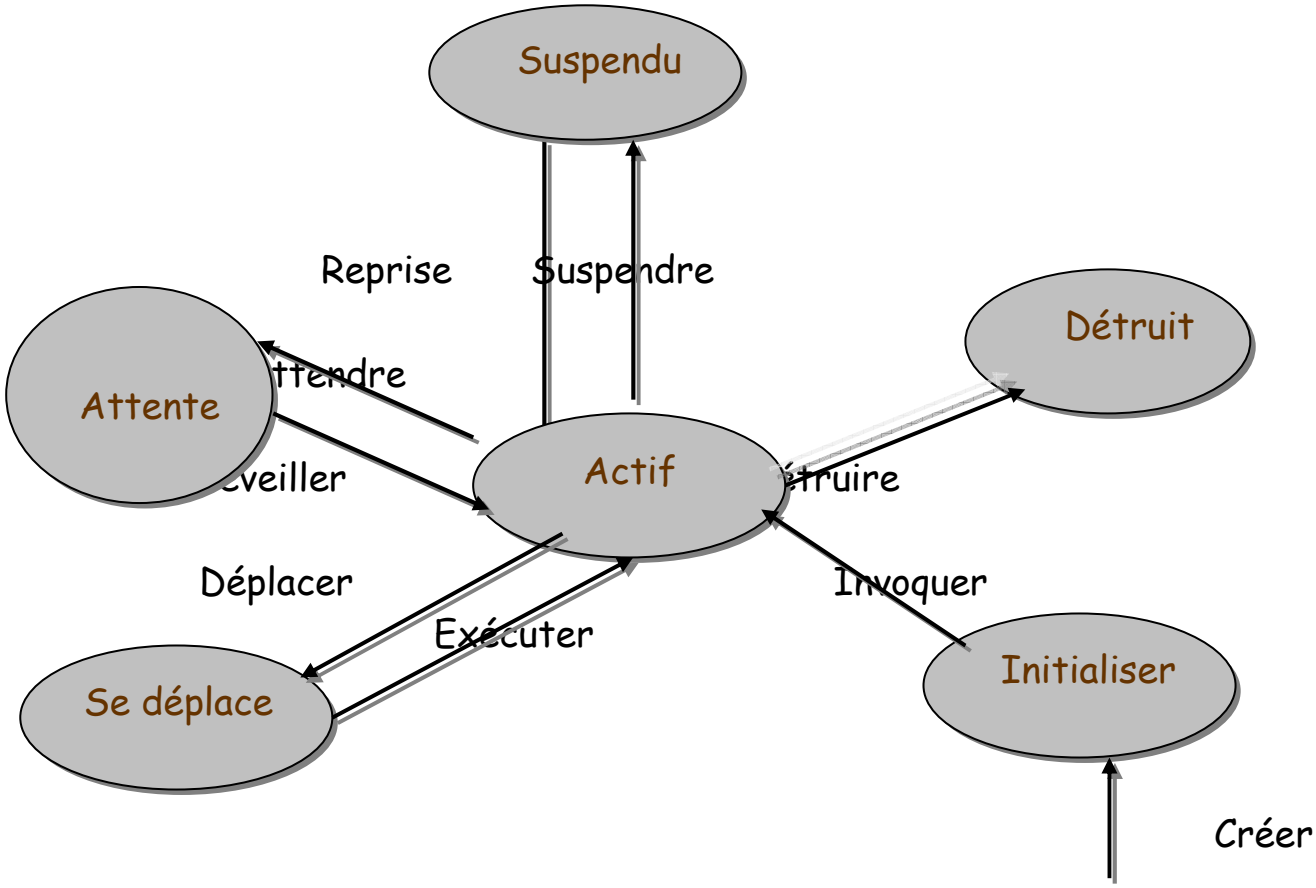


Fig1.2 *le cycle de vie d'un agent mobile*

3. Exemple d'un agent mobile adaptable

Un agent peut être décrit par trois niveaux de description d'un agent, et quand parle de niveau de description d'un agent nous entendons modèle d'agents, architecture d'agents et implémentation d'agents; alors avant de procéder au détaille de cet exemple d'agent mobile il est nécessaire d'expliquer ces termes qui constituent les différents niveaux de description d'un agent qui sont [Woo 1995]:

- ✓ Le *modèle* qui décrit comment l'agent est compris, ses propriétés et comment on peut les représenter.
- ✓ L'*architecture* qui est un niveau intermédiaire entre le modèle, le contrôle et l'implémentation.
- ✓ L'*implémentation* qui s'occupe de la réalisation pratique de l'architecture des agents à l'aide d'un langage de programmation.

Notre exemple d'architecture adaptative et flexible de l'agent mobile est celui proposée par Hacini et al [Hac 2006a] dont le travail constitue la base de ce projet comporte un ensemble de composants (voir Fig1.3):

- ✓ l'interface : permettant à l'agent mobile de communiquer avec son environnement cette communication est réalisée à travers deux composants qui sont l'actionneur (actuator) et le capteur (sensor). Ce dernier permet à l'agent mobile de percevoir et acquérir les informations de son environnement. Pour cela, trois types d'acquisition sont envisagées : l'observation, l'inspection et l'interaction.

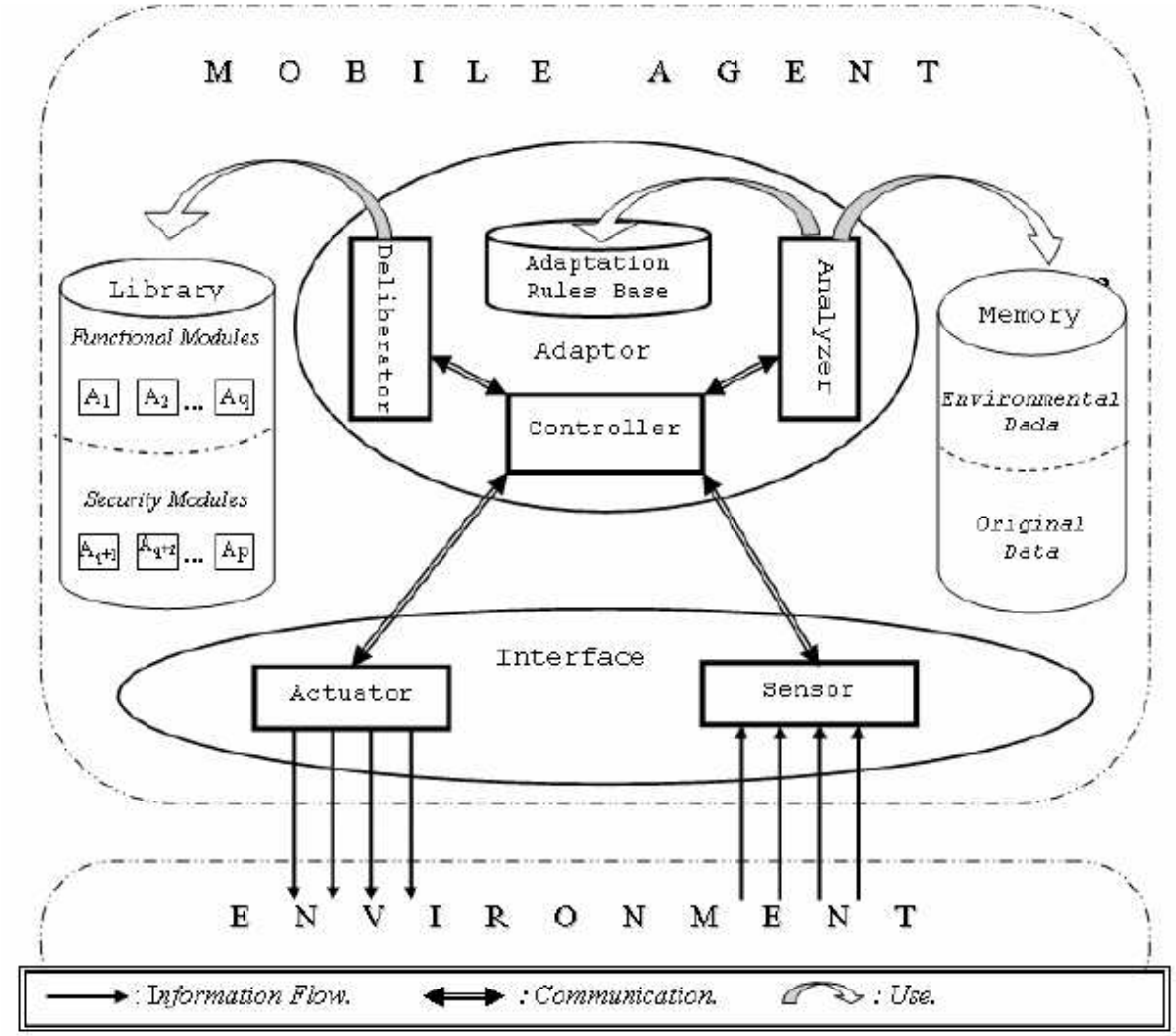


Fig1.3 *Architecture adaptative de l'agent mobile* [Hac 2007]

- ✓ l'adaptateur : c'est le composant responsable de l'adaptation du comportement de l'agent mobile.
- ✓ Une mémoire : dans laquelle l'agent sauvegarde les informations nécessaires à l'accomplissement de sa tâche.

Les détails décrivant les fonctionnalités de chaque composant peuvent être retrouvés dans **[**Hac 2007**]**.

4. LA SECURITE DANS LES SYSTÈMES D'AGENTS MOBILES

Le problème de la sécurité des agents mobiles qui est un problème sous-jacent à celui de la sécurité informatique, et particulièrement si ces dernières se trouvent au niveau un environnement ouvert et exposé tel que: Internet dans lequel la possibilité d'attaque de différentes natures se présente.
Une attaque est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel) ou bien même de l'utilisateur à des fins non autorisées.
Les motivations des attaques peuvent être de différentes sortes :

- obtenir un accès au système pour réaliser une machine capable d'attaquer d'autres machines (attaque par rebond).
- voler des informations telles que les informations secrets industriels, des informations privées sur un utilisateur (données bancaires), des informations sensibles d'une entreprise…
- empêcher le bon fonctionnement d'un service. . .

4.1 Les types d'attaques

Les attaques classiques dans les systèmes distribués sont diverses. Elles peuvent être passives ou actives. En ce qui concerne, le système à base de code mobile et particulièrement le cas de l'agent mobile où la capacité de mobilité de cet agent sur le réseau engendre d'autres types d'attaques, ces dernières peuvent être causées aussi bien par l'agent ou par l'hôte accueillant cet agent. Nous focalisons dans ce qui suit sur celles liées à l'interaction entre l'agent mobile et l'hôte visité.

L'échange entre l'agent mobile et l'hôte donne naissance à des comportements de malveillance liés à la nature de l'acteur qui les provoque. Par conséquent, on distingue les deux classes d'attaques suivantes:

- ✓ Les attaques des agents visant les hôtes.
- ✓ Les attaques des hôtes contre l'agent.

4.1.1 Les attaques des agents visant les hôtes

Cette première situation est perçue quand l'agent peut mettre en danger l'hôte accueillant sur lequel il s'exécute. Ce genre d'attaque a été largement étudié depuis de nombreuses années. On distingue principalement sept types d'attaques [Bob 2000]:

a. La mascarade

Une mascarade a lieu quand un agent non autorisé prétend être un autre agent. Elle peut avoir pour but d'obtenir des ressources auxquelles l'attaquant n'a normalement pas droit ou de faire endosser la responsabilité de certaines actions d'un autre agent.

b. Le déni de service

Un déni de service a lieu lorsqu'un agent consomme trop de ressources. Par exemple, la bande passante de la connexion réseau. Ces attaques peuvent être intentionnelles ou non (erreur de programmation). Le problème avec un agent mobile est que le code est en principe écrit en_dehors_de l'hôte qui l'exécute et il peut contenir du code malveillant.

Quand un agent arrive sur un hôte, il faut qu'il soit authentifié puis soumis à la politique de sécurité qui le concerne. Cela permet d'empêcher l'accès d'un utilisateur ou d'un processus non autorisés à des ressources protégées. S'ils arrivent à avoir accès, il y aura un vol d'information.

c. Les dégâts

Des dégâts peuvent être causés lorsqu'un agent détruit ou modifie des ressources ou des services en les reconfigurant, en les modifiant ou en les effaçant de la mémoire ou du disque. Tous les autres agents sur l'hôte qui utiliseront ce service ou cette ressource seront touchés.

d. Le harcèlement

Il y a harcèlement lorsqu'un agent mobile ennuie les gens par des attaques répétées. Cela arrive lorsqu'un agent mobile affiche à répétition, à titre d'exemple, des images publicitaires non désirées sur l'écran de l'hôte sur lequel il s'exécute.

e. L'ingénierie sociale

L'ingénierie sociale aura lieu lorsque les personnes ou les hôtes sont manipulés par l'agent mobile en utilisant la désinformation. Par exemple, un agent mobile peut demander le mot de passe de l'utilisateur sous la fausse autorité de l'administrateur système dans ce cas l'agent exploite la confiance existante entre l'administrateur et l'hôte pour réaliser des gains.

f. La bombe logique

Une bombe logique est une des attaques décrites ci-dessus dont le déclenchement est basé sur un événement externe (une date, un emplacement de l'hôte dans un certain périmètre du réseau).

Ces types d'attaques consistent à faire exécuter du code mobile malicieux au sein d'un environnement d'exécution. C'est l'attaque crainte par tous les fournisseurs de ressources et par tous ceux qui fournissent des services.

4.1.2 Les attaques des hôtes contre l'agent

Cette deuxième situation est caractérisée par des activités malveillantes des hôtes envers l'agent. Ce type d'attaque vient de l'environnement de calcul accueillant et responsable de l'exécution de l'agent. Elle Souligne que si un hôte exécute l'agent il aura l'autorisation d'accéder à son code et à son état. Par conséquent, l'agent est exposé aux différentes opérations légales ou illégales.

F. Hohl [Hoh 1998] définit un hôte malveillant comme étant un hôte capable d'exécuter un agent provenant d'un autre hôte, et qui essaye de nuire au bon fonctionnement de l'agent mobile d'une manière quelconque. Dans [Hoh 1998], les différentes attaques d'un hôte contre un agent mobile sont identifiées. Nous détaillons ces différentes attaques dans ce qui suit :

a. Espionnage du code

Pour exécuter l'agent mobile, l'hôte doit être en mesure de lire son code. La connaissance du code de l'agent mobile mène à:

- ✓ La connaissance de la stratégie de l'exécution de l'agent.
- ✓ La connaissance des structures physiques du code et des données dans la mémoire de l'hôte.
- ✓ Et parfois, la connaissance d'une partie des données de l'agent mobile.

b. Espionnage des données

La lecture des données privées d'un agent mobile par un hôte est très critique vu que cette attaque ne laisse pas de trace contrairement à l'attaque de modification des données. C'est un problème qui concerne certaines classes de données dont la simple connaissance implique une perte de confidentialité. La clé privée est un exemple de cette catégorie de données.

c. Espionnage de l'état

Dès que l'hôte prend connaissance du code de l'agent mobile et de ses données, il peut déterminer l'étape suivante de son exécution et même si on protège les données utilisées par l'agent mobile, il est difficile de protéger l'information concernant son état d'exécution. C'est un problème important parce qu'avec la connaissance du code, l'hôte malveillant peut déduire des informations sur l'état de l'agent. Par exemple, il peut savoir si une offre est meilleure ou non en observant simplement l'état d'exécution sans connaître les données de l'agent mobile.

d. Manipulation du code

Si l'hôte est capable de lire le code et s'il peut accéder à la mémoire réservée au code, il aura la possibilité de le modifier. Cette modification peut être permanente en implémentant, à titre d'exemple, des virus … afin d'attaquer d'autres hôtes se trouvant dans l'itinéraire de l'agent mobile ou bien temporaire en modifiant seulement la manière selon laquelle l'hôte exécute l'agent mobile.

e. Manipulation des données

Si l'hôte connaît la localisation physique des données dans la mémoire et la sémantique de leurs éléments, il peut modifier ces données. Un hôte attaquant peut modifier aussi bien les résultats obtenus par l'agent mobile au niveau des hôtes précédents, ainsi que les données propres à l'agent mobile (l'identité de l'hôte d'origine, le prix d'un produit, les caractéristiques techniques…..).

f. Manipulation de l'état

Même si on parvient à sécuriser les données de l'agent mobile, un hôte malveillant peut effectuer une attaque en manipulant l'état de l'agent mobile. Il peut modifier le comportement de celui-ci en modifiant son état d'exécution. L'hôte peut, par exemple, forcer l'agent à faire un choix qui avantage l'hôte attaquant.

g. Exécution incorrecte du code

Sans changer ni le code ni l'état d'exécution de l'agent mobile, un hôte malicieux peut modifier la façon dont il exécute le code de l'agent. Il peut par exemple retourner une fausse valeur quand il procède à la comparaison de son prix avec un prix minimal fixé par l'hôte d'origine.

h. Mascarade de l'hôte

L'émetteur de l'agent mobile doit s'assurer de l'identité de l'hôte qui reçoit cet agent. Si une tierce partie intercepte l'agent ou fait une copie de celui-ci, elle pourra masquer son identité en passant par celle du vrai récepteur et déclencher l'exécution de l'agent. La mascarade est suivie généralement d'une autre attaque comme l'attaque de l'espionnage des données.

i. Déni de service

Un hôte malicieux peut ainsi s'abstenir d'exécuter l'agent mobile i.e. arrêter ou retarder son exécution. Cette action est considérée comme une attaque étant donné que cet hôte peut connaître le dernier délai de validité de l'offre d'un autre hôte. L'hôte attaquant peut retarder l'agent jusqu'à ce que le délai de l'offre expire.

j. Espionnage des interactions avec les autres agents

Un agent mobile peut effectuer des achats à distance au niveau d'un hôte autre que celui où il est entrain d'exécuter son code. Si les interactions entre l'agent et cet hôte ne sont pas protégées, l'hôte courant peut observer ces achats et peut même espionner l'exécution du code de l'agent mobile. Cette attaque peut mener à l'attaque de la manipulation de ces interactions.

k. Manipulation des interactions avec les autres agents

Si l'hôte courant peut manipuler les communications de l'agent avec les agents qui s'exécutent au niveau d'autres hôtes, il peut agir sur l'identité de cet agent. L'hôte attaquant peut ainsi rediriger ces interactions de l'agent sur un autre hôte.

l. Retour des résultats erronés des appels systèmes effectués par l'agent

Un hôte attaquant peut retourner des résultats erronés des appels système que l'agent mobile exécute. A titre d'exemple, lorsque l'agent mobile veut vérifier si l'hôte courant est bien son hôte d'origine, il lance un appel système pour connaître l'identité de l'hôte courant. Celui ci peut retourner une fausse adresse en se faisant passer pour l'hôte d'origine. L'agent se trompe et agit comme s'il était chez lui.

m. Réexécution de l'agent

La réexécution à lieu lorsqu'un hôte copie l'agent, une partie de l'agent ou un message de celui-ci et le ré-exécute. Par exemple, un hôte malicieux peut ré-exécuter un message d'achat d'un produit ou de payement d'une facture ou tout simplement ré-exécuter l'agent mobile avec des données différentes.

4.2 Les techniques de protection

Après avoir présenté les types de menace pouvant altérer le bon fonctionnement de l'agent mobile ou bien de l'hôte visité, la présentation des techniques de protection qui visent à protéger ces deux entités contre les différents comportements malicieux est indispensable.

4.2.1 La protection de l'hôte

La protection de l'hôte contre l'agent mobile consiste à utiliser des mécanismes d'authentification, de contrôle d'accès, de vérification de la sémantique de l'agent mobile et le suivi des actions réalisées par l'agent durant sa vie sur l'hôte.

En outre, Certains hôtes exécutent l'agent mobile dans un environnement restreint appelé carré de sable ou bac à sable (sandbox) [Con 2005] et vérifient ainsi son comportement sans risque.

a. Sandboxing

Le sandboxing (connu en français sous le nom de « bac à sable ») est présent dans Java depuis la version 1.0 sortie en mai 1995.

La possibilité qu'offre Java de pouvoir créer des applets fût en grande partie responsable de son succès. Les applets sont des programmes java intégrés au sein de pages web. Ils sont chargés et exécutés automatiquement par le navigateur qui accède à la page. Cela pose des problèmes de sécurité évidents.

L'idée principale derrière le sandboxing [Gol 1996] est « qu'un programme ne peut faire des dégâts que si son accès au système d'exploitation sous-jacent n'est pas limité ». Ainsi, en limitant l'accès du programme aux ressources de la machine, on limite les risques. Pour cela, on va confiner le code à exécuter dans un environnement dont les accès au système d'exploitation sont contrôlés et limités (Fig1.4). Il faut, cependant, noter que le code qui s'exécute dans une sandbox ne peut avoir que des fonctionnalités réduites étant donné qu'il est limité sur les ressources auxquelles il peut accéder. En outre, l'approche de la Sandbox est assez lourde; car quelquefois il est suffisant d'établir des schémas de contrôle d'accès qui limitent l'impact d'une attaque.

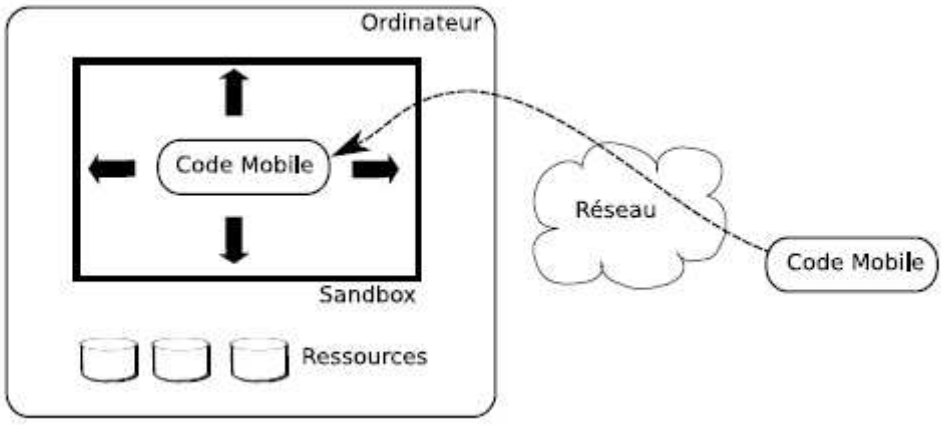


Fig1.4 *le sandbox* [Con 2005]

b. Signature du Code

Ce modèle a été utilisé par Microsoft au sein de ses contrôles activeX et par SUN dans le JDK Java 1.1 sous la dénomination d'applets signées. Le créateur du code va signer numériquement ce dernier. Il permet ainsi à toute personne qui le désire de vérifier la signature. Si la signature est valide, on peut être certain de la provenance du code (le fournisseur) et de son intégrité (le code n'aura pas subi de modification) comme présenté dans la figure (Fig1.5). Le code exécuté dans ce contexte est moins limité en termes de fonctionnalités que celui qui s'exécute dans une sandbox.

De plus, le code ne sera exécuté que si le système autorise l'exécution du code signé par la clé associée au créateur du programme. Il faut noter cependant que, même si l'intégrité du code pourrait être prouvée, cette solution ne permettrait pas de garantir le comportement de l'application lors de son exécution.

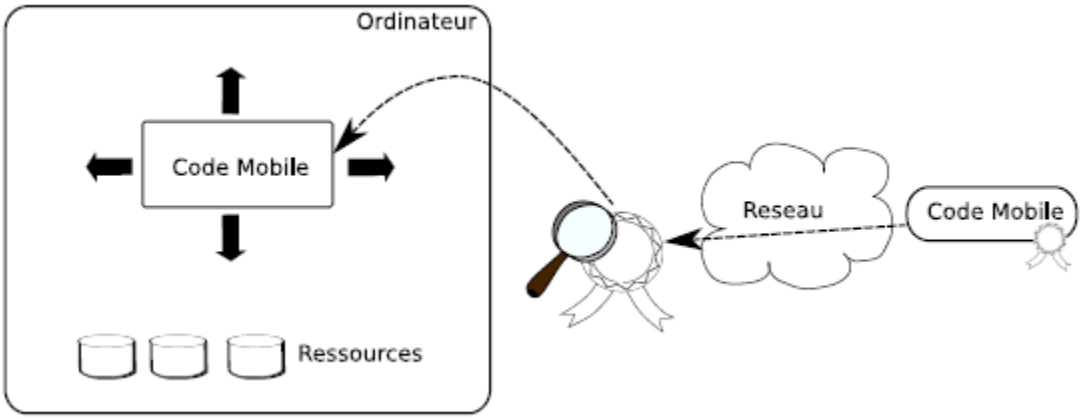


Fig1.5 *la Signature numérique du code* [Con 2005]

Ce système est donc dépend de l'algorithme de hachage générant la signature du code. Si ce dernier n'est pas suffisamment fiable au niveau de l'unicité des empreintes, un attaquant pourrait alors modifier le code de l'agent tout en obtenant une signature identique.

4.2.2 La protection de l'agent mobile

La protection d'un agent contre son hôte est connue dans la littérature sous le nom de « malicious host problem ». Ce problème vise à protéger l'agent mobile contre l'hôte qui l'exécute, les techniques de protection d'un agent sont subdivisées essentiellement en deux catégories les techniques préventives et les techniques de détection.

a. Les techniques de protection basées sur la prévention

La prévention s'exprime par une politique de cloisonnement des informations d'une part et par des règles de comportement des utilisateurs du système informatique, d'autre part. Le mécanisme de prévention a pour but de rendre l'accès et la modification de l'agent difficile. Parmi ces approches on peut trouver:

La technique proposée par wilhem [Wil 1997] consiste à utiliser un coprocesseur dédié à l'exécution de l'agent. L'agent s'exécute exclusivement à l'intérieur de ce périphérique et ne dialogue avec l'hôte visité qu'à travers une interface sécurisée appelé "tamper proof devices /Trusted Processing Environment (TPE) " ou " environnement d'exécution de confiance". Le périphérique TPE est fabriqué sous le contrôle d'une autorité de confiance et dispose d'un certificat et d'une politique de sécurité. Dans cette approche, les agents sont cryptés par la machine de leur propriétaire et ne seront plus exécutés par l'hôte visité mais par le périphérique TPE. Ainsi les agents resteront cryptés tout au long de leur parcours de migration et sur chaque hôte visité. Quand ils arrivent au niveau de leur hôte d'accueil, ils sont toujours cryptés et accèderont au périphérique TPE où ils seront décryptés puis exécutés.

La notion du Black box est utilisée dans la technique "Boite noire limité dans le temps" ou bien appelé en anglais "Time Limited Black Box".

Le Black box est définie comme un environnement software dans le quel seulement les entrées et les sorties sont observables contrairement au comportement interne.

La boite noire limité dans le temps garantit la sécurité pendant une période de temps [Hoh 1998]. Ce mécanisme est basé sur l'algorithme de confusion (MESS-UP) qui génère un agent à partir d'un agent initial qui a un code et des données différentes mais génère les mêmes résultats; ce nouveau code généré est difficile à analyser et sa sémantique est incompréhensible.

L'idée de protection de l'agent mobile proposée par Sander et Tschudin [San 1998] est la suivante : soit une fonction f matérialisée par un agent A, cette fonction est cryptée en E(f) qui cache les fonctionnalités et les détails de f. Un programme P(E(f)) est écrit pour implémenter E(f), ce qui produit comme résultat un nouvel agent B pour un agent A en entrée. L'agent B migre sur l'hôte distant où il sera exécuté sur une donnée x. Le résultat retourné est récupéré par le propriétaire en exécutant l'algorithme de décryptage $E^{-1}(P(E(f)))\ (x)=f(x)$. Au niveau du l'hôte distant, P(E(f)) (x) est exécuté. Ce qui cache les détails et assure la sécurité de l'agent.

L'utilisation des techniques de prévention est difficile et coûteuse pour assurer la protection des agents contre les différents faits malveillants. Ceci est dû essentiellement à leur exigence en matériel onéreux. Suit à ces limites, un ensemble de technique dite de détection sont présentes.

b. *Les techniques de protection basées sur la détection*

Le mécanisme de détection vise la détection des modifications illégales du code, de l'état et du flux d'exécution de l'agent mobile. Bien que le code statique puisse être facilement protégé par la signature digitale, l'état et le flux d'exécution sont des composants dynamiques et sont difficile à protéger. C'est pourquoi un nombre de mécanisme et d'approches de détection sont proposés:

La technique proposée par Esperza et al [Esp 2003] est basée, sur la limitation du temps d'exécution d'un agent dans les hôtes. Chaque hôte doit sauvegarder le temps d'arrivée et de fin d'exécution de l'agent puis les envoie avec les résultats à l'hôte d'origine, afin de vérifier, s'il y a une incohérence dans le temps d'exécution ou de transmission. Dans le cas où l'hôte est considéré comme suspect, il sera sanctionné, supprimé de l'itinéraire de l'agent, et ses résultats seront écartés et l'agent sera émis à nouveau.

Le protocole proposé par Vigna [Vig 1998] a pour objectif, la détection de n'importe quelle modification illégale du code, de l'état et du flux d'exécution du code de l'agent.

Ce mécanisme est basé sur l'utilisation des « post-mortem analysis of data » appelé « traces ». Celles-ci sont rassemblées pendant l'exécution de l'agent mobile sur l'hôte distant.

Les traces sont utilisées en tant que base de vérification de l'exécution du programme. Leur but est donc de vérifier l'historique de l'exécution de l'agent par rapport au programme de l'agent. Dans ce cas, le propriétaire de l'agent peut prouver que les opérations demandées ne sont jamais exécutées par l'agent et donc, on en déduit alors que l'hôte est malicieux.

Farmer et al [Far 1996c] définissent de leur côté, un mécanisme qui permet à un agent d'évaluer les privilèges dont il dispose sur un hôte particulier. Ce qui permet au propriétaire de l'agent de limiter les actions que l'agent peut effectuer. L'approche repose sur une fonction protégée qui permet l'évaluation de l'état de l'agent sur chaque hôte visité. La fonction sera exécutée une fois l'agent arrivé sur un hôte donné et permet de vérifier la stabilité de son état. L'existence d'une telle fonction protège l'agent en détectant les manipulations de son état. La fonction repose sur un calcul complexe à partir d'un ensemble de variables d'état. Une amélioration a été proposée par Jansen ([Jan 2000], [Jan 2001a], [Jan 2001b]) et qui consiste à séparer la structure de données définissant le comportement de l'agent de son propre code. Cette structure sera définie dans un certificat conforme à la norme X509[ISO9594-8]. Dans le certificat, on définit les droits et les responsabilités d'un agent sur un hôte donné. On distingue les certificats d'attributs dans lesquels on définit le comportement de l'agent et les certificats de politique servant à définir le comportement de l'hôte envers tous les agents qu'il accueille.

c. Discussion

Une synthèse discutant les avantages et les inconvénients des différentes approches de protection de l'agent mobile s'impose. Elle permettre de mettre en évidence les lacunes à combler et qui doivent servir de base à notre réflexion. L'approche décrite par Wilhem [Wil 1997] présente une solution très puissante pour sécuriser les agents sur l'hôte d'exécution ainsi qu'à travers le réseau. Toutefois, le périphérique TPE n'est pas facile à fabriquer ce qui explique son coût élevé. De plus, l'environnement d'exécution de confiance TPE ne présente pas les performances d'un ordinateur, ce qui réduit l'efficacité d'exécution de l'agent.

Concernant l'approche "Time Limited Black Box", elle garantit la sécurité pendant une période de temps [Hoh 1998] et après cette période, l'exécution sécurisée de l'agent n'est plus assurée. Par ailleurs, la principale difficulté dans ce mécanisme est comment estimer le temps de sécurité car il dépend de la capacité de calcul des hôtes malveillant. On peut lui reprocher aussi le manque de fondement théorique. De plus, la sécurité de l'agent est temporaire et n'est applicable qu'aux agents qui transportent des données à courte durée de validité. L'agent peut être enregistré et analysé lentement afin de déduire les données qu'il transporte. En outre, la taille du code généré est généralement plus grande que celle du code originale, et spécialement si on utilise le code obscurci[1].

La technique présentée par Sander et Tschudin [San 1998] présente une idée intéressante mais, la difficulté dans ce cas est de comment trouver la fonction qui s'exécute dans une forme cryptée. Actuellement, ce mécanisme est appliqué aux fonctions polynomiales et rationnelles et donne des résultats erronés pour des données ordinaires.

Nous notons que, les techniques de prévention sont coûteuses et difficile à implémenter. Les techniques [Far 1996c, Esp 2003, Vig 1998, Yar 1996] sont plus faciles à implémenter et présentent des idées intéressantes mais elles sont appliquées dans un cadre restreint. Le point fort de la technique proposée par vigna [Vig 1998] est que la répudiation est détectée d'une manière très simple et efficace. Cette approche présente plusieurs limites:

- Un tel protocole exige une infrastructure qui assure la distribution et la gestion des clés publiques, ainsi que l'établissement des bilans des services et la sanction des hôtes malicieux.
- Une cryptographie efficace nécessite une extension de clé et donc des ressources supplémentaires.
- La taille de la trace augmente au fur et à mesure durant l'exécution.

[1] En anglais : "obfuscated code ".

- Le mécanisme de la trace cryptographique est un mécanisme de détection capable d'identifier et de sanctionner les sites malveillants à partir d'une liste de suspects qu'il ne peut pas lui-même déterminer.

L'approche de Farmer et al [Far 1996c] protège l'agent contre une utilisation illicite en fournissant une preuve des intentions réelles de son propriétaire mais n'offre aucune protection des données que l'agent transporte. Nous citons, la technique de la limitation de temps d'exécution [Esp 2003] qui ne peut être utilisé que dans une application où l'agent mobile retourne à son propriétaire ou l'hôte d'origine. Si on imagine que l'agent a exécuté une opération d'achat au niveau d'un hôte malveillant, la vérification du temps d'exécution ne sert à rien. De plus, le protocole traite les hôtes honnêtes qui ont des capacités de calcul faible et les considère comme suspects si l'agent passe plus de temps que le temps d'exécution prévu.

Suite à cette discussion, nous avons visé notre réflexion à l'utilisation du concept de la confiance présenté au niveau des travaux de madame Hacini **[**Hac 2007**]** et nous avons stipulé ainsi pour quoi pas ne s'assurer d'avance que l'hôte d'accueil de l'agent mobile est un hôte de confiance avant l'accomplissement de la transaction affecté à cet l'agent.

5 CONCLUSION

Au niveau de ce chapitre, nous avons présenté les concepts de base relatifs aux agents mobiles, ainsi que ses différents types. En suite, nous avons étudié le problème de sécurité des agents mobiles en mettant en évidence les différents types d'attaques possibles provenant des hôtes ou bien des agents mobiles. Nous avons discuté la protection des deux acteurs en mettant l'accent sur celle de l'agent mobile.

Nous avons étudié les différentes techniques basées sur la prévention ou la détection garantissent l'exécution sécurisée des agents mobiles sur les différents hôtes. En se basant sur cette étude nous constatons que chaque approche essaye d'améliorer ou de travailler sur les inconvénients de celle qui la précède. En plus, en analysant ces différentes approches, nous avons conclus que la conception d'une solution générique de sécurité pour les agents mobiles reste un problème ouvert. Nous jugeons que l'utilisation d'un protocole ou d'un autre dépend des besoins spécifiques à l'application qui utilise le paradigme agent. Par exemple, l'utilisation du protocole de la limitation du temps d'exécution [Esp 2003] est plus sécuritaire dans les applications de recherche d'information à base d'agent mobile.

A cet effet, nous essayons de proposer une solution qui semble plus générale et qui se base sur l'utilisation de la notion capitale pour l'accomplissement de tout type de communication sur Internet qui est la confiance. Donc, notre réflexion a mis en évidence que la sécurité de l'agent mobile a un lien intrinsèque avec le degré de confiance de l'hôte visité. Nous considérons alors que la solution

aux problèmes cités repose sur la confiance inspirée par l'hôte visité et la détermination de sa responsabilité en cas d'attaque.

Notre objectif consiste alors, à l'établissement d'un ensemble de métriques permettant l'estimation de la valeur de la confiance placée en l'hôte visité, et par conséquent assurer que l'exécution de l'agent mobile se limite exclusivement aux des environnements de confiance. Avant de présenter les détails de ce calcul (qui seront présentés dans le chapitre 3) nous allons d'abord donner au niveau du chapitre suivant un aperçu sur le concept de la confiance ainsi que, quelques métriques servant à son évaluation.

Chapitre 2: LES METRIQUES DE LA CONFIANCE

1. INTRODUCTION

Le développement des systèmes informatiques distribués donne lieu à l'existence de plusieurs entités de différentes natures qui coopèrent et collaborent entre elles afin de réaliser des tâches particulières. La collaboration est le résultat de l'interaction, l'échange et même le partage d'un ensemble d'informations entre les différentes entités. Cet échange nécessite un certain degré de confiance qui varie selon l'importance des données échangées.

La question de la confiance est fréquemment posée dans différents domaines de la vie et une vaste littérature existe sur ce sujet. L'hétérogénéité des définitions et l'absence d'une définition simple et commune ne doit pas surprendre puisqu'il s'agit d'un phénomène traité par différentes disciplines. Ainsi, les points de vue recensés sont à replacer dans un contexte bien spécifique selon les objectifs finaux de chacune.

La confiance est donc utilisée sous plusieurs formes selon le domaine et le contexte de son utilisation. Elle peut être vue comme une métrique influencée par un ensemble de paramètres.

Dans le cas d'un agent mobile qui se déplace vers un hôte d'accueil afin de réaliser une tâche spécifique pour son propriétaire, il est raisonnable et nécessaire que ce dernier évalue le degré de la confiance de cet hôte pour pouvoir s'exécuter en toute sécurité. C'est l'idée qui nous a permis d'exploiter cette notion dans le contexte de sécurisation de l'agent mobile contre les différentes actions malicieuses des hôtes d'accueil.

Au niveau de ce chapitre, nous commençons par présenter le concept de la confiance, les différentes définitions existantes dans la littérature et quelques points de vue de catégorisation de cette dernière. Ensuite, nous exposons les différentes formes de gestion de cette confiance ainsi que les métriques utilisées dans les différents domaines en précisant les paramètres et les facteurs utilisés dans chacune des métriques. De plus, nous associons à chaque métrique quelques critiques.

2. La notion de la confiance et métrique

La question de la confiance est fréquemment posée dans différents domaines de la vie et c'est sans doute parce qu'elle est en crise qu'elle fait aujourd'hui l'objet d'une attention spécifique en particulier dans le domaine économique où elle est largement évoquée et analysée. A l'heure actuelle, il n'existe pas un consensus sur la définition de la confiance; ceci est dû essentiellement à sa nature ambiguë. Par conséquent, la notion de la confiance demeure confuse et l'établissement d'une définition cohérente reste encore à établir [Heb 2004].

Certains chercheurs préfèrent ne pas définir la confiance [Whi 1999, Ben 1999,…], tandis que d'autres chercheurs lui associent diverses définitions.

2.1 Définitions et avantages de la confiance

Dès les travaux fondateurs de Deutsch [Deu 1958], la confiance est définie par les intentions et les attentes croisées des personnes impliquées dans une situation d'échange. Suite à cette définition, une pléthore de définitions de la notion de la confiance a été présentée dans la littérature. Ces définitions sont liées aux domaines d'applications [Mck 2001] c'est-à-dire la mise en valeur de ses caractéristiques essentielles varie selon les disciplines, les auteurs et les domaines.

Des définitions simples peuvent être trouvées, comme en théorie des organisations où le concept de confiance s'associe aux concepts de coordination, de coopération et d'engagement, ou bien en marketing où la confiance est considérée comme un facteur important de la stabilité des relations d'échange fournisseurs-clients et inter-firmes [Heb 2004]. D'autre part, pour le professionnel du marketing Georges Fischer qui considère simplement que la confiance est un actif immatériel [Bel 2004].

De son côté, le scientifique des technologies de sécurité Michel Riguidel, définit la confiance comme " *une relation non réflexive, non symétrique et non transitive* ". "Non réflexive " signifie qu'on ne se fait pas nécessairement confiance à soi-même. "Non transitive" signifie que la confiance ne se transfère pas. "Non symétrique " signifie que la confiance n'est pas nécessairement réciproque [Bel 2004].

De leur côté, Mc Knight et Chervany [Mck 2001] ont considéré que la confiance est supportée par un ensemble de métriques. Ils l'ont définie comme la croyance en la bonne foi, la loyauté, la sincérité, la fidélité d'autrui (ou en ses capacités), la compétence et la qualification professionnelle. Ils ont réalisé une classification qui leur a permis d'établir cinq catégories (*Cf.* Section 2.2.).

D'un point de vue sociologique, Fukuyama et Putnam [Fuk 1995 et Put 1995] ont jugé que la confiance crée des capitaux sociaux, où le capital social est défini par Coleman [Col 1988] comme:" *the ability of people to work together for common purposes in groups and organizations* ".

D'un point de vue économique, la confiance représente un moyen pour diminuer les coûts associés aux critères de choix d'un produit/service et permettant de décider de la réalisation d'une transaction [Lin 2006].

Par ailleurs, Bhattacharya et al. [Bha 1998] ont fourni une discussion très stimulante sur la notion de confiance en se basant sur la définition suivante: « *Trust is an expectancy of positive (or nonnegative) outcomes that one can receive based on the expected action of another party in an interaction characterized by uncertainty* ». Une définition assez attrayante est celle de Rotter [Rot 1971] "Trust is a generalized expectancy held by an individual or group that the word, promise, verbal or written statement of another individual or group can be relieved on".

De toutes ces définitions découle le fait que la confiance est un élément fondateur de tout échange et c'est un facteur essentiel pour la stabilité et la continuité, dans le temps, des relations entre les parties. En plus des avantages économiques, les chercheurs soulignent aussi que la confiance dispose d'un impact important sur l'utilité des sites, et sur la fixation des intentions des visiteurs [Lee 2006].

2.2 Les catégories de la confiance

Beaucoup de chercheurs préfèrent définir la confiance à travers une ou plusieurs métriques. A cet effet, pour comprendre la confiance, il faut d'abord comprendre ses différentes dimensions. Ceci donne lieu à différentes formes de catégorisation. Nous en citons quelques unes:

Une forme de catégorisation de la confiance est celle présentée dans [Lee 2006] où Lee et ses collègues ont souligné que la communication sur Internet est basée essentiellement sur la confiance. Cette dernière est subdivisée en deux catégories représentant la confiance en membre et celle du service offert:

- ☒ La confiance en membre: un membre est l'unité communiqué (le site) ou bien le partenaire.
- ☒ La confiance en service offert : elle concerne tous les services proposés par le partenaire, cette catégorie est impliquée du fait que :
  - La crédibilité du service offert assure les promesses.
  - La qualité de service affecte l'utilité du site en fournissant des mesures de garantie.
  - La qualité de service affecte les intentions d'interaction avec le site visité.

Nous ajoutons aussi que la confiance en membre est influencée par deux paramètres importants qui sont l'aptitude d'un côté et la combinaison de l'intégrité et la bienveillance d'un autre côté, où :

- L'aptitude concerne des facteurs nécessaires qui sont l'exactitude, le bon état, et la sûreté de l'information.
- La réciprocité représente un facteur indispensable au niveau de l'intégrité et la bienveillance.

Nous notons qu'il existe une validation d'un ensemble d'hypothèses qui concerne l'influence de la confiance en (membre et/ou service) sur l'utilité du site, et la fixation des intentions. Pour plus d'information voir [Lee 2006].

De son côté, Zucker définit trois catégories de la confiance selon leur modes de production [Zuc 1986]:

La première considère que la confiance est basée directement sur les caractéristiques propres à la personne (elle ne fait pas l'objet d'échanges) et elle est construite à l'extérieur d'une relation. La deuxième forme est la confiance institutionnelle. Elle est attachée à une structure formelle qui garantit l'engagement effectif des acteurs. Elle peut être liée à une personne ou entreprise (une

marque qui reflète la crédibilité), ou bien liée à des intermédiaires. Ce dernier cas repose sur les garanties d'une tierce partie à propos de l'engagement de deux parties dans une relation d'échange. La troisième forme est la confiance relationnelle. Elle se caractérise par l'existence d'un ensemble de relations d'échange passées dans lesquelles les deux parties d'échanges partagent des valeurs communes dans le but de les transformer en objectifs communs. Cette confiance est le produit d'une relation, de son maintien ainsi que de son développement.

D'autre part, une catégorisation (16 catégories de 1^{ier} ordre et 5 catégories du $2^{ème}$ ordre (*Cf.* Table 1.1)) est posée par Mc Knight et Chervany [Mck 2001] pour comprendre la confiance de référence. Celle-ci signifie faire confiance à une référence par exemple à une personne ou bien à une marque. Plus généralement, elle signifie avoir confiance en quelqu'un ou en quelque chose.

Table 1.1. Les catégories de la confiance [Mck 2001].

Trust related Characteristic	**Second Order Concept Category**	**Count**	**% of Total**
1. Competent 2. Expert 3. Dynamic		14 3 3	
	COMPETENCE	20	20.4
4. Predictable	PREDICTABILITY	6	6.1
5. Good, Moral 6. Good will 7. Benevolent, Caring 8. Responsive		6 10 18 4	
	BENEVOLENCE	38	38.8
9. Honest 10. Credible 11. Reliable 12. Dependable		11 1 8 6	
	INTEGRITY	26	26.5
13. Open 3 14. Careful, Safe 15. Shared		3 3 1	

Understanding 16. Personally Attractive		1	
	OTHER	8	8.2
	Grand Total	98	100.0

Ces catégories sont arrangées, comme soulignent les auteurs, d'une manière intuitive. Nous remarquons, que la bienveillance possède un pourcentage important par rapport à la compétence, la prédictibilité, l'intégrité et à la dernière catégorie (la personnalité attrayante, ouverture, etc.) cela montre son impact sur la disposition de la confiance.

De leur côté, Lin et al [Lin 2005] ont défini la confiance en fonction de trois métriques: l'intégrité (integrity), la bienveillance (benevolence), et la compétence (ability) notées respectivement: I, B, A. Ces métriques sont utilisées pour estimer la confiance [Lin 2006]. Cette dernière est considérée comme un paramètre qui influe sur les performances de la chaine logiciel « supply chain[2] »

On souligne que le travail de Lin se situe dans le cadre de l'amélioration des performances des chaines logicielles.

☒ *La compétence:*

C'est la capacité reconnue d'un partenaire. Elle peut inclure sa qualité de contrôle, le temps d'exécution du service qui résulte, bien sûr, des caractéristiques du matériel et du logiciel du partenaire telles que la vitesse du processeur, la taille de la mémoire etc.

La compétence (A) est calculée par la formule suivante [Lin 2006]:

$$A = \left(\sum_{i=0}^{n} \frac{1}{q_i} \right) \Big/ n$$

Où :

q_i: indique la qualité de contrôle du partenaire "i".

n: indique la période de temps.

☒ *La bienveillance*

La bienveillance est la disposition affective d'une volonté de partenaire qui vise le bien et le bonheur.

La bienveillance est formulée comme suit [Lin 2006]:

$$B = b_1 \times drodd_i + b_2 \times drop_i + b_3 \times eimp_i$$

Sachant que: $\sum_{i=1}^{3} b_i = 1$

[2] Supply chain is a network of autonomous or semiautonomous business entities collectively responsible for procurement, manufacturing and distribution activities associated with one or more families of related products [Lin 2006].

$drodd_i$: c'est une estimation du cas où: le payement a été effectué avant la date limite.

$drop_i$: c'est une estimation du prix commandé.

$eimp_i$: représente le prix sur le marché.

i: indique le partenaire i

☒ *L'intégrité*

Elle désigne l'état des données lors de leur traitement (ou leur transfert) en vérifiant si elles n'ont subi aucune altération ou destruction volontaire ou accidentelle, et ont conservé un format permettant leur utilisation. L'intégrité des données comprend quatre éléments : l'intégralité, la précision, l'exactitude/authenticité et la validité.

L'intégrité est calculée par la formule suivante [Lin 2006]:

$$I = \sum_{i=0}^{n} (2 - \frac{dt_i}{ct_i}) \Big/ n$$

d_t: c'est le temps de livraison du produit commandé.

c_t: c'est le temps de livraison contractuel.

Dans ce cas la métrique finale de la confiance est donnée par:

CONFIANCE = a✕A+ b✕B +c✕I

Sachant que:

$0 \leq (a, b, c) < 1$ et $a + b + c = 1$

a, b, c : ce sont les poids d'importance des paramètres.

Cette métrique exploite six paramètres: q_i pour la compétence, $drodd_i$, $drop_i$, $eimp_i$ pour la bienveillance, et d_t, c_t pour l'intégrité.

On peut alors dire que la confiance T est une agrégation respectivement des valeurs de l'importance des paramètres I et de leurs poids w_i.

$$T = \sum_{k=1}^{3} W_k \times I_k \qquad \text{[Lin 2006]}$$

Cette formule ne permet pas d'identifier la cause du manque de la confiance, par conséquent on ne peut pas préciser un éventuel traitement du manque de confiance [Hac 2006].

2.3 La confiance et la réputation

Les notions de la confiance et de la réputation trouvent une importance cruciale dans les environnements ouverts tels que le domaine du commerce électronique, les systèmes de calcul pair à pair et les systèmes de recommandations. Si on parle de réputation on parle alors d'informations d'historiques de la transaction qui peuvent être récoltées localement [Wag 2003, Jŝa 2004] ou reçues à partir des observations des tierces parties de confiance [Res 2000].

Dans le domaine de pair à pair Wang et Vassileva ont défini la confiance comme : " la confiance est la croyance d'un pair dans les compétences, l'honnêteté d'un autre pair en se basant sur son expérience directe". La notion de réputation est définie en reprenant la définition de la confiance, mais en se basant cette fois sur la confiance des autres et non pas sur l'expérience directe [Wan 2003a].

La réputation est estimée par la formule suivante [Wan 2003b]:

$$r_{ij} = w_t * \frac{\sum_{l=1}^{k} tr_{il} * tr_{lj}}{\sum_{l=1}^{k} tr_{il}} + w_s * \frac{\sum_{z=1}^{g} tr_{zj}}{g}, \; w_t + w_s = 1$$

Où les paramètres suivants sont exploités:

r_{ij} est la valeur de la recommandation du pair *pj* qui est calculée par le pair *pi*.

tr_{il} est la confiance du pair *i* pour le pair *l*. Ce dernier appartient au groupe des pairs dont on possède une valeur de confiance.

tr_{lj} est la confiance du pair *l* pour le pair *j*.

tr_{zj} est la confiance du pair z pour le pair *j*. tel que le pair *i* n'a pas une valeur de confiance préalable sur le pair z.

w_t est le poids attribué au groupe des pairs dont on a une valeur de confiance.

w_s est le poids attribué au groupe de pair dont on n'a pas de valeur de confiance.

Les valeurs de w_t et w_s permettent d'ajuster l'importance d'un groupe.

Dans le même domaine de pair à pair Xiong et Liu [Xio 2003] utilisent la réputation comme étant un paramètre de calcul de la confiance T(u) d'un pair. Cette mesure est influencée par un ensemble de facteurs parmi lesquels nous citons:

- ✓ Les feedbacks de satisfaction obtenue lors de transactions avec les autres pairs.
- ✓ Le nombre de transactions réalisées par le pair pour une éventuelle comparaison des différents feedback. Ces deux facteurs sont quantitatifs.
- ✓ La crédibilité du pair qui permet d'évaluer sa réputation (c'est un facteur qualitatif obtenu du passé du pair).

En se basant sur ces paramètres, la métrique suivante est obtenue :

$$T(u) = \alpha * \frac{\sum_{i=1}^{I(u)} S(u,i) * Cr(p(u,i)) * TF(u,i)}{I(u)} + \beta * CF(u)$$

I(u): représente le nombre de transactions du pair "u" pour une période donnée.

S (u, i): cette valeur est envoyée par le pair "i" et concerne le nombre de satisfactions du pair "u "

P (u, i): dénote l'ensemble des pairs participant dans la $i^{ième}$ transaction avec "u".

Cr (P (u, i)): est la crédibilité des feedbacks soumis par P (u, i) ce qui permet d'évaluer sa réputation.

TF (u, i): c'est la confidence du contexte transactionnel dans la $i^{ième}$ transaction.

CF (u): c'est la confidence de la communauté des pairs intervenant dans la transaction.

α et β se sont les poids associés respectivement à la moyenne des satisfactions reçus (cette moyenne est pondérée par la Cr (P (u, i)) et TF (u, i)), et à la confidence CF (u).

La confidence de ces deux derniers paramètres est influencée par respectivement les caractéristiques de la transaction et ceux de la communauté elle-même des pairs intervenants dans la réalisation de la transaction.

De leur côté, Gomez et al [Gom 2006] ont présenté leur modèle de gestion de la confiance à travers les notions d'anticipation et de prédiction, où l'anticipation est considérée comme un mécanisme qui combine un ensemble d'hypothèses pour l'établissement de la prédiction des futurs événements. Dans ce cadre, l'anticipation utilise la contradiction entre l'information reçue et celle de l'expérience directe antérieure. Ce mécanisme est amélioré par un autre mécanisme qui se base sur un nombre considérable de notions : l'expérience directe ainsi que sur la confiance des autres parties (expérience indirecte), la qualité de service (QoS), la contradiction etc. on retrouve l'ensemble des formules dans [Gom 2007].

Tous ces mécanismes se basent sur la réputation distribuée. Cette information n'est pas publique et doit être fournie, contrairement à la confiance centralisée qui est visible par tout le système. Le e-bay, et le BBB-BEC qui sont largement utilisés dans le domaine du commerce électronique, emploient la réputation, dans ses deux formes. Celle-ci y joue un rôle important. A titre d'exemple, la réputation des vendeurs influe sur le nombre de transactions d'achat sur internet [Sta 2006]. Toutefois, l'utilisation exclusive de la réputation n'est pas toujours sécuritaire dans certaines situations et spécialement dans les domaines du e-commerce ou celui du e-business, dans le sens où un hôte pourrait choisir de rester honnête pendant une durée de temps t passé pour effectuer à l'instant de l'interaction t+1 une action malicieuse (malgré qu'il possède une bonne réputation jusqu'a l'instant t). D'autres limites peuvent être associées à l'utilisation de la réputation qui sont la disponibilité des informations de la réputation et les critères de vérification de ces informations. Le

cas de la réputation centralisée est probant et spécialement celui où l'organisme responsable de la gestion de certificat délivré est en période de maintenance. Ce problème est connu sous le nom de la « non tolérance aux pannes ». Par conséquent, la non disponibilité du site centralisé influe négativement sur la vérification de ce certificat. D'autre part, dans le cas de la réputation distribuée la valeur par défaut des réputations des nouveaux sites est un point de discussion.

Dans le cadre de notre travail, nous essayons d'exploiter et ajuster le calcul de la réputation présenté par Sené [Sen 2005] qui utilise les informations de la réputation reçue des différents hôtes (qui sont appelés les notes de confiance), ainsi que les informations locales qui concernent l'expérience directe. Ces informations sont organisées dans des vecteurs.

L'estimation de la valeur finale de la réputation nécessite un ensemble de paramètres indispensables tels que la crédibilité des hôtes, les valeurs positives ou négatives des notes de confiances reçues de chacun de ces hôtes, les critères de choix des valeurs reçues, etc. Les détails de ce calcul seront présentés dans le chapitre 3.

3. La relation entre la confiance et le risque

La relation exacte entre le risque et la confiance n'est pas encore claire [May 1995, Eng 2004] du fait qu'on ne sait pas s'il faut il considérer le risque comme un antécédent de la confiance ou bien comme un résultat de la confiance [May 1995].

En partant de la confiance, Gefen et al présentent trois modèles de relation entre le risque et la confiance [Gef 2002]:

Le premier suggère que le risque et la confiance agissent indépendamment sur le comportement alors que le second propose la relation de médiation et enfin une relation modérée est présentée au niveau du troisième modèle.

3.1 Le risque et la confiance agissent indépendamment sur le comportement:

Plusieurs études ont été réalisées dans le domaine de la science d'information qui focalisent sur l'effet de la confiance sur le comportement et son effet positif sur l'adaptation des intentions telles que la coopération électronique [Son 1999], sans parler du risque [Gaf 2000, Chr 2000] C'est-à-dire qu'il n'existe pas une relation de cause – effet (une relation de causalité) entre le risque et la confiance mais les deux affectent le comportement [Kim 2000] (voir Figure 2.1).

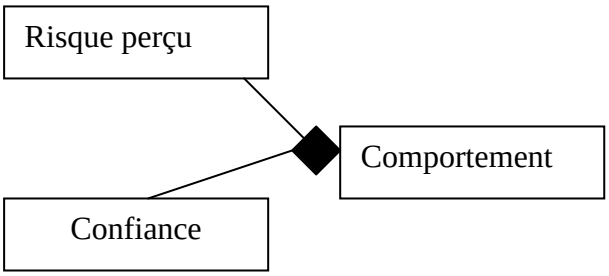


Fig2.1 Un modèle représentant l'effet indépendant de la confiance et du risque sur le comportement.

3.2 Une relation de médiation

Au niveau de cette relation plusieurs opinions ont été posées. Certaines stipulent que la confiance affecte le risque perçu d'une situation et par conséquent le comportement [jar 1999,2000]. Spécialement, dans le domaine du commerce électronique Ratnasingham et Kumar [Rat 2000] ont signalé que la confiance affecte la perception du bénéfique et la perception du risque, en outre Cheung et ses collègues [Cha 2000, Ein 2000, Sta 2006] ont affirmé que la confiance réduit l'incertain et le risque perçu par le client. A titre d'exemple, le risque perçu de donner l'argent à une amie est moins élevé que celui de le donner à un étranger. On peut conclure qu'au niveau de ce modèle il existe une relation causale entre le risque et la confiance (voir Figure 2.2).

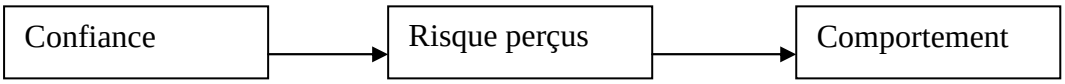


Fig2.2 Un modèle qui représente la relation de médiation entre le risque et la confiance et leur effet sur le comportement

3.3 Une relation modérée

Grazioli et Wang [Gra 2001] ont supposé que si la confiance est élevée, l'impact du risque sur le comportement est minimisé (voir Figure2.3). A titre d'exemple, les informations d'attitude d'un hôte ne sont pas importantes si le degré de la confiance associée à cet hôte est très élevé.

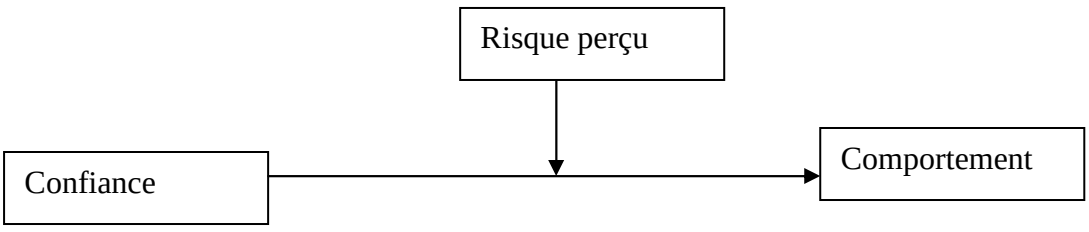


Fig2.3 Un modèle qui représente la relation modérée entre le risque et la confiance et leur effet sur le comportement

En analysant ces modèles, on peut conclure que chacun possède son cadre d'utilisation, et on remarque ainsi qu'il y a une influence directe ou indirecte de la confiance sur le risque et/ou le comportement, et que les stimuli qui augmentent la confiance sont les mêmes que ceux qui réduisent le risque.

D'un autre côté, si on parle du risque, comme un point de départ, plusieurs chercheurs ont donné plusieurs points de vue dans ce cadre parmi lesquels celui de Gray et Jŝang qui stipulent que l'augmentation du risque impose un fort besoin d'assurance de la confiance [Gra 2003, Jŝa 2003]. Une telle situation peut être vue dans le domaine du e-commerce où le risque est lié à deux facteurs importants qui sont la qualité du produit et le montant échangé entre les parties [Bha 2000]. Par conséquent, on peut conclure qu'une décision basée sur la confiance pour s'engager dans une transaction de profit important mène à une situation très risquée [Ruo 2005]. A cet effet, une prise de décision basée sur la confiance doit prendre en considération le facteur du risque avant l'engagement dans une transaction commercial.

Face à ce phénomène, quoi de plus normal que de retrouver en systèmes distribué des systèmes fondés sur la confiance et spécialement dans les systèmes multi agents et particulièrement lors de situations de risque et d'incertitude [Cas 2002]. On cite la technique SECURE (Secure Environments for Collaboration among Ubiquitous Roaming Entities) [Car 2003] qui utilise la relation entre le risque et la confiance pour construire son système de confiance. Cette méthode a fait ses preuves. Toutefois, l'évolution de l'aspect dynamique de la confiance est, dans ce cas, ambiguë.

Dans notre travail qui se situe dans le cadre de la sécurité de l'agent mobile, nous avons considéré le risque comme étant une métrique qui influe sur la confiance placée en l'hôte visité, et particulièrement sur le risque financier qui est un paramètre indispensable pour éviter une sous estimation de la confiance. Une telle évaluation influe négativement sur l'accomplissement de la transaction réalisée par l'agent mobile.

Pour la suite de notre travail nous avons décidé de considérer la confiance comme résultat d'un ensemble de métriques et son estimation résulte donc de l'agrégation de ces dernières; sa valeur dépend bien sûr du choix des métriques, des paramètres employés ainsi que des facteurs intervenant dans leur évaluation.

4. CONCLUSION

Vue l'importance de l'utilisation de la notion de la confiance dans les systèmes distribués, ce chapitre a été consacré à son étude. Nous y avons présenté les définitions existantes dans la littérature et les divers points de vue des chercheurs envers cette notion tels que les formes de sa catégorisation. De plus, nous avons considéré les différentes métriques de la confiance ainsi que sa relation importante avec le risque.

Compte tenu de cet état de l'art, nous avons constaté que la confiance est un concept assez flou pour un certain nombre de chercheurs même s'ils conviennent tous de l'importance de le prendre en compte lors de l'étude des interactions qui englobe deux parties. Nous pouvons affirmer que la confiance est une notion multi-facettes influencée par diverses métriques telles que la réputation ou le risque. Cependant ces deux métriques ne peuvent pas, à elles seules ou chacune à part, décider qu'un agent mobile va s'engager dans une transaction commerciale en toute sécurité. En effet, d'autres éléments interviennent tels que la disponibilité ou la compétence de l'hôte d'accueil.

La décision de l'agent mobile doit donc reposer sur une estimation rigoureuse de la confiance afin d'éviter des réactions inadaptées pouvant léser aussi bien l'agent mobile activant pour le compte d'un organisme que l'hôte d'accueil.

Ceci nous a poussés à déterminer les différentes métriques de la confiance pour la sécurisation de l'agent mobile.

Nous pouvons définir la confiance dans le contexte de la sécurité de l'agent mobile à travers un ensemble de métriques qui sont l'identification, la bienveillance, le risque, la réputation, ainsi que la disponibilité de l'hôte d'accueil. Notre objectif est de préciser au niveau de chaque métrique les paramètres et les facteurs qui influent sur l'estimation finale de la confiance de l'hôte visité. Les détails de ce calcul seront présentés dans le chapitre suivant.

Chapitre 3 : LA TECHNIQUE DE PROTECTION PROPOSEE

1. INTRODUCTION

Les études concernant la technologie d'agent mobile a fait couler beaucoup d'encre. La raison réside dans les diverses avantages offerts par ce paradigme dont l'impact sur l'optimisation de l'utilisation des réseaux est certain. Néanmoins, l'assurance d'une exécution sûre de l'agent mobile est un problème crucial qui doit être résolu afin que cette technologie soit acceptée et puisse être employée par différents applications telles que le e-Commerce.

Notre objectif est de proposer une technique de protection de l'agent mobile basée sur l'estimation de la confiance en l'hôte d'accueil.

L'environnement de confiance étant une des protections des plus sûres, l'agent mobile se trouve ainsi à l'abri des diverses attaques.

L'objectif de ce chapitre est de détailler la technique et la stratégie de l'agent mobile pour se protéger contre les différents actes malveillants.

Nous cernons au début la problématique et nous délimitons le cadre du travail qui se situe dans le volet de la protection de l'agent mobile en se basant sur l'estimation de la confiance de l'hôte d'accueil. Ensuite, nous précisons les paramètres nécessaires pour son établissement. Enfin, nous posons les métriques calculables par le propriétaire de l'agent mobile afin d'orienter le comportement de ce dernier et assurer son exécution saine.

2. La délimitation de cadre du travail

L'échange d'information sur internet nécessite un degré de confiance assez important qui est accumulé au fur et à mesure du déroulement de l'interaction de l'internaute avec le site visité. Par ailleurs, ces dernières années de nombreuses recherches se sont intéressées aux applications liées au e-Commerce afin de garantir des transactions plus efficaces. L'une des tendances qui vise l'amélioration du déroulement de ces transactions est l'utilisation des agents mobiles. Généralement l'agent mobile sélectionne un service en se basant sur des critères tels que la facilité de paiement, la garantie qui accompagne le produit ou la qualité du produit.

Avec l'expansion des attaques internet, les critères de chois ont évolué pour englober des autres caractéristiques telles que la réputation du fournisseur ou la sûreté de la transaction.

L'objectif de ce travail est, en premier lieu, de recenser l'ensemble des facteurs qui influent sur l'estimation de la confiance placée en l'hôte visité afin de permettre, en second lieu, à l'agent mobile de s'adapter en présentant un comportant adéquat.

Nous notons que cet objectif permet d'exploiter les caractéristiques de l'agent mobile qui est capable d'interagir avec l'hôte visité (interaction, observation et inspection) et de s'adapter.

Ce chapitre détaille la technique de protection proposée en précisant l'ensemble des métriques nécessaires à l'évaluation de la confiance lors d'une transaction en ligne.

3. La technique proposée

La notion de la confiance est spécifiée à travers un ensemble de dimensions ou bien métriques qui sont: la bienveillance, l'identification, le risque, la réputation, et la disponibilité. Ces dimensions découlent sur l'identification des différents facteurs qui peuvent être exploités par un agent mobile durant une transaction commerciale afin d'établir sa confiance

3.1 L'identification

L'identification est une métrique fondamentale dans le contexte des transactions électroniques. Elle sert principalement à l'authentification de l'hôte visité. Un ensemble de paramètres participe à son estimation. Nous citons, à titre d'exemple:

- L'identité et/ou le mot de passe
- La forme juridique ou domaine d'activité.
- L'adresse géographique complète.
- Les coordonnées téléphoniques et électroniques (e-mail)
- Le numéro d'immatriculation au registre de commerce ;
- Le numéro d'identification à la TVA,
- etc.

Ces informations sont récoltées par l'agent par interaction avec l'hôte à travers un questionnaire. L'identification est estimée par la formule suivante [Zai 2008]:

$$I = \frac{\sum_{k=1}^{n} V_k W_k}{\sum_{k=1}^{n} W_k} \qquad (1)$$

V_k: est une valeur binaire correspondant à la validité de la valeur du $k^{ème}$ paramètre.

W_k : désigne le poids exprimant l'importance du paramètre.

n : représente le nombre de paramètres intervenant dans l'estimation de l'identification.

3.2 La bienveillance

Elle concerne les bonnes intentions de l'hôte pouvant influer positivement sur l'exécution de la tâche de l'agent mobile. La bienveillance de l'hôte visité est interceptée durant son interaction avec l'agent. L'ensemble des paramètres qui influent sur cette métrique sont:

- Le nombre de fois de saisie des valeurs de paramètres demandés tel que le mot de passe. Il révèle le degré d'hésitation de l'hôte. La valeur de ce paramètre est interceptée par le biais d'un mécanisme d'observation. La formule qui estime ce paramètre est la suivante [Zait 2008]:

$$b_1 = \frac{\sum_{i=1}^{n} \frac{2}{p_i}}{n} \quad (2)$$

p_i : est le nombre de fois de saisie pour chaque paramètre évalué.
n: représente le nombre de paramètres à tester.

- La finesse du détail apporté à la facturation d'un produit révèle la bienveillance de celui qui l'a rédigée. En effet, une facture bien détaillée est un signe de bienveillance. Ce paramètre, noté b_2, est lié à un ensemble de facteurs tels que les frais de livraison du produit ou d'exécution du service (transport, douane, TVA) ou le prix (HT et TTC), la durée de vie et les limites géographiques de l'offre. Ces informations sont récoltées par l'agent durant l'interaction avec l'hôte.

$$b_2 = \frac{\sum_{i=1}^{k} S_i}{k} \quad (3)$$

S_i = 1 si la valeur du $i^{ème}$ facteur correspond bien aux offres (remise, baisse de TVA…) proposées, S_i=0 sinon. Dans ce cas une exception peut être déclenchée.
K : est le nombre des facteurs considéré.

- Un autre paramètre, noté b_3, participe à l'estimation de la bienveillance d'un hôte. Il concerne l'existence d'un contrat préalablement établi entre l'émetteur de l'agent et l'hôte visité. Ce contrat peut être examiné par l'agent afin de vérifier son intégrité en comparant l'empreinte du contrat (résultat d'une fonction de hachage à sens unique) qu'il détient avec celle calculée au niveau de l'hôte. Le mécanisme utilisé pour extraire cette information est l'inspection. Dans ce cas le résultat de cette inspection est binaire :

$$\begin{cases} 1 & \text{si le contrat est valide} \\ 0 & \text{sinon} \end{cases}$$

- la capacité de chiffrement est un paramètre de confiance pour la protection des données personnelles. Elle prouve l'aptitude de l'hôte d'accueil à protéger la confidentialité des informations qui lui sont révélées telles que le numéro de la carte de crédit. Cette capacité dépend éventuellement du type de chiffrement (symétrique ou asymétrique), de l'algorithme de chiffrement (récent ou non, faible ou fort) ainsi que de la taille de la clé utilisée (128, 256 ou 512). L'estimation de ce paramètre b_4 est basée sur les correspondances suivantes [Zai 2008]:

$$\alpha = \begin{cases} 0.25 & si\ la\ taille\ de\ la\ clé < 128bits \\ 0.5 & si\ 128 \leq taille\ de\ la\ clé < 256bits \\ 0.75 & si\ 256 \leq taille\ de\ la\ clé < 512bits \\ 1 & si\ la\ taille\ de\ la\ clé \geq 256bits \end{cases}$$

$$\beta = \begin{cases} 0.5 & si\ l'algorithme\ de\ chiffrement\ est\ symétrique \\ 1 & si\ l'algorithme\ de\ chiffrement\ est\ asymétrique \end{cases}$$

$$f = \begin{cases} 0.5 & si\ l'algorithme\ de\ chiffrement\ est\ faible\ (a\ déjà\ été\ cassé) \\ 1 & si\ l'algorithme\ de\ chiffrement\ est\ fort \end{cases}$$

Ce paramètre est alors évalué comme suit [Zai 2008]:

$$b_4 = \alpha \times \beta \times f \qquad (4)$$

- La présence d'un label ou d'un certificat est un signe de bienveillance du site. Un label est délivré par une tierce partie de confiance. Par ailleurs, un certificat est un élément qui contribue à assurer une meilleure garantie de sécurité et de confidentialité des données personnelles**.** A titre d'exemple, BBB-BEC (Bureau d'Ethique Commercial) ou l'AICPA (American Institute of Certified Public Accountants) gèrent une sorte de label « Web Trust » prouvant que ces sites sont régulièrement contrôlés. Ce paramètre peut facilement être vérifié en demandant une validation de cette information à l'organisme concerné (www.bbb-bec.com). Ce paramètre noté b_5 a pour valeur :

$$\begin{cases} 1 & si\ le\ certificat\ est\ valide \\ 0 & sinon \end{cases}$$

L'évaluation de la métrique de la bienveillance est apportée par la formule [Zai 2008]:

$$B = \frac{\sum_{i=1}^{nb} b_i}{nb} \qquad (5)$$

nb : représente le nombre de paramètres considéré pour l'estimation de la bienveillance.

3.3 La réputation

La notion de la réputation concerne l'historique des comportements de l'hôte visité. Elle est subdivisée en deux catégories dénotant la réputation directe et la réputation indirecte. Elle est dite indirecte lorsqu'elle est révélée par une tierce partie de confiance et elle est dite directe quand l'émetteur de l'agent mobile a déjà interagi avec cet hôte et possède donc une idée sur la manière dont il gère ses transactions. L'estimation de cette métrique a été inspirée par celle établie par Sené [Sen 2005]. Cependant, dans sa formule Sené s'appuie sur la réputation fournie par un ensemble de nœuds d'un réseau ad hoc (réputation indirecte) pour estimer la réputation directe. Dans notre approche, nous établissons l'hypothèse dans laquelle l'agent mobile se méfie de tout hôte visité. De plus, nous considérons que la réputation indirecte fournie par une tierce partie peut être périmée et n'est donc pas forcément crédible. Par conséquent, elle ne doit pas servir de support à la réputation directe évaluée par l'agent lui-même de manière dynamique.

Les informations de réputation reçues des différents hôtes (les notes de confiance), ainsi que les informations locales sont organisées dans des vecteurs. Pour calculer cette valeur, un ensemble de paramètres sont indispensables tels que la crédibilité aussi bien des hôtes que celle des notes reçues (*Cf.* Table 3.1)

Table 3.1. Paramètres intervenant dans le calcul de la réputation

Paramètres	Notation
Les notes de confiance antérieures établies par l'émetteur de l'agent mobile en l'hôte d'accueil j	NCa(j)
La crédibilité que possède l'émetteur de l'agent i en l'hôte k ayant émis ses notes[3]	$CR_i(k)$
Le nombre d'interactions considéré par l'hôte k ayant émis ses notes	ɵ
Le nombre d'interactions maximal considéré par l'émetteur de l'agent	$ɵ_{max}$
La valeur de la confiance associée aux notes de confiance à l'interaction x fournies par l'hôte k	$CNC_k(x)$
Les notes de confiance de l'hôte k en l'hôte j	$NC_k(j)$

- La réputation directe PK (Personal Knowledge) indique une expérience personnelle. Cette valeur est calculée à partir des notes détenues par l'émetteur de l'agent mobile relatives à des interactions antérieures. Elle est établie par la formule [Zai 2008]:

$$PK = \frac{\sum_{q=1}^{\theta} NCa_q(j)}{\theta} \qquad (6)$$

Où $NCa_q(j)$ exprime une note de confiance associée à l'interaction q avec l'hôte j et

θ: détermine le nombre d'interactions antérieures considéré avec $ɵ \leq ɵ_{max}$

- La réputation indirecte EK (External Knowledge) est relative à une expérience externe. Elle est calculée sur la base des notes reçues à partir d'un ensemble d'hôtes. La réputation externe est évaluée à l'aide de la formule:

[3] Note : pour $ɵ_{max}$, les ɵ dernières interactions sont prises en considération (c'est-à-dire les plus récentes).

$$EK = \frac{\sum_{q=1}^{m} NC_{kq}(j)}{m} \qquad (7)$$

Où $NC_{kq}(j)$ exprime une note de confiance associée à l'interaction q avec l'hôte j

Sachant que les valeurs des notes de confiance prises satisfont l'ensemble des conditions suivantes :

- La crédibilité dénotant la confiance que possède l'hôte i en l'hôte k doit être importante. Par exemple: $CR_i(k)>0.8$
- Les notes négatives sont prises en considération. Elles expriment, par exemple, que $NC_k(j)<0.5$
- La valeur de la crédibilité associée à la note de confiance fournie par l'hôte k doit être acceptable. Par exemple $CNC_k(x)\geq 0.6$.

m: indique le nombre des hôtes qui satisfont l'ensemble des conditions.

Nous notons que si plusieurs valeurs de l'ensemble des notes de confiance fournies par l'hôte k vérifient les conditions citées, la valeur de la note fournie qui possède une crédibilité importante est retenue et la valeur la plus récente est favorisée en cas d'égalité des valeurs.

En vertu des formules (6) et (7), celle de la réputation finale est établie :

$$R = \frac{\varepsilon[\theta \times PK] + \xi[\theta_{max} \times EK]}{(\varepsilon \times \theta) + (\xi \times \theta_{max})} \qquad (8)$$

ε, ξ : représentent les poids accordés respectivement aux valeurs des réputations directe et indirecte.

La valeur de ξ est plus petite que ε pour favoriser l'expérience personnelle de l'hôte émetteur de l'agent mobile.

3.4 Le risque

Dans une transaction dans le domaine du commerce électronique le risque est relié à deux facteurs:

- le risque lié au produit/service : il peut concerner la limite de validité du produit ou encore sa sensibilité telle qu'un produit chimique dangereux, ou un produit alimentaire dont la période de péremption est courte (par exemple les laitages). Ce dernier cas est principalement rattaché au délai de livraison du produit. De plus, cette métrique est liée au degré d'implication révélant les limites de responsabilité.

La durée de validité du produit/service est évaluée par la formule suivante [Zai 2008]:

$$Dv = d_{lm} - (d_a + d_{lv}) \qquad (9)$$

Où d_{lm} indique la date limite, d_a désigne la date actuelle et d_{lv} renseigne sur la durée de livraison.

Le facteur τ de vérification de la durée de validité prend la valeur 1 si Dv >0 et 0 sinon. Il est multiplié par un autre facteur dénoté S afin d'ajuster la valeur du risque en fonction d'une durée t soit de péremption du produit/service ou bien choisie par l'émetteur de l'agent mobile pour des raisons précises. L'estimation finale du paramètre r_1 est donnée par la formule ci-dessous [Zai 2008]:

$$r_1 = \tau \times S \qquad (10)$$

Sachant que S prend l'une des deux valeurs suivantes [Zai 2008]:

$$\begin{cases} 0.5, \text{si } D_v \leq t \\ 1, \quad \text{sinon} \end{cases}$$

La valeur t est attachée au degré d'implication de l'hôte d'accueil ainsi qu'à la sensibilité et au type du produit/service (alimentaire ou autre).

- le risque financier est proportionnel au montant mis en jeu. La fonction r_2 d'estimation de ce paramètre est calculée par la formule [Zai 2008]:

$$r_2 = \alpha \times x \qquad (11)$$

Où *x* désigne le montant mis en jeu et α est un facteur relatif à la sensibilité du produit/service et au mode de paiement. Par exemple, le paiement par le biais d'une banque diminue le risque.
Nous définissons les trois variantes suivantes de α:

- α est égale à β/x en cas de risque minime,
- α est égale à β/2x en cas de risqué moyen, et
- α est égale à β/3x en cas d'un risque élevé.

β appartient à l'intervalle [0,1] cette valeur est spécifié par l'émetteur de l'agent.
La métrique finale du risque est évaluée selon la formule [Zai 2008]:

$$K = \frac{r_1 + r_2}{2} \qquad (12)$$

3.5 La disponibilité

La disponibilité est une métrique importante qui intervient en dernier lieu pour confirmer ou infirmer la crédibilité de l'hôte visité. Cette métrique englobe deux paramètres :

- la sûreté des logiciels: l'utilisation des logiciels et des codes sûrs influe sur la disponibilité des systèmes informatiques.

- la compétence d'un hôte: elle est liée à sa capacité de calcul et au débit de connexion. La capacité de calcul est relative à l'infrastructure utilisée. Elle peut concerner la vitesse du processeur, la taille de la mémoire centrale, la taille du disque dur, ou celle de la mémoire cache. Par ailleurs, un faible débit du serveur influe négativement sur le temps de réponse et la disponibilité.

Cette métrique est utilisée après l'estimation de la confiance pour le traitement en cas de manque de confiance (*cf.* Table3.4). L'évaluation de cette métrique est directement liée au temps d'exécution et la formule qui l'estime est la suivante [Zai 2008]:

$$D = \frac{D_{HA}}{D_{EA}} \qquad (13)$$

Où D_{HA} exprime la durée d'exécution de l'agent mobile au niveau de l'hôte d'accueil, et D_{EA} indique la durée d'exécution de l'agent mobile estimé par l'émetteur de ce dernier.

3.5. Algorithme d'estimation de la confiance

A l'issue de la collecte des différentes valeurs de métriques de la confiance au niveau de l'hôte visité, l'agent mobile exécute un ensemble d'opérations (*cf.* Table3.2 [Hac 2006]) et envoie à son émetteur un message qui contient deux types de données: hachées et simples.

Les données hachées Concernent les hachées des valeurs des paramètres collectées dont les valeurs originales devraient exister au niveau de l'émetteur de l'agent mobile. À titre d'exemple, la validation du mot de passe est réalisée par la comparaison d l'haché reçu et celui stocké dans la base de donnée locale de l'émetteur de l'émetteur de l'agent mobile.

Les données simples (données non hachées) sont nécessaires au calcul de la confiance sous leurs formes réelles (non hachées). À titre d'exemple, f, α, et β sont émis sou leur forme originale. Ces trois valeurs contribuent dans l'estimation du paramètre lié à la capacité de cryptage au niveau de la métrique de la bienveillance.

Nous Notons que la fonction de cryptage à sens unique a été utilisée pour protéger les données confidentielles de l'hôte visité tel que le mot de passe.

En outre, puisque l'application de la fonction de hachage à sens unique sur des données de taille différentes donne comme résultat des informations hachées codées dans un nombre fixe de bits, cette solution optimise la taille du message transmis vers l'émetteur de l'agent.

Table3.2.Algorithme du comportement de l'agent mobile

Entrée : la clé publique P_o de l'émetteur de l'agent mobile, les clés de l'hôte courant (P_h, S_h), les données collectées.
Sortie : EM et ES.
1 : Collecter les données (correspondant aux valeurs des paramètres).
Soit {d_1, d_2…d_k) l'ensemble des données qui vont être haché.
2 : Appliquer une fonction de hachage à sens unique à chaque donnée
For i := 1 to k do $M_i = H_a (d_i)$ End For
3 : Concaténer toutes les empreintes et obtenir la clé intermédiaire :
$M = (M_1.M_2…M_k)$
4 : Chiffrer (M, NH) en utilisant la clé publique P_o de l'émetteur de l'agent mobile:
$EM = E_a$ (M, NH)
5 : Utiliser la clé privée S_h de l'hôte courant pour signer EM : $SM = s_a$ (EM)
6 : Emettre EM et SM vers son émetteur**.**

L'émetteur de l'agent mobile va, à son tour, exécuter des actions lui permettant l'estimation de la confiance (*cf.* Table3.3 [Hac 2006]). Elle porte essentiellement sur la récupération, à partir du message recu, des données servant à l'estimation de la confiance:

Table3.3.Algorithme de l'exécution de l'émetteur de l'agent mobile

Entrée : les clés (P_o, S_o) du propriétaire de l'agent mobile, la clé publique P_h de l'hôte courant, EM et ES
Sortie : EQ et SQ

1 : Recevoir EM et SM
2 : Vérifier SM en utilisant l'opération booléenne :
v(EM, SM)
3 : Décrypter EM en utilisant la clé privée de l'émetteur de l'agent mobile et obtenir :
$M= D_h$ (EM)
4 : Obtenir, à partir de M, k empreintes
H (d_1), H (d_2)…H (d_k) (en se basant sur le nombre de paramètres, leur position et la taille de chaque empreinte)
5 : Comparer les empreintes obtenues avec celles présentes dans la base de données.
6 : récupérer les données non haché (NH)
7 : Estimer la confiance en calculant la valeur de T.

La confiance T est calculée selon la formule :

$$T = (IW_1S_1) + (BW_2S_2) + (KW_3S_3) + (RW_4S_4) \quad (14)$$

Le paramètre $S_i \in \{0,1\}$ permet de déterminer la cause du manque de confiance. Ainsi, la valeur 0 de S_i indique que la valeur de la confiance estimée pour la $i^{ème}$ métrique est insuffisante.
Si la confiance est considérée comme insuffisante, la métrique de la disponibilité D est considérée (*cf.* Table3.4).

Table 3.4. Utilisation de la disponibilité pour le traitement du manque de confiance [Zai 2008]

Si (D >1) et (b_1>=1) alors Le degré de disponibilité de l'hôte d'accueil est bas et donc, tolérer la réexécution de l'agent à nouveau si ce n'est pas un déni de service. Sinon Si (S_1=1) et (S_2=1) et (S_3=1) et (S_4=0) alors tolérer l'exécution de l'agent et envoyer la décision si ce n'est pas un déni de service. Sinon

Après l'estimation de la confiance, l'émetteur de l'agent envoie sa décision qui concerne la réalisation ou non de la transaction.

4. Conclusion

L'importance de la notion de la confiance dans le domaine du e-commerce et des systèmes distribués explique son emploi pour la sécurisation de l'agent mobile. En effet, l'estimation de la confiance permet d'adapter le comportement de l'agent mobile en conséquence et garantir son exécution uniquement dans un environnement jugé de confiance. Dans ce chapitre, différentes métriques

permettant l’évaluation de la confiance ont été présentées. De même, les paramètres relatifs à chaque métrique ont été précisés et les formules, servant à leur évaluation, établies. Ces dernières sont simples et n’engendrent pas de surcoût en temps d’exécution; ce qui permet à l’agent mobile de réagir dans un délai convenable.

Suite au détaille de notre approche, le chapitre suivant est consacré à la validation de la formule de la confiance par le biais d’une simulation. Cette dernière s’intéresse à la vérification de l’impact des différentes métriques sur la valeur finale de la confiance.

Chapitre 4 : SIMULATION

ET

EXPIRIMENTATIONS

1. Introduction

Afin de valider notre contribution présentée dans le chapitre précédent, une phase de simulation s'avère indispensable. L'objectif principal de cette étape est de montrer les avantages de notre approche de protection des agents mobiles à travers une simulation au niveau d'une application de commerce électronique. Plus précisément, notre but est d'évaluer les capacités de notre approche de sécurité, qui est basée sur la métrique de la confiance, à détecter les menaces qui peuvent altérer le bon fonctionnement de l'agent mobile.

Ce chapitre regroupe la modélisation et les aspects techniques de la simulation de notre proposition. Nous commençons par donner une description de l'application par le biais d'une modélisation en utilisant UML. Par la suite, nous décrivons les outils techniques employés dans la mise en œuvre de la simulation. L'exemple de simulation est appliqué dans le contexte du commerce électronique dans une application de ventes des téléphones mobiles, de cartes de recharges téléphoniques, etc. On suppose que notre agent effectue des opérations d'achat, vente et de choix du produit. Afin de motiver l'intérêt de notre approche d'un point de vue pratique, nous avons décidé de focaliser sur les opérations d'achat dans lesquelles l'agent mobile achète des cartes de recharge ou bien des téléphones mobiles a travers des codes de retrait du compte bancaire de client. Le choix est justifié par le fait que l'opération d'achat englobe la plut part des paramètres constituant la métrique de la confiance.

Nous fournissons au fur et à mesure des exemples d'interface et de code afin de faciliter la compréhension de cette simulation.

2. Définition du commerce électronique

On appelle "commerce électronique" (ou *e-commerce*) l'utilisation d'un média électronique pour la réalisation de transactions commerciales *(Cf.* Figure 4.1). La plupart du temps, il s'agit de la vente de produits à travers le réseau internet, mais le terme de *e-commerce* englobe aussi les mécanismes d'achat par internet (B-to-B, B-to-C,…).

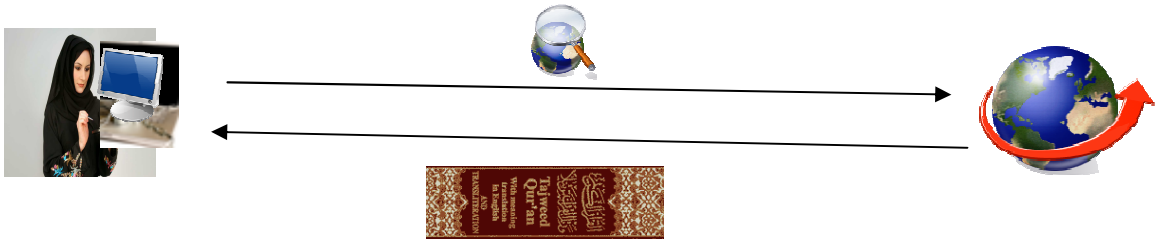


Figure4.1 La forme générale d'une transaction sur internet

- *B to C (business to consumer)* : Le commerce grand public ou la vente en ligne (prolongement du téléachat avec Télétel)

- *B to B (business to business)* : commerce inter-entreprise (Réseaux d'achat, places de marché...)
- *C to C (consumer to consumer)* : ventes aux enchères.
- *A to B (administration to business)* : appels d'offres en ligne, télé-déclarations…

Dans ce domaine tous les deux entités acheteur et vendeur ont besoin d'automatiser la manutention de leurs affaires financières électroniques. Ainsi, l'objectif du e-commerce est comme suit :

- exécution de transactions commerciales entre clients et fournisseurs.
- recherche de produits et services (catalogue).
- commande de produit.
- paiement.
- livraison du produit (éventuellement sous forme électronique).

Contraintes

- protection des informations confidentielle (client et fournisseur).
- respect des règles commerciales entre client et fournisseur (offre sincère, exécution du contrat de paiement).
- respect des droits de propriété (licence, droits d'auteur …).
- disponibilité du service.

3. Agent mobile et commerce électronique

Actuellement, les consommateurs et les entreprises commencent à partir à la recherche de produit sur le réseau et les vendeurs désirent trouver des clients. Seulement, l'extraordinaire quantité d'informations disponibles sur Internet complique les transactions commerciales au point de freiner le développement du commerce électronique aussi bien pour l'acheteur que pour le vendeur. Les agents intelligents et particulièrement mobiles constituent une des solutions qui contribuera à débloquer la situation. Par conséquent, à travers l'automatisation partielle de leurs processus commerciaux, les marchands en ligne peuvent non seulement gagner un nombre plus important de consommateurs à un coût plus faible, mais ils peuvent également collecter une quantité plus vaste d'informations sur leurs clients, dans une forme plus facile à exploiter. Cependant, le potentiel de la technologie agent n'est pas encore complètement exploité et des recherches sont encore nécessaires pour améliorer le fonctionnement des agents [Par 2008] et spécialement leur protection du fait qu'ils transportent des informations sensibles et confidentielles.

Nous allons simuler un ensemble d'exemples afin d'affirmer le degré de réalisation de notre contribution. Pour cela, nous commençons par éclaircir, la description générale de notre application à travers des schémas.

4. La description générale de l'application

La forme générale de notre simulation est présentée au niveau de la figure suivante (*Cf.* Figure 4.2):

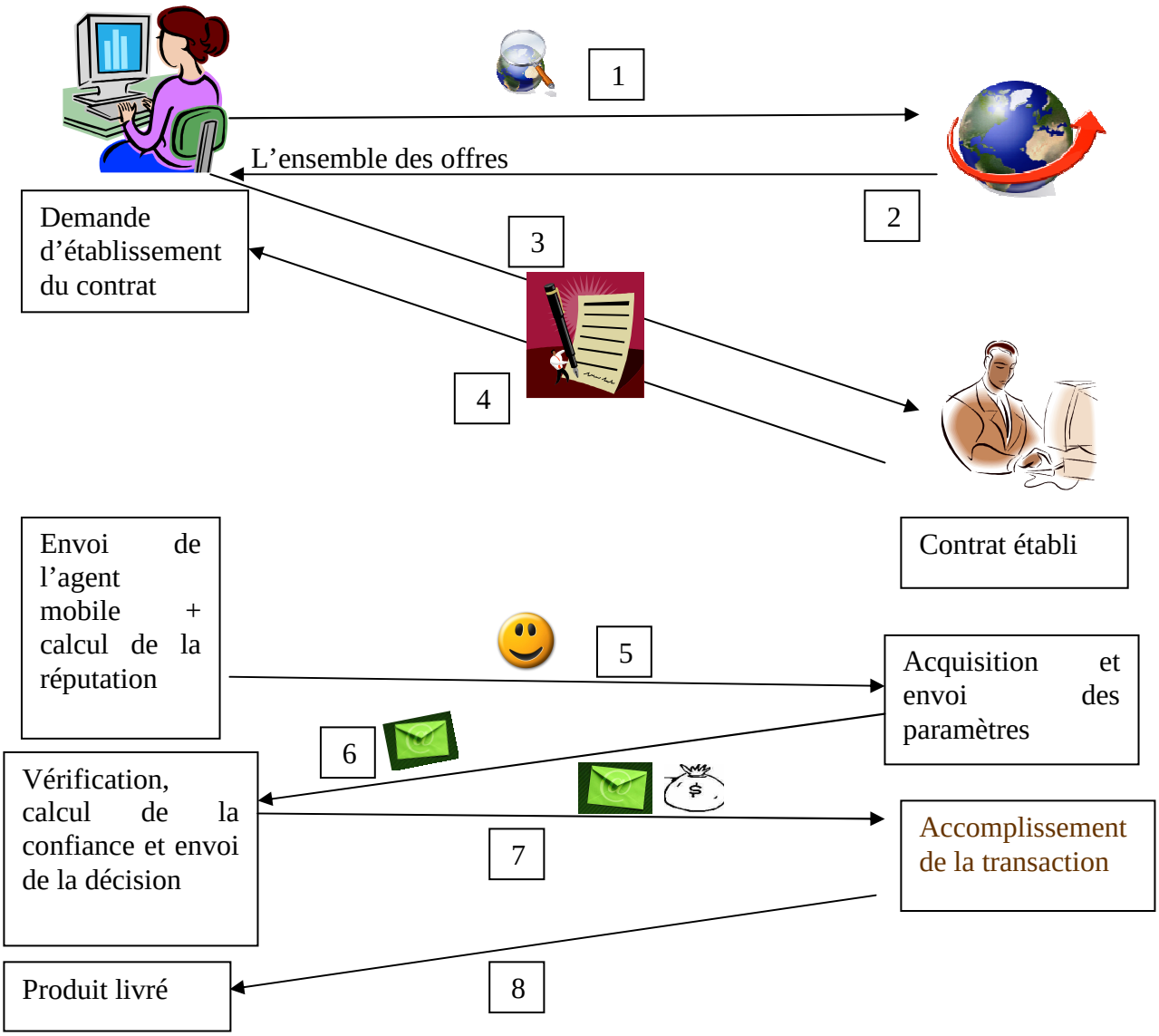


Figure4.2 : La description générale de la simulation

Cette description repose sur un ensemble d'hypothèses. Elles concernent la gestion des relations entre le l'émetteur de l'agent mobile, l'agent mobile et l'hôte visité :

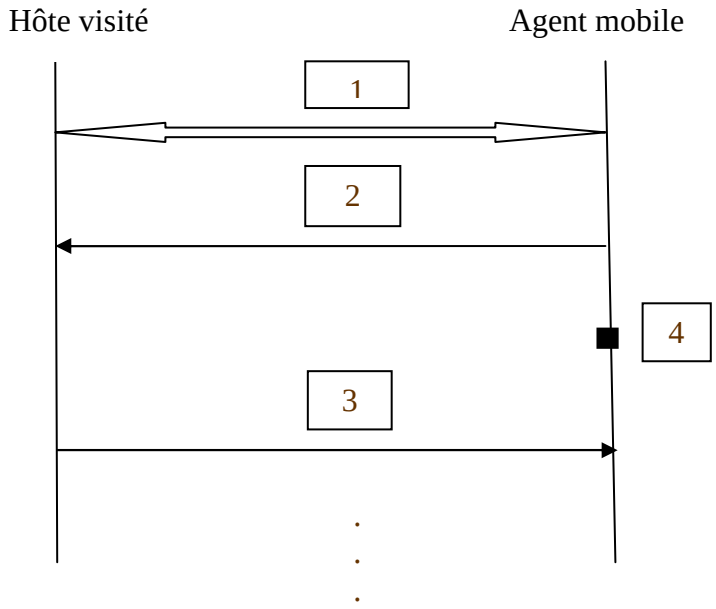
- Un contrat est établi entre l'émetteur de l'agent et l'hôte à visiter.
- L'émetteur de l'agent sauvegarde un ensemble d'informations (les informations initiales) de l'hôte à visité au niveau d'une base de données locale qui sont nécessaires à l'estimation de la confiance. Elles concernent des informations sur le produit ainsi que des informations privées de l'hôte à visiter (elles sont bien évidement liées à la transaction en cours).
- L'agent mobile ne fait confiance à aucun hôte. Il attend la décision de son hôte émetteur, le seul hôte qui est considéré comme sûr, pour accomplir la transaction.

- La réputation est calculée localement par l'émetteur de l'agent en parallèle à la récolte des paramètres par l'agent mobile au niveau de l'hôte d'accueil.
- Les valeurs des métriques obtenues seront sauvegardées au niveau d'une base de données. Elles vont servir au calcul de la réputation dans les transactions futures.

Dans ce qui suit, nous donnons une description détaillée de notre simulation à travers un ensemble de scénarios sous forme de diagrammes de séquence. Afin de mieux observer la dynamique du système nous focalisons sur la partie acquisition des paramètres et calcul de la confiance.

4.1 Le scénario d'acquisition des paramètres

Dés l'arrivée de l'agent mobile au niveau de la plate forme de l'hôte visité, il commence à récupérer l'ensemble des informations nécessaires. Cette récupération se base principalement sur l'interaction de l'agent mobile avec l'hôte visité; le diagramme de séquence suivant montre l'ensemble des interactions accomplies entre l'agent mobile et l'hôte visité :



1 : l'identification initiale (le protocole de sécurité de bas niveau : vérification de l'adresse IP…).

2 : l'agent mobile demande à l'hôte visité la valeur du paramètre considéré à travers le questionnaire.

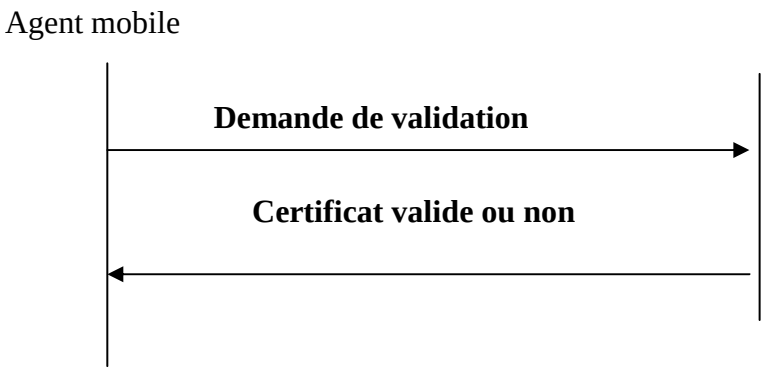
3 : l'hôte visité répond à l'agent mobile.

4 : l'agent mobile observe l'hôte visité pour calculer la valeur du paramètre b_1 de la métrique de la bienveuillance.

Ces trois dernières opérations sont répétées autant de fois qu'il existe de paramètres.

4.2 Le scénario de vérification du certificat

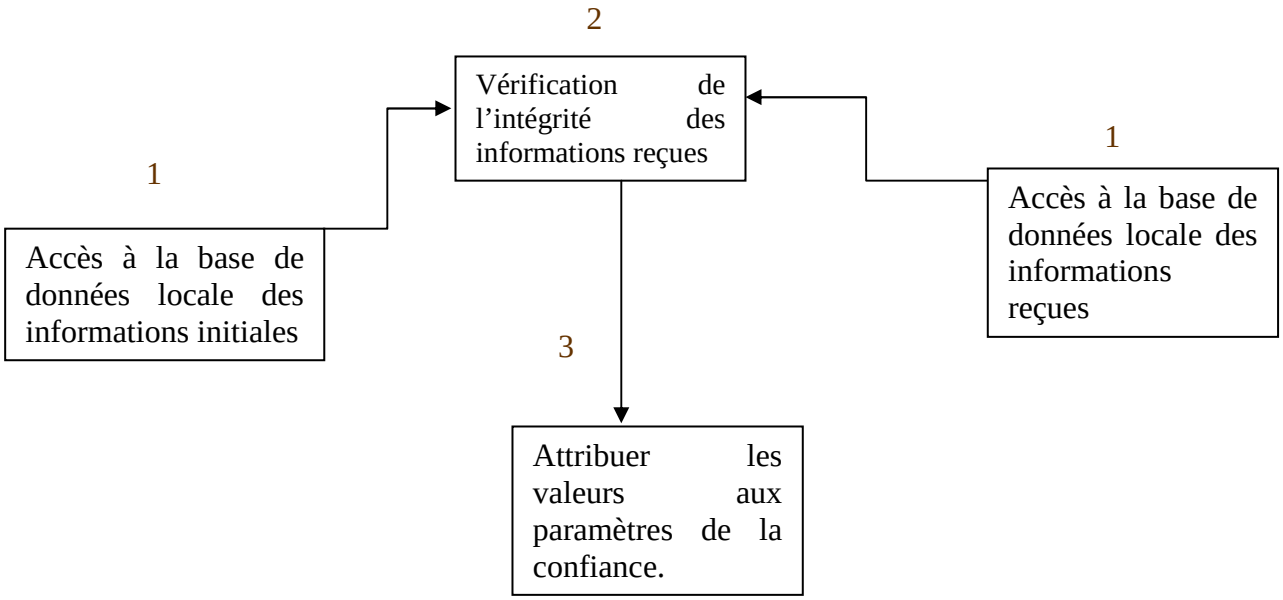
L'agent mobile vérifie la validité du certificat par le biais d'une autorité centrale d'une manière très simple (voir le diagramme de séquences suivant).



A la fin de la collecte des paramètres nécessaires, l'agent mobile envoie l'ensemble des informations à son émetteur après l'exécution des instructions de chiffrements décrits au niveau de la Table3.2 du chapitre précédent.

4.3 Le scénario de vérification des informations reçues

A la réception du message, l'émetteur exécute l'ensemble des instructions présentées dans la Table3.3 (voir chapitre 3), et sauvegarde ainsi les données reçues au niveau d'une base de données locale. Suite à l'extraction des informations (hachées et non hachées), l'émetteur vérifie l'intégrité des données hachées reçues en les comparant avec celles stockées au niveau de la base de données locale voir le schéma suivant :



Nous présentons un ensemble d'exemples de code qui servent à réaliser le calcul de la confiance.

Le code ci-dessous illustre le calcul de la métrique de l'indentification :

```
//  identification metric
     int para=0;
      int som=0;
      double prod=0;
for (para=0;para<9;para++)
{prod=prod+(Classe1.VI[para]*Classe1.piod
sid[para;([
som=som+Classe1.piodsid[para];}
   Classe1.I=(prod)/(som) ;
```

Les valeurs des paramètres de l'identification sont précisées par le code suivant en vérifiant l'intégrité des informations reçues avec celles stockées localement au niveau de la BD du propriétaire de l'agent mobile :

```
 //récupération des paramètres

   id= résultats3.getString("identité") ;
    acro= résultats3.getString("acronyme") ;;
    m2p= résultats3.getString("motdepasse") ;
    ad= résultats3.getString("adress") ;
    nreg= résultats3.getString("nregistre");
    itva= résultats3.getString("nidTVA") ;
    tel= résultats3.getString("numdetél") ;
    mail= résultats3.getString("email") ;
    domain= résultats3.getString("ledomaine") ;
     limitgéo= résultats3.getString("limitegéographique") ;
     limitoffre= résultats3.getString("durréedel'offre") ;
    PRIXHT=résultats3.getDouble("PRIXHT") ;
   TRANSPORT=résultats3.getDouble("TRANSPORT") ;
    TVA=résultats3.getInt("TVA") ;
    PRIXTTC=résultats3.getDouble("PRIXTTC") ;
       // vérification des paramètres

if (id2.equals(id))
     Classe1.VI[0]=1;              // variable de métrique
   else
     Classe1.VI[0]=0;
  if (acro2.equals(acro))
              Classe1.VI[1]=1;       // variable de métrique
  else
           Classe1.VI[1]=0;
  if (m2p2.equals(m2p))
            Classe1.VI[2]=1;         // variable de métrique
  else
          Classe1.VI[2]=0;
  if (ad2.equals(ad))
            Classe1.VI[3]=1;       // variable de métrique
  else
            Classe1.VI[3]=0;
```

```
            // vérification des paramètres

 if (nreg2.equals(nreg))
       Classe1.VI[4]=1;              // variable de métrique
     else
        Classe1.VI[4]=0;
  if (itva2.equals(itva))
       Classe1.VI[5]=1;              // variable de métrique
  else
     Classe1.VI[5]=0;
  if (tel2.equals(tel))
Classe1.VI[6]=1;              // variable de métrique
  else
    Classe1.VI[6]=0;
  if (mail2.equals(mail))
    Classe1.VI[7]=1;              // variable de métrique
   else
    Classe1.VI[7]=0;
 if (domain2.equals(domain))
         Classe1.VI[8]=1;              // variable de métrique
    else
    Classe1.VI[8]=0;
```

Le code suivant est obtenu de la classe responsable du calcul final de la confiance. Il montre la manière de traiter le cas du manque de confiance :

```
if(Classe1.I<Classe1.seuil)
        Classe1.sindice[0]=0;
      if(Classe1.B<Classe1.seuil)
        Classe1.sindice[1]=0;
      if(Classe1.R<Classe1.seuil)
        Classe1.sindice[2]=0;
      if(Classe1.K<Classe1.seuil)
        Classe1.sindice[3]=0;
Classe1.T=(Classe1.I*Classe1.sindice[0]*Classe1.POIDS[0])+(Class
e1.B*Classe1.sindice[1]*Classe1.POIDS[1])+(Classe1.R*Classe1.sin
dice[2]*Classe1.POIDS[2])+(Classe1.K*Classe1.sindice[3]*Classe1.
POIDS[3]) ;
System.out.println("LA MéTRIQUE FINALE DE LA CONFIANCE
EST :"+Classe1.T) ;
        double PKN=0;
        PKN=(Classe1.T/100) ;
       System.out.println("LA mise à jour de PK pour cette interaction
est :"+PKN);
```

```
 //            distrust treatment
if (Classe1.T<50)
 //           disponibilité
           if (Classe1.D>1 && Classe1.b1>=1)
      {
    Classe1.décision="ré-exécuter;"
    System.out.println("la capcité de calcule de l'hôte visité est bas
" ) ;}
   else
{if (Classe1.sindice[0]==1 && Classe1.sindice[1]==1 &&
Classe1.sindice[2]==0 && Classe1.sindice[3]==1(

        Classe1.décision="TRUST;"
       System.out.println("ENVOYé LA DéCISION D'ACHAT") ;   }
else

}      Classe1.décision="DISTRUST " ;
      System.out.println("hôte malicieux" ) ;
    else
{      Classe1.décision="TRUST;"
System.out.println("trustworthy host") ; }
    System.out.println("La DéCISION EST :"+Classe1.décision;(
    Connection conin = null;
Statement stmtin;
// inserer dans la BD métriques  l'identité +les métriques + décision
                                          .
                                          .
                                          .
```

5. L'environnement de développement

Le JBuilder X est un environnement de développement intégré ou IDE.

Le choix de JBuilder comme un environnement de développement a été motivé pour ces caractéristiques:

- ✓ Il fournit des informations détaillées sur la manière de développement des applications.
- ✓ Il explique les concepts de projet et de bibliothèque.
- ✓ La création des interfaces d'interaction de l'agent mobile avec l'hôte visité par l'utilisation d'interfaces utilisateur offertes par le JBuilder X. Cet interface explique comment utiliser l'EDI de JBuilder pour concevoir les interfaces d'une manière visuelle à travers l'utilisation des outils de conception visuelle. Ces derniers, nous ont permis de concevoir l'interface de l'agent mobile qui est attaché à différents événements.
- ✓ Le développement de notre simulation sur l'environnement de JBuilder X facilite son intégration, après préparation de l'environnement bien sûr, au niveau des plates formes spécialisées pour le traitement basé sur les agents tel que JADE.

6. Expérimentation

Au niveau de cette partie, nous déroulons notre application à travers un ensemble de scénario à partir desquels nous observons l'influence des différentes métriques sur la valeur finale de la confiance. On commence par le cas d'un hôte qui se comporte honnêtement puis on change les paramètres et les facteurs influant sur chaque métrique une par une.

6.1 Exemples expérimentaux

Scénario1 (cas d'un comportement normal): l'hôte d'accueil saisit les informations demandées d'une manière très correcte suivant les exigences de l'agent mobile (à titre d'exemple la figure suivante représente une interface pour récupérer les paramètres liés aux caractéristiques du produit (*Cf.* Figure 4.3).

Figure 4.3 Une interface pour récupérer les paramètres liés aux caractéristiques du produit

Les informations initiales stockées au niveau de l'émetteur de l'agent sont présentées dans les deux tables ci-dessous:

Information sur l'hôte visité															
N°	**identité**	**acronyme**	**motdepasse**	**adresse**	**Nregistre**	**NidTVA**	**Num de tél**	**email**	**Le domaine**	**PRIX HT**	**TRANSPORT**	**TVA**	**PRIXTTC**	**Limite géographique**	**Durrée de l'offre**
1	algérie télécom	actel	11ata	cne	85	89	213216 60201	actel@alg.com	commercial	100	3	7	110	illimité	illimité

Table4.1 les données stockées au niveau de la base de donnée locale de l'émetteur de l'agent mobile

Les valeurs précisées par l'émetteur						
N°	**D. estimé**	**Durée souhaitée**	**sensibilité**	**Degré de risque**	**Date actuelle**	**Adresse client**
1	21	50	0,34	min	03 09 2008	cne

Table4.2 les valeurs précisées par l'émetteur de l'agent mobile

Les informations que l'émetteur a reçues sont présentées ci après :

Recieves info																					
num	identité	acronyme	Mot depasse	adress	enregistre	nTVA	tél	email	Le domaine	PRIXHT	TRANSPORT	TVA	PRIXTTC	Durée de loffre	Limite géographique	hashdu contrat	Taille clé	Algo de chiffrement	Algo force	certificat	Date limite	Durée de livraison	D réel
343	algérie télécom	actel	11ata	cne	85	89	2132 1660 201	actel @alg.com	commercial	100	3	7	110	illimité	illimité	26640 373	0.75	0,5	1	1	02 04 2009	0	21

Table4.3 les valeurs reçues de l'agent mobile

Afin d'estimer la valeur finale de la confiance, nous avons associé à chaque métrique le poids qui lui convient (*Cf*. Table4.4). Nous notons que nous avons testé un ensemble de 300 cas pour aboutir aux valeurs de configuration contenues dans la Table 4.4. Elles concernent les poids devant être attribués à chaque métrique pour évaluer la confiance.

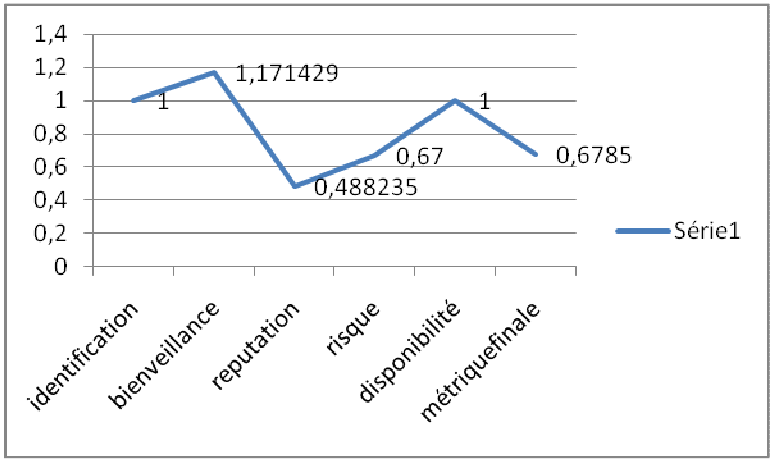
Les métriques	Les paramètres	Les poids des paramètres	Les poids
identification	identité	1	22
	Acronyme	1	
	E-mail	1	
	Mot de passe	2	
	Adresse géographique	1	
	Numéro de tel	1	
	Num d'identification au TVA	1	
	Num de registre de commerce	1	
	Le domaine	1	
bienveillance			28
réputation			25
Risque			25
Le facteur S			0.65

Table4.4 les poids associés à chaque métrique

Les valeurs des métriques obtenues sont présentées dans la table suivante :

N°	Identité de HV	identification	bienveillance	réputation	risque	Métrique finale	disponibilité	décision
14	algérie télécom	1	1,171429	0,488235	0,67	67,85	1	TRUST

Table4.5 les valeurs des métriques du scénario 1



Graphe4.1 la représentation graphique des résultats du premier scénario

Discussion: Dans ce cas l'hôte visité est considéré comme un hôte de confiance car il possède un degré de confiance ≥ 50.

Pour examiner l'impact des métriques, nous préférons garder le même exemple en changeant à chaque fois les valeurs des paramètres.

Scénario2 : Dans ce scénario le problème est au niveau de la métrique de l'identification, l'hôte visité donne des fausses informations concernant son authentification et essaye de désorienter l'agent et déduire les valeurs des paramètres demandées. Ce scénario se caractérise par le fait qu'au moins l'identité de l'hôte visité est juste, à cause de l'identification initial du protocole de sécurité de bas niveau.

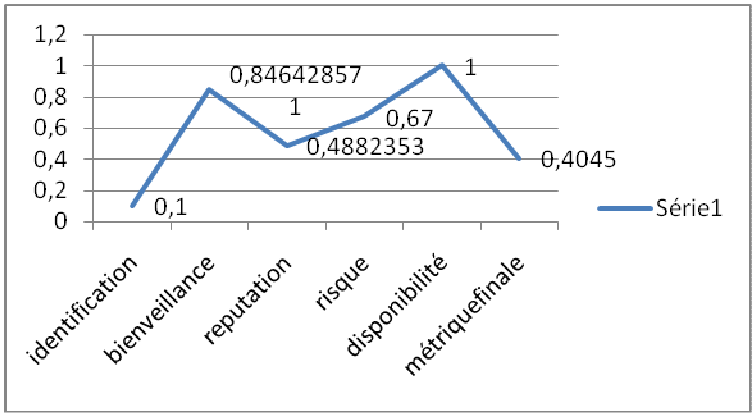
Recieves info																						
um	**identité**	**acronyme**	**motdepasse**	**adress**	**nregistre**	**nTVA**	**tél**	**email**	**ledomaine**	**PRIXHT**	**TRANSPORT**	**TVA**	**PRIXTTC**	**duréedelolffre**	**limitegéographique**	**hashduconntrat**	**tailleclé**	**algodechiffrement**	**algoforce**	**certificat**	**datelimite**	**duréedelivraison**	**Dréel**
48	algérie télécom	ACTEL	21fgtr	alg	54	96	213456987070	ACTEL@alg.com	télécommunication	100	3	7	110	illimité	illimité	-103012556 2	0,75	0,5	1	1	05 05 2009	1	24

Table 4.6 les informations reçues du scénario2

D'après les informations collectées par l'agent mobile, nous avons obtenu l'ensemble des valeurs des métriques suivant :

tabledesmétriques								
N°	**identitédeHV**	**identification**	**bienveillance**	**reputation**	**risque**	**disponibilité**	**métriquefinale**	**décision**
28	algérie télécom	0,1	0,846428571428572	0,4882353	0,67	1	40,45	DISTRUST

Table4.7 les valeurs des métriques du scénario 2



Graphe4.2 la représentation graphique des résultats du scénario2

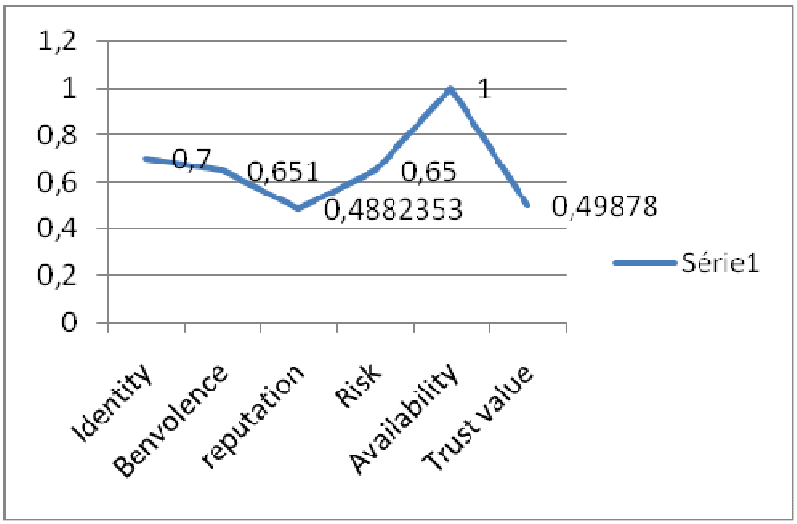
Discussion Lorsque l'hôte essaye de réaliser une mascarade, il tente de trouver les bonnes informations soit par un temps de réponse élevé ou bien par plusieurs saisies des informations demandées. Si c'est le cas, généralement la métrique de la bienveillance est influencée et l'attaques est détectée. Au niveau de ce cas de test, on montre que malgré que l'hôte essaye de répondre à temps aux demandes de l'agent mobile, l'attaque est détectée et l'hôte est considéré comme malicieux. Cette attaque est toujours détectée sauf si l'hôte d'accueil possède toutes les informations confidentielles de l'hôte réellement concerné par la visite de l'agent mobile.

Scénario3 : la réputation est mauvaise.

Dans ce cas si la valeur de la confiance est suffisante, on peut se trouver dans le cas du scénario1. Toutefois, si la valeur de confiance est insuffisante, on considère l'algorithme de la disponibilité (*Cf.* Table3.4) en appliquant la deuxième condition qui permet un envoi de décision positive si le manque de confiance est le résultat d'une mauvaise réputation (le facteur S de chaque métrique est égal à 1 sauf celui de la réputation), ce qui est observé au niveau de table suivante :

tabledesmétriques								
N°	**identitédeHV**	**identification**	**bienveillance**	**reputation**	**risque**	**disponibilité**	**métriquefinale**	**décision**
33	algérie télécom	0,7	0,6764285	0,4882353	0,65	1	49, 878	TRUST

Table 4.8 les informations reçus du scénario4



Graphe4.3 la représentation graphique des résultats du scénario3

Discussion: C'est vrai que la réputation de l'hôte visité est une métrique, mais nous la considérons comme secondaire car une forte réputation de l'hôte visité n'implique pas qu'il va se comporter d'une manière honnête et si on la considère comme une métrique de base elle augmente la valeur de la confiance calculée. Cette valeur peut donc désorienter le propriétaire de l'agent mobile qui peut prendre une décision erronée.

Scénario4 : Nous proposons un montant élevé (un facteur de la métrique du risque) pour examiner son impact sur la confiance. Dans ce cas, nous supposons que l'hôte visité se comporte d'une manière honnête.

Les informations reçues sont comme suit :

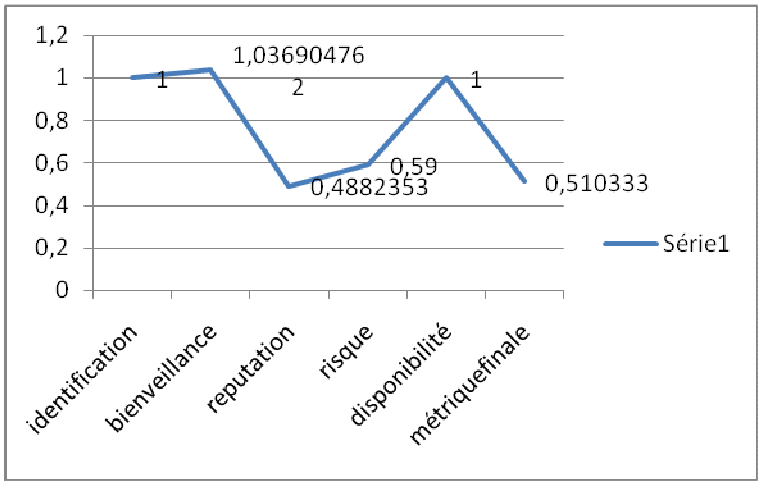
recievesinfo																							
num	**identité**	**acronyme**	**motdepasse**	**adress**	**nregistre**	**nTVA**	**tél**	**email**	**ledomaine**	**PRIXHT**	**TRANSPORT**	**TVA**	**PRIXTTC**	**duréedeloffre**	**limitegéographique**	**hashduocontrat**	**tailleclé**	**algodechiffrement**	**algoforce**	**certificat**	**datelimite**	**duréedelivraison**	**Dréel**
350	algérie télécom	actel	11ata	cne	85	89	21321660201	actel@alg.com	commercial	2000000	350	7	2140350	illimité	illimité	-53575697	0,75	0,5	1	1	12 12 2008	5	25

Table 4.9 les informations reçus du scénario4

Les informations de la table précédente résultent du tableau des métriques suivant:

tabledesmétriques								
N°	**identitédeHV**	**identification**	**bienveillance**	**reputation**	**risque**	**disponibilité**	**métriquefinale**	**décision**
30	algérie télécom	1	1,03690476190476	0,4882353	0,59	1	51,0333333333333	TRUST

Table 4.10 les informations reçues du scénario4



Graphe4.4 la représentation graphique des résultats du scénario4

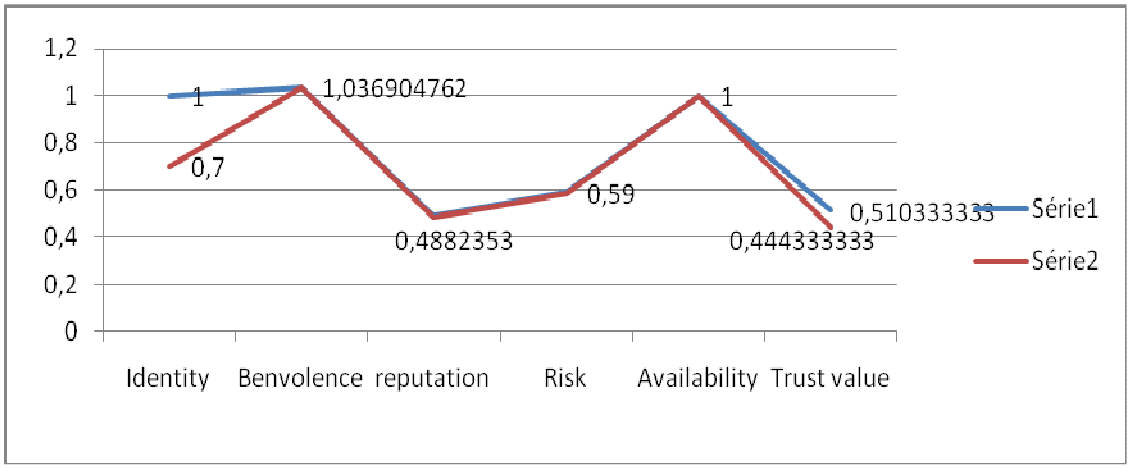
Discussion: Nous remarquons au niveau de ce scénario que la valeur de confiance diminue de 67,85 à 51.03 pour le même comportement de l'hôte visité (scénario 1) mais cette fois-ci avec un montant important (un risque financier important). De plus, l'augmentation du risque (la valeur de la métrique 0.59 n'est pas suffisamment grande) rend la valeur finale de la confiance plus sensible à la détection d'une altération au niveau des informations reçues. À cet effet, une décision totalement différente à la première peut être prise par le propriétaire de l'agent mobile (*Cf.* Graphe4.5). Ce qui permet d'affirmer que l'emploi des métriques est efficace pour détecter les comportements malicieux des hôtes visités. Ceci peut être observé à travers la Table4.11. En reprenant le scénario4 mais cette fois-ci avec une valeur de la métrique de l'identification plus petite (cette dernière est diminuée à cause de la réception de deux paramètres erronés au niveau de la métrique de l'identification) :

tabledesmétriques								
N°	**identitédeHV**	**identification**	**bienveillance**	**reputation**	**risque**	**disponibilité**	**métriquefinale**	**décision**
32	algérie télécom	0,7	1,036904762	0,4882353	0,59	1	0,4443333	DISTRUST

Table 4.11 les métriques calculées du scénario4 (modifié)

recievesinfo																					
num	**identité**	**acronyme**	**motdepasse**	**adress**	**nregistre**	**nTVA**	**tél**	**email**	**ledomaine**	**PRIXHT**	**TRANSPORT**	**TVA**	**PRIXTTC**	**duréedeloffre**	**limitegéographique**	**hashduocontrat**	**tailleclé**	**algodechiffrement**	**algoforce**	**certificat**	**datelimite**	**duréedelivraison**	**Dréel**
352	algérie télécom	actel	11ATA	cne	85	125	213012457	actel@alg.com	commercial	2000000	350	7	2140350	illimité	illimité	-1983469948	0,75	0,5	1	1	02 12 2008	3	27

Table 4.12 les informations reçues du scénario4 (modifié)



Graphe4.5 un graphe[4] montrant la sensibilité des métriques à une altération au niveau des informations reçues

[4] : Série1 représente le scenario 4 (l'hôte visité est de confiance).
Série2 représente le scenario 4 modifié (l'hôte visité est malicieux).

6.2 L'apport de notre technique de protection

Notre objectif était un des perspectives de la thèse de doctorat de madame Hacini au niveau de laquelle elle à commencé sa réflexion pour l'estimation de la confiance afin de l'utiliser comme un critère d'adaptation de l'agent mobile. Notre but se résume, à l'identification des métriques de confiance pour la sécurisation des agents mobiles.

L'apport de la technique de protection proposée ou plus spécifiquement l'apport des métriques rajoutées à la contribution de madame Hacini peut être observé dans le scénario 5 suivant :

- l'hôte visité n'est pas certifié.
- l'hôte essaye, après plusieurs tentatives, et a réussi dans la découverte des informations exactes requises par l'agent mobile telles que les données de l'identification.

Au niveau du travail de madame Hacini [Hac 2008] qui se base principalement sur l'identification pour calculer la confiance de l'hôte visité. Le résultat de ce scénario peut se résumer comme suit: après la réception des informations envoyées par l'agent à son hôte d'origine, ce dernier estime la confiance et considère l'hôte d'accueil comme un hôte qui possède un degré de confiance minimum donc appartient à l'intervalle ambigu (voir la série 2 du Graphe4.7). Dans ce cas, une décision d'exécution d'un service dégradé (ou nul quand l'hôte est jugé malicieux) est prise. Par contre, le résultat obtenu en appliquant notre métrique de confiance décide que l'hôte d'accueil est un hôte malicieux en passant par l'algorithme de traitement de manque de confiance et la transaction n'est effectuée (voir la série 1 du Graphe4.7).

recievesinfo

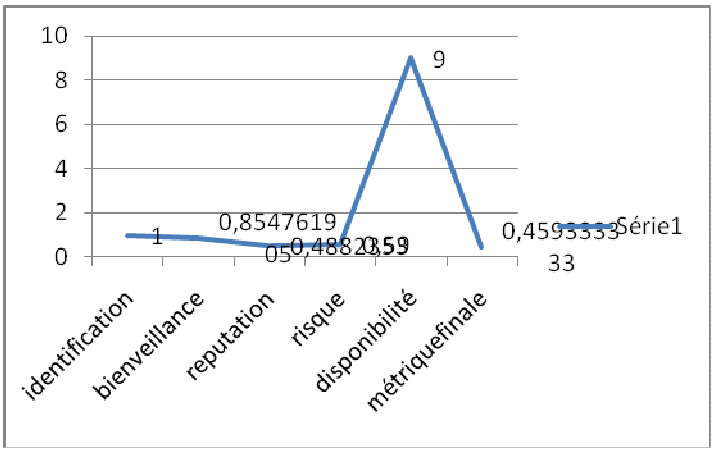
num	identité	acronyme	motdepasse	adress	nregistre	nTVA	tél	email	ledomaine	PRIXHT	TRANSPORT	TVA	PRIXTTC	duréedeloffre	limitegéographique	hashduocontrat	taillecléchiffrement	algodechiffrement	algoforce	certificat	datelimite	duréedelivraison	Drél
357	algérie télécom	actel	11ata	cne	85	89	213216602001	actel@alg.com	commercial	100	3	7	110	illimité	illimité	-53575697	0,75	1	1	1	02042009	1	209

Table 4.13 les informations reçues du scénario 5

tabledesmétriques

N°	identitédeHV	identification	bienveillance	reputation	risque	disponibilité	métriquefinale	décision
37	algérie télécom	1	0,854761904761905	0,4882353	0,59	9	45,9333333333333	DISTRUST

Table 4.14 les métriques calculées du scénario 5

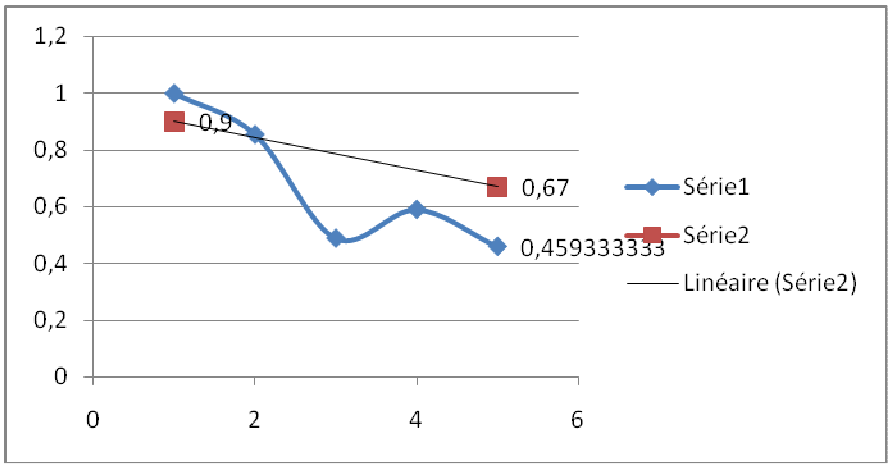


Graphe4.6 représentation graphique des résultats du scénario 5

Nous remarquons qu'au niveau du traitement de manque de confiance la disponibilité et la compétence de l'hôte d'accueil est élevée (*Cf.* Graphe4.6). Ainsi ce dernier profite de cette haute capacité de calcul pour déduire les informations demandées par l'agent mobile.

Finalement, l'apport peut être observé au niveau de la prise en compte de l'aspect multidimensionnel de la confiance d'un côté ainsi que dans l'exploitation des métriques au niveau de l'adaptabilité de l'agent mobile du fait que le risque et la réputation peuvent être considérés comme des facteurs d'adaptation.

Au niveau de la simulation suivante nous observons graphiquement (*Cf.* Graphe4.7) l'apport intéressant de la prise en compte de la caractéristique multidimensionnelle de la confiance :



Graphe4.7 représentation graphique du scénario 5 montrant l'apport de la prise en compte de l'aspect multi dimensionnelle de la confiance

7. Conclusion

Nous avons observé au niveau de ce chapitre des illustrations concernant notre simulation. Ces dernières se basent principalement sur le déroulement d'un ensemble de scénarios afin d'estimer le degré de confiance de l'hôte visité.

Pour cela, nous avons présenté un ensemble de diagramme UML qui démontrent la conception de notre simulation ainsi qu'une partie du code servant à la réalisation de notre simulation. Ce chapitre nous a permis de préciser l'impact de chaque métrique sur la valeur finale de la confiance placée en l'hôte d'accueil. Nous avons aussi évalué l'efficacité des métriques sur la détection des tentatives d'attaque contre l'agent mobile. Par ailleurs, nous avons considéré la nouvelle valeur de confiance comme étant une mise à jour de la réputation directe (réputation locale). Cette dernière peut être utilisée comme paramètre pour l'estimation de la crédibilité de l'hôte d'accueil au niveau des interactions futures.

CONCLUSION GENERALE

ET

PERSPECTIVES

CONCLUSION GENERALE

L'utilisation des agents mobiles offre de nombreux avantages. Ils permettent de réduire le trafic réseau pour une meilleure latence, rechercher des informations pertinentes dans un délai acceptable etc. Cependant le problème de sécurité qu'ils suscitent a freiné leur exploitation de manière significative. Notre contexte de travail se situe au centre de cette problématique.

Le problème de la sécurité qui nous intéresse résulte de l'exécution de l'agent mobile sur des hôtes qui lui sont inconnus et qui sont potentiellement malicieux. L'hôte visité a en effet la possibilité, à titre d'exemple, de modifier le comportement futur de l'agent pour atteindre des objectifs malveillants.

D'autre part, la notion de confiance se renforce et elle se détache des notions de sécurité et de fiabilité, elle influe sur les décisions à prendre. Ces dernières peuvent être des décisions d'exécution ou non. Pour cette raison, elle a suscité beaucoup d'intérêt dans le domaine de sécurité des systèmes informatiques.

Le travail effectué dans ce mémoire s'inscrit dans le cadre de la protection des agents mobiles contres les attaques provenant de leur environnement d'exécution en se basant sur la notion de la confiance. Pour cela, nous avons étudié le concept de confiance ainsi que les notions liées à la sécurisation des agents mobiles. Cette étude est fondée sur la contrainte de l'exécution de l'agent mobile uniquement dans des environnements jugés de confiance. Cette contrainte impose la précision d'un ensemble de cinq métriques servant à l'estimation de la crédibilité de l'hôte visité pour déterminer le comportement adéquat de l'agent mobile. Ces métriques sont simples et n'engendrent pas de surcoût en temps d'exécution ce qui permet à l'agent mobile de réagir dans un délai convenable.

Nous avons validé notre proposition par une simulation, an niveau de laquelle nous avons vérifié l'impact des différentes métriques sur la valeur finale de la confiance.

De plus, nous avons observé l'apport de la prise en compte de l'aspect multidimensionnelle de la confiance.

Finalement, cette simulation a permis d'affirmer que l'estimation de la confiance réalisée dans ce travail constitue un bon support de la protection des agents mobiles.

PERSPECTIVES

Notre objectif de départ était l'identification de l'ensemble des facteurs qui influent sur la confiance placé en l'hôte visité. A l'issue de ce travail, un ensemble de métriques exploitant les facteurs de confiance permettant l'estimation de la crédibilité de l'environnement d'exécution de l'agent mobile ont été établis. Étant donné, la rapide évolution des attaques internet cette approche de protection pourrait posséder des faiblesses qui pouvant être exploitées par des pirates. Pour cela, nous espérons tester cette approche sur un environnement d'exécution réel afin de pouvoir l'améliorer. Par ailleurs, des optimisations au niveau du calcul de la confiance peuvent être apportées. Nous pouvons citer, à titre d'exemple, la réduction de la taille du message envoyé par l'agent mobile. En outre, le renforcement des métriques par l'implication des paramètres permettant la détection des modifications au niveau du code de l'agent pourrait constituer une perspective intéressante à ce travail. Ceci sera réalisé en utilisant notamment la notion de trace d'exécution qui permet la capture de toutes les instructions de l'agent mobile exécutées par l'hôte d'accueil. En outre, le risque et la réputation pourrait être utilisés en tant que facteurs d'adaptabilité. Enfin, nous souhaitons, que ce mémoire soit un document de base pour les futures recherches.

Références bibliographiques

[Bel 2004] Arnaud Belleil, Daniel Kaplan ” Confiance et sécurité sur les réseaux ” Document de synthèse 12 octobre 2004.

[Ben 1999] Benassi, P. “TRUSTe: An Online privacy seal program.” *Communications of the ACM* (42:2), February, pp. 56-59, 1999.

[Bha 2000] A. Bhatnagar, S. Misra, and H.R. Rao, “On Risk, Convenience and Internet Shopping Behavior, Association for Computing Machinery”, *Communications of the ACM*, 43, 11, pp. 98-108, 2000.

[Bob 2000] Bob Tarr, Danko Nebesh, et Sterling Foster :”Introduction To Mobile Agent Systems and Applications”. Tools USA 2000 Mobile Agents. Department of Defense, 2000.

[Car 2003] M. Carbone, M. Nielsen, V. Sassone. “A Formal Model for Trust in Dynamic Networks“. In *Proc. Of 1st International Conference on Software Engineering and Formal Methods (SEFM’03)*, Sept. 2003, pp. 54–63, Brisbane, Australia, 2003.

[Cas 2002] C. Castelfranchi and R. Pedone. “A review on trust information technology”.http://alfebiite.ee.ie.ac.uk/docs/papers/D1/ab-d1-cas+ped-trust.pdf, 2002.

[Cha 2000] Cheung, C. and Lee, M.K.O. “Trust in Internet Shopping: A Proposed Model and Measurement Instrument,” in the Proceedings of the 6th Americas Conference on Information Systems, H.M. Chung (August 10-13, 2000, Long Beach, CA, pp.681-689, 2000.

[Chr 2000] Chircu, A.M., Davis, G.B. and Kaufmann, R.J. “Trust, Expertise and E-Commerce Intermediary Adoption,” in the Proceedings of the 6th Americas Conference on Information Systems, H.M. Chung (ed.), August 10-13, Long Beach, CA, pp.70-716, 2000.

[Col 1988] J. S. Coleman. “Social Capital in the Creation of Human Capital”. *American Journal of Sociology*, 94:95–120, 1988.

[Con 2005] Arnaud Contes : "une architecture de sécurité hiérarchique, adaptable et dynamique pour la grille " thèse de doctorat université de nice - sophia antipolis faculté des sciences, 2005.

[Dem 1996] Demazeau, Y. and Costa, A. R.”Populations and organisations in open multi-agent systems”. In *1st Symposium on Parallel and Distributed AI*, Hyderabad, India 1996.

[Deu 1958] Deutsch, M. "Trust and Suspicion," journal of *Conflict Resolution,* Vol. 2, No. 4, pp. 265-279. 1958.

[Ein 2000] Einwiller, S., Geissler, U. and Will, M. “Engendering Trust in Internet Businesses using Elements of Corporate Branding,” in the Proceedings of the 6th Americas Conference on Information Systems, H.M. Chung (ed.), August 10-13, 2000, Long Beach, CA, pp.733-739, 2000.

[Eng 2004] English, C., Terzis, S., Wagealla, W.: “Engineering trust based collaborations in a global computing environment”. In: Trust Management: Second International Conference, iTrust 2004, Oxford, UK, March 29–April 1, 2004. Proceedings. Volume LNCS 2995/2004. 120–134, 2004.

[Esp 2003] Oscar Esparza Miguel Soriano Jose L. Muñoz Jordi Forné :" A protocol for detecting malicious hosts based on limiting the execution time of mobile agents ".Proceedings of the Eighth IEEE International Symposium on Computers and Communication (ISCC’03).1530-1346/03.2003.

[Far 1996a] W.M. Farmer, J.D. Guttman and V.Swarup. “Security for Mobile Agents: Issues and Requirements” .In Proc. Of the 19th National Information Systems Security Conf, Pages 591-597, Baltimore, MD, USA, October 1996.

[Far 1996c] W Farmer, J D.Gottman et V .Swarup" security for mobile agents :authentication and state apparaisal" in proceeding of the European symposium on research in computer security (ESORICS) pages 118-130, 1996.

[Fer 1995] Ferber, J. *Les Systèmes Multi-Agents : “ vers une intelligence collective* “. InterEditions, 1995.

[Fra 1996] Franklin, S. and Graesser, A. C. (1996). “Is it an agent, or just a program?: A taxonomy for autonomous agents”. In *conference of the Third International Workshop on Agent Theories, Architectures and Languages (ATAL’96)*, pages 21–35.

[Fuk 1995] Francis Fukuyama. *Trust:” The Social Virtues and the Creation of Prosperity”*. The Free Press, New York, 1995.

[Gef 2000] Gefen, David, E-commerce: “The role of familiarity and trust” *Omega: The international journal of management science,* Vol. 28, No. 5, pp. 725-737, 2000.

[Gra 2001] Grazioli, S. and Wang, A. (2001). “Looking without seeing: Understanding unsophisticated consumers success and failure to detect internet deception” *Proceedings of the ICIS 2001*.

[Gef 2002] David Gefen V. Srinivasan Rao, et Noam Tractinsky:" The Conceptualization of Trust, Risk and Their Relationship in Electronic Commerce: The Need for Clarifications " Proceedings of the 36th Hawaii International Conference on System Sciences" (HICSS’03) IEEE.0-7695-1874-5/03 .2002.

[Gol 1996] Ian Goldberg, David Wagner, Randi Thomas, and Eric A. Brewer. ”A secure environment for untrusted helper applications”. In Proceedings of the 6th Usenix Security Symposium, San Jose, CA, USA, 1996.

[Gom 2006] Gomez, M.; Carbo, J.; and Benac, “An anticipatory model of trust”. In Anticipatory Behavior in Adaptive Learning Systems C. 2006.

[Gra 2003] Gray, E., Seigneur, J.M., Chen, Y., Jensen, C.: “Trust propagation in small worlds”. In: Trust Management: First International Conference, iTrust 2003, Heraklion, Crete, Greece, May 28–30, 2003. Proceedings. Volume LNCS 2692/2003. 239–254. 2003.

[Gom 2007] Mario Gomez, Clara Benac Earle and Javier Carb´o "Trust dynamics, motivational attitudes and epistemic actions", American Association for Artificial Intelligence (www.aaai.org). All rights reserved Copyright c 2007.

[Gra 1998] R.S. Gray, G. Cybenko, D. Kotz, and D. Rus. D'Agents: ”Security in a multiple-langage, mobile-agent system”. In G. Vigna, editor, Mobile Agent Security. LNCS, Springer-Verlag, Berlin, 1998.

[Gre 1998] M.S Greenberg.J.C Byington.T Holding. D. G Haper, "mobile agent and security" IEEE communication Magazine 373,377,379,380, pp 76-85, juillet 1998.

[Hac 2006] Salima Hacini, Zahia Guessoum, and Zizette Boufaïda "Using a Trust-Based Environment Key for Mobile Agent Code Protection" transactions on engineering, computing and technology volume 16 november issn 1305-5313 (326-331). enformatika v16 2006 issn 1305-5313 © 2006 world enformatika society, 2006.

[Hac 2006a] Salima Hacini, Haoua Cheribi, and Zizette Boufaïda: "Dynamic Adaptability using Reflexivity for Mobile Agent Protection" transactions on engineering, computing and technology volume 17 december 2006 issn 1305-5313. enformatika v17 2006 issn 1305-5313, world enformatika society, 2006.

[Hac 2007] Hacini, S., Guessoum, Z., Boufaïda, Z.: "TAMAP: A New Trust-based Approach for Mobile Agent Protection". Journal in computer virology. Springer Paris. ISSN 1772-9890 (print) 1772-9904 (online). Volume 3, N°4/November 2007, p 267-283, 2007.

[Hac 2008] Salima Hacini « Sécurité des Systèmes d’Information : Mise en oeuvre de la confiance et de l’adaptabilité pour la protection de l’agent mobile » Thèse de Doctorat en Sciences Spécialité : Informatique, Université Mentouri Constantine, 21 Avril 2008.

[Heb 2004] la création de la confiance sur internet: “une proposition de cadre conceptual. Working paper, HEC Genève, Juin 2004.

[Hoh 1998] F.Hohl, "time limited black box security: protecting mobile agents from malicious hosts", in mobile agents and security, LNCS 1419, springer –verlay, 1998.

[ISO9594-8] ITU-T Recommendation X.509 | ISO/IEC 9594-8: Information Technology Open Systems Interconnection -The Directory: Public Key and Attribute Certificate Frameworks, March 2000.

[Jan 2000] Wayne Jansen, “Countermeasures for mobile Agent security”, Computer Communications, Special issue on Advance Security Techniques for Network Protection, Elsevier Science, 2000.

[Jan 2001a] Wayne Jansen, "Determining Privileges of Mobile Agents", inProceedings of the Computer Security Applications Conference, December 2001.

[Jan 2001b] Wayne Jansen, "A Privilege Management Scheme for Mobile AgentSystems", First International Workshop on Security of Mobile Multiagent Systems, Autonomous Agents Conference, May 2001.

[jar 1999] Jarvenpaa, S.L. and Tractinsky Consumer trust in an Internet store: A Cross-cultural validation, *Journal of Computer Mediated Communication*, Vol. 5, No. 2, p. 1- 35, 1999.

[jar 2000] Jarvenpaa, S.L.; Tractinsky, N.; and Vitale, M. "Consumer Trust in an Internet Store, " *Information Technology and Management,* Vol. 1, Issue 12, pp. 45-71, 2000.

[Jŝa 2003] Jŝang, A., Hird, S., Faccer, E.: "Simulating the elect of reputation systems on e-markets". In: Trust Management: First International Conference, iTrust 2003, Heraklion, Crete, Greece, May 28–30, 2003. Proceedings. Volume LNCS 2692/2003. 179–194, 2003.

[Jŝa 2004] Jŝang, A., Presti, S.L.: "Analysing the relationship between risk and trust". In: Trust Management: Second International Conference, iTrust 2004, Oxford, UK, March 29–April 1, 2004. Proceedings. Volume LNCS 2995/2004.135–145, 2004.

[Kim 2000] Kim, K. and Prabhakar, B. "Initial trust, perceived risk, and the adoption of internet banking" *Proceedings of ICIS 2000*.

[Lee 2006] HyoungYong Lee, Hyunchul Ahn and Ingoo Han: " analysis of trust in the e-commerce adoption" Proceedings of the 39th Hawaii International Conference on System Sciences , 2006.

[Lin 2005] Lin, Fu.-ren., Sung, Y.-w., and Lo, Y.-p., "Effects of Trust Mechanisms on Supply Chain Performance Using Multiagent Simulation and Analysis", International *Journal of Electronic Commerce*, Vol.9, No. 4, pp.91-112, 2005.

[Lin 2006] Fu-ren Lin; Tsing Hua University. Yi-pong Lom ,Yu-wei Sung :" Effects of Switching Cost, Trust, and Information Sharing on Supply Chain Performance for B2B e-Commerce: A Multi-agent Simulation Study". Proceedings of the 39th Hawaii International Conference on System Sciences , 2006.

[May 1995] Mayer, R.C., Davis, J.H.: "An integrative model of organizational trust". The Academy of Management Review 20, 709–734, 1995.

[Mck 2001] D. Harrison McKnight; Norman L. Chervany Carlson." Conceptualizing Trust:A Typology and E-Commerce Customer Relationships Model " Proceedings of the 34th Hawaii International Conference on System Sciences , 2001.

[OBJE 1997] ObjectSpace, Inc."ObjectSpace Voyager Core Package Technical Overview". http://www.objectspace.com, 1997.

[Par 2008] PARASCHIV Corina " Les agents intelligents pour un nouveau commerce électronique" (Collection technique et scientifique des télécommunications) [e-book] date de parution - 09-2008.

[Pat 2005] Alexandre Patry (RALI) "La confiance sur le web sémantique " 9 / 28 ; 7 avril 2005.

[Pau 2001] Paulo Marques, Paulo Simões, Luís M. Silva, Fernando Boavida, and João G. Silva. Providing applications with mobile agent technology. In OpenArch'01 - Fourth IEEE International Conference on Open Architectures and Network Programming, Anchorage, Alaska, April 2001.

[Put 1995] R.D. Putnam." Tuning in, tuning out: The strange disappearance of social capital in America". *Political Science and Politics*, 28(4):664–683, 1995.

[Rat 2000] Ratnasingham, P. and Kumar, K. "Trading partner trust in electronic commerce participation," *Proceedings of ICIS 2000*.

[Res 2000] Resnick, P., Zeckhauser, R., Friedman, E., Kuwabara, K.: "Reputation systems". Communications of the ACM 43, 45–48, 2000.

[Rot 1971] J.B Rotter." Generalized expectancies for interpersonal trust". American psychologist, 26:443-453, 1971.

[Ruo 2005] Sini Ruohomaa and Lea Kutvonen"Trust Management Survey" P. Herrmann et al. (Eds.): iTrust 2005, LNCS 3477, pp. 77–92, 2005.c ┌ Springer-Verlag Berlin Heidelberg 2005.

[San 1998] T.sander and C. Tschudin .Towards Mobile Cryptography.In Processing of the 1998 IEEE Symposium on Security and PrivacymOakland ,CA May 1998.

[Sen 2005] Sylvain Sené rapport de stage "Modèle de diffusion de confiance pour les réseaux ad hoc" année universitaire 2004- 2005.

[Son 1999] Son, J-Y, Narasimhan, S., and Riggins, F.J. "Factors affecting the extent of electronic cooperation between firms: Economic and sociological perspectives" ICIS 1999.

[Sta 2006] Florian Stahl; Marion Freudenschuss" Falling in Love is a matter of Trust" About the Importance of Trust and Information Substitutes When Offering Digital Paid Services On Dating Websites ".Proceedings of the 39th Hawaii International Conference on System Sciences IEEE - 0-7695-2507-5/06.2006

[Tyr 2002] Tyrone Grandison, Morris Sloman "Specifying and Analysing Trust for Internet Applications". 2nd IFIP Conference on e-Commerce, e-Business, e-Government, I3e2002, Lisbon Oct. 2002

[Vig 1998] Vigna Giovanni "Cryptographic Traces for Mobile Agents" In *Mobile Agents and Security*, volume 1419 of *LNCS*. Springer-Verlag, Dip. Electtronica e Informazione, Politecnico di milano P.za L. Da Vinci 23, 20133 Milano, Italy vigna@elet.polimi.it, 1998.

[Wag 2003] Wagealla, W., Carbone, M., English, C., Terzis, S., Nixon, P.: "A formal model on trust lifecycle management". In: Workshop on Formal Aspects of Security and Trust (FAST2003) at FM2003. Volume IIT TR-10/2003. IIT-CNR, Italy (2003) 184–195 URL http://www.iit.cnr.it/FAST2003/fast-proc-final.pdf (TR-10/2003).

[Wan 2003a] Wang Y. Vassileva J. 'Trust and Reputation Model in Peerto- Peer Networks", Proc. of IEEE Conference on P2P Computing, Linkoeping, Sweden, September. Pages 150-157. 2003.

[Wan 2003b] Wang. Y., Vassileva. J. 'Bayesian Network Trust Model in Peer-to-Peer Networks'. Proceedings of Second International Workshop Peers and Peer-to-Peer Computing. 2003.

[Whi 1999] Ba, S., Whinston, A. B. and Zhang, H. "Building Trust in the Electronic Market through an Economic Incentive Mechanism," in De, P. & DeGross, J. I. (eds.), Proceedings of the Twentieth International Conference on Information Systems, December 13- 15, pp. 208-213, 1999.

[Wil 1997] U.G.Wilhem. "Cryptographically Protected Objects ".Technical report,Ecole Poly technique Fédérale de Lausanne, Switzerland,1997.

[Woo 1999] Wooldridge, M. Intelligent agents. InWeiss, G., editor, "*Multiagent systems : A modern approach to Distributed Artificial Intelligence*". MIT Press. 1999.

[Xio 2003] Li Xiong, Ling Liu "A ReputationBased Trust Model for PeertoPeer eCommerce Communities" *EC'03,* San Diego, California, USA. ACM 158113679X/03/0006, June 9–12, 2003.

[Yar 1996] Yaron Misky Robbert Van Rensse Soller Fred B Shneder. "Cryptographic support for fault _tolerant". Distributed computing Department of computer science Cornell University Ithaca ,New york 14853 USA July 5,1996.

[Zai 2008] Zaiter Meriem, Hacini Salima, Boufaida Zizette « Trust metrics identification for mobile agents protection » : à apparaitre au proceeding de la Conférence internationale arabe en Technologie qui aura lieu, le 16- 18 Décembre, Hammamet, Tunisia ACIT 2008.

[Zuc 1986] L. Zucker. "Production of trust: institutional sources of economic structure": 1840-1920. Reseach in organization behavior, 8:53-111, 1986.