A Hybrid Trust Management Model for MAS Based Trading Society

Kanagaraj Krishna and Muhammad bin Maarof
Information Security Group, University of Technology Malaysia, Malaysia

Abstract: *The widespread use of the Internet signals the need for a better understanding of trust as a basis for secure on-line interaction. In this paper we provide and discuss existing works on trust management models in the area of Multi Agent Systems and highlight the shortcomings. Our proposed model is not presented as the final solution to the issue. This new model will have a mechanism that allows agents to manage trust not by just one way but a few combinations of different types of trust in different situations. The proposed model is concerned with the general notion of trust, one that goes beyond cryptographic protocols. Findings from this paper can be used for future research work in the area of trust in Multi Agent Systems and to address further the importance of trust management on the Internet.*

Keywords: *Internet, trust management, Multi Agent System, hybrid approach, cryptography, untrustworthy agents.*

Received March 1, 2003; accepted May 12, 2003

1. Introduction

Internet services are increasingly being used in daily life for electronic commerce, web-based access to information and inter-personal interactions via electronic mail rather than voice or face-to-face, but there is still major concern about the trustworthiness of these services. There are no accepted techniques or tools for specification and reasoning about the trust [12]. The concept of trust may seem a little unusual to suggest for computers; it is thus worthwhile to put forward some reasons why it may prove useful. Implicit in the notion of distributed artificial intelligence is the concept of decentralization. Since decentralization implies a lack of central control, and with it lack of guidance in the right direction, it becomes necessary, in order to carry through successful interactions with other agents, to develop some judgement as to the worth of these interaction and the risk associated with them [22].

Software agents are increasingly being required to make decisions and act locally, but also operate in the context of a "global" multi-agent society. As these agents become fully autonomous they become forced to make decisions about when and when not to engage (for instance to request information, to delegate important tasks or to trade) with or trust other Agents. They must rely on beliefs and knowledge about those other Agents in the society. This reliance on beliefs forms the basis *trust relationship* between intentional entities [33]. Well known techniques to ensure that something is 'trusted' have been developed and strengthened, and these techniques include cryptographic algorithms, authentication protocols, and access control [2]. These methods cannot manage the more general concept of 'trustworthiness' and are currently lacking the complementary tool for managing trust effectively [3]. It is the aim of this research, to create a new trust management model through a hybrid approach that more comprehensively and realistically deals with the problem of trust, with particular emphasis on the specification and analysis of trust relationships.

We will continue in section 2 by clarifying our concept of trust, agent, multi agent systems. Section 3 will discuss previous work done. Section 4 will be on the justification for an hybrid approach and we provide an outline of our approach. The last section will be the summary, conclusion and future work of this research.

2. Research Methodology

In this section, we will discuss about the research process/flow that was used carried out to formulate the problem and come out with the initial solution in the form of a new trust management model. Figure 1 below, shows the research process flow practiced, which is systematic in the sense that it follows certain steps that are logical in order.

2.1. Problem Formulation

The main objective of the problem formulation phase is to focus on a subject for research [15]. For this purpose the subdividing approach has been used formulate the research problem. This approach divides the general area of research into progressively small units, subdividing it until one reaches a subject that is of interest and specific. The first phase is to identify the broad research area, which started from the interest in the issue of "trust" on the Internet. Through preliminary literature review relevant literature were obtained. The preliminary studies showed that one of the main issues that has been highlighted was trust among agents and focused more on multi-agent system. Research works on the issue of trust in MAS were identified to understand the background of this issue. From that, the scope of the research was scaled down to the management of trust in MAS. An overview for the background of the problem definition was formulated from preliminary literature review.

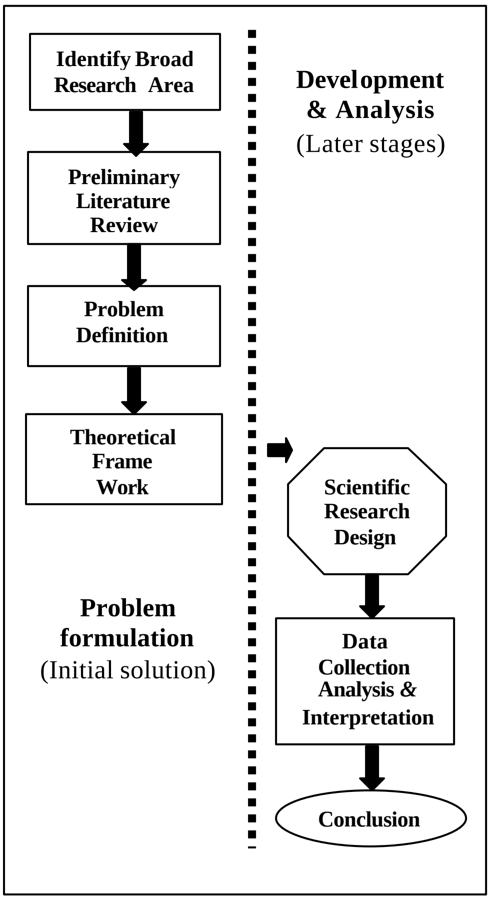
Identify Broad Research Area
Preliminary Literature Review
Problem Definition
Theoretical Frame Work
Problem formulation
(Initial solution)
Development & Analysis
(Later stages)
Scientific Research Design
Data Collection Analysis & Interpretation
Conclusion

Figure 1. Research process flow [15].

2.2. Theoretical Frame Work

At this stage focused and specific research has begun. Search for a new approach on the issue was carried out. Finally it was decided that a new trust management model would be designed using an hybrid approach. The initial result obtained from this research was used to formulate and design a new trust management model that combines elements form other existing models to form an improved version. This paper is basically only based on the model formulation. The next level, which consists of the simulation development and analysis of result will, not be discussed and kept for future work. Currently this phase is ongoing.

3. Background

This section will discuss the important terms involved in this paper and also discuss previous work done in this area.

3.1. Trust

Trust is a vast topic that incorporates trust establishment, trust management, and security concerns. Trust within entities is an extremely complex and dynamic phenomenon [24]. The lack of consensus with regards to trust has led authors to use the terms trust, authorization, and authentication interchangeably. The outcome of a trust decision is based on many things such as the trustor's propensity to trust, and its beliefs and past experiences relating to the trustee. For this paper, the term trust will be based on the definition by Tyrone Grandison that states [13]: *"Trust is the firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context"* (assuming dependability covers reliability and timeliness).

The earliest work on trust focused on individuals and used a psychological perspective [23]. From the research done on trust, we categorized it into three main elements that consist of objective trust, subjective trust and reputation.

In [10], Greck defines objective trust in the term "trust is a coherent collective agreement" -- which means that there is a collective equivalence on what is believed to be true and valid, oftentimes confusing trust with authorization or license". In general, trust can be seen as a form of absolute reliability in the subject of trust. This form is known as *objective trust* and is similar to the trust that we have in institutions or uniforms. Objective trust is the one based for example on the reliability of a system [8]. This type of trust is the natural tendency of individuals, based on their attitudes, personality and previous experiences, to trust other people.

In [10], Greck defines subjective trust in term "trust is what you know you know you know" -- you know, can recall at will and know how to use". Subjective trust is the mental state that influences the behaviour of an individual and is mediated by the specific nature of the transaction. Subjective trust, depends on the moment in time and the experiences accumulated between the truster and the subject of its trust. This form of trust presents an evolution over time called the dynamics of trust [16]. The agent to be either a trust-negative experience or a trust-positive one interprets each event that can influence the degree of trust. Although trust is something that is subjective belief, but as with real life, *"reputation is important, but no substitute for experience"* [20].

Some trusts are based on reputation of a particular agent. As what Misztal [25] says in his work, "[Reputation] helps us to manage the complexity of social life by singling out trustworthy people – in whose interest it is to meet promises". According to Abdul-Rahman et al [1], reputational information is important in making effective and informed trust decisions. He defines reputation as an expectation about an agent's behaviour based on information about or observations of its past behaviour. The definition of reputation for this paper will be based on Ostrom's

[26] work that states: *"Reputation is the perception that an agent creates through past actions about its intentions and norms."*

3.2. Trust Management

In [12], trust management is defined as:

"The activity of collecting, codifying, analyzing and presenting evidence relating to competence, honesty, security or dependability with the purpose of making assessments and decisions regarding trust relationships for Internet applications".

The definition above will be used for the purpose of this paper. This paper is not focused on Internet applications alone, which is mentioned in the definition but more on a general approach. Although this is the case, the definition also specifies the need to collect *(recommendation and objective trust)* and analyze to make decisions on trusting an entity. This is an important element in our approach. Trust can form an important factor in decision-making [5, 18, 21]. Thus, for Internet commerce or trading to achieve the same levels of acceptance as traditional commerce, trust management has to be an essential part of virtual communities.

3.3. Agent and MAS

An agent can be a software object, a robot, a living being, or anything that fulfills the basic concepts of agency. In the context of this paper, the use of the word *agent* will always imply *software agent* as opposed to any other kind, unless specifically stated. The following definition from [29] of an agent, will be used for this paper:

"A software object that perceives its environment through sensors and acts upon that environment through effectors to achieve one or more goals."

Combining several agents pursuing the same goal leads to the multi-agent system [4] also known as MAS. Similar to the term *agent*, it is difficult to find a commonly accepted definition of MAS. For the purposes of this paper, the Weiss definition of MAS will be used [32]:

"A system in which several interacting, intelligent agents pursue some set of goals or perform some set of tasks".

3.4. Previous Work

This section will look into previous work done in the areas related to trust in Multi Agent Systems, which is the focus of this research. The works have been divided into few categories for clarity of the issue. The categories are distributed approach, cryptography approach, subjective/ implicit approach, explicit approach, objective approach and social approach.

Yahalom et al [35, 36] discussed in significant detail the concept of trust in distributed systems. It was highlighted in their research, the fact that there is no effective formal way to reason about trust in distributed systems and to analyze trust requirements in security protocols, some kind of formal tool is needed. As a solution, they defined *trust classes*, made the distinction between *direct* and *recommendation* trust and proposed formalism to analyze trust in authentication protocols. However, their work falls short of defining a framework for building protocols with extended trust information.

In [27, 28], Rasmusson and Jansson came with a 'soft' approach to security by the introducing the idea of social control. The open system modelled in their work represents an electronic marketplace, which consists of buyer and seller 'actors'. It is up which consists of buyer and seller 'actors'. It is up to the good actors to identify 'cheaters' and propagate this information throughout the system. Social control attempts to remedy the situation where there is no easy way for a component to know all the other components in open systems, by relying on group behaviour to influence the behaviour of its group members.

Other related work includes Pretty Good Privacy [38], which helped inspire the research in distributed nature. Trust is also being used as a basis for cooperation among autonomous agents in the area of Distributed AI by Marsh [23]. His approach involves the addition of perceived risk and utility of committing resources in a cooperative relationship, which results in a complex trust calculation algorithm.

All this research done about trust in distributed environment, were general in discussion and not specific to the area of multi agent systems. In order to apply the result from research in distributed trust management, a few modifications has to be done to fit into the architecture of multi agent systems.

In [34], Wong and Sycara discussed a number of security and trust issues faced by MAS. Their work tried to provide an infrastructure to deal with such issues, make use of techniques that are well known in the network security literature, and they apply these techniques to MAS. As these authors mention, there is no measure proposed about trust or honesty. There is no way of ensuring that an Agent will carry out a task as expected, or of guiding an Agent to interact with other Agents that will probably be honest.

Another approach of dealing with security issues in MAS was made by Thirunavukkarasu, Finin and Mayfield [31]. They introduced a number of new KQML (Knowledge Query and Manipulation Language) [9] performatives enabling Agents to interact in a secure manner. These authors use classic network security techniques and do not propose any security or trust models. Approach to trust using cryptography didn't stop and was also continued by Jonsson [17]. His work described and discussed the various security/trust problems. It looked into the work of other authors in order to find solutions by trying to fill in the holes of these solutions if there are any. He tried to answer the question whether trust can be achieved using cryptography and came with a few suggestion to improve current cryptographic methods. But as a conclusion he suggested that the use of cryptography for must be considered as a minimum requirement.

Most of the work concerning trust in computer science have been concentrated in the area of security. These are mainly in the form of formal logics [7, 11] to analyze cryptographic protocols for design flaws and correctness. However, they are ill suited as general models of trust as their applications are for a specific domain and they were not designed to be automated. Furthermore, no concrete definition of trust was given – the authors assumed that the intuitive notion of trust is universal. However, this is unsatisfactory because although trust is an elusive notion that is hard to define, its lack of definition opens trust models to subjective interpretations and incompatible protocol implementations.

In implicit approaches, Agents use only a subjective probability to model the trustworthiness of the others. Schillo and Funk [30] conducted a number of simulations where Agents interact with each other using a modification of the prisoner' s dilemma (i.e. the disclosed prisoner' s dilemma with partner selection). Each single Agent builds a model of trustworthiness of the other Agents by gathering data on past behaviour and evaluating averages. When Agents are asked about their knowledge on other Agents, they are free to lie about their observations. Nevertheless, Schillo and Funk show that by averaging the values of a sufficient number of observations Agents can learn models almost twice as fast as other Agents that use only their own observations, while still reaching the same or better accuracy.

In [2], an approach to the problem of trust management was presented, which uses *recommendations* by Abdul-Rahman *et al*. Their work are based on four goals, to adopt a *decentralised* approach, *generalise* the notion of trust, lessen ambiguity (making trust statements more *explicit)* and facilitate the exchange of trust-related information via a *common protocol*. They highlighted the need for effective trust management in distributed systems, and proposed a protocol based on *recommendations*. This approaches doesn't consider trust from the perspective of real experience which is also an element in forming trust .

Explicit cognitive approaches appear more sophisticated, as they attempt to model the "mind" of the other Agents. Castelfranchi and Falcone [8], give a number of guidelines that should be taken into consideration when modelling the trustworthiness of other Agents. These authors separate the concept of trust from that of delegation and mention a number of beliefs that should exist before delegating a task to another Agent (i.e. competence, disposition, dependence beliefs etc.). They also assert that a subjective probability includes too many important beliefs and parameters. But this research is more on the conceptual level reasoning of trust and doesn't talk about the element of objective trust.

Witkowski M. *et al* [33], stress that trust should be based, whenever possible, on direct experience rather than on accumulated social attitude because as in real life, there is a limit to what can be achieved by wondering about what another entity might, or might not, do in any particular circumstance. They considered *objective Trust-Based Agents* (oTBAgents), Agents that select who they will trade with primarily on the basis of a trust measure built on past experiences of trading with those individuals. Experiments were done in an *Intelligent Network* (IN) infrastructure in which different types of Agent may form a trading community. A simulation has been done to analyze the behaviour of agents in different circumstances. Although they recognize trust both as a function of subjective beliefs and as a function of experience will be important to the construction of Agents in the future but concentration was only given in the research area of objective trust.

Following a social approach for security in MAS, Biswas, Debnath and Sen [6] have proposed a model where Agents have relatively complex behaviours. They use a probabilistic mechanism in which an Agent A will decide whether or not to honour a request for help by Agent B. This mechanism takes under consideration previous observations of Agent B, as well as the additional cost incurred by Agent A from Agent B. The researchers demonstrate that Agents that adapt their trust models over time and use the probabilistic decision mechanism are able to successfully withstand the invasion of selfish and exploitative Agents. This model consider all of their previous observations equally before delegating a task but for the purpose of this research we will prefer the approach proposed in [33], where the trust function of section place extra weight on recent experiences, although they are influenced by all experiences between the two Agents. This is a better approach because it simulates the real life behaviour where although you know someone for quite some time but still recent events (experience) plays an important part in any decision. Probabilistic approach is not a strong one in the area of trust, where decision can't be made just based on probability.

Zacharia *et al*, [37] developed methods that can automate the social mechanisms of reputation for the purposes of an electronic marketplace. These two collaborative reputation mechanisms are implemented and tested in the Kasbah electronic marketplace. In Kasbah, the reputation values of the individuals trying to buy or sell books or CDs are a major parameter of the behavior of the buying, selling or finding agents of the system. They stress that incorporating reputation mechanisms in online communities may induce social changes in the way users participate in the community. This work also concentrates only on the reputation mechanism (which comes under subjective trust) but from the social context.

4. Our Approach

As far as we know, there are only two other such similar approach to ours; that is Marsh's trust model

[23] and Abdul-Rahman *et al* [1]. In [23], although the sociological foundations of his model are strong, several shortcomings are present. Marsh tries to incorporate all aspects of social trust and introduces a large number of variables into his model. This makes his model large and complex because trust itself is a very complex and many faceted things.

Abdul-Rahman *et al* [1], aim is to provide a trust model based on the real world social properties of trust, founded on work from the social sciences. In their approach to discovering the 'real-world' characteristics of trust, they turned to the social sciences. They proposed a model, which deals exclusively with beliefs about the trustworthiness of agents based on experience and reputational (recommended) information. Their method is time consuming and laborious. Also it is not clear how the agents get needed information.

It can be said that an effective practical trust model for the virtual environment is not yet in existence [1]. In their proposed model, there is no mechanism that gives an option to have different combinations of trust for different situations. This will be the main concern of our work. For the purpose of this research, we chose to go for a hybrid approach to combine the benefits of few models into one to make it more effective. The new trust management model will be based on the Witkowski M, *et al* [33] *objective Trust-Based Agents* and Abdul-Rahman *et. al* [1, 2] distributed trust model. The former has the objective trust element and the latter combines subjective trust together with reputation.

The new model will encompass all three components of a trust based trading relationship, reputation, subjective trust and objective trust. Each has an important role to play at different times in the overall life of a trading partnership. In the paper as stated, most of the previously done works have been discussing about a particular element but the authors also state that these three elements are related and important in managing trust. This was stated in [33], as future work and it forms the motivation of our research. An additional mechanism that controls this three component will exist in this proposed model.

4.1. The Model

From the survey done on previous works relating to trust management in Multi Agent Systems, a few shortcomings were identified:

- Concentrated more on the security and cryptographic aspect [17].
- Most of the work were more general and concentrated more on trust in distributed environment rather than specifically of its application in a MAS environment [1, 2, 3].
- Concentrated on a specific type of trust either objective, subjective or reputation based trust only, rather than combining all as one which will reflect a more appropriate way of forming trust in a multi agent community [2, 3, 33].
- Models that are complex, time consuming and laborious [1, 12, 23].

The new model will highlight and approach the shortcomings identified by:

- Concerning with the general notion of trust, one that goes beyond cryptographic protocols. Our approach is intended to complement current security practices by forming a general model within which trust can be more effectively managed and to extend trust beyond certification and encryption.
- The new model was built specifically for Multi Agent System environment. To test the proposed new model, our test domain will be a multi agent trading scenario based on a simplified model for an *Intelligent Network* (IN) but not restricted to this or any particular application area.
- The model will encompass all three components of a trust based trading relationship, reputation, subjective trust and objective trust. Each has an important role to play at different times in the overall life of a trading partnership. This new model will have a mechanism that allows agents to manage trust not by just one way but a few combinations of different types of trust in different situations.
- The model is designed not to be too complex and laborious. Trust chain has been avoided for its complexity. Direct trust has been used for our approach.

The proposed model in Figure 2 has 3 main components consisting of objective trust-based agents, reputation and the trust mechanism. Together these components combine to form the trust opinion needed in decision-making.

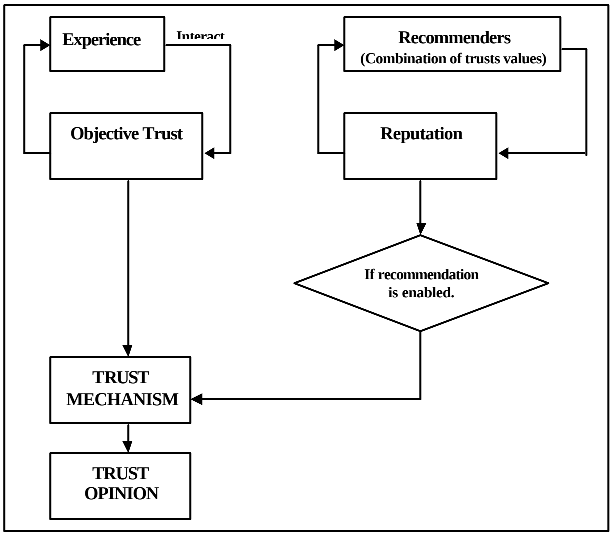

Figure 2. Hybrid trust management model.

4.1.1. Objective Trust

Each agent makes part of its trading decisions based on its past experiences of trading with other Agents in the IN, updating its trust vector, and so affecting its future decisions, based on each new transaction. Individual trust ratings are scaled from 0 (complete distrust) to 1.0 (complete trust). The use and management of these trust values is central to the operation of an agent, they are the principal way in which other agents are selected to trade with. The manner in which it is used, and the mechanism by which it is updated, define important aspects of an agents apparent “personality” (the way it appears to other Agents) within the society.

The formulations used for this component are normalised such that a string of positive experiences asymptotically moves trust ratings towards 1.0, and a string of negative experiences moves it towards 0.0. The function matches the intuition that trust is most enhanced by getting exactly what we requested, partially enhanced by getting some of our request and damaged by being excluded. The formulation also gives greater weight for recent experiences than earlier ones, the effect of past events are discounted with each new experience.

4.1.2. Reputation

Since it can be beyond each individual’s resources to evaluate all aspects of a given situation when making a trust decision, agents must rely on other sources of information. Indeed, if complete knowledge is possible, then trust is of no use anymore. In society, we obtain information from these ‘other sources’ by means of word of- mouth, i.e. a mechanism for propagating reputation. For this model the recommendation element in community is used to build reputation of a certain agent. This reputation is only used when trust ratings from based from experience is not sufficient. The flexibility of this model permits the reputation component to be enabled and disabled.

Each agent in the society has its own trust vector to rate other agents. This trust ratings will used when other agents request for recommendation to identify reputation of a certain agent. Recommendation rating values from other agents will combined to calculate reputation. Combining trust values is needed because there not necessarily unique recommendation paths, there will be sometime be several agent giving recommendation for the same agent. They will usually have different values, so a way is needed to draw a consistent conclusion. This is discussed in [1].

To maintain a strict trust management and lessen the implication of untrustworthy agents in the society a few rules are applied in this model for the reputation component. These are:

- Trust chain is not used.
- Only direct recommendation is accepted and ratings given from only one prior experience with an agent is not accepted.
- Recommenders are not selected based on ratings. All selected recommenders are assumed to be fully trustable, well known people with good judgement.

4.1.3. Trust Mechanism

This is the most important component of this trust management model. It forms the core of the model. After the two components of objective trust and reputation has been calculated, it will be brought to the trust mechanism to form trust opinion/decisions. This mechanism allows agents to manage trust not by just one way but a few combinations of different types of trust in different situations. This mechanism works based on a set of rules. The algorithm of this mechanism is shown below in Figure 3.

```
if (no previous experience) and (reputation
component enabled)

        if (reputation sufficient)

                Use reputation;
        else
                Explore to get experience
                based on exploration rate;

else if (experience exist) and  (reputation
component enabled)

        if (experience sufficient)

                Use both experience trust
                ratings combined with
                reputation if available;
        else
                Explore to get experience
                based on exploration rate;

else if (experience exist) and  (reputation
component disabled)

        if (experience sufficient)

                Use experience trust ratings
                only;
        else
                Explore to get experience
                based on exploration rate;

else
Explore to get experience based on
exploration rate.
```

Figure 3. Algorithm for the trust mechanism.

4.2. Model Architecture

The architecture of the proposed model is based on a distributed migration path. It uses a Master-Slave pattern, which is a common task design model, incorporated in a broad domain of parallel applications. This Master-Slave model is based on a divide and conquer strategy in which a master delegates tasks to one or more slaves that in turn are distributed throughout the system and work in parallel. The implementation of distributed migration path is considered to secure a prototype system because it has been implemented and tested by Kotzanikolaou *et. al* and has been successful in preventing attacks such as suppression of information [19], especially in MAS environment where agents travel from one destination to another.

The trust mechanism is controlled and executed by a customer agent who initiates a trading deal. The other two components of objective trust and reputation will be executed by two different slave agents generated by the customer agent before committing a trading deal with a certain trader agent. The customer agent acts as the master agent. The two slave agents are:

- OT agent (objective trust)
- Reputation agent

4.2.1. OT Agent Architecture

The architecture for the OT agents is shown in Figure 4. Customer agent generates OT agents to get information from trader agents who are known through past experiences (in the database) to know whether they available in the sense that they have the capacity to accommodate the request. This OT agent generates more slave agents if there are more then one known trader agents. If there are no known trader agents who are available, then new agents are approached through the same approach of generating slave agents

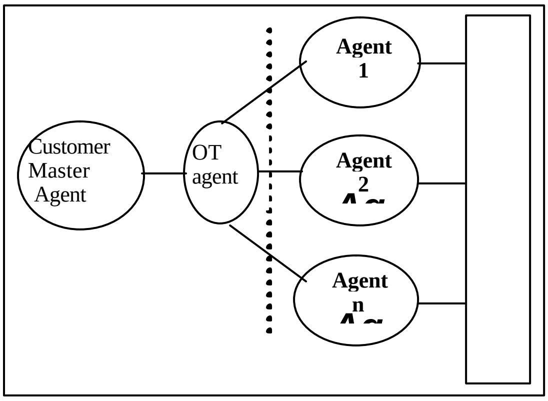

Figure 4. The OT agent architecture.

4.2.2. Reputation Agent Architecture

The architecture for the reputation agents is shown in Figure 5. The Reputation agents are only used if past experience with trader agents are not sufficient. Customer agent generates Reputation agents to get information from other trusted customer agents (in the database) to know whether they have available information on certain trader agent. This Reputation agent generates more slave agents if there are more then one known customer agents. After gathering reputation values from different customer agents, the Reputation agent calculates and sends the overall reputation of the trader agent to its master customer agents who requested it.

5. Conclusion and Future Work

The main contribution through this research is in the form of a new trust management model. Our approach is intended to complement current security practices by forming a general model within which trust can be more effectively managed and to extend trust beyond certification and encryption. In a world where people live with *uncertainty*, this new model copes with these uncertainties by allowing agents in a multi agent system to reason with different degrees of trust through the combination of objective (experience), subjective (recommendation) and reputation based trust management.

The proposed model is concerned with the *general notion of trust*, one that goes beyond cryptographic protocols. We believe that the model will be most suited to trust relationships that are short-term trust relationships or ad-hoc commercial transactions. Our model will not be suited to formal trust relationships based on legally binding contracts.

Future research will attempt to carry out simulation based on the proposed model test and study its behaviour pattern of the agents in different circumstances. We will present experimental results in a simulated trading environment using a simulation tool called SWARM, based on an Intelligent Networks (IN) scenario. Findings from this research can used for future research work in the area of trust in Multi Agent Systems and to address further the importance of trust management.

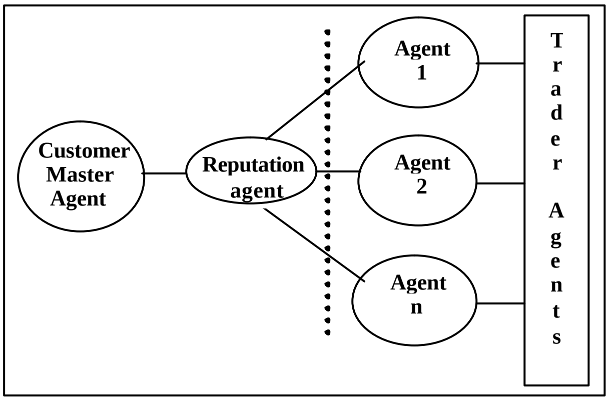

Figure 5. Reputation agent architecture.

References

[1] Abdul-Rahman A. and Hailes S., "Supporting Trust in Virtual Communities," *in Proceedings of Hawai'i International Conference on System Sciences*, Maui, Hawaii, 2000.

[2] Abdul-Rahman A. and Hailes S., "Using Recommendations for Managing Trust in Distributed Systems," *in Proceedings of IEEE Malaysia International Conference on Communication (MICC'97)*, Kuala Lumpur, Malaysia, 1997.

[3] Abdul-Rahman A. and Hailes S., "A Distributed Trust Model," *in Proceedings of ACM New Security Paradigms Workshop'97*, Cumbria, UK, 1997.

[4] Abeck S., Köppel A., and Seitz J., "A Management Architecture for Multi-Agent Systems," *in Proceedings of 3rd IEEE Workshop on Systems Management*, Newport, April 1998.

[5] Amoroso E. *et al.*, "Toward an Approach to Measuring Software Trust," *in Proceedings of*

IEEE Computer Society Symp. Research in Security and Privacy, http://ieeexplore.ieee.org/iel2/349/3628/00130788.pdf, 1991.

[6] Biswas A., Debnath S., and Sen S., "Believing Others: Pros and Cons," *in Proceedings of IJCAI'99 Workshop on Agents Learning About, From and With other Agents*, Stockholm, Sweden, 1999.

[7] Burrows M., Abadi M., and Needham R., "A Logic of Authentication," *ACM Transactions on Computer Systems*, vol. 8, no. 1, 1990.

[8] Castelfranchi C. and Pedone R., "A Review on Trust in Information Technology," *Unit of AI Cognitive Modelling and Interaction, National Research Council, Institute of Psychology*, Rome, Italy, 2000.

[9] Finin T. *et al.*, "KQML as an agent communication language," *Jeff Bradshaw (Ed.), Software Agent*, MIT Press, Cambridge, 1995.

[10] Gerck E., "Toward Real-World Models of Trust: Reliance on Received Information," http://www.mcg.org.br/trustdef.htm,1998.

[11] Gong L., Needham R., and Yahalom R., "Reasoning about Belief in Cryptographic Protocols," *in Proceedingsof IEEE Symposium on Research in Security and Privacy*, Oakland, 1990.

[12] Grandison T., Trust Specification and Analysis for Internet Applications, *PhD Thesis*, Imperial College of Science Technology and Medicine, Department of Computing, London, 2001.

[13] Grandison T. and Sloman M., "A Survey of Trust in Internet Applications," *IEEE Communications Surveys*, Fourth Quarter, 2000.

[14] Holland C. and Lockett A., "Business Trust and the Formation of Virtual Organizations," *31st Annual Hawaii Int. Conf System Sciences*, Hawaii, 1998.

[15] Johnson G., *Fire in the Mind*, Viking, London, 1996.

[16] Jonker C. and Treur J., "Formal Analysis of Models for the Dynamics of Trust Based on Experiences," *in Proceeding of Autonomous Agents '99, Workshop on Deception, Fraud and Trust in Agent Societies*, Seattle, pp. 81-94, 1999.

[17] Jönsson P., "Trust in Multi-Agent Systems: Is Cryptography a Way to Achieve Trust?," *presented in Blekinge Institute of Technology Student Workshop on Agent Programming (BITSWAP)*, 2001.

[18] Jøsang A. and Knapskog S. J. "A Metric for Trusted Systems," *21st National Security Conf.*, http://www.idt.ntnu.no/~ajos/papers.html, 1998.

[19] Kotzanikolaou P., Katsirelos G., and Chrissikopoulos V., "Mobile Agents for Secure Electronic Transactions," *in Mastorakis N. E. (Ed.), Recent Advances in Signal Processings and Communications*, World Scientific Engineering Society, pp. 363-368, 1999.

[20] Lorenz E. H., "Neither Friends nor Strangers: Informal Networks of Subcontracting in French Industry," *in Gambetta D. (Ed), Trust: Making and Breaking Cooperative Relations*, Basil Blackwell, Oxford, pp. 194-209, 1990.

[21] Manchala D. W., "Trust Metrics, Models and Protocols for Electronic Commerce Transactions," *in Proceedings of 18th Int. Conf. Distributed Computing Systems*, http://ieeexplore.ieee.org/iel4/5583/14954/00679731.pdf, 1998.

[22] Marsh S., "Trust and Reliance in Multi Agent System: A Preliminary Report," *MAAMAW'92*, Italy, 1992.

[23] Marsh S. P., Formalising Trust as a Computational Concept, *PhD Thesis*, University of Stirling, Scotland, 1994.

[24] McCauley C. and Kuhnert K. W., "A theoretical review and empirical investigation of employee trust in management," *Public Administration Quarterly*, vol. 16, no. 2, pp. 265-283, 1992.

[25] Misztal B., *Trust in Modern Societies*, Polity Press, Cambridge, MA, 1996.

[26] Ostrom E., "A Behavioral Approach to the Rational-Choice Theory of Collective Action," *American Political Science Review*, vol. 92, no. 1, pp. 1-22, 1999.

[27] Rasmusson L. and Jansson S., "Simulated Social Control for Secure Internet Commerce (position paper)," *in Proceedings of New Security Paradigms '96 Workshop*, Lake Arrowhead, CA, 1996.

[28] Rasmusson L. and Jansson S., "Personal Security Assistance for Secure Internet Commerce (position paper)," *in Proceedings of New Security Paradigms '96 Workshop*,1996.

[29] Roddy K. A. and Dickson M. R., Modeling Human and Organizational Behavior Using a Relation-Centric Multi-Agent System Design Paradigm, *Masters Thesis*, Naval Postgraduate School, Monterey, California, September 2000.

[30] Schillo M. and Funk P., "Learning from and about other Agents in Terms of Social Metaphors," *in Proceedings of Agents Learning about, from and with other Agents Workshop*, 1999.

[31] Thirunavukkarasu C., Finin T., and Mayfield J., "Secret Agents - A Security Architecture for the KQML," *in proceedings of ACM CIKM Intelligent Information Agents Workshop*, Baltimore, 1995.

[32] Weiss G. (Ed.), *Multiagent Systems: A Modern Approach to Distributed Artificial Intelligence*, MIT Press, Cambridge, 1999.

[33] Witkowski M., Artikis A., and Pitt J., "Trust and Cooperation in a Trading Society of Objective-Trust Based Agents," *in Proceedings of Deception, Fraud and Trust in Agent Societies workshop, Autonomous Agents 2000*, Barcelona, pp. 127-136, 2000.

[34] Wong H. C. and Sycara K., "Adding Security and Trust to Multi-Agent Systems," *in Proceedings of Autonomous Agents'99, Workshop on*

Deception, Fraud and Trust in Agent Societies, Seattle, pp. 149-161, 1999.

[35] Yahalom R., Kle in B., and Beth T., “Trust Relationships in Secure Systems: A Distributed Authentication Perspective,” *in Proceedings of IEEE Symposium on Research in Security and Privacy*, 1993.

[36] Yahalom R., Klein B., and Beth T., “Trust-Based Navigation in Distributed Systems,” *Computing Systems*, vol. 7, no. 1.

[37] Zacharia G., Moukas A., and Maes P., “Collaborative Reputation Mechanisms in Electronic Marketplaces,” *in Proceedings of the 32nd Hawaii International Conference on System Sciences*, Hawaii, 1999.

[38] Zimmermann P., *PGP User’s Guide*, MIT, October 1994.

Kanagaraj Krishna received his BSc degree in computer science, majoring in systems, from University of Technology Malaysia. Currently, doing postgraduate studies in the same university for MSc in computer science (security). Interest in CSCW and trust management related issues in computer agent community.

Muhammad bin Maarof is an associate professor at Faculty of Computer Science and Information System. He obtained his BSc in computer science and MSc in computer science from USA and his PhD from Aston University, Birmingham, United Kingdom in the area of information technology security. He is currently leading the Information Security Group in the faculty. Currently, he involves as head of a research in the areas of agent security, immune-base intrusion detection system and cryptography.