Chapter 1
The Roadmap of Trust and Trust Evaluation in Web Applications and Web Services

Lei Li and Yan Wang

Abstract In the 1980s and 1990s, the issue of trust in many aspects of life has drawn much attention in a significant number of studies in social science. Nowadays, with the development of Web applications, trust evaluation has become a significant and important issue, especially when a client has to select a trustworthy one from a pool of unknown service providers. An effective and efficient trust evaluation system is highly desirable and critical to clients for identifying potential risks, providing objective trust results and preventing huge monetary losses.

This research roadmap presents an overview of the general structure of trust, the bases of trust and the concepts of trust in different disciplines. Then the typical trust evaluation methods in each area of Web applications, including e-commerce, P2P networks, multi-agent systems, recommendation systems, social networks and service-oriented computing, are briefly introduced from technology, state of the art and scientific challenges standpoints. This roadmap provides not only the necessary background for on-going research activities and projects, but also the solid foundations for deciding on potential future research on trust evaluation in broader contexts.

1.1 Introduction

In our daily life, there are many occasions when we have to trust others to behave as they promised or as we expect them to do. For example, we trust a bus driver can take us to our destination on time; we trust a doctor to conduct a physical examination

Lei Li
Department of Computing, Macquarie University, Sydney, NSW 2109, Australia, e-mail: lei.li@mq.edu.au

Yan Wang
Department of Computing, Macquarie University, Sydney, NSW 2109, Australia, e-mail: yan.wang@mq.edu.au

and check whether we have an illness; we trust a motor mechanic to find out whether there is a problem in our car and then repair it; we trust a bank and deposit our money. Each time when we trust, we have to put something at risk: our lives, our assets, our properties, and so on. On these occasions, we may use a variety of clues and past experiences to believe in these individuals' good intentions towards us and decide on the extent to which we can trust them. This is the general procedure of trust evaluation in daily occasions [35].

Nowadays, with the development of information communication technologies, from time to time it is necessary to have some interactions with others on the Web. For example, download some files from others, or purchase some products or services from online e-commerce or e-service websites. In Web applications, when a client intends to have an interaction selected from a large pool of service providers, in addition to functionality, the trustworthiness of a service provider is a key factor in service provider selection. This makes trust evaluation a significant and important issue in Web applications, especially when the client has to select one from unknown service providers.

Conceptually, trust is the measure taken by one party of the willingness and ability of another party to act in the interest of the former party in a certain situation [30]. If the trust value is in the range of $[0,1]$, it can be taken as the subjective probability by which one party expects that another party can perform a given action [28].

The issue of trust has been actively studied in Peer-to-Peer (P2P) networks (e.g., [14, 29, 90]), which can be used for information-sharing systems (e.g., GNutella[1]). In a P2P system, it is quite natural for a client peer to doubt if a serving peer can provide the complete file prior to any download action, which may be quite time-consuming and network bandwidth-consuming. Unlike some trust management systems in e-commerce (EC) or service-oriented environments (SOC), in the P2P trust management system a requesting peer needs to inquire the trust data of a serving peer (target peer) from other peers who may have transacted with the serving peer [29, 56, 90]. The computation of the trust level of the serving peer from the collected trust ratings is then performed by the requesting peer rather than a central management server, because of the decentralized architecture of the P2P system.

Unlike P2P information-sharing networks or the eBay[2] reputation management system where a binary rating system is used [90], in SOC environments a trust rating is usually a value in the range of $[0,1]$ given by a service client [80, 84, 86], representing the subjective belief of the service client on their satisfaction with a service or a service provider. The trust value of a service or a service provider can be calculated by a trust management authority based on the collected trust ratings representing the reputation of the service or the service provider.

In general, in a trust management enabled system, service clients can provide feedback and trust ratings after completed transactions. Based on the ratings, the trust value of a service provider can be evaluated to reflect the quality of services in a

[1] http://www.gnutella.com/
[2] http://www.eBay.com/

certain time period. This trust evaluation approach in service-oriented environments is the focus of research works nowadays in service-oriented computing.

Effective and efficient trust evaluation is highly desirable and critical to service clients for identifying potential risks, providing objective trust results and preventing huge monetary loss [82].

In this chapter, the literature review on trust is organized as follows:

- Section 1.2 presents a general structure of trust, which provides a general global picture of trust. With this structure, it is easy to start a preliminary theoretical analysis of trust.
- Section 1.3 identifies the bases of trust, with which trust can be established from a variety of diverse sources of trust-related information.
- Section 1.4 briefly introduces the concepts of trust defined in multiple disciplines, including sociology, history, psychology, economics and so on.
- Section 1.5 focuses on trust evaluation models used in different areas of Web applications, including e-commerce, P2P networks, multi-agent systems, recommendation systems and social networks.
- Section 1.6 focuses on the typical trust evaluation methods used in service-oriented computing.
- In Section 1.7, the above mentioned trust evaluation methods in Web applications are categorized into different taxonomies with respect to trust evaluation techniques, the structure of trust and the bases of trust respectively.
- Finally, Section 1.8 concludes our work in this chapter.

1.2 General Structure of Trust

The general structure of trust has been proposed in [54] and graphically represented in Fig. 1.1. This structure provides a general global picture of trust, with which professionals, scientists and even ordinary citizens can start a preliminary theoretical analysis of trust. With primary trust and reflective trust as the horizontal axis, and micro-social trust and macro-social trust as the vertical axis, this presentation creates four spaces which correspond to four orthogonally placed forms of trust.

- Vertically, passing from the bottom half of Fig. 1.1 toward the top, we move from micro-social trust (i.e., personal, private and interpersonal trust) toward macro-social trust (i.e., professional, group and organizational trust).
- Horizontally, the left-hand side of Fig. 1.1 is characterized by trust as feelings, either based on the interdependence between the self and other, or associated with security or social cohesion [1]. As we move toward the right-hand part of Fig. 1.1, trust becomes conceptualized and rationalized [1]. Trust in the right-hand part of Fig. 1.1 is contractual, and is based on obligations and morality.
  In other words, in the left-hand side we focus on primary trust (i.e., immediately apprehended [preconceptual] forms of trust), while in the right-hand side trust is established between the self and a stranger, an institutions or a kind of group (i.e.,

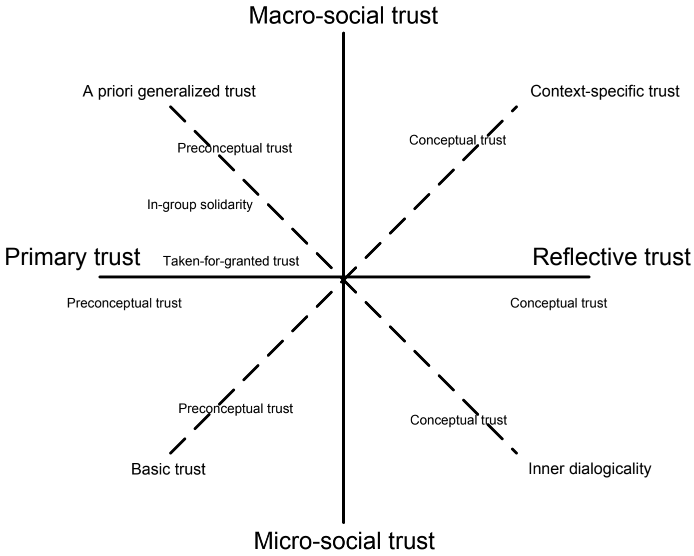

Fig. 1.1 General Structure of Trust

reflective trust [1]). However, once trust has been established, it transforms into common knowledge and becomes taken-for-granted and commonly understood. In contrast to the left-hand side of Fig. 1.1, this taken-for-grantedness arises from reflective thinking. There is also a case whereby, as a result of an individual's doubt trust is brought back into discourse explicitly. When trust is explicitly verbalized, it is no longer taken-for-granted and is partly or fully destroyed. It is necessary to establish trust from the very beginning again.

1.2.1 Basic Trust

Now let us focus on the bottom left quadrant of Fig. 1.1, the boundaries of which are determined by micro-social and primary trust. In the bottom left corner of this quadrant, there is what developmental psychologists describe as *basic trust* between a mother and her baby.

Basic trust is the first mark of an individual's mental life, even before feelings of autonomy and initiative develop [17]. Through the mutuality between a mother and her baby, basic trust evolves through mutual somatic experiences and "unmistakable communication" that creates security and continuity. With the presupposition that humans possess the capacity to make distinctions, the child, equipped with an innate capacity for intersubjectivity, learns through actions, experiences and communications to differentiate between the mental states of others, between feelings, and between trustworthy and untrustworthy relations [72].

1.2.2 A Priori Generalized Trust

Moving to the second quadrant in the top left part of Fig. 1.1, we can see that it is circumscribed by primary trust and macro-social trust. In the top left quadrant of Fig. 1.1, a *priori generalized trust* is above all a fundamental psychosocial feeling, and it is instantaneously apprehended, quite often without the awareness of those concerned [53]. Generally speaking, the top left quadrant contains trust which is characterized by the kinds of social relations in a society where individuals have certain kinds of social activities. In society, they conceive, create and communicate their social relations and trust with others. Social differentiation leads to the formation of social groups, associations and institutions in which individuals are bound together by impersonal relations. Particularly, in a heterogeneous and complex society like ours, trust is person-specific and content-specific [72]. In our society, during daily life we have to deal with strangers all the time, but here we only deal with one aspect of a stranger and not with the whole person. For example, we trust a motor mechanic to find out whether there is a problem in our car and then repair it, but we don't trust him/her on anything else, such as conducting a physical examination and checking whether we have an illness.

In this quadrant, somewhere more towards the intersection, we can place *in-group solidarity* [11], which can be taken as a special form of trust. It includes the social binding and bounding of close in-groups, such as the social cohesion and social ties within family, friends, neighbors, coactivists, and other communities.

1.2.3 Context-Specific Trust

Now we focus on the third quadrant of Fig. 1.1, and it is bounded by macro-social and reflective trust. This quadrant includes trust resulting from a variety of forms, ranging from cooperation to audits, strategies, calculations and so on. The typical form of trust located in this quadrant is *context-specific trust* [55], which can be derived from contextual information.

In the computer science discipline, it is firstly pointed out in [55] that trust is context sensitive: "Whilst I may trust my brother to drive me to the airport, I most certainly would not trust him to fly the plane!" Generally, context is any information characterizing the situation of an entity [75]. An entity, in turn, can be a person, a place, or an object that is considered relevant to the interaction between a user and an application, including the user and the application themselves [77]. A typical and simple context-specific trust evaluation process is as follows: in a trust management system, regarding entity A who has never interacted with entity B in the past, before making the decision to have an interaction with B, A asks other entities what are their trust ratings for B under the target context required by A. Then the trust from A to B will be established only if the weighted average of the trust ratings from other entities is larger than a threshold, where the weights of trust ratings are determined based on the similarity of the context of a trust rating and the target context required by A [65].

1.2.4 Inner Dialogicality

Finally, we arrive at the bottom right quadrant of Fig. 1.1, and in this quadrant we can place *inner dialogicality* [2]. By inner dialogicality, we mean the capacity of humans to carry out internal dialogues (i.e., dialogues within the self). For example, it could include evaluations of one's own and others' past experiences and present conduct, which reflects personal issues and predicts the future conduct. Inner dialogues include not only self-confidence but also self-doubt [54]. With inner dialogues, individuals can develop an awareness of how, where, when and why they can trust or have confidence in specific others (or in themselves).

With the proposed general structure of trust, any form of trust should fall into one of these four quadrants. As the forms of trust in the same quadrant have the similar properties, when we start to analysis a new form of trust, it is possible to begin the research with analyzing the evaluation approaches for other forms of trust in the same quadrant and then determine the corresponding evaluation approaches for the new form of trust.

1.3 Bases of Trust

In the proposed general structure of trust, there are a lot of forms of trust. But, how to establish trust? Research on identifying the bases of trust attempts to establish the conditions which lead to the emergence of trust, including psychological, social, and organizational factors that influence individuals' expectations about others' trustworthiness and their willingness to behave trustworthily during an interaction [1, 31]. The bases of trust are significant to understand trust and measure trust in computer science.

1.3.1 Dispositional Trust Establishment

Individuals behave differently in their general predisposition to trust different people [31]. To explain the origins of such dispositional trust, Rotter [68] proposed that individuals tend to build up general trustworthiness about other people from their early trust-related experiences (e.g., the basic trust proposed in Section 1.2.1). In addition, we usually assume that an individual has a relatively stable personality characteristic [68] in a certain situation, i.e., a relatively stable dispositional trust in a certain situation. However, as the dispositional trust is related to individuals' personal characteristic, it is usually hard to estimate its value directly.

1.3.2 History-based Trust Establishment

In the literature, it has been pointed out that individuals' willingness to engage in trusting others is largely a history dependent process [6]. Interactional histories provide decision makers with useful trust information on the estimation of others' dispositions, intentions and motivations. With the assumption of a relatively stable personality characteristic, this historical information also provides a basis for making predictions about others' future behaviors.

Interactional histories have a significant effect on two psychological facets of trust judgment.

- First, individuals' estimations about others' trustworthiness depend on their prior expectations about others' behaviors.
- Second, these expectations vary with subsequent experience, which either validates or discredits the expectations.

In this regard, history-based trust can be taken as an important basis for establishing knowledge-based or personalized trust [34].

Personalized knowledge about interaction history can provide important information for trust estimation. However, from time to time such knowledge is hard to obtain. In most situations, it is impossible for decision makers to accumulate sufficient knowledge about the potential individuals with whom they would like to transact. As a consequence, a variety of substitutes for such direct personalized knowledge about interaction history have to be utilized [13] and many other bases of trust have to be introduced.

1.3.3 Third Parties as Conduits of Trust

Considering the importance of personalized knowledge about interaction history regarding others' trustworthiness and its difficulty to obtain, third parties can be introduced as conduits of trust because of their diffusion of trust-related information.

In our daily life, the most common examples of using third parties as conduits of trust are gossip and word-of-mouth. These ways can provide a valuable source of second-hand knowledge about others [8], but the effects of these ways on trust estimations are complex and do not always have positive effects on the estimation of others' trustworthiness. That is because third parties usually tend to disclose only partial information about others [8]. In particular, when an individual has a strong relation to a prospective trustee, third parties usually prefer to convey the information which they believe the individual wants to hear, i.e., the information which strengthens the tie between third parties and the individual [31]. This will increase the certainty about the trustee's trustworthiness. Thus, in this situation, third parties tend to amplify such trust.

Third parties also play an important role in the development and diffusion of trust in social networks [78]. When there is no sufficient knowledge or interaction history available, individuals can turn to third parties for transferring their well-established trust relationships. This provides a base of trust which will be validated or discredited with subsequent experience.

1.3.4 Category-based Trust Establishment

Category-based trust refers to trust estimation based on the information regarding a trustee's membership in a social or an organizational category. For example, we can take gender, race or age as a social category to establish the category-based trust. This category information usually unknowingly influences others' estimations about the trustee's trustworthiness.

The theoretical foundation of category-based trust is established from the fact that due to the cognitive consequences of categorization and ingroup bias, individuals tend to attribute positive characteristics such as cooperativeness and trustworthiness to other ingroup members [7]. As a result, individuals can establish a kind of depersonalized trust (i.e., category-based trust) on other ingroup members only based on the awareness of their shared category membership.

1.3.5 Role-based Trust Establishment

Role-based trust focuses on trust estimation based on the knowledge that a trustee occupies a particular role in an organization rather than that a truster has the specific knowledge about the trustee's dispositions, intentions and motivations. To some extent, it is believable that technically competent role performance is usually aligned with corresponding roles in organizations [3]. For example, in the case of vehicle maintenance, we usually trust a motor mechanic to find out whether there is a problem with the car. Therefore, individuals can establish a kind of trust based on the knowledge of role relations, even without personalized knowledge or interaction history.

Role-based trust is established from the fact that there are some prerequisites to occupy a role in an organization, such as the training and socialization processes that role occupants have undergone, and their intentions to ensure their technically competent role performance.

Role-based trust can also be quite vulnerable, especially during organizational crises or when novel situations occur which confuse organizational roles or break down role-based interactions.

1.3.6 Rule-based Trust Establishment

Both formal and informal rules capture much of the knowledge about tacit understandings regarding transaction behaviors, interactional routines, and exchange practices [52]. Formal rules are determined by a trust management authority to establish trust between truster and trustee. For example, with the help of PayPal[3], a buyer can trust an unknown seller for a certain transaction. In contrast, informal rules are not explicitly determined by any trust management authority. Instead, they are formed by tradition, religion or routines. For example, in academic environments, early career researchers usually trust senior researchers to help them and guide their research path.

Rule-based trust is estimated not on a conscious calculation of consequences, but rather on shared understandings regarding rules of appropriate behaviors. Regarding the effects of rules on individuals' self-perceptions and expectations about other participants in a social network, rules can create and sustain high levels of trust within the social network [52].

1.4 Concept of Trust in Multiple Disciplines

Complex social phenomena like trust cannot be properly understood from the perspective of a single discipline or in separation from other social phenomena [54]. Although considerable attention to the problem of defining trust has been afforded [31], as it is understandable that a single researcher cannot master all the knowledge related to trust in all related disciplines, thus a concise and universally accepted definition of trust has remained elusive, and the concept of trust is usually based on analysis from the viewpoint of a single discipline, as discussed below.

From the perspective of sociology and history, according to Seligman [71], "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. The problem of trust emerges only in cases where there is "role negotiability", i.e., there is "open space" between roles and role expectations [71].

Seligman [71] also points out that trust is a modern phenomenon. What might appear as trust in premodern societies was nothing but "confidence in well-regulated and heavily sanctioned role expectations". Modernity saw the rise of individualism

[3] http://www.paypal.com.au/

and the proliferation of societal roles. There was thus a greater degree of negotiability of role expectations and a greater possibility for role conflicts, and this resulted in a greater potential for the development of trust in modern society.

From the perspective of sociology, Coleman [10] proposes a four-part definition of trust.

- Placement of trust allows actions that otherwise are not possible, i.e., trust allows actions to be conducted based on incomplete information on the case in hand.
- If the person in whom trust is placed (i.e., a trustee) is trustworthy, then the trustor will be better off than if s/he had not trusted. Conversely, if the trustee is untrustworthy, then the trustor will be worse off than if s/he had not trusted.
- Trust is an action that involves a voluntary transfer of resources (e.g., physical, financial, intellectual, or temporal) from the truster to the trustee with no real commitment from the trustee.
- A time lag exists between the extension of trust and the result of the trusting behavior.

This definition allows for the discussion of trust behaviors, which is useful in reasoning about human-computer trust and trust behaviors in social institutions.

From the perspective of psychology, trust is the belief in the person who you trust to do what you expect. Individuals in relationships characterized by high levels of social trust are more apt to exchange information and to act with benevolence toward others than those in relationships lacking trust. Misztal [63] points out three basic things that trust does in the lives of people: It makes social life predictable, creates a sense of community, and makes it easier for people to work together.

From the perspective of economics, trust is often conceptualized as reliability in transactions [54].

In all cases, trust involves many heuristic decision rules, requiring the trust management authority to handle a lot of complex information with great effort in rational reasoning [9].

1.5 Trust Evaluation in Web Applications

The issue of trust has been studied in some Web application fields.

1.5.1 Trust Evaluation in E-Commerce Environments

Trust is an important issue in e-commerce (EC) environments. At eBay[2], after each transaction, a buyer can give feedback with a rating of “positive”, “neutral” or “negative” to the system according to the service quality of the seller. eBay calculates the feedback score $S = P - N$, where P is the number of positive ratings left by buyers and N is the number of negative ratings. The positive feedback rate $R = \frac{P}{P+N}$ (e.g.,

$R = 99.1\%$) is then calculated and displayed on web pages. This is a simple trust management system providing valuable trust information to buyers.

In [96], the Sporas system is introduced to evaluate trust for EC applications based on the ratings of transactions in a recent time period. In this method, the ratings of later transactions are given higher weights as they are more important in trust evaluation. The Histos system proposed in [96] is a more personalized reputation system compared to Sporas. Unlike Sporas, the reputation of a seller in Histos depends on who makes the query, and how that person rated other sellers in the online community. In [74], Song et al. apply fuzzy logic to trust evaluation. Their approach divides sellers into multiple classes of trust ranks (e.g., a 5-star seller, or a 4-star seller). In [85], Wang and Lin present some reputation-based trust evaluation mechanisms (such as transaction-specific trust, raters' credibility and the social relationship between a rater and ratee) to more objectively depict the trust level of sellers on forthcoming transactions and the relationship between interacting entities.

1.5.2 Trust Evaluation in P2P Information Sharing Networks

The issue of trust has been actively studied in Peer-to-Peer (P2P) information sharing networks as a client peer needs to know prior to download actions which serving peer can provide complete files. In [14], Damiani et al. propose an approach for evaluating the trust of peers through a distributed polling algorithm and the *XRep* protocol before initiating any download action. This approach adopts a binary rating system and is based on the Gnutella[1] query broadcasting method. EigenTrust [29] adopts a binary rating system as well, and aims to collect the local trust values of all peers to calculate the global trust value of a given peer. Some other P2P studies also adopted the binary rating system. In [90], Xiong et al. propose a *PeerTrust* model which has two main features. First, they introduce three basic trust parameters (i.e., the feedback that a peer receives from other peers, the total number of transactions that a peer performs, the credibility of the feedback sources) and two adaptive factors in computing the trustworthiness of peers (i.e., transaction context factor and the community context factor). Second, they define some general trust metrics and formulas to aggregate these parameters into a final trust value. In [56], Marti et al. propose a voting reputation system that collects responses from other peers on a target peer. The final trust value is calculated by aggregating the values returned by responding peers and the requesting peer's experience with the target peer. In [99], Zhou et al. discover a power-law distribution in peer feedbacks, and develop a trust system with a dynamical selection on a small number of power nodes that are the most trustworthy in the system.

1.5.3 Trust Evaluation in Multi-Agent Systems

Trust has also drawn much attention in the field of multi-agent systems. In [76], Teacy et al. introduce the TRAVOS system (Trust and Reputation model for Agent-based Virtual OrganisationS) which calculates an agent's trust on an interaction partner using probability theory, taking into account the past interactions between agents. In [21], Griffiths proposes a multi-dimensional trust model which allows agents to model the trust value of others according to various criteria. In [69], Sabater et al. propose a model discussing trust development between groups. When calculating the trust from individual A to individual B, a few factors are considered, e.g., the interaction between A and B, the evaluation of A's group to B and B's group, and A's evaluation to B's group. In [15], a community-wide trust evaluation method is proposed where the final trust value is computed by aggregating the ratings (termed as votes in [15]) and other aspects (e.g., the rater's location and connection medium). In addition, this approach computes the trust level of an assertion (e.g., trustworthy or untrustworthy) as the aggregation of multiple fuzzy values representing the trust resulting from human interactions. In [26], during trust evaluation, the motivations of agents and the dependency relationships among them are also taken into account.

1.5.4 Trust-Aware Recommendation Systems

Conventional recommender systems mainly employ the information filtering techniques for making recommendations. In such systems, collaborative filtering approaches [25] or content-based filtering approaches [16, 64] are used for making recommendations, which collect ratings from the users with similar profiles or the items similar to the one a user liked in the past, respectively. However, these conventional approaches take users individually and do not address the trustworthiness of recommendations directly. In addition, as pointed out in [70], the sparsity of data in recommender systems has been an outstanding problem, which makes the filtering techniques less effective. Nevertheless, the ultimate goal of recommender systems is to provide high quality and trustworthy recommendations that can very likely be accepted by users. To this end, using the reviews/recommendations from social networks has drawn much attention in recent studies [48, 49].

Social influence occurs when one's emotions, opinions or behaviours are affected by others[4]. As indicated in Social Psychology [5, 18, 92], in the real society, a person prefers the recommendations from trusted friends. In addition, based on statistics, Sinha et al. [73] and Bedi et al. [4] have demonstrated that given a choice between the recommendations from trusted friends and those from recommender systems, in terms of quality and usefulness, trusted friends' recommendations are more preferred.

[4] http://qualities-of-a-leader.com/personal-mbti-type-analysis/

Social networks are important to recommender systems due to the data sparsity problem [48, 70] and the scenarios in real life that people turn to friends and friends' friends for soliciting opinions [5, 92], raising the need of trust propagation/inference in social networks (i.e., evaluating the trust between two non-adjacent participants). Earlier studies have adopted the averaging strategies [19], multiplication strategies [41, 81], or probabilistic approaches [32, 33] based on the trust values between adjacent participants. However, they ignore contextual factors that influence trust relations and trust inference (e.g., a person's recommendation role [88] or the social intimacy between people [45]), and/or simply take the confidence to other people as a probabilistic value without discussing from where the confidence comes. Most of the existing studies usually model their approaches intuitively, without following the principles from Social Science or Social Psychology. In some recent work [45, 46, 47], following the principles in Social Psychology [1, 61], both the recommendation role resulting from social positions (e.g., a professor) and expertise, and trust and social intimacy degree between adjacent participants in social networks have been taken into account.

1.5.5 Trust Evaluation in Social Networks

The studies of social network properties can be traced back to 1960's when the small-world characteristic in social networks was validated by Milgram [60] (i.e., the average path length between two Americans was found to be about 6.6 hops). In recent years, sociologists and computer scientists investigated the characteristics of popular online social networks (OSNs) [62] (e.g., Facebook[5], MySpace[6] and Flickr[7]), and validated the small-world and power-law characteristics (i.e., the probability that a node has a degree k is proportional to k^{-r}, $r > 1$).

In recent years, the new generation of social network based web application systems has drawn the attention from both academia and industry. The study in [44] has pointed out that it is a trend to build up social network based web applications (e.g., e-commerce or online recruitment systems). In real applications, according to a survey on 2600 hiring managers in 2008 by CareerBuilder (careerbuilder.com, a popular job hunting website), 22% of those managers used social networking sites to manually investigate potential employees. The ratio increased to 45% in June 2009 and 72% in January 2010. In Oct. 2011, eBay[2] announced their strategic plan to deepen the relationship with Facebook[5] for creating a new crop of e-commerce applications with social networking features, integrating both their e-commerce platform and social networking platform seamlessly[8].

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

[6] http://myspace.com

[7] http://flickr.com

[8] refer to the Reuters news "eBay and Facebook unveil e-commerce partnership" at http://www.reuters.com/article/2011/10/12/ebay-facebook-idUSN1E79B22Y20111012

In the literature, the issue of trust becomes increasingly important in social networks. In [81], Walter et al. identify that network density, the similarity of preference between agents, and the sparseness of knowledge about the trustworthiness of recommendations are crucial factors for trust-oriented recommendations in social networks. However, the trust-oriented recommendation can be attacked in various ways, such as sybil attack, where the attacker creates a potentially unlimited number of identities to provide feedback and increase trust level. In [94], Yu et al. present SybilGuard, a protocol for limiting the corruptive influences of sybil attacks, which depends on the established trust relationship between users in social networks.

Trust propagation, during which the trust of a target agent can be estimated from the trust of other agents, is an important problem in social networks. In [20], Golbeck et al. present trust propagation algorithms based on binary ratings. In social networks, many more non-binary trust propagation approaches have been proposed. In [22], Guha et al. develop a framework dealing with not only trust propagation but also distrust propagation. In [24], Hang et al. propose an algebraic approach to propagating trust in social networks, including a concatenation operator for the trust aggregation of sequential invocation, an aggregation operator for the trust aggregation of parallel invocation, and a selection operator for trust-oriented multiple path selection. In [79], Victor et al. present a trust propagation model, which takes into account fuzzified trust, fuzzified distrust, unavailable trust information and contradictory trust information simultaneously.

1.6 Trust Evaluation in Service-Oriented Environments

In recent years, Service-Oriented Computing (SOC) has emerged to be an increasingly important research area attracting attention from both the research and industry communities [50, 66]. In SOC applications, various services are provided to clients by different providers in a loosely-coupled environment. In such context, a service can refer to a transaction, such as selling a product online (i.e., the traditional online services), or a functional component implemented by Web service technologies [41]. When a client looks for a service from a large set of services offered by different service providers, in addition to functionality, the reputation-based trust level of a service provider is a very important concern from the view point of the service client [28, 41, 43, 50]. It is also a critical task for the trust management authority to be responsible for maintaining the list of reputable and trustworthy services and service providers, and making these information available to service clients [66].

In general, in a trust management mechanism enabled system, service clients can provide feedback and trust ratings after transactions. Then, the trust management system can calculate the trust value based on collected ratings reflecting the quality of recent transactions, with more weights assigned to later transactions [36, 82]. The trust value can be provided to service clients by publishing it on web or responding to their requests [36, 42]. An effective and efficient trust management system is highly desirable and critical for service clients to identify potential risks, providing objective trust results and preventing huge financial loss [28].

In the literature, the issue of trust has received much attention in the field of SOC. In [80], Vu et al. present a model to evaluate service trust by comparing the advertised service quality and the delivered service quality. If the advertised service quality is as good as the delivered service quality, the service is reputable. In [86], Wang et al. propose some trust evaluation metrics and a formula for trust computation with which a final trust value is computed. In addition, they propose a fuzzy logic based approach for determining reputation ranks that particularly differentiate the service periods of new and old (long-existing) service providers. The aim is to provide incentives to new service providers and penalize those old service providers with poor service quality. In [51], Malik et al. propose a set of decentralized techniques aiming at evaluating reputation-based trust with the ratings from clients to facilitate the trust-oriented selection and composition of Web services. In [12], Conner et al. present a trust model that allows service clients with different trust requirements to use different weight functions that place emphasis on different transaction attributes. This customized trust evaluation provides flexibility for service clients to have different trust values from the same feedback data.

Now let us introduce some important topics on trust evaluation in service-oriented environments.

1.6.1 Trust Vector and Its Evaluation

In the literature, in most existing trust evaluation models [14, 29, 43, 76, 80, 84, 86, 90, 96], a single final trust level (*FTL*) is computed to reflect the general or global trust level of a service provider accumulated in a certain time period (e.g., in the latest 6 months). This *FTL* may be presumably taken as a prediction of trustworthiness for forthcoming transactions. Single-trust-value approaches are easily adopted in trust-oriented service comparison and selection. However, a single trust value cannot preserve the trust features well, e.g., whether and how the trust trend changes. Certainly, a full set of trust ratings can serve for this purpose, but it is usually a large dataset as it should cover a long service period. A good option is to compute a small dataset to present a large set of trust ratings and well preserve its trust features.

In [36, 42], Li and Wang propose a trust vector with three values, including final trust level (*FTL*), service trust trend (*STT*) and service performance consistency level (*SPCL*), to depict a set of trust ratings. In addition to *FTL*, the service trust trend indicates whether the service trust ratings are becoming worse or better. *STT* is obtained from the slope of a regression line that best fits the set of ratings distributed over a time interval. The service performance consistency level indicates the extent to which the computed *STT* fits the given set of trust ratings. However, the computed trust vector can represent the set of ratings well only if these ratings imply consistent trust trend changes and are all very close to the obtained regression line.

In a more general case with trust ratings for a long service history, multiple time intervals (MTI) have to be determined, within each of which a trust vector can be obtained and can represent well all the corresponding ratings. In [40], Li and Wang propose three trust vector based MTI analysis approaches, which are better than the two existing boundary included MTI algorithms in [82]. The proposed bisection-based boundary excluded greedy MTI algorithm has a lower time complexity, and it is much faster than any of the other four MTI algorithms. The proposed boundary mixed optimal MTI analysis algorithm can guarantee the representation of a large set of trust ratings with a minimal set of values while highly preserving the trust features. Therefore, a small set of data can represent well a large set of trust ratings with well preserved trust features.

In the literature, there exist some other approaches using trust vectors, with different focuses. In [67], Ray et al. propose a trust vector that consists of the experience of a truster about a trustee, the knowledge of the truster regarding the trustee for a particular context, and the recommendation of other trustees. The focus of this model is how to address these three independent aspects of trust in evaluations. In [98], Zhao et al. propose a method using a trust vector to represent the directed link with a trust value between two peers. The trust vector includes a truster, a trustee and the trust value that the truster gives to the trustee. In [84], Wang et al. propose an approach to evaluate situational transaction trust in e-commerce environments, which binds a new transaction with the trust ratings of previous transactions. Since the situational trust vector includes service specific trust, service category trust, transaction amount category specific trust and price trust [83], it can deliver more objective transaction specific trust information to buyers and prevent some typical attacks.

1.6.2 Trust Evaluation in Composite Services

To satisfy the specified functionality requirement, a service may have to invoke other services forming composite Web services with complex invocations and trust dependency among services and service providers [59]. Meanwhile, given a set of various services, different compositions may lead to different service structures. In [57, 58], Medjahed et al. present some frameworks and algorithms for automatically generating composite services from specifications and rules. Although these certainly enrich the service provision, they greatly increase the computation complexity and thus make trustworthy service selection and discovery a very challenging task.

In real applications, the criteria of searching services should take into account not only functionalities but also other properties, such as QoS (quality of service) and trust. In the literature, a number of QoS-aware Web service selection mechanisms have been developed, aiming at QoS improvement in composite services [23, 89, 97]. In [97], Zeng et al. present a general and extensible model to evaluate the QoS of composite services. Based on their model, a service selection approach has been introduced using linear programming techniques to compute optimal execution plans for composite services. The work in [23] addresses the selection and composition of Web services based on functional requirements, transactional properties and QoS characteristics. In this model, services are selected in a way that satisfies user preferences, expressed as weights over QoS and transactional requirements. In [89], Xiao et al. present an autonomic service provision framework for establishing QoS-assured end-to-end communication paths across domains. Their algorithms can provide QoS guarantees over domains. The above works have their merits in different aspects. However, none of them has taken parallel invocation into account, which is fundamental and one of the most common existing invocations in composite services [59, 95].

Menascé [59] adopts an exhaustive search method to measure service execution time and cost involving probabilistic, parallel, sequential and fastest-predecessor-triggered invocations. However, the algorithm complexity is exponential. Yu et al. [95] study the service selection problem with multiple QoS constraints in composite services, and propose two optimal heuristic algorithms: the combinatorial algorithm and the graph-based algorithm. The former one models the service selection as a multidimension multichoice 0-1 knapsack problem. The latter one can be taken as a multiconstraint optimal path problem. Nevertheless, none of these works addresses any aspect of trust.

As pointed in [93], in richer service environments such as SOC or e-commerce, a rating in $[0,1]$ is more suitable. In [91], Xu et al. propose a reputation-enhanced QoS-based Web service discovery algorithm for service matching, ranking and selection based on existing Web service technologies. Malik et al. [51] propose a set of decentralized techniques aiming at evaluating reputation-based trust with the ratings from peers to facilitate trust-based selection and composition of Web services.

1.6.3 Subjective Trust Evaluation

Conceptually, if the trust value is in the range of [0,1], it can be taken as the subjective probability by which, one party expects that another party can perform a given action [28].

In [27], Jøsang describes a framework for combining and assessing subjective ratings from different sources based on Dempster-Shafer belief theory, which is a generalization of the Bayesian theory of subjective probability. Wang and Singh [87] set up a bijection from subjective ratings to trust values with a mathematical understanding of trust in a variety of multiagent systems. However, their models use either a binary rating (positive or negative) system or a triple rating (positive, negative or uncertain) systems that are more suitable for security-oriented or P2P file-sharing trust management systems.

Considering service invocation structures in composite services, in [37] Li and Wang propose a global trust evaluation approach, in which each rating is in the range of $[0,1]$. However, this approach has not taken the subjective probability property of trust into account. In [41], Li et al. propose a Bayesian inference based subjective trust evaluation approach which aggregates the subjective ratings from clients.

Nevertheless, this approach still has some drawbacks. Firstly, it assumes that the trust ratings of each service component conform to a normal distribution, which is continuous. However, trust ratings adopted in most existing rating systems[2,9,10] are discrete numbers. Thus, they cannot conform to a continuous distribution. Secondly, the proposed subjective probability approach (Bayesian inference) is to evaluate the trust values of service components, which is not used in the global trust evaluation of composite services. Therefore, although service invocation structures have been taken into account, the global trust evaluation of composite services does not keep the subjective probability property of trust. As in most existing rating systems[2,9,10] trust ratings are discrete numbers, the numbers of the occurrences of all ratings of each service component conform to a multinomial distribution [38]. Hence, in [38] Li and Wang propose a subjective trust estimation approach for service components based on Bayesian inference, which can aggregate the non-binary discrete subjective ratings given by service clients and keep the subjective probability property of trust ratings and trust results. Although the joint subjective probability approach proposed in [38] considers the trust dependency between service components caused by direct invocations, it does not take into account the composition of trust dependency, which is caused by indirect invocations in composite services. To solve this problem, in [39], on the basis of trust dependency caused by direct invocations, Li and Wang propose a SubjectivE probabiLity basEd deduCTIVE (SELECTIVE) approach to evaluate the subjective global trustworthiness of a composite service. All these processes follow subjective probability theory and keep the subjective probability property of trust in evaluations.

1.7 Trust Evaluation Taxonomy

Trust evaluation is based on the trusters' knowledge of trust, which is only in the trusters' minds. This makes the analysis process highly human-dependent and therefore prone to errors. Knowledge of trust can be abstract/general, or domain/application specific, etc. From different viewpoints, the trust evaluation approaches in Web applications (e.g., the ones presented in Section 1.5) can be categorized into different taxonomies as follows.

1.7.1 Trust Evaluation Technique Based Taxonomy

Similar to the taxonomy in [15, 82], we can categorize the above mentioned trust evaluation approaches in Web applications as follows according to their computation techniques. Some approaches may correlate to more than one category.

---

[9] http://www.epinions.com/
[10] http://www.youtube.com/

- *Category 1*: In this category, to evaluate trust it adopts the approach of calculating the summation or weighted average of ratings, like the models in [15, 21, 84, 86, 90, 96].
  In addition, based on the additive approach, a few studies address how to compute the final trust value by considering appropriate metrics. For example, later transactions are more important [96]; the evaluation approach should provide incentive to consistently good quality services and punish malicious service providers [86, 90]. Some other studies also consider context factors, e.g., the new transaction amount and service category [84], the rater's profile and location [15], or the relationship between the rater's group and the ratee [21].
- *Category 2*: This category addresses the subjective property of trust for trust rating aggregation, e.g., the work in [27, 38], where subjective probability theory is adopted in trust evaluation.
- *Category 3*: The approaches in this category (e.g., [76]) adopt Bayesian systems, which take binary ratings as input and compute reputation scores by statistically updating beta probability density functions (PDF).
- *Category 4*: This category uses flow models, e.g., in [12, 20, 22, 24, 79, 81, 94, 96, 99], which compute the trust of a target through some intermediate participants and the trust dependency between them.
- *Category 5*: While each of the above categories calculates a crisp value, the last category adopts fuzzy models, e.g., in [15, 86], where membership functions are used to determine the trustworthiness of targets.

1.7.2 Trust Structure Based Taxonomy

According to the general structure of trust described in Section 1.2, the trust evaluation approaches in Web applications (e.g., the ones presented in Section 1.5) can be categorized into the *first quadrant* of Fig. 1.1. This is not a big surprise since each trust evaluation approach in Web applications focuses on trust in a specific environment (e.g., e-commerce, P2P networks, service-oriented computing, multi-agent systems or social networks), and reflective and macro-social trust belongs to the first quadrant. In contrast, the second and third quadrants focus on primary (taken-for-granted) trust, and there is no necessity to have any trust evaluation approach in these quadrants. The fourth quadrant focuses on self trust evaluation.

1.7.3 Trust Bases Based Taxonomy

According to the bases of trust proposed in Section 1.3, the trust evaluation approaches presented in Section 1.5 can be analyzed as follows to find out which base of trust is adopted in each trust evaluation approach. Some approaches may be based on more than one bases of trust.

- *Dispositional Trust* focuses on the personality of a truster, with the assumption of a relatively stable personality characteristic, like the model in [76].
- *History-based Trust* is the most widely adopted trust base in trust evaluation. For example, it has been taken into account in [12, 14, 26, 29, 51, 56, 69, 74, 80, 84, 85, 86, 90, 96, 99].
- *Third Parties as Conduits of Trust* is another widely adopted trust base to evaluate trust. For example, it has been adopted by the models in [20, 22, 24, 26, 27, 69, 76, 79, 81, 94, 99].
- *Category-based Trust* addresses the information regarding a trustee's membership in a social or organizational category, e.g., in [69].
- *Role-based Trust* uses the knowledge that a trustee occupies a particular role in the organization, e.g., the work in [15, 26, 85].
- *Rule-based Trust* specifies formal or informal rules, which can determine trust, like the models in [21, 27, 86].

1.8 Conclusions

This chapter provides a general overview of the research studies on trust and trust evaluation. Conceptually, we present the general structure of trust, the bases of trust and the concepts of trust in different disciplines. The general structure of trust presents a general cross-disciplinary analysis of trust, and provides a general picture containing all kinds of trust. The bases of trust illustrate what leads to the emergence of trust. The concepts of trust present different aspects of trust from the different viewpoints of different disciplines.

In addition, the typical trust evaluation methods are introduced in a variety of Web application areas, including e-commerce, P2P networks, multi-agent systems, recommendation systems, social networks and service-oriented computing. Finally, these trust evaluation methods in Web applications can be categorized into different taxonomies. The trust evaluation methods presented in this chapter cover a wide range of applications and are based on many different types of mechanisms, and there is no single trust evaluation method that will be suitable in all contexts and applications. This roadmap provides not only the necessary background for on-going research activities and projects, but also the solid foundations for deciding on potential future research on trust evaluation in broader contexts.

References

1. P. S. Adler. Market, hierarchy, and trust: The knowledge economy and the future of capitalism. *Organization Science*, 12(2):215–234, 2001.
2. M. Bakhtin. *Speech Genres and Other Late Essays.* University of Texas Press, 1986.
3. B. Barber. *The logic and limits of trust.* Rutgers University Press, 1983.

4. P. Bedi, H. Kaur, and S. Marwaha. Trust based recommender system for semantic web. In *IJCAI 2007*, pages 2677–2682, 2007.
5. E. Berscheid and H. T. Reis. *Attraction and Close Relationships in The Handbook of Social Psychology*. Oxford University Press, 1998.
6. S. D. Boon and J. G. Holmes. The dynamics of interpersonal trust: Resolving uncertainty in the face of risk. In R. Hinde and J. Groebel, editors, *Cooperation and Prosocial Behavior*, pages 167–182. Cambridge Univ. Press, 1991.
7. M. B. Brewer. In-group favoritism: the subtle side of intergroup discrimination. In D. M. Messick and A. E. Tenbrunsel, editors, *Codes of Conduct: Behavioral Research and Business Ethics*, pages 160–171. Russell Sage Found, 1996.
8. R. S. Burt and M. Knez. Kinds of third-party effects on trust. *Rationality and Society*, 7:255–292, 1995.
9. C. Castelfranchi and R. Falcone. Trust is much more than subjective probability: Mental components and sources of trust. In *HICSS 2000*, 2000.
10. J. Coleman. *Foundations of Social Theory*. Belknap Press of Harvard University Press, 1998.
11. R. Collins. *Sociological Insight: an Introduction to Non-obvious Sociology*. Oxford University Press, 1992.
12. W. Conner, A. Iyengar, T. A. Mikalsen, I. Rouvellou, and K. Nahrstedt. A trust management framework for service-oriented environments. In *WWW 2009*, pages 891–900, 2009.
13. D. W. Creed and R. E. Miles. Trust in organizations: a conceptual framework linking organizational forms, managerial philosophies, and the opportunity costs of controls. In R. Kramer and T. Tyler, editors, *Trust in organizations: Frontiers of Theory and Research*, pages 16–38. Sage Publications, 1996.
14. E. Damiani, S. D. C. di Vimercati, S. Paraboschi, P. Samarati, and F. Violante. A reputation-based approach for choosing reliable resources in peer-to-peer networks. In *ACM Conference on Computer and Communications Security (CCS 2002)*, pages 207–216, 2002.
15. E. Damiani, S. D. C. di Vimercati, P. Samarati, and M. Viviani. A wowa-based aggregation technique on trust values connected to metadata. *Electr. Notes Theor. Comput. Sci.*, 157(3):131–142, 2006.
16. M. Deshpande and G. Karypis. Item-based top-*n* recommendation algorithms. *ACM Trans. Inf. Syst.*, 22(1):143–177, 2004.
17. E. Erikson. *Identity: Youth and Crisis*. W. W. Norton & Company, 1968.
18. S. Fiske. *Social Beings: Core Motives in Social Psychology*. John Wiley and Sons Press, 2009.
19. J. Golbeck. Generating predictive movie recommendations from trust in social networks. In *iTrust 2006*, pages 93–104, 2006.
20. J. Golbeck and J. A. Hendler. Inferring binary trust relationships in web-based social networks. *ACM Trans. Internet Techn.*, 6(4):497–529, 2006.
21. N. Griffiths. Task delegation using experience-based multi-dimensional trust. In *AAMAS 2005*, pages 489–496, 2005.
22. R. V. Guha, R. Kumar, P. Raghavan, and A. Tomkins. Propagation of trust and distrust. In *WWW 2004*, pages 403–412, 2004.
23. J. E. Haddad, M. Manouvrier, G. Ramirez, and M. Rukoz. QoS-driven selection of web services for transactional composition. In *ICWS 2008*, pages 653–660, 2008.
24. C.-W. Hang, Y. Wang, and M. P. Singh. Operators for propagating trust and their evaluation in social networks. In *AAMAS 2009*, pages 1025–1032, 2009.
25. J. L. Herlocker, J. A. Konstan, A. Borchers, and J. Riedl. An algorithmic framework for performing collaborative filtering. In *SIGIR 1999*, pages 230–237, 1999.
26. T. D. Huynh, N. R. Jennings, and N. R. Shadbolt. An integrated trust and reputation model for open multi-agent systems. *Autonomous Agents and Multi-Agent Systems*, 13(2):119–154, 2006.
27. A. Jøsang. Subjective evidential reasoning. In *IPMU 2002*, 2002.
28. 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.
29. S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina. The eigentrust algorithm for reputation management in p2p networks. In *WWW 2003*, pages 640–651, 2003.

30. D. H. Knight and N. L. Chervany. The meaning of trust. Technical Report WP9604, University of Minnesota, Management Information Systems Research Center, 1996.
31. R. M. Kramer. Trust and distrust in organizations: Emerging perspectives, enduring questions. *Annual Review of Psychology*, 50:569–598, 1999.
32. U. Kuter and J. Golbeck. Sunny: A new algorithm for trust inference in social networks using probabilistic confidence models. In *AAAI 2007*, pages 1377–1382, 2007.
33. U. Kuter and J. Golbeck. Using probabilistic confidence models for trust inference in web-based social networks. *ACM Trans. Internet Techn.*, 10(2), 2010.
34. R. J. Lewicki and B. B. Bunker. Trust in relationships: a model of trust development and decline. In B. Bunker and J. Rubin, editors, *Conflict, Cooperation, and Justice*. Jossey-Bass, 1995.
35. L. Li. *Trust Evaluation in Service-Oriented Environments*. PhD thesis, Macquarie University, 2011.
36. L. Li and Y. Wang. A trust vector approach to service-oriented applications. In *ICWS 2008*, pages 270–277, 2008.
37. L. Li and Y. Wang. Trust evaluation in composite services selection and discovery. In *IEEE SCC 2009*, pages 482–485, 2009.
38. L. Li and Y. Wang. Subjective trust inference in composite services. In *AAAI 2010*, pages 1377–1384, 2010.
39. L. Li and Y. Wang. A subjective probability based deductive approach to global trust evaluation in composite services. In *ICWS 2011*, pages 604–611, 2011.
40. L. Li and Y. Wang. The study of trust vector based trust rating aggregation in service-oriented environments. *World Wide Web*, In press, 2012.
41. L. Li, Y. Wang, and E.-P. Lim. Trust-oriented composite service selection and discovery. In *ICSOC/ServiceWave 2009*, pages 50–67, 2009.
42. L. Li, Y. Wang, and V. Varadharajan. Fuzzy regression based trust prediction in service-oriented applications. In *ATC 2009*, pages 221–235, 2009.
43. M. Li, X. Sun, H. Wang, Y. Zhang, and J. Zhang. Privacy-aware access control with trust management in web service. *World Wide Web*, 14(4):407–430, 2011.
44. G. Liu, Y. Wang, and L. Li. Trust management in three generations of web-based social networks. In *CPSC 2009*, pages 446–451, 2009.
45. G. Liu, Y. Wang, and M. A. Orgun. Optimal social trust path selection in complex social networks. In *AAAI 2010*, pages 1391–1398, 2010.
46. G. Liu, Y. Wang, and M. A. Orgun. Quality of trust for social trust path selection in complex social networks. In *AAMAS 2010*, pages 1575–1576, 2010.
47. 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 SCC 2010*, pages 130–137, 2010.
48. H. Ma, H. Yang, M. R. Lyu, and I. King. Sorec: social recommendation using probabilistic matrix factorization. In *CIKM 2008*, pages 931–940, 2008.
49. H. Ma, T. C. Zhou, M. R. Lyu, and I. King. Improving recommender systems by incorporating social contextual information. *ACM Trans. Inf. Syst.*, 29(2):9, 2011.
50. Z. Malik and A. Bouguettaya. Rater credibility assessment in web services interactions. *World Wide Web*, 12(1):3–25, 2009.
51. Z. Malik and A. Bouguettaya. RATEWeb: Reputation assessment for trust establishment among web services. *VLDB J.*, 18(4):885–911, 2009.
52. J. G. March. *Primer on Decision Making: How Decisions Happen*. Free Press, 1994.
53. I. Marková. *Trust and Democratic Transition in Post-Communist Europe*. Oxford University Press, 2004.
54. I. Marková, A. Gillespie, and J. Valsiner. *Trust and Distrust: Sociocultural Perspectives*. Information Age Publishing, 2008.
55. S. Marsh. *Formalising Trust as a Computational Concept*. University of Stirling, 1994.
56. S. Marti and H. Garcia-Molina. Limited reputation sharing in p2p systems. In *ACM EC 2004*, pages 91–101, 2004.
57. B. Medjahed and A. Bouguettaya. A multilevel composability model for semantic web services. *IEEE Trans. Knowl. Data Eng.*, 17(7):954–968, 2005.

58. B. Medjahed, A. Bouguettaya, and A. K. Elmagarmid. Composing web services on the semantic web. *VLDB J.*, 12(4):333–351, 2003.
59. D. A. Menascé. Composing web services: A QoS view. *IEEE Internet Computing*, 8(6):88–90, 2004.
60. S. Milgram. The small world problem. *Psychology Today*, 2(30), 1967.
61. R. Miller, D. Perlman, and S. Brehm. *Intimate Relationships*. McGraw-Hill College Press, 2007.
62. A. Mislove, M. Marcon, P. K. Gummadi, P. Druschel, and B. Bhattacharjee. Measurement and analysis of online social networks. In *Internet Measurement Comference 2007*, pages 29–42, 2007.
63. B. Misztal. *Trust in Modern Societies: The Search for the Bases of Social Order*. Polity Press, 1996.
64. R. J. Mooney and L. Roy. Content-based book recommending using learning for text categorization. In *ACM DL 2000*, pages 195–204, 2000.
65. L. Mui. *Computational Models of Trust and Reputation: Agents, Evolutionary Games, and Social Networks*. PhD thesis, Massachusetts Institute of Technology, Dec 2002.
66. M. P. Papazoglou, P. Traverso, S. Dustdar, and F. Leymann. Service-oriented computing: a research roadmap. *Int. J. Cooperative Inf. Syst.*, 17(2):223–255, 2008.
67. I. Ray and S. Chakraborty. A vector model of trust for developing trustworthy systems. In *9th European Symposium on Research Computer Security*, pages 260–275, 2004.
68. J. B. Rotter. Interpersonal trust, trustworthiness, and gullibility. *American Psychologist*, 35(1):1–7, 1980.
69. J. Sabater and C. Sierra. REGRET: reputation in gregarious societies. In *Agents 2001*, pages 194–195, 2001.
70. B. M. Sarwar, G. Karypis, J. A. Konstan, and J. Riedl. Item-based collaborative filtering recommendation algorithms. In *WWW 2001*, pages 285–295, 2001.
71. A. B. Seligman. *The Problem of Trust*. Princeton University Press, 2000.
72. G. Simmel. *The Sociology of Georg Simmel*. The Free Press, 1950.
73. R. R. Sinha and K. Swearingen. Comparing recommendations made by online systems and friends. In *DELOS Workshop 2001: Personalisation and Recommender Systems in Digital Libraries*, 2001.
74. S. Song, K. Hwang, R. Zhou, and Y.-K. Kwok. Trusted p2p transactions with fuzzy reputation aggregation. *IEEE Internet Computing*, 9(6):24–34, 2005.
75. T. Strang, C. Linnhoff-Popien, and K. Frank. Cool: A context ontology language to enable contextual interoperability. In *IFIP WG6.1 International Conference on Distributed Applications and Interoperable Systems 2003*, pages 236–247, 2003.
76. W. T. L. Teacy, J. Patel, N. R. Jennings, and M. Luck. Travos: Trust and reputation in the context of inaccurate information sources. *Autonomous Agents and Multi-Agent Systems*, 12(2):183–198, 2006.
77. S. Toivonen, G. Lenzini, and I. Uusitalo. Context-aware trust evaluation functions for dynamic reconfigurable systems. In *Proceedings of the WWW'06 Workshop on Models of Trust for the Web (MTW'06)*, 2006.
78. B. Uzzi. Social structure and competition in interfirm networks: The paradox of embeddedness. *Administrative Science Quarterly*, 42(1):35–67, 1997.
79. P. Victor, C. Cornelis, M. D. Cock, and P. P. da Silva. Gradual trust and distrust in recommender systems. *Fuzzy Sets and Systems*, 160(10):1367–1382, 2009.
80. L.-H. Vu, M. Hauswirth, and K. Aberer. QoS-based service selection and ranking with trust and reputation management. In *CoopIS 2005*, pages 466–483, 2005.
81. F. E. Walter, S. Battiston, and F. Schweitzer. A model of a trust-based recommendation system on a social network. *Autonomous Agents and Multi-Agent Systems*, 16(1):57–74, 2008.
82. Y. Wang and L. Li. Two-dimensional trust rating aggregations in service-oriented applications. *IEEE T. Services Computing*, 4(4):257–271, 2011.
83. Y. Wang, L. Li, and E.-P. Lim. Price trust evaluation in e-service oriented applications. In *CEC/EEE 2008*, pages 165–172, 2008.

84. Y. Wang and E.-P. Lim. The evaluation of situational transaction trust in e-service environments. In *ICEBE 2008*, pages 265–272, 2008.
85. Y. Wang and K.-J. Lin. Reputation-oriented trustworthy computing in e-commerce environments. *IEEE Internet Computing*, 12(4):55–59, 2008.
86. Y. Wang, K.-J. Lin, D. S. Wong, and V. Varadharajan. Trust management towards service-oriented applications. *Service Oriented Computing and Applications*, 3(2):129–146, 2009.
87. Y. Wang and M. P. Singh. Formal trust model for multiagent systems. In *International Joint Conference on Artificial Intelligence (IJCAI 2007)*, pages 1551–1556, 2007.
88. Y. Wang and V. Varadharajan. Role-based recommendation and trust evaluation. In *CEC/EEE 2007*, pages 278–288, 2007.
89. J. Xiao and R. Boutaba. QoS-aware service composition and adaptation in autonomic communication. *IEEE Journal on Selected Areas in Communications*, 23(12):2344–2360, 2005.
90. L. Xiong and L. Liu. PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities. *IEEE Trans. Knowl. Data Eng.*, 16(7):843–857, 2004.
91. Z. Xu, P. Martin, W. Powley, and F. Zulkernine. Reputation-enhanced QoS-based web services discovery. In *ICWS 2007*, pages 249–256, 2007.
92. I. Yaniv. Receiving other peoples' advice: Influence and benefit. *J. Artif. Intell. Res. (JAIR)*, 93(1).
93. B. Yu, M. P. Singh, and K. Sycara. Developing trust in large-scale peer-to-peer systems. *IEEE Symposium on Multi-Agent Security and Survivability*, pages 1–10, 2004.
94. H. Yu, M. Kaminsky, P. B. Gibbons, and A. D. Flaxman. Sybilguard: defending against sybil attacks via social networks. *IEEE/ACM Trans. Netw.*, 16(3):576–589, 2008.
95. T. Yu, Y. Zhang, and K.-J. Lin. Efficient algorithms for web services selection with end-to-end QoS constraints. *TWEB*, 1(1), 2007.
96. G. Zacharia and P. Maes. Trust management through reputation mechanisms. *Applied Artificial Intelligence*, 14(9):881–907, 2000.
97. L. Zeng, B. Benatallah, M. Dumas, J. Kalagnanam, and Q. Z. Sheng. Quality driven web services composition. In *WWW 2003*, pages 411–421, 2003.
98. H. Zhao and X. Li. Vectortrust: Trust vector aggregation scheme for trust management in peer-to-peer networks. In *18th Internatonal Conference on Computer Communications and Networks*, pages 1–6, 2009.
99. R. Zhou and K. Hwang. Powertrust: A robust and scalable reputation system for trusted peer-to-peer computing. *IEEE Trans. Parallel Distrib. Syst.*, 18(4):460–473, 2007.