MACQUARIE
University
SYDNEY · AUSTRALIA

Trust Prediction in Online Social Networks

by

Xiaoming Zheng

A thesis submitted in fulfillment
of the requirements for the degree of
Doctor of Philosophy
in the
Department of Computing
Faculty of Science and Engineering
Macquarie University

Supervisor: Prof. Mehmet A. Orgun
Associate Supervisor: A/Prof. Yan Wang

2015

Statement of Candidate

I certify that the work in this thesis entitled **"Trust Prediction in Online Social Networks"** has not previously been submitted for a degree nor has it been submitted as part of requirements for a degree to any other university or institution other than Macquarie University.

I also certify that the thesis is an original piece of research and it has been written by me. Any help and assistance that I have received in my research work and the preparation of the thesis itself have been appropriately acknowledged.

In addition, I certify that all information sources and literature used are indicated in the thesis.

Xiaoming Zheng

Xiaoming Zheng

17 September 2015

To my parents,

Shiqiang Zheng and Shouqing Wang,

who dedicated all their life to me

Abstract

Online Social Networks (OSNs) have become an integral part of daily life in recent years. They have been used as a means for a rich variety of activities, such as seeking service providers or recommendations. In these activities, trust is one of the most important factors for participants' decision-making process. Therefore, it is necessary and significant to predict the trust between two participants who have no direct interactions. My thesis aims to provide effective and efficient trust prediction approaches to evaluate trust values, which are introduced from the following four aspects.

The first aspect of the work is to study the factors that affect trust in OSNs and solve the trust network extraction problem. OSNs contain important participants, the trust relations between participants, and the contexts in which participants interact with each other. All of such information has a significant influence on the prediction of the trust from a source participant to a target participant without direct interactions. In addition, the trust network, containing a truster and a trustee without direct interactions, is the foundation to perform trust prediction. The extraction of a small-scale trust subnetwork can deliver efficient and effective trust prediction results. We propose two heuristic algorithms called NBACA and NACA for the extraction of such subnetworks.

The second aspect of the work is to address the trust prediction problem in the trust network without any contextual information. We first analyze and extract the features which affect the trust prediction from trust rating values in a trust network. Then, a new trust prediction model based on trust decomposition and matrix factorization is proposed to predict the trust value from a truster to a trustee. In this model, trust is first decomposed into trust tendency and tendency-reduced trust. Based on tendency-reduced trust ratings, matrix factorization with a regularization term is leveraged to predict the tendency-reduced values of missing trust ratings, incorporating both propagated trust and the similarity of users' rating habits. Finally, the missing trust ratings are composed with predicted tendency-reduced values and trust tendency values.

The third aspect of the work is to study the trust prediction problem in OSNs with social contextual information. We first categorize the factors that affect trust, and utilize them according to their categories, to transfer or calculate existing trust values. Then, a new trust transference method is proposed to predict the trust in a target context from that in different but relevant contexts. Next, a social context-aware trust prediction model based on matrix factorization is proposed to predict trust from a source participant to a target participant in various situations. Finally, we analyze the contextual trust prediction in three common scenarios.

The fourth aspect of the work is to study the dynamic trust to online service providers to assist the decision making regarding a future interaction. First, static features and dynamic features are extracted from historical interaction records. Then, Principal Component Analysis and Vector Quantization techniques are leveraged to reduce the dimension of features and project them into discrete values. Last, an approach based on Hidden Markov Model is proposed to model the dynamic changes of trust, and to predict the trust in the future interactions.

For all the proposed approaches, extensive experiments have been conducted or analyzed on real datasets, semi-synthetic datasets, synthetic datasets or real scenarios, which demonstrates that they are superior to the exiting approaches in terms of quality of results and efficiency.

Acknowledgments

First of all, I would like to express my sincere appreciation to my supervisor Prof. Mehmet A. Orgun and associate supervisor A/Prof. Yan Wang for letting me fulfill my dream of doctorate. They have continually and convincingly conveyed a spirit of adventure in regard to research and scholarship over the past few years. Without their persistent encouragement and endless guidance, this work would not have been possible. It is my great fortune to have them as my supervisors at Macquarie University.

In addition, my colleagues have helped me develop this work. I wish to express my thanks to Guanfeng Liu, Joe Zou, Haibing Zhang, Lie Qu and Bin Ye, for providing a friendly and enjoyable environment during these years.

Many thanks to the staff in the Department of Computing for their help. I would like to thank Donna Hua, Camille Hoffman, Sylvian Chow, Melina Chan, Fiona Yang and Jackie Walsh for their warm support.

Most important of all, I would like to thank my family. My parents, Shiqiang Zheng and Shouqing Wang, have always been there for me. Their love, support and encouragement have been the foundation for my life. I wish to thank them for all the opportunities they have made available to me, and for the support they have given me during my life. Without their love, unwavering support and inspiration, this work could never have been accomplished.

Publications

This thesis is based on the research work I have performed with the help of my supervisor and associate supervisor and other colleagues during my PhD program at the Department of Computing, Macquarie University between 2012 and 2015. Some parts of my research have been published in the following papers:

[1] **Xiaoming Zheng**, Yan Wang and Mehmet A. Orgun, Subnetwork Extraction in Social Networks, 14th IEEE International Conference on Trust (IEEE TrustCom 2015), August 20-22, Helsinki, Finland (**CORE2014 Rank A**).

[2] **Xiaoming Zheng**, Yan Wang and Mehmet A. Orgun, BiNet: Trust Subnetwork Extraction using Binary Ant Colony Algorithm in Contextual Social Networks, 22th IEEE International Conference on Web Services (IEEE ICWS 2015), pages 321-328, June 27-July 2 , New York, USA (**CORE2014 Rank A**).

[3] **Xiaoming Zheng**, Yan Wang, Mehmet A. Orgun, Guanfeng Liu and Haibin Zhang, Social Context-Aware Trust Prediction in Social Networks, 12th International Conference on Service Oriented Computing (ICSOC 2014), pages 527-534, November 3-6, 2014, Paris, France (**CORE2014 Rank A**).

[4] **Xiaoming Zheng**, Yan Wang, Mehmet A. Orgun, Youliang Zhong, Guanfeng Liu, Trust Prediction with Propagation and Similarity Regularization, 28th AAAI Conference on Artificial Intelligence (AAAI-14), pages 237-243, July 27-31, 2014, Qubec City, Qubec, Canada. (**CORE2014 Rank A***).

[5] **Xiaoming Zheng**, Yan Wang and Mehmet A. Orgun, Modeling the Dynamic Trust of Online Service Providers using HMM, 20th IEEE International Conference on Web Services (IEEE ICWS 2013), pages 459-466, June 27-July 2, Silicon Valley, California, USA (**CORE2014 Rank A**).

[6] Youliang Zhong, **Xiaoming Zheng**, Jian Yang, Mehmet Orgun, and Yan Wang, KPMCF: A Learning Model for Measuring Social Relationship Strength, 14th International Conference on Web Information Systems Engineering (WISE2013), pages 519-522, October 13-15, 2013, Nanjing, China (**CORE2014 Rank A**).

Contents

List of Figures

List of Tables

Chapter 1

Introduction

A social network is a social structure consisting of a set of nodes (i.e., individuals or organizations) and a set of links (i.e., interactions) connecting them, which is first proposed in 1800s [53, 50, 214]. Major developments of social networks took place in the 1930s in the fields of psychology, anthropology, and mathematics respectively [175, 176]. In psychology, social interactions between participants were first systematically recorded and analyzed by Moreno [176] in small groups, such as classrooms and work groups. In anthropology, the theoretical and ethnographic works of Malinowski et al. [135, 161, 105] form the foundation of social networks. And in sociology, Parsons [156] studied the social structure by analyzing the social relationships between participants, which provided the foundation for sociologist Blau's work in analyzing the relational ties of social units on social exchange theory [26].

Nowadays, a diverse range of online social networks (OSNs), such as Facebook[1], Renren[2], Twitter[3], LinkedIn[4] and Google+[5], have sprung up attracting an increasingly large number of participants. According to the statistics by a web statistic company *The eBusiness Knowledgebase*[6] on March 1st, 2015, the top 10 popular OSNs and the approximate number of the monthly unique visitors of them are listed in Table 1.1. From the table, we can see that, for the most popular OSN, Facebook, the number

[1] http://www.facebook.com/

[2] http://www.renren.com/

[3] http://www.twitter.com/

[4] http://www.linkedin.com/

[5] http://plus.google.com/

[6] http://www.ebizmba.com/

of unique visitors in a month approximates 900,000,000. Along with the continuous popularity of OSNs, in recent years, social networking websites have proliferated to be the platform for a variety of activities. For instance, according to a survey on 2600 hiring managers in 2009 by a popular job-hunting website CareerBuilder[7], 45% of those managers used social networking sites to investigate potential employees. In 2012, the ratio increased to 90%. Furthermore, by connecting with OSNs (e.g., Facebook and Twitter), at some e-commerce websites such as ThisNext[8] and eBay[9], buyers can recommend the products on these e-commerce websites to their friends who participate the OSNs. In this type of activities, trust is one of the most important factors for participants' decision making. Conceptually, trust is the belief that an entity, such as a person or an organization, will behave in an expected manner, despite the lack of the ability to monitor or control the environment in which it operates [180]. As most participants do not have previous direct interactions, approaches and mechanisms are required to predict the trustworthiness between participants who are unknown to each other.

Table 1.1: Top 10 popular OSNs

Ranking	Name	URL	Unique Monthly Visitors
#1	Facebook	facebook.com	900,000,000
#2	Twitter	twitter.com	310,000,000
#3	LinkedIn	linkedin.com	255,000,000
#4	Pinterest	pinterest.com	250,000,000
#5	Google+	plus.google.com	120,000,000
#6	Tumblr	tumblr.com	110,000,000
#7	Instagram	instagram.com	100,000,000
#8	VK	vk.com	80,000,000
#9	Flickr	flickr.com	65,000,000
#10	Vine	vine.co	42,000,000

An Online Social Network (OSN) can be represented as a graph, as shown in Fig. 1.1. A node in the graph represents a participant in an OSN while the edge

[7] http://www.careerbuilder.com/

[8] http://www.thisnext.com/

[9] http://www.ebay.com/

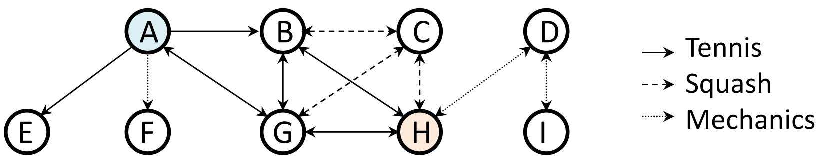
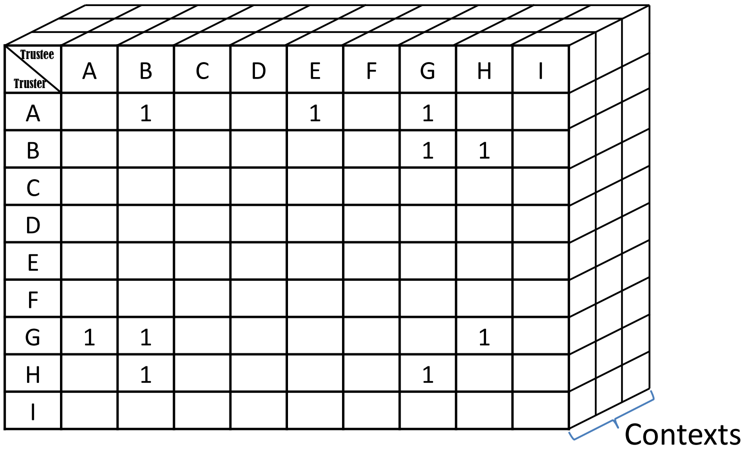


Figure 1.1: A contextual trust social network

Trustee Truster	A	B	E	G	H
A		1	1	1	
B				1	1
E					
G	1	1			1
H		1		1	

Figure 1.2: The social trust matrix in the context of playing tennis

pointing from one node to an adjacent node corresponds to their real-world or online interactions (e.g., $A \rightarrow B$ and $B \rightarrow C$ in Fig. 1.1). Different types of edges represent different contexts, which refer to any information available for characterizing the participants and the situations of interactions between them [206]. For example, a solid line refers to the relationship in playing tennis, a dashed line refers to squash and a dotted line refers to mechanics in Fig. 1.1. For adjacent nodes (i.e., the nodes with a directed link between them), the trust can be explicitly given by one participant to another based on their history of interactions. In OSNs, each participant usually has interacted with a number of others forming multiple connections from one node. All such participants and links form the social trust network (e.g., Fig. 1.1). In OSNs, such a trust network is essential and fundamental for the trust prediction of two nonadjacent participants, since it contains the important intermediate participants, the trust relations between those participants and social context. All of these have critical influences on the trust prediction between any unknown participants in OSNs. In addition, when a social trust network is represented in the form of a matrix regarding one context, it



Trustee / Truster	A	B	C	D	E	F	G	H	I
A		1			1		1		
B							1	1	
C									
D									
E									
F									
G	1	1						1	
H		1					1		
I									

Figure 1.3: A contextual social trust cube

is termed as a social trust matrix, e.g., Fig. 1.2. Furthermore, all the trust matrices, regarding all the contexts respectively, form a social trust cube (e.g., Fig. 1.3).

This thesis will focus on the following two types of significant challenging problems: trust network extraction and trust prediction in OSNs.

1.1 Challenges of Trust Prediction in OSNs

1.1.1 Trust Subnetwork Extraction

In a social network depicted in Fig. 1.1, suppose A is looking for a service provider, such as a tennis coach, and H is recommended to A as a tennis coach. However, A does not know H before. In such a situation, according to the theory of social psychology [39, 136] and computer science [65, 118], the trust of H in A's mind can be predicted using trust prediction methods [69, 66, 114, 131, 243]. Here we assume, playing tennis is the *target context*, i.e., the context in which the trust between a source node and a target node needs to be predicted. In A's mind, B, E and G are good tennis players. B, G and H trust each other and G also trusts A regarding tennis playing. C trusts B, G and H regarding squash playing and vice versa. D, F, H and I are good machinists. In order to predict if H will be a good tennis coach in A' mind, it

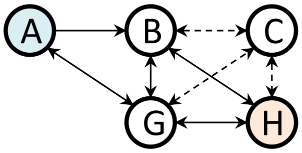


Figure 1.4: An extracted trust subnetwork

is unnecessary to use the whole social network in Fig. 1.1, because F, D and I are only good at mechanics while tennis player E has no knowledge of others, and they hardly affect the prediction of the trust to H in A's mind. Let us assume that this social network is only constructed in three contexts: tennis, squash and mechanics. In order to boost the efficiency and effectiveness of trust prediction regarding the target context tennis, the social subnetwork in Fig. 1.4 is extracted from Fig. 1.1 by removing the social relations in mechanics and keeping only the important social relations for the prediction of trust between A and H on tennis and squash playing, because mechanics is irrelevant to the target context tennis, while squash is relevant to tennis.

In the literature, there are some existing works focusing on *trust prediction*, i.e., the process of estimating a new pairwise trust relationship between two nonadjacent participants. Most of these works predict trust based on social graphs (e.g., Fig. 1.4) using inference approaches [66, 119], while a few of them predict trust from a trust matrix (i.e., Fig. 1.2 and 1.3, the representation of social networks in matrices rather than graphs) using matrix factorization approaches [78, 243]. However, all these works assume that the trust network has already been extracted, or even that the whole dataset is directly used.

Therefore, given any two participants who do not have any historical direct interactions, extracting a trust subnetwork containing them from a large-scale social network becomes a critical and fundamental step prior to performing any trust prediction. Such a task is called *trust subnetwork extraction*. An extracted subnetwork (e.g., Fig. 1.4) needs to satisfy the following requirements: (i) it should contain the source node, the target node and most of the nodes which are important for trust prediction between the source node and the target node; (ii) the scale of the subnetwork/matrix is kept relatively small; and (iii) a source participant may introduce constraints of trust relations or contextual information into the subnetwork extraction process for various purposes, such as employee recruitment and movie recommendation, which makes the problem more challenging.

Such an extracted trust subnetwork can help improve the effectiveness and efficiency of trust prediction [162, 117]. However, extracting such a trust subnetwork/matrix is a multi-objective optimization problem, which is known to be NP-complete [17, 117].

In the literature, there are very few approximation algorithms proposed for the NP-complete subnetwork extraction problem for trust prediction in online social networks. As the resource discovery problem in peer-to-peer (P2P) networks has some similar properties as the trust network extraction problem, some search strategies from P2P networks can be applied to trust network extraction. These approaches can be divided into two groups: *traversal methods* [35, 54] and *heuristic methods* [62, 63, 6, 73, 115, 117]. For the application on small-scale datasets, the traversal methods are able to search the best subnetwork by adopting methods, such as breadth-first search and depth-first search. However, on large-scale datasets, it is computationally unfeasible to find the optimum solution, and therefore, only heuristic methods can be used to find a near-optimal solution. Most of the relevant existing works do not consider the social context in online social networks, such as expertise (e.g., an expert in a domain) and preference (e.g., like playing tennis), which have significant influence on trust prediction [31, 111, 231] and can be obtained by data mining techniques [141, 193]. On the other hand, the existing works all rely on the existing social paths, which limits the performance of trust prediction as some aspects such as expertise can affect the trust without the need of social connections. In short, according to our knowledge, there is no existing approach that focuses on the context-aware trust subnetwork extraction problem specifically for trust prediction based on matrix factorization.

1.1.2 Social Trust Prediction

With the development of Internet, people are increasingly active in various large, open and dynamic network systems, including social networks, P2P systems, e-commerce and e-service [208]. Due to many reasons such as the lack of diligence from users and privacy concerns, missing trust values in a social trust network are inevitable [78]. On the other hand, uncertainty exists in online environments, especially those of e-commerce and e-service. The prediction of the trust about online service applications has been growing in importance [236][209][207]. Conceptually, *trust prediction* is the process of estimating a new pair-wise trust relationship between two participants in a context, who are not directly connected by interactions in the context [243]. The challenges of trust prediction are introduced in the following three different situations.

1.1.2.1 Single-Context Trust Prediction

Many online social networks (e.g., Advogato [1]) allow users to give a trust value to their friends, or to select a word from a list to describe the trust relationship between them and their friends. The missing trust values can be predicted from trust ratings in the forms of numbers or words.

The traditional approaches to predict trust are to evaluate trust from a source user to a target user along a path between them that consists of links and trust values [69]. This type of approaches is termed as propagation-based trust prediction (i.e., trust propagation/inference). Trust propagation has been studied in many web application areas, including e-commerce [209, 236, 235], P2P systems [220], and social networks [82, 66, 119]. On the other hand, a user tends to trust other users who are similar to himself/herself [112]. The trust value can be predicted from the behavior of giving ratings in the trust matrix using latent factor models, such as matrix factorization. Broadly speaking, latent factor-based trust prediction models are to estimate the trust between two users from their similar habits etc. revealed in the trust ratings [225, 226, 131].

In the literature, existing works predict trust either via trust propagation only [69, 66, 114, 206], or considering propagated trust and tendency [225, 226], or merely utilizing the similarity of rating values [131, 132]. In general, they have the following drawbacks. First, all the tendency, propagated trust and similarity influence the trust between two users. All of them should be utilized to predict pair-wise trust, rather than considering only one or two influential factors. Second, the similarity of trust rating distributions describes the similarity of users' behaviors in giving trust ratings. Thus, it is valuable for trust prediction [241]. However, it has been neglected in the literature. Third, all these factors are of different types, representing either personal properties or interpersonal properties. Therefore, they should be processed separately and differently so as to deliver high accuracy in trust prediction.

1.1.2.2 Context-Aware Trust Prediction

Besides trust values or ratings, in recent years, online social networks have an amount of context information, which can be mined by data mining techniques [141, 193]. Trust is context dependent [180] and it is rare for a person to have full trust on another in every facet [189]. For example, the case of full trust in all aspects is less than 1% at Epinions[10] and Ciao[11], both of which are popular product review websites [189]. In real life, people's trust to another is limited to certain domains. For instance, in Fig. 1.1, A trusts F in the context of mechanics because they had interactions in this context before. However, this does not mean A trusts F in the other contexts of playing tennis or playing squash. Therefore, the contextual information should be utilized to further improve trust prediction.

In the literature, some studies have suggested to predict trust taking into account some kind of social contextual information. Liu et al. [117] propose a randomized algorithm for searching a subnetwork from a source participant to a target one, which takes important contextual information into account for trust evaluation. An approx-

[10] http://www.epinions.com/
[11] http://www.ciao.co.uk/

imation algorithm is proposed in [118] to search the near optimal social trust path satisfying service providers with context constraints. Wang et al. [206] propose a probabilistic social trust model to infer trust along a path in a social network exploring all available social context information. Ma et al. [132] consider social tags to calculate the preference similarity between friends. Zhong et al. [244] propose the KPMCF model to learn social relationship strength by analyzing profile information including tags, groups etc.

However, as pointed out in [41], social tags have limited capacity in reflecting personal information, including individual preference, domain expertise, and the relationship and intimacy with others. Social context should contain any information that reflects an individual's social characteristics, and the social relationship with other people within a social network [206]. Currently, most trust prediction models suffer from the following drawbacks: (i) The property of trust values has not been studied sufficiently. For example, the similarity of people's trust can be modeled not only from the trust values, but also from their distributions [241]; (ii) The diversity of social contexts is not well dealt with. In real life, the connection between two people can be friendship, family member, business partnership, or classmate etc. Even with the same type of relationship—say friendship, their interaction frequency and interaction contexts can be largely different [206]; (iii) The ways to incorporate social information require further study, as inappropriate introduction of social information may introduce noise and degrade the trust prediction quality [122]; (iv) Differences of contextual information are not handled properly. For example, how to model the relationship of two contexts? To what extent, the trust in context c_i can be transferred to context c_j?

1.1.2.3 Dynamic Trust Prediction

Trust may change as time goes on especially in an online environment [241]. In online environments, especially in e-commerce and e-service environments, the system maintains the past interaction information for a certain period which offers the possibility to predict a participant's (e.g., a service provider's) future trust. There are many factors that affect a participant's trust [48]. For instance, in e-commerce web sites, such as eBay and Taobao[12], the trust to a seller can be binary, i.e., honest or cheating. It may vary unwittingly or consciously according to different items, different buyers etc. It is more likely to trade imprudently in the afternoon just before the closing time or in peak time [234, 235, 236]. So, the trust of a participant dynamically changes.

In the literature, a number of approaches have been proposed to model dynamic trust of participants in e-commerce and e-service environments. The Beta model is an early static model in which the trustworthiness of any service provider is assumed to be represented by a fixed probability distribution over outcomes [82]. The Beta model with a decay factor introduces an exponential decay factor to control the weight of each outcome according the time of occurrence [52]. Although this approach shows success in certain scenarios, it is not effective in other scenarios where the provider's behavior is highly dynamic. Several studies [52, 149] propose the Hidden Markov Model (HMM) approaches in modeling transaction results, only focusing on the outcomes of each past transaction. However, these approaches ignore the contextual information about each transaction. Liu and Datta [124] propose a Markov model based on contextual information, which extracts features from transaction contextual information as the HMM observation sequences, and treats the outcomes directly as the states of the models. However, it reveals the hidden states and the authors also assume a series of transactions occurring between a seller and the same customer, which can hardly be true in most actual scenarios. In addition, there could be more features to be taken into account, such as price changes, in addition to static features in the contextual information.

1.2 Contributions of the Work

To extract a trust subnetwork for a source participant and a target participant is the first step prior to the trust prediction between them. It is the foundation of any kind of

[12] http://www.taobao.com

trust prediction. Based on the extracted trust subnetwork, the trust prediction between two unknown participants is studied in three situations: single-context trust prediction, context-aware trust prediction, and dynamic trust prediction.

In order to address the above significant and challenging problems of the trust prediction in online environments of different situations, described in Section 1.1, this thesis makes four major contributions.

1. The first contribution in this thesis is to extract a small-scale subnetwork, from the original large-scale social trust network, containing most of the important nodes and contextual information with a high density rate, in order to make the trust prediction between two nonadjacent participants more efficient and effective.

   (a) The contextual factors that affect trust prediction between two participants in a complex online social network are analyzed, which includes role impact factor, reliability preference, social intimacy and existing trust.

   (b) A trust utility function is proposed to take the above trust impact factors into account to illustrate the attributes of each participant in a social network.

   (c) To address the NP-complete trust subnetwork extraction problem, inspired by the ant colony foraging process [47, 27], we propose two heuristic algorithms: (i) A novel binary ant colony algorithm (NBACA) is designed for the trust subnetwork extraction problems, by adding an initialization process and a mutation process and improving the path selection and pheromone update process of a conventional binary ant colony algorithms; (ii) A new ant colony algorithm (NACA) is designed for the subnetwork extraction problems. The mutation process designed for this algorithm enhances the mechanism of path selection and pheromone update processes, allowing it to further refine existing solutions.

The experiments, conducted on two popular social network datasets, Epinions and Slashdot[13], demonstrate the superior performance of our proposed approaches over the state-of-the-art approaches in terms of the quality of extracted trust subnetworks and execution time.

2. The second contribution in this thesis is to predict missing trust values from existing trust rating values, which incorporates more influential factors in matrix factorization in order to improve the performance of trust prediction.

   (a) Trust ratings are deeply analyzed and decomposed into trust tendencies (i.e., trustor tendency and trustee tendency) and tendency-reduced ratings, which enables trust prediction with tendency-reduced ratings to reduce the negative effect of trust tendency.

   (b) A new trust prediction model based on rating decomposition and matrix factorization is proposed. Our model considers the similarity of trust rating distributions to further differentiate the trust between users and optimize matrix factorization. This is particularly important when the common trust rating values are the same. In addition, our model considers both propagated trust and similarity factors, which consist the propagation and similarity regularization term of matrix factorization, in order to improve the trust prediction accuracy.

   Regarding the commonly used metrics of Mean Absolute Error (*MAE*) and Root Mean Square Error (*RMSE*), the experiments conducted on a real-world dataset, Advogato[14], have demonstrated significant improvements delivered by our model when comparing the trust prediction accuracy with the state-of-the-art approaches.

3. The third contribution in this thesis is social context-aware trust prediction,

[13] http://slashdot.org/

[14] http://www.trustlet.org/wiki/advogato_dataset

which utilizes social contextual information to further improve the accuracy of trust prediction in online social networks.

   (a) We analyze the personal properties and interpersonal properties which impact trust transference between contexts.

   (b) A new trust transference method is proposed to predict the trust in a target context from that in different but relevant contexts. In addition, the trust transference method mitigates the sparsity problem, and enhances the trust prediction accuracy.

   (c) A social context-aware trust prediction model based on matrix factorization is proposed to predict trust in various situations no matter whether there is a path from a source participant to a target participant. To the best of our knowledge, this is the first context-aware trust prediction model in social networks in the literature.

       Comparisons are conducted in trust inference between contexts, trust prediction without trust connection and trust inference based on trust paths. The experimental analysis in these three typical scenarios illustrates that the proposed model can mitigate the sparsity situation in social networks and generate more reasonable trust results than the state-of-the-art context-aware trust inference approach.

4. The fourth contribution in this thesis is to predict the trust value between an online service provider and a potential customer regarding a future transaction, considering the dynamic changes of the provider and contextual information in online environments, which tries to help customers avoid deceitful online providers.

   (a) The dynamic trust to service providers is modeled concerning a forthcoming transaction in light of as much information as we can consider, including static features, such as the provider's reputation and item price, and dynamic features, such as the latest profile changes of a service provider and price changes.

(b) Based on a service provider's historical transactions, we predict the trustworthiness of the service provider in a forthcoming transaction. In addition, Mutual Information theories [92] and the Principle Component Analysis method [4] are leveraged to eliminate redundant information and combine essential features to form lower dimensional feature vectors. Furthermore, by adopting Vector Quantization techniques [195], we apply the discrete HMM in a more powerful way, in which all the features extracted from both contextual information and the rating of each transaction are treated as observations of the HMM.

We evaluate our approach empirically in order to study its performance. Experiments are conducted in order to compare the prediction accuracy between our model and other representative ones. The experiment results illustrate that our approach significantly outperforms the state-of-the-art probabilistic trust methods in accuracy in the cases with complex changes.

1.3 Roadmap of the Thesis

This thesis is structured as follows.

Chapter 2 proposes a comprehensive literature review of online social networks, trust and three types of trust prediction methods: propagation-based trust prediction, latent factor-based trust prediction and dynamic trust prediction, each of which predicts trust values in both situations: trust rating vales only (single-context trust prediction) and contextual information (context-ware trust prediction).

Chapter 3 presents the factors that affect trust in an online social network. Then, two ACA-based trust subnetwork extraction approaches, called BiNet and TrustNet, are proposed, taking these trust impact factors into account. Experiments conducted on two popular datasets, Epinions and Slashdot, demonstrate that our approaches can extract subnetworks covering important participants and contextual information while keeping a high density rate, which is superior to the state-of-the-art approaches in terms of the quality of extracted subnetworks within the same execution time .This chapter is based on our papers published at ICWS2015 and TrustCom2015 (please refer to [2] and [1] in the publication list on pages ix).

Chapter 4 analyzes the personal properties and interpersonal properties, extracted from trust ratings, which affect trust prediction. Then a trust prediction model based on trust decomposition and matrix factorization is proposed, which takes into account these properties. Experiments conducted on a real trust rating dataset demonstrates better performance of our model compared with the existing ones in terms of MAE and RMSE. This chapter is based on our paper published at AAAI 2014 (please refer to [4] in the publication list on page ix).

Chapter 5 analyzes the contextual trust impact factors, proposes a trust transitivity approach to transit trust between relevant contexts, and proposes a trust prediction model based on matrix factorization. The experimental analysis demonstrates the effectiveness and capability of our model to predict trust, taking into account the contextual information in typical scenarios in the real world. This chapter is based on our paper published at ICSOC 2014 (please refer to [3] in the publication list on page ix).

Chapter 6 proposes a dynamic trust prediction approach based on Hidden Markov Model, taking both of the contextual information and trust as observations. In this approach, techniques, such as Mutual Information, Principle Component Analysis and Vector Quantization, are leveraged to lower the dimension of feature vectors and enhance the accuracy of dynamic trust prediction. Experiments conducted on synthetic datasets of different scenarios demonstrate that our approach is more effective in predicting the future trust in complex dynamics. This chapter is based on our paper published at ICWS 2013 (please refer to [5] in the publication list on page ix).

Finally, Chapter 7 concludes the work in this thesis and discusses some directions for future research opportunities.

Chapter 2

Literature Review

In recent years, a diverse range of Online Social Networks (OSNs) have attracted an increasingly large number of users and proliferated to be a platform for a variety of activities, where trust between participants has significantly affected their decision making. In the literature, a number of scholars, across different fields, have studied social network properties, the definitions, properties and influence of trust, the social contexts affecting trust, as well as trust prediction methods in OSNs. In this chapter, a literature review on the above aspects is organized as follows:

- Section 2.1 introduces the properties of social networks, and presents a new taxonomy of OSNs.
- Section 2.2 introduces the definitions of trust existing in different disciplines, the general properties of trust, the influence of trust, and the social contexts that affect trust.
- Section 2.3 reviews the studies on trust subnetwork extraction in OSNs.
- Section 2.4 reviews the existing studies on different types of trust prediction in OSNs, including propagation-based trust prediction, latent factor-based trust prediction, and dynamic trust prediction.

2.1 Online Social Networks

In the discipline of social science [214], a social network is described as a social structure made up of a set of entities (such as individuals or organizations) and the dyadic ties between these entities. A clear way of analyzing the structure of the whole social entities is provided in the perspective of social networks. In this section, social network properties and a new taxonomy of OSNs will be introduced.

2.1.1 Social Network Properties

The foundation of social network theory can be traced back to the theoretical and ethnographic work of Bronislaw Malinowski in anthropology [135] in 1913. Major development of social networks took place in the 1930s in different fields including psychology, anthropology and sociology, when Jacob Moreno systematically recorded and analyzed social interaction in small groups, and Talcott Parsons set the stage for taking a relational approach to understanding social structure [176, 175, 156].

The *small-world* characteristic (also known as ‘six degrees of separation’) in social networks was validated by Milgram [145] in the 1960s, illustrating that the average path length between two Americans was about six hops in an experiment of mail sending. In the 1970s, the influence of small-world characteristic on human interactions was further analyzed by Pool et al. [157].

Associativity is a pervasive phenomenon found in many networks and has a profound effect on the structural properties of a social network. Conceptually, associativity is the tendency for participants in a social network to be connected to others with similar characteristics in some way [152]. McPherson et al., [143] validate the associativity characteristic in social networks. Namely, in social networks, individuals commonly choose to associate with others similar to themselves in aspects such as age, nationality, location, race, income, educational level, religion and language.

A common property of many large social networks is that the node connectivity follows a *scale-free power-law distribution* [18, 10, 106]. Networks are usually open and formed by the continuous addition of new nodes (participants) to the system. Thus the number of nodes increases throughout the lifetime of the network, e.g., the World Wide Web grows exponentially over time by adding new web pages. Furthermore, the nodes with a high-degree connection tend to be connected to other nodes with a high-degree connection, which is discussed in detail by Li et al. [106]. In addition, new nodes tend to attach to existing well-connected sites preferentially [18], e.g., a new participant of Facebook is more likely to join a group of well-known popular participants with an already-high connectivity.

In graph theory, a *clustering coefficient* measures the degree to which nodes in a graph tend to cluster together. It is calculated as the average proportion, between the existing edge number and the maximum edge number, over each node's neighbors in a social network [215]. In addition, in a network with a high clustering coefficient, if A has a connection with B and C, then B has a high probability to connect with C. Holland et. al [74] have validated that a social network usually has a high clustering coefficient, which means most of the people we know may also know one another in the social network in real-world scenarios.

In the past few years, sociologists and computer scientists have begun to investigate the characteristics of online social networks, which are gaining growing popularity. Ahn et al. [8] compare the online social networks with real-life social networks by analyzing the structures of three online social networking services: Cyworld[1], MySpace[2] and Orkut[3], in terms of degree distribution, clustering coefficient, degree correlation and average path length. Mislove et al. [146] analyze the structure of many popular large-scale online social networks, including Flickr[4], YouTube[5], LiveJournal[6] and Orkut, and confirm the power-law, small-world and scale-free characteristics. Holme

[1] http://www.cyworld.com/

[2] https://myspace.com

[3] http://www.orkut.com

[4] http://www.flickr.com/

[5] http://www.youtube.com/

[6] http://www.livejournal.com

et al. [75] study the time evolution of an Internet dating community, Pussokram[7], in the aspects of clustering, correlations, average geodesic length, degree and reciprocity. McCallum et al. [141] discovers relationships and social roles from the Enron Email Dataset[8] using data mining techniques.

In recent years, the boundary between the social network and e-commerce has become vague. In 2005, Yahoo first introduced the concept of social commerce, which uses social networks in the context of e-commerce [3]. The service helps people establish an online presence, and exploits the user base for commercial purposes [8]. A Lucid Marketing survey finds that 68% of individuals consult friends and relatives before purchasing home electronics, which is more than the half who use search engines for product information [77]. Leskovec et al. [102] analyze the influence of social relationships in a person-to-person recommendation network for effective viral marketing. Guo et al. [70] analyze the influence of social interactions between buyers on the purchase decisions made by a buyer in buying products in Taobao, the world's largest online shopping website. In addition, e-commerce was integrated into online social networks, such as Twitter, as the mock-up of a new platform called Twitter Commerce in early 2014 [2].

2.1.2 The Categorization of OSNs

Online social networks can be extracted from many aspects, such as user relationships through transactions on e-commerce websites, email connections, affinities and co-authors in academic papers. Mislove et al. [146] point out that 1) online social networks are organized around users, in which, participants join a network, publish their profile and content, and create links with other participants; and 2) online social networks provide the basis for maintaining social relationships, finding user similarity and locating certain content and knowledge regarding users. Golbeck et al. [64, 65] define an online social network as "a web-based social network" which must possess

[7] http://www.pussokram.com/

[8] http://www.cs.cmu.edu/enron/

the following four characteristics: 1) accessibility over the web with a web browser, 2) explicitly stated relationships with others, 3) explicitly built-in support for users making connections, and 4) the visibility of relationships. Boyd et al. [29] define online social networks as "web-based services that allow individuals to 1) construct public or semi-public profiles within a bounded system, 2) articulate a list of other users with whom they share connections, and 3) view and traverse their list of connections and those made by others with the system." However, so far, there has not been a widely accepted formal definition of online social networks and it is still puzzling whether or not to put websites such as YouTube, eBay and Taobao in the scope of online social networks. Liu [113] provides a categorization, based on different socialites of participants in OSNs. Here, based on whether the social relationships are explicit, we divide online social networks into two categories: *explicit OSNs* and *implicit OSNs*.

2.1.2.1 The Explicit OSNs

Online social networks, such as LinkedIn, MySpace and Facebook, founded in 2002, 2003 and 2005 respectively, mainly focus on socialization and allow users to explicitly express social relationships (e.g., to add as "friends" and to join a group of interest) and share information (e.g., to post words, pictures, sights and even videos). The main characteristics of the explicit OSNs are summarized as below:

1. The social relationships between participants are explicitly specified by participants themselves, which are usually binary (i.e., "friends" or "non-friends").

2. They have provided a platform, where users who participate the OSNs can upload personal profiles, meet new participants and conduct some activities of communication, such as information sharing and recommendations.

3. Participants can make friends with friends' friends or other participants of interest (e.g., graduating from the same university and having the same interest).

2.1.2.2 The Implicit OSNs

There are also a number of websites, including e-commerce and e-service, which provide rich functionality but do not explicitly support the conventional social relationship. For example, the conventional e-commerce website eBay focuses on online commercial activities where merchant-consumer relationships are revealed by transactions and messages between them. The computer science bibliography website DBLP[9] collect the academic papers within this field. The relationships between authors can be mined by the co-author relationship in their publications. This type of online networking sites are termed as implicit OSNs, which have the following common characteristics.

1. There are no explicitly specified social relationships, e.g., the participants cannot keep their friendship lists and thus they cannot make new friends with friends of friends.
2. They are rich in functionality and focus on certain activities, such as e-commerce, e-services, email, blogs, publications and information sharing in the form of words, photos, sights and videos etc.
3. The relationships between participants can be implicitly revealed by their interactions in any types of activities, such as transactions in e-commerce, email communication, and co-authorship in publications.

2.1.2.3 The Future Development of OSNs

As social commerce is emerging, the boundary between the concepts of conventional online social networks and e-commerce or e-service websites is fading away. Currently, the development can be seen in the following three aspects:

1. E-commerce websites begin to allow participants to build their social networks in a more explicit way. For example, the largest e-commerce website Taobao

[9] http://dblp.uni-trier.de/

integrates an instant messaging tool, with which buyers can ask sellers about products, or seek advice from other buyers. In this tool, users can specify the relationships with sellers or others buyers.

2. Online social networks have begun to enrich their supported activities covering e-commerce or e-service, such as the mock-up of Twitter Commerce, in which apparently normal tweets can be expanded to reveal a buy button that enables consumers to make a purchase within the Twitter app.

3. A large number of people use online social networks to conduct commercial activities. For instance, many international students studying overseas use WeChat or QQ to post advertisements and provide overseas procurement services.

2.2 Overview of Trust

"*Trust is the glue of life. It's the most essential ingredient in effective communication. It's the foundational principle that holds all relationships.*" *— Stephen Covey*

Trust is defined as "firm belief in the reliability, truth, or ability of someone or something" in the Oxford Dictionary[10]. It is further explained as "acceptance of the truth of a statement without evidence or investigation" in the viewpoint of trustor (i.e., the subject that trusts a target entity) and "the state of being responsible for someone or something" in the viewpoint of trustee (i.e., the entity that is trusted by others). From the definition, it is clear that the trustees should be highly reliable and behave honestly in the interactions with trustors.

Actually, trust is a complex subject relating to many different aspects including belief, truth, competency and reliability. As there are complex factors affecting trust relationships, in the literature, there is no existing consensus definition on trust [95, 158], and trust cannot be easily modeled in a computational system [65]. In this section, the definitions of trust in different fields, the properties of general trust, the influence of

[10] http://www.oxforddictionaries.com/definition/english/trust

trust, and the social context that affects trust will be introduced.

2.2.1 Defining Trust

Trust is a common daily phenomenon. Humans would not succeed in facing the complexities of the world without trust, because without trust we are not able to reason sensibly in daily life [126]. It plays a role in multiple disciplines, including sociology, psychology, economics, political science, history, philosophy and computer science. In addition, there has not yet been a uniform definition of trust. In the literature, trust has been defined in different disciplines respectively [139].

2.2.1.1 Trust in Psychology

In psychology, the definition of trust given by Deutsch [44] is the most popular and widely accepted. He states that trusting behavior takes place when an individual confronts an ambiguous path leading to a perceived either beneficial or harmful result contingent on the action of another person. Jøsang et al. [87] state that "Trust is the subjective probability by which an individual expects that another performs a given action on which its welfare depends." More similar descriptions of trust can also be found in [170, 179]. The core of these definitions is that trust occurs when an individual believes the trusted other will act in an expected way, and the future action is committed by the individual based on that belief. In addition, Beatty et al. [22] point out that cognitive, emotive and behavioral aspects should be included in trust, where the cognitive aspect refers to a rational decision [12] based on the current knowledge of the trustee; the emotive aspect refers to emotional drive [194]; and behavioral aspect refers to the final actions. Misztal [147] states that trust affects people's lives in three aspects—it makes social life predictable, create the sense of community and eases the cooperation among people.

2.2.1.2 Trust in Sociology

Trust in sociology stems from the works of Luhmann [126], Barber [19] and Giddens [59]. The interest in trust has been growing, as trust is one of the main elements in social reality [177]. It is a means of overcoming the complexity of society, as people in society generally obey certain rules [126].

Furthermore, trust is attributable to relationships between social entities, both individuals and groups. Thus, the definition of trust in sociology can be further divided into an individual level and a societal level. The individual level is similar as the ones from psychology [171, 180]. For example, Sztompka [187] summarizes the definition of trust as "Trust is a bet about the future contingent actions of others," which is similar to the definition given by Deutsch [44] in Psychology. At this level, the specific trust between the trustors and trustees is termed as "relational trust", which is built up through repeated direct interactions between two parties and declines when betrayed [171]. At the societal level, trust is treated as one of properties of social groups. From the perspective of sociology, Luhmann [126] considers trust as "a means for reducing the complexity of society". Seligman [178] proposes a more detailed definition that "trust enters into social interaction in the interstices of systems, when for one reason or another systematically defined role expectations are no longer viable. If people play their roles according to role expectations, we can safely conduct our own transaction accordingly." Seligman [178] also points out that the problem of trust (distrust) emerges only in the situation where there is "role negotiability", i.e., a gap exists between roles and role expectations. At the societal level, a general belief of the trustor towards a group of members is termed as "generalized trust" [170]. It implies that the members of a group act as expected. For example, professors are always considered professional in their research fields. In human society, the generalized trust initializes the trust relationship between unfamiliar trustors and trustees, and makes opportunity for the relational trust to be established through forthcoming interactions between them. Moreover, Marsh [139] declares that ignoring either rational or generalized trust will lead to the inevitable loss of understanding trust as both personal and social concepts.

2.2.1.3 Trust in Economics

In the field of economics, the European Commission Joint Research Center [83] defines trust as “trust is the property of a business relationship, such that reliance can be placed on the business partners and the business transactions developed with them.” This definition implies the importance of trust in commercial activities, from the perspective of business management. In addition, trust is often conceptualized as reliability in transactions in economics [138].

More precisely, Akerlof [9] points out that trust affects economic costs. Ba et al. [16] demonstrate that trust can reduce transaction risks, mitigate information asymmetry and generate price premiums for reputable vendors. This phenomenon is quite evident in online trading environments, such as e-commerce and e-service, where consumers cannot directly interact with products and workers, and the credibility of online information may be doubtful [168]. The quality of products cannot be judged in advance because the online information is mainly posted by the vendors themselves. Thus, trust is considered by some economists as a mechanism to restrict opportunistic behavior and establish a reciprocal relationship between consumers and vendors.

2.2.1.4 Trust in Computer Science

In computer science, trust is a widely used term with various definitions among researchers. Bonatti et al. [28] categorize trust using reputation and policy. Mui et al. [150] define trust as “a subjective expectation an agent has about another’s future behavior based on the history of their encounters,” which is widely accepted as reputation-based trust. Reputation-based trust uses an entity’s historical behaviors or observations to compute trust, and may utilize information from others in the absence of first-hand knowledge [13]. For example, when a consumer purchases a product from an unknown eBay vendor, the initial trust is established only based on the experiences (ratings) of others. On the contrary, policy-based trust is established, when sufficient necessary conditions are met, to control access rights [13]. It is founded on logical rules and verifiable properties encoded in digital credentials [28]. The aim of policy-based trust is to determine whether an unknown participant can be trusted or not based on a certain number of credentials and a set of relevant policies.

Moreover, in computer science, a number of various trust prediction models are designed to help establish trust relationships by simulating the process of trust establishment among people in human society. For example, Marsh [139] proposes a set of variables and a method to incorporate them all into a continuous value in the range of $[-1, 1]$ to represent trust. The details of trust prediction will be presented in Section 2.4.

2.2.2 Properties of Trust

After reviewing the definitions of trust in different disciplines, this subsection summarizes the general properties of trust. These proposed properties are believed to be significant to the study of trust prediction, as they are based on either experimental verification or long-term observations of human activities, and provide the theoretical foundation for the design of various trust prediction approaches.

2.2.2.1 Trust is Subjective

In social psychology, trust is a subjective phenomenon as a personal psychological state [72, 136, 170]. It is determined by an individual's personal subjective attitude to another based on the individual's own psychological experience, evaluation and the domains of both. Even the trust towards the same individual can vary significantly. For instance, Alice trusts Bob, since Alice has a very good experience during all the historical interactions with Bob. But, Cathy distrusts Bob because of a betrayal. Golbeck [65] provides another example that the population split significantly when asked about whether or not to trust the current President's effective leadership.

Subjectivity is one of the major properties of trust in computer science [233]. Jøsang [84, 85] leverages subjective logic to explain trust and further explains that an opinion can be uniquely described from belief, disbelief and uncertainty. Moreover, the subjective property is also applied to evaluate the trustworthiness of a vendor in online trading environments, such as e-commerce [109]. For instance, eBay provides a rating system to assist vendors and buyers. A buyer can provide a rating (+1, 0, or -1) after each transaction regarding to the transaction quality. In particular, a number of mathematical models have been proposed to model the changes of subjective trustworthiness, such as the Beta model [82] and the Markov chain model [124]. In addition, some researchers treat the subjective property as personalization, e.g., Richardson et al. [167] consider that the user ratings in a trust management system attribute to personalization.

2.2.2.2 Trust is Asymmetric

Trust is asymmetric. This property means that trust between participants does not necessarily exist in both directions or to the same extent. For example, the buyer Alice trusts the vendor Bob, since Alice has had a very good experience during all her historical interactions of buying goods from Bob. But, conversely, Bob may not trust Alice any more, if Alice starts to sell products. In this example, the asymmetry is mainly caused by the different roles in the historical interactions.

However, even between two trusted individuals, the amounts of trust in each other's minds can differ significantly, due to different personal experiences, psychology and backgrounds, such as the trust between a supervisor and a research student. The student trusts the supervisor because of the ability of the supervisor in the research field. Yet, the supervisor trusts the student in the expectation of potential good working performance. So, the two directional trusts are totally different. This can be seen in a variety of hierarchies [223]. The asymmetric property is also named "one-way trust" in [40, 72]. In summary, trust is not reciprocal or equivalent between two entities, which must be taken into account in trust prediction (or evaluation).

2.2.2.3 Trust is Propagative

Propagation, also known as inference, is one of essential properties of trust, and establishes a trust relationship between unfamiliar entities. For instance, if Alice trusts Bob and Bob trusts Cathy, Alice might trust Cathy to some extent [66, 114]. In this case, Alice may not even know Cathy at all. The establishment of the trust to Cathy in Alice's mind depends both Alice's trust to Bob and Bob's trust to Cathy [228, 86]. This property enables trust information to be passed from one to another, resulting in forming a trust path from the source to the target. This meets the fact that when encountering an unknown person, it is common for people to ask trusted friends for opinions about how much to trust this new person [65].

Furthermore, the property of propagation sets up the foundation of a number of trust inference models, which evaluate trust from a source entity to a target entity along a trust path between them that consists of links and trust values [69]. In the propagation process, trust decays with the increase of propagation hops along a social trust path [39, 136]. In addition, as the multiple entities and contexts are involved in a trust path, trust propagation becomes complicated [114, 233]. In computer science, it has attracted more and more researchers to study trust propagation in large-scale complex social networks, such as finding the most trustworthy path [86, 116]. Moreover, it has also been studied in many web application areas including e-commerce [209, 236, 235], P2P systems [220], and social networks [82, 66, 119].

2.2.2.4 Trust is Context Dependent

Rousseasu et al. [171] review the concept of trust extensively and suggest that "research on trust requires the attention to context." It is also stated in [7, 212] that a person's trust in another person changes regarding different contexts, because expertise of a recommender may vary in different domains. Similar suggestions or statements can be found in a huge number of works in the literature, and the core is that "trust is highly context-dependent," as described by O'Hara et al. [154] in social psychology. Conceptually, context is generally defined as "the circumstances that form the setting for an event, statement, or idea, and in terms of which it can be fully understood," as stated in Oxford Dictionary[11].

In computer science, a more specific and widely accepted definition is proposed by Dey et al. [45]: "Context is any information that can be used to characterize the situation of an entity. An entity is a person, place or object that is considered relevant to the interaction between a user and an application, including the user and the application themselves." In addition, from the viewpoint of context, Grandison and Sloman [67] define trust as "the firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context". More specifically, McKnight et al. [142] propose "interpersonal and personal trust" as one of topological categories on trust. Namely, one person trusts another person in a specific context. For example, Alice may trust Bob as a mechanic in the specific context of servicing her car but probably not in the context of babysitting her children [5]; and "Whilst I may trust my brother to drive me to the airport, I most certainly would not trust him to fly the plane!" [139]. Furthermore, Marsh [139] proposes the concept of "situational trust" as an alternative way of contextual trust, suggesting that context affects trustworthiness. In addition, Mui [150] stresses that trust depends on the context in the viewpoint of reputation, and states "Bill Clinton's reputation as a politician is likely to be very different from his reputation as a cook," which means we could only trust Bill Clinton as a politician instead of a cook from past experiences.

In OSNs, Liu et al. [120] state that social context includes social relationship, social position, preference and residential location etc. And, trust can be transferred between relevant contexts [240, 206]. For example, if Alice trusts Bob in teaching Visual C (VC), Alice can also trust Bob in teaching Java to some extent, as the contexts of teaching VC and teaching Java are similar. Furthermore, it is indicated in social

[11] http://www.oxforddictionaries.com/definition/english/context

psychology that these social contexts have significant influence on trust prediction in OSNs [7, 111, 33] and a growing number of studies have been focusing on context in trust prediction in recent years [220, 121, 163, 209, 197, 108, 234, 165, 124].

2.2.2.5 Trust is Dynamic

It is easy to understand that trust is dynamic, which means the trust between two entities may change over time. The establishment process of trust itself has already indicated this property of trust. Rousseau et al. [171] state that trust can occur, intensify, or decay based on repeated direct interactions with new experiences, which reflects temporal characteristics of trust. Dealing with the changes of trust over time, there are three main types of ways in the literature: trust decay, trust time window and probabilistic trust models.

Trust may decay over time, because the experience based on which the trust is established fades over time. New interactions are usually more important than older ones for the prediction of the current trust towards an entity. Based on this characteristic, researchers in computer science gradually reduce the influence of old interactions, or increase the weight of recent interactions, when predicting trust [172, 90, 210, 134, 205, 82]. In particular, Spitz et al. [183] point out a common phenomenon in e-commerce websites that sellers can have a large lapse of time since their last transactions, in which the decay of trust over time is more essential.

Trust time window is another way to deal with the temporal characteristic of trust. For example, the e-commerce website eBay offers the choice of time window to be set to last one month, last six months or last twelve months. In addition, a number of researchers predict trust using a time window in different applications. For instance, PeerTrust [219, 220] allows users to set the time window; and Shi et al. [181] propose a mechanism for dynamic peer-to-peer trust based on time-window feedback. Furthermore, in some works, the hybrid of trust decay and time window is adopted [211, 210, 205].

Trust can fluctuate strategically, especially in on trading environments, where vendors strategically and consciously change their behaviors in order to maximize personal profit [241]. To deal with this type of difficult situations, probabilistic models are the most promising tools to deal with uncertainty. For instance, a Hidden Markov Model is leveraged by ElSalamouny et al. [52] to predict the trust of outcomes of future transactions. Liu et al. [124] propose a model based on Markov chains and context information to predict trust.

A more detailed review regarding dynamic trust prediction will be presented in Subsection 2.4.3.

2.2.3 The Influence of Trust

Having introduced the definition and property of trust, it is easy to recognize that trust is an essential element of many fields. Social scientists have illustrated that both real life societies and online communities greatly depend on trust [40, 57, 58]. For example, Uslaner et al. [198] argue societies with higher trust levels function better. Munns [151] state that in any society, trust is necessary for processes to operate efficiently and effectively.

For individuals in the reality of our society, trust is the foundation of the daily life. When a car is given to a mechanic for repair, trust is placed on the mechanic for his/her skill of car repair, and is expected to return the car in an expected condition [151]. Researchers in social psychology [60, 55] have indicted that people tend to accept the recommendations from their trusted friends rather than that from unknown others. A similar statement is also proposed by Bedi et al. [23] in computer science. Furthermore, some researchers [37, 41] have investigated the mechanism and extent of the influence of trust on individuals' decision-making process showing that trusted friends have significant influence on the process in both real societies and online environments.

Organizations have recognized the increasing importance of trust in terms of efficiency and effectiveness. Braddach et al. [30] state that trust is a control mechanism for companies. Wicks et al. [217] discuss trust in ethics and management, and point out that trust is an important part of improving company performance. Furthermore, Ring et al. [169] examine the influence of trust between two organizations showing that trust is a fundamental ingredient for inter-organizational cooperation. Similarly, Dodgeson [46] claims that trust facilitates strategic collaboration and cooperation. Moreover, trust is also studied regarding citizenship behavior [43, 94, 140], conflict resolution [155], organizational commitment [40], perception [34, 182] and satisfaction [11, 166, 38, 185].

In addition, trust has a great influence on government [104]. For instance, Chanley et al. [36] state that the decline of trust in government can lead to less evaluation of Congress and weaken government action; Van de Walle et al. [199] state “concerns for restoring citizens’ trust in government are at the core of public sector modernization”; and Warkentin et al. [213] point out that citizen trust is an important catalyst of e-Government.

2.2.4 Social Context that Affects Trust

A social network usually contains not only the trust links and nodes, but also complex social information describing each trust relationship, including social relationship type, social position, residential location, and preference. A number of features can be mined from the complex social information and utilized to analyze the trust between nodes. This subsection presents a detailed review of features extracted from social context information, which can be incorporated into trust prediction models and further improve their performance.

2.2.4.1 Definition of Social Context

Context is a multi-faceted concept across different research disciplines with various definitions [180]. In social science, Barnett et al. [20] define social contexts as “social environments that encompass the immediate physical surroundings, social relationships, and cultural milieus within which defined groups of people function and interact including built infrastructure; industrial and occupational structure; labor markets; social and economic processes; wealth; social, human, and health services; power relations; government; race relations; social inequality; cultural practices; the arts; religious institutions and practices; and beliefs about place and community."

In computer science, multiple definitions of social context have been proposed in some specific social networks. Yang et al. [222] give the definition of social context in micro-blog systems as "compared with traditional contexts that are defined based on textual information, social context in micro-blog systems need incorporate various dynamic social relationships, such as the follower-followee relationships between users, retweeting relationships and replying relationships between tweets." Ma et al. [128] define the social context in recommender systems, emphasizing "social context information including users' social trust network, tags issued by users, information about the interests of users, or properties of items."

In this thesis, we define social context as any information available for characterizing the participants and the situations of interactions between them. Furthermore, we adopt the terminology used in [206]. If participant p_1 has an interaction with participant p_2, the context about p_1 and p_2 in the social society is referred to as the social context, among which the interaction context refers to any information about the interaction including time, place, and type of services. If p_2 recommends a service to p_1, then the information about the service is referred to as the target context, when predicting the trust of p_2 in p_1's mind.

2.2.4.2 Social Contextual Impact Factors

Social context describes the context about participants. Before it can be utilized, the properties of each aspect must be extracted modeling the characteristics of participants and the relationships between them. In addition, social context can be divided into two groups according to the characteristics of impact factors: *personal properties* (e.g., social position, expertise, preference, indegree, outdegree, reliability, and location) and *interpersonal properties* (e.g., preference similarity, social intimacy, social relationship type, location distance, and trust).

Social Position: Social position is the position of an individual in a given community and culture [113]. In addition, an individual usually has multiple social positions in different domains [7]. For example, an individual can be a professor of computer science in a university and a tennis coach in spare time. In this case, the social positions of this person in computer science and teaching tennis can be greatly different.

Expertise: Expertise is a person's formal training and technical knowledge, often contrasted with the knowledge of people with no formal training [184, 201]. Expert judgments are attractive and especially important in the situations of stretched time and resources, inadequate existing data, unique circumstances, or requiring extrapolations. In addition, it is illustrated in social psychology [7, 42] that in a certain domain of interest, an expert's recommendation is more credible than that of a beginner.

Preference: Preference is an individual's attitude or affinity towards a set of objects in a decision making process [111]. A person may have different preferences in different domains [113]. For example, a professor may prefers collaborating with others of the same research area, and the same professor may also like watching movies on weekends.

Indegree: The indegree of a participant in a social network is the number of links connecting to him/her. A participant has a large indegree in an OSN means the participant is well-known in the community. It is illustrated in cognitive science [97] and computer science [159] that a well-known person is more credible than the ones interacting with less people. Moreover, in social science, Prell [159] has validated that the recommendation from a participant with a larger indegree is more credible.

Outdegree: The outdegree of a participant in a social network is the number of links connecting from him/her. A participant with a larger outdegree in an OSN has more opportunities to connect with others in the community, which means this participant is more active in social activities in the community.

Reliability: In a certain context, reliability means the rate a participant's suggestions are accepted by others [81]. It reflects a participant's ability to give useful suggestions which fit the others' favor.

Location: Locations of participants are the residential places where participants are living.

Preference Similarity: *"Things of a kind come together. People of a mind fall into the same group."* Similar to this old saying, in social psychology [126, 232], it is illustrated that a participant can trust and have more social interactions with others, with whom the participant has more similar preferences. For example, two individuals with the hobby of playing badminton are more likely to play badminton together. In addition, in computer science, Wang et al. [206] point out that the similarity of two participants' preferences can impact the trust between them to some extent.

Social Intimacy: Social intimacy refers to the frequency of connections between participants in a social network. The degree of social intimacy can impact trust, as people tend to trust those with more intimate social relationships [33]. It is also illustrated in social psychology [14, 31] that a participant can trust and have more social interactions with others with whom the participant has more intimate social relationships.

Social Relationship Type: Social relationship type in this thesis refers the nature of social relationships, such as "neighbors", "live together", "manager of", "member of ", "supervisor of", "competitor of", to name a few, as rich activities of participants in social networks can be categorized into different domains based on their characteristics [212]. In social science, Brehm [33] has indicated that two participants can have more than one type of social relationships. For example, Alice and Bob are classmates; both of them join the same club; and Alice is the daughter of Bob.

Location Distance: It is illustrated in social psychology [20, 61] that compared with the participants living far away, a participant can trust more and have more social interactions with others who live closer.

Trust: Trust is a belief that an entity, such as a person or an organization, will behave in an expected manner, despite the lack of the ability to monitor or control the environment in which it operates [180]. It can be impacted by all the above properties, and the trust value can be greatly different between the same two participants in different interaction contexts [212, 136]. A detailed review of the definition of trust has been presented in Subsection 2.2.1.

2.3 Trust Network Extraction in OSNs

In social networks, participants usually interact with multiple others. The interactions between participants contain a lot of information regarding giving trust ratings, transactions, sending emails, sharing information etc. and the context information when the interactions occurred. Then, a social trust network, such as Figs 1.1 or 1.2 in Chapter 1, is formed based on the trust relationships and context information between any two participants. Thus, the social trust network provides a foundation for predicting the trust to a target participant in a source participant's mind. However, predicting the trust between any participants who do not have any historical direct interactions from the entire social trust network can be very time-consuming, especially when the scale of the social trust network is large. Therefore, prior to trust prediction, it is an essential step for the accuracy and efficiency of trust prediction to extract a trust subnetwork for these two nonadjacent participants, which contains exclusively the important intermediate participants and relationships in the target context, and is kept relatively small in scale.

In the literature, there are few approximation algorithms proposed for the subnetwork extraction problem for trust prediction in online social networks [113, 242]. In addition, extracting a subnetwork from a cyclic network, such as social trust network, has been proved to be an NP-complete problem [146]. Fortunately, as the resource discovery problem in P2P networks has some similar properties as the trust subnetwork extraction problem, some search strategies from P2P networks can be applied to trust subnetwork extraction. These approaches can be divided into two groups: *traversal methods* and *heuristic methods*.

2.3.1 Traversal Methods

Traversal methods usually search the whole social trust network and have the capability to find the best subnetwork. This type of methods mainly includes breadth-first search (BFS) and depth-first search (DFS) and their variations, such as high degree search (HDS) and flooding-based search (FBS). HDS [6] sends a query to all its neighbors based on the BFS method to determine whether they contain the resources or not. Then, it broadcasts the search along directions of the highest degree using DFS method if none of the neighbors contain the resources until reaching a threshold or traversing all nodes. The typical FBS [113] searches the network from the source node using BFS strategy to find the target resource in a P2P network, and is applied in a large P2P network, Gnutella (rfc-gnutella.sourceforge.net), where users are allowed to directly exchange files over the Internet without going through a web site as a way of downloading music files from or sharing with other Internet users.

For the application on small-scale datasets, the traversal methods are able to search for the best subnetwork. However, on large datasets, it is computationally unfeasible to find the optimum solution. For example, FBS sends a query to every neighboring node in the network to find the target resource, which makes the FBS mechanism inherently unscalable in a large scale network.

2.3.2 Heuristic Methods

Compared with traversal methods, heuristic methods are to find a near-optimal solution in a large-scale network. We divide existing heuristic methods available for subnetwork extraction problem into the following three categories.

First, heuristic methods can be developed from traversal methods by incorporating heuristic strategies. By adding heuristic strategy to BFS, the time-to-live breadth first search (TTL-BFS) model [35, 54] is proposed, in which the time-to-live (TTL) is introduced to indicate the time consumption of BFS. TTL decreases as the depth of search increases and terminates TTL-BFS when TTL reaches 0. Another typical algorithm for locating resources in P2P networks is random walk search (RWS) [62, 63]. In this algorithm, the source node randomly selects K neighboring nodes (named random walkers) and sends out the queries. The process is repeated if the target is not found. Similar as TTL-BFS, each random walker has a TTL which limits the number of times the process is repeated.

Second, a few models are proposed specially for the trust subnetwork extraction problem from the perspective of trust propagation or inference. Hintsanen et al. [73] propose a model to find the most reliable subnetwork. They treat social networks as Bernoulli random graphs and extract a sub-graph by adding paths to the extracted sub-graph one by one till the most reliable status is reached. Liu et al. [115] propose a model to find K optimal social trust paths for the selection of trustworthy service providers in complex social networks. The K paths selected from a source participant to a target one actually form a subnetwork. Liu et al. [117] propose a social context-aware trust network extraction model, which applies an optimized Monte Carlo method to extract an optimal trust network from the source to the target participants, under user-given constraints of trust network utility yielding the highest utility. These existing works rely on trust paths and do not perform well for matrix factorization-based trust prediction approaches, as the density of extracted subnetwork is not considered, and even state-of-art subnetwork extraction models still need improving in the aspects of both efficiency and effectiveness.

Third, some heuristic algorithms based on bionics can be leveraged to solve the trust subnetwork extraction problem, such as Genetic Algorithm, Particle Swarm Algorithm and Ant Colony Algorithm. Among these algorithms, algorithms based on the ant colony are proved to be the most suitable one for problems such as trust subnetwork extraction [218, 242]. In addition, Jang et al. [80] propose a binary ant colony algorithm (BACA) in which the initial pheromone on paths is equally distributed, and the path selection only depends on the existing pheromone. This BACA can also be utilized to find the most reliable subnetwork. However, when compared with the above approaches, the performance of BACA is not improved much, as the scale of the selected subnetwork is affected by the initialization.

2.3.3 The Problems of Existing Methods

In summary, traversal methods [35, 54, 6] usually adopt methods, such as breadth-first search and depth-first search, and are applicable on small-scale datasets. However, on large-scale datasets, they are computationally unfeasible to find the optimum solution, and heuristic methods [62, 63, 6, 73, 115, 117] can be used to find a near-optimal solution. In addition, most of the relevant existing works do not consider the social context in online social networks, which has significant influence on trust prediction [31, 111, 231]. On the other hand, all the existing works rely on the existing social trust paths, which limits the performance of trust prediction, as some aspects, such as expertise, can affect the trust without the need of social connections. According to our knowledge, there is no existing approach focusing on the context-aware trust subnetwork extraction specifically for trust matrix-based trust prediction.

2.4 Trust Prediction

In human society, trust depends on a host of factors such as direct interaction, opinions, and motivations. [25]. But, in online social networks, people cannot directly interact with each other, and the credibility of online information may be doubtful [168]. As a result, trust mainly depends on the past experience with a participant, the profiles or descriptions, reputation etc. However, it is quite common for a participant in online environments to conduct activities with another participant without any previous direct knowledge, such as online shopping, recommender systems and online recruitment. Thus, an effective approach and mechanism to predict the trust between two participants without any direct connection is highly demanded.

The process of estimating a new pair-wise trust relationship between two participants who are not directly connected, based on existing observations, is termed as *trust*

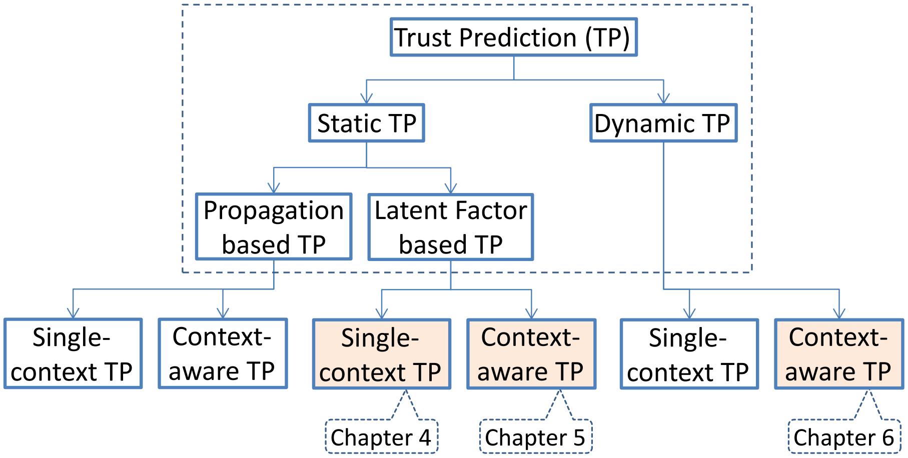


Figure 2.1: The categorization of trust prediction (TP)

prediction. In the literature, a number of trust prediction models have been proposed. As shown in Fig. 2.1, from the perspective of the different characteristics of algorithms, existing trust prediction models can be divided into *static trust prediction* and *dynamic trust prediction*. Furthermore, *static trust prediction* can be further divided into *propagation-based trust prediction* and *latent factor-based trust prediction*. In addition, based on application situations and dependent information, each of the above categories contains *single-context trust prediction* and *context-aware trust prediction*.

2.4.1 Propagation-based Trust Prediction

Propagation is an important property, as introduced in Subsection 2.2.2.3, which has been validated in both social psychology [39] and computer science [88, 65]. In addition, trust propagation has been studied in many application areas including e-commerce [209, 236, 235], P2P systems [220], and social networks [82, 66, 119]. Based on this property of trust, a type of trust prediction approaches named trust propagation or inference are proposed. Trust propagation/inference is the process of evaluating trust from a source participant to a target participant along a path between them that consists of trust links and trust values [69]. For example, if Alice trusts Bob, and Bob trusts Cathy, then Alice can trust Cathy to some extent [66, 114]. This means that if Alice needs a tennis coach, and Alice's trusted friend Bob is very satisfied with the experience when he learned tennis from the coach Cathy, then Alice can trust Cathy regarding teaching tennis to some extent, as Alice trusts Bob, believing Bob would tell the truth, and Bob believes Cathy is good tennis coach.

In earlier years, most of the trust prediction models focused on the propagation of trust along the trust paths connecting users. The most simple and typical approaches are based on either *multiplication strategy* or *averaging strategy*. When adopting multiplication strategy, the trustworthiness of a target participant, in a source participant's mind, is computed as the multiplication of the trust values between any two adjacent participants along the social trust path from the source participant to the target one. For example, if Alice trusts Bob with the trust value of T_{AB} and Bob trusts Cathy with trust values of T_{BC}, then the predicted trust value to Cathy in Alice's mind will be $T_{AC} = T_{AB}^{\alpha} * T_{BC}^{\beta}$, where α and β are coefficients. Adopting multiplication strategy, Walter et al. [200] propose a social network based recommendation system, in which the predicted trust value of a target recommender is calculated along a social trust path from a recommendee to a recommender. Lei et al. [110] propose a composite service trust evaluation method to compute the aggregated trust value of a composite service along a service composition path. When adopting the averaging strategy, the trustworthiness of a target, in a source participant's mind, is computed as the average trust value between any two adjacent participants along a social trust path. The predicted trust value to Cathy in Alice's mind will change to $T_{AC} = \alpha T_{AB} + \beta T_{BC}$, where, $\alpha + \beta = 1$. Adopting the averaging strategy, Gary et al. [68] propose a trust-based admission control model to predict the trust of unknown participants, and Golbeck et al. [65] propose a trust inference method to compute the inferred trust value of the target participant, which is further applied to FilmTrust.

In later years, the performance of propagation based trust prediction has been further improved by adding more information into the propagation process. Guha et al. [69] propose a trust propagation model considering the number of hops and the trust situations of intermediate nodes, when calculating the propagated trust value between a source user and the target one. Huang et al. [71] utilize operators such as concatenation, aggregation and selection to propagate trust. Kuter et al. [98] propose a trust inference model taking into account the confidence values given by domain experts. Lesani et al. [99, 100, 101] propose a trust propagation model using fuzzy logic which supports linguistic terms as low, medium low, medium high and high. Taherian et al. [188] infer trust values in web-based social networks based on the resistive network concept. The trust propagation model proposed by BuBois et al. [203] takes a trust network as a random graph and creates an inferred trust-metric space, in which a shorter distance means higher trust. Wang et al. [203] propose a flowtrust approach using network flows to model a trust graph to calculate the maximum amount of trust under flow theory.

Moreover, a few researchers have started to add social context information into trust inference models to further improve the performance of trust prediction. Liu et al. [116] argue that social relationships and recommendation roles are also important for trust propagation. Taking into account these factors, a Bayesian network-based trust inference model is proposed [114]. Furthermore, Wang et al. [206] propose a trust prediction model to infer the trust between non-adjacent participants in online social networks taking into account both the social context of participants and the context of the target service to be recommended. In this model, the characteristics of participants in a social network are divided into personal characteristics (e.g., preference and domain expertise) and mutual relations (e.g., existing trust, social intimacy and interaction context), and finally the social context-aware trust inference model is proposed based on probabilistic theories. The proposal of such works is based on these two foundations: 1) Trust is context-dependent [180] and it is rare for a person to have full trust on another in every facet [189]. For example, the case of full trust in all aspects is less than 1% at Epinions.com and Ciao.co.uk, both of which are popular product review websites [189]. 2) In real life, a person's trust to another is limited to certain domains, demonstrated by social psychologists [7, 39]. For instance, Alice trusts Bob in playing tennis and Bob trusts Cathy in repairing cars. In such a case, Alice may not trust Cathy in repairing cars at all, as playing tennis and repairing cars are not relevant contexts in the common sense of people and the trust in these two different contexts can be greatly different.

In summary, these existing trust propagation (or inference) models provide a type of feasible solutions to predict the trust values of a target participant in a source participant's mind along a social trust path from a source participant to a target one. They all possess the same feature that the trust values to be predicted must be calculated along a social trust path. There would be no trust values predicted, if there are no social trust paths connecting the source participant and the target one. However, trust can also be predicted from other aspects besides a social trust path. Lin et al. [112] demonstrate that people tend to trust others who are similar to themselves. For example, people from the same hometown or school are easy to become friends, and people prefer the recommendations from recommenders who have the same preferences as themselves. In addition, the reputation of a person is also an element affecting the trust towards the target, especially in online trading environments [134, 172, 28, 219, 87, 209]. For example, we may trust a professor in his/her research field more than his/her new students in real life, and we are more likely to buy items from sellers with a high reputation in e-commerce websites such as eBay and Taobao. Therefore, predicting trust not only from social trust paths has attracted a growing attention from researchers, and a review of this type of trust prediction will be presented in Subsection 2.4.2.

2.4.2 Latent Factor-based Trust Prediction

As propagation-based trust prediction models strictly depend on the social trust path from a source participant to a target participant, they are not able to predict the trust between two participants if there is no trust path between them, or if the path between them is so long that the trust along the path has decayed to zero. However, if trustees (the users who receive trust ratings) are regarded as the items in a recommender system, the general idea of latent factor-based approaches originally employed in recommender systems can be leveraged for trust prediction [225, 226].

Latent factor-based approaches, such as matrix factorization and factorization machine, analyze the relationships between trusters (the users who give trust ratings) and trustees, with factors representing latent characteristics of the participants to identify new truster-trustee associations [96]. They mainly rely on users' past behaviors, such as previous trust ratings, and are trained based on the available data and later used to predict the trust value between two non-adjacent participants. In addition, the propagated trust from a trust path can also be incorporated if needed.

2.4.2.1 Matrix Factorization

Matrix factorization is the foundation of most successful realizations of latent factor models [130, 127, 129, 131, 132, 227, 76, 79, 153, 186, 189, 190, 191, 221, 229]. In addition, in Netflix price competition, Koren et al. [96] have shown that matrix factorization methods outperform other rating prediction methods significantly, especially in sparse datasets. Matrix factorization models map truster-trustee rating matrix into a joint latent factor space of dimensionality l, so that each truster-trustee trust rating $r_{i,j}$ is modeled as the inner product of a truster-specific (user-specific) vector $u_i \in \mathbb{R}^l$ and a trustee-specific (item-specific) vector $v_j \in \mathbb{R}^l$ in that space, i.e., $r_{i,j} \approx u_i^T v_j$. For the whole trust rating matrix, we have $R \approx U^T V$, where, $U \in \mathbb{R}^{l\times n}$ and $V \in \mathbb{R}^{l\times n}$. This can be usually achieved by minimizing the Frobenius norm $||R - U^T V||_F^2$. In application, the matrix R usually contains a large amount of missing values and becomes a sparse matrix. In addition, in order to avoid overfitting, zero-mean spherical Gaussian priors are introduced [174]. Here, factorization is achieved by:

$$\min_{U,V} \sum_{i=1}^{n} \sum_{j=1}^{n} I_{ij}(r_{ij} - u_i^T v_j)^2 + \lambda_1 ||U||_F^2 + \lambda_2 ||V||_F^2, \tag{2.1}$$

where, I_{ij} is an indicator function. $I_{ij} = 1$ *iff.* user i (truster) rated user j (trustee), $i \neq j$. Otherwise, $I_{ij} = 0$. The gradient descent method [96] is usually utilized to realize this learning process.

Matrix factorization methods have a number of advantages, which can be summarized as follows: (i) many optimization methods can be applied in matrix factorization, such as gradient descent [49]; (ii) there is a good probabilistic interpretation with Gaussian noises in matrix factorization [144]; (iii) it is very flexible to incorporate prior knowledge [192]; (iv) it scales well to large-scale datasets, as it scales linearly with the number of observations [174]; and (v) it performs relatively well on sparse and imbalanced datasets [174].

2.4.2.2 Modifications of Matrix Factorization

In the literature, matrix factorization methods have been modified in different ways to achieve better prediction accuracy. According to the ways of incorporating prior knowledge, we summarize the existing trust prediction approaches that apply modified matrix factorization into the following two categories.

Semi-Latent Matrix Factorization: In conventional matrix factorization-based trust prediction models, the physical meaning of latent factors is not explicitly defined. We cannot point out which latent factor corresponds to which trust property. On the contrary, semi-latent matrix factorization-based trust prediction models expose part of the latent factors in the l-dimensional latent factor space by replacing the part of the latent factors with trust properties under physical meanings such as propagated trust, truster tendency and trustee tendency.

One typical semi-latent matrix factorization-based trust prediction model is proposed by Yao et al. [226]. In this model, the tendency and propagated trust values are treated as some of the latent factors of matrix factorization to boost trust prediction accuracy, while other latent factors of matrix factorization are kept unchanged and latent. In this matrix factorization model, the trust rating is represented as:

$$\hat{r}_{i,j} = u_i^T v_j + \alpha[\mu, x(u_i), y(v_j)]^T + \beta z_{u_i,v_j}^T. \tag{2.2}$$

where, $u_i^T v_j$ is the traditional part of matrix factorization with latent factors; $[\mu, x(u_i), y(v_j)]$

is the exposed latent factors representing global trust bias, truster bias and trustee bias; and the vector z_{u_i,v_j} is the exposed latent factors representing four types of propagated trust regarding direct propagation, transpose trust, co-citation and trust coupling. α and β are the coefficient vectors correspondingly. In this model, the training process of Equation (2.1) is changed to:

$$\begin{aligned}\min_{U,V,\alpha,\beta} \sum_{i=1}^{n}\sum_{j=1}^{n}(r_{ij} - (\alpha[\mu, x(u_i), y(v_j)]^T + \beta z_{u_i,v_j}^T + u_i^T v_j)^2 \\ + \lambda(||U||_F^2 + ||V||_F^2 + ||\alpha||^2 + ||\beta||^2),\end{aligned} \tag{2.3}$$

This type of matrix factorization-based trust prediction models have a very good visualization of the trust impact properties, and improves the performance of the trust prediction. However, the sparsity consideration is not revealed in this formulation. Whether the explosion of latent factors limits part of the capability of matrix factorization needs further studying. The trust properties in the model are limited and demand further research. For example, the social context information is not included.

Matrix Factorization with Social Regularization: This type of matrix factorization models focus on a user's preference and utilize the assumption that a user's preference should be similar to that of his/her social network. In other words, regularization terms are added to force a given user's preference to be closer to that of his/her social network. In addition, this type of matrix factorization models have the capability of incorporating the propagation of user favors in social networks and reducing the cold-start effect [192].

As the behavior of a user u_i is affected by the user's direct neighbors $\mathcal{N}_{u_i}$ [56], a social regularization term (*average-based regularization*) of $\sum_{i=1}^{n}(u_i - \sum_{u_k \in \mathcal{N}_i} S_{ik}u_k)^2$ is introduced into matrix factorization to force that the latent factors of user u_i is dependent on the latent factors of all the user's direct neighbors $u_k \in \mathcal{N}_{u_i}$, where $\sum_{u_k \in \mathcal{N}_i} S_{ik}u_k$ is the weighted average preference of users in u_i's neighbors [79, 192]. S_{ik} is the similarity of two users' previous ratings, which can be calculated by Vector Space Similarity (VSS) or Pearson Correlation Coefficient (PCC) [32, 79]. In addition, through a propagation mechanism, the neighbors $\mathcal{N}_{u_i}$ can be extended to almost all the users in the social network. Thus, the training process of Equation (2.1) is changed to:

$$\min_{U,V} \sum_{i=1}^{n} \sum_{j=1}^{n} I_{ij}(r_{ij} - u_i^T v_j)^2 + \alpha \sum_{i=1}^{n} (u_i - \sum_{u_k \in \mathcal{N}_i} S_{ik} u_k)^2 + \lambda(||U||_F^2 + ||V||_F^2). \quad (2.4)$$

However, for a given user u_i, users in his/her social network may have different favors. According to this intuition, a pair-wise social regularization is proposed as *individual-based regularization* $\sum_{i=1}^{n} \sum_{u_k \in \mathcal{N}_i} S_{ik}(u_i - u_k)^2$, in which the similarity of two users determines the closeness of the two users' preferences in the latent factor space [131]. Thus, the training process of Equation (2.1) is changed to:

$$\min_{U,V} \sum_{i=1}^{n} \sum_{j=1}^{n} I_{ij}(r_{ij} - u_i^T v_j)^2 + \alpha \sum_{i=1}^{n} \sum_{u_k \in \mathcal{N}_i} S_{ik}(u_i - u_k)^2 + \lambda(||U||_F^2 + ||V||_F^2). \quad (2.5)$$

A comparison between average-based regularization and individual-based regularization on the influence of the performance of matrix factorization is conducted by Ma et al. [131] and the conclusion is that the matrix factorization with individual-based regularization achieves better performance.

Moreover, the calculation of similarity S_{ik} between two users u_i and u_k is critical to matrix factorization with regularization models. In the literature, most existing models, including the above two, use VSS or PCC [32, 131, 79, 192]. The difference between VSS and PCC is that PCC takes into account the average rates while VSS does not.

In summary, matrix factorization with social regularization is a powerful tool for trust prediction. But, there are still a number of drawbacks in most existing works of this type. *Firstly*, all the tendency, propagated trust and similarity that influence the trust between two users should be utilized to predict pair-wise trust, rather than only one or two influential factors. *Secondly*, the similarity of trust rating distributions describes the similarity of users' behaviors in giving trust ratings. Thus, it is valuable for trust prediction [241]. However, it has been neglected in most existing works, which merely utilize the similarity of rating values. *Thirdly*, trust impact factors are of different types, representing either personal properties or interpersonal properties. They should be processed separately and differently so as to deliver high accuracy in trust prediction. *Finally*, trust is context-dependent [180] and it is rare for a person to have full trust on another in every facet [189]. Therefore, contextual information should be taken into account to trust prediction for further improvement.

2.4.2.3 Other Latent Models Available for Trust Prediction

As trust is a critical factor in the decision-making process of participants in online social networks [98], the prediction of trust is attracting more researchers.

Factorization machine is a regressive model that factorizes truster-trustee (user-item) collaborative data into real valued feature vectors [164]. It can be treated as a generalized model of matrix factorization, as most factorization models can be modeled as the special case of factorization machines [164]. In factorization machines, the interaction is represented by a tuple $(\mathbf{x}, r)$ consisting of a n-dimensional feature vector $\mathbf{x} = (x_1, x_2, ...x_n) \in \mathbb{R}^n$ and a corresponding label (rating) r. The second order factorization machine is the most common one used for prediction and recommendation, as only pairwise interactions are considered. This model can be formulated as:

$$\hat{r}(x) = w_0 + \sum_{j=1}^{n} w_j x_j + \sum_{j=1}^{n} \sum_{j'=j+1}^{n} w_{j,j'} x_j x_{j'}, \tag{2.6}$$

where, w_j are model parameters and $w_{j,j'} = \mathbf{v}_j \cdot \mathbf{v}_{j'}$ are factorized interaction parameters and $\mathbf{v}_j$ is k-dimensional factorized vector for feature j. In addition, this model can be trained by Gibbs Sampling, Stochastic Gradient Descent, Alternating Least-Squares and Markov Chain Monte Carlo methods [164].

Based on factorization machines, Loni et al. [125] propose a cross-domain collaborative filtering recommendation model, in which the auxiliary information is encoded as a real-valued feature vector as a supplement to the information of a user-item matrix. The authors constitute particular domains with specific types of items and utilize interaction information from auxiliary domains to generate recommendation in the target domain. In other words, encoding domain-specific knowledge in terms of real-valued feature vectors betters the exploitation of interaction patterns in an auxiliary domain with the help of factorization machines.

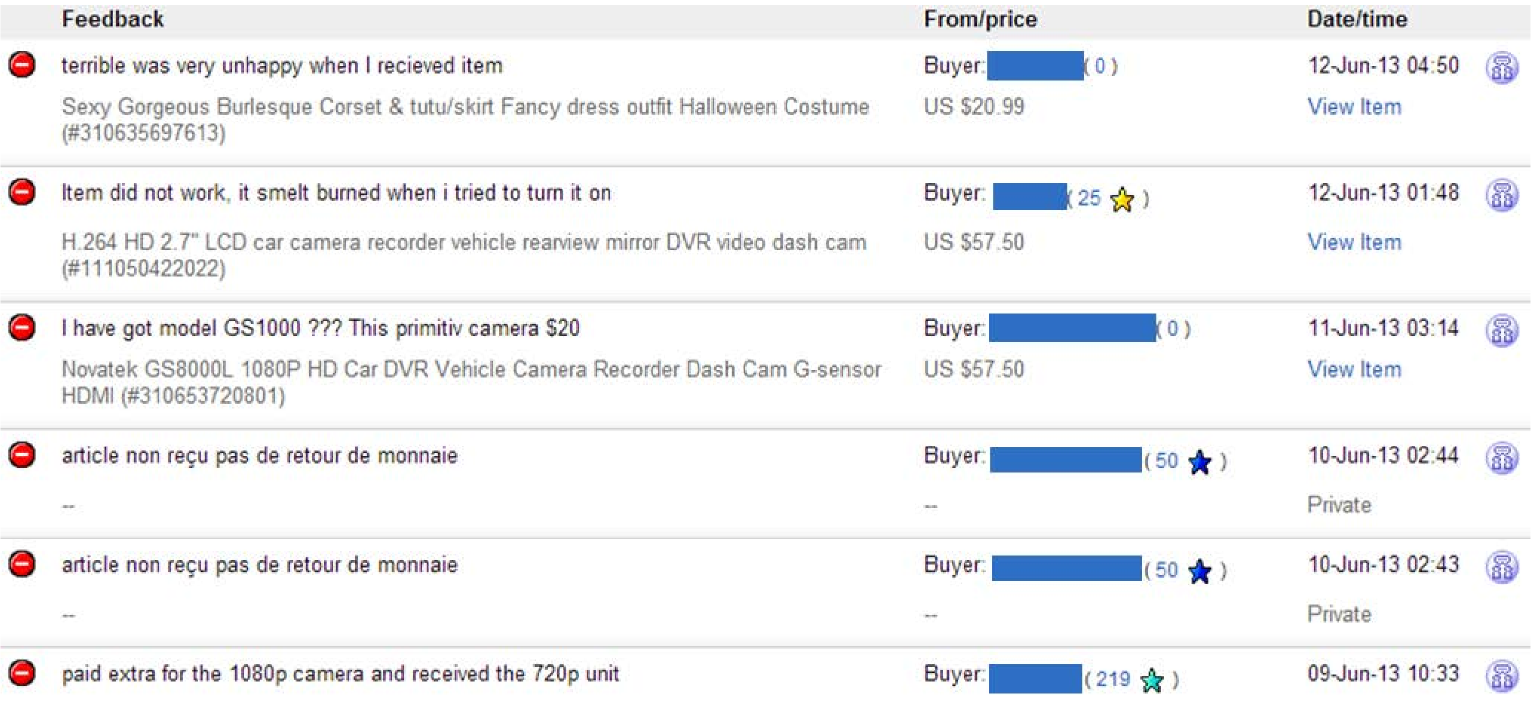
Moreover, utilizing factorization machines, Liu [122] proposes a trust network based context-aware social recommendation model, which takes into account both social and non-social contextual information. In his work, random walk is used to collect the most relevant ratings regarding the multi-dimensional trustworthiness of users from a trust network, and the factorization machine is applied to predict the missing ratings while considering the contexts. Especially, different from conventional factorization machine models, the n-dimensional feature vector is constructed of the information from a user, an item and any contexts regarding this interaction, and by this strategy, the contextual information is incorporated into the factorization machine model.

2.4.3 Dynamic Trust Prediction

Due to the nature of virtual communities, people including vendors (providers) and consumers do not meet or interact physically. As shown in Figure 2.4.3, the evidence of cheating can be easily seen in eBay community. In such an environment with uncertainty, the prediction of the dynamic trust about a vendor or a service provider in online environments has become increasingly important [107][209][207]. Modeling the dynamic trust of an online vendor or a service provider is a challenging task. According to the applied algorithms, the existing works are mainly classified into three categories.

2.4.3.1 Beta Models

One typical approach is the Beta reputation method proposed by Jøsang [82], which combines feedback and derives reputation ratings based on Beta probability density functions. The advantage of the Beta reputation system is its flexibility and simplicity



	Feedback	From/price	Date/time
⊖	terrible was very unhappy when I recieved item Sexy Gorgeous Burlesque Corset & tutu/skirt Fancy dress outfit Halloween Costume (#310635697613)	Buyer: [redacted] (0) US $20.99	12-Jun-13 04:50 View Item
⊖	Item did not work, it smelt burned when i tried to turn it on H.264 HD 2.7" LCD car camera recorder vehicle rearview mirror DVR video dash cam (#111050422022)	Buyer: [redacted] (25 ☆) US $57.50	12-Jun-13 01:48 View Item
⊖	I have got model GS1000 ??? This primitiv camera $20 Novatek GS8000L 1080P HD Car DVR Vehicle Camera Recorder Dash Cam G-sensor HDMI (#310653720801)	Buyer: [redacted] (0) US $57.50	11-Jun-13 03:14 View Item
⊖	article non reçu pas de retour de monnaie --	Buyer: [redacted] (50 ★) --	10-Jun-13 02:44 Private
⊖	article non reçu pas de retour de monnaie --	Buyer: [redacted] (50 ★) --	10-Jun-13 02:43 Private
⊖	paid extra for the 1080p camera and received the 720p unit	Buyer: [redacted] (219 ☆)	09-Jun-13 10:33

Figure 2.2: The real cheating behaviors happened at eBay

as well as its foundation on statistics theories. Later on, based on the intuition that recent information is more important for the prediction of dynamic trust, the Beta model is improved by adding a decay factor to control the weight of data [52], which makes the model focus more on recent data. Furthermore, Zhang and Cohen [238] model agent behaviors with a time window, in which the numbers of successful and failed transactions are aggregated with a forgetting rate, and the trustworthiness is adjusted accordingly. Although these approaches show success in certain scenarios, they are not effective in the scenarios where the vendor's (or provider's) behavior is highly dynamic or is changing strategically.

2.4.3.2 HMM-based Models

Several trust prediction methods based on Hidden Markov Model (HMM) have been proposed to deal with the dynamics of the online vendor or service provider. Several studies [52, 149] propose the HMM approach in modeling transaction results. In these models, the outcomes of each past transaction, say failure or success, are treated at the observation of HMM. This type of HMM-based approaches work much better than Beta model-based methods in detecting a service provider's changes, and are more suitable for modeling dynamics. However, such HMM-based approaches utilize only the outcomes of the past transactions as the observation sequence, but ignores the contextual information about each transaction, and makes the prediction a full guess.

To solve this problem, Liu and Datta [124] propose a contextual information-based Markov model, which extracts features from transaction contextual information as the observation sequences of HMM and treats the outcomes directly as the states of the models. Liu and Datta [124] also apply information theories and Multiple Discriminant Analysis to reduce the feature space. This approach utilizes the contextual information and speeds up the calculation, as it simplifies the training of HMM to the statistics of past records. However, it reveals the hidden states of HMM and the authors also assume a series of transactions occurring between a seller and the same customer, which can hardly be true in most actual scenarios. In addition, there could be more features to be taken into account, such as price changes, in addition to static features in the contextual information.

2.4.3.3 ANN-based Models

Besides HMM-based dynamic trust prediction models, Artificial Neural Network (ANN) is another favorite heuristic algorithm for the prediction of future trust values. For example, Azadeh [15] proposes an ANN-based trust prediction model. In this model both the linguistic expressions of trust values and the reliability of recommendations are taken into account; Z-numbers, introduced by Zadeh [230], are used to convert qualitative expressions to real numbers; and then ANN is applied to predict the trust values in the future.

However, there are a few disadvantages limiting ANN. The initialization and network topology design rely on the experience of a designer. ANN-based models are susceptible to over-fitting and hard to converge to the global optimal solution.

2.5 Conclusion

A general overview of the research works has been provided in this chapter including online social networks, trust, trust network extraction and trust prediction. First, we have presented the properties of social networks indicated by social scientists, and have categorized the online social networks according to their different characteristics. Second, we have provided a detailed overview of trust from the aspects of multi-discipline definition, property, influence and the social context that affects trust, as indicated by social scientists based on their long-term observation of a large number of human activities. Therefore, these properties of trust and social contexts should be considered in the trust prediction process in any situation. Third, we have reviewed the existing approaches that are able to extract a social trust subnetwork from the whole online social network, which is used to improve the efficiency and effectiveness of forthcoming trust prediction. Last but not least, we have analyzed the advantages and disadvantages of the existing studies of different categories of trust prediction, and the studies that can be leveraged for trust prediction in online social networks, including propagation-based trust prediction, latent factor-based trust prediction and dynamic trust prediction.

Chapter 3

Subnetwork Extraction in Trust Social Networks

As introduced in Chapter 1, Online Social Networks (OSNs) contain important participants, the trust relations between participants, and the contexts in which participants interact with each other. All of these are of great value for the prediction of the trust between a source participant and a target participant, which is important for a participant's decision-making process in many applications such as seeking service providers. However, predicting the trust from a source participant to a target one based on the whole social network is not really feasible. Prior to trust prediction, the extraction of a small-scale subnetwork containing most of the important nodes and contextual information with a high density rate could make trust prediction more efficient and effective.

In order to address this challenging subnetwork extraction problem, in this chapter, Section 3.1 describes the problem of social trust subnetwork extraction. In Section 3.2, we define a utility function to measure the trust factors of each node in a social network and formulate the subnetwork extraction problem. Section 3.3 presents the basic knowledge of Ant Colony Algorithm (ACA) which is the basis of our proposed models in the following sections. In Section 3.4, we propose a social context-aware trust subnetwork extraction model, called *BiNet*, which can extract a contextual subnetwork for the specific purpose of predicting the trust from a source node to a target node in the target social context of an item to be recommended. In this model, we design a novel binary ant colony algorithm (NBACA) with newly-designed initialization and mutation processes for subnetwork extraction incorporating the utility function. Then, we compare *BiNet* with the existing approaches in Section 3.5. The experiments conducted on two popular social network datasets, Epinions and Slashdot, demonstrate the superior performance of our proposed *BiNet* over the state-of-the-art approaches. In Section 3.6, we propose another social context-aware trust subnetwork extraction model, called *TrustNet*, in which, we design a novel ant colony algorithm (NACA) for the subnetwork extraction problem, by adding an mutation process and improving the path selection and pheromone update processes of traditional ACA. Next, *TrustNet* is compared with *BiNet* and other state-of-the-art approaches in Section 3.7 on both Epinions and Slashdot datasets. The results show that *TrustNet* is superior to *BiNet* and other state-of-the-art approaches in terms of the quality of extracted subnetworks within the same execution time. This chapter is finally summarized in Section 3.8.

3.1 The Trust Network Extraction Problem

OSNs are usually represented as graphs as shown in Fig. 3.1. A node in the graph represents a participant in an OSN while the edge pointing from one node to an adjacent node corresponds to their real-world or online interactions (e.g., $A \rightarrow B$ in Fig. 3.1). Different types of edges represent different contexts, which refer to any information available for characterizing the participants and the situations of interactions between them [206], e.g., a solid line refers to the relationship in Swift programming, a dashed line refers to C++ programming and a dotted line refers to tennis playing in Fig. 3.1. The trust can be explicitly given by one participant to another based on their history of interactions.

In Fig. 3.1, suppose A is looking for a collaborator such as a Swift programmer and H is recommended to A as a Swift programmer. But, A does not know H. Here we assume Swift programming is the *target context*, i.e., the context in which the trust between a source node and a target node needs to be predicted. In A's mind, B, E

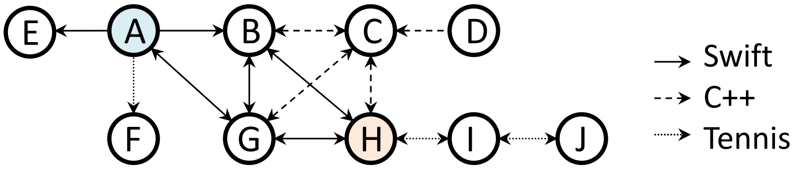


Figure 3.1: A social network

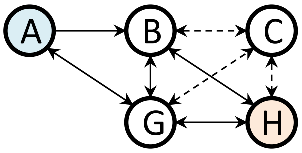


Figure 3.2: Subnetwork

and G are good Swift programmers. B, G and H trust each other and G also trusts A regarding Swift. C trusts B, G and H regarding C++ programming and vice versa. D also trusts C regarding C++. F, I, J and H are good tennis players. In order to predict if H will be a good Swift programmer in A's mind, it is unnecessary to use the whole social network in Fig. 3.1, because F, I and J are only good at tennis while Swift programmer E and C++ programmer D have little knowledge of others. Let us assume this social network is only constructed in three contexts: Swift, C++ and tennis. In order to boost the efficiency and effectiveness of trust prediction regarding the target context Swift, the social subnetwork in Fig. 3.2 is extracted from Fig. 3.1 by removing the social relations in tennis playing and keeping only the important social relations for the prediction of trust between A and H on Swift and C++ teaching, because 1) tennis is irrelevant to the target context Swift; 2) C++ is relevant to Swift; and 3) nodes, such as D and E, are not so important as others for the trust prediction task. In addition, the density of the subnetwork in Fig. 3.2 is raised from the original 0.23 of Fig. 3.1 to 0.6, which can enhance the trust prediction accuracy of matrix factorization-based approaches [89, 225, 243].

In the literature, there are some existing works focusing on *trust prediction*, i.e., the process of estimating a new pairwise trust relationship between two nonadjacent participants. Most of these works predict trust based on social graphs (e.g., Fig. 3.2) using inference approaches [66, 110, 118, 119, 206], while a few of them predict trust from a *trust matrix*, i.e., a representation of social networks in matrices rather than graphs, using matrix factorization approaches [225, 78, 243]. All of these trust prediction models assume that the trust network or matrix including the source and the target participants has already been extracted, or even that the whole dataset is directly used. However, subnetwork extraction is a necessary step prior to trust prediction as it provides the foundation for trust prediction, and can help improve the effectiveness and efficiency of trust prediction [162, 117]. In addition, extracting such a trust subnetwork/matrix is a multi-objective optimization problem, which is known to be NP-complete [17, 117].

An extracted subnetwork (e.g., Fig. 3.2) needs to satisfy the following requirements: (i) it should contain the source node, the target node and most of the nodes which are important for trust prediction between the source node and the target node; (ii) the scale of the subnetwork/matrix is kept relatively small; and (iii) a source participant may introduce constraints of trust relations or contextual information into the subnetwork extraction process for various purposes, such as employee recruitment and movie recommendation, which makes the problem more challenging.

In addition, there are very few approximation algorithms proposed for the NP-complete subnetwork extraction problem for trust prediction in online social networks. As introduced in Subsection 2.3.3, most existing works rely on trust paths and do not perform well for matrix factorization-based trust prediction approaches, as the density of the extracted subnetwork is not considered. And even the state-of-art subnetwork extraction models still need improvement in the aspects of both efficiency and effectiveness.

3.2 Formulation with Social Information

As an extracted subnetwork is specific to the subsequent trust prediction from a source node to a target node, and trust is affected by a number of social contexts which have been introduced in Section 2.2.4, the information affecting trust prediction must be considered in the subnetwork extraction process.

3.2.1 Trust Impact Factors

In order to utilize social information about participants and their interactions for the subnetwork extraction process, the social information in all relevant contexts needs to be organized into several aspects, which are called trust impact factors. The detail of each trust impact factor is described below.

In addition, a pre-process based on context relevance can be applied to determine the initial searching scope before proceeding to subnetwork extraction.

Role Impact Factor: In a certain context, the role impact factor (denoted as RIF) illustrates the impact of a participant's social position and expertise on his/her trustworthiness, based on the fact that a person who has expertise in a domain is more credible than others with less knowledge [117].

Reliability: In a certain context, reliability (RLB) measures the rate a participant's suggestions are accepted by others [81]. A participant with high reliability is likely to be sought suggestions from, which can affect the trust towards the participant. The reliability is calculated as one minus the deviation between the predicted rating and the actual ratings of a participant in [81].

Preference Similarity: It is illustrated in social psychology [232] that a participant can trust and have more social interactions with another participant, with whom he/she shares more preferences (e.g., both of them like teaching C++). Preference similarity (PS) between two participants' preferences can impact the trust between them to some extent [206]. Here, $PS_{i,j} = PS_{j,i}$ for participants i and j.

Social Intimacy: Social intimacy (SI) refers to the frequency of connections between participants in a social network. The degree of social intimacy can impact trust as people tend to trust those participants, with whom they have more intimate social relationships [33].

Existing Trust: Trust is a belief that an entity, such as a person or an organization, will behave in an expected manner, despite the lack of ability to monitor or control the environment in which it operates [180]. It can be impacted by all the above properties and the trust value can be greatly different between the same two participants in different interaction contexts [212]. Let $T_{i,j}$ denote the existing trust participant i gives to participant j. A higher $T_{i,j}$ indicates more trust to j in i's mind. Here, trust between two participants in a given context is not symmetrical, which means $T_{i,j}$ may not be equivalent to $T_{j,i}$.

3.2.2 Utility

For the extraction of a subnetwork which is specific to the prediction of the trust from a source participant to a target one, for each node in the subnetwork, we propose a *node utility* (denoted by u_i) which is the weighted sum of all the above trust impact factors in a subnetwork. It can be formulated by:

$$\mathsf{u}_i = F \cdot W' \tag{3.1}$$

where, W is a coefficient vector given by users; and

$$F = [RIF_i, RLB_i, SI_{s,i}, PS_{s,i}, T_{s,i}, SI_{i,t}, PS_{i,t}, T_{i,t}], \tag{3.2}$$

is a vector containing all the factors that affect the trust between the source participant and the target participant. These factors can be divided into three groups: (i) RIF_i and RLB_i are personal factors and are independent of the source and target participants; (ii) $SI_{s,i}$, $PS_{s,i}$ and $T_{s,i}$ are the factors revealing the relationship with the source participant; and (iii) $SI_{i,t}$, $PS_{i,t}$ and $T_{i,t}$ reveal the relationship with the target participant. $\mathsf{u}_i \in [0,1]$ as the range of each factor is $[0,1]$.

3.2.3 Formulation of the Problem

The problem can be described as finding a certain number of nodes (say m, $0 < m \leq n$) out of the n nodes to compose a subnetwork which increases the objective function value (the weighted sum of the average node utility of the extracted subnetwork and the density of the extracted subnetwork) as much as possible. The objective function is formulated as:

$$G(X) = \zeta \frac{\sum_{i=1}^{n} \mathsf{u}_i x_i}{\sum_{i=1}^{n} x_i} + \tilde{\zeta} D(X), \tag{3.3}$$

where $X = \langle x_i | i = 1, ..., n \rangle$ is a vector representing the selection of nodes for a subnetwork; $x_i = 1$ means the ith node is selected while $x_i = 0$ means the ith node is not selected. $\sum_{i=1}^{n} x_i$ is the number of the selected nodes. $D(X)$ is the density of the current subnetwork. $\mathsf{u}_i (i = 1, 2, ..., n)$ is the utility of node i calculated by Equation (3.1). ζ and $\tilde{\zeta}$ are the weights.

Therefore, the subnetwork extraction problem can be formulated as:

$$max\ G(X) \ \ s.t. \begin{cases} x_i \in \{0, 1\}, 1 \leq i \leq n \\ x_s + x_t = 2 \\ \mathsf{u}_i x_i \geq K_t \end{cases} \tag{3.4}$$

where, x_s and x_t are the selection of the source node and the target node; $x_s + x_t = 2$ means both of the source node and the target node must be selected; K_t is a threshold value of the judgment of the important nodes.

3.3 Brief Introduction to Ant Colony Algorithm

As ant colony algorithm (ACA) is a type of efficient approaches with robustness and global searching ability for solving multi-objective optimization problems [218, 47], our proposed subnetwork selection approach is based on ant colony algorithms. This section briefly introduces the basic idea of ACA.

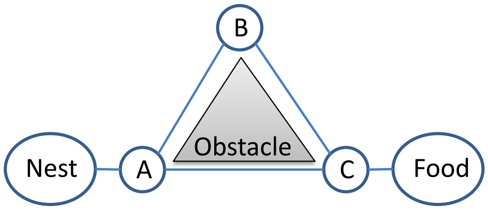


Figure 3.3: Demonstration of food finding process

ACA was first inspired by the observation of ant colonies in the early 1990s [27, 47]. Ants are social insects and live in colonies. Their behaviors are revealed by the whole colony rather than by individuals. When ants go out to search for food, initially, every ant randomly explores the area around its nest and leaves chemical pheromone on the path it travels. Once an ant finds a food source, it takes part of the food back to the nest leaving pheromone along all the way. When other ants come near paths with pheromone, they tend to choose the path, with a high probability, with the strongest pheromone which guides other ants to follow the same path. Meanwhile, the pheromone on the path is strengthened by each ant traveling along the path. Thus in the end, most ants will follow the same path to the food source from the nest. However, when choosing a path, individual ants can make incidental mistakes. Therefore, they have a certain probability not to choose the path with the highest pheromone, forming new paths and enabling most ants to find the shortest path [27].

Considering the example shown in Fig. 3.3, suppose that the distances of $A - B$, $A - C$ and $B - C$ are equal. At the beginning, there are N ants starting from their nest to find food by randomly choosing the paths. When the first few ants find food and return to the nest, the pheromone on the paths they have passed (i.e. $A - C$) is enhanced. Forthcoming ants have a higher probability to choose the path with more pheromone. After repeating several times, most ants will follow the path $A - C$ to fetch food which is the shorter way.

The ant colony algorithm simulates the process of foraging in an ant society and provides a mechanism for searching for optimal solutions. For the subnetwork extraction problem, the above foraging process has to be specially designed. Generally, there are normally two ways of applying ant colony algorithms: the binary way and the non-binary way, which will be detailed in Section 3.4 and Section 3.6.

3.4 The Proposed Novel Binary Ant Colony Algorithm

In this section, we propose our NBACA-based model to find a subnetwork in a social network including the source and target nodes. While the number of nodes in the extracted subnetwork should be as small as possible, it has to contain as many important nodes as possible. Thus, the final solution is a trade-off between a high average node importance and the density of the subnetwork.

3.4.1 The Design of Our NBACA

For the trust subnetwork extraction problem, the conventional BACA [80, 93] has two main disadvantages: (i) the number of the selected nodes in the extracted subnetwork fluctuates around the mathematical expectation of the number of the selected nodes in initialization; and (ii) the path selection process is only determined by pheromone information without any heuristic function from prior knowledge. These two disadvantages slow down the convergence speed of BACA. To overcome these disadvantages, a novel binary ant colony algorithm is designed.

Fig. 3.4 shows the designed weighted graph containing $n+1$ knots (stops) arranged in the order from 1 to $n+1$. Ant movement starts from knot 1. At each knot $i(i = 1, 2, ..., n)$, there are 2 directed paths $a[i, j](j \in \{0, 1\})$ connecting to knot $i+1$. On each path $a[i, j](i = 1, 2, ..., n; j = 0, 1)$, there is a value u_i, representing the utility of node i, and $\mathsf{U} = \{\mathsf{u}_i | i = 1, ..., n\}$. Therefore, an ant k going via path $a[i, 1]$ means the ith node is selected (noted by $x_i^k = 1$) by the ant k for the subnetwork, while the ant k going via path $a[i, 0]$ means the ith node is not selected ($x_i^k = 0$). The subnetwork selected by ant k is called solution k, represented by $X^k = \langle x_i^k | i = 1, ..., n\rangle$.

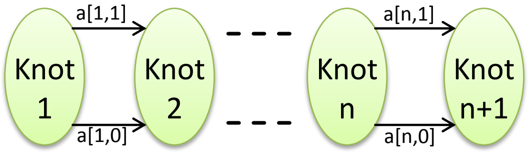


Figure 3.4: Construction of the weighted graph

Different from the conventional ACA and BACA, in our designed NBACA, the pheromone on path $a[i, j]$ is represented by a percentage value, denoted by $\tau_{ij}(t)$. Therefore, only one of the two paths from knot i to $i + 1$ needs to be stored in each iteration, as there are only two paths connecting knot i and knot $i + 1$ as well as $\tau_{i0}(t) = 1 - \tau_{i1}(t)$. The detailed processes in NBACA are summarized in the following subsections.

3.4.2 Initialization

In ants' natural world, when an ant selects a path for foraging, its selection is affected by the pheromone on each available path. And the path with more pheromone has a higher probability to be selected. Utilizing a random value and the node utility, our proposed initialization process is to produce the pheromone of each path at the beginning time $t = 0$. The initial pheromone on path $a[i, 1]$ can be formulated as:

$$\tau_{i1}(0) = \varphi\chi_i + \psi\eta_i \tag{3.5}$$

where, $\chi_i \sim \mathcal{N}(\mu, \sigma^2)$ represents a random distribution of the pheromone on each path. As there are two paths connecting two adjacent knots, the mathematical expectation μ of the distribution is fixed to 0.5, and the variance σ is adjustable. η_i is an expectation heuristic function representing the nodes' importance in a social network. Here, $\eta_i = \mathsf{u}_i / \max\{\mathsf{U}\}$ is the rate of node i's utility to the maximum node utility in the whole social network. Coefficients φ and ψ represent the weights of χ_i and η_i respectively. In addition, the initial pheromone on path $a[i, 0]$ is $\tau_{i0}(0) = 1 - \tau_{i1}(0)$ in our NBACA.

3.4.3 Path Selection

On path $a[i, j]$ at time $t(t = 0, 1, 2, ...)$, the probability of the path to be selected is determined by both the pheromone $\tau_{ij}(t)$ and the heuristic function value η_i. At time $t = 0$, y ants are created and put on knot 1. Then each ant selects a path and moves to the next knot according to both the pheromone on each path and the heuristic function. This process continues till the ant reaches the terminal knot $n + 1$. The solutions are represented by $\{X^k|k = 1, ..., y\}$.

At time t, the transition probability of ant $k(k = 1, 2, ..., y)$ moving from knot i $(i = 1, 2, ..., n)$ to knot $i + 1$ via path $a[i, 1]$ is:

$$p_{i1}^k(t) = \alpha\tau_{i1}(t) + \beta\eta_i \tag{3.6}$$

where, η_i is a heuristic function value which is the same as that in the initialization process. The larger η_i is, the more likely ant k selects node i (goes via the path $a[i, 1]$). α and β are the weights of the pheromone and the heuristic function when ants select the paths. In addition, the transition probability of moving via $a[i, 0]$ is:

$$p_{i0}^k(t) = 1 - p_{i1}^k(t). \tag{3.7}$$

3.4.4 Mutation

The mathematical expectation of the number of paths $a[i, 1]$ (selected nodes from a social network) is affected by the initialization [93]. In order to increase the variance of the number of selected nodes in each iteration, we propose a mutation process to produce new solutions especially with a different number of selected nodes. In the mutation process, ants can more easily forget the selection of paths corresponding to the unimportant nodes in a social network. For each ant k, this process is formulated as:

$$X_-^k = \langle x_i^k * 1\{p_{i1}^k > \lambda_i\}|i = 1, ..., n\rangle \tag{3.8}$$

$$X_+^k = \langle 1\{(x_i^k + 1\{p_{i1}^k > \lambda_i\}) > 0\} | i = 1, ..., n\rangle \tag{3.9}$$

where $\lambda_i \sim \mathcal{U}(0, 1)$ is a normal number obtained from a continuous uniform distribution. $1\{.\}$ is a Boolean function. It is equal to 1 if the condition in $\{\}$ is satisfied. Otherwise it equals 0. Eqs. (3.8) and (3.9) are able to generate solutions with less and more numbers of selected nodes from a social network respectively. Finally, an ant k obtains 3 different solutions after finishing its trip $\{X^k, X_-^k, X_+^k\}$.

Although the mutation process increases the calculation time of the quality of solutions, the overall execution time is reduced, because: 1) mutation process does not affect the time period of an ant's movement in all life time; 2) the extra two solutions are generated from the solution obtained by an ant using simple equations; and 3) the diversity of solutions in each iteration is increased greatly, which speeds up the convergence significantly.

3.4.5 Upgrade of Pheromone

When all the y ants reach the terminal knot, $3y$ feasible solutions $\{X^k, X_-^k, X_+^k | k = 1, ..., y\}$ can be obtained. If the best solution in the current iteration (denoted by X_{best}') is better than that of all the past iterations (the best-so-far solution, denoted by X_{best}), then, $X_{best} = X_{best}'$ and the pheromone on each path i is upgraded accordingly. The pheromone upgrade procedure consists of two parts: (i) the pheromone evaporation procedure which is applied to path i if node i is not selected for the so-far-best solution ($x_i = 0$ and $x_i \in X_{best}$) and is formulated as:

$$\tau_{i1}(t + 1) = (1 - \rho)\tau_{i1}(t) \tag{3.10}$$

and (ii) the pheromone intensification procedure which is only available for path i if node i is selected for the best-so-far solution ($x_i = 1$ and $x_i \in X_{best}$) and formulated as:

$$\tau_{i1}(t + 1) = \tau_{i1}(t) + \varrho|1 - \tau_{i1}(t)| \tag{3.11}$$

where $\rho(0 < \rho < 1)$ is a parameter called the pheromone evaporation rate and $(1 - \rho)$ is the pheromone residue rate; $\varrho(0 < \varrho < 1)$ is the pheromone increment rate on path $a[i, j]$ in the current iteration.

Because $p^k_{i0}(t) = 1 - p^k_{i1}(t)$ and the pheromone in our NBACA is presented as a percentage, the evaporation and intensification processes need to be conducted only on the paths of $a[i, 1](i = 1, 2, ..., n)$.

3.4.6 Algorithm

Algorithmic Process: The main process of finding the subnetwork in a social network using NBACA is described in Algorithm 1. In each iteration, the best solution, among the solution sets $X^{(NC)} = \{X^k, X^k_-, X^k_+ | k = 1, ..., y\}$ obtained from the y ants in the current iteration, is used to update the pheromone, if it is better than the so-far-best solution. Then, the next iteration starts using the updated pheromone information. Finally, the iteration process ends returning the best solution, when NC, the number of iterations already run, reaches the maximum value NC_{max} or NF, the number of iterations where the best-so-far solution stayed the same, reaches the preset maximum value NF_{max}.

Summary: Different from the conventional BACA, the design of our NBACA is greatly improved in each step. Its characteristics are as follows: (i) An initialization process is introduced. The pheromone on each path is initialized by both a random value generated from a Gaussian distribution and the node utility proposed in Section 3.2, which improves the initial probability of each path to be selected in ants' initial movement. (ii) In our designed NBACA, the pheromone information is represented by percentage values, which reduces the storage of pheromone information and simplifies path selection and pheromone update processes resulting in a reduction of execution time. (iii) A mutation strategy is first introduced into conventional BACA, which increases the solution range in each iteration and speeds up the convergence of

```
Algorithm 1: Binary Ant Colony Algorithm
Data: $\varphi$, $\psi$, $\alpha$, $\beta$, $\rho$, $\varrho$, $y$, $n$, $NC_{max}$, $NF_{max}$
Result: The best solution when the iteration ends
begin
    Initialize $NC$ & $NF$ & $X_{best}$;
    while $NC < NC_{max} \& NF < NF_{max}$ do
        Produce $y$ ants and put them on knot $1$;
        Initialize $\tau_{i1}(0)(i = 1, 2, ..., n)$;
        NC=NC+1;
        for each ant $k(k = 1, 2, ..., y)$ do
            for each movement $i(i = 1, ..., n)$ do
                Select next path $a[i, j]$ via Eq.(4);
                $x_i^k = j$;
            end
            Return $X^k = \langle x_i^k | i = 1, ..., n \rangle$;
            Get $X_-^k$ & $X_+^k$ via Eq.(3.8&3.9);
        end
        $X^{(NC)} = \{X^k, X_-^k, X_+^k | k = 1, ..., y\}$;
        $X'_{best} = arcmaxG(X^{(NC)})$;
        if $G(X'_{best}) > G(X_{best})$ then
            $X_{best} = X'_{best}$;
            Upgrade pheromone via Eq. (3.10&3.11);
        else
            NF=NF+1;
        end
    end
    Return $X_{best}$;
end
```

the NBACA. And (iv) our designed NBACA is not limited to the application of subnetwork extraction problems, and it can be applied to any case where the conventional ACA is applicable.

3.5 Experiments on NBACA

We have conducted experiments on two popular social network datasets, Epinions and Slashdot [103], and compared the performance of our *BiNet* with two state-of-the-art approaches, SCAN [117] and FDRS [73], and a baseline approach, BACO [80].

3.5.1 Dataset Description

Although, there are a number of studies on mining a single impact factor in social networks [141, 202], there is no dataset in place that contains all the contextual values we need. Thus, the experiments are conducted on semi-synthetic datasets which consist of the datasets from real social networks of **Epinions** (131,828 nodes and 841,372 edges) and **Slashdot** (82,144 nodes and 549,202 edges), and synthetic trust impact factor values. In order to demonstrate that the performance of our model is not data sensitive, 10 groups of the trust impact factor values are randomly generated for both Epinions and Slashdot datasets in the experiments respectively.

3.5.2 Comparisons

In order to evaluate the performance of our proposed model *BiNet*, we compare it with two state-of-the-art models, SCAN and FDRS, and a baseline model, BACO.

SCAN is a social context-aware trust network discovery approach which considers social contextual impact factors and finds the context-aware trust network under certain constraints of each trust impact factor, by adopting a Monte Carlo search method with optimization strategies [117].

FDRS is a fast discovery approach of reliable subnetworks which treats a social network as a Bernoulli random graph, and builds up the sub-graph by incrementally adding paths from a source node to a target node to an initially empty sub-graph until the addition of any paths will not increase the objective function value of the whole subnetwork [73].

BACO is a binary ant colony optimization algorithm which is based on the concept and principles of ant colony optimization to solve the binary and combinatorial optimization problems. It can be applied, as a baseline approach, to extract the trust subnetwork when the selection of a node in a social network is treated as the selection from binary paths in ants' movements [80].

In addition, all three models are coded and executed in Matlab R2012B on a desktop powered with an Intel i7-2600 CPU and 8G memory running Windows 7 64-bit Professional.

3.5.3 Experiment Setting

In order to compare the differences in efficiency and effectiveness between our proposed model *BiNet* and each of SCAN, FDRS and BACO, experiments are conducted on both Epinions and Slashdot datasets enhanced with synthetic trust impact factor values respectively, to find the near optimal subnetwork for each of 10 pairs of nodes which are randomly selected, with different social connection degrees, as the source-target node pairs.

In the experiments on the Epinions dataset, the subnetwork extraction for each source-target node pair is performed on the trust relationships of the Epinions dataset with each of the 10 groups of trust impact factor values. Likewise, in the experiments on the Slashdot dataset, the subnetwork extraction for each source-target node pair is performed with each of the 10 groups of trust impact factor values.

Then, the 10-time cross validation is applied for each of *BiNet*, SCAN, FDRS and BACO. In total, each model is run for 2000 times (2 datasets × 10 groups of impact factor values × 10-time cross validation × 10 source-target pairs). The average results on both datasets are plotted in Figs. 3.5-3.6 respectively.

Parameters, such as the trust factor constraints, only affect the utility values obtained in the experiments but do not affect the performance comparison between different models, as all models are compared on the same datasets. This type of parameters are given by users in application. Suppose, equal weights are given by users in the experiments. Other parameters, such as the ones in the ant colony algorithm, are determined by the experimental performance of the models after trying different parameter values using grid search, where $\zeta = \tilde{\zeta} = 0.5$, $\varphi = 0.2$, $\psi = 0.8$, $\alpha = \beta = 0.5$,

Table 3.1: The results of experiment 1 at 40^{th} second

Dataset	Cases	BiNet	SCAN	FDRS	BACO
Epinions	Min	0.575	0.540	0.485	0.294
	Improvement	-	6.1% higher	15.7% higher	48.9% higher
	Mean	0.631	0.587	0.541	0.301
	Improvement	-	**6.9% higher**	**14.3% higher**	**52.3% higher**
	Max	0.69	0.612	0.581	0.312
Slashdot	Improvement	-	11.3% higher	15.8% higher	54.8% higher
	Min	0.529	0.503	0.513	0.279
	Improvement	-	4.9% higher	3.0% higher	47.4% higher
	Mean	0.611	0.559	0.561	0.285
	Improvement	-	**8.5% higher**	**8.2% higher**	**53.4% higher**
	Max	0.657	0.599	0.598	0.292
	Improvement	-	8.8% higher	9.0% higher	55.6% higher

$\rho = 0.1$, $\varrho = 0.1$, $K_t = 0.5$, $NC_{max} = 400$ and $y = 40$.

3.5.4 Results and Analysis

Results: *BiNet*, SCAN and BACO are all iterative algorithms whose results get better as the time goes. In Figs. 3.5-3.6, we present the mean results over each group of datasets delivered within the first 40 seconds time limitation which are sufficient to demonstrate the performance of each model, as in real applications, we cannot really execute the models for such a long time. The best, mean and worst results on each group of datasets at the 40^{th} second are presented in Table 3.1. As the FDRS model is not an iterative model, it yields one fixed result on each dataset using over 100 seconds.

Fig. 3.5 shows the average objective function values (Eq.(3.3)) of the subnetworks extracted by all the four models on the Epinions dataset within the first 40 seconds. As time goes on, the best-so-far solutions of *BiNet*, SCAN and BACO become better, while the result of FDRS keeps unchanged as it is not an iterative algorithm. Our proposed *BiNet* outperforms all other three models after 3.2 seconds. At the 40^{th} second, the average objective function value of the subnetwork delivered by *BiNet* is

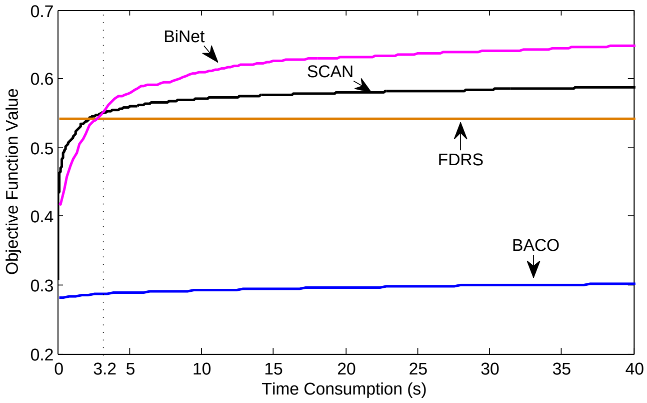


Figure 3.5: Results on Epinions dataset

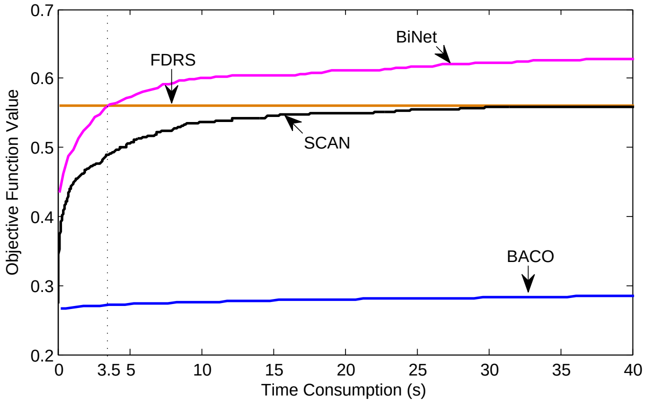


Figure 3.6: Results on Slashdot dataset

6.9% higher than the one delivered by SCAN, 14.3% higher than the one delivered by FDRS, and 52.3% higher than the one delivered by BACO.

Fig. 3.6 shows the average objective function values of the subnetworks extracted by the four models on the Slashdot dataset within the first 40 seconds. On this dataset, our *BiNet* outperforms both SCAN and BACO from the very beginning and outperforms FDRS after 3.5 seconds. At the 40^{th} second, the average result of *BiNet* is 8.5% higher than that of SCAN, 8.2% higher than that of FDRS, and 53.4% higher than that of BACO.

Analysis: The differences between our *BiNet* model and SCAN, FDRS and BACO on both datasets, especially, the significant improvement between *BiNet* and BACO, mainly come from the following aspects: (i) the initialization process of our proposed algorithm set up our model using both random values from the normal distribution and a heuristic function from nodes utilities, which makes our model able to find solutions with a relatively high utility from the first iteration without losing diversity; (ii) the mutation process generates an extra solution with a smaller number of selected nodes and another extra solution with a larger number of selected nodes in each iteration, and thus can broaden the scope of search in each iteration; (iii) the percentage representation of pheromone information only needs to record the pheromone on half the number of paths, and thus can save memory and reduce execution time; (iv) our designed model selects nodes from both pheromone information and a heuristic function, which speeds the convergence and betters the performance within a fixed time; (v) pheromone update process is kept simple, which makes our model more efficient; and (vi) the big improvement between *BiNet* and BACO demonstrates that our proposed model significantly overcomes the conventional disadvantages of BACAs.

In addition, our proposed model outperforms the other models in all the three cases presented in Table 3.1 shows that our model is not data sensitive and applies to a wide scope of applications.

3.6 The Proposed Novel Ant Colony Algorithm

Although our proposed NBACA has achieved a great improvement over the state-of-the-art approaches, the non-binary way of applying ACA is still worth trying, which can get a better diversity of solutions in each iteration than binary ACA. In this section, we propose a non-binary ant colony algorithm for subnetwork extraction problem in order to achieve better performance.

3.6.1 The Design of Our NACA

Inspired by the conventional ACA for the Knapsack problem [47, 239], we proposed a novel ant colony algorithm (NACA) for subnetwork extraction. In particular, a mutation process is designed in order to provide a strategy to remove the nodes already selected for the subnetwork.

Fig. 3.7 shows the designed weighted graph containing $n + 1$ knots (stops) arranged in the order from 1 to $n + 1$. Starting from each knot $i(i = 1, 2, ..., n)$, there are n directed paths $a[i, j](j = 1, 2, ..., n)$ connecting to knot $i + 1$. On each path $a[i, j](i, j = 1, 2, ..., n)$, there is a value u_j, the utility of node j. Therefore, "an ant going via path $a[i, j]$" means the jth node is selected by the ant for the subnetwork.

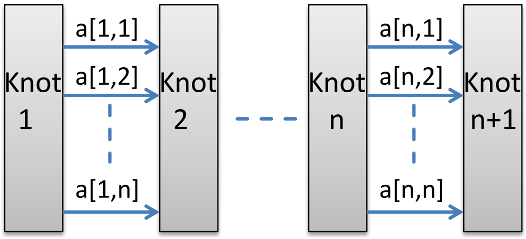


Figure 3.7: Construction of the weighted graph

3.6.2 Path Selection

In ants' natural world, when an ant selects a path for foraging, its selection is affected by the pheromone on each available path. A path with more pheromone has a higher probability to be selected. In ACA, the pheromone on path $a[i, j]$ at time $t(t = 0, 1, 2, ...)$ is denoted by $\tau_{ij}(t)$. At the beginning $t = 0$, the pheromone on each path is equal to a small positive value C, formulated as $\tau_{ij}(0) = C$ (note that if $C = 0$, the denominator will be 0). At time $t = 0$, y ants are created and put on knot 1. Then each ant selects a path and moves to the next knot according to the pheromone on each path and a heuristic factor independently. This process continues till the ant reaches the terminal condition.

At time t, affected by the current pheromone and utility information, the transition probability of ant k $(k = 1, 2, ..., y)$ moving from knot i $(i = 1, 2, ..., n)$ to knot $i + 1$ via path $a[i, j]$ is:

$$p_{ij}^{k}(t) = \begin{cases} \frac{[\tau_{ij}(t)]^{\alpha} \cdot [\eta_{ij}]^{\beta}}{\sum\limits_{f \in J_k(i)} [\tau_{if}(t)]^{\alpha} \cdot [\eta_{ij}]^{\beta}}, \text{if } j \in J_k(i) \\ 0, otherwise \end{cases} \tag{3.12}$$

where $\eta_{ij} = \frac{\mathsf{u}_j}{\sum_{i=1}^{n} \mathsf{u}_i}$ is the percentage of node j's utility in the whole social network. It is a heuristic function, the expectation to transit to knot $i + 1$ from i via $a[i, j]$. The larger η_{ij} is, the more likely ant k selects node j (goes via the path $a[i, j]$). $J_k(i)$ is the set of available paths ant k can select at knot i. $J_k(i) = \{1, 2, ..., n\} - tabu_k - tabu'_k$, where $tabu_k$ is a tabu table recording all the paths ant k has gone through and $tabu'_k$ is the tabu recording all the paths selected but discarded (i.e., nodes which cannot increase the value of Eq. (3.3)). In Fig. 3.7, for paths $a[i_1, j_1]$ and $a[i_2, j_2]$, if $j_1 = j_2$, then these two paths are considered the same. Any ant k is not allowed to select the same path when moving forward, which is controlled by the tabu mechanism, as each node in the whole social network is unique. α and β are the weights of the pheromone and the heuristic function when ants select the paths. α is a pheromone heuristic factor reflecting the importance of pheromone traces when the ants are moving. β is an expectation heuristic factor representing the importance of what an ant can see [239].

The path selection process will continue till no path under the constraints of Equation (3.4) could increase the value of Equation (3.3). Then, the ant k dies.

Suppose the selected numbers in $tabu_k$ are $\{j_1, j_2, ..., j_r\}$, where r is the number of paths the ant k has passed and $\{j_1, j_2, ..., j_r\} \in \{1, 2, ..., n\}$. The whole path passed by ant k is:

$$L^k = p_{j_1} + p_{j_2} + ... + p_{j_r}. \tag{3.13}$$

The solution is the set of nodes which correspond to the paths selected by ant k.

$$X^k = \langle x_i | i = 1, ..., n \rangle, \tag{3.14}$$

where $x_i = 1$ if $j_i \in$ *tabu*$_k$.

3.6.3 Upgrade of Pheromone

When all the y ants die, y feasible solutions can be obtained. Among the y solutions, if solution k is the best in the current iteration (denoted by L'_{best}) and is better than that of all past iterations (best-so-far solution, denoted by L_{best}), then, it is used to upgrade the pheromone on the paths ant k has passed. The pheromone upgrade procedure consists of two parts: (i) the pheromone evaporation procedure and (ii) the pheromone intensification procedure. These two procedures can be formulated as:

$$\tau_{ij}(t+1) = (1-\rho) \cdot \tau_{ij}(t) + \Delta\tau_{ij} \tag{3.15}$$

$$\Delta\tau_{ij} = \sum_{k=1}^{m} \Delta\tau_{ij}^k \tag{3.16}$$

where $\rho (0 < \rho < 1)$ is a parameter called *pheromone evaporation* rate and $(1-\rho)$ is *pheromone residue* rate which prevents the unlimited accumulation of pheromone on paths; $\Delta\tau_{ij}$ is the pheromone increment on path $a[i,j]$ in current generation while $\Delta\tau_{ij}^k$ is the pheromone on the path $a[i,j]$ left by ant k. $\Delta\tau_{ij}^k$ can be formulated as:

$$\Delta\tau_{ij}^k = \begin{cases} \frac{L^k}{Q}, \text{if ant } k \text{ passes path } a[i,j] \text{ in current iteration} \\ 0, \text{otherwise} \end{cases} \tag{3.17}$$

where Q is a positive constant; L^k is the solution obtained by ant k in current iteration.

3.6.4 Mutation

In order to further refine the selected nodes for the subnetwork, a new strategy named as mutation is introduced into the ACA to enable the algorithm to delete nodes from the extracted subnetwork utilizing the node utility when needed.

The mutation process selects a node i from the extracted subnetwork L'_{best} with the probability p' which enables that the nodes with lower utility in the selected subnetwork have a higher probability to be deleted from the subnetwork.

$$p'_i = \begin{cases} \frac{1-\mathtt{u}_i}{\sum_{j\in L'_{best}}(1-\mathtt{u}_j)}, \text{if } i \in L'_{best} \\ 0, \text{otherwise} \end{cases} \tag{3.18}$$

If deleting the selected node i betters the subnetwork, node i is deleted. This process is repeated till deleting any node from the extracted subnetwork cannot improve the corresponding value of equation (3.4).

3.6.5 Algorithm

The main process of finding the subnetwork in a social network using ant colony algorithm is described in Algorithm 2. The process runs for NC_{max} times. In each iteration, the best solution is selected from y solutions obtained from the y ants to update the pheromone. Then, the next iteration starts. Finally, the best solution is returned. In addition, NF_{max} is a counter for the number of iterations where the best-so-far solution has kept the same.

The algorithm 3 implements the process of getting the paths an ant passed during its life time. The ant dies when there is no available node to better Equation (3.4) after AF_{max} times of path selections via Equation (3.12). And the paths it has passed are the solution. After obtaining a complete solution, a mutation process is conducted on the current solution to refine the final solution. MF_{max} is the maximum number of

Algorithm 2: Ant Colony Algorithm Process

```
Data: $\alpha$, $\beta$, $\rho$, $NC_{max}$, $y$, $n$, $NF_{max}$, $AF_{max}$, $MF_{max}$
Result: $L_{best}$
begin
    Initialize $NC$, $NF$, $L_{best}$, $\tau_{ij}(0)$ $(i, j = 1, 2, ..., n)$;
    //Start the iteration and look for the best solution;
    while $NC < NC_{max}$ && $NF < NF_{max}$ do
        Produce $y$ ants and put them on knot $1$;
        $NC = NC + 1$ //count the running times;
        for each ant $k(k = 1, 2, ..., y)$ do
            Get path track $L^k$ via Algorithm 3
        end
        Calculate the best solution $L'_{best}$ in current iteration;
        //Update pheromone information if a better solution is gotten;
        if $G(L'_{best}) > G(L_{best})$ then
            $L_{best} = L'_{best}$;
            Upgrade pheromone via Eq. (3.15);
        else
            $NF = NF + 1$;
        end
    end
    Return best-so-far solution $L_{best}$;
end
```

mutation processes. Finally, a subnetwork from a social network is constructed from the corresponding nodes in the final solution and the connections between them.

Summary: (i) Each step of the ACA is designed by incorporating the node utility to extract a subnetwork maximizing the objective function value in each iteration; (ii) A mutation process is introduced into the conventional ACA to overcome the drawback that there is no mechanism to remove any nodes from the extracted subnetwork; (iii) The node utility is incorporated into the path selection process by a heuristic function to increase the objective function value; (iv) A double-tabu mechanism designed in path selection process improves the performance of the solution obtained by each ant; and (v) This algorithm is capable of searching the whole solution space, which can deliver a near-optimal solution, if it exists.

Algorithm 3: The Movement of Each Ant k

```
Data: $\alpha$, $\beta$, $n$, $AF_{max}$, $MF_{max}$,
Result: $L^k$
begin
    Initialize $tabu_k$, $tabu'_k$, $AF$, $MF$;
    Set available paths $J_k$;
    //An ant begins to move;
    for each movement $i(i = 1 : n)$ do
        Select next path $j_i$ via Eq. (3.12);
        if $j_i \notin \emptyset$ && $AF < AF_{max}$ then
            if $G(tabu_k) < G(tabu_k + j_i)$ then
                $tabu_k = tabu_k + j_i$;
                $i = i + 1$;
            else
                $AF = AF + 1$;
                $tabu'_k = tabu'_k + j_i$
            end
        else
            break;
        end
    end
    //Refine the solution already gotten;
    Set available paths $J'_k = tabu_k$;
    while $J'_k \neq \emptyset$ && $MF < MF_{max}$ do
        Select path $j_k$ from $J'_k$ via Eq. (3.18);
        $MF = MF + 1$;
        if $G(tabu_k - j_k) > G(tabu_k)$ then
            $tabu_k = tabu_k - j_k$;
        else
            break;
        end
    end
    Return $L^k = tabu_k$;
end
```

Table 3.2: The results of experiment 2 at 40^{th} second

Dataset	Cases	TrustNet	BiNet	SCAN	FDRS
Epinions	Min	0.643	0.575	0.540	0.485
	Improvement	-	10.6% higher	16.0% higher	24.6% higher
	Mean	0.709	0.631	0.587	0.541
	Improvement	-	**11.0%** higher	**17.2%** higher	**23.7%** higher
	Max	0.741	0.690	0.612	0.581
	Improvement	-	6.8% higher	17.4% higher	21.6% higher
Slashdot	Min	0.579	0.529	0.503	0.513
	Improvement	-	8.6% higher	13.1% higher	11.4% higher
	Mean	0.634	0.611	0.559	0.561
	Improvement	-	**3.6%** higher	**11.8%** higher	**11.5%** higher
	Max	0.670	0.657	0.599	0.598
	Improvement	-	1.9% higher	10.6% higher	10.7% higher

3.7 Experiments on NACA

3.7.1 Experimental Setup

In this experiment, we have compared the performance of our *TrustNet* with *BiNet* and two state-of-the-art approaches SCAN [117] and FDRS [73] on the same two popular social network datasets of Epinions and Slashdot [103], and in the same environment and experimental setting as subsection 3.5.1. In addition, the parameters for *TrustNet* are $\zeta = \tilde{\zeta} = 0.5$, $\rho = 0.1$, $\alpha = \beta = 1$, $K_t = 0.5$, $NC_{max} = 400$ and $y = 20$. Similar to experiments in Subsection 3.5, the 10-time cross validation is applied for each of *TrustNet*, *BiNet*, SCAN and FDRS. In total, each model is run for 2000 times (2 datasets × 10 groups of impact factor values × 10-time cross validation × 10 source-target pairs). The average results on both datasets are plotted in Figs. 3.8-3.9 respectively.

3.7.2 Results and Analysis

Results: *TrustNet*, *BiNet* and SCAN are all iterative algorithms whose results get better as the time goes. In Figs. 3.8-3.9, we present the mean results over each group

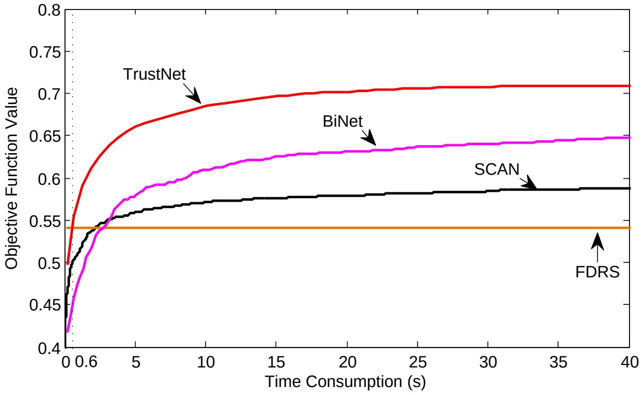


Figure 3.8: Results on Epinions dataset

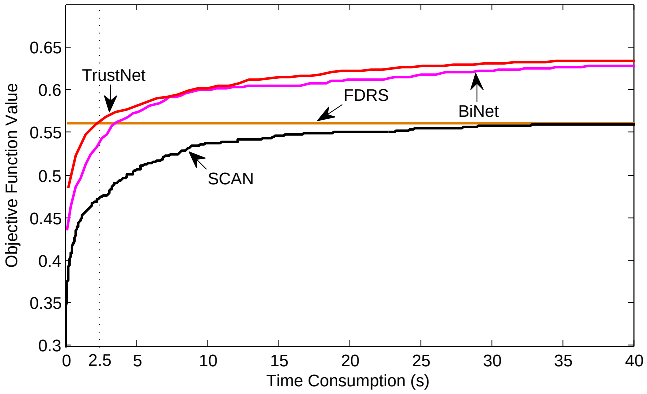


Figure 3.9: Results on Slashdot dataset

of datasets delivered within the first 40 seconds time limitation which are sufficient to demonstrate the performance of each model, as in real applications, we cannot really execute the models for such a long time. The best, mean and worst results on each group of datasets at the 40^{th} second are presented in Table 3.2. As the FDRS model is not an iterative model, it yields one fixed result on each dataset using up over 100 seconds.

Fig. 3.8 shows the average objective function values (Eq.(3.3)) of the subnetworks extracted by all the four models on the Epinions dataset within the first 40 seconds. As time goes on, the best-so-far solutions of *TrustNet*, *BiNet* and SCAN become better, while the result of FDRS keeps unchanged as it is not an iterative algorithm. Our proposed *TrustNet* outperforms all other three models after 0.6 second. At the 40^{th} second, the average objective function value of the subnetwork delivered by *TrustNet* is 11% higher than the one delivered by *BiNet*, 17.2% higher than the one delivered by SCAN, and 23.7% higher than the one delivered by FDRS.

Fig. 3.9 shows the average objective function values of the subnetworks extracted by the four models on the Slashdot dataset within the first 40 seconds. On this dataset, our *TrustNet* outperforms both *BiNet* and SCAN from the very beginning and outperforms FDRS after 2.5 seconds. At the 40^{th} second, the average result of *TrustNet* is 3.6% higher than that of *BiNet*, 11.8% higher than that of SCAN, and 11.5% higher than that of FDRS.

Analysis: Although *BiNet* has achieved significant improvement over BACA [242], our proposed *TrustNet* still outperforms *BiNet*, showing its advantages for subnetwork extraction. In summary, the result differences between our model *TrustNet* and state-of-the-art models on both datasets mainly come from the following aspects: (i) the mechanism of ant colony is capable of searching the whole solution space and deliver a near-optimal solution; (ii) the added mutation process further improves the iteration, which enables the algorithm to delete the previously selected bad nodes; (iii) the double-tabu mechanism in path selection allows an ant to try multiple times in selecting the path to go on before it dies, and thus improves the quality of the solution of each ant; (iv) both the path selection and pheromone update processes have been designed for the subnetwork extraction problem, taking the node utility into account in the form of a heuristic function; and (v) *TrustNet* is a non-binary way of applying ACA. Thus, its finial performance is not limited by initialization that does limit BACA.

3.8 Conclusion

In this chapter, we first present the social trust subnetwork extraction problem. Next, we have presented the formulation of the extraction problem, in which we have discussed the impact factors that affect the trust of a participant in another participant's opinion in online social networks and proposed a trust utility function that takes these impact factors to illustrate the attribute of each node.

Then, we have proposed two social context-aware trust subnetwork extraction models, *BiNet* and *TrustNet*, to search near-optimal solutions effectively and efficiently. In the model *BiNet*, we have proposed a novel binary ant colony algorithm in which an initialization process and a mutation process are designed and the conventional path selection and pheromone update process are improved for subnetwork extraction. The experiments, conducted on Epinions and Slashdot datasets enhanced with synthetic trust impact factor values, demonstrate that our proposed model outperforms the existing comparable heuristic methods in terms of the quality of extracted trust subnetworks. In particular, our newly-designed NBACA overcomes the disadvantages of the conventional BACA for subnetwork extraction. In the model *TrustNet*, we have proposed a new ant colony algorithm in which a mutation process is designed, and the conventional path selection and pheromone update process are improved for subnetwork extraction. The experiments, conducted on Epinions and Slashdot datasets enhanced with synthetic trust impact factor values, demonstrate that *TrustNet* outperforms the existing comparable heuristic methods and *BiNet* in terms of the quality of extracted trust subnetworks.

In addition, the proposed approaches do not rely on the paths in the online social networks, and are essential for the subsequent trust prediction process. Both of our proposed ant colony algorithms can be applied to any case where the traditional (binary) ant colony algorithm applies, but achieve significantly better performance.

Chapter 4

Single-Context Trust Prediction in OSNs

Online social networks (OSNs) have proliferated to be the platforms for a variety of rich activities, in which *trust*, the commitment to a future action based on a belief that it will lead to a good outcome [66], is one of the most critical factors for the decision-making of participants. In human society, trust depends on a host of factors such as direct interactions, opinions, motivations etc. [25]. But in OSNs, people cannot directly interact with each other, and the credibility of online information may be doubtful [168]. As a result, trust mainly depends on the past experience with a participant, profiles or descriptions, reputation etc. Many OSNs allow participants to give a trust rating to their friends or select a word from a list to describe the trust relationship between them and their friends, such as Advogato. In OSNs, a participant usually has given trust ratings to only a few of other participants. Thus, there is no direct trust existing between most of the participants in an OSN, i.e., the sparsity of the trust matrix is very high. However, it is quite common for a participant in online environments to conduct activities with another participant without any prior direct knowledge, such as online shopping, recommender systems and online recruitment. This demands effective approaches and mechanisms to predict the trust between two participants without any direct interaction.

Due to the fact that not every online social network provides contextual information, this chapter focuses on the trust prediction based on trust rating values (both literal and numerical) with matrix factorization. In addition, the dynamics of trust is not considered in this chapter, which will be introduced in Chapter 6. It is organized as follows. In Section 4.1, we discuss the drawbacks of current trust prediction models based on trust ratings, and introduce the motivation of the work in this chapter. Section 4.2 introduces the basic idea of conventional matrix factorization. Section 4.3 analyzes the properties extracted from trust ratings, which impact trust prediction, and proposes a matrix factorization-based trust prediction model. Experiments are described in Section 4.4, including datasets, measurement methods, comparisons with state-of-the-art approaches, experimental settings, experimental results and analysis. Section 4.5 summarizes our work in this chapter.

4.1 The Single-Context Trust Prediction Problem

In some online environments, where trust is given in the form of ratings without available contextual information, trust can mainly be predicted from these existing trust values (including propagated trust values) and the similarity of giving and receiving trust ratings. These two mechanisms form two groups of trust prediction approaches: propagation-based trust prediction (i.e., trust propagation/inference) and latent factor-based trust prediction depending on whether they are based on trust paths only.

Trust propagation/inference is the process of evaluating trust from a source participant to a target participant along a path between them that consists of links and trust values [69]. For example, as shown in Fig. 4.1, if participant A trusts participant B, and participant B trusts participant C, then A trusts C to some extent [66, 114]. Trust propagation has been studied in many web application areas including e-commerce [209, 236, 235], P2P systems [220], and social networks [82, 66, 119].

On the other hand, a participant tends to trust other participants who are similar to himself/herself [112]. Broadly speaking, *latent factor-based trust prediction*, such as matrix factorization, can estimate the trust between two participants from both their similarity (including similar habits, context and profiles) as well as propagated trust,

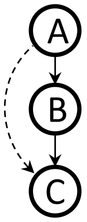


Figure 4.1: Trust propagation

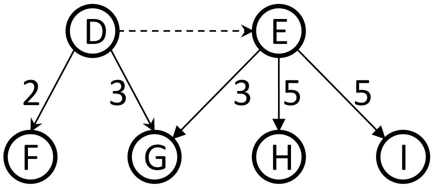


Figure 4.2: Trust ratings

by modeling the similarity of participants in a social network in a latent factor space.

In the application of predicting trust from trust ratings, similarity is calculated from two participants' common trust rating values given to others [131]. Such similarity is termed as *trust rating value similarity* in this chapter. In the meantime, it should be noted that similarity can also be calculated from two participants' distributions of trust ratings, which is termed as *trust rating distribution similarity*. Zheng et al. [241] have shown that the distribution of participants' trust ratings is an important property that influences the trust between the source participant and the target participant. Therefore, it is essential to take advantage of distribution to further boost trust prediction accuracy. For example, as shown in Fig. 4.2, the trust values given to G by D and E are the same. However, they come from two different distributions showing that even the same trust value given to G could be different in the minds of D and E — the trust value 3 is the higher value participant D has given, while it is the lower one in E's ratings.

Propagated trust and the two types of similarities are interpersonal properties. They influence the trust between two participants. By contrast, *trust tendency* (also termed as *trust bias* in [224, 226]) is a type of properties extracted from all the trust ratings that one participant gave or received, showing his/her dispositional tendency to trust others or to be trusted by others on average (termed as *truster tendency* and *trustee tendency* respectively) [224, 226]. Trust tendency is regarded as a very important concept in social science, and it is recognized as an integral part of the final trust decision [196]. For instance, some participants tend to give relatively high trust ratings more generously than others, while some participants receive higher trust ratings compared with others.

The details of trust tendency will be presented in Section 4.3.

In summary, to predict trust values from trust ratings without available contextual information, the existing works predict trust either via trust propagation only [69, 66, 114, 206], or considering propagated trust and tendency [225, 226], or merely utilizing the similarity of rating values [131, 132]. In addition, the way in which the influential properties are used needs to be improved as well. On one hand, personal properties such as tendencies are decomposed from every single participant's ratings and influence the participant's global ratings; on the other hand, interpersonal properties such as similarity and propagated trust are extracted from two participants' trust ratings to reflect the features between them. Therefore, the two types of properties should be treated differently in order to improve trust prediction accuracy.

In general, they have the following drawbacks needing to be overcome.

1. All the tendency, propagated trust and similarity influence the trust between two participants, all of which should be utilized to predict pair-wise trust, rather than considering only one or two influential properties.

2. The similarity of trust rating distributions describes the similarity of participants' behaviors in giving trust ratings, which has been neglected in the literature.

3. The two different types of properties are not processed separately and differently, which affects the accuracy of trust prediction.

4.2 Basic Matrix Factorization

In this section, we present the basic matrix factorization method from the viewpoint of trust prediction. Matrix factorization is an efficient and effective approach in recommender systems, which factorizes the user-item rating matrix into user-specific and item-specific matrices, and predicts missing data based on both matrices [131, 173, 174]. In the application of trust prediction, trustees are regarded as the "items" in recommender systems [225]. Thus, matrix factorization methods factorize the trust ratings matrix into truster-specific and trustee-specific matrices respectively.

We consider an $n \times n$ trust rating matrix R describing n trusters' numerical ratings on n trustees. The matrix factorization models map both trusters and trustees to a joint latent factor space of dimensionality l, so that truster-trustee trust ratings are modeled as inner products in that space. Accordingly, each truster i is associated with a vector $u_i \in \mathbb{R}^l$, while each trustee is associated with a vector $v_j \in \mathbb{R}^l$. Finally, all the vectors $\{u_i\}$ constitute the truster-specific matrix U indicating to what extent the corresponding participants trust others w.r.t. the specific latent factors. Meanwhile, vectors $\{v_j\}$ compose the trustee-specific matrix V indicating to what extent the corresponding participants are trusted by others w.r.t. the specific latent factors. So, the rating matrix R is factorized as a multiplication of l-rank factors,

$$R \approx U^T V, \tag{4.1}$$

where $U \in \mathbb{R}^{l \times n}$ and $V \in \mathbb{R}^{l \times n}$ with $l < n$. Once the factorization is completed, the missing ratings could be calculated from

$$r_{i,j} \approx u_i^T v_j. \tag{4.2}$$

Note that participant u_i and participant v_i are the same participant with two different roles—truster and trustee respectively. The factorization is achieved by minimizing the equation:

$$\frac{1}{2}||R - U^T V||_F^2, \tag{4.3}$$

where $||.||_F^2$ represents the Frobenius norm. Note that each participant only gives trust ratings to a few other participants. Hence, the matrix R contains a large amount of missing values as an extremely sparse matrix. Therefore, Eq. (4.3) is changed to

$$\min_{U,V} \frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} I_{ij}(r_{ij} - u_i^T v_j)^2, \tag{4.4}$$

where I_{ij} is an indicator function. $I_{ij} = 1$ *iff.* participant i (truster) rated participant j (trustee) , $i \neq j$. Otherwise, $I_{ij} = 0$. In order to avoid overfitting, two regularization terms from zero-mean spherical Gaussian priors [174] are placed into Eq. (4.2). Hence, we have

$$\min_{U,V} \frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} I_{ij}(r_{ij} - u_i^T v_j)^2 + \frac{\lambda_1}{2}||U||^2 + \frac{\lambda_2}{2}||V||^2, \tag{4.5}$$

where $\lambda_1 > 0$ and $\lambda_2 > 0$. Thus, the learning process of the method can be achieved by Eq. (4.5) using the gradient descent method [96].

4.3 The Proposed Trust Prediction Approach

In this section, we first discuss the properties influencing trust between participants in detail. Then we propose a novel method to incorporate these influential properties into a regularization in matrix factorization to improve trust prediction accuracy.

4.3.1 Properties that Influence Trust

In real life, trust is influenced by many properties, including trust tendency, propagated trust, value similarity, and distribution similarity [66, 131, 117, 81, 226, 237].

Trust Tendency: When rating others in trust, some participants give relatively higher trust ratings than others, showing different tendencies. On the other hand, some participants receive higher trust ratings than others, meaning that they are more likely to be trusted. So, there are two types of tendencies in trust ratings: *truster tendency* $T_u(i)$ and *trustee tendency* $T_v(i)$. Truster tendency can be considered as a personal property that implies a participant's average dispositional tendency to trust others. It can be calculated as the average of all the trust ratings a participant i gives to others [225]. On the other hand, trustee tendency can be treated as another personal property that shows a participant's tendency to be trusted. It can be calculated as the average of all the ratings a participant j has received [225]. $\hat{r}_{ij}$ is the trust ratings adjusted by both tendencies above termed as *tendency-reduced ratings* in the thesis.

Therefore, each trust rating r_{ij} can be decomposed as $r_{ij} = \alpha_1 T_u(i) + \alpha_2 T_v(j) + \alpha_3 \hat{r}_{ij}$, where, α's are the coefficients. Only $\hat{r}_{ij}$ is used for matrix factorization. Thus, the negative effect of trust tendency can be reduced.

Propagated Trust: It is concluded in social network studies that people can trust a stranger to some extent if the person is a friend's friend [69]. Thus, many trust propagation methods infer trust along a path between two participants without direct connections [66, 119]. Here, we adopt the propagation method introduced in [119, 110] to select the path with the highest propagated trust value $\mathit{infer}(i,j)$ between participant i and participant j by multiplication within H hops. If no path is available within H hops, we set $\mathit{infer}(i,j) = 0$. Here, $\mathit{infer}(i,j) \neq \mathit{infer}(j,i)$ in most circumstances because when participant i trusts participant j with a certain trust value, it does not mean participant j trusts participant i to the same extent.

Trust Rating Value Similarity: Conventionally, with the rating information of all the participants, the trust rating value similarity of two participants can be calculated from the common trust ratings that the two participants give to others [81]. The most prevalent approaches of this similarity evaluation are Vector Space Similarity (VSS) and Pearson Correlation Coefficient (PCC) [32]. VSS calculates the similarity from ratings of common trustees that participant i and participant j have rated respectively:

$$vss(i,j) = \frac{\sum\limits_{f \in I(i) \bigcap I(j)} r_{if} \cdot r_{jf}}{\sqrt{\sum\limits_{f \in I(i) \bigcap I(j)} r_{if}^2} \cdot \sqrt{\sum\limits_{f \in I(i) \bigcap I(j)} r_{jf}^2}}, \tag{4.6}$$

where participant f belongs to the subset of trustees that participant i and participant j both have rated. r_{if} and r_{jf} are the trust ratings participant i and participant j give to participant (trustee) f.

On the other hand, PCC takes into account the rating styles that some participants would like give relatively higher ratings to all the others while some may not. Hence, PCC adds a mean of ratings as follows:

$$pcc(i,j) = \frac{\sum\limits_{f \in I(i) \bigcap I(j)} (r_{if} - \overline{r}_i) \cdot (r_{jf} - \overline{r}_j)}{\sqrt{\sum\limits_{f \in I(i) \bigcap I(j)} (r_{if} - \overline{r}_i)^2} \cdot \sqrt{\sum\limits_{f \in I(i) \bigcap I(j)} (r_{jf} - \overline{r}_j)^2}}, \tag{4.7}$$

where $\overline{r}_i$ and $\overline{r}_j$ represent the average rates of participant i and participant j respectively. In addition, the range of the PCC is $[-1, 1]$. Thus, PCC is normalized into $[0, 1]$ in applications by $\mathfrak{q}(x) = (\mathfrak{p}(x) + 1)/2$ [131].

Trust Rating Distribution Similarity: The distribution of a participant's ratings reveals the participant's rating habits. For example, a participant gives diverse ratings with equal probability (Uniform distribution) while another participant prefers giving a certain trust rating value with a high probability (Gaussian distribution). The same trust value from these two distributions should be treated differently. Kullback-Leibler (KL) -distance (Relative Entropy) is a natural distance function from one participant's distribution of ratings to the other's [92]. It can depict the difference in trust rating distributions between two participants. For discrete probability distributions, the KL-distance is formulated as follows:

$$D_{KL}(i||j) = \sum_k \ln(\frac{P_i(k)}{P_j(k)}) P_i(k), \tag{4.8}$$

where $k \in K$ is the space of all the trust ratings that participant i has given; P_i and P_j are the trust rating distributions of participants i and j. As the range of KL-distance is $[0, \infty]$, we use the projection function $q(x) = e^{-p(x)}$ to convert the range to $[0, 1]$, where, after conversion, 1 means the two distributions are exactly the same while 0 means they are different.

Different from trust tendency, the last three properties have the same characteristics that they influence the trust between two participants and have the same value range and trend (after conversion). The weighted sum of interpersonal trust properties between participant i and participant j is termed as *trust property utility*, which can be formulated as:

$$TP(i,j) = \beta_1 infer(i,j) + \beta_2 pcc(i,j) + \beta_3 D_{KL}(i||j) \tag{4.9}$$

where β's are coefficients.

4.3.2 The Modified Matrix Factorization

As mentioned above, studies in social science have pointed out that people would like to seek suggestions from friends in the real world. They adopt suggestions according to the trust levels of friends which are influenced by interpersonal trust properties [24]. Hence, different from existing works, we propose a propagation and similarity regularization term to impose constraints between truster i and trustee f to minimize the distances between participant-specific vectors u_i and u_f. It is formulated as:

$$\frac{\gamma}{2}\sum_{i=1}^{n}\sum_{f\in\mathcal{F}^+(i)} TP(i,f)||u_i - u_f||_F^2, \tag{4.10}$$

where $\gamma > 0$, $\mathcal{F}^+(i)$ is the set of trustees who, at least, have a trust path connected from truster i. $TP(i,f)$ is the trust property utility in Eq. (4.9). If a trustee $f \in \mathcal{F}^+(i)$ of participant i has a very similar habit to i and a high trust value propagated from participant i, then the value of $TP(i,f)$ will be close to 1, otherwise it is close to 0. Furthermore, a small value of $TP(i,f)$ means that the distance between participant-specific vectors u_i to u_f should be large, while a large value of $TP(i,f)$ indicates the distance should be small. Thus, the trust property utility $TP(i,j)$ enables the matrix factorization method to incorporate the different similarities and propagated trust between participant i and his/her truster or trustee. Finally, our trust prediction model can be formulated as:

$$\begin{aligned}\min_{U,V}\mathcal{L}(R,U,V) =& \min_{U,V}\frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n}I_{ij}(\hat{r}_{ij}-u_i^T v_j)^2\\ &+\frac{\lambda_1}{2}||U||^2+\frac{\lambda_2}{2}||V||^2\\ &+\frac{\gamma}{2}\sum_{i=1}^{n}\sum_{f\in\mathcal{F}^+(i)}TP(i,f)||u_i-u_f||_F^2.\end{aligned} \tag{4.11}$$

In our model, $TP(i,j) \neq TP(j,i)$ in most cases, because trust propagation and KL-distance are asymmetric ($\mathit{infer}(i,j) \neq \mathit{infer}(j,i)$ and $D_{KL}(i||j) \neq D_{KL}(j||i)$) in most circumstances, indicating that "participant i trusts participant j" does not mean "participant j trusts participant i to the same extent".

This method improves the accuracy of trust prediction and propagates participants' trust ratings indirectly. In details, if participant i rates participant f and participant f rates participant g (suppose participant i does not rate participant g), the distances between feature vectors u_i and u_g is minimized when we minimize $TP(i,f)||u_i - u_f||_F^2$ and $TP(f,g)||u_f - u_g||_F^2$.

A local minimum value of the objective function (4.11) can be obtained using gradient descent methods in latent factors of u_i and v_i:

$$\begin{aligned}\frac{\partial\mathcal{L}}{\partial u_i} =& -\sum_{j=1}^{n}I_{ij}(\hat{r}_{ij}-u_i^T v_j)v_j+\lambda_1 u_i\\ &+\gamma\sum_{f\in\mathcal{F}^+(i)}TP(i,f)(u_i-u_f)\\ &+\gamma\sum_{g\in\mathcal{F}^-(i)}TP(g,i)(u_i-u_g),\end{aligned} \tag{4.12}$$

$$\frac{\partial\mathcal{L}}{\partial v_i} = -\sum_{i=1}^{n}I_{ij}(\hat{r}_{ij}-u_i^T v_j)u_j+\lambda_2 v_i. \tag{4.13}$$

where $\mathcal{F}^-(i)$ is a set of trusters, each of whom, at least, has a trust path to trustee i.

4.4 Experiments

In this section, we present and analyze the results of the experiments we have conducted on a real-world dataset to illustrate the trust prediction accuracy of our method in comparison with state-of-the-art approaches.

4.4.1 Dataset Description

The dataset Advogato[1] used in our experiments is obtained from a trust-based social network. The network collects trust data between participants and refreshes the dataset regularly. We adopt the dataset released on September 10th, 2013, which contains 7,425 participants. In the dataset, there are 56,535 trust ratings given by 6,633 trusters to 7,041 trustees, out of which 51,400 are pair-wise ratings and 5,135 are self-ratings. This paper aims to predict pair-wise ratings, and thus self-ratings are ignored. Trust ratings in this dataset are divided into 4 levels which are 'Observer', 'Apprentice', 'Journeyer' and 'Master' in ascending order. 'Observer' is the lowest trust level while 'Master' is the highest trust level. In our experiments, we map the trust levels of 'Observer', 'Apprentice', 'Journeyer' and 'Master' to 0.1, 0.4, 0.7 and 1 respectively.

4.4.2 Measures

In the area of prediction and recommendation, both the Mean Absolute Error (*MAE*) and the Root Mean Square Error (*RMSE*) are the most common metrics used to measure the prediction accuracy of a model [224, 226]. Thus, we adopt them to compare the prediction accuracy of our proposed approach with the related state-of-the-art approaches. The metric *MAE* is formulated as:

$$MAE = \frac{1}{T} \sum_{i,j} |r_{ij} - \tilde{r}_{ij}|, \tag{4.14}$$

[1] http://www.trustlet.org/wiki/advogato_dataset.

where r_{ij} denotes the actual trust ratings participant i gives to participant j. $\tilde{r}_{ij}$ represents the predicted trust ratings that participant i will give to participant j. T denotes the total number of trust ratings in the validation dataset. *MAE* weights the individual differences equally as a linear score.

The metric *RMSE* is defined as:

$$RMSE = \sqrt{\frac{1}{T}\sum_{i,j}(r_{ij} - \tilde{r}_{ij})^2}. \tag{4.15}$$

RMSE gives higher weights to larger errors as the errors are squared before taking their average. It is always larger or equal to the *MAE*. Both *MAE* and *RMSE* are usually used together to diagnose the variation in the errors of prediction. Lower values of *MAE* and *RMSE* mean better accuracy.

4.4.3 Comparisons

In order to evaluate the prediction accuracy of our approach, we compare it with the state-of-the-art promising approaches—an trust inference model (MATRI) [225] and matrix factorization with social regularization (MFISR) [132].

MATRI: This approach [225, 226] considers trust tendency and propagated trust to predict missing trust ratings, which treats trust tendency and propagated trust as some of the latent factors when conducting matrix factorization, while other latent factors in matrix factorization are kept unchanged.

MFISR: This approach [132] adds social regularization into conventional matrix factorization by introducing average-based and individual-based social regularization terms separately. In addition, matrix factorization with individual-based social regularization (MFISR) was proved to be more effective and accurate than that with average-based regularization. Therefore, in our experiments, we compare our method with MFISR.

The comparisons of the three models are conducted in the metrics of MAE and

RMSE on the same dataset of Advogato, respectively, where the smaller values of MAE and RMSE demonstrate better accuracy of trust prediction.

4.4.4 Experimental Settings

In our model, the coefficients α's and β's determine the weight of each property that influences the trust between two participants. They are essential to the trust prediction accuracy. In order to obtain the best coefficients, we treat each coefficient as a 'gene' and construct a 'chromosome' containing all the six coefficients of α's and β's. The prediction result from our modified matrix factorization is used as a fitness function. Thus, the real-valued Genetic Algorithm [148] has been used to determine the best weight for each trust property. To make comparison fair, this method is also used for both MATRI and MFISR to determine their coefficients on the same training dataset.

In total, we have conducted three groups of experiments with different percentages (80%, 60% and 40%) of the data for training. 10 groups of randomly generated initial matrices are used to initialize each model. In all of the three approaches, we use the same gradient descent method for the matrix factorization process and set $\lambda_1 = \lambda_2 = 0.01$,$\gamma = 0.1$, $H = 2$ and $l = 10$.

Setting of parameters γ and λ: γ and λ's are very important. γ controls to what extent propagation and similarity regularization should be incorporated, while λ's manage to what extent Gaussian priors should be incorporated. Figs. 4.3 and 4.4 show the impacts of γ, from which we can see no matter which training data setting is used, *MAE* and *RMSE* decrease when γ increases. But *MAE* and *RMSE* start to increase when γ is less than a certain threshold such as 0.1. Therefore, setting $\gamma = 0.1$ is proper. As the impact of λ's shares the same trend as γ in terms of both *MAE* and *RMSE*, the same method is used to determine $\lambda_1 = \lambda_2 = 0.01$.

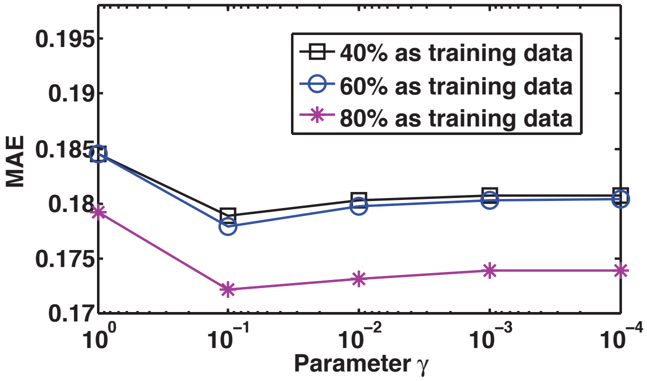


Figure 4.3: MAE

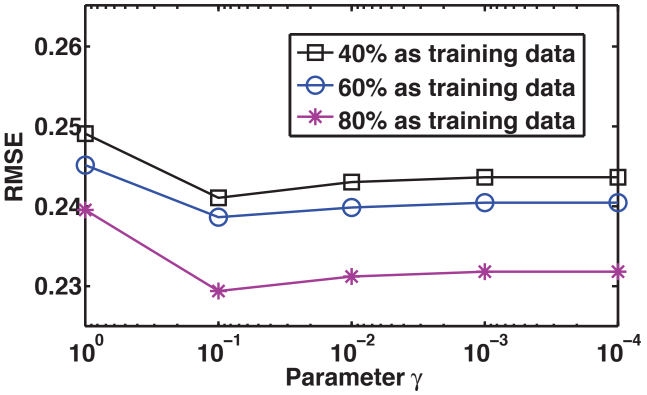


Figure 4.4: RMSE

4.4.5 Experimental Results and Analysis

For model validation, we have conducted repeated random sub-sampling for 10 times in each experiment. Finally, each model is experimented with 300 times (3 different percentages × 10 different initial matrices × 10 times cross validations). The experimental results, in the best, average and worst initialization cases, are shown in Table 4.1.

From the results of the three groups of experiments, we can see that in the best initialization cases, our model improves over MATRI by 11.4%–13.6% in terms of *MAE* and by 21.8%–24.0% in terms of *RMSE*. In the worst initialization cases, the improvements increase to 45.3%–46.4% in terms of *MAE* and 39.6%–41.4% in terms

Table 4.1: Experiment results

Training%	Cases	Metrics	Ours	MATRI	MFISR
80%	Best	*MAE*	**0.1717**	0.1938	0.4006
		RMSE	**0.2284**	0.3004	0.4856
	Average	*MAE*	**0.1802**	0.3091	0.3711
		RMSE	**0.2404**	0.3875	0.4561
	Worst	*MAE*	**0.1883**	0.3514	0.4476
		RMSE	**0.2474**	0.4222	0.5268
60%	Best	*MAE*	**0.1734**	0.1970	0.3578
		RMSE	**0.2362**	0.3022	0.4418
	Average	*MAE*	**0.1804**	0.3109	0.3774
		RMSE	**0.2413**	0.3889	0.4611
	Worst	*MAE*	**0.1862**	0.3476	0.3998
		RMSE	**0.2471**	0.4190	0.4827
40%	Best	*MAE*	**0.1792**	0.2073	0.3516
		RMSE	**0.2389**	0.3099	0.4517
	Average	*MAE*	**0.1821**	0.3165	0.3813
		RMSE	**0.2431**	0.3930	0.4643
	Worst	*MAE*	**0.1855**	0.3392	0.3924
		RMSE	**0.2481**	0.4111	0.4749

of *RMSE*. This result means that our model has better robustness. In other words, it not only performs well with the best initialization but also overcomes the worst initialization situations with slightly lower accuracy. In addition, our model improves MFISR by 49.0%–57.9% in terms of *MAE* and by 46.5%–53% in terms of *RMSE* in all initialization cases.

Summary: The experimental results have demonstrated that our model significantly outperforms the state-of-the-art models in trust prediction accuracy. This is due to the following reasons. *First*, in our model, both personal trust properties and interpersonal trust properties are comprehensively taken into account. *Second*, personal trust properties (i.e., tendencies) are utilized to produce tendency-reduced trust ratings, based on which, the negative effect of trust tendency is reduced. *Third*, different from personal properties, the weighted sum of all interpersonal trust properties becomes part of regularization in matrix factorization. That means propagated trust, trust rating value similarity and rating distribution similarity are all incorporated in trust prediction.

4.5 Conclusion

In this chapter, we have proposed a method of trust decomposition and a new matrix factorization-based trust prediction model with our trust regularization term. First, we have analyzed the properties of trust that can be extracted from existing trust rating values, and that can be leveraged to predict missing trust rating values. Then, these properties have been further divided into personal properties and interpersonal properties, and utilized respectively in different ways. Different from the existing approaches, the personal properties (i.e., trust tendencies) are used to decompose trust ratings into truster tendency, trustee tendency and tendency-reduced trust ratings, which can reduce the effect of trust tendency. The interpersonal properties (i.e., propagated trust and similarities) are incorporated into a propagation and similarity regularization term. In this regularization term, in addition to propagated trust, both the similarity of trust rating distributions and the similarity of trust rating values are included to further differentiate the trust between participants and optimize matrix factorization. Next, based on both rating decomposition and matrix factorization, we have proposed a new trust prediction model by adding such a regularization term to control the distance between participants in the latent factor space of matrix factorization. In particular, an important feature of our approach is that we do not impose any limitation on latent factors of matrix factorization. Finally, the experiments conducted on a real-world dataset have demonstrated significant improvements delivered by our model in trust prediction accuracy over the state-of-the-art approaches using the metrics of RMSE and MAE.

Chapter 5

Social Context-Aware Trust Prediction in OSNs

In Chapter 4, we have introduced the proposed matrix factorization-based approach to trust prediction from trust ratings without taking contextual information into account. This chapter will focus on context-aware trust prediction, as most recent OSNs contain contextual information of interactions, which can be mined by applying data mining techniques [141, 193]. In addition, context dependency is a basic property of trust, as described in Subsection 2.2.2.4, and it is rare for a person to have full trust on another in all aspects [189, 180]. For example, the case of full trust in all aspects is less than 1% at Epinions.com and Ciao.co.uk, both of which are popular product review websites [189]. In real life, one's trust to another is limited to certain domains. Therefore, contextual information is critical for accurate trust prediction. And utilizing social network information to infer or predict trust among people to recommend services from trustworthy providers has drawn growing attention, especially in online environments.

This chapter is organized as follows. We first describe the trust prediction based on contextual information in Section 5.1. Then, the personal properties and interpersonal properties of social context which impact trust transference between contexts are analyzed in Section 5.2. Next, in Section 5.3 a new trust transference method is proposed to predict the trust in a target context from that in different but relevant contexts. In addition, a social context-aware trust prediction model based on matrix factorization is proposed to predict trust in various situations no matter whether there is a path from a source participant to a target participant. To the best of our knowledge, this is the first context-aware trust prediction model in social networks in the literature. Finally, Section 5.4 presents the experiments and the experimental analysis illustrating that the proposed model can mitigate the sparsity situation in social networks and generate more reasonable trust results than the most recent state-of-the-art context-aware trust inference approach. Section 5.5 gives a summary of the work in this chapter.

5.1 The Trust Prediction Problem in Contextual Social Networks

Trust prediction is the process of estimating a new pair-wise trust relationship between two participants regarding a specific context, who are not directly connected by interactions in the context [243]. As described in Subsection 2.2.2.4, trust is context dependent. For example, A trusts B in teaching Visual C++ because B taught A C++ very well. In this situation, A can trust B in the context of teaching Java to some extent, because Java is a similar programming language as C++. This example indicates that trust can be transferred between relevant contexts to some extent.

As introduced in Section 2.4, recently, some studies have suggested taking into account some kind of social contextual information in trust propagation, which relies on trust paths and ignores participants not on the path. In addition, latent factor-based prediction methods also begin to incorporate some social contextual information. Furthermore, Wang et al. [206] point out that social context should contain any information to reflect an individual's social characteristics and the social relationship with other people within a social network.

However, most existing trust prediction models suffer from the following drawbacks: (i) The property of trust values has not been studied sufficiently. For example, the similarity of people's trust can be modeled not only from the trust values but also from their distributions [241]; (ii) The diversity of social contexts is not well dealt with. In real life, the connection between two people can be friendship, family member, business partnership, or classmate etc. Even within the same relationship, such as classmate, the interaction frequency and interaction context can be largely different [206]; (iii) The ways to incorporate social information require further study, as inappropriate introduction of social information may introduce noise and degrade the trust prediction quality [122]; (iv) The differences of contextual information are not handled properly. For example, how to model the relationship of two contexts? To what extent, the trust in context c_i can be transferred to context c_j?

Therefore, in order to address the above drawbacks, a new social context-aware trust prediction model is needed between a recommender and a recommendee.

5.2 Contextual Social Networks

In this section, we first introduce a social network structure containing important social contextual impact factors. Then, a trust matrix is constructed based on these impact factors in the social network, providing data for trust prediction.

Context is a multi-faceted concept across different research disciplines with various definitions [180]. In this chapter, we define *context* as any information available for characterizing the participants and the situations of interactions between them. Furthermore, we adopt the terminology used in [206]. If participant p_1 has an interaction with participant p_2, the context about p_1 and p_2 in the social society is referred to as the *social context*, among which the *interaction context* refers to any information about the interaction including time, place, type of services etc. If p_2 recommends a service to p_1, then the information about the service is referred to the *target context*.

5.2.1 Social Context

Social context describes the context about participants. Before it can be used to describe trust of participants, the properties of each aspect must be extracted modeling the characteristics of participants and the relationship between them. Therefore, social context can be divided into two groups according to the characteristics of each impact factor: *personal properties* (e.g., role impact factor, reliability and preference) and *interpersonal properties* (e.g., preference similarity, social intimacy and trust).

Role Impact Factor: Role impact factor has a significant influence on the trust between participants in a society [123]. It illustrates the impact of a participant's social position and expertise on his/her trustworthiness when making recommendations based on that the recommendation from a person who has expertise in a domain is more credible than others with less knowledge about the domain. Let $RIF_{p_k}^{c_i} \in [0,1]$ denote the participant p_k's role impact factor in context c_i, where $RIF_{p_k}^{c_i} = 1$ means p_k is an expert regarding context c_i while $RIF_{p_k}^{c_i} = 0$ indicates that p_k has no idea of context c_i. Therefore, higher $RIF_{p_k}^{c_i}$ would mean more influence when giving recommendations to others in context c_i.

There are various ways to calculate the role impact factor in different domains. For example, the social position between email users is discovered by mining the subjects and contents of emails in Enron Corporation[1] [91]. Using large databases such as DBLP[2] and ACM Digital Library[3], the role impact factor values of scholars can be calculated by some approaches, such as the PageRank model [193].

Recommendation Reliability: In a certain context, the reliability of recommendations measures the rate of a participant's recommendations accepted by recommendees [81]. Let $RLB_{p_k}^{c_i} \in [0,1]$ denote the participant p_k's reliability in context c_i, where $RLB_{p_k}^{c_i} = 1$ means that each of p_k's historical recommendations in context c_i has been accepted by the recommendee, while $RLB_{p_k}^{c_i} = 0$ indicates that p_k has had no recommendation accepted in context c_i in the past. Therefore, a higher $RLB_{p_k}^{c_i}$ indicates more influence when making recommendations to others in context c_i.

There are many different ways to measure the reliability values. For example, on

[1] http://www.cs.cmu.edu/∼enron/

[2] http://www.informatik.uni-trier.de/ ley/db/

[3] http://portal.acm.org/

the dataset MovieLens[4], the leave-one-out approach is used in [81] to calculate the deviation between the predicted rating and the actual ratings as the reliability of a participant.

Preference: Preference is an individual's attitude or affinity towards a set of objects in a decision making process [111]. This property may differ greatly between different contexts in real life. The similarity of two participants' preferences can impact the trust between them to some extent [206]. Let $PS^{c_i}_{p_x,p_y} \in [0,1]$ denote the preference similarity between participants p_x and p_y in context c_i. $PS^{c_i}_{p_x,p_y} = 1$ means that p_x and p_y have the same preference in context c_i, while $PS^{c_i}_{p_x,p_y} = 0$ indicates that there is no common preference in the interaction context c_i. Higher $PS^{c_i}_{p_x,p_y}$ means a high degree of similarity between p_x and p_y regarding context c_i and leads to higher trust between them in the same context. Here, $PS^{c_i}_{p_x,p_y} = PS^{c_i}_{p_y,p_x}$.

Since preferences are stored in users' profiles in some online social networks, such as Facebook[5], the similarity between users can then be mined [206]. In addition, on some e-commerce websites, the similarity can be calculated from the rating values given by users using models such as PCC and VSS [131]. Besides, this similarity can also be complemented from the distribution of these ratings [243].

Social Intimacy: Social intimacy refers to the frequency of connections between participants in a social network. The degree of social intimacy can impact trust as people tend to trust those with more intimate social relationships [33]. Let $SI^{c_i}_{p_x,p_y} \in [0,1]$ denote the social intimacy between participants p_x and p_y in context c_i in p_x's mind, where $SI^{c_i}_{p_x,p_y} = 1$ means, among the group of participants who have a social relationship with p_x, p_y has the most intimate relationship with p_x in context c_i, while $SI^{c_i}_{p_x,p_y} = 0$ indicates that p_y has the least intimate social relationship with p_x. Here, $SI^{c_i}_{p_x,p_y}$ is not equivalent to $SI^{c_i}_{p_y,p_x}$. For example, p_x interacts with all of his/her friends, including p_y, regularly (with equal frequency). On the contrary, p_y only interacts with p_x regularly among his/her friends. In this situation, between p_x and p_y, the social

[4] http://movielens.sumn.edu/
[5] http://www.facebook.com/

intimacy degree in p_y's mind must be larger than that in p_x's mind, i.e., $SI^{c_i}_{p_y,p_x} > SI^{c_i}_{p_x,p_y}$.

In the literature, there are many available approaches to the computation of the social intimacy degree. For example, in the Enron Corporation case, the intimacy degree can be extracted from pairs of emails between senders and receivers [91]. The coauthor relationship in DPLB or ACM Digital Library can be used to figure out the social intimacy between authors. Using these databases, models like PageRank [193], are able to calculate the social intimacy degree values.

Existing Trust: Trust is a belief that an entity, such as a person or an organization, will behave in an expected manner, despite the lack of ability to monitor or control the environment in which it operates [180]. It can be impacted by all the above properties and the trust value can be greatly different between the same two participants in different interaction contexts [212]. Let $T^{c_i}_{p_x,p_y} \in [0,1]$ denote the trust p_x gives to p_y in context c_i, where $T^{c_i}_{p_x,p_y} = 1$ means participant p_x fully trusts participant p_y on any recommendation in context c_i, while $T^{c_i}_{p_x,p_y} = 0$ indicates that p_x does not trust p_y at all in context c_i. Higher $T^{c_i}_{p_x,p_y}$ indicates more trust to p_y in p_x's mind. Here, trust between two participants in a given context is not symmetrical, so $T^{c_i}_{p_x,p_y}$ may not be equivalent to $T^{c_i}_{p_y,p_x}$.

5.2.2 Social Context Similarity

Interaction context is the information about the situation when the interaction happens between participants p_1 and p_2. For example, suppose that p_2 has recommended mobile phones to p_1 many times in the past. As a result, p_1 trusts p_2 with the value $T^{c_i}_{p_1,p_2} = 0.8$ in the context of mobile phones. Now p_2 recommends p_1 a laptop. As there is no historical recommendation in the context of laptops, and there does exist similarity between the contexts of mobile phones and laptops, we need to calculate the context similarity in order to determine how much p_1 can trust p_2 in the target context of recommending laptops. Let $CS^{c_i,c_j} \in [0,1]$ denote the similarity between two contexts c_i and c_j. Only when c_i and c_j are exactly the same context, $CS^{c_i,c_j} = 1$. And $CS^{c_i,c_j} = 0$ indicates that the information in context c_i is not relevant to c_j at all and cannot impact participants' trust in context c_j. Here, $CS^{c_i,c_j} = CS^{c_j,c_i}$. We adopt the classification of contexts introduced in [206] with a number of existing methods to compute similarity [234, 206], such as linear discriminant analysis and context hierarchy-based similarity calculation. In addition, the interaction context c_j is relevant to the interaction context c_i if $CS^{c_i,c_j} > \mu$ (μ is a threshold, e.g., 0.7), denoted as $c_i \sim c_j$. Otherwise, if c_j is irrelevant to c_i, denoted as $c_i \nsim c_j$.

5.2.3 Contextual Presentation of Trust

In order to apply our prediction model on the trust information in different contexts, we present a contextual trust matrix to represent the contextual information and social properties. Fig. 5.1 shows a social network graph in a context c_i, in which the arrows between nodes mean the existing trust resulting from past interactions. In context c_i, we construct a $N_p \times N_p$ matrix R, where N_p is the number of participants. In this 2-dimensional matrix, if we put the trust value between participants at each context, the structure can be shown as in Fig. 5.2.

The contextual social network graph is shown in Fig. 5.3 with the trust links in all contexts, where the superscript c_i, $i = 1...5$ indicates the context in which the trust exists. Once taking all contexts into consideration, the matrix R turns into a $N_p \times N_p \times N_c$ cube as shown in Fig. 5.4, where, N_c is the number of contexts.

In Fig. 5.2 and Fig. 5.4, only the trust values are shown in the matrix. Actually, each element in the matrix is a social property vector containing all the relative properties discussed in detail in this section.

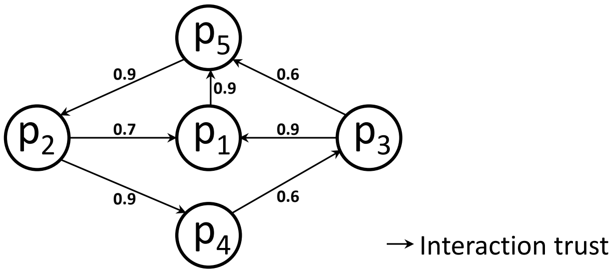


Figure 5.1: Social network graph in a context

	p_1	p_2	p_3	p_4	p_5
p_1					**0.9**
p_2	**0.7**			**0.9**	
p_3	**0.9**				**0.6**
p_4			**0.6**		
p_5		**0.9**			

Figure 5.2: Trust matrix in a context

5.3 The Proposed Contextual Trust Prediction Model

The process to predict the trust between participants p_x and p_y in the target context of c_j can be divided into two situations based on available information. They are discussed in the following subsections.

5.3.1 Trust Transference between Contexts

In the example described in Section 5.1, A's trust to B in the context of teaching C++ can be transferred to the context of teaching Java because Java and C++ are similar programming languages, which means that trust can be transferred between relevant contexts. In this subsection, we discuss trust transference for the prediction of the trust between two participants p_x and p_y when they have no prior interactions in the target context but have many interactions in relevant interaction contexts between each other. Conceptually, *trust transference* is the process to evaluate trust from that in

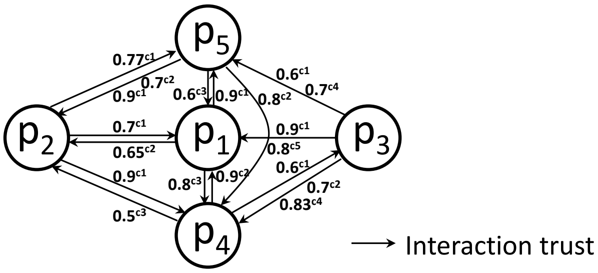
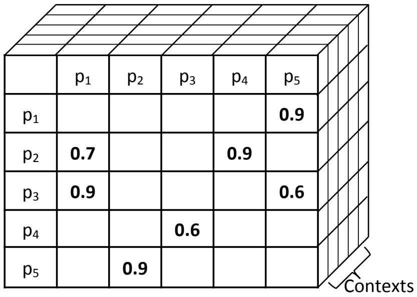


Figure 5.3: Contextual social network graph



	p1	p2	p3	p4	p5
p1					0.9
p2	0.7			0.9	
p3	0.9				0.6
p4			0.6		
p5		0.9			

Figure 5.4: Social trust matrices/cube

different but relevant contexts (termed as *interaction contexts*) to a *target context*, e.g., the context of an item to be recommended [206]. The result is called *transferred trust*.

As introduced in Section 5.2, personal properties and interpersonal properties can impact how much of the trust in interaction contexts can be transferred to that in a target context, which is termed as *trust transference degree*. Thus the transference degree of trust to p_y in p_x's mind from interaction context c_i to target context c_j can be calculated from the following equation:

$$\alpha_{p_x,p_y}^{c_i,c_j} = \omega_1 \cdot PS_{p_x,p_y}^{c_i} + \omega_2 \cdot SI_{p_x,p_y}^{c_i} + \omega_3 \cdot CS^{c_i,c_j} \tag{5.1}$$

This equation assumes that participant p_x trusts participant p_y with the trust value $T_{p_x,p_y}^{c_i}$ after interactions in context c_i in the past. It calculates the transference degree from the trust in interaction context c_i to the trust in target context c_j, when participant p_y makes recommendations to participant p_x. Here, $\{\omega_i\}, i = 1...3$ are the weights of the properties that impact the trust of p_y in the mind of p_x, and $\sum\limits_i \omega_i = 1$. Therefore, the trust value to p_y in the mind of p_x regarding the context c_i, $T^{c_i}_{p_x,p_y}$, can be transferred to the one in the target context c_j by $\alpha^{c_i,c_j}_{p_x,p_y} \cdot T^{c_i}_{p_x,p_y}$.

However, in the target context c_j, even if participant p_x has no interaction with participant p_y, p_x can trust p_y to some extent primarily due to p_y's social effect and his/her ability to give an appropriate recommendation, which can be depicted by the role impact factor and recommendation reliability. We use the term *"ego trust"* [139] to refer to this kind of trust, which can be formulated as:

$$BT^{c_j}_{p_x,p_y} = \delta_1 \cdot RIF^{c_j}_{p_y} + \delta_2 \cdot RLB^{c_j}_{p_y} \tag{5.2}$$

where, $\delta_1 + \delta_2 = 1$. Finally, based on the trust in all the interaction contexts C and the ego trust in the target context c_j, the transferred trust representing how much participant p_x can trust p_y in the target context c_j can be formulated as follows:

$$\tilde{T}^{c_j}_{p_x,p_y} = \beta_1 \max_{c_i \in C}\{\alpha^{c_i,c_j}_{p_x,p_y} \cdot T^{c_i}_{p_x,p_y}\} + \beta_2 BT^{c_j}_{p_x,p_y} \tag{5.3}$$

where, $\beta_1 + \beta_2 = 1$; $\max\limits_{c_i \in C}\{\cdot\}$ means the maximum trust value among all the trust values transferred from relevant contexts without ego trust. These coefficients can be calculated using the leave-one-out approach [81] in the historical data.

5.3.2 Trust Prediction based on Matrix Factorization

A more complicated situation is to predict trust between a source participant and a target participant when they have no interaction trust between each other in both the target context and relevant contexts, but they do have interactions with other participants respectively. In such a situation, even if all the trust in all the interaction contexts has been transferred to the target context using the method introduced in Subsection 5.3.1, the trust we want to predict in the target context is still absent. For instance, we want to predict the trust between p_2 and p_3 in Figs. 5.5 and 5.6.

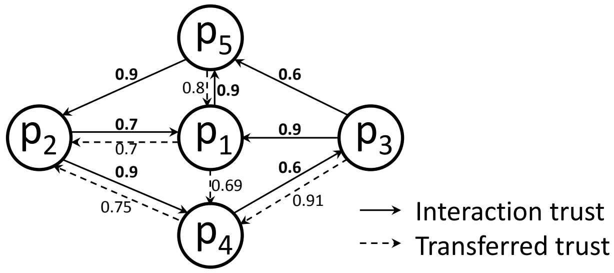
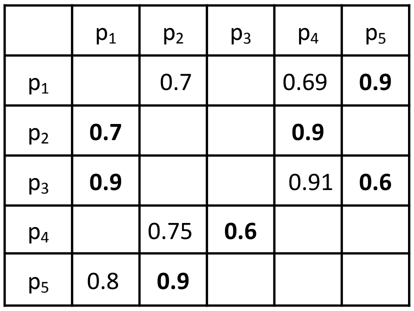


Figure 5.5: Graph presentation of contextual social network with transferred trust



	p1	p2	p3	p4	p5
p1		0.7		0.69	**0.9**
p2	**0.7**			**0.9**	
p3	**0.9**			0.91	**0.6**
p4		0.75	**0.6**		
p5	0.8	**0.9**			

Figure 5.6: Matrix presentation of contextual social network with transferred trust

However, the transference method of trust can assist trust prediction. With dashed arrows representing the trust calculated by Eq. (5.3) from the interaction contexts, the social network graph is shown in Fig. 5.5. Correspondingly, Fig. 5.6 shows a 2-dimensional trust matrix in which, the trust values in bold are interaction trust in the target context while the other trust values are transferred from all contexts as shown in Fig. 5.4.

In order to predict the trust between two participants in the target context at the situation where there is no trust information available between them in all the contexts, we modify the matrix factorization approach to fit the needs of trust prediction.

As shown in Fig. 5.6, the trust matrix R is a $N_p \times N_p$ matrix representing the trust from trusters (recommendees) to trustees (recommenders). The matrix factorization model maps trust values to a joint latent factor space of dimensionality l so that each trust value r_{xy} in matrix R is the inner product of truster vector $u_x \in \mathbb{R}^l$ (the relationship between truster x and the l latent factors) and trustee vector $v_y \in \mathbb{R}^l$ (the relationship between trustee y and the l latent factors).

$$r_{xy} \approx u_x^T v_y \tag{5.4}$$

Accordingly, the truster-trustee trust matrix R is modeled as the inner product of a truster-specific matrix $U = \{u_x\}$ and a trustee-specific matrix $V = \{v_y\}$.

$$R \approx U^T V \tag{5.5}$$

Note that, when $x = y$, participants u_x and v_y are the same participant with two different roles — truster and trustee (recommendee and recommender) respectively. Traditionally, the factorization process is approximated by Singular Value Decomposition by minimizing the following equation:

$$\frac{1}{2}||R - U^T V||_F^2, \tag{5.6}$$

where $||.||_F^2$ represents the Frobenius norm. Because each user only has trust values to a few other users, the matrix R contains a large amount of missing values as an extremely sparse matrix. Therefore, Eq. (5.6) is changed to

$$\min_{U,V} \frac{1}{2} \sum_{x=1}^{n} \sum_{y=1}^{n} (I_{xy} + \eta \tilde{I}_{xy})(r_{xy} - u_x^T v_y)^2, \tag{5.7}$$

where I_{xy} is an indicator function of interaction trust. $I_{xy} = 1$ *iff* participant p_x (truster) trusts participant p_y (trustee) in the target context originally, $x \neq y$. Otherwise, $I_{xy} = 0$. In addition, $\tilde{I}_{xy}$ is another indicator function of transferred trust. $\tilde{I}_{xy} = 1$ *iff* participant p_x (truster) has trust calculated by Eq. (5.3) to participant p_y (trustee), $x \neq y$. Otherwise, $\tilde{I}_{xy} = 0$. $\eta \in [0, 1]$ is a coefficient controlling the weight of transferred trust.

In order to avoid overfitting, two regularization terms from zero-mean spherical Gaussian priors [174] are placed into Eq. (5.7). In addition, a participant's properties are usually similar to those trusted by him/her in the social network [243], thus a social regularization is placed into Eq. (5.7). Hence, we have

$$\min_{U,V} \frac{1}{2}\sum_{x=1}^{n}\sum_{y=1}^{n}(I_{xy}+\eta\tilde{I}_{xy})(r_{xy}-u_x^T v_y)^2+\frac{\lambda_1}{2}||U||^2+\frac{\lambda_2}{2}||V||^2+\frac{\gamma}{2}\sum_{x=1}^{n}\sum_{f\in\mathcal{F}^+(x)} TP(x,f)||u_x-u_f||_F^2, \tag{5.8}$$

where $\lambda_1 > 0$ and $\lambda_2 > 0$; TP is a trust factor utility introduced in Eq. (4.9), which reduces the distance between two participants' truster-specific vectors according to their characteristics such as trust tendency. Once the learning process of the method is achieved by Eq. (5.8), the trust we want to predict can be calculated by Eq. (5.4).

5.4 Experiments

In this section, we evaluate the effectiveness of our model in typical scenarios including the basic cases of social networks in real world. We also compare our model with the state-of-the-art approach social context-aware trust inference (SocialTrust) [206], as well as the prevalent multiplication strategy (MUL) [110].

5.4.1 Scenario I: Comparison of Trust Inference between Contexts

In real life, a typical situation needing trust prediction is that a recommender and a recommendee do not have any interactions in the target context c_j. However, they have many interactions in the past in other relevant contexts $C = \{c_i\}$, $i = 1, ...n$ and $i \neq j$. Without any loss of generality, the trust values between two participants are generated using a random function in Matlab. We adopt the coefficients from SocialTrust [206] giving the same weight for each coefficient, where applicable, and set $\omega_1 = \omega_2 = \omega_3 = 0.333$, $\delta_1 = \delta_2 = 0.5$, $\beta_1 = \beta_2 = 0.5$, $CS^{c_1,c_2} = 0.8$, $CS^{c_1,c_3} = 0.1$. The context information we used in this case study can be found in Table 5.1.

In this situation, the trust to p_2 in p_1's mind can be calculated by Eq. (5.3). We also calculate the result using SocialTrust. They are presented in Table 5.2. Note that MUL

Table 5.1: Contextual tust to p_2 in p_1's mind

ID	Context	Context Relation	T_{p_1,p_2}	PS_{p_1,p_2}	SI_{p_1,p_2}	RIF_{p_1}	RIF_{p_2}	RLB_{p_1}	RLB_{p_2}
c_1	Teaching C++	$c_1 \sim c_2$ & $c_1 \nsim c_3$	?	0	0	0	0.8	0	0.9
c_2	Teaching Java	$c_2 \sim c_1$ & $c_2 \nsim c_3$	0.7	1	1	0.5	0.8	0.5	0.9
c_3	Car repair	$c_3 \nsim c_1$ & $c_3 \nsim c_2$	0.8	1	1	0.5	0.8	0.5	0.9

Table 5.2: Trust prediction results in all situations

Trust prediction models	Scenario I	Scenario II	Scenario III
MUL [110]	-	-	0.2
SocialTrust [206]	0.57	-	0.56
Our model	0.74	0.8	0.78

does not apply in this case, as it does not deal with trust between contexts.

SocialTrust neglects the concept of ego trust while taking the role impact factor of p_1 in the target context c_1 into account. In real life, this value should be 0 consistently, because when a participant seeks suggestions from others, he/she usually has no experience in the target context. Otherwise, he/she has his/her own trust in the target context already, and may not need recommendations. Therefore, our result is the most reasonable one in this scenario. It fits the case in real life that, a C++ teacher is usually also good at teaching Java, as they are similar contexts.

5.4.2 Scenario II: No Existing Paths

Since we have compared the transference methods in Subsection 5.4.1, in the following subsections, we assume that the transferred trust values from interaction contexts are the same so that the comparison of trust prediction models in the target context focuses on the same trust matrix.

In order to show that our proposed model does not rely on trust paths between the source and the target participants, this subsection considers the scenario in which there is no trust path between a source participant and a target participant. In other words, in this scenario, the source participant is not linked to the target participant by existing

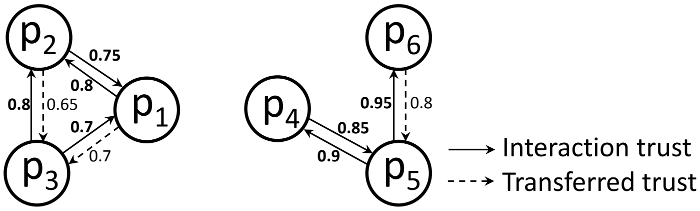
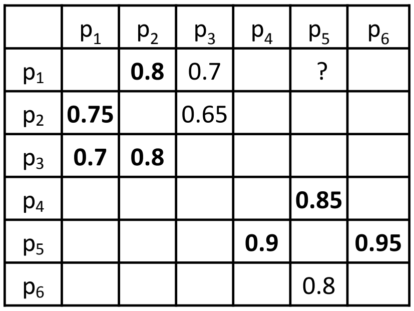


Figure 5.7: Social trust network graph in Scenario II



	p1	p2	p3	p4	p5	p6
p1		**0.8**	0.7		?	
p2	**0.75**		0.65			
p3	**0.7**	**0.8**				
p4					**0.85**	
p5				**0.9**		**0.95**
p6					0.8	

Figure 5.8: Contextual trust matrix in Scenario II

trust paths in all contexts. For example, when participant p_5 gives a recommendation to participant p_1, what is the trust to p_5 in p_1's mind in the social network as shown in Fig. 5.7? The trust values in bold fonts in Fig. 5.8 represent interaction trust in the target context while other trust values are transferred from relevant contexts. The question mark stands for the trust value we want to predict.

Because there is no path between the source participant and the target one, MUL and SocialTrust do not apply in this scenario. By contrast, our model detailed in Subsection 5.3.1 differentiates the interaction trust in the target context and the transferred trust from relevant contexts. It analyzes the features of the contextual trust matrix and predicts the trust in the target context based on these features.

As shown in Table 5.2, our model predicts the missing trust value as 0.8 which is in the trust value range of p_1's history and similar to the trust values p_5 receives. Thus, our model can generate a reasonable trust value in this scenario, which is not vulnerable to the lack of trust paths in the trust prediction process.

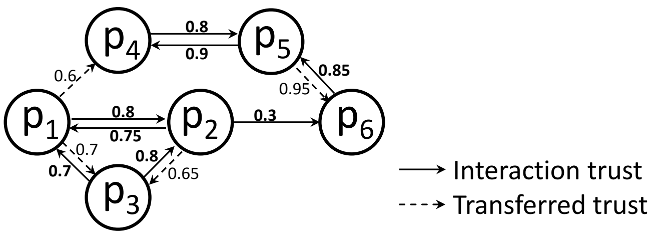
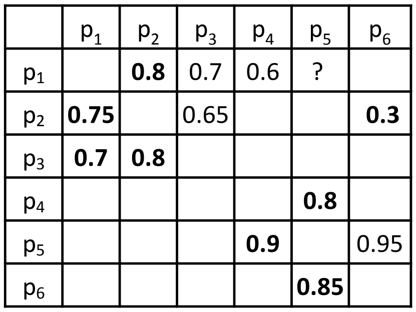


Figure 5.9: Social trust network graph in Scenario III



	p_1	p_2	p_3	p_4	p_5	p_6
p_1		**0.8**	0.7	0.6	?	
p_2	**0.75**		0.65			**0.3**
p_3	**0.7**	**0.8**				
p_4					**0.8**	
p_5				**0.9**		0.95
p_6					**0.85**	

Figure 5.10: Contextual trust matrix in Scenario III

5.4.3 Scenario III: More Connections than a Path

In this subsection, we consider a very common situation in social networks when making recommendations. As shown in Figs. 5.9 and 5.10, when participant p_5 gives a recommendation to participant p_1, there is a trust path in the target context connecting the source p_1 and the target p_5 in a social network. However, there are also some other participants in the social network connecting p_1 and p_5 respectively. These connections are believed to offer some valuable trust information and should be taken into account. But they do not form paths connecting the source participant and the target participant in the target context. Therefore, they are not useful in trust inference models, e.g., SocialTrust.

We give an example in Fig. 5.9, showing the interaction trust and transferred trust between contexts. Fig. 5.10 presents the trust matrix representing exactly the same social trust network, where the question mark stands for the trust to be predicted.

From Table 5.2, we can see that all MUL, SocialTrust and our model are able to predict the missing trust value in this scenario. But the trust value 0.78 predicted by our model is more reasonable than both 0.2 predicted by MUL and 0.56 predicted by SocialTrust for the following reasons: (i) in Fig. 5.10, participant p_5 receives relatively high trust values 0.85 and 0.8, indicating that p_5 tends to be trusted in the target context; (ii) the trust values to the others in p_1's mind are not very low, which means that p_1 tends to trust others. Therefore, the trust to p_5 in p_1's mind should not be very low.

In this scenario, because MUL does not deal with trust between contexts, its result relies on the trust path consisting of only the interaction trust in the target context. SocialTrust relies on paths consisting of both interaction trust and transferred trust in the target context, and gets a better result than MUL. However, the results of both SocialTrust and MUL are determined by each trust value on the trust path from the source participant to the target participant, while our model utilizes all the trust information in the trust matrix to predict T_{p_1,p_5}, as the trust information not on a path can also be used to extract features of participants.

5.5 Conclusion

As trust prediction is a context sensitive process, it is essential for the generation of trustworthy recommendations and still remains a challenging and complex task. In this chapter, we have first analyzed the properties that can impact trust transference between different but relevant contexts. Based on these impact properties, we have proposed a new trust transference method to transfer trust from interaction contexts to a target context considering personal properties and interpersonal properties and the features of contexts, which forms a social contextual trust matrix with a smaller sparsity degree. Then, a new social context-aware trust prediction model, with indicator functions of both interaction trust and transferred trust, has been proposed to predict trust from a source participant to a target participant. The proposed approach analyzes and incorporates the characteristics of participants' trust values, and predicts the missing trust in the target context using modified matrix factorization, regardless of whether or not there is a path connecting them. To the best of our knowledge, this is the first context-aware trust prediction model in social networks in the literature. It not only utilizes the trust relationships in the target context, but also incorporates the trust information from relevant contexts via our trust transference methods.

The experimental analysis shows that our proposed model transfers trust between contexts in a reasonable way and is able to predict trust between a source and a target participants in all the above situations. It leverages trust transference from relevant interaction contexts to target context to mitigate the traditional sparsity problem in the target context, which is particularly important when seeking recommendations from other disconnected participants in social networks.

Chapter 6

Dynamic Trust Prediction of Online Environments

Both the single-context trust prediction introduced in Chapter 4 and the context-aware trust prediction in Chapter 5 predict a static trust value no matter whether context is considered or not. As described in Subsection 2.2.2.5, trust changes over time, which is especially important in the online trading environments. Online trading takes place in a very complex environment full of uncertainty, in which deceitful service providers or sellers may strategically change their behaviors to maximize their profits. The proliferation of deception cases makes it essential to model the trust dynamics of a service provider and predict the trustworthiness of the service provider in future transactions. Therefore, this chapter focuses on modeling trust dynamics to predict future trust values in the online trading environments.

This chapter is organized as follows. We first analyze the dynamic trust prediction problem in Section 6.1. Then, Section 6.2 presents the feature extraction process for dynamic trust prediction of service providers concerning a forthcoming transaction in light of as much information as we can consider, including the *static features*, such as the provider's reputation and item price, and the *dynamic features*, such as the latest profile changes of a service provider and price changes. In Section 6.3, we first introduce the basic knowledge of HMM needed in this chapter; and then we propose an HMM-based dynamic trust prediction model to predict the trustworthiness of a service provider in a forthcoming transaction based on the features from the service provider's historical transactions. In this model, all the features extracted from both contextual information and the rating of each transaction are treated as observations of HMM. In Section 6.4 we evaluate our approach empirically in order to study its performance. The experiment results illustrate that our approach significantly outperforms the state-of-the-art probabilistic trust methods in accuracy in the cases with complex changes. Section 6.5 summaries the work in this chapter.

6.1 Description of Dynamic Trust Prediction

In recent years, people are increasingly active in various large, open and dynamic network systems including social networks, P2P systems, e-commerce and e-service [208]. Due to the nature of virtual communities, people including service providers and service consumers do not meet or interact physically. In such an environment with uncertainty, the prediction of the dynamic trust to a service provider in online service applications has been growing in importance [107, 209, 207]. Without trust, prudent business operators and clients may leave the Internet market and revert to traditional business [137]. In human society, trust depends on a host of factors such as past experience with a person, opinions, and motivations [25]. In electronic commerce and service environments, consumers cannot directly interact with products and workers, and the credibility of online information may be doubtful [168]. As a result, trust mainly relies on the past experience with a service provider or seller, the description of services, the provider's reputation etc. Thus how to determine the trust of a service provider becomes a major challenge to ensure that every forthcoming transaction is reliable for honest buyers. As the issue of trust exists in both e-commerce and e-service environments, in this chapter, we use the terms "seller" and "service provider" interchangeably.

A number of techniques have been proposed for establishing trust online. These techniques fall under two main categories: security based solutions and social control based solutions [133]. The former techniques include authentication, access control, and public key infrastructure. The latter techniques mainly focus on trust recommendations and reputation. So, trust emerges as the most popular concept to manage the uncertainty of service providers' behaviors online [204]. In addition, probabilistic trust can broadly be characterized as aiming to build probabilistic models upon which the future behavior can be predicted [51].

In online e-commerce and e-service environments, such as eBay and Amazon, the system maintains past transaction information for a certain period, which offers the possibility to infer a service provider's future action, and could provide useful advice to customers. As introduced in Subsection 2.4.3, a number of approaches have been proposed to model the behavior of a service provider. The Beta model is a static model but not effective when the provider's behavior is highly dynamic. Probabilistic models are the most promising tools to deal with dynamic uncertainty. One of the most typical and powerful probabilistic models is Hidden Markov Model (HMM). HMM is a stochastic model appropriate for nonstationary stochastic sequences whose statistical properties undergo distinct random transitions among a set of, say k, different stationary processes. In other words, HMMs are used to model piecewise stationary processes whose statistical properties do not change with time themselves [195]. HMM treats the list of transactions as a Markov chain and assumes the service provider's behavior has finite salient states which determine the distribution of the outcomes of transactions. A given state, which determines the distribution of observations, only depends on its previous state; thus, the trustworthiness of the next transaction could be inferred from the historically recorded list in the system.

The application of HMM for trust prediction has led to many approaches with different efficiencies and precisions. ElSalamouny et al. [52] uses HMM to predict the outcome of the future transaction based solely on the list of past outcomes, achieving better performance than the Beta model with a forgetting factor [82]. However, a transaction includes contextual information and an outcome/rating. The contextual information, which characterizes all the details of a transaction, may contain more clues leading to the outcome and can be utilized to predict the status of the future trans-

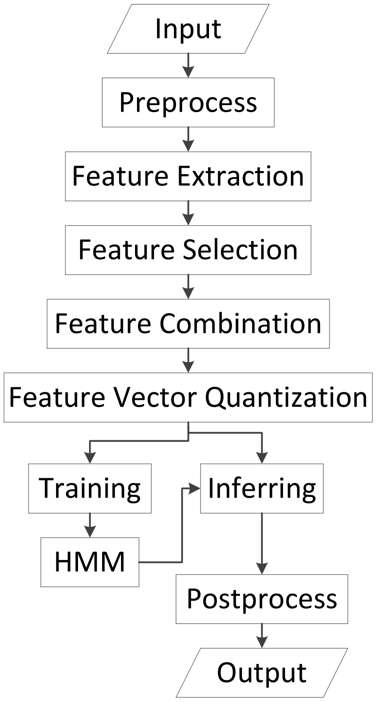


Figure 6.1: Flowchart of our approach

action. From contextual information, Liu and Datta [124] extract useful features, as observations, to construct an HMM to model the dynamic trust of a seller. However, they directly treat outcomes of transactions as hidden states, which eliminates the hidden characteristic of HMM and limits the ability of HMM to model a service provider' dynamics in trust/reputation.

In order to overcome the disadvantages of existing approaches, we propose a new approach as shown in Figure 6.1. We firstly analyze what features of transactions can affect the outcomes resulting in a more comprehensive characterization of contextual information. Based on contextual information, we extract not only static features but also dynamic changes as features. For instance, some sellers may change their profile before committing deception. Secondly, we boost the execution effectiveness through three steps: (i) we select the most powerful features as observations using information theories [92]; (ii) we use the Principal Component Analysis (PCA) algorithm [4] to combine the most powerful features to form relatively lower dimensional feature vectors; and (iii) we apply Vector Quantization (VQ) techniques [92] to project final feature vectors into discrete values. Lastly, we propose a Discrete Hidden Markov Model (DHMM) to model the trust trend. We treat all the contextual features and outcomes/ratings as HMM observations, and predict the most possible rating of the observation of the forthcoming transaction.

6.2 Producing Features

Liu and Datta [124] have shown that a service provider's interaction behavior can be estimated by contextual information. Based on the features extracted from the contextual information of transactions, we analyze the dynamic characters of the sellers in online trading web sites and build our own HMM trust model.

We propose four main steps to produce the most effective features from contextual information. Firstly, we conceptually choose as much information related to the behaviors of a seller as possible. Secondly, based on the data, we use information theories like mutual entropy to reveal the most powerful features and eliminate the least powerful ones. Thirdly, we use PCA to combine the feature vectors. In other words, the features are projected into another coordinate space with lower dimensionality. Lastly, Vector Quantization techniques are used to project the combined feature vector into different discrete observations that are provided to the Discrete Hidden Markov Model as the input.

6.2.1 Feature Extraction

Contextual information refers to all the information that characterizes the transactions and from which classifying features could be extracted. The state-of-the-art features used in HMM models usually can be divided into two main types—static features and dynamic features which also occur in the seller's behaviors. Here following Liu and

Datta's method [124], the static features are extracted from three aspects as described below.

1. About the service provider/seller: the contextual information includes the features about the provider who offers service. Taking eBay as an example, the features are mainly collected from the provider profiles including seller's system age, detailed connection information, actual age, gender, location, number of items sold already, reputation value, and average delivery time.

2. About the service: the contextual information contains item price, category average price, comments, the number of items in stock, the number of buyers etc.

3. About the social relationships: these kinds are the features concerning the relationships between the service provider and others, such as family, colleague, friend, acquaintance ties, community, organization, trust networks and so on.

In order to accurately model the dynamics of a service provider, the dynamics must be captured precisely to represent the changes of providers. For instance, some online sellers may change their profiles or prices before committing a cheating action, which can lead to an essential caution for the buyers.

In this step, we extract features which have the probability to distinguish the service providers' behaviors. However, not all of them may be essential. The next step is to refine the extracted features.

6.2.2 Feature Selection

To reduce the computation time and eliminate the less powerful features, we choose the mutual entropy to select and maintain the K most powerful features or the ones over a threshold as our final observation in the HMM model.

Entropy usually has two views: the lower bound on the average number of bits to encode our feature values or the measure of the uncertainty about the feature values [92]. Here the latter meaning is more suitable to our case.

Features are usually dependent on the exact e-commerce, e-service or auction web site. The potential features extracted are represented as $\Omega = \{w_1, w_2, ...\}$, where $w_r \in \Omega$ corresponds to an exact feature. Suppose we are given the past transaction list of a seller $\Theta = \{\theta^1, \theta^2, ...\}$, and all the transaction outcomes/ratings coming from a set of discrete quantitative variables in a certain range denoted by $L = \{l_1, l_2, ..., l_l\}$ with the probability distribution $P = \{p_1, p_2, ..., p_l\}$. According to the definition of entropy, the entropy of a seller's all past transactions Θ is:

$$H_P(\Theta) = E_P[log\tfrac{1}{p_j}] = \textstyle\sum_{j=1}^{l} P(\theta)log\tfrac{1}{p_j}$$

In the extremely simple situation, when all the feedback of a service provider's transaction history is positive, then according to the equation, the entropy of the feedback is 0. If there is 1/2 positive, 1/3 neutral and 1/6 negative feedback in this provider's history, the entropy is 1.459. If there is 1/3 positive, 1/3 neutral and 1/3 negative feedback in this provider's history, the entropy is 1.585. So it is clear that entropy can be utilized to identify different distributions of data.

For each feature $w_r \in \Omega$, we use $\Upsilon(w_r)$ to denote its value set. For each value $v \in \Upsilon(w_r)$, we represent all the past transactions associated with v for feature w_r by Θ^v. Then the Mutual Information between Θ and Θ^v represents the extent to which the knowledge of Θ^v reduces our uncertainty about Θ, which is:

$$\begin{aligned} I_p(\Theta; w_r) &= H_p(\Theta) - H_p(\Theta|w_r) \\ &= H_p(\Theta) - \sum_{v \in \Upsilon(w_r)} \frac{|\Theta^v|}{|\Theta|} H_p(\Theta^v) \end{aligned}$$

The mutual entropy actually calculates a certain feature's effect on the probability distribution of the entire feature data. So it is clear that the higher the Mutual Information is, the lower the corresponding entropy becomes, and as a result, the better the classification is [124]. Then the top K features or the features above a certain threshold are selected according to Mutual Information.

6.2.3 Feature Combination

So far it is not guaranteed that the feature vectors are best presented in the current orthogonal coordinate system. In other words, the variance of the vectors along the axes is not maximized. If it is, we could select the principal components and reduce the vector dimension. So, in order to further reduce the computation time and maintain only the essential information, we apply Principal Component Analysis [4] to simplify the features selected from Mutual Information.

Mathematically PCA is a procedure to determine an orthogonal transformation of the coordinate system to convert a set of observations of possibly correlated variables into a set of values of linearly uncorrelated variables such that in the new coordinate system, the variance of the transformed data along the new axes has been maximized [4]. PCA performs the transformation using the statistical nature of the information so that the number of principal components is less than or equal to the number of original variables keeping the information of the data set lossless or only with a little loss.

After applying PCA, we can find the key components and structure of data and eliminate noise and redundancy resulting in the reduction of the number of dimensions by calculating eigenvalues and eigenvectors. For each transaction, we denote the key features as a vector: E_i. After including the contextual information, the rating l_i is absorbed into the key features. The optimized feature vector together with the rating element forms the full feature vector, denoted by $\mathbb{E}_i = [E_i, l_i]$, describing the transaction's contextual information with little redundancy.

6.2.4 Feature Quantization

With the final feature vectors, we can either quantize them to discrete values and apply the Discrete Hidden Markov Model, or directly apply continuous HMM. Due to the fact that some information is discrete and the consideration of computation time, here we choose DHMM.

Vector Quantization is an area that has close affinity with clustering. This technique is mainly used for data compression which is a prerequisite for achieving better computer storage utilization and better bandwidth utilization, especially in communications [195].

Let $\mathbb{E} = \{\mathbb{E}_i\}$ be the set of all feature vectors for our prediction problem including the features extracted from contextual information and the rating, both of which are finally mapped to the observation of HMM. We separate $\mathbb{E}$ into M distinct regions $\{R_j\}$ that exhaust $\mathbb{E}$ and represent each of them with a code vector v_j (here in our problem that is simplified as a value). The major goal in VQ is to define the regions $\{R_j\}$ and their representatives $\{v_j\}$ so that the information loss (called distortion) is minimized. The discrete representatives $\{v_j\}$, projected from the feature vector $\{c_j\}$, are the observations of DHMM.

6.3 Markov Trust Prediction Models

Although statistical methods of Markov source or Hidden Markov Model were first introduced and studied in late 1960s, it is still popular in the pattern recognition area because of its richness in mathematical structure and good performance in practical applications [160]. It is very powerful for predicting the future trend based on sequential datasets. In this study, we modify HMM and make it suitable for e-commerce and e-service scenarios.

6.3.1 Basic Knowledge of HMM

A Hidden Markov Model is a statistical Markov model in which the system being modeled is assumed to be a Markov process with unobserved (hidden) states that control the mixture components to be selected for each observation [160]. So, each HMM has a hidden state sequence from a finite state set and its corresponding observation sequence. The basic structure is shown in Figure 6.2. It also obeys the Markov chain

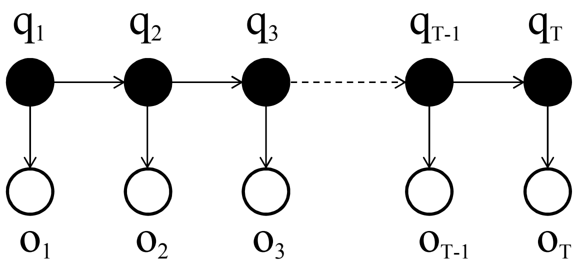


Figure 6.2: First-order hidden Markov chain

hypothesis: each state is only determined by the previous one; the distribution of observations is only dependent on its corresponding state and independent with other observations; the number of states is finite [92].

Suppose in a sequential data we have T observations $O = \{o_1, o_2, ..., o_T\}$, $o_i \in V = \{v_1, v_2, ..., v_M\}$ and the states we infer from the observation are $Q = \{q_1, q_2, ..., q_T\}$, $q_i \in S = \{s_1, s_2, ..., s_N\}$, where M is the number of distinct observation symbols and N is the number of states in the model. Then the HMM can be represented as [160]:
$\lambda = (V, S, A, B, \pi)$.
A is the state transition probability distribution:
$A = \{a_{ij}\}_{N\times N}$, where $a_{ij} = P(q_{t+1} = S_j|q_t = S_i)$, $1 \leq i, j \leq N, 1 \leq t \leq T$;
B is the emission probability distribution:
$B = \{b_j(k)\}_{N\times M}$, where $b_j(k) = P(v_k@t|q_t = S_j)$, $1 \leq j \leq N$, $1 \leq k \leq M$, $1 \leq t \leq T$;
π is the initial state distribution:
$\pi = \{\pi_i\}_{N\times 1}$, where $\pi_i = P(q_1 = s_i), 1 \leq i \leq N$.

In general, there are three basic HMM problems of interest to be solved for the model to be useful in real-world applications described as follows:

- **Problem 1:** Given the observation sequence O and a model λ, how to efficiently compute the probability of the observation sequence $P(O|\lambda)$?

- **Problem 2:** Given the observation sequence O and a model λ, how to choose a corresponding state sequence Q?

- **Problem 3:** How to adjust the model parameters λ?

In the application for the calculation of trustworthiness, we only refer to the basic Problem 1 and Problem 3. Our goal is to calculate the probability: $P(O_{t+1} = v_i | O_{1:t}, \lambda)$ which means the probability of the case that the next observation will be v_i if we have already known the past observations from time 1 to time t.

In the following sections, we present, in more detail, how to predict the outcome by HMM in the most powerful way.

6.3.2 Our Proposed HMM-based Approach

As stated before, the outcome-based HMM achieves better performance than the Beta model with a decay factor, and the Markov Model (MM)-based on contextual information with visualized states is even better than the outcome-based HMM in accuracy and efficiency. We therefore propose an HMM algorithm based on both contextual information and outcomes to model the service providers' behaviors with hidden states.

To further explain the use of HMM, we give a simple example. A malicious provider honestly sold cheap but good-quality items in 80 transactions to accumulate a good reputation and then started to deceive in the next 20 transactions. The history of this provider can be considered consisting of two states—honest and dishonest which are not visible. But when the provider was in the honest state in the first 80 transactions, we had very high probabilities (not 100% necessarily) to observe relative low prices, reputation rises and positive feedbacks. However, when the provider was in the dishonest state in the last 20 transactions, we were more likely to observe higher prices, reputation declines and negative feedbacks. Each transaction can be treated as one time point in HMM. The observations are the prices, reputation changes and feedbacks, all of which are determined by the hidden states (honest or dishonest). Therefore, the states are hidden but they can be predicted by the observations. Then the whole transaction history can be modeled by HMM.

Suppose that the past transactions of a service provider are denoted by $\Theta = \{\theta^1, \theta^2, ...\}$.

We also assume that the outcomes are discrete quantities such as rating numbers from 1 to 5. Using the HMM described above and the same symbols to model the transaction list which describes the behavior of the service provider, the service provider's behavior can be denoted by $\lambda = (V, S, A, B, \pi)$, or $\lambda = (A, B, \pi)$ for short, where there are N possible hidden states, denoted by S. The hidden states can be understood as the provider's working periods/states that determine the distribution of observations. M extracted features/observations are denoted by V. A and B are the transition probability matrix and the emission probability matrix respectively as described above. From Θ, we extract observation sequence $O = \{o_1, o_2, ..., o_T\}$ and train the model parameters λ with a finite number of hidden states which maximizes the expectation that the HMM λ could emit the observation sequence (the list of past transactions), where $O_i \in V$ and $q_i \in S$, $1 \leq i \leq T$. The observation and the state of the next transaction are denoted by O_{T+1} and q_{T+1} respectively.

To predict the next transaction behavior based on the past knowledge of a service provider, we need to calculate the probability distribution of the rating in the next transaction at time $T+1$ given the observation sequence for the past time $[1, T]$. In our model, a rating to a service provider is part of the observation. So, the probability of each possible observation in the forthcoming transaction can be computed by:

$$\begin{aligned} P(o_{T+1} = v_j | O_{1:T}, \lambda) &= \frac{P(o_{T+1} = v_j, O_{1:T}, |\lambda)}{P(O_{1:T}, |\lambda)} \\ &= \frac{P(o_{T+1} = v_j, O_{1:T} |\lambda)}{\sum_{j=1}^{N} P(o_{T+1} = v_j, O_{1:T}, |\lambda)} \end{aligned} \tag{6.1}$$

The numerator is the joint probability that observations $O_{1:T}$ are observed in the first T transactions and at next transaction $T+1$ the feature v_j is observed as the next observation. The denominator represents the sum of all the possible o_{T+1} together with previous observations $O_{1:T}$ given the model λ.

Following the structure in Figure 6.2 to calculate the probability of the observation sequence $P(O|\lambda)$, the most straightforward way is to enumerate every possible state sequence of length T (the number of observations) [160].

$$\begin{aligned} P(O_{1:T}|\lambda) &= \sum_{allQ_{1:T}} P(O_{1:T}|Q_{1:T},\lambda)P(Q_{1:T}|\lambda) \\ &= \sum_{q_1,q_2,...,q_T} \pi_{q_1} b_{q_1}(o_1) a_{q_1q_2} b_{q_2}(o_2) \\ &\quad ...a_{q_{T-1}q_T} b_{q_T}(o_T) \end{aligned} \tag{6.2}$$

where $Q_{1:T} = \{q_1, q_2, ..., q_T\}$ is a fixed state sequence which emits the observation sequence; $P(Q_{1:T}|\lambda)$ is the probability of the state sequence $Q_{1:T}$ given the model λ; $P(O_{1:T}|Q_{1:T},\lambda)$ is the probability of the observation sequence $O_{1:T}$ for the state sequence of $Q_{1:T}$ given the model λ.

According to Equation (6.2), the calculation of $P(O_{1:T}|\lambda)$ has a complexity of the order of $2T \times N^T$. Clearly a more efficient method is required. Fortunately, the Forward-Backward procedure [21] can solve the calculation problem.

The Forward algorithm could calculate $P(O_{1:T+1}|\lambda)$ avoiding an exponentially growing calculation. For $t = 1, 2, ..., T+1$ and $i, j = 1, 2, ..., N$, we define $\alpha_t(i) = P(O_{1:t}, q_t = s_i|\lambda)$, that is, the probability of the partial observation sequence $o_1, o_2, ..., o_t$ and state s_i at time t, given the model λ. The calculation of $\alpha_t(i)$ can be solved inductively as follows:

1. Initialization: $\alpha_1(i) = \pi_i B_i(1)$
2. Induction: $\alpha_{t+1}(j) = [\sum_{i=1}^{N} \alpha_t(i) a_{i,j}] b_j(t)$
3. Termination: $P(O_{1:T}|\lambda) = \sum_{i=1}^{N} \alpha_T(i)$

Then, we have $P(o_{T+1} = v_j, O_{1:T}|\lambda) = \sum_{i=1}^{N} \alpha_{T+1}(i)$
For the next transaction at time $T+1$, usually we have already known the contextual information so we can extract the feature vector E_{t+1} and limit the possible outcomes to a subset of the whole observation set $V' = \{v'_j\} \in V$, where the subset V' contains all the observations projected from the same feature vector together with different

possible ratings. Finally, the most possible predicted outcome of the next transaction is the rating in the observation with the highest probability:

$$o_{T+1} = \arg\max_{v'_j \in V'} [P(o_{T+1} = v'_j, O_{1:T}|\lambda)].$$

6.3.3 HMM Training

Given the output sequences: $\lambda = \arg\max_{\lambda} P(O_{1:T}|\lambda)$, the training procedure of HMM is to find the best state transition probability and observation emission probability. The task is usually carried out by the Baum-Welch algorithm [216] using the Forward-Backward algorithm. The Baum-Welch algorithm is a particular case of the Expectation Maximization (EM) algorithm. It could reestimate the parameters of HMM given only emissions/observations as training data by maximizing Baum's auxiliary function. The details can be found in [160][216].

We first define the three variables:

- $\beta_t(i) = P(O_{t+1:T}|q_t = s_i, \lambda)$: the probability of the partial observation sequence from $t+1$ to the end, given state s_i at time t and the model λ;
- $\gamma_t(i) = P(q_t = s_i|O, \lambda)$: the probability of being in state s_i at time t, given the observation sequence O and the model λ; and
- $\xi_t(i,j) = P(q_t = s_i, q_{t+1} = s_j|O, \lambda)$: the probability of being in state s_i at time t and state s_j at time $t+1$.

Then the iterative reestimating procedure could be conducted as follows:

$$\bar{\pi} = \gamma_1(i);$$

$$\bar{a}_{ij} = \frac{\sum_{t=1}^{T-1} \xi_t(i,j)}{\sum_{t=1}^{T-1} \gamma_t(i)};$$

$$\bar{b}_j(k) = \frac{\sum_{t=1, s.t. o_t = v_k}^{T} \gamma_t(j)}{\sum_{t=1}^{T} \gamma_t(j)}.$$

where $\bar{\pi}$ is the expected frequency in state s_i at time $t = 1$; $\bar{a}_{ij}$ is the ratio of the expected number of transitions from state s_i to state s_j to the expected number of transitions from state s_j; $\bar{b}_j(k)$ is the ratio of the expected number of times in state j and observation symbol v_k to the expected number of times in state j.

$\xi_t(i,j)$ and $\gamma_t(i)$ can be calculated by the Forward-Backward algorithm. We do not discuss the details here. Usually, there are a number of local minima and the data surface is complicated. The EM algorithm leads to local minima only. Fortunately, the local minima are usually adequate [160]. EM does not estimate the number of states. So, that must be given by experience or other algorithms such as standard gradient techniques. The initialization of HMM does affect performance, but it can be optimized by other standard optimization algorithms. Usually, the reestimating procedure could be conducted several times to lessen the effect of random initialization.

6.4 Evaluation

6.4.1 Experimental Methodology

With the APIs released by eBay, we have developed a program using PHP to extract real datasets from the popular e-commerce website eBay (http://www.ebay.com.au/). The data we obtained from eBay contains the records of transactions of sellers within three months. In order to evaluate the performance of our modified model and to compare it with the state-of-the-art models, we generate synthetic datasets following the scenarios in the real data. Each dataset has 1000 sellers, each of which has finished 100 transactions for the same item.

For the complexity issue, we assume binary values for each property of each transaction and select only typical features to evaluate the approach. We treat any transaction with 5 points (highest points in eBay) positive feedback as successful transactions. Otherwise, we handle them as unsuccessful transaction records. We use the category ID to differentiate items. Within the same category, the features we used contain static features (item price, the time each transaction occurred, reputation and quantity, all of which are calculated as the percentage of the averages in the same category) and dynamic features (price changes, reputation changes). To investigate the performance of feature extraction, we set the time one transaction occurred as random noise.

From the analysis of the real datasets, we consider two scenarios of sellers' behaviors:

- **Scenario I:** The sellers conducted a number of transactions with very good attitudes and quality, obtaining successful transaction records. Then they become imprudent, completing several unsuccessful forthcoming transactions.
- **Scenario II:** The sellers change their behaviors randomly but most of the transactions are still successful.

We perform the feature extraction process as described in Section 3. Based on the extracted features, we compare our approach with the outcome-based HMM [52] and the contextual information-based Markov Model [124] on the performance of the rates of correct predictions.

6.4.2 Results and Analysis

We compare the rates of correct predictions of our model with the outcome-based HMM (OHMM) [52] and the contextual information-based Markov Model (CIMM) [124] on the synthetic datasets in the above two scenarios.

Results of Scenario I: The sellers all remain prudent at the beginning and then start to become imprudent. In this scenario, we mainly compare the performance of the three approaches on different percentages of unsuccessful transactions. We synthesize 25 groups of seller transaction datasets and each group has 1000 sellers. For each seller, there are 100 records of recent transactions. The difference between the groups is that the sellers in the first group have unsuccessful outcomes only on the last transaction, the sellers in the second group are unsuccessful on the last 2 transactions, and so on.

For each approach, we use the first 99 transactions to train the models and use

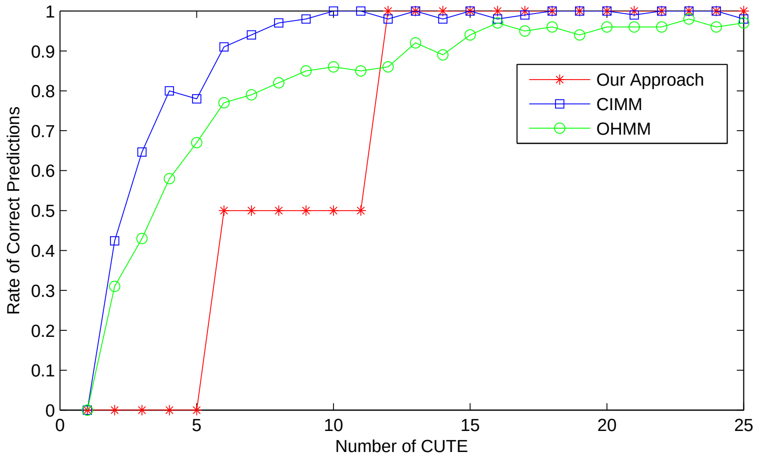


Figure 6.3: Rates of correct predictions in Scenario I

the last transaction to evaluate the rates of correct predictions. From the experimental results, we notice that in the first group, none of the three approaches can predict correctly with a zero correct rate, because there is no unsuccessful transaction in the training data. As the percentage of unsuccessful transactions goes higher, there are more unsuccessful transactions in training data. As a result, the rates of correct predictions delivered by the three approaches all improve.

Figure 6.3 shows the performance of each approach with different numbers of continuous unsuccessful transactions in the end (CUTE). In the results of the first several groups, our approach is not as good as the other models. But the performance of all the three approaches improve and the correct rates of our approach go up to 100%, equal to or better than the others while the number of unsuccessful transactions accumulates to more than 13. This is because the number of observations is larger when treating both features and outcomes as observations and the data is relatively less dynamic in this scenario.

Results of Scenario II: To compare the three approaches in Scenario II, we also synthesize a dataset of 1000 sellers. Each seller maintains 100 historical records of transactions. But in this scenario, the ratings of sellers are randomly generated following the rule that most of transactions are successful. The distributions of contextual in-

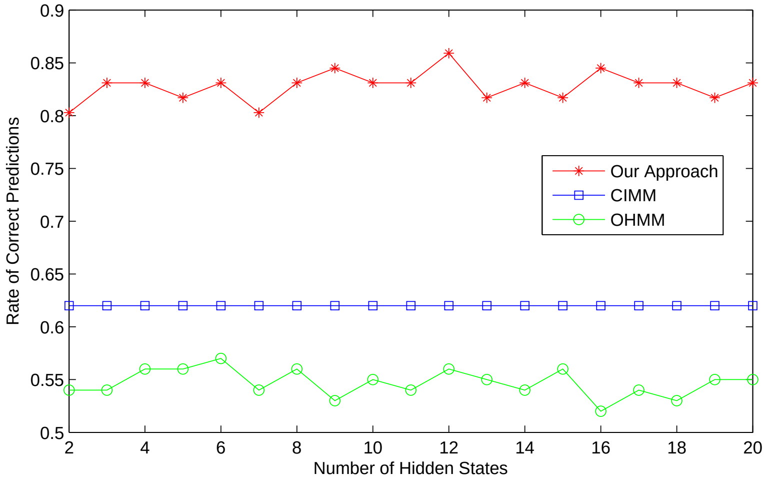


Figure 6.4: The effect of numbers of hidden states in Scenario II

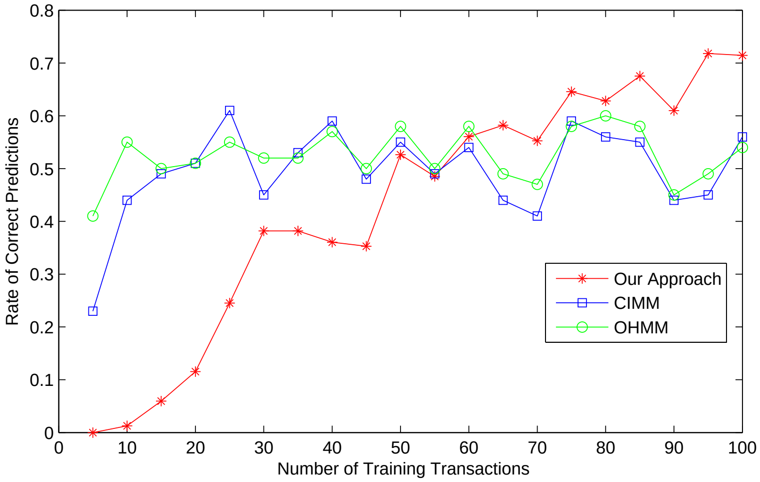


Figure 6.5: Comparison with various sizes of training data in Scenario II

formation at different ratings are different, which is the characteristic used to evaluate different prediction models. Figure 6.4 shows the performance of the three approaches with different hidden state numbers, where we use the first 99 transactions to train the three models and use the last transaction to examine the prediction result. Again, the performance of our approach and OHMM changes according to different numbers of hidden states, while CIMM could not change this parameter which is also plotted in the figure for comparison.

From Figure 6.4, we can see that the performance of our approach and OHMM fluctuates with different number of hidden states. On average, our approach achieves 21% higher than CIMM and 27% higher than OHMM on the rates of correct predictions. Thus, our approach significantly outperforms both OHMM and CIMM approaches in this scenario.

In addition, we also compare the three approaches with different sizes of training data. That is, for each seller, we use first x percent of the previous transactions to train the three models separately and predict the next transaction. The results of experiments presented in Figure 6.5 demonstrate that the size of training data affects the prediction performance of all the three approaches. Our approach outperforms the others on the rates of correct predictions when the number of training transactions is more than 55 out of 100. As the number of training transactions goes higher, our approach becomes much better than the others. The gap reaches the peak which is 16% better than the others when 99 transactions are used as training data. This is because there are more observations in our approach.

6.5 Conclusion

This chapter has proposed an HMM-based trust prediction model, which, differently from existing works, trades both contextual information and trust ratings as observations. First, this chapter has analyzed the features that can be extracted from historical transactions and are useful for dynamic trust prediction. Then, instead of directly using contextual information, the information theories and PCA have been utilized to refine these features, which significantly reduces calculation time, because these strategies preserve the essentials of contextual information, and reduce the noise in presenting the service provider's behaviors. Next, we have proposed an HMM-based trust prediction approach which is different from the outcome-based HMM and the contextual information-based Markov Model using outcomes as hidden states. In our model, both the refined features from contextual information and the rating of each transaction are projected by VQ to the observations of a discrete HMM to predict the future result, which, unlike previous methods, uses HMM in a different and more effective way. The experiments have been conducted on synthetic datasets regarding typical application scenarios. The experimental results have demonstrated that HMM based on both contextual information and outcomes needs more training data than the others, but is more effective in predicting the future results of a service provider in complex dynamics.

Chapter 7

Conclusions and Future Work

7.1 Conclusion

In recent years, Online Social Networks (OSNs) have attracted a growing number of participants and have grown to the platform for a variety of activities such as recruitment and recommendation. In such type of activities, trust is one of the most important factors for participants' decision making. However, most participants do not have previous direct interactions in OSNs. In addition, it is rare for a participant to have full trust on another in every facet [189, 180]. Therefore, predicting the trustworthiness between two unknown participants in OSNs becomes significant and necessary.

In order to predict reasonable trust values efficiently and effectively for different application environments, our studies in this thesis have been conducted in four main aspects. The contributions can be summarized as below.

1. The first aspect of the work presented in this thesis is social trust subnetwork extraction from large-scale social trust networks. This is an essential step for the performance of forthcoming trust prediction process.

   (a) As described in Subsection 2.2.4, social contexts have significant influence on trust prediction, yet are ignored by most existing trust prediction models. In our model, social contextual impact factors, including role impact factor, reliability, preference, social intimacy and existing trust, have been taken into account the social information.

   (b) We have proposed a trust utility function to incorporate the above social contextual impact factors to reflect participants' attributes in a social network. Via utility function, participants are allowed to place special constraints to each trust impact factor.

   (c) To extract a contextual subnetwork for the specific purpose of predicting the trust from a source participant to a target participant using latent factor-based prediction models, we have proposed two models named *BiNet* and *TrustNet*. In these two models, inspired by the ant colony foraging process [27, 47], we have designed a novel binary ant colony algorithm (NBACA) and a non-binary novel ant colony algorithm (NACA) for the subnetwork extraction problems respectively. In NBACA, an initialization process and a mutation process have been added and the path selection and pheromone update processes inherited from conventional BACA have been improved for the trust subnetwork extraction problem. In NACA, we have improved the path selection and pheromone update processes inherited from traditional ACA and added a mutation process that betters the performance of this algorithm. The experiments conducted on two popular social network datasets, Epinions and Slashdot, have demonstrated the superior performance of our proposed algorithms over the state-of-the-art approaches.

2. The second aspect of the work presented in this thesis is to predict trust values from the existing trust rating values using matrix factorization with regularization.

   (a) We have analyzed the properties which can be extracted from existing trust ratings including truster tendency, trustee tendency, propagated trust values, trust rating value similarity and trust rating distribution similarity.

   (b) We divide these properties into personal properties and interpersonal properties and utilize both of them in different ways. In order to reduce the negative effect of trust tendency, the personal properties (trust tendencies) have been used to decompose trust ratings into truster tendency, trustee tendency and tendency-reduced trust ratings. The interpersonal properties (propagated trust and similarities) have been incorporated into a propagation and similarity regularization term.

(c) Considering both propagated trust and similarity factors including the propagation and similarity regularization terms of matrix factorization, we have proposed a trust prediction model based on rating decomposition and matrix factorization to predict trust ratings from tendency-reduced ratings. Based on the commonly-used metrics of Mean Absolute Error and Root Mean Square Error, the experiments conducted on a real-world dataset have demonstrated significant improvements delivered by our model in trust prediction accuracy over the state-of-the-art approaches.

3. The third aspect of the work presented in this thesis is to predict trust values considering contextual information.

   (a) We have analyzed the social contexts in detail and proposed a new trust transference method to transfer trust from relevant interaction contexts into a target context, which reduces the sparsity of social contextual trust matrices.

   (b) We have proposed a context-aware trust prediction model based on matrix factorization to predict the trust from one participant to another regarding a specific target context in the contextual matrix processed by trust transference, which mitigates the traditional sparsity problem in the target context. This model is based on both propagated trust in the target context and similarity between participants, and does not rely on social paths. The conducted experiments have examined the model in three different typical situations, showing that our proposed transference method can transfer trust between contexts in a reasonable way, that the proposed prediction model can generate more reasonable trust values than the state-of-the-art method, and that our model is able to predict trust in the situation where is no trust path.

4. The last aspect of the work presented in this thesis is to predict future trust values in the dynamic online environments.

   (a) We have analyzed static and dynamic features that can be extracted from a seller's (or provider's) historical transactions and utilized to predict future trust. These features are selected, refined and projected using Mutual Information, Principle Component Analysis, and Vector Quantization respectively, producing the observation for HMM-based methods.

   (b) We have proposed an HMM-based dynamic trust prediction model to predict the trust value of a seller in the forthcoming transaction, in which both contextual information and transaction outcomes are incorporated into observations. The experiments conducted in two typical scenarios have demonstrated that our model is superior to existing models, and more effective in complex dynamic environments.

7.2 Future Work

We have completed a great deal of work in trust subnetwork extraction and trust prediction in different application situations, which provides critical technical foundations for a number of applications based on online social networks.

The following are some suggestions for future research in this direction. On one hand, the performance of social trust subnetwork extraction models can be further improved in terms of quality and efficiency by further optimizing our current extraction algorithms or proposing a new heuristic algorithm. In addition, trust subnetworks can also be extracted from the viewpoint of important links, or the mix with the current important nodes, to further improve the quality of extracted trust subnetwork.

On the other hand, as trust is dynamic and context sensitive, there is still room to study the factors that affect trust and the features that can be extracted from any information regarding trust. Then, a multi-dimensional context-aware trust prediction method can be proposed to model the changes of trust including conventional trust information, contextual information and time series, and to predict the future trust regarding specific context and time. In addition, this model includes suitable algorithms, such as tensor decomposition, and the study of efficient training methods.

Furthermore, based on the trust prediction model, a trust-oriented recommendation system can be developed taking full advantage of a social network with complex historical social contextual information. With the help of such a system, an employer is capable of finding the most trustworthy employees, a vendor can find loyal customers, a buyer can easily find the most trustworthy seller selling the product the buyer prefers, and many more similar cases can be imagined.

Appendix A

Notations Used in This Thesis

Table A.1: Notations used in Chapter 3

Notation	Representation	First occurrence
RIF	the role impact factor	Section 3.2.1
RLB	the reliability	Section 3.2.1
PS	the preference similarity	Section 3.2.1
SI	the social intimacy	Section 3.2.1
$T_{i,j}$	the trust of trustee j in truster i's mind	Section 3.2.1
u_i	a node utility	Section 3.2.1
F	a vector of all trust factors	Eq. 3.1
W	a coefficient vector given by users	Eq. 3.1
m	the number of nodes in a sub-network	Section 3.2.3
n	the number of nodes in a original network	Section 3.2.3
$G(X)$	the objective function	Eq. 3.3
X	the selected nodes	Eq. 3.3
x_i	a selected node	Eq. 3.3
$D(X)$	the density of current sub-network	Eq. 3.3
$\zeta \& \tilde{\zeta}$	the weights in Eq. 3.3	Eq. 3.3
x_s	the source node	Eq. 3.4
x_t	the target node	Eq. 3.4
K_t	a threshold value	Eq. 3.4
t	time	Section 3.4.1
$a[i,j]$	the path from knot i to $i+1$	Section 3.4.1
x_i^k	the node selected by ant k	Section 3.4.1
X^k	all the nodes selected by ant k	Section 3.4.1
$\tau_{ij}(t)$	the pheromone on path$a[i,j]$at time t	Section 3.4.1

Table A.2: Notations used in Chapter 3 (continued)

Notation	Representation	First occurrence
U	a set of node utilities	Section 3.4.1
χ_i	a random value	Eq. 3.5
η_i	the heuristic function	Eq. 3.5
$\varphi\&\psi$	the weights of $\chi_i\&\eta_i$ in Eq. 3.5	Eq. 3.5
$p_{ij}^k(t)$	the transition probability of ank k	Eq. 3.6
$\alpha\&\beta$	the weights of $\tau_{i1}(t)\&\eta_i$ in Eq. 3.6	Eq. 3.6
$1\{.\}$	a boolean function	Eq. 3.8
λ_i	a value from a uniform distribution	Eq. 3.8
$X_-^k\&X_+^k$	the solutions from mutation	Eq. 3.8&3.9
y	the number of ants	Section 3.4.5
X_{best}	the best-so-far solution	Section 3.4.5
X'_{best}	the best solution in the current iteration	Section 3.4.5
ρ	the pheromone evaporation rate	Eq. 3.10
ϱ	the pheromone increment rate	Eq. 3.11
NC	the number of iterations already run	Section 1
NF	the number of iterations where the best-so-far solution stayed the same	Section 1
$X^{(NC)}$	the solution set in an iteration	Section 1
NC_{max}	the maximum value of NC	Section 1
NF_{max}	the maximum value of NF	Section 1
$J_k(i)$	the set of available paths ant k can select at knot i	Eq. 3.12
$tabu_k$	the tabu recording all the paths ant k has gone through	Section 3.6.2
$tabu'_k$	the tabu recording all the paths selected but discarded	Section 3.6.2
L_k	the whole path passed by ant k	Eq. 3.13
L'_{best}	the best solution in the current iteration	Section 3.6.3
L_{best}	the best-so-far solution	Section 3.6.3
$\Delta\tau_{ij}$	the pheromone increment on path $a[i,j]$ in current generation	Eq. 3.16
$\Delta\tau_{ij}^k$	the pheromone on the path $a[i,j]$ left by ant k	Eq. 3.16
Q	a positive constant	Eq. 3.17
p'_i	the probability of node i to be removed	Section 3.6.4
AF	the number of times that adding a node cannot better the solution	Algorithm 3
AF_{max}	the maximum value of AF	Algorithm 3
MF	the count of mutation process	Algorithm 3
MF_{max}	the maximum value of MF	Algorithm 3
$J_k\&J'_k$	the set of available paths	Eq. 3.12

Table A.3: Notations used in both Chapter 4 and Chapter 5

Notation	Representation	First occurrence
R	a trust matrix	Section 4.2
l	the dimension of a joint latent factor space	Section 4.2
u_i	the truster vector	Section 4.2
v_j	the trustee vector	Section 4.2
$\mathbb{R}^l$	the joint latent factor space	Section 4.2
r_{ij}	the trust of trustee j in truster i's mind	Eq. 4.2
U	the truster-specific matrix	Section 4.2
V	the trustee-specific matrix	Section 4.2
$\|\|.\|\|_F^2$	the Frobenius norm	Eq. 4.3
I_{ij}	the indicator function of interaction trust	Eq. 4.4
λ_i	the coefficients of regularization terms	Eq. 4.5
TP	a trust property utility	Eq. 4.9
γ	the coefficient of our proposed regularization term	Eq. 4.10
$\mathcal{F}^+(i)$	the set of trustees with at least a link from truster i	Eq. 4.10

Table A.4: Notations used in Chapter 4

Notation	Representation	First occurrence
$\mathbb{R}^{l \times n}$	the joint latent factor space	Section 4.2
$T_u(i)$	truster tendency	Section 4.3.1
$T_v(i)$	trustee tendency	Section 4.3.1
$\hat{r}_{ij}$	a tendency reduced trust value	Section 4.3.1
α_i	coefficients in trust decomposition	Section 4.3.1
$infer(i,j)$	a propagated trust value	Section 4.3.1
H	the number of hops in propagation	Section 4.3.1
$vss(i,j)$	the Vector Space Similarity	Eq. 4.6
$pcc(i,j)$	the Pearson Correlation Coefficient	Eq. 4.7
$\mathfrak{q}(x)$	a normalization function $\mathfrak{q}(x) = (\mathfrak{p}(x) + 1)/2$	Section 4.3.1
$D_{KL}(i\|\|j)$	Kullback-Leibler (KL) -distance (Relative Entropy)	Eq. 4.8
$q(x)$	a projection function $q(x) = e^{-p(x)}$	Section 4.3.1
β_i	coefficients in Eq. 4.9	Eq. 4.9
$\mathcal{F}^-(i)$	the set of trusters with at least a link to trustee i	Eq. 4.13

Table A.5: Notations used in Chapter 5

Notation	Representation	First occurrence
c_i & c_j	a specific context	Section 5.1
p_k	a participant in a social network $k = x, y, 1, 2, ...$	Section 5.2
$RIF_{p_k}^{c_i}$	participant p_k's role impact factor in context c_i	Section 5.2.1
$RLB_{p_k}^{c_i}$	participant p_k's reliability in context c_i	Section 5.2.1
$PS_{p_x,p_y}^{c_i}$	the preference similarity between p_x and p_y in context c_i	Section 5.2.1
$SI_{p_x,p_y}^{c_i}$	the social intimacy between p_x and p_y in c_i in p_x's mind	Section 5.2.1
$T_{p_x,p_y}^{c_i}$	the trust p_x gives to p_y in context c_i	Section 5.2.1
CS^{c_i,c_j}	the similarity between two contexts c_i and c_j	Section 5.2.2
μ	a threshold value	Section 5.2.2
N_p	the number of participants	Section 5.2.3
N_c	the number of contexts	Section 5.2.3
$\alpha_{p_x,p_y}^{c_i,c_j}$	the transference degree of trust to p_y in p_x's mind from interaction context c_i to target context c_j	Eq. 5.1
ω_i	the weight of a property	Eq. 5.1
$BT_{p_x,p_y}^{c_j}$	the basic trust value	Eq. 5.2
δ_i	the coefficients in Eq. 5.2	Eq. 5.2
C	a set of contexts	Section 5.3.1
$\tilde{T}_{p_x,p_y}^{c_j}$	the transferred trust	Eq. 5.3
β_i	the coefficients in Eq. 5.3	Eq. 5.3
$\tilde{I}_{xy}$	the indicator function of transferred trust	Eq. 5.7
η	the coefficient controlling the weight of transferred trust	Eq. 5.7

Table A.6: Notations used in Chapter 6

Notation	Representation	First occurrence
k	the number of stationary processes	Section 6.1
Ω	potential features	Section 6.2.2
w_r	an exact features	Section 6.2.2
Θ	a seller's past transaction list	Section 6.2.2
θ^i	a past transaction	Section 6.2.2
L	a set of transaction outcomes/ratings	Section 6.2.2
l_i	a transaction outcome/rating	Section 6.2.2
P	the probability distribution of L	Section 6.2.2
p_i	the probability distribution of l_i	Section 6.2.2
$H_P(\Theta)$	the entropy of Θ	Section 6.2.2
$\Upsilon(w_r)$	the value set of w_r	Section 6.2.2
v	a value in $\Upsilon(w_r)$	Section 6.2.2
Θ^v	all the past transactions with v for w_r	Section 6.2.2
$I_p(\Theta; w_r)$	the mutual entropy	Section 6.2.2
E_i	a key feature vector	Section 6.2.3
$\mathbb{E}_i$	a full feature vector $\mathbb{E}_i = [E_i, l_i]$	Section 6.2.3
$\mathbb{E}$	the set of all feature vectors	Section 6.2.4
R_j	a distinct region	Section 6.2.4
M	the number of distinct observation symbols	Section 6.2.4
v_j	a code vector	Section 6.2.4
V	the feature set $V = \{v_1, v_2, ..., v_M\}$	Section 6.3.1
T	the number of observations	Section 6.3.1
O	a sequential observation set	Section 6.3.1
o_i	an observation $o_i \in V, i = 1, ..., T$	Section 6.3.1
Q	a sequential state set inferred from observations	Section 6.3.1
q_i	a state in $q_i \in S, i = 1, ..., T$	Section 6.3.1
S	the unique state set	Section 6.3.1
s_i	a unique state $i = 1, ..., N$	Section 6.3.1
N	the number of distinct states in a model	Section 6.3.1
λ	the presentation of an HMM $\lambda = (V, S, A, B, \pi)$	Section 6.3.1
A	the state transition probability distribution	Section 6.3.1
a_{ij}	$a_{ij} = P(q_{t+1} = S_j \| q_t = S_i)$, $1 \leq i, j \leq N, 1 \leq t \leq T$	Section 6.3.1

Table A.7: Notations used in Chapter 6 (continued)

Notation	Representation	First occurrence
B	the emission probability distribution	Section 6.3.1
$b_j(k)$	$b_j(k) = P(v_k@t\|q_t = S_j), 1 \leq j \leq N,$ $1 \leq k \leq M, 1 \leq t \leq T$	Section 6.3.1
π	the initial state distribution	Section 6.3.1
π_i	$\pi_i = P(q_1 = s_i), 1 \leq i \leq N$	Section 6.3.1
t	the time	Section 6.3.1
$O_{1:T}$	the observations in the first T transactions	Section 6.3.2
$Q_{1:T}$	the states emitting the first T transactions	Section 6.3.2
$P(O\|\lambda)$	the probability of the observation sequence given the model λ	Section 6.3.2
$P(Q_{1:T}\|\lambda)$	the probability of the state sequence $Q_{1:T}$ given the model λ	Section 6.3.2
$P(O_{1:T}\|Q_{1:T}, \lambda)$	the probability of the observation sequence $O_{1:T}$ for the state sequence of $Q_{1:T}$ given the model λ	Section 6.3.2
$\alpha_t(i)$	the probability of the partial observation sequence $o_1, o_2, ..., o_t$ and state s_i at time t, given the model λ	Section 6.3.2
$\beta_t(i)$	the probability of the partial observation sequence from $t + 1$ to the end, given state s_i at time t, and the model λ	Section 6.3.3
$\gamma_t(i)$	the probability of being in state s_i at time t, given observation sequence O and the model λ	Section 6.3.3
$\xi_t(i, j)$	the probability of being in state s_i at time t and state s_j at time $t + 1$	Section 6.3.3
$\bar{\pi}$	the expected frequency in state s_i at time $t = 1$	Section 6.3.3
$\bar{a}_{ij}$	the ratio of the expected number of transitions from state s_i to state s_j to the expected number of transitions from state s_j	Section 6.3.3
$\bar{b}_j(k)$	the ratio of the expected number of times in state j and observation symbol v_k to the expected number of times in state j	Section 6.3.3

Bibliography

[1] http://konect.uni-koblenz.de/networks/advogato.

[2] http://www.businessnewsdaily.com.

[3] http://www.socialcommercetoday.com.

[4] H. Abdi and L. J. Williams. Principal component analysis. *Wiley Interdisciplinary Reviews: Computational Statistics*, 2:433–459, 2010.

[5] A. Abdul-Rahman and S. Hailes. Supporting trust in virtual communities. In *Hawaii International Conference on System Sciences*, pages 1–9, 2000.

[6] L. A. Adamic, R. M. Lukose, and B. A. Huberman. Local search in unstructured networks. In *Handbook of Graphs and Networks*. Wiley, 2005.

[7] P. S. Adler. Market, hierarchy, and trust: The knowledge economy and the future of capitalism. *Organization Science*, 12(2):215–234, 2001.

[8] Y.-Y. Ahn, S. Han, H. Kwak, S. Moon, and H. Jeong. Analysis of topological characteristics of huge online social networking services. In *Proceedings of the 16th International Conference on World Wide Web*, pages 835–844, 2007.

[9] G. A. Akerlof. The market for "lemons": Quality uncertainty and the market mechanism. *The Quarterly Journal of Economics*, 84(3):488–500, 1970.

[10] L. A. Amaral, A. Scala, M. Barthelemy, and H. E. Stanley. Classes of small-world networks. *Proceedings of the National Academy of Sciences of the United States of America*, 97(21):11149–11152, 2000.

[11] S. S. Andeleeb. An experimental investigation of satisfaction and commitment in marketing channels: The role of trust and dependence. *Journal of Retailing*, 72(1):77–93, 1996.

[12] J. R. Anderson, D. Bothell, M. D. Byrne, S. Douglass, C. Lebiere, and Y. Qin. An integrated theory of the mind. *Psychological Review*, 111:1036–1060, 2004.

[13] D. Artz and Y. Gil. A survey of trust in computer science and the semantic web. *Journal of Web Semantics: Science, Services and Agents on the World Wide Web*, 5(2):58–71, 2007.

[14] R. Ashri, S. Ramchurn, J. Sabater, M. Luck, and N. Jennings. Trust evaluation through relationship analysis. In *Proceedings of the 4th International Joint Conference on Autonomous Agents and Multi-Agent Systems (AAMAS)*, pages 1005–1011, 2005.

[15] A. Azadeh, R. Kokabi, M. Saberi, F. K. Hussain, and O. K. Hussain. Trust prediction using z-numbers and artificial neural networks. In *IEEE International Conference on Fuzzy Systems*, pages 522–528, Beijing, China, 2014.

[16] S. Ba and P. A. Pavlou. Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior. *MIS Quarterly*, 26(3):243–268, 2002.

[17] S. Baase and A. V. Gelder. *Computer Algorithms: Introduction to Design and Analysis*. Addison-Wesley Publishing Company, 3rd edition, 1998.

[18] A.-L. Barabasi and R. Albert. Emergence of scaling in random networks. *Science*, 286(5439):509–512, 1999.

[19] B. Barber. *The Logic and Limits of Trust*. Rutgers University Press, 1983.

[20] E. Barnett and M. Casper. A definition of “social environment”. *American Journal of Public Health*, 91(3), 2001.

[21] L. E. Baum and J. A. Eagon. An inequality with applications to statistical estimation for probabilistic functions of Markov processes and to a model for ecology. *Bulletin of the American Mathematical Society*, 73:360–363, 1967.

[22] P. Beatty, I. Reay, S. Dick, and J. Miller. Consumer trust in e-commerce web sites: A meta-study. *ACM Computing Surveys*, 43(3):1–46, 2011.

[23] P. Bedi, H. Kaur, and S. Marwaha. Trust based recommender system for the semantic web. In *Proceedings of the 20th International Joint Conference on Artifical Intelligence (IJCAI)*, pages 2677–2682, San Francisco, CA, USA, 2007.

[24] E. Berscheid and H. T. Reis. Attraction and close relationships. *The Handbook of Social Psychology*, 2:193–281, 1998.

[25] H. Billhardt, R. Hermoso, S. Ossowski, and R. Centeno. Trust-based service provider selection in open environments. In *Proceedings of the ACM Symposium on Applied Computing*, pages 1375–1380, 2007.

[26] P. Blau. A theory of social integration. *American Journal of Sociology*, 65(6):545–556, 1960.

[27] C. Blum. Ant colony optimization: Introduction and recent trends. *Physics of Life Reviews*, 2(4):353–373, 2005.

[28] P. Bonatti, C. Duma, D. Olmedilla, and N. Shahmehri. An integration of reputation-based and policy-based trust management. In *Proceedings of the Semantic Web Policy Workshop*, 2005.

[29] D. Boyd and N. Ellison. Social network sites: Definition, history and scholarship. *Journal of Computer-Mediated Communication*, 13(1), 2007.

[30] J. L. Braddach and R. G. Eccles. Price, authority, and trust: From ideal types to plural forms. *Annual Review of Sociology*, 15:97–118, 1989.

[31] D. J. Brass. *A social Network Perspective on Industrial Organizational Psychology*. Industraial/Organizational Handbook, 2009.

[32] J. S. Breese, D. Heckerman, and C. Kadie. Empirical analysis of predictive algorithms for collaborative filtering. In *Proceedings of the 14th Conference on Uncertainty in Artificial Intelligence*, pages 43–52, 1998.

[33] S. Brehm. *Intimate Relationships*. Random House, 1985.

[34] J. Brockner, P. A. Siegel, J. P. Tyler, and C. Martin. When trust matters: The moderating effect of outcome favorability. *Administrative Science Quarterly*, 43:558–583, 1997.

[35] N. Chang and M. Liu. Revisiting the ttl-based controlled flooding search: Optimality and randomization. In *Proceedings of the 10th Annual International Conference on Mobile Computing and Networking*, pages 85–99, 2004.

[36] V. A. Chanley, T. J. Rudolph, and W. M. Rahn. The origins and consequences of public trust in government: A time series analysis. *Public Opinion Quarterly*, 64(3):239–256, 2000.

[37] Y.-S. Cho, G. V. Steeg, and A. Galstyan. Co-evolution of selection and influence in social networks. In *25th Conference on Artificial Intelligence (AAAI)*, 2011.

[38] S. Chow and R. Holden. Toward and understanding of loyalty: The moderating role of trust. *Journal of Managerial*, 43:558–583, 1997.

[39] B. Christianson and W. S. Harbison. Why isn't trust transitive? In *International Workshop on Security Protocols*, pages 171–176, 1996.

[40] K. Cook. *Trust in Society*. New York: Russell Sage Foundation, 2001.

[41] P. Cui, F. Wang, S. Yang, and L. Sun. Item-level social influence prediction with probabilistic hybrid factor matrix factorization. In *25th Conference on Artificial Intelligence (AAAI)*, 2011.

[42] M. Dalton. *Men Who Manage*. New York: Wiley, 1959.

[43] R. J. Deluga. The relation between trust in the supervisor and subordinate organizational citizenship behavior. *Military Psychology*, 7(1):1–16, 1995.

[44] M. Deutsch. Cooperation and trust: Some theoretical notes. In *Nebraska Symposium on Motivation*. Nebraska University Press, 1962.

[45] A. K. Dey, G. D. Abowd, and D. Salber. A conceptual framework and a toolkit for supporting the rapid prototyping of context-aware applications. *Human-Computer Interaction*, 16(3):97–166, 2001.

[46] M. Dodgeson. Learning, trust, and technological collaboration. *Human Relations*, 46(1):77–95, 1993.

[47] M. Dorigo. *Optimization, Learning and Natural Algorithms*. PhD thesis, Politecnico di Milano, 1992.

[48] S. Dorri Nogoorani and R. Jalili. Uncertainty in probabilistic trust models. In *IEEE 26th International Conference on Advanced Information Networking and Applications (AINA)*, pages 511–517, 2012.

[49] D. M. Dunlavy, T. G. Kolda, and E. Acar. Temporal link prediction using matrix and tensor factorizations. *ACM Transactions on Knowledge Discovery from Data*, 5(2):10:1–10:27, 2011.

[50] E. Durkheim. *The Division of Labor in Society*. New York: Free Press, 1893.

[51] B. Elizabeth, R. Aaishwarya, P. Kiruthika, M. Shrada, A. Prakash, and V. Uthariaraj. Bayesian based confidence model for trust inference in MANETs. In *International Conference on Recent Trends in Information Technology (ICRTIT)*, pages 402 –406, 2011.

[52] E. ElSalamouny, V. Sassone, and M. Nielsen. HMM-based trust model. In *International Workshop on Formal Aspects in Security and Trust (FAST)*, volume 5983 of *LNCS*, pages 21–35. Springer, 2009.

[53] T. Ferdinand. *Community and Society*. Michigan State University Press, 1887.

[54] I. Filali and F. Huet. Dynamic ttl-based search in unstructured peer-to-peer networks. In *Cluster, Cloud and Grid Computing (CCGrid)*, pages 438–447, 2000.

[55] S. Fiske. *Social Beings: Core Motives in Social Psychology*. John Wiley & Sons, 2009.

[56] N. E. Friedkin. *A Structrual Theory of Social Influence*. Cambridge University Press, 1988.

[57] F. Fukuyama. *Trust: The Social Virtues and The Creation of Prosperity*. New York: Free Press, 1996.

[58] F. Fukuyama. *The Moral Foundations of Trust*. Cambridge University Press, 2002.

[59] A. Giddens. *The Constitution of Society: Outline of the Theory of Structuration*. Polity Press, 1984.

[60] D. T. Gilbert, S. T. Fiske, and G. Lindzey. *The handbook of social psychology*. Oxford University Press, 1998.

[61] J. Gimpel, K. Karnes, J. Mctague, and S. Pearson-Merkowitz. Distance-decay in the political geography of friends-and-neighbors voting. *Political Geography*, 27:231–252, 2008.

[62] C. Gkantsidis, M. Mihail, and A. Saberi. Random walks in peer-to-peer networks. In *23rd Annual Joint Conference of the IEEE Computer and Communications Societies*, pages 120–130, 2004.

[63] C. Gkantsidis, M. Mihall, and A. Saberi. Random walks in peer-to-peer networks: algorithm and evaluation. *Performance Evaluation*, 63(3):241–263, 2006.

[64] J. Golbeck. Web-based social networks: A survey and future directions. Technical report, University of Maryland, 2005.

[65] J. Golbeck and J. Hendler. Inferring trust relationships in web-based social networks. Technical report, University of Maryland, 2006.

[66] J. Golbeck and J. A. Hendler. Inferring binary trust relationships in web-based social networks. *ACM Transactions on Internet Technology*, 6(4):497–529, 2006.

[67] T. Grandison and M. Sloman. A survey of trust in internet applications. *IEEE Communications Surveys & Tutorials*, 3(4):2–16, 2000.

[68] E. Gray, J. Seigneur, Y. Chen, and C. Jensen. Trust propagation in small world. In P. Nixon and S. Terzis, editors, *Proceedings of the 1st International Conference on Trust Management*, volume 2692 of *LNCS*, pages 239–254. Springer-Verlag, 2003.

[69] R. Guha, R. Kumar, P. Raghavan, and A. Tomkins. Propagation of trust and distrust. In *Proceedings of the 13th International Conference on World Wide Web (WWW)*, pages 403–412, 2004.

[70] S. Guo, M. Wang, and J. Leskovec. The role of social networks in online shopping: information passing, price of trust, and consumer choice. In *ACM Conference on Electronic Commerce*, pages 157–166, 2011.

[71] C.-W. Hang, Y. Wang, and M. P. Singh. Operators for propagating trust and their evaluation in social networks. In *Proceedings of the 8th International Conference on Autonomous Agents and Multiagent Systems (AAMAS)*, pages 1025–1032, 2009.

[72] R. Hardin. *Trust and Trustworthiness*. Russell Sage Foundation, 2002.

[73] P. Hintsanen, H. Toivonen, and P. Sevon. Fast discovery of reliable subnetworks. *IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, pages 104–111, 2010.

[74] P. W. Holland and S. Leinhardt. Transitivity in structural models of small groups. *Comparative Group Studies*, 2:107–124, 1971.

[75] P. Holme, C. R. Edling, and F. Liljeros. Structure and time evolution of an internet dating community. *Social Networks*, 26(2):155 – 174, 2004.

[76] L. Hong, A. S. Doumith, and B. D. Davison. Co-factorization machines: modeling user interests and predicting individual decisions in twitter. In *6th ACM International Conference on Web Search and Data Mining*, pages 557–566, Rome, Italy, 2013.

[77] J. Huang and X. Hu. Information passing in online recommendation. In *Proceedings of the 1st Workshop on User Engagement Optimization (UEO)*, pages 3–6. ACM, 2013.

[78] J. Huang, F. Nie, H. Huang, Y. Lei, and C. Ding. Social trust prediction using rank-k matrix recovery. In *Proceedings of the 23rd International Joint Conference on Artificial Intelligence (IJCAI)*, pages 2647–2653, 2013.

[79] M. Jamali and M. Ester. A matrix factorization technique with trust propagation for recommendation in social networks. In *Proceedings of the 2010 ACM Conference on Recommender Systems*, pages 135–142, Barcelona, Spain, 2010.

[80] S. Jang, J. Roh, W. Kim, T. Sherpa, J. Kim, and J. Park. A novel binary ant colony optimization: Application to the unit commitment problem of power systems. *Journal of Electrical Engineering & Technology*, 6(2):174 181, 2011.

[81] D. Jia, F. Zhang, and S. Liu. A robust collaborative filtering recommendation algorithm based on multidimensional trust model. *Journal of Software*, 8(1):11–18, 2013.

[82] A. Jøsang and R. Ismail. The beta reputation system. In *Proceedings of the 15th Bled Conference on Electronic Commerce*, 2002.

[83] S. Jones. TRUST-EC*: requirements for trust and confidence in e-commerce*. European Commission, Joint Research Center, 1999.

[84] A. Jøsang. Artificial reasoning with subjective logic. *Australian Workshop on Commonsense Reasoning*, 1997.

[85] A. Jøsang. A logic for uncertain probabilities. *Uncertainty, Fuzziness and Knowledge-Based Systems*, 9(3):279–212, 2001.

[86] A. Jøsang, E. Gray, and M. Kinateder. Simplification and analysis of transitive trust networks. *Web Intelligence and Agent Systems*, 4(2):139–161, 2006.

[87] A. Jøsang, R. Ismail, and C. Boyd. A survey of trust and reputation systems for online service provision. *Decision Support Systems*, 43(2):618–644, 2007.

[88] A. Jøsang and S. Pope. Semantic constraints for trust transitivity. In *Proceedings of the 2nd Asia-Pacific Conference on Conceptual Modelling (APCCM)*, pages 59–68, 2005.

[89] H. J. Jung. Quality assurance in crowdsourcing via matrix factorization based task routing. In *Proceedings of the Companion Publication of the 23rd International Conference on World Wide Web Companion*, pages 3–8, 2014.

[90] S. Kamvar, M. Schlosser, and H. Garcia-Molina. The eigentrust algorithm for reputation management in p2p networks. In *Proceedings of the 12th International Conference on World Wide Web (WWW)*, pages 640–651, 2003.

[91] B. Klimt and Y. Yang. Introducing the Enron Corpus. In *1st Conference on Email and Anti-Spam (CEAS)*, 2004.

[92] D. Koller and N. Friedman. *Probabilistic Graphical Models: Principles and Techniques*. MIT Press, 2009.

[93] M. Kong, P. Tian, and Y. Kao. A new ant colony optimization algorithm for the multidimensional knapsack problem. *Computer and Operations*, 35:2672–2683, 2008.

[94] M. A. Konovsky and S. D. Pugh. Citizenship behavior and social exchange. *Academy of Management Journal*, 37(3):656–669, 1994.

[95] K. Konrad, G. Fuchs, and J. Bathel. Trust and electronic commerce more than a technical problem. In *18th Symposium on Reliable Distributed Systems*, 1999.

[96] Y. Koren, R. Bell, and C. Volinsky. Matrix factorization techniques for recommender systems. *Computer*, 42(8):30–37, 2009.

[97] R. F. Korte. Biases in decision making and implications for human resource development. *Advances in Developing Human Resources*, 5(4):440–457, 2003.

[98] U. Kuter and J. Golbeck. Sunny: A new algorithm for trust inference in social networks using probabilistic confidence models. In *22nd Conference on Artificial Intelligence (AAAI)*, pages 1377–1382, 2007.

[99] M. Lesani and S. Bagheri. Applying and inferring fuzzy trust in semantic web social networks. In *Canadian Semantic Web Working Symposium*, pages 23–43, 2006.

[100] M. Lesani, S. Bagheri, and H. Abolhassani. Fuzzy trust and combining information, a blueprint for the semantic web trust layer. In *Joint 3rd International Conference on Soft Computing and Intelligent Systems and 7th International Symposium on advanced Intelligent Systems (SCIS & ISIS)*, Tokyo, Japan, 2006.

[101] M. Lesani and N. Montazeri. Fuzzy trust aggregation and personalized trust inference in virtual social networks. *Computational Intelligence*, 25(2):51–83, 2009.

[102] J. Leskovec, L. A. Adamic, and B. A. Huberman. The dynamics of viral marketing. In *Proceedings of the 7th ACM conference on Electronic commerce*, pages 228–237, 2006.

[103] J. Leskovec, D. Huttenlocher, and J. Kleinberg. Signed networks in social media. In *28th ACM Conference on Human Factors in Computing Systems (CHI)*, pages 1361–1370, 2010.

[104] M. Levi and L. Stoker. Policial trust and trustworthiness. *Annual Review of Political Science*, 3:475–507, 2000.

[105] C. Levi-Strauss. *The Elementary Structures of Kinship*. Beacon Press, 1947.

[106] L. Li, D. Alderson, J. Doyle, and W. Willinger. Towards a theory of scale-free graphs: Definition, properties, and implications. *Internet Mathematics*, 2(4):431–523, 2005.

[107] L. Li and Y. Wang. A trust vector approach to service-oriented applications. In *IEEE International Conference on Web Services (ICWS)*, pages 270–277, 2008.

[108] L. Li and Y. Wang. Context based trust normalization in service-oriented environments. In *IEEE International Conference on Autonomic and Trusted Computing*, pages 122–138, 2010.

[109] L. Li and Y. Wang. Subjective trust inference in composite services. In *24th AAAI Conference on Artificial Intelligence*, pages 1377–1384, 2010.

[110] L. Li, Y. Wang, and E.-P. Lim. Trust-oriented composite services selection and discovery. In *ICSOC/ServiceWave*, pages 50–67, 2009.

[111] S. Lichtenstein and P. Slovic. *The Construction of Preference*. Cambridge University Press, 2006.

[112] J. Lin, Z. Li, D. Wang, K. Salamatian, and G. Xie. Analysis and comparison of interaction patterns in online social network and social media. In *21st International Conference on Computer Communications and Networks*, pages 1 –7, 2012.

[113] G. Liu. *Trust Management in Online Socal Networks*. PhD thesis, Macquarie University, 2013.

[114] G. Liu, Y. Wang, and M. Orgun. Trust inference in complex trust-oriented social networks. In *International Conference on Computational Science and Engineering (CSE)*, pages 996–1001, 2009.

[115] G. Liu, Y. Wang, and M. Orgun. Finding k optimal social trust paths for the selection of trustworthy service providers in complex social networks. In *IEEE International Conference on Web Services (ICWS)*, pages 41–48, 2011.

[116] G. Liu, Y. Wang, and M. A. Orgun. Optimal social trust path selection in complex social networks. In *24th AAAI Conference on Artificial Intelligence*, pages 1391–1398, 2010.

[117] G. Liu, Y. Wang, and M. A. Orgun. Social context-aware trust network discovery in complex contextual social networks. In *26th Conference on Artificial Intelligence (AAAI)*, pages 101–107, 2012.

[118] G. Liu, Y. Wang, M. A. Orgun, and E.-P. Lim. A heuristic algorithm for trust-oriented service provider selection in complex social networks. In *IEEE International Conference on Services Computing (SCC)*, pages 130–137, 2010.

[119] G. Liu, Y. Wang, M. A. Orgun, and E.-P. Lim. Finding the optimal social trust path for the selection of trustworthy service providers in complex social networks. *IEEE Transactions on Services Computing*, 6(2):152–167, 2013.

[120] G. Liu, Y. Wang, M. A. Orgun, and H. Liu. Discovering trust networks for the selection of trustworthy service providers in complex contextual social networks. In *IEEE International Conference on Web Services (ICWS)*, pages 384–391, 2012.

[121] J. Liu and V. Issarny. Enhanced reputation mechanism for mobile Ad Hoc networks. In *International Conference on Trust Management*, pages 48–62, 2004.

[122] X. Liu. Towards context-aware social recommendation via trust networks. In *14th International Conference on Web Information System Engineering (WISE)*, volume 8180 of *Lecture Notes in Computer Science*, pages 121–134. Springer, 2013.

[123] X. Liu and K. Aberer. Soco: a social network aided context-aware recommender system. In *Proceedings of the 22nd International Conference on World Wide Web (WWW)*, pages 781–802, 2013.

[124] X. Liu and A. Datta. Modeling context aware dynamic trust using hidden markov model. In *26th Conference on Artificial Intelligence (AAAI)*, 2012.

[125] B. Loni, Y. Shi, M. Larson, and A. Hanjalic. Cross-domain collaborative filtering with factorization machines. In *Advances in Information Retrieval - 36th European Conference on IR Research*, pages 656–661, Amsterdam, The Netherlands, 2014.

[126] N. Luhmann. *Trust and power*. Chichester: Wiley, 1979.

[127] H. Ma, I. King, and M. R. Lyu. Learning to recommend with social trust ensemble. In *Proceedings of the 32nd Annual International ACM SIGIR Conference on Research and Development in Information Retrieval*, pages 203–210, Boston, MA, USA, 2009.

[128] H. Ma, I. King, and M. R. Lyu. Learning to recommend with explicit and implicit social relations. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 2(3):1–19, 2011.

[129] H. Ma, M. R. Lyu, and I. King. Learning to recommend with trust and distrust relationships. In *Proceedings of the 2009 ACM Conference on Recommender Systems*, pages 189–196, New York, NY, US, 2009.

[130] H. Ma, H. Yang, M. R. Lyu, and I. King. Sorec: social recommendation using probabilistic matrix factorization. In *Proceedings of the 17th ACM Conference on Information and Knowledge Management*, pages 931–940, Napa Valley, California, USA, 2008.

[131] H. Ma, D. Zhou, C. Liu, M. R. Lyu, and I. King. Recommender systems with social regularization. In *Proceedings of the 4th ACM International Conference on Web Search and Data Mining (WSDM)*, pages 287–296, 2011.

[132] H. Ma, T. C. Zhou, M. R. Lyu, and I. King. Improving recommender systems by incorporating social contextual information. *ACM Transactions on Information Systems*, 29(2):9:1–9:23, 2011.

[133] Z. Malik, I. Akbar, and A. Bouguettaya. Web services reputation assessment using a hidden markov model. In *ICSOC/ServiceWave*, pages 576–591, 2009.

[134] Z. Malik and A. Bouguettaya. RATEWeb: Reputation assessment for trust establishment among web services. *Very Large Databases*, 18(4):885–911, 2009.

[135] B. Malinowski. *The Family Among the Australian Aborigines: A Sociological Study*. University of London Press, 1913.

[136] R. Mansell and B. Collins. *Trust and crime in information societies*. Edward Elgar Publishing, 2005.

[137] R. Marchany and J. Tront. E-commerce security issues. In *Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS)*, pages 2500 – 2508, 2002.

[138] I. Markova, A. Gillespie, and J. Valsiner. *Trust and Distrust: Sociocultural Perspectives*. Information Age Publishing, 2008.

[139] S. P. Marsh. *Formalising Trust as a Computational Concept*. PhD thesis, University of Stirling, 1994.

[140] D. J. McAllister. Affect- and cognition-based trust as foundations for interpersonal cooperation in organizations. *Academy of Management Journal*, 38:24–59, 1995.

[141] A. McCallum, X. Wang, and A. Corrada-Emmanuel. Topic and role discovery in social networks with experiments on enron and academic email. *Journal of Artificial Intelligence Research*, 30(1):249–272, 2007.

[142] I. H. McKnight and N. L. Chervany. *The meanings of trust*. Technical Report, 1996.

[143] M. Mcpherson, L. Smith-Lovin, and J. M. Cook. Birds of a feather: Homophily in social networks. *Annual Review of Sociology*, 27:415–444, 2001.

[144] A. K. Menon and C. Elkan. Link prediction via matrix factorization. In *Machine Learning and Knowledge Discovery in Databases*, pages 437–452, Athens, Greece, 2011.

[145] S. Milgram. The small world problem. *Psychology Today*, 67(1):61–67, 1967.

[146] A. Mislove, M. Marcon, K. Gummadi, P. Druschel, and B. Bhattacharjee. Measurement and analysis of online social networks. In *Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement*, pages 29–42, 2007.

[147] B. Misztal. *Trust in Modern Societies: The Search for the Bases of Social Order*. Polity, 1996.

[148] M. Mitchell. *An Introduction to Genetic Algorithms*. MIT Press, 1998.

[149] M. E. G. Moe, B. E. Helvik, and S. J. Knapskog. TSR: trust-based secure manet routing using hmms. In *Proceedings of the 4th ACM Symposium on QoS and Security for Wireless and Mobile Networks*, pages 83–90, 2008.

[150] L. Mui. *Computational Models of Trust and Reputation: Agents, Evolutionary Games, and Social Networks*. PhD thesis, Massachusetts Institute of Technology, 2002.

[151] A. K. Munns. Potential influence of trust on the successful completion of a project. *International Journal of Project Management*, 13:19–24, 1995.

[152] M. E. J. Newman. Mixing patterns in networks. *Physical Review E*, 67(2), 2003.

[153] J. Noel, S. Sanner, K. Tran, P. Christen, L. Xie, E. V. Bonilla, E. Abbasnejad, and N. D. Penna. New objective functions for social collaborative filtering. In *Proceedings of the 21st International Conference on World Wide Web (WWW)*, pages 859–868, Lyon, France, 2012.

[154] K. O'Hara and W. Hutton. *Trust: From Socrates to Spin*. Icon Books, 2004.

[155] C. D. Parks, R. F. Henager, and S. D. Scamahorn. Trust and reactions to messages of intent in social dilemmas. *Journal of Conflict Resolution*, 40(1):134–151, 1996.

[156] T. Parsons. *The Structure of Social Action: A Study in Social Theory with Special Reference to a Group of European Writers*. New York: Free Press, 1937.

[157] I. Pool and M. Kochen. Contacts and influence. *Social Networks*, 1:1–48, 1978.

[158] D. Povey. Trust management. In *http://security.dstc.edu.au/presentations/trust/*, 1999.

[159] C. L. Prell. Community networking and social capital: Early investigation. *Journal of Computer Mediated Communication*, 8(3), 2003.

[160] L. Rabiner. A tutorial on hidden markov models and selected applications in speech recognition. *Proceedings of the IEEE*, 77(2):257 –286, 1989.

[161] A. R. Radcliffe-Brown. On social structure. *Journal of the Royal Anthropological Institute*, 70:1–2, 1940.

[162] B. Randell. Dependable pervasive systems. In *23rd International Symposium on Reliable Distributed Systems*, Florianpolis, Brazil, 2004.

[163] M. Rehak, M. Pechoucek, and J. M. Bradshaw. Representing context for multiagent trust modeling. In *IEEE/WIC/ACM International Conference on Intelligent Agent Technology*, pages 737–746, 2006.

[164] S. Rendle. Factorization machines with libfm. *ACM Transactions on Intelligent Systems and Technology*, 3(3):57:1–57:22, 2012.

[165] A. Rettinger, M. Nickles, and V. Tresp. Statistical relational learning of trust. *Machine Learning*, 82(2):191–209, 2011.

[166] G. A. Rich. The sales manager as a role model: Effects on trust, job satisfaction, and performance of salespeople. *Journal of the Academy of Marketing Science*, 25(4):319–328, 1997.

[167] M. Richardson, R. Agrawal, and P. Domingos. Trust management for the semantic web. In *International Semantic Web Conference*, pages 351–368, 2003.

[168] J. Riegelsberger, M. A. Sasse, and J. D. Mccarthy. Shiny happy people building trust? photos on e-commerce websites and consumer trust. In *Proceedings of*

the SIGCHI Conference on Human Factors in Computing Systems, pages 121–128, 2003.

[169] P. S. Ring and A. Van. Developmental processes of cooperative interorganizational relationships. *Academy of Management Review*, 19:90–118, 1994.

[170] J. B. Rotter. A new scale for the measurement of interpersonal trust. *Personality*, 35(4):651–665, 1967.

[171] D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer. Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, 23(3):393–404, 1998.

[172] J. Sabater and C. Sierra. REGRET: reputation in gregarious societies. In *Proceedings of the 5th International Conference on Autonomous Agents*, pages 194–195, 2001.

[173] R. Salakhutdinov and A. Mnih. Bayesian probabilistic matrix factorization using markov chain monte carlo. In *Proceedings of the 25th International Conference on Machine Learning*, pages 880–887, 2008.

[174] R. Salakhutdinov and A. Mnih. Probabilistic matrix factorization. In *Advances in Neural Information Processing Systems*, pages 1–8, 2008.

[175] J. Scott and P. J. Carrington. *The SAGE Handbook of Social Network Analysis*. Sage Publications, 2011.

[176] J. P. Scott. *Social Network Analysis: A Handbook*. Sage Publications, 2nd edition, 2000.

[177] J. R. Searle. *The Construction of Social Reality*. New York: Free Press, 1995.

[178] A. B. Seligman. *The Problem of Trust*. Princeton University Press, 2000.

[179] D. L. Shapiro, B. H. Sheppard, and L. Cheraskin. Business on a handshake. *Negotiation*, 8(4):365–377, 1992.

[180] W. Sherchan, S. Nepal, and C. Paris. A survey of trust in social networks. *ACM Computing Surveys*, 45(47):47:1–47:33, 2013.

[181] Z. Shi, J. Liu, and Z. Wang. Dynamic p2p trust model based on time-window feedback mechanism. *Journal on Communications*, 31(2):120–129, 2010.

[182] M. Siegrist. The influence of trust and perceptions of risks andbenefits on the acceptance of gene technology. *Risk Analysis*, 20(2):195–203, 2000.

[183] S. Spitz and Y. Tuchelmann. A trust model considering the aspects of time. In *International Conference on Computer and Electrical Engineering*, pages 550–554, 2009.

[184] P. Stern and F. H.V. *Understanding Risk: Informing Decisions in a Democratic Society*. National Academies Press, 1996.

[185] J. E. Swan, M. R. Bowers, and L. D. Richardson. Customer trust in the salesperson: An integrative review and meta-analysis of the empirical literature. *Journal of Business Research*, 44(2):93–107, 1999.

[186] P. Symeonidis, E. Tiakas, and Y. Manolopoulos. Product recommendation and rating prediction based on multi-modal social networks. In *Proceedings of the 2011 ACM Conference on Recommender Systems*, pages 61–68, Chicago, IL, USA, 2011.

[187] P. Sztompka. *Trust: A Sociological Theory*. Cambridge University Press, 1999.

[188] M. Taherian, M. Amini, and R. Jalili. Trust inference in web-based social networks using resistive networks. In *3d International Conference on Internet and Web Applications and Services (ICIW)*, pages 233–238, 2008.

[189] J. Tang, H. Gao, and H. Liu. mtrust: discerning multi-faceted trust in a connected world. In *5th ACM International Conference on Web Search and Data Mining (WSDM)*, pages 93–102. ACM, 2012.

[190] J. Tang, H. Gao, H. Liu, and A. Das Sarma. etrust: understanding trust evolution in an online world. In *Proceedings of the 18th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pages 253–261, 2012.

[191] J. Tang, X. Hu, H. Gao, and H. Liu. Exploiting local and global social context for recommendation. In *Proceedings of the 23rd International Joint Conference on Artificial Intelligence*, Beijing, China, 2013.

[192] J. Tang, X. Hu, and H. Liu. Social recommendation: a review. *Journal of Social Network Analysis and Mining*, 3(4):1113–1133, 2013.

[193] J. Tang, J. Zhang, L. Yao, J. Li, L. Zhang, and Z. Su. Arnetminer: Extraction and mining of academic social networks. In *Proceedings of the 14th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pages 990–998, New York, NY, USA, 2008.

[194] R. K. Taylor. Marketing strategies: Gaining a competitive advantage through the use of emotion. *Competitiveness Review*, 10(2):146–152, 2000.

[195] S. Theodoridis, A. Pikrakis, K. Koutroumbas, and D. Cavouras. *Introduction to Pattern Recognition: A Matlab Approach*. Academic Press, 2010.

[196] A. Tversky and D. Kahneman. Judgment under uncertainty: Heuristics and biases. *Science*, 185:1124–31, 1974.

[197] M. Uddin, M. Zulkernine, and S. Ahamed. CAT: A context-awareware trust model for open and dynamic systems. In *ACM Symposium on Applied Computing*, pages 2024–2029, 2008.

[198] E. Uslaner, D. Stolle, and M. Hooghe. *Trust, Democracy and Governance: Can Government Policies Influence Generalized Trust?*, chapter Generating Social Capital: Civic Society and Institutions in Comparative Perspective, pages 171–190. Palgrave Macmillan, New York, 2004.

[199] S. Van de Walle and G. Bouckaert. Public service performance and trust in government: The problem of causality. *International Journal of Public Administration*, 26(8-9):891–913, 2003.

[200] F. Walter, S. Battiston, and F. Schweitzer. A model of a trust-based recommendation system on a social network. *AAMAS Journal*, 16(1):57–74, 2008.

[201] D. N. Walton. *Appeal to expert opinion: arguments from authority*. Pennsylvania State University Press, 1997.

[202] C. Wang, J. Han, Y. Jia, J. Tang, D. Zhang, Y. Yu, and J. Guo. Mining advisor-advisee relationships from research publication networks. In *Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pages 203–212, 2010.

[203] G. Wang and J. Wu. Flowtrust: trust inference with network flows. *Frontiers of Computer Science in China*, 5(2):181–194, 2011.

[204] X. Wang, Y. Chen, and B. Xu. Trust service selection in pervasive computing. In *International Conference on Multimedia Information Networking and Security (MINES)*, pages 173 –176, 2009.

[205] Y. Wang and L. Li. Two-dimensional trust rating aggregations in service-oriented applications. *IEEE Transactions on Service Computing*, 4(4):257–271, 2011.

[206] Y. Wang, L. Li, and G. Liu. Social context-aware trust inference for trust enhancement in social network based recommendations on service providers. *World Wide Web Journal (WWWJ)*, 18(1):159–184, 2015.

[207] Y. Wang and E. P. Lim. The evaluation of situational transaction trust in e-service environments. In *IEEE International Conference on e-Business Engineering (ICEBE)*, pages 265–272. IEEE, 2008.

[208] Y. Wang and F. Lin. Trust and risk evaluation of transactions with different amounts in peer-to-peer e-commerce environments. In *IEEE International Conference on e-Business Engineering (ICEBE)*, pages 102–109, 2006.

[209] Y. Wang and K. J. Lin. Reputation-oriented trustworthy computing in e-commerce environments. *IEEE Internet Computing*, 12(4):55–59, 2008.

[210] Y. Wang and V. Varadharajan. Trust^2: Developing trust in peer-to-peer environments. In *International Conference on Services Computing*, pages 24–31, 2005.

[211] Y. Wang and V. Varadharajan. Two-phase peer evaluation in p2p e-commerce environments. In *International Conference on e-Technology, e-Commerce and e-Service*, pages 654–657, 2005.

[212] Y. Wang and V. Varadharajan. Role-based recommendation and trust evaluation. In *IEEE Joint Conference on E-Commerce Technology and Enterprise Computing, E-Commerce and E-Services*, pages 278–288, 2007.

[213] M. Warkentin, D. Gefen, P. A. Pavlou, and G. M. Rose. Encouraging citizen adoption of egovernment by building trust. *Electronic Markets*, 12(3), 2002.

[214] S. Wasserman. *Social Network Analysis: Methods and Applications*. Cambridge University Press, 1994.

[215] D. J. Watts and S. H. Strogatz. Collective dynamics of 'small-world' networks. *Nature*, 393(6684):409–10, 1998.

[216] L. R. Welch. Hidden markov models and the baum-welch algorithm. *IEEE Information Theory Society Newsletter*, 53(4), 2003.

[217] A. C. Wicks, S. L. Berman, and T. M. Jones. The structure of optimal trust: Moral and strategic implications. *Academy of Management Review*, 24(1):99–116, 1999.

[218] X. Xiao, D. Xiao, J. Lin, and Y. Xiao. Overview on multi-objective optimization problem research. *Application Research of Computers*, 28(3):806–808, 2011.

[219] L. Xiong and L. Liu. A reputation-based trust model for peer-to-peer ecommerce communities. In *IEEE International Conference on E-Commerce*, pages 275–284, 2003.

[220] L. Xiong and L. Liu. Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities. *IEEE Transactions on Knowledge and Data Engineering*, 16(15):843–857, 2004.

[221] S. Yang, B. Long, A. J. Smola, N. Sadagopan, Z. Zheng, and H. Zha. Like like alike: joint friendship and interest propagation in social networks. In *Proceedings of the 20th International Conference on World Wide Web (WWW)*, pages 537–546, Hyderabad, India, 2011.

[222] Z. Yang, K. Cai, J. Tang, L. Zhang, Z. Su, and J. Li. Social context summarization. In *Proceedings of the 34th International ACM SIGIR Conference on Research and Development in Information Retrieval*, pages 255–264, 2011.

[223] I. Yaniv and E. Kleinberger. Advice taking in decision making: Egocentric discounting and reputation formation. *Organizational Behavior and Human Decision Processes*, 83(2):260–281, 2000.

[224] Y. Yao, H. Tong, X. Yan, F. Xu, and J. Lu. Matrust: An effective multi-aspect trust inference model. *CoRR*, abs/1211.2041, 2012.

[225] Y. Yao, H. Tong, X. Yan, F. Xu, and J. Lu. Matri: a multi-aspect and transitive trust inference model. In *Proceedings of the 22nd international conference on World Wide Web*, pages 1467–1476, 2013.

[226] Y. Yao, H. Tong, X. Yan, F. Xu, and J. Lu. Multi-aspect + transitivity + bias: An integral trust inference model. *IEEE Transactions on Knowledge and Data Engineering*, 2013.

[227] C. A. Yeung and T. Iwata. Strength of social influence in trust networks in product review sites. In *Proceedings of the 4th International Conference on Web Search and Web Data Mining*, pages 495–504, Hong Kong, China, 2011.

[228] B. Yu and M. P. Singh. A social mechanism of reputation management in electronic communities. In *International Workshop on Cooperative Information Agents IV*, pages 154–165, 2000.

[229] Q. Yuan, L. Chen, and S. Zhao. Augmenting collaborative recommenders by fusing social relationships: Membership and friendship. In *Recommender Systems for the Social Web*, pages 159–175. Springer, 2012.

[230] L. A. Zadeth. A note on z-numbers. *International Journal of Information Sciences*, 181(14):2923 – 2932, 2011.

[231] R. Zajonc. Interpersonal attraction and attitude similarity. *Journal of Abnormal and Social Psychology*, 62(3):713–715, 1961.

[232] R. B. Zajonc. Mere exposure: A gateway to the subliminal. *Current Directions in Psychological Science*, 10(6):224–228, 2011.

[233] H. Zhang. *Context-Aware Transaction Trust Computation in E-Commerce Environments*. PhD thesis, Macquarie University, 2014.

[234] H. Zhang, Y. Wang, and X. Zhang. Transaction similarity-based contextual trust evaluation in e-commerce and e-service environments. In *IEEE International Conference on Web Services*, pages 500–507, 2011.

[235] H. Zhang, Y. Wang, and X. Zhang. Efficient contextual transaction trust computation in e-commerce environments. In *IEEE International Conference on*

Trust, Security and Privacy in Computing and Communications, pages 318–325, 2012.

[236] H. Zhang, Y. Wang, and X. Zhang. A trust vector approach to transaction context-aware trust evaluation in e-commerce and e-service environments. In *5th IEEE International Conference on Service Oriented Computing & Applications (SOCA)*, pages 1–8, 2012.

[237] H. Zhang, Y. Wang, and X. Zhang. The approaches to contextual transaction trust computation in e-commerce environments. *Security and Communication Networks*, 2013.

[238] J. Zhang and R. Cohen. Evaluating the trustworthiness of advice about seller agents in e-marketplaces: A personalized approach. *Electronic Commerce Research and Applications*, 7(3):330–340, 2008.

[239] Z. Zhang, W. Cheng, and X. Zhou. Research on intelligent diagnosis of mechanical fault based on ant colony algorithm. In *6th International Symposium on Neural Networks (ISNN)*, pages 631–640, 2009.

[240] X. Zheng, Y. Wang, A. M. Orgun, G. Liu, and H. Zhang. Social context-aware trust prediction in social networks. In *12th International Conference on Service Oriented Computing (ICSOC)*, pages 527–534, Paris, France, 2014.

[241] X. Zheng, Y. Wang, and M. Orgun. Modeling the dynamic trust of online service providers using HMM. In *IEEE 20th International Conference on Web Services (ICWS)*, pages 459–466, Silicon Valley, California, USA, 2013.

[242] X. Zheng, Y. Wang, and M. A. Orgun. Binet: Trust sub-network extraction using binary ant colony algorithm in contextual social networks. In *IEEE 22th International Conference on Web Services (ICWS)*, pages 321–328, New York, USA, 2015.

[243] X. Zheng, Y. Wang, M. A. Orgun, Y. Zhong, and G. Liu. Trust prediction with propagation and similarity regularization. In *28th AAAI Conference on Artificial Intelligence*, pages 237–243, Quebec City, Quebec, Canada, 2014.

[244] Y. Zhong, X. Zheng, J. Yang, M. A. Orgun, and Y. Wang. KPMCF: A learning model for measuring social relationship strength. In *14th International Conference on Web Information System Engineering (WISE)*, pages 519–522, Nanjing, China, 2013.