Research Article

Probabilistic Trust Evaluation with Inaccurate Reputation Reports

Bin Liu1,2,3 and Geng Yang1

1School of Computer Science and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210023, China
2State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210023, China
3Institute of Computer Technology, Nanjing University of Posts and Telecommunications, Nanjing 210023, China

Correspondence should be addressed to Bin Liu; bins@ieee.org

Received 10 March 2015; Revised 18 May 2015; Accepted 21 May 2015

Academic Editor: Amiya Nayak

Copyright © 2015 B. Liu and G. Yang. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

We are concerned with the problem of trust evaluation in the generic context of large scale open-ended systems. In such systems the truster agents have to interact with other trustee peers to achieve their goals, while the trustees may not behave as required in practice. The truster therefore has to predict the behaviors of potential trustees to identify reliable ones, based on past interaction experience. Due to the size of the system, often there is little or no past interaction between the truster and the trustee, that is, the case wherein the truster should resort to the third party agents, termed advisors here, inquiring about the reputation of the trustee. The problem is complicated by the possibility that the advisors may deliberately provide inaccurate and even misleading reputation reports to the truster. To this end, we develop techniques to take account of inaccurate reputations in modeling the behaviors of the trustee based on the Bayesian formalism. The core of the techniques is a proposed notion, termed Advisor-to-Truster relevance measure, based on which the incorrect reputation reports are rectified for use in the trust evaluation process. The benefit induced by the proposed techniques is verified by simulated experiments.

1. Introduction

Nowadays, many computational systems, such as peer-to-peer networks, e-commerce, and the Grid, are moving toward open, large-scale, dynamic, and distributed architectures [1–3]. In such open-ended systems, an agent often has to interact with other peers to achieve its goal, while the partner agents may be malicious and thus do not behave as required [4–9]. The new features of these systems, for example, scalability, mobility, autonomy, ubiquity, incomplete information, and global connectivity, imply that traditional security mechanisms are no longer applicable to find malicious agents or control their behaviors [9, 10]. One of the alternatives currently being investigated is an approach based on the notion of trust. The basic idea is to provide a quantitative evaluation for trust in each possible participating agent using history of its behavior [5–9]. The trust value here is a number expressing the level of trustworthiness and this view is known as the computational trust. Based on the output of this trust evaluation process, the truster agent can choose its interaction partners.

Due to the size of the system, there is often little or no past interactions between the truster and the trustee, which hinders the truster from evaluating the trustee's trustworthiness precisely enough. In this case, the truster can resort to the third party agents, termed advisors here, in order to collect more historical observations on the trustee's behavior [7–9]. The advisors are expected to provide honest report about the trustee's behavior to the truster, while, in practice, some advisors may deliberately provide inaccurate and even misleading reports to the truster. Thus, an efficient trust model taking account of possible inaccuracies in the advisors' reputation reports is required.

To this end, we develop techniques to take account of the aforementioned issues in modeling the behaviors of the trustee. The core of the techniques is a proposed notion,
termed Advisor-to-Truster relevance (ATTR) measure, based on which the incorrect reputation reports are rectified for use in the trust evaluation process.

The remainder of the paper is organized as follows. In Section 2, we formalise the general notion of probabilistic trust by introducing the typical beta trust model. The issues related with inaccurate reputations are pointed out precisely in a mathematical manner. In Section 3, we propose the notion termed ATTR measure and present the trust evaluation method using that measure. In Section 4, we test the performance of the proposed method via simulation experiments. Section 5 concludes the paper.

2. Beta Trust Model

In this section, we define the basic notion and mathematically formulate the problem illustrated in the Introduction. We use the same notion as in [9] and focus on the perspective of probabilistic trust. The task is then to build probabilistic models for agents’ behaviors using the outcomes of historical interactions. Using these models, a truster can estimate the probability of particular outcomes of the next interaction with a trustee. Such a probability defines the trust of the truster in the trustee. This notion of trust mimics the trusting relationship between human beings illustrated in [11].

The crucial part of any probabilistic trust model is a behaviour model, which is used to estimate the probabilities of future outcomes of the next interaction. Assume that the outcomes are either success or failure; a beta trust model is introduced in [8] and then followed by other works, for example, in [6, 7, 12]. The idea is to model the behavior of a trustee te by a beta probability distribution over possible outcomes, that is, success s or failure f, of an interaction with te. Given a sequence of outcomes h = o₁ ⋅ oₙ, parameters of this beta distribution can be estimated by Bayesian techniques [8].

The outcomes are binary here with the beta trust model. We therefore focus on the single probability θₚ of an interaction with the given trustee te will be successful. Under the assumption of fixed θₚ, a sequence of n outcomes h = o₁ ⋅ oₙ is a sequence of Bernoulli trials, and the number of successful outcomes in h is probabilistically distributed according to a binomial distribution

\[ P(h \text{ consists of } k \text{ successes}) = \binom{n}{k} \theta^{k}(1-\theta)^{n-k}. \]  

It has been recognized that the beta probability density function (pdf) indexed by the parameters α and β

\[ f(\theta \mid \alpha, \beta) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha) \Gamma(\beta)} \theta^{\alpha-1}(1-\theta)^{\beta-1}, \]  

where Γ is the gamma function, is a conjugate prior to the binomial distribution [13]. That is, if \( f(\theta \mid \alpha_{pr}, \beta_{pr}) \) is chosen as the a priori pdf of θₚ, then, given a sequence h of outcomes, the resulting a posteriori pdf of θₚ is \( f(\theta \mid \alpha_{post}, \beta_{post}) \), the beta pdf with parameters \( \alpha_{post} \) and \( \beta_{post} \), where the a posteriori parameters are related to the a priori ones and the outcome sequence h by the following equations:

\[ \alpha_{post} = \#s(h) + \alpha_{pr}, \]

\[ \beta_{post} = \#f(h) + \beta_{pr}, \]  

where \#s(h) and \#f(h) denote the numbers of successful and unsuccessful interactions in h, respectively.

Here the estimate for \( \theta_{te} \), the probability of having successful interaction, is naturally evaluated as the expected value of \( \theta_{te} \) according to its a posteriori pdf. Using the properties of the beta pdf, this expected value is given by

\[ E[\theta_{te}] = \frac{\alpha_{post}}{\alpha_{post} + \beta_{post}}. \]  

Observe that a uniform pdf, which assigns equal likelihood to all values of \( \theta_{te} \) in the range [0, 1], can be represented exactly by a beta distribution with chosen parameters \( \alpha = 1 \) and \( \beta = 1 \). Taking the uniform pdf as the a priori pdf for \( \theta_{te} \), which just indicates an “unbiased” prior belief about \( \theta_{te} \), as no value is more likely than another, then the parameters of the a posteriori pdf, namely, \( \alpha_{post} \) and \( \beta_{post} \), are related to the sequence h of outcomes as follows:

\[ \alpha_{post} = \#s(h) + 1, \]

\[ \beta_{post} = \#f(h) + 1, \]  

and the beta estimate for \( \theta_{te} \) is therefore given by \((\#s(h) + 1)/(\#s(h) + \#f(h) + 2)\).

As mentioned in the Introduction, the truster tr has to consider reputation reports provided by other peers, termed advisors here, about the trustee te under consideration to enhance the trust evaluation process, especially when there is little or no past interaction experience about the trustee. The beta trust model encompasses a mechanism for handling the reputation reports. It treats each interaction with the trustee as a Bernoulli trial regardless of the interacting partner. Given the representation of te’s behavior by the beta probability distribution (parametrised by \( \theta_{te} \)), the sequence h in the estimating equation (3) is correctly seen, therefore, as the sequence of the outcomes of all historical interactions with te regardless of its partners in these interactions. This allows for formulating a reputation report from an advisor ad as the pair

\[ (\#s(h_{ad}), \#f(h_{ad})) , \]  

where \#s(h_{ad}) (resp., \#f(h_{ad})) is the count of successful (resp., unsuccessful) interaction outcomes in the sequence h_{ad} of personal interactions between the advisor ad and the trustee te. With a set of reputation reports (provided by different advisors), a truster can evaluate the ingredients of the beta trust (5) as follows:

\[ \#s(h) = \sum_{ad} \#s(h_{ad}), \]

\[ \#f(h) = \sum_{ad} \#f(h_{ad}). \]
where the subscript \(ad\) is the index of the advisors that have interacted with the trustee in the past. Following the beta model for trust and reputation, the Dirichlet trust model is introduced in [5], which is also followed by [10]. This model generalises the beta trust model such that the outcome of an interaction is not restricted to be binary (success or failure) but rather takes a value from any set of discrete rating levels, for example, \{very bad, bad, average, good, and excellent\}.

Both the beta trust model and the Dirichlet trust model process the reputation reports provided by the advisors in the same way as for the outcomes of direct interactions of the trustee with the advisor. In another word, they do not take account of the possibility that the reputation reports, that is, \(g(h_{ad})\) and \(g(h_{ad})\) in (7), may be inaccurate and even misleading. To this end, we develop techniques to handle possible inaccuracies in the advisors’ reputation reports, which will be presented in the following section.

### 3. Handing Inaccurate Reputations Using Relevance Information

As mentioned above, the advisor peers may provide inaccurate and even misleading reputations reports to the trustee on the advisor, while many existing trust models, for example, the beta trust model and the Dirichlet trust model, do not take account of that. In this section, a notion of Advisor-to-Truster relevance (ATTR) measure is proposed, based on which we develop techniques in order to handle the inaccurate reputation reports in modeling the trust of the trustee in the advisor.

#### 3.1. Advisor-to-Truster Relevance (ATTR) Measure

The ATTR measure is used to quantify the extent to which the reputation report provided by an advisor \(ad\) is relevant with the trust evaluation outcome given by the trustee \(tr\). We introduce two different approaches to define the ATTR measure, one is based on the Cosine similarity measure, which found wide applications in the field of information retrieval [14–16], and the other one is developed by the authors.

To begin with, suppose that we have a trustee set \(\{te_1, \ldots, te_m\}\), each member of which has interactions with both the \(tr\) and \(ad\) in the past. Represent the reputation report of \(ad\) on the trustee \(te_i\), \(i \in \{1, \ldots, m\}\), as

\[
\left(\frac{\theta}{\theta} (h_{ad \rightarrow te_i}), \frac{\theta}{\theta} (h_{ad \rightarrow te_i})\right).
\]

Then the probability that the advisor \(ad\) will have a successful interaction with \(te_i\) is naturally estimated by

\[
\theta_{ad \rightarrow te_i} = \frac{\theta (h_{ad \rightarrow te_i})}{\theta (h_{ad \rightarrow te_i}) + \theta (h_{ad \rightarrow te_i})}. \quad (9)
\]

We then estimate the probability that the trustee \(tr\) will have a successful interaction with \(te_i\), denoted by \(\theta (h_{tr \rightarrow te_i})\), in a similar way. We construct two corresponding vectors, \(\theta_{ad}\) and \(\theta_{tr}\), in the same space of probabilities for \(ad\) and \(tr\), respectively; that is, \(\theta_{ad} = [\theta (h_{ad \rightarrow te_1}), \ldots, \theta (h_{ad \rightarrow te_m})], \theta_{tr} = [\theta (h_{tr \rightarrow te_1}), \ldots, \theta (h_{tr \rightarrow te_m})].\)

Now we introduce two metrics of the ATTR measure, namely, the cosine ATTR measure and the adjusted cosine ATTR measure, in the following.

#### 3.1.1. The Cosine ATTR Measure

Here the taxonomy of the ATTR measure is estimated as the cosine between the corresponding vectors, \(\theta_{ad}\) and \(\theta_{tr}\), as follows:

\[
R (ad, tr) = \cos \theta_{ad} \theta_{tr} = \frac{\theta_{ad} \times \theta_{tr}}{\|\theta_{ad}\| \times \|\theta_{tr}\|}, \quad (10)
\]

Observe that such cosine measure is a dot product scaled by magnitude, and, because of this scaling, it is normalized between 0 and 1. For a pair of two-dimensional vectors, such a cosine measure only depends on the included angle between the two vectors, regardless of the vectors’ magnitudes.

To further corroborate the above statement, consider two example cases. In the former one, we have \(\theta_{ad} = [0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1]\) and \(\theta_{tr} = [0.9, 0.9, 0.9, 0.9, 0.9, 0.9, 0.9, 0.9, 0.9, 0.9]\). In the latter case, we have \(\theta_{ad} = \theta_{tr} = [0.9, 0.9, 0.9, 0.9, 0.9, 0.9, 0.9, 0.9, 0.9, 0.9]\). It is easy to see that, in the former case, the physical meaning of the reputation report given by the advisor \(ad\) is totally reverse to that of the trustee \(tr\). This advisor \(ad\) in the former case is likely to be a malicious agent which deliberately reports reversed counts of successful and failing interactions to the trustee \(tr\). In the latter case, the physical meaning of the reputation report given by the advisor \(ad\) just coincides with that of the trustee \(tr\). However, using (10), we get the same relevance measure, that is, \(R(ad, tr) = 1\), for both cases. This result surely corroborates the above statement that the cosine measure only depends on the included angle between the two vectors, regardless of the magnitude. However, this is not a characteristic we want, since, using this measure, we will treat a remarkable malicious agent in the same way as for an ordinary honest peer. Clearly, to make full use of the reputation data, it requires us to develop a smarter relevance measure.

To this end, we propose the adjusted cosine measure in the following subsection.

#### 3.1.2. Adjusted Cosine ATTR Measure

To deal with the aforementioned counterintuitive property of the cosine ATTR measure, we propose here an adjusted cosine ATTR measure, which defines to be

\[
R (ad, tr) = \frac{\sum_{i=1}^{m} g (\theta_{tr \rightarrow te_i}) \times g (\theta_{ad \rightarrow te_i})}{\sqrt{\sum_{i=1}^{m} g (\theta_{tr \rightarrow te_i})^2 \sum_{j=1}^{m} g (\theta_{ad \rightarrow te_j})^2 + \exp (-99)}}, \quad (11)
\]

where \(g(\theta) = \theta - 0.5\). The item \(\exp(-99)\) present in the denominator is used to avoid the appearance of a zero-valued denominator. Compared with (10), it is seen that each \(\theta\) in (10) is substituted by a \(g(\theta)\) in (11). Since the number 0.5 is a naturally neutral probability value, a positive (resp., negative)
value of $\theta - 0.5$ just suggests a tendency for the outcome of the next interaction to be success (resp., failure). The magnitude of $\theta - 0.5$ indicates the magnitude of such a tendency. If all $\theta$s take the value of 0.5, which indicates that the advisor report reputations in a totally random manner, then no information about the trustee's trustworthiness will be drawn from its reputation report. In this case, we expect to calculate out a zero-valued ATTR measure. Using (II), we will indeed calculate out a zero-valued ATTR measure, which means that this measure conforms to our intuitive understanding on the notion of relevance in this special case.

Now let us reconsider the example cases presented above; that is, we have $\vec{p}_{ad} = \{0.1, 0.1, 0.1, 0.1, 0.1\}$ and $\vec{p}_{tr} = \{0.9, 0.9, 0.9, 0.9, 0.9\}$ in the first case and $\vec{p}_{ad} = \vec{p}_{tr} = \{0.9, 0.9, 0.9, 0.9, 0.9\}$ in the second case. Now using this adjusted cosine ATTR measure defined in (II), we will get relevance measures $R(ad, tr) = -1$ and $R(ad, tr) = 1$ for the former and latter cases, respectively. It is shown that the sign of the relevance value just gives a clear indication to discriminate the above two correlated but totally different cases. In another word, compared with the cosine ATTR measure, this new measure can provide more critical information on the relevance relationship between the advisor ad and the trustee tr.

3.2. Trust Evaluation Using ATTR. Here, we present our approach to trust evaluation using the proposed notion of ATTR measure.

The assumption behind the approach is that a given malicious advisor ad is more likely to provide reputation report about trustee $te_{m+1}$, with a similar error pattern as those provided in the past about other trustees, $te_1, \ldots, te_m$. For example, if a given advisor ad provided reversed counts of successful and failing interactions about $te_1, \ldots, te_m$ then, under this assumption, it is very likely that this advisor ad will also provide reversed counts of successful and failing interactions about the trustee $te_{m+1}$.

We present the proposed approach within the framework of beta trust model introduced in Section 2. To make the description as clear as possible, we rewrite the beta pdf here

$$f(\theta_{te} | \alpha, \beta) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha) \Gamma(\beta)} \theta_{te}^{\alpha-1} (1 - \theta_{te})^{\beta-1}. \quad (12)$$

Suppose that, just before seeing the reputation report provided by the advisor ad, the a priori pdf of $\theta_{te}$ is represented as $f(\theta_{te} | \alpha_{pri}, \beta_{pri})$. Then, upon receiving the reputation report from the advisor ad about the trustee te represented as $(s_f, h_{ad}), (s_f, h_{ad})$, this approach updates the a posteriori pdf, $f(\theta_{te} | \alpha_{post}, \beta_{post})$, by the following equations:

$$\alpha_{post} = \begin{cases} 
\alpha_{pri} - R(ad, tr) \times s_f(h_{ad}), & \text{if } R(ad, tr) < 0 \\
\alpha_{pri} + R(ad, tr) \times s_s(h_{ad}), & \text{otherwise},
\end{cases} \quad (13a)$$

$$\beta_{post} = \begin{cases} 
\beta_{pri} - R(ad, tr) \times s_s(h_{ad}), & \text{if } R(ad, tr) < 0 \\
\beta_{pri} + R(ad, tr) \times s_f(h_{ad}), & \text{otherwise}.
\end{cases} \quad (13b)$$

According to the Bayesian inference mechanism [17], the a posteriori pdf will change to be the a priori pdf when new observations, that is, new reputation reports here, arrive.

It is shown that, in this approach, the sign of ATTR determines whether to reverse the count numbers of successful and failing outcomes in the reputation reports and the magnitude determines to which extent the reported counts are discounted, for updating the a posteriori pdf.

4. Experiments

In this section, we design simulated experiments to examine how effectively we could cope with inaccurate reputation reports using the proposed notion of ATTR measure. We compare two implementations of the ATTR measure, based on the cosine measure and the adjusted cosine measure described in Section 3, respectively. The beta trust modeling approach described in Section 2 is included as the benchmark for performance comparison.

The objective here is to demonstrate that the proposed ATTR measure works. A comparative study of our method with other related methods, for example, TRAVOS [7] and BLADE [18], is certainly interesting but has not yet been performed and is not the intention here.

We are concerned with the ability of our methods to deal with the deceptive advisors at first. The deceptive advisors will report the reversed counts of successful and failing interactions with a trustee, which means that if the true counts of successful and failing interactions are $s$ and $f$, respectively, then it reports that the counts of successful and failing interactions to be $f$ and $s$, respectively. We simulated 20 deceptive advisors, each having a common training set of trustees with the trustee. Each training trustee has interacted with both the trustee and the advisor in the past, and the number of past interactions is randomly drawn from a uniform discrete distribution over the range $[5, 20]$. The number of trustees in each common training set is fixed to be 10.

We consider the process of aggregating 20 deceptive advisors one by one and this process is initialized by a trustee which knows nothing about the behavior of the potential trustee, and thus we use a beta pdf with chosen parameters $\alpha = 1$ and $\beta = 1$ to model it. The true probability $\theta_{te}$ that an interaction with the trustee te under consideration will be successful is 0.9. The difference between the mean of the predicted $\theta_{te}$ and the true value 0.9 is termed mean error here. As shown in Figure 1, using the adjusted cosine ATTR measure, the mean error converges to 0 quickly. In contrast, for the cosine measure and the traditional beta trust model, the mean error is much larger as the advisors’ reputation reports have been aggregated.

Figure 2 graphs change in the mean error of each method as the percentage of deceptive advisors grows, and this result is obtained by a Monte Carlo simulation consisting of 100 independent runs of each method with respect to each specific percentage value.

It is shown that, using the proposed adjusted cosine ATTR measure, we could cope with deceptive reputation reports very well.
Now we evaluate whether this ATTR measure will affect the efficiency of the trust evaluation process when the reputation reports are all accurate; namely, they are all provided by the honest advisors. Use the same setting as for the above deception experiment, except that the advisors now will report honestly the true interaction data to the trustor. The simulation result is shown in Figure 3, which reveals that all the involved methods perform equally well in this case. We could approximately deem that if the reputation reports are accurate, the ATTR based method automatically degenerates into the traditional beta trust model approach.

The same experimental setup is used to examine how the totally random reputation reports will affect the trust evaluation methods under consideration. The totally random reputation reports represent the reports in which the counts of successful and failing interactions are determined in a totally random manner regardless of the truth. In the simulation, the count of successful interactions is drawn from a uniform discrete distribution over \([0, \text{the total number of interactions}]\), where the total number of interactions is itself a random variable, whose value is randomly drawn from a uniform discrete distribution over the range \([5, 20]\). As shown in Figure 4, none of the involved methods performs well enough with totally random reputation reports aggregated.

Figure 5 graphs change in the mean error of each method as the percentage of abnormal advisors which produce totally randomly generated reputation reports grows. The same as
before, this result is obtained by a Monte Carlo simulation consisting of 100 independent runs of each method with respect to each specific percentage value. It is shown that the mean error of each method grows as the percentage of abnormal advisors grows, while the adjusted ATTR measure based method performs better than the others. Specifically, as this percentage is approaching the point 50%, the advantage of the adjusted cosine ATTR measure based method over the others becomes remarkable.

5. Conclusions

In this paper, we proposed techniques to cope with the problem of trust evaluation involving inaccurate reputation reports for large scale open-ended systems. The basic idea is to utilize the relevance information between the truster agent and the advisor agents. We proposed a notion termed ATTR measure to quantify such relevance information and developed two implementations of the ATTR measure. We demonstrated that one of the proposed implementations, namely, the adjusted cosine ATTR measure, could provide promising solutions to complex trust evaluation problems involving inaccurate reputation reports.

Through simulated experiments, it is shown that the proposed techniques perform remarkably satisfactorily in dealing with deceptive advisors and perform better than the other methods involved in dealing with inaccurate, totally random generated reputation reports.

The notion of ATTR measure is proposed here within the framework of beta trust model. It is also feasible to use this notion and develop corresponding techniques based on other probabilistic trust models, for example, the Dirichlet trust model [5, 10], which is a generalization of the beta trust model, in order to cope with inaccurate reputation reports.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work was partly supported by the National Natural Science Foundation (NSF) of China under Grant no. 61302158, the NSF of Jiangsu province under Grant no. BK20130869, the Natural Science Research Project of Department of Education of Jiangsu Province under Grant no. 13KJB520019, and the Scientific Research Foundation of Nanjing University of Posts and Telecommunications under Grant no. NY213030.

References

[1] R. Srinivasa Rao, S. V. L. Narasimham, M. Ramalinga Raju, and A. Srinivasa Rao, “Optimal network reconfiguration of large-scale distribution system using harmony search algorithm,” IEEE Transactions on Power Systems, vol. 26, no. 3, pp. 1080–1088, 2011.
[2] S. Muftic, “Secure world wide electronic commerce over an open network,” U.S. Patent no. 5,850,442, 1998.
[3] M. Ripeanu, I. Foster, and A. Iamnitchi, “Mapping the Gnutella network: properties of large-scale peer-to-peer systems and implications for system design,” IEEE Internet Computing Journal, vol. 6, 2002.
[4] S. Bijani and D. Robertson, “A review of attacks and security approaches in open multi-agent systems,” Artificial Intelligence Review, vol. 42, no. 4, pp. 607–636, 2014.
[5] A. Jøsang and J. Haller, “Dirichlet reputation systems,” in Proceedings of the 2nd International Conference on Availability, Reliability and Security (ARES’07), pp. 112–119, April 2007.
[6] L. Mui, M. Mohtashemi, and A. Halberstadt, “A computational model of trust and reputation,” in Proceedings of the 35th Annual Hawaii International Conference on System Sciences, pp. 2431–2439, Big Island, Hawaii, USA, 2002.
[7] W. T. L. Teacy, J. Patel, N. R. Jennings, and M. Luck, “TRAVOS: trust and reputation in the context of inaccurate information sources,” Autonomous Agents and Multi-Agent Systems, vol. 12, no. 2, pp. 183–198, 2006.
[8] A. Jøsang and R. Ismail, “The beta reputation system,” in Proceedings of the 15th Bled Electronic Commerce Conference, pp. 41–55, 2002.
[9] E. ElSalamouny, Probabilistic trust models in network security [Ph.D. thesis], University of Southampton, 2011.
[10] M. Nielsen, K. Krukow, and V. Sassone, “A bayesian model for event-based trust,” Electronic Notes in Theoretical Computer Science, vol. 172, pp. 499–521, 2007.
[11] D. Gambetta, “Can we trust trust?” in Trust: Making and Breaking Cooperative Relations, chapter 13, pp. 213–237, Department of Sociology, University of Oxford, 2000.
[12] S. Buchegger and J. Y. Le Boudec, “A robust reputation system for peer-to-peer and mobile Ad-hoc networks,” in Proceedings of the P2P Econ Workshop, pp. 1–6, 2004.
[13] G. Casella and R. L. Berger, Statistical Inference, Duxbury Press, Pacific Grove, Calif, USA, 2002.
[14] R. Mihalcea, C. Corley, and C. Strapparava, “Corpus-based and knowledge-based measures of text semantic similarity,”

FIGURE 5: The mean errors of the trust predictions versus the percentage of abnormal advisors which produce totally randomly generated reputation reports.
in Proceedings of the 21st National Conference on Artificial Intelligence (AAAI ’06), vol. 1, pp. 775–780, 2006.

[15] S. Tata and J. M. Patel, "Estimating the selectivity of tf-idf based cosine similarity predicates," ACM SIGMOD Record, vol. 36, no. 2, pp. 7–12, 2007.

[16] M. J. Pazzani and D. Billsus, "Content-based recommendation systems," in The Adaptive Web, pp. 325–341, Springer, Berlin, Germany, 2007.

[17] A. Gelman, J. B. Carlin, H. S. Stern et al., Bayesian Data Analysis, Chapman & Hall, 2014.

[18] K. Regan, P. Poupart, and R. Cohen, "Bayesian reputation modeling in E-marketplaces sensitive to subjectivity, deception and change," in Proceedings of the 21st National Conference on Artificial Intelligence, vol. 21, pp. 1206–1212, July 2006.
