Volume 3, Issue 9, September-2016, pp. 500-505 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

Cryptographic Protocol Based Laurel System for Multi agent Distributed Communication

Sreedhar Jyothi[1], Dr. A. Damodar[2]

[1]Student, M.S (part time research Program), Dept., of CS&E, JNTU, Ananthapur
[2]VC, SVU

Abstract: In order to expedite detection of unfaithful and malicious agents, an agent recognition mechanism is proposed for multi agent communication, which is based on a laurel model and a cryptographic protocol. A laurel system for multi agent communication can be let down by a set of malicious agents. Such a group can maliciously raise the laurel of one or more agents of the group. There is no known method to protect a laurel system against swindler agent groups. So there is a need for false proof laurel management mechanism to avoid malicious agents providing false state of laurel. The modern systems that entertain multi-agent communication are more vulnerable to agents who behaves maliciously or simply do not cooperate. The lack of core level trusted third party in multi agent communication strategy postures distinctive issues for laurel management. These issues feature agent recognition strategy, dependable laurel maintenance. The disadvantage of the existing system is the laurel of the agent that responds to a request is considered but the credibility of the agent that attempts to update the laurel of the other agent is ignored. This proposal aims to devise a model to encapsulate the laurel of both the agent that respond and the agent that request. The proposed protocol reduces the number of malicious transactions. It also manages the issue of highly inconsistent accessibility pattern of the agents in multi agent communication based systems.

Index Terms: Cryptography, Reputation Models, E-commerce, Trusted Models, Distributed Communication, Blind fold strategy, quality of service

1 INTRODUCTION

Networking technology of computers and communication systems, from closed network have evolved to open network, now accessible publicly. Trust and security issues have become critically important with the fast expansion of multi-agent systems or applications such as the E-business systems, Agent-to-Agent, Grid and Semantic Web which are open, anonymous and dynamic in nature. A multi-agent system is one in which many agents run concurrently, communicating among them and working toward either individual goals or a common objective [9]. Individual components in each system are both autonomous and flexible in their actions and due to this attackers/malicious agents are always seeking to spread malicious content in the multi-agent network. One of the solutions to minimize the threats is to evaluate the trust and reputation of interacting agents. Trust evaluation models use different standards in its opinion and with the existence of fraud and unreliable services, agents face dilemma in identifying and selecting efficient service with increasing choice of chance. With these research problems in mind, we propose a reputation-based dynamic trust evaluation model;

Dynamic trust evaluation models that are reputation-based depend on the quality of the service provided (QoS) by agent service provider. Reputation and trust of a transaction from Agent Q to Agent P where P avails the service of Q is generated by P on his observations of the Quality of the Service. The reputation of Q is updated by P according to the QoS, however the service quality P has associated for each transaction with Q may differ. In general it is assumed that consistent quality of service is provided over a long sample of time. The proposed reputation model based on the reputation values of a short period of time shows the QoS of every agent as an average. Though critical for sustaining good quality of service, the model is inefficient for direct transactions and where reputation values are updated many times over in short period of time.

Systems that provide reputation services build trust through social interactions where an evaluator is an agent who evaluates the trustworthiness of other agents without trusting third parties. Based on the evaluator's viewpoint on the accumulation of information, the reputation based trust models are divided into two basic types;

1) Direct/Local experience model and 2) Indirect/Global reputation model

The Direct experience model depends on direct transactions or inferences based on personal encounters and the Indirect experience model generates reputation from details that is not firsthand, collected indirectly. In global reputation models [17] an agent collects the feedback from other agents who previously had interactions with the agent whose reputation is being built. Globally due to presence of fraud and unreliable services, untrustworthy agents can implant feedbacks not true, it is very challenging to control indirect reputation model compared to the local/direct reputation model.

In the multi-agent system, for handling the threats associated with malicious agents a decentralized reputation-based dynamic trust mechanism is proposed. This model in the multi-agent network, we build reputation based on direct and indirect experiences for establishing trustworthiness of other agents for forecasting their probable actions with respect to a transaction thus minimizing losses associated with the failover in transaction.

This study and the proposed model concentrate on reputation and trust management in a multi-agent model. A reputation-based dynamic trust evaluation model is proposed which is a system that efficiently identifies unexpected premeditated variation in malicious activities.

2 REVIEW OF LITERATURE

When agents do not have complete information about their environment or their interaction partners, there is uncertainty. Trust helps in reducing uncertainty in interactions in open distributed systems. Ramchurn et. al. [9] examine the role of trust in multi agent systems. They conceptualize trust in two ways; system level and individual level trust. System level trust forces agents in the system to be trustworthy because of protocols and mechanisms that regulate the system. Individual level trust models give agents the ability to reason about the trustworthiness of their interaction partners. They state that system level trust can be enforced by designing interaction protocols that force participants to be truthful [38], or develop reputation mechanisms [17] [11] [35] that encourage interaction partners to behave in a trustworthy manner, or have security mechanisms [31] [32] that guarantee that new participants are trustworthy.

In [39], Sabater and Sierra provide a review of several computational trust and reputational models. They classify trust and reputation models on the following dimensions.

1. Conceptual Model: Based on their conceptual model, trust and reputation models are classified as cognitive models or game theoretical models. In cognitive models trust and reputation are considered to be the result of an agent's mental state in a cognitive sense [33]. Esfiandiari and Chandrashakeran [22] point out that in cognitive models "trust and reputation are made up of underlying beliefs and are a function of the degree of these beliefs." In game theoretical models trust and reputation models are the result of pragmatic games with utility functions, and numerical aggregation of past interactions [16] [27] [29].
2. Information sources: Trust and reputation models are classified based on the information sources used to compute trust and reputation. Four types of information sources are considered:
   - Direct Experiences: There are two types of direct experiences. An agent's own experience with another agent [29] [2] [35] and an agent's direct observation of other agents interactions [40] [3].
   - Witness Information: Information is provided to the agent by other members of the community [27] [35].
   - Sociological Information: This is based on the social relations between the agents, and the agents' roles in the society [37] [2]. Examples of social relations can be trade, competition, and collaboration. The roles of agents and their relationships with other agents influence their behavior and their interaction with other agents.
   - Prejudice: This is based on assigning reputation to an individual based on signs that identify the individual as a member of a group. Work described in [22] [2] uses this source of information in trust and reputation models.
3. Visibility types: Models are classified based on whether trust and reputation is considered a global property that is shared by all individuals, or a subjective property that is computed separately by each individual. In the first case, trust or reputation of an individual is updated at a central place. It is computed from the opinions of all individuals that have interacted with the individual that is being evaluated. When reputation is treated as a global property, there is a lack of personalization, since it assumes a common way of thinking. In [27] [19] [25] [35] reputation is updated at a central place. In the second case, each individual assesses another

individual separately based on its own interactions, or based on information gathered from friends or other sources. The work described in [16] [33] [29] [2] [40] [3] [30] [35] considers trust and reputation as a subjective property.

4. Model's granularity: In this dimension, models are classified based on whether trust and reputation is considered as context dependent or as non-context dependent. In a non-context dependent model the trust/reputation value for an individual is a single value [27] [40] [3] [35]. In a context dependent model the trust/reputation for an individual has different values, one for each context [16] [33] [22] [29] [2]. For example in a non-context dependent model, the reputation of a seller will be a single value. In a context dependent model, the reputation of a seller can have different values for different contexts like price, quality and delivery date.

5. Agent behavior assumption: There are three different levels of models based on the agent's capacity to deal with cheating agents.

- Level 0: The model does not consider cheating behavior [27] [30] [22] [35].
- Level 1: The model assumes that agents can hide or bias the information, but not lie [40].
- Level 2: This model assumes that agents can lie and have mechanisms to deal with it [2] [3].

6. Type of exchanged information: Models are classified on whether they assume Boolean information, or continuous measures. Models that use probabilistic methods work with Boolean information [16] [3], while models using aggregation mechanisms use continuous measures [27] [29] [2] [40].

7. Trust/reputation reliability measure: Models are classified based on whether the trust/reputation models provide the reliability of the trust/reputation values being computed. Number of experiences, reliability of the witnesses, and age of the information are used to compute the trust/reputation reliability measure [23] [2] [35].

3 AGENT SELECTION STRATEGY FOR MULTI AGENT COMMUNICATION SYSTEM

The lack of core level trusted third party in multi agent communication strategy postures distinctive issues for reputation management. These issues feature agent recognition strategy, dependable reputation maintenance. The disadvantage of the existing system is the reputation of the agent that responds to a request is considered but the credibility of the agent that attempts to update the reputation of the other agent is ignored.

Here we devised a model to encapsulate the reputation of both the agent that respond and the agent that request. The proposed protocol avoids spiteful elevation of the agent's reputation. It also manages the issue of highly inconsistent accessibility pattern of the agents in multi agent communication based systems.

3.1 Selecting response agent by its reputation:

The supplicant Agent spt that requires information selects the respondent agent rpt with the utmost reputation, then agents spt and rpt estimates mutual trust by exchanging their reputation.

A message msg sent by 'spt' to 'rpt' can be denoted as $spt \rightarrow rpt : msg$

puk_{rpt} Represents the public key of the agent rpt

prk_{rpt} Represents the private key of the agent rpt

The agent spt sends the request rq along with its identity spt_{idt} to all other agents possible to respond, which is by encrypting with public key of each rpt_i

$$spt \rightarrow \bigcup_{i=1}^{n} rpt^{i} : E_{puk_{rpt^{i}}}(spt_{idt}, rq, H(spt_{idt}), H(rq))$$

Here in the above equation $H(spt_{idt}), H(rq)$ represents the one way hash of the agent spt identity and the request rq respectively

Upon receiving the message sent by spt, the agent rpt decrypts it by prk_{rpt} and checks the request rq, if willing to respond, then the agent rpt verifies the self-assessed identity of the spt,

If 'spt_{idt}' is valid then it verifies its reputation as supplicant. Upon finding the satisfactory reputation of the supplicant spt, the agent rpt sends an encrypted message $rmsg$ to supplicant spt. The message $rmsg$ contains encrypted form of identity of agent rpt, reputation score rs, recent reputation updates frequency ruf, and reputation update divergence threshold $rudt$ along with the one way hash values of all these.

$$\bigcup_{i=1}^{n} rpt^{i} \to spt : E_{puk_{spt}}(rpt^{i}_{idt} : rpt^{i}_{rs} : rpt^{i}_{ruf} : rpt^{i}_{rudt} : H(rpt^{i}_{idt}).H(rpt^{i}_{rs}).H(rpt^{i}_{ruf}).H(rpt^{i}_{rudt}))$$

Upon receiving response messages from all possible agents, the supplicant agent spt, verifies their identity and picks response agents with valid identity, and then measures the credibility of those valid response agents by estimating their reputation rep. The digital certificate of the response agent rep will be verified as follows:

$$rpt_{sig} \cong H(rpt_{rs} + rpt_{salt})$$

Here in above equation rpt_{sig} represents the signature of the agent rpt available with agent spt and $H(rpt_{rs} + rpt_{salt})$ is one way hashing of the most recent updated reputation score of the rpt and salt used to generate the digital certificate signature of the agent rpt, which is by recent supplicant agent that accepted response from agent rpt.

The reputation rep of the response agent rpt^{i} can be measured as follows:

$$ruds_{rpt^{i}} = 1 - \frac{rpt^{i}_{rs}}{rpt^{i}_{rudt}}$$

Here in above equation $ruds_{rpt^{i}}$ represents the response update divergence score, which indicates the divergent number of supplicants involved to get the reputation score rs of the agent rpt^{i}.

$$rufs_{rpt^{i}} = 1 - \frac{rpt^{i}_{rs}}{rpt^{i}_{ruf}}$$

Here in the above equation $ruf_{rpt^{i}}$ indicates the reputation update frequency score of the agent rpt^{i}, reputation update frequency refers the ratio of response to requests received.

$$rep(rpt^{i}) = ruds_{rpt^{i}} + rufs_{rpt^{i}}$$

Finally supplicant agent spt opts to an agent rpt for response, if and only if $rep(rpt)$ is maximal than of any other agent with valid identity.

3.2 Updating reputation:

Once the required information is received by the agent spt from agent rpt, then supplicant agent spt initiates to update the reputation score of the responding agent rpt. According to the scope of the response received from the agent rpt, the supplicant agent spt fixes the reputation score of the response as -1, 0 or 1. (i) If response given by agent rpt is assessed as valid and helps to the further functional needs of the supplicant agent spt, then reputation score of the response as $rpt_{rs} + 1$, (ii) If the response is not helpful, but the intension of agent rpt is not suspicious, then reputation score of the response is $rpt_{rs} + 0$, (iii) The response sent by agent rpt is suspected as malicious with an intension of falsifying the further functionality of the supplicant agent spt, then the reputation score of the response is $rpt_{rs} - 1$.

Further the supplicant sends the message to rpt, which is regarding reputation score update. The agent rpt accepts the given reputation score by a blindfold approach. The supplicant agent spt sends a message to rpt as follows:

$$umsg = \{E_{ekey}(repscore, spt_{idt}), H(repscore + salt), H(spt_{idt})\}$$

$$spt \to rpt : umsg$$

Here in the above equation, E_{ekey} represents the encryption process that encrypts by using the key $ekey$, which is of the key pair $\{ekey, dkey\}$.The message contains the encrypted form of the reputation score given by supplicant agent spt against to the response given by agent rpt, the identity of the supplicant node and the one-way hash values of the both reputation score and identity. To avoid the conditional acceptance of the reputation score by response agent rpt, here supplicant agent sends it in encrypted format. Upon receiving the message, the agent rpt accepts $H(repscore + salt)$ as signature of the digital certificate and acknowledges the same by sending that certificate back to supplicant agent spt.Then supplicant agent spt shares a message msg with all other agents. The message msg contains the identity of the agent rpt and the new signature of the digital certificate of the agent rpt is shared with all other agents. Then supplicant agent spt sends the decryption key of the key pair $\{ekey, dkey\}$ along with $salt$ to the response agent rpt.

Upon receiving $dkey$, the agent rpt decrypts the encrypted message part of the '$umsg$' and updates its reputation score 'rs', 'ruf' and '$rudt$'. Further includes the '$salt$' to digital certificate that used to generate the signature of that digital certificate.

4 EXPERIMENTAL STUDY

Figure 1 shows the ratio of services successfully completed with positive or neutral reputation in proposed reputation based agent model and its performance advantage against Agent UNO strategy. The service completion advantage of proposal over Agent UNO is 1.5% more.

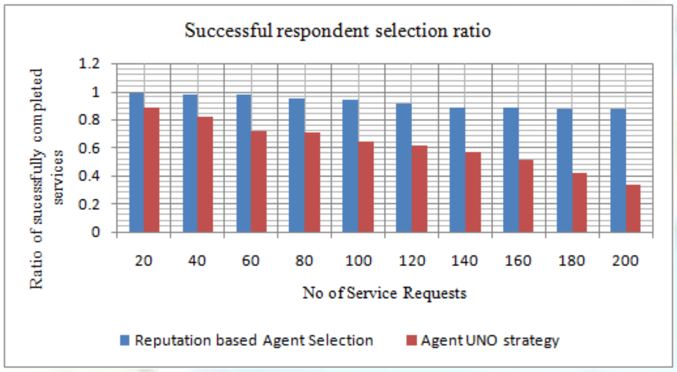

Figure 1: The service completion under positive or neutral reputation proportionality observed in proposed reputation based agent selection

Figure 2 maps proposed agent selection strategy against Agent UNO in agent selection optimality. The proposed model has an edge as Agent UNO used the ratio of 0.31 more respondent selection requests compared to proposed reputation based agent selection strategy.

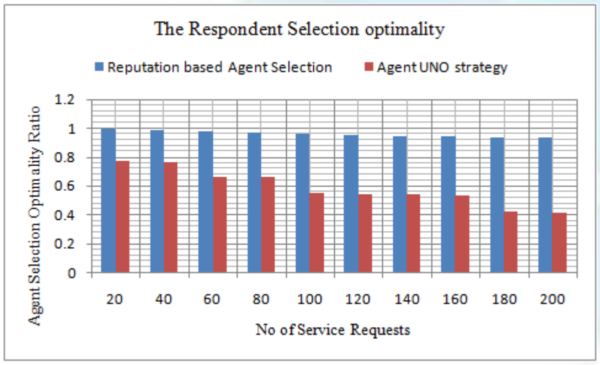

Figure 2: The Malicious agents' avoidance during respondent selection

Figure 3 shows that proposed strategy has considerably lesser payload expenses over Agent UNO, which is due to its reliable respondent selection strategy where the excessive payload garnered in proposed reputation based agent selection strategy compared to Agent UNO is lesser by 6.1%.

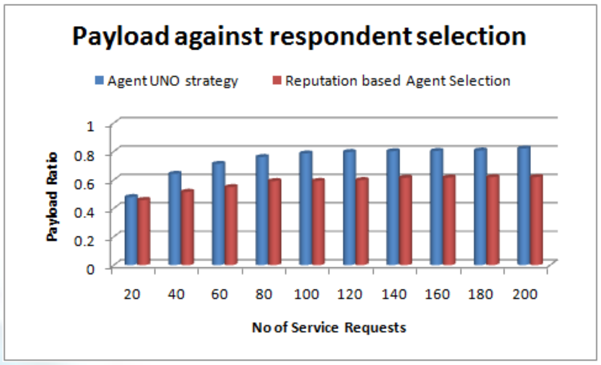

Figure 3: Process cost of Service completion by selecting reliable respondent.

5 CONCLUSION

The multi agent systems open a way to the malicious agents who can falsify the service completion by respondent selection. The motivation of an attacker can be either selfish or malicious. Being selfish, an attacker may respond maliciously against a service request. While being malicious, an attacker may respond to service request, though he unable to give service, thus causing chaos and interference for service seeking agents. Here in this thesis we explored the reputation aware agent selection strategy. The said model is significant and optimal towards multi agent systems. The experiment results indicating that the model devised here is proven to be robust under divergent number of respondents.

REFERENCES

[1] J.M. Vidal and E.H. Durfee, "The impact of Nested Agent Models in an Information Economy", Second Int. Conf. on Multi-Agent Systems, 377-384, 1996.

[2] J. Sabater, "Trust and Reputation for Agent Societies", Phd Thesis, Universitat Autnoma de Barcelona, 2003.

[3] S. Sen and N. Sajja, "Robustness of Reputation-based Trust: Boolean Case", Proc. of the First Int. Joint Conf. on Autonomous Agents and Multiagent Systems (AAMAS-02), Bologna, Italy, 288–293, 2002.

[4] M. Wooldridge, An Introduction to MultiAgent Systems, Chichester: John Wiley and Sons, 2002.

[5] T. Tran and R. Cohen, "Learning Algorithms for Software Agents in Uncertain and Untrusted Market Environments", Proc. of the Eighteenth Int. Joint Conf. on Artificial Intelligence, 2003.

[6] B. Krulwich, "The Bargainfinder Agent: Comparision Price Shopping on the Internet", Bots, and other Internet Beasties, J. Williams (Ed.), 257-263, Macmillan Computer Publishing, 1996.

[7] R. Till, "Transforming the way we do business", In: Electronic Commerce, T.Nash, editor, 9-12, Kogan Page, London, UK, 1998

[8] M. He, N. R. Jennings, and H. Leun. "On Agent-Mediated Electronic Commerce" IEEE Trans on Knowledge and Data Engineering, Vol. 15(4) 985-1003, 2003.

[9] S. D. Ramchurn, T. D. Huynh, and N. R. Jennings, "Trust in Multi-Agent systems", The Knowledge Engineering Review, Vol. 19(1), 1-25, 2004.

[10] K. Regan, T. Tran, and R. Cohen, "Sharing Models of Sellers amongst Buying Agents in Electronic Marketplaces", Decentralized Agent Based and Social Approaches to User Modelling (DASUM), July 2005.

[11] R. Jurca, and Faltings, B. (2003). "Towards Incentive-Compatible Reputation Management", In: Trust, reputation and security: theories and practice, Lecture Notes in AI, R. Falcone, S. Barber, L. Korba, & M. Singh, (Eds.), Springer-Verlag, Vol. 2631, 138–147, 2003.

[12] T. Tran, "Reputation-Oriented Reinforcement Learning Strategies for Economically-Motivated Agents in Electronic Market Environment", Ph.D. Dissertation, University of Waterloo, 2003.

[13] K. Regan, and R. Cohen, "A Model of Indirect Reputation Assessment for Adaptive Buying Agents in Electronic Markets", Business Agents and the Semantic Web (BASeWEB), May 2005.

[14] R.H. Guttman and P. Maes, "Agent-mediated Electronic Commerce: A Survey", The Knowledge Engineering Review, Vol. 13(2), 147-159, 1998.

[15] P. Maes, "Artificial Life Meets Entertainment: Life like Autonomous Agents," Communications of the ACM, Vol. 38(11), 108-114, 1995.

[16] A. Abdul-Rahman and S. Hailes, "Supporting Trust in Virtual Communities", Proc. Hawaii International Conference on System Sciences, Maui, Hawaii, 2000.

[17] C. Dellarocas, "Towards Incentive-compatible Reputation Management", Workshop on Deception, Fraud and Trust in Agent Societies, Bologna, Italy, 26–40, 2002.

[18] M. Wooldridge and N. Jennings, "Intelligent Agents: Theory and Practice", The Knowledge Engineering Review, Vol. 10(2), 115-152, 1995.

[19] EBay, www.ebay.com .

[20] R.B Doorenbos, O. Etzioni, and D. Weld, "A Scalable Comparison-Shopping Agent for the World Wide Web", First Int. Conf. on Autonomous Agents, 39- 48, 1997.

[21] P. Maes, R.H. Guttman, and A.G. Moukas, "Agents that Buy and Sell", Communications of the ACM, Vol. 42(3), 81-91, 1999.

[22] B. Esfandiari and S. Chandrasekharan, "On How Agents Make Friends: Mechanisms for Trust Acquisition", Proc. of the Fifth Int. Conf. on Autonomous Agents Workshop on Deception, Fraud and Trust in Agent Societies, 27-34, 2001.

[23] J. Carbo, J. Molina, and J. Davila, "Comparing Predictions of SPORAS vs. a Fuzzy Reputation Agent System", Third Int .l Conf. on Fuzzy Sets and Fuzzy Systems, Interlaken, 147–153, 2002.

[24] D. Huynh, N.R. Jennings, and N.R. Shadbolt, "Developing an Integrated Trust and Reputation Model for Open Multi-Agent Systems", Proc. of 7th Int. Workshop on Trust in Agent Societies, 65-74, New York, USA, 2004.

[25] Amazon, www.amazon.com .

[26] C. Goldman, S. Kraus, and O. Shehory, "Equilibria Strategies for Selecting Sellers and Satisfying Buyers," In: Lecture Notes in Artificial Intelligence, M. Klusch and F. Zambonelli (Eds.), Springer, Vol. 2182, 166-177, 2001.

[27] J. Carter, E. Bitting, and A. Ghorbani, "Reputation Formalization for an Information-Sharing Multi-Agent System", Computational Intelligence, Vol. 18(2), 515–534, 2002.

[28] T.D. Huynh, N.R. Jennings, and N.R. Shadbolt, "An Integrated Trust and Reputation Model for Open Multi-Agent Systems", Autonomous Agents and Multi-Agent Systems, Vol. 13(2), 119-154, Sep. 2006.

[29] S. Marsh, "Formalizing Trust as a Computational Concept", Ph.D. Thesis, Department of Mathematics and Computer Science, University of Stirling, 1994.

[30] B. Yu and M.P. Singh, "A Social Mechanism of Reputation Management in Electronic Communities", Cooperative Information Agents (CIA), Vol. 24, 154-165, Boston, USA, 2000.

[31] T. Grandison, and M. Sloman, "A Survey of Trust in Internet Application", IEEE Communications Surveys, Vol. 4(4), 2-16, 2000.

[32] Y. Mass, and O. Shehory, " Distributed Trust in Open Multi-Agent Systems", In: Trust in cyber-societies, R. Falcone, M. Singh, & Y. Tan, (Eds.), Springer-Verlag, 159–173, 2001.

[33] C. Castelfranchi, and R. Falcone, "Principles of Trust for MAS: Cognitive Anatomy, Social Importance, and Quantification", Proc. of the Intel Conf. on Multi-Agent Systems (ICMAS'98), Paris, France, 72–79, 1998.

[34] A. Greenwald and J. Kephart, "Shopbots and Pricebots", Proc. of the Sixteenth Int. Joint Conf . on Artificial Intelligence, Vol. 1, 506-511, 1999

[35] G. Zacharia and P. Maes, "Trust Management through Reputation Mechanisms", Applied Artificial Intelligence, Vol. 14(9), 881-907, 2000

[36] A. Chavez and P. Maes, "Kasbah: An Agent Marketplace for Buying and Selling Goods", First Int. Conf. on the Practical Application of Intelligent Agents and Multi-Agent Technology, London, UK, 1996.

[37] J. Sabater and C. Sierra " REGRET: A Reputation Model for Gregarious Societies", Proc. of the Fifth Int. Conf. on Autonomous Agents, Montreal, Canada, 194-195, 2001.

[38] T. Sandholm, "Distributed Rational Decision Making", In: Multi-Agent Systems: A Modern Approach to Distributed Artificial Intelligence, Weiss, G. (ed.), MIT Press, 1999.

[39] J. Sabater and C. Sierra, "Review on Computational Trust and Reputation Models", Artificial Intelligence Review, Vol. 24(1), 33-60, 2005

[40] M. Schillo, M. Rovatsos, and P. Funk, " Using Trust for Detecting Deceitful Agents in Artificial Societies", Special Issue of the Applied Artificial Intelligence Journal on Deception, Fraud and Trust in Agent Societies, Vol.14(8), 825–848, 2000.