ISSN : 0974 - 7435 Volume 10 Issue 23

2014

BioTechnology

An Indian Journal

FULL PAPER

BTAIJ, 10(23), 2014 [14275-14282]

Trust based privacy protection in social network and multi-agent system

Xianjia Meng*, Jian Feng Ma, YiChuan Wang, Di Lu
School of Computer science technology, Xidian University, Xi'an, 710071,Shaanxi Province, (P.R.CHINA)
E-mail: wddtsmxj8513@163.com

ABSTRACT

Social network and Cloud Computing environment have become popular as a medium for connecting like-minded people and disseminating information. The public accessibility of such environment with the ability to share opinions, thoughts, information, and experience offers great promise to enterprises and users. But the public of information also take the risk of your profile is Exposed to strangers. Data publishing has attracted much interest in research community due to the important concerns over the protection of individuals privacy. As a result several mechanisms with different notions of privacy have been proposed to measure, set and compare the level of privacy protection. In this paper, we propose a novel trust based framework for representing a formal model to evaluating privacy. we consider trust as the reason of privacy, user share their secret or information According to the level of trust, then we decide the privacy value from trust value,using the existing network's topology calculate trust value for the new contacts. We show that we can deterministic reduce the information leak and protect user's privacy.

KEYWORDS

Cloud computing; Social networks; Privacy; Trust.

INTRODUCTION

In recent times, the emergence of cloud computing and Web-based social networks such as twitter and Facebook has rapidly increase data and information propagation [1]. The public accessibility of Web-based social networks using mobile phones makes such platforms ubiquitous [2]. The resulting of these platforms offer new opportunities of abuse. Components exchange data will lead to privacy problems occur frequently. Adversaries might combine observed data to extract personal information and to identify the corresponding individuals. And the scams and fake identities made more risky and less reliable of online contacted [3].

The use of Social networks was initially limited to users interaction with their friends and families The phenomenal growth of social network users in recent times has not gone unnoticed. Governments and enterprises have started exploiting the potential use of social networks as platforms for delivering and improving their services [4,5]. Accompanied by the situation, given the open nature of Web-based social networks and their current level of popularity, users are increasingly concerned about privacy, an important consideration for them. In order to balance the open nature of social networks and safeguard the privacy concerns of users, it is important to create an environment where members can share their thoughts, opinions, and experiences in an open and honest way without concerns about privacy and fear of being judged [6].

Privacy and the security of data are vital issues in open and dynamic computing environment, where diverse agents continually join, interact, and leave. In such environments, some agents will inevitably be more trustworthy than others, displaying varying degrees of competence and self-interest in different interactions. When faced with the problem of choosing a partner with whom to interact or share information, agents should evaluate the potential candidates and determine which one is the most appropriate with respect to a given interaction and context. When making such evaluations, trust plays an important role.

This article propose an approach to computing privacy from existing trust values by aggregating probabilistic evidence,and propagating probabilities through user's interest and the privacy policy of environment. Existing trust values are accepted as subjective probabilities as observed by the agents or the user in the network, As such they are not necessarily consistent with each other, and they are used as evidence to be aggregated and propagated through the network, to estimate the privacy values. A concept of "reliance" is introduced to capture the aggregate trust. A Bayesian reliance network is defined on top of the trust net-work, and reliance is propagated through the network using transitivity. Finally, privacy values are inferred from the existing trust values and the reliance network. The algorithms are shown to have linear complexity in the number of nodes, and polynomial complexity in the number of edges per node. The algorithms found to significantly improve the accuracy over existing algorithms, at a slightly higher complexity than the existing algorithms. A heuristic modification to the algorithm also leads to significant improvement in the reach of the algorithm, while maintaining its advantages in accuracy and low complexity.

The rest of this article is organized as follows. Section 2 provides the trust models which includes the method of how to get trust values and the representation of trust set. Section 3 gives the Bayesian reliance network model, and the mapping of trust value to privacy value. Section 4 shows the algorithm's performance in use. The last section concludes the research.

TRUST MODEL

Trust is a broad concept of human mental problem. Establishing a trust relationship can through variety of ways, for example, in daily life the First Impressions is very important to build trust when we meet stranger. But in online market or social networks the situation may be not simple as that, because there always have many other trail to let us know the company or people Is trustworthy. How to Accurate modeling trust need to consider of two aspects factors, the first is how to get trust information, There are many ways to obtain trust, such as direct interaction experience, or through recommendations of others and so on. The second is the method of quantify. for example a Boolean value indicating the relationship of trust and non-trust, and the statistical approaches build trust in terms of probabilistic and statistical measures [7-10].

In social networks, trust information can be collected from three main sources:1 attitudes, 2 behaviors, 3 experiences[11]. In this paper we use an empirical based approach to get trust information, then create quadruple set for the mathematical representation. Definition of the set is showed below.

Definition 1 (trust set) Let A be an entity of trustor and B be an entity of trustee, the trust relationship of A to B is the ordered quadruple $T_B^A = (b, d, u, a)$ where:

b is the belief of B will feedback to A good result.
d is the belief of B will feedback to A bad result.
u is the uncertain of A whether belief b.
a is a priori probability in the absence of committed belief.

These components should satisfy b+d+u=1, and $b, d, u, a \in [0,1]$. Then the trust of A to B is calculate as: $t_B^A = b + au$.

The trust relationship can be represented on a triangle as in Figure 1, the point in the triangle represents a (b,d,u) triple, the belief,disbelief,and uncertainty-axes run from one edge to the opposite vertex towards the bottom right belief vertex. And the point on the base line indicate the base rate. The trust value t_B^A is formed by projecting the T_B^A point onto the base, parallel to the base rate director line. The trust set $T_B^A = (0.625, 0.25, 0.125, 0.4)$ with the trust value of $t_B^A = 0.675$ is showed as an example.

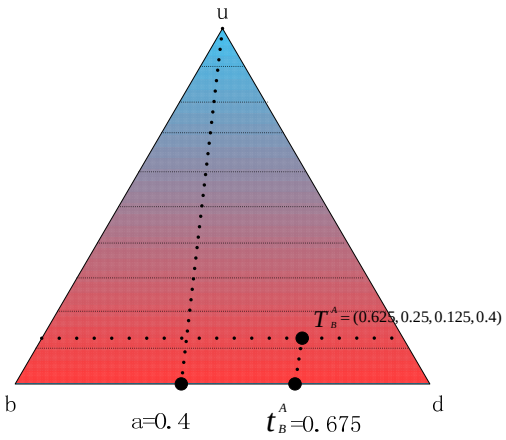

Figure (1) : the triangle of trust set

Before we described the quantitative relationship of trust, now we pay attention to how to get the components from evidence. For this goal,we should found a Mathematical Tools to build an equivalence between statistical observations and trust components. Evidence is conceptualized in terms of the numbers of positive and negative experiences. When an agent makes unambiguous direct observations of another, the corresponding evidence could be expressed as nature numbers, also include zero. Then combining evidence is trivial: let r denote the positive empirical of A interact to B, and s denote the negative empirical of A interact to B,p be the probability of a positive outcomes, the posterior probability of evidence $\langle r, s \rangle$ is the conditional probability of p given $\langle r, s \rangle$.

Definition 2 The conditional probability of p given $\langle r, s \rangle$ is

$$f(p|\langle r,s\rangle) = \frac{g(\langle r,s\rangle|p) f(p)}{\int_0^1 g(\langle r,s\rangle|p) f(p) dp} = \frac{p^r (1-p)^s}{\int_0^1 p^r (1-p)^s dp}$$

Where $g(\langle r,s\rangle|p) = \binom{r+s}{r} p^r (1-p)^s$.

Let $r = \alpha - 1,\ s = \beta - 1$,then

$$f(p|\langle r,s\rangle) = \frac{p^{\alpha-1}(1-p)^{\beta-1}}{\int_0^1 p^{\alpha-1}(1-p)^{\beta-1} dp} = Beta(p|\alpha,\beta)$$

With the restriction of $p \neq 0$ if $0 < \alpha < 1$, and $p \neq 1$ if $0 < \beta < 1$.

This is general Beta pdf without consider the base rate, then we will add the base rate a,

$$\begin{cases} \alpha = r + Wa \\ \beta = r + W(1-a) \end{cases}$$

So that an alternative representation of the beta pdf is:

$$Beta(p|r,s,a)$$

$$= \frac{\Gamma(r+s+W)}{\Gamma(r+Wa)\Gamma(s+W(1-a))} p^{(r+Wa-1)}(1-p)^{(s+W(1-a)-1)} \text{ Where } 0 \le p \le 1, r+Wa > 0, s+W(1-a) > 0,$$

With the restriction of $p \neq 0$ if $0 < r+Wa < 1$, and $p \neq 1$ if $0 < s+W(1-a) < 1$.

W is the prior weight generally set to 2 which insures that the prior beta pdf with default base rate a=0.5 is a uniform pdf. The probability expectation value of beta pdf is calculated as below:

$$E(Beta(p|\alpha,\beta)) = \frac{\alpha}{\alpha+\beta} = \frac{r+Wa}{s+W(1-a)}$$

The beta pdf is equivalent to trust set, and the parameters can map to each other. The mapping is showed below:

$$\begin{cases} b = \dfrac{r}{r+s+W} \\ d = \dfrac{s}{r+s+W} \\ u = \dfrac{W}{r+s+W} \end{cases}$$

$$\Updownarrow$$

$$\begin{cases} u \neq 0 \;\; s = \dfrac{Wd}{u} \;\; r = \dfrac{Wb}{u} \;\; \mathrm{u} + b + d = 1 \\ u = 0 \;\; s = d\infty \;\; r = b\infty \quad b + d = 1 \end{cases}$$

Now we can build the trust set from evidence, let me see an example of this, Suppose A interact with B have 10 good experience and 4 bad experience,the prior knowledge of A to B is 0.4. then the beta pdf is $Beta(p|10.8,5.2)$ illustrated as Figure 2.

which is equal to the Examples of trust value of previous section, the equivalence between beta pdf and trust set is very powerful, because trust set can be derived from statistical observations, also because trust set can be applied to density functions and vice versa.

$$Beta(p|10.8,5.2) \equiv \boldsymbol{T}_B^A = (0.625, 0.25, 0.125, 0.4)$$

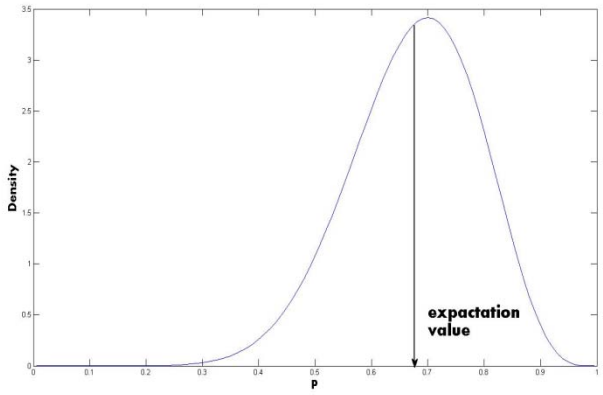

Figure 2 : the beta function of $Beta(p|10.8,5.2)$

MAPPING TRUST TO PRIVACY

Privacy is an ancient problem associated with the history of human. The privacy referred to in this paper is a very broad concept, it's not only the Personal information of user but also the sensitive information in any formal had been leaved from the procedure of online interaction. In social networks just like twitter or facebook we share Personal Information and Daily interesting on it. Although our friends can know our Current situation, but Strangers also can Access to personal homepage read news and get the Personal Information what we shared. It seems has big risk to expose our privacy, so there

are many approach to prevent strangers visit personal page, for example. We can set a list who can access to our homepage. Even more we can set friends to different groups, different Categories can see different content. Maybe these approach can Prevent unfamiliar user access, but our information is not really safe? Let's consider the situation said below. Alice and Bob are good friend in twitter, and Alice set Bob to 'bosom friend' group which has the highest authority to read all of her post information. Then Alice send a post contains some sensitive information only to the bosom friend, but Bob don't know this, and he think this post is very interesting then he post it to the public group, Alice's privacy is exposed. Figure 3 describe this.

The reason of privacy exposure before is the different context and Acknowledge of different individual, it's a hard problem to build a precision criterion for all the people to one thing [Blasé Ur 2013]. But we can refer that, if one get more our trust, we will share more secret to him. So there is a corresponding relationship of trust and privacy as a subject property. When an entity's privacy level is defined, the corresponding trust level's entities can access the Appropriate level of privacy information.

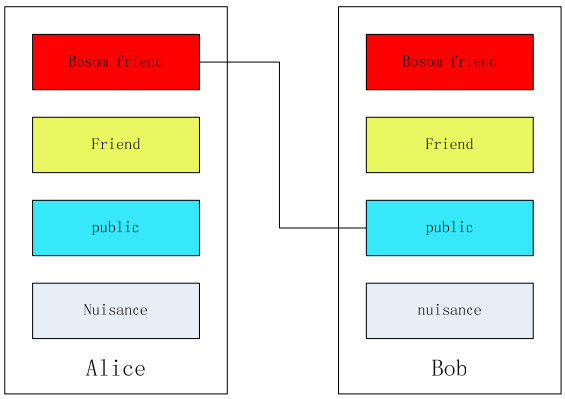

Figure 3 : example of privacy explose

So the key issue is built the mapping from trust context to privacy context. We use a Bayesian inference to reach the target [12]. The remainder of this section will be described in detail.

Even users have similarities that effect who they trust, but trust values of users or agents are not independent of each other, in other words,

$$t_C^{A\cup B} \neq t_C^A \times t_C^B \quad \text{(Eq.3.1}$$

But there is an except when B fully trust C, in this situation: $t_C^B = 1$

$$t_C^{A\cup B} = t_C^A \times t_C^B = t_C^A \quad \text{(Eq.3.2}$$

The concept of full trust, which is simply a trust value of 1, is critical in this article to avoid probabilistic independence issues. More importantly, full trust is very common in real trust networks. In fact, the semantics of partial trust, (trust< 1), tends to be quite complex for humans, and difficult to assess correctly. Consequently, approximately half of all observed trust values tend to be 1, full trust, in the Advagato network.

Let t^A be the probability of arbitrary agent will interact with A.

$$t^A = E(t_X^A) \quad \text{(Eq.3.3}$$

Where E is the expected value over all connected nodes to A, except A.

Using the Eq.3.3 and Eq.3.2 we can calculate the more general form:

$$t^{A\cup B} = E(t_X^{A\cup B}) = E(t_X^A) \quad \text{(Eq.3.4}$$

Where $t_X^B = 1$, X is connected to A but not equal to A.

Then we consider another relationship of A and B,. Let R_B^A denote the reliance of A on B, it is defined as the conditional probability that A will trust a randomly selected agent, when B trusts it fully. The R is an important relationship which propagation of reliance values throughout the network.

R_B^A can be computed from the existing trust values as:

$$R_B^A = E\left(\frac{t_X^{A\cup B}}{t_X^B = 1}\right) = E(t_X^A) \quad \text{(Eq.3.5}$$

For example there is an trust network as Figure 4 showed:

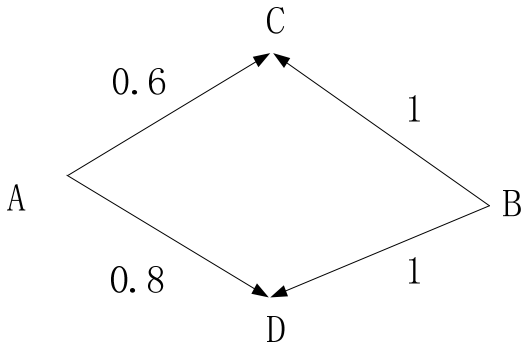

Figure 4 : A simple of trust network

The reliance of A and B can be computed as follow:

$$R_B^A = \frac{t_C^A + t_D^A}{2} = \frac{0.6+0.8}{2} = 0.7$$

Equation (3.5) defines the "reliance" concept in terms of the "trust" concept, and it will be used to create a reliance network overlaid on top of the trust network. Once a reliance network is created, it can be used to extend trust transitively in different context. This is because reliance is fundamentally different from trust, where trust is specific to the actions of an agent, but reliance is generalized to the actions of a random agent. Equivalently, if an agent A relies on another agent B, then if B fully trusts an agent C, then A will also trust C, from the definition of reliance; and if A's trust on C is full, any other agent that relies on A will also trust C, leading to transitivity of trust with respect to reliance. Since $R_B^A = E(t_X^A)$, R_B^A can be treated as the sample mean from the population of t_X^A, and in turn as an estimate of any member of the population of t_X^A where $t_X^B = 1$.

$t_X^A \approx R_B^A$ where $t_X^B = 1$.

Up to now we have introduced the trust reliance mechanism, it is useful to solve the problem of trust context mapping to privacy context. Let $t_X^A(\mathrm{P})$ denote trust value (in privacy context privacy value can be look upon as trust value for the uniform description) of A on B in privacy context, $t_X^A(\mathrm{T})$ denote trust value of A on B in trust context. As before statements, the reliance mechanism can learning trust values in one context from the trust values in another context. Let me see an simple example showed in Figure 5. We know the trust value of A on other agents in trust context, and Correspondence trust value of A on partial agents, we can compute the unknown trust value in context privacy Rely on the reliance of the two context.

The Formula is showed followed:

$R_{A(T)}^{A(P)} = E(t_X^A(\mathrm{P}))$ where $t_X^A(\mathrm{T}) = 1$

$t_N^A(\mathrm{P}) = R_{A(T)}^{A(P)}$ where $t_N^A(\mathrm{T}) = 1$

In this example $t_D^A(\mathrm{P})$ is computed as:

$$R_{A(T)}^{A(P)} = \frac{t_B^A(\mathrm{P}) + t_C^A(\mathrm{P})}{2} = \frac{0.6+0.8}{2} = 0.7$$

$$t_D^A(\mathrm{P}) = R_{A(T)}^{A(P)} = 0.7$$

Then we will consider more usual situation, we relaxing the total trust requirement to include partial trust in the computations. By assuming relative independence of observations and hence $E(t_X^{A\cup B}) = E(t_X^A \times t_X^B)$, we will get:

$$R_B^A = \frac{t^{A\cup B}}{t^B} = \frac{\sum_X t_X^A t_X^B}{\sum_X t_X^B}$$

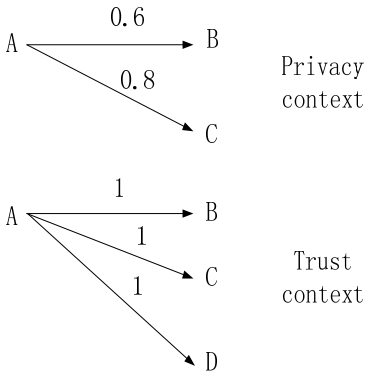

Figure 5 : Trust value map to privacy value

$$t_X^A \approx \frac{\sum_B R_B^A t_X^B}{\sum_X t_X^B}$$

for all agents X connected to A and B, and $X \neq A \neq B$.

EVALUATION

In our experiments, we use the trust data form Advogato projects which contains trust data for an open source software development community. The users of Advogato rate each other with their trustworthiness and reliability, we use the method is introduced in section 2 convert the empirical information to trust value. And we choose trust network contains 500 nodes and 24000 Edges. For varying the size of the network we randomly select subsets of the network created before. We have also implemented an existing approach to privacy protection, to compare them to the approach we developed. The transitivity approach computes the privacy from trust information, for example this method compute the trust value of A on B by finding all of exist paths from A to B in the trust network, then combining those paths to compute a single trust value. for comparing the two approach's performance,we consider two aspects matter: 1 how accuracy are the privacy value. 2 how much node's privacy value can be computed. We will describe separately below.

Let's consider accuracy first. in our test,accuracy is defined as 1-mean absolute error, as compared to the actual trust value. Figure 5 shows the accuracy of our approach in contrast to the transitivity approach. The x label presents edge/node ratio. Use this as variables to see how accuracy changes as the fill rate goes up. For basic graph theory when the edge l equal to n^2, the fill rate is max. we can see that the accuracy rate of our approach remain at 0.87 $\pm$ 0.05 throughout all Range. And it's a remarkable improvement over the transitive approach. The improvement is primarily due to the use of multiple reliance to propagate privacy.

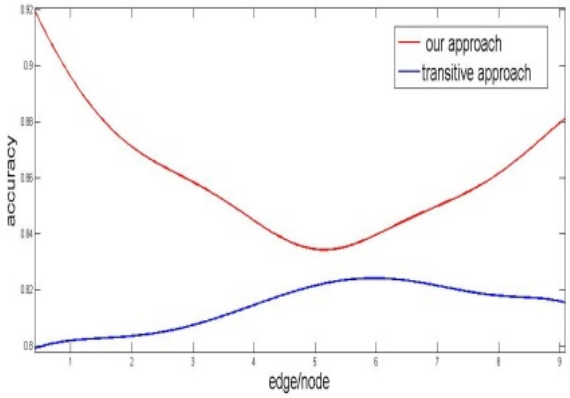

Figure 6 : the accuracy of our approach compare to transitive

Computable is defined the percentage of all possible privacy values in the network that can be calculated. Figure 6 shows the percentage of those that are computable, drawn against the fill rate. We find that our approach is competitive with the transitive approach.

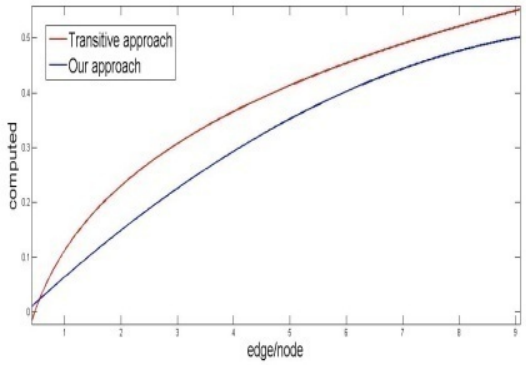

Figure 7 : the computable of our approach compare to transitive

CONCLUSION

Privacy has emerged as a significant impediment to achieving the information share transparently and efficiently. Social networks enable interaction with strangers without transcendental knowledge, then open up new commercial, communication opportunity. But those become dangerous because it is difficult to trust the new contacts even for simple transactions. There is existed many approach to handle privacy problem, they focus different profile of the privacy itself, just like cultural norms, legal issues and user expectations. However, the existing approach to evaluate privacy have significant Limitation in specific conditions. In this paper we propose a novel methods to protect privacy information. It uses the reliance concepts to build an mapping from trust value to privacy value, and the privacy is defined as a conditional probability, then the unknown privacy value can be computed from known privacy value from Bayesian network. This approach has led to significant improvement over existing approaches in the accuracy of compute privacy. The major limitation of our approach is the requirements that a certain percentage of trust value and privacy value are observed directly by the users. That assumes that the observed values should be correct and the users have the correct incentives to reveal their observed trust values and privacy values correctly.

ACKNOWLEDGEMENT

We thank our teacher professor ma for his guidance, This article was supported by the National Science and Technology Major Project (2012ZX02002003) in China.

REFERENCES

[1] Noor, T. H., Sheng, Q.Z.,Zeadally,S., and Jian, Y. 2013." Trust management of services in cloud environments: obstacles and solutions." ACM Comput. Surv. 46,1, Article 12(October 2013), 30 pages.

[2] Humphreys,L.2007."Mobile social networks and social practice: A case study of dodgeball."J. comput. mediated Comm. 13, 1,341-360.

[3] Moldoveanu, M.C and Baum, J.A.C. 2011. "I think you think I think you are lying" : The interactive epistemology of trust in social networks. Manage. Sci.57,2,393-412.

[4] Golbeck,j. 2010. "Trust and nuanced profile reliance in online social networks. "ACM Trans. World Wide Web.

[5] Golbeck,j and Handler,J.2006."Inferring trust relationships in Web based social networks." ACM Trans. Internet Tech. 6,4.

[6] Soren Preibusch. 2010." Experiments and fomal methods for privacy research.Privacy and Usability Methods "Pow-wow(PUMP) 2010.

[7] Josang, A. and Golbeck, J. 2009. "Challenges for robust trust and reputation systems." In proceedings of the 5th International workshop on security and trust management.

[8] Josang, A, Ismail, R, and Boyd, C. 2007. "A survey of trust and reputation systems for online service provision. "Decis. Support Syst. 43, 2,618-644.

[9] Josang,A 2011. "Mutiagent Preference Combination using Subjective Logic." International Workshop on preferences and Soft Constraints.

[10] YongHong Wang, Munindar P. Singh. 2010. "Evidence-based trust A mathematical Model geared for Multiagent systems. "ACM transactions on Autonomous and Adaptive Systems, Vol 5, No 3. September 2010.1-25.

[11] Wanita Sherchan, Surya Nepal, Cecile Paris. 2013. "A survey of trust in social networks." Surv.45, 4, Article 47,33 pages.

[12] Regan,K,Poupart, P, and Cohen,R. 2006. "Bayesian reputation modeling in electronic marketplaces." In proceedings of AAMAS conference on Artificial Intelligence. 1206-1212.