FUTURE TRUST FORECAST IN OPEN MOBILE AGENT ENVIRONMENT

Kłopotek A. Mieczysław
Institute of Computer Science, Polish Academy of Sciences, ul. J.K. Ordona 21, 01-237 Warszawa, Poland

Wolski Michał
Institute of Computer Science, University of Podlasie, ul. Sienkiewicza 51, 08-110 Siedlce, Poland

Keywords: Mobile agents, open environment reputation, simulation, trust.

Abstract: Open Mobile Agent Environments, where entities can join and leave the system at any time, are particularly susceptible to the attacks of malicious entities. Hence intense studies of potential solutions of related problems are needed, including proper and speedy estimation of node's trustworthiness. We propose an optimisation method for trust estimation (reputation forecasting) and apply it to two known reputation metrics (eBay and BetaSystem). We show results of simulations comparing the effectiveness of reputation discovery using the original algorithm and the optimized (forecasting reputation) one.

1 INTRODUCTION

Reputation mechanisms allow agents to establish trust in other agents' intentions and capabilities in the absence of direct interactions. In the context of e-commerce, the parties involved in mutual interactions may publicly rate their trading partner in terms of his compliance to the terms of trade (e.g. on eBay or Yahoo! Auctions). This benefits other, new agents considering interacting with those partners, who would otherwise have no idea about their trustworthiness. Reputation systems are an important building block for achieving trust within large distributed communities, especially when mutually unknown agents engage in ad-hoc transactions. In this article we present design of Open Mobile Agent's Environment Simulator and simulation results obtained with that tool. To demonstrate simulator features, we compare by simulation known reputations metrics (eBay and BetaSystem) algorithms and a new trust optimization algorithm (FutureTrust) that is dedicated especially to Open Mobile Agent's Environment, with respect to their efficiency in identifying trustworthiness of nodes.

2 OPEN ENVIRMONEMT ISSUES

Expansion of mobile agents software is due to the business requirements that need software which will co-operate with each other without early coordination. Hence agent has to have a trust to other agents before he begins transaction.

By trust we (or symmetrically, distrust) mean "... a particular level of the subjective probability with which an agent will perform a particular action, both before he can monitor such action (or independently of his capacity to monitor it) and in a context in which it affects his own action."(Misztal, 2004).

In large-scale open distributed systems, trust remains a fundamental challenge for the success of their operation. When we use Open Mobile Agent's Environment we think about scenarios like:

- system open in that agents can enter and leave at any time. This means that an agent could change its identity on re-entering and avoid punishment for any past wrongdoing.
- system that allows agents with different characteristics (for example, policies, abilities, roles) to enter it and interact with each other (Ramchurn and Jennings, 2004)

A. Mieczysław K. and Michał W. (2007).
FUTURE TRUST FORECAST IN OPEN MOBILE AGENT ENVIRONMENT.
In *Proceedings of the Third International Conference on Web Information Systems and Technologies - Internet Technology*, pages 353-356
DOI: 10.5220/0001271003530356

- no agent can know everything about its environment (Huynh and Jennings, 2006).

Co-operation without early coordination implies that agent has to have a trust to other agents and to the infrastructure before he begins transaction.

During his journey agent can interact with each of nodes and learn their behaviour over a number of encounters. This knowledge has to be memorized.

The agent faces challenges like:

- unknown network topology,
- evil (hostile) nodes damaging agents

An agent cannot cope with these issues alone, communities have to be formed. To simplify the problem, we assume that families of agents (agents that can fully trust one another, if meeting on a trusted node and sharing a common repository on trusted nodes) are sent out into an open environment. The problems of mobile agent trust and security in open environment are of extreme complexity. In this part of our research we skip communication problem between two or more agents and between agent and common repository. At this moment let us devote our attention only to reputation metrics.

While trusting one another, the family members have to evaluate appropriately the trust they may have to the environment. A number of potentially suitable global reputation systems, such as eBay, BetaSystem (Jøsang and Ismail, 2002), and local ones like EigenTrust (Kamvar and Schlosser, 2003), Sporas (Zacharia and Maes, 2000) have been elaborated, while other are under development. Comparative studies of usefulness of these metrics are needed and some tools have been elaborated for such analyses. Complex comparison of various metrics can be found in (Schlosser and Andreas, 2005). However, the testbed for metrics presented there is not suitable for our purposes of study of open environments, hence we built a Mobile Agents Reputation Simulator (MARS) which is a useful tool to compare global reputation systems (Wolski and Klopotek, 2006).

3 SIMULATIONS

In our research we test the effectiveness of trust algorithms by simulating an environment adhering to some predefined model, which is unknown for agents. Agents move from one node to another. During his journey an agent interacts with nodes and learns their behaviour over a number of encounters. Knowledge about node behavior will have to be stored in common repository, in form of a "reputation level", which is then compared to the "intrinsic" one (the one from the predefined simulation model).

In this paper we investigate with our simulator two of them: eBay Algorithm and BetaSystem Algorithm, which will be subject to our optimization (FutureTrust). Each algorithm has been tested on the same network, created in a random way, with topological features similar to the Internet.

We investigated networks consisting of :

- good nodes, which have attractive information for agents,
- neutral nodes, which have nothing interesting for agents,
- evil (bad, hostile) nodes, which destroy agent in case of interaction between agent and node.

We experimented with four node groups: good node family, neutral node family, and a random node family, composed of a mixture of nodes described in the previous three groups. Last one is variable node family, which consisted nodes which are very unstable. They change dynamically their behavior to towards visiting agents with each encounter. Behavior of "variable" nodes is based on normal distribution and is random with probability equal 0.33 for each kind of behavior.

3.1 BetaSystem and eBay Algorithm

First trust metrics, that we investigated, is well known eBay algorithm, which needs to maintain information on good and all transactions.

The next one was the Bayesian Reputation System called BetaSystem, allowing each agent to rate node positively or negatively (Jøsang and Ismail, 2002). In our simulations positive ratting is given to good nodes, and negative ratting is obtained by neutral and bad nodes.

3.2 FutureTrust Algorithm

Our agents have common repository, that means if one of agents has a good transaction each agent of a family will know about it. If a second agent has good transaction with particular nodes we can forecast that next agent will good transaction too. If so, we can construct a metric exploiting foreseen trust values in some iterations in the future.

In our research we consolidate known reputation metrics with stochastic process, which can tell us forecast reputation with particular probability in defined time in future. We sought to minimize risk relevant with forecasting of trust value and we want to answer to question: "What trust value will have this family of node's in the next iteration, next 10, 100 iterations?" To come to a solution we use two simplifying assumptions:

- trust value is similar to random walk, with reputation in short time period being a random variable with normal distribution
- for any time in the future reputation has log-normal distribution character.

Based on log-normal distribution we can forecast future value of trust (equation 1)

$$\ln(R_T) \approx \phi[\ln(R) + \mu \cdot T, \mu\sqrt{T}] \qquad (1)$$

where: T – time (number of iterations)

R – present reputations (enumerated by known trust metrics)

R_T – future reputation (in T iterations)

μ – variable responsibility for fluctuation of trust metrics

To compute future trust value we have to store information about positive and negative transactions in an incremental table.

Based on equation 1 we compute FutureTrust as (equation 2)

$$R_T = e^{\ln(R)+\mu\cdot T+c\cdot\mu\sqrt{T}} \, for \sum bad < \sum good$$

$$R_T = e^{\ln(R)+\mu\cdot T-c\cdot\mu\sqrt{T}} \, for \sum bad > \sum good \quad (2)$$

Where c – value of standard deviations (e.g. if μ=95% then c=1.96)

3.3 Comparison of Algorithms

Subsequent figures are representative to all experiments. We can see, that agents need time to learn node family trust estimate. For the small network we used (about 1000 nodes), the number of iterations (equal to the number of transactions of each surviving agent) needed by any algorithm was at most 30.

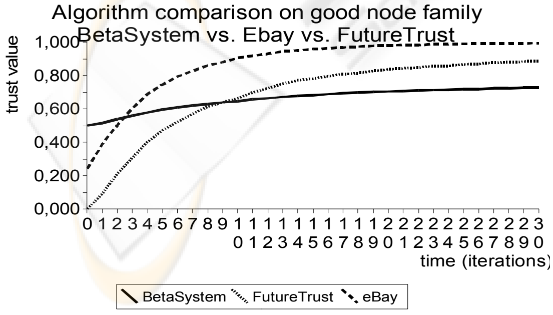

Figure 1: Algorithm comparison for good node family.

We assume that the best reputation algorithm is that one, which allows to set faster the correct value of trust for particular family of nodes.

On next figures we present a comparison between the basic algorithm version and the FutureTrust modifier. The FutureTrust parameters were set to: T = 50 (iterations) and μ = 0.01 - 1% changes of reputation.

First comparison refers to good nodes family. Figure 1 shows that eBay algorithm is very fast to recognize true reputation of node family.

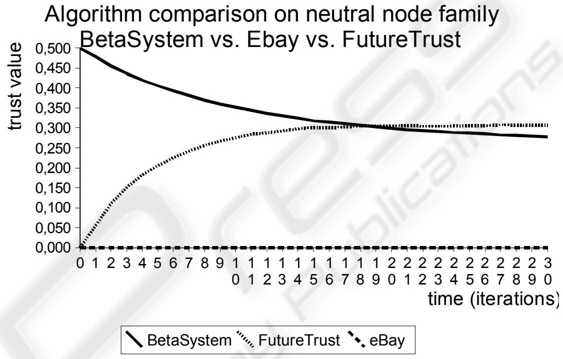

Figure 2: Algorithm comparison for neutral node family.

Figure 2 presents results for the second group of nodes: neutral one. We think that in that case the best algorithm is FutureTrust algorithm, because it is growing up to correct value of trust. Instead eBay algorithm is worthless because it doesn't notice any value.

Next family of nodes is the random family. This family is built of three types of nodes: good, neutral, evil and have constant structure of behaviour. It means node never changed their behaviour to any agents.

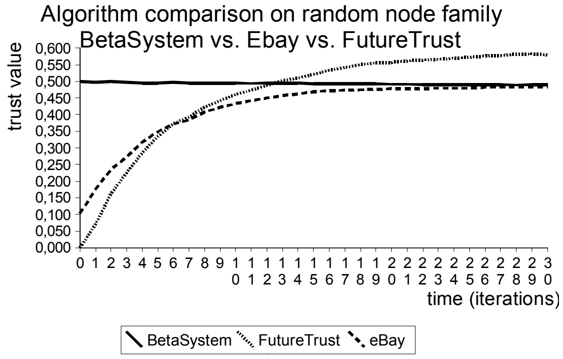

Figure 3: Algorithm comparison for random node family.

In that case the best algorithm is FutureTrust because its value of reputation for this kind of family is set to correct value faster than other algorithms.

Last but not least node family is the variable node family. It is very similar to random node family but the main difference is that in variable family each node always changes its behavior to agents.

In that part of our research we make assumption that three types of behavior of nodes (good, neutral, evil) switch with probability equal 0.333.

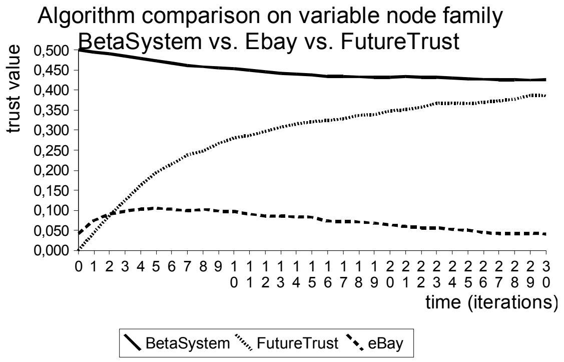

Figure 4: Algorithm comparison for variable node family.

Figures 4 demonstrates that in that case the best algorithm is BetaSystem or Future Trust algorithm, because only these algorithms set correct value of trust for the family.

Above figures show that assignment of forecast value of trust based on known metrics (equation 2) allows to reduce the number of iterations, which are needed to correctly recognize true reputation of nodes family.

It means, if we are forecasting future value of trust we can get benefits such us:

- faster recognition of true reputation of nodes,
- less cost of agents function,
- less load of agents system,
- less consumption of memory, where we store information about network.

4 CONCLUSION

In this paper we investigated some problems encountered when computing reputation in open environment. We reported on a comparative study two known metrics eBay and BetaSystem and our own based on future trust optimization.

We pointed at the very important problem of speed of recognition of intrinsic reputation for a family of nodes and demonstrated that our innovative technique based on forecasting trust value offers a solution.

We showed that usage of the FutureTrust optimization formula can reduce significantly the cost of computations related to trust determination.

While the current paper concentrates on trust estimation, a more important issue is to device a mechanism that allows exploration of only most trusted part of network so that agents can collect information (resources) faster. Beside this, in our future research we will check what happens when some nodes will clone or change a mobile agent and how different ways of mobile agents interaction with the common repository will have influence on reputation value in particular node family.

REFERENCES

Huynh D., Jennings N.R., Shadbolt N.R.: *An integrated trust and reputation model for open multi-agent systems*, Autonomous Agents and Multi-Agent Systems, Issue: Volume 13, Number 2, September 2006

Jøsang A. and Ismail R. *The Beta Reputation System*. In Proceedings of the 15th Bled Conference on Electronic Commerce, Bled, Slovenia, 17-19 June 2002,

Kamvar S. D., Schlosser M. T., Garcia-Molina H. :*The Eigentrust Algorithm for Reputation Management in P2P Networks*, (http://dbpubs.stanford.edu), 2003

Kłopotek M. A., Wolski M.: *Comparative Study of Trust Algorithms for Mobile Agent in Open Environment*, Proceedings of Artificial Intelligence Studies Vol.3, (26)/2006, pp 213-220

Misztal, B.: *Trust in Modern Societies*, Polity Press, Cambridge, Mass., (1996)

Ramchurn S.D., Jennings N. R.: *Trust in agent-based software*, Cyber Trust & Crime Prevention Project, 2004

Schlosser, Andreas, Voss, Marco and Brückner, *On the Simulation of Global Reputation Systems*. Journal of Artificial Societies and Social Simulation, Lars 2005

Wolski M. Kłopotek M.A.: *A Concept of Reputation for Mobile Agents Environments*, chapter in Polish Journal of Environmental Studies Vol. 15, No. 4C, 2006, pp. 207-211, ISSN 1230-1485, Świnoujście 2006

Zacharia G. and Maes P.: *Trust Management through Reputation Mechanisms*. Applied Artificial Intelligence, 14, 2000.