Building a Trust-based Social Agent Network

Sarah N. Lim Choi Keung and Nathan Griffiths

Department of Computer Science
University of Warwick
Coventry CV4 7AL, United Kingdom
{slck, nathan}@dcs.warwick.ac.uk

Abstract. Agents evolving in a multi-agent system interact with one another to achieve their individual goals. In trust-based agent models, agents form a local view of their environment from their direct interactions, and base their interaction decisions on the trustworthiness of the other agents. Agents can also obtain recommendations about other agents from third parties, either directly or indirectly. Reputation complements trust from direct interactions in providing information for agent selection. While trust and reputation ensure that an agent selects and interacts with the most appropriate provider, we believe that the agent can learn about the agent relationships and interconnections at the same time. By building a network of agents it interacts with, and with information about interaction details, trustworthiness, recommendation chain and reputation, the agent is in a better position to extract emergent information, such as potential new customers, suppliers, its competitors and potentially collusive groups of agents. In this paper we propose a mechanism for agents to build a representation of their local environment based on direct interactions, trust and reputation.

1 Introduction

Agents in an open and dynamic multi-agent system (MAS) interact with a group of agents within their area of interest. For instance, in an e-supply chain for computer hardware, an agent representing a part-built computer manufacturer may only be interested in a number of suppliers for computer parts and customer agents. To ensure that it selects the most appropriate agents for interaction, an evaluator can use the concepts of trust and reputation to minimise the uncertainty associated with agent interactions. It gathers trust information from the direct interactions it has with agents. This can be supplemented with reputation information from third party agents when the direct trust information is insufficient or not available. Reputation information is built from both direct and indirect recommendations along a recommendation chain.

We focus on the links that are formed when an evaluator interacts with other agents, both for service provision and recommendations. From direct interactions and direct recommendations, the evaluator has a local view of its environment. By further knowing who is involved in giving indirect recommendations along a recommendation chain, the evaluator can obtain an extended view of its environment. Together with information related to the strength of agent relationships, trustworthiness, reputation, experience and recency of interactions, the evaluator can deduce emergent information that is valuable

for future transactions. Emergent information includes the knowledge of potential new customers, new suppliers, who are its competitors and which group of agents are colluding.

The main contributions of this paper are: (i) describing how agents can build an extended view of their local environment, based on trust and reputation, and (ii) proposing potential uses of the emergent information that can be extracted from the extended view of the agent environment. The remaining parts of this paper are organised as follows. Section 2 outlines the related work in the areas of trust and agent networks and in collusion detection as a possible application of the emergent information from the agent network. In Section 3, we describe our mechanism for data collection and network building, which form part of our trust-based agent network model for decision making under uncertainty. Section 4 provides a discussion of how the emergent information can be used to further reduce an agent's interaction uncertainty, and finally Section 5 presents some conclusions and future work.

2 Related Work

Agents interacting in an environment naturally form networks, which potentially hold useful information about the network members and their relationships with one another. The evolution of networks brought more dynamic characteristics and the questions of how the networks are formed, maintained and used are still active research areas. Uncertainty is a characteristic property of interactions among self-interested agents. Thus, agents need to reliably predict the behaviour of other agents to ensure a high level of successful interactions. The concepts of trust and reputation have been proposed to improve the prediction of agent behaviour. We outline the relevant work on agent networks, trust and reputation in agent-based systems and discuss the issues that still need to be addressed, such as the accurate prediction of agent behaviour and collusion.

2.1 Social Networks

The search for relevant information involves finding the right sources, for instance, the agents who have the desired information or expertise. The social network is important in discovering these relevant information sources. An agent is only aware of a portion of the social network to which it belongs [1]. Additionally, due to issues such as privacy, agents will not list their social relationships on a central repository. Agents can however gather this information from distributed searches via referrals. Referrals are important for information flow. Studies of the phenomenon of word-of-mouth found referrals to be very effective in communicating product information among consumers and influencing their purchasing choices [2]. Further evidence that referrals are effective in searching large social networks has been demonstrated for instance by Milgram [3, 4], leading to the concept of *Six Degrees of Separation*. Milgram examined the social connectivity among people and his study involved asking participants to send a packet to a given individual with some information about the person. The participants had to send the packet through individuals they knew by their first name, hence the participants had to choose the most likely intermediary in the chain. Milgram concluded that

the individuals within the study were separated by an average of six intermediaries, or six degrees of separation.

Link Prediction. The high dynamism of social networks suggests the addition of new interactions and deletion of old links in the underlying social structure, thus making the understanding of the mechanisms of evolution of social networks important. Liben-Nowell and Kleinberg [5] study *link prediction* as a basic computational problem underlying social network evolution. They describe the problem as involving the accurate prediction of the edges that will be added to the network, during the interval from a time t to a given future time t'. They seek to discover the extent to which the evolution of a social network can be modelled using features intrinsic to the network itself. The link prediction problem is also relevant to the company environment, where the company can benefit from the interactions occurring within the informal social network among its members. These interactions serve to supplement the official hierarchy imposed by the organisation [1, 6]. In our view, the link prediction problem has parallels with the discovery of emergent information about an agent's environment through the agents' local views, which can be overlapped to some extent to give a wider perspective of the other agents in the system, their transactions and social links. Agents often have a notion of the agents in their environment from their direct interactions, in acquiring services or opinions. Indirect service interactions and recommendations are also useful in predicting the relationships among agents. For instance, an evaluator can infer from an indirect recommendation that the secondary recommender has used the target as a service provider. Although the aim of the recommendation request is to evaluate the trustworthiness of the target, the evaluator is also able to draw a link between the secondary recommender and the target, thus building a more complete view of its environment.

2.2 Trust and Reputation

Trust and reputation models have been developed to improve the success of interactions by minimising uncertainty. Many of the models are based on Marsh's trust formalism [7], in using trust to assess the likelihood that an agent honours its promises. Several of the existing models use the notion of an agent neighbourhood, the more relevant ones are briefly described below.

ReGreT is a model of trust and reputation with three dimensions of information: *individual*, *social* and *ontological*. The social dimension includes information on the experiences of other members of the evaluator's group, or neighbourhood, which is assumed to be a group of agents with some common knowledge. FIRE [8, 9] is a modular approach that integrates up to four types of trust and reputation from different information sources, according to availability: *interaction trust*, *role-based trust*, *witness reputation*, and *certified reputation*. The notion of neighbourhood is used by FIRE in its witness reputation module for searching for relevant witnesses. This is based on Yu and Singh's referral system for multi-agents, enabling them to share referrals for the location of relevant information [10]. Other trust-based network models include TrustNet [11], and Histos [12].

2.3 The Collusion Problem

Despite the ongoing research into agent systems, there remains some open issues that still need to be resolved to make multi-agent systems more widely used in real-life systems. The problem of collusion is a complex issue, especially in decentralised systems. Collusion is defined as a collaborative activity of a subset of users that grants its members benefits otherwise not gained as individuals [13]. We view collusion as occurring in centralised and decentralised systems, and within each, various solutions have been proposed to address collusion issues.

Collusion in Centralised Systems. Centralised systems include centralised reputation systems, such as eBay [1] and Amazon [2], where reputation values about individual agents are collected and managed by a central system and every user in the system sees the same reputation value for another user. In these centralised systems, members have a global view of the entire system and this view is unique to all. Jurca [14] proposes a method for designing incentive-compatible, collusion-resistant payment mechanisms, by using several reference reports. The idea behind deterring lying coalitions is to design incentive-compatible rewards that make honest reporting the unique or at least the "best" equilibrium. Meanwhile, Lian *et al.* [13] report on the analysis and measurement results of user collusion in Maze, a large-scale peer-to-peer (P2P) file-sharing system. Their aim is to observe user collusion in P2P networks that use incentive policies to encourage cooperation among nodes. They search for colluding behaviour by examining complete user logs and incrementally refine a set of collusion detectors to identify common collusion patterns. They found collusion patterns that are similar to those found in Web spamming.

Wang and Chiu [15, 16] propose to use social network analysis in online auction reputation systems to analyse the underlying structure of the accumulated reputation score and its corresponding transactional network. They demonstrate that network structures formed by transactional histories can be used to expose underlying opportunistic collusive seller behaviours. Transaction logs and social relationship structures are used to reconstruct the relationship profiles to supplement the lack of demographic data in the online environment. To identify ill-intended users, Wang and Chiu have used real world blacklist data, consisting of suspended fraudulent accounts collected from the Yahoo Taiwan Inc. online auction site. However, the lack of cooperation from online auction hosts limits data collection and the prediction capability.

Collusion in Decentralised Systems. In decentralised systems, such as P2P systems, trust and reputation information for members are collected and stored across the network by each individual member to help in predicting their future interactions. Moreover, individual members do not have a global view of the whole system. TrustGuard [17] is a framework designed to provide a dependable and efficient reputation system that focuses on the vulnerabilities of the reputation system to malicious behaviour, including

[1] http://www.ebay.com
[2] http://www.amazon.com

strategic oscillation of behaviour, shilling attacks, where malicious nodes submit dishonest feedback and collude with one another to boost their own ratings or bad-mouth non-malicious nodes, and fake transactions, which can lead to fake feedback. The main goal of TrustGuard's safeguard techniques is to maximise the cost that the malicious nodes have to pay in order to gain advantage of the trust system. The behaviour of non-malicious and malicious nodes are defined using game theory. The problem of fake transactions is tackled through having feedback bound to a transaction through a transaction proof, such that feedback can be successfully filed only if the node filing the feedback can show the proof of the transaction. To deal with the problem of dishonest feedback, a credibility factor is proposed that acts as a filter in estimating reputation-based trust value of a node in the presence of dishonest feedback.

Synthesis. Open issues, such as collusion, still need to be resolved in decentralised multi-agent systems. The main strategy to detect collusive behaviour, as used in centralised systems, is to have a global view of the system in order to identify the possible colluding agents. However, such a global view is not available to individual agents in a decentralised MAS, as there is no central management of agent information. Despite the limitations of an agent's local view of its environment, we believe that the local view can be complemented by recommendation information about other agents to form an extended view, so that individual agents can have access to a relevant set of information concerning their own transactions. Trust and reputation information, together with the agent network, can build and maintain the extended localised view of the agent environment.

3 Multi-agent Network Model

Our multi-agent network model is designed to capture the dynamic behaviours of agents, their interactions and any emergent behaviour and information. The model consists of three main components: (i) data collection, (ii) network building, and (iii) analysis of interaction data. The data collection module is largely presented in our previous work on agents using trust, as well as direct and indirect recommendations to better inform their decision making for agent interactions [18]. We supplement the history of past interactions with a history of relevant recommendations, and using these to build a network of the agent environment. With the combined information, agents are aware of a wider view of their environment, beyond their local view. We believe that analysing this extended view can help agents discover emergent information, that will allow them to take decisions on issues, such as collusion.

3.1 E-supply Chain Scenario

We consider the case of a computer hardware e-supply chain, where the component suppliers provide products to customers, which include computer systems manufacturers, computer shops and computer parts resellers. In a two-stage supply chain, a customer obtains components directly from the supplier, for instance the memory card and hard disk. A customer typically needs to purchase different types of components and there

are several suppliers that can do the job. In an e-supply environment, many computer manufacturers and resellers need to interact with various suppliers to source the necessary components to build or sell their systems. Customers can also act as suppliers for partly-assembled components, for example, a computer shop sells partly-built computers, to which components, such as hard disks and memory chips need to be added on. In this competitive industry, there are many stakeholders and they each try to get the most benefits and attain their individual goals and objectives. In an environment where suppliers have variable performance and reliability, a customer needs to ensure that it interacts with the most trustworthy supplier for the required product to minimise costs and production times. A computer systems manufacturer, denoted as Customer C_1, needs to purchase computer monitors and there are 3 suppliers, Supplier S_1, S_2 and S_3, with different offers. The cheaper supplier is not necessarily the best choice as it might also be the one providing the worse quality products. Using our model of trust and reputation, C_1 can make the decision on which supplier to use, based on previous interactions and recommendations from other agents.

Trust from Direct Interactions. An evaluator assesses another agent's direct trustworthiness from its history of past interactions. For instance, the evaluator, Customer C_1 wants to assess which of the 3 suppliers is the most trustworthy for future transactions. It has interacted with 2 of the suppliers previously, S_1 and S_2. From its interaction history, C_1 can assess how trustworthy each supplier has been, based on service characteristics, such as successful delivery, timeliness and cost. For a similar number of interactions, supplier S_1 has been trustworthy in all the important service characteristics 90% of the time, compared to 50% for supplier S_2. From this comparison, C_1 can decide to use supplier S_1 for its next order of computer monitors.

Reputation from Direct Recommendations. Customer C_1 also requires supplies of hard disks, a recent addition to the component parts it needs. There are 2 suppliers for this component, namely S_3 and S_4. C_1 has purchased from S_3 once before and has not interacted with S_4 previously. With insufficient past interactions to reliably assess the trustworthiness of either supplier, C_1 can complement information from direct trust with recommendations from agents that have previously interacted with S_3 and S_4. C_1 has a regular customer C_2, a computer shop, which resells computers and computer parts. Since C_2 stocks hard disks for resale from both suppliers, C_1 can obtain its opinion about these suppliers.

Reputation from Indirect Recommendations. Considering the case where C_1 wants to assess the trustworthiness of suppliers S_3 and S_4, but it has insufficient direct interactions with them to make an informed decision about whom to approach for the next order. This time, customer C_2 has not interacted with either suppliers, but it knows another agent C_3, which has interacted with both S_3 and S_4. C_2 therefore gives an indirect recommendation about the suppliers to C_1, based on C_3's experience.

3.2 Data Collection Component

Let us consider the representation of a customer agent, a_c, acting as an evaluator. Agent a_c records a partial history of provider interactions, $H_{i_s} = (\mathbb{P}\, i_s, count^+, count^-, ST, ST_c)$, where $i_s = (a_c, a_p, s, t)$ is a service interaction. The provider agent is a_p, s is the service performed at time t, $count^+$ and $count^-$ are the number of positive and negative interactions experienced by a_c respectively. ST is the situational trust in a_p and ST_c is the confidence in the situational trust value. The service s is defined as the service type and a set of dimensions, each defined as: $d = (d_{type}, d_e, d_a)$, where d_{type} is the dimension, d_e is the expected value, and d_a is the actual value following an interaction.

The evaluator a_c also holds a history of the recommendations, obtained from direct and indirect witnesses: $H_{i_r} = (\mathbb{P}\, i_r, count^+, count^-, RT, RT_c)$, where $\mathbb{P}\, i_r$ is the set of recommendations, RT is the recommendation trust in the witness and RT_c is the confidence in that trust. Recommendations are defined as $i_r = (a_c, a_t, a_r, s, t, r)$ where a_t is the target, a_r is the witness who gives recommendation r at time t, and s is the service recommended. Recommendations can be direct, $r^d = (s, a_r, count^+, count^-)$ or indirect, $r^i = (a_{r\prime}, r^d_{a_{r\prime}}) \vee (a_{r\prime}, r^i_{a_{r\prime\prime}})$, where $a_{r\prime}$ is an indirect recommender and $r^d_{a_{r\prime}}$ is the direct recommendation of $a_{r\prime}$, and $r^i_{a_{r\prime\prime}}$ is the indirect recommendation of the next witness in the recommender chain $a_{r\prime\prime}$.

As the evaluator takes into consideration recommendations to decide about provider selection, it updates its recommendation trust in the witnesses and also records the interaction results in its history. The interaction history gives a reflection of the relevant past transactions of an agent. The evaluator applies a decay function to the older interactions to give higher importance to the more recent ones. More details on the performance evaluation using trust and reputation can be found in [19].

3.3 Network Building Component

As an evaluator interacts with providers and witnesses it gathers information about interactions and relationships to build an agent network to better understand its environment. We consider three graph structures to represent an agent's environment: provider graph, witness graph, and a combined provider-witness graph. The nodes represent agents and the edges correspond to links between agents, including the strength of the link in terms of experience. For both the provider and witness graphs, these are further differentiated into service-oriented or agent-oriented graphs. Service-oriented graphs concern interactions and recommendations about a particular service, whereas agent-oriented graphs concern the agents in general. The agent-oriented provider graph is an example of a combined provider-witness graph as an evaluator constructs it from its own direct interactions and inferred interactions between other agents from the recommendations it receives.

Algorithm 1 shows how part of the agent graphs is constructed and updated, where r_μ is the currently processed recommendation. For a direct recommendation, an edge is created for each new recommender and the recommendation count is incremented. Indirect recommendations are updated recursively, with edges created or updated from the further recommender $a_{r\prime\prime}$ in the chain to a closer one $a_{r\prime}$. Moreover, the evaluator a_c also updates its provider graph to include the link between $a_{r\prime}$ and $a_{r\prime\prime}$, since $a_{r\prime}$

Algorithm 1 Provider and Witness Graph Updates for Indirect Recommendations

for all indirect recommendations r^i **do**
  if $r^i.a_{r\prime} \notin \mathbb{P}\, a_{r\prime}$ **then**
    add edge$(a_{r\prime}, a_c)$ in $a_c.witnessGraph$
  increment $count_{response}$
  repeat
    if $r^i.a_{r\prime\prime} \notin \mathbb{P}\, a_r$ **then**
      add edge$(a_{r\prime\prime}, a_{r\prime})$ in $a_c.providerGraph$
      increment $count_{response}$
  until $r_\mu = r^d$

obtained a direct recommendation from $a_{r\prime\prime}$. Every time an edge is added or updated, the number of accurate, inaccurate or unused recommendations is incremented; this is represented by $count_{response}$ in the algorithm.

The evaluator agent continuously maintains its provider and witness graphs throughout the period of interaction with other agents. The graphs contain a summary of the links between two agent nodes. For instance, the graph edges in provider graphs record the number of positive and negative interactions between the two agents. Meanwhile, the witness graph edges consist of the number of accurate and inaccurate recommendations by the witnesses, both for direct and indirect opinions. As in our trust model, where trust values are decayed according to how recent they are, the graph data is also subject to decay, but the decay function is applied when the data is used, rather than when it is recorded, since the agent might choose to apply different decay functions at different times.

4 Discussion: Analysis of Interaction Data Component

In this section, we give an overview of the third component of our model, which involves the analysis of the emergent data from the agent graphs. The collection of interaction data over medium to long term transaction periods of an agent enables it to make decisions about numerous aspects, particularly with the view to increase the success of its interactions and maximising its benefits. Besides using trust and reputation to efficiently select interaction partners and witnesses, that information, together with agent network details can bring more insight into other aspects of the agent environment. For instance, agent networking information helps in reinforcing the trust in the roles of witnesses to give accurate information. We believe that emergent information obtained from the multi-agent network can be used to find solutions to the issues of collusion. We discuss how the agent network can be analysed to extract clues to categorise potentially colluding agents.

4.1 Example Usage: Collusion Detection

Collusion detection is one of the potential uses of the emergent information from the agent network. Examples of simple collusion include: witness and target collusion,

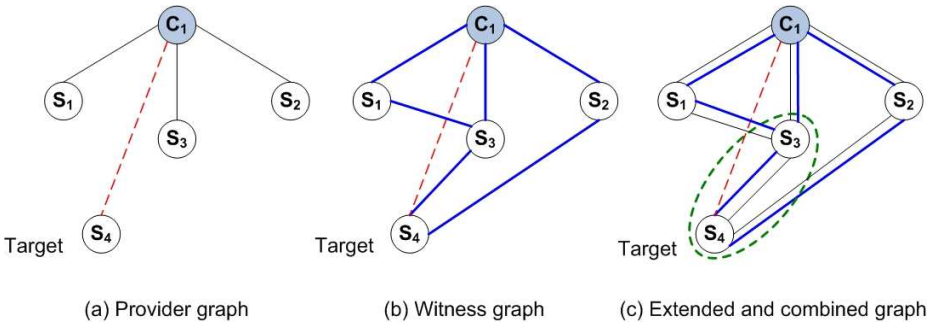

Fig. 1. Collusive behaviour between target and witness

where the witness promotes the target, collusion among witnesses to manipulate a target's reputation, and provider collusion over price. Collusive behaviour is characterised by elements such as heavy agent interactions or similar responses to queries as witnesses. Witness and target collusion is depicted in Figure 1, based on the e-supply chain scenario described in Section 3.1. The evaluator is Customer C_1, which is already using the services of three providers, Supplier S_1, S_2, and S_3. Now C_1 needs a new type of service, which is offered by Supplier S_4. However, C_1 has never interacted with S_4 and therefore decides to request for recommendations from agents who have. Figure 1(a) shows C_1's provider graph. The solid lines represent direct interactions between two agents, while the dashed line shows the target agent that the evaluator is considering for interaction. Agent C_1's witness graph, Figure 1(b) shows the recommenders it uses, through the bold solid lines in the diagram. For instance, S_1 has not interacted directly with S_4 and therefore only gives an indirect recommendation to C_1, via S_3.

The combination of the provider and witness graphs gives Figure 1(c), from which the evaluator can extract information not previously known about certain agent relationships. An additional provider graph edge, between S_1 and S_3 can be derived from the provider and witness graphs. Since S_1 has provided an indirect recommendation to C_1 and S_3 is the only secondary witness, this implies that S_1 and S_3 have direct service interactions. The dashed line circling S_3 and S_4 shows potential collusion between the witness S_3 and target S_4. C_1 requests recommendations about target S_4 from its three service providers, S_1, S_2 and S_3, who can be considered to be trustworthy enough to take their opinions into consideration. From the combined graph Figure 1(c), the evaluator C_1 observes over a period of interaction that S_1 and S_3 have similar recommendations about S_4, as compared to the recommendations of S_2. The emergent information is that S_1's indirect recommendation has been obtained along a recommendation chain of length 2, via S_3. Subsequently, as the recommendations from S_3 are more positive than that of S_2, and from its own initial direct interactions with $S4$, C_1 can suspect that S_3 is colluding with S_4 to promote S_4 as a trustworthy provider. Without the agent network, the evaluator, using only trust and recommendations, would eventually have a low recommendation trust in both witnesses S_1 and S_3, without identifying that S_3 was the dishonest agent. Recommendation trust ensures that the evaluator can distinguish between those witnesses giving accurate opinions, when these are compared to

the actual interaction with the target, if the recommendation is followed. However, low recommendation trust gives no indication of the reason behind the inaccuracy, whether it is only due to differing experiences or due to malicious intent.

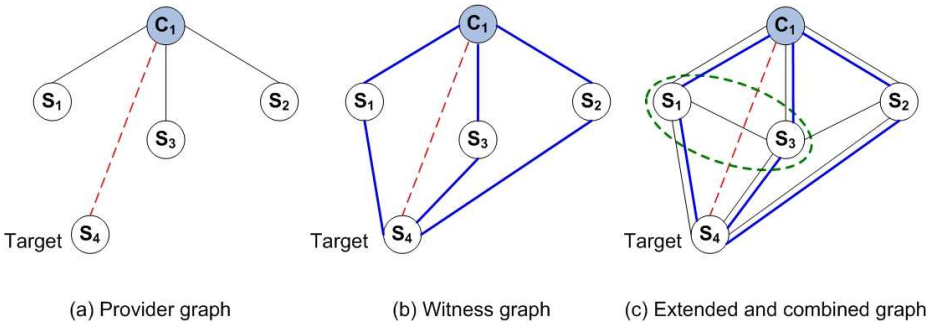

Fig. 2. Collusive behaviour between witnesses

Figure 2 shows an example of collusive behaviour among witnesses. The evaluator C_1 obtains recommendations about target S_4 from providers S_1, S_2, and S_3. Again, C_1 has had no past interactions with S_4. Figure 2(a) shows C_1's provider graph, with the solid lines representing direct service interactions and the dashed line indicates C_1's interest to interact with S_4. Figure 2(b) is different from Figure 1(b) as the recommendations obtained are all direct recommendations about S_4. The extended and combined graph, Figure 2(c) shows the additional information that the evaluator C_1 can infer from the trust and reputation information gathered. Frequent similarity of recommendations from S_1 and S_3, compared to other recommenders could suggest a potential case of collusion between these witnesses, especially if the opinions are inaccurate compared to the actual agent interaction. This is depicted by the dashed line circling S_1 and S_3 in Figure 2(c). Although S_2 and S_3 appear to have similar links as S_1 and S_3, the comparison of their recommendations helps determine that S_1 and S_3 are potentially collusive, while S_2 and S_3 are not considered in this category. Witnesses collude, for example, to lower the trustworthiness of the target as viewed by the evaluator to prevent the target from being swamped with interaction requests, which could potentially increase competition for the witnesses' to interact with the target as a supplier.

As part of the analysis of emergent data to detect collusion, Algorithm 2 outlines the partial collusion detection process after target a_β has just provided service s_β following recommendations. Initially, the set of potential colluders will include all the direct recommenders for target a_β about the service s_β. This set then needs to undergo further selection to ultimately obtain the smallest group of potential colluders. Based on this information, the evaluator can decide on subsequent interactions with the members of the suspected collusive group.

Algorithm 2 Partial Witness and Target Collusion Detection

for all direct recommendations r^d **do**
  if $(r^d.a_t = a_\beta)$ AND $(r^d.s = s_\beta)$ **then**
    for all dimensions $d \in r^d.s$ **do**
      if $d_a < d_e$ **then**
        add a_r to $\mathbb{P}$ *colluders*

5 Conclusions and Future Work

In this paper, we have presented the component of our multi-agent network model, where agents build a network of their local environment. Using interaction data and recommendations, agents can maintain their own representation of their neighbourhood. Their local view is extended from the inferences that can be made from the trust and reputation information available. Whilst existing models mention using some form of social network without specifying how this is done, we go further and show how the network is built and maintained through provider and witness graphs.

We have also outlined the third component of our model, involving the analysis of the emergent network data. We have an implementation of the first two components, that is, the data collection and network building modules. Our ongoing work focuses on the analysis of the network data to extract useful information about agent relationships, in particular, those involving the detection of some forms of collusion. We believe that using available trust and reputation information as a way to learn more about the agent environment is a new approach to solving issues that are usually solved through global access to agent information. With an extended view to the individual agent neighbourhood, agents are closer to make informed decisions about issues that do not necessarily concern only its immediate neighbours.

Future research in the field could further explore the actions to be followed after emergent information has been discovered about the agent environment. For instance, following collusion detection, an evaluator can decide to incorporate the knowledge of collusive agents into its decision making regarding future interactions with the agents concerned.

References

1. Kautz, H., Selman, B., Shah, M.: Referral Web: Combining social networks and collaborative filtering. Communications of the ACM **40**(3) (1997)
2. Brown, J.J., Reingen, P.H.: Social ties and word-of-mouth referral behavior. Journal of Consumer Behaviour **14**(3) (1987) 350–362
3. Milgram, S.: The small world problem. Psychology Today **2** (1967) 60–67
4. Travers, J., Milgram, S.: An experimental study of the small world problem. Sociometry **32**(4) (1969) 425–443
5. Liben-Nowell, D., Kleinberg, J.: The link prediction problem for social networks. In: Proceedings of the 12^{th} International Conference on Information and Knowledge Management. (2003) 556–559

6. Raghavan, P.: Social networks: From the Web to the enterprise. IEEE Internet Computing **6**(1) (2002) 91–94
7. Marsh, S.: Formalising Trust as a Computational Concept. PhD thesis, Department of Computer Science, University of Stirling (1994)
8. Huynh, T.D., Jennings, N.R., Shadbolt, N.: An integrated trust and reputation model for open multi-agent systems. Journal of Autonomous Agents and Multi-Agent Systems **13**(2) (2006) 119–154
9. Huynh, T.D., Jennings, N.R., Shadbolt, N.: Developing an integrated trust and reputation model for open multi-agent systems. In: Proceedings of the 7^{th} International Workshop on Trust in Agent Societies, New York, USA (2004) 65–74
10. Yu, B., Singh, M.P.: Searching social networks. In: Proceedings of the 2^{nd} International Joint Conference on Autonomous Agents and MultiAgent Systems (AAMAS 2003), ACM Press (2003) 65–72
11. Schillo, M., Funk, P., Rovatsos, M.: Using trust for detecting deceitful agents in artificial societies. Applied Artificial Intelligence, Special Issue on Trust, Deception, and Fraud in Agent Societies **14**(8) (2000) 825–848
12. Zacharia, G., Maes, P.: Trust management through reputation mechanisms. Applied Artificial Intelligence **14**(9) (2000) 881–907
13. Lian, Q., Zhang, Z., Yang, M., Zhao, B.Y., Dai, Y., Li, X.: An empirical study of collusion behavior in the Maze P2P file-sharing system. In: Proceedings of the 27^{th} International Conference on Distributed Computing Systems (ICDCS 2007), IEEE Computer Society (2007) 56
14. Jurca, R.: Truthful Reputation Mechanisms for Online Systems. Phd thesis, 3955, Ecole Polytechnique Fédérale de Lausanne (2007)
15. Wang, J.C., Chiu, C.C.: Recommending trusted online auction sellers using social network analysis. Expert Systems with Applications **34**(3) (2008) 1666–1679
16. Wang, J.C., Chiu, C.C.: Detecting online auction inflated-reputation behaviors using social network analysis. In: Annual Conference of the North American Association for Computational Social and Organizational Science (NAACSOS 2005). (2005)
17. Srivatsa, M., Liu, L.: Securing decentralized reputation management using TrustGuard. Journal of Parallel and Distributed Computing **66**(9) (2006) 1217–1232
18. Lim Choi Keung, S.N., Griffiths, N.: Towards improved partner selection using recommendations and trust. In Falcone, R., et al., eds.: Trust in Agent Societies (TRUST 2008). Volume 5396 of Lecture Notes in Computer Science. Springer-Verlag Berlin Heidelberg (2008) 43–64
19. Lim Choi Keung, S.N., Griffiths, N.: Using recency and relevance to assess trust and reputation. In: Proceedings of AISB 2008 Symposium on Behaviour Regulation in Multi-Agent Systems. Volume 4., The Society for the Study of Artificial Intelligence and Simulation of Behaviour (2008) 13–18