Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 5 (2011) 181–189

Procedia Computer Science

The 2nd International Conference on Ambient Systems, Networks and Technologies (ANT)

Collusion-Resistant Reputation Mechanism for Multi-Agents Systems

Babak Khosravifar[a], Jamal Bentahar[a,]a*, Mahsa Alishahi[a], Maziar Gomrokchi[a]

[a] *Concordia University, 1515 Ste-Catherine Street West, EV7.640, Montreal H3G 2W1, Canada*

Abstract

We address the collusion problem in a reputation-driven multi-agent system where agents represent service providers, consumers, and a controller. A game structure is proposed where players are supposed rational and payoff maximizers. The main issue addressed in this paper is how to maintain a collusion-resistant reputation mechanism. We analyze the behavior of different players with respect to the strategies adopted by the opponents. We provide theoretical analysis of the game and discuss the pure and mixed strategy Nash equilibrium along with best response analysis to identify conditions under which the players adopt truthful dominant strategies.

Keywords: reputation, multi-agent systems, game-theory;

1. Introduction

In multi-agent systems (MASs), establishing reputation is a must, and in the recent years different approaches to reputation have been proposed. Reputation is addressed by aggregating related parameters from different perspectives [1]. One important issue is the agents' tendency to act maliciously to take advantage of the system's vulnerability, which can be done by colluding with other agents. There have been some efforts addressing collusion resistance in reputation frameworks [1, 2]. However, some issues such as false alarms are yet to be addressed. In many existing frameworks, the malicious actions and collusion could be maintained by agents at any time (never end). A missing factor in these approaches is convergence towards a truthful setting. In this paper, the conditions that lead to this convergence are investigated using a game structure.

In this paper, we consider a network of providers and consumers, which are equipped with mechanisms capable of maximizing their payoffs. The proposed framework also contains a controller agent whose responsibility is to make the system trustful. A consumer agent is a rational service consumer that initiates

* Corresponding author. Tel.: +1 514 848 2424.5382; fax: +1 514 848 7131.
E-mail address: benthar@ciise.concordia.ca.

Selection and/or peer-review under responsibility of Prof. Elhadi Shakshuki and Prof. Muhammad Younas.
doi:10.1016/j.procs.2011.07.025

requests hoping to obtain an acceptable quality of service (QoS). There is a reputation mechanism that regulates the process of consumers selecting providers by ranking them using their reputation. The controller agent denoted by Cg objectively maintains a sound reputation mechanism by taking the provider and consumer actions under surveillance. As a matter of fact, the Cg applies some penalties in order to discourage the providers and consumers from colluding and acting maliciously.

The proposed framework is distinguished from existing frameworks, for example [2, 3], in the fact that a continuous game involving three players (provider, consumer, and controller agent) is modeled and analyzed. In this framework, the collusion between providers and consumers is thoroughly discussed (skipped in similar proposals) and the role of Cg in maintaining a sound reputation mechanism is discussed in details. The results of the proposed framework could be summarized as follows: (1) by analyzing different situations, rational agents (providers and consumers) can recognize some restrictions that encourage them to choose the best response leading to their maximum expected payoffs; and (2) the game-theoretic analysis enables the reputation mechanism designer to compute a detection threshold so that if reached, the mechanism will be collusion-resistant. These results are confirmed by simulations.

The remainder of this paper is organized as follows. In Section 2, we define some preliminaries of our proposed framework. In Section 3, we provide a theoretical and empirically analysis of the reputation game (involving three agents but grouped into two players) and discuss some results regarding collusion resistant reputation mechanism based on the environment characteristics. We continue our discussions on the same direction of the theoretical analysis in the implemented environment and observe the impacts that environmental characteristics impose on agents' behaviors. Section 4 discusses related work and finally Section 5 concludes the paper.

2. The Model

This section points out the preliminaries regarding the proposed framework.

Involved Agents. In our proposed model, we consider n consumer agents $u_1 \dots u_m$ (a typical consumer agent is denoted by u), m provider agents $w_1 \dots w_m$ (a typical provider agent is denoted by w), and a controller agent Cg. Each consumer agent u has a budget account in the system from which his requested services are paid and is equipped with a purchase mechanism that enables him to initiate a service request from a provider w specifying some buying parameters such as response time and price. Each provider agent w is characterized by his reputation, which affects his income in the system since the number of requests he can receive is reputation-dependant. He is also equipped with a selling mechanism that enables him to dynamically set up the selling parameters (response time and price) according to which a service is offered to the consumer agent u. The controller Cg is equipped with a supervision mechanism that enables him to investigate the truthfulness of the interactions among the involved agents and has access to the consumers' accounts and providers' reputations.

Reputation Mechanism. The typical agent u posts a feedback f reflecting the extent to which the offered service by the provider agent (say w) is satisfactory. The feedback f belongs to the interval [-1; 1], where -1; 0; +1 respectively represent complete dissatisfaction, no answer from the provider, and complete satisfaction. The accumulated feedback (posted by different consumers over time) is used to compute the reputation value of providers. There are a number of frameworks [1, 4] that address the reputation assessment problem ranging from simple mean values to more sophisticated distributions. However, the way the reputation is computed does not have impacts on our results. In fact, we are mainly interested in fraud in the feedback pool. Since choosing a service from the network of services is very selective, provider agents compete to increase their reputation (which is supposed to bring more requests from consumers). In our model, the agent Cg is responsible for investigating the feedback pool to capture malicious actions. What we mean by fraud is that a provider agent w can collude with one or many consumer agents to support him by posting faked positive feedback, which would increase w's reputation.

Consumer-Provider Strategy Profile. The consumer and provider agents follow 2 strategies: being truthful or malicious. In the truthful strategy, the provider provides the service and consumer posts the corresponding truthful feedback to the feedback pool. In the malicious strategy, the provider provides incentives (ε) to some consumers to motivate them providing continuous positive feedback even without receiving a service. Colluding with a consumer is aimed at increasing self reputation. This leads to increase provider's market share and thus obtain higher income. Other malicious strategies are possible such as decreasing competitors' reputation. However, to make the paper focused, we only consider the first possibility in this paper.

Collusion Scenario. To better analyze the game, it is worthy to explain the collusion scenario in details. The collusion we take into account in this paper could be triggered by either the providers or the consumers. But to be consistent and more realistic in our discussions, we only consider the trigger from the consumer. The reason behind this is the fact that the consumer is the one that receives incentive and high quality service. Therefore, he is more amenable to collusion [5]. As discussed in advance in this section, the provider aims to increase his reputation to obtain more requests. Besides acting truthfully and gaining positive feedback, the reputation increase could be caused by motivating a consumer to post a number of continuous positive feedback. For simplicity, we skip the process of malicious consumer finding the malicious provider (in order to complete the collusion). Recall w and u, respectively as malicious provider and consumer. To make the scenario simple but without losing generality, let us consider only one provider w colluding with one consumer u (the generalization to n consumers is straightforward). The collusion agreement established between w and u clarifies the number of fake positive feedback that u is going to post for w. Associated with the feedback pool is a window that represents a number, publicly known, of feedback that is accumulated in a fixed period of time, for instance an hour or a day. In this scenario, f_w is the percentage of this window that represents the fake positive feedback the consumer would post. Consequently, the provider receives f_w percentage increase on his positive feedback. Therefore, his reputation increases and thus, the expected number of requests increases as well (we will use ψ to denote the percentage of this increase). In this case, the malicious consumer would receive the amount of ε as incentive from the provider. This amount (i.e. ε) should be less than the amount gained by the provider ($\lambda_w \beta \psi$, where λ_w represents the mean request number in the fixed period of time relative to the window, and β denotes the price charged by w for offering the service) in the case of adopting the collusion strategy. Therefore, the provider always predicts the expected income before motivating a consumer to adopt the collusion.

Controller-Provider/Consumer Connection. The controller agent Cg continuously investigates the feedback pool and his detection strategy is based on applying some dynamically changing thresholds (this aspect is detailed in Section3.2). Associated with the feedback pool is a fixed size window that Cg considers in his investigation. The parameter w_c represents the percentage of this fixed size window that Cg is going to analyze. The value w_c would differ over time and the provider and consumer agents need to estimate or predict it when deciding about their strategies of acting truthfully or maliciously. The detection probability reflects the controller agent's accuracy in investigating the feedback pool. This probability could be increased over time when Cg applies some learning mechanisms to use information from past detections in the current investigation. Since the detection procedure does not affect the results of this paper, we only focus on the role of the parameter w_c. After deciding to penalize the collusion, Cg notifies both the provider and consumer by sending them a report revealing the parameters regarding the penalty process such as the considered window parameter w_c and the percentage df_c of detected fake feedback (explained in the following).

Four possibilities can be analyzed:

- Cg detects the actual collusion and gets +π as payoff. We consider the parameter D_c as the accuracy of detection. In analyzing the feedback pool within the window percentage w_c, Cg catches a percentage of this w_c, denoted by df_c, as the fake feedback and the assigned penalty ($(df_c/w_c)Pn$) to both the

provider and consumer is proportional to the detected fake feedback, where the public parameter Pn represents a maximum penalty assigned by Cg. When it affects the consumer, the penalty is applied to his budget (money is taken from his budget account in the system), and when it affects the provider, the penalty concerns his reputation, which then affects his income since the number of received requests will decrease. In this case, the report sent to both the provider and consumer reveals df_c and w_c.

- Cg ignores the actual collusion and gets -π as payoff. This is the worst case because the malicious provider increases his reputation and the malicious consumer receives the inventive of ε. This case, called false positive, decreases Cg's accuracy in detection.
- Cg detects the truthful action as collusion and gets -π as payoff. This is also harmful in the sense that the truthful provider is losing his reputation and the truthful consumer is losing money because of Cg's mistake. This is the case of false negative that negatively affects the Cg's accuracy.
- Cg ignores the truthful actions and gets + π as payoff. Socially speaking, this corresponds to the best situation, and the objective is to encourage all the players to converge towards such a situation.

3. Theoretical Analysis

There are important details in this game. It is worthy to note that the stage game is the example of a typical moment considering three particular players, which is generalized to a repeated game between all interacting agents. Information obtained from each stage game is used in the rest of agent's involved games. In this framework, we focus on identifying the optimum status where the collusion is discouraged at best. To have a better analysis on the payoffs of different players, we consider the situation where the provider and consumer act truthfully and the controller agent ignores the reaction as the ideal case. Therefore, in all the payoffs analysis in the rest of this section, we consider each payoff as the difference of the expected outcome of the chosen case with the ideal case. The expected gain/loss is computed using the variables that have been obtained in the past reports, such as the feedback window parameter w_c and the detected fake feedback df_c. If there is no past report on collusion, we assume the existence of default values that the provider (who has never been penalized) would use to analyze the expected payoffs.

If the collusion is detected, the controller agent penalizes the malicious provider and consumer, which would cause $(df_c/w_c)Pn\,\lambda_w\beta$ money loss for the provider and $(df_c/w_c)Pn$ money loss for the consumer. Therefore, the payoff of the provider would be $-(df_c/w_c)Pn\,\lambda_w\beta$ and of the consumer would be $-(df_c/w_c)Pn$ for the case where the collusion was actually made, and $-(\overline{df_c}/w_c)Pn\,\lambda_w\beta$ and $-(\overline{df_c}/w_c)Pn$ for the case where the controller has falsely considered the truth action as collusion. In this case, $\overline{df_c}$ is considered by the provider as the percentage of falsely detected rightful feedback. These values are previously reported by the controller agent in the penalty report. In case the collusion is ignored, the expected payoff for the provider would be the gained fee over the extra requests minus the incentive given to the consumer $\lambda_w\beta\psi - \varepsilon$ (recall that λ_w, ψ, β respectively represent the mean request sent to w, reputation increase amount as a result of collusion, and service fee charged by the provider). This case would bring $+\varepsilon$ for the consumer. Finally the case where the provider and consumer act truthfully, they both expect 0, which corresponds to the default case.

3.1. Analysis of the Pure Strategy Nash Equilibrium (PSNE)

Considering the payoffs shown in Table 1, the group 1 is Cg and the group 2 is formed by provider w and consumer u. In pure strategy Nash equilibrium, w and u would consider to collude when the obtained payoff is more than the one obtained in the case of acting truthfully. In the case where Cg ignores the collusion, obviously this collusion brings more payoffs ($\lambda_w\beta\psi - \varepsilon > 0$ for w and $\varepsilon > 0$ for u). However, if

Cg penalizes and if the obtained payoff is more in the collusion case, the group 2 would choose the collusion as the dominant strategy.

Table 1. Payoff table of 3 players in 2 groups

Group 2 (w & u) Truthful Collusion	Group 1 (Cg): Penalize	Group 1 (Cg): Ignore
	$+\pi$ $-(df_c/w_c)P_n\lambda_w\beta$, $-(df_c/w_c)P_n$	$-\pi$ $\lambda_w\beta\psi-\varepsilon$, ε
	$-\pi$ $-(\overline{df_c}/w_c)P_n\lambda_w\beta$,$-(\overline{df_c}/w_c)P_n$	$+\pi$ 0, 0

Proposition 1. In the repeated game of the stage game described above, if the falsely detected rightful feedback $\overline{df_c}$ (reported by Cg) is more than the correctly detected fake feedback df_c, the provider and consumer would choose the collusion as the dominant strategy.

Proof. In this repeated game, the payoffs are the summation of stage game payoffs, so since

$$\overline{df_c} > df_c, \sum_\infty \lambda_w \psi\beta - \varepsilon > 0, \sum_\infty \varepsilon > 0$$

$$\sum_\infty(-df_c/w_c)Pn\lambda_w\beta > \sum_\infty(-\overline{df_c}/w_c)Pn\lambda_w\beta \; and \; \sum_\infty(-df_c/w_c)Pn > \sum_\infty(-\overline{df_c}/w_c)Pn$$

both w and u will always choose to collude whatever the strategy of Cg. ¤

The following corollary is a direct consequence of Proposition 1.

Corollary 1. In the repeated game of the stage game described above, if the falsely detected rightful feedback $\overline{df_c}$ is more than the correctly detected fake feedback df_c, penalizing the collusion is PSNE.

Fig.1 shows two simulation results confirming Proposition 1 and Corollary 1. The left graph illustrates successful detection (reflected by df_c) versus failure detection (reflected by $\overline{df_c}$) of a controller agent in a network containing 1000 consumer agents and 200 provider agents. The right graph plots the number of collusion versus the time (number of runs of the simulation), which reflects the overall tendency to act maliciously. In this graph, we observe that the number of collusion increases with $\overline{df_c}$ - df_c.

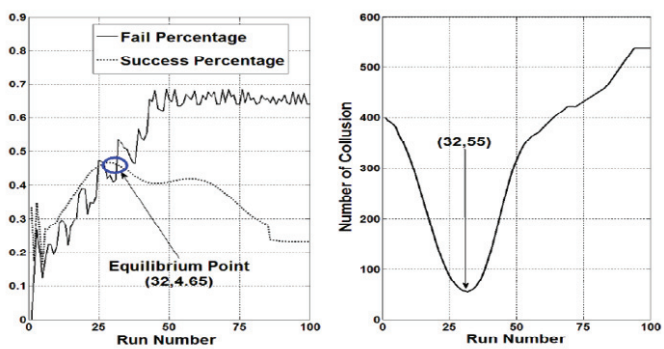

Fig. 1. Pure strategy Nash characteristics

In this game, staying in PSNE is, socially speaking, a harmful situation for all the players. Continuing on PSNE, both groups would lose their performances. In fact, the PSNE is achieved due to temporary analysis that players do aiming to maximize their payoffs without considering probabilities of detection. Therefore, we need to consider the case where the payoffs of the players in group 2 are subject to the accuracy of Cg and his detection probability. To analyze the details of this case, we need to consider the mixed strategy Nash equilibrium.

3.2. Analysis of the Mixed Strategy Nash Equilibrium (MSNE)

In the mixed strategy, we need to consider two probability distributions on the strategy profiles of the two groups of players (Cg and w & u). Let p be the probability of collusion, which is maintained by the provider and consumer. Therefore, 1-p is the probability of acting truthfully. The probability of collusion depends on many factors in the game. In fact, w and u would consider the Cg's accuracy of detection, window size, and expected payoffs before performing any action. Let q be the probability of Cg penalizing the malicious action and therefore, 1-q is the probability of ignoring the action. This probability should satisfy two properties: (1) it increases with the Cg's detection accuracy D_c, which evolves over time; and (2) it also increases with the quality of choosing w_c, the portion of the fixed size window that Cg is going to analyze. Equation 1 gives a definition of this probability that satisfies these properties. In this equation, f_w is the actual percentage of the fake feedback in the feedback pool. Notice that q ∈ [0; 1] since $0 \leq D_c$; $|w_c - f_w| \leq 1$. If the detection is completely wrong, then $|w_c - f_w| = 1$, and if it is completely correct, then $|w_c - f_w| = 0$, which means Cg is investigating a portion of feedback from the feedback pool where all of them are fake.

$$q = D_c(1 - |w_c - f_w|) \quad (1)$$

We define Cg.pro = (q, 1-q) as the probability distribution of the Cg's strategy profile and wu:pro = (p, 1-p) as the probability distribution of the strategy profile of group 2 players w and u. In the mixed strategy case, all the players need to estimate their expected payoffs with respect to their chosen strategies against the other player's probability distribution. Let Ew(C,Cg.pro) (resp. Ew(T,Cg.pro)) be the expected payoff of the provider choosing to collude (resp. to act truthfully) against the probability distribution of the controller agent. In the same way we define Eu(C,Cg.pro), Eu(T,Cg.pro), ECg(P,wu.pro) (P for penalizing) and ECg(I,wu.pro) (I for ignoring). We obtain the expected values as follows:

$$Ew(C, Cg.pro) = [(-df_c/w_c)\text{Pn}\lambda\_\text{w}\ \beta](q) + [\lambda_w \psi\beta - \varepsilon](1 - q) \quad (2)$$

$$Ew(T, Cg.pro) = \left[(\overline{\overline{-df_c}}/w_c)Pn\lambda_w\beta\right](q) + [0](1 - q) \quad (3)$$

$$Eu(C, Cg.pro) = [(-df_c/w_c)\text{Pn}](q) + [\varepsilon](1 - q) \quad (4)$$

$$Eu(T, Cg.pro) = \left[(\overline{\overline{-df_c}}/w_c)Pn\right](q) + [0](1 - q) \quad (5)$$

$$Ecg(P, wu.pro) = [+\pi](p) + [-\pi](1 - p) \quad (6)$$

$$Ecg(I, wu.pro) = [+\pi](p) + [-\pi](1 - p) \quad (7)$$

Best Response Analysis. All the players in this mixed strategy game aim at maximizing their payoffs. Therefore, for all their adopted strategies, we need to consider the best responses and discard the other strategies. For instance, the provider, who is seeking for maximizing his payoff by choosing a specific strategy, would discard any strategy in which his expected payoff is less than any other strategy. Since each player in each stage game chooses between only two strategies, and since any of these strategies could be the best response in a particular situation, we analyze the case where the expected payoffs are equal. By so doing, we can compute a threshold, which is used to identify which strategy is dominant. If these expected payoffs are not equal, that means one strategy would lead to a higher payoff and therefore,

the player would select that strategy as dominant. In this case, the mixed strategy probabilities would be (1,0) or (0,1), which is back to the pure strategy case.

The best response analysis in our mixed strategy game would enable the provider w and consumer u to obtain a probability threshold (μ) for their chosen strategy. Once the threshold is obtained, w and u would estimate the probability of the action to be chosen by Cg, and by comparing this probability with the threshold, they choose the best strategy that maximizes their payoffs. In the repeated mixed strategy game, w and u estimate the probability (denoted by q_w) that Cg penalizes their action based on previous detections. This probability should satisfy the same properties as for Equation1 and is computed in Equation 8. In this Equation, the accuracy of Cg is public, but the window parameter wc is considered as the window parameter that is reported to w and u in the most recent penalty report. The parameter f_w is also known to the provider and consumer. This probability could be compared against the obtained threshold μ by w and u to maximize their expected payoffs.

$$q=D_c(1-|\overline{w_c}-f_w|) \quad (8)$$

Theorem 1. In the mixed strategy repeated game, there is a threshold μ such that if $q_w > \mu$, acting truthfully is the dominant strategy for group 2. Otherwise, colluding is the dominant strategy.

Proof. We prove that the theorem holds for each stage game, so the repeated case follows. To find the dominant strategy for each stage game, we need to consider the case where the payoffs of the different strategies are the same. We have:

$$Ew(C,Cg.pro)=Ew(C,Cg.pro) => q_w=\mu_w=(\lambda_w\psi\beta-\varepsilon)/[(df_c-\overline{df_c})/w_cPn\lambda_w\beta+\lambda_w\psi\beta-\varepsilon]$$

$$Eu(C,Cg.pro)=Eu(C,Cg.pro) => q_w=\mu_u=(\varepsilon)/[(df_c-\overline{df_c})/w_cPn]$$

Let μ = max(μ_w , μ_u). If $q_w > \mu$, then Ew(C,Cg.pro) < Ew(T,Cg.pro) and Eu(C,Cg.pro) < Eu(T,Cg.pro), so the first part of the theorem follows, and the second part is straightforward. The threshold μ is the maximum of μ_w and μ_u (μ_w in case $2\varepsilon < \lambda_w\psi\beta$ and μ_u otherwise). ■

Corollary 2 that follows directly from Theorem 1 gives the the condition under which the MSNE is obtained.

Corollary 2. If the estimated probability of penalizing q_w exceeds the obtained threshold μ, then acting truthfully by w and u and being ignored by Cg is a MSNE.

Theorem 2. A collusion-resistant reputation mechanism is achieved when the controller agent maximizes the value of $((df_c-\overline{df_c})/w_c)Pn$.

Proof. From Theorem 1, we deduce that since $q_w \in [0, 1]$, if $\mu \geq 1$, then collusion would be the dominant strategy for the provider and consumer. From proof of Theorem 1, $\mu \geq 1$ occurs when $\overline{df_c} \geq df_c$. Therefore, to have a collusion-resistant mechanism, Cg would aim at minimizing the threshold μ used by the opponents since the estimated probability of penalizing is compared to this threshold. According to Theorem 1, to minimize μ in both cases, Cg has to maximize the value at the denominator $((df_c-\overline{df_c})/w_c)Pn$ as all the other factors are out of Cg's control. ■

In the repeated game, Cg has to consider the best window factor w_c that corresponds to the fake feedback submitted to the feedback pool. The value of w_c could be learned by Cg over time (while the detection accuracy D_c also increases over time). However, finding the best w_c is not guaranteed since there is always a risk of different fake feedback percentage maintained by the provider and consumer as a result of collusion agreement. Therefore, there is always a risk of false negative in penalizing the provider and consumer.

4. Related Work

We consider two groups of frameworks related to our proposed model. The first group is about approaches that have been proposed for reputation assessment in MAS. Maximilien and Singh [1, 8] provided a complete overview regarding the parameters required to evaluate an agent's reputation. Vogiatzis et al. [4] proposed a probabilistic model for computing the trust and reputation of rational agents in MAS. They proposed a set of assumptions that enable recognizing the agents that change their behavior to estimate their rates of change. Recently, Chapman et al. [6] developed a unified analytical framework for distributed agents investigating the best response with respect to sequential optimization problems, which consist of state evaluation, decision rule, and adjustment schedule procedures. Doing so, agents analyze the best response, which leads to their maximum payoff. In [9] J. Witkowski presents a reputation mechanism that elicits honest feedback in a Markov setting and requires a lower budget than the equivalent fixed setting. The objective is to show that hidden Markov models (HMM) provide a payment scheme that elicits honest reports from the agents after they have experienced the quality of the service. In general, honest reporting would cause the unique Nash equilibrium in induced game. A limitation of this setting is the high amount of common knowledge. Therefore, the collusion issue is not addressed in this work.

The second group includes approaches proposed to develop sound reputation mechanisms, where entities are encouraged to act truthfully [3, 5, 7, 10]. Khosravifar et al. [7, 10] developed a game-theoretic approach categorized in one-shot and repeated games to emphasize the learning mechanism used by the agents, which leads them favor truth telling. Kastidou et al. [3] developed a framework representing safe information exchange regarding reputation assessment and agents are motivated to honestly report reputation information. All these approaches aim at maintaining a sound reputation mechanism according to aggregation frameworks similar to the ones proposed in the first group. However, these frameworks consider scenarios where only a part of the network (either the provider or consumer) play important role, which reflect partial collusion, i.e. only between agents of the same type. We believe that in dynamic MAS, a sound reputation system should consider the benefits of all the players.

The closest model to our work is the collusion-resistant reputation mechanism proposed in [2] in which the authors investigate incentive-compatible payment mechanisms. Malicious agents' behaviors are analyzed in different scenarios to maintain an automated mechanism design that yields the best reputation assessment in the environment. The proposed mechanism is limited in the sense that it is based on a linear optimization setting that do not perform well in specific situations like when false alarms are generated through the reputation mechanism. In general, the reputation mechanism is assumed to function correctly, which makes lying a Nash equilibrium at some point. In our paper, we investigate the collusion and address the collusion-resistant setting under the assumption that the controller agent is also making mistakes. This overall encourages the provider and consumer agents to analyze the characteristics of the controller through the collusion reports sent to them.

5. Conclusion

The contribution of this paper is the proposition of a collusion-resistant reputation mechanism applicable to multi agent settings. The reputation mechanism is supervised by a controller agent that reveals the reputation value of provider agents to the consumers. The proposed approach investigates the settings under which the truth action is the Nash equilibrium. In the game-theoretic analysis, rational agents compute their expected payoff and according to the available information from past events in the game, they decide about their further actions. The objective of the controller agent is to update the settings such that the truth action yields the maximum gain for the provider and consumer agents. Our model is distinguished from related work in the sense that a game-theoretic (followed by empirical)

analysis considering all the agents that are involved in the reputation mechanism is provided together with its aggregation process. Moreover, false alarms generated by the controller agent are also considered by the providers and consumers in their strategies and being investigated in experiments.

Our plan for future work is to integrate optimization techniques to our game and investigate in details the best value for w_c, which potentially impacts the expected payoffs computed by the provider and consumer agents. We also need to analyze in depth the scenario where some providers can collude to destroy the reputation of others by causing false alarms generated by the controller.

References

[1] E. M. Maximilien, M. P. Singh, Conceptual model of web service reputation, SIGMOD Record, ACM Special Interest Group on Management of Data 31 (4) (2002.) 36–41.

[2] R. Jurca, B. Faltings, Collusion-resistant, incentive-compatible feedback payments, in: Proceeding of the ACM Conf. on E-Commerce, 2007, pp. 200–209.

[3] G. Kastidou, K. Larson, R. Cohen, Exchanging reputation information between communities: A payment-function approach, in: Proc. of the 21st International Joint Conference on Artificial Intelligence (IJCAI), 2009, pp. 195–200.

[4] G. Vogiatzis, I. MacGillivray, M. Chli, A probabilistic model for trust and reputation, in: Proceeding of 9'th International Conference on Authonomous Agent and Multi Agent Systems (AAMAS), 2010, pp. 225–232.

[5] R. Jurca, B. Faltings, W. Binder, Reliable QoS monitoring based on client feedback, in: Proceeding of the 16'th International World Wide Web Conference, 2007, pp. 1003–1011.

[6] A. Chapman, A. Rogers, N. Jennings, D. Leslie, A unifying framework for iterative approximate bestresponse algorithms for distributed constraint optimisation problems, Knowledge Engineering Review (in press).

[7] B. Khosravifar, J. Bentahar, A. Moazin, P. Thiran, On the reputation of agent-based web services, in: Proceeding of the 24'th Conference on Artificial Intelligence (AAAI), 2010, pp. 1352–1357.

[8] C. J. Hazard and M. P. Singh, An architectural approach to combining trust and reputation, in: Proceedings of the 13'th AAMAS Workshop on Trust in Agent Societies (Trust). May 2010.

[9] J. Witkowski, Eliciting honest reputation feedback in a Markov setting, in: Proceedings of the 21'st International Joint Conference on Artifical intelligence (IJCAI), 2009, pp. 330-335.

[10] B. Khosravifar, J. Bentahar, A. Moazin, P. Thiran, Analyzing communities of web services using incentives, in: International Journal of Web Services Research (IJWSR), 7 (3) 30-51, IGI Global.