Bootstrapping Trust Evaluation Using a Trust Certificate Model

Basmah Almoaber

Thesis submitted to the
Faculty of Graduate and Postdoctoral Studies
in partial fulfillment of the requirements for the degree of

Master of Science in Systems Science

uOttawa

University of Ottawa
Ottawa, Ontario, Canada
February 2015

Abstract

Trust plays a vital role in the decision to initiate any interaction. Rational agents may use past experiences and other agents' opinions to decide to trust, but due to the nature of open multi-agent systems, where agents can dynamically join and leave the system at any time, agents may find themselves dealing with complete strangers whom neither they nor their friends have encountered before. This situation forces the agents to choose partners randomly, which significantly increases the risk of encountering unreliable agents. For instance, service requesters may become reluctant to initiate communication with newly-joined service providers. And when the newcomers are service requesters, who are willing to exploit the environment, service providers may also hesitate to start any connection with them. As a result, newcomers are excluded from the competition and old agents lose the possibility of interacting with better agents. In this thesis, we address that issue by creating a Trust Certificate (TC) model in which each agent is equipped with a certificate that works as a reference by providing information about its holder. The information is obtained and stored by the agent itself and is available to other agents who request it to evaluate the holder's trustworthiness for a potential interaction. The stored information is about the agent's role in the society and its performance in past interactions. The TC model allows agents to retrieve reputation information and make initial trust evaluations when evidence is unavailable. It also helps agents to avoid the need to make random partner selection due to the information scarcity. We show how this model enhances

the interaction process between agents by evaluating it in the context of a simulated multi-agent system.

Acknowledgement

First and foremost, my greatest and deepest gratitude go to my husband, Abdullah, for his love, unwavering support and inspiration. It would not have been possible to finish this journey without his continued support and counsel.

I would like to express my endless gratitude to my beloved parents, Mohammed and Hanan, for supporting and encouraging me with their best wishes. They have always stood behind me my whole life.

I would like to especially thank my supervisor, Dr. Thomas Tran, for his guidance, help and advice.

I would also like to convey my sincere gratitude to Abdullah Aref and SasiKiran Reddy for their valuable assistance, comments, and support.

Finally, I would like to thank King Khalid University, Abha, Saudi Arabia for funding my graduate studies.

Table of Contents

List of Figures

List of Tables

List of Notations and Abbreviations

C_{RA}	Confidence in provider based on its number of ratings
C_{RO}	Confidence in the provider based on its number of roles
r_i	ith rating
RA_{max}	Maximum number of ratings
RA_{min}	Minimum number of ratings
RA_n	Number of the provider's ratings
RO_{max}	Maximum number of roles
RO_{min}	Minimum number of roles
RO_n	Number of the provider's roles
t_{r_i}	Rating recency function for rating r_i
$T_{Direct}(x, y)$	Direct-experience-based trust value
$T_{RA}(x, y)$	Initial rate-based trust value
$T_{Rate}(x, y)$	Total rate-based trust value
$T_{RO}(x, y)$	Initial role-based trust value
$T_{Role}(x, y)$	Total role-based trust value
$T_{Total}(x, y)$	Total trust value
VANETs	Vehicular ad-hoc networks
v_{ra}	Third party opinion

v_{ro}	Role value
w_{Direct}	Direct-experience-based coefficient
w_m	The set of coefficient
w_{Rate}	Rate-based coefficient
w_{Role}	Role-based coefficient
a	Range of consumer activity level
b	Confidence level (degree of belief) on the role
CA	Certificate authorities
CR	Certified reputation
$\Delta\tau(r_i)$	The time difference between the current time and the time when the rating r_i is recorded
MAS	Multi-agent System
MASON	Multi-Agent Simulator Of Neighborhoods (or Networks
N_c	Number of consumer agents
N_p	Total number of provider agents
N_{pa}	Number of average providers
N_{pg}	Number of perfect providers
N_{pi}	Number of infrequent providers
N_{pp}	Number of poor providers
R	Number of simulation runs
satUG	Satisfactory utility gain value
TC	Trust certificate
UG	Utility gain
x	Consumer
y	Provider

α	Positive increment factor
β	Negative decrement factor
λ	Recency scaling factor

Chapter 1: Introduction

Trust plays a vital role in the decision to initiate any interaction, and was previously considered as a notion related to human beings only. However, the introduction of software agents that act in a similar manner as humans makes trust an important research topic in the field of computer science and adds a new dimension to it; it creates the need to maintain trust in new forms supported by computer systems.

Computer network systems composed of autonomous software agents that interact with each other establishing the need for trust in interaction decisions. The term "trust" has been defined in many ways, in different domains. For our research, we find the following definition by Gambetta [11] to be the most appropriate:

> *"Trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action."*

In other words, trust is a subjective probability with which a service consumer agent believes a service provider agent will function as expected.

In this chapter, we introduce an overview of the context of our research. We identify the motivations, the problem statement, and the research contributions to the field of multi-agent systems and publications. Finally, we present the thesis structure.

1.1 Overview

> *"Trustworthiness, the capacity to commit oneself to fulfilling the legitimate expectations of others, is both the constitutive virtue of, and the key causal precondition for the existence of any society"* [10].

Agents always need to estimate the trustworthiness of their potential partners in order to identify reliable partners with whom to interact, and to avoid unreliable partners. Before investigating trust and its models further, we first introduce the basic concepts of agents and multi-agent systems, which will be used throughout this thesis.

1.1.1 Agents and Multi-Agent Systems

The first and main key concept is agents. According to [19]:

> *"An agent is an encapsulated computer system situated in some environment and capable of flexible, autonomous action in that environment in order to meet its design objectives."*

The agent is typically programmed to observe its surroundings, interact with other agents in the system, make decisions, and apply reasoning techniques to solve real-time problems. In addition to that, agents act autonomously to achieve predefined objectives and fulfill a specific role, and they can cooperate with other agents who have some of the same goals. In general, agents are reactive (able to respond in a

timely fashion to changes that occur in their environment), proactive (able to opportunistically adopt goals and take the initiative) and have the ability to engage in social activities (such as cooperative problem solving or negotiation) in order to achieve their goals [19, 22, 47].

In our research we have two main types of agents: service consumer agents and service provider agents. We refer to a service consumer agent as a consumer or evaluator. On the other hand, we refer to a service provider agent as a provider or target agent.

Agents are often deployed in environments in which they interact (work) together to solve a problem or achieve a common goal, which cannot be completed by individuals. Such environments are known as multi-agent systems (MAS). In some systems, agents from different owners with different objectives can freely join and leave at any time. These types of systems are known as open multi-agent systems. Open multi-agent systems have special characteristics (adapted from [5, 43]):

- Limited access to complete information: Agents cannot know everything about their environment and they do not have all the capabilities needed to solve problems.
- The environment is dynamic: It can change over the time and can consist of highly heterogeneous agents implemented by different owners, at different times, with different software tools and techniques. Agents can appear and disappear unexpectedly.
- The system is insecure: Due to the random distribution of agents in the systems and their independent decision making processes, not all agents will behave the same way. There may be incompetent, unreliable or malicious agents.

- The data is decentralized: The required information is distributed in the system and it could be costly for the agent to collect them.
- There is no global control: Agents are owned by different stakeholders with different goals. They are self-interested and there is no central authority to control them.

The above characteristics result in the need to evaluate the trustworthiness of each agent before any interaction. Trustworthiness can be established by evaluating the trust and reputation of the target agents.

1.1.2 Trust and Reputation

MAS require that agents be able to interoperate and coordinate with each other, in peer-to-peer interactions, to fulfill their own goals. However, agents can be self-interested, diverse and deceptive, and have unpredictable behavior, which increases the importance of trust and reputation in improving agents' strategic decision-making. Trusting agents to behave as expected involves risk. Rational agents may use past experiences and other agents' opinions to decide, in any particular transaction, if the expected utility gain (how much utility an agent gains from an interaction with other agent) surpasses the expected risks. Two important parameters are usually employed to make such decisions: trust and reputation.

The headmost parameter is trust, which reflects the agent's risk level when relying on the provided information or service of other agents for the fulfillment of their own goals [22]. Trust is a subjective measure that affects an agent's decision of whether or not to establish an interaction with others. Trusting other agents means expecting them to cooperate.

An agent's reliability estimation is not only limited to trust but also includes the word-of-mouth proliferation of the agent's trustworthiness, as perceived by other

agents in the system; this is referred to as reputation. The measured trust alone might not reflect the actual credibility of agents, so the combination of trust and reputation may increase that credibility. The presence of reputation encourages trusting and trustworthy behaviors among agents because it reflects the image of the agents in the system.

1.2 Motivation

A significant number of trust and reputation systems rely on the information gathered about agents' past behavior, and their reputation in the system, to predict their trustworthiness in future actions [3, 17, 20, 34, 37, 38, 39, 44, 48]. Those systems will be reviewed and discussed in Chapter 2. Nevertheless, agents in multi-agent systems face a number of challenges during trust formation, as follows [8, 17]:

- Interacting with self-interested and unreliable agents.
- Lacking trust and reputation sources.
- Interacting with a complete stranger.
- Frequent changes in the environment.

These challenges often force the agents to explore the environment to find partners. This exploration strategy causes a number of vulnerabilities for the agents. First, it involves a high degree of risk, especially when facing a malicious agent. Second, it may cost the agent a lot as it may take a greater number of interactions before a good partner is encountered [6]. Lastly, it may not be appropriate in the case of high-value interactions.

Under such circumstances, there is a need to develop a new model that can help agents overcome the trust formation challenges and enable agents to choose partners without the risk of exploring the system.

1.3 Problem Statement

After spending some time in the system, the agents gradually get acquainted with the environment and establish a connection with other agents. This helps them build their knowledge about how to distinguish between trustworthy and untrustworthy neighbors. In addition, they get to enhance their reputation values, which will help them in future interactions. However, due to the nature of open multi-agent systems (MAS) where agents can dynamically join and leave the system at any time, agents may find themselves dealing with complete strangers whom neither they nor their friends have encountered before. This situation forces the agents to choose partners randomly, which significantly increases the risk of encountering unreliable agents. For instance, service consumers may become reluctant to initiate communication with newly-joined service providers. And when the newcomers are service consumers, who are willing to exploit the environment, service providers may also hesitate to start any connection with them. As a result, newcomers are excluded from the competition and old agents lose the possibility of interacting with better agents. In our research, we address that issue by creating a Trust Certificate (TC) model. The TC model allows agents to retrieve reputation information and make initial trust evaluations when evidence is unavailable. It also helps agents to avoid the need to make a random partner selection due to the information scarcity.

1.4 Contributions

The main goal of this research is to provide an effective way to facilitate the trust formation for new agents and agents with no experience. We propose a *Trust Certificate (TC) model* as a possible solution to this issue.

The main contributions of our TC model are summarized as follows:

- It provides generic framework that can be applied in a wide range of open MAS applications.
- It allows the agents to store their own reputation information and share it with others, which helps them gain trust faster.
- It composes three trust metrics that give more accurate trust estimation. The first two metrics (role-based and rate-based) are used to find the initial trust value, and the third metric is to build and update the direct experience. The composed model defines a solution to reduce the risk of selecting unreliable partners when agents are without experience.
- It allows the consumer to evaluate the confidence in the providers to obtain more accurate trust estimation. By adding the confidence level to the trust evaluation, agents are able to select more reliable partners.
- It includes the use of digital signatures to ensure the integrity of the provided information.

1.5 Author's Publication

Basmah Almoaber and Thomas Tran " *A Trust Certificate Model for Multi-agent systems"* in Proceedings of the 6th International Conference on E-Technologies (MCETECH-15), Springer, May 2015, Montreal (Quebec), Canada.

1.6 Thesis Structure

The thesis is organized into six chapters:

Chapter 1, **Introduction,** is the current chapter.

Chapter 2, **Related Work,** presents an overview of the background of the relevant literature. It also discusses the trust information sources and their pros and cons.

Chapter 3, **Proposed Approach,** presents the Trust Certificate model and its components, discusses the proposed approach mechanism and then concludes by providing a comparison between the related approaches and our approach, based on some important characteristics.

Chapter 4, **Experimental Evaluation,** presents the empirical evaluation of the proposed approach and discusses the experimental results in comparison with the Random model.

Chapter 5, **Discussion,** discusses the experimental results of the evaluation of the model performance.

Chapter 6, **Conclusions and Future Work,** summarizes the conclusions of this work and discusses some future research directions.

Chapter 2: Related Work

Trust is essential to any interaction within MAS. This explains why many state-of-the-art trust and reputation models have been introduced. As a common factor, almost all of the models need some sort of information in order for them to work.

In open dynamic MAS, the information needed to evaluate an agent's trustworthiness can be drawn from a variety of sources. Due to the dynamic nature of MAS, the level of knowledge and the number of available sources may vary from time to time and from agent to agent.

This chapter offers a panoramic view of some trust information sources that are currently considered, in MAS literature, to evaluate the trustworthiness of agents. We divide our discussion into five sources: direct experiences and witness information, roles and relationships, social networks, certified reputation, and finally stereotypical trust.

In the second part of this chapter, we survey some of the existing models that are related to trust in MAS, especially those that consider the information scarcity issue. In our discussion, we consider the FIRE model [17], RCertPX [35], REGRET [39], as well as a few other approaches [8, 30, 31].

2.1 Sources of Trust

In MAS, agents rely on each other in order to achieve their goals. Therefore, trust and reputation models in MAS aim to equip the agents with tools that support trust evaluation, in order to avoid a partnership with untrustworthy peers. The trust evaluation is achieved on the basis of evidence, which can be drawn from a variety of sources. In highly dynamic MAS, the evidence required to form a trust evaluation may be scarce. To avoid that scarcity, it may be essential to consider a number of different sources of evidence. In this section, we review certain sources of trust that are currently considered in MAS literature for use in trust assessment.

2.1.1 Direct Experiences and Witness Information

These sources are the traditional information sources used by trust and reputation models; most models depend on them to evaluate the trustworthiness of any potential partner.

Direct experience is the most relevant and reliable information source, where the information used to compute trust is obtained from the experience of a direct interaction between two agents. That experience reflects the subjective opinion of the judging agent and can help the agent predict the future behavior of its partner [16]. The main idea is to estimate the trustworthiness of an agent by exploring the details of previous interactions with the same agent. This source was introduced for the first time by [29]. Many other models adapted the direct experience trust source, such as [17, 39, 48].

In the case that an agent does not have enough direct experience, it can rely on other agents in the system in order to replenish. Witness information (also known as indirect information or reputation) is based on other agents' experiences and opinions

about an agent. The collective opinions reflect the view of the society about an agent. It is the most abundant source of information that helps decrease the problems associated with dynamic societies. According to [3], the formal definition of reputation is

> *"An expectation about an agent's behavior based on information about, or observations of, its past behavior."*

The information can be gathered by asking other agents in the network for their opinions about another agent. The opinions are usually in the form of ratings about the evaluated agent's performance during an interaction. Models such as [17, 39] use the mechanism of collecting the ratings of a particular agent from other agents, and then combining them to estimate the trustworthiness of that agent.

All trust and reputation models in MAS, at the most basic level, combine direct experiences and witness information to calculate the trust value. However, direct experience is considered as the more reliable source and therefore has a larger influence on the resulted trust value, based on the fact that reputation providers may be dishonest, inaccurate or deceptive.

Due to the frequent change of the agents in the system, direct and witness information may be inadequate. Direct information is not always available and sometimes it is hard to locate a witness with honest and complete information. Furthermore, agents are not always open to share their information with others. Therefore, it is necessary to identify other sources of information from which trust evaluations may be formed.

2.1.2 Roles and Relationships

In MAS, learning about an agent's behaviors in roles and in relationships may be useful for trust evaluations. Normally, MAS societies have defined organizational structures and agents have well-defined roles [32]. The idea of roles and relationships is based on the assumption that an agent's behavior can be predicted based on its role in the society or on its relationship with the evaluator agent. Examples of roles in the society are authority, expert, buyer, seller, etc. Relationships can be categorized as friendships, co-workers, competitors, etc. This concept is based on the human society, where people tend to trust people with certain occupations, for example professors, doctors, or police [26].

The FIRE model [17] introduces role-based trust as one of its main sources of information. In this model, the trust results from the relationship between two agents. It is based on rules that capture the degree of knowledge an agent has about another agent or about the environment. For example, an agent may trust another agent because it is a member of a trustworthy group or owned by the same owner.

The REGRET model [39] also uses the notion of roles in evaluating the trust value, by assigning the agent a default level of trust based on its role within the system.

Another model that uses roles and relationships is [33]. The model introduces role-based trust as one of many trust metrics for modeling agent trust in vehicular ad-hoc networks (VANETs). Assuming that agents with roles identified by authorities are expected to behave in a certain way, each agent in the system is assigned a predefined role associated with a trust value. Roles can be one of four different roles: authority, expert, seniority and ordinary.

In the past, roles and relationships were not widely studied because the results varied based on different domains of application. Also, there was no standard way of computationally quantifying trust based on roles or relationships [16]. These days, however, roles and relationships are used as a worthy source of information and more focus is placed on studying them.

2.1.3 Social Networks

Social networks provide a useful source of trust information. A key example of this view is the concept of trust transitivity networks [6]. The idea in brief is that if A trusts B, and B trusts C, then A trusts C to some extent. Trust transitivity is based on the assumption that being trustworthy with respect to some task implies being trustworthy as a recommender about that task [13]. Social networks can be represented as directed graphs, where nodes represent entities in a structure and arcs represent some type of relationship. Edges between nodes can be labeled with the attributes of the relationship that are of interest [13]. An agent can give a trust value to another agent based on their interactions. If there is a trust path linking two nonadjacent agents, the source agent can evaluate the trustworthiness of the target agent along an existing path, based on the trust transitivity property [4, 6].

Social network analysis may be used to select the best possible witnesses for a particular target agent, as in REGRET [39, 40]. The REGRET model depends heavily on social networks to evaluate the trust value (social dimension). For instance, neighborhood reputation uses information extracted from the social relations between agents in order to calculate the trust value (more details about the REGRET model can be found in Section 2.2.3).

Another example of social networks is the referral systems [48] in which the agents cooperate by giving, pursuing, and evaluating referrals. Each agent in the

system maintains a list of contacts to query when needed. Selected contacts that receive a query can decide whether or not they can answer the query. If not, they may answer with a referral to others.

In MAS, the population is not stable as the agents join and leave the system frequently; this means that the information about the transitivity network structure is not always available. Additionally, building a social chain requires substantial computational and communication effort, and if the referral trust is inaccurate, the transitive trust may be invalid. Also, the resulted trust only relates to a certain context and cannot be transitive to different contexts.

2.1.4 Certified Reputation

When applying for a job, one of the key requirements is a reference or recommendation that provides an indication of the applicant's previous behavior. The same idea is adapted in MAS as one of the trust information sources. Certified reputation (CR) refers to "an agent reputation that is derived from third-party references about its previous performance" [18]. The difference between this type of reputation and witness information is that agents that adopt the CR mechanism will actively collect and present such references in order to seek the trust of their potential partners. This, in turn, moves the burden of obtaining and maintaining trust information from the trust evaluator to the agent being evaluated (in the same way as when applying for a job).

The certified reputation source overcomes some of the limitations that are associated with the other sources. For example, CR reduces the need to explore the environment to learn about other agents and build experience in the case of newcomers, which also decreases the risk of encountering unreliable partners. Furthermore, CR solves the problem of locating witnesses and therefore becomes an

effective alternative when comparing the time and costs of witnesses. The shortcoming of using CR is that third-party references might not be reliable and some agents may collude with other agents by providing false references.

The certified reputations trust model has been presented in [17] as their novel model of trust. In our research we also adopt CR as one of our trust information sources.

A similar idea to certified reputation is endorsement. A well-known agent in the system can endorse a certain agent by giving approval or support. Thus, new agents can use endorsement to bootstrap their reputation [31].

2.1.5 Stereotypical Trust

People tend to categorize others based on their visible features and use these categories to predict the behavior of unknown people. For example, working for a highly ranked firm gives the impression that the employee is highly skilled, so people tend to trust him/her more than the employee of a small firm. The same concept has been adapted to MAS to evaluate the trustworthiness of agents, especially when no other evidence is available anywhere within the society. In MAS, the visible features of agents are used to form generalized trust assessments under the assumption that there is a correlation between features and behavior [8, 25].

Stereotypical trust was introduced to the field of MAS as a trust model by many researchers. For instance [25] presents StereoTrust, in which agents form stereotypes by aggregating information from the context of the transaction, or the profiles of their interaction partners. The same idea is also discussed in [8]. Both approaches suggest sharing stereotypes to help newcomers who do not have enough past experience to form stereotypes. Regardless, the information scarcity issue still exists.

In this work we consider three information sources: direct experiences, roles and relationships, and certified reputation. We discuss our approach in greater detail in Chapter 3.

2.2 Related Approaches

In this section, we review some of the available systems and protocols that try to overcome uncertainties and risks in multi-agent systems. We highlight the advantages and disadvantages of these approaches.

2.2.1 FIRE

The FIRE model [16, 17] integrates four dimensions in order to compute the trustworthiness of a particular agent. 1) Interaction Trust (IT), which is based on previous experiences in interacting with the target agent to determine its trustworthiness; 2) Witness Reputation (WR), which is founded by collecting the experiences of other agents that interacted with the target agent to derive its trustworthiness; 3) Role-based Trust (RT), which deduces trust from the various relationships between the evaluator and the target agent (e.g. owned by the same company, friendship relationship, team-mate relationship). These relationships contribute to a prediction of trustworthiness for future interactions by assigning a predetermined trustworthiness value to the target agent, based on its role in the system; and 4) Certified Reputation (CR), which encourages the target agent to actively seek the trust of the evaluator by presenting arguments about its trustworthiness. Such arguments consist of certified references disclosed by third-party agents and made available upon request by an inquiring agent. CR is one of the novelties of the FIRE model. The addition of the CR dimension freed the agents from the need to look for witnesses who may be self-interested and not willing to share

their opinions. It also decreases the possibility that the evaluator fails to evaluate the trustworthiness of the target agent due to the lack of information [16].

Each of the aforementioned dimensions has a trust formula with an appropriate rating weight function to calculate the relevance or the reliability of the ratings. Moreover, the FIRE model defines a reliability measure to estimate the confidence level of the trust model. The model provides two forms of reliability: rating reliability, which is the reliability value of the rating set taken into account when computing the trust value, and deviation reliability, which is the deviation reliability value of the trust value. Basically, it calculates the deviation of ratings around the produced expected value to counteract the uncertainty due to the instability of agents. The two reliability values are combined to calculate the final reliability value of the produced trust value.

In general, the FIRE model is one of the distinguished models in open MAS. It integrates four information sources to provide a precise trust measure, handles the problem of newcomers partially, introduces a novel type of reputation called certified reputation, incorporates reliability measures, and deals with the dynamic characteristics of open MAS. However, the FIRE model still misses details on how to locate and select witnesses. It also needs a way to detect colluding references and to solve the problem when the provider has no past experience to share with the consumer.

In our model we did not consider witness opinion, as our intension is to address the issue when consumer agents are new and cannot locate witnesses. Thus, the research presented in this thesis is distinct from FIRE model in four aspects:

- **First,** FIRE model does not address the new agents problem completely; consumers still need to choose providers randomly in some cases and the CR

contains information about the previous experience of that provider only. On the other hand, the TC model allows a provider that has no experience to include credentials about its trustworthiness by acquiring membership from a recognized organization in order to use it as an endorsement. That also helps consumers who do not have any kind of relation with a provider to decide based on their trust in the organization rather than ignoring the provider because it is unknown to them.

- **Second,** the TC model adds a new metric to calculate the trust value on agents, which is to measure a consumer's level of confidence in a provider, based on number of roles and ratings the provider has.
- **Third,** the TC model includes an additional component, called ID part, to confirm the certificate integrity and to reduce the probability of receiving tampered certificates.
- **Fourth,** the proposed model introduces a direct trust calculation to update the consumer's database about providers after every transaction. That helps consumers to know their environment and differentiate between bad and good providers better.

In summary, the TC model provides help to new agents even those who have no experience at all. It also helps them learn about the system to increase their utility and decrease the number of unsatisfied transactions they may face.

2.2.2 RCertPX

RCertPX [35] is a reputation certificate in which the reputation data is stored and maintained by the provider in an independent manner. The certificate consists of two components: a header that contains information about the owner's identity, and the RCertUnit that encloses information about the transaction rating. The goal of the

certificate is to facilitate the retrieval of reputation information and guarantee the integrity of that information in peer-to-peer systems. The information is updated and digitally signed by the service consumer after each transaction, in order to prevent any tampering. The last consumer (rater) always digitally signs the whole certificate. When the consumer needs a certain service, all peers that have the needed service send their RCert to the consumer. The consumer then verifies the certificate's validity by contacting the last rater. If the last rater is not available (offline), then the one before it is contacted. After finding one of the raters, the certificate verification is done if the *TimeStamp* information in the *last-TimeStamp* matches what the rater created, and the *RevokedPeer* in the *last-TimeStamp* matches the next rater specified in the certificate. Based on the evaluation of all the RCerts received, the requesting peer makes its decision about which peer to choose as a provider. Upon the completion of the transaction, the consumer updates the provider's RCert and digitally signs it.

The RCertPX addresses the issue of integrity by using a digital signature to ensure that the owner has not tampered with the certificate content. It also addresses the issue of using old ratings and discarding the unsatisfied ratings by using the *last-TimeStamp* and contacting previous raters to verify the certificate validity. Although the protocol is complicated to ensure that a peer will not tamper with its reputation, it does not provide a trust model based on the stored ratings and it is still vulnerable to raters and ratees colluding to change the ratings.

In this research, we present a trust model to calculate the trust value of agents from ratings stored in the certificate and choose a suitable partner based on the resulted value. We also incorporate some metrics like rating time, degree of belief and confidence level in agents, to minimize the collude possibility between agents.

2.2.3 REGRET

REGRET [39, 40] is a reputation model that considers the use of social relationships between agents in e-commerce systems. The relations are presented in a graph structure called sociogram. The model includes three dimensions of reputation. First, the individual dimension, which calculates the trust based on the results of the direct interaction between the agents. Second, the social dimension, which is divided into three types:

1. Witness reputation based on the experience of others;
2. Neighborhood reputation that measures the reputation of individuals, who are neighbors with the target agent, and their social relationships with it using fuzzy rules. This can provide initial expectations about the behavior of that agent; and
3. System reputation, which examines the target agent's social role in the system to assign a default trust value to it. This system models the idea that groups can influence their members' behaviors.

The third and last dimension of the model is the ontological dimension. In this dimension, the trust value is not a result of a single aspect but a combination of reputations of different aspects. According to [40], for example, the reputation of a good seller is related to the reputation of providing good quality products, offering good prizes, and delivering the products quickly.

The REGRET model addresses the newcomers problem by using social relationships based on the assumption that an agent's behavior can be predicted using the information obtained from the analysis of its social relationships. It introduces the use of neighborhood reputation and system reputation to help newcomers. Although it initiates a promising solution to the problem, it is not readily available because it does

not explain how agents build their sociograms, which display their social relationships. Also, building such sociograms is based on the agent's knowledge of the environment, which is not suitable for new agents. It may not be applicable in environments with random and contradictory agents.

In contrast, the TC model consider the agents roles and relations from two aspects:

1. The relationship between the two agents.
2. The agent's role in the system.

So, consumers without knowledge about the environment can still benefit from the role part and use it as a part of their calculation.

2.2.4 Other Related Approaches

Many of the other proposed works have presented concepts that would help addressing the lack of direct experience and history issue in MAS. For instance, the stereotype model [8] is inspired by human organizational behavior to solve the problems related to cold-starts and newcomers. In this model, a consumer agent classifies its previous experiences with other agents into classes based on their features. Then the evaluator generalizes its experience with known partners to evaluate the trustworthiness of unknown agents (providers). Although the model is a valuable improvement in trust modeling, especially during cold-start and newcomer cases, it still needs to gather more information in order to be built. It does not cover the cases in which the consumer and the group are new with no direct experience or reputation available to build the stereotype.

Mass and Shehory [30] introduce the use of certificates to establish trust in MAS. The certificates are used to identify the agents, using public key infrastructure, and claim certain attributes about those agents. In fact, agents use the certificates to

gain the trust of other agents in the system. For instance, an agent that works as a stockbroker may present the following certificate [30]:

C = Cert (CityBank, Agent X, certType = Broker, Type = Nasdaq, Service = good) which states that CityBank asserts that Agent X is a stockbroker for stocks traded on Nasdaq, with a good service quality.

Based on a set of certificates, the evaluator agent uses a role assignment policy to assign the target agent to predefined roles, which establishes the trust. Although we use a similar certificate concept in our proposed approach, our certificate has a predefined format that combines two information sources to provide quantified information that can be used to estimate the trustworthiness of the target agent.

The idea of endorsement could be adapted as a bootstrap. The authors of [31] present a reputation and endorsement model to bootstrap the reputation of new service providers, allowing them to be chosen despite their lack of history. However, the endorsement does not reflect the actual performance of the providers.

2.3 Summary

In this chapter, we have reviewed literature related to trust in open MAS. More specifically, we focused our discussion on trust information sources and related approaches. We explained the main idea of each source then reviewed relevant approaches related to that source. The kind of information available to an agent may vary depending on the applications where the action is taking place. As seen from the review, some models rely on one information source while others rely on more than one. Actually, the more information sources used, the more the reliability of the calculated trust values increases.

We also reviewed works that attempt to deal with the information scarcity issue in open multi-agent systems.

Our research focus is on helping agents determine trust values themselves, without a central authority. For this reason, all the models reviewed are decentralized, where no central authority is needed for trust evaluation.

In the following chapter, we present our model and explain how it can help agents establishing trust in situations where not enough information is available.

Chapter 3: Proposed Approach

Most trust models in MAS evaluate agents' trust based on prior interaction history either using direct experience with the agent or using third parties reports (reputation). Unfortunately, there are cases in which the number of interactions is insufficient to produce trust value; for instance, when agents newly join the system and have no experience. In other cases, it can be difficult to locate third party witnesses and if found, they may not be willing to share their experiences. In this chapter, we present a new model called *Trust Certificate* (TC) model. This model allows agents to retrieve reputation information and make initial trust evaluations when evidences are unavailable. Generally, in the TC model, agents provide proofs about their capabilities and previous performance to gain other agents' trust. Our aim is to improve the performance of the existing models and help agents to avoid the need to make a random partner selection due to the information scarcity. We show how this model can enhance the partner selection and the interaction processes between agents by evaluating it in the context of a simulated multi-agent system in chapter 4.

The remainder of this chapter is organized as follows; Section 3.1 is an overview of the model and its components. Section 3.2 presents a glance at how to insure the certificate's integrity using digital signature. In section 3.3, we outline the sources of trust information used in the TC model and how to combine them to

calculate the total trust value. In section 3.4, we elaborate the model mechanism. Section 3.5 presents a comparison between the related approaches and our approach, based on some important features. Finally section 3.6 summarizes the chapter.

3.1 Trust Certificate Overview

Our TC model is inspired by a number of trust models [17, 30, 33]. It is designed to assist consumer agents in building trust in their potential partners and also to help new agents integrate into an agent society as reliable partners by using certificates. A certificate is a signed electronic document that contains some claims about the agent [30]. In our model, each agent is equipped with a certificate, which works as a reference by providing information about its holder. The information is obtained and stored by the agent itself and is available to other agents who request it to evaluate the holder's trustworthiness for a potential interaction. The stored information is about the agent's role in the society and its performance in past interactions.

The Trust Certificate of our model consists of three components: ID, role and certified reputation (Figure 3.1). The first part of the certificate is the ID part, which contains information about the owner to bind the certificate to its owner. Each agent has a unique identifier to prove its identity and owns the private key that corresponds to the public key in the certificate. The ID part contains the following elements:

- Owner ID: identifies the owner of the certificate.
- Owner public key[1]: which is used to authenticate the provider identity (more details in Section 3.2.1).

The second part of the certificate is role part, which contains information about the roles that the agent plays in the society. Identifying the provider's role gives

1 Each agent has a private key that should be matched with the public key to evaluate the validity of the certificate,

the service consumer a way to expect the provider's behavior [33]. In some cases, it also gives a predetermined level of trustworthiness about the service provider [17]. The roles can be a membership of a popular scheme or organization that provides a quality assurance about its members' services (e.g. authorized dealer) or it can be an endorsement certificate from a trusted agent or organization. An agent can have one or more roles or no role at all. Each role includes assigned role, issuers ID, issuer's signature and role expiry dates. The assigned role indicates the agent's role in the society. The issuer ID and the issuer signature are used to identify who issued the role and prevent any tamper to the role (more details in Section 3.2.2). The service consumer may use the issuer ID and issuer signature to verify the correctness of the provided information. Finally, the expiry date is used to ensure the validity of the role as agents can change their roles from time to time. The use of the role part helps new agents, with no reference about their performance, to advertise their trustworthiness and then start interacting with other agents in the system.

The third part of the certificate is certified reputation (CR), in which the provider agent stores the ratings of its interactions with other agents in a local database to be ready whenever needed by a service consumer prior to an interaction [18]. This type of references helps new agents to attract consumers to interact with them by showing their performance from past interactions. Agents can include many ratings in their certificate, but focusing on the recent ones as they carry more weight in trust evaluation. Each certified reputation contains five components:

- Rating value: indicates the rater's opinion about the interaction in the form of ratings.
- Rater ID: confirms the identity of the rater.
- Rater signature: ensures the validity of the rating.

- Time Stamp: stores the time of the interaction.
- Counter: keeps track of the number of stored interactions.

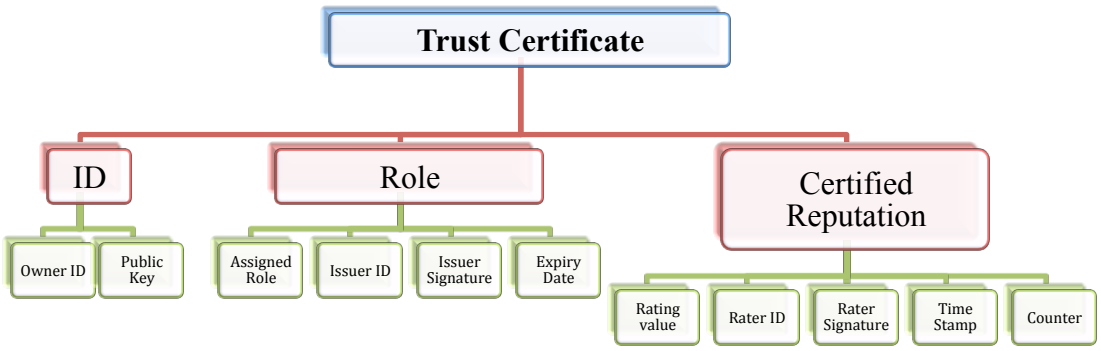

Figure 3.1: Trust Certificate

3.2 Trust Certificate Integrity

The intention of our Trust Certificate (TC) model is to minimize the involved risk in randomly relying on other agents in the network. Since service providers in the TC model are responsible for offering proofs about their trustworthiness, service consumers should have a way to verify the integrity of that proofs. In order for the consumer to check the validity of the certificate, it requires protocols to provide secrecy and authentication of both the provider's identity and the content of the certificate. The protocol that is used is *digital signature*, which is based on a system called *public key cryptography*. A provider is issued two keys, one private and one public. The keys are really two numbers related by an algorithm such that it is generally impossible to deduce one key from knowledge of the other. Digital signature is an attachment to a document used to verify or authenticate a ''signer'' and the document signed, much like a signature on a paper document [12]. It has the ability to verify the document author, date and time of signature, to authenticate document content and to be verified by third party to resolve disputes. Digital

signature is used in the TC model to guarantee the security of providers' certificates. The public key is authorized by the *Certificate Authorities* (CA), which can be any trusted central administration willing to ensure the authenticity of whom it issues the certificates for and their association with a given key.

The consumer needs to go through a series of verifications to validate any certificate:

1) Verify the provider identity using the ID part.

2) Verify that the certificate contents (role and CR) have not been altered.

The following subsections explain each one of the verifications briefly.

3.2.1 Verify the Provider Identity

The ID part in the certificate is used to bind the provider's public key to the provider's ID, which authenticate the provider and prove its identity. The provider proves its identity by using a public key and the private key that corresponds to that public key. The proof is done by the provider signing with its private key on the certificate and then the consumer can check the signature using the public key.

3.2.2 Verify the Certificate Contents

Authenticating the provider identity alone is not enough to ensure the certificate integrity. The certificate contents should also be verified by the consumer to avoid any malicious activities. Both role and certified reputation parts of the certificate include a signature. The rater/issuer encrypts some data with its private key to be its signature. After getting the provider's trust certificate, the consumer can decrypt the data using the rater's public key. A successful decryption is a proof that the rating (certificate) was indeed signed by rater (or the issuer) (see figure 3.2).

By verifying the certificate contents, two security key aspects are satisfied:

- *Issuer/Rater authentication:* The consumer needs to authenticate the issuer/rater identity. Digital signature can be used to authenticate agents, who issue roles for the provider or give rates about the providers' behavior.
- *Certificates security:* There is a necessity to secure the integrity of the certificates to ensure that content of the certificates are reliable, accurate and auditable. It is required to ensure that the provider can't alter the certificate's content.

Once the Trust Certificate integrity is ensured, it will bring in protection of the certificate against alteration. It also provides a way to guarantee that the issuer/rater cannot later deny having signing the certificate and the consumer has much more confidence in relying on the certificate in evaluating the provider's trustworthiness.

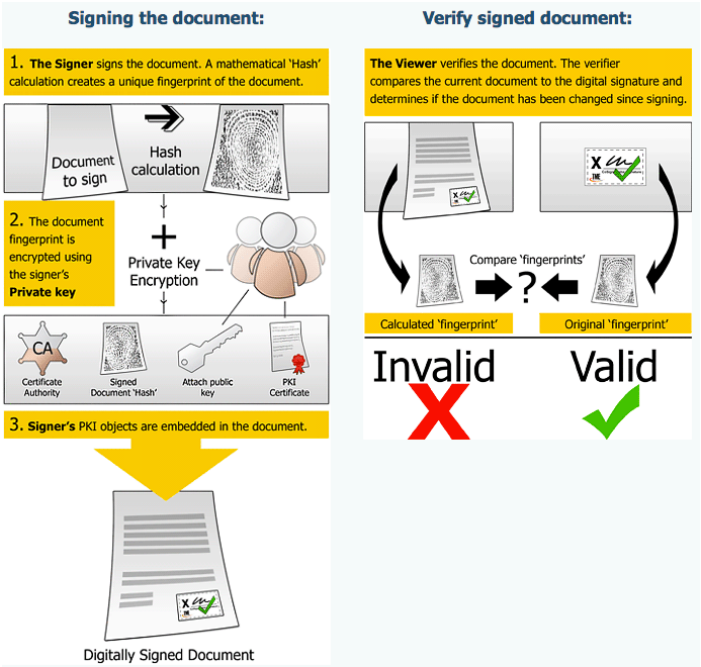

Figure 3.2: Digital Signature Process
Source: http://www.securedsigning.com/

3.3 Trust Evaluation Using Trust Certificate

Agents in MAS need to establish some level of trust in each other prior to any interaction. Establishing the essential trust requires some sort of information that can be obtained from many different sources. In the proposed TC model, three sources of trust information are integrated in order to estimate the trust value closely. These sources are:

- Role-based trust, based on roles played by the provider in the group and the relationships between the consumer and the provider.
- Rate-based trust, based on third party opinion about the provider previous behavior.
- Direct Experience-based trust, based on the consumer direct observation of the behavior of the provider.

Typical trust model includes a consumer agent x who evaluates the trustworthiness of a provider agent y, to establish an interaction. Every consumer agents has a local database to store its ratings about other agents and its own set of roles along with their values. At the same time, each provider stores the ratings it receives from others in its database. Trust value (ratings) is usually in the range [-1, 1] where -1, 1 and 0 indicate absolute distrust, absolute trust and neutral, respectively.

The remaining of this section explains how to calculate each trust component separately, and then how to combine them to obtain the total trust value.

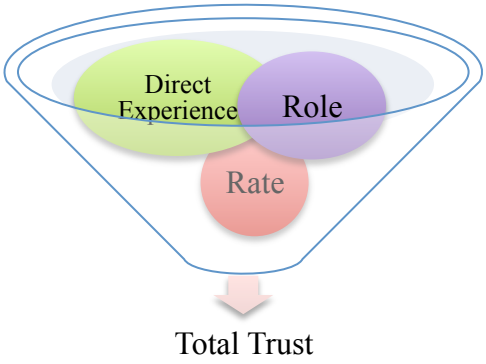

Figure 3.3: Trust Sources

3.3.1 Role-based Trust

The basic idea behind role-based trust is that the roles agents are playing in the system provide some information about their capabilities and future behavior. This kind of information is an alternative to experience in calculating trust, especially for newcomers.

An agent in the system can have one or more roles. There are a finite number of possible roles in each system, which can be classified into two types:

- First, the roles an agent can have by participating in a known organization or having a membership. The underlying assumption in membership is that agents belonging to a group would behave similarly and memberships can provide a quality assurance about the agent's performance. For example, a seller can obtain permission from a known manufacturer to hold the title 'authorized seller'. So, agents who trust that manufacturer will trust its authorized seller agent. This type of roles is found in the Trust Certificate of the provider.
- Second type of roles is that represents the relationship between agents. It defines the positions of agents in term of their importance to other agents in

the system. For instance, authority, seniority, or expert, etc. The agent's owner assigns this type of roles to it at the time of creation.

All agents should authenticate their roles by possessing certificates issued by trusted certificate authority. In our model these certificates are part of the Trust Certificate.

Since trust is a subjective measure, each consumer agent has its own list of roles with the matching trust values that represent the capacities of the provider agent, which has the role in the system, and their corresponding confidence levels. The confidence level of each role is based on the criteria of that role and the provider who owns it. For example, we tend to trust doctors with more years of experience more than first year doctors despite the fact that both of them have the same role "Doctor". Once the consumer agent knows the provider role, it looks up for the relevant values from its database. The set of roles is given to the consumer agent at the time of creation and is updated from time to time.

To calculate the role-based trust value for an agent, the evaluator should look up two components from its database for each role played by the agent: the value of the role $v_{ro} \in [-1, 1]$, where -1 means untrusted and 1 means trusted, and the confidence level (degree of belief) on that role $b \in [0, 1]$ where 0 indicates complete uncertainty and 1 for total confidence.

Since each consumer assigns two values (b, v_{ro}) to each role, we want a measure that captures the inter-relation (correlation) between b and v_{ro} values and estimates the future behavior of the provider based on those values. Such measure should reflect the relevance of each role's value because some roles count more strongly than others, in that they are given more weight (b) in the calculation. Moreover, our measure should vary from a minimum of -1 to a maximum of 1. We

can then define the role-based trust value of the provider as the weighted average of all roles based on the degree of belief:

$$T_{RO}(x, y) = \frac{\sum b \,.\, v_{ro}}{\sum b} \tag{3.1}$$

where $T_{RO}(x, y)$ is the initial role-based trust value that agent x has in agent y ($-1 \leq T_{RO}(x, y) \leq 1$) based on its roles in the system. In other words, the role-based trust of a provider is calculated as the sum of all its assigned roles weighted by the degree of consumer's belief in each role and divided by the sum of all the beliefs to normalize the value to the range [-1, 1].

Calculating the role-based trust value based on the roles and their individual beliefs alone may not be enough. We need to measure the reliability of the provider in terms of how much confidence we should put on the trust value resulted from formula (3.1) above. Hence, we define the measurement of such confidence in the provider based on the number of roles it has. The greater the number of roles it has, the larger the confidence is.

$$C_{RO} = \min\left(\frac{RO_n - RO_{min}}{RO_{max} - RO_{min}},\ 1\right) \tag{3.2}$$

where C_{RO} is the confidence in the provider y, RO_n is the number of roles the provider has, RO_{min} and RO_{max} are the minimum and maximum number of roles the provider can have, respectively. RO_{min} and RO_{max} are used to normalize C_{RO} into the range of [0, 1] where 0 indicates complete uncertainty and 1 total confidence. The minimum and maximum number of roles are application specific. For example in an agent-based market environment, the roles are perhaps only buyer, seller or advisor whereas

in an agent vehicular ad-hoc network, there could be more roles such as authority, seniority, expert and ordinary. A possible challenge a consumer may face is when a provider has only one role but that is a very important role such as "authority" or "expert", and the RO_{max} is large, then the confidence level C_{RO}may reduce the role-based trust value of that provider significantly. However, since the maximum number of roles is application specific, the consumer can adjust the value according to its needs to maintain the high role-based trust value for that provider.

Finally, after calculating the initial role-based trust value and measuring the confidence level in the provider, the total role-based trust value is calculated as follows:

$$T_{Role}(x, y) = T_{RO}(x, y) \cdot C_{RO} \tag{3.3}$$

where $\mathrm{T_{Role}(x, y)}$ is the total role-based trust value that agent x has in agent y ($-1 \leq \mathrm{T_{Role}(x, y)} \leq 1$) based on y's roles in the system and the confidence level C_{RO}.

Participating to multiple organizations and having multiple roles in the system are used as an indication about the agents expected trust. The idea is that, every role has an impact on the provider regardless the role type.

We illustrate the impact of the number of roles on the trust calculation by the following example: The consumer evaluates the role-based trust of two providers where the first provider y_1 has three roles A, B and C and the second provider y_2 has only two roles A and B, which have the same values as provider y_1's, as follows:

- Role A: v_{ro} = 0.4 and b = 0.2
- Role B: v_{ro} = 0.5 and b = 0.3

At first, the role-based trust value is the same for both parties 0.46 (Formula 3.1). But

if we add an extra role to y_1 (role C: v_{ro} = 0.2 and b = 0.1), then the trust value of y_1 becomes 0.42 (by Formula 3.1) and the trust value of y_2 remains as 0.46. This case shows some undesirability because it ignores the impact of the third role and, as a result, it gives more value to the second provider although the first provider has more roles.

To address this issue, we now use the number of roles as a measure of the confidence on the provider as in formula 3.2. To show the influence of Equation 3.2 on role-based trust value, we go back to the example in the previous paragraph and calculate the confidence of each provider based on the number of roles using RO_{min}= 0 and RO_{max}= 5. As a result, y_1 gets 0.6 confidence level and y_2 gets 0.4. The next step, we multiply the confidence level by the trust values of each provider (Formula 3.3) to get a more accurate evaluation. The final results give role-based trust values for both providers, including the confidence of the provider. In this example, y_1 gets 0.25 and y_2 gets 0.18, which are more desirable than using formula 3.1 alone.

This example shows the importance of adding the confidence measure to the process of evaluation illustrates that without using such a measurement results will not be accurate enough.

3.3.1.1 Rule of Decision:

The consumer makes its decision to trust the provider or not by evaluating the provider's roles and the confidence level through 3 steps:

1. Calculate the initial role-based trust value using the roles values and the level of confidence the consumer has in each individual role (Formula 3.1).
2. Calculate the confidence in the provider based on the number of roles the provider has (Formula 3.2).

3. Calculate the final role-based trust value by multiplying the initial role-based trust value by the confidence in the provider (Formula 3.3).

The consumer will tend to trust the provider on the ground of the role-based trust value when $T_{Role}(x, y)$ is closer to 1 (its maximum value). This is reasonable since the measure $T_{Role}(x, y)$ can get closer to 1 when both confidence level C_{RO} and role value $T_{RO}(x, y)$ increase (meaning agent y is increasingly trustworthy).

3.3.2 Rate-based Trust

Agents' reputation plays a fundamental role in trust decision process. However, it is not always possible to locate witnesses. That problem raises the need for an effective way to retrieve agent's reputation information and ensure its integrity. Rate-based trust is reputation information about the agents' past behavior that is provided by third party agents in the form of ratings. The difference here is that the agent obtains and stores the information in its local database and makes it available whenever needed by other agents for trustworthiness evaluation purposes.

In this type of trust, the consumer checks the previous behavior of the provider by using third party opinions. The ratings allow the provider to confirm its performance in order to gain the trust of its potential consumer. It starts by the agent asking its partners after every transaction to provide their feedback (ratings) about its performance and then stores it in its local database. So, when a new agent (consumer) is interested in partnership with that agent, the agent can provide its certified references to confirm its past performance and gains the consumer trust. On the other hand, the consumer agent calculates the rate-based trust from the set of certified ratings that it received from the potential partner.

Agents may be tempted to alter their ratings to obtain a higher rate. To prevent tampering, each rating is included in a certificate (*certified reputation)* that is digitally

signed for verification purposes. If the content of the certificate is tampered, the verification will fail. Another issue is that the agent tends to only present its best ratings and hide the bad ones. We can address this issue by considering the time decay effect of ratings using a rating recency function [17]. We use the recency of the ratings to give recent ratings more weight than older ones, so the effect of old ratings decreases as time goes by, and thus trust values computed based on old ratings should also be decreased accordingly. That should increase the accuracy of the calculated trust value as agents are forced to share their recent ratings to increase their probability of being trusted. The suggested recency function is based on the time difference between current time and the rating time to reflect precisely how old a rating is [17]:

$$t_{r_i} = e^{-\frac{\Delta\tau(r_i)}{\lambda}} \tag{3.4}$$

where t_{r_i} is recency of the rating r_i, $\Delta\tau(r_i)$ is the time difference between the current time and the time when the rating is recorded, and the parameter λ, called the recency scaling factor, is hand-picked for a particular application depending on the time unit used in order to make the rating recency function adjustable to suit the time granularity in different applications. The exponential function is used in the recency function because its shape over time fits the suggestion that the rating time should affect the trust value evaluation.

To calculate the rate-based trust value we use a similar approach as we use in role-based trust. Since we use recency function as a weight for the ratings, we want a measure that captures the correlation and estimates the future behavior of the provider based on its past behavior. Additionally, the measure should vary from a minimum of

-1 to a maximum of 1. We can then define the rate-based trust value of the provider as weighted average of all rates based on the time decay effect:

$$T_{RA}(x,y) = \frac{\sum t_{r_i} \cdot v_{ra}}{\sum t_{r_i}} \tag{3.5}$$

where $T_{RA}(x,y)$ is the initial rate-based trust value that agent x has in agent y ($-1 \leq T_{RA}(x,y) \leq 1$) based on third party opinion (v_{ra}). In short, the rate-based trust of a provider is calculated as the sum of all its available ratings weighted by the time decay effect, divided by the sum of all the time decay effects to normalize the value to the range [-1, 1].

Now, we define the measurement of confidence in the provider based on the total number of ratings it has: The greater the number of ratings it has, the larger the confidence is. The number of ratings can be seen as a measure of the provider's previous experience based on which we build our confidence. We assume that if the provider has participated in a lot of transactions and gained ratings from different consumers in the past, then it is considered to be an expert that can provide a more reliable service than a provider with less number of transactions.

$$C_{RA} = \min\left(\frac{RA_n - RA_{min}}{RA_{max} - RA_{min}},\ 1\right) \tag{3.6}$$

where C_{RA} is the confidence in provider y, RA_n is the number of ratings the provider has (which is the Counter parameter in the Certified Reputation part of the Trust Certificate), RA_{min} is the minimum number of ratings the provider can have and RA_{max} is the maximum number of ratings. RA_{min} and RA_{max} are used to normalize C_{RA} into the range of [0,1] where 0 indicates complete uncertainty and 1 total

confidence. The minimum and maximum number of ratings a provider can have are dependent on the application and the consumers' choice.

Then, the total rate-based trust value is calculated as follows:

$$T_{Rate}(x,y) = T_{RA}(x,y) \,.\, C_{RA} \tag{3.7}$$

where $T_{Rate}(x,y)$ is the total rate-based trust value that agent x has in agent y ($-1 \leq T_{Rate}(x,y) \leq 1$) based on y's previous experience with other agents in the system and x's level of confidence C_{RA}.

3.3.2.1 Rule of Decision:

The consumer makes its decision to trust a provider or not by evaluating the provider's previous ratings and the confidence level through 3 steps:

1. Calculate the initial rate-based trust value using the rates values and the time window in which the ratings were provided (Formula 3.5).
2. Calculate the confidence in the provider based on the number of ratings the provider has (Formula 3.6).
3. Calculate the final rate-based trust value by multiplying the initial rate-based trust value by the confidence in the provider (Formula 3.7).

The consumer will tend to trust the provider on the ground of the rate-based trust value when $T_{Rate}(x,y)$ is closer to 1 (its maximum value). This is reasonable since the measure $T_{Rate}(x,y)$ can get closer to 1 when both confidence level C_{RA} and rating value $T_{RA}(x,y)$ increase (meaning agent y is increasingly trustworthy).

3.3.3 Direct Experience-based Trust

The term direct experience-based trust refers to the trust that is gained through direct observation of agent's behavior. The consumer uses its previous direct interaction

with the provider to determine its trustworthiness depending on its satisfaction with the past interactions. It is also a continuous process. Whenever a new interaction happens between the provider and the consumer, the consumer's direct trust in that provider is updated based on the new observation.

Here we employ the direct-experience trust of [45]. Each agent rates its partner after each transaction depending on level of satisfaction and updates its database accordingly. Only the most recent trust values will be stored. Subsequently, the agent can query its database for the ratings to calculate its partners trust value.

The range of all trust value is [-1, 1], where 1 represents absolute trust and -1 represents absolute distrust. At first, when x has not interacted with y before, we set $T_{Direct}(x, y) = 0$ as no information about $y's$ behavior is available. Then after the first interaction, the consumer updates its experience with the provider according to the result of the interaction as following:

If the consumer is satisfied with the result, then the trust value increased by

$$T_{Direct}(x, y) \leftarrow \begin{cases} T_{Direct}(x, y) + \alpha(1 - T_{Direct}(x, y)) & if\ T_{Direct}(x, y) \geq 0, \\ T_{Direct}(x, y) + \alpha(1 + T_{Direct}(x, y)) & if\ T_{Direct}(x, y) < 0, \end{cases} \quad (3.8)$$

where $0 < \alpha < 1$ is a positive increment factor.

Otherwise, if the consumer is unsatisfied with the result, then the trust value decreased by

$$T_{Direct}(x, y) \leftarrow \begin{cases} T_{Direct}(x, y) + \beta(1 - T_{Direct}(x, y)) & if\ T_{Direct}(x, y) \geq 0, \\ T_{Direct}(x, y) + \beta(1 + T_{Direct}(x, y)) & if\ T_{Direct}(x, y) < 0, \end{cases} \quad (3.9)$$

where $-1 < \beta < 0$ is a negative decrement factor.

The two factors α and β are used to adjust the trust ratings of providers. The absolute values of α and β are varied depending on the data availability and services' importance. Trust should be difficult to build up, but easy to tear down, so the consumer may set $|\beta| > |\alpha|$ to protect itself from dishonest providers.

3.3.4 Total Trust

Since each trust component uses a separate source of information to produce trust values, we need to combine them to calculate the overall trust value. There is no guarantee that all the components will be available, so we will use the available sources. If only one component is available, then it is used solely to find the trust value. Otherwise the following formula is used:

$$T_{Total}(x, y) = \sum_{m=0}^{2} w_m T_m(x, y) \tag{3.10}$$

where $\mathrm{T_{Total}(x, y)}$ is the overall trust that agent x has in agent y, m is thus one of the Direct experience-based, Role-based or Rate-based trusts, and the weight $\mathrm{w_m}$ is set to reflects the importance of each component ($\sum \mathrm{w_m} = 1$). We give direct-experience trust higher weight than the others because it is based on the agent's own evidence and should be more reliable. If the two agents never interact before then we set w_{Direct} to 0 as no direct interaction between the two agents exists yet. We provide some general guidelines for setting w_m as follow:

Setting w_m values

Initially, $w_{Direct} = 0$. The other two parameters w_{Role} and w_{Rate} are set to arbitrary values so that they add up to 1. For example: w_{Role} = 0.5, w_{Rate} = 0.5. Because the direct experience-based trust is resulted from the direct observation of the consumer agent itself about the provider's performance, it should carry more weight than the other trust sources. As a result, we want a rule that allows for w_{Direct} gradually increasing toward 1 while both w_{Role} and w_{Rate} gradually decrease toward 0. To achieve this goal one approach is to recalculate the weights as follows:

$$w_{Role} \longleftarrow (w_{Role})^{n+1} \tag{3.11}$$

$$w_{Rate} \leftarrow (w_{Rate})^{n+1} \tag{3.12}$$

$$w_{Direct} \leftarrow 1 - w_{Role} - w_{Rate} \tag{3.13}$$

where n is the updating time step; for example a consumer agent may update the weights after every five interactions, or after every ten interactions, etc. with the same agent. Such updating rule increases the weight w_{Direct}, which gives direct experience-based trust more weight than other trust values, as desired.

3.4 The Mechanism of Trust Certificate

Every provider agent in the system is equipped with a Trust Certificate that is used by the consumer to evaluate the trustworthiness of the provider. Rational consumer agent always works to maximize its utility from any interaction. In cases where the interaction involves relying on another agent to fulfill the interaction requirements, the consumer needs to assess the provider's ability to cooperate honestly before starting the interaction. In this section we explain how the consumer uses the Trust Certificate model to predict the future behavior of its partner by calculating its total trust value.

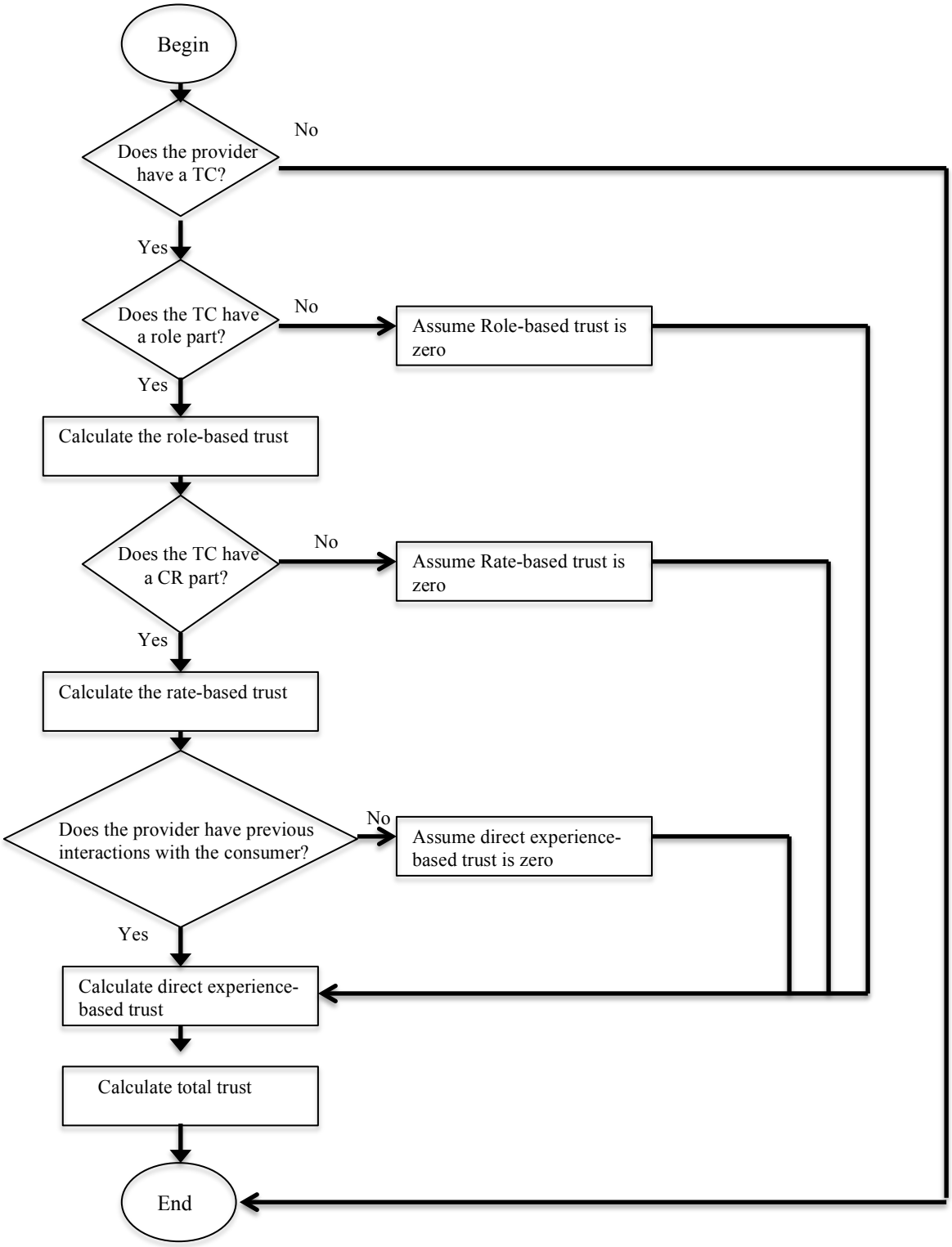

Figure 3.4: TC model transaction algorithm

The Trust Certificate model is used by an agent x (consumer) to evaluate the trustworthiness of agent y (provider) with a view to establish an interaction, as shown by the algorithm depicted in Figure 3.4.

The process for a consumer agent x to choose and have a transaction with a provider agent y occurs as follows:

1. Sends a service request to the system in order to find a provider.
2. Receives a list of interested providers along with their trust certificates.
3. Verifies the certificates' validity and integrity upon receiving them. If they are invalid or tampered with, then rates the provider as untrustworthy (see algorithm in Figure 3.5).
4. Assesses the provider's expected trust value, which is resulted from Role-based trust, Rate-based trust or Direct-experience-based trust. This starts with assessing the trust value for each component separately, and then combining them at the end to get the total trust value (as described by algorithm in Figure 3.4).
5. Chooses the provider with the highest trust value after evaluating all the certificates and calculating the trust values.
6. Sends an acknowledgement to the selected agent y indicating that it has been chosen to provide the service.
7. Starts the transaction.
8. Rates y after the transaction completion based on the final result then sends the rating to y along with the signature.
9. Updates its internal database with the new experience.

By the end of this step, both x and y have an experience with each other. They can use the experience in finding the trust value of each other in future interactions, share their ratings with other agent or use it in building a stereotype to evaluate other agents.

The consumer is not only evaluating the provider performance, but also evaluating the referees who give the certified references to the provider. It also revises and updates its internal role database according to the new experiences. We will leave these points for future work.

Algorithm 1: Verification Steps

For all received trust certificates
    if *Date is expired*
    or
    The public key doesn't match the private key
    or
    The information is tampered with
    then
    rates the provider as untrustworthy
    else
    Continue with the trust evaluation process (above)
    end if
end for all

Figure 3.5: The verification steps algorithm

3.5 TC model and Related Approaches

The main goal of the TC model is to help new consumers retrieving reputation information to evaluate their partners' trustworthiness when enough evidence is unavailable and also to help new providers integrating into the systems as reliable partners. We compare the existing related models (from section 2.2) with the TC Model for their ability in achieving the main goal. They are compared based on the following features:

1. The environments they are designed to work in.
2. Their ability to provider a trust model to calculate the trust value from the provided evidences.
3. Their ability to assist new consumers in evaluating the trust value.
4. Their ability to assist new providers to demonstrate their trustworthiness and gain consumers trust.
5. Their ability in producing trust values in cases where experiences are unavailable for both consumers and providers.
6. Their ability to provide proofs about the providers' identity.
7. Their ability to measure the confidence level on the providers.
8. Information sources used to calculate the trust value.
9. Measurement parameters that are used to increase the accuracy of the resulted tryst value.

Table 3.1 summarizes points 1 through 5, while Table 3.2 summarizes the remaining points. The meanings of symbols used in Tables (3.1 and 3.2) are as follows:

- P: the model addresses the corresponding feature partially.
- Y: the model satisfies the corresponding feature.
- N: the model does not satisfy the corresponding feature.
- N/A: the corresponding feature is not applicable.

Model	System	Trust model	Consider Consumers	Consider Providers	Work without Experience
TC	MAS	Y	Y	Y	Y
FIRE [17]	MAS	Y	Y	P	P
REGRET [39, 40]	E-commerce	Y	Y	N	N
Stereotype [8]	MAS	Y	Y	N	N
RCertPX [35]	Peer-to-peer	N	Y	N/A	N

Table 3.1: Comparing related models with the TC Model (Part 1)

Model	Identity check	Confidence level	Information sources	Measurement parameters
TC	Y	Y	▪Roles ▪Certified reputation	▪Belief in the roles ▪Time of ratings ▪Number of roles ▪Number of ratings
FIRE [17]	N	N	▪Roles ▪Certified reputation	▪Belief in the roles ▪Time of ratings
REGRET [39, 40]	N	N	▪Neighborhood Reputation ▪System reputation	▪Time
Stereotype [8]	N	N	▪Direct experience ▪Third party	▪Difference between actual opinions and those predicted by the model
RCertPX [35]	Y	N	▪Certified reputation	N/A

Table 3.2: Comparing related models with the TC Model (Part 2)

3.6 Summary

The need for trust establishment increases in systems where entities rely on each other in order to achieve their goals. An important version of these systems is open dynamic multi-agent systems. In such systems, agents can freely join and leave the society at any time, which may affect the system's structure. This feature introduces the problem of how to choose a partner, especially if we know that agents are self-interested and there is no central authority regulating the selection process. Many researchers address the problem by introducing computational trust models and current state of the art trust models generally consider trust as a function of prior interactions with a potential partner, whether it has been obtained directly or by other agents in the society. However, agents may encounter other agents who have no previous experience with and, at the same time, cannot have an access to other members' evaluations, e.g. when the agent is new to the system, the system itself is newly created, or the agents are not willing to share their experiences. In such cases, agents have no choice but to explore the population and choose partners randomly. This option involves high risk when the agent selects an unreliable partner.

Against this background, we propose a new model Trust Certificate (TC) model that relies on certificates. In this chapter we have introduced our Trust Certificate model and described its basic components. The model contains a certificate that comprises three parts ID, role and certified reputation. The consumer uses the certificate to calculate the expected behavior of potential providers and then choose a provider accordingly. The computed values are a result of combining three information sources: rate-based, role-based and direct experience-based. We also discuss the required procedures to ensure the certificate's integrity. We explained the

mechanism of the certificate and how the consumer uses it to find a partner. Finally, we compared the proposed model with the existing models.

In summary, the contributions of this model are: First, enabling agents to overcome the absence of trust evidence (direct and reputation). Secondly, helping new agents to emerge into the system and gain trust. Thirdly, providing new agents with the initial information that is required to build trust in order to protect them from relying on unreliable partners. Finally, reducing the risk of choosing partners randomly.

In the following chapter, we will evaluate our model to demonstrate its effectiveness in reducing the risk level that is associated with selecting partners in cases where not enough evidence is available.

Chapter 4: Experimental Simulation

In chapter 3, we argue that agents interacting in MAS can implement the Trust Certificate (TC) model in order to make initial trust evaluations when direct evidence and reputations are unavailable. We presented the model in detail and described how it could provide a solution to the information scarcity problem. To support our argument, we evaluate our TC model in the context of a simulated multi-agent system.

To evaluate the proposed model in a more practical manner, we have designed a simulation environment using MASON (Multi-Agent Simulator Of Neighborhoods (or Networks)) [1] and compared the TC model to the Random model, in which consumers select providers randomly, using multiple evaluation metrics. In this chapter, we present the experiments conducted with software simulations to examine the effectiveness of the proposed model. The experimental results demonstrate that the proposed TC model does reduce the risk of relying on untrustworthy providers; it also helps new providers to get selected by consumers.

Section 4.1 of this chapter describes the implemented simulation software and the experimental set-up. The test models are presented in Section 4.2. Section 4.3 provides details about the simulation operation, and the experimental results received

for both the consumer and the provider agents are reported and discussed in Section 4.4. Finally, the chapter concludes with a summary in Section 4.5.

4.1 Simulation Overview

An Agent Based Simulation Modeling approach is employed in this thesis to evaluate the proposed model. After reviewing how similar approaches have been evaluated, we decided to use the MASON platform, as it is already developed and tested, and it provides us with many of the tools we need to build our model.

MASON is a fast, discrete event multi-agent simulation library core in Java, designed to be the foundation for large custom-purpose Java simulations, and also to provide ample functionality for many lightweight simulation needs [27].

Before introducing the simulated models and the simulation results, we first clarify some important notions related to the simulation environment and its components. In the following subsections, we introduce the objective of the simulation and our assumptions. We also present the simulation environment with all the required components. In addition, we include a detailed description of the agents, as well as their roles in the system, plus all of their attributes. Finally, we conclude the section by presenting how to set up the simulator with all the parameters and variables, including the evaluation metrics.

4.1.1 Simulation Objective

The main objective of the simulation is to evaluate the validity of using the TC model to reduce the risk associated with the lack of trustworthy information, compared to random partner selection, and to help new agents start their life in the system. In summary, the simulation addresses the following questions:

- Does the Trust Certificate model help consumer agents select the most reliable partners?
- Does the Trust Certificate model help new provider agents to be selected for interactions?

4.1.2 Assumptions

To focus on the effectiveness of our proposed approach components, we have made some temporary assumptions. Some assumptions may look unrealistic for open MAS, but we are planning to expand the approach to more complex scenarios in the future. The assumptions are:

- ***All agents are willing to exchange information honestly***: In this assumption, we assume that agents are willing to collaborate and provide references to their partners. Although this is unrealistic, our focus here is to evaluate the effectiveness of the TC model in addressing the information scarcity issue before extending it to more complex scenarios. In the future, we plan to evaluate the efficiency of generating an agreement between agents on sharing references, and the efficiency of using the digital signature to insure the agents' honesty in sharing their information.
- ***Agents do not have any direct history or experience with each other***: the TC model is designed to address the cases where information is not available.
- ***No reputation (witness) information about providers is available for the consumers:*** our primary motivation in this thesis is to provide a way to overcome the consequences of missing the required information when evaluating the agents' trustworthiness. So, we examine the TC model in extreme cases where no information is available in order to verify its efficiency.

4.1.3 Simulation Environment

To evaluate the model described in Section 3.3, we designed an environment that simulates a multi-agent system with all of the relationships and interactions between agents. The environment is populated with 600 agents categorized by two agent types: (1) service consumer agents that are looking for service providers with whom to interact and consume the provided service; and (2) service provider agents that are supposed to provide services (more details about agents in Section 4.1.4). For the sake of clarity, we assume that in the system providers only offer one type of service. The performance of the providers affects the utility gained by the consumers during the interactions. If the provider is truthful with the consumer, the consumer agent gains a positive utility after the interaction; otherwise, it gains a negative utility (a loss). All agents (either service consumers or providers) are located randomly in the environment.

The agents are situated on a continuous 2-dimensional space field. We set the field width and height to 100x100. All agent locations, consumer activity levels (indicating how frequently they use the service), and provider types are assigned randomly as agents are created. Every consumer has the opportunity to choose its partner using either the TC model or the Random model. To ensure a fair comparison between the models, the same number of consumers examines each model.

We rely on random generators to set most of the TC model values. To design the role part, we create a set of seven roles (Senior, Junior, Expert, Friend, Authority, Member of organization, or owned by a known owner). For every role, we assign a different values and degree of belief to reflect the fact that roles are domain-specific. The role-based trust value is calculated by applying Equations 3.1, 3.2 and 3.3 to the

roles' corresponding parameters values: the confidence level (b) and the role value (v_{ro}).

The certified reputation part is set using a random generator to generate the ratings as well as the time when they are received. We then classify providers based on their performance level to reflect the returned utility range, as presented in Table 4.1. Equations 3.4, 3.5, 3.6 and 3.7 are used to calculate the rate-based trust value. The number of roles and ratings for providers is determined randomly and is between 0 and 5.

The simulation consists of a number of runs in which agents are activated, interact with one another, gain utility and build their internal databases with information about other agents in the environment. Each run of the simulation consists of a number of rounds. In each round, every consumer agent is given the opportunity to request a service based on its activity level in that round. At the end of each round, the results of the transactions that occurred are stored and the cycle continues (Section 4.3). Two environments are simulated (typical and dishonest) to compare the results, and each simulated environment is run 10 times in order to calculate the average and obtain more accurate results. More details on the simulated environments and the examined models are presented later in the section.

Provider Type	Utility Range
Perfect	[5, 10]
Average	[0, 5]
Poor	[-10, 0]
Infrequent	[-10, 10]

Table 4.1: Provider agent types

4.1.4 Agent Roles

The simulated MAS environment is populated with two types of agents: service consumers and service providers. Although one agent can play both roles at the same time, we separate them for simplicity. Also for the sake of simplicity, we assume that only one type of service is available in the simulated environment.

4.1.4.1 Consumer Agents

Consumer agents are the agents that use the services provided by the providers. Since the utility that each consumer agent gains from each transaction is determined by the performance of the provider, the main objective of the consumer agent is to select good providers and avoid bad ones. This selection can increase or decrease the consumer's utility gain (UG).

In the simulated environment, the consumer select its partners either by using the TC model or randomly. The selection process using the TC model starts by the consumer contacting the environment to locate nearby interested providers (in our simulation, interested providers were chosen based on the distance between the agents). Then, the consumer evaluates the trustworthiness of all the providers in the list. After that, it selects the provider with the highest trust value and uses its service.

In return, the consumer gains some utility from that provider, based on the provider's performance in that transaction. After the transaction, the consumer rates the provider based on the quality of the service with a trust rating between [-1, 1], and stores the rating in its internal database. Finally, the consumer shares the rating with the provider and the provider may store that rating as a reference for future interactions.

When using the Random method, the agent can choose its partner randomly from the list of interested providers by applying the steps below:

1. The consumer issues a request to the selected provider. In response, it receives an approval from the provider.
2. Upon completion of the transaction, the consumer rates the provider's performance based on the utility gain, and stores the result in its internal database.
3. The consumer informs the provider of its rating.

The consumer agents in the real world wait a certain amount of time between transactions. The frequency of the transactions is known as the activity level of that agent; the more frequent the transactions, the higher the activity level for the service. An agent's activity level ranges between 25% and 100% of the time.

In the simulation, the list of interested providers is set based on their distance from the consumer to simulate that only a subset of the providers are available to serve the consumer. We define the list with respect to the location for two reasons:

First: the resources available to the consumer (in terms of memory, communication cost and time for trust evaluation) are limited. Thus, it cannot evaluate all the providers in the system.

Second: In some applications like VANET, the location is used, as a metric when calculating the trust, relying on the assumption that an agent closed to the event is

likely to report more realistic data about the event [33]. In online marketplaces such as eBay, some vendors can only sell and ship goods to consumers in their countries. Additionally, the distance between the provider and the consumer can affect the service quality.

4.1.4.2 Provider Agents

Provider agents are the agents that provide services in the system to the consumers. The quality of the services (or the provider's performance) varies from one provider to another and is related to the utility that a consumer gains from an interaction with that provider. A poor performance means a low utility value and vice versa. The simulated values of the UG are in the range of [-10, 10].

To model the variety in the quality of the services provided in the real world, we assign one of the following types to each provider: *perfect*, *average*, *poor*, or *infrequent*. Provider agents of type perfect are always willing to provide good services, while providers of type average perform fairly well but not as exceptionally as the perfect providers do. The infrequent types are used to represent providers who perform based on their own personal motivations or the providers whose performance is affected by external factors. Poor, the last type, represents the providers who cheat all of the time. We consider agents of types perfect and average as good providers, and agents of types poor and infrequent as bad providers. The size of the bad provider population is adjusted in different simulations, in order to evaluate the relative performance of the TC model against the Random model.

Based on the assigned type, the provider returns a UG value that is randomly selected from its utility range [-10, 10] as presented in Table 4.1.

Good providers need to show their certificates to prove trustworthiness and attract consumers' attention, while bad providers need to hide their bad ratings in

order to deceive consumers about their behaviors to look like an agent with no history, because the probability of being selected as an agent with no history is much greater than being selected as a bad provider. Thus, not all bad providers show their certificates although the consumers ignore providers without certificates most of the time.

Bad providers may collude with other agents to boost their reputation. But consumers can use digital signature to verify the certificate integrity (Section 3.2). In our simulation, we give trust certificates to some bad providers to simulate the cases where bad agents may hide their ratings and to represent the fact that trust is a subjective measure; where, according to their own standards, consumers may consider an agent as a bad provider while it is recognized as a good one by other consumers. Therefore, we randomly give providers the roles[2] and assign them ratings from the range [-0.1, -1] randomly too.

4.1.5 Experimental Set-up

Before each experiment, the simulator is set up to replicate a particular environment using a set of variables and parameters.

4.1.5.1 Variables

The simulation variables and their values are presented in Table 4.2. Some of the variables will be changed based on the environment of interest; they will be identified later (Section 4.4.2). For example, the provider population includes four types of providers, based on their performance, and to represent a realistic environment we suggest that the provider population consist of 50% good providers (including perfect

2 The role values depend on the consumers' point of view (Section 3.3.1).

and average providers) and 50% bad providers (including poor and infrequent providers). The values will be used in all simulations unless otherwise specified.

Variable	Symbol	Value
Number of simulation runs	R	10
Number of consumer agents	N_c	500
Range of consumer activity level	a	[0.25, 1.00]
Total number of provider agents	N_p	100
Number of perfect providers	N_{pg}	10
Number of average providers	N_{pa}	40
Number of poor providers	N_{pp}	45
Number of infrequent providers	N_{pi}	5

Table 4.2: Simulation variables

4.1.5.2 Parameters

The default parameters of the simulation are presented in Table 4.3. The recency scaling factor is set to give a 100 step old rating half the impact of a new rating. Simulation time steps are used as the time value for the ratings. We set the minimum and maximum numbers of both roles and ratings that a provider agent can have to 0 and 5, respectively. We also set the weight coefficients w_k to reflect the importance of each component. We give direct-experience trust a higher weight than others because it is based on the agent's own evidence and is therefore more reliable. We start with 0.5 for both the rate and role-based trusts; and with 0 for the direct-experience trust. The values then change as the consumer gains more experience, up to a maximum of 1 for the direct-experience, as this indicates total trust in the direct

experience reliability factor. Finally, the satisfactory UG value is determined as the value that is greater than or equal to zero.

Parameters	Symbol	Value
Recencey Scaling Factor	λ	$-(100/\ln(0.5))$
Minimum number of roles	RO_{min}	0
Maximum number of roles	RO_{max}	5
Minimum number of ratings	RA_{min}	0
Maximum number of ratings	RA_{max}	5
Positive increment factor	α	0.1
Negative decrement factor	β	-0.2
Role-based coefficient (initial)	w_{Role}	0.5
Rate-based coefficient (initial)	w_{Rate}	0.5
Direct-experience-based coefficient (initial)	w_{Direct}	0.0
Satisfactory UG value	satUG	>= 0

Table 4.3: TC model default parameters

4.1.5.3 Evaluation Metrics

Considering our primary goal, which is to evaluate the effectiveness of using the TC model to select reliable service providers and to help new agents, three evaluation metrics are used for the comparisons:

1. ***Number of Good Interactions:*** Selecting a reliable provider results in a good interaction for the consumer. For each interaction, the result is recorded and the percentage of good interactions is calculated. This metric is applied to both the TC model and the Random model. We define good interactions as the

interactions where the consumers yield UGs that are greater than or equal to zero.

2. ***Average Utility Gain:*** We use the UG value as a measurement for the performance of each model in selecting reliable providers that give high UG to consumers, in every interaction. The UG of each consumer is recorded after each interaction, and the average is taken for all consumers that use the same model.
3. ***Percentage of Selected Providers with TC:*** This metric is used to evaluate how new providers are taking advantage of using the TC model to gain consumers' trust, in comparison to providers without trust certificate and providers who already have a history with the consumers.

4.2 Test Models

The purpose of designing the simulation is to evaluate the validity of using the TC model to select the most reliable provider and maximize the consumer's UG, when evidence is not available. Our focus is on assessing the efficiency of the TC model as a solution for data scarcity problem and as an addition to enhance the existing trust and reputation systems. For that reason, we test it in an isolation from other models and compare it to the Random model, where agents choose their partners randomly. An equal number of consumers are using each model when looking for providers. The outcomes of employing the TC model and the Random model are recorded and then examined in different test scenarios/environments, for comparison purposes. We also conduct an experiment to evaluate the efficiency of using the TC model to assist new providers in engaging in transactions with consumers.

In the TC model, the provider selection process starts when the consumer contacts the environment to locate interested nearby providers and then evaluates the trustworthiness of these providers by using the TC approach, as described in Section 3.3. Subsequently, the consumer selects the provider with the highest trust value, based on the claim that the provider that has the highest trust value is expected to return the highest UG. We implemented the TC model using the parameters as shown in Tables 4.3.

In the Random model, the consumer contacts the environment to locate interested nearby providers, as in the TC model, and then selects its partner randomly from that list.

After completing the transaction with the selected provider, the consumer gained some utility. Based on the consumer's level of satisfaction, it converts this utility value to a trust rating and then updates its internal database using Equations 3.8 and 3.9. After that, the consumer shares the computed trust value with the provider, in order to build the CR part of the Trust Certificates of that provider.

4.3 Simulation Operation

In each experiment, the environment is populated with a set of consumers and providers, while maintaining the proportion of agents specified by the simulation parameters. All agent locations, consumer activity level, and providers types are assigned randomly as agents are created. Every consumer has the opportunity to choose its partner using either the TC model or the Random model. To ensure a fair comparison between the models, the same number of consumers examines each model. We use the UG and the number of good interactions as measurements for the performance of each model in selecting reliable providers for interaction.

For each experiment, the simulator executes ten runs. Every run then executes five rounds. In each round, every consumer is given the chance to interact with the system, and the UG that results from any transaction is recorded for analysis and comparison. At the start of the run, consumers change their location to be able to examine a new set of providers.

In the following section, we present the implementation process and describe the results of different experiments for both consumers and providers.

4.4 Experiments and Results

After presenting the simulation environments and operations, we now present the experiments and their results. Our intention is to examine the TC model's ability to: (1) select reliable service providers; (2) reduce the risk caused by the lack of information and experiences; (3) maximize the utility gain of service consumers; and (4) benefit new providers as they merge into the system. In order to study all of these abilities, we conduct different experiments for the consumers and the providers.

4.4.1 Experiments for Consumers

In this experiments, we evaluate the contribution of the TC model in selecting reliable service providers using two environments. The two environments are each investigated in a separate experiment, as follows.

1. ***Typical Environment:*** examines the performance of the consumers when the proportion of good to bad providers is balanced (intended to simulate our real world).
2. ***Dishonest Environment:*** assesses the performance of the consumers when dishonest providers are heavily populated in the environment.

The behaviors of consumers implementing the test models in the two environments are recorded. In each of the two environments, the results obtained are presented and examined from two points of view: the percentage of all transactions in which good providers were selected and the average UG over all transactions. Then, the results are presented in graphs with an x-axis that plots the number of runs and a y-axis that either plots the average UG or the percentage of good interactions.

4.4.1.1 Typical Environment

In this experiment, we show how consumers behave in a typical (realistic) environment, where approximately half of the providers are good and the other half is bad. The specific set-up used in this environment is the same as in Tables 4.2 and 4.3.

Initially, we compare the percentage of good interactions to test whether the TC model helps consumers select good providers and avoid bad ones. From Figure 4.1, we can see that the TC model outperforms the Random model in the number of good interactions. Consumers using the TC model choose good providers 100% of the time. On the other hand, in the Random model, the consumers only obtained good interactions 60% of the time. The possible reason for this result is the trust sources that the TC model provides to the consumer enable the consumer to incorporate those sources to predict the future behavior of the potential providers and calculate the trust value.

Considering that the consumers using the TC model select good providers more consistently, they are expected to acquire higher utility than the consumers using the Random model. This is confirmed in Figure 4.2, where it is noticeable that TC model consumers yield higher UG than Random model consumers, all of the time, by more than 4 UG units. The TC model provides higher utility than the Random model by selecting good providers more often.

In Figure 4.2, we notice some fluctuates in the average UG values over the number of runs. That is because consumers are changing their locations at the start of each run. The location change means the consumer face a new group of providers to choose from and because providers are situated randomly around the environment, there is no guarantee about their service quality.

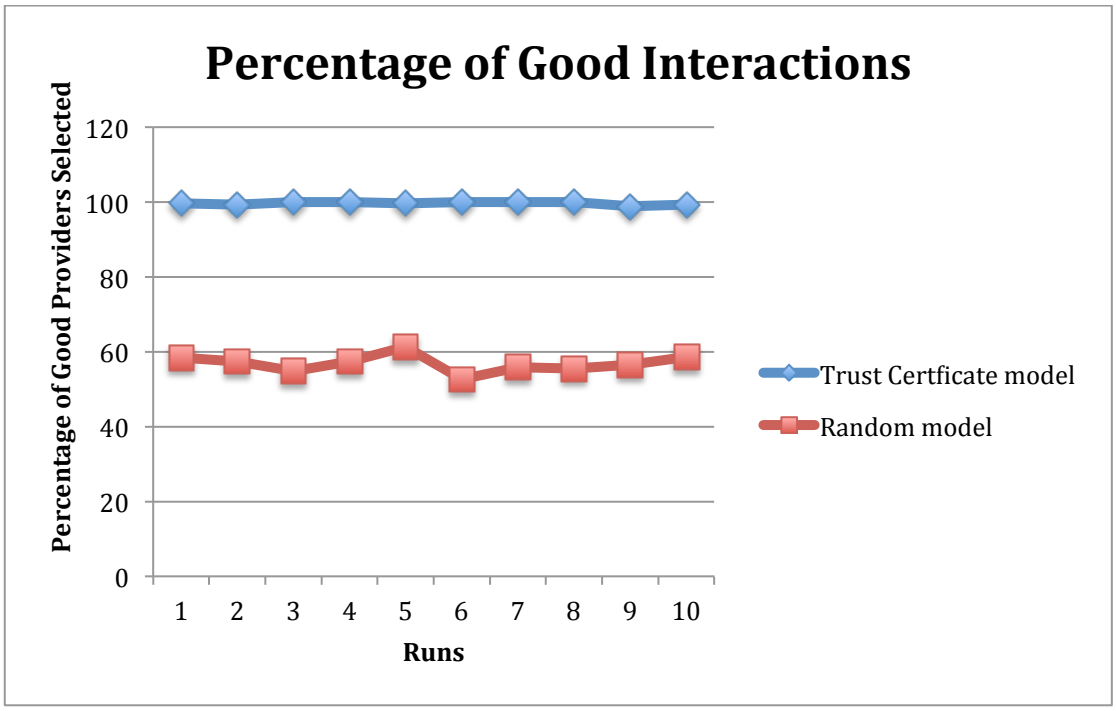

Figure 4.1: Percentage of good interactions in typical environment

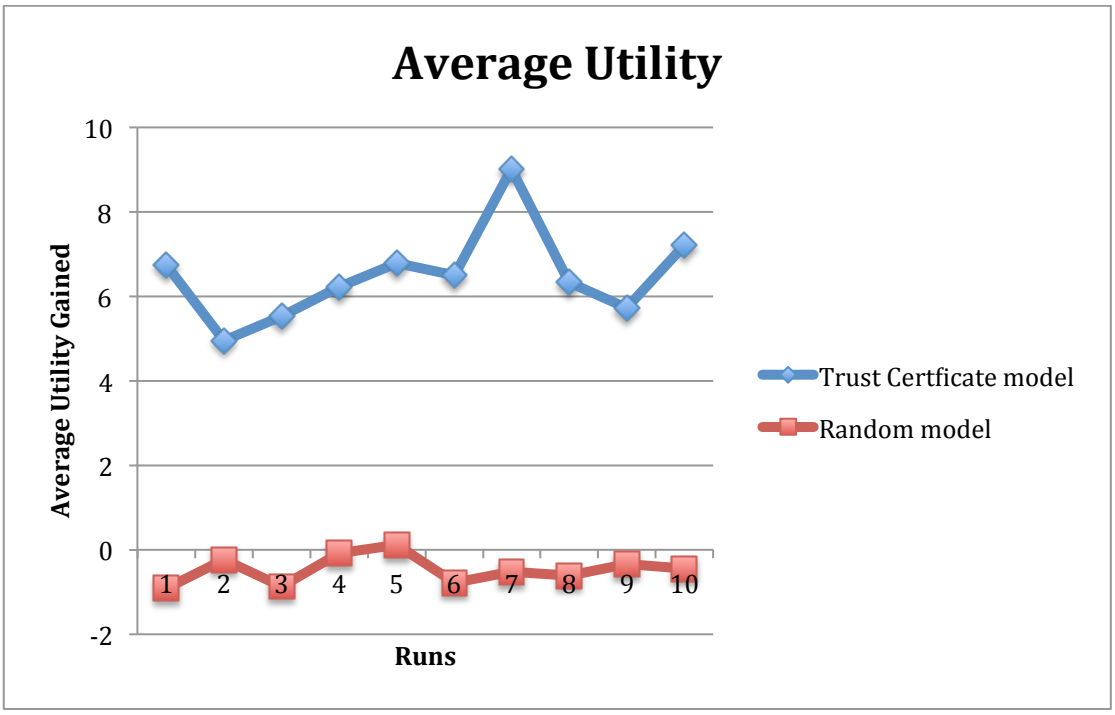

Figure 4.2: Average utility gain for all transactions in typical environment

4.4.1.2 Dishonest Environment

Having shown the TC model performance in a typical environment, we now present how the TC model performs in a dishonest environment that is heavily populated with bad (dishonest) providers. The suggested environment is populated with only 20% good providers; the remaining 80% are bad providers. Then, we re-ran the same experiment as in a typical environment, but with the new provider population distribution, as indicated in Table 4.4. The remaining variables and parameters are kept the same.

Our objective is to help consumers to assess, with some certainty, the provider's ability in providing a good quality service. This mission becomes increasingly difficult as the ratio of bad providers to good providers rises in the system. Thus, we need to test our proposed model efficiency in a critical environment where bad providers are dominating the system.

To prove the applicability of the TC model, we compare its percentage of good interactions and average UG with those obtained from the Random model.

Provider Type	Number
Perfect	5
Average	15
Poor	75
Infrequent	5

Table 4.4: Providers distribution for dishonest environment

Although the number of dishonest providers increases, the performance of the TC model continues to noticeably outperform the Random model.

In this experiment, the TC model shows robust results against bad providers (Figure 4.3). Consumers in the TC model still chose good providers almost 100% of the time; however, the percentage of good interactions in the Random model deteriorated significantly and could not exceed 35%.

Unlike the typical environment, consumers using the TC model, in dishonest environment fail to select good providers in a few interactions. That is because the environment is dominated by bad providers, so consumers sometimes find themselves comparing between bad providers only to select the less harmful provider.

In addition, by comparing the average UG, we notice that the consumers employing the TC model obtain higher UG values than their random counterparts, which means that the TC model performed better than the Random model, even when the environment is filled with bad providers.

From Figure 4.4, it can be seen that the increase in bad providers does affect the consumers who choose partners randomly.

As shown in the previous two experiments, the performance of the TC model is not steady. The results are affected because consumers are changing their location after each run, and the nearest providers have different profiles.

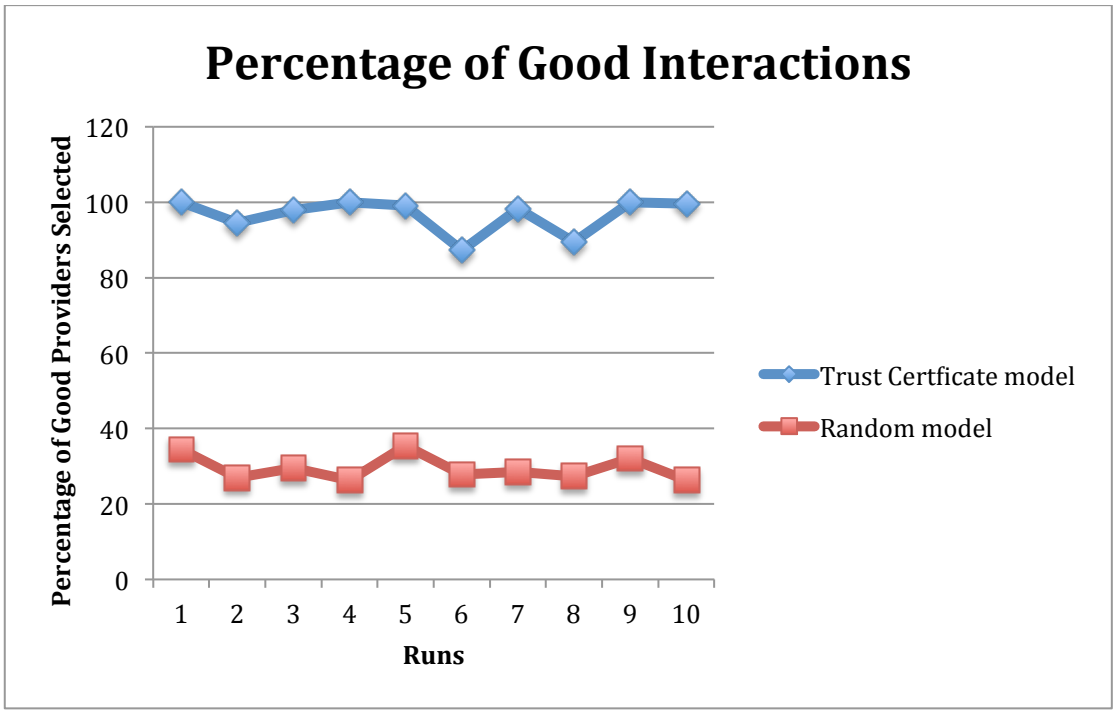

Figure 4.3: Percentage of good interactions in dishonest environment

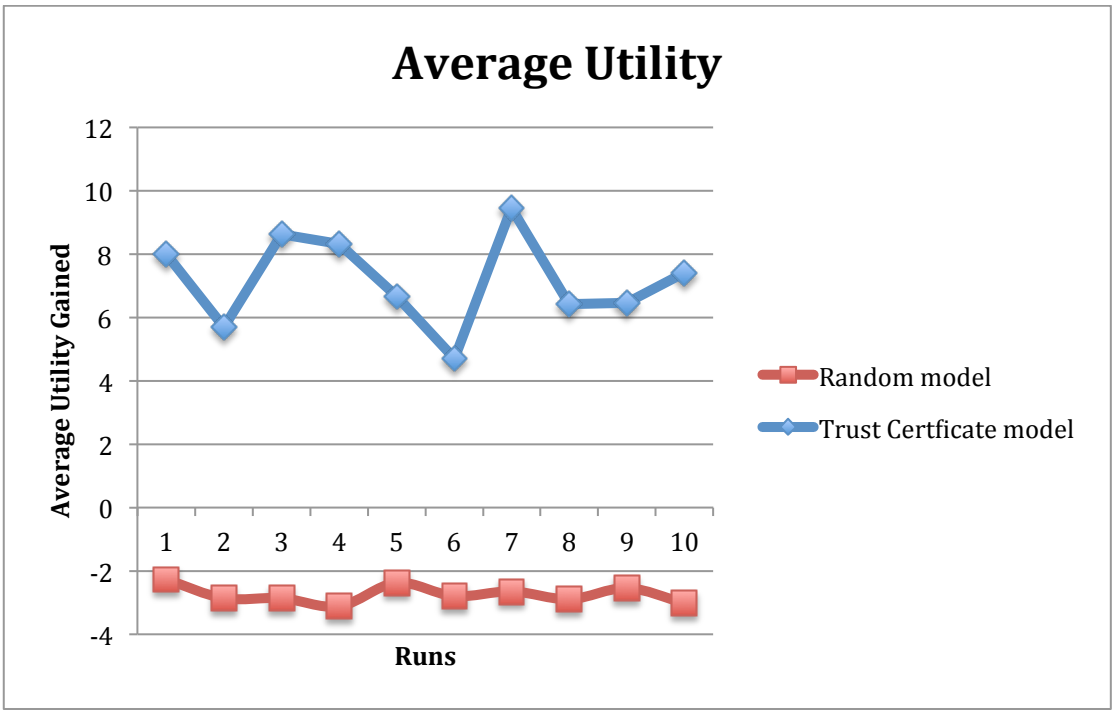

Figure 4.4: Average utility gain for all transactions in dishonest environment

Overall, consumers equipped with the TC model outperforms the consumers using the Random model in terms of an increase in the percentage of good providers selected, and a maximization of the average UG from the interactions. The results obtained through the previous two experiments demonstrate that the proposed approach of using the TC model solves the problem of the lack of direct history and experience, even in cases where the majority of provider agents in the system are bad.

4.4.2 Experiments for Providers

New providers, who are unknown to consumers, may be excluded from interactions due to consumers' hesitation to start any connection with them. We argued that, the TC model facilitates the new providers engagement in interactions. In order to confirm that argument, we conducted two experiments: one to evaluate how providers can get selected in new systems and one in active systems. The number of selected

providers in every experiment is recorded and presented in graphs to show the percentage of selected new providers in every run.

4.4.2.1 Providers in New Systems

To show how the TC model facilitates new providers in the promotion of their trustworthiness in new systems in which agents does not have any experience with each other, we re-ran the simulator using similar settings to that of the typical environment (Tables 4.2 and 4.3). The only difference here is that half of the providers have Trust Certificates and the other half does not. We ran the experiment for 10 runs with 100 interactions in every run. After every run, the number of selected providers who have certificate was recorded and the results are presented in (Figure 4.5). These results show that consumers chose providers with Trust Certificate between 93% and 98% of the time. In opposite, the providers without Trust Certificate were chosen 6% at the most.

The service consumer evaluates every provider in the list to calculate its trust value, and then selects the provider with the highest value. If the provider does not have a Trust Certificate, then the consumer assigns zero as the provider's trust value, which means neutral. As a result, that provider will be excluded from the interaction since other agents receive higher values. Providers without a certificate can be chosen under one condition: when other provider's expected trust value is less than zero, since zero is the highest value in this case.

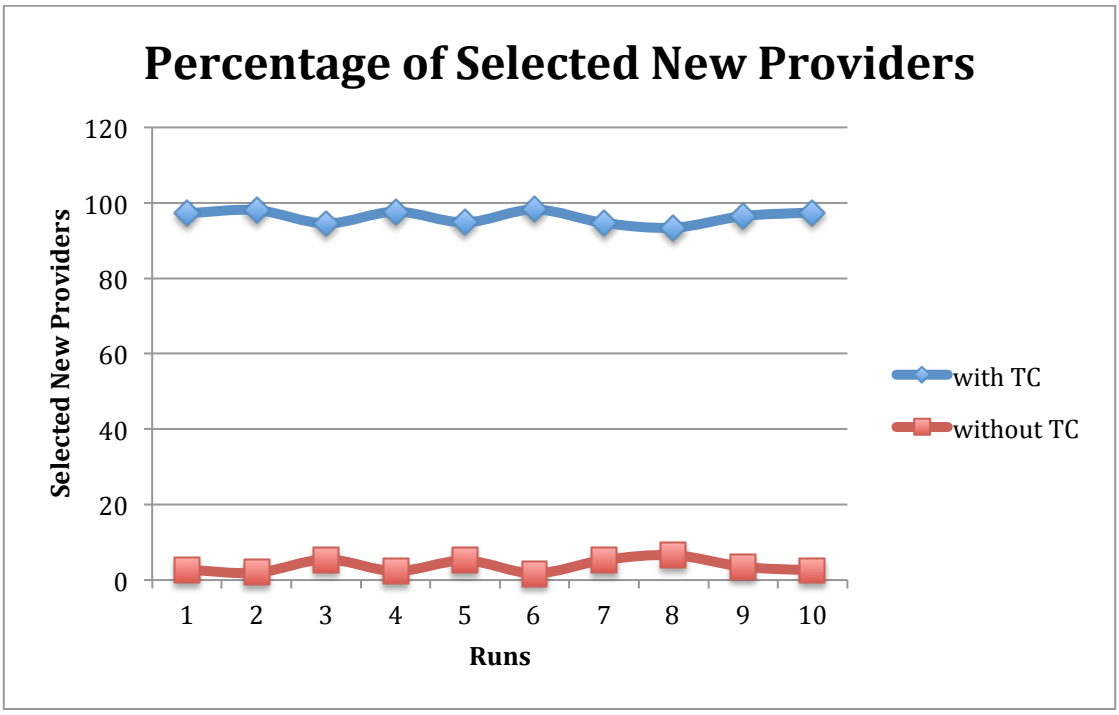

Figure 4.5: Percentage of selected providers in new systems

4.4.2.2 Providers in Active Systems

To show how new providers can still get selected after the consumers have learned about the system, we re-ran the simulator using similar settings to that of the typical environment (Tables 4.2 and 4.3). The experiment was run for 1000 interactions; 500 interaction initially to give every consumer a number of chances to interact with the system and learn who are good and bad providers. After the first 500 interactions, new providers were added and placed randomly into the system. The new added providers characteristics were set randomly as well. The experiment continued to run for another 500 interactions and calculated the percentage of those new providers that got selected by the consumers. Then, the above experiment was repeated 10 times and every time the same number of new providers (as before) was generated. We recorded the number of new providers that got selected at the end of every experiment and presented the results in graphs. We conducted the same experiment twice: one for good new providers and one for bad new providers.

- **New Good Providers**

In this section, we evaluate the TC model contribution toward the new providers engagement in the system. Our goal in this experiment is to answer the question: Does the TC model help new provider agents to be selected by consumers for interaction? We did the experiment, mentioned above, by adding new providers of types "perfect" and "average" to the system. The experiment is conducted using two different percentages (10% and 20%) of new provider agents to support the result by numerous evidences.

From Figures 4.6 and 4.7, it is observed that the new added providers are still get selected although the consumers have knowledge about the already existed providers and can distinguish between good and bad providers in the system.

By further examining the results presented in Figure 4.6, we notice that new added providers were selected 35% of the time. In some cases, new providers were only selected 10% of the time. The possible explanation for the variation in percentages is that, in some runs, the existing providers returned higher trust values than the new ones. However, the new providers can still benefit from the TC model to increase their probability in being selected for interactions in despite the fact that consumers have their own set of acquaintances.

Figure 4.7 illustrates the same findings as has been observed in the previous experiment. This confirms our intuition about the TC model beneficial to new providers.

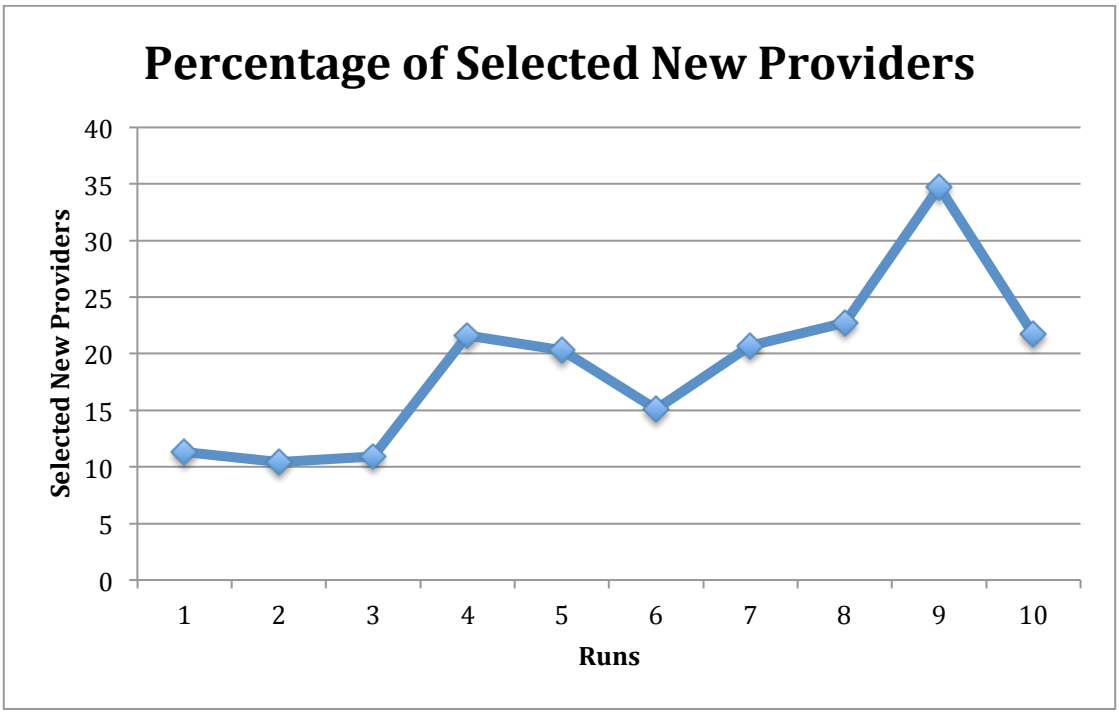

Figure 4.6: Percentage of selected providers with 10% new good providers

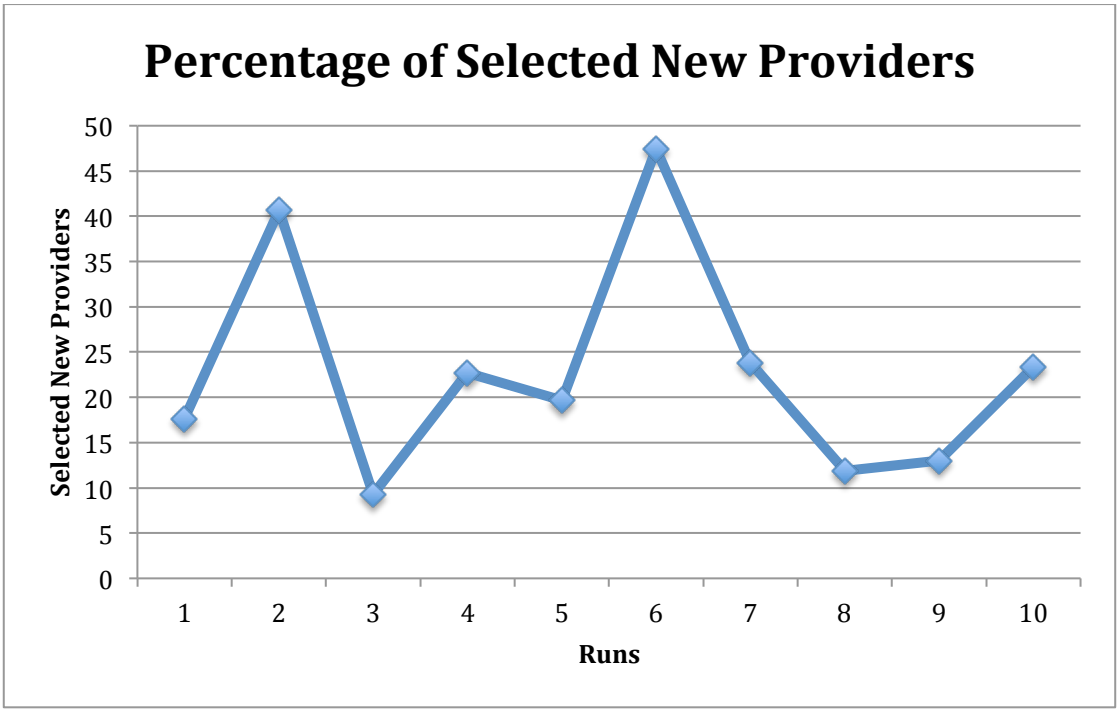

Figure 4.7: Percentage of selected providers with 20% new good providers

- **New Bad Providers**

The objective of this experiment is to evaluate how the TC model performs when new bad providers are added to the system. We re-ran the same experiment of new good providers but we added bad providers instead of the good providers.

In reviewing the results obtained from the experiment (presented in Figures 4.8 and 4.9), we can see that the consumers were learning about their environment and became very effective in detecting bad providers. Bad providers still could be selected but with very low probability. The only case bad provider can be selected is when the service consumer evaluates every provider in the list to calculate their trust value, and the bad provider has the highest value. For example, providers without a certificate can be chosen when other provider's expected trust value is less than zero, since zero is the highest value in this case. As we mentioned before, bad providers may hide their bad ratings to deceive the consumers.

Overall, the results obtained through this experiment demonstrate that the proposed TC model does not serve the bad providers intension to cheat, but does help new consumers to learn about their environment and avoid bad providers.

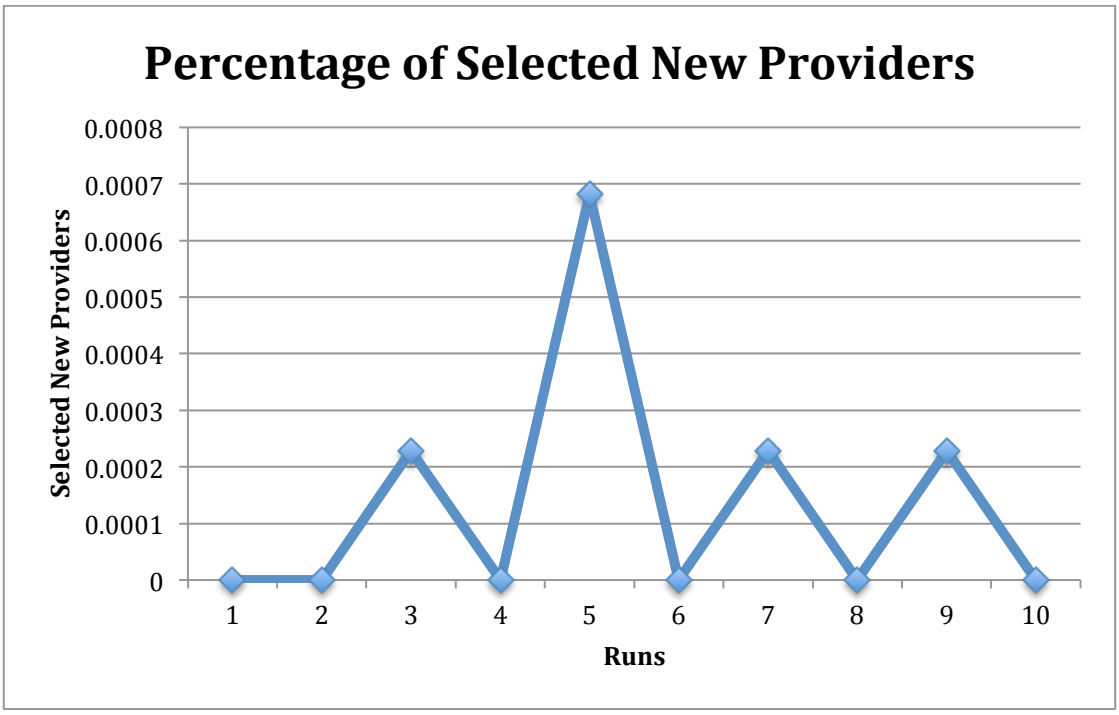

Figure 4.8: Percentage of selected providers with 10% new bad providers

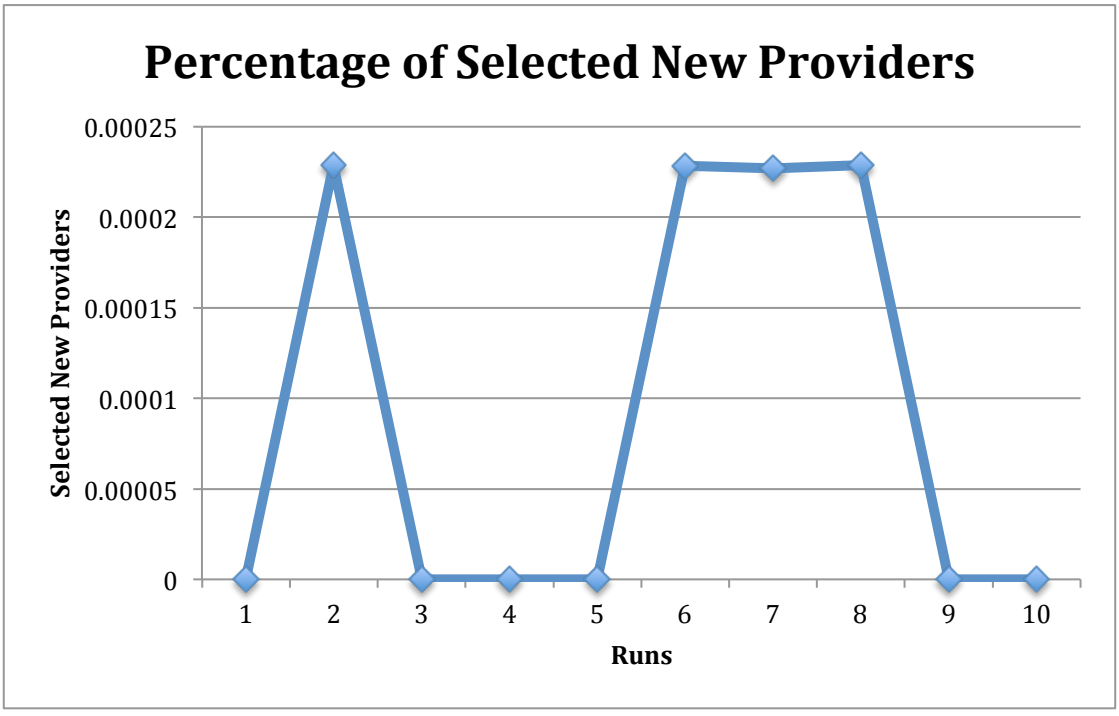

Figure 4.9: Percentage of selected providers with 20% new bad providers

In sum, through the experiments we ran above, it is confirmed that the TC model is beneficial to new providers in being selected for interactions and it is also beneficial to consumers in selecting reliable providers at the same time.

4.5 Summary

In this chapter, we evaluated the efficiency of the TC model using an empirical evaluation. We performed the evaluation separately from other models and parameters to produce as accurate results as possible. We also used the Random model as the benchmark for the comparison. Our results show that employing the TC model greatly improves the selection of reliable service providers, maximizes the utility gain of service consumers, and helps new providers.

To evaluate the proposed model in a more realistic mode, we have designed a simulation environment with a simple Agent Based system so that the benefits of the TC model can be judged with practical metrics.

Reviewing the results of the simulation shows that using the TC model addresses the problem of lack of evidence when building trust, and provides an alternative to the random selection of providers. It also shows the TC model's efficiency in selecting reliable service providers most of the time, and its ability to maximize the utility gain of service consumers. That efficiency demonstrates the TC model's ability of reducing the risk resulting from the lack of information and experiences. It also proves its ability to maximize the utility gain of service consumers.

The results also confirm the TC model's ability in facilitating the new providers in the promotion of their trustworthiness.

Chapter 5: Discussion

While reviewing many trust and reputation models during our research, we noticed some issues related to the evaluation of trust in situations where both direct history and reputation information are not accessible. The lack of such essential information increases the risk of trust evaluations when interacting with new, unknown agents. The reviewed models failed to provide support for new agents and to minimize the associated risk level. In this thesis, we address this problem by introducing the Trust Certificate (TC) model. We evaluate it through experimental analysis in the context of an agent-based simulation, in order to show its added value.

The results presented in the thesis demonstrate that the use of the TC model could help new agents and offer significant advantages in several areas of reputation modeling. In the following subsections, we present four areas that are satisfied by the use of our proposed model.

5.1 Select Reliable Service Providers

The underlying purpose of designing trust and reputation models, and evaluating agents' trustworthiness, is to help consumer agents select appropriate partners. New agents without experience in the system are extremely exposed and may choose unreliable, untrustworthy agents because of their lack of important experience. The

TC model benefits consumer agents, helping them choose reliable providers, as evidenced by its performance in comparison to the Random model.

Our experimental results show that the consumers using the TC model perform significantly better, over all transactions, in terms of choosing reliable providers. In all two environments, the TC model performed substantially better than the Random model, as presented in Section 4.4.1 The results obtained illustrate that consumers who use the TC model more consistently select good providers than those using the Random model. This is true even in environments where the majority of providers are bad.

The dishonest environments (Section 4.4.1.2) specifically examine the impact of using the TC model when the large majority of providers in the system are bad. Even in such an environment, the results show that the TC model outperforms the Random model.

5.2 Reduce the Risk Caused by Lack of Information and Experience

To evaluate the trustworthiness, most reputation models rely heavily on prior interactions between agents, either direct experience or through other agents in the society. For new agents in the system, this practice significantly increases the risk of engaging in bad transactions because of their lack of the required experience. The TC model overcomes this weakness by allowing agents to actively collect and provide the required data about their roles and previous performances to build the trust of their potential partners.

The efficiency of the TC model in reducing the risk to new agents is demonstrated by the results obtained from the experiments in Section 4.4.1. The

results of the experiments show that the TC model succeeded in ensuring a high percentage of good and successful interactions for the consumers. This means that the TC model succeeded in minimizing the risk of encountering dishonest providers when mandatory information was missing.

5.3 Maximize the Utility Gain for Consumers

Rational consumers need to rely on other agents to maximize their utilities. Subsequently, the performance of the provider affects the UG of the consumer; therefore, the consumer needs to measure the provider's trustworthiness, before any transaction, in order to ensure high performance and to maximize its utilities.

The performance of consumers who implement the TC model has been evaluated through the two environments presented in Section 4.4.1. The results show that users of the TC model achieved high UG in all transactions, even in cases where the number of bad providers is high.

This indicates that the TC model provides a suitable tool for consumers to make conscious decisions about which provider to choose in order to fulfill their goals and maximize their UGs. That contributes to an increase in performance for consumer agents that have neither prior experience nor information on the reputation of the providers in the system.

5.4 Benefit New Providers in the System

When a new provider enters the system, consumers may forego interactions with this provider as a precaution. This situation leaves the new provider with two options: either to sit and wait for a consumer to take a chance and select it randomly, or to use

the TC model to provide references about its roles and past behavior, and increase its possibilities of being selected for transactions.

The benefit to the providers of using the TC model is discussed in Section 4.4.2. The outcomes presented show promising results for the users of the TC model, as it helps new providers be selected by consumers.

Although the consumers already built their database and have their providers, new providers can have the chance of being selected by consumers when using the TC model.

5.5 Summary

In Chapter 2, we reviewed a number of trust approaches dealing with the issues of trust evaluation in cases where direct and indirect evidence are not available. We outlined the limitations of these approaches in dealing with those issues. In order to address these issues, we present our model, the Trust Certificate model, which promises to help agents overcome the limitations of information scarcity.

The proposed model promises to assist service consumers in the selection of reliable service providers, in order to maximize their UG. In addition to that, it also promises to reduce the risk of missing the required information when evaluating the trust. The promises of the proposed model are not only for the consumers but also for the service providers. The TC model considers boosting the new providers' reputations by helping them be chosen for interactions.

All of the above contributions offered by the TC model have been validated using experimental analysis, as discussed and presented in Chapter 4.

Chapter 6: Conclusions and Future Work

In this chapter, we summarize our approach and its ability to overcome the challenge of evaluating trust during a period of information dearth. In order to achieve that, we develop a trust model that enables agents to actively provide evidence about their trustworthiness to their perspective partners in order to participate in system interactions.

We also discuss the main contributions of the thesis and its limitations, and the possibilities for future work.

6.1 Conclusions

This thesis was created to address two challenges: 1) choosing partners randomly when agents find themselves dealing with complete strangers whom neither they nor their friends have encountered before, and 2) excluding newcomers from competition due to their lack of essential experience.

The TC model introduces the idea of equipping every agent in the system with a certificate. The certificate provides information about its holder and work as a reference about its trustworthiness by enabling the agent to collect and store its own reputation information and share it with others. Other agents in the system use the certificate to evaluate the trust value of their potential partners. The trust evaluation process integrates three trust metrics to closely predict the behavior of the future

partner and consequently choose a reliable one: role-based, rate-based and direct-experience-based trust. Every metric has its own parameters for example, the role-based trust value includes the degree of belief in the roles, and the confidence placed in the provider based on the roles number. The rate-based trust value incorporates the gap between the rating time and the evaluation time, and the confidence placed in the provider based on the number of ratings. The direct-experience-based trust value helps the agents learning about their environment and building their database for future interactions.

We believe the work done in the thesis, as well as its contributions, have resulted in a positive solution to the challenges. It also helps in reducing the cost for consumers, in terms of time and resources, as all the information is stored and provided by the providers. In addition, it assists new providers build their reputation faster.

In empirical evaluations, our model performed well compared to the Random model, specifically in enabling consumers to choose reliable providers and maximize their utility gain, reducing the risk resulting from the missing required information, and finally, helping new providers cope with their situation.

One limit is that the TC model cannot detect if agents collude to increase the number of their roles and ratings in order to increase their confidence level.

6.2 Future Work

We conclude our thesis by discussing some potential areas for future research, in order to expand and improve the model.

First, the performance of the TC model can be improved by integrating a learning technique to automatically adjust the parameters that determine the minimum

and maximum numbers of roles and ratings for every provider, as it is used to define the confidence in those providers. These modifications depend on the rating times and the importance of the tasks. For example, if the consumer defines a limited period of time to accept ratings, the maximum number of allowed ratings decreases. Also, if the task is very important to the consumer, the minimum and the maximum number of allowed ratings increase.

The next potential extension is to add a reliability measure for the raters and referees that provide the reports to the certificate. In the TC model, we assume that agents report their information trustfully, which is not suitable to the nature of agents. In order to avoid this assumption, we aim to have a reliability measure to evaluate the confidence that should be had in the third-party reporters, and use that measure as a factor in estimating the trust value. This addition will improve the TC model in two ways: 1) filter inaccurate reports; 2) boost the consumer's experience by including the ratings of the reporters. We can also promote the reporter's evaluation as an incentive for the agents to share their knowledge with others.

We also plan to expand our experiment evaluation by:

1. Examining the effectiveness of the application of the TC model compared to other reputation systems. The TC model can be used as an extension to improve existing models, especially in cold-start and newcomer cases.
2. Conducting more advance experiments to assess the effects of using the TC model to help new providers. We need to evaluate how new providers can survive in environments where agents already have their acquaintances and may not be welling to explore.

3. Generating an agreement between agents on sharing references, then evaluate the efficiency of it, and the efficiency of using the digital signature to insure the agents' honesty in sharing their information.

References

[1] (2014, May 15). *MASON Multiagent Simulation Toolkit. [Online]. HYPERLINK "http://cs.gmu.edu/~eclab/projects/mason/".*

[2] (2014, September 8). *Secured Signing. [Online]. HYPERLINK "http://www.securedsigning.com".*

[3] Abdul-Rahman and S. Hailes, "Supporting trust in virtual communities," *In System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference IEEE,* vol. 6, 2000.

[4] D. Artz and Y. Gil, "A survey of trust in computer science and the semantic web," *Web Semantics: Science, Services and Agents on the World Wide Web,* vol. 5, pp. 58-71, 2007.

[5] K. S. Barber and J. Kim, "Soft security: Isolating unreliable agents," *In Proceedings of the AAMAS 2002 Workshop on Deception, Fraud and Trust in Agent Societies, Bologna, Italy,* pp. 8-17, 2002.

[6] C. Burnett, "*Trust Assessment and Decision-Making in Dynamic Multi-Agent Systems*," *Doctoral Dissertation, University of Aberdeen,* 2011.

[7] C. Burnett, T. J. Norman and K. Sycara, "Trust decision-making in multi-agent systems," *In Proceedings of the Twenty-Second International Joint Conference on Artificial Intelligence AAAI Press,* vol. 1, pp. 115-120, 2011.

[8] C. Burnett, T. J. Norman and K. Sycara, "Bootstrapping trust evaluations through stereotypes," *In Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems,* vol. 1, pp. 241-248, 2010.

[9] C. Cormier, "Seniority as a Metric in Reputation Systems for E-Commerce," *Master's Dissertation, University of Ottawa,* 2011.

[10] J. Dunn, "The concept of trust in the politics of john locke," in *Philosophy in History: Essays on the Historiography of Philosophy*, R. Rorty, J. B. Schneewind and Q. Skinner, Eds. Cambridge: Cambridge University Press, 1984, pp. 279-301.

[11] D. Gambetta, "Can we trust trust," *Trust: Making and Breaking Cooperative Relations Electronic Edition, Department of Sociology, University of Oxford, Chapter 13,* pp. 213-237, 2000.

[12] Gupta, Y. A. Tung and J. R. Marsden, "Digital signature: use and modification to achieve success in next generational e-business processes," *Information & Management,* vol. 41, pp. 561-575, 2004.

[13] W. Hang, Y. Wang and M. and Singh, "Operators for propagating trust and their evaluation in social networks," *In Proceedings of the 8th International Conference on Autonomous Agents and Multiagent Systems,* vol. 2, pp. 1025-1032, 2009.

[14] R. Hermoso, H. Billhardt and S. Ossowski, "Role evolution in open multi-agent systems as an information source for trust," *In Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems,* vol. 1, pp. 217-224, 2010.

[15] A. Herzberg, Y. Mass, J. Michaeli, D. Naor and Y. Ravid, "Access control meets public key infrastructure, or: Assigning roles to strangers," *In*

Proceedings of Security and Privacy, 2000 IEEE Symposium on, pp. 2-14, 2000.

[16] T. D. Huynh, "*Trust and reputation in open multi-agent systems*," *Doctoral Dissertation, University of Southampton,* 2006.

[17] T. D. Huynh, N. R. Jennings and N. R. and Shadbolt, "An integrated trust and reputation model for open multi-agent systems," *Autonomous Agents and Multi-Agent Systems,* vol. 13, pp. 119-154, 2006.

[18] T. D. Huynh, N. R. Jennings and N. R. Shadbolt, "Certified reputation: how an agent can trust a stranger," *In Proceedings of the Fifth International Joint Conference on Autonomous Agents and Multiagent Systems,* pp. 1217-1224, 2006.

[19] N. R. Jennings, "An agent-based approach for building complex software systems," *Communications of the ACM,* vol. 44, pp. 35-41, 2001.

[20] R. Jurca and B. Faltings, "An incentive compatible reputation mechanism," *In Proceedings of the IEEE Conference on E-Commerce CEC03,* pp. 285-292, 2003.

[21] S. N. L. C. Keung and N. Griffiths, "Towards improved partner selection using recommendations and trust," *In Trust in Agent Societies. Springer Berlin Heidelberg,* pp. 43-64, 2008.

[22] B. Khosravifar, "*Trust and Reputation in Multi-Agent Systems*," *Doctoral Dissertation, Concordia University,* 2012.

[23] G. Liu, Y. Wang and M. A. Orgun, "Trust Transitivity in Complex Social Networks," *In AAAI,* vol. 11, pp. 1222-1229, 2011.

[24] S. Liu, H. Yu, C. Miao and A. C. Kot, "A fuzzy logic based reputation model against unfair ratings," *In Proceedings of the 2013 International*

Conference on Autonomous Agents and Multi-Agent Systems, International Foundation for Autonomous Agents and Multiagent Systems, pp. 821-828, 2013.

[25] X. Liu, A. Datta and K. and Rzadca, "Trust beyond reputation: A computational trust model based on stereotypes," *Electronic Commerce Research and Applications,* vol. 12, pp. 24-39, 2013.

[26] G. Lu, J. Lu, S. Yao and Y. J. and Yip, "A review on computational trust models for multi-agent systems," *The Open Information Science Journal,* vol. 2, pp. 18-25, 2009.

[27] S. Luke, "Multiagent Simulation And the MASON Library, Manual Version 17," *Department of Computer Science George Mason University,* 2013.

[28] F. G. Mármol and G. M. Pérez, "Trust and reputation models comparison ," *Internet Research,* vol. 21, pp. 138-153, 2011.

[29] S. P. Marsh, "Formalising trust as a computational concept," *Doctoral Dissertation, University of Stirling,* 1994.

[30] Y. Mass and O. Shehory, "Distributed trust in open multi-agent systems," *In Trust in Cyber-Societies. Springer Berlin Heidelberg,* pp. 159-174, 2001.

[31] E. M. Maximilien and M. P. Singh, "Reputation and endorsement for web services," *ACM SIGecom Exchanges,* vol. 3, pp. 24-31, 2001.

[32] M. Mccallum, W. W. Vasconcelos and T. J. Norman, "Organisational change through influence," *Autonomous Agents and Multi-Agent Systems,* vol. 17, pp. 157-189, 2008.

[33] U. F. Minhas, J. Zhang, T. Tran and R. Cohen, "Promoting effective exchanges between vehicular agents in traffic through transportation oriented trust modeling," *In Proceedings of the International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS) Workshop on Agents in Traffic and Transportation,* 2010.

[34] L. Mui, "*Computational models of trust and reputation: Agents, evolutionary games, and social networks*," *Doctoral Dissertation, Massachusetts Institute of Technology,* 2002.

[35] B. C. Ooi, C. Y. Liau and K. L. Tan, "Managing trust in peer-to-peer systems using reputation-based techniques," *In Advances in Web-Age Information Management. Springer Berlin Heidelberg,* pp. 2-12, 2003.

[36] S. D. Ramchurn, D. Huynh and N. R. Jennings, "Trust in multi-agent systems," *The Knowledge Engineering Review,* vol. 19, pp. 1-25, 2004.

[37] J. Sabater, "*Trust and Reputation for Agent Societies,*" Bellaterra, Catalonia, Spain: Monografies de l'Institut d'Investigació en Intel· ligencia Artificial, 20, 2003.

[38] J. Sabater and C. Sierra, "Reputation and social network analysis in multi-agent systems," *In Proceedings of the First International Joint Conference on Autonomous Agents and Multi-Agent Systems (AAMAS),* pp. 475-482, 2002.

[39] J. Sabater and C. Sierra, "Regret: A reputation model for gregarious societies," *In Fourth Workshop on Deception Fraud and Trust in Agent Societies,* vol. 70, 2001.

[40] J. Sabater and C. Sierra, "Social ReGreT, a reputation model based on social relations," *ACM SIGecom Exchanges,* vol. 3, pp. 44-56, 2001.

[41] S. Sen, "A comprehensive approach to trust management," *In Proceedings of the 2013 International Conference on Autonomous Agents and Multi-Agent Systems. International Foundation for Autonomous Agents and Multiagent Systems,* pp. 797-800, 2013.

[42] D. Shin and G. J. Ahn, "Role-based privilege and trust management," *Computer Systems Science and Engineering,* vol. 20, pp. 401, 2005.

[43] K. Sycara, "Multiagent Systems," *AI Magazine,* vol. 10, pp. 79-93, 1998.

[44] W. L. Teacy, J. Patel, Jennings N. R. and M. Luck, "TRAVOS: Trust and reputation in the context of inaccurate information sources." *Autonomous Agents and Multi-Agent Systems,* vol. 12, pp. 183-198, 2006.

[45] T. Tran, "Protecting buying agents in e-marketplaces by direct experience trust modelling," *Knowledge and Information Systems,* vol. 22, pp. 65-100, 2010.

[46] H. C. Wong and K. Sycara, "Adding security and trust to multiagent systems," *Applied Artificial Intelligence,* vol. 14, pp. 927-941, 2000.

[47] M. Wooldridge, "Agent-based software engineering," *IEE Proceedings-Software,* vol. 144, pp. 26-37, 1997.

[48] B. Yu and M. P. Singh, "Searching social networks," *In Proceedings of the Second International Joint Conference on Autonomous Agents and Multiagent Systems, ACM,* pp. 65-72, 2003.