IJCSEC- International Journal of Computer Science and Engineering Communications.
Vol.3, Issue 2, 2015, Page.676-684,ISSN: 2347–8586

SUBJECTIVE AND OBJECTIVE TRUSTED BINARY AND CONTINUOUS INFERENCE MODELS FOR WEB SERVICE QOS

Premalatha.S
PG scholar Computer Science and Engineering
SKP Engineering College, Tiruvannamalai, Tamil Nadu, India
premalathamegala@gmail.com

Rajesh.A
P.hD scholar Computer Science and Engineering
SKP Engineering College, Tiruvannamalai, Tamil Nadu, India

Kumaresan.A
P.hD scholar Computer Science and Engineering
SKP Engineering College, Tiruvannamalai, Tamil Nadu, India

Abstract- Trust is an important factor that is used as a criterion for service selection. It creates service as well as building block for many real applications. Existing trust model either use properties like transitivity, multi-aspect, bias to do trust evaluation or user preferences for different quality of service is consider for trust evaluation these leads to security bleach in real application. In proposed system a trust model is created to combine both user preferences QOS and important properties of trust evaluation are considered to do trust evaluation this model is applicable to both binary and continuous scenario and works well on trust evaluation, and can reduce the malicious ratings. This method evaluates on data sets show to achieves improvement over several existing benchmark, for both numerical trustworthiness scores and predicting binary and continuous trust/distrust signs.

Index Terms:Trust inference, trust prediction, transitivity property, multi-aspect property, latent factors, trust bias.

I INTRODUCTION

Trust is essential to reduce uncertainty and boost many real-world existing applications such as social networks, peer-to-peer networks, e-commerce and semantics web, etc. Trust inference can be calculated by using three properties such as transitivity, multi-aspect, trust bias. The basic assumption behind most of the existing trust inference methods is the transitivity property of trust, which is rooted in the social structural balance theory. For example, Alice trust Bob and Bob trust carol, Alice might also trust carol to some extent. This model as a whole, have been widely studied and successfully applied in many real-world settings.

In additional transitivity property explores another equal important property, that is the multi aspect of trust, composes of multiple factors, and different users may have different preference factors. For example in e-commerce some users might care about delivery time, some of them might care about product quality; some others give a higher ratings to the factors of product quality. Finally, this model to enhance trust model to improves inference models.Main contribution of this paper are summarised as follows:

1) Trust Models: We proposed a trust model to integrates transitivity, multi-aspect and trust bias into one single trust inference model.
2) Inference Algorithms: We proposed a family of algorithms. It finds a local optimal solution with linear complexity. It applies to both binary and continuous trust inference scenarios.
3) Performance Improvements: we conducted extensive experimental evaluations on data sets, it improves significant performance improvements in both continuous and binary inference models. In continuous, for example, our MATRI outperforms the best known existing methods by 26.7%-40.7% in terms of prediction accuracy; and by computation, our MATRI is much faster in terms of on-line response, achieving upto 7 orders of magnitude speedup.
Accordingly, trust is introduced to resolve the web service problem [5,6]. There are two lines of research [7,8]; The first line is based on the "credential-based" approach for traditional identity authentication mechanism. This approach ensured such as PolicyMaker[7], KeyNote[8] and their derived methods. In this case, the "Credential-Based" approach is not capable to provide a rational trust evaluation result. This focus on "experience-Based" approach. The second line is based on the "experience based" approach. Some researchers point out that trust model should be irrational and should take subjective factors into consideration.

II PROBLEM DEFINITION

In this section, we formally define our trust inference prob-lem. Table 1 lists the main symbols we use throughout the paper.Following conventions, we use bold capital letters for matrices, and bold lower case letters for vectors.For example, we use a partially observed matrix **T** to model the locally-generated trust relationships, where the existing/observed trust relationships are represented as non-zero trust ratings and non-existing/unobserved rela-tionships are represented as '?'. As for the observed trust rating, we represent it as a real number between 0 and 1 (a higher rating means more trustworthiness) in the continu-ous case, and +1/-1 (+1 means trust and -1 means distrust) in the binary case. We use calligraphic font K to denote the set of observed trustor-trustee indices in **T**. Similar to MATLAB, we also denote the i^{th} row of matrix **T** as **T**$(i, :)$, and the transpose of a matrix with a prime. In addition, we denote the number of users as n and the number of charac-terized factors as s. Without loss of generality, we assume that the goal of our trust model is to infer the unseen trust relationship from the user u to another user v, where u is the trustor and v is the unknown trustee to u.
Based on these notations, we first define the basic trust inference problem as follows:
Problem 1. *The Basic Trust Inference Problem*
Given: *an $n \times n$ partially observed trust matrix* **T**, *a trustor u, and a trustee v, where* $1 \; u, v \; n \; (u \_= v)$ *and* **T**$(u, v) = '?';$
Find: *the estimated trustworthiness score/sign* **T**(u, v).
In the above problem definition, given a trustor-trustee pair, the only information we need as input is the locally-generated trust ratings (i.e., the partially observed matrix **T**). The goal of trust inference is to infer the new trust rat-ings (i.e., unseen/unobserved trustworthiness scores in the partially observed matrix **T**) by collecting the knowledge from existing trust relationships. As mentioned before, one of our goals is to capture the multi-aspect property of trust. In this paper, we propose a multi-aspect model for such trust inference in Problem 1. That is, we want to infer an $n \times s$ *trustor matrix* **F** whose element indicates to what extent the corresponding person trusts others wrt a specific aspect/factor. Similarly, we want to infer another $n \times s$ *trustee matrix* **G** whose element indi-cates to what extent the corresponding person is trusted by others wrt a specific aspect/factor. Such trustor and trustee matrices are in turn used to infer the unseen trustworthi-ness scores.

2.1 AN ILLUSTRATIVE EXAMPLE

To further illustrate our multi-aspect trust inference prob-lem (Problem 1), we give an intuitive example for inferring the continuous trustworthiness scores as shown in Fig. 1. In this example, we observe several locally-generated pair-wise trust relationships between five users (e.g., *Alice*','*Bob*', '*Carol*', '*David*', and '*Elva*') as shown in Fig. 1(a). Each observation contains a trustor, a trustee, and a numerical trust rating from the trustor to the trustee. We then model these observations as a 5×5 partially observed matrix **T** (see Fig. 1(b)) where **T***(i, j)* is the trust rating from the i^{th} user to the j^{th} user if the rating is observed and **T***(i, j)* = '?– other-wise. Notice that we do not consider self-ratings and thus represent the diagonal elements of **T** as '/'. By setting the number of factors $s = 2$, our goal is to infer two 5×2 matri-ces **F** and **G** (see Fig. 1(c)) from the input matrix **T**. Each row of the two matrices is for the corresponding user, and each column of the matrices represents a certain aspect/factor in trust inference (e.g., 'delivering time', 'product price', etc). For example, we can see that *Alice* trusts others strongly wrt both 'delivering time' and 'product price' (based on **F**), and she is in turn moderately trusted by oth-ers wrt these two factors (based on **G**). On the other hand, both *Bob* and *Carol* put more emphasis on the delivering time, while *David* and *Elva* care more about the product price.Once **F** and **G** are inferred, we can use these two matrices to estimate the unseen trustworthiness scores (i.e., the '?' elements in **T**). For instance, the trustworthiness from *Carol* to Alice can be estimated as T(3,1)=F(3,:)G(1,:)'=0.5, This estimation is reasonable because *Carol* has the same preference as *Bob* and the trustworthiness score from *Bob* to *Alice* is also 0.5.In the next two sections, we will mainly focus on (1) how to infer **F** and **G**; and (2) how to incorporate trust bias and trust transitivity.

III THE OPTIMIZATION FORMULATION

In this section, we propose our optimization formulation to integrate all the three important properties in trust inference, including all the three properties. We start with the continuous trust inference for inferring numerical trustworthiness scores, and then present some meccessary adaptations for the binary case of trust/distrust signs. Finally, we discuss some generalizations of our formulation.

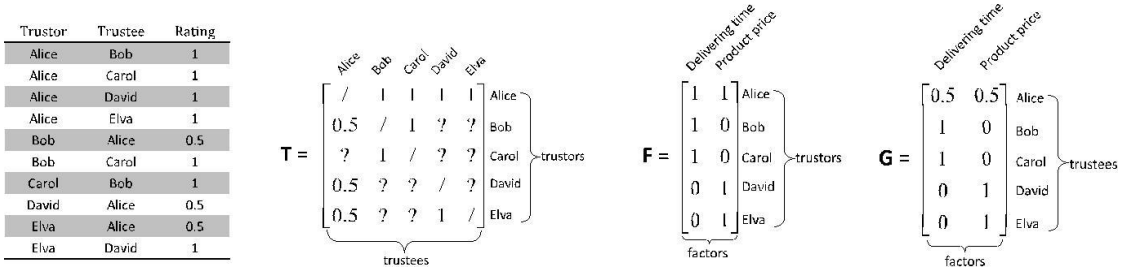
3.1 FORMULATION OF TRUST MATRIX:

At initial stage, Matrix can be formed by using the trustors and trustees. To be specific, in the trust matrix T, if we treat its rows (i.e, trustors) as a users and its columns(i.e., trustees) as items. Its entries as (i.e., trustworthiness scores) as item ratings. Trust matrix as T. Inferred trust matrix as F and trustee matrix as G. Trust is essential to reduce uncertainty and boost collaborations in many real-world applications including social networks, e-commerce, peer-to- peer networks, semantic web, etc. In these applications, trust inference is widely used as the mechanisms to build trust among unknown users. Typically, trust inference takes as its input the existing trust ratings that are locally generated through direct interactions, and outputs as estimated trustworthiness score indicates to what extent the trustor could expect the trustee to perform a given action.

The basic assumption behind most of the existing trust inference methods is the transitivity property of trust, which is rooted in the social structural balance theory. This property essentially means that if Alice trust Bob and Bob trust Carol. Alice might also trust Carol to some extent. This method belongs to T matrix i.e., trustee and trustor. In additional to transitivity, it explore another property Multi-Aspect of trust. The basic assumption behind the multi-aspect methods is that trust is the composition of multiple factors and different users may have different preferences for these factors. For example, in e-commerce, some users might care about the factor of delivering time, whereas other give a higher weight to the factor of product price. Therefore it forms the F and G matrix.

3.2 TRUST BIAS:

Trust bias is an integral part in the final trust decision. For instance, some users tend to give higher trust ratings than others, and some users have relatively higher capability in terms of being trusted than others. Bias achieve the user priority in various factor will be analyzed for outlier detection compared to other user. Before formulating bias user rating are genuine to under rating (or) over related. Bias factors are



Trustor	Trustee	Rating
Alice	Bob	1
Alice	Carol	1
Alice	David	1
Alice	Elva	1
Bob	Alice	0.5
Bob	Carol	1
Carol	Bob	1
David	Alice	0.5
Elva	Alice	0.5
Elva	David	1

Fig1. Illustrative example for multi-aspect trust inference problem. (a) Observed locally-generated pair-wise trust relationships. (b)Partially observed trust matrix **T**. (c) Inferred trustor matrix **F** and trustee matrix **G.**

a) Global bias: The global bias represent the average level of trust in the community. The intuition behind this is that users tend to rate optimistically in some reciprocal environments(eg.,e-commerce) while they are more conservative in others(eg., security-related applications).

b) Trustor bias: The trustor bias based on the observation that some trustors tend to generously give higher trust rating than others. This bias reflects the propensity of a given trustor to others, and it may vary a lot among different trustors.Accordingly, We can model the trustor bias as vector **x** with x(i) indicationg the trust propensity of the i^{th} trustor.

Trustee bias: The third type of bias aims to characterize the fact the some trustees might have relatively higher capability in terms of being trusted than others. Similar to second type of bias, this type of bias as vector y, where y(j) indicates the overall capability of the j^{th} trustee compared to the average.

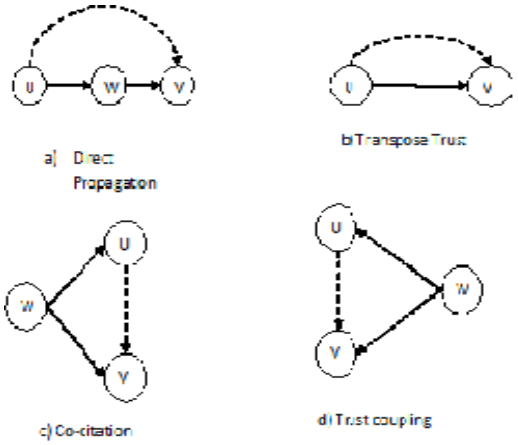
$$\mathbf{F,G}\sum \mathbf{T(i,j)-F(i,:)G(j,:)'})^2+\lambda\|\mathbf{F}\|^2+\lambda\|\mathbf{G}\|^2$$

Subjected to: $F(:,1)=\mu 1, G(:,1)=\alpha_1 1/\sqrt{n}$ (global bias)
$F(:,1)=\mu 1, G(:,1)=\alpha_1 1/\sqrt{n}$ (trustor bias)
$F(:,1)=\mu 1, G(:,1)=\alpha_1 1/\sqrt{n}$ (trustee bias)

3.3 TRUST PROPAGATION:

In Trust inference models are based on trust propagation where trust is propagated aong connected users in the trust networks.It contains four groups Direct propagation, transpose trust, co-citation and trust coupling.

Figure 2: The four propagation operators. The solid lines indicate exsisting trust relationship, and the dotted lines indicate propagated trust



Direct Propagation: Direct Propagation is probably the most intuitive way to propagate trust as shown in fig (a). The Basic operator in the figure presents the two-step propagation and it can be generalized to multiple steps. We define the first group of (t-1) propagation elements in the matrix form as $\mathbf{T^2,T^3,....T^t}$ where t is the largest propagation step.

Transpose trust: The second operator is the transpose trust as shown in fig (b). This operator indicates that user V's trust on user U can cause some level of trust in the opposite direction. site direction. This group of *t.*propagation elements can be represented in the matrix form as $\mathbf{T}^{'}$, $(\mathbf{T}')^2$, $(\mathbf{T}^{'})^3$, . . . , $(\mathbf{T}^{'})^t$.

Co-citation: Co-citation is found to be very powerful to predict trust and distrust in the Epinions website. As shown in fig (c), co-citation means that if two users u and v are both trusted by another user w, then u might also trust v to some extent. Based on the transitive closure computation, we can represent this group of propagation elements as $\mathbf{(T'T), (T'T)^2, (T'T)^3,....(T'T)^t}$.

Trust coupling: Finally, fig (d) shows the trust coupling operator, which means that if two user both trust another user, they might also trust each other. Similar to co-citation, we represent the fourth group propagation elements as $\mathbf{(TT'),(TT')^2,(TT')^3,....(T,T')^t}$.

IV THE PROPOSED MATRI ALGORITHM

In this section, we present the proposed algorithm(MATRI) to solve trust inference problem followed by some effectiveness and efficiency analysis.

4.1 THE MATRI ALGORITHM FOR CONTINUOUS CASE

This Case contains trustor/trustee matrices(F_0,G_0) due to coupling between them as well as fact that most entries of the T matrix are unknown[19]. Therefore, it seeking for global optimal solution, we try to find the local minima by alternatively updating the coefficients and the trustor/trustee matrices while fixing the other.

4..1.1 Sub-routine 1: Updating the trustor/trustee Matrices

First, let us consider how to update the trustor/trustee matrices. When we fix the coefficients (αand β).

Algorithm 1 alternateUpdate($\mathbf{P,F_0,G_0}$).

Input: the nxn matrix P, the nxr matrix F_0, and the fixed n x r matrix G_0

Output: The updated matrix F_1 of F_0

1: $F_1 = F_0$;
2: ***for*** *i=1:n* ***do***
3: *a=the vector of column indices of existing elements in P(i,j)(j=1,2,...n);*
4: *column vector* $d = 0_{|a|x1}$

5: *matrix $G_1=0_{|a|xr}$;*
6: ***for*** *j=1|a| 7: d(j)=P(I,a(j));*
8: *$G_1(j,:)=G_0(a(j),:)$;*
9: ***end for***
10: *$F_1(i,:)=(G_1'G_1+\lambda. Irxr)^{-1} G_1'd$;*
11: ***end for***
12: ***return F_1***

Where αand β are fixed coeffients, and '?' means the rating is unknown.The below algorithm are used to update and compute the propagation as we discussed in the Optimization formulation.

Algorithm 2 updateMatrix(**P,r).**
Input: The n x n matix P, and the latent factor size r
Output: The n x n trustor matrix F_0 and then n x r trustee matrix G_0

1: *generate the n x r matrices F_0 and G_0 randomly;*
2: ***While*** *not convergent* ***do***
3: *F_0 =alternateUpdate(P, F_0, G_0);*
4: *G_0=alternateUpdate(p', F_0, G_0);*
5: ***end while***
6: ***return [****F_0, G_0****];*

Algorithm 3 *computePropagation(T,l,t).*
Input*: The n x n matrix trust T, the latent factor size l, and the maximum propagation step t*
Output: *The propagation vector Z_{ij} for all (i,j) ϵ K*
1: *[L,R] = updateMatrix(T,l);*
2: ***for*** *each (i,j) ϵ K* ***do***
3: *compute Z_{ij}*
4: ***end for***
5: ***return*** *[Z_{ij}] (i,j) ϵ K ;*

4.1.2 Sub-routine 2: Computing Trust Propagation

Here, we consider how to update the coefficients(αand β) when we fix the trustor/trustee matrices.

TABLE: SYMBOL

Algorithm 4 MATRI($\mathbf{T}$, $\mathcal{K}$, r, l, t, u, v).

Input: The $n \times n$ partially observed trust matrix $\mathbf{T}$, the set of observed trustor-trustee pairs $\mathcal{K}$, the latent factor size r, the low rank l for trust propagation, the maximum propagation step t, trustor u, and trustee v

Output: The estimated trustworthiness score $\hat{\mathbf{T}}(u, v)$

Pre-computation stage:

compute bias: $[\mu, \mathbf{x}, \mathbf{y}]$ = computeBias($\mathbf{T}$) by Eq. (4);
compute propagation: $\mathbf{z}_{ij}$ = computePropagation($\mathbf{T}, l, t$), $(i, j) \in \mathcal{K}$;
initialize $\alpha_1 = \alpha_2 = \alpha_3 = 1$, $\beta_1 = \beta_2 = \ldots = \beta_{4t-1} = 0$;
while not convergent **do**
  for each $(i, j) \in \mathcal{K}$ **do**
    $\mathbf{P}(i, j) = \mathbf{T}(i, j) - (\boldsymbol{\alpha}'[\mu, \mathbf{x}(i), \mathbf{y}(j)]' + \boldsymbol{\beta}'\mathbf{z}_{ij})$;
  end for
  $[\mathbf{F}_0, \mathbf{G}_0]$ = updateMatrix($\mathbf{P}$, r);
  for each $(i, j) \in \mathcal{K}$ **do**
    $\mathbf{P}(i, j) = \mathbf{T}(i, j) - \mathbf{F}_0(i, :)\mathbf{G}_0(j, :)'$;
  end for
  $[\boldsymbol{\alpha}, \boldsymbol{\beta}]$ = updateCoefficient($\mathbf{P}$, μ, $\mathbf{x}$, $\mathbf{y}$, $\mathbf{z}_{ij}$) by Eq. (15);
end while

On-line query response stage:

return $\hat{\mathbf{T}}(u, v) = \mathbf{F}_0(u, :)\mathbf{G}_0(v, :)' + \boldsymbol{\alpha}'[\mu, \mathbf{x}(u), \mathbf{y}(v)]' + \boldsymbol{\beta}'\mathbf{z}_{uv}$;

Symbol	Definition and Description
$\mathbf{T}$	the partially observed trust matrix
$\mathbf{F}, \mathbf{G}$	the characterized trustor and trustee matrices
$\mathbf{F}_0, \mathbf{G}_0$	the sub-matrix of $\mathbf{F}$ and $\mathbf{G}$
$\mathbf{T}'$	the transpose of matrix $\mathbf{T}$
$\mathbf{T}(i, j)$	the element at the i^{th} row and j^{th} column of $\mathbf{T}$
$\mathbf{T}(i, :)$	the i^{th} row of matrix $\mathbf{T}$
$\mathcal{K}$	the set of observed trustor-trustee pairs in $\mathbf{T}$
μ	the global bias
$\mathbf{x}, \mathbf{y}$	the vector of trustor bias and trustee bias
$\mathbf{x}(i)$	the i^{th} element of vector $\mathbf{x}$
$\mathbf{z}_{ij}$	the vector of propagation elements for trustor-trustee pair (i, j)
n	the number of users
p, r	the number of bias and latent factors
s	total number of factors, $s = p + r$
t	the maximum propagation step
α_i, β_j	the weights/coefficients for bias and propagation
u, v	the trustor and the trustee
m_1, m_2, m_3	the maximum iteration number
ξ_1, ξ_2, ξ_3	the threshold to terminate the iteration

V EFFICIENCY RESULTS

We now present the efficiency results of MATRI. For efficiency experiments, we report the average wall-clock time. All the experiments were run on a machine with two 2.4GHz Intel Cores and 4GB memory. *(A) Speed Comparison*. We first present the on-line response of MATRI in the continuous case. We compare MATRI with the trust propagation models, i.e., *Cert Prop*

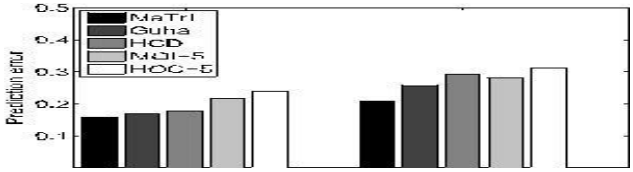
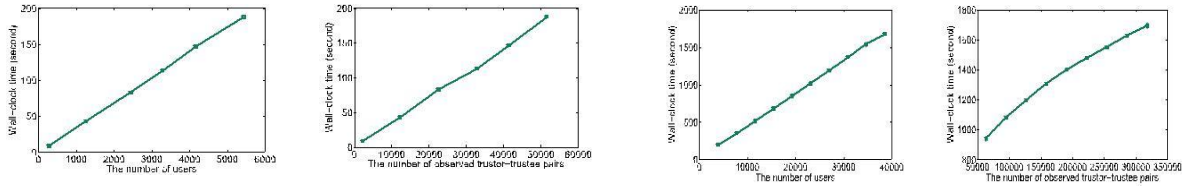


Fig. 4. Comparisons with benchmark binary trust inference and link sign prediction models. Lower is better. The proposed MATRI significantly outperforms all the other existing models wrt prediction error on both data sets.

(B) Scalability. Next, we present the scalability result of MATRI by reporting the wall-clock time of the pre-computational stage (i.e., step 1-13 in Alg. 4) in the continu-ous case. For *advogato* data set, we directly report the results on all the six snapshots (i.e., *advogato-1*, . . . , *advogato-6*). For *PGP*, we use its subsets to study the scalability. The result is shown in Fig. 6, which is consistent with the complex-ity analysis in Section 4.3. As we can see from the figure, MATRI scales linearly wrt to both n and $|K|$, indicating that it is suitable for large-scale applications. The scalability result for the binary case is similar, and we omit the figures for brevity.



(a) **(b)** **(c)** **(d)**

Fig. 3. Scalability of the proposed MATRI for continuous case. MATRI scales linearly wrt the data size (n and $|K|$). (a) Wall-clock time vs. n on *advogato*. (b) Wall-clock time vs. $|K|$ on *advogato*. (c) Wall-clock time vs. n on *PGP*. (d) Wall-clock time vs. $|K|$ on *PGP*.

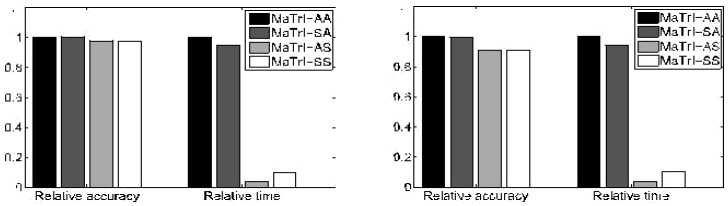


Fig. 4. Comparisons of alternative solutions of MATRI. Compared to MATRI-AA, MATRI-SS and MATRI-AS are more than 10x faster while preserving more than 90% accuracy on both data sets. (a) *advogato* data set. (b) *PGP* data set.

(C) Comparisons of the Alternatives of MATRI. As men-tioned before, the stochastic gradient descent method (SGD) could also be used for the continuous trust inference prob-lem in computing propagation vector and solving Eq. (5). We now experimentally evaluate the efficiency of all the four alternatives of MATRI. We use MATRI-AA to denote the original MATRI, MATRI-SA to denote the case when we use SGD in the propagation step, MATRI-AS.

VI RELATED WORK

In this section, we briefly review related work, includ-ing trust propagation models, multi-aspect trust inference models, etc.

Trust Propagation Models. To date, a large body of trust inference models are based on trust propagation where trust is propagated along connected users in the trust net-work, i.e., the web of locally-generated trust ratings. Based on the interpretation of trust propagation, we further cate-gorize these models into two classes: *path interpretation* and *component interpretation*.The proposed MATRI integrates the trust propagation with two other important properties, i.e., the multi-aspect of trust and trust bias. In addition, our multi-aspect model offers a natural way to speed up on-line query response; as well as to mitigate the sparsity or coverage problem in trust inference where some trustor and trustee might not be connected with each other - both are known limitations with the current trust propagation models [10].

Multi-Aspect Trust Inference Models. Social scientists have explored the multi-aspect property of trust for several years [8]. In computer science, there also exist a few trust inference models that *explicitly* explores the trust propagation.

Trust Bias in Trust Inference. In sociology, it was dis-covered a long time ago that *trust bias* is an integral part in the final trust decision [9]. Nonetheless, this important aspect has been largely ignored in most of the existing trust inference models. One exception is from Nguyen *et al*. [13], which learns the importance of several trust bias related features derived from a social trust framework. Recently, Mishra *et al*. [25] propose an iterative algorithm to compute trust bias. Different from these existing works, our focus is to incorporate various types of trust bias as specified factors/aspects to increase the accuracy of trust inference.

VII CONCLUSION

In this paper, we have proposed a trust inference model, as well as a family of algorithms to apply the model to both continuous and binary inference scenarios. The basic idea of the proposed MATRI is to leverage the multi-aspect property of trust by characterizing several aspects/factors for each trustor and trustee based on the existing trust relationships. In addition, MATRI incorporates the trust propagation and trust bias; and further learns their rela-tive weights. By integrating all these important properties, our experimental evaluations on real benchmark data sets show that MATRI leads to significant improvement over several benchmark approaches in prediction accuracy, for both quantifying numerical trustworthiness scores and pre-dicting binary trust/distrust signs. The proposed MATRI is also nimble - it is up to 7 orders of magnitude faster than the existing trust propagation methods in the on-line query response, and in the meanwhile it enjoys the linear scalabil-ity for the pre-computational stage in both time and space. Future work includes investigating the capability of MATRI to address the trust dynamics.

REFERENCES

[1] C. Ziegler and G. Lausen, "Propagation models for trust and distrust in social networks," *Inform. Syst. Front.*, vol. 7, no. 4, pp.337–358, 2005.

[2] A. Jøsang and R. Ismail, "The Beta reputation system," in *Proc. 15th Bled Electron. Comm. Conf.*, vol. 160. Bled, Slovenia, Jun. 2002.

[3] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The Eigentrust algorithm for reputation management in P2P net-works," in *Proc. 12th Int. Conf. WWW*, Budapest, Hungary, 2003, pp.640–651.

[4] M. Richardson, R. Agrawal, and P. Domingos, "Trust management for the semantic web," in *Proc. 2nd ISWC*, Sanibel Island, FL, USA, 2003, pp. 351–368.

[5] D. Cartwright and F. Harary, "Structural balance: A generalization of Heider's theory," *Psychol. Rev.*, vol. 63, no. 5, pp. 277–293, 1956.

[6] G. Liu, Y. Wang, and M. Orgun, "Trust transitivity in complex social networks," in *Proc. AAAI*, 2011, pp. 1222–1229.

[7] D. Gefen, "Reflections on the dimensions of trust and trustwor-thiness among online consumers," *ACM SIGMIS Database*, vol. 33, no. 3, pp. 38–53, 2002.

[8] D. Sirdeshmukh, J. Singh, and B. Sabol, "Consumer trust, value, and loyalty in relational exchanges," *J. Marketing*, vol. 66, no. 1, pp.15–37, 2002.

[9] A. Tversky and D. Kahneman, "Judgment under uncertainty: Heuristics and biases," *Sci.*, vol. 185, no. 4157, pp. 1124–1131, 1974.

[10] Y. Yao, H. Tong, F. Xu, and J. Lu, "Subgraph extraction for trust inference in social networks," in *Proc. IEEE/ACM Int. Conf. ASONAM*, Istanbul, Turkey, 2012, pp. 163–170.

[11] L. Xiong and L. Liu, "Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities," *IEEE Trans. Knowl. Data Eng.*, vol. 16, no. 7, pp. 843–857, Jul. 2004.

[12] J. Tang, H. Gao, and H. Liu, "mTrust: Discerning multi-faceted trust in a connected world," in *Proc. 5th ACM Int. Conf. WSDM*, Washingtion, DC, USA, 2012, pp. 93–102.

[13] V. Nguyen, E. Lim, J. Jiang, and A. Sun, "To trust or not to trust? Predicting online trusts using trust antecedent framework," in *Proc. 9th IEEE ICDM*, Miami, FL, USA, 2009, pp. 896–901.

[14] Y. Koren, "Factorization meets the neighborhood: A multifaceted collaborative filtering model," in *Proc. 14th ACM SIGKDD Int. Conf. KDD*, New York, NY, USA, 2008, pp. 426–434.

[15] R. Guha, R. Kumar, P. Raghavan, and A. Tomkins, "Propagation of trust and distrust," in *Proc. 13th Int. Conf. WWW*, New York, NY, USA, 2004, pp. 403–412.

[16] Y. Koren, R. Bell, and C. Volinsky, "Matrix factorization techniques for recommender systems," *Comput.*, vol. 42, no. 8, pp. 30–37, 2009.

[17] P. Massa and P. Avesani, "Controversial users demand local trust metrics: An experimental study on epinions. com community," in *Proc. 20th Nat. Conf. AAAI*, 2005, pp. 121–126.

[18] B. Lang, "A computational trust model for access control in P2P," *Sci. China Inform. Sci.*, vol. 53, no. 5, pp. 896–910, 2010.

[19] R. Bell, Y. Koren, and C. Volinsky, "Modeling relationships at mul-tiple scales to improve accuracy of large recommender systems," in *Proc. 13th ACM SIGKDD Int. Conf. KDD*, New York, NY, USA, 2007, pp. 95–104.

[20] H. Ma, M. Lyu, and I. King, "Learning to recommend with trust and distrust relationships," in *Proc. 3rd ACM Conf. RecSys*, New York, NY, USA, 2009, pp. 189–196.

[21] A. Buchanan and A. Fitzgibbon, "Damped Newton algorithms for matrix factorization with missing data," in *Proc. IEEE CVPR*, vol. 2. Washington, DC, USA, 2005, pp. 316–322.

[22] X. Liu, A. Datta, K. Rzadca, and E. Lim, "Stereotrust: A group based personalized trust model," in *Proc. 18th ACM CIKM*, Hong Kong, China, 2009, pp. 7–16.

[23] D. Watts and S. Strogatz, "Collective dynamics of 'small-world' networks," *Nature*, vol. 393, no. 6684, pp. 440–442, 1998.

[24] J. Leskovec, J. Kleinberg, and C. Faloutsos, "Graphs over time: Densification laws, shrinking diameters and possible explana-tions," in *Proc. 11th ACM SIGKDD Int. Conf. KDD*, Chicago, IL, USA, 2005, pp. 177–187.

[25] C.-W. Hang, Y. Wang, and M. P. Singh, "Operators for propagating trust and their evaluation in social networks," in *Proc. 8th Int. Conf. AAMAS*, Budapest, Hungary, 2009, pp. 1025–1032.

[26] J. Leskovec, D. Huttenlocher, and J. Kleinberg, "Predicting posi-tive and negative links in online social networks," in *Proc. 19th Int. Conf. WWW*, Raleigh, NC, USA, 2010, pp. 641–650.

[27] Y. Wang and M. P. Singh, "Trust representation and aggregation in a distributed agent system," in *Proc. 21st Nat. Conf. AAAI*, 2006, pp.1425–1430.

[28] Y. Wang and M. P. Singh, "Formal trust model for multiagent systems," in *Proc. 20th IJCAI*, San Francisco, CA, USA, 2007, pp.1551–1556.

[29] C. Hsieh, K. Chiang, and I. Dhillon, "Low rank modeling of signed networks," in *Proc. 18th ACM SIGKDD Int. Conf. KDD*, Beijing, China, 2012, pp. 507–515.

[30] K.-Y. Chiang, N. Natarajan, A. Tewari, and I. S. Dhillon, "Exploiting longer cycles for link prediction in signed net-works," in *Proc. 20th ACM CIKM*, Glasgow, Scotland, U.K., 2011, pp.1157–1162.